ユーザーガイド

AWS Security Hub

AWS Security Hub: ユーザーガイド

Table of Contents

AWS Security Hubとは？

AWS Security Hub では、AWS のセキュリティ状態を包括的に把握することが可能で、セキュリティ業界標準およびベストプラクティスに照らした AWS 環境評価を行うのに有効です。

Security Hub は、複数の AWS アカウント、AWS のサービス、およびサポートされているサードパーティパートナー、製品からセキュリティデータを収集して、セキュリティの傾向を分析し、最も優先度の高いセキュリティ問題を特定するのに役立ちます。

組織のセキュリティ状態を管理しやすくするために、Security Hub は複数のセキュリティ標準をサポートしています。これらには、AWS の策定した AWS 基礎セキュリティのベストプラクティス (FSBP) 基準、Center for Internet Security Industry (CIS)、Payment Center for Internet Security Industry Data Security Standard (PCI DSS)、および米国標準技術研究所 (NIST) などの外部コンプライアンスフレームワークなどがあります。セキュリティ標準ごとに複数のセキュリティ管理が含まれており、それぞれがセキュリティのベストプラクティスを表しています。Security Hub はセキュリティコントロールに対するチェックを実行し、コントロールの検出結果を生成して、セキュリティのベストプラクティスに対するコンプライアンス評価をサポートします。

Security Hub は、コントロールの検出結果の生成に加えて、Amazon AWS のサービス、Amazon Inspector GuardDuty、Amazon Macie などの他の およびサポートされているサードパーティー製品からの検出結果も受け取ります。こうして、セキュリティ関連のさまざまな問題を一元的に把握できます。Security Hub の結果を他の AWS のサービス およびサポートされているサードパーティ製品に送信することもできます。

Security Hub には、セキュリティ問題の分類と修正に役立つ自動化機能が備わっています。たとえば、自動化ルールを使用して、セキュリティチェックが失敗した場合に重要な結果を自動的に更新できます。Amazon との統合を活用して EventBridge 、特定の結果への自動応答をトリガーすることもできます。

トピック

Security Hub の利点

Security Hub が複数の AWS 環境にまたがってお客様のコンプライアンスとセキュリティ体制を監視する際に役立つ主な方法をいくつか紹介します。

検出結果の収集と優先順位付けの労力削減

Security Hub は、統合された AWS のサービス および AWS パートナー製品からセキュリティ結果を収集し、複数のアカウント間で優先順位付けする労力を軽減します。Security Hub は、AWS Security Finding 形式 (ASFF) と呼ばれる標準検出結果形式を使用して検出結果を取得します。これにより、無数の情報源からの検出結果を複数の形式で管理する必要がなくなります。また、Security Hub はプロバイダー全体にわたり結果を関連付け、結果を優先順位付けします。

ベストプラクティスと標準に対する自動セキュリティチェック

Security Hub は、AWS のベストプラクティスと業界標準に基づいて、継続的なアカウントレベルの設定とセキュリティチェックを自動的に実行します。Security Hub は、これらのチェックの結果からセキュリティスコアを算出し、注意の必要なアカウントとリソースを特定します。

アカウントとプロバイダーでの結果の統合ビュー

Security Hub は複数のアカウントとプロバイダーの製品間のセキュリティ結果を統合して、Security Hub コンソールに結果を表示します。Security Hub API、AWS CLI、または SDK を通じて結果を取得することもできます。現在のセキュリティ状態を全体的に把握して傾向をとらえ、潜在的な問題を特定し、必要な修復手順を実行することができます。

検出結果の更新と修復を自動化する機能

定義した基準に基づいて結果を変更または抑制する自動化ルールを作成できます。Security Hub は Amazon との統合もサポートしています EventBridge。特定の検出結果の修復を自動化するために、検出結果を生成したときに実行するカスタムアクションを定義できます。たとえば、チケット発行システムや自動修復システムに結果を送信するなどのカスタムアクションを設定できます。

Security Hub へのアクセス

Security Hub はほとんどの AWS リージョン で利用可能です。Security Hub を現在利用できるリージョンのリストについては、「AWS 全般のリファレンス」の「AWS Security Hub エンドポイントとクォータ」を参照してください。AWS アカウント での AWS リージョン の管理について詳しくは、「AWS Account Management リファレンスガイド」の「アカウントで使用できる AWS リージョン を指定する」を参照してください。

各リージョンでは、次のいずれかの方法で Security Hub にアクセスして使用できます。

Security Hub コンソール

AWS Management Console は、AWS リソースの作成と管理に使用できるブラウザベースのインターフェイスです。そのコンソールの一部として、Security Hub コンソールは Security Hub アカウント、データ、およびリソースへのアクセスを提供します。Security Hub コンソールを使用して、結果の表示、自動化ルールの作成、集約リージョンの作成といった Security Hub のタスクを実行できます。

Security Hub API

Security Hub API では、Security Hub のアカウント、データ、およびリソースに対し、プログラムによるアクセスが可能になります。この API を使用すると、HTTPS リクエストを Security Hub に直接送信できます。API の詳細については、「AWS Security Hub API リファレンス」を参照してください。

AWS CLI

AWS CLI を使用すると、システムのコマンドラインでコマンドを実行して Security Hub のタスクを実行できます。場合によっては、コマンドラインを使用した方が、コンソールを使用するよりも高速で便利になります。コマンドラインは、タスクを実行するスクリプトを作成する場合にも便利です。AWS CLI のインストールおよび使用の方法については、AWS Command Line Interface ユーザーガイドを参照してください。

AWS SDK

AWS は、さまざまなプログラミング言語とプラットフォーム (Java、Go、Python、C++、.NET など) のライブラリとサンプルコードで設定される SDK を提供します。SDK を使用すると、優先言語で Security Hub や他の AWS のサービス に対し、便利なプログラムによるアクセスが可能になります。SDK は、暗号署名によるリクエスト、エラーの管理、リクエストの自動再試行などのタスクも処理します。AWS SDK のインストールと使用の詳細については、AWS での構築ツールを参照してください。

Important

Security Hub は、有効にした後に生成された結果のみを検出して統合します。Security Hub を有効化する前に生成されたセキュリティ結果までさかのぼって、検出したり統合したりすることはありません。
Security Hub は、アカウントで有効にしたリージョンでの検出結果のみを受信し、処理します。

CIS AWS Foundations Benchmark セキュリティチェックに完全に準拠するには、サポートされるすべての AWS リージョンで Security Hub を有効にする必要があります。

関連サービス

ご使用の AWS 環境をさらに安全に保護するには、他の AWS のサービス も Security Hub と組み合わせて使用することをお勧めします。

Security Hub の検出結果を送受信するその他の AWS のサービス のリストについては、「AWS のサービスAWS Security Hub との統合」を参照してください。

Security Hub は、ほとんどのコントロールのセキュリティチェックの実行に、AWS Config からのサービスリンクのルールを使用します。Security Hub がコントロールの検出結果のほとんどを生成するには、AWS Config を有効にして、AWS Config にリソースを記録する必要があります。詳細については、「の設定 AWS Config」を参照してください。

Security Hub の無料トライアルと料金

AWS アカウント で初めて Security Hub を有効にすると、そのアカウントは自動的に 30 日間の Security Hub 無料トライアルに登録されます。

無料トライアル期間中に Security Hub を使用する場合、AWS Config アイテムなどの Security Hub がやり取りする他のサービスについては使用量に応じて課金されます。Security Hub セキュリティ標準によってアクティブ化されている AWS Config ルールに対して課金されることはありません。

無料トライアルが終了するまで、Security Hub の使用に対して課金されることはありません。

> **Note**
>
> Security Hub 無料トライアルは、中国 (北京) リージョンではサポートされていません。

使用状況の詳細と見積もりコストの表示

Security Hub は、Security Hub を 30 日間使用した場合の推定コストなどを含んだ、使用状況に関する情報を提供します。使用状況の詳細には、無料トライアルの残り時間が含まれます。使用状況に関する情報から、無料トライアル終了後の Security Hub のコストを容易に理解することができます。使用状況に関する情報は、無料トライアルの終了後にも確認できます。

使用状況に関する情報を (コンソール) に表示するには、以下の手順を実行します。

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。
2. ナビゲーションペインの [設定] で [使用状況] を選択します。

予想される月額コストは、30 日間で推定された、アカウントの Security Hub による結果とセキュリティチェックの使用状況に基づいています。

使用状況情報と推定コストは、現在の アカウントと現在の リージョンについてのみ表示されます。集約リージョンでは、使用情報と見積コストには、リンクされたリージョンは含まれません。リンクされたリージョンの詳細については、「the section called “クロスリージョン集約の仕組み”」を参照してください。

料金詳細

取得した結果とセキュリティチェックに関する Security Hub の課金方法については、「Security Hub の料金」を参照してください。

Security Hub の概念

このトピックでは、サービスの開始に役立つ AWS Security Hub の主要な概念と用語について説明します。

アカウント

AWS リソースを含む標準の Amazon Web Services (AWS) アカウント。アカウント AWS で にサインインし、Security Hub を有効にできます。

アカウントは他のアカウントを招待して、Security Hub を有効にし、Security Hub 内でそのアカウントと関連付けることができます。メンバーシップの招待の承諾はオプションです。招待が承諾されると、アカウントは管理者アカウントになり、追加されたアカウントはメンバーアカウントになります。管理者アカウントは、メンバーアカウントの結果を表示できます。

に登録している場合 AWS Organizations、組織は組織の Security Hub 管理者アカウントを指定します。Security Hub 管理者アカウントは、他の組織アカウントをメンバーアカウントとして有効にできます。

アカウントは、同時に管理アカウントとメンバーアカウントの両方になることはできません。アカウントに付与される管理者アカウントは 1 つだけです。

詳細については、「管理者アカウントおよびメンバーアカウントの管理」を参照してください。

管理者アカウント

Security Hub のアカウントには、関連付けられたメンバーアカウントの結果を表示するためのアクセス権が付与されます。

アカウントには次のいずれかの方法で管理者アカウントが付与されます:

- あるアカウントが他のアカウントを招待し、Security Hub で関連付けられます。このような招待されたアカウントが招待を承諾すると、そのアカウントはメンバーアカウントになり、招待したアカウントは管理者アカウントになります。
- あるアカウントが、組織管理アカウントによって Security Hub 管理者アカウントとして指定されます。Security Hub 管理者アカウントは、任意の組織アカウントをメンバーアカウントとして有効にできます。また、他のアカウントをメンバーアカウントに招待することもできます。

アカウントに付与される管理者アカウントは 1 つだけです。アカウントは、同時に管理アカウントとメンバーアカウントの両方になることはできません。

集約リージョン

集約リージョンを設定すると、複数の のセキュリティ検出結果を 1 つのペイン AWS リージョンに表示できます。

集約リージョンは、結果の表示と管理を行うリージョンです。結果は、リンクされたリージョンから集約リージョンに集約されます。結果の更新は、リージョン全体で複製されます。

集約リージョンでは、[Security standards] (セキュリティ基準)、[Insights] (インサイト)、[Findings] (結果) の各ページに、リンクされたすべてのリージョンの結果が表示されます。

「クロスリージョン集約」を参照してください。

アーカイブ済みの結果

RecordState が ARCHIVED に設定されている結果。結果がアーカイブされる場合、結果プロバイダーでは結果の関連性がなくなったとみなしているということを意味します。レコードの状態には、結果の調査のステータスを追跡するワークフローステータスは含まれません。

結果プロバイダーは、Security Hub API のBatchImportFindings オペレーション を使用して、作成した結果をアーカイブします。Security Hub は、コントロールが無効化された場合、または関連付けられたリソースが削除された場合に、次のいずれかの基準に基づいて、コントロールの結果を自動的にアーカイブします。

- 3〜5日間、結果が更新されていない (これはベストエフォートであり、保証されません)。
- 関連付けられた AWS Config 評価は を返しますNOT_APPLICABLE。

デフォルトでは、アーカイブされた結果は Security Hub コンソールの結果リストから除外されます。アーカイブされた結果を含めるようにフィルターを更新できます。

Security Hub API の GetFindings オペレーションでは、アクティブな結果とアーカイブされた結果の両方が返されます。レコード状態のフィルターを含めることができます。

```
"RecordState": [
    {
        "Comparison": "EQUALS",
        "Value": "ARCHIVED"
    }
],
```

AWS Security Finding 形式 (ASFF)

Security Hub によって集約または生成された結果の内容の標準化された形式。 AWS Security Finding 形式を使用すると、Security Hub を使用して、 AWS セキュリティチェックの実行によってセキュリティサービス、サードパーティーソリューション、または Security Hub 自体によって生成された結果を表示および分析できます。詳細については、「AWS Security Finding 形式 (ASFF)」を参照してください。

コントロール

情報の機密性、完全性、可用性を保護し、定義された一連のセキュリティ要件を満たすように設計された、情報システムまたは組織に対して規定された保護または対策。セキュリティ標準はコントロールのコレクションに関連付けられています。

セキュリティコントロールという用語は、標準全体でコントロール ID とタイトルが 1 つしかないコントロールを指します。標準コントロールという用語は、標準固有のコントロール ID とタイトルを持つコントロールを指します。現在、Security Hub は AWS GovCloud (US) Region と中国リージョンの標準コントロールのみをサポートしています。セキュリティコントロールは、その他すべてのリージョンでサポートされています。

カスタムアクション

選択した結果を に送信するための Security Hub メカニズム EventBridge。カスタムアクションは Security Hub で作成されます。その後、 EventBridge ルールにリンクされます。このルールでは、カスタムアクション ID に関連付けられた結果を受け取ったときに実行する特定のアクションが定義されています。カスタムアクションを使用すると、例えば特定の結果や少数の一連の結果を応答または修復ワークフローに送信できます。詳細については、「the section called “カスタムアクションを作成する (コンソール)”」を参照してください。

委任管理者アカウント (Organizations)

Organizations では、サービスの委任管理者アカウントが組織のサービスの使用を管理できます。

Security Hub では、Security Hub 管理者アカウントが Security Hub の委任管理者アカウントとしての役割も担います。組織管理アカウントによって初めて Security Hub 管理者アカウントが指定されたとき、Security Hub では Organizations を呼び出して、そのアカウントを委任管理者アカウントに指定します。

次に、組織管理アカウントは、すべてのリージョンで Security Hub 管理者アカウントとして委任管理者アカウントを選択する必要があります。

結果

セキュリティチェックまたはセキュリティ関連の検出の監視可能なレコード。Security Hub は、コントロールのセキュリティチェックが完了した後に検出結果を生成します。これらはコントロールの検出結果と呼ばれます。検出結果は、サードパーティ製品の統合から得られる場合もあります。

Security Hub での結果の詳細については、「結果」を参照してください。

> **Note**
>
> 結果は、最新の更新から 90 日後、または更新が行われない場合は作成日から 90 日後に削除されます。検出結果を 90 日以上保存するには、検出結果を Amazon S3 バケットにルーティング EventBridge するルールを で設定できます。 Amazon S3

クロスリージョン集約

結果、インサイト、コントロールコンプライアンスのステータス、セキュリティスコアを、リンクされたリージョンから集約リージョンへ集約。次に、集約リージョンのすべてのデータを表示し、集約リージョンの結果とインサイトを更新できます。

「クロスリージョン集約」を参照してください。

結果の取り込み

他の AWS のサービスやサードパーティーのパートナープロバイダーから Security Hub への検出結果のインポート。

結果取り込みイベントには、新しい結果と既存の結果の更新が含まれます。

インサイト

関連する結果のコレクションで、集約ステートメントとオプションのフィルターによって定義されます。インサイトは、注意と介入が必要なセキュリティ領域を特定します。Security Hub には、変更不能なマネージド (デフォルト) インサイトがいくつか用意されています。カスタム Security Hub インサイトを作成して、 AWS 環境と使用状況に固有のセキュリティ問題を追跡することもできます。詳細については、「インサイト」を参照してください。

リンクされたリージョン

クロスリージョン集約を有効にすると、リンクされたリージョンは、結果、インサイト、コントロールコンプライアンスのステータス、セキュリティスコアを、集約リージョンに集約するリージョンとなります。

リンクされたリージョンでは、[Findings] (結果) および [Insights] (インサイト) ページに、そのリージョンの結果のみが表示されます。

「クロスリージョン集約」を参照してください。

メンバーアカウント

結果を確認してアクションを実行する許可を管理者アカウントに付与したアカウント。

アカウントは次のいずれかの方法でメンバーアカウントになります。

- 別のアカウントからの招待を承諾する。
- 組織アカウントの場合、Security Hub 管理者アカウントによってメンバーアカウントとして有効にされる。

関連する要件

コントロールにマッピングされる一連の業界または規制要件。

ルール

コントロールが遵守されているかどうかを評価するために使用される一連の自動条件。ルールは、評価されると、合格または不合格が指定されます。ルールは、評価によって合格または不合格を特定できなかった場合、警告状態になります。ルールを評価できない場合、そのルールは使用不可の状態になります。

セキュリティチェック

、、、WARNINGまたは NOT_AVAILABLE状態になる 1 つのリソースに対するルールPASSEDFAILEDの特定 point-in-time の評価。セキュリティチェックを実行すると、結果が生成されます。

Security Hub 管理者アカウント

組織の Security Hub メンバーシップを管理する組織アカウント。

組織管理アカウントが各リージョンの Security Hub 管理者アカウントを指定します。組織管理アカウントは、すべてのリージョンで同じ Security Hub 管理者アカウントを選択する必要があります。

Security Hub 管理者アカウントは、Organizations 内の Security Hub の委任管理者アカウントでもあります。

Security Hub 管理者アカウントは、任意の組織アカウントをメンバーアカウントとして有効にできます。また、他のアカウントをメンバーアカウントに招待することもできます。

セキュリティ標準

特性を指定するトピックについてパブリッシュされたステートメント。通常は測定可能で、コントロールの形式であり、コンプライアンスを満たしているか、達成している必要があります。セキュリティ標準は規制の枠組みや、ベストプラクティス、社内のポリシーなどに基づいています。コントロールは、Security Hub でサポートされている 1 つ以上の標準に関連付けることができます。Security Hub のセキュリティ標準の詳細については、「標準とコントロール」を参照してください。

重要度

Security Hub コントロールに割り当てられる重要度は、コントロールの重要性を特定します。コントロールの重要度は、[Critical] (重要)、[High] (高)、[Medium] (中)、[Low] (低) または [Informational] (情報) のいずれかです。コントロールの結果に割り当てられる重要度は、そのコントロール自体の重要度と同等です。Security Hub でコントロールに重要度を割り当てる方法については、「コントロール結果への重要度の割り当て」を参照してください。

ワークフローステータス

結果の調査ステータス。`Workflow.Status` 属性を使用して追跡します。

ワークフローステータスは、初期状態では `NEW` です。リソース所有者に結果に対するアクションを実行するように通知した場合は、ワークフローステータスを `NOTIFIED` に設定できます。結果に問題がなく、アクションが不要な場合は、ワークフローステータスを `SUPPRESSED` に設定します。結果を確認して修正したら、ワークフローステータスを `RESOLVED` に設定します。

デフォルトでは、ほとんどの結果リストに含まれている結果のワークフローステータスは、`NEW` または `NOTIFIED` のみです。コントロールの結果リストには、ステータスが `RESOLVED` の結果も含まれます。

`GetFindings` オペレーションでは、ワークフローステータスのフィルターを含めることができます。

```
"WorkflowStatus": [
    {
        "Comparison": "EQUALS",
```

```
        "Value": "RESOLVED"
    }
],
```

Security Hub コンソールには、結果のワークフローステータスを設定するオプションがあります。お客様 (または結果プロバイダーの結果をお客様に代わって更新する SIEM、チケット発行、インシデント管理、または SOAR ツール) は、`BatchUpdateFindings` を使用してワークフローステータスを更新することもできます。

Security Hub を有効にする前の推奨事項

以下の推奨事項は、 の使用を開始するのに役立ちます AWS Security Hub。

との統合 AWS Organizations

AWS Organizations は、 AWS 管理者が複数の および AWS アカウント 組織単位 (OUs。予算、セキュリティ、コンプライアンスのニーズをサポートするように設計されたアカウント管理および一括請求 (コンソリデーティッドビリング) 機能が備わっています。追加料金なしで提供され、Security Hub AWS のサービス、Amazon 、Amazon Macie などの複数の GuardDutyと統合されます。

アカウントの管理を自動化および合理化するために、Security Hub と AWS Organizationsを統合することを強く推奨しています。Security Hub を使用する複数の がある場合は AWS アカウント 、Organizations と統合できます。

統合を有効にする手順については、「Security Hub と の統合 AWS Organizations」をご参照ください。

中央設定の使用

Security Hub と Organizations を統合すると、中央設定と呼ばれる機能を使用して組織の Security Hub を設定および管理できます。管理者が組織のセキュリティ範囲をカスタマイズできるため、中央設定を使用することを強くお勧めします。必要に応じて、委任管理者はメンバーアカウントによる独自のセキュリティカバレッジの設定を許可できます。

中央設定を使用すると、委任管理者はアカウント、OUs、および 全体で Security Hub を設定できます AWS リージョン。委任管理者は、設定ポリシーを作成して Security Hub を設定します。設定ポリシー内では、以下の設定を指定できます。

- Security Hub が有効か無効か
- どのセキュリティ基準を有効または無効にするか
- どのセキュリティコントロールを有効または無効にするか
- コントロール選択用のパラメータをカスタマイズするかどうか

委任管理者は、組織全体を対象とする単一の設定ポリシーを作成することも、さまざまなアカウントや OU に異なる設定ポリシーを作成することもできます。例えば、テストアカウントと本稼働アカウントでは異なる設定ポリシーを使用できます。

設定ポリシーを使用するメンバーアカウントと OU は一元管理され、委任管理者のみが設定できます。委任管理者は、特定のメンバーアカウントと OU をセルフマネージド型として指定して、メンバーがリージョン単位で独自の設定を行えるようにすることができます。

中央設定の詳細については、「中央設定の仕組み」を参照してください。

の設定 AWS Config

AWS Security Hub は、サービスにリンクされた AWS Config ルールを使用して、ほとんどのコントロールのセキュリティチェックを実行します。

これらのコントロールをサポートする AWS Config には、 AWS リージョン Security Hub が有効になっている各 で、管理者アカウントとメンバーアカウントの両方を含むすべてのアカウントで を有効にする必要があります。さらに、有効な標準ごとに、有効なコントロールに必要なリソースを記録するように設定 AWS Config する必要があります。

Security Hub 標準を有効にする AWS Config 前に、 でリソース記録を有効にすることをお勧めします。リソース記録が有効になっていないときに Security Hub がセキュリティチェックを実行しようとすると、チェックはエラーを返します。

Security Hub はお客様 AWS Config に代わって管理しません。既に AWS Config を有効にしている場合は、 AWS Config コンソールまたは APIsを使用して設定を行うことができます。

標準を有効にしているが、 を有効にしていない場合 AWS Config、Security Hub は次のスケジュールに従って AWS Config ルールを作成しようとします。

- 標準を有効にした当日
- 標準を有効にした翌日
- 標準を有効にしてから 3 日後
- 標準を有効にしてから 7 日後 (その後は 7 日ごとに継続的に)

中央設定を使用する場合、Security Hub は、1 つ以上の標準を有効にする設定ポリシーを再適用するときに AWS Config ルールの作成も試みます。

の有効化 AWS Config

AWS Config をまだ有効にしていない場合は、次のいずれかの方法で有効にできます。

- コンソールまたは AWS CLI - AWS Config コンソールまたは AWS Config を使用して手動で を有効にできます AWS CLI。「AWS Config 開発者ガイド」の「AWS Configの開始方法」を参照してください。
- AWS CloudFormation template – 多数のアカウント AWS Config で を有効にする場合は、CloudFormation テンプレート Enable AWS Config を使用して を有効に AWS Configできます。このテンプレートにアクセスするには、「 ユーザーガイド」のAWS CloudFormation StackSets 「サンプルテンプレートAWS CloudFormation 」を参照してください。
- Github スクリプト – Security Hub は、リージョン間で複数のアカウントに対して Security Hub を有効にするGitHub スクリプトを提供します。このスクリプトは、Organizations と統合していない場合、あるいは、自分の組織に属さないアカウントがある場合などに有用です。このスクリプトを使用して Security Hub を有効にすると、これらのアカウント AWS Config に対しても自動的に が有効になります。

AWS Config を有効にして Security Hub セキュリティチェックを実行する方法の詳細については、「の最適化 AWS Security HubAWS Config 」を参照してクラウドセキュリティ体制を効果的に管理してください。

でリソース記録を有効にする AWS Config

でリソース記録をデフォルト設定 AWS Config で有効にすると、実行中の で AWS リージョン が AWS Config 検出した、サポートされているすべてのタイプのリージョンリソースが記録されます。また、 を設定 AWS Config して、サポートされているタイプのグローバルリソース を記録することもできます。グローバルリソースは 1 つのリージョンに記録するだけで済みます (中央設定を使用している場合は、これをホームリージョンにすることをお勧めします)。

CloudFormation StackSets を使用して を有効にする場合は AWS Config、2 つの異なる を実行することをお勧めします StackSets。1 つのリージョンでグローバルリソースを含むすべてのリソースを記録する StackSet には、1 つを実行します。1 秒実行 StackSet して、他のリージョンのグローバルリソースを除くすべてのリソースを記録します。

の一機能である高速セットアップを使用して、アカウントとリージョン AWS Config 全体で でリソース記録 AWS Systems Managerをすばやく設定することもできます。Quick Setup の最中に、グローバルリソースを記録するリージョンを選択できます。詳細については、AWS Systems Manager ユーザーガイドの「AWS Config 設定レコーダー」を参照してください。

セキュリティコントロール Config.1 は、アグリゲータ内のリンクされたリージョン以外のリージョン (ホームリージョンと、検出結果アグリゲータにまったくないリージョン) について、そのリー

ジョンが (IAM) グローバルリソースを記録 AWS Identity and Access Management せず、IAM グローバルリソースの記録を必要とするコントロールを有効にしている場合、失敗した検出結果を生成します。リンクされたリージョンでは、Config.1 は IAM グローバルリソースが記録されているかどうかをチェックしません。各コントロールに必要なリソースのリストについては、「」を参照してくださいAWS Config コントロールの検出結果を生成するために必要な リソース。

なお、マルチアカウントスクリプトを使用して Security Hub を有効にした場合、グローバルリソースを含むすべてのリソースのリソース記録が、すべてのリージョンで自動的に有効になることにご注意ください。その後、単一のリージョンのみでグローバルリソースを記録するように設定を更新できます。詳細については、「 AWS Config デベロッパーガイド」の「 AWS Config リソースレコードの選択」を参照してください。

Security Hub が AWS Config ルールに依存するコントロールの検出結果を正確にレポートするには、関連するリソースの記録を有効にする必要があります。コントロールとその関連 AWS Config リソースのリストについては、「継続的な記録とリソースの状態の変化の毎日の記録の中から選択したAWS Config コントロールの検出結果を生成するために必要な リソース.AWS Config lets」を参照してください。毎日記録することを選択した場合、 AWS Config は、リソースの状態に変化があったとき、各 24 時間の最後にリソース設定データを配信します。変化がなければ、データは配信されません。そのため、変更によってトリガーされるコントロールに関する Security Hub の検出結果の生成が 24 時間周期の終了まで遅れる可能性があります。

> **Note**
>
> セキュリティチェック後に新しい結果を生成して古い結果にならないようにするには、構成レコーダーにアタッチされた IAM ロールに基盤となるリソースを評価するための十分な許可が必要です。

コストに関する考慮事項

リソースの記録に関連するコストの詳細については、「AWS Security Hub の料金」と「AWS Config の料金」を参照してください。

Security Hub は、 AWS Config 設定項目を更新することで、`AWS::Config::ResourceCompliance`設定レコーダーのコストに影響を与える可能性があります。更新は、 AWS Config ルールに関連付けられた Security Hub コントロールがコンプライアンス状態を変更する、有効または無効になる、またはパラメータが更新されるたびに発生する可能性があります。Security Hub にのみ AWS Config 設定レコーダーを使用し、他の目的でこの設定項目

を使用しない場合は、 AWS Config コンソールまたは で記録をオフにすることをお勧めします AWS CLI。これにより、 AWS Config コストを削減できます。Security Hub でセキュリティチェックを行うために AWS::Config::ResourceCompliance を記録する必要はありません。

Security Hub を有効にする

AWS Security Hub を有効にする場合、AWS Organizations と統合する方法と、手動で行う方法があります。

マルチアカウントおよびマルチリージョン環境では、Organizations との統合を強くお勧めします。スタンドアロンアカウントをお持ちの場合は、Security Hub を手動で設定する必要があります。

必要なアクセス許可を確認する

Amazon Web Services (AWS) にサインアップしたら、Security Hub を有効にして、その機能を使用する必要があります。Security Hub を有効にするには、まず Security Hub コンソールと API オペレーションへのアクセスを可能にするアクセス許可を設定する必要があります。これは、AWS Identity and Access Management (IAM) を使用して自分の IAM アイデンティティに `AWSSecurityHubFullAccess` という名前の AWS 管理ポリシーをアタッチすることで、自分でまたは AWS 管理者が実行できます。

Organizations 統合を使用して Security Hub を有効にして管理するには、`AWSSecurityHubOrganizationsAccess` という名前の AWS 管理ポリシーもアタッチする必要があります。

詳細については、「AWSAWS Security Hub の マネージドポリシー」を参照してください。

Security Hub と Organizations との統合を有効にする

AWS Organizations を使用して Amazon Hub の使用を開始するには、組織の AWS Organizations 管理アカウントで組織の Security Hub 委任管理者アカウントとしてのアカウントを指定します。Security Hub は、現在のリージョンの委任管理者アカウントで自動的に有効になります。

ご希望の方法を選択し、手順に従って委任管理者を指定します。

Security Hub console

オンボーディング時に Security Hub 委任管理者を指定するには

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。
2. [Go to Security Hub] (Security Hub に移動) を選択します。組織の管理アカウントにサインインするよう求めるメッセージが表示されます。

3. [委任された管理者アカウント] セクションの [委任された管理者を指定] ページで、委任された管理者アカウントを指定します。委任された管理者には、他の AWS セキュリティおよびコンプライアンスサービスと同一の設定を選択することをお勧めします。
4. [委任された管理者を設定] を選択します。

Security Hub API

Organizations 管理アカウントから `EnableOrganizationAdminAccount` API を呼び出します。Security Hub の委任された管理者アカウントの AWS アカウント ID を指定します。

AWS CLI

Organizations 管理アカウントから `enable-organization-admin-account` コマンドを実行します。Security Hub の委任された管理者アカウントの AWS アカウント ID を指定します。

コマンドの例:

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

Organizations との統合の詳細については、「Security Hub と の統合 AWS Organizations」を参照してください。

委任管理者を指定した後は、中央設定を使用して、引き続き Security Hub の設定を行うことをお勧めします。コンソールにそのように求めるプロンプトが表示されます。中央設定を使用することにより、組織の Security Hub を有効化および設定するプロセスを簡素化し、組織のセキュリティを十分に確保できます。

中央設定により、委任された管理者は Security Hub をリージョンごとに設定するのではなく、複数の組織アカウントとリージョンにわたってカスタマイズできます。組織全体の設定ポリシーを作成することも、アカウントや OU ごとに異なる設定ポリシーを作成することもできます。ポリシーでは、関連するアカウントで Security Hub を有効にするか無効にするか、およびどのセキュリティ標準とコントロールを有効にするかを指定します。

委任された管理者は、アカウントを一元管理型またはセルフマネージド型として指定できます。一元管理型アカウントは、委任された管理者のみが設定できます。セルフマネージド型アカウントは、独自の設定を指定できます。

中央設定を使用しない場合、委任管理者が Security Hub を設定する機能が制限されます。詳細については、「によるアカウントの管理 AWS Organizations」を参照してください。

Security Hub を手動で有効にする

スタンドアロンアカウントをお持ちの場合、または AWS Organizations と統合しない場合は、Security Hub を手動で有効にする必要があります。スタンドアロンアカウントは AWS Organizations と統合できないため、手動で有効化する必要があります。

Security Hub を手動で有効にする場合は、Security Hub 管理者アカウントを指定し、他のアカウントを招待してメンバーアカウントにします。管理者とメンバーの関係は、メンバーアカウント候補が招待を受け入れたときに確立されます。

ご希望の方法を選択し、手順に従って Security Hub を有効にします。コンソールから Security Hub を有効にする場合は、サポートされているセキュリティ標準を有効にするオプションも提供されています。

Security Hub console

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。
2. Security Hub コンソールを初めて開く場合は、[Security Hub に移動] を選択します。
3. ウェルカムページには、Security Hub がサポートするセキュリティ基準が [セキュリティ基準] セクションに一覧表示されます。

   基準のチェックボックスを選択して有効にします。チェックボックスをオフにすると無効になります。

   標準またはその個々のコントロールは、いつでも有効または無効にできます。セキュリティ基準とコントロールの管理については、「Security controls and standards in AWS Security Hub」を参照してください。
4. [Enable Security Hub] (Security Hub の有効化) を選択します。

Security Hub API

`EnableSecurityHub` API を呼び出します。API から Security Hub を有効にすると、以下のデフォルトのセキュリティ基準が自動的に有効になります。

- AWS Foundational Security Best Practices
- Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0

これらの標準を有効にしない場合は、`EnableDefaultStandards` を `false` に設定します。

また Tags パラメータを使用して、ハブリソースにタグ値を割り当てることもできます。

AWS CLI

enable-security-hub コマンドを実行します。デフォルトの標準を有効にするには、--enable-default-standards を含めます。デフォルトの標準を有効にしない場合は、--no-enable-default-standards を含めます。デフォルトのセキュリティ基準は次のとおりです。

- AWS Foundational Security Best Practices
- Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-
standards | --no-enable-default-standards]
```

例

```
aws securityhub enable-security-hub --enable-default-standards --tags
 '{"Department": "Security"}'
```

マルチアカウント有効化スクリプト

> **Note**
>
> このスクリプトの代わりに、中央設定を使用して複数のアカウントとリージョンで Security Hub を有効にして設定することをお勧めします。

GitHub の Security Hub マルチアカウント有効化スクリプトでは、複数のアカウントやリージョンの Security Hub の有効化が許可されています。スクリプトを使用することで、メンバーアカウントへの招待の送信と AWS Config の有効化のプロセスも自動化されます。

このスクリプトは、グローバルリソースを含むすべてのリソースのリソースレコーディングを、すべてのリージョンで自動的に有効にします。グローバルリソースの記録を 1 つのリージョンに制限するものではありません。

複数のアカウントとリージョンで Security Hub を無効にするための、対応するスクリプトがあります。

Security Hub を有効にした後の手順

Security Hub を有効にしたら、セキュリティへの対応で重要なセキュリティ基準とセキュリティコントロールを有効にすることをお勧めします。コントロールを有効にすると、Security Hub はセキュリティチェックの実行とコントロール検出結果の生成を開始します。Security Hub と他の AWS のサービスやサードパーティーのソリューションとの統合を活用して、Security Hub でその検出結果を確認することもできます。

中央設定の仕組み

中央設定は、複数の AWS アカウント および AWS リージョンにわたって Security Hub を設定し、管理する際に役立つ Security Hub の機能です。中央設定を使用するには、まず Security Hub と を統合する必要があります AWS Organizations。組織を作成し、組織に対して委任された Security Hub 管理者アカウントを指定することで、サービスを統合できます。

委任された Security Hub 管理者アカウントで、Security Hub サービス、セキュリティ標準、およびセキュリティコントロールを複数のリージョンの組織アカウントと組織単位 (OU) で設定する方法を指定できます。これらの設定は、ホームリージョンと呼ばれる 1 つのプライマリリージョンから、わずか数ステップで設定できます。中央設定を使用しない場合は、各アカウントとリージョンで個別に Security Hub を設定する必要があります。

中央設定を使用する場合、委任された管理者が設定するアカウントと OU を選択できます。委任された管理者がメンバーアカウントまたは OU をセルフマネージド型に指定した場合、メンバーは各リージョンで独自の設定を個別に構成できます。委任された管理者がメンバーアカウントまたは OU を一元管理型に指定した場合、委任された管理者のみが複数のリージョンにわたってメンバーアカウントまたは OU を設定できます。組織内のすべてのアカウントと OU を、一元管理型、すべてセルフマネージド型、または両方の組み合わせとして指定できます。

一元管理型アカウントを設定するには、委任された管理者が Security Hub の設定ポリシーを使用します。設定ポリシーにより、委任された管理者は Security Hub を有効にするか無効にするか、またどの標準とコントロールを有効または無効にするかを指定できます。またこのポリシーを使用して、特定のコントロールのパラメータをカスタマイズすることもできます。

設定ポリシーは、ホームリージョンとリンクされたすべてのリージョンで有効になります。委任された管理者は、中央設定の使用を開始する前に、組織のホームリージョンとリンクされたリージョンを指定します。委任された管理者は、組織全体に単一の設定ポリシーを作成することも、複数の設定ポリシーを作成してさまざまなアカウントや OU の変数設定を行うこともできます。

このセクションでは、中央設定の概要について説明します。

中央設定の利点

中央設定には、次のような利点があります。

Security Hub サービスと機能の設定を簡素化する

中央設定を使用する場合、Security Hub によって組織のセキュリティ上のベストプラクティスを設定するプロセスに誘導されます。また、作成された設定ポリシーは、指定したアカウントと OU に自動的にデプロイされます。新しいセキュリティコントロールを自動的に有効にするなど、Security Hub の既存の設定がある場合は、それらの設定を設定ポリシーの開始点として使用できます。さらに、Security Hub コンソールの [設定] ページには、設定ポリシーの概要と、各ポリシーを使用するアカウントおよび OU がリアルタイムで表示されます。

複数のアカウントやリージョンにまたがる設定

中央設定を使用すると、Security Hub を複数のアカウントとリージョンにまたがって設定を行うことができます。これにより、組織の各部署で一貫した設定と適切なセキュリティ対策が確保されます。

さまざまなアカウントや OU で異なる設定に対応

中央設定により、組織のアカウントと OU をさまざまな方法で設定できます。例えば、テストアカウントと本稼働アカウントでは異なる設定が必要になる場合があります。組織に追加する際に新しいアカウントを対象とする設定ポリシーを作成することもできます。

設定のずれを防ぐ

設定のずれは、サービスや機能に対してユーザーが行った変更が、委任された管理者が行った選択と競合する場合に発生します。中央設定によりこのずれを防止します。アカウントまたは OU を一元管理型として指定する場合に設定できるのは、組織の委任管理者のみです。特定のアカウントや OU で独自の設定を行う場合は、セルフマネージド型に指定できます。

中央設定を使用する必要のあるユーザー

中央設定は、複数の Security Hub アカウントを含む AWS 環境に最適です。複数のアカウントに対して Security Hub を一元管理できるように設計されています。

中央設定を使用して、Security Hub サービス、セキュリティ標準、およびセキュリティコントロールを設定できます。また、この設定を使用して特定のコントロールのパラメータをカスタマイズすることもできます。標準とコントロールについては、「AWS Security Hub のセキュリティコントロールと標準」を参照してください。

中央設定に関する用語と概念

以下の主要な用語と概念を理解しておくと、Security Hub の中央設定を使用する際に役立ちます。

中央設定

組織に対して委任された Security Hub 管理者アカウントが、複数のアカウントとリージョンにわたって Security Hub サービス、セキュリティ標準、およびセキュリティコントロールを設定する際に役立つ、Security Hub の機能。これらの設定を行うには、委任された管理者が組織内の一元管理型アカウントに対して Security Hub 設定ポリシーを作成し、管理します。セルフマネージド型アカウントは、リージョンごとに独自の設定を個別に行うことができます。中央設定を使用するには、Security Hub と を統合する必要があります AWS Organizations。

ホームリージョン

設定ポリシーを作成および管理することで、 AWS リージョン 委任管理者が Security Hub を一元的に設定する 。設定ポリシーは、ホームリージョンとリンクされたすべてのリージョンで有効になります。

ホームリージョンは、リンクされたリージョンから検出結果、インサイト、その他のデータを受け取る Security Hub 集約リージョンとしても機能します。

2019 年 3 月 20 日以降に AWS 導入されたリージョンは、オプトインリージョンと呼ばれます。オプトインリージョンをホームリージョンにすることはできませんが、リンクされたリージョンにすることはできます。オプトインリージョンのリストについては、「AWS アカウント管理リファレンスガイド」の「Considerations before enabling and disabling Regions」を参照してください。

リンクされたリージョン

ホームリージョンから設定 AWS リージョン 可能な 。設定ポリシーは、ホームリージョンの委任管理者によって作成されます。ポリシーは、ホームリージョンとリンクされたすべてのリージョンで有効になります。中央設定を使用するには、リンクされたリージョンを少なくとも 1 つ指定する必要があります。

また、リンクされたリージョンによって、検出結果、インサイト、その他のデータがホームリージョンに送信されます。

2019 年 3 月 20 日以降に AWS 導入されたリージョンは、オプトインリージョンと呼ばれます。設定ポリシーを適用する前に、そのようなリージョンをアカウントで有効にする必要がありま

す。Organizations 管理アカウントでは、メンバーアカウントのオプトインリージョンを有効にできます。詳細については、「AWS リージョン アカウント管理リファレンスガイド」の「アカウントで使用できる を指定する」を参照してください。 AWS

Security Hub の設定ポリシー

委任された管理者が一元管理型アカウントに設定できる Security Hub 設定のコレクション。これには、以下が含まれます。

- Security Hub を有効または無効にするかどうか。
- 1 つ以上のセキュリティ標準を有効にするかどうか。
- 有効になっている標準でどのセキュリティコントロールを有効にするか。委任された管理者は、有効にする必要のある特定のコントロールのリストを指定することでこれを実行できます。Security Hub によって、リリース時の新しいコントロールを含め、他のすべてのコントロールが無効になります。または、委任された管理者が無効にする必要のある特定のコントロールのリストを指定し、Security Hub でリリース時の新しいコントロールを含め、他のすべてのコントロールを有効にすることもできます。
- オプションで、有効な複数の標準で有効になっているコントロールを選択してパラメータをカスタマイズできます。

設定ポリシーは、少なくとも 1 つのアカウント、組織単位 (OU)、またはルートに関連付けられると、ホームリージョンとリンクされたすべてのリージョンで有効になります。

Security Hub コンソールでは、委任された管理者が Security Hub 推奨設定ポリシーを選択するか、カスタム設定ポリシーを作成できます。Security Hub API と では AWS CLI、委任管理者はカスタム設定ポリシーのみを作成できます。委任された管理者は、最大 20 のカスタム設定ポリシーを作成できます。

推奨される設定ポリシーでは、Security Hub、 AWS の基本的なセキュリティのベストプラクティス (FSBP) 標準、すべての既存および新規の FSBP コントロールが有効になっています。パラメータを受け入れるコントロールは、デフォルト値を使用します。推奨される設定ポリシーは、組織全体に適用されます。

組織に異なる設定を適用したり、異なるアカウントや OU に異なる設定ポリシーを適用したりするには、カスタム設定ポリシーを作成します。

ローカル設定

Security Hub と を統合した後の、組織のデフォルトの設定タイプ AWS Organizations。ローカル設定では、委任された管理者が、現在のリージョンの新しい組織アカウントで Security Hub とデ

フォルトのセキュリティ標準を自動的に有効にするよう選択できます。委任された管理者がデフォルトの標準を自動的に有効にすると、これらの標準に含まれるすべてのコントロールも、新しい組織アカウントのデフォルトパラメータを使用して自動的に有効になります。これらの設定は既存のアカウントには適用されないため、アカウントを組織に追加した後に設定のずれが生じる可能性があります。デフォルトの標準に含まれる特定のコントロールの無効化、および追加の標準とコントロールの設定は、アカウントやリージョンごとに個別に行う必要があります。

ローカル設定では、設定ポリシーの使用がサポートされていません。設定ポリシーを使用するには、中央設定に切り替える必要があります。

手動アカウント管理

Security Hub を と統合していない場合、 AWS Organizations またはスタンドアロンアカウントがある場合は、各リージョンで各アカウントの設定を個別に指定する必要があります。手動によるアカウント管理では、設定ポリシーの使用がサポートされていません。

中央設定 API

一元管理型アカウントの設定ポリシーを管理するために Security Hub の委任された Security Hub 管理者のみがホームリージョンで使用する Security Hub オペレーション。オペレーションは次のとおりです。

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

アカウント固有の API

Security Hub、標準、およびコントロールを account-by-account ベースで有効または無効にするために使用できる Security Hub オペレーション。これらのオペレーションは、個々のリージョンで使用されます。

セルフマネージド型アカウントは、アカウント固有のオペレーションを使用して独自の設定を行うことができます。一元管理型アカウントは、ホームリージョンとリンクされたリージョンでは以下のアカウント固有のオペレーションを使用することができません。これらのリージョンで中央設定オペレーションと設定ポリシーによって一元管理型アカウントを設定できるのは、委任された管理者のみです。

- `BatchDisableStandards`
- `BatchEnableStandards`
- `BatchUpdateStandardsControlAssociations`
- `DisableSecurityHub`
- `EnableSecurityHub`
- `UpdateStandardsControl`

アカウントのステータスをチェックするために、一元管理されたアカウントの所有者は Security Hub API の `Get`または `Describe`オペレーションを使用できます。

中央設定の代わりにローカル設定または手動アカウント管理を使用する場合は、これらのアカウント固有のオペレーションを使用できます。

セルフマネージド型アカウントは、 `*Invitations`および `*Members`オペレーションを使用することもできます。ただし、セルフマネージド型アカウントはこれらのオペレーションを使用しないことをお勧めします。委任された管理者の組織とは異なる組織に属するメンバーがメンバーアカウントにある場合、ポリシーの関連付けが失敗する可能性があります。

組織単位 (OU)

AWS Organizations および Security Hub では、 のグループのコンテナ AWS アカウント。また、組織単位 (OU) は他の OU に含めることもでき、上下反転したツリーのような階層を作成できます。最上部には親 OU があり、下に向かって OU の枝が広がり、先端にはツリーの葉であるアカウントがあります。OU は、厳密に親を 1 つ持つことができ、各組織アカウントを厳密に 1 つの OU のメンバーにすることができます。

OUs は AWS Organizations または で管理できます AWS Control Tower。詳細については、「AWS Organizations ユーザーガイド」の「組織単位の管理」または「AWS Control Tower ユーザーガイド」の「AWS Control Towerで組織とアカウントを管理する」を参照してください。

委任された管理者は、設定ポリシーを特定のアカウントや OU に関連付けたり、組織内のすべてのアカウントや OU を対象とするルートに関連付けたりできます。

一元管理型

委任された管理者のみが設定ポリシーを使用して複数のリージョンにわたり設定できるアカウント、OU、またはルート。

委任された管理者アカウントで、アカウントが一元管理型かどうかを指定します。委任された管理者は、アカウントのステータスを一元管理型からセルフマネージド型に、またはその逆に変更することもできます。

セルフマネージド型

独自の Security Hub 設定を管理するアカウント、OU、またはルート。セルフマネージド型アカウントは、アカウント固有のオペレーションを使用して、各リージョンで個別に Security Hub を設定します。これとは対照的に、一元管理型アカウントは、設定ポリシーによって複数のリージョンにわたり委任された管理者のみが設定できます。

委任された管理者アカウントで、アカウントがセルフマネージド型かどうかを指定します。委任された管理者アカウントは、アカウントのステータスをセルフマネージド型から一元管理型に、またはその逆に変更することもできます。

委任された管理者は、アカウントまたは OU にセルフマネージド型の動作を適用できます。また、アカウントや OU は親からセルフマネージド型の動作を継承することもできます。委任された管理者アカウント自体をセルフマネージド型アカウントにすることもできます。

設定ポリシーの関連付け

設定ポリシーとアカウント、組織単位 (OU)、またはルートとの間のリンク。ポリシーが関連付けられている場合、アカウント、OU、またはルートでは設定ポリシーで定義された設定を使用します。関連付けは次のいずれかの場合に発生します。

- 委任された管理者が設定ポリシーをアカウント、OU、またはルートに直接適用する場合
- アカウントまたは OU が親 OU またはルートから設定ポリシーを継承する場合

関連付けは、別の設定が適用または継承されるまで発生します。

適用された設定ポリシー

委任された管理者が設定ポリシーをターゲットアカウント、OU、またはルートに直接適用する、設定ポリシーの関連付けタイプ。ターゲットは設定ポリシーで定義されている方法で設定され、委任された管理者のみが設定を変更できます。ルートに適用した場合、設定ポリシーは、アプリケーションまたは最も近い親からの継承によって異なる設定を使用していない、組織内のすべてのアカウントと OU に影響します。

委任された管理者は、特定のアカウント、OU、またはルートにセルフマネージド型の設定を適用することもできます。

継承された設定ポリシー

アカウントまたは OU が最も近い親 OU またはルートの設定を採用する、設定ポリシーの関連付けタイプ。設定ポリシーがアカウントや OU に直接適用されない場合、最も近い親 OU の設定が継承されます。ポリシーのすべての要素は継承されます。つまり、アカウントや OU はポリシーの一部だけを選択的に継承することはできません。最も近い親がセルフマネージド型の場合、子アカウントまたは OU は親のセルフマネージド型の動作を継承します。

継承によって適用された設定を上書きすることはできません。つまり、設定ポリシーまたはセルフマネージド型の設定がアカウントまたは OU に直接適用された場合、その設定が使用され、親の設定は継承されません。

ルート

AWS Organizations および Security Hub では、組織の最上位親ノード。委任された管理者が設定ポリシーをルートに適用すると、そのポリシーは組織内のすべてのアカウントと OU に関連付けられます。ただし、アプリケーションまたは継承によって別のポリシーが使用されている場合や、セルフマネージド型として指定されている場合は除きます。管理者がルートをセルフマネージド型として指定した場合、アプリケーションまたは継承で設定ポリシーを使用する場合を除き、組織内のすべてのアカウントと OU はセルフマネージド型になります。ルートがセルフマネージド型で、現在設定ポリシーが存在しない場合、組織内のすべての新規アカウントで現在の設定が保持されます。

組織に追加した新しいアカウントは、特定の OU に割り当てられるまではルートに属します。新しいアカウントが OU に割り当てられない場合、委任された管理者がセルフマネージド型アカウントとして指定しない限り、そのアカウントはルート設定を継承します。

中央設定の使用を開始する

AWS Security Hub 委任管理者アカウントは、中央設定を使用して、複数のアカウントや組織単位 (OU) の Security Hub、標準、およびコントロールを AWS リージョンで設定できます。

このセクションでは、中央設定の前提条件と使用開始方法について説明します。

中央設定の前提条件

中央設定の使用を開始する前に、Security Hub と AWS Organizations を統合し、ホームリージョンを指定する必要があります。Security Hub コンソールを使用する場合、これらの前提条件は中央設定のオプトインワークフローに含まれています。

Organizations との統合

中央設定を使用するには、Security Hub と Organizations を統合する必要があります。

これらのサービスを統合するには、まず Organizations で組織を作成します。次に Organizations 管理アカウントから Security Hub 委任管理者アカウントを指定します。手順については、「Security Hub と の統合 AWS Organizations」を参照してください。

必ず、目的のホームリージョンで委任管理者を指定してください。中央設定の使用を開始すると、すべてのリンクされたリージョンにも同じ委任管理者が自動的に設定されます。Organizations 管理アカウントは、委任管理者アカウントとして設定することはできません。

> **Important**
>
> 中央設定を使用する場合、Security Hub コンソールまたは Security Hub API を使用して委任された管理者アカウントを変更または削除することはできません。Organizations 管理アカウントが AWS Organizations API を使用して Security Hub 委任管理者を変更または削除すると、Security Hub は自動的に中央設定を停止します。設定ポリシーの関連付けも解除され、削除されます。メンバーアカウントには、委任管理者が変更または削除される前の設定が保持されます。

ホームリージョンの指定

中央設定を使用するにはホームリージョンを指定する必要があります。ホームリージョンは、委任管理者が組織を設定するリージョンです。

中央設定を使用するには、ホームリージョンから設定可能なリンクされたリージョンを少なくとも 1 つ指定する必要があります。

> **Note**
>
> ホームリージョンは、AWS でオプトインリージョンとして指定されているリージョンにすることはできません。オプトインリージョンは、デフォルトでは無効となっています。オ

プトインリージョンのリストについては、「AWS アカウント管理リファレンスガイド」の「Considerations before enabling and disabling Regions」を参照してください。

委任管理者は、ホームリージョンからのみ設定ポリシーを作成および管理できます。設定ポリシーは、ホームリージョンとリンクされたすべてのリージョンで有効になります。これらのリージョンのサブセットにのみ適用され、他のリージョンには適用されない設定ポリシーは作成できません。

ホームリージョンは、リンクされたリージョンから検出結果、インサイト、その他のデータを受け取る Security Hub 集約リージョンでもあります。

クロスリージョン集約の集約リージョンを既に設定している場合、それが中央設定のデフォルトのホームリージョンになります。現在の検出結果アグリゲータを削除し、目的のホームリージョンに新しいアグリゲータを作成することで、中央設定の使用を開始する前にホームリージョンを変更できます。検出結果アグリゲータは、ホームリージョンとリンクされたリージョンを指定する Security Hub リソースです。

ホームリージョンを指定する場合は、集約リージョンを設定する手順に従ってください。ホームリージョンを既に指定している場合は、GetFindingAggregator API を呼び出して、現在どのリージョンがリンクされているかなどの詳細を確認できます。

中央設定の開始

ご希望の方法を選択し、手順に従って組織の中央設定の使用を開始します。

Security Hub console

組織を一元的に設定するには

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。
2. ナビゲーションペインで、[設定]、[設定] の順に選択します。次に、[中央設定を開始] を選択します。

   Security Hub にオンボーディングする場合は、[Security Hub に移動] を選択します。
3. [委任された管理者を指定] ページで、委任管理者アカウントを選択するか、アカウント ID を入力します。該当する場合は、他の AWS セキュリティおよびコンプライアンスサービスに設定したのと同じ委任管理者を選択することをお勧めします。[委任された管理者を設定] を選択します。

4. [組織を一元化] ページの [リージョン] セクションで、ホームリージョンを選択します。続行するには、ホームリージョンにサインインする必要があります。クロスリージョン集約の集約リージョンを既に設定している場合、そのリージョンがホームリージョンとして表示されます。ホームリージョンを変更するには、[リージョンの設定を編集] を選択します。これにより、ご希望のホームリージョンを選択して、このワークフローに戻ることができます。
5. ホームリージョンにリンクするリージョンを少なくとも 1 つ選択してください。必要に応じて、将来サポートされるリージョンをホームリージョンに自動的にリンクするかどうかを選択します。ここで選択したリージョンは、委任管理者がホームリージョンから設定できます。設定ポリシーは、ホームリージョンとすべてのリンクされたリージョンで有効になります。
6. [確認して続行] を選択します。
7. 中央設定を使用できるようになりました。続けてコンソールのプロンプトに従い、最初の設定ポリシーを作成します。設定ポリシーを作成する準備がまだ整っていない場合は、[まだ設定する準備ができていません] を選択します。ポリシーは、後でナビゲーションペインで [設定]、[設定] の順に選択して作成できます。設定ポリシーの作成手順については、「Security Hub 設定ポリシーの作成と関連付け」を参照してください。

Security Hub API

Security Hub を一元的に設定するには

1. 委任管理者アカウントの認証情報を使用して、ホームリージョンから UpdateOrganizationConfiguration API を呼び出します。
2. `AutoEnable` フィールドは `false` に設定されます。
3. `OrganizationConfiguration` オブジェクト内の `ConfigurationType` フィールドを `CENTRAL` に設定します。このアクションには以下の影響があります。

   - すべてのリンクされたリージョンで、呼び出しアカウントを Security Hub 委任管理者として指定します。
   - すべてのリンクされたリージョンの委任管理者アカウントで Security Hub を有効にします。
   - Security Hub を使用する、組織に属している新規および既存のアカウントについて、呼び出しアカウントを Security Hub 委任管理者として指定します。これはホームリージョンとすべてのリンクされたリージョンで発生します。呼び出しアカウントは、新しい組織アカウントが Security Hub が有効になっている設定ポリシーに関連付けられている場合にの

み、その委任管理者として設定されます。呼び出しアカウントは、既存の組織アカウントで Security Hub が既に有効になっている場合のみ、その委任管理者として設定されます。

- すべてのリンクされたリージョンで AutoEnable を `false` に設定し、ホームリージョンとすべてのリンクされたリージョンで AutoEnableStandards を `NONE` に設定します。中央設定を使用する場合、これらのパラメータはホームリージョンやリンクされたリージョンには関係ありませんが、設定ポリシーを使用すると、Security Hub とデフォルトのセキュリティ基準を組織アカウントで自動的に有効にできます。

4. 中央設定を使用できるようになりました。委任管理者は、組織で Security Hub を設定するための設定ポリシーを作成できます。設定ポリシーの作成手順については、「Security Hub 設定ポリシーの作成と関連付け」を参照してください。

API リクエストの例:

```
{
    "AutoEnable": false,
    "OrganizationConfiguration": {
        "ConfigurationType": "CENTRAL"
    }
}
```

AWS CLI

Security Hub を一元的に設定するには

1. 委任管理者アカウントの認証情報を使用して、ホームリージョンから update-organization-configuration コマンドを実行します。
2. `no-auto-enable` パラメータを指定します。
3. `organization-configuration` オブジェクト内の `ConfigurationType` フィールドを `CENTRAL` に設定します。このアクションには以下の影響があります。

   - すべてのリンクされたリージョンで、呼び出しアカウントを Security Hub 委任管理者として指定します。
   - すべてのリンクされたリージョンの委任管理者アカウントで Security Hub を有効にします。
   - Security Hub を使用する、組織に属している新規および既存のアカウントについて、呼び出しアカウントを Security Hub 委任管理者として指定します。これはホームリージョン

とすべてのリンクされたリージョンで発生します。呼び出しアカウントは、新しい組織アカウントが Security Hub が有効になっている設定ポリシーに関連付けられている場合にのみ、その委任管理者として設定されます。呼び出しアカウントは、既存の組織アカウントで Security Hub が既に有効になっている場合のみ、その委任管理者として設定されます。

- すべてのリンクされたリージョンで自動有効化オプションを no-auto-enable に設定し、ホームリージョンとすべてのリンクされたリージョンで auto-enable-standards を NONE に設定します。中央設定を使用する場合、これらのパラメータはホームリージョンやリンクされたリージョンには関係ありませんが、設定ポリシーを使用すると、Security Hub とデフォルトのセキュリティ基準を組織アカウントで自動的に有効にできます。

4. 中央設定を使用できるようになりました。委任管理者は、組織で Security Hub を設定するための設定ポリシーを作成できます。設定ポリシーの作成手順については、「Security Hub 設定ポリシーの作成と関連付け」を参照してください。

コマンドの例:

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}'
```

アカウントと OUs の管理タイプの選択

中央設定を使用すると、 AWS Security Hub 委任管理者は各組織アカウントと組織単位 (OU) を一元管理型または自己管理型として指定できます。アカウントまたは OU の管理タイプによって、Security Hub の設定を指定および変更する方法が決まります。

セルフマネージドアカウントまたは OU は、各 で独自の Security Hub 設定を個別に設定できます AWS リージョン。委任された管理者は、セルフマネージド型アカウントまたは OU に対して Security Hub を設定することはできず、設定ポリシーをそれらに関連付けることもできません。対照的に、ホームリージョンとリンクされたリージョンの一元管理型アカウントおよび OU に対しては、委任された管理者のみが Security Hub を設定することができます。設定ポリシーは、一元管理型アカウントおよび OU に関連付けることができます。

委任された管理者は、アカウントまたは OU のステータスをセルフマネージド型と一元管理型の間で切り替えることができます。デフォルトでは、Security Hub API を使用して中央設定を開始する場合、すべてのアカウントと OU がセルフマネージド型になります。コンソールでは、管理タイプは

最初の設定ポリシーによって異なります。最初のポリシーに関連付けられるアカウントと OU は、一元管理型です。その他のアカウントと OU は、デフォルトではセルフマネージド型になります。

設定ポリシーをセルフマネージドアカウントに関連付けると、ポリシーはセルフマネージドの指定を上書きします。アカウントは一元管理され、設定ポリシーに反映された設定を採用します。

子アカウントと OU は、セルフマネージド型の親からセルフマネージド型の動作を継承でき、同様に一元管理型の親から設定ポリシーを継承できます。詳細については、「アプリケーションと継承によるポリシーの関連付け」を参照してください。

セルフマネージドアカウントまたは OU は、親ノードまたはルートから設定ポリシーを継承できません。例えば、組織内のすべてのアカウントと OUs にルートから設定ポリシーを継承させる場合は、セルフマネージド型ノードの管理タイプを一元管理型に変更する必要があります。

セルフマネージド型アカウントの設定の指定

セルフマネージド型アカウントは、リージョンごとに独自の設定を行う必要があります。

セルフマネージドアカウントの所有者は、各リージョンで Security Hub API の以下のオペレーションを呼び出して設定を行うことができます。

- Security Hub サービスを有効または無効にする `EnableSecurityHub` および `DisableSecurityHub`
- 標準を有効または無効にする `BatchEnableStandards` または `BatchDisableStandards`
- コントロールを有効または無効にする `BatchUpdateStandardsControlAssociations` または `UpdateStandardsControl`

セルフマネージド型アカウントは、 `*Invitations`および `*Members`オペレーションを使用することもできます。ただし、セルフマネージド型アカウントはこれらのオペレーションを使用しないことをお勧めします。メンバーアカウントに、委任された管理者の組織とは異なる組織に属する独自のメンバーがある場合、ポリシーの関連付けが失敗する可能性があります。

Security Hub API アクションの説明については、AWS Security Hub API のリファレンスを参照してください。

セルフマネージド型アカウントは、Security Hub コンソールまたは を使用して AWS CLI 、各リージョンで設定を構成することもできます。

セルフマネージド型アカウントでは、Security Hub の設定ポリシーおよびポリシーの関連付けに関連する API を呼び出すことはできません。中央設定 API を呼び出し、設定ポリシーを使用して一元管理型アカウントを設定できるのは、委任された管理者のみです。

アカウントと OUs の管理タイプの選択

ご希望の方法を選択し、手順に従って、アカウントまたは OU を一元管理型またはセルフマネージド型に指定します。

Security Hub console

アカウントまたは OU の管理タイプを選択するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   ホームリージョンの Security Hub 委任管理者アカウントの認証情報を使用してサインインします。
2. [設定] を選択します。
3. [組織] タブで、ターゲットアカウントまたは OU を選択します。[編集] を選択します。
4. 委任された管理者がターゲットアカウントまたは OU の設定を行う場合は、[設定を定義] ページの [管理タイプ] で、[一元管理] を選択します。次に、既存の設定ポリシーをターゲットと関連付ける場合は、[特定のポリシーを適用] を選択します。ターゲットに最も近い親の設定を継承させる場合は、[自分の組織から継承] を選択します。アカウントまたは OU で独自の設定を行う場合は、[セルフマネージド] を選択します。
5. [次へ] をクリックします。変更内容を見直して、[保存] を選択します。

Security Hub API

アカウントまたは OU の管理タイプを選択するには

1. ホームリージョンの Security Hub 委任管理者アカウントから StartConfigurationPolicyAssociation API を呼び出します。
2. アカウントまたは OU で独自の設定を制御する場合は、`ConfigurationPolicyIdentifier` フィールドに `SELF_MANAGED_SECURITY_HUB` と入力します。委任された管理者がアカウントまたは OU の設定を制御する場合は、関連する設定ポリシーの Amazon リソースネーム (ARN) または ID を指定します。
3. `Target` フィールドに、管理タイプを変更するターゲットの AWS アカウント ID、OU ID、またはルート ID を指定します。これにより、セルフマネージド型の動作または指定した設

定ポリシーがターゲットに関連付けられます。ターゲットの子アカウントは、セルフマネージド型の動作または設定ポリシーを継承できます。

セルフマネージド型アカウントを指定する API リクエストの例:

```
{
    "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

アカウントまたは OU の管理タイプを選択するには

1. ホームリージョンの Security Hub 委任管理者アカウントで、start-configuration-policy-association コマンドを実行します。
2. アカウントまたは OU で独自の設定を制御するには、`configuration-policy-identifier` フィールドに `SELF_MANAGED_SECURITY_HUB` と指定します。委任された管理者がアカウントまたは OU の設定を制御する場合は、関連する設定ポリシーの Amazon リソースネーム (ARN) または ID を指定します。
3. `target` フィールドに、管理タイプを変更するターゲットの AWS アカウント ID、OU ID、またはルート ID を指定します。これにより、セルフマネージド型の動作または指定した設定ポリシーがターゲットに関連付けられます。ターゲットの子アカウントは、セルフマネージド型の動作または設定ポリシーを継承できます。

セルフマネージド型アカウントを指定するコマンドの例:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
--target '{"AccountId": "123456789012"}'
```

Security Hub 設定ポリシーの仕組み

委任管理者アカウントは、組織内の Security Hub、セキュリティ標準、セキュリティコントロールを設定する設定 AWS Security Hub ポリシーを作成できます。設定ポリシーを作成した後に、委任管理

者はそれをアカウント、組織単位 (OU)、またはルートに関連付けることができます。委任管理者は設定ポリシーを表示、編集、削除することもできます。

ポリシーに関する考慮事項

Security Hub で設定ポリシーを作成する前に、次の点について考えます。

- 設定ポリシーを有効にするには関連付ける必要がある — 設定ポリシーを作成した後に、1 つ以上のアカウント、組織単位 (OU)、またはルートに関連付けることができます。設定ポリシーは、直接適用するか、親 OU からの継承によってアカウントまたは OU に関連付けることができます。
- アカウントまたは OU は 1 つの設定ポリシーにのみ関連付けることができます。設定の競合を防ぐため、アカウントまたは OU は、常に 1 つの設定ポリシーにのみ関連付けることができます。または、アカウントまたは OU をセルフマネージドすることもできます。
- 設定ポリシーが完全である — 設定ポリシーには設定の完全な仕様が記載されています。例えば、子アカウントでは、あるポリシーの一部のコントロールの設定と、別のポリシーのその他のコントロールの設定を受け入れることはできません。ポリシーを子アカウントに関連付けるときは、その子アカウントで使用したい設定のすべてがポリシーで指定されていることを確認します。
- 設定ポリシーを元に戻すことはできません – アカウントまたは OUs に関連付けた後、設定ポリシーを元に戻すオプションはありません。例えば、 CloudWatch コントロールを無効にする設定ポリシーを特定のアカウントと関連付けてから、そのポリシーの関連付けを解除した場合、そのアカウントでは CloudWatch コントロールは引き続き無効になります。 CloudWatch コントロールを再度有効にするには、アカウントをコントロールを有効にする新しいポリシーに関連付けることができます。または、アカウントをセルフマネージドに変更し、アカウント内の各 CloudWatch コントロールを有効にすることもできます。
- 設定ポリシーが、ホームリージョンとリンクされているすべてのリージョンで有効になっている — 設定ポリシーは、ホームリージョンとリンクされているすべてのリージョンの関連付けられているアカウントのすべてに影響します。これらのリージョンの一部でのみ有効で、他のリージョンでは有効にならない設定ポリシーを作成することはできません。ただし、グローバルリソースが関与するコントロールは例外です。

  2019 年 3 月 20 日以降に AWS 導入されたリージョンは、オプトインリージョンと呼ばれます。設定ポリシーを有効にする前に、アカウントでこのようなリージョンを有効にする必要があります。Organizations 管理アカウントでは、メンバーアカウントのオプトインリージョンを有効にできます。オプトインリージョンを有効にする手順については、「 AWS リージョン アカウント管理リファレンスガイド」の「アカウントで使用できる を指定する」を参照してください。 AWS

ポリシーでホームリージョンまたは 1 つ以上のリンクされたリージョンでは使用できないコントロールが設定されている場合、Security Hub は使用できないリージョンのコントロール設定をスキップし、コントロールが利用可能なリージョンの設定を適用します。

- 設定ポリシーがリソースである — リソースとして、設定ポリシーには、Amazon リソースネーム (ARN) と一意識別子 (UUID) があります。ARN は次の形式を使用します: `arn:`*`partition:`*`securityhub:`*`region`*`:`*`delegated administrator account ID`*`:configuration-policy/`*`configuration policy UUID`*。セルフマネージド設定には ARN または UUID がありません。セルフマネージド設定の識別子は ですSELF_MANAGED_SECURITY_HUB。

設定ポリシーのタイプ

各設定ポリシーでは、次の設定を指定します。

- Security Hub を有効または無効にします。
- 1 つ以上のセキュリティ標準を有効にします。
- 有効な標準でどのセキュリティコントロールが有効になっているかを示します。そのためには、有効にすべき特定のコントロールのリストを指定します。Security Hub は、リリース時に新しいコントロールを含め、他のすべてのコントロールを無効にします。または、無効にすべき特定のコントロールのリストを指定して、Security Hub がリリースされた時点の新しいコントロールを含め、他のすべてのコントロールを有効化することもできます。
- オプションで、有効な標準全体で有効になっているコントロールを選択してパラメータをカスタマイズできます。

中央設定ポリシーには AWS Config レコーダー設定は含まれません。Security Hub がコントロールの検出結果を生成するには AWS Config 、必要なリソースの記録を個別に有効にして有効にする必要があります。詳細については、「の設定 AWS Config」を参照してください。

中央設定を使用する場合、Security Hub はホームリージョンを除くすべてのリージョンでグローバルリソースを含むコントロールを自動的に無効にします。設定ポリシーを使用して有効にするその他のコントロールは、使用可能なすべてのリージョンで有効になります。これらのコントロールの結果を 1 つのリージョンのみに制限するには、 AWS Config レコーダー設定を更新し、ホームリージョンを除くすべてのリージョンでグローバルリソースの記録をオフにします。中央設定を使用する場合、ホームリージョンおよびリンクされたリージョンで利用できないコントロールのカバレッジがありま

せん。グローバルリソースに関連するコントロールのリストについては、「」を参照してくださいグローバルリソースを処理するコントロール。

推奨される設定ポリシー

Security Hub コンソールで初めて設定ポリシーを作成する場合、Security Hub の推奨されるポリシーを選択するオプションもあります。

推奨ポリシーにより、Security Hub、 AWS Foundational Security Best Practices (FSBP) 標準、および既存および新規のすべての FSBP コントロールが有効になります。パラメータを受け入れるコントロールは、デフォルト値を使用します。推奨されるポリシーはルート (新規および既存のすべてのアカウントと OU) に適用されます。組織用の推奨されるポリシーを作成した後に、委任管理者アカウントから変更できます。例えば、追加の標準やコントロールを有効にしたり、特定の FSBP コントロールを無効にしたりできます。設定ポリシーを変更する手順については、「Security Hub 設定ポリシーの更新」を参照してください。

カスタム設定ポリシー

委任管理者は、推奨されるポリシーの代わりに最大 20 件のカスタム設定ポリシーを作成できます。1 つのカスタムポリシーを組織全体に関連付けることも、別のカスタムポリシーをさまざまなアカウントや OU に関連付けることもできます。カスタム設定ポリシーの場合は、必要な設定を指定します。例えば、FSBP、Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0、および Amazon Redshift のコントロールを除くこれらの標準のすべてのコントロールを有効にするカスタムポリシーを作成できます。カスタム設定ポリシーで使用する細分性のレベルは、組織全体で想定された範囲のセキュリティカバレッジによって異なります。

> **Note**
>
> Security Hub を無効にする設定ポリシーを、委任管理者アカウントに関連付けることはできません。このようなポリシーは他のアカウントと関連付けることはできますが、委任管理者との関連付けはスキップされます。委任管理者アカウントは現在の設定を保持します。

カスタム設定ポリシーを作成した後に、推奨される設定を反映するように設定ポリシーを更新することで、推奨される設定ポリシーに切り替えることができます。ただし、最初のポリシーを作成した後は、Security Hub コンソールに推奨される設定ポリシーを作成する選択肢は表示されません。

アプリケーションと継承によるポリシーの関連付け

最初に中央設定にオプトインした時点では、組織は関連付けられておらず、オプトイン前と同じように動作します。その後、委任管理者は、設定ポリシーまたはセルフマネージド型の動作とアカウント、OUs、またはルート間の関連付けを確立できます。関連付けは、アプリケーションまたは継承によって確立できます。

委任管理者アカウントから、設定ポリシーをアカウント、OU、またはルートに直接適用できます。または、委任された管理者は、アカウント、OU、またはルートにセルフマネージド型の指定を直接適用することもできます。

直接アプリケーションがない場合、アカウントまたは OU は、設定ポリシーまたはセルフマネージド動作を持つ最も近い親の設定を継承します。最も近い親が設定ポリシーに関連付けられている場合、子はそのポリシーを継承し、設定できるのはホームリージョンの委任管理者のみです。最も近い親がセルフマネージド型の場合、子はセルフマネージド型の動作を継承し、各 で独自の設定を指定できます AWS リージョン。

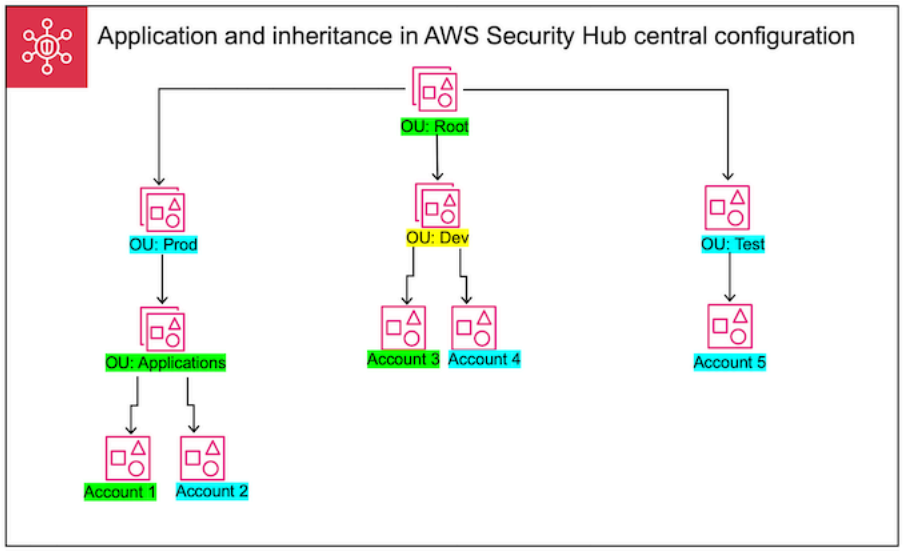
アプリケーションは継承よりも優先されます。つまり、継承によって、委任された管理者がアカウントまたは OU に直接適用した設定ポリシーやセルフマネージド型の指定が上書きされることはありません。

設定ポリシーをセルフマネージドアカウントに直接適用すると、ポリシーはセルフマネージドの指定を上書きします。アカウントは一元管理され、設定ポリシーに反映された設定を採用します。

設定ポリシーをルートに直接適用することをお勧めします。ルートにポリシーを適用すると、組織に参加する新しいアカウントは、別のポリシーに関連付けたり、セルフマネージド型として指定したりしない限り、自動的にルートポリシーを継承します。

アプリケーションまたは継承によって、一度に 1 つのアカウントまたは OU に関連付けることができる設定ポリシーは 1 つだけです。これは設定の競合を防ぐためのものです。

次の図は、中央設定におけるポリシーの適用と継承の仕組みを示しています。



この例では、緑色で強調表示されているノードには設定ポリシーが適用されています。青色で強調表示されているノードには、設定ポリシーが適用されていません。黄色で強調表示されているノードは、セルフマネージド型として指定されています。各アカウントと OU は以下の設定を使用します。

- OU:Root (緑) — この OU は、適用されている設定ポリシーを使用します。
- OU:Prod (青) — この OU は OU:Root から設定ポリシーを継承します。
- OU:Applications (緑) — この OU は、適用されている設定ポリシーを使用します。
- Account 1 (緑) — このアカウントは、適用されている設定ポリシーを使用します。
- Account 2 (青) — このアカウントは OU:Applications の設定ポリシーを継承します。
- OU:Dev (黄) — この OU はセルフマネージド型です。
- Account 3 (緑) — このアカウントは、適用されている設定ポリシーを使用します。
- Account 4 (青) — このアカウントは OU:Dev のセルフマネージド型の動作を継承します。
- OU:Test (青) — このアカウントは OU:Root の設定ポリシーを継承します。
- Account 5 (青) — このアカウントは OU:Root の設定ポリシーを継承します。これは、その直接の親である OU:Test には設定ポリシーが関連付けられていないためです。

設定ポリシーのテスト

設定ポリシーの効果をテストするには、設定ポリシーを組織全体に広く関連付ける前に、そのポリシーを 1 つのアカウントまたは OU に関連付けることができます。

設定ポリシーをテストするには

1. カスタム設定ポリシーを作成します。ただし、どのアカウントにも適用しないでください。Security Hub の有効化、標準、およびコントロールに指定されている設定が正しいことを確認します。
2. 子アカウントや OU を持たないテストアカウントまたは OU に設定ポリシーを適用します。
3. テストアカウントまたは OU が、ホームリージョンとリンクされているすべてのリージョンで設定ポリシーを想定どおりに使用していることを確認します。また、組織内の他のすべてのアカウントと OU が引き続きセルフマネージドされ、各地域で独自の設定を変更できることを確認できます。

1 つのアカウントまたは OU で設定ポリシーをテストした後に、その設定ポリシーを他のアカウントや OU に関連付けることができます。ポリシーの作成と関連付けの手順については、「Security Hub 設定ポリシーの作成と関連付け」を参照してください。適用されたアカウントの子アカウントは、セルフマネージド型であるか、別の設定ポリシーが適用されている場合を除き、ポリシーを継承します。また、必要に応じて設定ポリシーを編集したり、追加の設定ポリシーを作成したりすることもできます。

Security Hub 設定ポリシーの作成と関連付け

委任された管理者アカウントは、 AWS Security Hub 設定ポリシーを作成し、組織アカウント、組織単位 (OUs)、またはルートに関連付けることができます。セルフマネージド設定をアカウント、OUs、またはルートに関連付けることもできます。

初めて設定ポリシーを作成する場合は、最初に「Security Hub 設定ポリシーの仕組み」を確認することをお勧めします。

任意のアクセス方法を選択し、手順に従って設定ポリシーまたはセルフマネージド設定を作成して関連付けます。Security Hub コンソールを使用する場合、設定を複数のアカウントまたは OUs に同時に関連付けることができます。Security Hub API または を使用する場合 AWS CLI、各リクエストで設定を関連付けることができるアカウントまたは OU は 1 つだけです。

> **Note**
>
> 中央設定を使用する場合、Security Hub は、ホームリージョンを除くすべてのリージョンでグローバルリソースを含むコントロールを自動的に無効にします。設定ポリシーを使用して有効にするその他のコントロールは、使用可能なすべてのリージョンで有効になります。これらのコントロールの結果を 1 つのリージョンのみに制限するには、 AWS Config レコー

ダー設定を更新し、ホームリージョンを除くすべてのリージョンでグローバルリソース記録をオフにします。中央設定を使用する場合、ホームリージョンおよびリンクされたリージョンで利用できないコントロールのカバレッジがありません。グローバルリソースに関連するコントロールのリストについては、「」を参照してくださいグローバルリソースを処理するコントロール。

Security Hub console

設定ポリシーを作成して関連付けるには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   ホームリージョンの Security Hub 委任管理者アカウントの認証情報を使用してサインインします。

2. ナビゲーションペインで、[設定] および [ポリシー] タブを選択します。次に、[ポリシーの作成] を選択します。

3. 設定ポリシーを初めて作成する場合は、[組織を設定] ページの [設定タイプ] に 3 つのオプションが表示されます。既に 1 つ以上の設定ポリシーを作成している場合は、[カスタムポリシー] オプションのみが表示されます。

   - 推奨ポリシーを使用するには、組織全体で AWS 推奨される Security Hub 設定を使用するを選択します。推奨ポリシーは、すべての組織アカウントで Security Hub を有効にし、AWS Foundational Security Best Practices (FSBP) 標準を有効にし、すべての新規および既存の FSBP コントロールを有効にします。コントロールはデフォルトのパラメータ値を使用します。
   - 設定ポリシーを後で作成するには、[まだ設定する準備ができていません] を選択します。
   - [カスタムポリシー] を選択して、カスタム設定ポリシーを作成します。Security Hub を有効にするか無効にするか、どの標準を有効にするか、それらの標準でどのコントロールを有効にするかを指定します。オプションで、カスタムパラメータをサポートする 1 つ以上の有効になっているコントロールにカスタムパラメータ値を指定します。

4. [アカウント] セクションで、設定ポリシーを適用するターゲットアカウント、OU、またはルートを選択します。

   - 設定ポリシーをルートに適用する場合は、[すべてのアカウント] を選択します。これには、別のポリシーが適用されていない、または継承されていない組織内のすべてのアカウントと OU が含まれます。

- 設定ポリシーを特定のアカウントまたは OU に適用する場合は、[特定のアカウント] を選択します。アカウント ID を入力するか、組織構造からアカウントと OU を選択します。ポリシーは、作成時に最大 15 個のターゲット (アカウント、OUsに適用できます。より大きな数値を指定するには、作成後にポリシーを編集し、追加のターゲットに適用します。
- [委任された管理者のみ] を選択すると、現在の委任管理者アカウントに設定ポリシーが適用されます。

5. [次へ] をクリックします。
6. [確認と適用] ページで、設定ポリシーの詳細を確認します。次に、[ポリシーを作成して適用] を選択します。ホームリージョンとリンクされたリージョンでは、このアクションは、この設定ポリシーに関連付けられているアカウントの既存の設定よりも優先されます。アカウントは、アプリケーションを通じて設定ポリシーに関連付けることも、親ノードから継承して設定ポリシーに関連付けることもできます。適用されたターゲットの子アカウントと OU は、特に除外されたり、セルフマネージド型であったり、別の設定ポリシーを使用したりしない限り、この設定ポリシーを自動的に継承します。

Security Hub API

設定ポリシーを作成して関連付けるには

1. ホームリージョンの Security Hub 委任管理者アカウントから CreateConfigurationPolicy API を呼び出します。
2. `Name` には、設定ポリシーの一意の名前を入力します。オプションで、`Description` に設定ポリシーの説明を入力します。
3. `ServiceEnabled` フィールドで、Security Hub をこの設定ポリシーで有効にするか無効にするかを指定します。
4. `EnabledStandardIdentifiers` フィールドで、この設定ポリシーで有効にする Security Hub 標準を指定します。
5. `SecurityControlsConfiguration` オブジェクトで、この設定ポリシーで有効または無効にするコントロールを指定します。`EnabledSecurityControlIdentifiers` を選択すると、指定したコントロールが有効になります。有効になっている標準に含まれるその他のコントロール (新しくリリースされたコントロールを含む) は無効になります。`DisabledSecurityControlIdentifiers` を選択すると、指定したコントロールが無効になります。有効になっている標準に含まれるその他のコントロール (新しくリリースされたコントロールを含む) が有効になります。

6. オプションで、SecurityControlCustomParameters フィールドに、パラメータをカスタマイズする有効なコントロールを指定します。ValueType フィールドに CUSTOM を指定し、Value フィールドにカスタムパラメータ値を指定します。値のデータ型が正しく、Security Hub で指定された有効な範囲内である必要があります。カスタムパラメータ値をサポートするコントロールのみ選択します。詳細については、「カスタムコントロールパラメータ」を参照してください。
7. 設定ポリシーをアカウントまたは OU に適用するには、ホームリージョン内の Security Hub 委任管理者アカウントから StartConfigurationPolicyAssociation API を呼び出します。
8. ConfigurationPolicyIdentifier フィールドには、ポリシーの Amazon リソースネーム (ARN) またはユニバーサル一意識別子 (UUID) を指定します。ARN と UUID は CreateConfigurationPolicy API によって返されます。セルフマネージド設定の場合、 ConfigurationPolicyIdentifierフィールドは と等しくなりますSELF_MANAGED_SECURITY_HUB。
9. Target フィールドには、この設定ポリシーを適用する OU、アカウント、またはルート ID を指定します。各 API リクエストに指定できるターゲットは 1 つのみです。選択したターゲットの子アカウントと OU は、セルフマネージド型であるか、別の設定ポリシーを使用している場合を除き、自動的にこの設定ポリシーを継承します。

設定ポリシーを作成する API リクエストの例:

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
```

```
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

設定ポリシーを関連付ける API リクエストの例:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}
```

AWS CLI

設定ポリシーを作成して関連付けるには

1. ホームリージョンの Security Hub 委任管理者アカウントで、create-configuration-policy コマンドを実行します。
2. name には、設定ポリシーの一意の名前を入力します。オプションで、description に設定ポリシーの説明を入力します。
3. ServiceEnabled フィールドで、Security Hub をこの設定ポリシーで有効にするか無効にするかを指定します。
4. EnabledStandardIdentifiers フィールドで、この設定ポリシーで有効にする Security Hub 標準を指定します。
5. SecurityControlsConfiguration フィールドで、この設定ポリシーで有効または無効にするコントロールを指定します。EnabledSecurityControlIdentifiers を選択すると、指定したコントロールが有効になります。有効になっている標準に含まれ

るその他のコントロール (新しくリリースされたコントロールを含む) は無効になります。DisabledSecurityControlIdentifiers を選択すると、指定したコントロールが無効になります。有効になっている標準に適用されるその他のコントロール (新しくリリースされたコントロールを含む) が有効になります。

6. オプションで、SecurityControlCustomParameters フィールドに、パラメータをカスタマイズする有効なコントロールを指定します。ValueType フィールドに CUSTOM を指定し、Value フィールドにカスタムパラメータ値を指定します。値のデータ型が正しく、Security Hub で指定された有効な範囲内である必要があります。カスタムパラメータ値をサポートするコントロールのみ選択します。詳細については、「カスタムコントロールパラメータ」を参照してください。
7. 設定ポリシーをアカウントまたは OU に適用するには、ホームリージョンの Security Hub 委任管理者アカウントで start-configuration-policy-association コマンドを実行します。
8. configuration-policy-identifier フィールドに、設定ポリシーの Amazon リソースネーム (ARN) または ID を入力します。この ARN と ID は、create-configuration-policy コマンドによって返されます。
9. target フィールドには、この設定ポリシーを適用する OU、アカウント、またはルート ID を指定します。コマンドを実行するたびに指定できるターゲットは 1 つのみです。選択したターゲットの子は、セルフマネージド型であるか、別の設定ポリシーを使用している場合を除き、この設定ポリシーを自動的に継承します。

設定ポリシーを作成するコマンドの例:

```
aws securityhub --region us-east-1 create-configuration-policy \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}}'
```

設定ポリシーを関連付けるコマンドの例:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
```

```
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}'
```

StartConfigurationPolicyAssociation API は、AssociationStatus というフィールドを返します。このフィールドは、ポリシーの関連付けが保留中か、成功または失敗の状態かを示します。ステータスが PENDING から SUCCESS または FAILURE に変わるまで、最大 24 時間かかることがあります。関連付けのステータスの詳細については、「設定の関連付けステータス」を参照してください。

Security Hub 設定ポリシーの表示

委任管理者アカウントは、組織の AWS Security Hub 設定ポリシーとその詳細を表示できます。

任意の方法を選択し、その手順に従って設定ポリシーを表示します。

Console

設定ポリシーを表示するには

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。

   ホームリージョンの Security Hub 委任管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで、[設定]、[設定] の順に選択します。
3. [ポリシー] タブを選択すると、設定ポリシーの概要が表示されます。
4. 設定ポリシーを選択し、[詳細を表示] を選択すると、そのポリシーに関するその他の詳細が表示されます。

API

設定ポリシーを表示するには

すべての設定ポリシーの概要リストを表示するには、ホームリージョンの Security Hub 委任管理者アカウントから ListConfigurationPolicies API を呼び出します。オプションのページ分割パラメータを指定できます。

API リクエストの例:

```
{
    "MaxResults": 5,
    "NextToken": "U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf"
}
```

特定の設定ポリシーの詳細を表示するには、ホームリージョンの Security Hub 委任管理者アカウントから GetConfigurationPolicy API を呼び出します。詳細を表示する設定ポリシーの Amazon リソースネーム (ARN) または ID を指定します。

API リクエストの例:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

すべての設定ポリシーとその関連付けの概要リストを表示するには、ホームリージョンの Security Hub 委任管理者アカウントから ListConfigurationPolicyAssociations API を呼び出します。オプションで、ページ分割パラメータを指定したり、特定のポリシー ID、関連付けタイプ、または関連付けステータスで結果をフィルタリングしたりできます。

API リクエストの例:

```
{
    "AssociationType": "APPLIED"
}
```

特定のアカウント、OU、またはルートの関連付けを表示するには、ホームリージョンの Security Hub 委任管理者アカウントから GetConfigurationPolicyAssociation または BatchGetConfigurationPolicyAssociations API を呼び出します。Target の場合、アカウント番号、OU ID、またはルート ID を指定します。

```
{
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

設定ポリシーを表示するには

すべての設定ポリシーの概要リストを表示するには、ホームリージョンの Security Hub 委任管理者アカウントから list-configuration-policies コマンドを実行します。

コマンドの例:

```
aws securityhub --region us-east-1 list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf
```

特定の設定ポリシーに関する詳細を表示するには、ホームリージョンの Security Hub 委任管理者アカウントから get-configuration-policy コマンドを実行します。詳細を表示する設定ポリシーの Amazon リソースネーム (ARN) または ID を指定します。

```
aws securityhub --region us-east-1 get-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

すべての設定ポリシーとそれらのアカウント関連付けの概要リストを表示するには、ホームリージョンの Security Hub 委任管理者アカウントから list-configuration-policy-associations コマンドを実行します。オプションで、ページ分割パラメータを指定したり、特定のポリシー ID、関連付けタイプ、または関連付けステータスで結果をフィルタリングしたりできます。

```
aws securityhub --region us-east-1 list-configuration-policy-associations \
--association-type "APPLIED"
```

特定のアカウントの関連付けを表示するには、ホームリージョンの Security Hub 委任管理者アカウントから get-configuration-policy-association または batch-get-configuration-policy-associations コマンドを実行します。target の場合、アカウント番号、OU ID、またはルート ID を指定します。

```
aws securityhub --region us-east-1 get-configuration-policy-association \
```

```
--target '{"AccountId": "123456789012"}'
```

設定の関連付けステータス

以下の中央設定 API オペレーションは、AssociationStatus というフィールドを返します。

- BatchGetConfigurationPolicyAssociations
- GetConfigurationPolicyAssociation
- ListConfigurationPolicyAssociations
- StartConfigurationPolicyAssociation

このフィールドは、基礎となる設定が設定ポリシーの場合とセルフマネージド型の動作の場合の両方で返されます。

AssociationStatus の値は、ポリシーの関連付けが保留中か、成功または失敗の状態かを示します。ステータスが PENDING から SUCCESS または FAILURE に変わるまで、最大 24 時間かかることがあります。親 OU またはルートの関連付けステータスは、子のステータスによって異なります。すべての子の関連付けステータスが SUCCESS の場合、親の関連付けステータスは SUCCESS です。1 人以上の子の関連付けステータスが FAILED の場合、親の関連付けステータスは FAILED です。

AssociationStatus の値もすべてのリージョンによって異なります。ホームリージョンとリンクされているすべてのリージョンで関連付けが成功すると、AssociationStatus の値は SUCCESS になります。これらの 1 つ以上のリージョンで関連付けに失敗すると、AssociationStatus の値は FAILED になります。

以下の動作は、AssociationStatus の値にも影響します。

- ターゲットが親 OU またはルートの場合、すべての子が SUCCESS または FAILED ステータスの場合にのみ SUCCESS または FAILED の AssociationStatus が含まれます。最初に親を設定に関連付けた後に、子アカウントまたは OU の関連付けステータスが変更された場合 (リンクされたリージョンが追加または削除された場合など)、StartConfigurationPolicyAssociation API を再度呼び出さない限り、その変更によって親の関連付けステータスは更新されません。
- ターゲットがアカウントの場合、関連付けにホームリージョンとすべてのリンクされたリージョンの SUCCESS または FAILED の結果がある場合に限り、そのアカウントには SUCCESS または FAILED の AssociationStatus があります。ターゲットアカウントを初めて設定に関

連付けた後に、ターゲットアカウントの関連付けステータスが変更された場合 (リンクされたリージョンが追加または削除された場合など)、その関連付けステータスは更新されます。ただし、`StartConfigurationPolicyAssociation` API を再度呼び出さない限り、変更によって親の関連付けステータスは更新されません。

リンクされた新しいリージョンを追加すると、Security Hub は、新しいリージョンの `PENDING`、`SUCCESS`、`FAILED` ステータスにある既存の関連付けをレプリケートします。

関連付け失敗の一般的な原因

設定ポリシーの関連付けは、次の一般的な原因で失敗することがあります。

- Organizations 管理アカウントがメンバーではない — 設定ポリシーを Organizations 管理アカウントに関連付ける場合、そのアカウントの Security Hub は既に有効になっている必要があります。これにより、管理アカウントが組織内のメンバーアカウントになります。
- AWS Config が有効になっていない、または正しく設定されていない — 設定ポリシーで標準を有効にするには、AWS Config を有効にして、関連するリソースを記録するように設定する必要があります。
- 委任管理者アカウントから関連付ける必要がある — 委任管理者アカウントにサインインすると、ポリシーをターゲットアカウントと OU にのみ関連付けることができます。
- ホームリージョンから関連付ける必要がある — ホームリージョンにサインインすると、ポリシーをターゲットアカウントと OU にのみ関連付けることができます。
- オプトイン地域が有効化されていない — 委任管理者が有効化していないオプトインリージョンの場合、リンクされたリージョンのメンバーアカウントまたは OU に対するポリシーの関連付けが失敗します。委任管理者アカウントからリージョンを有効化した後で再試行できます。
- メンバーアカウントが一時停止している — 一時停止されたメンバーアカウントにポリシーを関連付けようとすると、ポリシーの関連付けが失敗します。

Security Hub 設定ポリシーの更新

委任管理者アカウントは、必要に応じて AWS Security Hub 設定ポリシーを更新できます。委任管理者は、ポリシー設定、ポリシーが関連付けられているアカウントまたは OU、またはその両方を更新できます。ポリシー設定が更新されると、設定ポリシーに関連付けられているアカウントは、更新されたポリシーの使用を自動的に開始します。

設定ポリシーを作成したときと同様に、次のポリシー設定を更新できます。

- Security Hub を有効または無効にします。
- 1 つ以上のセキュリティ標準を有効にします。
- 有効な標準でどのセキュリティコントロールが有効になっているかを示します。そのためには、有効にすべき特定のコントロールのリストを指定します。Security Hub は、リリース時に新しいコントロールを含め、他のすべてのコントロールを無効にします。または、無効にすべき特定のコントロールのリストを指定して、Security Hub がリリースされた時点の新しいコントロールを含め、他のすべてのコントロールを有効化することもできます。
- オプションで、有効な標準全体で有効になっているコントロールを選択してパラメータをカスタマイズできます。

任意の方法を選択し、その手順に従って設定ポリシーを更新します。

中央設定を使用する場合、Security Hub は、ホームリージョンを除くすべてのリージョンでグローバルリソースを含むコントロールを自動的に無効にします。設定ポリシーを使用して有効にするその他のコントロールは、使用可能なすべてのリージョンで有効になります。これらのコントロールの結果を 1 つのリージョンのみに制限するには、 AWS Config レコーダー設定を更新し、ホームリージョンを除くすべてのリージョンでグローバルリソース記録をオフにします。中央設定を使用する場合、ホームリージョンおよびリンクされたリージョンで利用できないコントロールのカバレッジがありません。グローバルリソースに関連するコントロールのリストについては、「」を参照してくださいグローバルリソースを処理するコントロール。

Console

設定ポリシーを更新するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   ホームリージョンの Security Hub 委任管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで、[設定]、[設定] の順に選択します。
3. [Policies] タブを選択します。
4. 編集する設定ポリシーを選択したら、[編集] を選択します。必要に応じて、ポリシーの設定を編集します。ポリシーの設定を変更せずにそのまま維持する場合は、このセクションはそのままにします。
5. [次へ] を選択します。必要に応じて、ポリシーの関連付けを編集します。ポリシーの関連付けを変更せずにそのまま維持する場合は、このセクションはそのままにします。ポリシーの

更新時に、最大 15 個のターゲット (アカウント、OUs、またはルート) にポリシーを関連付けたり関連付けを解除したりできます。

6. [次へ] をクリックします。
7. 更新内容を確認して [保存] を選択して適用します。ホームリージョンとリンクされたリージョンでは、このアクションは、この設定ポリシーに関連付けられているアカウントの既存の設定よりも優先されます。アカウントは、アプリケーションを通じて設定ポリシーに関連付けることも、親ノードから継承することもできます。

API

設定ポリシーを更新するには

1. 設定ポリシーの設定を更新するには、ホームリージョンの Security Hub の委任管理者アカウントから UpdateConfigurationPolicy API を呼び出します。
2. 更新する設定ポリシーの Amazon リソースネーム (ARN) または ID を指定します。
3. `ConfigurationPolicy` の下のフィールドに、更新された値を入力します。オプションで、更新の理由も指定できます。
4. この設定ポリシーに新しい関連付けを追加するには、ホームリージョンの Security Hub 委任管理者アカウントから StartConfigurationPolicyAssociation API を呼び出します。1 つ以上の現在の関連付けを削除するには、ホームリージョンの Security Hub 委任管理者アカウントから StartConfigurationPolicyDisassociation API を呼び出します。
5. `ConfigurationPolicyIdentifier` フィールドには、関連付けを更新する設定ポリシーの ARN または ID を指定します。
6. `Target` フィールドには、関連付けるまたは関連付けを解除するアカウント、OU、またはルート ID を指定します。このアクションは、指定した OU またはアカウントに対する以前のポリシー関連付けを上書きします。

> **Note**
>
> `UpdateConfigurationPolicy` API を呼び出すと、Security Hub は、`EnabledStandardIdentifiers`、`EnabledSecurityControlIdentifiers`、`Disabled` のフィールドの完全なリスト置換を実行します。この API を呼び出すたびに、有効にする標準の全リストと、有効または無効にしてパラメータをカスタマイズするコントロールの全リストを指定します。

設定ポリシーを更新する API リクエストの例:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Disabling CloudWatch.1",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2",
                    "CloudWatch.1"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

AWS CLI

設定ポリシーを更新するには

1. 設定ポリシーの設定を更新するには、ホームリージョンの Security Hub 委任管理者アカウントから update-configuration-policy コマンドを実行します。
2. 更新する設定ポリシーの Amazon リソースネーム (ARN) または ID を指定します。
3. configuration-policy の下のフィールドに、更新された値を入力します。オプションで、更新の理由も指定できます。
4. この設定ポリシーに新しい関連付けを追加するには、ホームリージョンの Security Hub 委任管理者アカウントから start-configuration-policy-association コマンドを実行します。1 つ以上の現在の関連付けを削除するには、ホームリージョンの Security Hub 委任管理者アカウントから start-configuration-policy-disassociation コマンドを実行します。
5. configuration-policy-identifier フィールドには、関連付けを更新する設定ポリシーの ARN または ID を指定します。
6. target フィールドには、関連付けるまたは関連付けを解除するアカウント、OU、またはルート ID を指定します。このアクションは、指定した OU またはアカウントに対する以前のポリシー関連付けを上書きします。

> **Note**
>
> update-configuration-policy コマンドを実行すると、Security Hub は、EnabledStandardIdentifiers、EnabledSecurityControlIdentifiers、Disabled のフィールドの完全なリスト置換を実行します。このコマンドを実行するたびに、有効にする標準の全リストと、有効または無効にしてパラメータをカスタマイズするコントロールの全リストを指定します。

設定ポリシーを更新するコマンドの例:

```
aws securityhub update-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--description "Updated configuration policy" \
--updated-reason "Disabling CloudWatch.1" \
```

```
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2","CloudWatch.1"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}'
```

StartConfigurationPolicyAssociation API は、AssociationStatus というフィールドを返します。このフィールドは、ポリシーの関連付けが保留中か、成功または失敗の状態かを示します。ステータスが PENDING から SUCCESS または FAILURE に変わるまで、最大 24 時間かかることがあります。関連付けのステータスの詳細については、「設定の関連付けステータス」を参照してください。

Security Hub 設定ポリシーの削除と関連付けの解除

委任管理者アカウントは AWS Security Hub 設定ポリシーを削除できます。また、委任管理者アカウントは設定ポリシーを保持したまま、特定のアカウントや組織単位 (OU) との関連付けを解除することもできます。

以下のセクションでは、この両方のオプションについて説明します。

設定ポリシーの削除

設定ポリシーを削除すると、組織には存在しなくなります。ターゲットアカウント、OU、および組織ルートは設定ポリシーを使用できなくなります。削除された設定ポリシーに関連付けられていたターゲットは、最も近い親の設定ポリシーを継承するか、最も近い親がセルフマネージド型の場合はセルフマネージド型になります。ターゲットに別の設定を使用する場合は、そのターゲットを新しい設定ポリシーに関連付けることができます。詳細については、「Security Hub 設定ポリシーの作成と関連付け」を参照してください。

適切なセキュリティカバレッジを確保するために、少なくとも 1 つの設定ポリシーを作成して組織に関連付けることをお勧めします。

設定ポリシーを削除する前に、現在適用されているアカウント、OU、またはルートからポリシーの関連付けを解除する必要があります。

任意の方法を選択し、その手順に従って設定ポリシーを削除します。

Console

設定ポリシーを削除するには

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。

   ホームリージョンの Security Hub 委任管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで、[設定]、[設定] の順に選択します。
3. [Policies] タブを選択します。削除する設定ポリシーを選択し、[削除] を選択します。設定ポリシーがまだアカウントまたは OU に関連付けられている場合は、削除する前にポリシーとそれらのターゲットとの関連付けを解除するように求められます。
4. 確認メッセージを確認します。「**`confirm`**」と入力し、[削除] を選択します。

API

設定ポリシーを削除するには

ホームリージョンの Security Hub 委任管理者アカウントから DeleteConfigurationPolicy API を呼び出します。

削除する設定ポリシーの Amazon リソースネーム (ARN) または ID を指定します。`ConflictException` エラーを受け取った場合でも、設定ポリシーは組織内のアカウントまたは OU に適用されます。このエラーを解決するには、削除する前に、設定ポリシーとこれらのアカウントまたは OU との関連付けを解除します。

設定ポリシーを削除する API リクエストの例:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

設定ポリシーを削除するには

ホームリージョンの Security Hub 委任管理者アカウントで、delete-configuration-policy コマンドを実行します。

削除する設定ポリシーの Amazon リソースネーム (ARN) または ID を指定します。`ConflictException` エラーを受け取った場合でも、設定ポリシーは組織内のアカウントまたは OU に適用されます。このエラーを解決するには、削除する前に、設定ポリシーとこれらのアカウントまたは OU との関連付けを解除します。

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

アカウントと OU からの設定の関連付けの解除

委任管理者アカウントで、ターゲットアカウント、OU、またはルートと、現在適用されている設定ポリシーまたはセルフマネージド型設定との関連付けを解除できます。ターゲットの関連付けの解除は、適用された設定からのみ可能で、継承された設定からはできません。継承された設定を変更するには、影響を受けるアカウントまたは OU に設定ポリシーまたはセルフマネージド型の動作を適用します。また、必要な変更を含む新しい設定ポリシーを、最も近い親に適用することもできます。

関連付けを解除しても設定ポリシーは削除されません。ポリシーはアカウントに保持されるため、組織内の他のターゲットと関連付けることができます。関連付けの解除が完了すると、影響を受けるターゲットは、設定ポリシーまたは最も近い親のセルフマネージド型の動作を継承します。継承が可能な設定がない場合、ターゲットは関連付け解除前の設定を保持しますが、セルフマネージド型になります。

任意の方法を選択し、その手順に従って、アカウント、OU、またはルートと現在の設定との関連付けを解除します。

Console

アカウントまたは OU と現在の設定との関連付けを解除するには

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。

   ホームリージョンの Security Hub 委任管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで、[設定]、[設定] の順に選択します。
3. [組織] タブで、現在の設定との関連付けを解除したいアカウント、OU、またはルートを選択します。[Edit] (編集) を選択します。

4. 委任管理者がターゲットに直接ポリシーを適用できるようにするには、[構成を定義] ページの [管理] で、適用される [ポリシー] を選択します。ターゲットに最も近い親の設定を継承する場合は、[継承済み] を選択します。いずれの場合も、委任管理者がターゲットの設定をコントロールします。アカウントまたは OU に独自の設定を管理する場合は、[セルフマネージド] を選択します。
5. 変更を確認したら、[次へ] と [適用] を選択します。このアクションは、対象範囲内のアカウントまたは OU の既存の設定が現在の選択内容と矛盾する場合、それらの設定を上書きします。

API

アカウントまたは OU と現在の設定との関連付けを解除するには

1. ホームリージョンの Security Hub 委任管理者アカウントから StartConfigurationPolicyDisassociation API を呼び出します。
2. `ConfigurationPolicyIdentifier` の場合、関連付けを解除する設定ポリシーの Amazon リソースネーム (ARN) または ID を指定します。セルフマネージド型の動作との関連付けを解除するには、このフィールドに `SELF_MANAGED_SECURITY_HUB` を指定します。
3. `Target` の場合、この設定ポリシーとの関連付けを解除するアカウント、OU、またはルートを指定します。

設定ポリシーの関連付けを解除する API リクエストの例:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

アカウントまたは OU と現在の設定との関連付けを解除するには

1. ホームリージョンの Security Hub 委任管理者アカウントで、start-configuration-policy-disassociation コマンドを実行します。

2. `configuration-policy-identifier` の場合、関連付けを解除する設定ポリシーの Amazon リソースネーム (ARN) または ID を指定します。セルフマネージド型の動作との関連付けを解除するには、このフィールドに `SELF_MANAGED_SECURITY_HUB` を指定します。
3. `target` の場合、この設定ポリシーとの関連付けを解除するアカウント、OU、またはルートを指定します。

設定ポリシーの関連付けを解除するコマンドの例:

```
aws securityhub --region us-east-1 start-configuration-policy-disassociation \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"RootId": "r-f6g7h8i9j0example"}'
```

標準またはコントロールのコンテキストの中央設定

中央設定は、 AWS Security Hub コンソールの [設定] ページから、または特定のセキュリティ標準またはセキュリティコントロールのコンテキストで使用できます。この機能をコンテキストで使用すると、既存のワークフローと統合した方法で、組織全体の標準とコントロールを設定できます。さらに、検出結果を確認しながら、どの標準とコントロールが自分の環境に最も関連性があるかを見出し、同時に設定することができます。

コンテキスト内の設定は、Security Hub コンソールでのみ実行できます。プログラムによって UpdateConfigurationPolicy API を呼び出し、特定の標準やコントロールの組織内での設定方法を変更する必要があります。

コンテキスト内のセキュリティ標準の設定

手順に従い、中央設定を使用してコンテキスト内のセキュリティ標準を設定します。

コンテキスト内のセキュリティ標準を設定するには (コンソールのみ)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub でコンソールを開きます。

   ホームリージョンの Security Hub 委任管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで [セキュリティ標準] を選択します。

3. 設定する標準で、[設定] を選択します。特定の標準を選択し、標準の詳細ページから [設定] を選択することもできます。コンソールには、既存の Security Hub 設定ポリシー (設定ポリシー) と各ポリシーにおけるこの標準のステータスが一覧表示されます。
4. 各設定ポリシーの標準を有効または無効にするオプションを選択します。
5. 変更を加えたら、[次へ] を選択します。
6. 変更内容を確認したら、[適用] を選択します。このアクションは、設定ポリシーに関連付けられているすべてのアカウントと OU に影響します。設定はホームリージョンとリンクされたすべてのリージョンで有効になります。

コンテキスト内のセキュリティコントロールの設定

手順に従い、中央設定を使用してコンテキスト内のセキュリティコントロールを設定します。

コンテキスト内のセキュリティコントロールを設定するには (コンソールのみ)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub でコンソールを開きます。

   ホームリージョンの Security Hub 委任管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで [コントロール] を選択します。
3. 特定のコントロールを選択し、[設定] を選択します。コンソールには、現在の設定ポリシーと、各ポリシーにおけるコントロールのステータスが一覧表示されます。
4. 各設定ポリシーのコントロールを有効または無効にするオプションを選択します。コントロールパラメーターをカスタマイズすることもできます。
5. 変更を加えたら、[次へ] を選択します。
6. 変更内容を確認したら、[適用] を選択します。このアクションは、設定ポリシーに関連付けられているすべてのアカウントと OU に影響します。設定はホームリージョンとリンクされたすべてのリージョンで有効になります。

中央設定の使用を停止する

AWS Security Hub で中央設定の使用を停止すると、委任管理者は複数の AWS アカウント、組織単位 (OU)、および AWS リージョンにわたる Security Hub、セキュリティ基準、およびのセキュリティコントロールを設定できなくなります。代わりに、組織アカウントは各リージョンでその設定のほとんどを個別に設定する必要があります。

> **Important**
>
> 中央設定の使用を停止する前に、まずアカウントと OU を現在の設定から切り離す必要があります (それが設定ポリシーか、セルフマネージド型動作であるかは関係ありません)。
> 中央設定の使用を停止する前に、設定ポリシーも削除する必要があります。

中央設定を停止すると、次の変更が行われます。

- 委任管理者は、組織の設定ポリシーを作成できなくなります。
- 設定ポリシーが適用または継承されたアカウントは、現在の設定を保持しますが、セルフマネージド型になります。
- 組織はローカル設定に切り替わります。ローカル設定では、Security Hub 設定の大部分を組織アカウントとリージョンごとに個別に設定する必要があります。委任管理者は、Security Hub、デフォルトのセキュリティ基準、および新しい組織アカウントのデフォルト標準に含まれるすべてのコントロールを自動的に有効にすることを選択できます。デフォルトの標準は、AWS Foundational Security Best Practices (FSBP) と Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 です。これらの設定は現在のリージョンでのみ有効で、新しい組織アカウントにのみ影響します。委任管理者は、どの標準がデフォルトになるかを変更できません。ローカル設定では、設定ポリシーの使用や OU レベルでの設定はサポートされていません。

中央設定の使用を停止しても、委任管理者アカウントの ID は変わりません。ホームリージョンとリンクされたリージョンも変更されません (ホームリージョンは集約リージョンと呼ばれることになり、検出結果の集約に使用できます)。

お好みの方法を選択し、手順に従って中央設定の使用を停止し、ローカル設定に切り替えます。

Security Hub console

中央設定の使用を停止するには

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。

   ホームリージョンの Security Hub 委任管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで、[設定]、[設定] の順に選択します。
3. [概要] セクションで [編集] を選択します。

4. [組織設定を編集] ボックスで、[ローカル設定] を選択します。まだ行っていない場合は、中央設定を停止する前に、現在の設定ポリシーの関連付けを解除して削除するよう求められます。セルフマネージド型として指定されているアカウントまたは OU は、セルフマネージド型設定との関連付けを解除する必要があります。これをコンソールで行うには、各セルフマネージド型アカウントまたは OU の管理タイプを [一元管理] と [自分の組織から継承] に変更します。
5. 必要に応じて、新しい組織アカウントのローカル設定のデフォルト設定を選択します。
6. [確認] を選択します。

Security Hub API

中央設定の使用を停止するには

1. UpdateOrganizationConfiguration API を呼び出します。
2. `OrganizationConfiguration` オブジェクト内の `ConfigurationType` フィールドを `LOCAL` に設定します。既存の設定ポリシーまたはポリシーの関連付けがある場合、API はエラーを返します。設定ポリシーの関連付けを解除するには、`StartConfigurationPolicyDisassociation` API を呼び出します。設定ポリシーを削除するには、`DeleteConfigurationPolicy` API を呼び出します。
3. 新しい組織アカウントで Security Hub を自動的に有効にする場合は、`AutoEnable` フィールドを `true` に設定します。デフォルトでは、このフィールドの値は `false` で、Security Hub は新しい組織アカウントで自動的には有効になりません。必要に応じて、新しい組織アカウントでデフォルトのセキュリティ基準を自動的に有効にする場合は、`AutoEnableStandards` フィールドを `DEFAULT` に設定します。これは、デフォルト値です。新しい組織アカウントでデフォルトのセキュリティ基準を自動的に有効化しない場合は、`AutoEnableStandards` フィールドを `NONE` に設定します。

API リクエストの例:

```
{
    "AutoEnable": true,
    "OrganizationConfiguration": {
        "ConfigurationType" : "LOCAL"
    }
}
```

AWS CLI

中央設定の使用を停止するには

1. update-organization-configuration コマンドを実行します。
2. organization-configuration オブジェクト内の ConfigurationType フィールドを LOCAL に設定します。既存の設定ポリシーまたはポリシーの関連付けがある場合、このコマンドはエラーを返します。設定ポリシーの関連付けを解除するには、start-configuration-policy-disassociation コマンドを実行します。設定ポリシーを削除するには、delete-configuration-policy コマンドを実行します。
3. 新しい組織アカウントで Security Hub を自動的に有効にする場合は、auto-enable パラメータを使用します。デフォルトでは、このパラメータの値は no-auto-enable で、Security Hub は新しい組織アカウントで自動的には有効になりません。必要に応じて、新しい組織アカウントでデフォルトのセキュリティ基準を自動的に有効にする場合は、auto-enable-standards フィールドを DEFAULT に設定します。これは、デフォルト値です。新しい組織アカウントでデフォルトのセキュリティ基準を自動的に有効化しない場合は、auto-enable-standards フィールドを NONE に設定します。

```
aws securityhub --region us-east-1 update-organization-configuration \
--auto-enable \
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

管理者アカウントおよびメンバーアカウントの管理

AWS 環境に複数のアカウントがある場合は、AWS Security Hub を使用するアカウントをメンバーアカウントとして扱い、単一の管理者アカウントに関連付けることができます。管理者は全体的なセキュリティ状況を監視し、メンバーアカウントに対して許可されたアクションを実行できます。管理者は、推定使用コストのモニタリングやアカウントクォータの評価など、さまざまなアカウント管理および管理タスクも大規模に実行できます。

メンバーアカウントを管理者と関連付けるには、Security Hub を AWS Organizations と統合する方法と、Security Hub でメンバーシップの招待を手動で送信して受け入れる方法の 2 つがあります。

AWS Organizations を使用したアカウントの管理

AWS Organizations はグローバルアカウント管理サービスであり、AWS 管理者は複数の AWS アカウントを統合して管理できます。予算、セキュリティ、コンプライアンスのニーズをサポートするように設計されたアカウント管理および一括請求 (コンソリデーティッドビリング) 機能が備わっています。追加料金なしで提供され、AWS Security Hub や Amazon Macie、Amazon GuardDuty を含む、複数の AWS のサービスと統合されています。詳細については、「AWS Organizations ユーザーガイド」を参照してください。

Security Hub と AWS Organizations を統合する場合は、Organizations 管理アカウントで Security Hub 委任管理者を指定します。Security Hub は、指定された AWS リージョン委任管理者アカウントで自動的に有効になります。

委任された管理者を指定した後は、中央設定を使用して Security Hub でアカウントを管理することをお勧めします。これは、Security Hub をカスタマイズし、組織の適切なセキュリティカバレッジを確保するための最も効率的な方法です。

中央設定により、委任された管理者は Security Hub をリージョンごとに設定するのではなく、複数の組織アカウントとリージョンにわたってカスタマイズできます。組織全体の設定ポリシーを作成することも、アカウントや OU ごとに異なる設定ポリシーを作成することもできます。ポリシーでは、関連するアカウントで Security Hub を有効にするか無効にするか、およびどのセキュリティ標準とコントロールを有効にするかを指定します。

委任された管理者は、アカウントを一元管理型またはセルフマネージド型として指定できます。一元管理型アカウントは、委任された管理者のみが設定できます。セルフマネージド型アカウントは、独自の設定を指定できます。

中央設定にオプトインしない場合、委任された管理者が Security Hub を設定できる権限は、ローカル設定と呼ばれるより限定的な権限に制限されます。ローカル設定では、委任された管理者は、現在のリージョンの新しい組織アカウントで Security Hub とデフォルトのセキュリティ標準を自動的に有効にできます。ただし、既存のアカウントではこれらの設定を使用しないため、アカウントを組織に追加した後に設定のずれが生じる可能性があります。

これらの新しいアカウント設定に加え、ローカル設定もアカウントおよびリージョンに固有です。各組織のアカウントで、Security Hub のサービス、標準、コントロールをリージョンごとに個別に設定する必要があります。また、ローカル設定では設定ポリシーの使用もサポートされていません。

招待によるアカウントの手動での管理

スタンドアロンアカウントをお持ちの場合、または Organizations と統合していない場合は、Security Hub で招待によってメンバーアカウントを手動で管理する必要があります。スタンドアロンアカウントは Organizations と統合できないため、手動で管理する必要があります。今後アカウントを追加する場合は、中央設定を使用して AWS Organizations と統合することをお勧めします。

手動によるアカウント管理を使用する場合は、アカウントを Security Hub 管理者として指定します。管理者アカウントは、メンバーアカウントのデータを表示したり、メンバーアカウントの検出結果に基づいて特定のアクションを実行したりできます。メンバー候補アカウントが招待を承諾すると、Security Hub 管理者は他のアカウントをメンバーアカウントに招待し、管理者とメンバーの関係が確立されます。

手動によるアカウント管理では、設定ポリシーの使用がサポートされていません。設定ポリシーがない場合、管理者はアカウントごとに変数設定を行うことになり Security Hub を一元的にカスタマイズすることができません。代わりに、各組織アカウントが各リージョンで個別に Security Hub を有効にして設定する必要があります。これにより、Security Hub を使用するすべてのアカウントとリージョンで適切なセキュリティカバレッジを確保することがより困難になり、時間もかかります。また、メンバーアカウントが管理者の入力なしに独自の設定を指定できるため、設定のずれが生じる可能性もあります。

招待によってアカウントを管理する方法については、「招待によるアカウントの管理」を参照してください。

によるアカウントの管理 AWS Organizations

AWS Security Hub と統合し AWS Organizations、組織内のアカウントの Security Hub を管理できます。

Security Hub を と統合するには AWS Organizations、 で組織を作成します AWS Organizations。組織における Security Hub 委任管理者は、Organizations の管理アカウントによって指定されます。その後、委任された管理者は組織内の他のアカウントに対して Security Hub を有効にし、それらのアカウントを Security Hub のメンバーアカウントとして追加して、メンバーアカウントに対して許可されたアクションを実行できるようにします。Security Hub 委任管理者は、最大 10,000 のメンバーアカウントに対して Security Hub を有効にし、管理できます。

委任された管理者が設定できる範囲は、中央設定を使用するかどうかによって異なります。中央設定を有効にすると、各メンバーアカウントや AWS リージョンで個別に Security Hub を設定する必要がなくなります。委任された管理者は、特定のメンバーアカウントや複数のリージョンの組織単位 (OU) に特定の Security Hub 設定を適用できます。

Security Hub 委任管理者アカウントは、メンバーアカウントに対して次のアクションを実行できます。

- 中央設定を使用する場合は、Security Hub の設定ポリシーを作成し、メンバーアカウントと OU に対して Security Hub を一元的に設定する。設定ポリシーを使用して、Security Hub、標準、コントロールを有効または無効にできます。
- 組織に追加された新しいアカウントを Security Hub メンバーアカウントとして自動的に処理する。中央設定を使用する場合、OU に関連付けられた設定ポリシーには、その OU に含まれる既存のアカウントと新しいアカウントが含まれます。
- 既存の組織アカウントを Security Hub メンバーアカウントとして処理する。中央設定を使用すると、この処理は自動的に行われます。
- 組織に属するメンバーアカウントの関連付けを解除します。中央設定を使用している場合は、メンバーアカウントをセルフマネージド型として指定してからでないと、そのアカウントの関連付けを解除できません。または、Security Hub を無効にする設定ポリシーを、特定の一元管理型メンバーアカウントに関連付けることもできます。

委任された管理者がメンバーアカウントに対して実行できるアクションの完全なリストについては、「アカウントに許可されるアクション」を参照してください。

このセクションのトピックでは、Security Hub を と統合する方法 AWS Organizations と、組織内のアカウントの Security Hub を管理する方法について説明します。該当する場合は、各セクションで、中央設定を使用するユーザーにとっての管理上の利点と相違点について説明します。

トピック

- Security Hub と の統合 AWS Organizations

- 新しい組織アカウントで Security Hub を自動的に有効にする
- 新しい組織アカウントで Security Hub を手動で有効にする
- 組織からメンバーアカウントの関連付けを解除する

Security Hub と の統合 AWS Organizations

AWS Security Hub と を統合するには AWS Organizations、Organizations で組織を作成し、組織管理アカウントを使用して委任された Security Hub 管理者アカウントを指定します。これにより、Security Hub が Organizations の信頼されたサービスとして有効になります。また、委任された管理者アカウントの現在の AWS リージョン で Security Hub を有効にし、委任された管理者がメンバーアカウントの Security Hub を有効にしたり、メンバーアカウントのデータを表示したり、メンバーアカウントで許可されているその他のアクションを実行したりできるようにします。

中央設定を使用する場合、委任された管理者は組織のアカウントで Security Hub サービス、標準、およびコントロールを設定する方法を指定する Security Hub 設定ポリシーを作成することもできます。

組織の作成

組織は、 を統合するために作成するエンティティであり AWS アカウント 、単一のユニットとして管理できます。

組織を作成するには、 AWS Organizations コンソールを使用するか、 または SDK APIs AWS CLI のいずれかのコマンドを使用します。詳細の手順については、「AWS Organizations ユーザーガイド」の「組織の作成」を参照してください。

を使用して AWS Organizations 、組織内のすべてのアカウントを一元的に表示および管理できます。組織には、1 つの管理アカウントと、ゼロ以上のメンバーアカウントを含みます。アカウントを階層ツリーのような構造に編成し、ルートを最上部に置いて組織単位 (OU) をその下にネストすることができます。各アカウントは、ルートの下に直接置くか、階層内の OU のいずれかに配置できます。OU は特定のアカウントのコンテナです。例えば、財務運用に関連するアカウントをすべて含めた財務 OU を作成できます。

委任された Security Hub 管理者の選択に関する推奨事項

手動の招待プロセスから管理者アカウントがあり、 でアカウント管理に移行する場合は AWS Organizations、そのアカウントを委任された Security Hub 管理者として指定することをお勧めします。

Security Hub APIs とコンソールでは、組織管理アカウントを委任された Security Hub 管理者にすることができますが、2 つの異なるアカウントを選択することをお勧めします。これは、請求管理のために組織の管理アカウントにアクセスできるユーザーと、セキュリティ管理のために Security Hub にアクセスする必要があるユーザーが異なる可能性があるためです。

複数のリージョンで、同一の委任管理者を使用することが推奨されます。中央設定にオプトインすると、Security Hub によってホームリージョンとリンクされたリージョンで同一の委任管理者が自動的に指定されます。

委任された管理者を設定するアクセス許可を確認する

委任された Security Hub 管理者アカウントを指定して削除するには、組織管理アカウントに Security Hub の `EnableOrganizationAdminAccount`および `DisableOrganizationAdminAccount`アクションに対するアクセス許可が必要です。Organizations の管理アカウントには、Organizations の管理権限も必要です。

必要な許可をすべて付与するには、組織の管理アカウントの IAM プリンシパルに次の Security Hub マネージドポリシーをアタッチします。

- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess

委任管理者の指定

委任された Security Hub 管理者アカウントを指定するには、Security Hub コンソール、Security Hub API、または を使用できます AWS CLI。Security Hub は委任された管理者を現在の AWS リージョン にのみ設定するため、他のリージョンでもこのアクションを繰り返す必要があります。中央設定の使用を開始すると、Security Hub によってホームリージョンとリンクされたリージョンで同一の委任管理者が自動的に設定されます。

組織管理アカウントは、委任された Security Hub 管理者アカウントを指定するために Security Hub を有効にする必要はありません。

組織管理アカウントは、委任された Security Hub 管理者アカウントではないことをお勧めします。ただし、組織管理アカウントを Security Hub の委任された管理者として選択すると、管理アカウントで Security Hub が有効になっている必要があります。管理アカウントの Security Hub が有効になっていない場合は、Security Hub を手動で有効にする必要があります。Security Hub を組織管理アカウントで自動的に有効にすることはできません。

> **Note**
>
> 次のいずれかの方法を使用して、委任された Security Hub 管理者を指定する必要があります。Organizations APIs で委任された Security Hub 管理者を指定しても、Security Hub には反映されません。
> 任意の方法を選択し、手順に従って委任された Security Hub 管理者アカウントを指定します。

Security Hub console

オンボーディング中に委任された Security Hub 管理者を指定するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. [Go to Security Hub] (Security Hub に移動) を選択します。組織管理アカウントにサインインするように求められます。
3. [委任された管理者アカウント] セクションの [委任された管理者を指定] ページで、委任された管理者アカウントを指定します。委任された管理者には、他の AWS セキュリティおよびコンプライアンスサービスと同一の設定を選択することをお勧めします。
4. [委任された管理者を設定] を選択します。中央設定でオンボーディングを続行するには、委任された管理者アカウントにサインインするよう求められます (まだサインインしていない場合)。中央設定を開始しない場合は、[キャンセル] を選択します。委任された管理者は設定されますが、中央設定はまだ使用しません。

設定ページから委任された Security Hub 管理者を指定するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. Security Hub ナビゲーションペインで、[Settings] (設定) を選択します。次に [Generate] (生成) を選択します。
3. Security Hub 管理者アカウントが現在割り当てられている場合は、新しいアカウントを指定する前に、現在のアカウントを削除する必要があります。

   現在のアカウントを削除するには、[Delegated Administrator] (代理管理者) で、[Remove] (削除) を選択します。
4. Security Hub 管理者アカウントとして指定するアカウントのアカウント ID を入力します。。

すべてのリージョンで同じ Security Hub 管理者アカウントを指定する必要があります。他のリージョンで指定したアカウントとは異なるアカウントを指定すると、コンソールはエラーを返します。

5. [委任] を選択します。

Security Hub API, AWS CLI

組織管理アカウントから、Security Hub API の EnableOrganizationAdminAccountオペレーションを使用します。を使用している場合は AWS CLI、 enable-organization-admin-account コマンドを実行します。委任された Security Hub 管理者の AWS アカウント ID を指定します。

次の例では、委任された Security Hub 管理者を指定します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub enable-organization-admin-account --admin-account-id 123456789012
```

委任管理者の削除または変更

> **Warning**
>
> 中央設定を使用する場合、Security Hub コンソールまたは Security Hub API を使用して委任された管理者アカウントを変更または削除することはできません。組織管理アカウントが AWS Organizations コンソールまたは AWS Organizations APIs を使用して委任された Security Hub 管理者を変更または削除する場合、Security Hub は自動的に中央設定を停止し、設定ポリシーとポリシーの関連付けを削除します。メンバーアカウントには、委任された管理者が変更または削除される前の設定が保持されます。

委任された Security Hub 管理者アカウントを削除できるのは、組織管理アカウントのみです。

委任された Security Hub 管理者を変更するには、まず現在の委任された管理者アカウントを削除してから、新しいアカウントを指定する必要があります。

Security Hub コンソールを使用して、あるリージョンの委任管理者を削除すると、その管理者はすべてのリージョンから自動的に削除されます。

Security Hub API は、委任された Security Hub 管理者アカウントを API コールまたはコマンドが発行されたリージョンからのみ削除します。他のリージョンでもこの操作を繰り返す必要があります。

Organizations API を使用して委任された Security Hub 管理者アカウントを削除すると、すべてのリージョンで自動的に削除されます。

委任された管理者の削除 (Organizations API、 AWS CLI)

Organizations を使用して、すべてのリージョンで委任された Security Hub 管理者を削除できます。

中央設定を使用してアカウントを管理している場合、委任された管理者アカウントを削除すると、設定ポリシーとポリシーの関連付けも削除されます。メンバーアカウントには、委任された管理者が変更または削除される前の設定が保持されます。ただし、削除済みの委任管理者からは、これらのアカウントを管理できなくなります。これらはリージョンごとに個別に設定する必要があるセルフマネージド型アカウントになります。

任意の方法を選択し、手順に従って で委任された Security Hub 管理者アカウントを削除します AWS Organizations。

Organizations API, AWS CLI

委任された Security Hub 管理者を削除するには

組織管理アカウントから、Organizations API の DeregisterDelegatedAdministratorオペレーションを使用します。を使用している場合は AWS CLI、 deregister-delegated-administrator コマンドを実行します。委任された管理者のアカウント ID と Security Hub のサービスプリンシパル を指定しますsecurityhub.amazonaws.com。

次の例では、委任された Security Hub 管理者を削除します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws organizations deregister-delegated-administrator --account-id 123456789012 --
service-principal securityhub.amazonaws.com
```

委任された管理者の削除 (Security Hub コンソール)

Security Hub コンソールを使用して、すべてのリージョンで委任された Security Hub 管理者を削除できます。

委任された Security Hub 管理者アカウントが削除されると、メンバーアカウントは削除された委任された Security Hub 管理者アカウントから関連付けが解除されます。

ただし、Security Hub はメンバーアカウントで引き続き有効になっています。新しい Security Hub 管理者がメンバーアカウントとして有効にするまで、これらのアカウントはスタンドアロンアカウントになります。

組織管理アカウントが Security Hub で有効なアカウントでない場合は、「セキュリティハブへようこそ」ページの オプションを使用します。

委任された Security Hub 管理者アカウントを Security Hub へようこそページから削除するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. [Go to Security Hub] (Security Hub に移動) を選択します。
3. [Delegated Administrator] (代理管理者) で、[Remove] (削除) を選択します。

組織管理アカウントが Security Hub で有効なアカウントである場合、[Settings] (設定) ページの [General] (全般) タブのオプションを使用します。

設定ページから委任された Security Hub 管理者アカウントを削除するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. Security Hub ナビゲーションペインで、[Settings] (設定) を選択します。次に [Generate] (生成) を選択します。
3. [Delegated Administrator] (代理管理者) で、[Remove] (削除) を選択します。

委任された管理者の削除 (Security Hub API、 AWS CLI)

の Security Hub API または Security Hub オペレーションを使用して AWS CLI 、委任された Security Hub 管理者を削除できます。上記のいずれかの方法で委任された管理者を削除する場合、API コールまたはコマンドが発行されたリージョンでのみ削除されます。Security Hub は他のリージョンを更新せず、 の委任管理者アカウントも削除しません AWS Organizations。

任意の方法を選択し、以下の手順に従って Security Hub で委任された Security Hub 管理者アカウントを削除します。

Security Hub API, AWS CLI

委任された Security Hub 管理者を削除するには

組織管理アカウントから、Security Hub API の DisableOrganizationAdminAccountオペレーションを使用します。を使用している場合は AWS CLI、 disable-organization-admin-account コマンドを実行します。委任された Security Hub 管理者のアカウント ID を指定します。

次の例では、委任された Security Hub 管理者を削除します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

と Security Hub の統合を無効にする AWS Organizations

AWS Organizations 組織が と統合されると AWS Security Hub、Organizations 管理アカウントは統合を無効にできます。Organizations 管理アカウントのユーザーは、 AWS Organizationsの Security Hub に対する信頼されたアクセスを無効にすることができます。

Security Hub の信頼されたアクセスを無効化すると、以下が起こります。

- Security Hub は、 で信頼されたサービスとしてのステータスを失います AWS Organizations。
- Security Hub 委任管理者アカウントは、すべての AWS リージョンですべての Security Hub メンバーアカウントの Security Hub の設定、データ、およびリソースにアクセスできなくなります。
- 中央設定を使用していた場合、Security Hub は組織での中央設定の使用を自動的に停止します。設定ポリシーとポリシーの関連付けは削除されます。アカウントでは、信頼されたアクセスを無効にする前の設定が保持されます。
- Security Hub のすべてのメンバーアカウントがスタンドアロンアカウントになり、現在の設定が保持されます。Security Hub が 1 つ以上のリージョン内のメンバーアカウントに対して有効化されている場合、Security Hub はそのリージョン内のアカウントに対して有効化された状態が継続します。有効になっている標準とコントロールも変わりません。これらの設定は、アカウントやリージョンごとに個別に変更できます。ただし、そのアカウントはどのリージョンの委任管理者とも関連付けられなくなります。

信頼されたサービスアクセスを無効にする結果の詳細については、 ユーザーガイドの「他の AWS Organizations で AWS のサービスを使用するAWS Organizations 」を参照してください。

信頼されたアクセスを無効にするには、 AWS Organizations コンソール、Organizations API、または を使用できます AWS CLI。Security Hub の信頼されたサービスへのアクセスを無効にできるの

は、Organizations 管理アカウントのユーザーのみです。必要なアクセス許可に関する詳細は、AWS Organizations ユーザーガイドの信頼できるアクセスを無効にするために必要なアクセス許可を参照してください。

信頼されたアクセスを無効にする前に、必要に応じて組織の委任管理者に連絡して、メンバーアカウントの Security Hub を無効にし、それらのアカウントの Security Hub リソースをクリーンアップしてください。

お好みの方法を選択し、手順に従って、Security Hub の信頼されたアクセスを無効にします。

Organizations console

Security Hub の信頼されたアクセスを無効にするには

1. AWS Organizations 管理アカウントの認証情報 AWS Management Console を使用して にサインインします。
2. Organizations コンソール (https://console.aws.amazon.com/organizations/) を開きます。
3. ナビゲーションペインで [Services (サービス)] を選択します。
4. [統合されたサービス] で [AWS Security Hub] を選択します。
5. Disable trusted access (信頼されたアクセスを無効にする) を選択します。
6. 信頼されたアクセスを無効化することを確認します。

Organizations API

Security Hub の信頼されたアクセスを無効にするには

AWS Organizations API の DisableAWSServiceAccess オペレーションを呼び出します。`ServicePrincipal` パラメータで、Security Hub サービスプリンシパル (`securityhub.amazonaws.com`) を指定します。

AWS CLI

Security Hub の信頼されたアクセスを無効にするには

AWS Organizations API の disable-aws-service-access コマンドを実行します。`service-principal` パラメータで、Security Hub サービスプリンシパル (`securityhub.amazonaws.com`) を指定します。

例:

```
aws organizations disable-aws-service-access --service-principal
 securityhub.amazonaws.com
```

新しい組織アカウントで Security Hub を自動的に有効にする

新しいアカウントが組織に参加すると、 AWS Security Hub コンソールのアカウントページのリストに追加されます。組織アカウントの場合、[Type] (タイプ) は [By organization] (組織別) になります。デフォルトでは、組織を追加しても新しいアカウントが Security Hub メンバーになることはありません。ステータスは、[Not a member] (メンバーではない) です。委任管理者アカウントは、新しいアカウントをメンバーとして自動的に追加し、組織に参加するときにこれらのアカウントで Security Hub を有効にできます。

> **Note**
>
> 多くの AWS リージョン は に対してデフォルトでアクティブになっていますが AWS アカウント、特定のリージョンを手動でアクティブ化する必要があります。これらのリージョンは、このドキュメントではオプトインリージョンと呼ばれます。オプトインリージョンの新しいアカウントで Security Hub を自動的に有効にするには、アカウントでそのリージョンを最初にアクティブ化する必要があります。アカウント所有者のみがオプトインリージョンをアクティブ化できます。オプトインリージョンの詳細については、「AWS リージョン を使用できるアカウントを指定する」を参照してください。

このプロセスは、中央設定 (推奨) を使用するかローカル設定を使用するかによって異なります。

新しい組織アカウントを自動的に有効にする (中央設定)

中央設定 を使用する場合、Security Hub が有効になっている設定ポリシーを作成することで、新規および既存の組織アカウントで Security Hub を自動的に有効にできます。その後、ポリシーを組織のルートまたは特定の組織単位 (OUsに関連付けることができます。

Security Hub が有効になっている設定ポリシーを特定の OU に関連付けると、その OU に属するすべてのアカウント (既存および新規) で Security Hub が自動的に有効になります。OU に属さない新しいアカウントはセルフマネージド型で、Security Hub が自動的に有効になることはありません。Security Hub が有効になっている設定ポリシーをルートに関連付けると、組織に追加するすべてのアカウント (既存および新規) で Security Hub が自動的に有効になります。例外は、アカウントがアプリケーションまたは継承によって異なるポリシーを使用している場合や、セルフマネージド型である場合です。

設定ポリシーでは、OU で有効にするセキュリティ標準とコントロールを定義することもできます。有効な標準に関するコントロールの検出結果を生成するには、OU のアカウントで、必要なリソースを記録する AWS Config ように有効化および設定されている必要があります。 AWS Config 録画の詳細については、「 の有効化と設定 AWS Config」を参照してください。

設定ポリシーの作成手順については、「Security Hub 設定ポリシーの作成と関連付け」を参照してください。

新しい組織アカウントを自動的に有効にする (ローカル設定)

ローカル設定を使用して自動有効化をオンにすると、Security Hub で新しい組織アカウントがメンバーとして追加され、現在のリージョンでそのアカウントの Security Hub が有効になります。他のリージョンは影響を受けません。また、自動有効化をオンにしても、既にメンバーアカウントとして追加されていない限り、既存の組織アカウントで Security Hub が有効になることはありません。

自動有効化をオンにしてから現在のリージョンで新しいアカウントが組織に追加されると、そのアカウントのデフォルトのセキュリティ標準も自動的に有効になります。デフォルトの標準は AWS 、Foundational Security Best Practices (FSBP) と Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 です。デフォルトの標準を変更することはできません。組織全体で他の標準を有効にする場合や、特定のアカウントや OU の標準を有効にする場合は、中央設定を使用することをお勧めします。

デフォルトの標準 (およびその他の有効な標準) のコントロール結果を生成するには、組織内のアカウントで必要なリソースを記録する AWS Config ように を有効にして設定する必要があります。AWS Config 録画の詳細については、「 の有効化と設定 AWS Config」を参照してください。

お好みの方法を選択し、手順に従って、新しい組織アカウントの Security Hub を自動的に有効にします。これらの手順は、ローカル設定を使用する場合にのみ適用されます。

Security Hub console

新しい組織アカウントを Security Hub メンバーとして自動的に有効にするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   委任された管理者アカウントの認証情報を使用してサインインします。
2. Security Hub のナビゲーションペインの [設定] で、[設定] を選択します。
3. [アカウント] セクションで、[アカウントの自動有効化] をオンにします。

Security Hub API

新しい組織アカウントを Security Hub メンバーとして自動的に有効にするには

委任された管理者のアカウントで、`UpdateOrganizationConfiguration` API を呼び出します。`AutoEnable` フィールドを `true` に設定すると、新しい組織アカウントで Security Hub が自動的に有効になります。

AWS CLI

新しい組織アカウントを Security Hub メンバーとして自動的に有効にするには

委任された管理者アカウントで、`update-organization-configuration` コマンドを実行します。新しい組織アカウントで Security Hub を自動的に有効にするには、`auto-enable` パラメータを追加します。

```
aws securityhub update-organization-configuration --auto-enable
```

新しい組織アカウントで Security Hub を手動で有効にする

新しい組織アカウントが組織に加わるときに Security Hub を自動的に有効にしない場合は、それらのアカウントをメンバーとして追加し、組織への加わった後に手動で Security Hub を有効にできます。また、以前に組織との関連付けを解除した AWS アカウント で Security Hub を手動で有効にする必要があります。

> **Note**
>
> 中央設定を使用している場合、このセクションの内容は適用されません。中央設定を使用する場合は、指定したメンバーアカウントや組織単位 (OU) で Security Hub を有効にする設定ポリシーを作成できます。また、それらのアカウントや OU で特定の標準やコントロールを有効にすることもできます。

アカウントが既に別の組織内のメンバーアカウントである場合、アカウントの Security Hub を有効にすることはできません。

また、現在一時停止されているアカウントの Security Hub を有効にすることもできません。一時停止中のアカウントでサービスを有効にしようとすると、アカウントのステータスが [アカウント停止] に変更されます。

- アカウントで Security Hub が有効になっていない場合、そのアカウントに対して Security Hub が有効になります。 AWS Foundational Security Best Practices (FSBP) 標準と CIS AWS Foundations Benchmark v1.2.0 も、デフォルトのセキュリティ標準をオフにしない限り、アカウントで有効になります。

  Organizations 管理アカウントは例外です。Organizations 管理アカウントに対して Security Hub を自動的に有効にすることはできません。Organizations 管理アカウントで Security Hub をメンバーアカウントとして追加する前に、Security Hub を手動で有効にする必要があります。
- アカウントで Security Hub が既に有効になっている場合、Security Hub はアカウントに対して変更を加えません。メンバーシップのみが有効になります。

Security Hub がコントロールの検出結果を生成するには、メンバーアカウントが AWS Config を有効にし、必要なリソースを記録するように設定する必要があります。詳細については、「AWS Config の有効化と設定」を参照してください。

お好みの方法を選択し、手順に従って、Security Hub メンバーアカウントとして組織アカウントを有効にします。

Security Hub console

Security Hub メンバーとして組織アカウントを手動で有効にするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   委任された管理者アカウントの認証情報を使用してサインインします。
2. Security Hub のナビゲーションペインの [設定] で、[設定] を選択します。
3. [アカウント] リストで、有効にする各組織アカウントを選択します。
4. [アクション]、[メンバーを追加] の順に選択します。

Security Hub API

Security Hub メンバーとして組織アカウントを手動で有効にするには

委任された管理者のアカウントで、`CreateMembers` API を呼び出します。有効にするアカウントごとに、アカウント ID を指定します。

手動による招待プロセスとは異なり、`CreateMembers` を呼び出して組織アカウントを有効にする場合、招待を送信する必要はありません。

AWS CLI

Security Hub メンバーとして組織アカウントを手動で有効にするには

委任された管理者アカウントで、`create-members` コマンドを実行します。有効にするアカウントごとに、アカウント ID を指定します。

手動による招待プロセスとは異なり、`create-members` を実行して組織アカウントを有効にする場合、招待を送信する必要はありません。

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

例

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

組織からメンバーアカウントの関連付けを解除する

AWS Security Hub メンバーアカウントからの結果の受信と表示を停止するには、組織からメンバーアカウントの関連付けを解除します。

> **Note**
>
> 中央設定を使用する場合、関連付け解除の仕組みが異なります。1 つ以上の一元管理型メンバーアカウントで、Security Hub を無効にする設定ポリシーを作成できます。それ以降もこれらのアカウントは引き続き組織に含まれますが、Security Hub の検出結果は生成されません。中央設定を使用しているが、手動で招待したメンバーアカウントも含まれている場合は、手動で招待した 1 つ以上のアカウントの関連付けを解除できます。

を使用して管理されているメンバーアカウントは AWS Organizations 、管理者アカウントからアカウントの関連付けを解除できません。メンバーアカウントの関連付けを解除できるのは管理者アカウントのみです。

メンバーアカウントの関連付けを解除しても、アカウントは削除されません。その代わり、組織からメンバーアカウントが削除されます。関連付けが解除されたメンバーアカウントはスタン

ドアロンになり AWS アカウント 、Security Hub と の統合によって管理されなくなります AWS Organizations。

お好みの方法を選択し、手順に従って、組織とのメンバーアカウントの関連付けを解除します。

Security Hub console

組織とのメンバーアカウントの関連付けを解除するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   委任された管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインの [設定] で [設定] を選択します。
3. [アカウント] セクションで、関連付けを解除するアカウントを選択します。中央設定を使用している場合は、手動で招待したアカウントを [Invitation accounts] タブから選択して関連付けを解除できます。このタブは、中央設定を使用する場合にのみ表示されます。
4. [Actions] (アクション) を選択してから、[Disassociate account] (アカウントの関連付けを解除する) を選択します。

Security Hub API

組織とのメンバーアカウントの関連付けを解除するには

委任された管理者のアカウントで、`DisassociateMembers` API を呼び出します。関連付けを解除するには、メンバーアカウントの AWS アカウント IDs を指定する必要があります。メンバーアカウントのリストを表示するには、`ListMembers` API を呼び出します。

AWS CLI

組織とのメンバーアカウントの関連付けを解除するには

委任された管理者アカウントで、`>disassociate-members` コマンドを実行します。関連付けを解除するには、メンバーアカウントの AWS アカウント IDs を指定する必要があります。メンバーアカウントのリストを表示するには、`> list-members` コマンドを実行します。

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

例

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

AWS Organizations コンソール、または AWS SDKsを使用して AWS CLI、組織からメンバーアカウントの関連付けを解除することもできます。詳細については、「AWS Organizations ユーザーガイド」の「組織からのメンバーアカウントの削除」を参照してください。

招待によるアカウントの管理

Security Hub を と統合 AWS Organizations するか、メンバーシップの招待を手動で送信して承諾することで、2 つの方法で複数の AWS Security Hub アカウントを一元管理できます。スタンドアロンアカウントをお持ちの場合、または Organizations と統合していない場合は、手動プロセスを使用する必要があります。手動によるアカウント管理では、Security Hub 管理者がアカウントをメンバーに招待します。管理者とメンバーの関係は、候補となるメンバーが招待を承諾したときに確立されます。Security Hub の管理者アカウントは、最大 1,000 件の招待ベースのメンバーアカウントに対応する Security Hub を管理できます。

> **Tip**
>
> Security Hub で招待ベースの組織を作成する場合は、代わりに後で AWS Organizationsの使用に移行できます。複数のメンバーアカウントがある場合は、 を使用してアカウントを管理することをお勧めします AWS Organizations。

手動による招待プロセスで招待したアカウントについては、検出結果やその他のデータのクロスリージョン集約を使用できます。ただし、クロスリージョン集約を機能させるには、管理者は集約リージョンとすべてのリンクされたリージョンからメンバーアカウントを招待する必要があります。さらに、管理者にメンバーアカウントの結果を表示できるようにするには、メンバーアカウントで集約リージョンとすべてのリンクされたリージョンで Security Hub が有効になっている必要があります。

手動で招待されたメンバーアカウントでは、設定ポリシーはサポートされていません。代わりに、手動の招待プロセスを使用する AWS リージョン ときに、各メンバーアカウントと で Security Hub 設定を個別に設定する必要があります。

また、自分の組織に属していないアカウントについては、手動による招待ベースのプロセスを使用する必要があります。たとえば、組織にテストアカウントを含めない場合もあります。あるいは、複数の組織のアカウントを 1 つの Security Hub 管理者アカウントに統合することもあります。Security Hub 管理者アカウントは、他の組織に属するアカウントに招待を送信する必要があります。

Security Hub コンソールの [設定] ページでは、招待によって追加されたアカウントが [招待アカウント] タブに表示されます。中央設定の仕組みを使用しているが、組織外のアカウントも招待している

場合は、このタブで招待ベースのアカウントの検出結果を確認できます。ただし、Security Hub 管理者は、設定ポリシーを使用して複数のリージョンに招待ベースのアカウントを設定することはできません。

このセクションのトピックでは、招待を使用してメンバーアカウントを管理する方法について説明します。

トピック

メンバーアカウントの追加と招待

アカウントは、招待を受け入れるアカウントの AWS Security Hub 管理者になります。

別のアカウントからの招待を承諾すると、自分のアカウントはメンバーアカウントになり、招待したアカウントが自分の管理者になります。

自分のアカウントが管理者アカウントである場合、メンバーアカウントになるための招待を承諾することはできません。

メンバーアカウントの追加は、以下のステップで構成されています。

1. 管理者アカウントで、メンバーアカウントをメンバーアカウントのリストに追加します。
2. 管理者アカウントから、メンバーアカウントに招待を送信します。
3. メンバーアカウントは招待を承諾します。

メンバーアカウントを追加する

Security Hub コンソールから、メンバーアカウントのリストにアカウントを追加することができます。Security Hub コンソールでアカウントを個別に選択するか、アカウント情報を含む `.csv` ファイルをアップロードします。

各アカウントについて、アカウント ID と E メールアドレスを指定する必要があります。メールアドレスは、アカウントのセキュリティ問題について連絡する E メールアドレスである必要があります。アカウントの検証には使用されません。

お好みの方法を選択し、手順に従ってメンバーアカウントを追加します。

Security Hub console

メンバーアカウントのリストにアカウントを追加するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   管理者アカウントの認証情報を使用してサインインします。
2. 左側のペインで、[Settings] (設定) を選択します。
3. [Settings] (設定) ページで [Accounts] (アカウント) を選択してから、[Add accounts] (アカウントの追加) を選択します。その後、アカウントを個別に追加するか、アカウントのリストを含む `.csv` ファイルをアップロードできます。
4. アカウントを選択するには、次のいずれかを実行します。

   - アカウントを個別に追加するには、[Enter accounts] (アカウントを入力) に、追加するアカウントのアカウント ID と E メールアドレスを入力して [Add] (追加) を選択します。

     アカウントごとにこのプロセスを繰り返します。
   - カンマ区切り値 (.csv) ファイルを使用して複数のアカウントを追加するには、まずファイルを作成します。ファイルには、追加する各アカウントのアカウント ID と E メールアドレスを含める必要があります。

     `.csv` リストには 1 行に 1 つのアカウントが入力されている必要があります。`.csv` ファイルの 1 行目には、ヘッダーが含まれている必要があります。ヘッダーの、一列目は **`Account ID`** で二列目は **`Email`** です。

     続く各行には、追加するアカウントの有効なアカウント ID および E メールアドレスが含まれている必要があります。

     `.csv` ファイルをテキストエディタで表示した場合、次のようになります。

     ```
     Account ID,Email
     111111111111,user@example.com
     ```

スプレッドシートプログラムでは、フィールドは別々の列に表示されます。基になる形式はコンマで区切られています。アカウント ID の書式設定は 10 進数以外の数値にする必要があります。たとえば、アカウント ID 444455556666 の場合、書式設定を 444455556666.0 とすることはできません。また、数値の書式設定によってアカウント ID の先頭のゼロが削除されないようにしてください。

ファイルを選択するには、コンソールで [Upload list (.csv)] (リストのアップロード (.csv)) を選択します。次に [Browse] (参照) を選択します。

ファイルを選択したら、[Add accounts] (アカウントの追加) を選択します。

5. アカウントの追加が完了したら、[Accounts to be added] (追加するアカウント) で [Next] (次) を選択します。

Security Hub API

メンバーアカウントのリストにアカウントを追加するには

管理者アカウントで、`CreateMembers` API を呼び出します。追加するメンバーアカウントごとに、 AWS アカウント ID を指定する必要があります。

AWS CLI

メンバーアカウントのリストにアカウントを追加するには

管理者アカウントで、`create-members` コマンドを実行します。追加するメンバーアカウントごとに、 AWS アカウント ID を指定する必要があります。

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

例

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

メンバーアカウントを招待する

メンバーアカウントを追加した後、メンバーアカウントに招待を送信します。管理者が関連付けを解除したアカウントに招待を再送信することもできます。

Security Hub console

メンバー候補アカウントを招待するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで、[Settings] (設定) を選択し、[Accounts] (アカウント) を選択します。
3. 招待するアカウントの [Status] (ステータス) 列の [Invite] (招待) を選択します。
4. 確認を求められたら [Invite] (招待) を選択します。

> **Note**
>
> 関連付けを解除されたアカウントに招待を再送信するには、[アカウント] ページで関連付けを解除された各アカウントを選択します。[アクション] で、[招待の再送信] を選択します。

Security Hub API

メンバー候補アカウントを招待するには

管理者アカウントで、`InviteMembers` API を呼び出します。招待するアカウントごとに、AWS アカウント ID を指定する必要があります。

AWS CLI

メンバー候補アカウントを招待するには

管理者アカウントで、`invite-members` コマンドを実行します。招待するアカウントごとに、AWS アカウント ID を指定する必要があります。

```
aws securityhub invite-members --account-ids <accountIDs>
```

例

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

メンバーアカウントへの招待を承諾する

メンバーアカウントへの招待を承諾または拒否することができます。

招待を承諾すると、アカウントは AWS Security Hub メンバーアカウントになります。招待を送信したアカウントは、Security Hub 管理者アカウントになります。管理者アカウントのユーザーは、Security Hub でメンバーアカウントの結果を表示できます。

招待を拒否すると、アカウントは管理者アカウントのメンバーアカウントのリストで、[Resigned] (辞退) とマークされます。

メンバーアカウントへの招待は 1 つしか承諾できません。

招待を承諾または拒否する前に、Security Hub を有効にする必要があります。

すべての Security Hub アカウントで、すべてのリソースを記録する AWS Config ように有効化および設定されている必要があります。の要件の詳細については AWS Config、「 の有効化と設定 AWS Config」を参照してください。

招待を承諾する

お好みの方法を選択し、手順に従ってメンバーアカウントへの招待を承諾します。

Security Hub console

メンバーシップの招待を承諾するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. ナビゲーションペインで、[Settings] (設定) を選択し、[Accounts] (アカウント) を選択します。
3. [管理者アカウント] セクションで、[承諾] をオンにし、[招待を承諾] を選択します。

Security Hub API

メンバーシップの招待を承諾するには

`AcceptAdministratorInvitation` API を呼び出します。招待識別子と管理者アカウントの AWS アカウント ID を指定する必要があります。招待の詳細を取得するには、`ListInvitations` オペレーションを使用します。

AWS CLI

メンバーシップの招待を承諾するには

accept-administrator-invitation コマンドを実行します。招待識別子と管理者アカウントの AWS アカウント ID を指定する必要があります。招待の詳細を取得するには、list-invitations コマンドを実行します。

```
aws securityhub accept-administrator-invitation --administrator-
id <administratorAccountID> --invitation-id <invitationID>
```

例

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --
invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

> **Note**
>
> Security Hub コンソールは引き続き AcceptInvitation を使用します。最終的には AcceptAdministratorInvitation を使用するように変更されます。この機能へのアクセスを制御する IAM ポリシーは、引き続き AcceptInvitation を使用する必要があります。また、コンソールで AcceptAdministratorInvitation の使用が開始された後に正しい許可が設定されているようにするには、ポリシーに AcceptAdministratorInvitation を追加する必要があります。

招待を拒否する

メンバーアカウントへの招待を拒否できます。Security Hub コンソールで招待を拒否すると、管理者アカウントのメンバーアカウントのリストで、アカウントが [退会済み] とマークされます。

招待を拒否するには、招待を受けたメンバーアカウントにサインインする必要があります。

お好みの方法を選択し、手順に従ってメンバーアカウントへの招待を拒否します。

Security Hub console

メンバーシップへの招待を拒否するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

2. ナビゲーションペインで、[Settings] (設定) を選択し、[Accounts] (アカウント) を選択します。
3. [管理者アカウント] セクションで、[招待を辞退] を選択します。

Security Hub API

メンバーシップへの招待を拒否するには

DeclineInvitations API を呼び出します。招待を発行した管理者アカウントの AWS アカウント ID を指定する必要があります。招待に関する情報を表示するには、ListInvitations オペレーションを使用します。

AWS CLI

メンバーシップへの招待を拒否するには

decline-invitations コマンドを実行します。招待を発行した管理者アカウントの AWS アカウント ID を指定する必要があります。招待に関する情報を表示するには、list-invitations コマンドを実行します。

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

例

```
aws securityhub decline-invitations --account-ids "123456789012"
```

メンバーアカウントの関連付けを解除する

AWS Security Hub 管理者アカウントは、メンバーアカウントの関連付けを解除して、そのアカウントからの検出結果の受信と表示を停止できます。メンバーを削除する前に、メンバーアカウントの関連付けを解除する必要があります。

メンバーアカウントの関連付けを解除すると、メンバーアカウントのリストには残りますが、ステータスが [Removed (Disassociated)] (削除 (関連付け解除)) になります。アカウントは、メンバーアカウントの管理者アカウント情報から削除されます。

アカウントの結果の受信を再開するには、招待を再送信します。メンバーアカウントを完全に削除するには、メンバーアカウントを削除します。

お好みの方法を選択し、手順に従って、手動で招待されたメンバーアカウントと管理者アカウントの関連付けを解除します。

Security Hub console

手動で招待したメンバーアカウントの関連付けを解除するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインの [設定] で [設定] を選択します。
3. [アカウント] セクションで、関連付けを解除するアカウントを選択します。
4. [Actions] (アクション) を選択してから、[Disassociate account] (アカウントの関連付けを解除する) を選択します。

Security Hub API

手動で招待したメンバーアカウントの関連付けを解除するには

管理者アカウントで、`DisassociateMembers` API を呼び出します。関連付けを解除するメンバーアカウントの AWS アカウント IDs を指定する必要があります。メンバーアカウントのリストを表示するには、`ListMembers` オペレーションを使用します。

AWS CLI

手動で招待したメンバーアカウントの関連付けを解除するには

管理者アカウントで、`disassociate-members` コマンドを実行します。関連付けを解除するメンバーアカウントの AWS アカウント IDs を指定する必要があります。メンバーアカウントのリストを表示するには、`list-members` コマンドを実行します。

```
aws securityhub disassociate-members --account-ids <accountIds>
```

例

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

メンバーアカウントの削除

AWS Security Hub 管理者アカウントは、招待によって追加されたメンバーアカウントを削除できます。有効なアカウントを削除する前に、関連付けを解除する必要があります。

メンバーアカウントを削除すると、そのメンバーアカウントはリストから完全に削除されます。アカウントのメンバーシップを復元するには、アカウントを追加し、まったく新しいメンバーアカウントであるかのように再度招待する必要があります。

組織に属するアカウントや、 との統合を使用して管理されているアカウントは削除できません AWS Organizations。

お好みの方法を選択し、手順に従って手動で招待されたメンバーアカウントを削除します。

Security Hub console

手動で招待したメンバーアカウントを削除するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   管理者アカウントを使用してサインインします。
2. ナビゲーションペインで、[設定] を選択し、[設定] を選択します。
3. [招待アカウント] タブを選択します。次に、削除するアカウントを選択します。
4. [アクション] を選択し、[削除] を選択します。このオプションは、アカウントの関連付けを解除した場合にのみ使用できます。メンバーアカウントを削除する前に、関連付けを解除する必要があります。

Security Hub API

手動で招待したメンバーアカウントを削除するには

管理者アカウントで、`DeleteMembers` API を呼び出します。削除するメンバーアカウントの AWS アカウント ID を指定する必要があります。メンバーアカウントのリストを取得するには、`ListMembers` API を呼び出します。

AWS CLI

手動で招待したメンバーアカウントを削除するには

管理者アカウントで、delete-members コマンドを実行します。削除するメンバーアカウントの AWS アカウント ID を指定する必要があります。メンバーアカウントのリストを取得するには、list-members コマンドを実行します。

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

例

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

管理者アカウントから関連付けを解除する

招待によってアカウントが AWS Security Hub メンバーアカウントとして追加された場合は、管理者アカウントからメンバーアカウントの関連付けを解除できます。メンバーアカウントの関連付けを解除すると、Security Hub は、そのアカウントから管理者アカウントへ結果を送信しません。

との統合を使用して管理されているメンバーアカウントは AWS Organizations 、管理者アカウントからアカウントの関連付けを解除できません。Security Hub 委任管理者のみが、Organizations で管理されているメンバーアカウントの関連付けを解除できます。

管理者アカウントとの関連付けを解除すると、管理者アカウントのメンバーリストには残りますが、アカウントはステータスが [Resigned] (辞退) になります。ただし、管理者アカウントはアカウントの結果を受信しません。

管理者アカウントとの関連付けを解除しても、メンバーになるための招待は残ります。この招待は、今後再度承諾できます。

Security Hub console

管理者アカウントとの関連付けを解除するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. ナビゲーションペインで、[Settings] (設定) を選択し、[Accounts] (アカウント) を選択します。
3. [管理者アカウント] セクションで、[承諾] をオフにし、[更新] を選択します。

Security Hub API

管理者アカウントとの関連付けを解除するには

DisassociateFromAdministratorAccount API を呼び出します。

AWS CLI

管理者アカウントとの関連付けを解除するには

disassociate-from-administrator-account コマンドを実行します。

```
aws securityhub disassociate-from-administrator-account
```

> **Note**
>
> Security Hub コンソールは引き続き DisassociateFromMasterAccount を使用します。最終的には DisassociateFromAdministratorAccount を使用するように変更されます。この機能へのアクセスを制御する IAM ポリシーは、引き続き DisassociateFromMasterAccount を使用する必要があります。また、コンソールで DisassociateFromAdministratorAccount の使用が開始された後に正しい許可が設定されているようにするには、ポリシーに DisassociateFromAdministratorAccount を追加する必要があります。

アカウント管理のための AWS Organizations への移行

AWS Security Hub でアカウントを手動で管理する場合は、メンバー候補アカウントを招待し、AWS リージョンごとに各メンバーアカウントを個別に設定する必要があります。

Security Hub と AWS Organizations を統合することで、招待の送信を省略し、組織内での Security Hub の設定やカスタマイズの方法をより細かく制御できるようになります。

AWS Organizations 統合を使用するだけでなく、組織外のアカウントを手動で招待するという複合的なアプローチを使用することもできます。ただし、Organizations の統合のみを使用することをお勧めします。中央設定は、複数のアカウントやリージョンにわたって Security Hub を管理するのに役立つ機能であり、Organizations と統合する場合にのみ使用できます。

このセクションでは、手動による招待ベースのアカウント管理から AWS Organizations によるアカウント管理に移行する方法について説明します。

Security Hub と AWS Organizations の統合

まず、Security Hub と AWS Organizations を統合する必要があります。

次の手順を完了することで、これらのサービスを統合できます。

- AWS Organizations で組織を作成します。手順については、「AWS Organizations ユーザーガイド」の「組織の作成」を参照してください。
- Organizations 管理アカウントから、Security Hub 委任管理者アカウントを指定します。

> **Note**
>
> Organizations 管理アカウントを DA アカウントとして使用することはできません。

詳細な手順については、「Security Hub と の統合 AWS Organizations」を参照してください。

前述の手順を完了すると、AWS Organizations で Security Hub の信頼されたアクセスを付与することになります。また、委任された管理者アカウントの Security Hub が、現在の AWS リージョンで有効になります。

委任された管理者は、主に組織のアカウントを Security Hub メンバーアカウントとして追加することで、Security Hub で組織を管理できます。また、管理者は、そのアカウントの特定の Security Hub 設定、データ、およびリソースにアクセスできます。

Organizations を使用してアカウント管理に移行しても、招待ベースのアカウントが自動的に Security Hub のメンバーになることはありません。Security Hub メンバーになることができるのは、新しい組織に追加したアカウントのみです。

中央設定とローカル設定

統合をアクティブ化すると、Organizations でアカウントを管理できるようになります。詳細については、によるアカウントの管理 AWS Organizationsを参照してください。アカウント管理は、組織の設定タイプによって異なります。

組織には、ローカルと中央という 2 種類の設定タイプがあります。デフォルトの設定タイプは、ローカル設定です。現在の設定タイプを確認するには、Security Hub コンソールのナビゲーションペインで [設定] を選択し、次に [設定] を選択します。`DescribeOrganizationConfiguration` API を呼び出して設定タイプを表示することもできます。

ローカル設定では、新しいアカウントを組織に追加する際に、委任された管理者アカウントで、Security Hub とデフォルトのセキュリティ標準を自動的に有効化できます。これらの新しいアカウント設定は、現在のリージョンで有効化されます。その他の Security Hub 設定は、各リージョンのメンバーアカウントごとに個別に設定する必要があります。

ローカル設定ではなく中央設定を使用することをお勧めします。中央設定では、委任された管理者アカウントは、複数のリージョンで有効な Security Hub 設定ポリシーを作成し、組織のさまざまなアカウントや組織単位 (OU) で Security Hub 機能を指定できます。1 つの設定ポリシーを組織全体に適用することも、異なる設定ポリシーを異なるアカウントや OU に適用することもできます。例えば、本番稼働用アカウントで有効にする標準とコントロールのセットと、テストアカウントで有効にする標準とコントロールを別にすることができます。DA は必要に応じて設定ポリシーを編集できます。

中央設定の動作の詳細については、「中央設定の仕組み」を参照してください。

ローカル設定から中央設定へ切り替える手順については、「中央設定の使用を開始する」を参照してください。

アカウントに許可されるアクション

管理者アカウントとメンバーアカウントは、次のテーブルに記載された AWS Security Hub アクションを使用できます。テーブルの値の意味は次のとおりです。

- すべて - アカウントは、同じ管理者のすべてのメンバーアカウントに対してアクションを実行できます。
- 現在 — アカウントは、ユーザー自身 (現在サインインしているアカウント) に対してのみアクションを実行できます。
- ダッシュ — アカウントがアクションを実行できないことを示します。

テーブルに記載されているように、許可されるアクションは、AWS Organizations と統合しているかどうかや、組織が使用している設定タイプによって異なります。中央設定とローカル設定の違いについては、「AWS Organizations を使用したアカウントの管理」を参照してください。

Security Hub では、メンバーアカウントの検出結果を管理者アカウントにコピーすることはありません。Security Hub では、すべての結果が、特定のアカウントの特定のリージョンに取り込まれます。管理者アカウントは、各リージョンのメンバーアカウントの結果を表示および管理できます。

集約リージョンを設定する場合は、管理者アカウントで、集約リージョンにレプリケートされたリンク済みリージョンのメンバーアカウントの検出結果を表示および管理することができます。クロスリージョン集約の詳細については、「クロスリージョン集約」を参照してください。

この表は、管理者およびメンバーアカウントのデフォルトの許可を示しています。カスタム IAM ポリシーを使用することで、Security Hub の機能へのアクセスをさらに制限できます。ガイダンスと例については、ブログ記事「IAM ポリシーを AWS Security Hub ユーザーペルソナに合わせる」を参照してください。

Organizations と統合して中央設定を使用する場合に許可されるアクション

Organizations と統合して中央設定を使用する場合、管理者アカウントとメンバーアカウントは次のように Security Hub のアクションにアクセスできます。

[アクション]	Security Hub 委任管理者アカウント	一元管理型メンバーアカウント	セルフマネージド型メンバーアカウント
Security Hub 設定ポリシーを作成および管理する	セルフマネージド型アカウントおよび一元管理型アカウント用	–	–
組織のアカウントを表示する	すべて	–	–
メンバーアカウントの関連付けを解除する	すべて	–	–
メンバーアカウントを削除する	組織以外のアカウントすべて	–	–
Security Hub を無効にする	現在のアカウントおよび一元管理型アカウント用	–	Current
検出結果と検索履歴を表示する	すべて	Current	Current

[アクション]	Security Hub 委任管理者アカウント	一元管理型メンバーアカウント	セルフマネージド型メンバーアカウント
結果を更新する	すべて	Current	Current
インサイトの結果を表示する	すべて	Current	Current
コントロールの詳細を表示する	すべて	Current	Current
統合コントロール検出結果のオン/オフを切り替える	すべて	–	–
標準を有効または無効にする	現在のアカウントおよび一元管理型アカウント用	–	Current
コントロールを有効または無効にする	現在のアカウントおよび一元管理型アカウント用	–	Current
統合を有効または無効にする	Current	Current	Current
クロスリージョン集約を設定する	すべて	–	–
ホームリージョンとリンクされたリージョンを選択する	すべて (ホームリージョンを変更するには、中央設定をいったん停止して再起動する必要があります)	–	–
カスタムアクションを設定する	Current	Current	Current

[アクション]	Security Hub 委任管理者アカウント	一元管理型メンバーアカウント	セルフマネージド型メンバーアカウント
自動化ルールを設定する	すべて	–	–
カスタムインサイトを設定する	Current	Current	Current

Organizations と統合してローカル設定を使用する場合に許可されるアクション

Organizations と統合してローカル設定を使用する場合、管理者アカウントとメンバーアカウントは次のように Security Hub のアクションにアクセスできます。

[アクション]	Security Hub 委任管理者アカウント	メンバーアカウント
Security Hub 設定ポリシーを作成および管理する	–	–
組織のアカウントを表示する	すべて	–
メンバーアカウントの関連付けを解除する	すべて	–
メンバーアカウントを削除する	–	–
Security Hub を無効にする	–	現在 (アカウントと委任された管理者との関連付けが解除されている場合)
検出結果と検索履歴を表示する	すべて	Current
結果を更新する	すべて	Current
インサイトの結果を表示する	すべて	Current

[アクション]	Security Hub 委任管理者アカウント	メンバーアカウント
コントロールの詳細を表示する	すべて	Current
統合コントロール検出結果のオン/オフを切り替える	すべて	–
標準を有効または無効にする	Current	Current
新しい組織アカウントで Security Hub とデフォルトの標準を自動的に有効にする	現在のアカウントと新しい組織アカウント用	–
コントロールを有効または無効にする	Current	Current
統合を有効または無効にする	Current	Current
クロスリージョン集約を設定する	すべて	–
カスタムアクションを設定する	Current	Current
自動化ルールを設定する	すべて	–
カスタムインサイトを設定する	Current	Current

招待ベースのアカウントで許可されるアクション

AWS Organizations との統合ではなく招待ベースの方法を使用して手動でアカウントを管理する場合、管理者アカウントとメンバーアカウントは次のように Security Hub のアクションにアクセスできます。

[アクション]	Security Hub 管理者アカウント	メンバーアカウント
Security Hub 設定ポリシーを作成および管理する	–	–
組織のアカウントを表示する	すべて	–
メンバーアカウントの関連付けを解除する	すべて	Current
メンバーアカウントを削除する	すべて	–
Security Hub を無効にする	現在 (有効なメンバーアカウントがない場合)	現在 (アカウントと管理者アカウントの関連付けが解除されている場合)
検出結果と検索履歴を表示する	すべて	Current
結果を更新する	すべて	Current
インサイトの結果を表示する	すべて	Current
コントロールの詳細を表示する	すべて	Current
統合コントロール検出結果のオン/オフを切り替える	すべて	–
標準を有効または無効にする	Current	Current
新しい組織アカウントで Security Hub とデフォルトの標準を自動的に有効にする	–	–
コントロールを有効または無効にする	Current	Current

[アクション]	Security Hub 管理者アカウント	メンバーアカウント
統合を有効または無効にする	Current	Current
クロスリージョン集約を設定する	すべて	–
カスタムアクションを設定する	Current	Current
自動化ルールを設定する	すべて	–
カスタムインサイトを設定する	Current	Current

アカウント管理に関する制約と推奨事項

次のセクションでは、 AWS Security Hubでメンバーアカウントを管理する際に留意すべきいくつかの制約と推奨事項をまとめています。

メンバーアカウントの最大数

との統合を使用する場合 AWS Organizations、Security Hub は各 の委任管理者アカウントごとに最大 10,000 のメンバーアカウントをサポートします AWS リージョン。Security Hub を手動で有効化して管理する場合、Security Hub は各リージョンの管理者アカウントごとに最大 1,000 のメンバーアカウントの招待をサポートします。

アカウントとリージョン

組織別のメンバーシップ

Security Hub を と統合する場合 AWS Organizations、Organizations 管理アカウントは Security Hub の委任管理者 (DA) アカウントを指定できます。Organizations 管理アカウントを組織の DA として設定することはできません。これは Security Hub では許可されていますが、Organizations 管理アカウントを DA にしないことをお勧めします。

すべてのリージョンで、同一の DA を選択することが推奨されます。中央設定を使用する場合、Security Hub は組織の Security Hub を設定したすべてのリージョンに同じ DA アカウントを設定します。

また、 AWS セキュリティ関連の問題を一元的に管理できるように、セキュリティおよびコンプライアンスサービス全体で同じ DA アカウントを選択することをお勧めします。

招待によるメンバーシップ

招待によって作成されたメンバーアカウントの場合、管理者アカウントとメンバーのアカウントの関連付けは、招待の送信元の 1 つのリージョンでのみ作成されます。管理者アカウントでは、使用する各リージョンの Security Hub を有効にする必要があります。次に、管理者アカウントは各アカウントをそのリージョンのメンバーアカウントに招待します。

管理者とメンバーの関係性に関する制限

> **Note**
>
> と Security Hub の統合を使用していて AWS Organizations、メンバーアカウントを手動で招待していない場合、このセクションは適用されません。

アカウントを、管理者アカウントとメンバーアカウントの両方のアカウントとして同時に設定することはできません。

メンバーアカウントは、一度に 1 つの管理者アカウントのみと関連付けることができます。Security Hub 管理者アカウントによって組織アカウントが有効になっている場合、そのアカウントは別のアカウントからの招待を承諾することができません。アカウントが既に招待を承諾している場合、組織の Security Hub 管理者アカウントでそのアカウントを有効にすることはできません。また、他のアカウントからの招待を受信することはできません。

手動の招待プロセスでは、メンバーシップの招待の承諾はオプションです。

サービス間の管理者アカウントの調整

Security Hub は、Amazon 、Amazon Inspector GuardDuty、Amazon Macie などのさまざまな AWS のサービスからの結果を集約します。Security Hub では、ユーザーは GuardDuty 調査結果からピボットして Amazon Detective で調査を開始することもできます。

ただし、これらの他のサービスで設定した管理者とメンバーの関係が、Security Hub に自動的に適用されることはありません。Security Hub ではこれらすべてのサービスで、管理者アカウントと同じアカウントを使用することを推奨しています。この管理者アカウントは、セキュリティツールを担当するアカウントである必要があります。また、 AWS Configの集約アカウントもこのアカウントが担う必要があります。

例えば、 GuardDuty 管理者アカウント A のユーザーは、 GuardDuty コンソールでメンバーアカウント B と C の結果 GuardDutyを確認できます。アカウント A が Security Hub を有効にした場合、アカウント A のユーザーは Security Hub のアカウント B とアカウント C の結果を自動的に表示 GuardDutyしません。これらのアカウントには、Security Hub 管理者とメンバーの関係も必要になります。

これを行うには、アカウント A をSecurity Hub 管理者アカウントにし、アカウント B と C が Security Hub のメンバーアカウントになるようにします。

アカウントアクションが Security Hub データに及ぼす影響

これらのアカウントアクションは、AWS Security Hub データに次の影響を与えます。

Security Hub を無効にする

中央設定を使用する場合、委任された管理者 (DA) は、特定のアカウントや組織単位 (OU) で AWS Security Hub を無効にする Security Hub 設定ポリシーを作成できます。この場合、指定したアカウントとホームリージョンおよびリンクされたリージョンの OU では Security Hub が無効になります。

中央設定を使用しない場合、Security Hub を有効にした各アカウントとリージョンで、Security Hub を個別に無効にする必要があります。

Security Hub が管理者アカウントで無効になっている場合、管理者アカウントに新しい検出結果は生成されません。また、DA アカウントで Security Hub が無効になっている場合は、中央設定を使用できません。結果は生成後 90 日後に削除されます。

他の AWS のサービスとの統合が削除されます。

有効になっているセキュリティ標準およびコントロールは無効になります。

カスタムアクション、インサイト、サードパーティー製品のサブスクリプションを含む、その他の Security Hub データと設定は保持されます。

管理者アカウントからメンバーアカウントとの関連付けを解除する

メンバーアカウントが管理者アカウントとの関連付けを解除されると、管理者アカウントはそのメンバーアカウントの検出結果を表示するための許可を失います。ただし、Security Hub では引き続き両方のアカウントが有効です。

中央設定を使用する場合、DA は DA アカウントとの関連付けが解除されたメンバーアカウントに Security Hub を設定できません。

管理者アカウントに対して定義されたカスタム設定または統合は、過去のメンバーアカウントからの結果には適用されません。例えば、アカウントの関連付けが解除された後に、管理者アカウントのカスタムアクションを、Amazon EventBridge ルールのイベントパターンとして使用することが可能です。ただし、このカスタムアクションをメンバーアカウントで使用することはできません。

Security Hub 管理者アカウントの [アカウント] リストでは、削除されたアカウントのステータスが [関連付けを解除済み] になります。

メンバーアカウントが組織から削除されている場合

メンバーアカウントが組織から削除されると、Security Hub 管理者アカウントはそのメンバーアカウントの結果を表示するための許可を失います。ただし、Security Hub では、両方のアカウントが削除前と同じ設定で引き続き有効になっています。

中央設定を使用する場合、委任された管理者が所属する組織からメンバーアカウントが削除された後は、そのメンバーアカウントに Security Hub を設定することはできません。ただし、手動で変更しない限り、アカウントは削除前の設定を保持します。

Security Hub 管理者アカウントの [アカウント] リストでは、削除されたアカウントのステータスが [削除済み] になります。

アカウントが停止されている場合

AWS でアカウントが停止されると、そのアカウントは Security Hub で結果を表示するための許可を失います。そのアカウントに対して新しい結果は生成されません。中断されたアカウントの管理者アカウントは、既存のアカウントの結果を表示できます。

組織アカウントの場合、メンバーアカウントのステータスが [Account Suspended] (アカウントの停止) に変更されることもあります。これは、管理者アカウントがアカウントを有効にしようとしたときにアカウントが停止されている場合に発生します。[Account Suspended] (アカウントの停止)になっている場合、管理者アカウントは、そのアカウントの結果を表示することはできません。それ以

外の場合、停止ステータスによってメンバーアカウントのステータスに影響が生じることはありません。

中央設定を使用する場合、委任された管理者が設定ポリシーを一時停止中のアカウントに関連付けようとしても、ポリシーの関連付けは失敗します。

90 日後、アカウントは削除または再アクティブ化されます。アカウントが再アクティブ化されると、その Security Hub 許可が復元されます。メンバーアカウントのステータスが [Account Suspended] (アカウントの停止) の場合、管理者アカウントでそのアカウントを手動で有効にする必要があります。

アカウントの閉鎖

AWS アカウント が閉鎖されている場合、Security Hub は次のように対応します。

Security Hub では、アカウントの閉鎖の発効日から 90 日間にわたり、そのアカウントの結果が保持されます。90 日経過後、Security Hub では、そのアカウントのすべての結果が完全に削除されます。

- 結果を 90 日以上保持するには、結果をアーカイブするか、EventBridge ルールでカスタムアクションを使用して Amazon S3 バケットに結果を保存します。Security Hub で結果が保持されている限り、閉鎖されたアカウントを再度開いた際に、Security Hub でそのアカウントの結果を復元することができます。
- アカウントが Security Hub 管理者アカウントの場合、アカウントは管理者として削除され、すべてのメンバーアカウントもすべて削除されます。アカウントがメンバーアカウントの場合、Security Hub 管理者アカウントとの関連付けが解除され、メンバーから削除されます。
- 詳細については、「AWS 請求とコスト管理ユーザーガイド」の「アカウントの解約」を参照してください。

> **Important**
>
> AWS GovCloud (US) リージョンの顧客の場合
>
> - アカウントを閉鎖する前に、ポリシーデータおよびその他のアカウントリソースをバックアップしてから、削除します。アカウントを閉鎖した後は、そのアカウントへのアクセス権はなくなります。

クロスリージョン集約

クロスリージョン集約を使用すると、複数のリージョンの結果、結果の更新、インサイト、コントロールコンプライアンスのステータス、セキュリティスコアを 1 つの集約リージョンに集約できます。その後は、これらすべてのデータを集約リージョンで管理できます。

> **Note**
>
> では AWS GovCloud (US)、クロスリージョン集約は、 全体の検出結果、検出結果の更新、インサイトに対してのみサポートされます AWS GovCloud (US)。具体的には、 (米国東部) と AWS GovCloud （ AWS GovCloud 米国西部) の間の結果、結果の更新、インサイトのみを集約できます。中国リージョンでは、クロスリージョン集約は、中国リージョンの結果、結果の更新、インサイトにのみ使用できます。具体的には、中国 (北京) と中国 (寧夏) の間の結果、結果の更新、インサイトのみを集約できます。

例えば、米国東部 (バージニア北部) を集約リージョンとして設定し、米国西部 (オレゴン) と米国西部 (北カリフォルニア) をリンクされたリージョンとして設定するとします。米国東部 (バージニア北部) の [Findings] (結果) ページを見ると、上記 3 つのリージョンすべての結果が表示されます。これらの結果に対する更新は、3 つのリージョンすべてに反映されています。

コントロールの有効ステータスは各リージョンで変更する必要があります。コントロールが、リンクされたリージョンでは有効になっていても、集約リージョンでは無効になっている場合、そのコントロールのコンプライアンスステータスは集約リージョンで確認できます。ただし、集約リージョンからそのコントロールを有効または無効にすることはできません。

リージョンを横断してセキュリティスコアとコンプライアンスステータスを表示するには、Security Hub を使用する IAM ロールに次のアクセス権限を追加します。

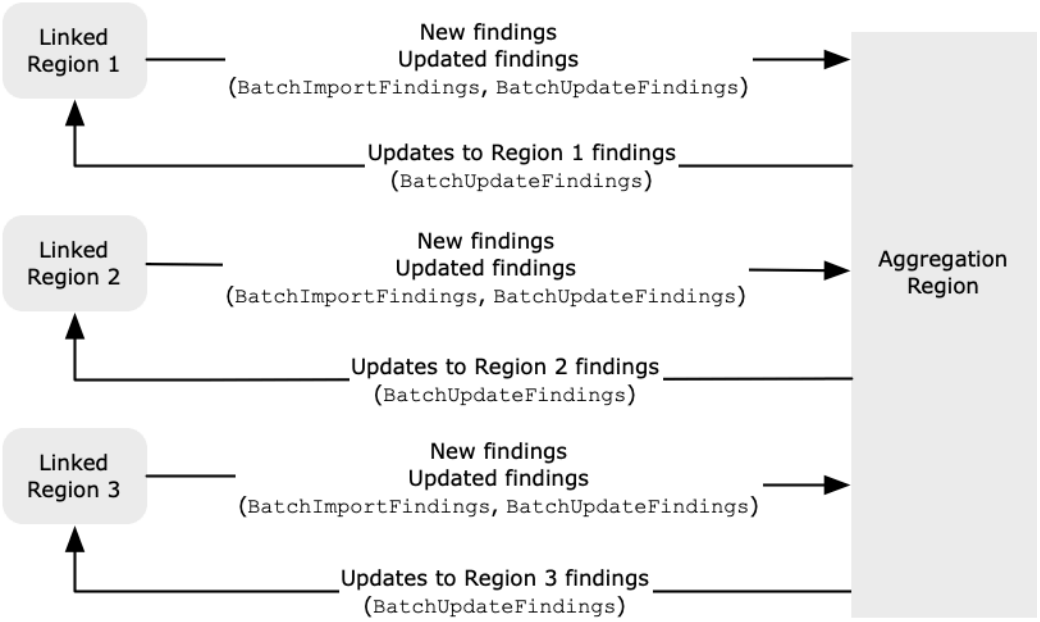
- `ListSecurityControlDefinitions`
- `BatchGetStandardsControlAssociations`
- `BatchUpdateStandardsControlAssociations`

クロスリージョン集約の仕組み

クロスリージョン集約を有効にすると、Security Hub はリンクされたリージョンから集約リージョンに次のデータをレプリケートします。これは、クロスリージョン集約が有効になっているすべてのアカウントで発生します。

- 結果
- インサイト
- コントロールコンプライアンスステータス
- セキュリティスコア

以前のリストの新しいデータだけでなく、Security Hub はリンクされたリージョンと集約リージョン間で、データの更新のレプリケートも行います。リンクされたリージョンで発生した更新は、集約リージョンにレプリケートされます。集約リージョンで発生した更新は、元のリンクされたリージョンにレプリケートされます。



集約リージョンとリンクされたリージョンに相反する更新がある場合は、最も新しい更新が使用されます。

クロスリージョン集約によって、Security Hub のコストが増えることはありません。Security Hub が新しいデータや更新を複製しても、請求は発生しません。

集約リージョンでは、[Summary] (概要)ページに、リンクされたリージョン全体のアクティブな結果が表示されます。詳細については、「Viewing a cross-Region summary of findings by severity」を参照してください。結果を分析するその他の [Summary] (概要) ページのパネルには、リンクされたリージョン全体からの情報も表示されます。

集約リージョンのセキュリティスコアは、リンクされているすべてのリージョンで有効になっているコントロールと、合格の状態にあるコントロールの数を比較して計算されます。また、コントロールが 1 つ以上のリンクされたリージョンで有効になっている場合、そのコントロールは、集約リージョンの [Security standards] (セキュリティ標準) の詳細ページに表示されます。標準の詳細ページの、コントロールのコンプライアンスステータスには、リンクされたリージョンの結果が反映されています。1 つまたは複数のリンクされたリージョンでコントロールに関連付けられたセキュリティチェックが失敗した場合、そのコントロールのコンプライアンスステータスは、集約リージョンの標準の詳細ページに [Failed] (失敗) と表示されます。セキュリティチェックの数値には、リンクされているすべてのリージョンの結果が含まれます。

Security Hub は、アカウントで Security Hub が有効になっているリージョンからのみ、データを集約します。Security Hub は、クロスリージョン集約の設定に基づいて自動的にアカウントで有効にされることはありません。

管理者アカウントとメンバーアカウントの集計

スタンドアロンアカウント、メンバーアカウント、管理者アカウントは、クロスリージョン集約を設定できます。管理者によって設定されている場合、管理対象アカウントでクロスリージョン集約を使用するには、管理者アカウントの存在が不可欠です。管理者アカウントがメンバーアカウントから削除または関連付けが解除されると、メンバーアカウントのクロスリージョン集約は停止します。これは、管理者とメンバーの関係が始まる前にアカウントでクロスリージョン集約が有効になっている場合にも当てはまります。

管理者アカウントがクロスリージョン集約を有効にすると、Security Hub は、管理者アカウントがすべてのリンクされたリージョンで生成したデータを集約リージョンにレプリケートします。さらに、Security Hub はその管理者に関連付けられているメンバーアカウントを識別し、各メンバーアカウントは管理者のクロスリージョン集約設定を継承します。Security Hub は、メンバーアカウントがすべてのリンクされたリージョンで生成するデータを集約リージョンにレプリケートします。

管理者は、管理対象リージョン内のすべてのメンバーアカウントからセキュリティ検出結果にアクセスして管理できます。ただし、Security Hub 管理者として、すべてのメンバーアカウントとリンクされたリージョンから集約されたデータを表示するには、集約リージョンにサインインする必要があります。

Security Hub メンバーアカウントとして、すべてのリンクされたリージョンからアカウントから集約されたデータを表示するには、集約リージョンにサインインする必要があります。メンバーアカウントには、他のメンバーアカウントのデータを表示するアクセス許可はありません。

管理者アカウントは、メンバーアカウントを手動で招待したり、 と統合されている組織の委任された管理者として機能したりすることができます AWS Organizations。手動で招待されたメンバーアカウント の場合、クロスリージョン集約を機能させるには、管理者は集約リージョンとすべてのリンクされたリージョンからアカウントを招待する必要があります。さらに、管理者にメンバーアカウントの結果を表示できるようにするには、メンバーアカウントで集約リージョンとすべてのリンクされたリージョンで Security Hub が有効になっている必要があります。他の目的で集約リージョンを使用しない場合は、そのリージョンで Security Hub 標準と統合を無効にして、課金を防ぐことができます。

クロスリージョン集約を使用する予定で、複数の管理者アカウントがある場合は、次のベストプラクティスに従うことをお勧めします。

- 各管理者アカウントに、異なるメンバーアカウントが含まれている。
- 各管理者アカウントが、リージョン間で同じメンバーアカウントを有している。
- 各管理者アカウントに、別の集約リージョンを使用する。

> **Note**
>
> クロスリージョン集約が中央設定にどのように影響するかについては、「」を参照してください中央設定とクロスリージョン集約。

中央設定とクロスリージョン集約

中央設定は Security Hub のオプトイン機能であり、 と統合する場合に使用できます AWS Organizations。中央設定を使用すると、委任管理者アカウントは、組織の複数のアカウントと組織単位 (OU) の Security Hub サービス、標準、およびコントロールを設定できます。アカウントと OU を設定するには、委任管理者が Security Hub 設定ポリシーを作成します。設定ポリシーを使用して、Security Hub を有効にするか無効にするか、およびどの標準とコントロールを有効にするかを定義できます。委任管理者は、設定ポリシーを特定のアカウント、OU、またはルート (組織全体) に関連付けます。

委任管理者は、集約リージョンからのみ組織の設定ポリシーを作成および管理できます。また、設定ポリシーは、集約リージョンおよびすべてのリンクされたリージョンで有効になります。一部のリン

クされたリージョンにのみ適用され、他のリージョンには適用されない設定ポリシーは作成できません。中央設定では、集約リージョンはホームリージョンと呼ばれます。同じリージョンが、中央設定ではホームリージョンとして機能し、クロスリージョン集約では集約リージョンとして機能します。クロスリージョン集約については、「クロスリージョン集約」を参照してください。

中央設定を使用するには、ホームリージョンと少なくとも 1 つのリンクされたリージョンを指定する必要があります。

クロスリージョン集約設定を変更すると、設定ポリシーに影響する可能性があります。リンクされたリージョンを追加すると、設定ポリシーはそのリージョンで有効になります。リージョンがオプトインリージョンの場合、設定ポリシーをそこで有効にするにはリージョンを有効にする必要があります。また、リンクされたリージョンを削除すると、設定ポリシーはそのリージョンでは有効ではなくなります。そのリージョンのアカウントは、リンクされたリージョンが削除されたときの設定を維持します。これらの設定は変更できますが、アカウントとリージョンごとに個別に変更する必要があります。

ホームリージョンを削除または変更すると、設定ポリシーとポリシーの関連付けが削除されます。どのリージョンでも中央設定を使用したり、設定ポリシーを作成したりできなくなります。アカウントは、ホームリージョンが変更または削除される前の設定を維持します。これらの設定はいつでも変更できますが、中央設定を使用しなくなったため、設定はアカウントとリージョンごとに個別に変更する必要があります。新しいホームリージョンを指定すれば、中央設定を使用して設定ポリシーを再作成できます。

中央設定の詳細については、「中央設定の仕組み」を参照してください。

クロスリージョン集約を有効にする

集約リージョンとして AWS リージョン 指定する からクロスリージョン集約を有効にする必要があります。

デフォルトで無効になっているリージョンは、集約リージョンとして使用できません。デフォルトで無効になっているリージョンのリストについては、「AWS 全般のリファレンス」の「リージョンを有効にする」を参照してください。

クロスリージョン集約を有効にする (コンソール)

クロスリージョン集約を有効にする場合、リンクされたリージョンを選択します。また、Security Hub が選択したリージョンのサポートを開始し、そのリージョンが選択されている場合に、新しいリージョンを自動的にリンクするかどうかも選択します。

クロスリージョン集約を拡張するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. AWS リージョン セレクターを使用して、集約リージョンとして使用するリージョンにサインインします。
3. Security Hub ナビゲーションメニューで、[設定]、[リージョン] の順に選択します。
4. [検出結果の集約] で、[検出結果の集約を設定] を選択します。

   デフォルトでは、集約リージョンは [No aggregation Region] (集約リージョンなし) に設定されています。
5. [集約リージョン] で、オプションを選択して、現在のリージョンを集約リージョンとして指定します。
6. 必要に応じて、[リンクされたリージョン] で、データの集約元となるリージョンを選択します。
7. Security Hub がサポートし、ユーザーが選択している場合に、パーティション内の新しいリージョンから自動的にデータを集約するには、[Link future Regions] (将来のリージョンをリンクする) を選択します。
8. [保存] を選択します。

クロスリージョン集約の有効化 (Security Hub API、 AWS CLI)

クロスリージョン集約は、Security Hub API を使用して有効にすることができます。

Security Hub API からクロスリージョン集約を有効にするには、結果アグリゲーターを作成します。集約リージョンとして使用するリージョンから、結果アグリゲーターを作成する必要があります。

結果アグリゲータを作成するには (Security Hub API、 AWS CLI)

- Security Hub API: 集約リージョンとして使用するリージョンから、`CreateFindingAggregator` オペレーションを使用します。`RegionLinkingMode` では、以下のオプションの中から選択します。
  - `ALL_REGIONS` - Security Hub はすべてのリージョンのデータを集約します。Security Hub は、新しいリージョンがサポートされ、ユーザーが選択している場合に、それらの結果も集約します。
  - `ALL_REGIONS_EXCEPT_SPECIFIED` - Security Hub は、除外するリージョンを以外のすべてのリージョンのデータを集約します。Security Hub は、新しいリージョンがサポートされ、ユー

ザーが選択している場合に、それらの結果も集約します。Regions を使用して、集約から除外するリージョンのリストを提供します。

- SPECIFIED_REGIONS - Security Hub は、リージョンの選択されたリストからデータを集約します。Security Hub は、新しいリージョンのデータを自動で集約しません。Regions を使用して、集約するリージョンのリストを提供します。

- AWS CLI: コマンドラインで create-finding-aggregator コマンドを実行します。各リージョンはスペースで区切ります。

```
aws securityhub create-finding-aggregator --region <aggregation Region> --region-linking-mode ALL_REGIONS | ALL_REGIONS_EXCEPT_SPECIFIED | SPECIFIED_REGIONS --regions <Region list>
```

以下の例では、クロスリージョン集約が、選択したリージョンに対して設定されています。集約リージョンは米国東部 (バージニア北部) です。リンクされたリージョンは、米国西部 (北カリフォルニア)と米国西部 (オレゴン) です。

```
aws securityhub create-finding-aggregator --region us-east-1 --region-linking-mode
 SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

クロスリージョン集約設定の表示

現在のクロスリージョン集約の設定は、どのリージョンからでも閲覧できます。設定には、集約リージョン、リンクされたリージョン、および新しいリージョンを自動的にリンクするためのオプションが含まれます。

現在のクロスリージョン集約の設定を表示する (コンソール)

[Settings] (設定) ページ の [Regions] (リージョン) タブには、現在のクロスリージョン集約の設定が表示されます。この設定は、どのリージョンからでも閲覧できます。メンバーアカウントは、管理者アカウントが設定したクロスリージョン集約の設定も閲覧できます。

クロスリージョン集約が有効になっていない場合、[Regions] (リージョン) タブには、クロスリージョン集約を有効にするためのオプションが表示されます。the section called “クロスリージョン集約を有効にする” を参照してください。クロスリージョン集約を有効にできるのは、管理者アカウントとスタンドアロンアカウントのみです。

クロスリージョン集約が有効になっている場合、[Regions] (リージョン) タブには、以下の情報が表示されます。

- 集約リージョン
- Security Hub がサポートし、ユーザーが選択している新しいリージョンの、結果、インサイト、コントロールステータス、セキュリティスコアを自動的に集約するかどうか
- リンクされたリージョンのリスト

現在のクロスリージョン集約設定の表示 (Security Hub API、 AWS CLI)

Security Hub API または を使用して AWS CLI 、現在のクロスリージョン集約設定を表示できます。クロスリージョン集約の設定は、どのリージョンからでも閲覧できます。

現在のクロスリージョン集約の設定を表示するには (Security Hub API、 AWS CLI)

- Security Hub API: `GetFindingAggregator` APIを使用します。リクエストするときには、結果アグリゲーター ARN を提供する必要があります。結果アグリゲーター ARN を取得するには、`ListFindingAggregators` を使用します。
- AWS CLI: コマンドラインで `get-finding-aggregator` コマンドを実行します。結果アグリゲーター ARN を取得するには、`list-finding-aggregators` を使用します。

```
aws securityhub get-finding-aggregator --finding-aggregator-arn <finding aggregator
 ARN>
```

クロスリージョン集約の設定を更新する

クロスリージョン集約の設定を更新し、現在の集約リージョンのリンクされた AWS リージョン を変更することができます。また、新しいリージョンの結果、インサイト、コントロールステータス、セキュリティスコアを自動的に集約するかどうかを変更することもできます。

クロスリージョン集約の変更は、オプトインリージョンが AWS アカウントで有効になるまで、そのリージョンには実装されません。2019 年 3 月 20 日以降に導入 AWS されたリージョンは、オプトインリージョンです。

リンクされたリージョンからデータを集約することを止めても、Security Hub は、集約リージョンから既に集約したデータを削除しません。

更新プロセスを使用して集約リージョンを変更することはできません。集約リージョンを変更するには、以下を実行する必要があります:

1. クロスリージョン集約を停止します。「the section called “クロスリージョン集約を停止する”」を参照してください。
2. 新しい集約リージョンにするリージョンに変更します。
3. クロスリージョン集約を有効にします。the section called “クロスリージョン集約を有効にする” を参照してください。

クロスリージョン集約の設定を更新する (コンソール)

現在の集約リージョンの、クロスリージョン集約の設定を更新する必要があります。

集約リージョン AWS リージョン 以外の では、結果の集約パネルに、集約リージョンの設定を編集する必要があるというメッセージが表示されます。このメッセージを選択すると、集約リージョンに移動するためのリンクが表示されます。

現在の集約リージョンのリンクされたリージョンを変更するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. 現在の集約リージョンに変更します。
3. Security Hub ナビゲーションメニューで、[Settings] (設定)、[Regions] (リージョン) の順に選択します。
4. [Finding aggregation] (結果の集約) で、[Edit] (編集) を選択します。
5. [Linked Regions] (リンクされたリージョン) で、選択したリンクされたリージョンを更新します。
6. 必要に応じて、[Link future Regions] (将来のリージョンをリンクする) の選択を変更します。この設定は、Security Hub に新しいリージョンへのサポートが追加され、ユーザーがそのリージョンを選択している場合に、Security Hub で自動的にリンクするかどうかを決定します。
7. [Save] (保存) を選択します。

クロスリージョン集約設定の更新 (Security Hub API、 AWS CLI)

Security Hub API または を使用して AWS CLI 、クロスリージョン集約設定を更新できます。現在の集約リージョンの、クロスリージョン集約を更新する必要があります。

リージョンのリンクモードを変更できます。リンクモードが ALL_REGIONS_EXCEPT_SPECIFIED または SPECIFIED_REGIONS の場合、除外されるリージョンまたは含まれるリージョンのリストを変更できます。

除外または含まれるリージョンのリストを変更する場合は、更新時に完全なリストを提供する必要があります。例えば、現在、米国東部 (オハイオ) からの結果を集約していて、米国西部 (オレゴン) の結果も集約したい場合には、UpdateFindingAggregator を呼び出すときに、米国東部 (オハイオ) と米国西部 (オレゴン) の両方を含む Regions リストを提供します。

クロスリージョン集約を更新するには (Security Hub API、 AWS CLI)

- Security Hub API: UpdateFindingAggregator API オペレーションを使用します。結果アグリゲーターを識別するには、結果アグリゲーター ARN を提供する必要があります。結果アグリゲーター ARN を取得するには、ListFindingAggregators を使用します。

  リージョンリンクモードと、除外または含まれるリージョンの更新されたリストを提供します。

- AWS CLI: コマンドラインで update-finding-aggregator コマンドを実行します。各リージョンはスペースで区切ります。

```
aws securityhub update-finding-aggregator --region <aggregation Region> --finding-
aggregator-arn <finding aggregator ARN> --region-linking-mode ALL_REGIONS |
 ALL_REGIONS_EXCEPT_SPECIFIED | SPECIFIED_REGIONS --regions <Region list>
```

  以下の例では、クロスリージョン集約の設定が、選択したリージョンの集約に変更されています。コマンドは、現在の集約リージョンである米国東部 (バージニア北部) から実行されます。リンクされたリージョンは、米国西部 (北カリフォルニア)と米国西部 (オレゴン) です。

```
aws securityhub update-finding-aggregator --region us-east-1 --finding-aggregator-arn
 arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-
a456-426652340000 --region-linking-mode SPECIFIED_REGIONS --regions us-west-1 us-
west-2
```

クロスリージョン集約を停止する

データを集約する必要がなくなった場合、または集約リージョンを変更したい場合は、クロスリージョン集約を停止します。

クロスリージョン集約を停止すると、Security Hub はデータの集約を停止します。それによって、集約リージョンから既存の集約データが削除されることはありません。

クロスリージョン集約を停止する (コンソール)

現在の集約リージョンの、クロスリージョン集約の設定を停止する必要があります。

集約リージョン以外のリージョンの場合、[Finding aggregation] (結果の集約) パネルに、集約リージョンで設定を編集する必要があることを示すメッセージが表示されます。このメッセージを選択して、集約リージョンへと切り替えるリンクを表示します。

クロスリージョン集約を停止するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. 現在の集約リージョンに変更します。
3. Security Hub ナビゲーションメニューで、[Settings] (設定)、[Regions] (リージョン) の順に選択します。
4. [Finding aggregation] (結果の集約) で、[Edit] (編集) を選択します。
5. [Aggregation Region] (集約リージョン) で、[No aggregation Region] (集約リージョンなし) を選択します。
6. [Save] (保存) を選択します。
7. 確認ダイアログの確認フィールドに、**`Confirm`** と入力します。
8. [Confirm] (確認) を選択します。

クロスリージョン集約の停止 (Security Hub API、 AWS CLI)

クロスリージョン集約は、Security Hub API を使用して停止することができます。集約リージョンの、クロスリージョン集約を停止する必要があります。

クロスリージョン集約を停止するには (Security Hub API、 AWS CLI)

- Security Hub API: `DeleteFindingAggregator` オペレーションを使用します。削除する結果アグリゲーターを識別するには、結果アグリゲーター ARN を提供します。結果アグリゲーター ARN を取得するには、`ListFindingAggregators` を使用します。
- AWS CLI: コマンドラインで `delete-finding-aggregator` コマンドを実行します。

```
aws securityhub delete-finding-aggregator <finding aggregator ARN> --
region <aggregation Region>
```

AWS Security Hub の検出結果

AWS Security Hub は、複数のプロバイダーからの大量の検出結果に対処する複雑さを排除します。これにより、すべての AWS アカウント、リソース、ワークロードを管理し、セキュリティを高めるために必要となる労力が軽減されます。

Security Hub は、以下のソースから結果を受け取ります。

- Security Hub は、有効にしたコントロールに対してチェックを行います。「the section called “コントロールの結果を生成および更新する”」を参照してください。
- 有効に AWS のサービス した との統合。「the section called “AWS のサービス 統合”」を参照してください。
- 有効にしたサードパーティー製品との統合。「the section called “新しいサードパーティー製品の統合”」を参照してください。
- 設定したカスタム統合。「the section called “カスタム製品統合の使用”」を参照してください。

Security Hub は、 AWS Security Finding 形式と呼ばれる標準の検出結果形式を使用して検出結果を使用します。検出結果形式の詳細については、「the section called “Finding 形式”」を参照してください。

Security Hub は、結果を統合された製品全体と関連づけて、最も重要なものに優先順位を付けます。

結果プロバイダーは、結果の追加インスタンスを反映するように結果を更新できます。結果を更新して、調査とその結果に関する詳細を提供することができます。

Security Hub では、リージョン全体の結果も集約することができるため、すべての結果を 1 つの場所に表示することも可能です。「クロスリージョン集約」を参照してください。

トピック

- AWS Security Hubでの結果の作成と更新
- 結果の詳細と履歴の管理と確認
- の検出結果に対するアクションの実行 AWS Security Hub
- AWS Security Finding 形式 (ASFF)

AWS Security Hubでの結果の作成と更新

では AWS Security Hub、検出結果は次のいずれかのタイプの検出結果プロバイダーから発信されます。

- Security Hub で有効なセキュリティコントロール
- 別の との有効な統合 AWS のサービス
- サードパーティー製品との有効な統合

結果の作成後は、結果プロバイダーまたはお客様が結果を更新することができます。

- 結果プロバイダーは、`BatchImportFindings` API オペレーションを使用して、結果に関する一般情報を更新します。結果プロバイダーは、自身が作成した結果のみを更新できます。
- お客様は `BatchUpdateFindings` API オペレーションを使用して、調査結果の調査のステータスを更新します。 `BatchUpdateFindings` は、お客様に代わってチケット発行、インシデント管理、オーケストレーション、修復、または SIEM ツールでも使用できます。

  お客様は Security Hub コンソールから、結果のワークフローステータスを管理し、結果をカスタムアクションに送信することができます。「the section called “結果に対してアクションを実行するには”」を参照してください。

Security Hub も結果を自動的に更新して削除します。90 日以内に更新されなかった場合、すべての結果は自動的に削除されます。

クロスリージョン集約を有効にすると、Security Hub は、リンクされたリージョンから集約リージョンに新しい結果を自動的に集約します。Security Hub も、更新情報を結果に複製します。リンクされたリージョンで発生した更新は、集約リージョンに複製されます。集約リージョンで発生した更新は、リンクされたリージョンにレプリケートされます。クロスリージョン集約の詳細については、「クロスリージョン集約」を参照してください。

トピック

- BatchImportFindings を使用して結果を作成および更新する
- BatchUpdateFindings を使用して結果を更新する

BatchImportFindings を使用して結果を作成および更新する

結果プロバイダーは、BatchImportFindings API オペレーションを使用して、新しい結果を作成し、作成した結果に関する情報を更新します。自分自身で作成したのではない結果を更新することはできません。

顧客、SIEMs、チケット発行ツール、SOAR ツールはBatchUpdateFindings、 を使用して、検出結果プロバイダーからの調査結果の調査に関連する更新を行います。the section called “BatchUpdateFindings を使用する” を参照してください。

が結果を作成または更新するBatchImportFindingsリクエスト AWS Security Hub を受信するたびに、Amazon でSecurity Hub Findings - Importedイベントが自動的に生成されます EventBridge。「the section called “自動応答および自動修復”」を参照してください。

アカウントとバッチサイズに対する要件

BatchImportFindings を、次のいずれかで呼び出す必要があります。

- 結果に関連付けられているアカウント。関連付けられたアカウントの識別子は、結果の AwsAccountId 属性の値です。
- 公式の Security Hub パートナー統合で許可リストに載っているアカウント。

Security Hub は、Security Hub が有効になっているアカウントの結果更新のみを受け入れます。結果プロバイダーも有効にする必要があります。Security Hub が無効になっているが、結果プロバイダーとの統合が有効になっていない場合は、結果は FailedFindings リストで返され、InvalidAccess エラーが表示されます。

BatchImportFindings は、バッチあたり最大 100 件、1 回の結果あたり最大 240 KB、バッチあたり最大 6 MB の結果を受け入れます。スロットリングレートの制限は、各リージョンの 1 アカウントあたり 10 TPS で、バーストは 30 TPS です。

結果を作成するか更新するかの決定

結果を作成するか更新するかを決定するために、Security Hub は ID フィールドをチェックします。ID の値が既存の結果と一致しない場合は、新しい結果が作成されます。

ID が既存の結果と一致する場合、Security Hub は UpdatedAt フィールドに更新がないかをチェックします。

- 更新上の UpdatedAt が一致するか、既存の結果の UpdatedAt より前に発生した場合、更新は無視されます。
- 更新上の UpdatedAt が既存の結果の UpdatedAt の後に発生している場合、既存の結果は更新されます。

BatchImportFindings の制限された属性

既存の検出結果の場合、検出結果プロバイダーは BatchImportFindingsを使用して次の属性とオブジェクトを更新できません。これらの属性は、BatchUpdateFindings を使用してのみ更新できます。

- Note
- UserDefinedFields
- VerificationState
- Workflow

Security Hub は、これらの属性とオブジェクトのBatchImportFindingsリクエストで提供されたコンテンツを無視します。お客様、またはお客様を代行する他のプロバイダーは、BatchUpdateFindings を使用して更新します。

FindingProviderFields を使用する

また、検出結果プロバイダーは、 BatchImportFindingsを使用して次の属性を更新しないでください。

- Confidence
- Criticality
- RelatedFindings
- Severity
- Types

代わりに、結果プロバイダーは FindingProviderFields オブジェクトを使用して、これらの属性の値を提供します。

例

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

BatchImportFindings リクエストの場合、Security Hub はトップレベル属性内および FindingProviderFields 内の値を以下のとおり処理します。

(推奨) **BatchImportFindings** は **FindingProviderFields** 内の属性の値を提供しますが、対応するトップレベル属性には値を提供しません。

例えば、BatchImportFindings は FindingProviderFields.Confidence を提供しますが、Confidence は提供しません。これは、BatchImportFindings リクエストに推奨されるオプションです。

Security Hub は、FindingProviderFields 内の属性の値を更新します。

属性が によってまだ更新されていない場合にのみ、最上位属性に値をレプリケートしますBatchUpdateFindings。

BatchImportFindings は、トップレベル属性の値を提供しますが、**FindingProviderFields** 内の対応する属性には値を提供しません。

例えば、BatchImportFindings は Confidence を提供しますが、FindingProviderFields.Confidence は提供しません。

Security Hub は、値を使用して FindingProviderFields の属性を更新します。既存の値はすべて上書きされます。

Security Hub は、属性が BatchUpdateFindings によってまだ更新されていない場合にのみ、トップレベルの属性を更新します。

BatchImportFindings は、**FindingProviderFields** のトップレベル属性と対応する属性の両方の値を提供します。

例えば、BatchImportFindings は Confidence と FindingProviderFields.Confidence の両方を提供します。

新しい結果を得るために、Security Hub では FindingProviderFields 内の値を使用して、FindingProviderFields 内のトップレベル属性と対応する属性の両方を入力します。指定された最上位属性値は使用されません。

既存の結果の場合、Security Hub は両方の値を使用します。ただし、トップレベルの属性値が更新されるのは、BatchUpdateFindings により属性がまだ更新されていない場合のみです。

からの batch-import-findings コマンドの使用 AWS CLI

では AWS Command Line Interface、 batch-import-findings コマンドを使用して検出結果を作成または更新します。

各結果は JSON オブジェクトとして提供します。

例

```
aws securityhub batch-import-findings --findings
    [{
        "AwsAccountId": "123456789012",
        "CreatedAt": "2019-08-07T17:05:54.832Z",
        "Description": "Vulnerability in a CloudTrail trail",
        "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0/rule/2.2",
        "Id": "Id1",
        "ProductArn": "arn:aws:securityhub:us-west-1:123456789012:product/123456789012/
default",
        "Resources": [
            {
                "Id": "arn:aws:cloudtrail:us-west-1:123456789012:trail/TrailName",
                "Partition": "aws",
                "Region": "us-west-1",
                "Type": "AwsCloudTrailTrail"
            }
        ],
        "SchemaVersion": "2018-10-08",
```

```
        "Title": "CloudTrail trail vulnerability",
        "UpdatedAt": "2020-06-02T16:05:54.832Z",
        "Types": [
            "Software and Configuration Checks/Vulnerabilities/CVE"
        ],
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "0"
        }
    }]'
```

BatchUpdateFindings を使用して結果を更新する

BatchUpdateFindings アクションは、検出結果プロバイダーからの結果をお客様が処理する場合の情報を更新するために使用します。これは、お客様や、お客様の代行として動作する SIEM、チケット発券、インシデント管理、または SOAR ツールが使用します。を使用してBatchUpdateFindings、 AWS Security Finding 形式 (ASFF) の特定のフィールドを更新できます。

BatchUpdateFindings を使用して、新しい検出結果を作成することはできません。これを使用すると、一度に 100 件までの検出結果を更新できます。

Security Hub は、結果の更新BatchUpdateFindingsリクエストを受信するたびに、Amazon でSecurity Hub Findings - Importedイベントを自動的に生成します EventBridge。the section called “自動応答および自動修復” を参照してください。

BatchUpdateFindings は検出結果の UpdatedAtフィールドを変更しません。 は検出結果プロバイダーからの最新の更新UpdatedAtのみを反映します。

BatchUpdateFindings の使用可能なフィールド

管理者アカウントは、>BatchUpdateFindings を使用して、自分のアカウントまたはメンバーアカウントの検出結果を更新できます。メンバーアカウントは、>BatchUpdateFindings を使用して、自分のアカウントの検出結果を更新できます。

お客様のみ > BatchUpdateFindings を使用して、以下のフィールドとオブジェクトを更新できます。

- Confidence
- Criticality

- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

デフォルトでは、管理者アカウントとメンバーアカウントは、上記のすべてのフィールドとフィールド値にアクセスできます。Security Hub では、フィールドとフィールド値へのアクセスを制限するためのコンテキストキーも提供されています。

例えば、メンバーアカウントが Workflow.Status を RESOLVED のみに設定できるようにする場合などです。または、メンバーアカウントに Severity.Label の変更を許可したくない場合などもあります。

BatchUpdateFindings へのアクセスの設定

IAM ポリシーを設定してアクセスを制限し、フィールドとフィールド値を更新するための BatchUpdateFindings の使用を制限できます。

BatchUpdateFindings へのアクセスを制限するステートメントで、以下の値を使用します：

- Action は securityhub:BatchUpdateFindings
- Effect は Deny。
- Condition では、以下に基づいて BatchUpdateFindings リクエストを拒否できます。
  - 結果に特定のフィールドが含まれる。
  - 結果に特定のフィールド値が含まれる。

条件キー

これらは、BatchUpdateFindings へのアクセスを制限するための条件キーです。

ASFF フィールド

ASFF フィールドの条件キーは以下のとおりです：

```
securityhub:ASFFSyntaxPath/<fieldName>
```

<fieldName> を ASFF フィールドで置き換えます。BatchUpdateFindings へのアクセスを設定する場合は、1 つの親レベルのフィールドではなく、IAM ポリシーに 1 つ以上の特定の ASFF フィールドを含めます。例えば、Workflow.Status フィールドへのアクセスを制限するには、Workflow 親レベルフィールドの代わりに securityhub:ASFFSyntaxPath/Workflow.Status をポリシーに含める必要があります。

フィールドに対するすべての更新を禁止する

ユーザーが特定のフィールドを更新できないようにするには、以下のような条件を使用します。

```
 "Condition": {
                "Null": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "false"
               }
}
```

例えば、以下のステートメントは、BatchUpdateFindings を使用してワークフローの状態を更新できないことを示しています。

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
        "Null": {
            "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
        }
    }
}
```

特定のフィールド値の許可を禁止する

ユーザーがフィールドを特定の値に設定できないようにするには、以下のような条件を使用します:

```
"Condition": {
                "StringEquals": {
```

```
                    "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
                }
}
```

例えば、以下のステートメントは、BatchUpdateFindings を使用して Workflow.Status に SUPPRESSED を設定できないことを示しています。

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
}
```

許可されていない値のリストを提供することもできます。

```
 "Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
 "<fieldValue2>", "<fieldValuen>" ]
                }
}
```

例えば、以下のステートメントは、BatchUpdateFindings を使用して Workflow.Status を RESOLVED または SUPPRESSED に設定できないことを示しています。

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": [
            "RESOLVED",
            "NOTIFIED"
        ]
```

```
    }
}
```

からの コマンドの使用 batch-update-findingsAWS CLI

では AWS Command Line Interface、 batch-update-findings コマンドを使用して検出結果を更新します。

更新する各検出結果に対して、検出結果を生成した製品の検出結果 ID と ARN の両方を提供します。

```
--finding-identifiers ID="<findingID1>",ProductArn="<productARN>"
 ID="<findingID2>",ProductArn="<productARN2>"
```

更新する属性を提供するときは、JSON 形式またはショートカット形式のどちらかを使用できます。

以下は、JSON 形式を使用する Note オブジェクトの更新例です。

```
--note '{"Text": "Known issue that is not a risk.", "UpdatedBy": "user1"}'
```

以下は、同じ更新をショートカット形式を使用した場合の例です。

```
--note Text="Known issue that is not a risk.",UpdatedBy="user1"
```

AWS CLI コマンドリファレンスには、各フィールドの JSON 構文とショートカット構文が記載されています。

以下の > batch-update-findings 例では、2 つの結果を更新して、メモを追加し、重要度ラベルを変更してから、それらを解決します。

```
aws securityhub batch-update-findings --finding-identifiers Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2::product/aws/securityhub" Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" --note '{"Text": "Known issue that is not a
 risk.", "UpdatedBy": "user1"}' --severity '{"Label": "LOW"}' --workflow '{"Status":
 "RESOLVED"}'
```

これは同じ例ですが、JSON の代わりにショートカットを使用しています。

```
aws securityhub batch-update-findings --finding-identifiers Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" --note Text="Known issue that is not a
 risk.",UpdatedBy="user1" --severity Label="LOW" --workflow Status="RESOLVED"
```

結果の詳細と履歴の管理と確認

AWS Security Hub コンソールで結果リストを表示するには、複数の方法があります。

- 検出結果ページ — 有効なすべてのコントロールと製品統合の結果の包括的なリストを表示します。デフォルトでは、 NEWまたは NOTIFIED ワークフローステータスのアクティブな結果が表示されます。
- コントロールの詳細ページ — 特定のコントロールについて過去 24 時間以内に生成された検出結果のリストを表示します。
- インサイトページ – 一致するインサイトの検出結果のリストを表示します。インサイトはコレクション固有の結果です。詳細については、「the section called “インサイト結果と結果の表示”」を参照してください。
- 統合ページ – 統合製品 AWS のサービス またはサードパーティー製品によって生成された結果のリストを表示します。

これらのリストの結果をフィルタリングしてグループ化し、特定のタイプの結果に絞ることができます。前のページで特定の結果を選択して、その詳細を表示することもできます。

プログラムで検出結果のリストを表示するには、Security Hub API の `GetFindings`オペレーションを使用します。フィルターを含めて、特定のタイプの検出結果を取得できます。

クロスリージョン集約を有効にすると、複数のリージョンからコントロールステータス、セキュリティスコア、インサイト、結果を取得できます。集約リージョンでは、結果データには集約リージョンとリンクされたリージョンのデータが含まれます。他のリージョンでは、検出結果はそのリージョンにのみ固有です。クロスリージョン集約の設定については、「」を参照してくださいクロスリージョン集約。

結果のフィルタリングとグループ化 (コンソール)

Security Hub コンソールの検出結果ページ、統合ページ、またはインサイトページに検出結果のリストを表示すると、レコードの状態とワークフローのステータスに基づいてリストが事前にフィルタリングされます。これは、インサイトまたは統合のフィルターに加えて追加されるフィルターです。

レコードの状態は、検出結果がアクティブかアーカイブされているかを示します。デフォルトでは、検出結果リストにはアクティブな検出結果のみが表示されます。検出結果は検出結果プロバイダーによってアーカイブできます。 AWS Security Hub また、関連付けられたリソースが削除されると、コントロールの検出結果も自動的にアーカイブされます。

ワークフローステータスは、結果の調査のステータスを示します。デフォルトでは、結果リストには、ワークフローステータスが `NEW` または `NOTIFIED` の結果のみが表示されます。検出結果のワークフローステータスを更新できます。

結果の集約を有効にし、集約リージョンにサインインしている場合は、結果とインサイトページでリージョン別に結果をフィルタリングできます。

コントロールの検出結果の操作については、「」を参照してくださいthe section called “結果のフィルタリングとソート”。このページの情報は、検出結果 、インサイト 、統合 ページの検出結果リストに適用されます。

フィルターを追加する

リストの範囲を変更するには、リストにフィルターを追加できます。

最大 10 個の属性でフィルタリングできます。各属性に対して、最大 20 個のフィルター値を提供できます。

結果リストをフィルタリングする場合、Security Hub は AND ロジックをフィルターセットに適用します。つまり、結果は、指定されたすべてのフィルターに一致する場合にのみ一致となります。例えば、 を製品名のフィルター GuardDuty として追加し、 をリソースタイプのフィルターAwsS3Bucketとして追加する場合、一致する検出結果はこれらの両方の基準と一致する必要があります。

ただし、同じ属性に異なる値を使用するフィルターの場合、Security Hub は OR ロジックを適用します。例えば、 GuardDuty と Amazon Inspector の両方を製品名のフィルター値として追加します。この場合、検出結果は GuardDuty または Amazon Inspector のいずれかによって生成された場合に一致します。

結果リストにフィルターを追加するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. 結果リストを表示するには、以下のいずれかを実行します。
   - Security Hub ナビゲーションペインで、[Findings] (結果) を選択します。
   - Security Hub ナビゲーションペインで、[Insights] (インサイト) を選択します。インサイトを選択します。次に、検出結果リストで、インサイトの結果を選択します。
   - Security Hub ナビゲーションペインで、[Integrations] (統合) を選択します。統合の [See findings] (結果を表示) を選択します。
3. フィルターの追加ボックスのフィルター で、フィルターを選択します。

   会社名または製品名 でフィルタリングすると、コンソールは最上位の フィールドCompanyNameと ProductNameフィールドを使用します。API は、ProductFields にある値を使用します。
4. フィルターの一致タイプを選択します。

   文字列フィルターの場合、次の比較オプションの中から選択できます。

   - is - フィルター値と完全に一致する値を検索します。
   - starts with - フィルター値で始まる値を検索します。
   - is not - フィルター値と一致しない値を検索します。
   - does not start with - フィルター値で始まらない値を検索します。

   数値フィルターの場合、単一の数値 ([Simple] (シンプル)) を指定するか、数値の範囲 ([Range] (範囲)) を指定するかを選択できます。

   日時フィルターの場合、現在の日時からの時間の長さ ([Rolling window] (ローリングウィンドウ)) を指定するか、特定の日付範囲 ([Fixed range] (固定範囲)) を指定するかを選択できます。

   複数のフィルターを追加した場合、以下のように相互作用します。

   - is および starts with フィルターは OR で結合されます。フィルター値のいずれかが含まれている場合に、値が一致となります。例えば、[Severity label is CRITICAL] (重要度ラベルは重大) および [Severity label is HIGH] (重要度ラベルは高)と指定している場合、結果には重要度が重大な結果と重要度の高い結果の両方が含まれます。

- is not および does not start with フィルターは AND で結合されます。値は、これらのフィルター値を一切含まなかった場合にのみ一致となります。例えば、重要度ラベルが LOW ではなく、重要度ラベルが MEDIUM でない場合、結果には重要度が低または中の結果は含まれません。

フィールドで is フィルターがある場合、 is not または does not start with filter on the same field は使用できません。

5. フィルター値を指定します。

   文字列フィルターの場合、フィルター値は大文字と小文字が区別されます。

   例えば、Security Hub からの結果の場合、[Product name] (製品名) は Security Hub です。EQUALS 演算子を使用して Security Hub からの結果を表示する場合は、フィルター値として **`Security Hub`** を入力する必要があります。**`security hub`** と入力すると、一致結果には何も表示されません。

   同様に、PREFIX 演算子を使用して **`Sec`** と入力すると、Security Hub の結果が表示されますが、**`sec`** と入力すると、Security Hub の一致結果には何も表示されません。

6. [Apply] (適用) を選択します。

結果をグループ化する

フィルターを変更することに加えて、選択した属性の値に基づいて結果をグループ化することもできます。

結果をグループ化すると、結果のリストが、一致する結果内の選択した属性の値のリストに置き換えられます。各値に対して、他のフィルター条件に一致する結果の数がリストに表示されます。

例えば、検出結果を AWS アカウント ID でグループ化すると、アカウント識別子のリストと、各アカウントの一致する検出結果の数が表示されます。

なお、Security Hub で表示できる値の数は最大 100 個です。グループ化値の数が 100 を超える場合、最初の 100 個のみが表示されます。

属性値を選択すると、その値と一致した結果のリストが表示されます。

結果リスト内の結果をグループ化するには

1. 結果リストで、[Add filters] (フィルターを追加する) ボックスを選択します。

2. グループ化 で、 によるグループ化を選択します。
3. リストで、グループ化に使用する属性を選択します。
4. [Apply] (適用) を選択します。

フィルター値またはグループ化属性を変更する

既存のフィルターの場合、フィルター値を変更することができます。グループ化属性を変更することもできます。

例えば、[Record state] (レコードの状態) フィルターを変更して、`ACTIVE` の結果ではなく `ARCHIVED` の結果を検索することができます。

フィルターまたはグループ化属性を編集するには

1. フィルタリングされた結果リストで、フィルターまたはグループ化属性を選択します。
2. [Group by] (グループ化の条件) で新しい属性を選択し、[Apply] (適用) を選択します。
3. フィルターの場合は新しい値を選択し、[Apply] (適用) を選択します。

フィルターまたはグループ化属性を削除する

フィルターまたはグループ化属性を削除するには、x アイコンを選択します。

リストが自動的に更新され、変更が反映されます。グループ化属性を削除すると、リストがフィールド値のリストから結果のリストへと戻ります。

利用可能な結果情報

Security Hub コンソールで、または Security Hub API の GetFindingsオペレーションを呼び出すことで、さまざまな検出結果の詳細を取得できます。以下は、取得できる検出結果の詳細のタイプの一部リストです。

- アプリケーションメタデータ – アプリケーションを作成した場合、検出結果に関係するアプリケーションの名前と Amazon リソースネーム (ARN) を指定します。 と は AWS 、アプリケーションタグを追加しました。でアプリケーションを作成することをお勧めしますAWS Service Catalog AppRegistry。
- 検出結果の履歴 – 過去 90 日間の検出結果の履歴を提供します。
- Detective での調査結果 (コンソールのみ ） — 自動ログ収集、セキュリティ分析、 AWS のサービス リソース探索ツールを使用して Detective での検出結果をさらに調査するためのリンクを提供

します。この情報は、Detective を有効にした AWS のサービス 場合にのみ、他の から受け取った Security Hub の検出結果に含まれます。

- 検出結果プロバイダーフィールド – 信頼度、重要度、関連する検出結果、重要度、検出結果タイプについて、検出結果プロバイダーの値を表示します。
- Parameters – セキュリティコントロールの現在のパラメータ値を表示します。Security Hub は、コントロールのセキュリティチェックを行う際にこれらのパラメータ値を使用します。
- 修復 — 失敗したコントロールの検出結果を修復する手順へのリンクを提供します。
- リソース — 結果に関係する AWS リソースに関する情報を提供します。
- リソースタグ — 検出結果に関係するリソースのタグキーと値に関する情報を提供します。タグ付け API の `GetResources`オペレーションでサポートされているリソースに AWS Resource Groups タグ付けできます。Security Hub は、サービスにリンクされたロールを介してこのオペレーションを呼び出し、 AWS Security Finding Format (ASFF) `Resource.Id`フィールドにリソース ARN が入力されている場合に AWS リソースタグを取得します。無効なリソース IDsは無視されます。検出結果にリソースタグを含める方法の詳細については、「」を参照してくださいタグ。
- タイプと関連する検出結果 – 検出結果タイプに関する情報が含まれます。
- 脆弱性の詳細 — 検出結果および影響を受けるパッケージで検出された脆弱性に関する情報。これらの詳細は、Amazon Inspector が Security Hub に送信する検出結果に対して Amazon Inspector を有効にすると表示されます。

以下のセクションで、検出結果の詳細にアクセスする方法を理解します。

結果履歴の確認

検出結果の履歴は、過去 90 日間に検出結果に加えられた変更を追跡できる Security Hub の機能です。アクティブな検出結果とアーカイブされた検出結果に利用できます。検出結果の履歴は、変更内容、発生日時、どのユーザーによって行われたかなど、検出結果に対して加えられた変更の履歴を改変不能な形で記録します。

特に、AWS Security Finding 形式 (ASFF) のフィールドに加えられた変更を追跡できます。Security Hub は、手動で行った変更と自動化ルールによる変更を追跡します。

検出結果の履歴は、Security Hub コンソール、API、および で確認できます AWS CLI。

Security Hub 管理者アカウントにサインインしている場合は、管理者アカウントとすべてのメンバーアカウントにおける検出結果の履歴を取得できます。

任意の方法を選択し、手順に従って検出結果の履歴を確認します。

Security Hub console

結果履歴の確認

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. 左のナビゲーションペインで [検出結果] を選択します。
3. 検出結果を選択します。表示されるパネルで、[履歴] タブを選択します。

Security Hub API

結果履歴の確認

1. を実行するかGetFindings、 を使用している場合は AWS CLI、 get-findings コマンドを実行します。必要に応じて適切なフィルターを使用して、履歴を表示する結果を特定します。API のレスポンスから検出結果の `ProductArn` と `Id` を取得できます。これらのフィールドの値は、3 番目のステップで必要になります。
2. を実行するかGetFindingHistory、 を使用している場合は AWS CLIコマンドを実行しますget-finding-history。
3. `ProductArn` および `Id` フィールドを使用して、履歴を取得する検出結果を特定します。フィールドの詳細については、「AwsSecurityFindingIdentifier」を参照してください。リクエストあたり 1 つの検出結果の履歴のみ取得できます。
4. `StartTime`. と の値を指定`EndTime`して、結果履歴を特定の期間に制限します。
5. `MaxResults` の値を指定すると、特定の結果件数に限定した検出結果の履歴を取得できます。指定しない場合、API レスポンスによって最初の 100 件の結果が返されます。
6. `NextToken` の値を指定すると、次の 100 件の結果 (該当する場合) を表示できます。最初の API リクエストでは、`NextToken` の値は `NULL` でなければなりません。

次の CLI コマンドは、指定された結果の履歴を取得します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub get-finding-history \
--region us-west-2 \
--finding-identifier Id="a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2:123456789012:product/123456789012/default" \
--max-results 2 \
```

```
--start-time "2021-09-30T15:53:35.573Z" \
--end-time "2021-09-31T15:53:35.573Z"
```

結果の詳細の確認

任意の方法を選択し、手順に従って Security Hub で検出結果の詳細を表示します。

Security Hub console

結果の詳細の確認

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. 結果リストを表示するには、次のいずれかのアクションを実行します。
   - Security Hub ナビゲーションペインで、[Findings] (結果) を選択します。必要に応じて検索フィルターを追加して、結果リストを絞り込みます。
   - Security Hub ナビゲーションペインで、[Insights] (インサイト) を選択します。インサイトを選択します。次に、検出結果リストで、インサイトの結果を選択します。
   - Security Hub ナビゲーションペインで、[Integrations] (統合) を選択します。統合の [See findings] (結果を表示) を選択します。
3. 結果のタイトルを選択します。
4. 検出結果の詳細パネルから、次のように追加のアクションを実行できます。
   - 結果の完全な JSON を表示するには、結果 ID を選択します。JSON の検出結果 から、検出結果 JSON をダウンロードします。
   - AWS Config ルールに基づく検出結果について、該当するルールのリストを表示するには、ルール を選択します。
   - Macie で調査を選択して、Macie コンソールの検出結果で検出された機密データを調査します。このオプションは、Amazon Macie とその機密データ自動検出機能を有効にする場合にのみ使用できます。
   - リソースを選択すると、結果に関係するリソースに関する情報が表示されます。
   - Amazon Detective で調査 を選択して、Detective コンソールで検出結果を調査します。このオプションは、Amazon Detective を有効にした場合にのみ使用できます。
   - 履歴タブを選択すると、最大 90 日間の検出結果履歴が表示されます。

> **Note**
>
> 検出結果の詳細パネルの上部には、アカウント、重要度、日付、ステータスなどが含まれた、検出結果に関する概要情報が表示されます。と統合 AWS Organizations し、サインインしているアカウントが組織メンバーアカウントである場合、詳細パネルにはアカウント名が含まれます。Organizations 統合ではなく手動で招待されたメンバーアカウントの場合、詳細パネルにはアカウント ID のみが表示されます。

Security Hub API

結果の詳細の確認

Security Hub API の `GetFindings`オペレーションを使用するか、 を使用している場合は AWS CLI get-findings コマンドを実行します。

`Filters` パラメータに 1 つ以上の値を指定して、取得する結果を絞り込むことができます。

結果の量が多すぎる場合は、 `MaxResults`パラメータを使用して結果を指定された数に制限し、`NextToken`パラメータを使用して結果をページ分割できます。`SortCriteria` パラメータを使用して、結果を特定のフィールドでソートします。

クロスリージョン集約を有効にし、集約リージョンからこのオペレーションを呼び出すと、結果には集約リージョンとリンクされたリージョンの結果が含まれます。

次の CLI コマンドは、指定されたフィルターに一致する検出結果を取得し、`LastObservedAt`フィールドの降順でソートします。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub get-findings \
--filters '{"GeneratorId":[{"Value": "aws-
foundational","Comparison":"PREFIX"}],"WorkflowStatus": [{"Value":
 "NEW","Comparison":"EQUALS"}],"Confidence": [{"Gte": 85}]}' --sort-criteria
 '{"Field": "LastObservedAt","SortOrder": "desc"}' --page-size 5 --max-items 100
```

PowerShell

結果の詳細の確認

1. `Get-SHUBFinding` コマンドレットを使用します。

2. オプションで、Filter パラメータを入力して、取得したい結果を絞り込むこともできます。

例

```
Get-SHUBFinding -Filter @{AwsAccountId =
 [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =
 "XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =
 "EQUALS"; Value = 'FAILED'}}
```

> **Note**
>
> CompanyName または で結果をフィルタリングするとProductName、Security Hub は ProductFields ASFF オブジェクトの一部である値を使用します。Security Hub では、最上位の フィールドCompanyNameと ProductNameフィールドは使用されません。

の検出結果に対するアクションの実行 AWS Security Hub

AWS Security Hub では、調査結果の調査の現在のステータスを追跡できます。

また、結果をカスタムアクションに送信して、処理することもできます。

トピック

- 結果のワークフローステータスを設定する
- カスタムアクションに結果を送信する

結果のワークフローステータスを設定する

ワークフローステータスは、検出結果に対する調査の進行状況を追跡します。ワークフローステータスは、個々の結果に固有のものです。新しい検出結果の生成には影響しません。例えば、検出結果のワークフローステータスを SUPPRESSEDまたは AWS Security Hub に設定RESOLVEDしても、 は同じ問題に対して新しい検出結果を生成できません。

ワークフローステータスの値は以下のいずれかになります。

NEW

レビューする前の結果の初期の状態です。

AWS のサービスなどの統合 から取り込まれた検出結果 AWS Configの初期NEWステータスは です。

また、Security Hub は以下の場合に、ワークフローステータス NOTIFIED または RESOLVED を NEW にリセットします。

- RecordState が ARCHIVED から ACTIVE に変更した場合。
- Compliance.Status が PASSED から FAILED 、WARNING、または NOT_AVAILABLE に変更した場合。

これらの変更は、追加の調査が必要であることを意味します。

NOTIFIED

セキュリティ問題についてリソース所有者に通知したことを示しています。このステータスは、自分がリソース所有者ではなく、セキュリティ問題を解決するためにリソース所有者からの介入が必要な場合に使用できます。

次のいずれかが発生すると、ワークフローステータスは NOTIFIED から NEW に自動的に変更されます。

- RecordState が ARCHIVED から ACTIVE に変更した場合。
- Compliance.Status が PASSED から FAILED 、WARNING、または NOT_AVAILABLE に変更した場合。

SUPPRESSED

結果をレビューし、アクションが必要だとは判断しなかったことを示しています。

RecordState が ARCHIVED から ACTIVE に変更されても、SUPPRESSED 結果のワークフローステータスは変わりません。

RESOLVED

この結果はレビューおよび修正され、現在は解決済みと見なされていることを示しています。

以下のいずれかが発生しない限り、結果は RESOLVED を維持します。

- RecordState が ARCHIVED から ACTIVE に変更した場合。
- Compliance.Status が PASSED から FAILED 、WARNING、または NOT_AVAILABLE に変更した場合。

こういったケースでは、ワークフローステータスは自動的に NEW にリセットされます。

コントロールからの結果については、Compliance.Status が PASSED の場合には、Security Hub がワークフローのステータスを自動的に RESOLVED に設定します。

結果のワークフローステータスを設定する

希望する方法を選択し、手順に従って 1 つ以上の結果のワークフローステータスを設定します。

特定の結果のワークフローステータスを自動的に更新するには、自動化ルール を参照してください。

Security Hub console

結果のワークフローステータスを設定するには、以下を実行します。

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. 結果リストを表示するには、以下のいずれかを実行します。
   - Security Hub ナビゲーションペインで、[Findings] (結果) を選択します。
   - Security Hub ナビゲーションペインで、[Insights] (インサイト) を選択します。インサイトを選択します。次に、検出結果リストで、インサイトの結果を選択します。
   - Security Hub ナビゲーションペインで、[Integrations] (統合) を選択します。統合の [See findings] (結果を表示) を選択します。
   - Security Hub ナビゲーションペインで、[Security standards] (セキュリティ標準) を選択します。[View results] (検出結果の表示) を選択して、コントロールのリストを表示します。次にコントロールを選択すると、そのコントロールの検出結果のリストが表示されます。
3. 結果リストで、更新するそれぞれの結果のチェックボックスを選択します。
4. リストの上部にある [Workflow status] (ワークフローステータス) で、ステータスを選択します。
5. ワークフローステータスの設定ダイアログボックスで、ワークフローステータスを更新する理由の詳細を示すオプションのメモを入力します。ステータスの設定 を選択します。

Security Hub API

BatchUpdateFindings API を呼び出します。検出結果を生成した製品の検出結果 ID と ARN の両方を提供します。これらの詳細は、GetFindingsAPI を呼び出すことで取得できます。

AWS CLI

batch-update-findings コマンドを実行します。検出結果を生成した製品の検出結果 ID と ARN の両方を提供します。これらの詳細は、get-findings コマンドを実行することで取得できます。

```
batch-update-findings --finding-identifiers
 Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

例

```
aws securityhub batch-update-findings --finding-identifiers
 Id="arn:aws:securityhub:us-west-1:123456789012:subscription/
pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --
workflow Status="RESOLVED"
```

カスタムアクションに結果を送信する

Amazon で Security Hub を自動化する AWS Security Hub カスタムアクションを作成できます EventBridge。カスタムアクションの場合、イベントタイプは Security Hub Findings - Custom Action になります。

カスタムアクションの作成に関する情報と詳細な手順については、「the section called “自動応答および自動修復”」を参照してください。

カスタムアクションを設定したら、そのアクションに結果を送信できます。

カスタムアクション (コンソール) に結果を送信するには、以下を実行します。

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. 結果リストを表示するには、以下のいずれかを実行します。
   - Security Hub ナビゲーションペインで、[Findings] (結果) を選択します。
   - Security Hub ナビゲーションペインで、[Insights] (インサイト) を選択します。インサイトを選択します。次に、検出結果リストで、インサイトの結果を選択します。
   - Security Hub ナビゲーションペインで、[Integrations] (統合) を選択します。統合の [See findings] (結果を表示) を選択します。

- Security Hub ナビゲーションペインで、[Security standards] (セキュリティ標準) を選択します。[View results] (検出結果の表示) を選択して、コントロールのリストを表示します。次に、コントロール名を選択します。

3. 結果リストで、カスタムアクションに送信する各結果のチェックボックスを選択します。

   一度に最大 20 件の結果を送信できます。

4. [Actions] (アクション) から、カスタムアクションを選択します。

AWS Security Finding 形式 (ASFF)

AWS Security Hub は、 AWS セキュリティサービスおよびサードパーティー製品統合からの結果を消費、集約、整理、優先順位付けします。Security Hub は、 AWS Security Finding 形式 (ASFF) と呼ばれる標準の検出結果形式を使用してこれらの検出結果を処理します。これにより、時間のかかるデータ変換作業が不要になります。その後、複数の製品から取り込まれた結果を相互に関連付けて、最も重要なものを優先します。

トピック

- AWS Security Finding Format (ASFF) 構文
- ASFF フィールドと値への統合の影響
- ASFF の例

AWS Security Finding Format (ASFF) 構文

このページでは、 AWS Security Finding 形式 (ASFF) の結果の JSON の完全な概要を示します。この形式は JSON スキーマから派生しています。リンクされたオブジェクト名をクリックすると、そのオブジェクトの検出例が表示されます。Security Hub の調査結果をここに示すリソースや例と比較して、調査結果の解釈に役立てることができます。

必要となる ASFF 属性の説明を表示するには、「the section called “必須の最上位属性”」を参照してください。

その他の最上位 ASFF 属性の説明を表示するには、「the section called “オプションの最上位属性”」を参照してください。

```
"Findings": [
    {
     "Action": {
```

```
      "ActionType": "string",
      "AwsApiCallAction": {
       "AffectedResources": {
        "string": "string"
       },
       "Api": "string",
       "CallerType": "string",
       "DomainDetails": {
        "Domain": "string"
       },
       "FirstSeen": "string",
       "LastSeen": "string",
       "RemoteIpDetails": {
        "City": {
         "CityName": "string"
        },
        "Country": {
         "CountryCode": "string",
         "CountryName": "string"
        },
        "IpAddressV4": "string",
        "Geolocation": {
         "Lat": number,
         "Lon": number
        },
        "Organization": {
         "Asn": number,
         "AsnOrg": "string",
         "Isp": "string",
         "Org": "string"
        }
       },
       "ServiceName": "string"
      },
      "DnsRequestAction": {
       "Blocked": boolean,
       "Domain": "string",
       "Protocol": "string"
      },
      "NetworkConnectionAction": {
       "Blocked": boolean,
       "ConnectionDirection": "string",
       "LocalPortDetails": {
        "Port": number,
```

```
        "PortName": "string"
       },
       "Protocol": "string",
       "RemoteIpDetails": {
        "City": {
         "CityName": "string"
        },
        "Country": {
         "CountryCode": "string",
         "CountryName": "string"
        },
        "IpAddressV4": "string",
        "Geolocation": {
         "Lat": number,
         "Lon": number
        },
        "Organization": {
         "Asn": number,
         "AsnOrg": "string",
         "Isp": "string",
         "Org": "string"
        }
       },
       "RemotePortDetails": {
        "Port": number,
        "PortName": "string"
       }
      },
      "PortProbeAction": {
       "Blocked": boolean,
       "PortProbeDetails": [{
        "LocalIpDetails": {
         "IpAddressV4": "string"
        },
        "LocalPortDetails": {
         "Port": number,
         "PortName": "string"
        },
        "RemoteIpDetails": {
         "City": {
          "CityName": "string"
         },
         "Country": {
          "CountryCode": "string",
```

```
          "CountryName": "string"
         },
         "GeoLocation": {
          "Lat": number,
          "Lon": number
         },
         "IpAddressV4": "string",
         "Organization": {
          "Asn": number,
          "AsnOrg": "string",
          "Isp": "string",
          "Org": "string"
         }
        }
       }]
      }
     },
     "AwsAccountId": "string",
     "AwsAccountName": "string",
     "CompanyName": "string",
     "Compliance": {
      "AssociatedStandards": [{
       "StandardsId": "string"
      }],
      "RelatedRequirements": ["string"],
      "SecurityControlId": "string",
      "SecurityControlParameters": [
       {
        "Name": "string",
        "Value": ["string"]
       }
     ],
      "Status": "string",
      "StatusReasons": [
       {
        "Description": "string",
        "ReasonCode": "string"
       }
      ]
     },
     "Confidence": number,
     "CreatedAt": "string",
     "Criticality": number,
     "Description": "string",
```

```
    "FindingProviderFields": {
     "Confidence": number,
     "Criticality": number,
     "RelatedFindings": [{
      "ProductArn": "string",
      "Id": "string"
     }],
     "Severity": {
      "Label": "string",
      "Normalized": number,
      "Original": "string"
     },
     "Types": ["string"]
    },
    "FirstObservedAt": "string",
    "GeneratorId": "string",
    "Id": "string",
    "LastObservedAt": "string",
    "Malware": [{
     "Name": "string",
     "Path": "string",
     "State": "string",
     "Type": "string"
    }],
    "Network": {
     "DestinationDomain": "string",
     "DestinationIpV4": "string",
     "DestinationIpV6": "string",
     "DestinationPort": number,
     "Direction": "string",
     "OpenPortRange": {
      "Begin": integer,
      "End": integer
     },
     "Protocol": "string",
     "SourceDomain": "string",
     "SourceIpV4": "string",
     "SourceIpV6": "string",
     "SourceMac": "string",
     "SourcePort": number
    },
    "NetworkPath": [{
     "ComponentId": "string",
     "ComponentType": "string",
```

```
      "Egress": {
       "Destination": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       },
       "Protocol": "string",
       "Source": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       }
      },
      "Ingress": {
       "Destination": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       },
       "Protocol": "string",
       "Source": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       }
      }
     }],
     "Note": {
      "Text": "string",
      "UpdatedAt": "string",
      "UpdatedBy": "string"
     },
     "PatchSummary": {
      "FailedCount": number,
      "Id": "string",
      "InstalledCount": number,
```

```
      "InstalledOtherCount": number,
      "InstalledPendingReboot": number,
      "InstalledRejectedCount": number,
      "MissingCount": number,
      "Operation": "string",
      "OperationEndTime": "string",
      "OperationStartTime": "string",
      "RebootOption": "string"
    },
    "Process": {
      "LaunchedAt": "string",
      "Name": "string",
      "ParentPid": number,
      "Path": "string",
      "Pid": number,
      "TerminatedAt": "string"
    },
    "ProductArn": "string",
    "ProductFields": {
      "string": "string"
    },
    "ProductName": "string",
    "RecordState": "string",
    "Region": "string",
    "RelatedFindings": [{
      "Id": "string",
      "ProductArn": "string"
    }],
    "Remediation": {
      "Recommendation": {
        "Text": "string",
        "Url": "string"
      }
    },
    "Resources": [{
      "ApplicationArn": "string",
      "ApplicationName": "string",
      "DataClassification": {
        "DetailedResultsLocation": "string",
        "Result": {
          "AdditionalOccurrences": boolean,
          "CustomDataIdentifiers": {
            "Detections": [{
              "Arn": "string",
```

```
          "Count": integer,
          "Name": "string",
          "Occurrences": {
           "Cells": [{
            "CellReference": "string",
            "Column": integer,
            "ColumnName": "string",
            "Row": integer
           }],
           "LineRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "OffsetRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "Pages": [{
            "LineRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "OffsetRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          }
         }],
         "TotalCount": integer
        },
        "MimeType": "string",
        "SensitiveData": [{
         "Category": "string",
         "Detections": [{
```

```
          "Count": integer,
          "Occurrences": {
           "Cells": [{
            "CellReference": "string",
            "Column": integer,
            "ColumnName": "string",
            "Row": integer
           }],
           "LineRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "OffsetRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "Pages": [{
            "LineRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "OffsetRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          },
          "Type": "string"
         }],
         "TotalCount": integer
        }],
        "SizeClassified": integer,
        "Status": {
         "Code": "string",
         "Reason": "string"
```

```
        }
       }
      },
      "Details": {
       "AwsAmazonMQBroker": {
        "AutoMinorVersionUpgrade": boolean,
        "BrokerArn": "string",
        "BrokerId": "string",
        "BrokerName": "string",
        "Configuration": {
         "Id": "string",
         "Revision": integer
        },
        "DeploymentMode": "string",
        "EncryptionOptions": {
         "UseAwsOwnedKey": boolean
        },
        "EngineType": "string",
        "EngineVersion": "string",
        "HostInstanceType": "string",
        "Logs": {
         "Audit": boolean,
         "AuditLogGroup": "string",
         "General": boolean,
         "GeneralLogGroup": "string"
        },
        "MaintenanceWindowStartTime": {
         "DayOfWeek": "string",
         "TimeOfDay": "string",
         "TimeZone": "string"
        },
        "PubliclyAccessible": boolean,
        "SecurityGroups": [
         "string"
        ],
        "StorageType": "string",
        "SubnetIds": [
         "string",
         "string"
        ],
        "Users": [{
         "Username": "string"
        }]
       },
```

```
        "AwsApiGatewayRestApi": {
         "ApiKeySource": "string",
         "BinaryMediaTypes": [" string"],
         "CreatedDate": "string",
         "Description": "string",
         "EndpointConfiguration": {
          "Types": ["string"]
         },
         "Id": "string",
         "MinimumCompressionSize": number,
         "Name": "string",
         "Version": "string"
        },
        "AwsApiGatewayStage": {
         "AccessLogSettings": {
          "DestinationArn": "string",
          "Format": "string"
         },
         "CacheClusterEnabled": boolean,
         "CacheClusterSize": "string",
         "CacheClusterStatus": "string",
         "CanarySettings": {
          "DeploymentId": "string",
          "PercentTraffic": number,
          "StageVariableOverrides": [{
           "string": "string"
          }],
          "UseStageCache": boolean
         },
         "ClientCertificateId": "string",
         "CreatedDate": "string",
         "DeploymentId": "string",
         "Description": "string",
         "DocumentationVersion": "string",
         "LastUpdatedDate": "string",
         "MethodSettings": [{
          "CacheDataEncrypted": boolean,
          "CachingEnabled": boolean,
          "CacheTtlInSeconds": number,
          "DataTraceEnabled": boolean,
          "HttpMethod": "string",
          "LoggingLevel": "string",
          "MetricsEnabled": boolean,
          "RequireAuthorizationForCacheControl": boolean,
```

```
          "ResourcePath": "string",
          "ThrottlingBurstLimit": number,
          "ThrottlingRateLimit": number,
          "UnauthorizedCacheControlHeaderStrategy": "string"
         }],
         "StageName": "string",
         "TracingEnabled": boolean,
         "Variables": {
          "string": "string"
         },
         "WebAclArn": "string"
        },
        "AwsApiGatewayV2Api": {
         "ApiEndpoint": "string",
         "ApiId": "string",
         "ApiKeySelectionExpression": "string",
         "CorsConfiguration": {
          "AllowCredentials": boolean,
          "AllowHeaders": ["string"],
          "AllowMethods": ["string"],
          "AllowOrigins": ["string"],
          "ExposeHeaders": ["string"],
          "MaxAge": number
         },
         "CreatedDate": "string",
         "Description": "string",
         "Name": "string",
         "ProtocolType": "string",
         "RouteSelectionExpression": "string",
         "Version": "string"
        },
        "AwsApiGatewayV2Stage": {
         "AccessLogSettings": {
          "DestinationArn": "string",
          "Format": "string"
         },
         "ApiGatewayManaged": boolean,
         "AutoDeploy": boolean,
         "ClientCertificateId": "string",
         "CreatedDate": "string",
         "DefaultRouteSettings": {
          "DataTraceEnabled": boolean,
          "DetailedMetricsEnabled": boolean,
          "LoggingLevel": "string",
```

```
          "ThrottlingBurstLimit": number,
          "ThrottlingRateLimit": number
         },
         "DeploymentId": "string",
         "Description": "string",
         "LastDeploymentStatusMessage": "string",
         "LastUpdatedDate": "string",
         "RouteSettings": {
          "DetailedMetricsEnabled": boolean,
          "LoggingLevel": "string",
          "DataTraceEnabled": boolean,
          "ThrottlingBurstLimit": number,
          "ThrottlingRateLimit": number
         },
         "StageName": "string",
         "StageVariables": [{
          "string": "string"
         }]
        },
        "AwsAppSyncGraphQLApi": {
         "AwsAppSyncGraphQlApi": {
          "AdditionalAuthenticationProviders": [
          {
           "AuthenticationType": "string",
           "LambdaAuthorizerConfig": {
            "AuthorizerResultTtlInSeconds": integer,
            "AuthorizerUri": "string"
           }
          },
          {
           "AuthenticationType": "string"
          }
          ],
          "ApiId": "string",
          "Arn": "string",
          "AuthenticationType": "string",
          "Id": "string",
          "LogConfig": {
           "CloudWatchLogsRoleArn": "string",
           "ExcludeVerboseContent": boolean,
           "FieldLogLevel": "string"
          },
          "Name": "string",
          "XrayEnabled": boolean
```

```
        }
       },
       "AwsAthenaWorkGroup": {
        "Description": "string",
        "Name": "string",
        "WorkgroupConfiguration": {
         "ResultConfiguration": {
          "EncryptionConfiguration": {
           "EncryptionOption": "string",
           "KmsKey": "string"
          }
         }
        },
        "State": "string"
       },
       "AwsAutoScalingAutoScalingGroup": {
        "AvailabilityZones": [{
         "Value": "string"
        }],
        "CreatedTime": "string",
        "HealthCheckGracePeriod": integer,
        "HealthCheckType": "string",
        "LaunchConfigurationName": "string",
        "LoadBalancerNames": ["string"],
        "LaunchTemplate": {
                       "LaunchTemplateId": "string",
                       "LaunchTemplateName": "string",
                       "Version": "string"
                   },
        "MixedInstancesPolicy": {
         "InstancesDistribution": {
          "OnDemandAllocationStrategy": "string",
          "OnDemandBaseCapacity": number,
          "OnDemandPercentageAboveBaseCapacity": number,
          "SpotAllocationStrategy": "string",
          "SpotInstancePools": number,
          "SpotMaxPrice": "string"
         },
         "LaunchTemplate": {
          "LaunchTemplateSpecification": {
           "LaunchTemplateId": "string",
           "LaunchTemplateName": "string",
           "Version": "string"
          },
```

```
          "CapacityRebalance": boolean,
          "Overrides": [{
           "InstanceType": "string",
           "WeightedCapacity": "string"
          }]
         }
        }
       },
       "AwsAutoScalingLaunchConfiguration": {
        "AssociatePublicIpAddress": boolean,
        "BlockDeviceMappings": [{
         "DeviceName": "string",
         "Ebs": {
          "DeleteOnTermination": boolean,
          "Encrypted": boolean,
          "Iops": number,
          "SnapshotId": "string",
          "VolumeSize": number,
          "VolumeType": "string"
         },
         "NoDevice": boolean,
         "VirtualName": "string"
        }],
        "ClassicLinkVpcId": "string",
        "ClassicLinkVpcSecurityGroups": ["string"],
        "CreatedTime": "string",
        "EbsOptimized": boolean,
        "IamInstanceProfile": "string"
       },
       "ImageId": "string",
       "InstanceMonitoring": {
        "Enabled": boolean
       },
       "InstanceType": "string",
       "KernelId": "string",
       "KeyName": "string",
       "LaunchConfigurationName": "string",
       "MetadataOptions": {
        "HttpEndPoint": "string",
        "HttpPutReponseHopLimit": number,
        "HttpTokens": "string"
       },
       "PlacementTenancy": "string",
       "RamdiskId": "string",
```

```
        "SecurityGroups": ["string"],
        "SpotPrice": "string",
        "UserData": "string"
       },
       "AwsBackupBackupPlan": {
        "BackupPlan": {
         "AdvancedBackupSettings": [{
          "BackupOptions": {
           "WindowsVSS":"string"
          },
          "ResourceType":"string"
         }],
         "BackupPlanName": "string",
         "BackupPlanRule": [{
          "CompletionWindowMinutes": integer,
          "CopyActions": [{
           "DestinationBackupVaultArn": "string",
           "Lifecycle": {
            "DeleteAfterDays": integer,
            "MoveToColdStorageAfterDays": integer
           }
          }],
          "Lifecycle": {
           "DeleteAfterDays": integer
          },
          "RuleName": "string",
          "ScheduleExpression": "string",
          "StartWindowMinutes": integer,
          "TargetBackupVault": "string"
         }]
        },
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "VersionId": "string"
      },
       "AwsBackupBackupVault": {
        "AccessPolicy": {
         "Statement": [{
          "Action": ["string"],
          "Effect": "string",
          "Principal": {
           "AWS": "string"
          },
          "Resource": "string"
```

```
        }],
        "Version": "string"
       },
       "BackupVaultArn": "string",
       "BackupVaultName": "string",
       "EncryptionKeyArn": "string",
       "Notifications": {
        "BackupVaultEvents": ["string"],
        "SNSTopicArn": "string"
       }
      },
      "AwsBackupRecoveryPoint": {
       "BackupSizeInBytes": integer,
       "BackupVaultName": "string",
       "BackupVaultArn": "string",
       "CalculatedLifecycle": {
        "DeleteAt": "string",
        "MoveToColdStorageAt": "string"
       },
       "CompletionDate": "string",
       "CreatedBy": {
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "BackupPlanVersion": "string",
        "BackupRuleId": "string"
       },
       "CreationDate": "string",
       "EncryptionKeyArn": "string",
       "IamRoleArn": "string",
       "IsEncrypted": boolean,
       "LastRestoreTime": "string",
       "Lifecycle": {
        "DeleteAfterDays": integer,
        "MoveToColdStorageAfterDays": integer
       },
       "RecoveryPointArn": "string",
       "ResourceArn": "string",
       "ResourceType": "string",
       "SourceBackupVaultArn": "string",
       "Status": "string",
       "StatusMessage": "string",
       "StorageClass": "string"
      },
      "AwsCertificateManagerCertificate": {
```

```
        "CertificateAuthorityArn": "string",
        "CreatedAt": "string",
        "DomainName": "string",
        "DomainValidationOptions": [{
         "DomainName": "string",
         "ResourceRecord": {
          "Name": "string",
          "Type": "string",
          "Value": "string"
         },
         "ValidationDomain": "string",
         "ValidationEmails": ["string"],
         "ValidationMethod": "string",
         "ValidationStatus": "string"
        }],
        "ExtendedKeyUsages": [{
         "Name": "string",
         "OId": "string"
        }],
        "FailureReason": "string",
        "ImportedAt": "string",
        "InUseBy": ["string"],
        "IssuedAt": "string",
        "Issuer": "string",
        "KeyAlgorithm": "string",
        "KeyUsages": [{
         "Name": "string"
        }],
        "NotAfter": "string",
        "NotBefore": "string",
        "Options": {
         "CertificateTransparencyLoggingPreference": "string"
        },
        "RenewalEligibility": "string",
        "RenewalSummary": {
         "DomainValidationOptions": [{
          "DomainName": "string",
          "ResourceRecord": {
           "Name": "string",
           "Type": "string",
           "Value": "string"
          },
          "ValidationDomain": "string",
          "ValidationEmails": ["string"],
```

```
          "ValidationMethod": "string",
          "ValidationStatus": "string"
         }],
         "RenewalStatus": "string",
         "RenewalStatusReason": "string",
         "UpdatedAt": "string"
        },
        "Serial": "string",
        "SignatureAlgorithm": "string",
        "Status": "string",
        "Subject": "string",
        "SubjectAlternativeNames": ["string"],
        "Type": "string"
       },
       "AwsCloudFormationStack": {
        "Capabilities": ["string"],
        "CreationTime": "string",
        "Description": "string",
        "DisableRollback": boolean,
        "DriftInformation": {
         "StackDriftStatus": "string"
        },
        "EnableTerminationProtection": boolean,
        "LastUpdatedTime": "string",
        "NotificationArns": ["string"],
        "Outputs": [{
         "Description": "string",
         "OutputKey": "string",
         "OutputValue": "string"
        }],
        "RoleArn": "string",
        "StackId": "string",
        "StackName": "string",
        "StackStatus": "string",
        "StackStatusReason": "string",
        "TimeoutInMinutes": number
       },
       "AwsCloudFrontDistribution": {
        "CacheBehaviors": {
         "Items": [{
          "ViewerProtocolPolicy": "string"
         }]
        },
        "DefaultCacheBehavior": {
```

```
         "ViewerProtocolPolicy": "string"
        },
        "DefaultRootObject": "string",
        "DomainName": "string",
        "Etag": "string",
        "LastModifiedTime": "string",
        "Logging": {
         "Bucket": "string",
         "Enabled": boolean,
         "IncludeCookies": boolean,
         "Prefix": "string"
        },
        "OriginGroups": {
         "Items": [{
          "FailoverCriteria": {
           "StatusCodes": {
            "Items": [number],
            "Quantity": number
           }
          }
         }]
        },
        "Origins": {
         "Items": [{
          "CustomOriginConfig": {
           "HttpPort": number,
           "HttpsPort": number,
           "OriginKeepaliveTimeout": number,
           "OriginProtocolPolicy": "string",
           "OriginReadTimeout": number,
           "OriginSslProtocols": {
            "Items": ["string"],
            "Quantity": number
           }
          },
          "DomainName": "string",
          "Id": "string",
          "OriginPath": "string",
          "S3OriginConfig": {
           "OriginAccessIdentity": "string"
          }
         }]
        },
        "Status": "string",
```

```
        "ViewerCertificate": {
         "AcmCertificateArn": "string",
         "Certificate": "string",
         "CertificateSource": "string",
         "CloudFrontDefaultCertificate": boolean,
         "IamCertificateId": "string",
         "MinimumProtocolVersion": "string",
         "SslSupportMethod": "string"
        },
        "WebAclId": "string"
       },
       "AwsCloudTrailTrail": {
        "CloudWatchLogsLogGroupArn": "string",
        "CloudWatchLogsRoleArn": "string",
        "HasCustomEventSelectors": boolean,
        "HomeRegion": "string",
        "IncludeGlobalServiceEvents": boolean,
        "IsMultiRegionTrail": boolean,
        "IsOrganizationTrail": boolean,
        "KmsKeyId": "string",
        "LogFileValidationEnabled": boolean,
        "Name": "string",
        "S3BucketName": "string",
        "S3KeyPrefix": "string",
        "SnsTopicArn": "string",
        "SnsTopicName": "string",
        "TrailArn": "string"
       },
       "AwsCloudWatchAlarm": {
        "ActionsEnabled": boolean,
        "AlarmActions": ["string"],
        "AlarmArn": "string",
        "AlarmConfigurationUpdatedTimestamp": "string",
        "AlarmDescription": "string",
        "AlarmName": "string",
        "ComparisonOperator": "string",
        "DatapointsToAlarm": number,
        "Dimensions": [{
         "Name": "string",
         "Value": "string"
        }],
        "EvaluateLowSampleCountPercentile": "string",
        "EvaluationPeriods": number,
        "ExtendedStatistic": "string",
```

```
        "InsufficientDataActions": ["string"],
        "MetricName": "string",
        "Namespace": "string",
        "OkActions": ["string"],
        "Period": number,
        "Statistic": "string",
        "Threshold": number,
        "ThresholdMetricId": "string",
        "TreatMissingData": "string",
        "Unit": "string"
      },
      "AwsCodeBuildProject": {
        "Artifacts": [{
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
        }],
        "SecondaryArtifacts": [{
                    "ArtifactIdentifier": "string",
                    "Type": "string",
                    "Location": "string",
                    "Name": "string",
                    "NamespaceType": "string",
                    "Packaging": "string",
                    "Path": "string",
                    "EncryptionDisabled": boolean,
                    "OverrideArtifactName": boolean
                }],
        "EncryptionKey": "string",
        "Certificate": "string",
        "Environment": {
          "Certificate": "string",
          "EnvironmentVariables": [{
            "Name": "string",
            "Type": "string",
            "Value": "string"
          }],
          "ImagePullCredentialsType": "string",
```

```
        "PrivilegedMode": boolean,
        "RegistryCredential": {
         "Credential": "string",
         "CredentialProvider": "string"
        },
        "Type": "string"
       },
       "LogsConfig": {
        "CloudWatchLogs": {
         "GroupName": "string",
         "Status": "string",
         "StreamName": "string"
        },
        "S3Logs": {
         "EncryptionDisabled": boolean,
         "Location": "string",
         "Status": "string"
        }
       },
       "Name": "string",
       "ServiceRole": "string",
       "Source": {
        "Type": "string",
        "Location": "string",
        "GitCloneDepth": integer
       },
       "VpcConfig": {
        "VpcId": "string",
        "Subnets": ["string"],
        "SecurityGroupIds": ["string"]
       }
      },
      "AwsDmsEndpoint": {
       "CertificateArn": "string",
       "DatabaseName": "string",
       "EndpointArn": "string",
       "EndpointIdentifier": "string",
       "EndpointType": "string",
       "EngineName": "string",
       "KmsKeyId": "string",
       "Port": integer,
       "ServerName": "string",
       "SslMode": "string",
       "Username": "string"
```

```
      },
      "AwsDmsReplicationInstance": {
       "AllocatedStorage": integer,
       "AutoMinorVersionUpgrade": boolean,
       "AvailabilityZone": "string",
       "EngineVersion": "string",
       "KmsKeyId": "string",
       "MultiAZ": boolean,
       "PreferredMaintenanceWindow": "string",
       "PubliclyAccessible": boolean,
       "ReplicationInstanceClass": "string",
       "ReplicationInstanceIdentifier": "string",
       "ReplicationSubnetGroup": {
           "ReplicationSubnetGroupIdentifier": "string"
       },
       "VpcSecurityGroups": [
           {
               "VpcSecurityGroupId": "string"
           }
       ]
      },
      "AwsDmsReplicationTask": {
       "CdcStartPosition": "string",
       "Id": "string",
       "MigrationType": "string",
       "ReplicationInstanceArn": "string",
       "ReplicationTaskIdentifier": "string",
       "ReplicationTaskSettings": {
        "string": "string"
       },
       "SourceEndpointArn": "string",
       "TableMappings": {
        "string": "string"
       },
       "TargetEndpointArn": "string"
      },
      "AwsDynamoDbTable": {
       "AttributeDefinitions": [{
        "AttributeName": "string",
        "AttributeType": "string"
       }],
       "BillingModeSummary": {
        "BillingMode": "string",
        "LastUpdateToPayPerRequestDateTime": "string"
```

```
        },
        "CreationDateTime": "string",
        "DeletionProtectionEnabled": boolean,
        "GlobalSecondaryIndexes": [{
         "Backfilling": boolean,
         "IndexArn": "string",
         "IndexName": "string",
         "IndexSizeBytes": number,
         "IndexStatus": "string",
         "ItemCount": number,
         "KeySchema": [{
          "AttributeName": "string",
          "KeyType": "string"
         }],
         "Projection": {
          "NonKeyAttributes": ["string"],
          "ProjectionType": "string"
         },
         "ProvisionedThroughput": {
          "LastDecreaseDateTime": "string",
          "LastIncreaseDateTime": "string",
          "NumberOfDecreasesToday": number,
          "ReadCapacityUnits": number,
          "WriteCapacityUnits": number
         }
        }],
        "GlobalTableVersion": "string",
        "ItemCount": number,
        "KeySchema": [{
         "AttributeName": "string",
         "KeyType": "string"
        }],
        "LatestStreamArn": "string",
        "LatestStreamLabel": "string",
        "LocalSecondaryIndexes": [{
         "IndexArn": "string",
         "IndexName": "string",
         "KeySchema": [{
          "AttributeName": "string",
          "KeyType": "string"
         }],
         "Projection": {
          "NonKeyAttributes": ["string"],
          "ProjectionType": "string"
```

```
        }
       }],
       "ProvisionedThroughput": {
        "LastDecreaseDateTime": "string",
        "LastIncreaseDateTime": "string",
        "NumberOfDecreasesToday": number,
        "ReadCapacityUnits": number,
        "WriteCapacityUnits": number
       },
       "Replicas": [{
        "GlobalSecondaryIndexes": [{
         "IndexName": "string",
         "ProvisionedThroughputOverride": {
          "ReadCapacityUnits": number
         }
        }],
        "KmsMasterKeyId": "string",
        "ProvisionedThroughputOverride": {
         "ReadCapacityUnits": number
        },
        "RegionName": "string",
        "ReplicaStatus": "string",
        "ReplicaStatusDescription": "string"
       }],
       "RestoreSummary": {
        "RestoreDateTime": "string",
        "RestoreInProgress": boolean,
        "SourceBackupArn": "string",
        "SourceTableArn": "string"
       },
       "SseDescription": {
        "InaccessibleEncryptionDateTime": "string",
        "KmsMasterKeyArn": "string",
        "SseType": "string",
        "Status": "string"
       },
       "StreamSpecification": {
        "StreamEnabled": boolean,
        "StreamViewType": "string"
       },
       "TableId": "string",
       "TableName": "string",
       "TableSizeBytes": number,
       "TableStatus": "string"
```

```
      },
      "AwsEc2ClientVpnEndpoint": {
       "AuthenticationOptions": [
        {
         "MutualAuthentication": {
          "ClientRootCertificateChainArn": "string"
         },
         "Type": "string"
        }
       ],
       "ClientCidrBlock": "string",
       "ClientConnectOptions": {
        "Enabled": boolean
       },
       "ClientLoginBannerOptions": {
        "Enabled": boolean
       },
       "ClientVpnEndpointId": "string",
       "ConnectionLogOptions": {
        "Enabled": boolean
       },
       "Description": "string",
       "DnsServer": ["string"],
       "ServerCertificateArn": "string",
       "SecurityGroupIdSet": [
        "string"
       ],
       "SelfServicePortalUrl": "string",
       "SessionTimeoutHours": "integer",
       "SplitTunnel": boolean,
       "TransportProtocol": "string",
       "VpcId": "string",
       "VpnPort": integer
      },
      "AwsEc2Eip": {
       "AllocationId": "string",
       "AssociationId": "string",
       "Domain": "string",
       "InstanceId": "string",
       "NetworkBorderGroup": "string",
       "NetworkInterfaceId": "string",
       "NetworkInterfaceOwnerId": "string",
       "PrivateIpAddress": "string",
       "PublicIp": "string",
```

```
        "PublicIpv4Pool": "string"
      },
      "AwsEc2Instance": {
       "IamInstanceProfileArn": "string",
       "ImageId": "string",
       "IpV4Addresses": ["string"],
       "IpV6Addresses": ["string"],
       "KeyName": "string",
       "LaunchedAt": "string",
       "MetadataOptions": {
        "HttpEndpoint": "string",
        "HttpProtocolIpv6": "string",
        "HttpPutResponseHopLimit": number,
        "HttpTokens": "string",
        "InstanceMetadataTags": "string"
       },
       "Monitoring": {
        "State": "string"
       },
       "NetworkInterfaces": [{
        "NetworkInterfaceId": "string"
       }],
       "SubnetId": "string",
       "Type": "string",
       "VirtualizationType": "string",
       "VpcId": "string"
      },
      "AwsEc2LaunchTemplate": {
       "DefaultVersionNumber": "string",
       "ElasticGpuSpecifications": ["string"],
       "ElasticInferenceAccelerators": ["string"],
       "Id": "string",
       "ImageId": "string",
       "LatestVersionNumber": "string",
       "LaunchTemplateData": {
        "BlockDeviceMappings": [{
         "DeviceName": "string",
         "Ebs": {
          "DeleteonTermination": boolean,
          "Encrypted": boolean,
          "SnapshotId": "string",
          "VolumeSize": number,
          "VolumeType": "string"
         }
```

```
        }],
        "MetadataOptions": {
         "HttpTokens": "string",
         "HttpPutResponseHopLimit" : number
        },
        "Monitoring": {
         "Enabled": boolean
        },
        "NetworkInterfaces": [{
         "AssociatePublicIpAddress" : boolean
        }]
       },
       "LaunchTemplateName": "string",
       "LicenseSpecifications": ["string"],
       "SecurityGroupIds": ["string"],
       "SecurityGroups": ["string"],
       "TagSpecifications": ["string"]
      },
      "AwsEc2NetworkAcl": {
       "Associations": [{
        "NetworkAclAssociationId": "string",
        "NetworkAclId": "string",
        "SubnetId": "string"
       }],
       "Entries": [{
        "CidrBlock": "string",
        "Egress": boolean,
        "IcmpTypeCode": {
         "Code": number,
         "Type": number
        },
        "Ipv6CidrBlock": "string",
        "PortRange": {
         "From": number,
         "To": number
        },
        "Protocol": "string",
        "RuleAction": "string",
        "RuleNumber": number
       }],
       "IsDefault": boolean,
       "NetworkAclId": "string",
       "OwnerId": "string",
       "VpcId": "string"
```

```
      },
      "AwsEc2NetworkInterface": {
       "Attachment": {
        "AttachmentId": "string",
        "AttachTime": "string",
        "DeleteOnTermination": boolean,
        "DeviceIndex": number,
        "InstanceId": "string",
        "InstanceOwnerId": "string",
        "Status": "string"
       },
       "Ipv6Addresses": [{
        "Ipv6Address": "string"
       }],
       "NetworkInterfaceId": "string",
       "PrivateIpAddresses": [{
        "PrivateDnsName": "string",
        "PrivateIpAddress": "string"
       }],
       "PublicDnsName": "string",
       "PublicIp": "string",
       "SecurityGroups": [{
        "GroupId": "string",
        "GroupName": "string"
       }],
       "SourceDestCheck": boolean
      },
      "AwsEc2RouteTable": {
       "AssociationSet": [{
        "AssociationState": {
         "State": "string"
        },
        "Main": boolean,
        "RouteTableAssociationId": "string",
        "RouteTableId": "string"
       }],
       "PropogatingVgwSet": [],
       "RouteTableId": "string",
       "RouteSet": [
        {
         "DestinationCidrBlock": "string",
         "GatewayId": "string",
         "Origin": "string",
         "State": "string"
```

```
        },
        {
         "DestinationCidrBlock": "string",
         "GatewayId": "string",
         "Origin": "string",
         "State": "string"
        }
       ],
       "VpcId": "string"
      },
      "AwsEc2SecurityGroup": {
       "GroupId": "string",
       "GroupName": "string",
       "IpPermissions": [{
        "FromPort": number,
        "IpProtocol": "string",
        "IpRanges": [{
         "CidrIp": "string"
        }],
        "Ipv6Ranges": [{
         "CidrIpv6": "string"
        }],
        "PrefixListIds": [{
         "PrefixListId": "string"
        }],
        "ToPort": number,
        "UserIdGroupPairs": [{
         "GroupId": "string",
         "GroupName": "string",
         "PeeringStatus": "string",
         "UserId": "string",
         "VpcId": "string",
         "VpcPeeringConnectionId": "string"
        }]
       }],
       "IpPermissionsEgress": [{
        "FromPort": number,
        "IpProtocol": "string",
        "IpRanges": [{
         "CidrIp": "string"
        }],
        "Ipv6Ranges": [{
         "CidrIpv6": "string"
        }],
```

```
        "PrefixListIds": [{
         "PrefixListId": "string"
        }],
        "ToPort": number,
        "UserIdGroupPairs": [{
         "GroupId": "string",
         "GroupName": "string",
         "PeeringStatus": "string",
         "UserId": "string",
         "VpcId": "string",
         "VpcPeeringConnectionId": "string"
        }]
       }],
       "OwnerId": "string",
       "VpcId": "string"
      },
      "AwsEc2Subnet": {
       "AssignIpv6AddressOnCreation": boolean,
       "AvailabilityZone": "string",
       "AvailabilityZoneId": "string",
       "AvailableIpAddressCount": number,
       "CidrBlock": "string",
       "DefaultForAz": boolean,
       "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "string",
        "Ipv6CidrBlock": "string",
        "CidrBlockState": "string"
       }],
       "MapPublicIpOnLaunch": boolean,
       "OwnerId": "string",
       "State": "string",
       "SubnetArn": "string",
       "SubnetId": "string",
       "VpcId": "string"
      },
      "AwsEc2TransitGateway": {
       "AmazonSideAsn": number,
       "AssociationDefaultRouteTableId": "string",
       "AutoAcceptSharedAttachments": "string",
       "DefaultRouteTableAssociation": "string",
       "DefaultRouteTablePropagation": "string",
       "Description": "string",
       "DnsSupport": "string",
       "Id": "string",
```

```
        "MulticastSupport": "string",
        "PropagationDefaultRouteTableId": "string",
        "TransitGatewayCidrBlocks": ["string"],
        "VpnEcmpSupport": "string"
      },
      "AwsEc2Volume": {
        "Attachments": [{
          "AttachTime": "string",
          "DeleteOnTermination": boolean,
          "InstanceId": "string",
          "Status": "string"
        }],
        "CreateTime": "string",
        "DeviceName": "string",
        "Encrypted": boolean,
        "KmsKeyId": "string",
        "Size": number,
        "SnapshotId": "string",
        "Status": "string",
        "VolumeId": "string",
        "VolumeScanStatus": "string",
        "VolumeType": "string"
      },
      "AwsEc2Vpc": {
        "CidrBlockAssociationSet": [{
          "AssociationId": "string",
          "CidrBlock": "string",
          "CidrBlockState": "string"
        }],
        "DhcpOptionsId": "string",
        "Ipv6CidrBlockAssociationSet": [{
          "AssociationId": "string",
          "CidrBlockState": "string",
          "Ipv6CidrBlock": "string"
        }],
        "State": "string"
      },
      "AwsEc2VpcEndpointService": {
        "AcceptanceRequired": boolean,
        "AvailabilityZones": ["string"],
        "BaseEndpointDnsNames": ["string"],
        "ManagesVpcEndpoints": boolean,
        "GatewayLoadBalancerArns": ["string"],
        "NetworkLoadBalancerArns": ["string"],
```

```
        "PrivateDnsName": "string",
        "ServiceId": "string",
        "ServiceName": "string",
        "ServiceState": "string",
        "ServiceType": [{
         "ServiceType": "string"
        }]
       },
       "AwsEc2VpcPeeringConnection": {
        "AccepterVpcInfo": {
         "CidrBlock": "string",
         "CidrBlockSet": [{
          "CidrBlock": "string"
         }],
         "Ipv6CidrBlockSet": [{
          "Ipv6CidrBlock": "string"
         }],
         "OwnerId": "string",
         "PeeringOptions": {
          "AllowDnsResolutionFromRemoteVpc": boolean,
          "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
          "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
         },
         "Region": "string",
         "VpcId": "string"
        },
        "ExpirationTime": "string",
        "RequesterVpcInfo": {
         "CidrBlock": "string",
         "CidrBlockSet": [{
          "CidrBlock": "string"
         }],
         "Ipv6CidrBlockSet": [{
          "Ipv6CidrBlock": "string"
         }],
         "OwnerId": "string",
         "PeeringOptions": {
          "AllowDnsResolutionFromRemoteVpc": boolean,
          "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
          "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
         },
         "Region": "string",
         "VpcId": "string"
        },
```

```
        "Status": {
         "Code": "string",
         "Message": "string"
        },
        "VpcPeeringConnectionId": "string"
       },
       "AwsEc2VpnConnection": {
        "Category": "string",
        "CustomerGatewayConfiguration": "string",
        "CustomerGatewayId": "string",
        "Options": {
         "StaticRoutesOnly": boolean,
         "TunnelOptions": [{
          "DpdTimeoutSeconds": number,
          "IkeVersions": ["string"],
          "OutsideIpAddress": "string",
          "Phase1DhGroupNumbers": [number],
          "Phase1EncryptionAlgorithms": ["string"],
          "Phase1IntegrityAlgorithms": ["string"],
          "Phase1LifetimeSeconds": number,
          "Phase2DhGroupNumbers": [number],
          "Phase2EncryptionAlgorithms": ["string"],
          "Phase2IntegrityAlgorithms": ["string"],
          "Phase2LifetimeSeconds": number,
          "PreSharedKey": "string",
          "RekeyFuzzPercentage": number,
          "RekeyMarginTimeSeconds": number,
          "ReplayWindowSize": number,
          "TunnelInsideCidr": "string"
         }]
        },
        "Routes": [{
         "DestinationCidrBlock": "string",
         "State": "string"
        }],
        "State": "string",
        "TransitGatewayId": "string",
        "Type": "string",
        "VgwTelemetry": [{
         "AcceptedRouteCount": number,
         "CertificateArn": "string",
         "LastStatusChange": "string",
         "OutsideIpAddress": "string",
         "Status": "string",
```

```
        "StatusMessage": "string"
       }],
       "VpnConnectionId": "string",
       "VpnGatewayId": "string"
      },
      "AwsEcrContainerImage": {
       "Architecture": "string",
       "ImageDigest": "string",
       "ImagePublishedAt": "string",
       "ImageTags": ["string"],
       "RegistryId": "string",
       "RepositoryName": "string"
      },
      "AwsEcrRepository": {
       "Arn": "string",
       "ImageScanningConfiguration": {
        "ScanOnPush": boolean
       },
       "ImageTagMutability": "string",
       "LifecyclePolicy": {
        "LifecyclePolicyText": "string",
        "RegistryId": "string"
       },
       "RepositoryName": "string",
       "RepositoryPolicyText": "string"
      },
      "AwsEcsCluster": {
       "ActiveServicesCount": number,
       "CapacityProviders": ["string"],
       "ClusterArn": "string",
       "ClusterName": "string",
       "ClusterSettings": [{
        "Name": "string",
        "Value": "string"
       }],
       "Configuration": {
        "ExecuteCommandConfiguration": {
         "KmsKeyId": "string",
         "LogConfiguration": {
          "CloudWatchEncryptionEnabled": boolean,
          "CloudWatchLogGroupName": "string",
          "S3BucketName": "string",
          "S3EncryptionEnabled": boolean,
          "S3KeyPrefix": "string"
```

```
          },
          "Logging": "string"
         }
        },
        "DefaultCapacityProviderStrategy": [{
         "Base": number,
         "CapacityProvider": "string",
         "Weight": number
        }],
        "RegisteredContainerInstancesCount": number,
        "RunningTasksCount": number,
        "Status": "string"
       },
       "AwsEcsContainer": {
        "Image": "string",
        "MountPoints": [{
         "ContainerPath": "string",
         "SourceVolume": "string"
        }],
        "Name": "string",
        "Privileged": boolean
       },
       "AwsEcsService": {
        "CapacityProviderStrategy": [{
         "Base": number,
         "CapacityProvider": "string",
         "Weight": number
        }],
        "Cluster": "string",
        "DeploymentConfiguration": {
         "DeploymentCircuitBreaker": {
          "Enable": boolean,
          "Rollback": boolean
         },
         "MaximumPercent": number,
         "MinimumHealthyPercent": number
        },
        "DeploymentController": {
         "Type": "string"
        },
        "DesiredCount": number,
        "EnableEcsManagedTags": boolean,
        "EnableExecuteCommand": boolean,
        "HealthCheckGracePeriodSeconds": number,
```

```
        "LaunchType": "string",
        "LoadBalancers": [{
         "ContainerName": "string",
         "ContainerPort": number,
         "LoadBalancerName": "string",
         "TargetGroupArn": "string"
        }],
        "Name": "string",
        "NetworkConfiguration": {
         "AwsVpcConfiguration": {
          "AssignPublicIp": "string",
          "SecurityGroups": ["string"],
          "Subnets": ["string"]
         }
        },
        "PlacementConstraints": [{
         "Expression": "string",
         "Type": "string"
        }],
        "PlacementStrategies": [{
         "Field": "string",
         "Type": "string"
        }],
        "PlatformVersion": "string",
        "PropagateTags": "string",
        "Role": "string",
        "SchedulingStrategy": "string",
        "ServiceArn": "string",
        "ServiceName": "string",
        "ServiceRegistries": [{
         "ContainerName": "string",
         "ContainerPort": number,
         "Port": number,
         "RegistryArn": "string"
        }],
        "TaskDefinition": "string"
       },
       "AwsEcsTask": {
        "CreatedAt": "string",
        "ClusterArn": "string",
        "Group": "string",
        "StartedAt": "string",
        "StartedBy": "string",
        "TaskDefinitionArn": "string",
```

```
        "Version": number,
        "Volumes": [{
         "Name": "string",
         "Host": {
          "SourcePath": "string"
         }
        }],
        "Containers": [{
         "Image": "string",
         "MountPoints": [{
          "ContainerPath": "string",
          "SourceVolume": "string"
         }],
         "Name": "string",
         "Privileged": boolean
        }]
       },
       "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [{
         "Command": ["string"],
         "Cpu": number,
         "DependsOn": [{
          "Condition": "string",
          "ContainerName": "string"
         }],
         "DisableNetworking": boolean,
         "DnsSearchDomains": ["string"],
         "DnsServers": ["string"],
         "DockerLabels": {
          "string": "string"
         },
         "DockerSecurityOptions": ["string"],
         "EntryPoint": ["string"],
         "Environment": [{
          "Name": "string",
          "Value": "string"
         }],
         "EnvironmentFiles": [{
          "Type": "string",
          "Value": "string"
         }],
         "Essential": boolean,
         "ExtraHosts": [{
          "Hostname": "string",
```

```
          "IpAddress": "string"
        }],
        "FirelensConfiguration": {
         "Options": {
          "string": "string"
         },
         "Type": "string"
        },
        "HealthCheck": {
         "Command": ["string"],
         "Interval": number,
         "Retries": number,
         "StartPeriod": number,
         "Timeout": number
        },
        "Hostname": "string",
        "Image": "string",
        "Interactive": boolean,
        "Links": ["string"],
        "LinuxParameters": {
         "Capabilities": {
          "Add": ["string"],
          "Drop": ["string"]
         },
         "Devices": [{
          "ContainerPath": "string",
          "HostPath": "string",
          "Permissions": ["string"]
         }],
         "InitProcessEnabled": boolean,
         "MaxSwap": number,
         "SharedMemorySize": number,
         "Swappiness": number,
         "Tmpfs": [{
          "ContainerPath": "string",
          "MountOptions": ["string"],
          "Size": number
         }]
        },
        "LogConfiguration": {
         "LogDriver": "string",
         "Options": {
          "string": "string"
         },
```

```
          "SecretOptions": [{
           "Name": "string",
           "ValueFrom": "string"
          }]
         },
         "Memory": number,
         "MemoryReservation": number,
         "MountPoints": [{
          "ContainerPath": "string",
          "ReadOnly": boolean,
          "SourceVolume": "string"
         }],
         "Name": "string",
         "PortMappings": [{
          "ContainerPort": number,
          "HostPort": number,
          "Protocol": "string"
         }],
         "Privileged": boolean,
         "PseudoTerminal": boolean,
         "ReadonlyRootFilesystem": boolean,
         "RepositoryCredentials": {
          "CredentialsParameter": "string"
         },
         "ResourceRequirements": [{
          "Type": "string",
          "Value": "string"
         }],
         "Secrets": [{
          "Name": "string",
          "ValueFrom": "string"
         }],
         "StartTimeout": number,
         "StopTimeout": number,
         "SystemControls": [{
          "Namespace": "string",
          "Value": "string"
         }],
         "Ulimits": [{
          "HardLimit": number,
          "Name": "string",
          "SoftLimit": number
         }],
         "User": "string",
```

```
        "VolumesFrom": [{
         "ReadOnly": boolean,
         "SourceContainer": "string"
        }],
        "WorkingDirectory": "string"
       }],
       "Cpu": "string",
       "ExecutionRoleArn": "string",
       "Family": "string",
       "InferenceAccelerators": [{
        "DeviceName": "string",
        "DeviceType": "string"
       }],
       "IpcMode": "string",
       "Memory": "string",
       "NetworkMode": "string",
       "PidMode": "string",
       "PlacementConstraints": [{
        "Expression": "string",
        "Type": "string"
       }],
       "ProxyConfiguration": {
        "ContainerName": "string",
        "ProxyConfigurationProperties": [{
         "Name": "string",
         "Value": "string"
        }],
        "Type": "string"
       },
       "RequiresCompatibilities": ["string"],
       "Status": "string",
       "TaskRoleArn": "string",
       "Volumes": [{
        "DockerVolumeConfiguration": {
         "Autoprovision": boolean,
         "Driver": "string",
         "DriverOpts": {
          "string": "string"
         },
         "Labels": {
          "string": "string"
         },
         "Scope": "string"
        },
```

```
        "EfsVolumeConfiguration": {
         "AuthorizationConfig": {
          "AccessPointId": "string",
          "Iam": "string"
         },
         "FilesystemId": "string",
         "RootDirectory": "string",
         "TransitEncryption": "string",
         "TransitEncryptionPort": number
        },
        "Host": {
         "SourcePath": "string"
        },
        "Name": "string"
       }]
      },
      "AwsEfsAccessPoint": {
       "AccessPointId": "string",
       "Arn": "string",
       "ClientToken": "string",
       "FileSystemId": "string",
       "PosixUser": {
        "Gid": "string",
        "SecondaryGids": ["string"],
        "Uid": "string"
       },
       "RootDirectory": {
        "CreationInfo": {
         "OwnerGid": "string",
         "OwnerUid": "string",
         "Permissions": "string"
        },
        "Path": "string"
       }
      },
      "AwsEksCluster": {
       "Arn": "string",
       "CertificateAuthorityData": "string",
       "ClusterStatus": "string",
       "Endpoint": "string",
       "Logging": {
        "ClusterLogging": [{
         "Enabled": boolean,
         "Types": ["string"]
```

```
        }]
       },
       "Name": "string",
       "ResourcesVpcConfig": {
        "EndpointPublicAccess": boolean,
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       },
       "RoleArn": "string",
       "Version": "string"
      },
      "AwsElasticBeanstalkEnvironment": {
       "ApplicationName": "string",
       "Cname": "string",
       "DateCreated": "string",
       "DateUpdated": "string",
       "Description": "string",
       "EndpointUrl": "string",
       "EnvironmentArn": "string",
       "EnvironmentId": "string",
       "EnvironmentLinks": [{
        "EnvironmentName": "string",
        "LinkName": "string"
       }],
       "EnvironmentName": "string",
       "OptionSettings": [{
        "Namespace": "string",
        "OptionName": "string",
        "ResourceName": "string",
        "Value": "string"
       }],
       "PlatformArn": "string",
       "SolutionStackName": "string",
       "Status": "string",
       "Tier": {
        "Name": "string",
        "Type": "string",
        "Version": "string"
       },
       "VersionLabel": "string"
      },
      "AwsElasticSearchDomain": {
       "AccessPolicies": "string",
       "DomainStatus": {
```

```
        "DomainId": "string",
        "DomainName": "string",
        "Endpoint": "string",
        "Endpoints": {
         "string": "string"
        }
       },
       "DomainEndpointOptions": {
        "EnforceHTTPS": boolean,
        "TLSSecurityPolicy": "string"
       },
       "ElasticsearchClusterConfig": {
        "DedicatedMasterCount": number,
        "DedicatedMasterEnabled": boolean,
        "DedicatedMasterType": "string",
        "InstanceCount": number,
        "InstanceType": "string",
        "ZoneAwarenessConfig": {
         "AvailabilityZoneCount": number
        },
        "ZoneAwarenessEnabled": boolean
       },
       "ElasticsearchVersion": "string",
       "EncryptionAtRestOptions": {
        "Enabled": boolean,
        "KmsKeyId": "string"
       },
       "LogPublishingOptions": {
        "AuditLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        },
        "IndexSlowLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        },
        "SearchSlowLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        }
       },
       "NodeToNodeEncryptionOptions": {
        "Enabled": boolean
       },
```

```
        "ServiceSoftwareOptions": {
         "AutomatedUpdateDate": "string",
         "Cancellable": boolean,
         "CurrentVersion": "string",
         "Description": "string",
         "NewVersion": "string",
         "UpdateAvailable": boolean,
         "UpdateStatus": "string"
        },
        "VPCOptions": {
         "AvailabilityZones": [
          "string"
         ],
         "SecurityGroupIds": [
          "string"
         ],
         "SubnetIds": [
          "string"
         ],
         "VPCId": "string"
        }
       },
       "AwsElbLoadBalancer": {
        "AvailabilityZones": ["string"],
        "BackendServerDescriptions": [{
         "InstancePort": number,
         "PolicyNames": ["string"]
        }],
        "CanonicalHostedZoneName": "string",
        "CanonicalHostedZoneNameID": "string",
        "CreatedTime": "string",
        "DnsName": "string",
        "HealthCheck": {
         "HealthyThreshold": number,
         "Interval": number,
         "Target": "string",
         "Timeout": number,
         "UnhealthyThreshold": number
        },
        "Instances": [{
         "InstanceId": "string"
        }],
        "ListenerDescriptions": [{
         "Listener": {
```

```
          "InstancePort": number,
          "InstanceProtocol": "string",
          "LoadBalancerPort": number,
          "Protocol": "string",
          "SslCertificateId": "string"
         },
         "PolicyNames": ["string"]
        }],
        "LoadBalancerAttributes": {
         "AccessLog": {
          "EmitInterval": number,
          "Enabled": boolean,
          "S3BucketName": "string",
          "S3BucketPrefix": "string"
         },
         "ConnectionDraining": {
          "Enabled": boolean,
          "Timeout": number
         },
         "ConnectionSettings": {
          "IdleTimeout": number
         },
         "CrossZoneLoadBalancing": {
          "Enabled": boolean
         },
         "AdditionalAttributes": [{
                         "Key": "string",
                         "Value": "string"
                     }]
        },
        "LoadBalancerName": "string",
        "Policies": {
         "AppCookieStickinessPolicies": [{
          "CookieName": "string",
          "PolicyName": "string"
         }],
         "LbCookieStickinessPolicies": [{
          "CookieExpirationPeriod": number,
          "PolicyName": "string"
         }],
         "OtherPolicies": ["string"]
        },
        "Scheme": "string",
        "SecurityGroups": ["string"],
```

```
        "SourceSecurityGroup": {
         "GroupName": "string",
         "OwnerAlias": "string"
        },
        "Subnets": ["string"],
        "VpcId": "string"
       },
       "AwsElbv2LoadBalancer": {
        "AvailabilityZones": {
         "SubnetId": "string",
         "ZoneName": "string"
        },
        "CanonicalHostedZoneId": "string",
        "CreatedTime": "string",
        "DNSName": "string",
        "IpAddressType": "string",
        "LoadBalancerAttributes": [{
         "Key": "string",
         "Value": "string"
        }],
        "Scheme": "string",
        "SecurityGroups": ["string"],
        "State": {
         "Code": "string",
         "Reason": "string"
        },
        "Type": "string",
        "VpcId": "string"
       },
       "AwsEventSchemasRegistry": {
        "Description": "string",
        "RegistryArn": "string",
        "RegistryName": "string"
       },
       "AwsEventsEndpoint": {
        "Arn": "string",
        "Description": "string",
        "EndpointId": "string",
        "EndpointUrl": "string",
        "EventBuses": [
            {
                "EventBusArn": "string"
            },
            {
```

```
                "EventBusArn": "string"
            }
        ],
        "Name": "string",
        "ReplicationConfig": {
            "State": "string"
        },
        "RoleArn": "string",
        "RoutingConfig": {
            "FailoverConfig": {
                "Primary": {
                    "HealthCheck": "string"
                },
                "Secondary": {
                    "Route": "string"
                }
            }
        },
        "State": "string"
      },
      "AwsEventsEventBus": {
        "Arn": "string",
        "Name": "string",
        "Policy": "string"
      },
      "AwsGuardDutyDetector": {
        "FindingPublishingFrequency": "string",
        "ServiceRole": "string",
        "Status": "string",
        "DataSources": {
          "CloudTrail": {
            "Status": "string"
          },
          "DnsLogs": {
            "Status": "string"
          },
          "FlowLogs": {
            "Status": "string"
          },
          "S3Logs": {
            "Status": "string"
          },
          "Kubernetes": {
            "AuditLogs": {
```

```
          "Status": "string"
         }
        },
        "MalwareProtection": {
         "ScanEc2InstanceWithFindings": {
          "EbsVolumes": {
           "Status": "string"
          }
         },
         "ServiceRole": "string"
        }
       }
      },
      "AwsIamAccessKey": {
       "AccessKeyId": "string",
       "AccountId": "string",
       "CreatedAt": "string",
       "PrincipalId": "string",
       "PrincipalName": "string",
       "PrincipalType": "string",
       "SessionContext": {
        "Attributes": {
         "CreationDate": "string",
         "MfaAuthenticated": boolean
        },
        "SessionIssuer": {
         "AccountId": "string",
         "Arn": "string",
         "PrincipalId": "string",
         "Type": "string",
         "UserName": "string"
        }
       },
       "Status": "string"
      },
      "AwsIamGroup": {
       "AttachedManagedPolicies": [{
        "PolicyArn": "string",
        "PolicyName": "string"
       }],
       "CreateDate": "string",
       "GroupId": "string",
       "GroupName": "string",
       "GroupPolicyList": [{
```

```
        "PolicyName": "string"
       }],
       "Path": "string"
      },
      "AwsIamPolicy": {
       "AttachmentCount": number,
       "CreateDate": "string",
       "DefaultVersionId": "string",
       "Description": "string",
       "IsAttachable": boolean,
       "Path": "string",
       "PermissionsBoundaryUsageCount": number,
       "PolicyId": "string",
       "PolicyName": "string",
       "PolicyVersionList": [{
        "CreateDate": "string",
        "IsDefaultVersion": boolean,
        "VersionId": "string"
       }],
       "UpdateDate": "string"
      },
      "AwsIamRole": {
       "AssumeRolePolicyDocument": "string",
       "AttachedManagedPolicies": [{
        "PolicyArn": "string",
        "PolicyName": "string"
       }],
       "CreateDate": "string",
       "InstanceProfileList": [{
        "Arn": "string",
        "CreateDate": "string",
        "InstanceProfileId": "string",
        "InstanceProfileName": "string",
        "Path": "string",
        "Roles": [{
         "Arn": "string",
         "AssumeRolePolicyDocument": "string",
         "CreateDate": "string",
         "Path": "string",
         "RoleId": "string",
         "RoleName": "string"
        }]
       }],
       "MaxSessionDuration": number,
```

```
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
        },
        "RoleId": "string",
        "RoleName": "string",
        "RolePolicyList": [{
         "PolicyName": "string"
        }]
       },
       "AwsIamUser": {
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "GroupList": ["string"],
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
        },
        "UserId": "string",
        "UserName": "string",
        "UserPolicyList": [{
         "PolicyName": "string"
        }]
       },
       "AwsKinesisStream": {
        "Arn": "string",
        "Name": "string",
        "RetentionPeriodHours": number,
        "ShardCount": number,
        "StreamEncryption": {
         "EncryptionType": "string",
         "KeyId": "string"
        }
       },
       "AwsKmsKey": {
        "AWSAccountId": "string",
        "CreationDate": "string",
        "Description": "string",
        "KeyId": "string",
```

```
        "KeyManager": "string",
        "KeyRotationStatus": boolean,
        "KeyState": "string",
        "Origin": "string"
       },
       "AwsLambdaFunction": {
        "Architectures": [
         "string"
        ],
        "Code": {
         "S3Bucket": "string",
         "S3Key": "string",
         "S3ObjectVersion": "string",
         "ZipFile": "string"
        },
        "CodeSha256": "string",
        "DeadLetterConfig": {
         "TargetArn": "string"
        },
        "Environment": {
         "Variables": {
          "Stage": "string"
         },
         "Error": {
          "ErrorCode": "string",
          "Message": "string"
         }
        },
        "FunctionName": "string",
        "Handler": "string",
        "KmsKeyArn": "string",
        "LastModified": "string",
        "Layers": {
         "Arn": "string",
         "CodeSize": number
        },
        "PackageType": "string",
        "RevisionId": "string",
        "Role": "string",
        "Runtime": "string",
        "Timeout": integer,
        "TracingConfig": {
         "Mode": "string"
        },
```

```
        "Version": "string",
        "VpcConfig": {
         "SecurityGroupIds": ["string"],
         "SubnetIds": ["string"]
        },
        "MasterArn": "string",
        "MemorySize": number
       },
       "AwsLambdaLayerVersion": {
        "CompatibleRuntimes": [
         "string"
        ],
        "CreatedDate": "string",
        "Version": number
       },
       "AwsMskCluster": {
        "ClusterInfo": {
         "ClientAuthentication": {
          "Sasl": {
           "Scram": {
            "Enabled": boolean
           },
           "Iam": {
            "Enabled": boolean
           }
          },
          "Tls": {
           "CertificateAuthorityArnList": [],
           "Enabled": boolean
          },
          "Unauthenticated": {
           "Enabled": boolean
          }
         },
         "ClusterName": "string",
         "CurrentVersion": "string",
         "EncryptionInfo": {
          "EncryptionAtRest": {
           "DataVolumeKMSKeyId": "string"
          },
          "EncryptionInTransit": {
           "ClientBroker": "string",
           "InCluster": boolean
          }
```

```
        },
        "EnhancedMonitoring": "string",
        "NumberOfBrokerNodes": integer
       }
      },
      "AwsNetworkFirewallFirewall": {
       "DeleteProtection": boolean,
       "Description": "string",
       "FirewallArn": "string",
       "FirewallId": "string",
       "FirewallName": "string",
       "FirewallPolicyArn": "string",
       "FirewallPolicyChangeProtection": boolean,
       "SubnetChangeProtection": boolean,
       "SubnetMappings": [{
        "SubnetId": "string"
       }],
       "VpcId": "string"
      },
      "AwsNetworkFirewallFirewallPolicy": {
       "Description": "string",
       "FirewallPolicy": {
        "StatefulRuleGroupReferences": [{
         "ResourceArn": "string"
        }],
        "StatelessCustomActions": [{
         "ActionDefinition": {
          "PublishMetricAction": {
           "Dimensions": [{
            "Value": "string"
           }]
          }
         },
         "ActionName": "string"
        }],
        "StatelessDefaultActions": ["string"],
        "StatelessFragmentDefaultActions": ["string"],
        "StatelessRuleGroupReferences": [{
         "Priority": number,
         "ResourceArn": "string"
        }]
       },
       "FirewallPolicyArn": "string",
       "FirewallPolicyId": "string",
```

```
        "FirewallPolicyName": "string"
      },
      "AwsNetworkFirewallRuleGroup": {
       "Capacity": number,
       "Description": "string",
       "RuleGroup": {
        "RulesSource": {
         "RulesSourceList": {
          "GeneratedRulesType": "string",
          "Targets": ["string"],
          "TargetTypes": ["string"]
         },
         "RulesString": "string",
         "StatefulRules": [{
          "Action": "string",
          "Header": {
           "Destination": "string",
           "DestinationPort": "string",
           "Direction": "string",
           "Protocol": "string",
           "Source": "string",
           "SourcePort": "string"
          },
          "RuleOptions": [{
           "Keyword": "string",
           "Settings": ["string"]
          }]
         }],
         "StatelessRulesAndCustomActions": {
          "CustomActions": [{
           "ActionDefinition": {
            "PublishMetricAction": {
             "Dimensions": [{
              "Value": "string"
             }]
            }
           },
           "ActionName": "string"
          }],
          "StatelessRules": [{
           "Priority": number,
           "RuleDefinition": {
            "Actions": ["string"],
            "MatchAttributes": {
```

```
            "DestinationPorts": [{
             "FromPort": number,
             "ToPort": number
            }],
            "Destinations": [{
             "AddressDefinition": "string"
            }],
            "Protocols": [number],
            "SourcePorts": [{
             "FromPort": number,
             "ToPort": number
            }],
            "Sources": [{
             "AddressDefinition": "string"
            }],
            "TcpFlags": [{
             "Flags": ["string"],
             "Masks": ["string"]
            }]
           }
          }
         }]
        }
       },
       "RuleVariables": {
        "IpSets": {
         "Definition": ["string"]
        },
        "PortSets": {
         "Definition": ["string"]
        }
       }
      },
      "RuleGroupArn": "string",
      "RuleGroupId": "string",
      "RuleGroupName": "string",
      "Type": "string"
     },
     "AwsOpenSearchServiceDomain": {
      "AccessPolicies": "string",
      "AdvancedSecurityOptions": {
       "Enabled": boolean,
       "InternalUserDatabaseEnabled": boolean,
       "MasterUserOptions": {
```

```
          "MasterUserArn": "string",
          "MasterUserName": "string",
          "MasterUserPassword": "string"
         }
        },
        "Arn": "string",
        "ClusterConfig": {
         "DedicatedMasterCount": number,
         "DedicatedMasterEnabled": boolean,
         "DedicatedMasterType": "string",
         "InstanceCount": number,
         "InstanceType": "string",
         "WarmCount": number,
         "WarmEnabled": boolean,
         "WarmType": "string",
         "ZoneAwarenessConfig": {
          "AvailabilityZoneCount": number
         },
         "ZoneAwarenessEnabled": boolean
        },
        "DomainEndpoint": "string",
        "DomainEndpointOptions": {
         "CustomEndpoint": "string",
         "CustomEndpointCertificateArn": "string",
         "CustomEndpointEnabled": boolean,
         "EnforceHTTPS": boolean,
         "TLSSecurityPolicy": "string"
        },
        "DomainEndpoints": {
         "string": "string"
        },
        "DomainName": "string",
        "EncryptionAtRestOptions": {
         "Enabled": boolean,
         "KmsKeyId": "string"
        },
        "EngineVersion": "string",
        "Id": "string",
        "LogPublishingOptions": {
         "AuditLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "IndexSlowLogs": {
```

```
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "SearchSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         }
        },
        "NodeToNodeEncryptionOptions": {
         "Enabled": boolean
        },
        "ServiceSoftwareOptions": {
         "AutomatedUpdateDate": "string",
         "Cancellable": boolean,
         "CurrentVersion": "string",
         "Description": "string",
         "NewVersion": "string",
         "OptionalDeployment": boolean,
         "UpdateAvailable": boolean,
         "UpdateStatus": "string"
        },
        "VpcOptions": {
         "SecurityGroupIds": ["string"],
         "SubnetIds": ["string"]
        }
       },
       "AwsRdsDbCluster": {
        "ActivityStreamStatus": "string",
        "AllocatedStorage": number,
        "AssociatedRoles": [{
         "RoleArn": "string",
         "Status": "string"
        }],
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZones": ["string"],
        "BackupRetentionPeriod": integer,
        "ClusterCreateTime": "string",
        "CopyTagsToSnapshot": boolean,
        "CrossAccountClone": boolean,
        "CustomEndpoints": ["string"],
        "DatabaseName": "string",
        "DbClusterIdentifier": "string",
        "DbClusterMembers": [{
         "DbClusterParameterGroupStatus": "string",
```

```
        "DbInstanceIdentifier": "string",
        "IsClusterWriter": boolean,
        "PromotionTier": integer
       }],
       "DbClusterOptionGroupMemberships": [{
        "DbClusterOptionGroupName": "string",
        "Status": "string"
       }],
       "DbClusterParameterGroup": "string",
       "DbClusterResourceId": "string",
       "DbSubnetGroup": "string",
       "DeletionProtection": boolean,
       "DomainMemberships": [{
        "Domain": "string",
        "Fqdn": "string",
        "IamRoleName": "string",
        "Status": "string"
       }],
       "EnabledCloudwatchLogsExports": ["string"],
       "Endpoint": "string",
       "Engine": "string",
       "EngineMode": "string",
       "EngineVersion": "string",
       "HostedZoneId": "string",
       "HttpEndpointEnabled": boolean,
       "IamDatabaseAuthenticationEnabled": boolean,
       "KmsKeyId": "string",
       "MasterUsername": "string",
       "MultiAz": boolean,
       "Port": integer,
       "PreferredBackupWindow": "string",
       "PreferredMaintenanceWindow": "string",
       "ReaderEndpoint": "string",
       "ReadReplicaIdentifiers": ["string"],
       "Status": "string",
       "StorageEncrypted": boolean,
       "VpcSecurityGroups": [{
        "Status": "string",
        "VpcSecurityGroupId": "string"
       }]
      },
      "AwsRdsDbClusterSnapshot": {
       "AllocatedStorage": integer,
       "AvailabilityZones": ["string"],
```

```
        "ClusterCreateTime": "string",
        "DbClusterIdentifier": "string",
        "DbClusterSnapshotAttributes": [{
         "AttributeName": "string",
         "AttributeValues": ["string"]
        }],
        "DbClusterSnapshotIdentifier": "string",
        "Engine": "string",
        "EngineVersion": "string",
        "IamDatabaseAuthenticationEnabled": boolean,
        "KmsKeyId": "string",
        "LicenseModel": "string",
        "MasterUsername": "string",
        "PercentProgress": integer,
        "Port": integer,
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcId": "string"
       },
       "AwsRdsDbInstance": {
        "AllocatedStorage": number,
        "AssociatedRoles": [{
         "RoleArn": "string",
         "FeatureName": "string",
         "Status": "string"
        }],
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZone": "string",
        "BackupRetentionPeriod": number,
        "CACertificateIdentifier": "string",
        "CharacterSetName": "string",
        "CopyTagsToSnapshot": boolean,
        "DBClusterIdentifier": "string",
        "DBInstanceClass": "string",
        "DBInstanceIdentifier": "string",
        "DbInstancePort": number,
        "DbInstanceStatus": "string",
        "DbiResourceId": "string",
        "DBName": "string",
        "DbParameterGroups": [{
         "DbParameterGroupName": "string",
         "ParameterApplyStatus": "string"
```

```
        }],
        "DbSecurityGroups": ["string"],
        "DbSubnetGroup": {
         "DbSubnetGroupArn": "string",
         "DbSubnetGroupDescription": "string",
         "DbSubnetGroupName": "string",
         "SubnetGroupStatus": "string",
         "Subnets": [{
          "SubnetAvailabilityZone": {
           "Name": "string"
          },
          "SubnetIdentifier": "string",
          "SubnetStatus": "string"
         }],
         "VpcId": "string"
        },
        "DeletionProtection": boolean,
        "Endpoint": {
         "Address": "string",
         "Port": number,
         "HostedZoneId": "string"
        },
        "DomainMemberships": [{
         "Domain": "string",
         "Fqdn": "string",
         "IamRoleName": "string",
         "Status": "string"
        }],
        "EnabledCloudwatchLogsExports": ["string"],
        "Engine": "string",
        "EngineVersion": "string",
        "EnhancedMonitoringResourceArn": "string",
        "IAMDatabaseAuthenticationEnabled": boolean,
        "InstanceCreateTime": "string",
        "Iops": number,
        "KmsKeyId": "string",
        "LatestRestorableTime": "string",
        "LicenseModel": "string",
        "ListenerEndpoint": {
         "Address": "string",
         "HostedZoneId": "string",
         "Port": number
        },
        "MasterUsername": "admin",
```

```
        "MaxAllocatedStorage": number,
        "MonitoringInterval": number,
        "MonitoringRoleArn": "string",
        "MultiAz": boolean,
        "OptionGroupMemberships": [{
         "OptionGroupName": "string",
         "Status": "string"
        }],
        "PendingModifiedValues": {
         "AllocatedStorage": number,
         "BackupRetentionPeriod": number,
         "CaCertificateIdentifier": "string",
         "DbInstanceClass": "string",
         "DbInstanceIdentifier": "string",
         "DbSubnetGroupName": "string",
         "EngineVersion": "string",
         "Iops": number,
         "LicenseModel": "string",
         "MasterUserPassword": "string",
         "MultiAZ": boolean,
         "PendingCloudWatchLogsExports": {
          "LogTypesToDisable": ["string"],
          "LogTypesToEnable": ["string"]
         },
         "Port": number,
         "ProcessorFeatures": [{
          "Name": "string",
          "Value": "string"
         }],
         "StorageType": "string"
        },
        "PerformanceInsightsEnabled": boolean,
        "PerformanceInsightsKmsKeyId": "string",
        "PerformanceInsightsRetentionPeriod": number,
        "PreferredBackupWindow": "string",
        "PreferredMaintenanceWindow": "string",
        "ProcessorFeatures": [{
         "Name": "string",
         "Value": "string"
        }],
        "PromotionTier": number,
        "PubliclyAccessible": boolean,
        "ReadReplicaDBClusterIdentifiers": ["string"],
        "ReadReplicaDBInstanceIdentifiers": ["string"],
```

```
        "ReadReplicaSourceDBInstanceIdentifier": "string",
        "SecondaryAvailabilityZone": "string",
        "StatusInfos": [{
         "Message": "string",
         "Normal": boolean,
         "Status": "string",
         "StatusType": "string"
        }],
        "StorageEncrypted": boolean,
        "TdeCredentialArn": "string",
        "Timezone": "string",
        "VpcSecurityGroups": [{
         "VpcSecurityGroupId": "string",
         "Status": "string"
        }]
       },
       "AwsRdsDbSecurityGroup": {
        "DbSecurityGroupArn": "string",
        "DbSecurityGroupDescription": "string",
        "DbSecurityGroupName": "string",
        "Ec2SecurityGroups": [{
         "Ec2SecurityGroupuId": "string",
         "Ec2SecurityGroupName": "string",
         "Ec2SecurityGroupOwnerId": "string",
         "Status": "string"
        }],
        "IpRanges": [{
         "CidrIp": "string",
         "Status": "string"
        }],
        "OwnerId": "string",
        "VpcId": "string"
       },
       "AwsRdsDbSnapshot": {
        "AllocatedStorage": integer,
        "AvailabilityZone": "string",
        "DbInstanceIdentifier": "string",
        "DbiResourceId": "string",
        "DbSnapshotIdentifier": "string",
        "Encrypted": boolean,
        "Engine": "string",
        "EngineVersion": "string",
        "IamDatabaseAuthenticationEnabled": boolean,
        "InstanceCreateTime": "string",
```

```
        "Iops": number,
        "KmsKeyId": "string",
        "LicenseModel": "string",
        "MasterUsername": "string",
        "OptionGroupName": "string",
        "PercentProgress": integer,
        "Port": integer,
        "ProcessorFeatures": [],
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
        "SourceDbSnapshotIdentifier": "string",
        "SourceRegion": "string",
        "Status": "string",
        "StorageType": "string",
        "TdeCredentialArn": "string",
        "Timezone": "string",
        "VpcId": "string"
      },
      "AwsRdsEventSubscription": {
        "CustomerAwsId": "string",
        "CustSubscriptionId": "string",
        "Enabled": boolean,
        "EventCategoriesList": ["string"],
        "EventSubscriptionArn": "string",
        "SnsTopicArn": "string",
        "SourceIdsList": ["string"],
        "SourceType": "string",
        "Status": "string",
        "SubscriptionCreationTime": "string"
      },
      "AwsRedshiftCluster": {
        "AllowVersionUpgrade": boolean,
        "AutomatedSnapshotRetentionPeriod": number,
        "AvailabilityZone": "string",
        "ClusterAvailabilityStatus": "string",
        "ClusterCreateTime": "string",
        "ClusterIdentifier": "string",
        "ClusterNodes": [{
          "NodeRole": "string",
          "PrivateIPAddress": "string",
          "PublicIPAddress": "string"
        }],
        "ClusterParameterGroups": [{
          "ClusterParameterStatusList": [{
```

```
          "ParameterApplyErrorDescription": "string",
          "ParameterApplyStatus": "string",
          "ParameterName": "string"
         }],
         "ParameterApplyStatus": "string",
         "ParameterGroupName": "string"
        }],
        "ClusterPublicKey": "string",
        "ClusterRevisionNumber": "string",
        "ClusterSecurityGroups": [{
         "ClusterSecurityGroupName": "string",
         "Status": "string"
        }],
        "ClusterSnapshotCopyStatus": {
         "DestinationRegion": "string",
         "ManualSnapshotRetentionPeriod": number,
         "RetentionPeriod": number,
         "SnapshotCopyGrantName": "string"
        },
        "ClusterStatus": "string",
        "ClusterSubnetGroupName": "string",
        "ClusterVersion": "string",
        "DBName": "string",
        "DeferredMaintenanceWindows": [{
         "DeferMaintenanceEndTime": "string",
         "DeferMaintenanceIdentifier": "string",
         "DeferMaintenanceStartTime": "string"
        }],
        "ElasticIpStatus": {
         "ElasticIp": "string",
         "Status": "string"
        },
        "ElasticResizeNumberOfNodeOptions": "string",
        "Encrypted": boolean,
        "Endpoint": {
         "Address": "string",
         "Port": number
        },
        "EnhancedVpcRouting": boolean,
        "ExpectedNextSnapshotScheduleTime": "string",
        "ExpectedNextSnapshotScheduleTimeStatus": "string",
        "HsmStatus": {
         "HsmClientCertificateIdentifier": "string",
         "HsmConfigurationIdentifier": "string",
```

```
        "Status": "string"
       },
       "IamRoles": [{
        "ApplyStatus": "string",
        "IamRoleArn": "string"
       }],
       "KmsKeyId": "string",
       "LoggingStatus":{
                   "BucketName": "string",
                   "LastFailureMessage": "string",
                   "LastFailureTime": "string",
                   "LastSuccessfulDeliveryTime": "string",
                   "LoggingEnabled": boolean,
                   "S3KeyPrefix": "string"
               },
       "MaintenanceTrackName": "string",
       "ManualSnapshotRetentionPeriod": number,
       "MasterUsername": "string",
       "NextMaintenanceWindowStartTime": "string",
       "NodeType": "string",
       "NumberOfNodes": number,
       "PendingActions": ["string"],
       "PendingModifiedValues": {
        "AutomatedSnapshotRetentionPeriod": number,
        "ClusterIdentifier": "string",
        "ClusterType": "string",
        "ClusterVersion": "string",
        "EncryptionType": "string",
        "EnhancedVpcRouting": boolean,
        "MaintenanceTrackName": "string",
        "MasterUserPassword": "string",
        "NodeType": "string",
        "NumberOfNodes": number,
        "PubliclyAccessible": "string"
       },
       "PreferredMaintenanceWindow": "string",
       "PubliclyAccessible": boolean,
       "ResizeInfo": {
        "AllowCancelResize": boolean,
        "ResizeType": "string"
       },
       "RestoreStatus": {
        "CurrentRestoreRateInMegaBytesPerSecond": number,
        "ElapsedTimeInSeconds": number,
```

```
        "EstimatedTimeToCompletionInSeconds": number,
        "ProgressInMegaBytes": number,
        "SnapshotSizeInMegaBytes": number,
        "Status": "string"
       },
       "SnapshotScheduleIdentifier": "string",
       "SnapshotScheduleState": "string",
       "VpcId": "string",
       "VpcSecurityGroups": [{
        "Status": "string",
        "VpcSecurityGroupId": "string"
       }]
      },
      "AwsRoute53HostedZone": {
       "HostedZone": {
        "Id": "string",
        "Name": "string",
        "Config": {
         "Comment": "string"
        }
       },
       "NameServers": ["string"],
       "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
         "CloudWatchLogsLogGroupArn": "string",
         "Id": "string",
         "HostedZoneId": "string"
        }
       },
       "Vpcs": [
        {
         "Id": "string",
         "Region": "string"
        }
       ]
      },
      "AwsS3AccessPoint": {
       "AccessPointArn": "string",
       "Alias": "string",
       "Bucket": "string",
       "BucketAccountId": "string",
       "Name": "string",
       "NetworkOrigin": "string",
       "PublicAccessBlockConfiguration": {
```

```
        "BlockPublicAcls": boolean,
        "BlockPublicPolicy": boolean,
        "IgnorePublicAcls": boolean,
        "RestrictPublicBuckets": boolean
       },
       "VpcConfiguration": {
        "VpcId": "string"
       }
      },
      "AwsS3AccountPublicAccessBlock": {
       "BlockPublicAcls": boolean,
       "BlockPublicPolicy": boolean,
       "IgnorePublicAcls": boolean,
       "RestrictPublicBuckets": boolean
      },
      "AwsS3Bucket": {
       "AccessControlList": "string",
       "BucketLifecycleConfiguration": {
        "Rules": [{
         "AbortIncompleteMultipartUpload": {
          "DaysAfterInitiation": number
         },
         "ExpirationDate": "string",
         "ExpirationInDays": number,
         "ExpiredObjectDeleteMarker": boolean,
         "Filter": {
          "Predicate": {
           "Operands": [{
             "Prefix": "string",
             "Type": "string"
            },
            {
             "Tag": {
              "Key": "string",
              "Value": "string"
             },
             "Type": "string"
            }
           ],
           "Type": "string"
          }
         },
         "Id": "string",
         "NoncurrentVersionExpirationInDays": number,
```

```
          "NoncurrentVersionTransitions": [{
           "Days": number,
           "StorageClass": "string"
          }],
          "Prefix": "string",
          "Status": "string",
          "Transitions": [{
           "Date": "string",
           "Days": number,
           "StorageClass": "string"
          }]
         }]
        },
        "BucketLoggingConfiguration": {
         "DestinationBucketName": "string",
         "LogFilePrefix": "string"
        },
        "BucketName": "string",
        "BucketNotificationConfiguration": {
         "Configurations": [{
          "Destination": "string",
          "Events": ["string"],
          "Filter": {
           "S3KeyFilter": {
            "FilterRules": [{
             "Name": "string",
             "Value": "string"
            }]
           }
          },
          "Type": "string"
         }]
        },
        "BucketVersioningConfiguration": {
         "IsMfaDeleteEnabled": boolean,
         "Status": "string"
        },
        "BucketWebsiteConfiguration": {
         "ErrorDocument": "string",
         "IndexDocumentSuffix": "string",
         "RedirectAllRequestsTo": {
          "HostName": "string",
          "Protocol": "string"
         },
```

```
        "RoutingRules": [{
         "Condition": {
          "HttpErrorCodeReturnedEquals": "string",
          "KeyPrefixEquals": "string"
         },
         "Redirect": {
          "HostName": "string",
          "HttpRedirectCode": "string",
          "Protocol": "string",
          "ReplaceKeyPrefixWith": "string",
          "ReplaceKeyWith": "string"
         }
        }]
       },
       "CreatedAt": "string",
       "ObjectLockConfiguration": {
        "ObjectLockEnabled": "string",
        "Rule": {
         "DefaultRetention": {
          "Days": integer,
          "Mode": "string",
          "Years": integer
         }
        }
       },
       "OwnerAccountId": "string",
       "OwnerId": "string",
       "OwnerName": "string",
       "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": boolean,
        "BlockPublicPolicy": boolean,
        "IgnorePublicAcls": boolean,
        "RestrictPublicBuckets": boolean
       },
       "ServerSideEncryptionConfiguration": {
        "Rules": [{
         "ApplyServerSideEncryptionByDefault": {
          "KMSMasterKeyID": "string",
          "SSEAlgorithm": "string"
         }
        }]
       }
      },
      "AwsS3Object": {
```

```
        "ContentType": "string",
        "ETag": "string",
        "LastModified": "string",
        "ServerSideEncryption": "string",
        "SSEKMSKeyId": "string",
        "VersionId": "string"
      },
      "AwsSagemakerNotebookInstance": {
        "DirectInternetAccess": "string",
        "InstanceMetadataServiceConfiguration": {
          "MinimumInstanceMetadataServiceVersion": "string"
        },
        "InstanceType": "string",
        "LastModifiedTime": "string",
        "NetworkInterfaceId": "string",
        "NotebookInstanceArn": "string",
        "NotebookInstanceName": "string",
        "NotebookInstanceStatus": "string",
        "PlatformIdentifier": "string",
        "RoleArn": "string",
        "RootAccess": "string",
        "SecurityGroups": ["string"],
        "SubnetId": "string",
        "Url": "string",
        "VolumeSizeInGB": number
      },
      "AwsSecretsManagerSecret": {
        "Deleted": boolean,
        "Description": "string",
        "KmsKeyId": "string",
        "Name": "string",
        "RotationEnabled": boolean,
        "RotationLambdaArn": "string",
        "RotationOccurredWithinFrequency": boolean,
        "RotationRules": {
          "AutomaticallyAfterDays": integer
        }
      },
      "AwsSnsTopic": {
        "ApplicationSuccessFeedbackRoleArn": "string",
        "FirehoseFailureFeedbackRoleArn": "string",
        "FirehoseSuccessFeedbackRoleArn": "string",
        "HttpFailureFeedbackRoleArn": "string",
        "HttpSuccessFeedbackRoleArn": "string",
```

```
        "KmsMasterKeyId": "string",
        "Owner": "string",
        "SqsFailureFeedbackRoleArn": "string",
        "SqsSuccessFeedbackRoleArn": "string",
        "Subscription": {
         "Endpoint": "string",
         "Protocol": "string"
        },
        "TopicName": "string"
       },
       "AwsSqsQueue": {
        "DeadLetterTargetArn": "string",
        "KmsDataKeyReusePeriodSeconds": number,
        "KmsMasterKeyId": "string",
        "QueueName": "string"
       },
       "AwsSsmPatchCompliance": {
        "Patch": {
         "ComplianceSummary": {
          "ComplianceType": "string",
          "CompliantCriticalCount": integer,
          "CompliantHighCount": integer,
          "CompliantInformationalCount": integer,
          "CompliantLowCount": integer,
          "CompliantMediumCount": integer,
          "CompliantUnspecifiedCount": integer,
          "ExecutionType": "string",
          "NonCompliantCriticalCount": integer,
          "NonCompliantHighCount": integer,
          "NonCompliantInformationalCount": integer,
          "NonCompliantLowCount": integer,
          "NonCompliantMediumCount": integer,
          "NonCompliantUnspecifiedCount": integer,
          "OverallSeverity": "string",
          "PatchBaselineId": "string",
          "PatchGroup": "string",
          "Status": "string"
         }
        }
       },
       "AwsStepFunctionStateMachine": {
        "StateMachineArn": "string",
        "Name": "string",
        "Status": "string",
```

```
        "RoleArn": "string",
        "Type": "string",
        "LoggingConfiguration": {
         "Level": "string",
         "IncludeExecutionData": boolean
        },
        "TracingConfiguration": {
         "Enabled": boolean
        }
       },
       "AwsWafRateBasedRule": {
        "MatchPredicates": [{
         "DataId": "string",
         "Negated": boolean,
         "Type": "string"
        }],
        "MetricName": "string",
        "Name": "string",
        "RateKey": "string",
        "RateLimit": number,
        "RuleId": "string"
       },
       "AwsWafRegionalRateBasedRule": {
        "MatchPredicates": [{
         "DataId": "string",
         "Negated": boolean,
         "Type": "string"
        }],
        "MetricName": "string",
        "Name": "string",
        "RateKey": "string",
        "RateLimit": number,
        "RuleId": "string"
       },
       "AwsWafRegionalRule": {
        "MetricName": "string",
        "Name": "string",
        "RuleId": "string",
        "PredicateList": [{
            "DataId": "string",
            "Negated": boolean,
            "Type": "string"
        }]
       },
```

```
      "AwsWafRegionalRuleGroup": {
       "MetricName": "string",
       "Name": "string",
       "RuleGroupId": "string",
       "Rules": [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }]
      },
      "AwsWafRegionalWebAcl": {
       "DefaultAction": "string",
       "MetricName" : "string",
       "Name": "string",
       "RulesList" : [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string",
        "ExcludedRules": [{
         "ExclusionType": "string",
         "RuleId": "string"
        }],
        "OverrideAction": {
         "Type": "string"
        }
       }],
       "WebAclId": "string"
      },
      "AwsWafRule": {
       "MetricName": "string",
       "Name": "string",
       "PredicateList": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
       }],
       "RuleId": "string"
      },
```

```
      "AwsWafRuleGroup": {
       "MetricName": "string",
       "Name": "string",
       "RuleGroupId": "string",
       "Rules": [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }]
      },
      "AwsWafv2RuleGroup": {
       "Arn": "string",
       "Capacity": number,
       "Description": "string",
       "Id": "string",
       "Name": "string",
       "Rules": [{
        "Action": {
        "Allow": {
         "CustomRequestHandling": {
          "InsertHeaders": [
           {
           "Name": "string",
           "Value": "string"
           },
           {
           "Name": "string",
           "Value": "string"
           }
          ]
         }
        }
        },
        "Name": "string",
        "Priority": number,
        "VisibilityConfig": {
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string",
         "SampledRequestsEnabled": boolean
        }
       }],
```

```
        "VisibilityConfig": {
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string",
         "SampledRequestsEnabled": boolean
        }
       },
       "AwsWafWebAcl": {
        "DefaultAction": "string",
        "Name": "string",
        "Rules": [{
         "Action": {
          "Type": "string"
         },
         "ExcludedRules": [{
          "RuleId": "string"
         }],
         "OverrideAction": {
          "Type": "string"
         },
         "Priority": number,
         "RuleId": "string",
         "Type": "string"
        }],
        "WebAclId": "string"
       },
       "AwsWafv2WebAcl": {
        "Arn": "string",
        "Capacity": number,
        "CaptchaConfig": {
         "ImmunityTimeProperty": {
          "ImmunityTime": number
         }
        },
        "DefaultAction": {
         "Block": {}
        },
        "Description": "string",
        "ManagedbyFirewallManager": boolean,
        "Name": "string",
        "Rules": [{
         "Action": {
          "RuleAction": {
           "Block": {}
          }
```

```
        },
        "Name": "string",
        "Priority": number,
        "VisibilityConfig": {
         "SampledRequestsEnabled": boolean,
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string"
        }
       }],
       "VisibilityConfig": {
        "SampledRequestsEnabled": boolean,
        "CloudWatchMetricsEnabled": boolean,
        "MetricName": "string"
       }
      },
      "AwsXrayEncryptionConfig": {
       "KeyId": "string",
       "Status": "string",
       "Type": "string"
      },
      "Container": {
       "ContainerRuntime": "string",
       "ImageId": "string",
       "ImageName": "string",
       "LaunchedAt": "string",
       "Name": "string",
       "Privileged": boolean,
       "VolumeMounts": [{
        "Name": "string",
        "MountPath": "string"
       }]
      },
      "Other": {
       "string": "string"
      },
      "Id": "string",
      "Partition": "string",
      "Region": "string",
      "ResourceRole": "string",
      "Tags": {
       "string": "string"
      },
      "Type": "string"
     }],
```

```
      "SchemaVersion": "string",
      "Severity": {
       "Label": "string",
       "Normalized": number,
       "Original": "string"
      },
      "Sample": boolean,
      "SourceUrl": "string",
      "Threats": [{
       "FilePaths": [{
        "FileName": "string",
        "FilePath": "string",
        "Hash": "string",
        "ResourceId": "string"
       }],
       "ItemCount": number,
       "Name": "string",
       "Severity": "string"
      }],
      "ThreatIntelIndicators": [{
       "Category": "string",
       "LastObservedAt": "string",
       "Source": "string",
       "SourceUrl": "string",
       "Type": "string",
       "Value": "string"
      }],
      "Title": "string",
      "Types": ["string"],
      "UpdatedAt": "string",
      "UserDefinedFields": {
       "string": "string"
      },
      "VerificationState": "string",
      "Vulnerabilities": [{
       "CodeVulnerabilities": [{
        "Cwes": [
         "string",
         "string"
        ],
        "FilePath": {
         "EndLine": integer,
         "FileName": "string",
         "FilePath": "string",
```

```
        "StartLine": integer
       },
       "SourceArn":"string"
      }],
      "Cvss": [{
       "Adjustments": [{
        "Metric": "string",
        "Reason": "string"
       }],
       "BaseScore": number,
       "BaseVector": "string",
       "Source": "string",
       "Version": "string"
      }],
      "EpssScore": number,
      "ExploitAvailable": "string",
      "FixAvailable": "string",
      "Id": "string",
      "LastKnownExploitAt": "string",
      "ReferenceUrls": ["string"],
      "RelatedVulnerabilities": ["string"],
      "Vendor": {
       "Name": "string",
       "Url": "string",
       "VendorCreatedAt": "string",
       "VendorSeverity": "string",
       "VendorUpdatedAt": "string"
      },
      "VulnerablePackages": [{
       "Architecture": "string",
       "Epoch": "string",
       "FilePath": "string",
       "FixedInVersion": "string",
       "Name": "string",
       "PackageManager": "string",
       "Release": "string",
       "Remediation": "string",
       "SourceLayerArn": "string",
       "SourceLayerHash": "string",
       "Version": "string"
      }]
     }],
     "Workflow": {
      "Status": "string"
```

```
      },
      "WorkflowState": "string"
    }
]
```

ASFF フィールドと値への統合の影響

Security Hub には、次の 2 種類の統合があります。

- [統合コントロールビュー] (常に有効。無効にできません) — 各コントロールには、標準全体で 1 つの識別子があります。Security Hub コンソールの [コントロール] ページには、さまざまな標準のすべてのコントロールが表示されます。
- [統合されたコントロールの検出結果] (有効無効を切り替え可) — [統合されたコントロールの検出結果] を有効にすると、チェックが複数の標準で共有されている場合でも、セキュリティハブはセキュリティチェックに対して単一の検出結果を生成します。これは検索時のノイズを減らすためのものです。2023 年 2 月 23 日以降に Security Hub を有効にした場合、統合コントロールの検出結果はデフォルトで有効になります。それ以外の場合は、デフォルトで無効になっています。ただし、Security Hub メンバーアカウントで [統合されたコントロールの検出結果] が有効になるのは、管理者アカウントで有効になっている場合のみです。管理者アカウントでこの機能が無効になっている場合、メンバーアカウントでも無効になります。この機能を有効にする手順については、「[統合されたコントロールの検出結果] を有効にする」を参照してください。

どちらの機能でも、AWS Security Finding 形式 (ASFF) のコントロール検出結果フィールドと値に変更が加えられます。このセクションでは、これらの変更の概要を示します。

統合コントロールビュー — ASFF の変更

統合コントロールビュー機能では、ASFF のコントロール結果フィールドと値に次の変更が導入されました。

ワークフローがこれらのコントロール検出結果フィールドの値に依存していない場合は、何もする必要はありません。

これらのコントロール結果フィールドの特定の値に依存するワークフローがある場合は、ワークフローを更新して現在の値を使用します。

ASFF フィールド	統合コントロールビューのリリース前のサンプル値	統合コントロールビューのリリース後のサンプル値および変更の説明
コンプライアンス。SecurityControlId	該当なし (新しいフィールド)	EC2.2 標準全体で単一のコントロール ID を導入します。`ProductFields.RuleId` は、CIS v1.2.0 コントロールに引き続き標準ベースのコントロール ID を提供します。`ProductFields.ControlId` は、他の標準のコントロールについて、引き続き標準ベースのコントロール ID を提供します。
コンプライアンス。AssociatedStandards	該当なし (新しいフィールド)	[{"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"}] コントロールが有効になっている標準を示します。
ProductFields.ArchivalReasons:0/説明	該当なし (新しいフィールド)	「統合統制結果がオンまたはオフになっているため、結果はアーカイブ済み状態

ASFF フィールド	統合コントロールビューのリリース前のサンプル値	統合コントロールビューのリリース後のサンプル値および変更の説明
		になっています。これにより、新しい結果が生成されるときに、以前の状態の結果がアーカイブされます。」 Security Hub が既存の結果をアーカイブした理由について説明します。
ProductFields.ArchivalReasons:0/ReasonCode	該当なし (新しいフィールド)	「統合統制結果更新」 Security Hub が既存の調査結果をアーカイブした理由を示します。
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation このフィールドは標準を参照しないようになりました。

ASFF フィールド	統合コントロールビューのリリース前のサンプル値	統合コントロールビューのリリース後のサンプル値および変更の説明
Remediation.Recommendation.Text	「この問題を解決する方法については、AWS Security Hub PCI DSS ドキュメントを参照してください。」	「この問題を修正する方法については、AWS Security Hub コントロールのドキュメントを参照してください。」 このフィールドは標準を参照しないようになりました。
Remediation.Recommendation.Url	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation このフィールドは標準を参照しないようになりました。

統合されたコントロールの検出結果 — ASFF の変更

統合統制結果を有効にした場合、ASFF の統制結果のフィールドと値に次の変更が加えられると、影響を受ける可能性があります。これらの変更は、統合コントロールビューについて前述した変更に加えて行われます。

ワークフローがこれらのコントロール検出結果フィールドの値に依存していない場合は、何もする必要はありません。

これらのコントロール結果フィールドの特定の値に依存するワークフローがある場合は、ワークフローを更新して現在の値を使用します。

> **Note**
>
> AWS v2.0.0 の自動セキュリティレスポンスは、統合統制結果をサポートします。このバージョンのソリューションを使用すると、[統合されたコントロールの検出結果] を有効にしてもワークフローを維持できます。

ASFF フィールド	統合統制結果を有効にする前の値の例	[統合されたコントロールの検出結果] を有効にした後の値の例と変更の説明
GeneratorId	aws-foundational-security-best-practices/v/1.0.0/Config.1	security-control/Config.1 このフィールドは標準を参照しないようになりました。
タイトル	PCI.Config.1 AWS Config を有効にする必要があります	AWS Config を有効にする必要があります このフィールドは、標準固有の情報を参照しなくなりました。
ID	arn:aws:securityhub:eu-central-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.IAM.5/finding/ab6d6a26-a156-48f0-9403-115983e5a956	arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/ab6d6a26-a156-48f0-9403-115983e5a956 このフィールドは標準を参照しないようになりました。
ProductFields.ControlId	PCI.EC2.2	Removed。代わりに `Compliance.SecurityControlId` を参照してください。 このフィールドは削除され、標準にとらわれない単一のコントロール ID が優先されます。

ASFF フィールド	統合統制結果を有効にする前の値の例	[統合されたコントロールの検出結果] を有効にした後の値の例と変更の説明
ProductFields.RuleId	1.3	Removed。代わりに `Compliance.SecurityControlId` を参照してください。 このフィールドは削除され、標準にとらわれない単一のコントロール ID が優先されます。
説明	この PCI DSS コントロール AWS Config は、現在のアカウントとリージョンで が有効になっているかどうかをチェックします。	この AWS コントロールは、現在のアカウントとリージョンで が有効になっているかどうか AWS Config をチェックします。 このフィールドは標準を参照しないようになりました。

緊急度	"Severity": {
	
	"Product": 90,
	
	"Label": "CRITICAL",
	
	"Normalized": 90,
	
	"Original": "CRITICAL"
	
	}
		"Severity": {
		
		"Label": "CRITICAL",
		
		"Normalized": 90,
		
		"Original": "CRITICAL"
		
		}
		
		Security Hub は、Product フィールドを使用して検出結果の重要度を記述しなくなりました。

型	["Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"]	["Software and Configuration Checks/Industry and Regulatory Standards"] このフィールドは標準を参照しないようになりました。

ASFF フィールド	統合統制結果を有効にする前の値の例	[統合されたコントロールの検出結果] を有効にした後の値の例と変更の説明
コンプライアンス。RelatedRequirements	["PCI DSS 10.5.2", 「PCI DSS 11.5」、 「CIS AWS Foundations 2.5」〕	["PCI DSS v3.2.1/10.5.2", "PCI DSS v3.2.1/11.5", 「CIS AWS Foundations Benchmark v1.2.0/2.5」」 このフィールドには、有効なすべての標準に関連する要件が表示されます。
CreatedAt	2022-05-05T08:18:13.138Z	2022-09-25T08:18:13.138Z 形式は変わりませんが、統合統制結果を有効にすると値がリセットされます。
FirstObservedAt	2022-05-07T08:18:13.138Z	2022-09-28T08:18:13.138Z 形式は変わりませんが、統合統制結果を有効にすると値がリセットされます。
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation	Removed。代わりに `Remediation.Recommendation.Url` を参照してください。
ProductFields.StandardsArn	arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0	Removed。代わりに `Compliance.AssociatedStandards` を参照してください。
ProductFields.StandardsControlArn	arn:aws:securityhub:us-east-1:123456789012:control/aws-foundational-security-best-practices/v/1.0.0/Config.1	Removed。Security Hub は、標準全体でセキュリティチェックの結果を 1 つ生成します。

ASFF フィールド	統合統制結果を有効にする前の値の例	[統合されたコントロールの検出結果] を有効にした後の値の例と変更の説明
ProductFields.StandardsGuideArn	arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0	Removed。代わりに `Compliance.AssociatedStandards` を参照してください。
ProductFields.StandardsGuideSubscriptionArn	arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0	Removed。Security Hub は、標準全体でセキュリティチェックの結果を 1 つ生成します。
ProductFields.StandardsSubscriptionArn	arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0	Removed。Security Hub は、標準全体でセキュリティチェックの結果を 1 つ生成します。
ProductFields.aws/securityhub/FindingId	arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0/Config.1/finding/751c2173-7372-4e12-8656-a5210dfb1d67	arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/Config.1/finding/751c2173-7372-4e12-8656-a5210dfb1d67 このフィールドは標準を参照しないようになりました。

統合統制結果を有効にした後の、顧客提供の ASFF フィールドの値

[統合されたコントロールの検出結果] を有効にすると、Security Hub は標準全体で 1 つの検出結果を生成し、元の検出結果をアーカイブします (標準ごとに個別の検出結果)。アーカイブされた結果を表示するには、[Record state] (レコード状態) フィルターを [ARCHIVED] (アーカイブ) に設定してセキュリティハブコンソールの [Findings] (結果) ページにアクセスするか、`GetFindings` API アクションを使用することができます。Security Hub コンソールまたは BatchUpdateFindings API を使用

して元の検出結果に加えた更新は、新しい検出結果には保持されません (必要に応じて、アーカイブされた検出結果を参照してこのデータを復元できます) 。

顧客提供の ASFF フィールド	統合統制結果を有効にした後の変更の説明
信頼度	空の状態にリセットされます。
緊急性	空の状態にリセットされます。
注記	空の状態にリセットされます。
RelatedFindings	空の状態にリセットされます。
緊急度	結果のデフォルトの重要度 (コントロールの重要度と同じ)。
型	標準に依存しない値にリセットされます。
UserDefinedFields	空の状態にリセットされます。
VerificationState	空の状態にリセットされます。
ワークフロー	新たに失敗した検出結果のデフォルト値は `NEW` になります。新たに成功した検出結果のデフォルト値は `RESOLVED` になります。

[統合されたコントロールの検出結果] を有効にする前と後のジェネレーター ID

[統合されたコントロールの検出結果] を有効にした場合、コントロールのジェネレーター ID は以下のリストのように変更されます。これらは、2023 年 2 月 15 日の時点で Security Hub がサポートしていたコントロールに適用されます。

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.1	セキュリティコントロール/CloudWatch.1
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.10	security-control/IAM.16

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.11	security-control/IAM.17
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.12	security-control/IAM.4
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.13	security-control/IAM.9
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.14	security-control/IAM.6
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.16	security-control/IAM.2
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.2	security-control/IAM.5
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.20	security-control/IAM.18
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.22	security-control/IAM.1
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.3	security-control/IAM.8
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.4	security-control/IAM.3
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.5	security-control/IAM.11
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.6	security-control/IAM.12
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.7	security-control/IAM.13

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.8	security-control/IAM.14
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.9	security-control/IAM.15
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.1	セキュリティコントロール/CloudTrail.1
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.2	セキュリティコントロール/CloudTrail.4
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.3	セキュリティコントロール/CloudTrail.6
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.4	セキュリティコントロール/CloudTrail.5
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.5	security-control/Config.1
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.6	セキュリティコントロール/CloudTrail.7
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.7	セキュリティコントロール/CloudTrail.2
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.8	security-control/KMS.4
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.9	security-control/EC2.6
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.1	セキュリティコントロール/CloudWatch.2
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.2	セキュリティコントロール/CloudWatch.3

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.3	セキュリティコントロール/CloudWatch.1
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.4	セキュリティコントロール/CloudWatch.4
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.5	セキュリティコントロール/CloudWatch.5
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.6	セキュリティコントロール/CloudWatch.6
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.7	セキュリティコントロール/CloudWatch.7
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.8	セキュリティコントロール/CloudWatch.8
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.9	セキュリティコントロール/CloudWatch.9
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.10	セキュリティコントロール/CloudWatch.10
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.11	セキュリティコントロール/CloudWatch.11
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.12	セキュリティコントロール/CloudWatch.12
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.13	セキュリティコントロール/CloudWatch.13
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.14	セキュリティコントロール/CloudWatch.14
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/4.1	security-control/EC2.13

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/4.2	security-control/EC2.14
arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/4.3	security-control/EC2.2
cis-aws-foundations-benchmark/v/1.4.0/1.10	security-control/IAM.5
cis-aws-foundations-benchmark/v/1.4.0/1.14	security-control/IAM.3
cis-aws-foundations-benchmark/v/1.4.0/1.16	security-control/IAM.1
cis-aws-foundations-benchmark/v/1.4.0/1.17	security-control/IAM.18
cis-aws-foundations-benchmark/v/1.4.0/1.4	security-control/IAM.4
cis-aws-foundations-benchmark/v/1.4.0/1.5	security-control/IAM.9
cis-aws-foundations-benchmark/v/1.4.0/1.6	security-control/IAM.6
cis-aws-foundations-benchmark/v/1.4.0/1.7	セキュリティコントロール/CloudWatch.1
cis-aws-foundations-benchmark/v/1.4.0/1.8	security-control/IAM.15
cis-aws-foundations-benchmark/v/1.4.0/1.9	security-control/IAM.16
cis-aws-foundations-benchmark/v/1.4.0/2.1.2	security-control/S3.5
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.1	security-control/S3.1
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.2	security-control/S3.8
cis-aws-foundations-benchmark/v/1.4.0/2.2.1	security-control/EC2.7
cis-aws-foundations-benchmark/v/1.4.0/2.3.1	security-control/RDS.3
cis-aws-foundations-benchmark/v/1.4.0/3.1	セキュリティコントロール/CloudTrail.1
cis-aws-foundations-benchmark/v/1.4.0/3.2	セキュリティコントロール/CloudTrail.4

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
cis-aws-foundations-benchmark/v/1.4.0/3.4	セキュリティコントロール/CloudTrail.5
cis-aws-foundations-benchmark/v/1.4.0/3.5	security-control/Config.1
cis-aws-foundations-benchmark/v/1.4.0/3.6	security-control/S3.9
cis-aws-foundations-benchmark/v/1.4.0/3.7	セキュリティコントロール/CloudTrail.2
cis-aws-foundations-benchmark/v/1.4.0/3.8	security-control/KMS.4
cis-aws-foundations-benchmark/v/1.4.0/3.9	security-control/EC2.6
cis-aws-foundations-benchmark/v/1.4.0/4.3	セキュリティコントロール/CloudWatch.1
cis-aws-foundations-benchmark/v/1.4.0/4.4	セキュリティコントロール/CloudWatch.4
cis-aws-foundations-benchmark/v/1.4.0/4.5	セキュリティコントロール/CloudWatch.5
cis-aws-foundations-benchmark/v/1.4.0/4.6	セキュリティコントロール/CloudWatch.6
cis-aws-foundations-benchmark/v/1.4.0/4.7	セキュリティコントロール/CloudWatch.7
cis-aws-foundations-benchmark/v/1.4.0/4.8	セキュリティコントロール/CloudWatch.8
cis-aws-foundations-benchmark/v/1.4.0/4.9	セキュリティコントロール/CloudWatch.9
cis-aws-foundations-benchmark/v/1.4.0/4.10	セキュリティコントロール/CloudWatch.10
cis-aws-foundations-benchmark/v/1.4.0/4.11	セキュリティコントロール/CloudWatch.11
cis-aws-foundations-benchmark/v/1.4.0/4.12	セキュリティコントロール/CloudWatch.12
cis-aws-foundations-benchmark/v/1.4.0/4.13	セキュリティコントロール/CloudWatch.13
cis-aws-foundations-benchmark/v/1.4.0/4.14	セキュリティコントロール/CloudWatch.14
cis-aws-foundations-benchmark/v/1.4.0/5.1	security-control/EC2.21
cis-aws-foundations-benchmark/v/1.4.0/5.3	security-control/EC2.2

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/Account.1	security-control/Account.1
aws-foundational-security-best-practices/v/1.0.0/ACM.1	security-control/ACM.1
aws-foundational-security-best-practices/v/1.0.0/APIGateway.1	security-control/APIGateway.1
aws-foundational-security-best-practices/v/1.0.0/APIGateway.2	security-control/APIGateway.2
aws-foundational-security-best-practices/v/1.0.0/APIGateway.3	security-control/APIGateway.3
aws-foundational-security-best-practices/v/1.0.0/APIGateway.4	security-control/APIGateway.4
aws-foundational-security-best-practices/v/1.0.0/APIGateway.5	security-control/APIGateway.5
aws-foundational-security-best-practices/v/1.0.0/APIGateway.8	security-control/APIGateway.8
aws-foundational-security-best-practices/v/1.0.0/APIGateway.9	security-control/APIGateway.9
aws-foundational-security-best-practices/v/1.0.0/AutoScaling.1	セキュリティコントロール/AutoScaling.1
aws-foundational-security-best-practices/v/1.0.0/AutoScaling.2	セキュリティコントロール/AutoScaling.2
aws-foundational-security-best-practices/v/1.0.0/AutoScaling.3	セキュリティコントロール/AutoScaling.3
aws-foundational-security-best-practices/v/1.0.0/Autoscaling.5	security-control/Autoscaling.5

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/AutoScaling.6	セキュリティコントロール/AutoScaling.6
aws-foundational-security-best-practices/v/1.0.0/AutoScaling.9	セキュリティコントロール/AutoScaling.9
aws-foundational-security-best-practices/v/1.0.0/CloudFront.1	セキュリティコントロール/CloudFront.1
aws-foundational-security-best-practices/v/1.0.0/CloudFront.3	セキュリティコントロール/CloudFront.3
aws-foundational-security-best-practices/v/1.0.0/CloudFront.4	セキュリティコントロール/CloudFront.4
aws-foundational-security-best-practices/v/1.0.0/CloudFront.5	セキュリティコントロール/CloudFront.5
aws-foundational-security-best-practices/v/1.0.0/CloudFront.6	セキュリティコントロール/CloudFront.6
aws-foundational-security-best-practices/v/1.0.0/CloudFront.7	セキュリティコントロール/CloudFront.7
aws-foundational-security-best-practices/v/1.0.0/CloudFront.8	セキュリティコントロール/CloudFront.8
aws-foundational-security-best-practices/v/1.0.0/CloudFront.9	セキュリティコントロール/CloudFront.9
aws-foundational-security-best-practices/v/1.0.0/CloudFront.10	セキュリティコントロール/CloudFront.10
aws-foundational-security-best-practices/v/1.0.0/CloudFront.12	セキュリティコントロール/CloudFront.12
aws-foundational-security-best-practices/v/1.0.0/CloudTrail.1	セキュリティコントロール/CloudTrail.1

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2	セキュリティコントロール/CloudTrail.2
aws-foundational-security-best-practices/v/1.0.0/CloudTrail.4	セキュリティコントロール/CloudTrail.4
aws-foundational-security-best-practices/v/1.0.0/CloudTrail.5	セキュリティコントロール/CloudTrail.5
aws-foundational-security-best-practices/v/1.0.0/CodeBuild.1	セキュリティコントロール/CodeBuild.1
aws-foundational-security-best-practices/v/1.0.0/CodeBuild.2	セキュリティコントロール/CodeBuild.2
aws-foundational-security-best-practices/v/1.0.0/CodeBuild.3	セキュリティコントロール/CodeBuild.3
aws-foundational-security-best-practices/v/1.0.0/CodeBuild.4	セキュリティコントロール/CodeBuild.4
aws-foundational-security-best-practices/v/1.0.0/Config.1	security-control/Config.1
aws-foundational-security-best-practices/v/1.0.0/DMS.1	security-control/DMS.1
aws-foundational-security-best-practices/v/1.0.0/DynamoDB.1	security-control/DynamoDB.1
aws-foundational-security-best-practices/v/1.0.0/DynamoDB.2	security-control/DynamoDB.2
aws-foundational-security-best-practices/v/1.0.0/DynamoDB.3	security-control/DynamoDB.3
aws-foundational-security-best-practices/v/1.0.0/EC2.1	security-control/EC2.1

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/EC2.3	security-control/EC2.3
aws-foundational-security-best-practices/v/1.0.0/EC2.4	security-control/EC2.4
aws-foundational-security-best-practices/v/1.0.0/EC2.6	security-control/EC2.6
aws-foundational-security-best-practices/v/1.0.0/EC2.7	security-control/EC2.7
aws-foundational-security-best-practices/v/1.0.0/EC2.8	security-control/EC2.8
aws-foundational-security-best-practices/v/1.0.0/EC2.9	security-control/EC2.9
aws-foundational-security-best-practices/v/1.0.0/EC2.10	security-control/EC2.10
aws-foundational-security-best-practices/v/1.0.0/EC2.15	security-control/EC2.15
aws-foundational-security-best-practices/v/1.0.0/EC2.16	security-control/EC2.16
aws-foundational-security-best-practices/v/1.0.0/EC2.17	security-control/EC2.17
aws-foundational-security-best-practices/v/1.0.0/EC2.18	security-control/EC2.18
aws-foundational-security-best-practices/v/1.0.0/EC2.19	security-control/EC2.19
aws-foundational-security-best-practices/v/1.0.0/EC2.2	security-control/EC2.2

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/EC2.20	security-control/EC2.20
aws-foundational-security-best-practices/v/1.0.0/EC2.21	security-control/EC2.21
aws-foundational-security-best-practices/v/1.0.0/EC2.23	security-control/EC2.23
aws-foundational-security-best-practices/v/1.0.0/EC2.24	security-control/EC2.24
aws-foundational-security-best-practices/v/1.0.0/EC2.25	security-control/EC2.25
aws-foundational-security-best-practices/v/1.0.0/ECR.1	security-control/ECR.1
aws-foundational-security-best-practices/v/1.0.0/ECR.2	security-control/ECR.2
aws-foundational-security-best-practices/v/1.0.0/ECR.3	security-control/ECR.3
aws-foundational-security-best-practices/v/1.0.0/ECS.1	security-control/ECS.1
aws-foundational-security-best-practices/v/1.0.0/ECS.10	security-control/ECS.10
aws-foundational-security-best-practices/v/1.0.0/ECS.12	security-control/ECS.12
aws-foundational-security-best-practices/v/1.0.0/ECS.2	security-control/ECS.2
aws-foundational-security-best-practices/v/1.0.0/ECS.3	security-control/ECS.3

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/ECS.4	security-control/ECS.4
aws-foundational-security-best-practices/v/1.0.0/ECS.5	security-control/ECS.5
aws-foundational-security-best-practices/v/1.0.0/ECS.8	security-control/ECS.8
aws-foundational-security-best-practices/v/1.0.0/EFS .1	security-control/EFS.1
aws-foundational-security-best-practices/v/1.0.0/EFS .2	security-control/EFS.2
aws-foundational-security-best-practices/v/1.0.0/EFS .3	security-control/EFS.3
aws-foundational-security-best-practices/v/1.0.0/EFS .4	security-control/EFS.4
aws-foundational-security-best-practices/v/1.0.0/EKS.2	security-control/EKS.2
aws-foundational-security-best-practices/v/1.0.0/ElasticBeanstalk.1	セキュリティコントロール/ElasticBeanstalk.1
aws-foundational-security-best-practices/v/1.0.0/ElasticBeanstalk.2	セキュリティコントロール/ElasticBeanstalk.2
aws-foundational-security-best-practices/v/1.0.0/ELBv2.1	security-control/ELB.1
aws-foundational-security-best-practices/v/1.0.0/ELB.2	security-control/ELB.2
aws-foundational-security-best-practices/v/1.0.0/ELB.3	security-control/ELB.3

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/ELB.4	security-control/ELB.4
aws-foundational-security-best-practices/v/1.0.0/ELB.5	security-control/ELB.5
aws-foundational-security-best-practices/v/1.0.0/ELB.6	security-control/ELB.6
aws-foundational-security-best-practices/v/1.0.0/ELB.7	security-control/ELB.7
aws-foundational-security-best-practices/v/1.0.0/ELB.8	security-control/ELB.8
aws-foundational-security-best-practices/v/1.0.0/ELB.9	security-control/ELB.9
aws-foundational-security-best-practices/v/1.0.0/ELB.10	security-control/ELB.10
aws-foundational-security-best-practices/v/1.0.0/ELB.11	security-control/ELB.11
aws-foundational-security-best-practices/v/1.0.0/ELB.12	security-control/ELB.12
aws-foundational-security-best-practices/v/1.0.0/ELB.13	security-control/ELB.13
aws-foundational-security-best-practices/v/1.0.0/ELB.14	security-control/ELB.14
aws-foundational-security-best-practices/v/1.0.0/EMR.1	security-control/EMR.1
aws-foundational-security-best-practices/v/1.0.0/ES.1	security-control/ES.1

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/ES.2	security-control/ES.2
aws-foundational-security-best-practices/v/1.0.0/ES.3	security-control/ES.3
aws-foundational-security-best-practices/v/1.0.0/ES.4	security-control/ES.4
aws-foundational-security-best-practices/v/1.0.0/ES.5	security-control/ES.5
aws-foundational-security-best-practices/v/1.0.0/ES.6	security-control/ES.6
aws-foundational-security-best-practices/v/1.0.0/ES.7	security-control/ES.7
aws-foundational-security-best-practices/v/1.0.0/ES.8	security-control/ES.8
aws-foundational-security-best-practices/v/1.0.0/GuardDuty.1	セキュリティコントロール/GuardDuty.1
aws-foundational-security-best-practices/v/1.0.0/IAM.1	security-control/IAM.1
aws-foundational-security-best-practices/v/1.0.0/IAM.2	security-control/IAM.2
aws-foundational-security-best-practices/v/1.0.0/IAM.21	security-control/IAM.21
aws-foundational-security-best-practices/v/1.0.0/IAM.3	security-control/IAM.3
aws-foundational-security-best-practices/v/1.0.0/IAM.4	security-control/IAM.4

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/IAM.5	security-control/IAM.5
aws-foundational-security-best-practices/v/1.0.0/IAM.6	security-control/IAM.6
aws-foundational-security-best-practices/v/1.0.0/IAM.7	security-control/IAM.7
aws-foundational-security-best-practices/v/1.0.0/IAM.8	security-control/IAM.8
aws-foundational-security-best-practices/v/1.0.0/Kinesis.1	security-control/Kinesis.1
aws-foundational-security-best-practices/v/1.0.0/KMS.1	security-control/KMS.1
aws-foundational-security-best-practices/v/1.0.0/KMS.2	security-control/KMS.2
aws-foundational-security-best-practices/v/1.0.0/KMS.3	security-control/KMS.3
aws-foundational-security-best-practices/v/1.0.0/Lambda.1	security-control/Lambda.1
aws-foundational-security-best-practices/v/1.0.0/Lambda.2	security-control/Lambda.2
aws-foundational-security-best-practices/v/1.0.0/Lambda.5	security-control/Lambda.5
aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall.3	セキュリティコントロール/NetworkFirewall.3
aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall.4	セキュリティコントロール/NetworkFirewall.4

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall.5	セキュリティコントロール/NetworkFirewall.5
aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall.6	セキュリティコントロール/NetworkFirewall.6
aws-foundational-security-best-practices/v/1.0.0/Opensearch.1	security-control/Opensearch.1
aws-foundational-security-best-practices/v/1.0.0/Opensearch.2	security-control/Opensearch.2
aws-foundational-security-best-practices/v/1.0.0/Opensearch.3	security-control/Opensearch.3
aws-foundational-security-best-practices/v/1.0.0/Opensearch.4	security-control/Opensearch.4
aws-foundational-security-best-practices/v/1.0.0/Opensearch.5	security-control/Opensearch.5
aws-foundational-security-best-practices/v/1.0.0/Opensearch.6	security-control/Opensearch.6
aws-foundational-security-best-practices/v/1.0.0/Opensearch.7	security-control/Opensearch.7
aws-foundational-security-best-practices/v/1.0.0/Opensearch.8	security-control/Opensearch.8
aws-foundational-security-best-practices/v/1.0.0/RDS.1	security-control/RDS.1
aws-foundational-security-best-practices/v/1.0.0/RDS.10	security-control/RDS.10
aws-foundational-security-best-practices/v/1.0.0/RDS.11	security-control/RDS.11

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/RDS.12	security-control/RDS.12
aws-foundational-security-best-practices/v/1.0.0/RDS.13	security-control/RDS.13
aws-foundational-security-best-practices/v/1.0.0/RDS.14	security-control/RDS.14
aws-foundational-security-best-practices/v/1.0.0/RDS.15	security-control/RDS.15
aws-foundational-security-best-practices/v/1.0.0/RDS.16	security-control/RDS.16
aws-foundational-security-best-practices/v/1.0.0/RDS.17	security-control/RDS.17
aws-foundational-security-best-practices/v/1.0.0/RDS.18	security-control/RDS.18
aws-foundational-security-best-practices/v/1.0.0/RDS.19	security-control/RDS.19
aws-foundational-security-best-practices/v/1.0.0/RDS.2	security-control/RDS.2
aws-foundational-security-best-practices/v/1.0.0/RDS.20	security-control/RDS.20
aws-foundational-security-best-practices/v/1.0.0/RDS.21	security-control/RDS.21
aws-foundational-security-best-practices/v/1.0.0/RDS.22	security-control/RDS.22
aws-foundational-security-best-practices/v/1.0.0/RDS.23	security-control/RDS.23

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/RDS.24	security-control/RDS.24
aws-foundational-security-best-practices/v/1.0.0/RDS.25	security-control/RDS.25
aws-foundational-security-best-practices/v/1.0.0/RDS.3	security-control/RDS.3
aws-foundational-security-best-practices/v/1.0.0/RDS.4	security-control/RDS.4
aws-foundational-security-best-practices/v/1.0.0/RDS.5	security-control/RDS.5
aws-foundational-security-best-practices/v/1.0.0/RDS.6	security-control/RDS.6
aws-foundational-security-best-practices/v/1.0.0/RDS.7	security-control/RDS.7
aws-foundational-security-best-practices/v/1.0.0/RDS.8	security-control/RDS.8
aws-foundational-security-best-practices/v/1.0.0/RDS.9	security-control/RDS.9
aws-foundational-security-best-practices/v/1.0.0/Redshift.1	security-control/Redshift.1
aws-foundational-security-best-practices/v/1.0.0/Redshift.2	security-control/Redshift.2
aws-foundational-security-best-practices/v/1.0.0/Redshift.3	security-control/Redshift.3
aws-foundational-security-best-practices/v/1.0.0/Redshift.4	security-control/Redshift.4

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/Redshift.6	security-control/Redshift.6
aws-foundational-security-best-practices/v/1.0.0/Redshift.7	security-control/Redshift.7
aws-foundational-security-best-practices/v/1.0.0/Redshift.8	security-control/Redshift.8
aws-foundational-security-best-practices/v/1.0.0/Redshift.9	security-control/Redshift.9
aws-foundational-security-best-practices/v/1.0.0/S3.1	security-control/S3.1
aws-foundational-security-best-practices/v/1.0.0/S3.12	security-control/S3.12
aws-foundational-security-best-practices/v/1.0.0/S3.13	security-control/S3.13
aws-foundational-security-best-practices/v/1.0.0/S3.2	security-control/S3.2
aws-foundational-security-best-practices/v/1.0.0/S3.3	security-control/S3.3
aws-foundational-security-best-practices/v/1.0.0/S3.5	security-control/S3.5
aws-foundational-security-best-practices/v/1.0.0/S3.6	security-control/S3.6
aws-foundational-security-best-practices/v/1.0.0/S3.8	security-control/S3.8
aws-foundational-security-best-practices/v/1.0.0/S3.9	security-control/S3.9

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/SageMaker.1	セキュリティコントロール/SageMaker.1
aws-foundational-security-best-practices/v/1.0.0/SageMaker.2	セキュリティコントロール/SageMaker.2
aws-foundational-security-best-practices/v/1.0.0/SageMaker.3	セキュリティコントロール/SageMaker.3
aws-foundational-security-best-practices/v/1.0.0/SecretsManager.1	セキュリティコントロール/SecretsManager.1
aws-foundational-security-best-practices/v/1.0.0/SecretsManager.2	セキュリティコントロール/SecretsManager.2
aws-foundational-security-best-practices/v/1.0.0/SecretsManager.3	セキュリティコントロール/SecretsManager.3
aws-foundational-security-best-practices/v/1.0.0/SecretsManager.4	セキュリティコントロール/SecretsManager.4
aws-foundational-security-best-practices/v/1.0.0/SQS.1	security-control/SQS.1
aws-foundational-security-best-practices/v/1.0.0/SSM.1	security-control/SSM.1
aws-foundational-security-best-practices/v/1.0.0/SSM.2	security-control/SSM.2
aws-foundational-security-best-practices/v/1.0.0/SSM.3	security-control/SSM.3
aws-foundational-security-best-practices/v/1.0.0/SSM.4	security-control/SSM.4
aws-foundational-security-best-practices/v/1.0.0/WAF.1	security-control/WAF.1

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/WAF.2	security-control/WAF.2
aws-foundational-security-best-practices/v/1.0.0/WAF.3	security-control/WAF.3
aws-foundational-security-best-practices/v/1.0.0/WAF.4	security-control/WAF.4
aws-foundational-security-best-practices/v/1.0.0/WAF.6	security-control/WAF.6
aws-foundational-security-best-practices/v/1.0.0/WAF.7	security-control/WAF.7
aws-foundational-security-best-practices/v/1.0.0/WAF.8	security-control/WAF.8
aws-foundational-security-best-practices/v/1.0.0/WAF.10	security-control/WAF.10
pci-dss/v/3.2.1/PCI.AutoScaling.1	セキュリティコントロール/AutoScaling.1
pci-dss/v/3.2.1/PCI.CloudTrail.1	セキュリティコントロール/CloudTrail.2
pci-dss/v/3.2.1/PCICloudTrail..2	セキュリティコントロール/CloudTrail.3
pci-dss/v/3.2.1/PCI.CloudTrail.3	セキュリティコントロール/CloudTrail.4
pci-dss/v/3.2.1/PCI.CloudTrail.4	セキュリティコントロール/CloudTrail.5
pci-dss/v/3.2.1/PCI.CodeBuild.1	セキュリティコントロール/CodeBuild.1
pci-dss/v/3.2.1/PCICodeBuild..2	セキュリティコントロール/CodeBuild.2
pci-dss/v/3.2.1/PCI.Config.1	security-control/Config.1
pci-dss/v/3.2.1/PCI.CW.1	セキュリティコントロール/CloudWatch.1

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
pci-dss/v/3.2.1/PCI.DMS.1	security-control/DMS.1
pci-dss/v/3.2.1/PCI.EC2.1	security-control/EC2.1
pci-dss/v/3.2.1/PCI.EC2.2	security-control/EC2.2
pci-dss/v/3.2.1/PCI.EC2.4	security-control/EC2.12
pci-dss/v/3.2.1/PCI.EC2.5	security-control/EC2.13
pci-dss/v/3.2.1/PCI.EC2.6	security-control/EC2.6
pci-dss/v/3.2.1/PCI.ELBv2.1	security-control/ELB.1
pci-dss/v/3.2.1/PCI.ES.1	security-control/ES.2
pci-dss/v/3.2.1/PCI.ES.2	security-control/ES.1
pci-dss/v/3.2.1/PCIGuardDuty..1	セキュリティコントロール/GuardDuty.1
pci-dss/v/3.2.1/PCI.IAM.1	security-control/IAM.4
pci-dss/v/3.2.1/PCI.IAM.2	security-control/IAM.2
pci-dss/v/3.2.1/PCI.IAM.3	security-control/IAM.1
pci-dss/v/3.2.1/PCI.IAM.4	security-control/IAM.6
pci-dss/v/3.2.1/PCI.IAM.5	security-control/IAM.9
pci-dss/v/3.2.1/PCI.IAM.6	security-control/IAM.19
pci-dss/v/3.2.1/PCI.IAM.7	security-control/IAM.8
pci-dss/v/3.2.1/PCI.IAM.8	security-control/IAM.10
pci-dss/v/3.2.1/PCI.KMS.1	security-control/KMS.4
pci-dss/v/3.2.1/PCI.Lambda.1	security-control/Lambda.1

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
pci-dss/v/3.2.1/PCI.Lambda.2	security-control/Lambda.3
pci-dss/v/3.2.1/PCI.Opensearch.1	security-control/Opensearch.2
pci-dss/v/3.2.1/PCI.Opensearch.2	security-control/Opensearch.1
pci-dss/v/3.2.1/PCI.RDS.1	security-control/RDS.1
pci-dss/v/3.2.1/PCI.RDS.2	security-control/RDS.2
pci-dss/v/3.2.1/PCI.Redshift.1	security-control/Redshift.1
pci-dss/v/3.2.1/PCI.S3.1	security-control/S3.3
pci-dss/v/3.2.1/PCI.S3.2	security-control/S3.2
pci-dss/v/3.2.1/PCI.S3.3	security-control/S3.7
pci-dss/v/3.2.1/PCI.S3.5	security-control/S3.5
pci-dss/v/3.2.1/PCI.S3.6	security-control/S3.1
pci-dss/v/3.2.1/PCISageMaker..1	セキュリティコントロール/SageMaker.1
pci-dss/v/3.2.1/PCI.SSM.1	security-control/SSM.2
pci-dss/v/3.2.1/PCI.SSM.2	security-control/SSM.3
pci-dss/v/3.2.1/PCI.SSM.3	security-control/SSM.1
service-managed-aws-control-tower/v/1.0.0/ACM.1	security-control/ACM.1
service-managed-aws-control-tower/v/1.0.0/APIGateway.1	security-control/APIGateway.1
service-managed-aws-control-tower/v/1.0.0/APIGateway.2	security-control/APIGateway.2

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/APIGateway.3	security-control/APIGateway.3
service-managed-aws-control-tower/v/1.0.0/APIGateway.4	security-control/APIGateway.4
service-managed-aws-control-tower/v/1.0.0/APIGateway.5	security-control/APIGateway.5
service-managed-aws-control-tower/v/1.0.0/AutoScaling.1	セキュリティコントロール/AutoScaling.1
service-managed-aws-control-tower/v/1.0.0/AutoScaling.2	セキュリティコントロール/AutoScaling.2
service-managed-aws-control-tower/v/1.0.0/AutoScaling.3	セキュリティコントロール/AutoScaling.3
service-managed-aws-control-tower/v/1.0.0/AutoScaling.4	セキュリティコントロール/AutoScaling.4
service-managed-aws-control-tower/v/1.0.0/Autoscaling.5	security-control/Autoscaling.5
service-managed-aws-control-tower/v/1.0.0/AutoScaling.6	セキュリティコントロール/AutoScaling.6
service-managed-aws-control-tower/v/1.0.0/AutoScaling.9	セキュリティコントロール/AutoScaling.9
service-managed-aws-control-tower/v/1.0.0/CloudTrail.1	セキュリティコントロール/CloudTrail.1
service-managed-aws-control-tower/v/1.0.0/CloudTrail.2	セキュリティコントロール/CloudTrail.2
service-managed-aws-control-tower/v/1.0.0/CloudTrail.4	セキュリティコントロール/CloudTrail.4

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/CloudTrail.5	セキュリティコントロール/CloudTrail.5
service-managed-aws-control-tower/v/1.0.0/CodeBuild.1	セキュリティコントロール/CodeBuild.1
service-managed-aws-control-tower/v/1.0.0/CodeBuild.2	セキュリティコントロール/CodeBuild.2
service-managed-aws-control-tower/v/1.0.0/CodeBuild.4	セキュリティコントロール/CodeBuild.4
service-managed-aws-control-tower/v/1.0.0/CodeBuild.5	セキュリティコントロール/CodeBuild.5
service-managed-aws-control-tower/v/1.0.0/DMS.1	security-control/DMS.1
service-managed-aws-control-tower/v/1.0.0/DynamoDB.1	security-control/DynamoDB.1
service-managed-aws-control-tower/v/1.0.0/DynamoDB.2	security-control/DynamoDB.2
service-managed-aws-control-tower/v/1.0.0/EC2.1	security-control/EC2.1
service-managed-aws-control-tower/v/1.0.0/EC2.2	security-control/EC2.2
service-managed-aws-control-tower/v/1.0.0/EC2.3	security-control/EC2.3
service-managed-aws-control-tower/v/1.0.0/EC2.4	security-control/EC2.4
service-managed-aws-control-tower/v/1.0.0/EC2.6	security-control/EC2.6

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/EC2.7	security-control/EC2.7
service-managed-aws-control-tower/v/1.0.0/EC2.8	security-control/EC2.8
service-managed-aws-control-tower/v/1.0.0/EC2.9	security-control/EC2.9
service-managed-aws-control-tower/v/1.0.0/EC2.10	security-control/EC2.10
service-managed-aws-control-tower/v/1.0.0/EC2.15	security-control/EC2.15
service-managed-aws-control-tower/v/1.0.0/EC2.16	security-control/EC2.16
service-managed-aws-control-tower/v/1.0.0/EC2.17	security-control/EC2.17
service-managed-aws-control-tower/v/1.0.0/EC2.18	security-control/EC2.18
service-managed-aws-control-tower/v/1.0.0/EC2.19	security-control/EC2.19
service-managed-aws-control-tower/v/1.0.0/EC2.20	security-control/EC2.20
service-managed-aws-control-tower/v/1.0.0/EC2.21	security-control/EC2.21
service-managed-aws-control-tower/v/1.0.0/EC2.22	security-control/EC2.22
service-managed-aws-control-tower/v/1.0.0/ECR.1	security-control/ECR.1

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/ECR.2	security-control/ECR.2
service-managed-aws-control-tower/v/1.0.0/ECR.3	security-control/ECR.3
service-managed-aws-control-tower/v/1.0.0/ECS.1	security-control/ECS.1
service-managed-aws-control-tower/v/1.0.0/ECS.2	security-control/ECS.2
service-managed-aws-control-tower/v/1.0.0/ECS.3	security-control/ECS.3
service-managed-aws-control-tower/v/1.0.0/ECS.4	security-control/ECS.4
service-managed-aws-control-tower/v/1.0.0/ECS.5	security-control/ECS.5
service-managed-aws-control-tower/v/1.0.0/ECS.8	security-control/ECS.8
service-managed-aws-control-tower/v/1.0.0/ECS.10	security-control/ECS.10
service-managed-aws-control-tower/v/1.0.0/ECS.12	security-control/ECS.12
service-managed-aws-control-tower/v/1.0.0/EFS .1	security-control/EFS.1
service-managed-aws-control-tower/v/1.0.0/EFS .2	security-control/EFS.2
service-managed-aws-control-tower/v/1.0.0/EFS .3	security-control/EFS.3

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/EFS .4	security-control/EFS.4
service-managed-aws-control-tower/v/1.0.0/EKS.2	security-control/EKS.2
service-managed-aws-control-tower/v/1.0.0/ELB.2	security-control/ELB.2
service-managed-aws-control-tower/v/1.0.0/ELB.3	security-control/ELB.3
service-managed-aws-control-tower/v/1.0.0/ELB.4	security-control/ELB.4
service-managed-aws-control-tower/v/1.0.0/ELB.5	security-control/ELB.5
service-managed-aws-control-tower/v/1.0.0/ELB.6	security-control/ELB.6
service-managed-aws-control-tower/v/1.0.0/ELB.7	security-control/ELB.7
service-managed-aws-control-tower/v/1.0.0/ELB.8	security-control/ELB.8
service-managed-aws-control-tower/v/1.0.0/ELB.9	security-control/ELB.9
service-managed-aws-control-tower/v/1.0.0/ELB.10	security-control/ELB.10
service-managed-aws-control-tower/v/1.0.0/ELB.12	security-control/ELB.12
service-managed-aws-control-tower/v/1.0.0/ELB.13	security-control/ELB.13

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/ELB.14	security-control/ELB.14
service-managed-aws-control-tower/v/1.0.0/ELBv2.1	security-control/ELBv2.1
service-managed-aws-control-tower/v/1.0.0/EMR.1	security-control/EMR.1
service-managed-aws-control-tower/v/1.0.0/ES.1	security-control/ES.1
service-managed-aws-control-tower/v/1.0.0/ES.2	security-control/ES.2
service-managed-aws-control-tower/v/1.0.0/ES.3	security-control/ES.3
service-managed-aws-control-tower/v/1.0.0/ES.4	security-control/ES.4
service-managed-aws-control-tower/v/1.0.0/ES.5	security-control/ES.5
service-managed-aws-control-tower/v/1.0.0/ES.6	security-control/ES.6
service-managed-aws-control-tower/v/1.0.0/ES.7	security-control/ES.7
service-managed-aws-control-tower/v/1.0.0/ES.8	security-control/ES.8
service-managed-aws-control-tower/v/1.0.0/ElasticBeanstalk.1	セキュリティコントロール/ElasticBeanstalk.1
service-managed-aws-control-tower/v/1.0.0/ElasticBeanstalk.2	セキュリティコントロール/ElasticBeanstalk.2

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/GuardDuty.1	セキュリティコントロール/GuardDuty.1
service-managed-aws-control-tower/v/1.0.0/IAM.1	security-control/IAM.1
service-managed-aws-control-tower/v/1.0.0/IAM.2	security-control/IAM.2
service-managed-aws-control-tower/v/1.0.0/IAM.3	security-control/IAM.3
service-managed-aws-control-tower/v/1.0.0/IAM.4	security-control/IAM.4
service-managed-aws-control-tower/v/1.0.0/IAM.5	security-control/IAM.5
service-managed-aws-control-tower/v/1.0.0/IAM.6	security-control/IAM.6
service-managed-aws-control-tower/v/1.0.0/IAM.7	security-control/IAM.7
service-managed-aws-control-tower/v/1.0.0/IAM.8	security-control/IAM.8
service-managed-aws-control-tower/v/1.0.0/IAM.21	security-control/IAM.21
service-managed-aws-control-tower/v/1.0.0/Kinesis.1	security-control/Kinesis.1
service-managed-aws-control-tower/v/1.0.0/KMS.1	security-control/KMS.1
service-managed-aws-control-tower/v/1.0.0/KMS.2	security-control/KMS.2

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/KMS.3	security-control/KMS.3
service-managed-aws-control-tower/v/1.0.0/Lambda.1	security-control/Lambda.1
service-managed-aws-control-tower/v/1.0.0/Lambda.2	security-control/Lambda.2
service-managed-aws-control-tower/v/1.0.0/Lambda.5	security-control/Lambda.5
service-managed-aws-control-tower/v/1.0.0/NetworkFirewall.3	セキュリティコントロール/NetworkFirewall.3
service-managed-aws-control-tower/v/1.0.0/NetworkFirewall.4	セキュリティコントロール/NetworkFirewall.4
service-managed-aws-control-tower/v/1.0.0/NetworkFirewall.5	セキュリティコントロール/NetworkFirewall.5
service-managed-aws-control-tower/v/1.0.0/NetworkFirewall.6	セキュリティコントロール/NetworkFirewall.6
service-managed-aws-control-tower/v/1.0.0/Opensearch.1	security-control/Opensearch.1
service-managed-aws-control-tower/v/1.0.0/Opensearch.2	security-control/Opensearch.2
service-managed-aws-control-tower/v/1.0.0/Opensearch.3	security-control/Opensearch.3
service-managed-aws-control-tower/v/1.0.0/Opensearch.4	security-control/Opensearch.4
service-managed-aws-control-tower/v/1.0.0/Opensearch.5	security-control/Opensearch.5

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/Opensearch.6	security-control/Opensearch.6
service-managed-aws-control-tower/v/1.0.0/Opensearch.7	security-control/Opensearch.7
service-managed-aws-control-tower/v/1.0.0/Opensearch.8	security-control/Opensearch.8
service-managed-aws-control-tower/v/1.0.0/RDS.1	security-control/RDS.1
service-managed-aws-control-tower/v/1.0.0/RDS.2	security-control/RDS.2
service-managed-aws-control-tower/v/1.0.0/RDS.3	security-control/RDS.3
service-managed-aws-control-tower/v/1.0.0/RDS.4	security-control/RDS.4
service-managed-aws-control-tower/v/1.0.0/RDS.5	security-control/RDS.5
service-managed-aws-control-tower/v/1.0.0/RDS.6	security-control/RDS.6
service-managed-aws-control-tower/v/1.0.0/RDS.8	security-control/RDS.8
service-managed-aws-control-tower/v/1.0.0/RDS.9	security-control/RDS.9
service-managed-aws-control-tower/v/1.0.0/RDS.10	security-control/RDS.10
service-managed-aws-control-tower/v/1.0.0/RDS.11	security-control/RDS.11

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/RDS.13	security-control/RDS.13
service-managed-aws-control-tower/v/1.0.0/RDS.17	security-control/RDS.17
service-managed-aws-control-tower/v/1.0.0/RDS.18	security-control/RDS.18
service-managed-aws-control-tower/v/1.0.0/RDS.19	security-control/RDS.19
service-managed-aws-control-tower/v/1.0.0/RDS.20	security-control/RDS.20
service-managed-aws-control-tower/v/1.0.0/RDS.21	security-control/RDS.21
service-managed-aws-control-tower/v/1.0.0/RDS.22	security-control/RDS.22
service-managed-aws-control-tower/v/1.0.0/RDS.23	security-control/RDS.23
service-managed-aws-control-tower/v/1.0.0/RDS.25	security-control/RDS.25
service-managed-aws-control-tower/v/1.0.0/Redshift.1	security-control/Redshift.1
service-managed-aws-control-tower/v/1.0.0/Redshift.2	security-control/Redshift.2
service-managed-aws-control-tower/v/1.0.0/Redshift.4	security-control/Redshift.4
service-managed-aws-control-tower/v/1.0.0/Redshift.6	security-control/Redshift.6

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/Redshift.7	security-control/Redshift.7
service-managed-aws-control-tower/v/1.0.0/Redshift.8	security-control/Redshift.8
service-managed-aws-control-tower/v/1.0.0/Redshift.9	security-control/Redshift.9
service-managed-aws-control-tower/v/1.0.0/S3.1	security-control/S3.1
service-managed-aws-control-tower/v/1.0.0/S3.2	security-control/S3.2
service-managed-aws-control-tower/v/1.0.0/S3.3	security-control/S3.3
service-managed-aws-control-tower/v/1.0.0/S3.5	security-control/S3.5
service-managed-aws-control-tower/v/1.0.0/S3.6	security-control/S3.6
service-managed-aws-control-tower/v/1.0.0/S3.8	security-control/S3.8
service-managed-aws-control-tower/v/1.0.0/S3.9	security-control/S3.9
service-managed-aws-control-tower/v/1.0.0/S3.12	security-control/S3.12
service-managed-aws-control-tower/v/1.0.0/S3.13	security-control/S3.13
service-managed-aws-control-tower/v/1.0.0/SageMaker.1	セキュリティコントロール/SageMaker.1

統合統制結果をオンにする前の GeneratorID	統合統制結果をオンにした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/SecretsManager.1	セキュリティコントロール/SecretsManager.1
service-managed-aws-control-tower/v/1.0.0/SecretsManager.2	セキュリティコントロール/SecretsManager.2
service-managed-aws-control-tower/v/1.0.0/SecretsManager.3	セキュリティコントロール/SecretsManager.3
service-managed-aws-control-tower/v/1.0.0/SecretsManager.4	セキュリティコントロール/SecretsManager.4
service-managed-aws-control-tower/v/1.0.0/SQS.1	security-control/SQS.1
service-managed-aws-control-tower/v/1.0.0/SSM.1	security-control/SSM.1
service-managed-aws-control-tower/v/1.0.0/SSM.2	security-control/SSM.2
service-managed-aws-control-tower/v/1.0.0/SSM.3	security-control/SSM.3
service-managed-aws-control-tower/v/1.0.0/SSM.4	security-control/SSM.4
service-managed-aws-control-tower/v/1.0.0/WAF.2	security-control/WAF.2
service-managed-aws-control-tower/v/1.0.0/WAF.3	security-control/WAF.3
service-managed-aws-control-tower/v/1.0.0/WAF.4	security-control/WAF.4

統合がコントロール ID とタイトルに与える影響

統合されたコントロールビューと統合されたコントロールの検出結果は、コントロール ID とタイトルを標準間で標準化します。セキュリティコントロール ID とセキュリティコントロールタイトルという用語は、これらの標準にとらわれない値を指します。次の表に、セキュリティコントロール ID とタイトルを標準固有のコントロール ID とタイトルにマッピングする方法について示します。AWS Foundational Security Best Practices (FSBP) 標準に属するコントロールの IDs とタイトルが変更されていません。

Security Hub コンソールには、統合統制結果がアカウントで有効または無効になっているかどうかにかかわらず、標準に依存しないセキュリティ統制 IDs とセキュリティ統制タイトルが表示されます。ただし、アカウントで統合統制結果が無効になっている場合、Security Hub の検出結果には標準固有の統制タイトル (PCI および CIS v1.2.0 の場合) が含まれます。アカウントで統合コントロールの検出結果がオフになっている場合、Security Hub の検出結果には標準固有のコントロール ID とセキュリティコントロール ID が含まれます。統合がコントロール検出結果に与える影響の詳細については、「コントロールの検出結果のサンプル」を参照してください。

サービスマネージドスタンダード: の一部であるコントロールの場合 AWS Control Tower、統合コントロールの検出結果が有効になっていると、検出結果のコントロール ID とタイトルからプレフィックスがCT.削除されます。

このテーブルで独自のスクリプトを実行するには、.csv ファイルとしてダウンロードしてください。

標準	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.2.0	1.1 ルートユーザーの使用を避ける	〔CloudWatch.1〕「ルート」ユーザーの使用に対してログメトリクスフィルターとアラームが存在する必要があります
CIS v1.2.0	1.10 IAM パスワードポリシーでパスワードの再使用を防止していることを確認する	[IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています
CIS v1.2.0	1.11 IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認する	[IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します

標準	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.2.0	1.12 ルートユーザーのアクセスキーが存在しないことを確認する	[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
CIS v1.2.0	1.13 MFA がルートユーザーで有効になっていることを確認する	[IAM.9] ルートユーザーに対して MFA を有効にする必要があります
CIS v1.2.0	1.14 ハードウェア MFA がルートユーザーで有効になっていることを確認する	[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
CIS v1.2.0	1.16 IAM ポリシーがグループまたはロールだけにアタッチされていることを確認する	[IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
CIS v1.2.0	1.2 コンソールパスワードを持つすべての IAM ユーザーに対して多要素認証 (MFA) が有効であることを確認する	[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
CIS v1.2.0	1.20 でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support	[IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support
CIS v1.2.0	1.22 完全な「*:*」管理者権限を許可する IAM ポリシーが作成されていないことを確認する	[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
CIS v1.2.0	1.3 90 日間以上使用されていない認証情報は無効にします。	[IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
CIS v1.2.0	1.4 アクセスキーは 90 日ごとに更新します。	[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります

標準	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.2.0	1.5 IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認する	[IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します
CIS v1.2.0	1.6 IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認する	[IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します
CIS v1.2.0	1.7 IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認する	[IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します
CIS v1.2.0	1.8 IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認する	[IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します
CIS v1.2.0	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する	[IAM.15] 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します
CIS v1.2.0	2.1 すべてのリージョンで CloudTrail が有効になっていることを確認する	〔CloudTrail.1] CloudTrail 読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン追跡を有効にして設定する必要があります
CIS v1.2.0	2.2 CloudTrail ログファイルの検証が有効になっていることを確認する	〔CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります
CIS v1.2.0	2.3 CloudTrail ログの保存に使用される S3 バケットがパブリックにアクセスできないようにする	〔CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットがパブリックにアクセスできないようにする

標準	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.2.0	2.4 CloudTrail 証跡が CloudWatch ログと統合されていることを確認する	〔CloudTrail.5] CloudTrail 証跡は Amazon CloudWatch Logs と統合する必要があります
CIS v1.2.0	2.5 AWS Config が有効になっていることを確認する	[Config.1] AWS Config を有効にし、サービスにリンクされたロールをリソース記録に使用する必要があります
CIS v1.2.0	2.6 S3 バケットで CloudTrail S3 バケットアクセスログ記録が有効になっていることを確認する	〔CloudTrail.7] S3 バケットで CloudTrail S3 バケットアクセスログ記録が有効になっていることを確認する
CIS v1.2.0	2.7 CloudTrail ログが KMS CMKs	〔CloudTrail.2] 保管時の暗号化を有効にする CloudTrail 必要があります
CIS v1.2.0	2.8 カスタマー作成の CMK のローテーションが有効になっていることを確認します	[KMS.4] AWS KMS キーローテーションを有効にする必要があります
CIS v1.2.0	2.9 すべての VPC で VPC フローログ記録が有効になっていることを確認します	[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします
CIS v1.2.0	3.1 不正な API 呼び出しに対してログメトリクスフィルターとアラームが存在することを確認します	〔CloudWatch.2] 不正な API コールに対してログメトリクスフィルターとアラームが存在することを確認する
CIS v1.2.0	3.10 セキュリティグループの変更に対するメトリクスフィルターとアラームが存在することを確認します	〔CloudWatch.10] セキュリティグループの変更に対するログメトリクスフィルターとアラームが存在することを確認する

標準	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.2.0	3.11 ネットワークアクセスコントロールリスト (NACL) への変更に対するログメトリクスとアラームが存在することを確認します	〔CloudWatch.11] ネットワークアクセスコントロールリスト (NACL) の変更に対するログメトリクスフィルターとアラームが存在することを確認する
CIS v1.2.0	3.12 ネットワークゲートウェイへの変更に対するログメトリクスとアラームが存在することを確認します	〔CloudWatch.12] ネットワークゲートウェイの変更に対するログメトリクスフィルターとアラームが存在することを確認する
CIS v1.2.0	3.13 ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認します	〔CloudWatch.13] ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認する
CIS v1.2.0	3.14 VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認します	〔CloudWatch.14] VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認する
CIS v1.2.0	3.2 MFA を使用しないマネジメントコンソールサインインに対してログメトリックフィルターとアラームが存在することを確認する	〔CloudWatch.3] MFA を使用しない マネジメントコンソールサインインのログメトリクスフィルターとアラームが存在することを確認する
CIS v1.2.0	3.3 ルートユーザーに使用するログメトリックフィルターとアラームが存在することを確認する	〔CloudWatch.1]「ルート」ユーザーの使用に対してログメトリクスフィルターとアラームが存在する必要があります
CIS v1.2.0	3.4 IAM ポリシーの変更に対するログメトリックフィルターとアラームが存在することを確認する	〔CloudWatch.4] IAM ポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認する

標準	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.2.0	3.5 CloudTrail 設定変更のログメトリクスフィルターとアラームが存在することを確認する	〔CloudWatch.5] CloudTrail AWS Configログメトリクスフィルターとアラームが設定変更用に存在することを確認する
CIS v1.2.0	3.6 AWS Management Console 認証の失敗に対してログメトリクスフィルターとアラームが存在することを確認する	〔CloudWatch.6] AWS Management Console 認証の失敗に対してログメトリクスフィルターとアラームが存在することを確認する
CIS v1.2.0	3.7 カスタマー作成の CMK の無効化またはスケジュールされた削除に対してログメトリクスフィルターとアラームが存在することを確認します	〔CloudWatch.7] カスタマーマネージドキーの無効化またはスケジュールされた削除のためのログメトリクスフィルターとアラームが存在することを確認する
CIS v1.2.0	3.8 S3 バケットの変更に対してログメトリクスフィルターとアラームが存在することを確認します	〔CloudWatch.8] S3 バケットポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認する
CIS v1.2.0	3.9 AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する	〔CloudWatch.9] AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する
CIS v1.2.0	4.1 どのセキュリティグループでも 0.0.0.0/0 からポート 22 への入力を許可しないようにします	[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります
CIS v1.2.0	4.2 どのセキュリティグループでも 0.0.0.0/0 からポート 3389 への入力を許可しないようにします	[EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります

標準	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.2.0	4.3 すべての VPC のデフォルトセキュリティグループがすべてのトラフィックを制限するようにします。	[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします
CIS v1.4.0	1.10 コンソールパスワードを持つすべての IAM ユーザーに対して多要素認証 (MFA) が有効であることを確認する	[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
CIS v1.4.0	1.14 アクセスキーは 90 日以内ごとに更新されているのを確認する	[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
CIS v1.4.0	1.16 完全な「*:*」管理権限を許可する IAM ポリシーがアタッチされていないことを確認する	[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
CIS v1.4.0	1.17 でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support	[IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support
CIS v1.4.0	1.4 ルートユーザーアカウントのアクセスキーが存在しないことを確認する	[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
CIS v1.4.0	1.5 ルートユーザーアカウントで MFA が有効であることを確認する	[IAM.9] ルートユーザーに対して MFA を有効にする必要があります
CIS v1.4.0	1.6 ルートユーザーアカウントでハードウェア MFA が有効であることを確認する	[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります

標準	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.4.0	1.7 管理および日常のタスクでのルートユーザーの使用を排除する	〔CloudWatch.1〕「ルート」ユーザーの使用に対してログメトリクスフィルターとアラームが存在する必要があります
CIS v1.4.0	1.8 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する	[IAM.15] 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します
CIS v1.4.0	1.9 IAM パスワードポリシーでパスワードの再使用を防止していることを確認する	[IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています
CIS v1.4.0	2.1.2 S3 バケットポリシーが HTTP リクエストを拒否するように設定されていることを確認する	[S3.5] S3 汎用バケットでは、SSL を使用するリクエストが必要です
CIS v1.4.0	2.1.5.1 S3 ブロックパブリックアクセス設定を有効にする必要があります	[S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります
CIS v1.4.0	2.1.5.2 S3 ブロックパブリックアクセス設定は、バケットレベルで有効にする必要があります	[S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります
CIS v1.4.0	2.2.1 EBS ボリュームの暗号化が有効であることを確認する	[EC2.7] EBS のデフォルト暗号化を有効にすることをお勧めします
CIS v1.4.0	2.3.1 RDS インスタンスで暗号化が有効であることを確認する	[RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。

標準	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.4.0	3.1 すべてのリージョンで CloudTrail が有効になっていることを確認する	〔CloudTrail.1] CloudTrail 読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン追跡を有効にして設定する必要があります
CIS v1.4.0	3.2 CloudTrail ログファイルの検証が有効になっていることを確認する	〔CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります
CIS v1.4.0	3.4 CloudTrail 証跡が CloudWatch ログと統合されていることを確認する	〔CloudTrail.5] CloudTrail 証跡は Amazon CloudWatch Logs と統合する必要があります
CIS v1.4.0	3.5 すべてのリージョンで AWS Config が有効になっていることを確認する	[Config.1] AWS Config を有効にし、サービスにリンクされたロールをリソース記録に使用する必要があります
CIS v1.4.0	3.6 S3 バケットで CloudTrail S3 バケットアクセスログ記録が有効になっていることを確認する	〔CloudTrail.7] S3 バケットで CloudTrail S3 バケットアクセスログ記録が有効になっていることを確認する
CIS v1.4.0	3.7 CloudTrail ログが KMS CMKs	〔CloudTrail.2] 保管時の暗号化を有効にする CloudTrail 必要があります
CIS v1.4.0	3.8 カスタマー作成の CMK のローテーションが有効になっていることを確認する	[KMS.4] AWS KMS キーローテーションを有効にする必要があります
CIS v1.4.0	3.9 すべての VPC で VPC フローログ記録が有効になっていることを確認する	[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします

標準	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.4.0	4.4 IAM ポリシーの変更に対するログメトリックフィルターとアラームが存在することを確認する	〔CloudWatch.4] IAM ポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認する
CIS v1.4.0	4.5 CloudTrail 設定変更のログメトリクスフィルターとアラームが存在することを確認する	〔CloudWatch.5] CloudTrail AWS Configログメトリクスフィルターとアラームが設定変更用に存在することを確認する
CIS v1.4.0	4.6 AWS Management Console 認証の失敗に対してログメトリクスフィルターとアラームが存在することを確認する	〔CloudWatch.6] AWS Management Console 認証の失敗に対してログメトリクスフィルターとアラームが存在することを確認する
CIS v1.4.0	4.7 カスタマー作成の CMK の無効化またはスケジュールされた削除に対してログメトリックフィルターとアラームが存在することを確認する	〔CloudWatch.7] カスタマーマネージドキーの無効化またはスケジュールされた削除のためのログメトリクスフィルターとアラームが存在することを確認する
CIS v1.4.0	4.8 S3 バケットの変更に対してログメトリックフィルターとアラームが存在することを確認する	〔CloudWatch.8] S3 バケットポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認する
CIS v1.4.0	4.9 AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する	〔CloudWatch.9] AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する
CIS v1.4.0	4.10 セキュリティグループの変更に対するログメトリックフィルターとアラームが存在することを確認する	〔CloudWatch.10] セキュリティグループの変更に対するログメトリクスフィルターとアラームが存在することを確認する

標準	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.4.0	4.11 ネットワークアクセスコントロールリスト (NACL) への変更に対するログメトリックフィルターとアラームが存在することを確認する	〔CloudWatch.11] ネットワークアクセスコントロールリスト (NACL) の変更に対するログメトリクスフィルターとアラームが存在することを確認する
CIS v1.4.0	4.12 ネットワークゲートウェイへの変更に対するログメトリックフィルターとアラームが存在することを確認する	〔CloudWatch.12] ネットワークゲートウェイの変更に対するログメトリクスフィルターとアラームが存在することを確認する
CIS v1.4.0	4.13 ルートテーブルの変更に対してログメトリックフィルターとアラームが存在することを確認する	〔CloudWatch.13] ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認する
CIS v1.4.0	4.14 VPC の変更に対してログメトリックフィルターとアラームが存在することを確認する	〔CloudWatch.14] VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認する
CIS v1.4.0	5.1 ネットワーク ACL が 0.0.0.0/0 からリモートサーバー管理ポートへの侵入を許可していないことを確認する	[EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります
CIS v1.4.0	5.3 すべての VPC のデフォルトセキュリティグループがすべてのトラフィックを制限するようにします	[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします

標準	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
PCI DSS v3.2.1	PCI.AutoScaling.1 ロードバランサーに関連付けられた Auto Scaling グループは、ロードバランサーのヘルスチェックを使用する必要があります	〔AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要があります
PCI DSS v3.2.1	PCI.CloudTrail.1 CloudTrail logs は、AWS KMS CMKs を使用して保管時に暗号化する必要があります	〔CloudTrail.2] 保管時の暗号化を有効にする CloudTrail 必要があります
PCI DSS v3.2.1	PCI.CloudTrail.2 CloudTrail を有効にする必要があります	〔CloudTrail.3] 少なくとも 1 つの CloudTrail 証跡を有効にする必要があります
PCI DSS v3.2.1	PCI.CloudTrail.3 CloudTrail ログファイルの検証を有効にする必要があります	〔CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります
PCI DSS v3.2.1	PCI.CloudTrail.4 CloudTrail trails は Amazon CloudWatch Logs と統合する必要があります	〔CloudTrail.5] CloudTrail 証跡は Amazon CloudWatch Logs と統合する必要があります
PCI DSS v3.2.1	PCI.CodeBuild.1 CodeBuild GitHub または Bitbucket ソースリポジトリ URLs は OAuth を使用する必要があります	〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください
PCI DSS v3.2.1	PCI.CodeBuild.2 CodeBuild project 環境変数にはクリアテキスト認証情報を含めないでください	〔CodeBuild.2] CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください
PCI DSS v3.2.1	PCI.Config.1 AWS Config を有効にする必要があります	[Config.1] AWS Config を有効にし、サービスにリンクされたロールをリソース記録に使用する必要があります

標準	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
PCI DSS v3.2.1	PCI.CW.1「ルート」ユーザーの使用に対するログメトリックフィルターとアラームが存在する必要があります	〔CloudWatch.1]「ルート」ユーザーの使用に対してログメトリクスフィルターとアラームが存在する必要があります
PCI DSS v3.2.1	PCI.DMS.1 Database Migration Service のレプリケーションインスタンスはパブリックではない必要があります	[DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります
PCI DSS v3.2.1	PCI.EC2.1 EBS スナップショットをパブリックに復元可能であってはなりません	[EC2.1] Amazon EBS スナップショットはパブリックに復元できないようにすることをお勧めします
PCI DSS v3.2.1	PCI.EC2.2 VPC のデフォルトのセキュリティグループで、インバウンドトラフィックとアウトバウンドトラフィックを禁止する必要があります	[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします
PCI DSS v3.2.1	PCI.EC2.4 未使用の EC2 EIP を削除する必要があります	[EC2.12] 未使用の Amazon EC2 EIP を削除することをお勧めします
PCI DSS v3.2.1	PCI.EC2.5 セキュリティグループは、0.0.0.0/0 からポート 22 への入力を許可しないようにする必要があります	[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります
PCI DSS v3.2.1	PCI.EC2.6 VPC フローログ記録をすべての VPC で有効にする必要があります	[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします

標準	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
PCI DSS v3.2.1	PCI.ELBV2.1 Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります	[ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります
PCI DSS v3.2.1	PCI.ES.1 Elasticsearch ドメインは VPC 内に存在する必要があります	[ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります
PCI DSS v3.2.1	PCI.ES.2 Elasticsearch ドメインで保管中の暗号化を有効にする必要があります	[ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります
PCI DSS v3.2.1	PCI.GuardDuty.1 GuardDuty を有効にする必要があります	〔GuardDuty.1] GuardDuty を有効にする必要があります
PCI DSS v3.2.1	PCI.IAM.1 IAM ルートユーザーのアクセスキーが存在していてはなりません	[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
PCI DSS v3.2.1	PCI.IAM.2 IAM ユーザーには IAM ポリシーをアタッチしてはなりません	[IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
PCI DSS v3.2.1	PCI.IAM.3 IAM ポリシーで、完全な「*」管理者権限を許可してはなりません	[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
PCI DSS v3.2.1	PCI.IAM.4 ルートユーザーに対してハードウェア MFA を有効にする必要があります	[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
PCI DSS v3.2.1	PCI.IAM.5 ルートユーザーに対して仮想 MFA を有効にする必要があります	[IAM.9] ルートユーザーに対して MFA を有効にする必要があります

標準	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
PCI DSS v3.2.1	PCI.IAM.6 すべての IAM ユーザーに対して MFA を有効にする必要があります	[IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
PCI DSS v3.2.1	PCI.IAM.7 IAM ユーザー認証情報が事前定義された日数以内に使用されない場合、認証情報を無効にする必要があります	[IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
PCI DSS v3.2.1	PCI.IAM.8 IAM ユーザーのパスワードポリシーには強力な設定が必要です	[IAM.10] IAM ユーザーのパスワードポリシーには強力な AWS Config設定が必要です
PCI DSS v3.2.1	PCI.KMS.1 カスタマーマスターキー (CMK) ローテーションを有効にする必要があります	[KMS.4] AWS KMS キーローテーションを有効にする必要があります
PCI DSS v3.2.1	PCI.Lambda.1 Lambda 関数は、パブリックアクセスを禁止する必要があります	[Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります
PCI DSS v3.2.1	PCI.Lambda.2 Lambda 関数は VPC 内に存在する必要があります	[Lambda.3] Lambda 関数は VPC 内に存在する必要があります
PCI DSS v3.2.1	PCI.Opensearch.1 OpenSearch ドメインは VPC 内にある必要があります	[Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません
PCI DSS v3.2.1	PCI.Opensearch.2 EBS スナップショットをパブリックに復元可能であってはなりません	[Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります
PCI DSS v3.2.1	PCI.RDS.1 RDS スナップショットはプライベートである必要があります	[RDS.1] RDS スナップショットはプライベートである必要があります

標準	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
PCI DSS v3.2.1	PCI.RDS.2 RDS DB インスタンスでパブリックアクセスを禁止する必要があります	[RDS.2] RDS DB インスタンスは、PubliclyAccessible AWS Config設定によって決定されるパブリックアクセスを禁止する必要があります
PCI DSS v3.2.1	PCI.Redshift.1 Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります	[PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります
PCI DSS v3.2.1	PCI.S3.1 S3 バケットはパブリック書き込みアクセスを禁止する必要があります	[S3.3] S3 汎用バケットはパブリック書き込みアクセスをブロックする必要があります
PCI DSS v3.2.1	PCI.S3.2 S3 バケットではパブリック読み取りアクセスを禁止する必要があります	[S3.2] S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります
PCI DSS v3.2.1	PCI.S3.3 S3 バケットでクロスリージョンレプリケーションを有効にする必要があります	[S3.7] S3 汎用バケットはクロスリージョンレプリケーションを使用する必要があります
PCI DSS v3.2.1	PCI.S3.5 S3 バケットは Secure Socket Layer を使用するリクエストを要求する必要があります	[S3.5] S3 汎用バケットでは、SSL を使用するリクエストが必要です
PCI DSS v3.2.1	PCI.S3.6 S3 パブリックアクセスブロック設定を有効にする必要があります	[S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります
PCI DSS v3.2.1	PCI.SageMaker.1 Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません	〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません

標準	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
PCI DSS v3.2.1	PCI.SSM.1 Systems Manager によって管理される EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります	[SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
PCI DSS v3.2.1	PCI.SSM.2 Systems Manager によって管理される EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります	[SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
PCI DSS v3.2.1	PCI.SSM.3 EC2 インスタンスは によって管理する必要があります AWS Systems Manager	[SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager

統合に向けたワークフローの更新

ワークフローが統制結果フィールドの特定の形式に依存していない場合は、何もする必要はありません。

ワークフローが表に記載されているコントロール結果フィールドの特定形式に依存している場合は、ワークフローを更新する必要があります。例えば、特定のコントロール ID のアクションをトリガーする Amazon CloudWatch Events ルールを作成した場合 (コントロール ID が CIS 2.7 と等しい場合は AWS Lambda 関数を呼び出すなど)、そのコントロールの `Compliance.SecurityControlId`フィールドである CloudTrail.2 を使用するようにルールを更新します。

変更されたコントロール検出結果フィールドまたは値のいずれかを使用してカスタムインサイトを作成した場合は、現在のフィールドまたは値を使用するようにインサイトを更新します。

ASFF の例

以下のセクションでは、 AWS Security Finding 形式 (ASFF) の必須属性とオプション属性の例と、ASFF がサポートする各リソースの例を示します。

トピック

必須の最上位属性

Security Hub のすべての検出結果には、 AWS Security Finding 形式 (ASFF) の次の最上位属性が必要です。これらの必須属性の詳細については、「AWS Security Hub API リファレンス」の「AwsSecurityFinding」を参照してください。

AwsAccountId

検出結果が適用される AWS アカウント ID。

例

```
"AwsAccountId": "111111111111"
```

CreatedAt

結果によってキャプチャされた潜在的なセキュリティ問題がいつ作成されたかを示します。

例

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

> **Note**
>
> Security Hub では、結果は、最新の更新から 90 日後、または更新が行われない場合は作成日から 90 日後に削除されます。検出結果を 90 日以上保存するには、Amazon で検出結果を S3 バケットにルーティング EventBridge するルールを設定できます。

説明

結果の説明。このフィールドには、固有ではない定型テキスト、または結果のインスタンスに固有の詳細を指定できます。

Security Hub が生成するコントロール検出結果の場合、このフィールドにはコントロールの説明が表示されます。

[統合されたコントロールの検出結果] を有効にした場合、このフィールドは標準を参照しません。

例

```
"Description": "This AWS control checks whether AWS Config is enabled in the current
 account and Region."
```

GeneratorId

結果を生成したソリューションに固有のコンポーネント (個別のロジック単位) の識別子。

Security Hub が生成するコントロールの検出結果について、[統合されたコントロールの検出結果] を有効にした場合、このフィールドは標準を参照しません。

例

```
"GeneratorId": "security-control/Config.1"
```

ID

結果の製品に固有の識別子。Security Hub が生成するコントロール検出結果の場合、このフィールドには検出結果の Amazon リソースネーム (ARN) が表示されます。

[統合されたコントロールの検出結果] を有効にした場合、このフィールドは標準を参照しません。

例

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/
ab6d6a26-a156-48f0-9403-115983e5a956

"
```

ProductArn

サードパーティーの検出製品が Security Hub に登録された後に、その製品を一意に識別するための Security Hub によって生成された Amazon リソースネーム (ARN)。

このフィールドの形式は `arn:`*`partition`*`:securityhub:`*`region`*`:`*`account-id`*`:product/`*`company-id`*`/`*`product-id` です。

- Security Hub と統合されている AWS サービスcompany-idの場合、 はaws「」で、 は AWS パブリックサービス名product-idである必要があります。 AWS 製品およびサービスはアカウントに関連付けられていないため、ARN の account-idセクションは空です。Security Hub とまだ統合されていない AWS サービスはサードパーティー製品と見なされます。
- パブリック製品の場合、company-id および product-id は登録時に指定された ID 値である必要があります。
- プライベート製品の場合、company-id はアカウント ID である必要があります。product-id は、予約語の "default"、または登録時に指定された ID である必要があります。

例

```
// Private ARN
    "ProductArn": "arn:aws:securityhub:us-east-1:111111111111:product/111111111111/
default"

// Public ARN

    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty"
    "ProductArn": "arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-
pro"
```

リソース

Resources オブジェクトは、検出結果が参照するリソースを記述する一連の AWS リソースデータ型を提供します。

例

```
"Resources": [
  {
    "ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0",
```

```
    "ApplicationName": "SampleApp",
    "DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
                        }
                    },
                    {
                        "Count": 59,
                        "Type": "EMAIL_ADDRESS",
                        "Occurrences": {
                            "Pages": [
                                {
                                    "PageNumber": 1,
                                    "OffsetRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                     },
                                    "LineRange": {
```

```
                                    "Start": 1,
                                    "End": 100,
                                    "StartColumn": 10
                                }
                            }
                        ]
                    }
                },
                {
                    "Count": 2229,
                    "Type": "URL",
                    "Occurrences": {
                       "LineRanges": [
                           {
                               "Start": 1,
                               "End": 13
                           }
                       ]
                    }
                },
                {
                    "Count": 13826,
                    "Type": "NameDetection",
                    "Occurrences": {
                        "Records": [
                            {
                                "RecordIndex": 1,
                                "JsonPath": "$.ssn.value"
                            }
                        ]
                    }
                },
                {
                    "Count": 32,
                    "Type": "AddressDetection"
                }
            ],
            "TotalCount": 32
        }
    ],
    "CustomDataIdentifiers": {
        "Detections": [
            {
                "Arn": "1712be25e7c7f53c731fe464f1c869b8",
```

```
                    "Name": "1712be25e7c7f53c731fe464f1c869b8",
                    "Count": 2,
                }
            ],
            "TotalCount": 2
        }
    }
},
 "Type": "AwsEc2Instance",
 "Id": "arn:aws:ec2:us-west-2:123456789012:instance/i-abcdef01234567890",
 "Partition": "aws",
 "Region": "us-west-2",
 "ResourceRole": "Target",
 "Tags": {
  "billingCode": "Lotus-1-2-3",
  "needsPatching": true
 },
 "Details": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
  "ImageId": "ami-79fd7eee",
  "IpV4Addresses": ["1.1.1.1"],
  "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
  "KeyName": "testkey",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "MetadataOptions": {
   "HttpEndpoint": "enabled",
   "HttpProtocolIpv6": "enabled",
   "HttpPutResponseHopLimit": 1,
   "HttpTokens": "optional",
   "InstanceMetadataTags": "disabled"
  }
 },
  "NetworkInterfaces": [
  {
   "NetworkInterfaceId": "eni-e5aa89a3"
  }
  ],
  "SubnetId": "PublicSubnet",
  "Type": "i3.xlarge",
  "VirtualizationType": "hvm",
  "VpcId": "TestVPCIpv6"
 }
```

```
]
```

SchemaVersion

結果に使用されている形式のスキーマバージョン。このフィールドの値は、 AWSで識別される正式公開バージョンの 1 つである必要があります。現在のリリースでは、 AWS Security Finding 形式のスキーマバージョンは です2018-10-08。

例

```
"SchemaVersion": "2018-10-08"
```

緊急度

結果の重要性を定義します。このオブジェクトの詳細については、AWS Security Hub API リファレンスの「Severity」を参照してください。

Severity は検索結果の最上位オブジェクトであり、FindingProviderFields オブジェクトの下にネストされています。

結果に含まれるトップレベルの Severity オブジェクトの値は、BatchUpdateFindings API によってのみ更新してください。

重要度情報を提供するには、BatchImportFindings API リクエストを行うときに結果プロバイダーが FindingProviderFields の下にある Severity オブジェクトを更新する必要があります。
新しい検出結果のBatchImportFindingsリクエストが のみを提供するLabelか、 のみを提供する場合Normalized、Security Hub は他のフィールドの値を自動的に入力します。
Product および Originalフィールドも入力できます。

最上位Finding.Severityオブジェクトは存在するが、存在しない場合、Security Hub Finding.FindingProviderFieldsはFindingProviderFields.Severityオブジェクトを作成し、その全体をそのFinding.Severity objectオブジェクトにコピーします。これにより、最上位Severityオブジェクトが上書きされても、プロバイダーが提供する元の詳細がFindingProviderFields.Severity構造内に保持されます。

結果の重要度には、関連するアセットまたは基になるリソースの重要度は考慮されません。重要度は、結果に関連付けられたリソースの重要度のレベルとして定義されます。例えば、ミッションクリティカルなアプリケーションに関連付けられているリソースは、非本番稼働用テストに関連付けられたリソースより重大度が高くなります。リソースの重要度に関する情報をキャプチャするには、Criticality フィールドを使用します。

結果のネイティブ重要度スコアを ASFF の Severity.Label の値に変換する際には、以下のガイダンスを使用することを推奨します。

- INFORMATIONAL – このカテゴリには、PASSED、WARNING、NOT AVAILABLE チェック、または機密データの ID が含まれる場合があります。
- LOW — 将来の侵害につながる可能性のある結果。例えば、このカテゴリには、脆弱性、設定の弱点、公開されたパスワードなどが含まれる場合があります。
- MEDIUM – 現在進行中の侵害を示していても、攻撃者が目標を達成した兆候が見られない結果。例えば、このカテゴリには、マルウェアアクティビティ、ハッキングアクティビティ、異常な動作の検出などが含まれます。
- HIGH または CRITICAL – 実際のデータ損失、漏洩、サービス拒否など、攻撃者が目標を達成したことを示す結果。

例

```
"Severity": {
    "Label": "CRITICAL",
    "Normalized": 90,
    "Original": "CRITICAL"
}
```

タイトル

結果のタイトル。このフィールドには、固有ではない定型テキスト、または結果のインスタンスに固有の詳細を指定できます。

コントロール検出結果の場合、このフィールドにはコントロールのタイトルが表示されます。

[統合されたコントロールの検出結果] を有効にした場合、このフィールドは標準を参照しません。

例

```
"Title": "AWS Config should be enabled"
```

型

namespace/*category*/*classifier* の形式の 1 つ以上の結果タイプで、結果を分類します。[統合されたコントロールの検出結果] を有効にした場合、このフィールドは標準を参照しません。

Types は、BatchUpdateFindings のみを使用して更新する必要があります。

結果プロバイダーが Types に値を提供する場合は、FindingProviderFields にある Types 属性を使用する必要があります。

以下のリストでは、最上位の項目は名前空間、2 番目のレベルの項目はカテゴリ、3 番目のレベルの項目は分類子です。検索プロバイダーでは、定義済みの名前空間を使用して、結果の並べ替えおよびグループ化を行うことが推奨されます。定義済みのカテゴリおよび分類子を使用することが推奨される場合もありますが、必須ではありません。Software and Configuration Checks 名前空間でのみ、分類子が定義されています。

名前空間/カテゴリ/分類子の部分パスを定義することができます。例えば、以下の結果タイプはすべて有効です。

- TTP
- TTP/防衛回避
- TTPs防御回避/CloudTrailStopped

次のリストの tactics、techniques、procedures (TTP) カテゴリは、MITRE ATT&CK MatrixTM に対応しています。Unusual Behaviors (異常動作) の名前空間は、一般的な異常動作 (統計的異常など) を反映しており、特定の TTP とは一致していません。ただし、Unusual Behaviors と TTP の両方の結果で結果を分類することは可能です。

名前空間、カテゴリ、分類子のリスト:

- ソフトウェアおよび設定チェック
  - 脆弱性
    - CVE
  - AWS セキュリティのベストプラクティス
    - ネットワーク到達可能性
    - ランタイム動作分析
  - 業界および規制の基準
    - AWS 基本的なセキュリティのベストプラクティス
    - CIS Host Hardening Benchmark
    - CIS AWS Foundations Benchmark
    - PCI-DSS

    - クラウドセキュリティアライアンス規制
    - ISO 90001 規制
    - ISO 27001 規制
    - ISO 27017 規制
    - ISO 27018 規制
    - SOC 1
    - SOC 2
    - HIPAA 規制 (米国)
    - NIST 800-53 規制 (米国)
    - NIST CSF 規制 (米国)
    - IRAP 規制 (オーストラリア)
    - K-ISMS 規制 (韓国)
    - MTCS 規制 (シンガポール)
    - FISC安全対策基準 (日本)
    - マイナンバー法 (日本)
    - ENS 規制 (スペイン)
    - Cyber Essentials Plus 規制 (英国)
    - G-Cloud 規制 (英国)
    - C5 規制 (ドイツ)
    - IT-Grundschutz 規制 (ドイツ)
    - GDPR 規制 (ヨーロッパ)
    - TISAX 規制 (ヨーロッパ)
  - パッチ管理
- TTP
  - 初回アクセス
  - 実行
  - 永続的
  - 権限昇格
  - 防衛回避
  - 認証情報アクセス

  - 発見
  - 横方向への移動
  - 収集
  - コマンドアンドコントロール
- 効果
  - データ流出
  - データ漏えい
  - データ破壊
  - サービス拒否
  - リソース消費
- 異常な動作
  - アプリケーション
  - ネットワークフロー
  - IP アドレス
  - ユーザー
  - VM
  - コンテナ
  - サーバーレス
  - プロセス
  - データベース
  - データ
- 機密データの識別
  - PII
  - パスワード
  - リーガル
  - 金融
  - セキュリティ
  - ビジネス

例

```
"Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
    ]
```

UpdatedAt

結果プロバイダーが最後に結果レコードを更新した日時を示します。

このタイムスタンプは、結果レコードが最後または最も最近に更新された時刻を反映しています。したがって、イベントまたは脆弱性が最後または最も最近に検出された日時を反映する `LastObservedAt` タイムスタンプとは異なる可能性があります。

結果レコードを更新する際には、このタイムスタンプを現在のタイムスタンプに更新する必要があります。結果レコードの作成時には、`CreatedAt` と `UpdatedAt` のタイムスタンプが同じである必要があります。結果レコードを更新した後は、このフィールドの値が、そのレコードに含まれる以前のすべての値よりも最近の値になる必要があります。

`UpdatedAt` は `BatchUpdateFindings` API オペレーションを使用して更新できません。これは `BatchImportFindings` を使用してのみ更新できます。

例

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

> **Note**
>
> Security Hub では、結果は、最新の更新から 90 日後、または更新が行われない場合は作成日から 90 日後に削除されます。検出結果を 90 日以上保存するには、Amazon で検出結果を S3 バケットにルーティング EventBridge するルールを設定できます。

オプションの最上位属性

これらの最上位属性は、 AWS Security Finding 形式 (ASFF) ではオプションです。これらの属性の詳細については、 API リファレンスAwsSecurityFindingの「」を参照してください。 AWS Security Hub

アクション

Action オブジェクトは、リソースに影響する、またはリソースに対して実行されたアクションの詳細を提供します。

例

```
"Action": {
    "ActionType": "PORT_PROBE",
    "PortProbeAction": {
        "PortProbeDetails": [
            {
                "LocalPortDetails": {
                    "Port": 80,
                    "PortName": "HTTP"
                  },
                "LocalIpDetails": {
                     "IpAddressV4": "192.0.2.0"
                 },
                "RemoteIpDetails": {
                    "Country": {
                        "CountryName": "Example Country"
                    },
                    "City": {
                        "CityName": "Example City"
                    },
                   "GeoLocation": {
                       "Lon": 0,
                       "Lat": 0
                   },
                   "Organization": {
                       "AsnOrg": "ExampleASO",
                       "Org": "ExampleOrg",
                       "Isp": "ExampleISP",
                       "Asn": 64496
                   }
                }
            }
        ],
        "Blocked": false
    }
}
```

AwsAccountName

検出結果が適用される AWS アカウント 名前。

例

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

結果を生成した製品の会社の名前。コントロールベースの検出結果の場合、会社は です AWS。

Security Hub は、各結果に対してこの属性を自動的に入力します。BatchImportFindings または BatchUpdateFindings を使用して更新することはできません。カスタム統合を使用している場合は例外です。「the section called “カスタム製品統合の使用”」を参照してください。

Security Hub コンソールを使用して会社名で結果をフィルタリングする場合は、この属性を使用します。Security Hub API を使用して会社名で結果をフィルタリングする場合は、ProductFields の aws/securityhub/CompanyName 属性を使用します。Security Hub は、これら 2 つの属性を同期しません。

例

```
"CompanyName": "AWS"
```

コンプライアンス

Compliance オブジェクトは、コントロールに関連する結果の詳細を提供します。この属性は、Security Hub コントロールから生成された結果と、 が Security Hub AWS Config に送信する結果に対して返されます。

例

```
"Compliance": {
    "AssociatedStandards": [
        {"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
        {"StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
        {"StandardsId": "standards/nist-800-53/v/5.0.0"}
    ],
    "RelatedRequirements": [
        "NIST.800-53.r5 AC-4",
```

```
        "NIST.800-53.r5 AC-4(21)",
        "NIST.800-53.r5 SC-7",
        "NIST.800-53.r5 SC-7(11)",
        "NIST.800-53.r5 SC-7(16)",
        "NIST.800-53.r5 SC-7(21)",
        "NIST.800-53.r5 SC-7(4)",
        "NIST.800-53.r5 SC-7(5)"
    ],
    "SecurityControlId": "EC2.18",
    "SecurityControlParameters":[
        {
            "Name": "authorizedTcpPorts",
            "Value": ["80", "443"]
        },
        {
            "Name": "authorizedUdpPorts",
            "Value": ["427"]
        }
    ],
    "Status": "NOT_AVAILABLE",
    "StatusReasons": [
        {
            "ReasonCode": "CONFIG_RETURNS_NOT_APPLICABLE",
            "Description": "This finding has a compliance status of NOT AVAILABLE
 because AWS Config sent Security Hub a finding with a compliance state of Not
 Applicable. The potential reasons for a Not Applicable finding from Config are that
 (1) a resource has been moved out of scope of the Config rule; (2) the Config rule has
 been deleted; (3) the resource has been deleted; or (4) the logic of the Config rule
 itself includes scenarios where Not Applicable is returned. The specific reason why
 Not Applicable is returned is not available in the Config rule evaluation."
        }
    ]
}
```

信頼度

特定することが想定されている挙動または問題を、結果が正確に特定できる可能性。

Confidence は、BatchUpdateFindings のみを使用して更新する必要があります。

結果プロバイダーが Confidence に値を提供する場合は、FindingProviderFields にある Confidence 属性を使用する必要があります。「the section called “FindingProviderFields を使用する”」を参照してください。

Confidence は、比率スケールを使用して 0～100 ベースで採点されます。0 は 0% の信頼度を意味し、100 は 100% の信頼度を意味します。例えば、ネットワークトラフィックの統計的偏差に基づくデータの不正引き出しは、実際の不正引き出しが確認されていないため、信頼性が低くなります。

例

```
"Confidence": 42
```

緊急性

結果に関連付けられているリソースに割り当てられている重要度です。

Criticality は、BatchUpdateFindings API オペレーションを呼び出すことによってのみ更新してください。このオブジェクトは BatchImportFindings で更新しないでください。

結果プロバイダーが Criticality に値を提供する場合は、FindingProviderFields にある Criticality 属性を使用する必要があります。「the section called “FindingProviderFields を使用する”」を参照してください。

Criticality は、比率スケールを使用して 0～100 ベースで採点され、完全な整数のみをサポートしています。スコア 0 は、基になるリソースに重要性がないことを示しており、スコア 100 は最も重要なリソース用に予約されています。

各リソースに対して、Criticality を割り当てる際に以下の点を考慮してください。

- 影響を受けたリソースに機密データ (PII が含まれる S3 バケットなど) が含まれていないか?
- 影響を受けたリソースにより、攻撃者はアクセスレベルを深めたり、能力を広げて悪意のあるアクティビティ (sysadmin アカウントへの侵害など) をさらに実行したりすることができるか?
- 当該のリソースは、ビジネスクリティカルなアセット (例えば、侵害された場合、収益に大きな影響を与える可能性がある主要なビジネスシステム) なのか？

ガイドラインは次の通りです。

- ミッションクリティカルなシステムに電力を供給するリソースや、機密性の高いデータが含まれるリソースは、75～100 の範囲で採点することができます。
- 重要な (クリティカルではない) システムに電力を供給しているリソースや、やや重要なデータを含むリソースは、25～74 の範囲で採点することができます。
- 重要でないシステムに電力を供給しているリソースや、機密でないデータを含むリソースは、0～24 の範囲で採点する必要があります。

例

```
"Criticality": 99
```

FindingProviderFields

FindingProviderFields には次の属性が含まれます。

- Confidence
- Criticality
- RelatedFindings
- Severity
- Types

前述のフィールドは FindingProviderFields オブジェクトの下にネストされますが、最上位の ASFF フィールドと同じ名前の冪形があります。新しい検出結果が検出結果プロバイダーによって Security Hub に送信されると、Security Hub は、対応する最上位フィールドに基づいてオブジェクトが空の場合、FindingProviderFieldsオブジェクトを自動的に入力します。

検出結果プロバイダーは、FindingProviderFieldsBatchImportFindingsSecurity Hub API のオペレーションを使用して更新できます。検出結果プロバイダーは、このオブジェクトを で更新できませんBatchUpdateFindings。

Security Hub が BatchImportFindings から FindingProviderFields および対応する最上位属性への更新を処理する方法についての詳細は、「the section called “FindingProviderFields を使用する”」を参照してください。

お客様は、 BatchUpdateFindingsオペレーションを使用して最上位フィールドを更新できます。お客様は を更新できませんFindingProviderFields。

例

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
```

```
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

FirstObservedAt

結果によってキャプチャされた潜在的なセキュリティ問題が最初に検出された時期を示します。

このタイムスタンプは、イベントまたは脆弱性が最初に検出された時刻を反映しています。したがって、この結果記録が作成された時間を反映する CreatedAt タイムスタンプとは異なる可能性があります。

このタイムスタンプは、結果記録が次に更新されるまでイミュータブルである必要がありますが、より正確なタイムスタンプがあると判別された場合は更新できます。

例

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

結果でキャプチャされた潜在的なセキュリティ上の問題が、セキュリティ検出製品によって最後に検出された日時を示します。

このタイムスタンプは、イベントまたは脆弱性が最後にまたは最近検出された時刻を反映します。したがって、これはこの結果記録が最後に更新された日時または最近更新された日時が反映される UpdatedAt タイムスタンプとは異なる可能性があります。

このタイムスタンプを提供することもできますが、最初の観測時には必要ありません。最初の観測時にこのフィールドを指定する場合は、タイムスタンプが FirstObservedAt タイムスタンプと同じである必要があります。結果が観測されるたびに、最後に検出されたタイムスタンプを反映するようにこのフィールドを更新する必要があります。

例

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

Malware

`Malware` オブジェクトは、検出結果に関連するマルウェアのリストを提供します。

例

```
"Malware": [
    {
        "Name": "Stringler",
        "Type": "COIN_MINER",
        "Path": "/usr/sbin/stringler",
        "State": "OBSERVED"
    }
]
```

Network (廃止)

`Network` オブジェクトは、結果に関するネットワーク関連情報を提供します。

このオブジェクトは廃止されました。このデータを提供するには、`Resources` 内のリソースにデータをマッピングするか、`Action` オブジェクトを使用できます。

例

```
"Network": {
    "Direction": "IN",
    "OpenPortRange": {
        "Begin": 443,
        "End": 443
    },
    "Protocol": "TCP",
    "SourceIpV4": "1.2.3.4",
    "SourceIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "SourcePort": "42",
    "SourceDomain": "example1.com",
    "SourceMac": "00:0d:83:b1:c0:8e",
    "DestinationIpV4": "2.3.4.5",
    "DestinationIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "DestinationPort": "80",
    "DestinationDomain": "example2.com"
```

```
}
```

NetworkPath

NetworkPath オブジェクトは、結果に関連するネットワークパスに関する情報を提供します。NetworkPath 内の各エントリは、パスのコンポーネントを表しています。

例

```
"NetworkPath" : [
    {
        "ComponentId": "abc-01a234bc56d8901ee",
        "ComponentType": "AWS::EC2::InternetGateway",
        "Egress": {
            "Destination": {
                "Address": [ "192.0.2.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": ["203.0.113.0/24"]
            }
        },
        "Ingress": {
            "Destination": {
                "Address": [ "198.51.100.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                 ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": [ "203.0.113.0/24" ]
            }
        }
```

```
    }
]
```

注記

Note オブジェクトは、結果に追加できるユーザー定義のメモを指定します。

結果プロバイダーは、結果に対する最初のメモは提供できますが、それ以降にメモを追加することはできません。メモは BatchUpdateFindings を使用してのみ更新できます。

例

```
"Note": {
    "Text": "Don't forget to check under the mat.",
    "UpdatedBy": "jsmith",
    "UpdatedAt": "2018-08-31T00:15:09Z"
}
```

PatchSummary

PatchSummary オブジェクトは、選択したコンプライアンス標準に対するインスタンスのパッチコンプライアンス状態についての概要を提供します。

例

```
"PatchSummary" : {
    "FailedCount" : 0,
    "Id" : "pb-123456789098",
    "InstalledCount" : 100,
    "InstalledOtherCount" : 1023,
    "InstalledPendingReboot" : 0,
    "InstalledRejectedCount" : 0,
    "MissingCount" : 100,
    "Operation" : "Install",
    "OperationEndTime" : "2018-09-27T23:39:31Z",
    "OperationStartTime" : "2018-09-27T23:37:31Z",
    "RebootOption" : "RebootIfNeeded"
}
```

プロセス

Process オブジェクトは、結果に関するプロセス関連の詳細を提供します。

例：

```
"Process": {
    "LaunchedAt": "2018-09-27T22:37:31Z",
    "Name": "syslogd",
    "ParentPid": 56789,
    "Path": "/usr/sbin/syslogd",
    "Pid": 12345,
    "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

Security Hub が検出結果を受信し、処理を開始するタイミングを示します。

これは `CreatedAt` および `UpdatedAt` とは異なります。これらは、検出結果プロバイダーのセキュリティ問題や検出結果のやり取りに関係する必須のタイムスタンプです。`ProcessedAt` タイムスタンプは、Security Hub が検出結果の処理を開始する時刻を示します。処理が完了すると、検出結果がユーザーのアカウントに表示されます。

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

セキュリティ検出結果製品に、定義された AWS Security Finding 形式に含まれないソリューション固有の追加の詳細を含めることができるデータ型。

Security Hub コントロールによって生成された結果の場合、`ProductFields` にコントロールに関する情報が含まれています。「the section called “コントロールの結果を生成および更新する”」を参照してください。

このフィールドには冗長データを含めず、 AWS Security Finding 形式フィールドと競合するデータを含めないでください。

`aws/`「」プレフィックスは、 AWS 製品およびサービスの予約済み名前空間のみを表し、サードパーティー統合の結果とともに送信しないでください。

必須ではありませんが、製品はフィールド名を `company-id/product-id/field-name` のフォーマットにすることが推奨されます。ここにある、`company-id` と `product-id` は、結果の `ProductArn` にあるものと一致します。

参照するフィールド `Archival` は、Security Hub が既存の結果をアーカイブするときに使用されます。例えば、コントロールまたは標準を無効にしたり、統合統制結果を有効または無効にしたりすると、Security Hub は既存の結果をアーカイブします。

このフィールドには、検出結果を生成したコントロールを含む標準に関する情報が含まれる場合もあります。

例

```
"ProductFields": {
    "API", "DeleteTrail",
    "ArchivalReasons:0/Description": "The finding is in an ARCHIVED state because
 consolidated control findings has been turned on or off. This causes findings in the
 previous state to be archived when new findings are being generated.",
    "ArchivalReasons:0/ReasonCode": "CONSOLIDATED_CONTROL_FINDINGS_UPDATE",
    "aws/inspector/AssessmentTargetName": "My prod env",
    "aws/inspector/AssessmentTemplateName": "My daily CVE assessment",
    "aws/inspector/RulesPackageName": "Common Vulnerabilities and Exposures",
    "generico/secure-pro/Action.Type", "AWS_API_CALL",
    "generico/secure-pro/Count": "6",
    "Service_Name": "cloudtrail.amazonaws.com"
}
```

ProductName

結果を生成した製品の名前を提供します。コントロールベースの結果の場合、製品名は Security Hub になります。

Security Hub は、各結果に対してこの属性を自動的に入力します。`BatchImportFindings` または `BatchUpdateFindings` を使用して更新することはできません。カスタム統合を使用している場合は例外です。「the section called “カスタム製品統合の使用”」を参照してください。

Security Hub コンソールを使用して製品名で結果をフィルタリングする場合は、この属性を使用します。

Security Hub API を使用して製品名で結果をフィルタリングする場合は、`ProductFields` の `aws/securityhub/ProductName` 属性を使用します。

Security Hub は、これら 2 つの属性を同期しません。

RecordState

結果のレコード状態を提供します。

デフォルトでは、サービスによって最初に生成されたときの結果は ACTIVE と見なされます。

ARCHIVED 状態は、結果がビューで非表示になるべきであることを示します。アーカイブされた結果はすぐに削除されません。検索やレビュー、レポートを行うことができます。関連付けられたリソースが削除された場合、リソースが存在しない場合、またはコントロールが無効になっている場合、Security Hub でコントロールベースの結果が自動的にアーカイブされます。

RecordState は結果プロバイダー専用であり、BatchImportFindings によってのみ更新できます。これは BatchUpdateFindings を使用して更新することはできません。

結果に対する調査状態を追跡する場合は、RecordState ではなく Workflow を使用してください。

レコードの状態が ARCHIVED から ACTIVE に変更され、結果のワークフローステータスが NOTIFIED または RESOLVED の場合、Security Hub はワークフローステータスを自動的に NEW に設定します。

例

```
"RecordState": "ACTIVE"
```

リージョン

結果の生成 AWS リージョン 元の を指定します。

Security Hub は、各結果に対してこの属性を自動的に入力します。BatchImportFindings または BatchUpdateFindings を使用して更新することはできません。

例

```
"Region": "us-west-2"
```

RelatedFindings

現在の結果に関連する結果のリストを提供します。

RelatedFindings は、BatchUpdateFindings API オペレーションでのみ更新してください。このオブジェクトは BatchImportFindings で更新しないでください。

BatchImportFindings リクエストの場合、結果プロバイダーは FindingProviderFields の RelatedFindings オブジェクトを使用する必要があります。

RelatedFindings 属性の詳細については、AWS Security Hub APIリファレンスの「RelatedFinding」を参照してください。

例

```
"RelatedFindings": [
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000" },
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "AcmeNerfHerder-111111111111-x189dx7824" }
]
```

修正

Remediation オブジェクトは、結果に対処するために推奨される修復ステップに関する情報を提供します。

例

```
"Remediation": {
    "Recommendation": {
        "Text": "For instructions on how to fix this issue, see the AWS Security Hub
 documentation for EC2.2.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation"
    }
}
```

サンプル

結果がサンプルの結果かどうかを指定します。

```
"Sample": true
```

SourceUrl

SourceUrl オブジェクトは、検出製品内の現在の結果に関するページにリンクする URL を提供します。

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

ThreatIntelIndicator オブジェクトは、結果に関連する脅威インテリジェンスの詳細を提供します。

例

```
"ThreatIntelIndicators": [
  {
    "Category": "BACKDOOR",
    "LastObservedAt": "2018-09-27T23:37:31Z",
    "Source": "Threat Intel Weekly",
    "SourceUrl": "http://threatintelweekly.org/backdoors/8888",
    "Type": "IPV4_ADDRESS",
    "Value": "8.8.8.8",
  }
]
```

脅威

Threats オブジェクトは、結果によって検出された脅威の詳細を表示します。

例

```
"Threats": [{
    "FilePaths": [{
        "FileName": "b.txt",
        "FilePath": "/tmp/b.txt",
        "Hash": "sha256",
        "ResourceId": "arn:aws:ec2:us-west-2:123456789012:volume/vol-032f3bdd89aee112f"
    }],
    "ItemCount": 3,
    "Name": "Iot.linux.mirai.vwisi",
    "Severity": "HIGH"
}]
```

UserDefinedFields

結果に関連付けられている名前と値の文字列ペアのリストを提供します。結果に追加されるカスタムのユーザー定義フィールドです。これらのフィールドは、特定の設定で自動生成されることがあります。

結果プロバイダーでは、このフィールドを製品で生成されるデータに使用しないでください。代わりに、検出結果プロバイダーは標準の AWS Security Finding 形式ProductFieldsフィールドにマッピングされないデータに フィールドを使用できます。

これらのフィールドは、BatchUpdateFindings を使用してのみ更新できます。

例

```
"UserDefinedFields": {
    "reviewedByCio": "true",
    "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

結果の正確性を提供します。結果プロバイダーは、このフィールドに値 UNKNOWN を設定できます。検出製品のシステムに意味のあるアナログが存在する場合、検出製品はこの値を提供する必要があります。このフィールドは一般的に、結果調査後のユーザーの決定またはアクションに従って入力されます。

結果プロバイダーはこの属性の初期値を提供できますが、それ以降は更新できません。この属性は、BatchUpdateFindings を使用してのみ更新できます。

```
"VerificationState": "Confirmed"
```

脆弱性

Vulnerabilities オブジェクトは、結果に関連付けられている脆弱性のリストを提供します。

例

```
"Vulnerabilities" : [
    {
        "CodeVulnerabilities": [{
            "Cwes": [
                "CWE-798",
                "CWE-799"
            ],
            "FilePath": {
                "EndLine": 421,
                "FileName": "package-lock.json",
                "FilePath": "package-lock.json",
```

```
                "StartLine": 420
            },
                "SourceArn":"arn:aws:lambda:us-east-1:123456789012:layer:AWS-AppConfig-
Extension:114"
        }],
        "Cvss": [
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N",
                "Version": "V3"
            },
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:L/AC:M/Au:N/C:C/I:N/A:N",
                "Version": "V2"
            }
        ],
        "EpssScore": 0.015,
        "ExploitAvailable": "YES",
        "FixAvailable": "YES",
        "Id": "CVE-2020-12345",
        "LastKnownExploitAt": "2020-01-16T00:01:35Z",
        "ReferenceUrls":[
           "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12418",
            "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17563"
        ],
        "RelatedVulnerabilities": ["CVE-2020-12345"],
        "Vendor": {
            "Name": "Alas",
            "Url":"https://alas.aws.amazon.com/ALAS-2020-1337.html",
            "VendorCreatedAt":"2020-01-16T00:01:43Z",
            "VendorSeverity":"Medium",
            "VendorUpdatedAt":"2020-01-16T00:01:43Z"
        },
        "VulnerablePackages": [
            {
                "Architecture": "x86_64",
                "Epoch": "1",
                "FilePath": "/tmp",
                "FixedInVersion": "0.14.0",
                "Name": "openssl",
                "PackageManager": "OS",
                "Release": "16.amzn2.0.3",
                "Remediation": "Update aws-crt to 0.14.0",
```

```
                "SourceLayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:id",
                "SourceLayerHash":
 "sha256:c1962c35b63a6ff6ce7df6e042ee82371a605ca9515569edec46ff14f926f001",
                "Version": "1.0.2k"
            }
        ]
    }
]
```

ワークフロー

`Workflow` オブジェクトは、結果の調査ステータスに関する情報を提供します。

このフィールドは、お客様が修復、オーケストレーション、チケット発行ツールで使用することを目的としています。結果の提供元を見つけるためのものではありません。

`Workflow` フィールドは `BatchUpdateFindings` でのみ更新できます。お客様は、コンソールから更新することもできます。「the section called “結果のワークフローステータスを設定する”」を参照してください。

例

```
"Workflow": {
    "Status": "NEW"
}
```

WorkflowState （ 廃止 ）

このオブジェクトは廃止され、`Workflow` オブジェクトの `Status` フィールドによって置き換えられています。

このフィールドは、結果のワークフローステータスを提供します。検出製品は、このフィールドに値 `NEW` を設定できます。検出製品のシステムに意味のあるアナログが存在する場合、検出製品はこの値を提供することができます。

例

```
"WorkflowState": "NEW"
```

Resources

`Resources` オブジェクトは、結果に関連するリソースについての情報を提供します。

最大 32 個のリソースからなるオブジェクト配列が含まれます。

リソース名のフォーマット方法については、「AWS Security Finding Format (ASFF) 構文」を参照してください。

各リソースオブジェクトの例については、以下のリストから選択してください。

トピック

- リソース属性
- AwsAmazonMQ
- AwsApiGateway
- AwsAppSync
- AwsAthena
- AwsAutoScaling
- AwsBackup
- AwsCertificateManager
- AwsCloudFormation
- AwsCloudFront
- AwsCloudTrail
- AwsCloudWatch
- AwsCodeBuild
- AwsDms
- AwsDynamoDB
- AwsEc2
- AwsEcr
- AwsEcs
- AwsEfs
- AwsEks
- AwsElasticBeanstalk
- AwsElasticSearch
- AwsElb
- AwsEventBridge

- AwsGuardDuty
- AwsIam
- AwsKinesis
- AwsKms
- AwsLambda
- AwsMsk
- AwsNetworkFirewall
- AwsOpenSearchService
- AwsRds
- AwsRedshift
- AwsRoute53
- AwsS3
- AwsSageMaker
- AwsSecretsManager
- AwsSns
- AwsSqs
- AwsSsm
- AwsStepFunctions
- AwsWaf
- AwsXray
- Container
- Other

リソース属性

AWS Security Finding 形式 (ASFF) の `Resources` オブジェクトの説明と例を次に示します。これらのフィールドの詳細については、「リソース」を参照してください。

ApplicationArn

検出結果に関連するアプリケーションの Amazon リソースネーム (ARN) を識別します。

例

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0"
```

ApplicationName

検出結果に関連するアプリケーションの名前を識別します。

例

```
"ApplicationName": "SampleApp"
```

DataClassification

DataClassification フィールドは、リソースで検出された機密データに関する情報を提供します。

例

```
"DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
```

```
                        "Records": [],
                        "Cells": []
                    }
                },
                {
                    "Count": 59,
                    "Type": "EMAIL_ADDRESS",
                    "Occurrences": {
                        "Pages": [
                            {
                                "PageNumber": 1,
                                "OffsetRange": {
                                    "Start": 1,
                                    "End": 100,
                                    "StartColumn": 10
                                },
                                "LineRange": {
                                    "Start": 1,
                                    "End": 100,
                                    "StartColumn": 10
                                }
                            }
                        ]
                    }
                },
                {
                    "Count": 2229,
                    "Type": "URL",
                    "Occurrences": {
                       "LineRanges": [
                           {
                               "Start": 1,
                               "End": 13
                           }
                       ]
                   }
               },
               {
                   "Count": 13826,
                   "Type": "NameDetection",
                   "Occurrences": {
                        "Records": [
                            {
                                "RecordIndex": 1,
```

```
                                "JsonPath": "$.ssn.value"
                            }
                        ]
                    }
                },
                {
                    "Count": 32,
                    "Type": "AddressDetection"
                }
            ],
            "TotalCount": 32
        }
    ],
    "CustomDataIdentifiers": {
        "Detections": [
            {
                "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                "Name": "1712be25e7c7f53c731fe464f1c869b8",
                "Count": 2,
            }
        ],
        "TotalCount": 2
    }
  }
}
```

詳細

Details フィールドは、適切なオブジェクトを使用する単一のリソースに関する追加情報を提供します。各リソースは、Resources オブジェクト内の個別のリソースオブジェクトで指定する必要があります。

結果のサイズが最大の 240 KB を超えた場合、Details オブジェクトは結果から削除されます。AWS Config ルールを使用するコントロールの検出結果については、 AWS Config コンソールでリソースの詳細を表示できます。

Security Hub には、サポートされているリソースタイプに使用できる一連のリソースの詳細が用意されています。これらの詳細は、Type オブジェクトの値に対応しています。可能な場合、提供されたタイプを使用してください。

例えば、リソースが S3 バケットの場合、リソース Type を AwsS3Bucket に設定し、AwsS3Bucket オブジェクトにリソースの詳細を指定します。

Other オブジェクトでは、カスタムのフィールドや値を指定できます。Other オブジェクトは、次の場合に使用できます。

- リソースタイプ (リソース Type の値) に対応する詳細オブジェクトがない場合。リソースの詳細を指定するには、Other オブジェクトを使用します。
- リソースタイプのオブジェクトに、入力するすべてのフィールドが含まれていない場合。この場合は、リソースタイプの詳細オブジェクトを使用して、使用可能なフィールドに入力します。Other オブジェクトを使用して、タイプ固有のオブジェクトに含まれていないフィールドに入力してください。
- リソースタイプが提供されたタイプのいずれでもない場合。この場合、Resource.Type を Other に設定し、Other オブジェクトを使用して詳細を入力します。

例


```
"Details": {
  "AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IpV4Addresses": ["1.1.1.1"],
    "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    },
    "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
    ],
    "SubnetId": "PublicSubnet",
    "Type": "i3.xlarge",
    "VirtualizationType": "hvm",
    "VpcId": "TestVPCIpv6"
  },
  "AwsS3Bucket": {
    "OwnerId": "da4d66eac431652a4d44d490a00500bded52c97d235b7b4752f9f688566fe6de",
```

```
    "OwnerName": "acmes3bucketowner"
  },
  "Other": { "LightPen": "blinky", "SerialNo": "1234abcd"}
}
```

ID

指定されたリソースタイプの識別子。

Amazon AWS リソースネーム (ARNsで識別されるリソースの場合、これは ARN です。

ARN がない AWS リソースの場合、これはリソースを AWS 作成したサービスによって定義された識別子です。 ARNs

AWS リソース以外の場合、これはリソースに関連付けられている一意の識別子です。

例

```
"Id": "arn:aws:s3:::example-bucket"
```

パーティション

リソースが置かれているパーティション。パーティションは のグループです AWS リージョン。各 AWS アカウント は 1 つのパーティションにスコープされます。

以下のパーティションがサポートされています。

- aws – AWS リージョン
- aws-cn - 中国リージョン
- aws-us-gov – AWS GovCloud (US) Region

例

```
"Partition": "aws"
```

リージョン

このリソース AWS リージョン が配置されている のコード。リージョンコードの一覧については、「リージョンエンドポイント」を参照してください。

例

```
"Region": "us-west-2"
```

ResourceRole

結果におけるリソースのロールを識別します。リソースは、結果アクティビティのターゲットか、アクティビティを実行するアクターのどちらかです。

例

```
"ResourceRole": "target"
```

タグ

Security Hub に取り込まれる検出結果には、統合製品 AWS のサービス やサードパーティー製品からの検出結果など、リソースタグを追加できます。タグ付け API の `GetResources`オペレーションがサポートするリソースに AWS Resource Groups タグ付けできます。サポートされているリソースのリストについては、「Resource Groups Tagging API をサポートするサービス」を参照してください。

タグを追加すると、結果の処理時にリソースに関連付けられたタグがわかります。`Tags` 属性を含めることができるのは、タグが関連付けられているリソースのみです。リソースにタグが関連付けられていない場合は、結果に `Tags` 属性を含めないでください。

検出結果にリソースタグを含めることで、データエンリッチメントパイプラインを構築したり、セキュリティ検出結果のメタデータを手動で強化したりする必要がなくなります。タグを使用して、結果とインサイトを検索またはフィルタリングし、自動化ルールを作成することもできます。

タグに適用される制限の詳細については、「タグの命名制限と要件」を参照してください。

このフィールドには、 AWS リソースに存在するタグのみを指定できます。 AWS Security Finding 形式で定義されていないデータを提供するには、`Other`詳細サブフィールドを使用します。

例

```
"Tags": {
    "billingCode": "Lotus-1-2-3",
    "needsPatching": "true"
}
```

タイプ

詳細を提供しているリソースのタイプです。

可能な限り、提供されているリソースタイプの中の 1 つ (AwsEc2Instance または AwsS3Bucket など) を使用してください。

リソースタイプが提供されているリソースタイプと一致しない場合は、リソース Type を Other に設定し、Other 詳細サブフィールドを使用して詳細を入力します。

サポートされる値のリストについては、「Resources」を参照してください。

例

```
"Type": "AwsS3Bucket"
```

AwsAmazonMQ

AwsAmazonMQ リソースの AWS Security Finding 形式 (ASFF) の例を次に示します。

AwsAmazonMQBroker

AwsAmazonMQBroker は、Amazon MQ で実行されるメッセージブローカー環境である Amazon MQ ブローカーに関する情報を提供します。

次の例は、AwsAmazonMQBroker オブジェクトの ASFF を示しています。AwsAmazonMQBroker 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsAmazonMQBroker」を参照してください。

例

```
"AwsAmazonMQBroker": {
    "AutoMinorVersionUpgrade": true,
    "BrokerArn": "arn:aws:mq:us-east-1:123456789012:broker:TestBroker:b-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerId": "b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerName": "TestBroker",
    "Configuration": {
        "Id": "c-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "Revision": 1
    },
```

```
    "DeploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
    "EncryptionOptions": {
        "UseAwsOwnedKey": true
    },
    "EngineType": "ActiveMQ",
    "EngineVersion": "5.17.2",
    "HostInstanceType": "mq.t2.micro",
    "Logs": {
        "Audit": false,
        "AuditLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/
audit",
        "General": false,
        "GeneralLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111/general"
    },
    "MaintenanceWindowStartTime": {
        "DayOfWeek": "MONDAY",
        "TimeOfDay": "22:00",
        "TimeZone": "UTC"
    },
    "PubliclyAccessible": true,
    "SecurityGroups": [
        "sg-021345abcdef6789"
    ],
    "StorageType": "efs",
    "SubnetIds": [
        "subnet-1234567890abcdef0",
        "subnet-abcdef01234567890"
    ],
    "Users": [
        {
            "Username": "admin"
        }
    ]
}
```

AwsApiGateway

`AwsApiGateway` リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsApiGatewayRestApi

`AwsApiGatewayRestApi` オブジェクトには、Amazon API Gateway のバージョン 1 の REST API に関する情報が含まれています。

以下は、 AWS Security Finding 形式 (ASFF) の AwsApiGatewayRestApi 検出の例です。AwsApiGatewayRestApi 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsApiGatewayRestApiDetails「」を参照してください。

例

```
AwsApiGatewayRestApi: {
    "Id": "exampleapi",
    "Name": "Security Hub",
    "Description": "AWS Security Hub",
    "CreatedDate": "2018-11-18T10:20:05-08:00",
    "Version": "2018-10-26",
    "BinaryMediaTypes" : ["-'*~1*'"],
    "MinimumCompressionSize": 1024,
    "ApiKeySource": "AWS_ACCOUNT_ID",
    "EndpointConfiguration": {
        "Types": [
            "REGIONAL"
        ]
    }
}
```

AwsApiGatewayStage

AwsApiGatewayStage オブジェクトは、Amazon API Gateway ステージ バージョン 1 に関する情報を提供します。

以下は、 AWS Security Finding 形式 (ASFF) の AwsApiGatewayStage 検出の例です。AwsApiGatewayStage 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsApiGatewayStageDetails「」を参照してください。

例

```
"AwsApiGatewayStage": {
    "DeploymentId": "n7hlmf",
    "ClientCertificateId": "a1b2c3",
    "StageName": "Prod",
    "Description" : "Stage Description",
    "CacheClusterEnabled": false,
    "CacheClusterSize" : "1.6",
    "CacheClusterStatus": "NOT_AVAILABLE",
    "MethodSettings": [
        {
```

```
            "MetricsEnabled": true,
            "LoggingLevel": "INFO",
            "DataTraceEnabled": false,
            "ThrottlingBurstLimit": 100,
            "ThrottlingRateLimit": 5.0,
            "CachingEnabled": false,
            "CacheTtlInSeconds": 300,
            "CacheDataEncrypted": false,
            "RequireAuthorizationForCacheControl": true,
            "UnauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER",
            "HttpMethod": "POST",
            "ResourcePath": "/echo"
        }
    ],
    "Variables": {"test": "value"},
    "DocumentationVersion": "2.0",
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "CanarySettings": {
        "PercentTraffic": 0.0,
        "DeploymentId": "ul73s8",
        "StageVariableOverrides" : [
            "String" : "String"
        ],
        "UseStageCache": false
    },
    "TracingEnabled": false,
```

```
    "CreatedDate": "2018-07-11T10:55:18-07:00",
    "LastUpdatedDate": "2020-08-26T11:51:04-07:00",
    "WebAclArn" : "arn:aws:waf-regional:us-west-2:111122223333:webacl/
cb606bd8-5b0b-4f0b-830a-dd304e48a822"
}
```

AwsApiGatewayV2Api

AwsApiGatewayV2Api オブジェクトには、Amazon API Gateway のバージョン 2 API に関する情報が含まれています。

以下は、 AWS Security Finding 形式 (ASFF) の AwsApiGatewayV2Api 検出の例です。AwsApiGatewayV2Api 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」の[AwsApiGatewayV2ApiDetails]」を参照してください。

例

```
"AwsApiGatewayV2Api": {
    "ApiEndpoint": "https://example.us-west-2.amazonaws.com",
    "ApiId": "a1b2c3d4",
    "ApiKeySelectionExpression": "$request.header.x-api-key",
    "CreatedDate": "2020-03-28T00:32:37Z",
   "Description": "ApiGatewayV2 Api",
   "Version": "string",
    "Name": "my-api",
    "ProtocolType": "HTTP",
    "RouteSelectionExpression": "$request.method $request.path",
   "CorsConfiguration": {
        "AllowOrigins": [ "*" ],
        "AllowCredentials": true,
        "ExposeHeaders": [ "string" ],
        "MaxAge": 3000,
        "AllowMethods": [
          "GET",
          "PUT",
          "POST",
          "DELETE",
          "HEAD"
        ],
        "AllowHeaders": [ "*" ]
    }
}
```

AwsApiGatewayV2Stage

AwsApiGatewayV2Stage には、Amazon API Gateway のバージョン 2 ステージに関する情報が含まれています。

以下は、 AWS Security Finding 形式 (ASFF) の AwsApiGatewayV2Stage 検出の例です。AwsApiGatewayV2Stage 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsApiGatewayV2StageDetails」を参照してください。

例

```
"AwsApiGatewayV2Stage": {
    "CreatedDate": "2020-04-08T00:36:05Z",
    "Description" : "ApiGatewayV2",
    "DefaultRouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "DeploymentId": "x1zwyv",
    "LastUpdatedDate": "2020-04-08T00:36:13Z",
    "RouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "StageName": "prod",
    "StageVariables": [
        "function": "my-prod-function"
    ],
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
```

```
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "AutoDeploy": false,
    "LastDeploymentStatusMessage": "Message",
    "ApiGatewayManaged": true,
}
```

AwsAppSync

AwsAppSync リソース AWS のセキュリティ検出結果形式 (ASFF) の例を次に示します。

AwsAppSyncGraphQLApi

AwsAppSyncGraphQLApi は、アプリケーションのトップレベルコンストラクトである AWS AppSync GraphQL API に関する情報を提供します。

次の例は、AwsAppSyncGraphQLApi オブジェクトの ASFF を示しています。AwsAppSyncGraphQLApi 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsAppSyncGraphQLApi」を参照してください。

例

```
"AwsAppSyncGraphQLApi": {
    "AdditionalAuthenticationProviders": [
    {
     "AuthenticationType": "AWS_LAMBDA",
     "LambdaAuthorizerConfig": {
      "AuthorizerResultTtlInSeconds": 300,
      "AuthorizerUri": "arn:aws:lambda:us-east-1:123456789012:function:mylambdafunc"
     }
    },
    {
     "AuthenticationType": "AWS_IAM"
    }
    ],
```

```
    "ApiId": "021345abcdef6789",
    "Arn": "arn:aws:appsync:eu-central-1:123456789012:apis/021345abcdef6789",
    "AuthenticationType": "API_KEY",
    "Id": "021345abcdef6789",
    "LogConfig": {
     "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/appsync-
graphqlapi-logs-eu-central-1",
     "ExcludeVerboseContent": true,
     "FieldLogLevel": "ALL"
    },
    "Name": "My AppSync App",
    "XrayEnabled": true,
}
```

AwsAthena

AwsAthena リソースの AWS Security Finding 形式 (ASFF) の例を次に示します。

AwsAthenaWorkGroup

AwsAthenaWorkGroup は、Amazon Athena ワークグループに関する情報を提供します。ワークグループは、ユーザー、チーム、アプリケーション、ワークロードを分離するのに役立ちます。また、データ処理の制限を設定したり、コストを追跡したりするのにも役立ちます。

次の例は、AwsAthenaWorkGroup オブジェクトの ASFF を示しています。AwsAthenaWorkGroup 属性の説明を表示するには、AWS Security Hub 「 API リファレンスAwsAthenaWorkGroup」の「」を参照してください。

例

```
"AwsAthenaWorkGroup": {
    "Description": "My workgroup for prod workloads",
    "Name": "MyWorkgroup",
    "WorkgroupConfiguration" {
        "ResultConfiguration": {
            "EncryptionConfiguration": {
                "EncryptionOption": "SSE_KMS",
                "KmsKey": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
            }
        }
    },
        "State": "ENABLED"
```

```
}
```

AwsAutoScaling

AwsAutoScaling リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsAutoScalingAutoScalingGroup

AwsAutoScalingAutoScalingGroup オブジェクトは、オートスケーリンググループの詳細を提供します。

以下は、 AWS Security Finding 形式 (ASFF) の AwsAutoScalingAutoScalingGroup 検出の例です。AwsAutoScalingAutoScalingGroup 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsAutoScalingAutoScalingGroupDetails「」を参照してください。

例

```
"AwsAutoScalingAutoScalingGroup": {
        "CreatedTime": "2017-10-17T14:47:11Z",
        "HealthCheckGracePeriod": 300,
        "HealthCheckType": "EC2",
        "LaunchConfigurationName": "mylaunchconf",
        "LoadBalancerNames": [],
        "LaunchTemplate": {
            "LaunchTemplateId": "string",
            "LaunchTemplateName": "string",
            "Version": "string"
        },
        "MixedInstancesPolicy": {
            "InstancesDistribution": {
                "OnDemandAllocationStrategy": "prioritized",
                "OnDemandBaseCapacity": number,
                "OnDemandPercentageAboveBaseCapacity": number,
                "SpotAllocationStrategy": "lowest-price",
                "SpotInstancePools": number,
                "SpotMaxPrice": "string"
            },
            "LaunchTemplate": {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "string",
                    "LaunchTemplateName": "string",
                    "Version": "string"
                 },
```

```
                "CapacityRebalance": true,
                "Overrides": [
                    {
                       "InstanceType": "string",
                       "WeightedCapacity": "string"
                    }
                ]
            }
        }
    }
}
```

AwsAutoScalingLaunchConfiguration

AwsAutoScalingLaunchConfiguration オブジェクトは、起動設定に関する詳細を提供します。

AWS Security Finding 形式 (ASFF) AwsAutoScalingLaunchConfigurationの結果の例を次に示します。

AwsAutoScalingLaunchConfiguration 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsAutoScalingLaunchConfigurationDetails「」を参照してください。

例

```
AwsAutoScalingLaunchConfiguration: {
    "LaunchConfigurationName": "newtest",
    "ImageId": "ami-058a3739b02263842",
    "KeyName": "55hundredinstance",
    "SecurityGroups": [ "sg-01fce87ad6e019725" ],
    "ClassicLinkVpcSecurityGroups": [],
    "UserData": "...Base64-Encoded user data..."
    "InstanceType": "a1.metal",
    "KernelId": "",
    "RamdiskId": "ari-a51cf9cc",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/sdh",
            "Ebs": {
                "VolumeSize": 30,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true,
```

```
                "SnapshotId": "snap-ffaa1e69",
                "VirtualName": "ephemeral1"
            }
        },
        {
            "DeviceName": "/dev/sdb",
            "NoDevice": true
        },
        {
            "DeviceName": "/dev/sda1",
            "Ebs": {
                "SnapshotId": "snap-02420cd3d2dea1bc0",
                "VolumeSize": 8,
                "VolumeType": "gp2",
                "DeleteOnTermination": true,
                "Encrypted": false
            }
        },
        {
            "DeviceName": "/dev/sdi",
            "Ebs": {
                "VolumeSize": 20,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true
            }
        },
        {
            "DeviceName": "/dev/sdc",
            "NoDevice": true
        }
    ],
    "InstanceMonitoring": {
        "Enabled": false
    },
    "CreatedTime": 1620842933453,
    "EbsOptimized": false,
    "AssociatePublicIpAddress": true,
    "SpotPrice": "0.045"
}
```

AwsBackup

AwsBackup リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsBackupBackupPlan

AwsBackupBackupPlan オブジェクトは、 AWS Backup のバックアップ計画に関する情報を提供します。 AWS Backup バックアッププランは、 AWS リソースをバックアップするタイミングと方法を定義するポリシー式です。

次の例は、 AwsBackupBackupPlan オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsBackupBackupPlan 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsBackupBackupPlan「」を参照してください。

例

```
"AwsBackupBackupPlan": {
    "BackupPlan": {
     "AdvancedBackupSettings": [{
      "BackupOptions": {
       "WindowsVSS":"enabled"
      },
      "ResourceType":"EC2"
     }],
     "BackupPlanName": "test",
     "BackupPlanRule": [{
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "DailyBackups",
      "ScheduleExpression": "cron(0 5 ? * * *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
      },
      {
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
```

```
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "Monthly",
      "ScheduleExpression": "cron(0 5 1 * ? *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
     }]
    },
    "BackupPlanArn": "arn:aws:backup:us-east-1:858726136373:backup-
plan:b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "BackupPlanId": "b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "VersionId": "ZDVjNDIzMjItYTZiNS00NzczLTg4YzctNmExMWM2NjZhY2E1"
}
```

AwsBackupBackupVault

AwsBackupBackupVault オブジェクトは、 AWS Backup のバックアップボールトに関する情報を提供します。 AWS Backup バックアップボールトは、バックアップを保存および整理するコンテナです。

次の例は、 AwsBackupBackupVault オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsBackupBackupVault 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsBackupBackupVault「」を参照してください。

例

```
"AwsBackupBackupVault": {
    "AccessPolicy": {
     "Statement": [{
      "Action": [
       "backup:DeleteBackupVault",
       "backup:DeleteBackupVaultAccessPolicy",
       "backup:DeleteRecoveryPoint",
       "backup:StartCopyJob",
       "backup:StartRestoreJob",
```

```
        "backup:UpdateRecoveryPointLifecycle"
       ],
       "Effect": "Deny",
       "Principal": {
        "AWS": "*"
       },
       "Resource": "*"
      }],
      "Version": "2012-10-17"
     },
     "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:aws/efs/
automatic-backup-vault",
     "BackupVaultName": "aws/efs/automatic-backup-vault",
     "EncrytionKeyArn": "arn:aws:kms:us-east-1:444455556666:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
     "Notifications": {
      "BackupVaultEvents": ["BACKUP_JOB_STARTED", "BACKUP_JOB_COMPLETED",
 "COPY_JOB_STARTED"],
      "SNSTopicArn": "arn:aws:sns:us-west-2:111122223333:MyVaultTopic"
     }
}
```

AwsBackupRecoveryPoint

AwsBackupRecoveryPoint オブジェクトは、 AWS Backup のバックアップに関する情報 (復旧ポイント) を提供します。 AWS Backup 復旧ポイントは、指定した時刻のリソースの内容を表します。

次の例は、 AwsBackupRecoveryPoint オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsBackupBackupVault 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsBackupRecoveryPoint「」を参照してください。

例

```
"AwsBackupRecoveryPoint": {
    "BackupSizeInBytes": 0,
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "BackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/
automatic-backup-vault",
    "CalculatedLifecycle": {
     "DeleteAt": "2021-08-30T06:51:58.271Z",
     "MoveToColdStorageAt": "2020-08-10T06:51:58.271Z"
    },
```

```
    "CompletionDate": "2021-07-26T07:21:40.361Z",
    "CreatedBy": {
     "BackupPlanArn": "arn:aws:backup:us-east-1:111122223333:backup-plan:aws/
efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanId": "aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanVersion": "ZGM4YzY5YjktMWYxNC00ZTBmLWE5MjYtZmU5OWNiZmM5ZjIz",
     "BackupRuleId": "2a600c2-42ad-4196-808e-084923ebfd25"
    },
    "CreationDate": "2021-07-26T06:51:58.271Z",
    "EncryptionKeyArn": "arn:aws:kms:us-east-1:111122223333:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "IamRoleArn": "arn:aws:iam::111122223333:role/aws-service-role/
backup.amazonaws.com/AWSServiceRoleForBackup",
    "IsEncrypted": true,
    "LastRestoreTime": "2021-07-26T06:51:58.271Z",
    "Lifecycle": {
     "DeleteAfterDays": 35,
     "MoveToColdStorageAfterDays": 15
    },
    "RecoveryPointArn": "arn:aws:backup:us-east-1:111122223333:recovery-point:151a59e4-
f1d5-4587-a7fd-0774c6e91268",
    "ResourceArn": "arn:aws:elasticfilesystem:us-east-1:858726136373:file-system/
fs-15bd31a1",
    "ResourceType": "EFS",
    "SourceBackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/
efs/automatic-backup-vault",
    "Status": "COMPLETED",
    "StatusMessage": "Failure message",
    "StorageClass": "WARM"
}
```


AwsCertificateManager

`AwsCertificateManager` リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsCertificateManagerCertificate

`AwsCertificateManagerCertificate` オブジェクトは、 AWS Certificate Manager (ACM) 証明書に関する詳細を提供します。

AWS Security Finding 形式 (ASFF) `AwsCertificateManagerCertificate`の結果の例を次に示します。`AwsCertificateManagerCertificate` 属性の説明を表示するには、AWS Security Hub「 API リファレンス」のAwsCertificateManagerCertificateDetails「」を参照してください。

例


```
"AwsCertificateManagerCertificate": {
    "CertificateAuthorityArn": "arn:aws:acm:us-west-2:444455556666:certificate-
authority/example",
    "CreatedAt": "2019-05-24T18:12:02.000Z",
    "DomainName": "example.amazondomains.com",
    "DomainValidationOptions": [
        {
            "DomainName": "example.amazondomains.com",
            "ResourceRecord": {
                "Name": "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                "Type": "CNAME",
                "Value": "_example.acm-validations.aws."
             },
             "ValidationDomain": "example.amazondomains.com",
             "ValidationEmails": [sample_email@sample.com],
             "ValidationMethod": "DNS",
             "ValidationStatus": "SUCCESS"
        }
    ],
    "ExtendedKeyUsages": [
        {
            "Name": "TLS_WEB_SERVER_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.1"
        },
        {
            "Name": "TLS_WEB_CLIENT_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.2"
        }
    ],
    "FailureReason": "",
    "ImportedAt": "2018-08-17T00:13:00.000Z",
    "InUseBy": ["arn:aws:amazondomains:us-west-2:444455556666:loadbalancer/example"],
    "IssuedAt": "2020-04-26T00:41:17.000Z",
    "Issuer": "Amazon",
    "KeyAlgorithm": "RSA-1024",
    "KeyUsages": [
        {
            "Name": "DIGITAL_SIGNATURE",
        },
        {
            "Name": "KEY_ENCIPHERMENT",
        }
```

```
    ],
    "NotAfter": "2021-05-26T12:00:00.000Z",
    "NotBefore": "2020-04-26T00:00:00.000Z",
    "Options": {
        "CertificateTransparencyLoggingPreference": "ENABLED",
    }
    "RenewalEligibility": "ELIGIBLE",
    "RenewalSummary": {
        "DomainValidationOptions": [
            {
                "DomainName": "example.amazondomains.com",
                "ResourceRecord": {
                    "Name":
 "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                    "Type": "CNAME",
                    "Value": "_example.acm-validations.aws.com",
                },
                "ValidationDomain": "example.amazondomains.com",
                "ValidationEmails": ["sample_email@sample.com"],
                "ValidationMethod": "DNS",
                "ValidationStatus": "SUCCESS"
            }
        ],
        "RenewalStatus": "SUCCESS",
        "RenewalStatusReason": "",
        "UpdatedAt": "2020-04-26T00:41:35.000Z",
    },
    "Serial": "02:ac:86:b6:07:2f:0a:61:0e:3a:ac:fd:d9:ab:17:1a",
    "SignatureAlgorithm": "SHA256WITHRSA",
    "Status": "ISSUED",
    "Subject": "CN=example.amazondomains.com",
    "SubjectAlternativeNames": ["example.amazondomains.com"],
    "Type": "AMAZON_ISSUED"
}
```

AwsCloudFormation

`AwsCloudFormation` リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsCloudFormationStack

`AwsCloudFormationStack` オブジェクトは、 最上位のテンプレートでリソースとしてネストされている AWS CloudFormation スタックの詳細を表示します。

次の例は、 AwsCloudFormationStack オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsCloudFormationStack 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsCloudFormationStackDetails「」を参照してください。

例

```
"AwsCloudFormationStack": {
 "Capabilities": [
  "CAPABILITY_IAM",
  "CAPABILITY_NAMED_IAM"
 ],
 "CreationTime": "2022-02-18T15:31:53.161Z",
 "Description": "AWS CloudFormation Sample",
 "DisableRollback": true,
 "DriftInformation": {
  "StackDriftStatus": "DRIFTED"
 },
 "EnableTerminationProtection": false,
 "LastUpdatedTime": "2022-02-18T15:31:53.161Z",
 "NotificationArns": [
  "arn:aws:sns:us-east-1:978084797471:sample-sns-cfn"
 ],
 "Outputs": [{
  "Description": "URL for newly created LAMP stack",
  "OutputKey": "WebsiteUrl",
  "OutputValue": "http://ec2-44-193-18-241.compute-1.amazonaws.com"
 }],
 "RoleArn": "arn:aws:iam::012345678910:role/exampleRole",
 "StackId": "arn:aws:cloudformation:us-east-1:978084797471:stack/sample-stack/
e5d9f7e0-90cf-11ec-88c6-12ac1f91724b",
 "StackName": "sample-stack",
 "StackStatus": "CREATE_COMPLETE",
 "StackStatusReason": "Success",
 "TimeoutInMinutes": 1
}
```

AwsCloudFront

AwsCloudFront リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsCloudFrontDistribution

AwsCloudFrontDistribution オブジェクトは、Amazon CloudFront ディストリビューション設定に関する詳細を提供します。

以下は、 AWS Security Finding 形式 (ASFF) の AwsCloudFrontDistribution 検出の例です。AwsCloudFrontDistribution 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsCloudFrontDistributionDetails「」を参照してください。

例

```
"AwsCloudFrontDistribution": {
    "CacheBehaviors": {
        "Items": [
            {
               "ViewerProtocolPolicy": "https-only"
            }
         ]
    },
    "DefaultCacheBehavior": {
         "ViewerProtocolPolicy": "https-only"
    },
    "DefaultRootObject": "index.html",
    "DomainName": "d2wkuj2w9l34gt.cloudfront.net",
    "Etag": "E37HOT42DHPVYH",
    "LastModifiedTime": "2015-08-31T21:11:29.093Z",
    "Logging": {
         "Bucket": "myawslogbucket.s3.amazonaws.com",
         "Enabled": false,
         "IncludeCookies": false,
         "Prefix": "myawslog/"
     },
     "OriginGroups": {
          "Items": [
              {
                 "FailoverCriteria": {
                     "StatusCodes": {
                          "Items": [
                              200,
                              301,
                              404
                          ]
                          "Quantity": 3
```

```
                    }
                }
            }
        ]
    },
    "Origins": {
        "Items": [
            {
                "CustomOriginConfig": {
                    "HttpPort": 80,
                    "HttpsPort": 443,
                    "OriginKeepaliveTimeout": 60,
                    "OriginProtocolPolicy": "match-viewer",
                    "OriginReadTimeout": 30,
                    "OriginSslProtocols": {
                      "Items": ["SSLv3", "TLSv1"],
                      "Quantity": 2
                    }
                }
            },
        ]
    },
                "DomainName": "my-bucket.s3.amazonaws.com",
                "Id": "my-origin",
                "OriginPath": "/production",
                "S3OriginConfig": {
                    "OriginAccessIdentity": "origin-access-identity/cloudfront/
E2YFS67H6VB6E4"
                }
        ]
    },
    "Status": "Deployed",
    "ViewerCertificate": {
           "AcmCertificateArn": "arn:aws:acm::123456789012:AcmCertificateArn",
           "Certificate": "ASCAJRRE5XYF52TKRY5M4",
           "CertificateSource": "iam",
           "CloudFrontDefaultCertificate": true,
           "IamCertificateId": "ASCAJRRE5XYF52TKRY5M4",
           "MinimumProtocolVersion": "TLSv1.2_2021",
           "SslSupportMethod": "sni-only"
     },
     "WebAclId": "waf-1234567890"
}
```

AwsCloudTrail

AwsCloudTrail リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsCloudTrailTrail

AwsCloudTrailTrail オブジェクトは、 AWS CloudTrail トレイルに関する詳細を表示します。

以下は、 AWS Security Finding 形式 (ASFF) の AwsCloudTrailTrail 検出の例です。AwsCloudTrailTrail 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsCloudTrailTrailDetails「」を参照してください。

例

```
"AwsCloudTrailTrail": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:CloudTrail/regression:*",
    "CloudWatchLogsRoleArn": "arn:aws:iam::866482105055:role/
CloudTrail_CloudWatchLogs",
    "HasCustomEventSelectors": true,
    "HomeRegion": "us-west-2",
    "IncludeGlobalServiceEvents": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "KmsKeyId": "kmsKeyId",
    "LogFileValidationEnabled": true,
    "Name": "regression-trail",
    "S3BucketName": "cloudtrail-bucket",
    "S3KeyPrefix": "s3KeyPrefix",
    "SnsTopicArn": "arn:aws:sns:us-east-2:123456789012:MyTopic",
    "SnsTopicName": "snsTopicName",
    "TrailArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail"
}
```

AwsCloudWatch

AwsCloudWatch リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsCloudWatchAlarm

AwsCloudWatchAlarm オブジェクトは、 CloudWatch アラームの状態が変化したときにメトリクスをモニタリングしたりアクションを実行したりする Amazon アラームに関する詳細を提供します。

次の例は、 AwsCloudWatchAlarm オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsCloudWatchAlarm 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsCloudWatchAlarmDetails「」を参照してください。

例

```
"AwsCloudWatchAlarm": {
 "ActonsEnabled": true,
 "AlarmActions": [
  "arn:aws:automate:region:ec2:stop",
  "arn:aws:automate:region:ec2:terminate"
 ],
 "AlarmArn": "arn:aws:cloudwatch:us-west-2:012345678910:alarm:sampleAlarm",
 "AlarmConfigurationUpdatedTimestamp": "2022-02-18T15:31:53.161Z",
 "AlarmDescription": "Alarm Example",
 "AlarmName": "Example",
 "ComparisonOperator": "GreaterThanOrEqualToThreshold",
 "DatapointsToAlarm": 1,
 "Dimensions": [{
  "Name": "InstanceId",
  "Value": "i-1234567890abcdef0"
 }],
 "EvaluateLowSampleCountPercentile": "evaluate",
 "EvaluationPeriods": 1,
 "ExtendedStatistic": "p99.9",
 "InsufficientDataActions": [
  "arn:aws:automate:region:ec2:stop"
 ],
 "MetricName": "Sample Metric",
 "Namespace": "YourNamespace",
 "OkActions": [
  "arn:aws:swf:region:account-id:action/actions/AWS_EC2.InstanceId.Stop/1.0"
 ],
 "Period": 1,
 "Statistic": "SampleCount",
 "Threshold": 12.3,
 "ThresholdMetricId": "t1",
 "TreatMissingData": "notBreaching",
 "Unit": "Kilobytes/Second"
}
```

AwsCodeBuild

AwsCodeBuild リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsCodeBuildProject

AwsCodeBuildProject オブジェクトは、 AWS CodeBuild プロジェクトに関する情報を提供します。

以下は、 AWS Security Finding 形式 (ASFF) の AwsCodeBuildProject 検出の例です。AwsCodeBuildProject 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsCodeBuildProjectDetails「」を参照してください。

例

```
"AwsCodeBuildProject": {
   "Artifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
   ],
   "SecondaryArtifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
   ],
   "EncryptionKey": "string",
   "Certificate": "string",
```

```
   "Environment": {
      "Certificate": "string",
      "EnvironmentVariables": [
           {
                "Name": "string",
                "Type": "string",
                "Value": "string"
           }
      ],
   "ImagePullCredentialsType": "string",
   "PrivilegedMode": boolean,
   "RegistryCredential": {
       "Credential": "string",
       "CredentialProvider": "string"
   },
   "Type": "string"
   },
   "LogsConfig": {
        "CloudWatchLogs": {
             "GroupName": "string",
             "Status": "string",
             "StreamName": "string"
        },
        "S3Logs": {
             "EncryptionDisabled": boolean,
             "Location": "string",
             "Status": "string"
        }
   },
   "Name": "string",
   "ServiceRole": "string",
   "Source": {
        "Type": "string",
        "Location": "string",
        "GitCloneDepth": integer
   },
   "VpcConfig": {
        "VpcId": "string",
        "Subnets": ["string"],
        "SecurityGroupIds": ["string"]
   }
}
```

AwsDms

AwsDms リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsDmsEndpoint

AwsDmsEndpoint オブジェクトは、 AWS Database Migration Service （ AWS DMS) エンドポイントに関する情報を提供します。エンドポイントは、データストアに関する接続、データストアタイプ、および場所情報を提供します。

次の例は、 AwsDmsEndpoint オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsDmsEndpoint 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsDmsEndpointDetails「」を参照してください。

例

```
"AwsDmsEndpoint": {
    "CertificateArn": "arn:aws:dms:us-
east-1:123456789012:cert:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWFI",
    "DatabaseName": "Test",
    "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJVBNPK6MJQVFVQA",
    "EndpointIdentifier": "target-db",
    "EndpointType": "TARGET",
    "EngineName": "mariadb",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "Port": 3306,
    "ServerName": "target-db.exampletafyu.us-east-1.rds.amazonaws.com",
    "SslMode": "verify-ca",
    "Username": "admin"
}
```

AwsDmsReplicationInstance

AwsDmsReplicationInstance オブジェクトは、 AWS Database Migration Service （ AWS DMS) レプリケーションインスタンスに関する情報を提供します。DMS はレプリケーション インスタンスを使用してソースデータストアに接続し、ソースデータを読み取り、ターゲットデータストアが使用できるようにデータをフォーマットします。

次の例は、 AwsDmsReplicationInstance オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsDmsReplicationInstance 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsDmsReplicationInstanceDetails「」を参照してください。

例

```
"AwsDmsReplicationInstance": {
    "AllocatedStorage": 50,
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1b",
    "EngineVersion": "3.5.1",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "MultiAZ": false,
    "PreferredMaintenanceWindow": "wed:08:08-wed:08:38",
    "PubliclyAccessible": true,
    "ReplicationInstanceClass": "dms.c5.xlarge",
    "ReplicationInstanceIdentifier": "second-replication-instance",
    "ReplicationSubnetGroup": {
        "ReplicationSubnetGroupIdentifier": "default-vpc-2344f44f"
    },
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-003a34e205138138b"
        }
    ]
}
```

AwsDmsReplicationTask

AwsDmsReplicationTask オブジェクトは、 AWS Database Migration Service （ AWS DMS) レプリケーションタスクに関する情報を提供します。レプリケーションタスクは、一連のデータをソースエンドポイントからターゲットエンドポイントに移動します。

次の例は、 AwsDmsReplicationInstance オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsDmsReplicationInstance 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsDmsReplicationInstance「」を参照してください。

例

```
"AwsDmsReplicationTask": {
    "CdcStartPosition": "2023-08-28T14:26:22",
```

```
    "Id": "arn:aws:dms:us-
east-1:123456789012:task:YDYUOHZIXWKQSUCBMUCQCNY44SJW74VJNB5DFWQ",
    "MigrationType": "cdc",
    "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4YOUGIMYJUI",
    "ReplicationTaskIdentifier": "test-task",
    "ReplicationTaskSettings": "{\"Logging\":{\"EnableLogging\":false,
\"EnableLogContext\":false,\"LogComponents\":[{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"TRANSFORMATION\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",
\"Id\":\"SOURCE_UNLOAD\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"IO\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TARGET_LOAD\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"PERFORMANCE\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SOURCE_CAPTURE\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SORTER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"REST_SERVER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id
\":\"VALIDATOR_EXT\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"TARGET_APPLY\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TASK_MANAGER
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TABLES_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"METADATA_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_FACTORY\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMON\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"ADDONS\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"DATA_STRUCTURE
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMUNICATION\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_TRANSFER\"}],\"CloudWatchLogGroup
\":null,\"CloudWatchLogStream\":null},\"StreamBufferSettings\":{\"StreamBufferCount
\":3,\"CtrlStreamBufferSizeInMB\":5,\"StreamBufferSizeInMB\":8},\"ErrorBehavior
\":{\"FailOnNoTablesCaptured\":true,\"ApplyErrorUpdatePolicy\":\"LOG_ERROR\",
\"FailOnTransactionConsistencyBreached\":false,\"RecoverableErrorThrottlingMax\":1800,
\"DataErrorEscalationPolicy\":\"SUSPEND_TABLE\",\"ApplyErrorEscalationCount\":0,
\"RecoverableErrorStopRetryAfterThrottlingMax\":true,\"RecoverableErrorThrottling
\":true,\"ApplyErrorFailOnTruncationDdl\":false,\"DataTruncationErrorPolicy\":
\"LOG_ERROR\",\"ApplyErrorInsertPolicy\":\"LOG_ERROR\",\"EventErrorPolicy\":
\"IGNORE\",\"ApplyErrorEscalationPolicy\":\"LOG_ERROR\",\"RecoverableErrorCount
\":-1,\"DataErrorEscalationCount\":0,\"TableErrorEscalationPolicy\":\"STOP_TASK
\",\"RecoverableErrorInterval\":5,\"ApplyErrorDeletePolicy\":\"IGNORE_RECORD\",
\"TableErrorEscalationCount\":0,\"FullLoadIgnoreConflicts\":true,\"DataErrorPolicy
\":\"LOG_ERROR\",\"TableErrorPolicy\":\"SUSPEND_TABLE\"},\"TTSettings
\":{\"TTS3Settings\":null,\"TTRecordSettings\":null,\"EnableTT\":false},
\"FullLoadSettings\":{\"CommitRate\":10000,\"StopTaskCachedChangesApplied
\":false,\"StopTaskCachedChangesNotApplied\":false,\"MaxFullLoadSubTasks
\":8,\"TransactionConsistencyTimeout\":600,\"CreatePkAfterFullLoad\":false,
\"TargetTablePrepMode\":\"DO_NOTHING\"},\"TargetMetadata\":{\"ParallelApplyBufferSize
\":0,\"ParallelApplyQueuesPerThread\":0,\"ParallelApplyThreads\":0,\"TargetSchema
\":\"\",\"InlineLobMaxSize\":0,\"ParallelLoadQueuesPerThread\":0,\"SupportLobs
```

```
\":true,\"LobChunkSize\":64,\"TaskRecoveryTableEnabled\":false,\"ParallelLoadThreads
\":0,\"LobMaxSize\":0,\"BatchApplyEnabled\":false,\"FullLobMode\":true,
\"LimitedSizeLobMode\":false,\"LoadMaxFileSize\":0,\"ParallelLoadBufferSize\":0},
\"BeforeImageSettings\":null,\"ControlTablesSettings\":{\"historyTimeslotInMinutes
\":5,\"HistoryTimeslotInMinutes\":5,\"StatusTableEnabled\":false,
\"SuspendedTablesTableEnabled\":false,\"HistoryTableEnabled\":false,\"ControlSchema
\":\"\",\"FullLoadExceptionTableEnabled\":false},\"LoopbackPreventionSettings
\":null,\"CharacterSetSettings\":null,\"FailTaskWhenCleanTaskResourceFailed
\":false,\"ChangeProcessingTuning\":{\"StatementCacheSize\":50,\"CommitTimeout
\":1,\"BatchApplyPreserveTransaction\":true,\"BatchApplyTimeoutMin\":1,
\"BatchSplitSize\":0,\"BatchApplyTimeoutMax\":30,\"MinTransactionSize\":1000,
\"MemoryKeepTime\":60,\"BatchApplyMemoryLimit\":500,\"MemoryLimitTotal\":1024},
\"ChangeProcessingDdlHandlingPolicy\":{\"HandleSourceTableDropped\":true,
\"HandleSourceTableTruncated\":true,\"HandleSourceTableAltered\":true},
\"PostProcessingRules\":null}",
    "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:TZPWV2VCXEGHYOKVKRNHAKJ4Q3RUXACNGFGYWRI",
    "TableMappings": "{\"rules\":[{\"rule-type\":\"selection\",\"rule-id\":
\"969761702\",\"rule-name\":\"969761702\",\"object-locator\":{\"schema-name\":\"%table
\",\"table-name\":\"%example\"},\"rule-action\":\"exclude\",\"filters\":[]}]}",
    "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:ABR8LBOQB3CZY33F7XV253NAJVBNPK6MJQVFVQA"
}
```

AwsDynamoDB

AwsDynamoDB リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsDynamoDbTable

AwsDynamoDbTable オブジェクトは、Amazon DynamoDB テーブルに関する詳細を表示します。

以下は、 AWS Security Finding 形式 (ASFF) の AwsDynamoDbTable 検出の例です。AwsDynamoDbTable 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsDynamoDbTableDetails「」を参照してください。

例

```
"AwsDynamoDbTable": {
    "AttributeDefinitions": [
        {
            "AttributeName": "attribute1",
            "AttributeType": "value 1"
        },
```

```
        {
            "AttributeName": "attribute2",
            "AttributeType": "value 2"
        },
        {
            "AttributeName": "attribute3",
            "AttributeType": "value 3"
        }
    ],
    "BillingModeSummary": {
        "BillingMode": "PAY_PER_REQUEST",
        "LastUpdateToPayPerRequestDateTime": "2019-12-03T15:23:10.323Z"
    },
    "CreationDateTime": "2019-12-03T15:23:10.248Z",
    "DeletionProtectionEnabled": true,
    "GlobalSecondaryIndexes": [
        {
            "Backfilling": false,
            "IndexArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
index/exampleIndex",
            "IndexName": "standardsControlArnIndex",
            "IndexSizeBytes": 1862513,
            "IndexStatus": "ACTIVE",
            "ItemCount": 20,
            "KeySchema": [
                {
                    "AttributeName": "City",
                    "KeyType": "HASH"
                },
                {
                    "AttributeName": "Date",
                    "KeyType": "RANGE"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
            "ProvisionedThroughput": {
                "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
                "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
                "NumberOfDecreasesToday": 0,
                "ReadCapacityUnits": 100,
                "WriteCapacityUnits": 50
```

```
            },
        }
    ],
    "GlobalTableVersion": "V1",
    "ItemCount": 2705,
    "KeySchema": [
        {
            "AttributeName": "zipcode",
            "KeyType": "HASH"
        }
     ],
     "LatestStreamArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
stream/2019-12-03T23:23:10.248",
    "LatestStreamLabel": "2019-12-03T23:23:10.248",
    "LocalSecondaryIndexes": [
        {
            "IndexArn": "arn:aws:dynamodb:us-east-1:111122223333:table/exampleGroup/
index/exampleId",
            "IndexName": "CITY_DATE_INDEX_NAME",
            "KeySchema": [
                {
                    "AttributeName": "zipcode",
                    "KeyType": "HASH"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
        }
    ],
    "ProvisionedThroughput": {
        "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
        "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
        "NumberOfDecreasesToday": 0,
        "ReadCapacityUnits": 100,
        "WriteCapacityUnits": 50
    },
    "Replicas": [
        {
            "GlobalSecondaryIndexes":[
                {
                    "IndexName": "CITY_DATE_INDEX_NAME",
                    "ProvisionedThroughputOverride": {
```

```
                        "ReadCapacityUnits": 10
                    }
                }
            ],
            "KmsMasterKeyId" : "KmsKeyId"
            "ProvisionedThroughputOverride": {
                "ReadCapacityUnits": 10
            },
            "RegionName": "regionName",
            "ReplicaStatus": "CREATING",
            "ReplicaStatusDescription": "replicaStatusDescription"
        }
    ],
    "RestoreSummary" : {
        "SourceBackupArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
backup/backup1",
        "SourceTableArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable",
        "RestoreDateTime": "2020-06-22T17:40:12.322Z",
        "RestoreInProgress": true
    },
    "SseDescription": {
        "InaccessibleEncryptionDateTime": "2018-01-26T23:50:05.000Z",
        "Status": "ENABLED",
        "SseType": "KMS",
        "KmsMasterKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key1"
    },
    "StreamSpecification" : {
        "StreamEnabled": true,
        "StreamViewType": "NEW_IMAGE"
    },
    "TableId": "example-table-id-1",
    "TableName": "example-table",
    "TableSizeBytes": 1862513,
    "TableStatus": "ACTIVE"
}
```

AwsEc2

AwsEc2 リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsEc2ClientVpnEndpoint

AwsEc2ClientVpnEndpoint オブジェクトは、 AWS Client VPN エンドポイントに関する情報を提供します。クライアント VPN エンドポイントは、クライアント VPN セッションを有効にして管

理するために作成して設定するリソースです。これは、すべてのクライアント VPN セッションの終了ポイントです。

次の例は、 AwsEc2ClientVpnEndpoint オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEc2ClientVpnEndpoint 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEc「2ClientVpnEndpointDetails」を参照してください。

例

```
"AwsEc2ClientVpnEndpoint": {
    "AuthenticationOptions": [
        {
            "MutualAuthentication": {
                "ClientRootCertificateChainArn": "arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            },
            "Type": "certificate-authentication"
        }
    ],
    "ClientCidrBlock": "10.0.0.0/22",
    "ClientConnectOptions": {
        "Enabled": false
    },
    "ClientLoginBannerOptions": {
        "Enabled": false
    },
    "ClientVpnEndpointId": "cvpn-endpoint-00c5d11fc4729f2a5",
    "ConnectionLogOptions": {
        "Enabled": false
    },
    "Description": "test",
    "DnsServer": ["10.0.0.0"],
    "ServerCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "SecurityGroupIdSet": [
        "sg-0f7a177b82b443691"
    ],
    "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/endpoints/
cvpn-endpoint-00c5d11fc4729f2a5",
    "SessionTimeoutHours": 24,
    "SplitTunnel": false,
    "TransportProtocol": "udp",
    "VpcId": "vpc-1a2b3c4d5e6f1a2b3",
```

```
    "VpnPort": 443
}
```

AwsEc2Eip

AwsEc2Eip オブジェクトは、Elastic IP アドレスに関する情報を提供します。

次の例は、 AwsEc2Eip オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEc2Eip 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEc「2EipDetails」を参照してください。

例

```
"AwsEc2Eip": {
    "InstanceId": "instance1",
    "PublicIp": "192.0.2.04",
    "AllocationId": "eipalloc-example-id-1",
    "AssociationId": "eipassoc-example-id-1",
    "Domain": "vpc",
    "PublicIpv4Pool": "anycompany",
    "NetworkBorderGroup": "eu-central-1",
    "NetworkInterfaceId": "eni-example-id-1",
    "NetworkInterfaceOwnerId": "777788889999",
    "PrivateIpAddress": "192.0.2.03"
}
```

AwsEc2Instance

AwsEc2Instance オブジェクトは、Amazon EC2 インスタンスの詳細を提供します。

次の例は、 AwsEc2Instance オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEc2Instance 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEc「2InstanceDetails」を参照してください。

例

```
"AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
    "ImageId": "ami-1234",
    "IpV4Addresses": [ "1.1.1.1" ],
    "IpV6Addresses": [ "2001:db8:1234:1a2b::123" ],
    "KeyName": "my_keypair",
    "LaunchedAt": "2018-05-08T16:46:19.000Z",
```

```
    "MetadataOptions": {
     "HttpEndpoint": "enabled",
     "HttpProtocolIpv6": "enabled",
     "HttpPutResponseHopLimit": 1,
     "HttpTokens": "optional",
     "InstanceMetadataTags": "disabled",
    },
    "Monitoring": {
     "State": "disabled"
    },
    "NetworkInterfaces": [
      {
         "NetworkInterfaceId": "eni-e5aa89a3"
      }
    ],
    "SubnetId": "subnet-123",
    "Type": "i3.xlarge",
    "VpcId": "vpc-123"
}
```

AwsEc2LaunchTemplate

`AwsEc2LaunchTemplate` オブジェクトには、インスタンス設定情報を指定する Amazon Elastic Compute Cloud の起動テンプレートに関する詳細が含まれています。

次の例は、 `AwsEc2LaunchTemplate` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEc2LaunchTemplate` 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEc「2LaunchTemplateDetails」を参照してください。

例

```
"AwsEc2LaunchTemplate": {
    "DefaultVersionNumber": "1",
    "ElasticGpuSpecifications": ["string"],
    "ElasticInferenceAccelerators": ["string"],
    "Id": "lt-0a16e9802800bdd85",
    "ImageId": "ami-0d5eff06f840b45e9",
    "LatestVersionNumber": "1",
    "LaunchTemplateData": {
     "BlockDeviceMappings": [{
      "DeviceName": "/dev/xvda",
      "Ebs": {
       "DeleteonTermination": true,
```

```
        "Encrypted": true,
        "SnapshotId": "snap-01047646ec075f543",
        "VolumeSize": 8,
        "VolumeType:" "gp2"
       }
      }],
      "MetadataOptions": {
       "HttpTokens": "enabled",
       "HttpPutResponseHopLimit" : 1
      },
      "Monitoring": {
       "Enabled": true,
      "NetworkInterfaces": [{
       "AssociatePublicIpAddress" : true,
      }],
    "LaunchTemplateName": "string",
    "LicenseSpecifications": ["string"],
    "SecurityGroupIds": ["sg-01fce87ad6e019725"],
    "SecurityGroups": ["string"],
    "TagSpecifications": ["string"]
}
```

AwsEc2NetworkAcl

AwsEc2NetworkAcl オブジェクトには、Amazon EC2 ネットワークアクセスコントロールリスト (ACL) の詳細が含まれています。

次の例は、 AwsEc2NetworkAcl オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEc2NetworkAcl 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEc「2NetworkAclDetails」を参照してください。

例

```
"AwsEc2NetworkAcl": {
    "IsDefault": false,
    "NetworkAclId": "acl-1234567890abcdef0",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234abcd",
    "Associations": [{
        "NetworkAclAssociationId": "aclassoc-abcd1234",
        "NetworkAclId": "acl-021345abcdef6789",
        "SubnetId": "subnet-abcd1234"
   }],
```

```
   "Entries": [{
        "CidrBlock": "10.24.34.0/23",
        "Egress": true,
        "IcmpTypeCode": {
            "Code": 10,
            "Type": 30
        },
        "Ipv6CidrBlock": "2001:DB8::/32",
        "PortRange": {
            "From": 20,
            "To": 40
        },
        "Protocol": "tcp",
        "RuleAction": "allow",
        "RuleNumber": 100
   }]
}
```

AwsEc2NetworkInterface

AwsEc2NetworkInterface オブジェクトは、Amazon EC2 ネットワークインターフェイスに関する情報を提供します。

次の例は、 AwsEc2NetworkInterface オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEc2NetworkInterface 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEc「2NetworkInterfaceDetails」を参照してください。

例

```
"AwsEc2NetworkInterface": {
    "Attachment": {
        "AttachTime": "2019-01-01T03:03:21Z",
        "AttachmentId": "eni-attach-43348162",
        "DeleteOnTermination": true,
        "DeviceIndex": 123,
        "InstanceId": "i-1234567890abcdef0",
        "InstanceOwnerId": "123456789012",
        "Status": 'ATTACHED'
    },
    "SecurityGroups": [
        {
            "GroupName": "my-security-group",
            "GroupId": "sg-903004f8"
```

```
        },
    ],
    "NetworkInterfaceId": 'eni-686ea200',
    "SourceDestCheck": false
}
```

AwsEc2RouteTable

`AwsEc2RouteTable` オブジェクトは、Amazon EC2 ルートテーブルに関する情報を提供します。

次の例は、 `AwsEc2RouteTable` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEc2RouteTable` 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEc「2RouteTableDetails」を参照してください。

例

```
"AwsEc2RouteTable": {
    "AssociationSet": [{
     "AssociationSet": {
      "State": "associated"
        },
     "Main": true,
     "RouteTableAssociationId": "rtbassoc-08e706c45de9f7512",
     "RouteTableId": "rtb-0a59bde9cf2548e34",
    }],
    "PropogatingVgwSet": [],
    "RouteTableId": "rtb-0a59bde9cf2548e34",
    "RouteSet": [
     {
      "DestinationCidrBlock": "10.24.34.0/23",
      "GatewayId": "local",
      "Origin": "CreateRouteTable",
      "State": "active"
     },
     {
      "DestinationCidrBlock": "10.24.34.0/24",
      "GatewayId": "igw-0242c2d7d513fc5d3",
      "Origin": "CreateRoute",
      "State": "active"
     }
    ],
    "VpcId": "vpc-0c250a5c33f51d456"
}
```

AwsEc2SecurityGroup

AwsEc2SecurityGroup オブジェクトは、Amazon EC2 セキュリティグループについての説明を表示します。

次の例は、 AwsEc2SecurityGroup オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEc2SecurityGroup 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEc「2SecurityGroupDetails」を参照してください。

例

```
"AwsEc2SecurityGroup": {
    "GroupName": "MySecurityGroup",
    "GroupId": "sg-903004f8",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1a2b3c4d",
    "IpPermissions": [
        {
            "IpProtocol": "-1",
            "IpRanges": [],
            "UserIdGroupPairs": [
                {
                    "UserId": "123456789012",
                    "GroupId": "sg-903004f8"
                }
            ],
            "PrefixListIds": [
                {"PrefixListId": "pl-63a5400a"}
            ]
        },
        {
            "PrefixListIds": [],
            "FromPort": 22,
            "IpRanges": [
                {
                    "CidrIp": "203.0.113.0/24"
                }
            ],
            "ToPort": 22,
            "IpProtocol": "tcp",
            "UserIdGroupPairs": []
        }
    ]
```

```
}
```

AwsEc2Subnet

AwsEc2Subnetオブジェクトは、Amazon EC2 内のサブネットに関する情報を提供します。

次の例は、 AwsEc2Subnet オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEc2Subnet 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEc「2SubnetDetails」を参照してください。

例

```
AwsEc2Subnet: {
    "AssignIpv6AddressOnCreation": false,
    "AvailabilityZone": "us-west-2c",
    "AvailabilityZoneId": "usw2-az3",
    "AvailableIpAddressCount": 8185,
    "CidrBlock": "10.0.0.0/24",
    "DefaultForAz": false,
    "MapPublicIpOnLaunch": false,
    "OwnerId": "123456789012",
    "State": "available",
    "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/subnet-d5436c93",
    "SubnetId": "subnet-d5436c93",
    "VpcId": "vpc-153ade70",
    "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "subnet-cidr-assoc-EXAMPLE",
        "Ipv6CidrBlock": "2001:DB8::/32",
        "CidrBlockState": "associated"
   }]
}
```

AwsEc2TransitGateway

AwsEc2TransitGateway オブジェクトは、仮想プライベートクラウド (VPC) とオンプレミスネットワークを相互接続する Amazon EC2 トランジットゲートウェイに関する詳細を提供します。

AWS Security Finding 形式 (ASFF) AwsEc2TransitGatewayの結果の例を次に示します。AwsEc2TransitGateway 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEc「2TransitGatewayDetails」を参照してください。

例

```
"AwsEc2TransitGateway": {
 "AmazonSideAsn": 65000,
 "AssociationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "AutoAcceptSharedAttachments": "disable",
 "DefaultRouteTableAssociation": "enable",
 "DefaultRouteTablePropagation": "enable",
 "Description": "sample transit gateway",
 "DnsSupport": "enable",
 "Id": "tgw-042ae6bf7a5c126c3",
 "MulticastSupport": "disable",
 "PropagationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "TransitGatewayCidrBlocks": ["10.0.0.0/16"],
 "VpnEcmpSupport": "enable"
}
```

AwsEc2Volume

AwsEc2Volume オブジェクトは、Amazon EC2 ボリュームに関する詳細を提供します。

次の例は、 AwsEc2Volume オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEc2Volume 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEc「2VolumeDetails」を参照してください。

例

```
"AwsEc2Volume": {
    "Attachments": [
      {
        "AttachTime": "2017-10-17T14:47:11Z",
        "DeleteOnTermination": true,
        "InstanceId": "i-123abc456def789g",
        "Status": "attached"
      }
     ],
    "CreateTime": "2020-02-24T15:54:30Z",
    "Encrypted": true,
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "Size": 80,
    "SnapshotId": "",
    "Status": "available"
}
```

AwsEc2Vpc

AwsEc2Vpc オブジェクトは、Amazon EC2 VPC の詳細を提供します。

次の例は、 AwsEc2Vpc オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEc2Vpc 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEc「2VpcDetails」を参照してください。

例

```
"AwsEc2Vpc": {
    "CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlock": "192.0.2.0/24",
            "CidrBlockState": "associated"
        }
    ],
    "DhcpOptionsId": "dopt-4e42ce28",
    "Ipv6CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlockState": "associated",
            "Ipv6CidrBlock": "192.0.2.0/24"
       }

    ],
    "State": "available"
}
```

AwsEc2VpcEndpointService

AwsEc2VpcEndpointService オブジェクトには、VPC エンドポイントサービスの設定に関する詳細が含まれています。

次の例は、 AwsEc2VpcEndpointService オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEc2VpcEndpointService 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEc「2VpcEndpointServiceDetails」を参照してください。

例

```
"AwsEc2VpcEndpointService": {
```

```
    "ServiceType": [
      {
        "ServiceType": "Interface"
      }
    ],
    "ServiceId": "vpce-svc-example1",
    "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example1",
    "ServiceState": "Available",
    "AvailabilityZones": [
      "us-east-1"
    ],
    "AcceptanceRequired": true,
    "ManagesVpcEndpoints": false,
    "NetworkLoadBalancerArns": [
      "arn:aws:elasticloadbalancing:us-east-1:444455556666:loadbalancer/net/my-network-
load-balancer/example1"
    ],
    "GatewayLoadBalancerArns": [],
    "BaseEndpointDnsNames": [
      "vpce-svc-04eec859668b51c34.us-east-1.vpce.amazonaws.com"
    ],
    "PrivateDnsName": "my-private-dns"
}
```

AwsEc2VpcPeeringConnection

`AwsEc2VpcPeeringConnection` オブジェクトは、2 つの VPC 間のネットワーク接続に関する詳細を表示します。

次の例は、 `AwsEc2VpcPeeringConnection` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEc2VpcPeeringConnection` 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEc「2VpcPeeringConnectionDetails」を参照してください。

例

```
"AwsEc2VpcPeeringConnection": {
 "AccepterVpcInfo": {
  "CidrBlock": "10.0.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "10.0.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
```

```
    "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
   }],
   "OwnerId": "012345678910",
   "PeeringOptions": {
    "AllowDnsResolutionFromRemoteVpc": true,
    "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
    "AllowEgressFromLocalVpcToRemoteClassicLink": true
   },
   "Region": "us-west-2",
   "VpcId": "vpc-i123456"
  },
  "ExpirationTime": "2022-02-18T15:31:53.161Z",
  "RequesterVpcInfo": {
   "CidrBlock": "192.168.0.0/28",
   "CidrBlockSet": [{
    "CidrBlock": "192.168.0.0/28"
   }],
   "Ipv6CidrBlockSet": [{
    "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
   }],
   "OwnerId": "012345678910",
   "PeeringOptions": {
    "AllowDnsResolutionFromRemoteVpc": true,
    "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
    "AllowEgressFromLocalVpcToRemoteClassicLink": true
   },
   "Region": "us-west-2",
   "VpcId": "vpc-i123456"
  },
  "Status": {
   "Code": "initiating-request",
   "Message": "Active"
  },
  "VpcPeeringConnectionId": "pcx-1a2b3c4d"
}
```


AwsEc2VpnConnection

AwsEc2VpnConnection オブジェクトは、Amazon EC2 VPN 接続の詳細を提供します。

次の例は、 AwsEc2VpnConnection オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEc2VpnConnection 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEc「2VpnConnectionDetails」を参照してください。

例

```
"AwsEc2VpnConnection": {
    "VpnConnectionId": "vpn-205e4f41",
    "State": "available",
    "CustomerGatewayConfiguration": "",
    "CustomerGatewayId": "cgw-5699703f",
    "Type": "ipsec.1",
    "VpnGatewayId": "vgw-2ccb2245",
    "Category": "VPN"
    "TransitGatewayId": "tgw-09b6f3a659e2b5elf",
    "VgwTelemetry": [
        {
            "OutsideIpAddress": "92.0.2.11",
            "Status": "DOWN",
            "LastStatusChange": "2016-11-11T23:09:32.000Z",
            "StatusMessage": "IPSEC IS DOWN",
            "AcceptedRouteCount": 0
        },
        {
            "OutsideIpAddress": "92.0.2.12",
            "Status": "DOWN",
            "LastStatusChange": "2016-11-11T23:10:51.000Z",
            "StatusMessage": "IPSEC IS DOWN",
            "AcceptedRouteCount": 0
        }
    ],
    "Routes": [{
        "DestinationCidrBlock": "10.24.34.0/24",
        "State": "available"
   }],
    "Options": {
        "StaticRoutesOnly": true
        "TunnelOptions": [{
            "DpdTimeoutSeconds": 30,
            "IkeVersions": ["ikev1", "ikev2"],
            "Phase1DhGroupNumbers": [14, 15, 16, 17, 18},
            "Phase1EncryptionAlgorithms": ["AES128", "AES256"],
            "Phase1IntegrityAlgorithms": ["SHA1", "SHA2-256"],
            "Phase1LifetimeSeconds": 28800,
            "Phase2DhGroupNumbers": [14, 15, 16, 17, 18],
            "Phase2EncryptionAlgorithms": ["AES128", "AES256"],
            "Phase2IntegrityAlgorithms": ["SHA1", "SHA2-256"],
            "Phase2LifetimeSeconds": 28800,
```

```
            "PreSharedKey": "RltXC3REhTw1RAdiM2s1uMfkkSDLyGJoe1QEWeGxqkQ=",
            "RekeyFuzzPercentage": 100,
            "RekeyMarginTimeSeconds": 540,
            "ReplayWindowSize": 1024,
            "TunnelInsideCidr": "10.24.34.0/23"
        }]
   }
}
```

AwsEcr

AwsEcr リソース AWS のセキュリティ検出結果形式の例を次に示します。

AwsEcrContainerImage

AwsEcrContainerImage オブジェクトは、Amazon ECR イメージに関する情報を提供します。

次の例は、 AwsEcrContainerImage オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEcrContainerImage 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEcrContainerImageDetails「」を参照してください。

例

```
"AwsEcrContainerImage": {
    "RegistryId": "123456789012",
    "RepositoryName": "repository-name",
    "Architecture": "amd64"
    "ImageDigest":
 "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
    "ImageTags": ["00000000-0000-0000-0000-000000000000"],
    "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

AwsEcrRepository オブジェクトは、Amazon Elastic Container Registry リポジトリに関する情報を提供します。

次の例は、 AwsEcrRepository オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEcrRepository 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEcrRepositoryDetails「」を参照してください。

例

```
"AwsEcrRepository": {
    "LifecyclePolicy": {
        "RegistryId": "123456789012",
    },
    "RepositoryName": "sample-repo",
    "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
    "ImageScanningConfiguration": {
        "ScanOnPush": true
    },
    "ImageTagMutability": "IMMUTABLE"
}
```

AwsEcs

AwsEcs リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsEcsCluster

AwsEcsCluster オブジェクトは、Amazon Elastic Container Service クラスターに関する詳細を提供します。

次の例は、 AwsEcsCluster オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEcsCluster 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEcsClusterDetails「」を参照してください。

例

```
    "AwsEcsCluster": {
        "CapacityProviders": [],
        "ClusterSettings": [
            {
                "Name": "containerInsights",
                "Value": "enabled"
            }
        ],
        "Configuration": {
            "ExecuteCommandConfiguration": {
                "KmsKeyId": "kmsKeyId",
                "LogConfiguration": {
                    "CloudWatchEncryptionEnabled": true,
                    "CloudWatchLogGroupName": "cloudWatchLogGroupName",
                    "S3BucketName": "s3BucketName",
                    "S3EncryptionEnabled": true,
```

```
                    "S3KeyPrefix": "s3KeyPrefix"
                },
                "Logging": "DEFAULT"
            }
        }
        "DefaultCapacityProviderStrategy": [
            {
                "Base": 0,
                "CapacityProvider": "capacityProvider",
                "Weight": 1
            }
        ]
    }
```

AwsEcsContainer

AwsEcsContainer オブジェクトには、Amazon ECS コンテナの詳細が含まれています。

次の例は、 AwsEcsContainer オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEcsContainer 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEcsContainerDetails「」を参照してください。

例

```
"AwsEcsContainer": {
    "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
    "MountPoints": [{
        "ContainerPath": "/mnt/etc",
        "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
}
```

AwsEcsService

AwsEcsService オブジェクトは、Amazon ECS クラスター内のサービスに関する詳細を提供します。

次の例は、 AwsEcsService オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEcsService 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEcsServiceDetails「」を参照してください。

例

```
"AwsEcsService": {
    "CapacityProviderStrategy": [
        {
            "Base": 12,
            "CapacityProvider": "",
            "Weight": ""
        }
    ],
    "Cluster": "arn:aws:ecs:us-east-1:111122223333:cluster/example-ecs-cluster",
    "DeploymentConfiguration": {
        "DeploymentCircuitBreaker": {
            "Enable": false,
            "Rollback": false
        },
        "MaximumPercent": 200,
        "MinimumHealthyPercent": 100
    },
    "DeploymentController": "",
    "DesiredCount": 1,
    "EnableEcsManagedTags": false,
    "EnableExecuteCommand": false,
    "HealthCheckGracePeriodSeconds": 1,
    "LaunchType": "FARGATE",
    "LoadBalancers": [
        {
            "ContainerName": "",
            "ContainerPort": 23,
            "LoadBalancerName": "",
            "TargetGroupArn": ""
        }
    ],
    "Name": "sample-app-service",
    "NetworkConfiguration": {
        "AwsVpcConfiguration": {
            "Subnets": [
                "Subnet-example1",
                "Subnet-example2"
            ],
        "SecurityGroups": [
                "Sg-0ce48e9a6e5b457f5"
        ],
        "AssignPublicIp": "ENABLED"
```

```
        }
    },
    "PlacementConstraints": [
        {
            "Expression": "",
            "Type": ""
        }
    ],
    "PlacementStrategies": [
        {
            "Field": "",
            "Type": ""
        }
    ],
    "PlatformVersion": "LATEST",
    "PropagateTags": "",
    "Role": "arn:aws:iam::111122223333:role/aws-servicerole/ecs.amazonaws.com/
ServiceRoleForECS",
    "SchedulingStrategy": "REPLICA",
    "ServiceName": "sample-app-service",
    "ServiceArn": "arn:aws:ecs:us-east-1:111122223333:service/example-ecs-cluster/
sample-app-service",
    "ServiceRegistries": [
        {
            "ContainerName": "",
            "ContainerPort": 1212,
            "Port": 1221,
            "RegistryArn": ""
        }
    ],
    "TaskDefinition": "arn:aws:ecs:us-east-1:111122223333:task-definition/example-
taskdef:1"
}
```

AwsEcsTask

`AwsEcsTask` オブジェクトは、Amazon ECS タスクの詳細を提供します。

次の例は、 `AwsEcsTask` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEcsTask` 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」の[AwsEcsTask](#)「」を参照してください。

例

```
"AwsEcsTask": {
 "ClusterArn": "arn:aws:ecs:us-west-2:123456789012:task/MyCluster/1234567890123456789",
 "CreatedAt": "1557134011644",
 "Group": "service:fargate-service",
 "StartedAt": "1557134011644",
 "StartedBy": "ecs-svc/1234567890123456789",
 "TaskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-definition/sample-
fargate:2",
 "Version": 3,
 "Volumes": [{
  "Name": "string",
  "Host": {
   "SourcePath": "string"
  }
 }],
 "Containers": {
  "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
   "ContainerPath": "/mnt/etc",
   "SourceVolume": "vol-03909e9"
  }],
  "Name": "knote",
  "Privileged": true
 }
}
```

AwsEcsTaskDefinition

AwsEcsTaskDefinition オブジェクトには、タスク定義に関する詳細が含まれています。タスク定義は、Amazon Elastic Container Service タスクのコンテナとボリューム定義について説明しています。

次の例は、 AwsEcsTaskDefinition オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEcsTaskDefinition 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEcsTaskDefinitionDetails「」を参照してください。

例

```
    "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [
            {
```

```
                "Command": ['ruby', 'hi.rb'],
                "Cpu":128,
                "Essential": true,
                "HealthCheck": {
                    "Command": ["CMD-SHELL", "curl -f http://localhost/ || exit 1"],
                    "Interval": 10,
                    "Retries": 3,
                    "StartPeriod": 5,
                    "Timeout": 20
                },
                "Image": "tongueroo/sinatra:latest",
                "Interactive": true,
                "Links": [],
                "LogConfiguration": {
                    "LogDriver": "awslogs",
                    "Options": {
                        "awslogs-group": "/ecs/sinatra-hi",
                        "awslogs-region": "ap-southeast-1",
                        "awslogs-stream-prefix": "ecs"
                    },
                    "SecretOptions": []

                },
                "MemoryReservation": 128,
                "Name": "web",
                "PortMappings": [
                    {
                        "ContainerPort": 4567,
                        "HostPort":4567,
                        "Protocol": "tcp"
                    }
                ],
                "Privileged": true,
                "StartTimeout": 10,
                "StopTimeout": 100,
            }
        ],
        "Family": "sinatra-hi",
        "NetworkMode": "host",
        "RequiresCompatibilities": ["EC2"],
        "Status": "ACTIVE",
        "TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
    }
```

AwsEfs

AwsEfs リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsEfsAccessPoint

AwsEfsAccessPoint オブジェクトは Amazon Elastic File System に保存されているファイルに関する詳細を表示します。

次の例は、 AwsEfsAccessPoint オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEfsAccessPoint 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEfsAccessPointDetails「」を参照してください。

例

```
"AwsEfsAccessPoint": {
 "AccessPointId": "fsap-05c4c0e79ba0b118a",
 "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/
fsap-05c4c0e79ba0b118a",
 "ClientToken": "AccessPointCompliant-ASk06ZZSXsEp",
 "FileSystemId": "fs-0f8137f731cb32146",
 "PosixUser": {
  "Gid": "1000",
  "SecondaryGids": ["0", "4294967295"],
  "Uid": "1234"
 },
 "RootDirectory": {
  "CreationInfo": {
   "OwnerGid": "1000",
   "OwnerUid": "1234",
   "Permissions": "777"
  },
  "Path": "/tmp/example"
 }
}
```

AwsEks

AwsEks リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsEksCluster

AwsEksCluster オブジェクトは、Amazon EKS クラスターに関する詳細を提供します。

次の例は、 AwsEksCluster オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEksCluster 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEksClusterDetails「」を参照してください。

例

```
{
  "AwsEksCluster": {
    "Name": "example",
    "Arn": "arn:aws:eks:us-west-2:222222222222:cluster/example",
    "CreatedAt": 1565804921.901,
    "Version": "1.12",
    "RoleArn": "arn:aws:iam::222222222222:role/example-cluster-
ServiceRole-1XWBQWYSFRE2Q",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": false,
      "SubnetIds": [
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    },
    "Logging": {
      "ClusterLogging": [
        {
          "Types": [
            "api",
            "audit",
            "authenticator",
            "controllerManager",
            "scheduler"
          ],
          "Enabled": true
        }
      ]
    },
    "Status": "CREATING",
    "CertificateAuthorityData": {},
  }
}
```

AwsElasticBeanstalk

AwsElasticBeanstalk リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsElasticBeanstalkEnvironment

AwsElasticBeanstalkEnvironment オブジェクトには、 AWS Elastic Beanstalk 環境に関する詳細が含まれています。

次の例は、 AwsElasticBeanstalkEnvironment オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsElasticBeanstalkEnvironment 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsElasticBeanstalkEnvironmentDetails「」を参照してください。

例

```
"AwsElasticBeanstalkEnvironment": {
    "ApplicationName": "MyApplication",
    "Cname": "myexampleapp-env.devo-2.elasticbeanstalk-internal.com",
    "DateCreated": "2021-04-30T01:38:01.090Z",
    "DateUpdated": "2021-04-30T01:38:01.090Z",
    "Description": "Example description of my awesome application",
    "EndpointUrl": "eb-dv-e-p-AWSEBLoa-abcdef01234567890-021345abcdef6789.us-
east-1.elb.amazonaws.com",
    "EnvironmentArn": "arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/
MyApplication/myapplication-env",
    "EnvironmentId": "e-abcd1234",
    "EnvironmentLinks": [
        {
            "EnvironmentName": "myexampleapp-env",
            "LinkName": "myapplicationLink"
        }
    ],
    "EnvironmentName": "myapplication-env",
    "OptionSettings": [
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSize",
            "Value": "100"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "Timeout",
```

```
            "Value": "600"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSizeType",
            "Value": "Percentage"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "IgnoreHealthCheck",
            "Value": "false"
        },
        {
            "Namespace": "aws:elasticbeanstalk:application",
            "OptionName": "Application Healthcheck URL",
            "Value": "TCP:80"
        }
    ],
    "PlatformArn": "arn:aws:elasticbeanstalk:us-east-1::platform/Tomcat 8 with Java 8
 running on 64bit Amazon Linux/2.7.7",
    "SolutionStackName": "64bit Amazon Linux 2017.09 v2.7.7 running Tomcat 8 Java 8",
    "Status": "Ready",
    "Tier": {
        "Name": "WebServer"
       "Type": "Standard"
       "Version": "1.0"
    },
    "VersionLabel": "Sample Application"
}
```

AwsElasticSearch

AwsElasticSearch リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsElasticSearchDomain

AwsElasticSearchDomain オブジェクトは、Amazon OpenSearch Service ドメインに関する詳細を提供します。

次の例は、 AwsElasticSearchDomain オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsElasticSearchDomain 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsElasticSearchDomainDetails「」を参照してください。

例

```
"AwsElasticSearchDomain": {
    "AccessPolicies": "string",
    "DomainStatus": {
           "DomainId": "string",
           "DomainName": "string",
           "Endpoint": "string",
           "Endpoints": {
                  "string": "string"
           }
    },
    "DomainEndpointOptions": {
           "EnforceHTTPS": boolean,
           "TLSSecurityPolicy": "string"
    },
    "ElasticsearchClusterConfig": {
           "DedicatedMasterCount": number,
           "DedicatedMasterEnabled": boolean,
           "DedicatedMasterType": "string",
           "InstanceCount": number,
           "InstanceType": "string",
           "ZoneAwarenessConfig": {
                  "AvailabilityZoneCount": number
           },
           "ZoneAwarenessEnabled": boolean
    },
    "ElasticsearchVersion": "string",
    "EncryptionAtRestOptions": {
           "Enabled": boolean,
           "KmsKeyId": "string"
    },
    "LogPublishingOptions": {
           "AuditLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
           },
           "IndexSlowLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
           },
           "SearchSlowLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
           }
```

```
    },
    "NodeToNodeEncryptionOptions": {
           "Enabled": boolean
    },
    "ServiceSoftwareOptions": {
           "AutomatedUpdateDate": "string",
           "Cancellable": boolean,
           "CurrentVersion": "string",
           "Description": "string",
           "NewVersion": "string",
           "UpdateAvailable": boolean,
           "UpdateStatus": "string"
    },
    "VPCOptions": {
           "AvailabilityZones": [
                 "string"
           ],
           "SecurityGroupIds": [
                 "string"
           ],
           "SubnetIds": [
                 "string"
           ],
          "VPCId": "string"
    }
}
```

AwsElb

AwsElb リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsElbLoadBalancer

AwsElbLoadBalancer オブジェクトには、Classic Load Balancer に関する詳細が含まれます。

次の例は、 AwsElbLoadBalancer オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsElbLoadBalancer 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsElbLoadBalancerDetails「」を参照してください。

例

```
"AwsElbLoadBalancer": {
    "AvailabilityZones": ["us-west-2a"],
    "BackendServerDescriptions": [
```

```
         {
            "InstancePort": 80,
            "PolicyNames": ["doc-example-policy"]
        }
    ],
    "CanonicalHostedZoneName": "Z3DZXE0EXAMPLE",
    "CanonicalHostedZoneNameID": "my-load-balancer-444455556666.us-
west-2.elb.amazonaws.com",
    "CreatedTime": "2020-08-03T19:22:44.637Z",
    "DnsName": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
    "HealthCheck": {
        "HealthyThreshold": 2,
        "Interval": 30,
        "Target": "HTTP:80/png",
        "Timeout": 3,
        "UnhealthyThreshold": 2
    },
    "Instances": [
        {
            "InstanceId": "i-example"
        }
    ],
    "ListenerDescriptions": [
        {
            "Listener": {
                "InstancePort": 443,
                "InstanceProtocol": "HTTPS",
                "LoadBalancerPort": 443,
                "Protocol": "HTTPS",
                "SslCertificateId": "arn:aws:iam::444455556666:server-certificate/my-
server-cert"
            },
            "PolicyNames": ["ELBSecurityPolicy-TLS-1-2-2017-01"]
        }
    ],
    "LoadBalancerAttributes": {
        "AccessLog": {
            "EmitInterval": 60,
            "Enabled": true,
            "S3BucketName": "doc-example-bucket",
            "S3BucketPrefix": "doc-example-prefix"
        },
        "ConnectionDraining": {
            "Enabled": false,
```

```
            "Timeout": 300
        },
        "ConnectionSettings": {
            "IdleTimeout": 30
        },
        "CrossZoneLoadBalancing": {
            "Enabled": true
        },
        "AdditionalAttributes": [{
            "Key": "elb.http.desyncmitigationmode",
            "Value": "strictest"
        }]

    },
    "LoadBalancerName": "example-load-balancer",
    "Policies": {
        "AppCookieStickinessPolicies": [
            {
                "CookieName": "",
                "PolicyName": ""
            }
        ],
        "LbCookieStickinessPolicies": [
            {
                "CookieExpirationPeriod": 60,
                "PolicyName": "my-example-cookie-policy"
            }
        ],
        "OtherPolicies": [
            "my-PublicKey-policy",
            "my-authentication-policy",
            "my-SSLNegotiation-policy",
            "my-ProxyProtocol-policy",
            "ELBSecurityPolicy-2015-03"
        ]
    },
    "Scheme": "internet-facing",
    "SecurityGroups": ["sg-example"],
    "SourceSecurityGroup": {
        "GroupName": "my-elb-example-group",
        "OwnerAlias": "444455556666"
    },
    "Subnets": ["subnet-example"],
    "VpcId": "vpc-a01106c2"
```

```
}
```

AwsElbv2LoadBalancer

`AwsElbv2LoadBalancer` オブジェクトは、ロードバランサーに関する情報を提供します。

次の例は、 `AwsElbv2LoadBalancer` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsElbv2LoadBalancer` 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsElbv「2LoadBalancerDetails」を参照してください。

例

```
"AwsElbv2LoadBalancer": {
                        "AvailabilityZones": {
                            "SubnetId": "string",
                            "ZoneName": "string"
                        },
                        "CanonicalHostedZoneId": "string",
                        "CreatedTime": "string",
                        "DNSName": "string",
                        "IpAddressType": "string",
                        "LoadBalancerAttributes": [
                            {
                                "Key": "string",
                                "Value": "string"
                            }
                        ],
                        "Scheme": "string",
                        "SecurityGroups": [ "string" ],
                        "State": {
                            "Code": "string",
                            "Reason": "string"
                        },
                        "Type": "string",
                        "VpcId": "string"
                    }
```

AwsEventBridge

`AwsEventBridge` リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsEventSchemasRegistry

AwsEventSchemasRegistry オブジェクトは、Amazon EventBridge スキーマレジストリに関する情報を提供します。スキーマは、 に送信されるイベントの構造を定義します EventBridge。スキーマレジストリは、スキーマを収集して論理的にグループ化するコンテナです。

次の例は、 AwsEventSchemasRegistry オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEventSchemasRegistry 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEventSchemasRegistry「」を参照してください。

例

```
"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
    "RegistryName": "schema-registry"
}
```

AwsEventsEndpoint

AwsEventsEndpoint オブジェクトは、Amazon EventBridge グローバルエンドポイントに関する情報を提供します。エンドポイントは、アプリケーションの可用性をリージョンフォールトトレラントにすることによって、アプリケーションの可用性を向上することができます。

次の例は、 AwsEventsEndpoint オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEventsEndpoint 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEventsEndpointDetails「」を参照してください。

例

```
"AwsEventsEndpoint": {
    "Arn": "arn:aws:events:us-east-1:123456789012:endpoint/my-endpoint",
    "Description": "This is a sample endpoint.",
    "EndpointId": "04k1exajoy.veo",
    "EndpointUrl": "https://04k1exajoy.veo.endpoint.events.amazonaws.com",
    "EventBuses": [
        {
            "EventBusArn": "arn:aws:events:us-east-1:123456789012:event-bus/default"
        },
        {
            "EventBusArn": "arn:aws:events:us-east-2:123456789012:event-bus/default"
        }
```

```
    ],
    "Name": "my-endpoint",
    "ReplicationConfig": {
        "State": "ENABLED"
    },
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/
Amazon_EventBridge_Invoke_Event_Bus_1258925394",
    "RoutingConfig": {
        "FailoverConfig": {
            "Primary": {
                "HealthCheck": "arn:aws:route53:::healthcheck/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
            },
            "Secondary": {
                "Route": "us-east-2"
            }
        }
    },
    "State": "ACTIVE"
}
```

AwsEventsEventbus

AwsEventsEventbus オブジェクトは、Amazon EventBridge グローバルエンドポイントに関する情報を提供します。エンドポイントは、アプリケーションの可用性をリージョンフォールトトレラントにすることによって、アプリケーションの可用性を向上することができます。

次の例は、 AwsEventsEventbus オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEventsEventbus 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsEventsEventbusDetails「」を参照してください。

例

```
"AwsEventsEventbus":
    "Arn": "arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus",
    "Name": "my-event-bus",
    "Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AllowAllAccountsFromOrganizationToPutEvents\",\"Effect\":\"Allow
\",\"Principal\":\"*\",\"Action\":\"events:PutEvents\",\"Resource\":
\"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\",\"Condition
\":{\"StringEquals\":{\"aws:PrincipalOrgID\":\"o-ki7yjtkjv5\"}}},{\"Sid\":
\"AllowAccountToManageRulesTheyCreated\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
\"arn:aws:iam::123456789012:root\"},\"Action\":[\"events:PutRule\",\"events:PutTargets
```

```
\",\"events:DeleteRule\",\"events:RemoveTargets\",\"events:DisableRule
\",\"events:EnableRule\",\"events:TagResource\",\"events:UntagResource\",
\"events:DescribeRule\",\"events:ListTargetsByRule\",\"events:ListTagsForResource\"],
\"Resource\":\"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\",\"Condition\":
{\"StringEqualsIfExists\":{\"events:creatorAccount\":\"123456789012\"}}}]}"
```

AwsGuardDuty

AwsGuardDuty リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsGuardDutyDetector

AwsGuardDutyDetector オブジェクトは、Amazon GuardDuty ディテクターに関する情報を提供します。ディテクターは、 GuardDuty サービスを表すオブジェクトです。が動作可能になる GuardDuty には、ディテクターが必要です。

次の例は、 AwsGuardDutyDetector オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsGuardDutyDetector 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsGuardDutyDetector「」を参照してください。

例

```
"AwsGuardDutyDetector": {
    "FindingPublishingFrequency": "SIX_HOURS",
    "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Status": "ENABLED",
    "DataSources": {
        "CloudTrail": {
            "Status": "ENABLED"
        },
        "DnsLogs": {
            "Status": "ENABLED"
        },
        "FlowLogs": {
            "Status": "ENABLED"
        },
        "S3Logs": {
             "Status": "ENABLED"
         },
         "Kubernetes": {
             "AuditLogs": {
                "Status": "ENABLED"
```

```
            }
        },
        "MalwareProtection": {
            "ScanEc2InstanceWithFindings": {
               "EbsVolumes": {
                   "Status": "ENABLED"
                }
            },
           "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/malware-
protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    }
}
```

AwsIam

AwsIam リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsIamAccessKey

AwsIamAccessKey オブジェクトには、結果に関連する IAM アクセスキーの詳細が含まれています。

次の例は、 AwsIamAccessKey オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsIamAccessKey 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsIamAccessKeyDetails「」を参照してください。

例

```
"AwsIamAccessKey": {
                        "AccessKeyId": "string",
                        "AccountId": "string",
                        "CreatedAt": "string",
                        "PrincipalId": "string",
                        "PrincipalName": "string",
                        "PrincipalType": "string",
                        "SessionContext": {
                            "Attributes": {
                                "CreationDate": "string",
                                "MfaAuthenticated": boolean
                            },
                            "SessionIssuer": {
                                "AccountId": "string",
                                "Arn": "string",
```

```
                            "PrincipalId": "string",
                            "Type": "string",
                            "UserName": "string"
                        }
                    },
                    "Status": "string"
                }
```

AwsIamGroup

AwsIamGroup オブジェクトには IAM グループに関する詳細が含まれています。

次の例は、 AwsIamGroup オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsIamGroup 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsIamGroupDetails「」を参照してください。

例

```
"AwsIamGroup": {
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleManagedAccess",
            "PolicyName": "ExampleManagedAccess",
        }
    ],
    "CreateDate": "2020-04-28T14:08:37.000Z",
    "GroupId": "AGPA4TPS3VLP7QEXAMPLE",
    "GroupName": "Example_User_Group",
    "GroupPolicyList": [
        {
            "PolicyName": "ExampleGroupPolicy"
        }
    ],
    "Path": "/"
}
```

AwsIamPolicy

AwsIamPolicy オブジェクトは IAM 許可ポリシーを表します。

次の例は、 AwsIamPolicy オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsIamPolicy 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsIamPolicyDetails「」を参照してください。

例

```
"AwsIamPolicy": {
    "AttachmentCount": 1,
    "CreateDate": "2017-09-14T08:17:29.000Z",
    "DefaultVersionId": "v1",
    "Description": "Example IAM policy",
    "IsAttachable": true,
    "Path": "/",
    "PermissionsBoundaryUsageCount": 5,
    "PolicyId": "ANPAJ2UCCR6DPCEXAMPLE",
    "PolicyName": "EXAMPLE-MANAGED-POLICY",
    "PolicyVersionList": [
        {
            "VersionId": "v1",
            "IsDefaultVersion": true,
            "CreateDate": "2017-09-14T08:17:29.000Z"
        }
    ],
    "UpdateDate": "2017-09-14T08:17:29.000Z"
}
```

AwsIamRole

AwsIamRole オブジェクトには、IAM ロールに関する情報 (ロールのすべてのポリシーを含む) が含まれています。

次の例は、 AwsIamRole オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsIamRole 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsIamRoleDetails「」を参照してください。

例

```
"AwsIamRole": {
    "AssumeRolePolicyDocument": "{'Version': '2012-10-17','Statement': [{'Effect':
 'Allow','Action': 'sts:AssumeRole'}]}",
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExamplePolicy1",
            "PolicyName": "Example policy 1"
        },
        {
```

```
            "PolicyArn": "arn:aws:iam::444455556666:policy/ExamplePolicy2",
            "PolicyName": "Example policy 2"
        }
        ],
        "CreateDate": "2020-03-14T07:19:14.000Z",
        "InstanceProfileList": [
            {
                "Arn": "arn:aws:iam::333333333333:ExampleProfile",
                "CreateDate": "2020-03-11T00:02:27Z",
                "InstanceProfileId": "AIPAIXEU4NUHUPEXAMPLE",
                "InstanceProfileName": "ExampleInstanceProfile",
                "Path": "/",
                "Roles": [
                    {
                       "Arn": "arn:aws:iam::444455556666:role/example-role",
                        "AssumeRolePolicyDocument": "",
                        "CreateDate": "2020-03-11T00:02:27Z",
                        "Path": "/",
                        "RoleId": "AROAJ52OTH4H7LEXAMPLE",
                        "RoleName": "example-role",
                    }
                ]
            }
        ],
        "MaxSessionDuration": 3600,
        "Path": "/",
        "PermissionsBoundary": {
            "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
            "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
        },
        "RoleId": "AROA4TPS3VLEXAMPLE",
        "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
        "RolePolicyList": [
            {
                "PolicyName": "Example role policy"
            }
        ]
    }
```

AwsIamUser

`AwsIamUser` オブジェクトは、ユーザーに関する情報を提供します。

次の例は、 AwsIamUser オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsIamUser 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsIamUserDetails「」を参照してください。

例

```
"AwsIamUser": {
    "AttachedManagedPolicies": [
        {
            "PolicyName": "ExamplePolicy",
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleAccess"
        }
    ],
    "CreateDate": "2018-01-26T23:50:05.000Z",
    "GroupList": [],
    "Path": "/",
    "PermissionsBoundary" : {
        "PermissionsBoundaryArn" : "arn:aws:iam::aws:policy/AdministratorAccess",
        "PermissionsBoundaryType" : "PermissionsBoundaryPolicy"
    },
    "UserId": "AIDACKCEVSQ6C2EXAMPLE",
    "UserName": "ExampleUser",
    "UserPolicyList": [
        {
            "PolicyName": "InstancePolicy"
        }
    ]
}
```

AwsKinesis

AwsKinesis リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsKinesisStream

AwsKinesisStream オブジェクトは、Amazon Kinesis Data Streams の詳細を表示します。

次の例は、 AwsKinesisStream オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsKinesisStream 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsKinesisStreamDetails「」を参照してください。

例

```
"AwsKinesisStream": {
 "Name": "test-vir-kinesis-stream",
 "Arn": "arn:aws:kinesis:us-east-1:293279581038:stream/test-vir-kinesis-stream",
 "RetentionPeriodHours": 24,
 "ShardCount": 2,
 "StreamEncryption": {
  "EncryptionType": "KMS",
  "KeyId": "arn:aws:kms:us-east-1:293279581038:key/849cf029-4143-4c59-91f8-
ea76007247eb"
 }
}
```

AwsKms

AwsKms リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsKmsKey

AwsKmsKey オブジェクトは、 に関する詳細を提供します AWS KMS key。

次の例は、 AwsKmsKey オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsKmsKey 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsKmsKeyDetails「」を参照してください。

例

```
"AwsKmsKey": {
                        "AWSAccountId": "string",
                        "CreationDate": "string",
                        "Description": "string",
                        "KeyId": "string",
                        "KeyManager": "string",
                        "KeyRotationStatus": boolean,
                        "KeyState": "string",
                        "Origin": "string"
                    }
```

AwsLambda

AwsLambda リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsLambdaFunction

AwsLambdaFunction オブジェクトは、Lambda 関数の設定に関する詳細を提供します。

次の例は、 AwsLambdaFunction オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsLambdaFunction 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsLambdaFunctionDetails「」を参照してください。

例

```
"AwsLambdaFunction": {
    "Architectures": [
        "x86_64"
    ],
    "Code": {
        "S3Bucket": "DOC-EXAMPLE-BUCKET",
        "S3Key": "samplekey",
        "S3ObjectVersion": "2",
        "ZipFile": "myzip.zip"
    },
    "CodeSha256": "1111111111111abcdef",
    "DeadLetterConfig": {
        "TargetArn": "arn:aws:lambda:us-east-2:123456789012:queue:myqueue:2"
    },
    "Environment": {
        "Variables": {
            "Stage": "foobar"
         },
        "Error": {
            "ErrorCode": "Sample-error-code",
            "Message": "Caller principal is a manager."
         }
     },
    "FunctionName": "CheckOut",
    "Handler": "main.py:lambda_handler",
    "KmsKeyArn": "arn:aws:kms:us-west-2:123456789012:key/mykey",
    "LastModified": "2001-09-11T09:00:00Z",
    "Layers": {
        "Arn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:3",
        "CodeSize": 169
    },
    "PackageType": "Zip",
    "RevisionId": "23",
```

```
    "Role": "arn:aws:iam::123456789012:role/Accounting-Role",
    "Runtime": "go1.7",
    "Timeout": 15,
    "TracingConfig": {
        "Mode": "Active"
    },
    "Version": "$LATEST$",
    "VpcConfig": {
        "SecurityGroupIds": ["sg-085912345678492fb", "sg-08591234567bdgdc"],
         "SubnetIds": ["subnet-071f712345678e7c8", "subnet-07fd123456788a036"]
    },
    "MasterArn": "arn:aws:lambda:us-east-2:123456789012:\$LATEST",
    "MemorySize": 2048
}
```

AwsLambdaLayerVersion

`AwsLambdaLayerVersion` オブジェクトは、Lambda レイヤーのバージョンに関する詳細を提供します。

次の例は、 `AwsLambdaLayerVersion` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsLambdaLayerVersion` 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsLambdaLayerVersionDetails「」を参照してください。

例

```
"AwsLambdaLayerVersion": {
    "Version": 2,
    "CompatibleRuntimes": [
        "java8"
    ],
    "CreatedDate": "2019-10-09T22:02:00.274+0000"
}
```

AwsMsk

`AwsMsk` リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsMskCluster

`AwsMskCluster` オブジェクトは Amazon Managed Streaming for Apache Kafka (Amazon MSK) クラスターに関する情報を提供します。

次の例は、 AwsMskCluster オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsMskCluster 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsMskClusterDetails「」を参照してください。

例

```
"AwsMskCluster": {
        "ClusterInfo": {
            "ClientAuthentication": {
                "Sasl": {
                    "Scram": {
                        "Enabled": true
                    },
                    "Iam": {
                        "Enabled": true
                    }
                },
                "Tls": {
                    "CertificateAuthorityArnList": [],
                    "Enabled": false
                },
                "Unauthenticated": {
                    "Enabled": false
                }
            },
            "ClusterName": "my-cluster",
            "CurrentVersion": "K2PWKAKR8XB7XF",
            "EncryptionInfo": {
                "EncryptionAtRest": {
                    "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
                "EncryptionInTransit": {
                    "ClientBroker": "TLS",
                    "InCluster": true
                }
            },
            "EnhancedMonitoring": "PER_TOPIC_PER_BROKER",
            "NumberOfBrokerNodes": 3
        }
}
```

AwsNetworkFirewall

AwsNetworkFirewall リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsNetworkFirewallFirewall

AwsNetworkFirewallFirewall オブジェクトには AWS Network Firewall ファイアウォールに関する詳細が含まれています。

次の例は、 AwsNetworkFirewallFirewall オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsNetworkFirewallFirewall 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsNetworkFirewallFirewallDetails「」を参照してください。

例

```
"AwsNetworkFirewallFirewall": {
    "DeleteProtection": false,
    "FirewallArn": "arn:aws:network-firewall:us-east-1:024665936331:firewall/
testfirewall",
    "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
    "FirewallId": "dea7d8e9-ae38-4a8a-b022-672a830a99fa",
    "FirewallName": "testfirewall",
    "FirewallPolicyChangeProtection": false,
    "SubnetChangeProtection": false,
    "SubnetMappings": [
        {
            "SubnetId": "subnet-0183481095e588cdc"
        },
        {
            "SubnetId": "subnet-01f518fad1b1c90b0"
        }
    ],
    "VpcId": "vpc-40e83c38"
}
```

AwsNetworkFirewallFirewallPolicy

AwsNetworkFirewallFirewallPolicy オブジェクトは、ファイアウォールポリシーに関する詳細を提供します。ファイアウォールポリシーは、ネットワークファイアウォールの動作を定義します。

次の例は、 AwsNetworkFirewallFirewallPolicy オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsNetworkFirewallFirewallPolicy 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsNetworkFirewallFirewallPolicyDetails「」を参照してください。

例

```
"AwsNetworkFirewallFirewallPolicy": {
   "FirewallPolicy": {
    "StatefulRuleGroupReferences": [
        {
            "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/PatchesOnly"
        }
    ],
    "StatelessDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessRuleGroupReferences": [
       {
          "Priority": 1,
          "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1"
       }
     ]
   },
   "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
   "FirewallPolicyId": "9ceeda22-6050-4048-a0ca-50ce47f0cc65",
   "FirewallPolicyName": "InitialFirewall",
   "Description": "Initial firewall"
}
```

AwsNetworkFirewallRuleGroup

AwsNetworkFirewallRuleGroup オブジェクトは、 AWS Network Firewall ルールグループに関する詳細を提供します。ルールグループはネットワークトラフィックを検査および制御するために使用します。ステートレスルールグループは、個々のパケットに適用されます。ステートフルルールグループは、トラフィックフローのコンテキスト内のパケットに適用されます。

ルールグループは、ファイアウォールポリシーで参照されます。

次の例は、 AwsNetworkFirewallRuleGroup オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsNetworkFirewallRuleGroup 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsNetworkFirewallRuleGroupDetails「」を参照してください。

例 - ステートレスルールグループ

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 600,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1",
    "RuleGroupId": "fb13c4df-b6da-4c1e-91ec-84b7a5487493",
    "RuleGroupName": "Stateless-1"
    "Description": "Example of a stateless rule group",
    "Type": "STATELESS",
    "RuleGroup": {
        "RulesSource": {
            "StatelessRulesAndCustomActions": {
                "CustomActions": [],
                "StatelessRules": [
                    {
                        "Priority": 1,
                        "RuleDefinition": {
                            "Actions": [
                                "aws:pass"
                            ],
                            "MatchAttributes": {
                                "DestinationPorts": [
                                    {
                                        "FromPort": 443,
                                        "ToPort": 443
                                    }
                                ],
                                "Destinations": [
                                    {
                                        "AddressDefinition": "192.0.2.0/24"
                                    }
                                ],
                                "Protocols": [
                                            6
                                ],
                                "SourcePorts": [
                                    {
```

```
                                        "FromPort": 0,
                                        "ToPort": 65535
                                    }
                                ],
                                "Sources": [
                                    {
                                         "AddressDefinition": "198.51.100.0/24"
                                    }
                                ]
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

例 - ステートフルルールグループ

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 100,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/tupletest",
    "RuleGroupId": "38b71c12-da80-4643-a6c5-03337f8933e0",
    "RuleGroupName": "ExampleRuleGroup",
    "Description": "Example of a stateful rule group",
    "Type": "STATEFUL",
    "RuleGroup": {
        "RuleSource": {
             "StatefulRules": [
                 {
                     "Action": "PASS",
                     "Header": {
                         "Destination": "Any",
                         "DestinationPort": "443",
                         "Direction": "ANY",
                         "Protocol": "TCP",
                         "Source": "Any",
                         "SourcePort": "Any"
                     },
                     "RuleOptions": [
                         {
```

```
                        "Keyword": "sid:1"
                    }
                ]
            }
        ]
    }
}
```

以下は、AwsNetworkFirewallRuleGroup 属性の、有効な値の例の一覧です。

- Action

  有効な値: PASS | DROP | ALERT

- Protocol

  有効な値: IP | TCP | UDP | ICMP | HTTP | FTP | TLS | SMB | DNS | DCERPC | SSH | SMTP | IMAP | MSN | KRB5 | IKEV2 | TFTP | NTP | DHCP

- Flags

  有効な値: FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

- Masks

  有効な値: FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

AwsOpenSearchService

AwsOpenSearchService リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsOpenSearchServiceDomain

AwsOpenSearchServiceDomain オブジェクトには、Amazon OpenSearch Service ドメインに関する情報が含まれています。

次の例は、 AwsOpenSearchServiceDomain オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsOpenSearchServiceDomain 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsOpenSearchServiceDomainDetails「」を参照してください。

例

```
"AwsOpenSearchServiceDomain": {
    "AccessPolicies": "IAM_Id",
    "AdvancedSecurityOptions": {
        "Enabled": true,
        "InternalUserDatabaseEnabled": true,
        "MasterUserOptions": {
            "MasterUserArn": "arn:aws:iam::123456789012:user/third-master-use",
            "MasterUserName": "third-master-use",
            "MasterUserPassword": "some-password"
        }
    },
    "Arn": "arn:aws:Opensearch:us-east-1:111122223333:somedomain",
    "ClusterConfig": {
        "InstanceType": "c5.large.search",
        "InstanceCount": 1,
        "DedicatedMasterEnabled": true,
        "ZoneAwarenessEnabled": false,
        "ZoneAwarenessConfig": {
            "AvailabilityZoneCount": 2
        },
        "DedicatedMasterType": "c5.large.search",
        "DedicatedMasterCount": 3,
        "WarmEnabled": true,
        "WarmCount": 3,
        "WarmType": "ultrawarm1.large.search"
    },
    "DomainEndpoint": "https://es-2021-06-23t17-04-qowmgghud5vofgb5e4wmi.eu-
central-1.es.amazonaws.com",
    "DomainEndpointOptions": {
        "EnforceHTTPS": false,
        "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07",
        "CustomEndpointCertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/bda1bff1-79c0-49d0-abe6-50a15a7477d4",
        "CustomEndpointEnabled": true,
        "CustomEndpoint": "example.com"
    },
    "DomainEndpoints": {
        "vpc": "vpc-endpoint-h2dsd34efgyghrtguk5gt6j2foh4.us-east-1.es.amazonaws.com"
    },
    "DomainName": "my-domain",
    "EncryptionAtRestOptions": {
        "Enabled": false,
        "KmsKeyId": "1a2a3a4-1a2a-3a4a-5a6a-1a2a3a4a5a6a"
```

```
    },
    "EngineVersion": "7.1",
    "Id": "123456789012",
    "LogPublishingOptions": {
        "IndexSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-index-slow-logs",
            "Enabled": true
        },
        "SearchSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        },
        "AuditLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        }
    },
    "NodeToNodeEncryptionOptions": {
        "Enabled": true
    },
    "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "2022-04-28T14:08:37.000Z",
        "Cancellable": false,
        "CurrentVersion": "R20210331",
        "Description": "There is no software update available for this domain.",
        "NewVersion": "OpenSearch_1.0",
        "UpdateAvailable": false,
        "UpdateStatus": "COMPLETED",
        "OptionalDeployment": false
    },
    "VpcOptions": {
        "SecurityGroupIds": [
            "sg-2a3a4a5a"
        ],
        "SubnetIds": [
            "subnet-1a2a3a4a"
        ],
    }
}
```

AwsRds

AwsRds リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsRdsDbCluster

AwsRdsDbCluster オブジェクトは、Amazon RDS データベースクラスターの詳細を提供します。

次の例は、 AwsRdsDbCluster オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsRdsDbCluster 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsRdsDbClusterDetails「」を参照してください。

例

```
"AwsRdsDbCluster": {
    "ActivityStreamStatus": "stopped",
    "AllocatedStorage": 1,
    "AssociatedRoles": [
        {
        "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
        "Status": "PENDING"
        }
    ],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1c",
        "us-east-1e"
    ],
    "BackupRetentionPeriod": 1,
    "ClusterCreateTime": "2020-06-22T17:40:12.322Z",
    "CopyTagsToSnapshot": true,
    "CrossAccountClone": false,
    "CustomEndpoints": [],
    "DatabaseName": "Sample name",
    "DbClusterIdentifier": "database-3",
    "DbClusterMembers": [
        {
        "DbClusterParameterGroupStatus": "in-sync",
        "DbInstanceIdentifier": "database-3-instance-1",
        "IsClusterWriter": true,
        "PromotionTier": 1,
        }
```

```
    ],
    "DbClusterOptionGroupMemberships": [],
    "DbClusterParameterGroup": "cluster-parameter-group",
    "DbClusterResourceId": "cluster-example",
    "DbSubnetGroup": "subnet-group",
    "DeletionProtection": false,
    "DomainMemberships": [],
    "Status": "modifying",
    "EnabledCloudwatchLogsExports": [
        "audit",
        "error",
        "general",
        "slowquery"
    ],
    "Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
    "Engine": "aurora-mysql",
    "EngineMode": "provisioned",
    "EngineVersion": "5.7.mysql_aurora.2.03.4",
    "HostedZoneId": "ZONE1",
    "HttpEndpointEnabled": false,
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "MasterUsername": "admin",
    "MultiAz": false,
    "Port": 3306,
    "PreferredBackupWindow": "04:52-05:22",
    "PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
    "ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",
    "ReadReplicaIdentifiers": [],
    "Status": "Modifying",
    "StorageEncrypted": true,
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example-1"
        }
    ],
}
```

AwsRdsDbClusterSnapshot

`AwsRdsDbClusterSnapshot` オブジェクトには、Amazon RDS DB クラススナップショットに関する情報が含まれています。

次の例は、 AwsRdsDbClusterSnapshot オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsRdsDbClusterSnapshot 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsRdsDbClusterSnapshotDetails「」を参照してください。

例

```
"AwsRdsDbClusterSnaphot": {
    "AllocatedStorage": 0,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1d",
        "us-east-1e"
    ],
    "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
    "DbClusterIdentifier": "database-2",
    "DbClusterSnapshotAttributes": [{
        "AttributeName": "restore",
        "AttributeValues": ["123456789012"]
    }],
    "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
    "Engine": "aurora",
    "EngineVersion": "5.6.10a",
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "LicenseModel": "aurora",
    "MasterUsername": "admin",
    "PercentProgress": 100,
    "Port": 0,
    "SnapshotCreateTime": "2020-06-22T17:40:12.322Z",
    "SnapshotType": "automated",
    "Status": "available",
    "StorageEncrypted": true,
    "VpcId": "vpc-faf7e380"
}
```

AwsRdsDbInstance

AwsRdsDbInstance オブジェクトは、Amazon RDS DB インスタンスに関する詳細を提供します。

次の例は、 AwsRdsDbInstance オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsRdsDbInstance 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsRdsDbInstanceDetails「」を参照してください。

例

```
"AwsRdsDbInstance": {
    "AllocatedStorage": 20,
    "AssociatedRoles": [],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1d",
    "BackupRetentionPeriod": 7,
    "CaCertificateIdentifier": "certificate1",
    "CharacterSetName": "",
    "CopyTagsToSnapshot": true,
    "DbClusterIdentifier": "",
    "DbInstanceArn": "arn:aws:rds:us-east-1:111122223333:db:database-1",
    "DbInstanceClass": "db.t2.micro",
    "DbInstanceIdentifier": "database-1",
    "DbInstancePort": 0,
    "DbInstanceStatus": "available",
    "DbiResourceId": "db-EXAMPLE123",
    "DbName": "",
    "DbParameterGroups": [
        {
            "DbParameterGroupName": "default.mysql5.7",
            "ParameterApplyStatus": "in-sync"
        }
    ],
    "DbSecurityGroups": [],


    "DbSubnetGroup": {
        "DbSubnetGroupName": "my-group-123abc",
        "DbSubnetGroupDescription": "My subnet group",
        "VpcId": "vpc-example1",
        "SubnetGroupStatus": "Complete",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-123abc",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1d"
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-456def",
                "SubnetAvailabilityZone": {
```

```
                    "Name": "us-east-1c"
                },
                "SubnetStatus": "Active"
            }
      ],
        "DbSubnetGroupArn": ""
    },
    "DeletionProtection": false,
    "DomainMemberships": [],
    "EnabledCloudWatchLogsExports": [],
    "Endpoint": {
        "address": "database-1.example.us-east-1.rds.amazonaws.com",
        "port": 3306,
        "hostedZoneId": "ZONEID1"
    },
    "Engine": "mysql",
    "EngineVersion": "5.7.22",
    "EnhancedMonitoringResourceArn": "arn:aws:logs:us-east-1:111122223333:log-
group:Example:log-stream:db-EXAMPLE1",
    "IamDatabaseAuthenticationEnabled": false,
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "Iops": "",
    "KmsKeyId": "",
    "LatestRestorableTime": "2020-06-24T05:50:00.000Z",
    "LicenseModel": "general-public-license",
    "ListenerEndpoint": "",
    "MasterUsername": "admin",
    "MaxAllocatedStorage": 1000,
    "MonitoringInterval": 60,
    "MonitoringRoleArn": "arn:aws:iam::111122223333:role/rds-monitoring-role",
    "MultiAz": false,
    "OptionGroupMemberships": [
        {
            "OptionGroupName": "default:mysql-5-7",
            "Status": "in-sync"
        }
    ],
    "PreferredBackupWindow": "03:57-04:27",
    "PreferredMaintenanceWindow": "thu:10:13-thu:10:43",
    "PendingModifiedValues": {
        "DbInstanceClass": "",
        "AllocatedStorage": "",
        "MasterUserPassword": "",
        "Port": "",
```

```
        "BackupRetentionPeriod": "",
        "MultiAZ": "",
        "EngineVersion": "",
        "LicenseModel": "",
        "Iops": "",
        "DbInstanceIdentifier": "",
        "StorageType": "",
        "CaCertificateIdentifier": "",
        "DbSubnetGroupName": "",
        "PendingCloudWatchLogsExports": "",
        "ProcessorFeatures": []
    },
    "PerformanceInsightsEnabled": false,
    "PerformanceInsightsKmsKeyId": "",
    "PerformanceInsightsRetentionPeriod": "",
    "ProcessorFeatures": [],
    "PromotionTier": "",
    "PubliclyAccessible": false,
    "ReadReplicaDBClusterIdentifiers": [],
    "ReadReplicaDBInstanceIdentifiers": [],
    "ReadReplicaSourceDBInstanceIdentifier": "",
    "SecondaryAvailabilityZone": "",
    "StatusInfos": [],
    "StorageEncrypted": false,
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Timezone": "",
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-example1",
            "Status": "active"
        }
    ]
}
```

AwsRdsDbSecurityGroup

AwsRdsDbSecurityGroup オブジェクトには、Amazon Relational Database Service に関する情報が含まれます。

次の例は、 AwsRdsDbSecurityGroup オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsRdsDbSecurityGroup 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsRdsDbSecurityGroupDetails「」を参照してください。

例

```
"AwsRdsDbSecurityGroup": {
    "DbSecurityGroupArn": "arn:aws:rds:us-west-1:111122223333:secgrp:default",
    "DbSecurityGroupDescription": "default",
    "DbSecurityGroupName": "mysecgroup",
    "Ec2SecurityGroups": [
        {
          "Ec2SecurityGroupuId": "myec2group",
          "Ec2SecurityGroupName": "default",
          "Ec2SecurityGroupOwnerId": "987654321021",
          "Status": "authorizing"
        }
    ],
    "IpRanges": [
        {
          "Cidrip": "0.0.0.0/0",
          "Status": "authorizing"
        }
    ],
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234567f"
}
```

AwsRdsDbSnapshot

AwsRdsDbSnapshot オブジェクトには、Amazon RDS DB クラススナップショットに関する詳細が含まれています。

次の例は、 AwsRdsDbSnapshot オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsRdsDbSnapshot 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsRdsDbSnapshotDetails「」を参照してください。

例

```
"AwsRdsDbSnapshot": {
    "DbSnapshotIdentifier": "rds:database-1-2020-06-22-17-41",
    "DbInstanceIdentifier": "database-1",
    "SnapshotCreateTime": "2020-06-22T17:41:29.967Z",
    "Engine": "mysql",
    "AllocatedStorage": 20,
    "Status": "available",
    "Port": 3306,
```

```
    "AvailabilityZone": "us-east-1d",
    "VpcId": "vpc-example1",
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "MasterUsername": "admin",
    "EngineVersion": "5.7.22",
    "LicenseModel": "general-public-license",
    "SnapshotType": "automated",
    "Iops": null,
    "OptionGroupName": "default:mysql-5-7",
    "PercentProgress": 100,
    "SourceRegion": null,
    "SourceDbSnapshotIdentifier": "",
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Encrypted": false,
    "KmsKeyId": "",
    "Timezone": "",
    "IamDatabaseAuthenticationEnabled": false,
    "ProcessorFeatures": [],
    "DbiResourceId": "db-resourceexample1"
}
```

AwsRdsEventSubscription

AwsRdsEventSubscription には、RDS イベント通知サブスクリプションの詳細が含まれています。サブスクリプションにより、RDS は SNS トピックにイベントを送信できます。

次の例は、 AwsRdsEventSubscription オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsRdsEventSubscription 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsRdsEventSubscriptionDetails「」を参照してください。

例

```
"AwsRdsEventSubscription": {
    "CustSubscriptionId": "myawsuser-secgrp",
    "CustomerAwsId": "111111111111",
    "Enabled": true,
    "EventCategoriesList": [
        "configuration change",
        "failure"
    ],
    "EventSubscriptionArn": "arn:aws:rds:us-east-1:111111111111:es:my-instance-events",
    "SnsTopicArn": "arn:aws:sns:us-east-1:111111111111:myawsuser-RDS",
```

```
    "SourceIdsList": [
        "si-sample",
        "mysqldb-rr"
    ],
    "SourceType": "db-security-group",
    "Status": "creating",
    "SubscriptionCreationTime": "2021-06-27T01:38:01.090Z"
}
```

AwsRedshift

AwsRedshift リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsRedshiftCluster

AwsRedshiftCluster オブジェクトには、Amazon Redshift クラスターに関する詳細が含まれています。

次の例は、 AwsRedshiftCluster オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsRedshiftCluster 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsRedshiftClusterDetails「」を参照してください。

例

```
"AwsRedshiftCluster": {
    "AllowVersionUpgrade": true,
    "AutomatedSnapshotRetentionPeriod": 1,
    "AvailabilityZone": "us-west-2d",
    "ClusterAvailabilityStatus": "Unavailable",
    "ClusterCreateTime": "2020-08-03T19:22:44.637Z",
    "ClusterIdentifier": "redshift-cluster-1",
    "ClusterNodes": [
        {
            "NodeRole": "LEADER",
            "PrivateIPAddress": "192.0.2.108",
            "PublicIPAddress": "198.51.100.29"
        },
        {
            "NodeRole": "COMPUTE-0",
            "PrivateIPAddress": "192.0.2.22",
            "PublicIPAddress": "198.51.100.63"
        },
        {
             "NodeRole": "COMPUTE-1",
```

```
            "PrivateIPAddress": "192.0.2.224",
            "PublicIPAddress": "198.51.100.226"
        }
        ],
    "ClusterParameterGroups": [
        {
            "ClusterParameterStatusList": [
                {
                    "ParameterName": "max_concurrency_scaling_clusters",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "enable_user_activity_logging",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "auto_analyze",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "query_group",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "datestyle",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "extra_float_digits",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "search_path",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "statement_timeout",
```

```
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "wlm_json_configuration",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "require_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "use_fips_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                }
            ],
            "ParameterApplyStatus": "in-sync",
            "ParameterGroupName": "temp"
        }
    ],
    "ClusterPublicKey": "JalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY Amazon-Redshift",
    "ClusterRevisionNumber": 17498,
    "ClusterSecurityGroups": [
        {
            "ClusterSecurityGroupName": "default",
            "Status": "active"
        }
    ],
    "ClusterSnapshotCopyStatus": {
        "DestinationRegion": "us-west-2",
        "ManualSnapshotRetentionPeriod": -1,
        "RetentionPeriod": 1,
        "SnapshotCopyGrantName": "snapshotCopyGrantName"
    },
    "ClusterStatus": "available",
    "ClusterSubnetGroupName": "default",
    "ClusterVersion": "1.0",
    "DBName": "dev",
    "DeferredMaintenanceWindows": [
        {
            "DeferMaintenanceEndTime": "2020-10-07T20:34:01.000Z",
```

```
            "DeferMaintenanceIdentifier": "deferMaintenanceIdentifier",
            "DeferMaintenanceStartTime": "2020-09-07T20:34:01.000Z"
        }
     ],
    "ElasticIpStatus": {
        "ElasticIp": "203.0.113.29",
        "Status": "active"
    },
    "ElasticResizeNumberOfNodeOptions": "4",
    "Encrypted": false,
    "Endpoint": {
        "Address": "redshift-cluster-1.example.us-west-2.redshift.amazonaws.com",
        "Port": 5439
    },
    "EnhancedVpcRouting": false,
    "ExpectedNextSnapshotScheduleTime": "2020-10-13T20:34:01.000Z",
    "ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
    "HsmStatus": {
        "HsmClientCertificateIdentifier": "hsmClientCertificateIdentifier",
        "HsmConfigurationIdentifier": "hsmConfigurationIdentifier",
        "Status": "applying"
    },
    "IamRoles": [
        {
             "ApplyStatus": "in-sync",
             "IamRoleArn": "arn:aws:iam::111122223333:role/RedshiftCopyUnload"
        }
    ],
    "KmsKeyId": "kmsKeyId",
    "LoggingStatus": {
        "BucketName": "test-bucket",
        "LastFailureMessage": "test message",
        "LastFailureTime": "2020-08-09T13:00:00.000Z",
        "LastSuccessfulDeliveryTime": "2020-08-08T13:00:00.000Z",
        "LoggingEnabled": true,
        "S3KeyPrefix": "/"
    },
    "MaintenanceTrackName": "current",
    "ManualSnapshotRetentionPeriod": -1,
    "MasterUsername": "awsuser",
    "NextMaintenanceWindowStartTime": "2020-08-09T13:00:00.000Z",
    "NodeType": "dc2.large",
    "NumberOfNodes": 2,
    "PendingActions": [],
```

```
    "PendingModifiedValues": {
        "AutomatedSnapshotRetentionPeriod": 0,
        "ClusterIdentifier": "clusterIdentifier",
        "ClusterType": "clusterType",
        "ClusterVersion": "clusterVersion",
        "EncryptionType": "None",
        "EnhancedVpcRouting": false,
        "MaintenanceTrackName": "maintenanceTrackName",
        "MasterUserPassword": "masterUserPassword",
        "NodeType": "dc2.large",
        "NumberOfNodes": 1,
        "PubliclyAccessible": true
    },
    "PreferredMaintenanceWindow": "sun:13:00-sun:13:30",
    "PubliclyAccessible": true,
    "ResizeInfo": {
        "AllowCancelResize": true,
        "ResizeType": "ClassicResize"
    },
    "RestoreStatus": {
        "CurrentRestoreRateInMegaBytesPerSecond": 15,
        "ElapsedTimeInSeconds": 120,
        "EstimatedTimeToCompletionInSeconds": 100,
        "ProgressInMegaBytes": 10,
        "SnapshotSizeInMegaBytes": 1500,
        "Status": "restoring"
    },
    "SnapshotScheduleIdentifier": "snapshotScheduleIdentifier",
    "SnapshotScheduleState": "ACTIVE",
     "VpcId": "vpc-example",
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example"
        }
    ]
}
```

AwsRoute53

AwsRoute53 リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsRoute53HostedZone

この AwsRoute53HostedZone オブジェクトは、ホストゾーンに割り当てられた 4 つのネームサーバーを含む Amazon Route 53 ホストゾーンに関する情報を提供します。ホストゾーンは単一の親ドメイン名に属する、まとめて管理できるレコードの集合を表します。

次の例は、 AwsRoute53HostedZone オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsRoute53HostedZone 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsRoute「53HostedZoneDetails」を参照してください。

例

```
"AwsRoute53HostedZone": {
    "HostedZone": {
        "Id": "Z06419652JEMGO9TA2XKL",
        "Name": "asff.testing",
        "Config": {
            "Comment": "This is an example comment."
        }
    },
    "NameServers": [
        "ns-470.awsdns-32.net",
        "ns-1220.awsdns-12.org",
        "ns-205.awsdns-13.com",
        "ns-1960.awsdns-51.co.uk"
    ],
    "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-
group:asfftesting:*",
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "HostedZoneId": "Z00932193AF5H180PPNZD"
        }
    },
    "Vpcs": [
        {
            "Id": "vpc-05d7c6e36bc03ea76",
            "Region": "us-east-1"
        }
    ]
}
```

AwsS3

AwsS3 リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsS3AccessPoint

AwsS3AccessPoint は、Amazon S3 アクセスポイントに関する情報を提供します。S3 アクセスポイントは、S3 バケットにアタッチされた名前付きのネットワークエンドポイントで、S3 オブジェクトのオペレーションを実行するために使用できます。

次の例は、 AwsS3AccessPoint オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsS3AccessPoint 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsS3AccessPointDetails」を参照してください。

例

```
"AwsS3AccessPoint": {
        "AccessPointArn": "arn:aws:s3:us-east-1:123456789012:accesspoint/asff-access-
point",
        "Alias": "asff-access-point-hrzrlukc5m36ft7okagglf3gmwluquse1b-s3alias",
        "Bucket": "DOC-EXAMPLE-BUCKET1",
        "BucketAccountId": "123456789012",
        "Name": "asff-access-point",
        "NetworkOrigin": "VPC",
        "PublicAccessBlockConfiguration": {
            "BlockPublicAcls": true,
            "BlockPublicPolicy": true,
            "IgnorePublicAcls": true,
            "RestrictPublicBuckets": true
        },
        "VpcConfiguration": {
            "VpcId": "vpc-1a2b3c4d5e6f1a2b3"
        }
}
```

AwsS3AccountPublicAccessBlock

AwsS3AccountPublicAccessBlock は、アカウントの Amazon S3 パブリックアクセスブロックに関する情報を提供します。

次の例は、 AwsS3AccountPublicAccessBlock オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsS3AccountPublicAccessBlock 属性の説明を表示するには、AWS

Security Hub 「 API リファレンス」のAwsS3AccountPublicAccessBlockDetails」を参照してください。

例

```
"AwsS3AccountPublicAccessBlock": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": false,
    "RestrictPublicBuckets": true
}
```

AwsS3Bucket

AwsS3Bucket オブジェクトは、Amazon S3 バケットに関する詳細を提供します。

次の例は、 AwsS3Bucket オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsS3Bucket 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsS3BucketDetails」を参照してください。

例

```
"AwsS3Bucket": {
    "AccessControlList": "{\"grantSet\":null,\"grantList\":[{\"grantee\":{\"id\":
\"4df55416215956920d9d056aa8b99803a294ea221222bb668b55a8c6bca81094\",\"displayName
\":null},\"permission\":\"FullControl\"},{\"grantee\":\"AllUsers\",\"permission\":
\"ReadAcp\"},{\"grantee\":\"AuthenticatedUsers\",\"permission\":\"ReadAcp\"}",,
    "BucketLifecycleConfiguration": {
       "Rules": [
           {
               "AbortIncompleteMultipartUpload": {
                   "DaysAfterInitiation": 5
               },
               "ExpirationDate": "2021-11-10T00:00:00.000Z",
               "ExpirationInDays": 365,
               "ExpiredObjectDeleteMarker": false,
               "Filter": {
                   "Predicate": {
                       "Operands": [
                           {
                               "Prefix": "tmp/",
                               "Type": "LifecyclePrefixPredicate"
                           },
```

```
                        {
                            "Tag": {
                                "Key": "ArchiveAge",
                                "Value": "9m"
                            },
                            "Type": "LifecycleTagPredicate"
                        }
                    ],
                    "Type": "LifecycleAndOperator"
                }
            },
            "ID": "Move rotated logs to Glacier",
            "NoncurrentVersionExpirationInDays": -1,
            "NoncurrentVersionTransitions": [
                {
                    "Days": 2,
                    "StorageClass": "GLACIER"
                }
            ],
            "Prefix": "rotated/",
            "Status": "Enabled",
            "Transitions": [
                {
                    "Date": "2020-11-10T00:00:00.000Z",
                    "Days": 100,
                    "StorageClass": "GLACIER"
                }
            ]
        }
    ]
},
"BucketLoggingConfiguration": {
 "DestinationBucketName": "s3serversideloggingbucket-858726136312",
 "LogFilePrefix": "buckettestreadwrite23435/"
},
"BucketName": "DOC-EXAMPLE-BUCKET1",
"BucketNotificationConfiguration": {
 "Configurations": [{
  "Destination": "arn:aws:lambda:us-east-1:123456789012:function:s3_public_write",
  "Events": [
   "s3:ObjectCreated:Put"
  ],
  "Filter": {
   "S3KeyFilter": {
```

```
        "FilterRules": [
        {
         "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.PREFIX",
         "Value": "pre"
        },
        {
         "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.SUFFIX",
         "Value": "suf"
        },
        ]
       }
      },
      "Type": "LambdaConfiguration"
     }]
    },
    "BucketVersioningConfiguration": {
     "IsMfaDeleteEnabled": true,
     "Status": "Off"
    },
    "BucketWebsiteConfiguration": {
     "ErrorDocument": "error.html",
     "IndexDocumentSuffix": "index.html",
     "RedirectAllRequestsTo": {
      "HostName": "example.com",
      "Protocol": "http"
     },
     "RoutingRules": [{
      "Condition": {
       "HttpErrorCodeReturnedEquals": "Redirected",
       "KeyPrefixEquals": "index"
         },
      "Redirect": {
       "HostName": "example.com",
       "HttpRedirectCode": "401",
       "Protocol": "HTTP",
       "ReplaceKeyPrefixWith": "string",
       "ReplaceKeyWith": "string"
      }
     }]
    },
    "CreatedAt": "2007-11-30T01:46:56.000Z",
    "ObjectLockConfiguration": {
     "ObjectLockEnabled": "Enabled",
     "Rule": {
```

```
      "DefaultRetention": {
       "Days": null,
       "Mode": "GOVERNANCE",
       "Years": 12
      },
     },
    },
    "OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
    "OwnerName": "s3bucketowner",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "BlockPublicPolicy": true,
        "IgnorePublicAcls": true,
        "RestrictPublicBuckets": true,
    },
    "ServerSideEncryptionConfiguration": {
        "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "AES256",
                    "KMSMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
                }
            }
        ]
     }
}
```

AwsS3Object

AwsS3Object オブジェクトは、Amazon S3 オブジェクトに関する情報を提供します。

次の例は、 AwsS3Object オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsS3Object 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsS3ObjectDetails」を参照してください。

例

```
"AwsS3Object": {
    "ContentType": "text/html",
    "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
    "LastModified": "2012-04-23T18:25:43.511Z",
    "ServerSideEncryption": "aws:kms",
```

```
    "SSEKMSKeyId": "arn:aws:kms:us-west-2:123456789012:key/4dff8393-e225-4793-
a9a0-608ec069e5a7",
    "VersionId": "ws31OurgOOjH_HHllIxPE35P.MELYaYh"
}
```

AwsSageMaker

AwsSageMaker リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsSageMakerNotebookInstance

AwsSageMakerNotebookInstance オブジェクトは、Jupyter SageMaker Notebook App を実行する機械学習コンピューティングインスタンスである Amazon Notebook インスタンスに関する情報を提供します。

次の例は、 AwsSageMakerNotebookInstance オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsSageMakerNotebookInstance 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsSageMakerNotebookInstanceDetails「」を参照してください。

例

```
"AwsSageMakerNotebookInstance": {
    "DirectInternetAccess": "Disabled",
    "InstanceMetadataServiceConfiguration": {
     "MinimumInstanceMetadataServiceVersion": "1",
    },
    "InstanceType": "ml.t2.medium",
    "LastModifiedTime": "2022-09-09 22:48:32.012000+00:00",
    "NetworkInterfaceId": "eni-06c09ac2541a1bed3",
    "NotebookInstanceArn": "arn:aws:sagemaker:us-east-1:001098605940:notebook-instance/
sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm",
    "NotebookInstanceName":
 "SagemakerNotebookInstanceRootAccessDisabledComplia-8MYjcyofZiXm",
    "NotebookInstanceStatus": "InService",
    "PlatformIdentifier": "notebook-al1-v1",
    "RoleArn": "arn:aws:iam::001098605940:role/sechub-SageMaker-1-scenar-
SageMakerCustomExecution-1R0X32HGC38IW",
    "RootAccess": "Disabled",
    "SecurityGroups": [
     "sg-06b347359ab068745"
    ],
    "SubnetId": "subnet-02c0deea5fa64578e",
```

```
    "Url":
 "sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm.notebook.us-
east-1.sagemaker.aws",
    "VolumeSizeInGB": 5
}
```

AwsSecretsManager

AwsSecretsManager リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsSecretsManagerSecret

AwsSecretsManagerSecret オブジェクトは、Secrets Manager シークレットの詳細を提供します。

次の例は、 AwsSecretsManagerSecret オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsSecretsManagerSecret 属性の説明を表示するには、AWS Security Hub 「 API リファレンスAwsSecretsManagerSecretDetails」の「」を参照してください。

例

```
"AwsSecretsManagerSecret": {
    "RotationRules": {
        "AutomaticallyAfterDays": 30
    },
    "RotationOccurredWithinFrequency": true,
    "KmsKeyId": "kmsKeyId",
    "RotationEnabled": true,
    "RotationLambdaArn": "arn:aws:lambda:us-
west-2:777788889999:function:MyTestRotationLambda",
    "Deleted": false,
    "Name": "MyTestDatabaseSecret",
    "Description": "My test database secret"
}
```

AwsSns

AwsSns リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsSnsTopic

AwsSnsTopic オブジェクトには、Amazon Simple Notification Service トピックの詳細が含まれています。

次の例は、 AwsSnsTopic オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsSnsTopic 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsSnsTopicDetails「」を参照してください。

例

```
"AwsSnsTopic": {
    "ApplicationSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
ApplicationSuccessFeedbackRoleArn",
    "FirehoseFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseFailureFeedbackRoleArn",
    "FirehoseSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseSuccessFeedbackRoleArn",
    "HttpFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpFailureFeedbackRoleArn",
    "HttpSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpSuccessFeedbackRoleArn",
    "KmsMasterKeyId": "alias/ExampleAlias",
    "Owner": "123456789012",
    "SqsFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsFailureFeedbackRoleArn",
    "SqsSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsSuccessFeedbackRoleArn",
    "Subscription": {
         "Endpoint": "http://sampleendpoint.com",
         "Protocol": "http"
    },
    "TopicName": "SampleTopic"
}
```

AwsSqs

AwsSqs リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsSqsQueue

AwsSqsQueue オブジェクトには、Amazon Simple Queue Service キューに関する情報が含まれています。

次の例は、 AwsSqsQueue オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsSqsQueue 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsSqsQueueDetails「」を参照してください。

例

```
"AwsSqsQueue": {
    "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
    "KmsDataKeyReusePeriodSeconds": 60,,
    "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "QueueName": "sample-queue"
}
```

AwsSsm

AwsSsm リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsSsmPatchCompliance

AwsSsmPatchCompliance オブジェクトは、インスタンスにパッチを適用する際に使用したパッチベースラインに基づいて、インスタンスのパッチの状態に関する情報を提供します。

次の例は、 AwsSsmPatchCompliance オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsSsmPatchCompliance 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsSsmPatchComplianceDetails「」を参照してください。

例

```
"AwsSsmPatchCompliance": {
    "Patch": {
        "ComplianceSummary": {
            "ComplianceType": "Patch",
            "CompliantCriticalCount": 0,
            "CompliantHighCount": 0,
            "CompliantInformationalCount": 0,
            "CompliantLowCount": 0,
            "CompliantMediumCount": 0,
            "CompliantUnspecifiedCount": 461,
            "ExecutionType": "Command",
            "NonCompliantCriticalCount": 0,
            "NonCompliantHighCount": 0,
            "NonCompliantInformationalCount": 0,
            "NonCompliantLowCount": 0,
            "NonCompliantMediumCount": 0,
            "NonCompliantUnspecifiedCount": 0,
            "OverallSeverity": "UNSPECIFIED",
            "PatchBaselineId": "pb-0c5b2769ef7cbe587",
```

```
            "PatchGroup": "ExamplePatchGroup",
            "Status": "COMPLIANT"
        }
    }
}
```

AwsStepFunctions

AwsStepFunctions リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsStepFunctionStateMachine

AwsStepFunctionStateMachine このオブジェクトは、 AWS Step Functions 一連のイベント駆動型ステップで構成されるワークフローであるステートマシンに関する情報を提供します。

次の例は、 AwsStepFunctionStateMachine オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsStepFunctionStateMachine 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsStepFunctionStateMachine「」を参照してください。

例

```
"AwsStepFunctionStateMachine": {
    "StateMachineArn": "arn:aws:states:us-
east-1:123456789012:stateMachine:StepFunctionsLogDisableNonCompliantResource-
fQLujTeXvwsb",
    "Name": "StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
    "Status": "ACTIVE",
    "RoleArn": "arn:aws:iam::123456789012:role/teststepfunc-
StatesExecutionRole-1PNM71RVO1UKT",
    "Type": "STANDARD",
    "LoggingConfiguration": {
        "Level": "OFF",
        "IncludeExecutionData": false
    },
    "TracingConfiguration": {
        "Enabled": false
    }
}
```

AwsWaf

AwsWaf リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsWafRateBasedRule

AwsWafRateBasedRule オブジェクトには、グローバルリソースの AWS WAF レートベースのルールに関する詳細が含まれています。 AWS WAF レートベースのルールは、リクエストを許可、ブロック、またはカウントするタイミングを示す設定を提供します。レートベースのルールには、指定した期間に届くリクエストの数が含まれます。

次の例は、 AwsWafRateBasedRule オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsWafRateBasedRule 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsWafRateBasedRuleDetails「」を参照してください。

例

```
"AwsWafRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRateBasedRule

AwsWafRegionalRateBasedRule オブジェクトには、リージョンリソースのレートベースのルールに関する詳細が含まれています。レートベースのルールは、リクエストを許可、ブロック、またはカウントするタイミングを示す設定を提供します。レートベースのルールには、指定した期間に届くリクエストの数が含まれます。

次の例は、 AwsWafRegionalRateBasedRule オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsWafRegionalRateBasedRule 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsWafRegionalRateBasedRuleDetails「」を参照してください。

例

```
"AwsWafRegionalRateBasedRule":{
    "MatchPredicates" : [{
```

```
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRule

AwsWafRegionalRule オブジェクトは、 AWS WAF リージョンルール に関する詳細を提供します。このルールは、許可、ブロック、またはカウントするウェブリクエストを識別します。

次の例は、 AwsWafRegionalRule オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsWafRegionalRule 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsWafRegionalRuleDetails「」を参照してください。

例

```
"AwsWafRegionalRule": {
    "MetricName": "SampleWAF_Rule__Metric_1",
    "Name": "bb-waf-regional-rule-not-empty-conditions-compliant",
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de95fe",
    "PredicateList": [{
        "DataId": "127d9346-e607-4e93-9286-c1296fb5445a",
        "Negated": false,
        "Type": "GeoMatch"
    }]
}
```

AwsWafRegionalRuleGroup

AwsWafRegionalRuleGroup オブジェクトは、 AWS WAF リージョンルールグループに関する詳細を表示します。ルールグループは、ウェブアクセスコントロールリスト (ウェブ ACL) に追加される事前定義済みルールのコレクションです。

次の例は、 AwsWafRegionalRuleGroup オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsWafRegionalRuleGroup 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsWafRegionalRuleGroupDetails「」を参照してください。

例

```
"AwsWafRegionalRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFClassicRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW"
        }
    }],
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
}
```

AwsWafRegionalWebAcl

AwsWafRegionalWebAcl は、 AWS WAF リージョンウェブアクセスコントロールリスト (ウェブ ACL) の詳細を提供します。ウェブ ACL には、許可、ブロック、またはカウントするリクエストを識別するルールが含まれています。

以下は、 AWS Security Finding 形式 (ASFF) の AwsWafRegionalWebAcl 検出の例です。AwsApiGatewayV2Stage 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsWafRegionalWebAclDetails「」を参照してください。

例

```
"AwsWafRegionalWebAcl": {
    "DefaultAction": "ALLOW",
    "MetricName" : "web-regional-webacl-metric-1",
    "Name": "WebACL_123",
    "RulesList": [
        {
            "Action": {
                "Type": "Block"
            },
            "Priority": 3,
            "RuleId": "24445857-852b-4d47-bd9c-61f05e4d223c",
            "Type": "REGULAR",
            "ExcludedRules": [
```

```
                {
                    "ExclusionType": "Exclusion",
                    "RuleId": "Rule_id_1"
                }
            ],
            "OverrideAction": {
                "Type": "OVERRIDE"
            }
        }
    ],
    "WebAclId": "443c76f4-2e72-4c89-a2ee-389d501c1f67"
}
```

AwsWafRule

`AwsWafRule` は、 AWS WAF ルールに関する情報を提供します。 AWS WAF ルールは、許可、ブロック、またはカウントするウェブリクエストを識別します。

AWS Security Finding 形式 (ASFF) `AwsWafRule`の結果の例を次に示します。`AwsApiGatewayV2Stage` 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsWafRuleDetails「」を参照してください。

例

```
"AwsWafRule": {
    "MetricName": "AwsWafRule_Metric_1",
    "Name": "AwsWafRule_Name_1",
    "PredicateList": [{
        "DataId": "cdd225da-32cf-4773-1dc2-3bca3ed9c19c",
        "Negated": false,
        "Type": "GeoMatch"
    }],
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de953e"
}
```

AwsWafRuleGroup

`AwsWafRuleGroup` は、 AWS WAF ルールグループに関する情報を提供します。 AWS WAF ルールグループは、ウェブアクセスコントロールリスト (ウェブ ACL) に追加される事前定義済みルールのコレクションです。

AWS Security Finding 形式 (ASFF) AwsWafRuleGroupの結果の例を次に示します。AwsApiGatewayV2Stage 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsWafRuleGroupDetails「」を参照してください。

例

```
"AwsWafRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW",
        },
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
    }]
}
```

AwsWafv2RuleGroup

AwsWafv2RuleGroup オブジェクトは、 AWS WAF V2 ルールグループに関する詳細を提供します。

次の例は、 AwsWafv2RuleGroup オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsWafv2RuleGroup 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsWafv「2RuleGroupDetails」を参照してください。

例

```
"AwsWafv2RuleGroup": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/wafv2rulegroupasff/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1000,
    "Description": "Resource for ASFF",
    "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "wafv2rulegroupasff",
    "Rules": [{
     "Action": {
     "Allow": {
      "CustomRequestHandling": {
       "InsertHeaders": [
```

```
        {
        "Name": "AllowActionHeader1Name",
        "Value": "AllowActionHeader1Value"
        },
        {
        "Name": "AllowActionHeader2Name",
        "Value": "AllowActionHeader2Value"
        }
       ]
      }
     },
     "Name": "RuleOne",
     "Priority": 1,
     "VisibilityConfig": {
      "CloudWatchMetricsEnabled": true,
      "MetricName": "rulegroupasff",
      "SampledRequestsEnabled": false
     }
    }],
    "VisibilityConfig": {
     "CloudWatchMetricsEnabled": true,
     "MetricName": "rulegroupasff",
     "SampledRequestsEnabled": false
    }
}
```

AwsWafWebAcl

AwsWafWebAcl オブジェクトは、 AWS WAF ウェブ ACL に関する詳細を提供します。

次の例は、 AwsWafWebAcl オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsWafWebAcl 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsWafWebAclDetails「」を参照してください。

例

```
"AwsWafWebAcl": {
    "DefaultAction": "ALLOW",
    "Name": "MyWafAcl",
    "Rules": [
        {
            "Action": {
                "Type": "ALLOW"
```

```
            },
            "ExcludedRules": [
                {
                    "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98"
                }
            ],
            "OverrideAction": {
                "Type": "NONE"
            },
            "Priority": 1,
            "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98",
            "Type": "REGULAR"
        }
    ],
    "WebAclId": "waf-1234567890"
}
```

AwsWafv2WebAcl

AwsWafv2WebAcl オブジェクトは、 AWS WAF V2 ウェブ ACL の詳細を提供します。

次の例は、 AwsWafv2WebAcl オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsWafv2WebAcl 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsWafv「2WebAclDetails」を参照してください。

例

```
"AwsWafv2WebAcl": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/WebACL-RoaD4QexqSxG/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1326,
    "CaptchaConfig": {
     "ImmunityTimeProperty": {
      "ImmunityTime": 500
     }
    },
    "DefaultAction": {
     "Block": {}
    },
    "Description": "Web ACL for JsonBody testing",
    "ManagedbyFirewallManager": false,
    "Name": "WebACL-RoaD4QexqSxG",
    "Rules": [{
```

```
     "Action": {
      "RuleAction": {
       "Block": {}
      }
     },
     "Name": "TestJsonBodyRule",
     "Priority": 1,
     "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "JsonBodyMatchMetric"
     }
    }],
    "VisibilityConfig": {
     "SampledRequestsEnabled": true,
     "CloudWatchMetricsEnabled": true,
     "MetricName": "TestingJsonBodyMetric"
    }
}
```

AwsXray

AwsXray リソースのセキュリティ AWS 検出結果形式の例を次に示します。

AwsXrayEncryptionConfig

AwsXrayEncryptionConfig オブジェクトには、 の暗号化設定に関する情報が含まれています AWS X-Ray。

次の例は、 AwsXrayEncryptionConfig オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsXrayEncryptionConfig 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のAwsXrayEncryptionConfigDetails「」を参照してください。

例

```
"AwsXRayEncryptionConfig":{
    "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
    "Status": "UPDATING",
    "Type":"KMS"
}
```

Container

結果に関連するコンテナの詳細。

次の例は、 Container オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。Container 属性の説明を表示するには、AWS Security Hub 「 API リファレンス」のContainerDetails「」を参照してください。

例

```
"Container": {
    "ContainerRuntime": "docker",
    "ImageId": "image12",
    "ImageName": "1111111/
knotejs@sha256:372131c9fef111111111111115f4ed3ea5f9dce4dc3bd34ce21846588a3",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "Name": "knote",
    "Privileged": true,
    "VolumeMounts": [{
        "Name": "vol-03909e9",
        "MountPath": "/mnt/etc"
    }]
}
```

Other

Other オブジェクトでは、カスタムのフィールドや値を指定できます。次の場合に Other オブジェクトを使用します。

- リソースタイプに対応する Details オブジェクトがない場合。リソースの詳細を指定するには、Other オブジェクトを使用します。
- リソースタイプの Details オブジェクトに、入力するすべてのフィールドが含まれていない場合。この場合は、リソースタイプの Details オブジェクトを使用して、使用可能な属性を入力します。Other オブジェクトを使用して、タイプ固有のオブジェクトに含まれていない属性に入力してください。
- リソースタイプが提供されたタイプのいずれでもない場合。この場合、Resource.Type を Other に設定し、Other オブジェクトを使用して詳細を入力します。

Type: 最大 50 個のキーバリューペアのマップ

各キーバリューペアは、次の要件を満たしている必要があります。

- キーは 128 文字未満である必要があります。
- 値は 1,024 文字未満である必要があります。

AWS Security Hub のインサイト

AWS Security Hub インサイトは、関連する結果の集合です。注意と介入が必要なセキュリティ工リアを識別します。たとえば、インサイトによって、不十分なセキュリティ慣行を示す結果の対象として EC2 インスタンスが指摘される場合があります。インサイトには、複数の提供元からの結果がまとめられます。

各インサイトは、group by ステートメントとオプションのフィルターによって定義されます。group by ステートメントは、一致する結果をグループ化する方法を示し、インサイトが適用される項目のタイプを識別します。たとえば、インサイトがリソース識別子によってグループ化されている場合、インサイトによってリソース識別子のリストが生成されます。オプションのフィルターは、インサイトの一致する結果を特定します。例えば、特定のプロバイダーからの結果または特定のタイプのリソースに関連付けられた結果のみが、表示されるようにできます。

Security Hub には、組み込みのマネージド型インサイトがいくつか用意されています。マネージド型インサイトを変更または削除することはできません。

お客様の AWS 環境に固有のセキュリティ上の問題と使用状況を追跡するために、カスタムインサイトを作成することもできます。

インサイトは、一致する結果を生成する統合または標準を有効にしている場合にのみ、結果を返します。たとえば、マネージド型インサイト 29 などです。Top resources by counts of failed CIS checks (失敗した CIS チェック数でのトップリソース) は、CIS AWS Foundations 標準を有効にした場合にのみ、結果を返します。

トピック

インサイトのリストの表示とフィルタリング

[Insights] (インサイト) ページには、利用可能なインサイトのリストが表示されます。

デフォルトでは、リストにはマネージド型インサイトとカスタムインサイトの両方が表示されます。インサイトタイプに基づいてインサイトリストをフィルタリングするには、フィルターフィールドの横にあるドロップダウンメニューからインサイトタイプを選択します。

- 使用できるインサイトをすべて表示するには、[All insights] (すべてのインサイト) を選択します。これがデフォルトのオプションです。
- マネージド型インサイトのみを表示するには、[Security Hub managed insights] (Security Hub マネージド型インサイト) を選択します。
- カスタムインサイトのみを表示するには、[Custom insights] (カスタムインサイト) を選択します。

インサイト名のテキストに基づいてインサイトリストをフィルタリングすることもできます。

フィルターフィールドに、リストのフィルタリングに使用するテキストを入力します。フィルターでは、大文字と小文字は区別されません。フィルターは、インサイト名の全体または一部にそのテキストが含まれているインサイトを検索します。

インサイト結果と結果の表示とアクションの実行

インサイトごとに、 AWS Security Hub はまずフィルター条件に一致する結果を決定し、次にグループ化属性を使用して一致する結果をグループ化します。

[Insights] (インサイト) コンソールページで、結果と結果を表示して、それらに対してアクションを実行できます。

クロスリージョン集約を有効にすると、集約リージョンでは、マネージド型インサイトの結果に、集約リージョンとリンクされたリージョンの結果が含まれます。カスタムインサイト結果では、インサイトがリージョンでフィルタリングされない場合、結果に、集約リージョンとリンクされたリージョンからの結果が含まれます。

他のリージョンでは、インサイト結果に含まれるのはそのリージョンの結果のみです。

クロスリージョン集約の設定方法については、「クロスリージョン集約」を参照してください。

インサイト結果の表示とアクションの実行 (コンソール)

インサイト結果は、インサイトの結果をグループ化したリストで構成されます。例えば、インサイトがリソース識別子に基づいてグループ化されている場合、インサイト結果はリソース識別子のリストになります。結果のリストの各項目は、その項目に一致する結果の数を示します。

結果が、リソース識別子またはリソースタイプでグループ化されている場合、結果には、一致する結果のすべてのリソースが含まれます。これには、フィルター条件で指定されたリソースタイプとは異なるタイプのリソースが含まれます。例えば、インサイトでは S3 バケットに関連付けられている結果が識別されます。一致する結果に S3 バケットリソースと IAM アクセスキーリソースの両方が含まれている場合、インサイト結果にはそれらの両方のリソースが一覧表示されます。

結果のリストは、一致する結果が最も多いものから最も少ないものへとソートされます。

Security Hub では 100 件の結果しか表示されません。グループ化値の数が 100 を超える場合、最初の 100 個のみが表示されます。

インサイト結果には、結果のリストに加えて、次の属性に一致した結果の数を要約した一連のチャートが表示されます。

- 重要度ラベル - 各重要度ラベルの結果の数
- AWS アカウント ID – 一致する結果の上位 5 つのアカウント IDs
- リソースタイプ - 一致する結果の上位 5 つのリソースタイプ
- リソース ID - 一致する結果の上位 5 つのリソース ID
- 製品名 - 一致する結果の上位 5 つの結果プロバイダー

カスタムアクションを設定している場合、選択した結果をカスタムアクションに送信できます。アクションは、`Security Hub Insight Results`イベントタイプの CloudWatch ルールに関連付ける必要があります。「the section called “自動応答および自動修復”」を参照してください。

カスタムアクションを設定していない場合は、[Actions] (アクション) メニューは無効です。

インサイト結果のリストを表示して、アクションを実行するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. ナビゲーションペインで、[Insights] (インサイト) を選択します。
3. インサイト結果のリストを表示するには、インサイト名を選択します。
4. カスタムアクションに送信する結果ごとにチェックボックスを選択します。
5. [Actions] (アクション) メニューから、カスタムアクションを選択します。

インサイト結果の表示 (Security Hub API、 AWS CLI)

インサイト結果を表示するには、API コールまたは AWS Command Line Interfaceを使用します。

インサイト結果を表示するには (Security Hub API、 AWS CLI)

- Security Hub API - `GetInsightResults` オペレーションを使用します。インサイトを特定して結果を返すには、インサイト ARN が必要です。カスタムインサイトのインサイト ARN を取得するには、`GetInsights` オペレーションを使用します。
- AWS CLI - コマンドラインで `get-insight-results` コマンドを実行します。

```
aws securityhub get-insight-results --insight-arn <insight ARN>
```

例:

```
aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

インサイト結果の結果の表示 (コンソール)

インサイト結果のリストから、結果ごとに結果のリストを表示できます。

インサイトの結果を表示して、アクションを実行するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. ナビゲーションペインで、[Insights] (インサイト) を選択します。
3. インサイト結果のリストを表示するには、インサイト名を選択します。
4. インサイト結果の結果のリストを表示するには、インサイト結果のリストからその項目を選択します。

結果リストには、ワークフローステータスが `NEW` または `NOTIFIED` で、選択されたインサイト結果のアクティブな結果が表示されます。

結果リストから、以下のアクションを実行できます。

- リストのフィルターとグループ化を変更する
- 個々の結果の詳細を表示する
- 結果のワークフローステータスを更新する
- カスタムアクションに結果を送信する

マネージド型インサイト

AWS Security Hub では、あらかじめ用意されたマネージド型インサイトを利用することができます。

Security Hub のマネージド型インサイトを編集または削除することはできません。インサイトの結果と検出結果を表示し、それらに対してアクションを実行できます。また、マネージド型インサイトを新しいカスタムインサイトのベースとして使用することができます。

すべてのインサイトと同様、マネージド型インサイトは、一致する結果をする製品統合またはセキュリティ標準が有効にされている場合にのみ、結果を返します。

リソース識別子でグループ化されたインサイトの場合、結果には、一致する結果のすべてのリソースの識別子が含まれます。これには、フィルター条件のリソースタイプとは異なるタイプのリソースが含まれます。例えば、インサイト 2 では Amazon S3 バケットに関連付けられている結果が識別されます。一致する結果に S3 バケットリソースと IAM アクセスキーリソースの両方が含まれている場合、インサイト結果には両方のリソースが含まれます。

Security Hub には、次のマネージド型インサイトが用意されています。

1. ほとんどの結果を含む AWS リソース

   ARN: `arn:aws:securityhub:::insight/securityhub/default/1`

   グループ化の基準: リソース識別子

   結果フィルター:

   - レコードの状態が `ACTIVE`
   - ワークフローステータスが `NEW` または `NOTIFIED`

2. パブリック書き込みまたは読み取り許可を含む S3 バケット

   ARN: `arn:aws:securityhub:::insight/securityhub/default/10`

   グループ化の基準: リソース識別子

   結果フィルター:

   - タイプが `Effects/Data Exposure` で始まる
   - リソースタイプが `AwsS3Bucket`
   - レコードの状態が `ACTIVE`

- ワークフローステータスが NEW または NOTIFIED

3. 最も多くの結果を生成している AMI

   ARN: arn:aws:securityhub:::insight/securityhub/default/3

   グループ化の基準: EC2 インスタンスイメージ ID

   結果フィルター:

   - リソースタイプが AwsEc2Instance
   - レコードの状態が ACTIVE
   - ワークフローステータスが NEW または NOTIFIED

4. 既知の戦略、手法、および手順 (TTP) に含まれる EC2 インスタンス

   ARN: arn:aws:securityhub:::insight/securityhub/default/14

   グループ化の基準: リソース ID

   結果フィルター:

   - タイプが TTPs で始まる
   - リソースタイプが AwsEc2Instance
   - レコードの状態が ACTIVE
   - ワークフローステータスが NEW または NOTIFIED

5. 疑わしいアクセスキーアクティビティに関連する AWS プリンシパル

   ARN: arn:aws:securityhub:::insight/securityhub/default/9

   グループ化の基準: IAM アクセスキーのプリンシパル名

   結果フィルター:

   - リソースタイプが AwsIamAccessKey
   - レコードの状態が ACTIVE
   - ワークフローステータスが NEW または NOTIFIED

6. セキュリティ標準/ベストプラクティスを満たさない AWS リソースインスタンス

   ARN: arn:aws:securityhub:::insight/securityhub/default/6

   グループ化の基準: リソース ID

結果フィルター:

- タイプが Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

7. 潜在的なデータの不正引き出しに関連付けられている AWS リソース

   ARN: arn:aws:securityhub:::insight/securityhub/default/7

   グループ化の基準: リソース ID

   結果フィルター:

   - タイプが Effects/Data Exfiltration/ で始まる
   - レコードの状態が ACTIVE
   - ワークフローステータスが NEW または NOTIFIED

8. 不正なリソース消費に関連付けられている AWS リソース

   ARN: arn:aws:securityhub:::insight/securityhub/default/8

   グループ化の基準: リソース ID

   結果フィルター:

   - タイプが Effects/Resource Consumption で始まる
   - レコードの状態が ACTIVE
   - ワークフローステータスが NEW または NOTIFIED

9. セキュリティ標準/ベストプラクティスを満たさない S3 バケット

   ARN: arn:aws:securityhub:::insight/securityhub/default/11

   グループ化の基準: リソース ID

   結果フィルター:

   - リソースタイプが AwsS3Bucket
   - タイプが Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices
   - レコードの状態が ACTIVE

- ワークフローステータスが NEW または NOTIFIED

10. 機密データを含む S3 バケット

    ARN: arn:aws:securityhub:::insight/securityhub/default/12

    グループ化の基準: リソース ID

    結果フィルター:

    - リソースタイプが AwsS3Bucket
    - タイプが Sensitive Data Identifications/ で始まる
    - レコードの状態が ACTIVE
    - ワークフローステータスが NEW または NOTIFIED

11. 漏洩した可能性がある認証情報

    ARN: arn:aws:securityhub:::insight/securityhub/default/13

    グループ化の基準: リソース ID

    結果フィルター:

    - タイプが Sensitive Data Identifications/Passwords/ で始まる
    - レコードの状態が ACTIVE
    - ワークフローステータスが NEW または NOTIFIED

12. 重要な脆弱性のセキュリティパッチが欠落している EC2 インスタンス

    ARN: arn:aws:securityhub:::insight/securityhub/default/16

    グループ化の基準: リソース ID

    結果フィルター:

    - タイプが Software and Configuration Checks/Vulnerabilities/CVE で始まる
    - リソースタイプが AwsEc2Instance
    - レコードの状態が ACTIVE
    - ワークフローステータスが NEW または NOTIFIED

13. 一般的な異常な動作に関連する EC2 インスタンス

    ARN: arn:aws:securityhub:::insight/securityhub/default/17

グループ化の基準: リソース ID

結果フィルター:

- タイプが Unusual Behaviors で始まる
- リソースタイプが AwsEc2Instance
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

14. インターネットからアクセス可能なポートを持つ EC2 インスタンス

ARN: arn:aws:securityhub:::insight/securityhub/default/18

グループ化の基準: リソース ID

結果フィルター:

- タイプが Software and Configuration Checks/AWS Security Best Practices/Network Reachability で始まる
- リソースタイプが AwsEc2Instance
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

15. セキュリティ標準/ベストプラクティスを満たさない EC2 インスタンス

ARN: arn:aws:securityhub:::insight/securityhub/default/19

グループ化の基準: リソース ID

結果フィルター:

- タイプが次のいずれかで始まる。
  - Software and Configuration Checks/Industry and Regulatory Standards/
  - Software and Configuration Checks/AWS Security Best Practices
- リソースタイプが AwsEc2Instance
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

16. インターネットに開放されている EC2 インスタンス

ARN: arn:aws:securityhub:::insight/securityhub/default/21

グループ化の基準: リソース ID

結果フィルター:

- タイプが Software and Configuration Checks/AWS Security Best Practices/Network Reachability で始まる
- リソースタイプが AwsEc2Instance
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

17. 敵対的な偵察に関連付けられている EC2 インスタンス

ARN: arn:aws:securityhub:::insight/securityhub/default/22

グループ化の基準: リソース ID

結果フィルター:

- タイプが TTPs/Discovery/Recon で始まる
- リソースタイプが AwsEc2Instance
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

18. マルウェアに関連付けられている AWS リソース

ARN: arn:aws:securityhub:::insight/securityhub/default/23

グループ化の基準: リソース ID

結果フィルター:

- タイプが次のいずれかで始まる。
  - Effects/Data Exfiltration/Trojan
  - TTPs/Initial Access/Trojan
  - TTPs/Command and Control/Backdoor
  - TTPs/Command and Control/Trojan
  - Software and Configuration Checks/Backdoor
  - Unusual Behaviors/VM/Backdoor
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

19. 暗号通貨の問題に関連付けられている AWS リソース

    ARN: arn:aws:securityhub:::insight/securityhub/default/24

    グループ化の基準: リソース ID

    結果フィルター:

    - タイプが次のいずれかで始まる。
      - Effects/Resource Consumption/Cryptocurrency
      - TTPs/Command and Control/CryptoCurrency
    - レコードの状態が ACTIVE
    - ワークフローステータスが NEW または NOTIFIED
20. 不正なアクセス試行に関連付けられている AWS リソース

    ARN: arn:aws:securityhub:::insight/securityhub/default/25

    グループ化の基準: リソース ID

    結果フィルター:

    - タイプが次のいずれかで始まる。
      - TTPs/Command and Control/UnauthorizedAccess
      - TTPs/Initial Access/UnauthorizedAccess
      - Effects/Data Exfiltration/UnauthorizedAccess
      - Unusual Behaviors/User/UnauthorizedAccess
      - Effects/Resource Consumption/UnauthorizedAccess
    - レコードの状態が ACTIVE
    - ワークフローステータスが NEW または NOTIFIED
21. 先週ヒット数が最も多かった脅威インテリジェンス指標

    ARN: arn:aws:securityhub:::insight/securityhub/default/26

    結果フィルター:

    - 過去 7 日以内に作成
22. 結果数による上位アカウント

    ARN: arn:aws:securityhub:::insight/securityhub/default/27

グループ化の基準: AWS アカウント ID

結果フィルター:

- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

23. 結果数による上位製品

ARN: arn:aws:securityhub:::insight/securityhub/default/28

グループ化の基準: 製品名

結果フィルター:

- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

24. 結果数による重要度

ARN: arn:aws:securityhub:::insight/securityhub/default/29

グループ化の基準: 重要度ラベル

結果フィルター:

- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

25. 結果数による上位 S3 バケット

ARN: arn:aws:securityhub:::insight/securityhub/default/30

グループ化の基準: リソース ID

結果フィルター:

- リソースタイプが AwsS3Bucket
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

26. 結果数による上位 EC2 インスタンス

ARN: arn:aws:securityhub:::insight/securityhub/default/31

グループ化の基準: リソース ID

結果フィルター:

- リソースタイプが AwsEc2Instance
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

27. 結果数による上位 AMI

ARN: arn:aws:securityhub:::insight/securityhub/default/32

グループ化の基準: EC2 インスタンスイメージ ID

結果フィルター:

- リソースタイプが AwsEc2Instance
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

28. 結果数による上位 IAM ユーザー

ARN: arn:aws:securityhub:::insight/securityhub/default/33

グループ化の基準: IAM アクセスキー ID

結果フィルター:

- リソースタイプが AwsIamAccessKey
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

29. 失敗した CIS チェック数による上位リソース

ARN: arn:aws:securityhub:::insight/securityhub/default/34

グループ化の基準: リソース ID

結果フィルター:

- ジェネレーター ID が arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule で始まる
- 最終日に更新
- コンプライアンス状況が FAILED

- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

30. 調査数による上位統合

ARN: arn:aws:securityhub:::insight/securityhub/default/35

グループ化の基準: 製品 ARN

結果フィルター:

- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

31. セキュリティチェックの失敗が最も多いリソース

ARN: arn:aws:securityhub:::insight/securityhub/default/36

グループ化の基準: リソース ID

結果フィルター:

- 最終日に更新
- コンプライアンス状況が FAILED
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

32. 不審なアクティビティに関連する IAM ユーザー

ARN: arn:aws:securityhub:::insight/securityhub/default/37

グループ化の基準: IAM ユーザー

結果フィルター:

- リソースタイプが AwsIamUser
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

33. ほとんどの AWS Health 検出結果を含むリソース

ARN: arn:aws:securityhub:::insight/securityhub/default/38

グループ化の基準: リソース ID

結果フィルター:

- ProductNameがHealth

34. ほとんどの AWS Config 検出結果を含むリソース

ARN: arn:aws:securityhub:::insight/securityhub/default/39

グループ化の基準: リソース ID

結果フィルター:

- ProductNameがConfig

35. 最も検出結果の多いアプリケーション

ARN: arn:aws:securityhub:::insight/securityhub/default/40

グループ化の基準: ResourceApplicationArn

結果フィルター:

- RecordStateがACTIVE
- Workflow.Status が NEW または NOTIFIED

カスタムインサイト

AWS Security Hub のマネージド型インサイトに加えて、Security Hub にカスタムインサイトを作成して、環境に固有の問題とリソースを追跡できます。カスタムインサイトでは、問題のキュレーションされたサブセットを追跡することができます。

以下に、設定に役立つカスタムインサイトの例をいくつか示します。

- 管理者アカウントを所有している場合は、カスタムインサイトを設定して、メンバーアカウントに影響を与えているクリティカルな結果および重要度の高い結果を追跡できます。
- 特定の統合されていますAWSサービスでは、カスタムインサイトを設定して、そのサービスからのクリティカルな結果および重大度が高い結果を追跡できます。
- サードパーティー統合に依存する場合、カスタムインサイトを設定して、その統合された製品からクリティカルな結果と重大度が高い結果を追跡できます。

まったく新しいカスタムインサイトを作成するか、既存のカスタムインサイトまたはマネージド型インサイトから作成を開始できます。

各インサイトは、次のオプションを使用して設定できます。

- Grouping attribute (グループ化属性) - グループ化属性によって、インサイト結果リストに表示される項目が決定します。例えば、グループ化属性が [Product name] (製品名) の場合、インサイト結果には、結果プロバイダー別に結果の数が表示されます。
- Optional filters (オプションのフィルター) - フィルターにより、インサイトの一致する結果が絞り込まれます。

  結果をクエリするとき、Security Hub はブール AND 論理をフィルターのセットに適用します。つまり、結果は、指定されたすべてのフィルターに一致する場合にのみ一致となります。例えば、フィルターが「製品名が GuardDuty」と「リソースタイプが `AwsS3Bucket`」である場合、一致となる結果はこれらの両方の条件に一致する必要があります。

  ただし、Security Hub では、同じ属性に異なる値を使用するフィルターにはブール OR 論理を適用します。例えば、フィルターが「製品名が GuardDuty」と「製品名が Amazon Inspector」である場合、結果は、GuardDuty または Amazon Inspector のいずれかによって生成されていれば一致となります。

リソース識別子またはリソースタイプをグループ化属性として使用する場合、インサイト結果には、一致する結果内のすべてのリソースが含まれます。このリストは、リソースタイプフィルターに一致するリソースに限定されません。例えば、インサイトは S3 バケットに関連付けられている結果を特定し、それらの結果をリソース識別子でグループ化します。一致する結果には、S3 バケットリソースと IAM アクセスキーリソースの両方が含まれます。インサイト結果には、両方のリソースが含まれます。

カスタムインサイトの作成 (コンソール)

コンソールから、まったく新しいインサイトを作成できます。

カスタムインサイトを作成するには

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。
2. ナビゲーションペインで、[Insights] (インサイト) を選択します。
3. [Create insight] (インサイトの作成) を選択します。
4. インサイトのグループ化属性を選択するには:

   a. 検索ボックスを選択して、フィルターオプションを表示します。

   b. [Group by] (グループ化の条件) を選択します。

c. このインサイトに関連付けられている結果をグループ化するのに使用する属性を選択します。

d. [Apply] (適用) を選択します。

5. (オプション) このインサイトに使用する追加のフィルターを選択します。フィルターごとに、フィルター条件を定義し、[Apply] (適用) を選択します。
6. [Create insight] (インサイトの作成) を選択します。
7. [Insight name] (インサイトの名前) を入力し、[Create insight] (インサイトの作成) を選択します。

カスタムインサイトの作成 (プログラマティック)

お好みの方法を選択し、手順に従って Security Hub でプログラムに従ってカスタムインサイトを作成します。フィルターを指定して、インサイト内の結果のコレクションを特定のサブセットに絞り込むことができます。

次のタブには、カスタムインサイトを作成するための手順がいくつかの言語で記載されています。その他の言語でのサポートについては、構築に役立つツールAWSを参照してください。

Security Hub API

1. `CreateInsight` オペレーションを実行します。
2. `Name` パラメータにカスタムインサイトの名前を指定します。
3. `Filters` パラメーターを入力して、インサイトに含める結果を指定します。
4. `GroupByAttribute` パラメーターを入力して、インサイトに含まれる結果をグループ化するために使用する属性を指定します。
5. オプションで、特定のフィールドで調査結果をソートする `SortCriteria` パラメーターを指定します。

クロスリージョン集約 を有効にしていて、集約リージョンからこの API を呼び出すと、インサイトは集約とリンクされたリージョンでの一致する結果に適用されます。

AWS CLI

1. コマンドラインで、`create-insight` コマンドを実行します。
2. `name` パラメータにカスタムインサイトの名前を指定します。
3. `filters` パラメーターを入力して、インサイトに含める結果を指定します。

4. group-by-attribute パラメーターを入力して、インサイトに含まれる結果をグループ化するために使用する属性を指定します。

クロスリージョン集計を有効にして、このコマンドを集約リージョンから実行した場合、インサイトは集約とリンクされたリージョンでの一致する結果に適用されます。

```
aws securityhub create-insight --name <insight name> --filters <filter values> --
group-by-attribute <attribute name>
```

例

```
aws securityhub create-insight --name "Critical role findings" --filters
 '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

1. New-SHUBInsight コマンドレットを使用します。
2. Name パラメータにカスタムインサイトの名前を指定します。
3. Filter パラメーターを入力して、インサイトに含める結果を指定します。
4. GroupByAttribute パラメーターを入力して、インサイトに含まれる結果をグループ化するために使用する属性を指定します。

クロスリージョン集約を有効にしていて、集約リージョンからこのコマンドレットを使用すると、インサイトは集約とリンクされたリージョンでの一致する結果に適用されます。

例

```
$Filter = @{
    AwsAccountId = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "XXX"
    }
    ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = 'FAILED'
    }
}
```

```
New-SHUBInsight -Filter $Filter -Name TestInsight -GroupByAttribute ResourceId
```

カスタムインサイトの変更 (コンソール)

既存のカスタムインサイトのグループ化値とフィルターを変更できます。変更後、元のインサイトのまま更新内容を保存するか、新しいインサイトとして更新されたバージョンを保存できます。

インサイトを変更するには

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。
2. ナビゲーションペインで、[Insights] (インサイト) を選択します。
3. 変更するカスタムインサイトを選択します。
4. 必要に応じてインサイト設定を編集します。
   - インサイトで結果のグループ化に使用される属性を変更するには:
     a. 既存のグループ化を削除するには、[Group by] (グループ化の条件) 設定の横にある X を選択します。
     b. 検索ボックスを選択します。
     c. グループ化に使用する属性を選択します。
     d. [Apply] (適用) を選択します。
   - インサイトからフィルターを削除するには、フィルターの横にある円で囲まれた X を選択します。
   - インサイトにフィルターを追加するには:
     a. 検索ボックスを選択します。
     b. フィルターとして使用する属性と値を選択します。
     c. [Apply] (適用) を選択します。
5. 更新が完了したら、[Save insight] (インサイトの保存) を選択します。
6. プロンプトが表示されたら、次のいずれかを実行します。
   - 既存のインサイトを更新して変更を反映させる場合は、[Update ***<Insight_Name>***] (<Insight_Name> を更新) を選択してから、[Save insight] (インサイトの保存) を選択します。
   - 更新内容を使用して新しいインサイトを作成する場合は、[Save new insight] (新しいインサイトの保存) を選択します。[Insight name] (インサイトの名前) に入力して、[Save insight] (インサイトの保存) を選択します。

カスタムインサイトの変更 (プログラマティック)

カスタムインサイトを変更するには、希望の方法を選択し、手順に従います。

Security Hub API

1. UpdateInsight オペレーションを実行します。
2. カスタムインサイトを特定するには、インサイトの Amazon リソースネーム (ARN) を指定します。カスタムインサイトの ARN を取得するには、GetInsightsオペレーションを実行します。
3. 必要に応じて、Name, Filters と GroupByAttribute パラメータを更新します。

AWS CLI

1. コマンドラインで、update-insight コマンドを実行します。
2. カスタムインサイトを特定するには、インサイトの Amazon リソースネーム (ARN) を指定します。カスタムインサイトの ARN を取得するには、get-insightsコマンドを実行します。
3. 必要に応じて、name, filters と group-by-attribute パラメータを更新します。

```
aws securityhub update-insight --insight-arn <insight ARN> [--name <new name>] [--
filters <new filters>] [--group-by-attribute <new grouping attribute>]
```

例

```
aws securityhub update-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value":
 "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' --
name "High severity role findings"
```

PowerShell

1. Update-SHUBInsight コマンドレットを使用します。
2. カスタムインサイトを特定するには、インサイトの Amazon リソースネーム (ARN) を指定します。カスタムインサイトの ARN を取得するには、Get-SHUBInsightコマンドレットを使用します。

3. 必要に応じて、Name, Filter と GroupByAttribute パラメータを更新します。

例

```
$Filter = @{
    ResourceType = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "AwsIamRole"
    }
    SeverityLabel = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "HIGH"
    }
}

Update-SHUBInsight -InsightArn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" -Filter $Filter -Name "High severity role findings"
```

マネージド型インサイトからの新しいカスタムインサイトの作成 (コンソール)

マネージド型インサイトに変更を保存したり、マネージド型インサイトを削除したりすることはできません。マネージド型インサイトを新しいカスタムインサイトのベースとして使用することはできます。

マネージド型インサイトから新しいカスタムインサイトを作成するには

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。
2. ナビゲーションペインで、[Insights] (インサイト) を選択します。
3. 作成元になるマネージド型インサイトを選択します。
4. 必要に応じてインサイト設定を編集します。

   - インサイトで結果のグループ化に使用される属性を変更するには:

     a. 既存のグループ化を削除するには、[Group by] (グループ化の条件) 設定の横にある X を選択します。

     b. 検索ボックスを選択します。

c. グループ化に使用する属性を選択します。

d. [Apply] (適用) を選択します。

- インサイトからフィルターを削除するには、フィルターの横にある円で囲まれた X を選択します。
- インサイトにフィルターを追加するには:

a. 検索ボックスを選択します。

b. フィルターとして使用する属性と値を選択します。

c. [Apply] (適用) を選択します。

5. 更新が完了したら、[Create insight] (インサイトの作成) を選択します。
6. プロンプトが表示されたら、[Insight name] (インサイト名) に入力し、[Create insight] (インサイトの作成) を選択します。

カスタムインサイトの削除 (コンソール)

カスタムインサイトは、不要になった場合、削除できます。マネージド型インサイトは、削除することはできません。

カスタムインサイトを削除するには

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。
2. ナビゲーションペインで、[Insights] (インサイト) を選択します。
3. 削除するカスタムインサイトを見つけます。
4. そのインサイトで、その他のオプションを表示するためのアイコン (カードの右上隅にある 3 つのドット) を選択します。
5. [Delete] (削除) をクリックします。

カスタムインサイトの削除 (プログラマティック)

カスタムインサイトの削除は、希望の方法を選択し、手順に従います。

Security Hub API

1. `DeleteInsight` オペレーションを実行します。
2. 削除するカスタムインサイトを特定するには、インサイト ARN を指定します。カスタムインサイトの ARN を取得するには、`GetInsights`オペレーションを実行します。

AWS CLI

1. コマンドラインで、delete-insight コマンドを実行します。
2. カスタムインサイトを特定するには、インサイト ARN を指定します。カスタムインサイトの ARN を取得するには、get-insightsコマンドを実行します。

```
aws securityhub delete-insight --insight-arn <insight ARN>
```

例

```
aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

PowerShell

1. Remove-SHUBInsight コマンドレットを使用します。
2. カスタムインサイトを特定するには、インサイト ARN を指定します。カスタムインサイトの ARN を取得するには、Get-SHUBInsightコマンドレットを使用します。

例

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

オートメーション

Security Hub の自動化により、仕様に基づいて検出結果を迅速に修正および修復できます。

Security Hub は現在、次の 2 種類の自動化をサポートしています。

- 自動化ルール — 定義した基準に基づいて、ほぼリアルタイムで検出結果を自動的に更新および非表示にします。
- 自動対応と修復 — 特定の検出結果やインサイトに対して実行する自動アクションを定義するカスタム EventBridge ルールを作成できます。

自動化ルールは EventBridge ルールよりも先に適用されます。つまり、EventBridge に送信される前に自動化ルールがトリガーされ、検出結果が更新されます。その後、EventBridge のルールが更新された検出結果に適用されます。

セキュリティコントロールの自動化を設定するときは、タイトルや説明ではなく、コントロール ID に基づいてフィルタリングすることをお勧めします。Security Hub でコントロールのタイトルや説明を更新することがありますが、コントロール ID は変わりません。

トピック

- 自動化ルール
- 自動応答および自動修復

自動化ルール

自動化ルールを使用すると、Security Hub の検出結果を自動的に更新できます。検出結果が取り込まれると、Security Hub は検出結果の非表示、重要度の変更、結果へのメモの追加など、さまざまなルールアクションを適用できます。このようなルールアクションは、検出結果が指定した基準 (結果に関連付けられているリソースまたはアカウント ID、タイトルなど) に一致した場合に有効になります。

自動化ルールの使用例には、次のようなものがあります。

- 検出結果のリソース ID がビジネス上重要なリソースを参照している場合、検出結果の重大度を `CRITICAL` に上げます。
- 検出結果が特定の本番稼働用アカウントのリソースに影響する場合は、検出結果の重要度を `HIGH` から `CRITICAL` に引き上げます。

- INFORMATIONAL 重要度を持つ SUPPRESSED ワークフローステータスの特定の検出結果を割り当てます。

自動化ルールを使用して、 AWS Security Finding 形式 (ASFF) で選択した検出結果フィールドを更新できます。ルールは、新しい検出結果と更新された検出結果の両方に適用されます。

カスタムルールを最初から作成することも、Security Hub が提供するルールテンプレートを使用することもできます。ルールテンプレートを使用する場合は、使用状況に合わせて必要に応じて変更できます。

自動化ルールの仕組み

Security Hub 管理者は、ルール条件を定義して自動化ルールを作成できます。検出結果が定義済みの条件と一致すると、Security Hub はその結果にルールアクションを適用します。使用可能な条件とアクションの詳細については、「使用可能なルール基準とルールアクション」を参照してください。

Security Hub 管理者アカウントのみが自動化ルールを作成、削除、編集、表示できます。管理者が作成したルールは、管理者アカウントとすべてのメンバーアカウントの検出結果に適用されます。メンバーアカウント ID をルール条件に指定することで、Security Hub 管理者は自動化ルールを使用して特定のメンバーアカウントの検出結果を更新したり、検出結果に対してアクションを実行したりすることもできます。

自動化ルールは、 AWS リージョン それが作成された にのみ適用されます。複数のリージョンにルールを適用するには、委任された管理者がリージョンごとにルールを作成する必要があります。ルールの作成は、Security Hub コンソール、Security Hub API、または AWS CloudFormation を使用して実行できます。また、マルチリージョンデプロイスクリプトを使用することも可能です。

自動化ルールによって検出結果がどのように変化したかを知るには、「結果履歴の確認」を参照してください。

> **Important**
>
> 自動化ルールは、ルールの作成後に Security Hub が生成または取り込む新規および更新された検出結果に適用されます。Security Hub は、12～24 時間ごと、または関連リソースの状態が変化したときに、コントロール検出結果を更新します。詳細については、「Schedule for running security checks」を参照してください。自動化ルールは、プロバイダーが提供する元の検出結果フィールドを評価します。BatchUpdateFindings オペレーションを通じてルールを作成した後に結果フィールドを更新しても、ルールはトリガーされません。

Security Hub は現在、管理者アカウントで最大 100 の自動化ルールをサポートしています。

ルールの順序

自動化ルールを作成するときは、各ルールに順序を割り当てます。これにより、Security Hub が自動化ルールを適用する順序が決まり、複数のルールが同じ検出結果または結果フィールドに関連する場合に重要になってきます。

複数のルールアクションが同じ検出結果または結果フィールドに関連する場合、ルール順序の数値が最も大きいルールが最後に適用され、最終的な結果となります。

Security Hub コンソールでルールを作成すると、Security Hub はルールの作成順序に基づいて、ルールの順序を自動的に割り当てます。最後に作成されたルールは、ルール順序の数値が最も小さいため、最初に適用されます。Security Hub は後続のルールを昇順で適用します。

Security Hub API または を使用してルールを作成すると AWS CLI、Security Hub は`RuleOrder`最初に数値が最も低いルールを適用します。その後、後続のルールを昇順で適用します。複数の検出結果に同じ `RuleOrder` がある場合、Security Hub は `UpdatedAt` フィールドに以前の値のルールを最初に適用します (つまり、最後に編集されたルールが最後に適用されます)。

ルールの順序はいつでも変更できます。

ルール順序の例:

ルール A (ルール順序は **1**):

- ルール A の基準
  - `ProductName` = `Security Hub`
  - `Resources.Type` は `S3 Bucket`
  - `Compliance.Status` = `FAILED`
  - `RecordState` は `NEW`
  - `Workflow.Status` = `ACTIVE`
- ルール A のアクション
  - `Confidence` を `95` に更新
  - `Severity` を `CRITICAL` に更新

ルール B (ルールの順序は **2**):

- ルール B の基準
  - AwsAccountId = 123456789012
- ルール B のアクション
  - Severity を INFORMATIONAL に更新

ルール A のアクションは、ルール A の基準に一致する Security Hub の検出結果に最初に適用されます。次に、ルール B のアクションが指定されたアカウント ID の Security Hub の検出結果に適用されます。この例では、ルール B が最後に適用されるため、指定されたアカウント ID からの検出結果における Severity の最終値は INFORMATIONAL です。ルール A のアクションに基づくと、一致した検出結果の Confidence の最終値は 95 です。

使用可能なルール基準とルールアクション

現在、次の ASFF フィールドが自動化ルールの条件としてサポートされています。

ASFF フィールド	フィルター	フィールドタイプ
AwsAccountId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
AwsAccountName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
CompanyName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
ComplianceAssociatedStandardsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列

ASFF フィールド	フィルター	フィールドタイプ
ComplianceSecurityControlId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
ComplianceStatus	Is, Is Not	選択:[FAILED, NOT_AVAILABLE , PASSED, WARNING]
Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	数
CreatedAt	Start, End, DateRange	日付 (形式例: 2022-12-01T21:47:39.269Z)
Criticality	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	数
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
FirstObservedAt	Start, End, DateRange	日付 (形式例: 2022-12-01T21:47:39.269Z)
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列

ASFF フィールド	フィルター	フィールドタイプ
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
LastObservedAt	Start, End, DateRange	日付 (形式例: 2022-12-01T21:47:39.269Z)
NoteText	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
NoteUpdatedAt	Start, End, DateRange	日付 (形式例: 2022-12-01T21:47:39.269Z)
NoteUpdatedBy	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
ProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
ProductName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列

ASFF フィールド	フィルター	フィールドタイプ
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	マッピング
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列

ASFF フィールド	フィルター	フィールドタイプ
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
ResourceTags	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	マッピング
ResourceType	Is, Is Not	選択 (ASFF がサポートするリソースを参照)
SeverityLabel	Is, Is Not	選択: [CRITICAL, HIGH, MEDIUM, LOW, INFORMATIONAL]
SourceUrl	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
Title	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
Type	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
UpdatedAt	Start, End, DateRange	日付 (形式例: 2022-12-01T21:47:39.269Z)

ASFF フィールド	フィルター	フィールドタイプ
UserDefinedFields	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	マッピング
VerificationState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
WorkflowStatus	Is, Is Not	選択: [NEW, NOTIFIED, RESOLVED, SUPPRESSED]

現在、次の ASFF フィールドが自動化ルールのアクションとしてサポートされています。

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

特定の ASFF フィールドの詳細については、「AWS Security Finding 形式」および「ASFF の例」を参照してください。

> **Tip**
>
> Security Hub で特定のコントロールに関する検出結果の生成を停止したい場合は、自動化ルールを使用する代わりにコントロールを無効にすることをお勧めします。コントロールを無効にすると、Security Hub はそのコントロールに対するセキュリティチェックの実行を停止し、検出結果の生成を停止するため、そのコントロールに対する料金は発生しません。自

動化ルールを使用し、定義した条件に一致する検出結果に関して、特定の ASFF フィールド値を変更することをおすすめします。コントロールの無効化に関する詳細については、「すべての標準におけるコントロールの有効化と無効化」を参照してください。

自動化ルールの作成

カスタムルールを最初から作成することも、事前に入力されている Security Hub のルールテンプレートを使用することもできます。

一度に作成できる自動化ルールは 1 つだけです。複数の自動化ルールを作成するには、コンソールの手順を複数回実行するか、必要なパラメータを指定して API またはコマンドを複数回呼び出します。

ルールを検出結果に適用させる各リージョンとアカウントで自動化ルールを作成する必要があります。

Security Hub コンソールで自動化ルールを作成すると、Security Hub では、そのルールが適用される検出結果のプレビューが表示されます。ルール条件に CONTAINS または NOT_CONTAINS フィルターが含まれている場合のプレビューは現在サポートされていません。これらのフィルターは、マッピングフィールドタイプと文字列フィールドタイプに対して選択できます。

Important

AWS では、ルール名、説明、またはその他のフィールドに個人を特定できる情報、機密情報、または機密情報を含めないことをお勧めします。

テンプレートからのルールの作成 (コンソールのみ)

現在、Security Hub コンソールのみがルールテンプレートをサポートしています。これらのテンプレートは自動化ルールの一般的な使用事例を反映しており、この機能を使うのに役立ちます。以下の手順を完了して、コンソールのテンプレートから自動化ルールを作成します。

Console

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   Security Hub 管理者アカウントにサインインします。
2. ナビゲーションペインで [オートメーション] を選択します。

3. [Create rule (ルールの作成)] を選択します。[ルールタイプ] で、[テンプレートからルールを作成] を選択します。
4. ドロップダウンメニューからルールテンプレートを選択します。
5. (オプション) 使用状況の必要に応じて、[ルール]、[基準]、[自動化アクション] セクションを変更します。少なくとも 1 つのルール基準と 1 つのルールアクションを指定する必要があります。

   選択した基準でサポートされている場合、コンソールには、基準に一致する検出結果のプレビューが表示されます。
6. [ルールステータス] では、ルールを作成した後でそのルールを [有効] にするか [無効] にするかを選択します。
7. (オプション) [詳細設定] セクションを展開します。このルールをルール条件に一致する検出結果に適用する最後のルールにしたい場合は、[これらの条件に一致する検出結果については後続のルールを無視する] を選択します。
8. (オプション) [タグ] でタグをキーと値のペアとして追加すると、ルールを簡単に識別できるようになります。
9. [Create rule (ルールの作成)] を選択します。

カスタムルールの作成

ご希望の方法を選択し、次の手順を完了させ、カスタム自動化ルールを作成します。

Console

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   Security Hub 管理者アカウントにサインインします。
2. ナビゲーションペインで [オートメーション] を選択します。
3. [Create rule (ルールの作成)] を選択します。[ルールタイプ] で [カスタムルールを作成] を選択します。
4. [ルール] セクションで、一意のルール名とルールの説明を入力します。
5. [基準] では、[キー]、[オペレータ]、および [値] のドロップダウンメニューを使用して、ルール条件を指定します。少なくとも 1 つのルール基準を指定する必要があります。

   選択した基準でサポートされている場合、コンソールには、基準に一致する検出結果のプレビューが表示されます。

6. [自動アクション] の場合は、ドロップダウンメニューを使用して、検出結果がルール条件に一致したときに更新する結果フィールドを指定します。少なくとも 1 つのルールアクションを指定する必要があります。
7. [ルールステータス] では、ルールを作成した後でそのルールを [有効] にするか [無効] にするかを選択します。
8. (オプション) [詳細設定] セクションを展開します。このルールをルール条件に一致する検出結果に適用する最後のルールにしたい場合は、[これらの条件に一致する検出結果については後続のルールを無視する] を選択します。
9. (オプション) [タグ] でタグをキーと値のペアとして追加すると、ルールを簡単に識別できるようになります。
10. [Create rule (ルールの作成)] を選択します。

API

1. Security Hub 管理者アカウントで、`CreateAutomationRule` を実行します。この API は、特定の Amazon リソースネーム (ARN) を使用してルールを作成します。
2. ルールの名前と説明を入力します。
3. このルールを、ルール条件に一致する検出結果に適用する最後のルールにする場合は、`IsTerminal` パラメーターを `true` に設定します。
4. `RuleOrder` パラメータでは、ルールの順序を指定します。Security Hub は、このパラメータで最初に小さい数値のルールを適用します。
5. `RuleStatus` パラメータでは、Security Hub を有効にするかどうかを指定し、作成後、検出結果にルールを適用し始めます。値を指定しない場合、デフォルトは `ENABLED` になります。値が `DISABLED` の場合、ルールは作成後に一時停止されます。
6. `Criteria` パラメータでは、Security Hub に検出結果のフィルタリングで使用したい条件を指定します。ルールアクションは、条件に一致する検出結果に適用されます。サポートされている条件のリストについては、「使用可能なルール基準とルールアクション」を参照してください。
7. `Actions` パラメータでは、検出結果と定義した条件が一致した場合に Security Hub に実行させたいアクションを指定します。サポートされているアクションのリストについては、使用可能なルール基準とルールアクション を参照してください。

API リクエストの例:

```
{
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
                "Text": "Known issue that is not a risk.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }],
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "GeneratorId": [{
            "Value": "aws-foundational-security-best-practices/v/1.0.0/IAM.1",
            "Comparison": "EQUALS"
        }]
    },
    "Description": "Sample rule description",
    "IsTerminal": false,
    "RuleName": "sample-rule-name",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
}
```

AWS CLI

1. Security Hub 管理者アカウントで、`create-automation-rule` コマンドを実行します。このコマンドは、特定の Amazon リソースネーム (ARN) を使用してルールを作成します。
2. ルールの名前と説明を入力します。
3. このルールを、ルール条件に一致する検出結果に適用される最後のルールにする場合は、`is-terminal` パラメータを含めます。それ以外の場合は、`no-is-terminal` パラメータを含めます。
4. `rule-order` パラメータでは、ルールの順序を指定します。Security Hub は、このパラメータで最初に小さい数値のルールを適用します。
5. `rule-status` パラメータでは、Security Hub を有効にするかどうかを指定し、作成後、検出結果にルールを適用し始めます。値を指定しない場合、デフォルトは `ENABLED` になります。値が `DISABLED` の場合、ルールは作成後に一時停止されます。
6. `criteria` パラメータでは、Security Hub に検出結果のフィルタリングで使用したい条件を指定します。ルールアクションは、条件に一致する検出結果に適用されます。サポートされている条件のリストについては、「使用可能なルール基準とルールアクション」を参照してください。
7. `actions` パラメータでは、検出結果と定義した条件が一致した場合に Security Hub に実行させたいアクションを指定します。サポートされているアクションのリストについては、使用可能なルール基準とルールアクション を参照してください。

コマンドの例:

```
aws securityhub create-automation-rule \
--actions '[{
 "Type": "FINDING_FIELDS_UPDATE",
 "FindingFieldsUpdate": {
 "Severity": {
 "Label": "HIGH"
 },
 "Note": {
 "Text": "Known issue that is a risk. Updated by automation rules",
 "UpdatedBy": "sechub-automation"
 }
 }
 }]' \
--criteria '{
 "SeverityLabel": [{
```

```
 "Value": "INFORMATIONAL",
 "Comparison": "EQUALS"
 }]
 }' \
--description "A sample rule" \
--no-is-terminal \
--rule-name "sample rule" \
--rule-order 1 \
--rule-status "ENABLED" \
--region us-east-1
```

自動化ルールを表示する

ご希望の方法を選択し、手順に従って自動化ルールと各ルールの詳細を確認してください。

Console

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   Security Hub 管理者アカウントにサインインします。
2. ナビゲーションペインで [オートメーション] を選択します。
3. ルール名を選択します。または、ルールを選択してください。
4. [アクション]、[ログの表示] の順に選択します。

API

1. アカウントの自動化ルールを表示するには、Security Hub 管理者アカウントから `ListAutomationRules` を実行します。この API は、使用中のルールのルール ARN とその他のメタデータを返します。この API には入力パラメータは必要ありませんが、オプションで結果の数を制限するために `MaxResults` を指定したり、ページ区切りパラメータとして `NextToken` を指定したりできます。`NextToken` の初期値は `NULL` である必要があります。

   API リクエストの例:

   ```
   {
    "MaxResults": 50,
    "NextToken": "cVpdnSampleTokenYcXgTockBW44c"
   ```

```
}
```

2. ルールの基準やアクションなど、その他のルールの詳細については、Security Hub 管理者アカウントから BatchGetAutomationRules を実行してください。

   API リクエストの例:

```
{
    "AutomationRulesArns": [
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
    ]
}
```

AWS CLI

1. アカウントの自動化ルールを表示するには、Security Hub 管理者アカウントから list-automation-rules コマンドを実行します。このコマンドは、使用中のルールのルール ARN とその他のメタデータを返します。このコマンドには入力パラメータは必要ありませんが、オプションで結果の数を制限するために max-results を指定したり、ページ区切りパラメータとして next-token を指定したりできます。

   コマンドの例:

```
aws securityhub list-automation-rules  \
--max-results 5 \
--next-token cVpdnSampleTokenYcXgTockBW44c \
--region us-east-1
```

2. ルールの基準やアクションなど、その他のルールの詳細については、Security Hub 管理者アカウントから batch-get-automation-rules コマンドを実行します。

   コマンドの例:

```
aws securityhub batch-get-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-
east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
 "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222"]' \
--region us-east-1
```

自動化ルールの編集

自動化ルールを編集すると、ルール編集後に Security Hub が生成または取り込む新しい検出結果や更新された結果に変更が適用されます。

ご希望の方法を選択し、手順に従って自動化ルールの内容を編集します。1 回のリクエストで 1 つ以上のルールを編集できます。ルール順序の編集方法については、「ルール順序の編集」を参照してください。

Console

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   Security Hub 管理者アカウントにサインインします。
2. ナビゲーションペインで [オートメーション] を選択します。
3. 編集するルールを選択します。[アクション]、[編集] の順に選択します。
4. 必要に応じてルールを変更し、[変更を保存] を選択します。

API

1. Security Hub 管理者アカウントで、`BatchUpdateAutomationRules` を実行します。
2. `RuleArn` パラメータでは、編集するルールの ARN を指定します。
3. 編集するパラメータの新しい値を指定します。`RuleArn` 以外の任意のパラメータを編集できます。

   API リクエストの例:

```
{
    "UpdateAutomationRulesRequestItems": [
```

```
        {
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "RuleOrder": 15,
            "RuleStatus": "Enabled"
        },
        {
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "RuleStatus": "Disabled"
        }
    ]
}
```

AWS CLI

1. Security Hub 管理者アカウントで、batch-update-automation-rules コマンドを実行します。
2. RuleArn パラメータでは、編集するルールの ARN を指定します。
3. 編集するパラメータの新しい値を指定します。RuleArn 以外の任意のパラメータを編集できます。

コマンドの例:

```
aws securityhub batch-update-automation-rules \
--update-automation-rules-request-items '[
    {
      "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
          "Note": {
            "Text": "Known issue that is a risk",
            "UpdatedBy": "sechub-automation"
          },
          "Workflow": {
            "Status": "NEW"
          }
        }
      }],
      "Criteria": {
        "SeverityLabel": [{
```

```
          "Value": "LOW",
          "Comparison": "EQUALS"
        }]
      },
      "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "RuleOrder": 14,
      "RuleStatus": "DISABLED",
    }
  ]' \
--region us-east-1
```

ルール順序の編集

場合によっては、ルールの条件とアクションはそのままで、Security Hub が自動化ルールを適用する順序を変更する場合もあります。ご希望の方法を選択し、手順に従ってルールの順序を編集します。

Console

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   Security Hub 管理者アカウントにサインインします。
2. ナビゲーションペインで [オートメーション] を選択します。
3. 順序を変更するルールを選択します。[優先度を編集] を選択します。
4. ルールの優先度を 1 単位上げるには、[上に移動] を選択します。ルールの優先度を 1 単位下げるには、[下に移動] を選択します。ルールに [1] の順序を割り当てるには、[先頭に移動] を選択します (これにより、このルールが他の既存のルールよりも優先されます)。

> **Note**
>
> Security Hub コンソールでルールを作成すると、Security Hub はルールの作成順序に基づいて、ルールの順序を自動的に割り当てます。最後に作成されたルールは、ルール順序の数値が最も小さいため、最初に適用されます。

API

1. Security Hub 管理者アカウントで、`BatchUpdateAutomationRules` を実行します。

2. `RuleArn` パラメータでは、順序を編集するルールの ARN を指定します。
3. `RuleOrder` フィールドの値を変更します。

> **Note**
>
> 複数のルールに同じ `RuleOrder` がある場合、Security Hub は `UpdatedAt` フィールドに以前の値のルールを最初に適用します (つまり、最後に編集されたルールが最後に適用されます)。

AWS CLI

1. Security Hub 管理者アカウントで、`batch-update-automation-rules` コマンドを実行します。
2. `RuleArn` パラメータでは、順序を編集するルールの ARN を指定します。
3. `RuleOrder` フィールドの値を変更します。

> **Note**
>
> 複数のルールに同じ `RuleOrder` がある場合、Security Hub は `UpdatedAt` フィールドに以前の値のルールを最初に適用します (つまり、最後に編集されたルールが最後に適用されます)。

自動化ルールを削除する

自動化ルールを削除すると、Security Hub はそのルールをアカウントから削除し、検出結果に適用されなくなります。

ご希望の方法を選択し、手順に従って自動化ルールを削除します。1 回のリクエストで 1 つ以上のルールを削除できます。

> **Tip**
>
> 削除の代わりに、ルールを無効にすることもできます。これにより、ルールは後で使用できるよう保持されますが、Security Hub は、有効にするまで一致する検出結果にはルールを適用しません。

Console

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   Security Hub 管理者アカウントにサインインします。
2. ナビゲーションペインで [オートメーション] を選択します。
3. 削除するルールを選択します。[アクション]、[削除] の順に選択します (ルールを保持しながら一時的に無効にするには、[無効] を選択します)。
4. 選択を確認して、[削除] をクリックします。

API

1. Security Hub 管理者アカウントで、`BatchDeleteAutomationRules` を実行します。
2. `AutomationRulesArns` パラメータでは、削除するルールの ARN を指定します (ルールを保持しながら一時的に無効にするには、`RuleStatus` パラメータの `DISABLED` を指定します)。

API リクエストの例:

```
{
    "AutomationRulesArns": [
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
    ]
}
```

AWS CLI

1. Security Hub 管理者アカウントで、batch-delete-automation-rules コマンドを実行します。
2. automation-rules-arns パラメータでは、削除するルールの ARN を指定します (ルールを保持しながら一時的に無効にするには、RuleStatus パラメータの DISABLED を指定します)。

コマンドの例:

```
aws securityhub batch-delete-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"]' \
--region us-east-1
```

自動化ルールの例

このセクションでは、一般的な使用事例の自動化ルールの例をいくつか紹介します。これらの例は、Security Hub コンソールのルールテンプレートに対応しています。

S3 バケットなどの特定のリソースが危険にさらされている場合は、重要度を「重大」に引き上げます。

この例では、検出結果の ResourceId が特定の Amazon Simple Storage Service (Amazon S3) バケットである場合にルール条件が一致します。ルールアクションは、一致した検出結果の重要度を CRITICAL に変更することです。このテンプレートを変更して他のリソースに適用できます。

API リクエストの例:

```
{
    "IsTerminal": true,
    "RuleName": "Elevate severity of findings that relate to important resources",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity to CRITICAL when specific resource such as an S3 bucket is at risk",
    "Criteria": {
        "ProductName": [{
```

```
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "ResourceId": [{
            "Value": "arn:aws:s3:::examplebucket/developers/design_info.doc",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "This is a critical resource. Please review ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

CLI コマンドの例:

```
aws securityhub create-automation-rule \
--is-terminal \
--rule-name "Elevate severity of findings that relate to important resources" \
--rule-order 1 \
--rule-status "ENABLED" \
```

```
--description "Elevate finding severity to CRITICAL when specific resource such as an
 S3 bucket is at risk" \
--criteria '{
"ProductName": [{
"Value": "Security Hub",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"ResourceId": [{
"Value": "arn:aws:s3:::examplebucket/developers/design_info.doc",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "This is a critical resource. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

本番稼働用アカウントのリソースに関連する検出結果の重大度を上げます。

この例では、特定の本番稼働用アカウントで重要度 HIGH の検出結果が生成されると、ルール条件が一致します。ルールアクションは、一致した検出結果の重要度を CRITICAL に変更することです。

API リクエストの例:

```
{
    "IsTerminal": false,
    "RuleName": "Elevate severity for production accounts",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity from HIGH to CRITICAL for findings that
 relate to resources in specific production accounts",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "HIGH",
            "Comparison": "EQUALS"
        }],
        "AwsAccountId": [
        {
            "Value": "111122223333",
            "Comparison": "EQUALS"
        },
        {
            "Value": "123456789012",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
```

```
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "A resource in production accounts is at risk. Please review
 ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

CLI コマンドの例:

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Elevate severity of findings that relate to resources in production
 accounts" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Elevate finding severity from HIGH to CRITICAL for findings that relate
 to resources in specific production accounts" \
--criteria '{
"ProductName": [{
"Value": "Security Hub",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "HIGH",
"Comparison": "EQUALS"
}],
"AwsAccountId": [
{
"Value": "111122223333",
"Comparison": "EQUALS"
```

```
},
{
"Value": "123456789012",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "A resource in production accounts is at risk. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

情報の検出結果を非表示にする

この例では、Amazon から Security Hub に送信されたINFORMATIONAL重要度の検出結果に対してルール基準が一致されます GuardDuty。ルールアクションは、一致した検出結果のワークフローステータスを SUPPRESSED に変更することです。

API リクエストの例:

```
{
    "IsTerminal": false,
    "RuleName": "Suppress informational findings",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Suppress GuardDuty findings with INFORMATIONAL severity",
    "Criteria": {
        "ProductName": [{
            "Value": "GuardDuty",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
```

```
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "INFORMATIONAL",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
                "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL
 severity",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

CLI コマンドの例:

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Suppress informational findings" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Suppress GuardDuty findings with INFORMATIONAL severity" \
--criteria '{
"ProductName": [{
"Value": "GuardDuty",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
```

```
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "INFORMATIONAL",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Workflow": {
"Status": "SUPPRESSED"
},
"Note": {
"Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

自動応答および自動修復

Amazon EventBridge を使用すると、アプリケーションの可用性の問題やリソースの変化などのシステムイベントに自動的に対応するように AWS のサービスを自動化できます。AWS サービスのイベントは、ほぼリアルタイムで、保証に基づいて EventBridge に配信されます。簡単なルールを記述して、注目するイベントと、イベントがルールに一致した場合に自動的に実行するアクションを指定できます。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 関数の呼び出し
- Amazon EC2 Run Command の呼び出し
- Amazon Kinesis Data Streams へのイベントの中継
- AWS Step Functions ステートマシンのアクティブ化
- Amazon SNS トピックまたは Amazon SQS キューの通知

- サードパーティーのチケット発行、チャット、SIEM、またはインシデント対応および管理ツールへの結果の送信

Security Hub は、すべての新しい結果と既存の結果のすべての更新を EventBridge イベントとして EventBridge に自動的に送信します。また、選択した結果とインサイト結果を EventBridge に送信できるカスタムアクションを作成することもできます。

次に、それぞれの種類のイベントに応答するように EventBridge ルールを設定します。

EventBridge の使用方法の詳細については、「Amazon EventBridge ユーザーガイド」を参照してください。

> **Note**
>
> ベストプラクティスとして、EventBridge にアクセスするためにユーザーに付与された許可が、必要な許可のみを付与する最小特権の IAM ポリシーを使用していることを確認してください。
> 詳細については、「Amazon EventBridge でのアイデンティティとアクセス管理」を参照してください。

クロスアカウントの自動応答と自動修復のための一連のテンプレートは、AWS ソリューションでも使用できます。このテンプレートでは、EventBridge イベントルールと Lambda 関数を利用します。AWS CloudFormation と AWS Systems Manager を使用してソリューションをデプロイします。このソリューションによって、完全に自動化された応答と修復のアクションが作成されます。また、Security Hub カスタムアクションを使用して、ユーザによってトリガーされる応答と修復のアクションを作成することもできます。ソリューションの設定方法と使用方法の詳細については、「AWS での自動化されたセキュリティ対応」ソリューションページを参照してください。

トピック

- EventBridge との Security Hub 統合のタイプ
- Security Hub の EventBridge イベント形式
- 自動的に送信される結果の EventBridge ルールの設定
- カスタムアクションを使用して結果とインサイト結果を EventBridge に送信する

EventBridge との Security Hub 統合のタイプ

Security Hub では、次の EventBridge イベントタイプを使用して、EventBridge との次のタイプの統合をサポートします。

Security Hub の EventBridge ダッシュボードの [All Events] (すべてのイベント) には、これらのイベントタイプがすべて含まれています。

すべての結果 (Security Hub Findings - Imported)

Security Hub は、すべての新しい結果と既存の結果のすべての更新を EventBridge イベントとして Security Hub Findings - Imported に自動的に送信します。各 Security Hub Findings - Imported イベントには 1 つの結果が含まれています。

どの `BatchImportFindings` および `BatchUpdateFindings` リクエストでも Security Hub Findings - Imported イベントがトリガーされます。

管理者アカウントの場合、EventBridge のイベントフィードには、管理者アカウントとメンバーアカウントの両方からの結果に関するイベントが含まれます。

集約リージョンでは、イベントフィードには、集約リージョンとリンクされたリージョンからの結果のイベントが含まれます。クロスリージョン結果は、ほぼリアルタイムでイベントフィードに追加されます。結果の集約を設定する方法については、「クロスリージョン集約」を参照してください。

結果を自動的に Amazon S3 バケット、修復ワークフロー、またはサードパーティーツールにルーティングするルールを EventBridge で定義できます。ルールでは、結果に特定の属性値が含まれている場合にのみルールを適用するフィルターを指定できます。

このメソッドを使用して、すべての結果、または固有の特徴を持つすべての結果を応答または修復ワークフローに自動的に送信します。

「the section called “自動的に送信される結果のルールの設定”」を参照してください。

カスタムアクションの結果 (Security Hub Findings - Custom Action)

Security Hub では、カスタムアクションに関連付けられた結果も Security Hub Findings - Custom Actionイベントとして EventBridge に送信します。

これは、コンソールを操作し、特定の結果、または少数の一連の結果を応答または修復ワークフローに送信するアナリストの役に立ちます。一度に最大 20 件の結果のカスタムアクションを選択できます。各結果は、個別の EventBridge イベントとして EventBridge に送信されます。

カスタムアクションを作成したら、カスタムアクションにカスタムアクション ID を割り当てます。この ID を使用すると、そのカスタムアクション ID に関連付けられた結果を受け取った後、指定されたアクションを実行する EventBridge ルールを作成できます。

「the section called “カスタムアクションの設定と使用方法”」を参照してください。

例えば、Security Hub で `send_to_ticketing` というカスタムアクションを作成するとします。次に EventBridge で、`send_to_ticketing` カスタムアクション ID を含む結果を EventBridge が受信したときにトリガーされるルールを作成します。ルールには、結果をチケット発行システムに送信するロジックが含まれています。次に、Security Hub 内で結果を選択して Security Hub のカスタムアクションを使用して、手動で結果をチケット発行システムに送信できます。

EventBridge に Security Hub の検出結果を送信して処理を続行する方法の例については、「AWS パートナーネットワーク (APN) ブログ」の「AWS Security Hub カスタムアクションと PagerDuty との統合方法」および「AWS Security Hub でカスタムアクションを有効にする方法」を参照してください。

カスタムアクションのインサイト結果 (Security Hub Insight Results)

カスタムアクションを使用すると、インサイト結果のセットも Security Hub Insight Results イベントとして EventBridge に送信できます。インサイト結果は、インサイトに一致するリソースです。インサイト結果を EventBridge に送信するとき、結果を EventBridge に送信しているわけではないことに注意してください。インサイト結果に関連付けられたリソース識別子を送信しているだけです。最大 100 個のリソース識別子を一度に送信できます。

結果に対するカスタムアクションと同様に、Security Hub でカスタムアクションを作成してから、EventBridge でルールを作成します。

「the section called “カスタムアクションの設定と使用方法”」を参照してください。

例えば、同僚と共有する必要がある特定のインサイト結果があるとします。この場合、カスタムアクションを使用して、チャットまたはチケット発行システム経由で、そのインサイト結果を同僚に送信できます。

Security Hub の EventBridge イベント形式

Security Hub Findings - Imported、Security Findings - Custom Action、および Security Hub Insight Results イベントタイプでは、次のイベント形式を使用します。

イベント形式は、Security Hub が EventBridge にイベントを送信するときに使用される形式です。

Security Hub Findings - Imported

Security Hub から EventBridge に送信される Security Hub Findings - Imported イベントには、次の形式が使用されます。

```
{
   "version":"0",
   "id":"CWE-event-id",
   "detail-type":"Security Hub Findings - Imported",
   "source":"aws.securityhub",
   "account":"111122223333",
   "time":"2019-04-11T21:52:17Z",
   "region":"us-west-2",
   "resources":[
      "arn:aws:securityhub:us-west-2::product/aws/macie/arn:aws:macie:us-
west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/
f2893b211841"
   ],
   "detail":{
      "findings": [{
         <finding content>
       }]
   }
}
```

<finding content> は、イベントによって送信される結果の JSON 形式のコンテンツです。各イベントは 1 つの結果を送信します。

結果の属性の詳細なリストについては、「AWS Security Finding 形式 (ASFF)」を参照してください。

このようなイベントによってトリガーされる EventBridge ルールを設定する方法については、「the section called “自動的に送信される結果のルールの設定”」を参照してください。

Security Hub Findings - Custom Action

Security Hub から EventBridge に送信される Security Hub Findings - Custom Action イベントには、次の形式が使用されます。各結果は個別のイベントで送信されます。

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
```

```
  "detail-type": "Security Hub Findings - Custom Action",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:securityhub:us-west-1:111122223333:action/custom/custom-action-name"
  ],
  "detail": {
    "actionName":"custom-action-name",
    "actionDescription": "description of the action",
    "findings": [
      {
        <finding content>
      }
    ]
  }
}
```

<finding content> は、イベントによって送信される結果の JSON 形式のコンテンツです。各イベントは 1 つの結果を送信します。

結果の属性の詳細なリストについては、「AWS Security Finding 形式 (ASFF)」を参照してください。

このようなイベントによってトリガーされる EventBridge ルールを設定する方法については、「the section called “カスタムアクションの設定と使用方法”」を参照してください。

Security Hub Insight Results

Security Hub から EventBridge に送信される Security Hub Insight Results イベントには、次の形式が使用されます。

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Insight Results",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [
```

```
      "arn:aws:securityhub:us-west-1:111122223333::product/aws/macie:us-
west-1:222233334444:test/trigger/1ec9cf700ef6be062b19584e0b7d84ec/alert/f2893b211841"
  ],
  "detail": {
    "actionName":"name of the action",
    "actionDescription":"description of the action",
    "insightArn":"ARN of the insight",
    "insightName":"Name of the insight",
    "resultType":"ResourceAwsIamAccessKeyUserName",
    "number of results":"number of results, max of 100",
    "insightResults": [
        {"result 1": 5},
        {"result 2": 6}
    ]
  }
}
```

このようなイベントによってトリガーされる EventBridge ルールを作成する方法については、「the section called “カスタムアクションの設定と使用方法”」を参照してください。

自動的に送信される結果の EventBridge ルールの設定

Security Hub Findings - Imported イベントの受信時に実行するアクションを定義するルールを EventBridge で作成できます。Security Hub Findings - Imported イベントは、`BatchImportFindings` と `BatchUpdateFindings` の両方による更新によってトリガーされます。

各ルールには、ルールをトリガーするイベントを識別するイベントパターンが含まれています。イベントパターンにはイベントソース (`aws.securityhub`) とイベントタイプ (Security Hub Findings - Imported) が必ず含まれています。イベントパターンでは、ルールが適用される結果を識別するためのフィルターを指定することもできます。

次に、ルールによってルールターゲットが識別されます。ターゲットは、EventBridge が Security Hub Findings - Imported イベントを受信し、検索条件がフィルターと一致したときに実行されるアクションです。

ここで説明する手順では、EventBridge コンソールを使用します。このコンソールを使用すると、EventBridge による CloudWatch Logs への書き込みを有効にする必要なリソースベースポリシーが EventBridge によって自動的に作成されます。

また、EventBridge API の `PutRule` API オペレーションを使用することもできます。ただし、EventBridge API を使用する場合は、リソースベースのポリシーを作成する必要があります。必

要なポリシーの詳細については、「Amazon EventBridge ユーザーガイド」の「CloudWatch Logs の許可」を参照してください。

イベントパターンの形式

Security Hub Findings - Imported イベントのイベントパターンの形式は次のとおりです。

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- source は、イベントを生成するサービスとして Security Hub を示します。
- detail-type は、イベントのタイプを示します。
- detail はオプションで、イベントパターンのフィルター値を提供します。イベントパターンに detail フィールドが含まれていない場合、すべての結果でルールがトリガーされます。

結果は、どの結果属性に基づいてもフィルタリングできます。属性ごとに、1 つ以上の値のカンマ区切りの配列を指定します。

```
"<attribute name>": [ "<value1>", "<value2>"]
```

属性に複数の値を指定すると、それらの値は OR で結合されます。結果にリストされている値が含まれている場合、結果は個々の属性のフィルターと一致しています。例えば、Severity.Label の値として INFORMATIONAL と LOW の両方を指定した場合、結果に INFORMATIONAL または LOW の重要度ラベルが含まれていると、結果は一致となります。

属性が AND で結合されている場合、結果が、指定されたすべての属性のフィルター条件に一致すると、その結果は一致となります。

属性値を指定するときは、AWS Security Finding 形式 (ASFF) 構造内でその属性の位置を反映させる必要があります。

> **Tip**
>
> コントロールの検出結果をフィルタリングする場合は、`Title` または `Description` ではなく、`SecurityControlId` または `SecurityControlArn` ASFF フィールドをフィルターとして使用することをお勧めします。前者のフィールドは変更される可能性がありますが、コントロール ID と ARN は静的な識別子です。

次の例では、イベントパターンによって `ProductArn` と `Severity.Label` のフィルタ値が提供されています。したがって、Amazon Inspector が生成し、その重要度のラベルが `INFORMATIONAL` または `LOW` である場合は、結果が一致します。

```
{
    "source": [
        "aws.securityhub"
     ],
    "detail-type": [
        "Security Hub Findings - Imported"
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
    }
}
```

イベントルールの作成

定義済みのイベントパターンまたはカスタムのイベントパターンを使用して、EventBridge でルールを作成することができます。定義済みのパターンを選択した場合、EventBridge で `source` と `detail-type` が自動的に入力されます。EventBridge には、次の結果の属性のフィルター値を指定するフィールドもあります。

- `AwsAccountId`

- `Compliance.Status`
- `Criticality`
- `ProductArn`
- `RecordState`
- `ResourceId`
- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

EventBridge ルールを作成するには

1. Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) を開きます。
2. 次の値を使用して、検索イベントをモニタリングする EventBridge ルールを作成します。
   - ルールタイプ では、イベントパターンを持つルール を選択します。
   - イベントパターンの作成方法を選択します。

次を使用してイベントパターンを作成するには	手順	
テンプレート	[Event pattern] (イベントパターン) のセクションで、次のオプションを選択します。 • [イベントパターンフォーム] では、AWS[サービス] を選択します。 • [AWS のサービス] で、[Security Hub] を選択します。 • [Event type] (イベントタイプ)で、[Security Hub Findings - Imported]	

次を使用してイベントパターンを作成するには	手順	
	(Security Hub 調査結果 - インポート) を選択します。 • (オプション) ルールをより具体的にしたいときは、フィルタ値を追加します。例えば、ルールを、アクティブなレコード状態を持つ結果のみに限定するときは、[Specific Record state(s)] (特定のレコード状態) で [Active] (アクティブ) を選択します。	

次を使用してイベントパターンを作成するには	手順	
カスタムのイベントパターン (カスタムパターンは、EventBridge コンソールに表示されない属性に基づいて結果をフィルタリングするときに使用します)。	• [Event pattern] (イベントパターン) セクションで [Custom patterns (JSON editor)] (カスタムパターン (JSONエディター)) を選択し、次のイベントパターンをテキストエリアに貼付けます。 `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "<attribute name> ": [ "<value1>", "<value2>"] } } }` • イベントパターンを更新し、フィルタとして使用する属性および属性値を追加します。 例えば、検証状態が TRUE_POSITIVE である結果にのみルールを適用	

次を使用してイベントパターンを作成するには	手順	
	するときは、次のパターン例を使用します。 `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "VerificationState": ["TRUE_POSITIVE"] } } }`	

- [Target types] (ターゲットタイプ) で [AWS service] AWS Lambda のサービス) を選択し、[Select a target] (ターゲットを選択) でターゲット (Amazon SNS のトピックや 関数など) を選択します。ターゲットは、ルールで定義したイベントパターンに一致するイベントが返されたときにトリガーされます。

ルールの作成に関する詳細については、「Amazon EventBridge ユーザーガイド」の「イベントに反応する Amazon EventBridge ルールの作成」を参照してください。

カスタムアクションを使用して結果とインサイト結果を EventBridge に送信する

Security Hub カスタムアクションを使用して結果またはインサイト結果を EventBridge に送信するには、まず Security Hub でカスタムアクションを作成します。次に、EventBridge でカスタムアクションに適用されるルールを定義します。

最大 50 個のカスタムアクションを作成できます。

クロスリージョン集約を有効にし、集約リージョンの結果を管理する場合は、集約リージョンでカスタムアクションを作成します。

EventBridge のルールでは、カスタムアクションの ARN が使用されます。

カスタムアクションを作成する (コンソール)

カスタムアクションを作成するときは、名前、説明、および一意の識別子を指定します。

Security Hub (コンソール) でカスタムアクションを作成するには

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。
2. ナビゲーションペインで、[Settings] (設定) を選択して、[Custom actions] (カスタムアクション) を選択します。
3. [Create custom action] (カスタムアクションの作成) を選択します。
4. アクションの [Name] (名前)、[Description] (説明)、および [Custom action ID] (カスタムアクション ID) を指定します。

   [Name] (名前) は 20 文字未満で指定する必要があります。

   [Custom action ID] (カスタムアクション ID) は AWS アカウントごとに一意にする必要があります。
5. [Create custom action] (カスタムアクションの作成) を選択します。
6. [Custom action ARN] (カスタムアクション ARN) を書き留めます。この ARN は、EventBridge でルールを作成してこのアクションに関連付けるときに使用する必要があります。

カスタムアクションを作成する (Security Hub API、AWS CLI)

カスタムアクションを作成するには、API コールまたは AWS Command Line Interface を使用します。

カスタムアクションを作成するには (Security Hub API、AWS CLI)

- Security Hub API - `CreateActionTarget` オペレーションを使用します。カスタムアクションを作成するときは、名前、説明、およびカスタムアクション識別子を指定します。
- AWS CLI - コマンドラインで `create-action-target` コマンドを実行します。

```
create-action-target --name <customActionName> --
description <customActionDescription> --id <customActionidentifier>
```

例

```
aws securityhub create-action-target --name "Send to remediation" --description
 "Action to send the finding for remediation tracking" --id "Remediation"
```

EventBridge でルールを定義する

カスタムアクションを処理するには、EventBridge で対応するルールを作成する必要があります。ルールの定義には、カスタムアクションの ARN が含まれます。

Security Hub Findings - Custom Action イベントのイベントパターンの形式は次のとおりです。

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Security Hub Insight Results イベントのイベントパターンの形式は次のとおりです。

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
```

```
  "resources": [ "<custom action ARN>" ]
}
```

どちらのパターンでも、*<custom action ARN>* がカスタムアクションの ARN です。したがって、複数のカスタムアクションに適用されるルールを構成できます。

ここで説明する手順では、EventBridge コンソールを使用します。このコンソールを使用すると、EventBridge による CloudWatch Logs への書き込みを有効にする必要なリソースベースポリシーが EventBridge によって自動的に作成されます。

また、EventBridge API の `PutRule` API オペレーションを使用することもできます。ただし、EventBridge API を使用する場合は、リソースベースのポリシーを作成する必要があります。必要なポリシーの詳細については、「Amazon EventBridge ユーザーガイド」の「CloudWatch Logs の許可」を参照してください。

EventBridge でルールを定義するには

1. Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) を開きます。
2. ナビゲーションペインで Rules] (ルール) を選択します。
3. ルールの作成 を選択します。
4. ルールの名前と説明を入力します。
5. イベントバス] では、このルールに関連付けるイベントバスを選択します。このルールをアカウントからのイベントと一致させるには、[default] (デフォルト) を選択します。アカウントの AWS サービスがイベントを発行すると、常にアカウントのデフォルトのイベントバスに移動します。
6. [Rule type] (ルールタイプ) では、[Rule with an event pattern] (イベントパターンを持つルール) を選択します。
7. [Next] (次へ) を選択します。
8. [Event source] (イベントソース) で、[AWSevents] (イベント) を選択します。
9. [イベントパターン] で、[イベントパターンフォーム] を選択します。
10. [イベントパターンフォーム] では、AWS[サービス] を選択します。
11. [AWS のサービス] で、[Security Hub] を選択します。
12. [イベントタイプ] の場合は、次のいずれかの操作を実行します。

    - 結果をカスタムアクションに送信するときに適用するルールを作成するには、[Security Hub Findings - Custom Action] (Security Hub 結果 - カスタムアクション) を選択します。

- インサイト結果をカスタムアクションに送信するときに適用するルールを作成するには、[Security Hub Insight Results] (Security Hub インサイト結果) を選択します。

13. [Specific custom action ARNs] (特定のカスタムアクション ARN) を選択し、カスタムアクション ARN を追加します。

    このルールを複数のカスタムアクションに適用する場合は、[Add] (追加) を選択し、カスタムアクション ARN をさらに追加します。

14. [Next] (次へ) をクリックします。
15. [Select targets] (ターゲットの選択) で、このルールが一致した場合に呼び出すターゲットを選択し設定します。
16. [Next] (次へ) をクリックします。
17. (オプション) ルールに 1 つ以上のタグを入力します。詳細については、Amazon EventBridge ユーザーガイドのAmazon EventBridge のタグを参照してください。
18. 次へ をクリックします。
19. ルールの詳細を確認し、ルールの作成 を選択します。

    アカウントで、結果またはインサイト結果に対してカスタムアクションを実行すると、EventBridge でイベントが生成されます。

結果とインサイト結果のカスタムアクションを選択する

Security Hub カスタムアクションと EventBridge ルールを作成すると、結果とインサイト結果を EventBridge に送信して、さらに管理および処理することができます。

イベントは、そのイベントが表示されているアカウントでのみ、EventBridge に送信されます。管理者アカウントを使用して結果を表示すると、イベントは管理者アカウントで EventBridge に送信されます。

AWS API コールを有効にするには、ターゲットコードの実装時に、ロールをメンバーアカウントに切り替える必要があります。つまり、切り替えるロールは、アクションが必要な各メンバーにもデプロイされる必要があります。

結果を EventBridge に送信するには

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。
2. 結果のリストを表示します。

- [Findings] (結果) では、有効になっているすべての製品の統合とコントロールの結果を表示できます。
- [Security standards] (セキュリティ標準) では、選択したコントロールから生成された結果のリストに移動できます。「the section called “コントロールの詳細の表示”」を参照してください。
- [Integrations] (統合) では、有効にした統合によって生成された結果のリストに移動できます。「the section called “統合先からの結果の表示”」を参照してください。
- [Insights] (インサイト) では、インサイト結果のリストに移動できます。「the section called “インサイト結果と結果の表示”」を参照してください。

3. 結果を選択して、EventBridge に送信します。一度に最大 20 件の結果を選択できます。
4. [Actions] (アクション) ドロップダウンから、適用する EventBridge ルールと一致するカスタムアクションを選択します。

   Security Hub によって、結果ごとに個別の Security Hub Findings - Custom Action イベントが送信されます。

インサイト結果を EventBridge に送信するには

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。
2. ナビゲーションペインで、[Insights] (インサイト) を選択します。
3. [Insights] (インサイト) ページで、EventBridge に送信する結果が含まれているインサイトを選択します。
4. EventBridge に送信するインサイト結果を選択します。一度に最大 20 件の結果を選択できます。
5. [Actions] (アクション) ドロップダウンから、適用する EventBridge ルールと一致するカスタムアクションを選択します。

AWS Security Hub での製品の統合

AWS Security Hub は、複数の AWS サービスおよびサポートされている AWS パートナーネットワーク (APN) セキュリティソリューションからセキュリティ結果データを集約できます。この集約により、AWS 環境全体のセキュリティとコンプライアンスを包括的に把握できます。

また、独自のカスタムセキュリティ製品から生成された結果を送信することもできます。

> **Important**
>
> Security Hub は、サポートされている AWS およびパートナーの製品の統合から、AWS アカウント で Security Hub を有効にした後に生成された結果のみを受信し、集約します。Security Hub を有効化する前に生成されたセキュリティ結果を、さかのぼって受け取ったり統合したりすることはありません。

取り込まれた結果に対して Security Hub が課金する方法の詳細については、「Security Hub の料金」を参照してください。

トピック

製品統合の管理

の「統合」ページ AWS Management Console では、利用可能なすべての製品統合 AWS とサードパーティー製品統合にアクセスできます。 AWS Security Hub API には、統合を管理できるオペレーションも用意されています。

> **Note**
>
> 一部のリージョンでは統合を利用できない場合があります。現在のリージョンで統合がサポートされていない場合は、[Integration] (統合) ページに表示されません。

「the section called “中国 (北京) および中国 (寧夏) でサポートされている統合”」および「the section called “AWS GovCloud （米国東部) および AWS GovCloud （米国西部) でサポートされている統合”」も参照してください。

統合のリストの表示とフィルター処理 (コンソール)

[Integrations] (統合) ページから、統合のリストを表示およびフィルターできます。

統合のリストを表示するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. Security Hub ナビゲーションペインで、[Integrations] (統合) を選択します。

[Integrations] (統合) ページで、他の AWS のサービスとの統合が最初に一覧表示され、その後にサードパーティー製品との統合が一覧表示されます。

統合ごとに、[Integration] (統合) ページに以下の情報が表示されます。

- 会社名
- 製品名
- 統合の説明
- 統合が適用されるカテゴリ
- 統合を有効にする方法
- 統合の現在のステータス

以下のフィールドにテキストを入力してリストをフィルタリングできます。

- 会社名
- 製品名
- 統合の説明
- カテゴリ

製品統合に関する情報の表示 (Security Hub API、 AWS CLI)

製品統合に関する情報を表示するには、API コールまたは AWS Command Line Interfaceを使用します。すべての製品インテグレーションに関する情報、または有効にした製品インテグレーションに関する情報を表示できます。

利用可能なすべての製品統合に関する情報を表示するには (Security Hub API、 AWS CLI)

- Security Hub API - `DescribeProducts` オペレーションを使用します。返すべき特定の製品統合を特定するには、`ProductArn` パラメータを使用して、統合 ARN を指定します。
- AWS CLI - コマンドラインで `describe-products` コマンドを実行します。返すべき特定の製品統合を特定するには、統合 ARN を指定します。

```
aws securityhub describe-products --product-arn "<integrationARN>"
```

例

```
aws securityhub describe-products --product-arn "arn:aws:securityhub:us-
east-1::product/3coresec/3coresec"
```

ユーザーが有効にした製品統合に関する情報を表示するには (Security Hub API、 AWS CLI)

- Security Hub API - `ListEnabledProductsForImport` オペレーションを使用します。
- AWS CLI - コマンドラインで `list-enabled-products-for-import` コマンドを実行します。

```
aws securityhub list-enabled-products-for-import
```

統合の有効化

[Integration] (統合) ページで、統合を有効にするための手順が統合別に表示されます。

他のサービスとの統合のほとんどで AWS 、必要なステップは他のサービスを有効にすることだけです。統合情報には、サービスのホームページへのリンクが含まれています。他のサービスを有効にすると、Security Hub がサービスから結果を受信できるようにするリソースレベルの許可が自動的に作成されて適用されます。

サードパーティー製品統合の場合、 から統合を購入し AWS Marketplace、統合を設定する必要がある場合があります。統合情報には、それらのタスクを実行するためのリンクが含まれます。

で複数のバージョンの製品が利用可能な場合は AWS Marketplace、サブスクライブするバージョンを選択し、「サブスクライブ」に進みます。例えば、一部の製品では、標準バージョンと AWS GovCloud (US) バージョンが提供されています。

製品の統合を有効にすると、リソースポリシーがその製品サブスクリプションに自動的に添付されます。このリソースポリシーは、Security Hub がその製品から結果を受け取るために必要な許可を定義します。

統合先からの結果のフローの無効化と有効化 (コンソール)

[Integrations] (統合) ページで、結果を送信する統合の場合、[Status] (ステータス) 情報には、結果を現在受信しているかどうかが示されます。

結果の受け入れを停止するには、[Stop accepting findings] (結果の受け入れを停止) を選択します。

結果の受け入れを再開するには、[Accept findings] (結果の受け入れ) を選択します。

統合からの検出結果フローの無効化 (Security Hub API、 AWS CLI)

統合先からの結果のフローを無効にするには、API コールまたは AWS Command Line Interfaceを使用できます。

統合からの検出結果のフローを無効にするには (Security Hub API、 AWS CLI)

- Security Hub API - `DisableImportFindingsForProduct` オペレーションを使用します。無効にする統合先を特定するには、サブスクリプションの ARN が必要です。現在有効な統合先のサブスクリプション ARN を取得するには、`ListEnabledProductsForImport` オペレーションを使用します。
- AWS CLI - コマンドラインで `disable-import-findings-for-product` コマンドを実行します。

```
aws securityhub disable-import-findings-for-product --product-subscription-
arn <subscription ARN>
```

例

```
aws securityhub disable-import-findings-for-product --product-subscription-arn
 "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/
crowdstrike-falcon"
```

統合からの検出結果のフローの有効化 (Security Hub API、 AWS CLI)

統合先からの結果のフローを有効にするには、API コールまたは AWS Command Line Interfaceを使用します。

統合からの検出結果のフローを有効にするには (Security Hub API、 AWS CLI)

- Security Hub API - `EnableImportFindingsForProduct` オペレーションを使用します。Security Hub を有効にして、統合先から結果を受信するには、製品 ARN が必要です。利用可能な統合先の ARN を取得するには、`DescribeProducts` オペレーションを使用します。
- AWS CLI: コマンドラインで `enable-import-findings-for-product` コマンドを実行します。

  ```
  aws securityhub enable-import-findings-for-product --product-arn <integration ARN>
  ```

  例

  ```
  aws securityhub enable-import-findings-for product --product-arn
   "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
  ```

統合先からの結果の表示

結果を受信する統合先 ([Status] (ステータス) が [Accepting findings] (結果を受信する) になっている) の場合、結果のリストを表示するには、[See findings] (結果の表示) を選択します。

結果リストには、ワークフローステータスが `NEW` または `NOTIFIED` である、選択した統合先のアクティブな結果が表示されます。

クロスリージョン集約を有効にすると、集約リージョンでは、リストに、集約リージョンと、統合が有効にされているリンクされたリージョンの結果が含まれます。Security Hub では、クロスリージョン集約の設定に基づき統合が自動的に有効になることはありません。

他のリージョンでは、統合先の結果リストには、現在のリージョンの結果のみが含まれます。

クロスリージョン集約の設定方法については、クロスリージョン集約 を参照してください。

結果リストから、以下のアクションを実行できます。

- リストのフィルターとグループ化を変更する
- 個々の結果の詳細を表示する
- 結果のワークフローステータスを更新する
- カスタムアクションに結果を送信する

AWS のサービスAWS Security Hub との統合

AWS Security Hub は、他のいくつかの との統合をサポートしています AWS のサービス。

> **Note**
>
> 一部の統合は、一部の でのみ使用できます AWS リージョン。
> 特定のリージョンで統合がサポートされていない場合は、Security Hub コンソールの [統合] ページのリストに表示されません。
> 詳細については、「中国 (北京) および中国 (寧夏) でサポートされている統合」および「AWS GovCloud （米国東部) および AWS GovCloud （米国西部) でサポートされている統合」を参照してください。

以下に示されていない限り、Security Hub に結果を送信する AWS のサービス 統合は、Security Hub を有効にすると自動的に有効になります。Security Hub の検出結果を受け取る統合では、アクティベーションに追加の手順が必要になる場合があります。詳細については、各統合に関する情報を確認してください。

Security Hub と AWS のサービス統合の概要

以下は、Security Hub に結果を送信したり、Security Hub から結果を受け取ったりする AWS サービスの概要です。

統合 AWS サービス	[Direction] (方向)	
AWS Config	結果の送信	

統合 AWS サービス	[Direction] (方向)	
AWS Firewall Manager	結果の送信	
Amazon GuardDuty	結果の送信	
AWS Health	結果の送信	
AWS Identity and Access Management Access Analyzer	結果の送信	
Amazon Inspector	結果の送信	
AWS IoT Device Defender	結果の送信	
Amazon Macie	結果の送信	
AWS Systems Manager Patch Manager	結果の送信	
AWS Audit Manager	結果の受信	
AWS Chatbot	結果の受信	
Amazon Detective	結果の受信	
Amazon Security Lake	結果の受信	
AWS Systems Manager Explorer と OpsCenter	結果の受信と更新	
AWS Trusted Advisor	結果の受信	

AWS Security Hub に結果を送信する サービス

以下のサービスは、結果を Security Hub に送信することで Security Hub と AWS 統合します。Security Hub は、結果を AWS Security Finding 形式に変換します。

AWS Config（結果を送信）

AWS Config は、 AWS リソースの設定を評価、監査、評価できるサービスです。 は AWS 、リソース設定 AWS Config を継続的にモニタリングおよび記録し、記録された設定を目的の設定と照らし合わせて評価を自動化できます。

との統合を使用すると AWS Config、マネージドルールとカスタムルールの評価の結果 AWS Config を Security Hub の結果として確認できます。これらの結果は、他の Security Hub の結果と一緒に表示でき、セキュリティ体制を包括的に概観できます。

AWS Config は Amazon EventBridge を使用して AWS Config ルール評価を Security Hub に送信します。Security Hub は、このルール評価を AWS Security Finding 形式に従う結果に変換します。その後 Security Hub は、Amazon リソースネーム (ARN) や作成日など、影響を受けるリソースに関する詳細情報を取得することで、ベストエフォートベースで結果を強化します。 AWS Config ルール評価のリソースタグは Security Hub の検出結果に含まれません。

この統合に関する詳細は、以下のセクションを参照してください。

が Security Hub に結果 AWS Config を送信する方法

Security Hub のすべての結果で、ASFF と呼ばれる標準の JSON 形式が使用されます。ASFF には、検出結果のオリジン、影響を受けるリソース、および検出結果の現在のステータスに関する詳細が含まれます。 AWS Config は、マネージドルールとカスタムルールの評価を 経由で Security Hub に送信します EventBridge。Security Hub は、ルール評価を ASFF に従う結果に変換し、ベストエフォートベースで結果を強化します。

が Security Hub AWS Config に送信する検出結果のタイプ

統合がアクティブ化されると、 はすべての AWS Config マネージドルールとカスタムルールの評価を Security Hub AWS Config に送信します。セキュリティコントロールのチェックの実行に使用されるものなど、サービスにリンクされた AWS Config ルール の評価のみが除外されます。

Security Hub への AWS Config 結果の送信

統合がアクティブ化されると、Security Hub は から結果を受け取るために必要なアクセス許可を自動的に割り当てます AWS Config。Security Hub は、この統合をアクティブ化し、Amazon AWS Config 経由で から検出結果をインポートする安全な方法を提供する service-to-service レベルアクセス許可を使用します EventBridge。

結果が送信されるまでのレイテンシー

が新しい検出結果 AWS Config を作成すると、通常 5 分以内に Security Hub で検出結果を表示できます。

Security Hub が使用できない場合の再試行

AWS Config は、 を通じてベストエフォートベースで結果を Security Hub に送信します EventBridge。イベントが Security Hub に正常に配信されない場合、 EventBridge は最大 24 時間または 185 回のいずれか早い方まで配信を再試行します。

Security Hub での既存の AWS Config 検出結果の更新

AWS Config が Security Hub に結果を送信すると、同じ結果の更新を Security Hub に送信して、結果アクティビティの追加の観察結果を反映することができます。更新は `ComplianceChangeNotification` イベントについてのみ送信されます。コンプライアンスの変更が行われない場合、更新は Security Hub に送信されません。Security Hub では、結果は、最新の更新から 90 日後、または更新が行われない場合は作成日から 90 日後に削除されます。

関連付けられたリソースを削除 AWS Config しても、Security Hub は から送信された結果をアーカイブしません。

AWS Config 結果が存在するリージョン

AWS Config 検出結果はリージョンベースで発生します。 AWS Config は検出結果が発生したのと同じリージョンの Security Hub に検出結果を送信します。

Security Hub で AWS Config の結果の表示

AWS Config 検出結果を表示するには、Security Hub ナビゲーションペインから検出結果を選択します。検出結果をフィルタリングして AWS Config 検出結果のみを表示するには、検索バーのドロップダウンで製品名を選択します。[Config] (設定) をクリックし、[Apply] (適用) を選択します。

Security Hub で AWS Config の検出結果名の解釈

Security Hub は、 AWS Config ルール評価を . AWS Config rule 評価に従う結果に変換しますAWS Security Finding 形式 (ASFF)。ASFF とは異なるイベントパターンを使用します。次の表は、Security Hub に表示される AWS Config ルール評価フィールドと ASFF をマッピングしたものです。

Config ルール評価の検索タイプ	ASFF 結果タイプ	ハードコードされた値
詳細。awsAccountId	AwsAccountId	
詳細newEvaluationResult。resultRecordedTime	CreatedAt	
詳細newEvaluationResult。resultRecordedTime	UpdatedAt	
	ProductArn	"arn:<partition>:securityhub:<region>::product/aws/config"
	ProductName	"Config"
	CompanyName	"AWS"
	リージョン	"eu-central-1"
configRuleArn	GeneratorId, ProductFields	
detail.ConfigRuleARN/検索/ハッシュ	ID	
詳細。configRuleName	タイトル、 ProductFields	
詳細。configRuleName	説明	「この結果は、構成ルール `${detail.ConfigRuleName}` のリソースコンプライアンスの変更に対して作成されます。」
構成項目「ARN」または Security Hub の computed ARN	Resources[i].id	
detail.resourceType	Resources[i].Type	"AwsS3Bucket"

Config ルール評価の検索タイプ	ASFF 結果タイプ	ハードコードされた値
	Resources[i].Partition	"aws"
	Resources[i].Region	"eu-central-1"
構成項目「構成」	Resources[i].Details	
	SchemaVersion	「2018-10-08」
	Severity.Label	以下の「重要度ラベルの解釈」を参照してください。
	Types	["Software and Configuration Checks"]
detail.newEvaluationResult.complianceType	Compliance.Status	「FAILED」、「NOT_AVAILABLE」、「PASSED」、または「WARNING」
	Workflow.Status	Compliance.Status が「PASSED」で AWS Config 結果が生成された場合、または Compliance.Status が「FAILED」から「PASSED」に変わった場合は、「解決済み」です。それ以外の場合、Workflow.Status は「NEW」になります。この値は BatchUpdateFindings API オペレーションで変更できます。

重要度ラベルの解釈

AWS Config ルール評価のすべての結果には、ASFF のデフォルトの重要度ラベル MEDIUM があります。結果の重要度ラベルは、`BatchUpdateFindings` API オペレーションで更新できます。

からの一般的な検出結果 AWS Config

Security Hub は、 AWS Config ルール評価を ASFF に従う結果に変換します。ASFF AWS Config のからの一般的な検出結果の例を次に示します。

> **Note**
>
> 説明が 1,024 文字を超えると 1,024 文字まで切り捨てられ、末尾に「(truncated)」(切り捨て) と表示されます。


```
{
 "SchemaVersion": "2018-10-08",
 "Id": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/45g070df80cb50b68fa6a43594kc6fda1e517932",
 "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/config",
 "ProductName": "Config",
 "CompanyName": "AWS",
 "Region": "eu-central-1",
 "GeneratorId": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-
mburzq",
 "AwsAccountId": "123456789012",
 "Types": [
  "Software and Configuration Checks"
 ],
 "CreatedAt": "2022-04-15T05:00:37.181Z",
 "UpdatedAt": "2022-04-19T21:20:15.056Z",
 "Severity": {
  "Label": "MEDIUM",
  "Normalized": 40
 },
 "Title": "s3-bucket-level-public-access-prohibited-config-integration-demo",
 "Description": "This finding is created for a resource compliance change for config
 rule: s3-bucket-level-public-access-prohibited-config-integration-demo",
 "ProductFields": {
  "aws/securityhub/ProductName": "Config",
  "aws/securityhub/CompanyName": "AWS",
  "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
config/arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/46f070df80cd50b68fa6a43594dc5fda1e517902",
  "aws/config/ConfigRuleArn": "arn:aws:config:eu-central-1:123456789012:config-rule/
config-rule-mburzq",
```

```
  "aws/config/ConfigRuleName": "s3-bucket-level-public-access-prohibited-config-
integration-demo",
  "aws/config/ConfigComplianceType": "NON_COMPLIANT"
 },
 "Resources": [{
  "Type": "AwsS3Bucket",
  "Id": "arn:aws:s3:::config-integration-demo-bucket",
  "Partition": "aws",
  "Region": "eu-central-1",
  "Details": {
   "AwsS3Bucket": {
    "OwnerId": "4edbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
    "CreatedAt": "2022-04-15T04:32:53.000Z"
   }
  }
 }],
 "Compliance": {
  "Status": "FAILED"
 },
 "WorkflowState": "NEW",
 "Workflow": {
  "Status": "NEW"
 },
 "RecordState": "ACTIVE",
 "FindingProviderFields": {
  "Severity": {
   "Label": "MEDIUM"
  },
  "Types": [
   "Software and Configuration Checks"
  ]
 }
}
```


統合の有効化と構成

Security Hub を有効にすると、この統合は自動的にアクティブ化されます。 AWS Config すぐに Security Hub に結果の送信が開始されます。

検出結果の Security Hub への公開の停止

Security Hub への結果送信を停止するには、Security Hub コンソール、Security Hub API、または AWS CLIを使用します。

「統合先からの結果のフローの無効化と有効化 (コンソール)」または「統合からの検出結果フローの無効化 (Security Hub API、 AWS CLI) 」を参照してください。

AWS Firewall Manager （結果を送信）

Firewall Manager は、リソースのウェブアプリケーションファイアウォール (WAF) ポリシーまたはウェブアクセスコントロールリスト (ウェブ ACL) ルールが非準拠である場合に、結果を Security Hub に送信します。Firewall Manager は、 AWS Shield Advanced がリソースを保護していない場合、または攻撃が特定された場合にも結果を送信します。

Security Hub を有効にすると、この統合は自動的に有効になります。Firewall Manager は、検出結果を Security Hub に送信します。

統合の詳細については、Security Hub コンソールの [Integrations] (統合) ページを参照してください。

Firewall Manager の詳細については、「AWS WAF 開発者ガイド」を参照してください。

Amazon GuardDuty （結果を送信）

GuardDuty は、生成したすべての結果を Security Hub に送信します。

からの新しい検出 GuardDuty 結果は、5 分以内に Security Hub に送信されます。検出結果の更新は、Amazon の「更新された検出結果 GuardDuty 」設定に基づいて送信 EventBridge されます。

GuardDuty 設定ページを使用して GuardDuty サンプル検出結果を生成すると、Security Hub はサンプル検出結果を受け取り、検出結果タイプのプレフィックスを省略[Sample]します。例えば、のサンプル検出結果タイプ GuardDuty `[SAMPLE] Recon:IAMUser/ResourcePermissions`は Security Hub `Recon:IAMUser/ResourcePermissions`で として表示されます。

Security Hub を有効にすると、この統合は自動的に有効になります。 GuardDuty はすぐに Security Hub への検出結果の送信を開始します。

GuardDuty 統合の詳細については、「Amazon ユーザーガイド」のAWS 「Security Hub との統合」を参照してください。 GuardDuty

AWS Health （結果を送信）

AWS Health は、リソースのパフォーマンスと AWS サービスとアカウントの可用性を継続的に可視化します。 AWS Health イベントを使用することで、サービスおよびリソースの変更が、 AWSで実行されるアプリケーションにどのような影響を及ぼすか確認することができます。

との統合 AWS Health では、 は使用されませんBatchImportFindings。代わりに、 service-to-service イベントメッセージング AWS Health を使用して結果を Security Hub に送信します。

統合の詳細については、以下のセクションを参照してください。

が Security Hub に結果 AWS Health を送信する方法

Security Hub では、セキュリティの問題が調査結果として追跡されます。検出結果の中には、他の AWS のサービスやサードパーティーパートナーによって検出された問題に由来するものもあります。Security Hub には、セキュリティの問題を検出し、検出結果を生成するために使用する一連のルールもあります。

Security Hub には、これらすべてのソースからの結果を管理するためのツールが用意されています。結果の一覧を表示およびフィルタリングして、結果の詳細を表示できます。「結果の詳細と履歴の管理と確認」を参照してください。結果の調査状況を追跡することもできます。「の検出結果に対するアクションの実行 AWS Security Hub」を参照してください。

Security Hub のすべての結果で、AWS Security Finding 形式 (ASFF) と呼ばれる標準の JSON 形式が使用されます。ASFF には、問題のソース、影響を受けるリソース、および結果の現在の状態に関する詳細が含まれます。

AWS Health は、結果を Security Hub に送信する AWS サービスの 1 つです。

が Security Hub AWS Health に送信する検出結果のタイプ

統合を有効にすると、 は生成するすべてのセキュリティ関連の検出結果を Security Hub AWS Health に送信します。結果は AWS Security Finding 形式 (ASFF) を使用して Security Hub に送信されます。セキュリティ関連の調査結果は、次のように定義されています。

- AWS セキュリティサービスに関連する検出結果
- AWS Health typeCode 内の `security`、`abuse`、または という単語`certificate`を含む結果
- AWS Health サービスが `risk`または である検出結果 `abuse`

Security Hub への AWS Health 結果の送信

からの検出結果を受け入れることを選択すると AWS Health、Security Hub は からの検出結果を受信するために必要なアクセス許可を自動的に割り当てます AWS Health。Security Hub は、この統合を有効にし、 EventBridge ユーザーに代わって Amazon AWS Health 経由で から検出結果をインポートする安全で簡単な方法を提供する service-to-service レベルアクセス許可を使用します。Accept

Findings を選択すると、Security Hub に からの結果を使用するアクセス許可が付与されます AWS Health。

結果が送信されるまでのレイテンシー

が新しい検出結果 AWS Health を作成すると、通常 5 分以内に Security Hub に送信されます。

Security Hub が使用できない場合の再試行

AWS Health は、 を通じてベストエフォートベースで結果を Security Hub に送信します EventBridge。イベントが Security Hub に正常に配信されない場合、 EventBridge はイベントの送信を 24 時間再試行します。

Security Hub の既存の結果を更新する

AWS Health が Security Hub に結果を送信すると、同じ結果に更新を送信して、検出結果アクティビティの追加の観察結果を Security Hub に反映できます。

結果が存在するリージョン

グローバルイベントの場合、 AWS Health は、us-east-1 (AWS パーティション)、cn-northwest-1 (中国パーティション)、および gov-us-west-1 (GovCloud パーティション) の Security Hub に結果を送信します。 は、イベントが発生するのと同じリージョンの Security Hub にリージョン固有のイベント AWS Health を送信します。

Security Hub で AWS Health の結果の表示

Security Hub で AWS Health 検出結果を表示するには、ナビゲーションパネルから検出結果を選択します。検出結果をフィルタリングして AWS Health 検出結果のみを表示するには、製品名フィールドからヘルスを選択します。

Security Hub で AWS Health の検出結果名の解釈

AWS Health は、 を使用して検出結果を Security Hub に送信しますAWS Security Finding 形式 (ASFF)。 AWS Health 検出では、Security Hub ASFF 形式とは異なるイベントパターンが使用されます。以下の表は、Security Hub に表示される ASFF に対応するすべての AWS Health 検出結果フィールドの詳細を示しています。

Health 結果タイプ	ASFF 結果タイプ	ハードコードされた値
アカウント	AwsAccountId	

Health 結果タイプ	ASFF 結果タイプ	ハードコードされた値
detail.StartTime	CreatedAt	
detail.eventDescription.latestDescription	説明	
詳細。eventTypeCode	GeneratorId	
detail.eventArn (including account) + hash of detail.startTime	ID	
「arn: aws: securityhub:<region>:: product/aws/health」	ProductArn	
アカウントまたは resourceId	Resources[i].id	
	Resources[i].Type	「その他」
	SchemaVersion	「2018-10-08」
	Severity.Label	以下の「重要度ラベルの解釈」を参照してください。
AWS Health 「-」の詳細。eventTypeCode	タイトル	
-	Types	["Software and Configuration Checks"]
event.time	UpdatedAt	
Health コンソール上のイベントの URL	SourceUrl	

重要度ラベルの解釈

ASFF 結果の重要度ラベルは、次のロジックを使用して決定されます。

- 次の場合、重要度は [CRITICAL]:
  - AWS Health 検出結果の `service`フィールドには 値があります `Risk`
  - AWS Health 結果の `typeCode`フィールドには 値があります `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`
  - AWS Health 結果の `typeCode`フィールドには 値があります。 `AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK`
  - AWS Health 結果の `typeCode`フィールドには 値があります。 `AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES`

  次の場合、重要度は [HIGH]:
  - AWS Health 検出結果の `service`フィールドには 値があります `Abuse`
  - AWS Health 検出結果の `typeCode`フィールドには 値が含まれます。 `SECURITY_NOTIFICATION`
  - AWS Health 検出結果の `typeCode`フィールドには 値が含まれます。 `ABUSE_DETECTION`

  次の場合、重要度は [MEDIUM]:
  - 結果の `service` フィールドが次のいずれかである。`ACM`、`ARTIFACT`、`AUDITMANAGER`、`BACKUP`、`CLOUDENDURE`、`CLOUDHSM`、`CLOUDTRAIL`、`CLOU`
  - AWS Health 結果の [typeCode] フィールドに値 `CERTIFICATE` が含まれている
  - AWS Health 結果の [typeCode] フィールドに値 `END_OF_SUPPORT` が含まれている

からの一般的な検出結果 AWS Health

AWS Health は、 を使用して結果を Security Hub に送信しますAWS Security Finding 形式 (ASFF)。以下は、 からの一般的な検出結果の例です AWS Health。

> **Note**
>
> 説明が 1,024 文字を超えると 1,024 文字まで切り捨てられ、末尾に (truncated) (切り捨て) と表示されます。

```
{
            "SchemaVersion": "2018-10-08",
            "Id": "arn:aws:health:us-east-1:123456789012:event/SES/
AWS_SES_CMF_PENDING_TO_SUCCESS/
```

```
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-
b533-78e29f49de96/101F7FBAEFC663977DA09CFF56A29236602834D2D361E6A8CA5140BFB3A69B30",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/health",
            "GeneratorId": "AWS_SES_CMF_PENDING_TO_SUCCESS",
            "AwsAccountId": "123456789012",
            "Types": [
                "Software and Configuration Checks"
            ],
            "CreatedAt": "2022-01-07T16:34:04.000Z",
            "UpdatedAt": "2022-01-07T19:17:43.000Z",
            "Severity": {
                "Label": "MEDIUM",
                "Normalized": 40
            },
            "Title": "AWS Health - AWS_SES_CMF_PENDING_TO_SUCCESS",
            "Description": "Congratulations! Amazon SES has successfully detected the
 MX record required to use 4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com as a custom MAIL FROM domain for verified identity cmf.pinpoint.sysmon-
iad.adzel.com in AWS Region US East (N. Virginia).\\n\\nYou can now use this MAIL
 FROM domain with cmf.pinpoint.sysmon-iad.adzel.com and any other verified identity
 that is configured to use it. For information about how to configure a verified
 identity to use a custom MAIL FROM domain, see http://docs.aws.amazon.com/ses/latest/
DeveloperGuide/mail-from-set.html .\\n\\nPlease note that this email only applies to
 AWS Region US East (N. Virginia).",
            "SourceUrl": "https://phd.aws.amazon.com/phd/home#/event-log?
eventID=arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
            "ProductFields": {
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
aws/health/arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
                "aws/securityhub/ProductName": "Health",
                "aws/securityhub/CompanyName": "AWS"
            },
            "Resources": [
                {
                    "Type": "Other",
                    "Id": "4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com"
                }
            ],
            "WorkflowState": "NEW",
            "Workflow": {
                "Status": "NEW"
```

```
            },
            "RecordState": "ACTIVE",
            "FindingProviderFields": {
                "Severity": {
                    "Label": "MEDIUM"
                },
                "Types": [
                    "Software and Configuration Checks"
                ]
            }
        }
    ]
}
```

統合の有効化と構成

Security Hub を有効にすると、この統合は自動的に有効になります。 AWS Health はすぐに Security Hub に結果を送信し始めます。

検出結果の Security Hub への公開の停止

Security Hub への結果の送信を停止するには、Security Hub コンソール、Security Hub API、または を使用できます AWS CLI。

「統合先からの結果のフローの無効化と有効化 (コンソール)」または「統合からの検出結果フローの無効化 (Security Hub API、 AWS CLI) 」を参照してください。

AWS Identity and Access Management Access Analyzer （結果を送信）

IAM Access Analyzer では、すべての結果が Security Hub に送信されます。

IAM Access Analyzer は、論理ベースの推論を使用して、アカウントでサポートされるリソースに適用されたリソースベースのポリシーを分析します。IAM Access Analyzer は、外部プリンシパルがアカウント内のリソースにアクセスすることを許可するポリシーステートメントを検出すると、検出結果を生成します。

IAM Access Analyzer では、組織に適用されるアナライザーの検出結果を確認できるのは管理者アカウントだけです。組織アナライザーの場合、`AwsAccountId` ASFF フィールドには管理者アカウント ID が反映されます。`ProductFields` 下の `ResourceOwnerAccount`フィールドには、検出結果が発見されたアカウントが表示されます。アカウントごとにアナライザーを個別に有効にすると、Security Hub は複数の検出結果を生成します。1 つは管理者アカウント ID を識別し、もう 1 つはリソースアカウント ID を識別します。

詳細については、「IAM ユーザーガイド」の「AWS Security Hub との統合」を参照してください。

Amazon Inspector (結果の送信)

Amazon Inspector は、 AWS のワークロードにおける脆弱性を継続的にスキャンする脆弱性管理サービスです。Amazon Inspector は、Amazon Elastic Container Registry に存在する EC2 インスタンスとコンテナイメージを自動的に検出してスキャンします。このスキャンでは、ソフトウェアの脆弱性と意図しないネットワークへのエクスポージャーがないかチェックします。

Security Hub を有効にすると、この統合は自動的に有効になります。Amazon Inspector から生成されたすべての検出結果が Security Hub に直ちに送信開始されます。

統合の詳細については、Amazon Inspector ユーザーガイド」のAWS 「Security Hub との統合」を参照してください。

Security Hub は、Amazon Inspector Classic から結果を受信することもできます。Amazon Inspector Classic は、サポートされているすべてのルールパッケージの評価実行によって生成された Security Hub に、結果を送信します。

統合の詳細については、Amazon Inspector Classic ユーザーガイド」のAWS 「Security Hub との統合」を参照してください。

Amazon Inspector と Amazon Inspector Classic の結果では、同じ製品の ARN が使用されます。Amazon Inspector の調査結果には、`ProductFields` に次のエントリがあります。

```
"aws/inspector/ProductVersion": "2",
```

AWS IoT Device Defender （ 結果を送信 ）

AWS IoT Device Defender は、IoT デバイスの設定を監査し、接続されたデバイスをモニタリングして異常な動作を検出し、セキュリティリスクを軽減するセキュリティサービスです。

AWS IoT Device Defender と Security Hub の両方を有効にしたら、Security Hub コンソール の統合ページにアクセスし、監査、検出、またはその両方の結果を受け入れるを選択します。 AWS IoT Device Defender 監査と検出は、すべての結果を Security Hub に送信し始めます。

AWS IoT Device Defender Audit は、特定の監査チェックタイプと監査タスクの一般的な情報を含むチェック概要を Security Hub に送信します。 AWS IoT Device Defender Detect は、機械学習 (ML)、統計、静的動作に関する違反の検出結果を Security Hub に送信します。Audit も、検出結果の更新を Security Hub に送信します。

この統合の詳細については、「 AWS IoT デベロッパーガイド」のAWS 「Security Hub との統合」を参照してください。

Amazon Macie (結果の送信)

Macie からの結果では、組織が Amazon S3 に保存しているデータに、ポリシー違反の可能性があること、または個人を特定できる情報 (PII) などの機密データが存在することを示すことがあります。

Security Hub を有効にすると、Macie はポリシー検出結果を自動的に Security Hub に送信し始めます。機密データの調査結果も Security Hub に送信するように統合を構成できます。

Security Hub では、ポリシーまたは機密データの結果のタイプが、ASFF と互換性のある値に変更されます。例えば、Macie での `Policy:IAMUser/S3BucketPublic` 結果タイプは、Security Hub では `Effects/Data Exposure/Policy:IAMUser-S3BucketPublic` と表示されます。

Macie は、生成されたサンプル結果を Security Hub に送信します。結果のサンプルでは、影響を受けるリソースの名前は `macie-sample-finding-bucket` であり、`Sample` フィールドの値は `true` です。

詳細については、「Amazon Macie ユーザーガイド」の「Amazon Macie と AWS Security Hub との統合」を参照してください。

AWS Systems Manager Patch Manager (結果を送信)

AWS Systems Manager お客様のフリート内のインスタンスがパッチコンプライアンス標準に準拠していない場合、Patch Manager は結果を Security Hub に送信します。

Patch Manager は、セキュリティ関連のアップデートと他のタイプのアップデートの両方でマネージドインスタンスにパッチを適用するプロセスを自動化します。

Security Hub を有効にすると、この統合は自動的に有効になります。Systems Manager Patch Manager は、検出結果を Security Hub に直ちに送信します。

Patch Manager の使用の詳細については、「AWS Systems Manager ユーザーガイド」の「AWS Systems Manager Patch Manager」を参照してください。

AWS Security Hub から結果を受け取る のサービス

以下の AWS サービスは Security Hub と統合されており、Security Hub から結果を受け取ります。特に明記されている場合、統合されたサービスは結果を更新する場合もあります。この場合、統合されたサービスで行った更新が見つかると、Security Hub にも反映されます。

AWS Audit Manager（検出結果を受信）

AWS Audit Manager は Security Hub から結果を受け取ります。これらの結果は、Audit Manager ユーザーが監査の準備をするうえで役立ちます。

Audit Manager の詳細については、「Audit AWS Manager ユーザーガイド」を参照してください。AWSAWS Audit Managerでサポートされている Security Hub のチェックでは、Security Hub が結果を Audit Manager に送信するコントロールの一覧が表示されます。

AWS Chatbot（検出結果を受信）

AWS Chatbot は、Slack チャネルと Amazon Chime チャットルームの AWS リソースをモニタリングして操作するのに役立つインタラクティブなエージェントです。

AWS Chatbot は Security Hub から結果を受け取ります。

Security Hub と AWS Chatbot の統合の詳細については、「 AWS Chatbot 管理者ガイド」の「Security Hub の統合の概要」を参照してください。

Amazon Detective (結果の受信)

Detective は、 AWS リソースからログデータを自動的に収集し、機械学習、統計分析、グラフ理論を使用して、セキュリティ調査を迅速かつ効率的に視覚化して実行できるようにします。

Security Hub と Detective の統合により、Security Hub の Amazon GuardDuty の検出結果から Detective にピボットできます。その後、Detective のツールと視覚化を使用して調査することができます。統合には、Security Hub または Detective に追加の設定をする必要はありません。

他の から受け取った検出結果の場合 AWS のサービス、Security Hub コンソールの検出結果の詳細パネルには、Detective サブセクションに調査が含まれます。そのサブセクションには Detective へのリンクが含まれており、調査結果によって特定されたセキュリティ問題をさらに調査できます。Security Hub の調査結果に基づいて Detective で行動グラフを作成して、より効果的な調査を行うこともできます。詳細については、「Amazon Detective 管理ガイド」の「AWS セキュリティ結果」を参照してください。

クロスリージョン集約を有効にし、集約リージョンから方向を転換した場合、検出元のリージョンで Detective が開きます。

リンクが機能しない場合のトラブルシューティングのアドバイスについては、「ピボットのトラブルシューティング」を参照してください。

Amazon Security Lake (結果の受信)

Security Lake は、完全マネージド型のセキュリティデータレイクサービスです。Security Lake を使用すると、クラウド、オンプレミス、カスタムソースのセキュリティデータを、アカウントに保存されているデータレイクに自動的に一元化できます。サブスクライバーは、Security Lake のデータを調査や分析のユースケースに使用できます。

この統合をアクティブ化するには、両方のサービスを有効にし、Security Lake コンソール、Security Lake API、または でソースとして Security Hub を追加する必要があります AWS CLI。これらの手順を完了すると、Security Hub はすべての検出結果を Security Lake に送信し始めます。

Security Lake は、Security Hub の検出結果を自動的に正規化し、Open Cybersecurity Schema Framework (OCSF) と呼ばれる標準化されたオープンソーススキーマに変換します。Security Lake では、Security Hub の検出結果を使用するサブスクライバーを 1 人以上追加できます。

Security Hub をソースとして追加する手順やサブスクライバーを作成する手順など、この統合の詳細については、「Amazon Security Lake ユーザーガイド」のAWS 「Security Hub との統合」を参照してください。

AWS Systems Manager Explorer と OpsCenter （ 結果の受信と更新 ）

AWS Systems Manager Security Hub から検出結果を探索して OpsCenter 受け取り、それらの検出結果を Security Hub で更新します。

Explorer は、カスタマイズ可能なダッシュボードを提供し、ユーザーの運用の健全性と AWS 環境のパフォーマンスに関する主要なインサイトと分析を提供します。

OpsCenter は、運用作業項目を表示、調査、解決するための一元的な場所を提供します。

Explorer と の詳細については OpsCenter、「 ユーザーガイド」の「オペレーション管理AWS Systems Manager 」を参照してください。

AWS Trusted Advisor （ 検出結果を受信 ）

Trusted Advisor は、数十万の AWS 顧客にサービスを提供することから学んだベストプラクティスを活用します。 Trusted Advisor はお客様の AWS 環境を検査し、コスト削減、システムの可用性とパフォーマンスの向上、セキュリティギャップの解消に役立つ機会があればレコメンデーションを行います。

Trusted Advisor と Security Hub の両方を有効にすると、統合は自動的に更新されます。

Security Hub は、 AWS 基本的なセキュリティのベストプラクティスチェックの結果を に送信します Trusted Advisor。

Security Hub と の統合の詳細については Trusted Advisor、 AWS サポートユーザーガイドの「 での AWS Security Hub コントロールの表示 AWS Trusted Advisor」を参照してください。

利用可能なサードパーティーパートナー製品の統合

AWS Security Hub は、複数のサードパーティーパートナー製品と統合されています。統合は、次のいずれかのアクションを実行します。

- 生成された結果を Security Hub に送信します。
- Security Hub から結果を受信します。
- Security Hub の結果を更新します。

Security Hub に結果を送信する統合には、Amazon リソースネーム (ARN) があります。

> **Note**
>
> 一部の統合は、一部の でのみ使用できます AWS リージョン。
> Security Hub コンソールの [Integrations] (統合) ページには、現在のリージョンでサポートされているすべての統合が一覧表示されます。
> 詳細については、「中国 (北京) および中国 (寧夏) でサポートされている統合」および「AWS GovCloud （米国東部) および AWS GovCloud （米国西部) でサポートされている統合」を参照してください。

セキュリティソリューションをお持ちで、Security Hub パートナーになることにご関心がある場合は、<securityhub-partners@amazon.com> までご連絡ください。詳細については、「AWS Security Hub パートナー統合ガイド」を参照してください。

サードパーティーの Security Hub との統合の概要

以下は、Security Hub に結果を送信するまたは Security Hub から結果を受信するサードパーティーパートナーの統合の概要です。

Integration	[Direction] (方向)	ARN (該当する場合)
3CORESec – 3CORESec NTA	結果の送信	arn:aws:securityhub: <REGION>::product/3coresec/3coresec
Alert Logic – SIEMless Threat Management	結果の送信	arn:aws:securityhub: <REGION>:733251395267:product/alertlogic/althreatmanagement
Aqua Security – Aqua Cloud Native Security Platform	結果の送信	arn:aws:securityhub: <REGION>::product/aquasecurity/aquasecurity
Aqua Security – Kube-bench	結果の送信	arn:aws:securityhub: <REGION>::product/aqua-security/kube-bench
Armor – Armor Anywhere	結果の送信	arn:aws:securityhub: <REGION>:679703615338:product/armordefense/armoranywhere
AttackIQ – AttackIQ	結果の送信	arn:aws:securityhub: <REGION>::product/attackiq/attackiq-platform
Barracuda Networks – Cloud Security Guardian	結果の送信	arn:aws:securityhub: <REGION>:151784055945:product/barra

Integration	[Direction] (方向)	ARN (該当する場合)
		cuda/cloudsecurity guardian
BigID – BigID Enterprise	結果の送信	arn:aws:securityhub: *<REGION>*::product/bigid/bigid-enterprise
Blue Hexagon – Blue Hexagon forAWS	結果の送信	arn:aws:securityhub: *<REGION>*::product/blue-hexagon/blue-hexagon-for-aws
Capitis Solutions – C2VS	結果の送信	arn:aws:securityhub: *<REGION>*::product/capitis/c2vs
Check Point – CloudGuard IaaS	結果の送信	arn:aws:securityhub: *<REGION>*:758245563457:product/checkpoint/cloudguard-iaas
Check Point – CloudGuard Posture Management	結果の送信	arn:aws:securityhub: *<REGION>*:634729597623:product/checkpoint/dome9-arc
Claroty – xDome	結果の送信	arn:aws:securityhub: *<REGION>*::product/claroty/xdome

Integration	[Direction] (方向)	ARN (該当する場合)
Cloud Storage Security – Antivirus for Amazon S3	結果の送信	arn:aws:securityhub: <REGION>::product/cloud-storage-security/antivirus-for-amazon-s3
Contrast Security	結果の送信	arn:aws:securityhub: <REGION>::product/contrast-security/security-assess
CrowdStrike – CrowdStrike Falcon	結果の送信	arn:aws:securityhub: <REGION>:517716713836:product/crowdstrike/crowdstrike-falcon
CyberArk – Privileged Threat Analytics	結果の送信	arn:aws:securityhub: <REGION>:749430749651:product/cyberark/cyberark-pta
Data Theorem – Data Theorem	結果の送信	arn:aws:securityhub: <REGION>::product/data-theorem/api-cloud-web-secure
Drata	結果の送信	arn:aws:securityhub: <REGION>::product/drata/drata-integration

Integration	[Direction] (方向)	ARN (該当する場合)
Forcepoint – Forcepoint CASB	結果の送信	arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-casb
Forcepoint – Forcepoint Cloud Security Gateway	結果の送信	arn:aws:securityhub: *<REGION>*::product/forcepoint/forcepoint-cloud-security-gateway
Forcepoint – Forcepoint DLP	結果の送信	arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-dlp
Forcepoint – Forcepoint NGFW	結果の送信	arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-ngfw
Fugue – Fugue	結果の送信	arn:aws:securityhub: *<REGION>*::product/fugue/fugue
Guardicore – Centra 4.0	結果の送信	arn:aws:securityhub: *<REGION>*::product/guardicore/guardicore

Integration	[Direction] (方向)	ARN (該当する場合)
HackerOne – Vulnerability Intelligence	結果の送信	arn:aws:securityhub: *<REGION>*::product/hackerone/vulnerability-intelligence
JFrog – Xray	結果の送信	arn:aws:securityhub: *<REGION>*::product/jfrog/jfrog-xray
Juniper Networks – vSRX Next Generation Firewall	結果の送信	arn:aws:securityhub: *<REGION>*::product/juniper-networks/vsrx-next-generation-firewall
k9 Security – Access Analyzer	結果の送信	arn:aws:securityhub: *<REGION>*::product/k9-security/access-analyzer
Lacework – Lacework	結果の送信	arn:aws:securityhub: *<REGION>*::product/lacework/lacework
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	結果の送信	arn:aws:securityhub: *<REGION>*::product/mcafee-skyhigh/mcafee-mvision-cloud-aws
NETSCOUT – NETSCOUT Cyber Investigator	結果の送信	arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator

Integration	[Direction] (方向)	ARN (該当する場合)
Palo Alto Networks – Prisma Cloud Compute	結果の送信	arn:aws:securityhub: *<REGION>*:496947949261:product/twistlock/twistlock-enterprise
Palo Alto Networks – Prisma Cloud Enterprise	結果の送信	arn:aws:securityhub: *<REGION>*:188619942792:product/paloaltonetworks/redlock
Plerion – Cloud Security Platform	結果の送信	arn:aws:securityhub: *<REGION>*::product/plerion/cloud-security-platform
Prowler – Prowler	結果の送信	arn:aws:securityhub: *<REGION>*::product/prowler/prowler
Qualys – Vulnerability Management	結果の送信	arn:aws:securityhub: *<REGION>*:805950163170:product/qualys/qualys-vm
Rapid7 – InsightVM	結果の送信	arn:aws:securityhub: *<REGION>*:336818582268:product/rapid7/insightvm
SecureCloudDB – SecureCloudDB	結果の送信	arn:aws:securityhub: *<REGION>*::product/securecloudddb/securecloudddb

Integration	[Direction] (方向)	ARN (該当する場合)
SentinelOne – SentinelOne	結果の送信	arn:aws:securityhub: *<REGION>*::product/sentinelone/endpoint-protection
Snyk	結果の送信	arn:aws:securityhub: *<region>*::product/snyk/snyk
Sonrai Security – Sonrai Dig	結果の送信	arn:aws:securityhub: *<REGION>*::product/sonrai-security/sonrai-dig
Sophos – Server Protection	結果の送信	arn:aws:securityhub: *<REGION>*:064897671886:product/sophos/sophos-server-protection
StackRox – StackRox Kubernetes Security	結果の送信	arn:aws:securityhub: *<REGION>*::product/stackrox/kubernetes-security
Sumo Logic – Machine Data Analytics	結果の送信	arn:aws:securityhub: *<REGION>*:956882708938:product/sumologicinc/sumologic-mda
Symantec – Cloud Workload Protection	結果の送信	arn:aws:securityhub: *<REGION>*:754237914691:product/symantec-corp/symantec-cwp

Integration	[Direction] (方向)	ARN (該当する場合)
Tenable – Tenable.io	結果の送信	arn:aws:securityhub: *<REGION>*:422820575223:product/tenable/tenable-io
Trend Micro – Cloud One	結果の送信	arn:aws:securityhub: *<REGION>*::product/trend-micro/cloud-one
Vectra – Cognito Detect	結果の送信	arn:aws:securityhub: *<REGION>*:978576646331:product/vectra-ai/cognito-detect
Wiz	結果の送信	arn:aws:securityhub: *<REGION>*::product/wiz-security/wiz-security
Atlassian - Jira Service Management	結果の受信と更新	該当しない
Atlassian - Jira Service Management Cloud	結果の受信と更新	該当しない
Atlassian – Opsgenie	結果の受信	該当しない
Fortinet – FortiCNP	結果の受信	該当しない
IBM – QRadar	結果の受信	該当しない
Logz.io Cloud SIEM	結果の受信	該当しない
MetricStream	結果の受信	該当しない

Integration	[Direction] (方向)	ARN (該当する場合)
MicroFocus – MicroFocus Arcsight	結果の受信	該当しない
New Relic Vulnerability Management	結果の受信	該当しない
PagerDuty – PagerDuty	結果の受信	該当しない
Palo Alto Networks – Cortex XSOAR	結果の受信	該当しない
Palo Alto Networks – VM-Series	結果の受信	該当しない
Rackspace Technology – Cloud Native Security	結果の受信	該当しない
Rapid7 – InsightConnect	結果の受信	該当しない
RSA – RSA Archer	結果の受信	該当しない
ServiceNow – ITSM	結果の受信と更新	該当しない
Slack – Slack	結果の受信	該当しない
Splunk – Splunk Enterprise	結果の受信	該当しない
Splunk – Splunk Phantom	結果の受信	該当しない
ThreatModeler	結果の受信	該当しない
Trellix – Trellix Helix	結果の受信	該当しない
Caveonix – Caveonix Cloud	結果の送受信	`arn:aws:securityhub: <REGION>::product/caveonix/caveonix-cloud`

Integration	[Direction] (方向)	ARN (該当する場合)
Cloud Custodian – Cloud Custodian	結果の送受信	arn:aws:securityhub: *<REGION>*::product/cloud-custodian/cloud-custodian
DisruptOps, Inc. – DisruptOPS	結果の送受信	arn:aws:securityhub: *<REGION>*::product/disruptops-inc/disruptops
Kion	結果の送受信	arn:aws:securityhub: *<REGION>*::product/cloudtamerio/cloudtamerio
Turbot – Turbot	結果の送受信	arn:aws:securityhub: *<REGION>*:453761072151:product/turbot/turbot

Security Hub に結果を送信するサードパーティーの統合

以下のサードパーティーパートナー製品の統合によって、結果が Security Hub に送信されるようになります。Security Hub は、結果を AWS Security Finding 形式に変換します。

3CORESec – 3CORESec NTA

統合タイプ: 送信

製品 ARN: arn:aws:securityhub:*<REGION>*::product/3coresec/3coresec

3CORESec は、オンプレミスと AWS システムの両方にマネージド検出サービスを提供します。Security Hub との統合により、マルウェア、権限のエスカレーション、横方向の移動、不適切なネットワークセグメンテーションなどの脅威を可視化できます。

製品リンク

パートナードキュメント

Alert Logic – SIEMless Threat Management

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

脆弱性とアセットの可視性、脅威の検出とインシデント管理、割り当てられた SOC アナリストオプションなど AWS WAF、適切なレベルのカバレッジを取得します。

製品リンク

パートナードキュメント

Aqua Security – Aqua Cloud Native Security Platform

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP) は、CI/CD パイプラインからランタイム運用環境まで、コンテナベースのアプリケーションおよびサーバーレスアプリケーションの完全なライフサイクルセキュリティを提供します。

製品リンク

パートナードキュメント

Aqua Security – Kube-bench

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-bench は、Center·for·Internet·Security (CIS) Kubernetes Benchmark を環境に対して実行するオープンソースツールです。

製品リンク

パートナードキュメント

Armor – Armor Anywhere

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywhere は、 のマネージドセキュリティとコンプライアンスを提供します AWS。

製品リンク

パートナードキュメント

AttackIQ – AttackIQ

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platform は、MITRE ATT&CK Framework と連携して現実的な敵対的動作をエミュレートし、全体的なセキュリティ体制の検証と改善を支援します。

製品リンク

パートナードキュメント

Barracuda Networks – Cloud Security Guardian

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentry は、パブリッククラウドでアプリケーションを構築し、ワークロードをパブリッククラウドに移行するだけでなく、組織の安全性を維持するのに役立ちます。

AWS Marketplace リンク

製品リンク

BigID – BigID Enterprise

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

BigID Enterprise Privacy Management Platform は、企業がすべてのシステムで機密データ (PII) を管理および保護するのに役立ちます。

製品リンク

パートナードキュメント

Blue Hexagon – Blue Hexagonの場合 AWS

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagon は、リアルタイム脅威検出プラットフォームです。深層学習の原則を使用して、マルウェアやネットワークの異常を含む既知の脅威、および未知の脅威を検出します。

AWS Marketplace リンク

パートナードキュメント

Capitis Solutions – C2VS

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/capitis/c2vs`

C2VS は、アプリケーション固有の設定ミスとその根本原因を自動的に特定するように設計された、カスタマイズ可能なコンプライアンスソリューションです。

製品リンク

パートナードキュメント

Check Point – CloudGuard IaaS

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuard は、包括的な脅威防止セキュリティを に簡単に拡張 AWS し、クラウド内のアセットを保護します。

製品リンク

パートナードキュメント

Check Point – CloudGuard Posture Management

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

検証可能なクラウドネットワークセキュリティ、高度な IAM 保護、および包括的なコンプライアンスとガバナンスを提供する SaaS プラットフォームです。

製品リンク

パートナードキュメント

Claroty – xDome

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDome は、産業 (OT)、医療 (IoMT)、エンタープライズ (IoT) 環境内の拡張型モノのインターネット (XIoT) 全体で組織によるサイバーフィジカルシステムの保護を支援します。

製品リンク

パートナードキュメント

Cloud Storage Security – Antivirus for Amazon S3

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Security は、Amazon S3 オブジェクト向けのクラウドネイティブなマルウェア対策およびウイルス対策スキャンを提供します。

Antivirus for Amazon S3 は、Amazon S3 内のオブジェクトとファイルのマルウェアや脅威に対するスキャンを、リアルタイムおよびスケジュールされたタイミングで実行します。問題のあるファイルや感染したファイルに可視性を提供し、修復します。

製品リンク

パートナードキュメント

Contrast Security – Contrast Assess

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assess は、Web アプリ、API、マイクロサービスの脆弱性をリアルタイムで検出する IAST ツールです。Contrast Assess は Security Hub と統合することで、すべてのワークロードを一元的に可視化して対応できるようになります。

製品リンク

パートナードキュメント

CrowdStrike – CrowdStrike Falcon

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

CrowdStrike Falcon は、単一の軽量センサーで次世代のウイルス対策、エンドポイントの検出と対応、および 24 時間 365 日管理されるクラウド経由のハンティングを統合します。

製品リンク

パートナードキュメント

CyberArk – Privileged Threat Analytics

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat Analytics は、特権アカウントでのリスクの高いアクティビティや動作を収集、検出、アラートし、進行中の攻撃を阻止するよう対応します。

製品リンク

パートナードキュメント

Data Theorem – Data Theorem

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data Theorem は、セキュリティ上の欠陥やデータプライバシーのギャップを探して、ウェブアプリケーション、APIs、クラウドリソースを継続的にスキャンし、 AppSec データ侵害を防ぎます。

製品リンク

パートナードキュメント

Drata

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drata はコンプライアンス自動化プラットフォームです。SOC2 や ISO、GDPR など、さまざまなフレームワークのコンプライアンスの達成および維持に貢献します。Drataと Security Hub を統合することで、セキュリティの検出結果を 1 か所にまとめることができます。

AWS Marketplace リンク

パートナードキュメント

Forcepoint – Forcepoint CASB

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASB では、クラウドアプリケーションの使用を検出し、リスクを分析して、SaaS およびカスタムアプリケーションの適切なコントロールを実施できます。

製品リンク

パートナードキュメント

Forcepoint – Forcepoint Cloud Security Gateway

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Forcepoint Cloud Security Gateway は、ユーザーがどこにいるか、データがどこにあるかに関わらず、可視性、制御、脅威保護を提供する統合型クラウドセキュリティサービスです。

製品リンク

パートナードキュメント

Forcepoint – Forcepoint DLP

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLP は、人間が主体のリスクに対処し、ユーザーが作業するすべての場所とデータが存在するすべての場所を可視化して制御します。

製品リンク

パートナードキュメント

Forcepoint – Forcepoint NGFW

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFW では、ネットワークを管理し、脅威に対応するために必要なスケーラビリティ、保護、インサイトを使用して、 AWS 環境をエンタープライズネットワークに接続できます。

製品リンク

パートナードキュメント

Fugue – Fugue

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugue は、エージェントレスでスケーラブルなクラウドネイティブプラットフォームであり、同じポリシーを使用して infrastructure-as-code とクラウドランタイム環境の継続的な検証を自動化します。

製品リンク

パートナードキュメント

Guardicore – Centra 4.0

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centra は、最新のデータセンターやクラウドにおけるワークロードのフローの可視化、マイクロセグメンテーション、および違反検出を行います。

製品リンク

パートナードキュメント

HackerOne – Vulnerability Intelligence

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

HackerOne プラットフォームは、世界中のハッカーのコミュニティと提携して、最も関連性の高いセキュリティ問題を発見します。Vulnerability Intelligence を使用することで、組織では自動スキャ

ンを上回る対策を講じることができます。HackerOne のホワイトハッカーによって検証され再現された脆弱性が共有されます。

AWS マーケットプレイスリンク

パートナードキュメント

JFrog – Xray

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xray は、セキュアなソフトウェアサプライチェーンを実行できるように、ライセンスコンプライアンスとセキュリティの脆弱性についてバイナリを継続的にスキャンするユニバーサルアプリケーションセキュリティソフトウェア構成分析 (SCA) ツールです。

AWS Marketplace リンク

パートナードキュメント

Juniper Networks – vSRX Next Generation Firewall

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks' vSRX Virtual Next Generation Firewall は、高度なセキュリティ、セキュアな SD-WAN、堅牢なネットワーク、組み込みオートメーションを備えた完全なクラウドベースの仮想ファイアウォールを提供します。

AWS Marketplace リンク

パートナードキュメント

製品リンク

k9 Security – Access Analyzer

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Security は、 AWS Identity and Access Management アカウントで重要なアクセス変更が発生したときに通知します。を使用するとk9 Security、ユーザーと IAM ロールが重要な AWS のサービスとデータにアクセスできることを理解できます。

k9 Security は継続的デリバリー用に構築されており、 AWS CDK と Terraform の実用的なアクセス監査とシンプルなポリシー自動化で IAM を運用できます。

製品リンク

パートナードキュメント

Lacework – Lacework

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/lacework/lacework`

Lacework は、クラウド向けのデータ駆動型セキュリティプラットフォームです。Lacework Cloud Security Platform は、クラウドセキュリティを大規模に自動化し、スピードと安全性を備えたイノベーションの実現を可能にします。

製品リンク

パートナードキュメント

McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

McAfee MVISION Cloud Native Application Protection Platform (CNAPP) は、お客様の AWS 環境にクラウドのセキュリティ体制管理 (CSPM) およびクラウドワークロード保護プラットフォーム (CWPP) を提供します。

製品リンク

パートナードキュメント

NETSCOUT – NETSCOUT Cyber Investigator

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

NETSCOUT Cyber Investigator は、企業全体のネットワーク脅威、リスク調査、フォレンジック分析プラットフォームで、サイバー脅威によるビジネスへの影響を軽減します。

製品リンク

パートナードキュメント

Palo Alto Networks – Prisma Cloud Compute

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Compute は、VM、コンテナ、およびサーバーレスプラットフォームを保護する、クラウドネイティブのサイバーセキュリティプラットフォームです。

製品リンク

パートナードキュメント

Palo Alto Networks – Prisma Cloud Enterprise

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

クラウドセキュリティ分析、高度な脅威検出、コンプライアンスモニタリングにより、 AWS デプロイを保護します。

製品リンク

パートナードキュメント

Plerion – Cloud Security Platform

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerion は、脅威・リスク主導型の独自のアプローチを採用したクラウドセキュリティプラットフォームであり、ワークロード全体にわたって予防、検出、是正措置を提供します。Plerion と Security Hub を統合することで、お客様はセキュリティの検出結果を 1 か所で一元管理し、それに基づいて行動することができます。

AWS Marketplace リンク

パートナードキュメント

Prowler – Prowler

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowler は、セキュリティのベストプラクティス、強化、継続的モニタリングに関連する AWS チェックを実行するためのオープンソースのセキュリティツールです。

製品リンク

パートナードキュメント

Qualys – Vulnerability Management

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM) は脆弱性を継続的にスキャンして識別し、アセットを保護します。

製品リンク

パートナードキュメント

Rapid7 – InsightVM

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVM は、最新の環境のための脆弱性管理を提供し、脆弱性の検出、優先順位付け、および修復を効率化します。

製品リンク

パートナードキュメント

SecureCloudDB – SecureCloudDB

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/securecloudddb/securecloudddb`

SecureCloudDB は、内部および外部のセキュリティ体制とアクティビティを包括的に可視化するクラウドネイティブなデータベースセキュリティツールです。セキュリティ違反にフラグを立てて、悪用可能なデータベースの脆弱性に対する修復を提供します。

製品リンク

パートナードキュメント

SentinelOne – SentinelOne

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOne は、自律型の Extended Detection and Response (XDR) プラットフォームで、エンドポイント、コンテナ、クラウドワークロード、および IoT デバイスにわたって、AI を使用した防止、検知、対応、ハンティングなどを行います。

AWS Marketplace リンク

製品リンク

Snyk

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snyk には、 AWS で実行中のワークロードのセキュリティリスクについてアプリケーションコンポーネントをスキャンするセキュリティプラットフォームが用意されています。これらのリスクは検出結果として Security Hub に送信され、デベロッパーやセキュリティチームが残りの AWS セキュリティ検出結果とともにそれらを視覚化して優先順位を付けるのに役立ちます。

AWS Marketplace リンク

パートナードキュメント

Sonrai Security – Sonrai Dig

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Dig は、クラウドの誤った構成とポリシー違反を監視および修正することで、セキュリティとコンプライアンス体制の改善を可能にします。

製品リンク

パートナードキュメント

Sophos – Server Protection

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protection は、包括的な defense-in-depth 手法を使用して、重要なアプリケーションとデータを組織の中核で保護します。

製品リンク

パートナードキュメント

StackRox – StackRox Kubernetes Security

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRox により、ビルド、デプロイ、実行など、コンテナのライフサイクル全体にわたってコンプライアンスとセキュリティポリシーを適用することで、エンタープライズにおけるコンテナと Kubernetes のデプロイを大規模に保護できます。

製品リンク

パートナードキュメント

Sumo Logic – Machine Data Analytics

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logic は、DevSecOps チームが AWS アプリケーションを構築、実行、および保護することができる、安全なマシンデータ分析プラットフォームです。

製品リンク

パートナードキュメント

Symantec – Cloud Workload Protection

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protection は、マルウェア対策、侵入防止、およびファイルの整合性モニタリングにより、Amazon EC2 インスタンスを完全に保護します。

製品リンク

パートナードキュメント

Tenable – Tenable.io

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

脆弱性を正確に特定し、調査し、優先順位を付けます。クラウドで管理されます。

製品リンク

パートナードキュメント

Trend Micro – Cloud One

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud One は、適切なセキュリティ情報を適切なタイミングで適切な場所のチームに提供します。この統合により、セキュリティ検出結果が Security Hub にリアルタイムで送信され、Security Hub の AWS リソースとTrend Micro Cloud Oneイベントの詳細の可視性が向上します。

AWS Marketplace リンク

パートナードキュメント

Vectra – Cognito Detect

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectra は、高度な AI を適用してサイバーセキュリティを変革し、隠れたサイバー攻撃者による盗難や損害を事前に検出して対応します。

AWS Marketplace リンク

パートナードキュメント

Wiz – Wiz Security

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wiz は、、ユーザー、ワークロード全体の設定、脆弱性、ネットワーク、IAM 設定 AWS アカウント、シークレットなどを継続的に分析し、実際のリスクを表す重大な問題を検出します。Wiz と

Security Hub を統合すると、Wiz が検出した問題を Security Hub コンソールから視覚化して対応できます。

AWS Marketplace リンク

パートナードキュメント

Security Hub から結果を受信するサードパーティーの統合

以下のサードパーティーパートナー製品の統合によって、結果が Security Hub から受信されるようになります。特に明記されている場合、製品は結果を更新する場合もあります。この場合、パートナー製品で行った更新が見つかると、Security Hub にも反映されます。

Atlassian - Jira Service Management

統合タイプ: 受信と更新

AWS Service Management Connector の は、Security Hub から に結果Jiraを送信しますJira。 Jiraの問題は、結果に基づいて作成されます。Jira の課題が更新されると、Security Hub の対応する結果も更新されます。

統合では Jira サーバーと Jira データセンターのみがサポートされています。

統合の概要とその仕組みについては、「AWS Security Hub - Atlassian Jira Service Management との双方向統合」の動画をご覧ください。

製品リンク

パートナードキュメント

Atlassian - Jira Service Management Cloud

統合タイプ: 受信と更新

Jira Service Management Cloud は、Jira Service Management のクラウドコンポーネントです。

AWS Service Management Connector の は、Security Hub から に結果Jiraを送信しますJira。検出結果は、Jira Service Management Cloud での問題の作成をトリガーします。Jira Service Management Cloud で問題を更新すると、対応する検出結果が Security Hub でも更新されます。

製品リンク

パートナードキュメント

Atlassian – Opsgenie

統合タイプ: 受信

Opsgenie は、常時稼働のサービスを運用するための最新のインシデント管理ソリューションであり、開発および運用チームがサービス中断の計画を立て、インシデント中の管理を維持できるようにします。

Security Hub と統合することで、ミッションクリティカルなセキュリティ関連のインシデントが適切なチームにルーティングされるため、即座の解決が可能となります。

製品リンク

パートナードキュメント

Fortinet – FortiCNP

統合タイプ: 受信

FortiCNP は、セキュリティの結果を実用的なインサイトに集約し、リスクスコアに基づいてセキュリティの洞察に優先順位を付けてアラートの疲労を軽減し、修復を加速するクラウドネイティブ保護製品です。

AWS Marketplace リンク

パートナードキュメント

IBM – QRadar

統合タイプ: 受信

IBM QRadar SIEM は、迅速かつ正確に脅威を検出し、優先順位付けし、調査、および対応する機能をセキュリティチームに提供します。

製品リンク

パートナードキュメント

Logz.io Cloud SIEM

統合タイプ: 受信

Logz.io はログとイベントデータの高度な相関関係を提供し、セキュリティチームがセキュリティの脅威をリアルタイムで検出、分析、対応できるようにする Cloud SIEM のプロバイダです。

製品リンク

パートナードキュメント

MetricStream – CyberGRC

統合タイプ: 受信

MetricStream CyberGRC は、サイバーセキュリティリスクの管理、測定、軽減に役立ちます。Security Hub の検出結果を受け取ることで、CyberGRC はこれらのリスクをより詳細に把握できるため、サイバーセキュリティへの投資を優先して IT ポリシーを遵守することができます。

AWS Marketplace リンク

製品リンク

MicroFocus – MicroFocus Arcsight

統合タイプ: 受信

ArcSight はリアルタイムの効果的な脅威の検出と対応を加速し、レスポンスのオートメーションとオーケストレーションにより、イベントの相関と監視対象外の分析を統合します。

製品リンク

パートナードキュメント

New Relic Vulnerability Management

統合タイプ: 受信

New Relic Vulnerability Management は Security Hub からセキュリティに関する検出結果を受け取るので、スタック全体のコンテキストでセキュリティとパフォーマンステレメトリを一元的に把握できます。

AWS Marketplace リンク

パートナードキュメント

PagerDuty – PagerDuty

統合タイプ: 受信

PagerDuty のデジタル運用管理プラットフォームを使用すると、あらゆるシグナルが自動的に適切なインサイトとアクションに変換されることで、顧客に影響を与える問題を事前に軽減できます。

AWS ユーザーは、PagerDuty一連の AWS 統合を使用して、 AWS およびハイブリッド環境を自信を持ってスケーリングできます。

PagerDuty を Security Hub の集約および整理されたセキュリティアラートと組み合わせれば、チームは脅威応答プロセスを自動化し、潜在的な問題を防ぐためのカスタムアクションを迅速に設定することが可能になります。

クラウド移行プロジェクトを実施している PagerDuty ユーザーは、移行のライフサイクルを通して発生する問題の影響を軽減しながら、迅速に移行することができます。

製品リンク

パートナードキュメント

Palo Alto Networks – Cortex XSOAR

統合タイプ: 受信

Cortex XSOAR は、セキュリティ製品スタック全体と統合してインシデント対応とセキュリティ運用を迅速化する、Security Orchestration, Automation, and Response (SOAR) プラットフォームです。

製品リンク

パートナードキュメント

Palo Alto Networks – VM-Series

統合タイプ: 受信

Palo Alto VM-Series と Security Hub との統合により、脅威インテリジェンスを収集し、セキュリティポリシーの自動更新として VM-Series 次世代ファイアウォールに送信して、悪質な IP アドレスアクティビティをブロックします。

製品リンク

パートナードキュメント

Rackspace Technology – Cloud Native Security

統合タイプ: 受信

ネイティブ AWS セキュリティ製品に加えて、Rackspace Technology は Rackspace SOC による 24 時間 365 日のモニタリング、高度な分析、脅威の軽減によるマネージドセキュリティサービスを提供します。

製品リンク

Rapid7 – InsightConnect

統合タイプ: 受信

Rapid7 InsightConnect は、セキュリティ上のオーケストレーションとオートメーションのソリューションであり、コードをほとんどまたは一切使用せずに SOC 操作を最適化することが可能です。

製品リンク

パートナードキュメント

RSA – RSA Archer

統合タイプ: 受信

RSA Archer IT およびセキュリティリスク管理では、ビジネスにとって重要な資産を特定し、セキュリティポリシーと標準を確立して伝え、攻撃を検出して対応し、セキュリティ上の欠陥を特定して修正し、明確な IT リスク管理のベストプラクティスを確立できます。

製品リンク

パートナードキュメント

ServiceNow – ITSM

統合タイプ: 受信と更新

ServiceNow と Security Hub との統合により、Security Hub からのセキュリティ結果を ServiceNow ITSM で表示することができます。また、Security Hub から結果を受信したときに、ServiceNow でインシデントまたは問題を自動的に作成するよう設定することもできます。

これらのインシデントや問題が更新されると、Security Hub の結果が更新されます。

統合の概要とその仕組みについては、「AWS Security Hub - ServiceNow ITSM との双方向統合」の動画をご覧ください。

製品リンク

パートナードキュメント

Slack – Slack

統合タイプ: 受信

Slack は、人、データ、およびアプリケーションを 1 か所に集約するビジネステクノロジースタックのレイヤーです。人々が効果的に協力し、重要な情報を見つけ、何十万もの重要なアプリケーションやサービスにアクセスして、最善の仕事ができるようにします。

製品リンク

パートナードキュメント

Splunk – Splunk Enterprise

統合タイプ: 受信

Splunk は、Security Hub の検出結果のコンシューマーとして Amazon CloudWatch Events を使用します。データを Splunk に送信すると、高度なセキュリティ分析と SIEM を実行できます。

製品リンク

パートナードキュメント

Splunk – Splunk Phantom

統合タイプ: 受信

AWS Security Hub のSplunk Phantomアプリケーションでは、検出結果は に送信され、追加の脅威インテリジェンス情報を含むPhantom自動コンテキストエンリッチメントや、自動応答アクションを実行します。

製品リンク

パートナードキュメント

ThreatModeler

統合タイプ: 受信

ThreatModeler は、エンタープライズソフトウェアとクラウド開発のライフサイクルを保護し、スケールする自動化された脅威モデリングソリューションです。

製品リンク

パートナードキュメント

Trellix – Trellix Helix

統合タイプ: 受信

Trellix Helix は、クラウドホスト型のセキュリティ運用プラットフォームであり、組織は、アラートから修正までのあらゆるインシデントを制御できるようになります。

製品リンク

パートナードキュメント

Security Hub に結果を送信し、Security Hub から結果を受信するサードパーティーの統合

以下のサードパーティーパートナー製品の統合によって、結果が Security Hub に送信され、結果が Security Hub から受信されるようになります。

Caveonix – Caveonix Cloud

統合タイプ: 送信と受信

製品 ARN: `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

Caveonix AI 搭載プラットフォームは、クラウドネイティブのサービスや VM、コンテナを対象に、ハイブリッドクラウドの可視性、評価、緩和を自動化します。 AWS Security Hub と統合され、AWS データと高度な分析をCaveonixマージして、セキュリティアラートとコンプライアンスに関するインサイトを提供します。

AWS Marketplace リンク

パートナードキュメント

Cloud Custodian – Cloud Custodian

統合タイプ: 送信と受信

製品 ARN: `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodian により、ユーザーをクラウドで適切に管理できます。シンプルな YAML DSL を使用することでルールの定義が容易で、クラウドインフラストラクチャを適切に管理でき、セキュリティとコストの最適化の両方を実現することができます。

製品リンク

パートナードキュメント

DisruptOps, Inc. – DisruptOPS

統合タイプ: 送信と受信

製品 ARN: `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

DisruptOps の Security Operations Platform は、自動化されたガードレールを使用することにより、組織がクラウド内でベストプラクティスを維持するのに役立ちます。

製品リンク

パートナードキュメント

Kion

統合タイプ: 送信と受信

製品 ARN: `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion (旧 cloudtamer.io) は、 の完全なクラウドガバナンスソリューションです AWS。 Kionは、ステークホルダーにクラウド運用を可視化し、クラウドユーザーがアカウントを管理し、予算とコストを管理し、継続的なコンプライアンスを確保するのに役立ちます。

製品リンク

パートナードキュメント

Turbot – Turbot

統合タイプ: 送信と受信

製品 ARN: `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbot は、クラウドインフラストラクチャの安全性、準拠性、スケーラブル性を保証し、そのコストを最適化します。

製品リンク

パートナードキュメント

カスタム製品インテグレーションを使用して調査結果を AWS Security Hub に送信する

Security Hub は、 AWS 統合サービスやサードパーティ製品によって生成された結果に加えて、他のカスタムセキュリティ製品によって生成された結果も使用できます。

`BatchImportFindings`API オペレーションを使用して、これらの結果を手動で Security Hub に送信できます。

カスタム統合を設定する場合は、「Security Hub パートナー統合ガイド」で提供される「ガイドラインとチェックリスト」を使用します。

カスタムセキュリティ製品からの結果の送信に関する要件と推奨事項

`BatchImportFindings` API オペレーションを正常に呼び出すには、あらかじめ Security Hub を有効にしておく必要があります。

the section called “Finding 形式” を使用して結果の詳細を指定する必要があります。カスタム統合からの結果には、以下の要件と推奨事項を使用します。

製品 ARN の設定

Security Hub を有効にすると、Security Hub 用のデフォルトの製品 Amazon リソースネーム (ARN) が現在のアカウントで生成されます。

この製品 ARN の形式は、`arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default` です。例えば、`arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default` です。

`BatchImportFindings` API オペレーションを呼び出すときに、この製品 ARN を `ProductArn` 属性の値として使用します。

会社名と製品名の定義

`BatchImportFindings` を使用して、Security Hub に結果を送信するカスタム統合の優先会社名と製品名を設定します。

事前設定された会社名と製品名 (個人名とデフォルト名) のそれぞれが指定した名前で置き換えられ、Security Hub コンソールと各結果の JSON に表示されます。「BatchImportFindings を使用して結果を作成および更新する」を参照してください。

結果 ID の設定

`Id` 属性を使用して、独自の結果の ID を提供、管理、および増分する必要があります。

新しい結果にはそれぞれ固有の結果 ID が必要です。カスタム製品が同じ結果 ID で複数の結果を送信した場合、Security Hub は最初の結果のみを処理します。

アカウント ID の設定

`AwsAccountId` 属性を使用して、自分のアカウント ID を指定する必要があります。

作成日と更新日の設定

`CreatedAt` および `UpdatedAt` 属性に独自のタイムスタンプを渡す必要があります。

カスタム製品からの結果の更新

カスタム製品から新しい結果を送信するだけでなく、`BatchImportFindings` API オペレーションを使用して、カスタム製品から既存の結果を更新することもできます。

既存の結果を更新するには、既存の結果 ID を (`Id` 属性を介して) 使用します。リクエストで更新された適切な情報 (変更された `UpdatedAt` タイムスタンプを含む) を使用して、完全な結果を再送信します。

カスタム統合の例

次のカスタム製品の統合例をガイドとして使用して、独自のカスタムソリューションを作成できます。

Chef InSpec スキャンからの結果を Security Hub に送信する

Chef InSpecコンプライアンススキャンを実行し、結果を Security Hub AWS CloudFormation に送信するテンプレートを作成できます。

詳細については、「Chef InSpec および AWS Security Hub の継続的なコンプライアンスモニタリング」を参照してください。

Trivy によって検出されたコンテナの脆弱性を Security Hub へ送信する

AWS CloudFormation AquaSecurity Trivyコンテナに脆弱性がないかスキャンするテンプレートを作成し、その脆弱性の検出結果を Security Hub に送信できます。

詳細については、「AWS Security Hub Trivy によるコンテナ脆弱性スキャンのための CI/CD パイプラインを構築する方法」を参照してください。

AWS Security Hub のセキュリティコントロールと標準

AWS Security Hub は、サポートされているさまざまな およびサードパーティー製品のセキュリティ検出結果を消費、集約 AWS 、分析します。

Security Hub は、ルールに対して自動的かつ継続的なセキュリティチェックを実行することで、独自の検出結果も生成します。ルールはセキュリティコントロールによって表されます。コントロールは、1 つ以上のセキュリティ標準で有効になっている場合もあります。コントロールは、標準の要件が満たされているかどうかの判断に役立ちます。

コントロールに対するセキュリティチェックでは、セキュリティ体制をモニタリングし、注意が必要な特定の AWS アカウント またはリソースを特定するために使用できる検出結果が生成されます。各コントロールは AWS サービスとリソースに関連しています。例えば、CloudTrail.4 コントロールに対するセキュリティチェックにより、ログにログファイルの検証が設定されているかどうかが決まります AWS CloudTrail 。コントロールの詳細については、「セキュリティコントロールの表示と管理」を参照してください。

有効な 1 つ以上の Security Hub 標準でコントロールを有効にできます。標準を有効にすると、Security Hub は、その標準に適用されるコントロールを自動的に有効化します。セキュリティ標準により、特定のコンプライアンスフレームワークに集中できます。Security Hub は、各標準に適用されるコントロールを定義します。セキュリティ標準の詳細については、「セキュリティ標準の表示と管理」を参照してください。

セキュリティチェックの結果に基づいて、Security Hub は全体的なセキュリティスコアと標準固有のセキュリティスコアを計算します。これらのスコアは、セキュリティ体制を理解するのに役立ちます。スコアの詳細については、「セキュリティスコアの計算方法」を参照してください。

セキュリティチェックにおける Security Hub の料金については、「Security Hub の料金」を参照してください。

トピック

- 標準とコントロールを設定するための IAM 権限
- Security Hub のセキュリティチェックとセキュリティスコア
- Security Hub 標準のリファレンス
- セキュリティ標準の表示と管理
- Security Hub コントロールのリファレンス

- セキュリティコントロールの表示と管理

標準とコントロールを設定するための IAM 権限

セキュリティコントロールに関する情報を表示し、標準でセキュリティコントロールを有効または無効にするには、 アクセスに使用する AWS Identity and Access Management (IAM) ロールに、次の API アクションを呼び出すアクセス許可 AWS Security Hub が必要です。これらのアクションに対する権限を追加しないと、API を呼び出すことはできません。必要な権限を取得するには、セキュリティハブのマネージドポリシーを使用します。または、カスタム IAM ポリシーを更新してこれらのアクションの権限を含めることもできます。カスタムポリシーには、`DescribeStandardsControls` と `UpdateStandardsControl` API の権限も含める必要があります。

- **`BatchGetSecurityControls`** – 現在のアカウントと のセキュリティコントロールのバッチに関する情報を返します AWS リージョン。
- **`ListSecurityControlDefinitions`** — 指定された標準に適用されるセキュリティコントロールについての情報を返します。
- **`ListStandardsControlAssociations`** — アカウントで有効になっている各標準で、セキュリティコントロールが現在有効か無効かを識別します。
- **`BatchGetStandardsControlAssociations`** — セキュリティコントロールのバッチについて、指定された標準の各コントロールが有効か無効かを識別します。
- **`BatchUpdateStandardsControlAssociations`** — コントロールを含む標準のセキュリティコントロールを有効化するか、標準のコントロールを無効化するために使用します。これは、管理者がメンバーアカウントによるコントロールの有効化または無効化を許可しない場合に、既存の `UpdateStandardsControl` API の代わりとして一括で使用することができます。

前述の API に加えて、IAM ロールに **`BatchGetControlEvaluations`** を呼び出す権限を追加する必要があります。この権限は、コントロールの有効化およびコンプライアンスステータス、コントロールの検出結果の数、コントロールの全体的なセキュリティスコアを Security Hub コンソールに表示するために必要です。コンソールのみが を呼び出すため**`BatchGetControlEvaluations`**、この IAM アクセス許可は公開されている Security Hub APIs または AWS CLI コマンドに直接対応していません。

コントロールと標準に関連する API の詳細については、AWS Security Hub API リファレンスをご覧ください。

Security Hub のセキュリティチェックとセキュリティスコア

有効にするコントロールごとに、 はセキュリティチェック AWS Security Hub を実行します。セキュリティチェックは、 AWS リソースがコントロールに含まれるルールに準拠しているかどうかを決定します。

一部のチェックは定期的なスケジュールで実行されます。その他のチェックは、リソースの状態が変更された場合にのみ実行されます。詳細については、「the section called “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。

多くのセキュリティチェックでは、 AWS Config マネージドルールまたはカスタムルールを使用してコンプライアンス要件を確立します。これらのチェックを実行するには、 を設定する必要があります AWS Config。詳細については、「the section called “AWS Config ルールとセキュリティチェック”」を参照してください。カスタムの Lambda 関数を使用して実行されるチェックもあります。カスタム Lambda 関数は Security Hub によって管理され、お客様には表示されません。

Security Hub はセキュリティチェックを実行すると、検出結果を生成してコンプライアンスステータスを割り当てます。コンプライアンスステータスの詳細については、「結果のコンプライアンスステータスの値」を参照してください。

Security Hub は、コントロール検出結果のコンプライアンス状況を使用して、全体的なコントロールステータスを決定します。Security Hub は、有効になっているすべてのコントロールと特定の標準のセキュリティスコアも計算します。詳細については、「the section called “コンプライアンスステータスとコントロールステータス”」および「the section called “セキュリティスコアの決定”」を参照してください。

[統合されたコントロールの検出結果] を有効にしている場合、コントロールが複数の標準に関連付けられていても、Security Hub は単一の検出結果を生成します。詳細については、「統合されたコントロールの検出結果」を参照してください。

トピック

- Security Hub が AWS Config ルールを使用してセキュリティチェックを実行する方法
- AWS Config コントロールの検出結果を生成するために必要な リソース
- セキュリティチェックの実行スケジュール
- コントロールの結果を生成および更新する
- コンプライアンスステータスとコントロールステータス
- セキュリティスコアの決定

Security Hub が AWS Config ルールを使用してセキュリティチェックを実行する方法

環境のリソースでセキュリティチェックを実行するには、 は標準で指定されたステップを使用する AWS Security Hub か、特定の AWS Config ルールを使用します。一部のルールはマネージドルールであり、 AWS Configによって管理されます。その他のルールは、Security Hub によって作成されるカスタムルールです。

AWS Config Security Hub がコントロールに使用する ルールは、Security Hub サービスによって有効および制御されるため、サービスにリンクされたルールと呼ばれます。

これらの AWS Config ルールに対するチェックを有効にするには、まずアカウント AWS Config でを有効にし、必要なリソースのリソース記録を有効にする必要があります。を有効にする方法については、 AWS Config「」を参照してくださいの設定 AWS Config。必要なリソース記録については、「AWS Config コントロールの検出結果を生成するために必要な リソース」を参照してください。

Security Hub がサービスリンクルールを生成する方法

AWS Config サービスにリンクされたルールを使用するすべてのコントロールについて、Security Hub は必要なルールのインスタンスを AWS 環境内に作成します。

これらのサービスリンクルールは Security Hub に固有です。同じルールの他のインスタンスが既に存在している場合も、これらのサービスリンクルールが作成されます。サービスリンクルールでは `securityhub` が元のルール名の前に追加され、一意の識別子がルール名の後に追加されます。例えば、元の AWS Config マネージドルール の場合`vpc-flow-logs-enabled`、サービスにリンクされたルール名は のようになります`securityhub-vpc-flow-logs-enabled-12345`。

コントロールの評価に使用できる AWS Config ルールの数には制限があります。Security Hub が作成するカスタム AWS Config ルールは、その制限にはカウントされません。アカウントのマネージドルール AWS Config の上限にすでに達している場合でも、セキュリティ標準を有効にできます。AWS Config ルールの制限の詳細については、「 AWS Config デベロッパーガイド」の「サービスの制限」を参照してください。

コントロールの AWS Config ルールに関する詳細の表示

AWS Config マネージドルールを使用するコントロールの場合、コントロールの説明には AWS Config ルールの詳細へのリンクが含まれます。カスタムルールは、コントロールの説明からはリンクされていません。コントロールの説明については、「Security Hub コントロールのリファレンス」を参照してください。リストからコントロールを選択すると、その説明が表示されます。

これらのコントロールから生成された検出結果の場合、検出結果の詳細には関連する AWS Config ルールへのリンクが含まれます。検出結果の詳細から AWS Config ルールに移動するには、選択したアカウントで に移動するための IAM アクセス許可も必要です AWS Config。

[Findings] (結果) ページ、[Insights] (インサイト) ページ、および [Integrations] (統合) ページの結果の詳細には、 AWS Config ルールの詳細への [Rules] (ルール) リンクが含まれます。「結果の詳細の確認」を参照してください。

コントロールの詳細ページで、結果リストの調査列に AWS Config ルールの詳細へのリンクが含まれています。検出結果リソースの AWS Config ルールの表示 を参照してください。

AWS Config コントロールの検出結果を生成するために必要な リソース

AWS Security Hub は、Security Hub コントロールに対してセキュリティチェックを実行してコントロールの検出結果を生成します。一部のコントロールは、特定のリソースへのコンプライアンスを評価する AWS Config ルールを使用します。スケジュールタイプが変更トリガーであるコントロールについて、Security Hub が検出結果を生成するためには、 AWS Configで、必要なリソースの記録をオンにする必要があります。定期的スケジュールタイプの大半のコントロールのリソースを記録する必要はありません。ただし、定期的なコントロールの中には、コンプライアンスの変化を検出するためにリソースの記録を要求するものもあります。

このページでは、標準全体で必要なリソースのリストと、必要なリソースを標準ごとに分類したリストを示します。最初の表には、各リソースを使用する Security Hub コントロールも一覧表示されています。

AWS Config ルールに基づくセキュリティチェックによって検出結果が生成された場合、検出結果の詳細には、関連する AWS Config ルールへのルールリンクが含まれます。 AWS Config ルールに移動するには、アカウントに AWS Config ルールを表示するための AWS Identity and Access Management (IAM) アクセス許可が必要です。

> **Note**
>
> コントロールが利用できない AWS リージョン では、対応するリソースは では使用できません AWS Config。Security Hub コントロールに関するリージョン制限の一覧については、リージョン別のコントロールの可用性 を参照してください。

AWS Config すべてのコントロールに必要な リソース

Security Hub が AWS Config ルールを使用する有効な Security Hub 変更トリガーコントロールの検出結果を生成するには、これらのリソースを に記録する必要があります AWS Config。この表には、どのコントロールが特定のリソースを必要とするかも示されています。1 つのコントロールが複数のリソースを必要とする場合もあります。

サービス	必要なリソース	関連するコントロール
Amazon API Gateway	`AWS::ApiGateway::Stage`	APIGateway.1 APIGateway.2 APIGateway.3 APIGateway.4 APIGateway.5
	`AWS::ApiGatewayV2::Stage`	APIGateway.1 APIGateway.9
AWS AppSync	`AWS::AppSync::GraphQLApi`	AppSync.2 AppSync.4 AppSync.5
AWS Backup (AWS Backup)	`AWS::Backup::BackupPlan`	バックアップ.5
	`AWS::Backup::BackupVault`	バックアップ.3
	`AWS::Backup::RecoveryPoint`	Backup.1 バックアップ.2

サービス	必要なリソース	関連するコントロール
	`AWS::Backup::ReportPlan`	バックアップ.4
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`	ACM.1 ACM.2 ACM.3
Amazon Athena	`AWS::Athena::DataCatalog`	Athena.2
	`AWS::Athena::WorkGroup`	Athena.3
AWS CloudFormation	`AWS::CloudFormation::Stack`	CloudFormation.2

サービス	必要なリソース	関連するコントロール
Amazon CloudFront	`AWS::CloudFront::Distribution`	CloudFront.1 CloudFront.3 CloudFront.4 CloudFront.5 CloudFront.6 CloudFront.7 CloudFront.8 CloudFront.9 CloudFront.10 CloudFront.13 CloudFront.14
AWS CloudTrail	`AWS::CloudTrail::Trail`	CloudTrail.9
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	CloudWatch.15 CloudWatch.17
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	CodeArtifact.1
AWS CodeBuild	`AWS::CodeBuild::Project`	CodeBuild.1 CodeBuild.2 CodeBuild.3 CodeBuild.4

サービス	必要なリソース	関連するコントロール
Amazon Detective	`AWS::Detective::Graph`	Detective.1
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate`	DMS.2

	`AWS::DMS::Endpoint`	`DMS.9`
		`DMS.10`
		`DMS.11`
		`DMS.12`

	`AWS::DMS::EventSubscription`	DMS.3
	`AWS::DMS::ReplicationInstance`	DMS.4 DMS.6
	`AWS::DMS::ReplicationSubnetGroup`	DMS.5
	`AWS::DMS::ReplicationTask`	DMS.7 DMS.8
Amazon DynamoDB	`AWS::DynamoDB::Table`	DynamoDB.1 DynamoDB.2 DynamoDB.5 DynamoDB.6

サービス	必要なリソース	関連するコントロール
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::ClientVpnEndpoint	EC2.51
	AWS::EC2::CustomerGateway	EC2.36
	AWS::EC2::EIP	EC2.12 EC2.37
	AWS::EC2::FlowLog	EC2.48
	AWS::EC2::Instance	EC2.4 EC2.8 EC2.9 EC2.17 EC2.24 EC2.38 EMR.1 SSM.1
	AWS::EC2::InternetGateway	EC2.39
	AWS::EC2::LaunchTemplate	EC2.25

サービス	必要なリソース	関連するコントロール
	AWS::EC2::NatGateway	EC2.40
	AWS::EC2::NetworkAcl	EC2.16 EC2.21 EC2.41
	AWS::EC2::NetworkInterface	EC2.22 EC2.35
	AWS::EC2::RouteTable	EC2.42
	AWS::EC2::SecurityGroup	EC2.2 EC2.13 EC2.14 EC2.18 EC2.19 EC2.43
	AWS::EC2::Subnet	EC2.15 EC2.44 ElastiCache.7
	AWS::EC2::TransitGateway	EC2.23 EC2.52

サービス	必要なリソース	関連するコントロール
	AWS::EC2::TransitGatewayAttachment	EC2.33
	AWS::EC2::TransitGatewayRouteTable	EC2.34
	AWS::EC2::Volume	EC2.3 EC2.45
	AWS::EC2::VPC	EC2.6 EC2.46
	AWS::EC2::VPCEndpointService	EC2.47
	AWS::EC2::VPCPeeringConnection	EC2.49
	AWS::EC2::VPNConnection	EC2.20
	AWS::EC2::VPNGateway	EC2.50

サービス	必要なリソース	関連するコントロール
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	AutoScaling.1 AutoScaling.2 AutoScaling.6 AutoScaling.9 AutoScaling.10
	`AWS::AutoScaling::LaunchConfiguration`	AutoScaling.3 Autoscaling.5
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`	SSM.3
	`AWS::SSM::ManagedInstanceInventory`	SSM.1
	`AWS::SSM::PatchCompliance`	SSM.2
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`	ECR.4
	`AWS::ECR::Repository`	ECR.2 ECR.3

サービス	必要なリソース	関連するコントロール
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`	ECS.12 ECS.14
	`AWS::ECS::Service`	ECS.2 ECS.10 ECS.13
	`AWS::ECS::TaskDefinition`	ECS.1 ECS.3 ECS.4 ECS.5 ECS.8 ECS.9 ECS.15
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`	EFS.3 EFS.4 EFS .5
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`	EKS.2 EKS.6 EKS.8
	`AWS::EKS::IdentityProviderConfig`	EKS.7

サービス	必要なリソース	関連するコントロール
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`	ElasticBeanstalk.1 ElasticBeanstalk.2 ElasticBeanstalk.3
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`	ELB.2 ELB.3 ELB.5 ELB.7 ELB.8 ELB.9 ELB.10 ELB.14
	`AWS::ElasticLoadBalancingV2::LoadBalancer`	ELB.1 ELB.4 ELB.5 ELB.6 ELB.12 ELB.13 ELB.16

サービス	必要なリソース	関連するコントロール
ElasticSearch	AWS::Elasticsearch::Domain	ES.3 ES.4 ES.5 ES.6 ES.7 ES.8 ES.9
Amazon EventBridge	AWS::Events::EventBus	EventBridge.2 EventBridge.3
	AWS::Events::Endpoint	EventBridge.4
AWS Global Accelerator	AWS::GlobalAccelerator::Accelerator	GlobalAccelerator.1
AWS Glue	AWS::Glue::Job	Glue.1
Amazon GuardDuty	AWS::GuardDuty::Detector	GuardDuty.4
	AWS::GuardDuty::Filter	GuardDuty.2
	AWS::GuardDuty::IPSet	GuardDuty.3

サービス	必要なリソース	関連するコントロール
AWS Identity and Access Management (IAM)	`AWS::IAM::Group`	IAM.27 KMS.2
	`AWS::IAM::Policy`	IAM.1 IAM.21 KMS.1
	`AWS::IAM::Role`	IAM.24 IAM.27 KMS.2
	`AWS::IAM::User`	IAM.2 IAM.3 IAM.5 IAM.8 IAM.19 IAM.22 IAM.25 IAM.27 KMS.2
AWS Identity and Access Management Access Analyzer	`AWS::AccessAnalyzer::Analyzer`	IAM.23
AWS IoT	`AWS::IoT::Authorizer`	IoT.4

サービス	必要なリソース	関連するコントロール
	AWS::IoT::Dimension	IoT.3
	AWS::IoT::MitigationAction	IoT.2
	AWS::IoT::Policy	IoT.6
	AWS::IoT::RoleAlias	IoT.5
	AWS::IoT::SecurityProfile	IoT.1
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias	S3.17
	AWS::KMS::Key	KMS.3 S3.17
Amazon Kinesis	AWS::Kinesis::Stream	Kinesis.1 Kinesis.2
AWS Lambda	AWS::Lambda::Function	Lambda.1 Lambda.2 Lambda.3 Lambda.5 Lambda.6

サービス	必要なリソース	関連するコントロール
Amazon MSK	`AWS::MSK::Cluster`	MSK.1 MSK.2
Amazon MQ	`AWS::AmazonMQ::Broker`	MQ.2 MQ.3 MQ.4 MQ.5 MQ.6
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	NetworkFirewall.1 NetworkFirewall.7 NetworkFirewall.9
	`AWS::NetworkFirewall::FirewallPolicy`	NetworkFirewall.3 NetworkFirewall.4 NetworkFirewall.5 NetworkFirewall.8
	`AWS::NetworkFirewall::RuleGroup`	NetworkFirewall.6

サービス	必要なリソース	関連するコントロール
Amazon OpenSearch サービス	`AWS::OpenSearch::Domain`	Opensearch.1 Opensearch.2 Opensearch.3 Opensearch.4 Opensearch.5 Opensearch.6 Opensearch.7 Opensearch.8 Opensearch.9 Opensearch.10 Opensearch.11

サービス	必要なリソース	関連するコントロール
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`	DocumentDB.1 DocumentDB.2 DocumentDB.4 DocumentDB.5 Neptune.1 Neptune.2 Neptune.4 Neptune.5 Neptune.7 Neptune.8 Neptune.9 RDS.7 RDS.12 RDS.14 RDS.15 RDS.16 RDS.24 RDS.27 RDS.28 RDS.34 RDS.35

サービス	必要なリソース	関連するコントロール
	`AWS::RDS::DBClusterSnapshot`	DocumentDB.3 Neptune.3 Neptune.6 RDS.1 RDS.4 RDS.29
	`AWS::RDS::DBInstance`	RDS.2 RDS.3 RDS.5 RDS.6 RDS.8 RDS.9 RDS.10 RDS.11 RDS.13 RDS.17 RDS.18 RDS.23 RDS.25 RDS.30

サービス	必要なリソース	関連するコントロール
	AWS::RDS::DBSecurityGroup	RDS.31
	AWS::RDS::DBSnapshot	RDS.1 RDS.4 RDS.32
	AWS::RDS::DBSubnetGroup	RDS.33
	AWS::RDS::EventSubscription	RDS.19 RDS.20 RDS.21 RDS.22
Amazon Redshift	AWS::Redshift::Cluster	Redshift.1 Redshift.2 Redshift.3 Redshift.4 Redshift.6 Redshift.7 Redshift.8 Redshift.9 Redshift.10 Redshift.11

サービス	必要なリソース	関連するコントロール
	AWS::Redshift::ClusterParameterGroup	Redshift.2
	AWS::Redshift::ClusterSnapshot	Redshift.13
	AWS::Redshift::ClusterSubnetGroup	Redshift.14
	AWS::Redshift::EventSubscription	Redshift.12
Amazon Route 53	AWS::Route53::HostedZone	Route53.2
	AWS::Route53::HealthCheck	Route53.1
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccessPoint	S3.19
	AWS::S3::AccountPublicAccessBlock	S3.2 S3.3

サービス	必要なリソース	関連するコントロール
	AWS::S3::Bucket	S3.2 S3.3 S3.5 S3.6 S3.7 S3.8 S3.9 S3.10 S3.11 S3.12 S3.13 S3.14 S3.15 S3.17 S3.20
AWS Secrets Manager	AWS::SecretsManager::Secret	SecretsManager.1 SecretsManager.2 SecretsManager.5
AWS Service Catalog	AWS::ServiceCatalog::Portfolio	ServiceCatalog.1

サービス	必要なリソース	関連するコントロール
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet`	SES.2
	`AWS::SES::ContactList`	SES.1
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`	SNS.1 SNS.3
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`	SQS.1 SQS.2
Amazon SageMaker	`AWS::SageMaker::NotebookInstance`	SageMaker.2 SageMaker.3
AWS Step Functions	`AWS::StepFunctions::StateMachine`	StepFunctions.1
	`AWS::StepFunctions::Activity`	StepFunctions.2
AWS Transfer Family	`AWS::Transfer::Workflow`	Transfer.1
AWS WAF	`AWS::WAF::Rule`	WAF.6
	`AWS::WAF::RuleGroup`	WAF.7

サービス	必要なリソース	関連するコントロール
	AWS::WAF::WebACL	WAF.1 WAF.8
	AWS::WAFRegional::Rule	WAF.2
	AWS::WAFRegional::RuleGroup	WAF.3
	AWS::WAFRegional::WebACL	WAF.4
	AWS::WAFv2::RuleGroup	WAF.12
	AWS::WAFv2::WebACL	WAF.10 WAF.11

FSBP 標準に必要なリソース

Security Hub が AWS Config ルールを使用する有効な AWS Foundational Security Best Practices (FSBP) 変更トリガーコントロールの検出結果を正確にレポートするには、これらのリソースを に記録する必要があります AWS Config。この標準の詳細については、「AWS Foundational Security Best Practices (FSBP) 標準」を参照してください。

サービス	必要なリソース
Amazon API Gateway	AWS::ApiGateway::Stage AWS::ApiGatewayV2::Stage
AWS AppSync	AWS::AppSync::GraphQLApi

サービス	必要なリソース
AWS Backup	`AWS::Backup::RecoveryPoint`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CodeBuild	`AWS::CodeBuild::Project`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint`
	`AWS::DMS::ReplicationInstance`
	`AWS::DMS::ReplicationTask`

Amazon DynamoDB	`AWS::DynamoDB::Table`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

サービス	必要なリソース

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`
	`AWS::EC2::Instance`
	`AWS::EC2::LaunchTemplate`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::TransitGateway`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`

サービス	必要なリソース
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MSK	`AWS::MSK::Cluster`

AWS Network Firewall	`AWS::NetworkFirewall::Firewall`
	`AWS::NetworkFirewall::FirewallPolicy`
	`AWS::NetworkFirewall::RuleGroup`

Amazon OpenSearch サービス	`AWS::OpenSearch::Domain`

サービス	必要なリソース

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Route 53	`AWS::Route53::HostedZone`

Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint`
	`AWS::S3::AccountPublicAccessBlock`
	`AWS::S3::Bucket`

Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
Amazon SageMaker	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Step Functions	`AWS::StepFunctions::StateMachine`

サービス	必要なリソース

AWS WAF	`AWS::WAF::Rule`
	`AWS::WAF::RuleGroup`
	`AWS::WAF::WebACL`
	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::RuleGroup`
	`AWS::WAFv2::WebACL`

CIS AWS Foundations Benchmark に必要なリソース

Center for Internet Security (CIS) AWS Foundations Benchmark に適用される有効なコントロールのセキュリティチェックを実行するには、Security Hub は Amazon Web Services のセキュリティ保護のチェックに規定された正確な監査ステップを実行するか、特定の AWS Config マネージドルールを使用します。

この標準の詳細については、「CIS AWS Foundations Benchmark」を参照してください。

CIS v3.0.0 に必要なリソース

Security Hub が AWS Config ルールを使用する有効な CIS v3.0.0 変更トリガーコントロールの検出結果を正確にレポートするには、これらのリソースを に記録する必要があります AWS Config。

サービス	必要なリソース

Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::Instance`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::SecurityGroup`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`

サービス	必要なリソース

	`AWS::IAM::User`
	
	`AWS::IAM::Role`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

CIS v1.4.0 に必要な リソース

Security Hub が AWS Config ルールを使用する有効な CIS v1.4.0 変更トリガーコントロールの検出結果を正確にレポートするには、これらのリソースを に記録する必要があります AWS Config。

サービス	必要なリソース

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::NetworkAcl`
	
	`AWS::EC2::SecurityGroup`

AWS Identity and Access Management (IAM)	`AWS::IAM::Policy`
	
	`AWS::IAM::User`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

CIS v1.2.0 に必要な リソース

Security Hub が AWS Config ルールを使用する有効な CIS v1.2.0 変更トリガーコントロールの検出結果を正確にレポートするには、これらのリソースを に記録する必要があります AWS Config。

サービス	必要なリソース
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::SecurityGroup`

サービス	必要なリソース
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` `AWS::IAM::User`

NIST SP 800-53 Rev. 5 に必要なリソース

Security Hub が有効な米国国立標準技術研究所 (NIST) SP 800-53 Rev. 5 の変更トリガーコントロールの検出結果を正確にレポートするには AWS Config 、これらのリソースを に記録する必要があります AWS Config。リソースを記録する必要があるのは、変更がトリガーされたスケジュールタイプのあるコントロールのリソースだけです。この標準の詳細については、「米国国立標準技術研究所 (NIST) SP 800-53 Rev. 5」を参照してください。

サービス	必要なリソース
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint`
	`AWS::DMS::ReplicationInstance`
	`AWS::DMS::ReplicationTask`

サービス	必要なリソース
Amazon DynamoDB	`AWS::DynamoDB::Table`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`
	`AWS::EC2::EIP`
	`AWS::EC2::Instance`
	`AWS::EC2::LaunchTemplate`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::TransitGateway`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`

サービス	必要なリソース
Amazon EKS	`AWS::EKS::Cluster`
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EventBridge	`AWS::Events::Endpoint` `AWS::Events::EventBus`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MSK	`AWS::MSK::Cluster`
Amazon MQ	`AWS::AmazonMQ::Broker`

サービス	必要なリソース
AWS Network Firewall	AWS::NetworkFirewall::Firewall AWS::NetworkFirewall::FirewallPolicy AWS::NetworkFirewall::RuleGroup
Amazon OpenSearch サービス	AWS::OpenSearch::Domain
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBCluster AWS::RDS::DBClusterSnapshot AWS::RDS::DBInstance AWS::RDS::DBSnapshot AWS::RDS::EventSubscription
Amazon Redshift	AWS::Redshift::Cluster
Amazon Route 53	AWS::Route53::HostedZone
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccountPublicAccessBlock AWS::S3::AccessPoint AWS::S3::Bucket
AWS Service Catalog	AWS::ServiceCatalog::Portfolio
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue

サービス	必要なリソース

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

Amazon SageMaker	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`

AWS WAF	`AWS::WAF::Rule`
	`AWS::WAF::RuleGroup`
	`AWS::WAF::WebACL`
	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::RuleGroup`
	`AWS::WAFv2::WebACL`

PCI DSS v3.2.1 に必要なリソース

Security Hub が AWS Config ルールを使用する有効な Payment Card Industry Data Security Standard (PCI DSS) コントロールの検出結果を正確にレポートするには、これらのリソースを に記録する必要があります AWS Config。この標準の詳細については、「Payment Card Industry Data Security Standard (PCI DSS)」を参照してください。

サービス	必要なリソース
AWS CodeBuild	`AWS::CodeBuild::Project`

サービス	必要なリソース

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::EIP`
	`AWS::EC2::Instance`
	`AWS::EC2::SecurityGroup`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` `AWS::IAM::User`
AWS Lambda	`AWS::Lambda::Function`
Amazon OpenSearch サービス	`AWS::OpenSearch::Domain`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccountPublicAccessBlock` `AWS::S3::Bucket`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

リソースタグ付け標準に必要な AWS リソース

AWS Resource Tagging Standard のすべてのコントロールは変更がトリガーされ、 AWS Config ルールを使用します。Security Hub がこれらのコントロールの検出結果を正確にレポートするには、次のリソースを に記録する必要があります AWS Config。リソースを記録する必要があるのは、変更がトリガーされたスケジュールタイプのあるコントロールのリソースだけです。この標準の詳細については、「AWS リソースタグ付け標準」を参照してください。

サービス	必要なリソース
AWS AppSync	`AWS::AppSync::GraphQLApi`
Amazon Athena	`AWS::Athena::DataCatalog` `AWS::Athena::WorkGroup`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`

AWS Backup (AWS Backup)	`AWS::Backup::BackupPlan`
	`AWS::Backup::BackupVault`
	`AWS::Backup::RecoveryPlan`
	`AWS::Backup::ReportPlan`

AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CloudTrail	`AWS::CloudTrail::Trail`
AWS CodeArtifact	`AWS::CodeArtifact::Repository`
Amazon Detective	`AWS::Detective::Graph`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate`
	`AWS::DMS::EventSubscription`
	`AWS::DMS::ReplicationInstance`

サービス	必要なリソース
	`AWS::DMS::ReplicationSubnetGroup`
Amazon DynamoDB	`AWS::DynamoDB::Trail`

サービス	必要なリソース
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::CustomerGateway AWS::EC2::EIP AWS::EC2::FlowLog AWS::EC2::Instance AWS::EC2::InternetGateway AWS::EC2::NatGateway AWS::EC2::NetworkAcl AWS::EC2::NetworkInterface AWS::EC2::RouteTable AWS::EC2::SecurityGroup AWS::EC2::Subnet AWS::EC2::TransitGateway AWS::EC2::TransitGatewayAttachment AWS::EC2::TransitGatewayRouteTable AWS::EC2::Volume AWS::EC2::VPC AWS::EC2::VPCEndpointService AWS::EC2::VPCPeeringConnection AWS::EC2::VPNGateway

サービス	必要なリソース
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster` `AWS::EKS::IdentityProviderConfig`
AWS Elastic Beanstalk (Elastic Beanstalk)	`AWS::ElasticBeanstalk::Environment`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EventBridge	`AWS::Events::EventBus`
AWS Global Accelerator	`AWS::GlobalAccelerator::Accelerator`
AWS Glue	`AWS::Glue::Job`

Amazon GuardDuty	`AWS::GuardDuty::Detector`
	`AWS::GuardDuty::Filter`
	`AWS::GuardDuty::IPSet`

AWS Identity and Access Management (IAM)	`AWS::IAM::Role` `AWS::IAM::User`

サービス	必要なリソース
AWS Identity and Access Management Access Analyzer (IAM Access Analyzer)	`AWS::AccessAnalyzer::Analyzer`

AWS IoT	`AWS::IoT::Authorizer`
	`AWS::IoT::Dimension`
	`AWS::IoT::MitigationAction`
	`AWS::IoT::Policy`
	`AWS::IoT::RoleAlias`
	`AWS::IoT::SecurityProfile`

Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` `AWS::NetworkFirewall::FirewallPolicy`
Amazon OpenSearch サービス	`AWS::OpenSearch::Domain`

Amazon Relational Database Service	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSecurityGroup`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::DBSubnetGroup`

サービス	必要なリソース

Amazon Redshift	`AWS::Redshift::Cluster`
	`AWS::Redshift::ClusterSnapshot`
	`AWS::Redshift::ClusterSubnetGroup`
	`AWS::Redshift::EventSubscription`

Amazon Route 53	`AWS::Route53::HealthCheck`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet` `AWS::SES::ContactList`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
AWS Step Functions	`AWS::StepFunctions::Activity`
AWS Transfer Family	`AWS::Transfer::Workflow`

サービスマネージドスタンダードに必要なリソース： AWS Control Tower

Security Hub が AWS Config ルールを使用する有効なサービスマネージドスタンダード： AWS Control Tower 変更トリガーコントロールの検出結果を正確にレポートするには、次のリソースを に記録する必要があります AWS Config。この標準の詳細については、「サービスマネージドスタンダード： AWS Control Tower」を参照してください。

サービス	必要なリソース
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`

サービス	必要なリソース
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CodeBuild	`AWS::CodeBuild::Project`
Amazon DynamoDB	`AWS::DynamoDB::Table`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::Instance`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`

サービス	必要なリソース
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` `AWS::NetworkFirewall::RuleGroup`
Amazon OpenSearch サービス	`AWS::OpenSearch::Domain`

サービス	必要なリソース

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccountPublicAccessBlock` `AWS::S3::Bucket`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

AWS Secrets Manager	`AWS::SecretsManager::Secret`

AWS WAF	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::WebACL`

セキュリティチェックの実行スケジュール

セキュリティ標準を有効にすると、 は 2 時間以内にすべてのチェックの実行 AWS Security Hub を開始します。ほとんどのチェックは 25 分以内に実行開始されます。Security Hub は、コントロールの基礎となるルールを評価することによってチェックを実行します。コントロールのチェックの最初の実行が完了するまで、ステータスは [No data] (データなし) です。

新しい標準を有効にすると、Security Hub は、他の有効な標準で有効になっているコントロールと同じ基盤となる AWS Config サービスにリンクされたルールを使用するコントロールの検出結果を生成するまでに最大 24 時間かかる場合があります。例えば、 AWS Foundational Security Best Practices (FSBP) 標準で Lambda.1 を有効にすると、Security Hub はサービスにリンクされたルールを作成し、通常は数分で結果を生成します。その後、Payment Card Industry Data Security Standard (PCI DSS) で Lambda.1 を有効にすると、Security Hub は Lambda.1 と同じサービスリンクルールを使用するため、このコントロールの検出結果を生成するまでに最大 24 時間かかります。

最初のチェックの後、各コントロールのスケジュールは、定期的に実行されるか、変更によってトリガーされます。

- 定期的なチェック – このチェックは、最後の実行から 12 時間または 24 時間以内に自動的に実行されます。周期は Security Hub によって決定され、変更はできません。定期的なコントロールは、チェック実行時の評価を反映したものになります。定期的な統制結果のワークフローステータスを更新し、次のチェックで検出結果のコンプライアンスステータスが同じままであっても、ワークフローステータスは変更された状態のままです。例えば、KMS.4 の AWS KMS key ローテーションに失敗した検出結果がある場合、 を有効にしてから検出結果を修正すると、Security Hub はワークフローステータスを から NEWに変更しますRESOLVED。次の定期チェックの前に KMS キーローテーションを無効にすると、検出結果のワークフローステータスは RESOLVED のままになります。
- 変更によってトリガーされるチェック — これらのチェックは、関連するリソースの状態が変更されたときに実行されます。リソースの状態の変化を継続的に記録するか、毎日記録 AWS Config するかを選択します。日次記録を選択した場合、 は、リソースの状態に変更があった場合に、24 時間ごとにリソース設定データを AWS Config 配信します。変化がなければ、データは配信されません。これにより、24 時間経過するまで、Security Hub の検出結果の生成が遅れる場合があります。選択した記録期間に関係なく、Security Hub AWS Config は 18 時間ごとに をチェックして、からのリソースの更新が見逃されていないことを確認します。

一般的に、Security Hub は、可能な限り、チェックが変更によってトリガーされるルールを使用します。リソースが変更によってトリガーされるルールを使用するには、 AWS Config 設定項目をサポートしている必要があります。

マネージド AWS Config ルールに基づくコントロールの場合、コントロールの説明には、 AWS Config デベロッパーガイドのルールの説明へのリンクが含まれます。この説明には、ルールが変更によってトリガーされるか、定期的に実行されるかについての記述が含まれます。

Security Hub カスタム Lambda 関数を使用するチェックは、定期的に実行されます。

コントロールの結果を生成および更新する

AWS Security Hub は、セキュリティコントロールに対するチェックを実行して検出結果を生成します。これらの検出結果は AWS Security Finding 形式 (ASFF) を使用します。結果のサイズが最大 240 KB を超えると、`Resource.Details` オブジェクトが削除されます。リソースによって AWS Config バックアップされるコントロールについては、 AWS Config コンソールでリソースの詳細を表示できます。

Security Hub は通常、コントロールのセキュリティチェックごとに課金されます。ただし、複数のコントロールが同じ AWS Config ルールを使用する場合、Security Hub は AWS Config ルールに対するチェックごとに 1 回のみ課金します。[統合されたコントロールの検出結果] を有効にすると、コントロールが複数の有効化された標準に含まれている場合でも、Security Hub はセキュリティチェックに対して単一の検出結果を生成します。

例えば、この AWS Config ルール`iam-password-policy`は、Center for Internet Security (CIS) AWS Foundations Benchmark 標準および Foundational Security Best Practices 標準の複数のコントロールで使用されます。Security Hub がその AWS Config ルールに対してチェックを実行するたびに、関連するコントロールごとに個別の検出結果が生成されますが、チェックに対して課金されるのは 1 回だけです。

統合されたコントロールの検出結果

アカウントで [統合されたコントロールの検出結果] を有効にすると、コントロールが複数の有効化された標準に適用されている場合でも、Security Hub はコントロールのセキュリティチェックごとに単一の検出結果または検出結果の更新を生成します。コントロールとそれらが適用される標準の一覧については、「Security Hub コントロールのリファレンス」を参照してください。[統合されたコントロールの検出結果] は、有効と無効を切り替えることができます。検出結果のノイズを減らすため、オンにすることをお勧めします。

2023 年 2 月 23 日より AWS アカウント 前に で Security Hub を有効にした場合は、このセクションの後半の手順に従って統合統制結果を有効にする必要があります。2023 年 2 月 23 日以降に Security Hub を有効にすると、[統合されたコントロールの検出結果] がアカウントで自動的に有効になります。ただし、Security Hub の AWS Organizationsとの統合を使用するか、手動の招待プロセスで招待されたメンバーアカウントを使用する場合、メンバーアカウントで [統合されたコントロールの検出結果] が有効になるのは、管理者アカウントで有効になっている場合のみです。管理者アカウントでこの機能が無効になっている場合、メンバーアカウントも無効になります。この挙動は、新規および既存のメンバーアカウントに適用されます。

アカウントで [統合されたコントロールの検出結果] を無効にすると、Security Hub は、コントロールを含む有効な各標準の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。例えば、有効な 4 つの標準が同じ基盤となる AWS Config ルールとコントロールを共有する場合、コントロールのセキュリティチェック後に 4 つの個別の検出結果を受け取ります。[統合されたコントロールの検出結果] を有効にすると、検出結果が 1 つのみになります。統合が検出結果に与える影響の詳細については、「コントロールの検出結果のサンプル」を参照してください。

[統合されたコントロールの検出結果] を有効にすると、Security Hub は標準と別に新しい検出結果を生成し、元の標準ベースの検出結果をアーカイブします。一部のコントロールの検出結果フィールドや値が変更され、既存のワークフローに影響を与える可能性があります。これらの変更の詳細については、「統合されたコントロールの検出結果 — ASFF の変更」を参照してください。

[統合されたコントロールの検出結果] を有効にすると、[サードパーティの統合] が Security Hub から受け取る検出結果にも影響する可能性があります。AWS v2.0.0 の自動セキュリティレスポンスは、統合統制結果をサポートします。

[統合されたコントロールの検出結果] を有効にする

[統合されたコントロールの検出結果] を有効にするには、管理者アカウントまたはスタンドアロンアカウントにサインインする必要があります。

> **Note**
>
> [統合されたコントロールの検出結果] を有効にした後、Security Hub が新しい統合された検出結果を生成し、元の標準ベースの検出結果をアーカイブするまで、最大 24 時間かかります。その間、アカウントには、標準に依存しない検出結果と標準に基づく検出結果が混在する可能性があります。

Security Hub console

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. ナビゲーションペインで 設定 を選択します。
3. [General] (全般) タブを選択します。
4. [Controls] (コントロール) については、[Consolidated control findings] (統合統制結果) をオンにします。
5. [保存] を選択します。

Security Hub API

1. UpdateSecurityHubConfiguration を実行します。
2. `ControlFindingGenerator` を `SECURITY_CONTROL` と等しい値に設定します。

   リクエストの例:

```
{
   "ControlFindingGenerator": "SECURITY_CONTROL"
}
```

AWS CLI

1. update-security-hub-configuration コマンドを実行します。
2. `control-finding-generator` を `SECURITY_CONTROL` と等しい値に設定します。

```
aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

[統合されたコントロールの検出結果] を無効にする

[統合されたコントロールの検出結果] を無効にするには、管理者アカウントまたはスタンドアロンアカウントにサインインする必要があります。

> **Note**
>
> [統合されたコントロールの検出結果] を無効にした後、Security Hub が新しい標準ベースの検出結果を生成し、統合された検出結果をアーカイブするまで、最大 24 時間かかります。その間、アカウントには、標準ベースの検出結果と統合された検出結果が混在する可能性があります。

Security Hub console

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. ナビゲーションペインで 設定 を選択します。
3. [General] (全般) タブを選択します。
4. [コントロール] については [編集] を選択し、[統合されたコントロールの検出結果] を無効にします。
5. [保存] を選択します。

Security Hub API

1. `UpdateSecurityHubConfiguration` を実行します。
2. `ControlFindingGenerator` を `STANDARD_CONTROL` と等しい値に設定します。

   リクエストの例:

```
{
   "ControlFindingGenerator": "STANDARD_CONTROL"
}
```

AWS CLI

1. `update-security-hub-configuration` コマンドを実行します。
2. `control-finding-generator` を `STANDARD_CONTROL` と等しい値に設定します。

```
aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

コントロールの結果の Compliance 詳細

コントロールのセキュリティチェックによって生成された検出結果の場合、 AWS Security Finding Format (ASFF) の Compliance フィールドには、コントロールの検出結果に関連する詳細が含まれます。Compliance フィールドに含まれている情報は次のとおりです。

`AssociatedStandards`

コントロールが有効になっている有効な標準です。

`RelatedRequirements`

すべての有効な標準のコントロールに関連する要件のリストです。これらは、Payment Card Industry Data Security Standard (PCI DSS) など、コントロールに関するサードパーティのセキュリティフレームワークの要件です。

`SecurityControlId`

Security Hub がサポートするセキュリティ標準全体のコントロールの識別子です。

`Status`

特定のコントロールに対して Security Hub によって実行された最新のチェックの結果です。前回のチェックの結果は 90 日間、アーカイブされた状態で保持されます。

`StatusReasons`

`Compliance.Status` の値の理由のリストが含まれています。`StatusReasons` には、理由ごとの理由コードと説明が示されます。

次の表に、使用可能な状況の理由コードと説明を示します。修正手順は、どのコントロールがその理由コードを使って検出結果を生成したかによって異なります。Security Hub コントロールのリファレンス からコントロールを選択すると、そのコントロールの修正手順が表示されます。

理由コード	Compliance.Status	説明
`CLOUDTRAIL_METRIC_FILTER_NOT_VALID`	`FAILED`	マルチリージョン CloudTrail の証跡に有効なメトリクスフィルターがありません。

理由コード	Compliance.Status	説明
CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT	FAILED	マルチリージョン証 CloudTrail 跡にはメトリクスフィルターはありません。
CLOUDTRAIL_MULTI_REGION_NOT_PRESENT	FAILED	アカウントには、必要な設定のマルチリージョン CloudTrail 証跡がありません。
CLOUDTRAIL_REGION_INVAILD	WARNING	マルチリージョンの CloudTrail 証跡が現在のリージョンにありません。
CLOUDWATCH_ALARM_ACTIONS_NOT_VALID	FAILED	有効なアラームアクションが存在しません。
CLOUDWATCH_ALARMS_NOT_PRESENT	FAILED	CloudWatch アラームはアカウントに存在しません。
CONFIG_ACCESS_DENIED	NOT_AVAILABLE	AWS Config アクセスが拒否されました。
	AWS Config ステータスは ConfigError	AWS Config が有効で、十分なアクセス許可が付与されていることを確認します。
CONFIG_EVALUATIONS_EMPTY	PASSED	AWS Config は、ルールに基づいてリソースを評価しました。 ルールがスコープ内の AWS リソースに適用されなかったか、指定されたリソースが削除されたか、評価結果が削除されました。

理由コード	Compliance.Status	説明
CONFIG_RETURNS_NOT_APPLICABLE	NOT_AVAILABLE	コンプライアンスステータスは です。これは、 が該当なし のステータスを AWS Config 返したNOT_AVAILABLE ためです。 AWS Config はステータスの理由を提供しません。ステータスが Not Applicable である理由は、以下のように考えられます。 • リソースが AWS Config ルールのスコープから削除されました。 • AWS Config ルールが削除されました。 • リソースが削除された。 • AWS Config ルールロジックは、該当なしのステータスを生成できます。

理由コード	Compliance.Status	説明
CONFIG_RULE_EVALUATION_ERROR	NOT_AVAILABLE AWS Config ステータスは ConfigError	この理由コードは、いくつかの異なる種類の評価エラーに使用されます。 説明には、具体的な理由の情報が含まれます。 エラーの種類は、次のいずれかになります。 • 許可が不足しているため、評価を実行できない。説明には、欠落している特定の許可が含まれます。 • パラメータの値が欠落しているか、無効。説明には、パラメータとパラメータ値の要件が含まれます。 • S3 バケットからの読み取り中のエラー。説明では、バケットが識別され、特定のエラーが表示されます。 • AWS サブスクリプションがありません。 • 評価の一般的なタイムアウト。 • 停止中のアカウント。
CONFIG_RULE_NOT_FOUND	NOT_AVAILABLE AWS Config ステータスは ConfigError	AWS Config ルールは作成中です。

理由コード	Compliance.Status	説明
INTERNAL_SERVICE_ERROR	NOT_AVAILABLE	不明なエラーが発生しました。
LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE	FAILED	Security Hub が カスタム Lambda ランタイムのチェックを実行できません。
S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION	WARNING	このルールに関連付けられた S3 バケットが別のリージョンまたはアカウントにあるため、結果が WARNING 状態になっています。 このルールは、クロスリージョンまたはクロスアカウントのチェックをサポートしていません。 このリージョンまたはアカウントでは、このコントロールを無効にすることをお勧めします。リソースがあるリージョンまたはアカウントでのみ実行します。
SNS_SUBSCRIPTION_NOT_PRESENT	FAILED	CloudWatch Logs メトリクスフィルターに有効な Amazon SNS サブスクリプションがありません。

理由コード	Compliance.Status	説明
SNS_TOPIC_CROSS_ACCOUNT	WARNING	結果が WARNING 状態です。 このルールに関連付けられた SNS トピックは、別のアカウントによって所有されています。現在のアカウントでは、サブスクリプション情報を取得できません。 SNS トピックを所有するアカウントは、SNS トピックへの sns:ListSubscriptionsByTopic 許可を現在のアカウントに付与する必要があります。
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	このルールに関連付けられた SNS トピックが別のリージョンまたはアカウントにあるため、結果が WARNING 状態です。 このルールは、クロスリージョンまたはクロスアカウントのチェックをサポートしていません。 このリージョンまたはアカウントでは、このコントロールを無効にすることをお勧めします。リソースがあるリージョンまたはアカウントでのみ実行します。
SNS_TOPIC_INVALID	FAILED	このルールに関連付けられている SNS トピックが無効です。
THROTTLING_ERROR	NOT_AVAILABLE	関連する API オペレーションが許可されたレートを超えました。

コントロールの結果の ProductFields 詳細

Security Hub がセキュリティチェックを実行して統制結果を生成する場合、ASFF の ProductFields 属性には次のフィールドが含まれます。

`ArchivalReasons:0/Description`

Security Hub が既存の結果をアーカイブした理由について説明します。

例えば、統制または標準を無効にしたり、統合統制結果を有効または無効にしたりすると、Security Hub は既存の結果をアーカイブします。

`ArchivalReasons:0/ReasonCode`

Security Hub が既存の結果をアーカイブした理由を示します。

例えば、統制または標準を無効にしたり、統合統制結果を有効または無効にしたりすると、Security Hub は既存の結果をアーカイブします。

`StandardsGuideArn` または `StandardsArn`

コントロールに関連付けられた標準の ARN。

CIS AWS Foundations Benchmark 標準の場合、 フィールドは ですStandardsGuideArn。

PCI DSS および AWS Foundational Security Best Practices 標準の場合、 フィールドは ですStandardsArn。

[統合されたコントロールの検出結果] を有効にすると、これらのフィールドは `Compliance.AssociatedStandards` に合わせて削除されます。

`StandardsGuideSubscriptionArn` または `StandardsSubscriptionArn`

標準へのアカウントのサブスクリプションの ARN。

CIS AWS Foundations Benchmark 標準の場合、 フィールドは ですStandardsGuideSubscriptionArn。

PCI DSS および AWS Foundational Security Best Practices 標準の場合、 フィールドは ですStandardsSubscriptionArn。

[統合されたコントロールの検出結果] を有効にすると、これらのフィールドは削除されます。

`RuleId` または `ControlId`

コントロールの識別子。

CIS AWS Foundations Benchmark 標準の場合、 フィールドは ですRuleId。

他の標準の場合、このフィールドは `ControlId` です。

[統合されたコントロールの検出結果] を有効にすると、これらのフィールドは `Compliance.SecurityControlId` に合わせて削除されます。

`RecommendationUrl`

コントロールの修復情報の URL。[統合されたコントロールの検出結果] を有効にすると、このフィールドは `Remediation.Recommendation.Url` に合わせて削除されます。

`RelatedAWSResources:0/name`

結果に関連付けられたリソースの名前。

`RelatedAWSResource:0/type`

コントロールに関連付けられたリソースのタイプ。

`StandardsControlArn`

コントロールの ARN。[統合されたコントロールの検出結果] を有効にすると、このフィールドは削除されます。

`aws/securityhub/ProductName`

コントロールベースの結果の場合、製品名は Security Hub になります。

`aws/securityhub/CompanyName`

コントロールベースの検出結果の場合、会社名は です AWS。

`aws/securityhub/annotation`

コントロールによって検出された問題の説明。

`aws/securityhub/FindingId`

結果の識別子。[統合されたコントロールの検出結果] を有効にした場合、このフィールドは標準を参照しません。

コントロール結果への重要度の割り当て

Security Hub コントロールに割り当てられる重要度は、コントロールの重要性を特定します。コントロールの重要度により、コントロールの結果に割り当てられる重要度ラベルが決まります。

重要度の基準

コントロールの重要度は、以下の基準の評価に基づいて決定されます:

- 脅威アクターがコントロールに関連する設定の弱点を利用する際の難易度

  この難易度は、弱点を利用して脅威シナリオを実行するために必要な洗練度または複雑さの度合いによって決まります。
- 弱点が AWS アカウント または リソースの侵害につながる可能性はどの程度ありますか？

  AWS アカウント または リソースの侵害は、データまたは AWS インフラストラクチャの機密性、完全性、または可用性が何らかの形で損なわれることを意味します。

  侵害の可能性は、脅威シナリオが AWS サービスまたはリソースの中断または侵害につながる可能性を示します。

例えば、次の設定の弱点について検討します。

- ユーザーアクセスキーが 90 日ごとにローテーションされません。
- IAM ルートユーザーキーが存在します。

どちらの弱点も、攻撃者が悪用する際の難易度は同程度です。両方の弱点とも、攻撃者は認証情報の盗難やその他の方法を使用してユーザーキーを取得します。その後、このユーザーキーを使用して、許可されない方法でリソースにアクセスします。

ただし、脅威アクターによって取得されたアクセスキーがルートユーザーのものである場合、よりアクセス性が高いため、侵害の可能性はより高くなります。この結果、ルートユーザーキーの弱点は、重要度が高くなります。

重要度では、基になるリソースの重大度は考慮されていません。重大度は、結果に関連付けられているリソースの重要性の程度として定義されます。例えば、ミッションクリティカルなアプリケーションに関連付けられているリソースは、非本番稼働用テストに関連付けられたリソースより重大度が高くなります。リソース重要度情報をキャプチャするには、 AWS Security Finding 形式 (ASFF) の `Criticality`フィールドを使用します。

次の表に、悪用行為の難易度と、セキュリティラベルが侵害される可能性を示します。

	侵害の可能性が非常に高い	侵害の可能性が高い	侵害の可能性が低い	侵害の可能性が非常に低い
悪用行為が非常に簡単	重大	重大	高	中
悪用行為がやや簡単	重大	高	中	中
悪用行為がやや難しい	高	中	中	低
悪用行為が非常に難しい	中	中	低	低

重要度の定義

重要度ラベルは次のように定義されています。

重大 - この問題は、さらに悪化しないように直ちに修復する必要があります。

例えば、公開された S3 バケットは重大な重要度の結果と考えられます。非常に多くの脅威アクターによって、公開された S3 バケットがスキャンされるため、公開された S3 バケット内のデータは、他者によって発見およびアクセスされる可能性があります。

一般に、パブリックにアクセス可能なリソースは、セキュリティ上の重大な問題と見なされます。重大な結果への対応は、緊急性が最も高くなります。また、リソースの重大度も考慮する必要があります。

高 - この問題は短期的な優先事項として対処する必要があります。

例えば、デフォルトの VPC セキュリティグループがインバウンドおよびアウトバウンドトラフィックに対して開かれている場合、重要度が高いと考えられます。脅威アクターがこの方法を使用して VPC を侵害することは、やや簡単であるためです。また、脅威アクターが VPC 内に侵入すると、リソースを中断または流出させる可能性があります。

Security Hub では、重要度の高い結果を短期的な優先事項として扱うことを推奨しています。すぐに修復手順を実行する必要があります。また、リソースの重大度も考慮する必要があります。

中 - この問題は、中期的な優先事項として対処する必要があります。

例えば、転送中のデータの暗号化が欠如している場合、重要度が中程度の結果と考えられます。この弱点を利用するには、高度な man-in-the-middle 攻撃が必要です。つまり、やや難しい攻撃手法です。脅威シナリオが成功すると、一部のデータが侵害される可能性があります。

Security Hub では、できるだけ早く、関連するリソースを調査することを推奨しています。また、リソースの重大度も考慮する必要があります。

低 - この問題には、独自のアクションは必要ありません。

例えば、フォレンジック情報の収集に失敗した場合、重要度が低いと考えられます。この管理は将来の侵害を防ぐのに役立ちますが、フォレンジックが実行されない限り、侵害に直接つながりません。

重要度の低い結果については、すぐにアクションを実行する必要はありませんが、他の問題と相関関係がある場合は、コンテキストを入手できます。

情報 - 設定の弱点は見つかりませんでした。

つまり、ステータスは PASSED、WARNING、または NOT AVAILABLE です。

推奨されるアクションはありません。通知目的の結果は、顧客が準拠状態であることを実証するのに役立ちます。

コントロールの結果を更新するためのルール

特定のルールで後続のチェックを行うと、新しい結果が生成される場合があります。例えば、「ルートユーザーの使用を避ける」のステータスが FAILED から PASSED に変更される場合があります。この場合、最新の結果を含む新しい結果が生成されます。

指定されたルールで行われた後続のチェックで結果が生成され、その結果が現在の結果と同じ場合、既存の結果が更新されます。新しい結果は生成されません。

Security Hub では、関連付けられたリソースが削除されたか、リソースが存在しないか、コントロールが無効になっている場合、コントロールから結果を自動的にアーカイブします。関連付けられたサービスが現在使用されていないため、リソースがすでに存在しない可能性もあります。結果は、次のいずれかの基準に基づいて自動的にアーカイブされます:

- 結果が 3~5 日間更新されていません (これはベスト工フォートであり、保証されません)。
- 関連付けられた AWS Config 評価が を返しましたNOT_APPLICABLE。

コンプライアンスステータスとコントロールステータス

AWS Security Finding 形式の Compliance.Statusフィールドは、コントロール結果の結果を記述します。Security Hub は、コントロール検出結果のコンプライアンス状況を使用して、全体的なコントロールステータスを決定します。コントロールのステータスは、Security Hub コンソールのコントロールの詳細ページに表示されます。

管理者アカウントの場合、コントロールステータスには管理者アカウントとメンバーアカウントのコントロールステータスが反映されます。具体的には、コントロールの全体的なステータスは、管理者アカウントまたはメンバーアカウントに 1 つ以上の失敗した検出結果がある場合、失敗と表示されます。集約リージョンを設定している場合、集約リージョンのコントロールステータスには、集約リージョンとリンクされたリージョンのコントロールステータスが反映されます。具体的には、コントロールの全体的なステータスは、集約リージョンまたはリンクされたリージョンのいずれかに失敗した検出結果が 1 つ以上ある場合、失敗と表示されます。

Security Hub は通常、Security Hub コンソールの 概要ページまたはセキュリティ標準ページに初めてアクセスしてから 30 分以内に初期コントロールステータスを生成します。コントロールステータスを表示するには、AWS Config リソース記録を設定する必要があります。コントロールステータスが初めて生成されると、Security Hub は過去 24 時間の結果に基づいて 24 時間ごとにコントロールステータスを更新します。コントロールの詳細ページのタイムスタンプは、コントロールステータスが最後に更新された日時を示します。

> **Note**
>
> 有効にしてから、最初のコントロールステータスのコントロールが中国リージョンと AWS GovCloud (US) Regionで生成されるまで、最大で 24 時間かかります。

結果のコンプライアンスステータスの値

各結果のコンプライアンスステータスには、次のいずれかの値が割り当てられています。

- PASSED – コントロールがこの検出結果のセキュリティチェックに合格したことを示します。Security Hub を自動的に Workflow.Status に設定しますRESOLVED。

  結果の Compliance.Status が PASSED から FAILED、WARNING、または NOT_AVAILABLE に変更され、かつ Workflow.Status が NOTIFIED または RESOLVED の場合、Security Hub は Workflow.Status を NEW に自動的に設定します。

コントロールに対応するリソースがない場合、Security Hub はアカウントレベルでPASSED結果を生成します。コントロールに対応するリソースがあるが、そのリソースを削除すると、Security Hub は検出NOT_AVAILABLE結果を作成し、すぐにアーカイブします。18 時間後、コントロールに対応するリソースがなくなったため、PASSED結果が表示されます。

- FAILED – コントロールがこの検出結果のセキュリティチェックに合格しなかったことを示します。
- WARNING – チェックが完了したことを示しますが、Security Hub はリソースが PASSEDまたは FAILED状態であるかどうかを判断できません。
- NOT_AVAILABLE – サーバーが失敗したか、リソースが削除されたか、 AWS Config 評価の結果がであったため、チェックを完了できないことを示しますNOT_APPLICABLE。

  AWS Config 評価結果が の場合NOT_APPLICABLE、Security Hub は自動的に結果をアーカイブします。

コントロールステータスの値

Security Hub は、コントロールの検出結果のコンプライアンスステータスから全体的なコントロールステータスを取得します。コントロールステータスを決定する際、Security Hub は が RecordStateである検出結果ARCHIVEDと が Workflow.Statusである検出結果を無視しますSUPPRESSED。

コントロールステータスには、次のいずれかの値が割り当てられています。

- 合格 – すべての検出結果のコンプライアンスステータスが であることを示しますPASSED。
- Failed – 少なくとも 1 つの検出結果のコンプライアンスステータスが であることを示しますFAILED。
- Unknown – 少なくとも 1 つの検出結果のコンプライアンスステータスが WARNINGまたは であることを示しますNOT_AVAILABLE。コンプライアンスステータスが の検出結果はありませんFAILED。
- データなし - コントロールの結果がないことを示します。例えば、新しく有効化されたコントロールは、Security Hub がその検出結果の生成を開始するまで、このステータスになります。コントロールは、すべての検出結果が である場合、SUPPRESSEDまたは現在のリージョンで使用できない場合も、このステータスになります。
- 無効 — 現在のアカウントとリージョンでコントロールが無効になっていることを示します。現在のアカウントとリージョンでは、このコントロールに対して現在セキュリティチェックは実行され

ていません。ただし、無効化されたコントロールの検出結果には、無効化後最大 24 時間のコンプライアンスステータスの値が含まれる場合があります。

セキュリティスコアの決定

Security Hub コンソールの [概要] ページと [コントロール] ページには、有効になっているすべての標準のセキュリティスコアの概要が表示されます。[セキュリティ基準] ページで、Security Hub は有効な標準別に 0〜100% のセキュリティスコアをも表示します。

Security Hub を初めて有効にすると、Security Hub は、Security Hub コンソールの [概要] ページまたは [セキュリティ基準] ページへの最初のアクセスから 30 分以内にセキュリティスコアの概要と標準のセキュリティスコアを計算します。スコアは、これらのページにアクセスしたときに有効になっている標準に対してのみ生成されます。現在有効になっている標準のリストを表示するには、`GetEnabledStandards` API オペレーションを呼び出します。さらに、スコアが表示されるように AWS Config リソース記録を設定する必要があります。セキュリティスコアの概要は、標準のセキュリティスコアの平均値です。

最初のスコア生成の後、Security Hub はセキュリティスコアを 24 時間ごとに更新します。Security Hub には、セキュリティスコアが最後に更新されたときの時刻が表示されます。

> **Note**
>
> 中国リージョンおよび AWS GovCloud (US) Regionでは、最初のセキュリティスコアが作成されるまで、最大 24 時間かかる場合があります。

統合コントロールの検出結果を有効にしている場合、セキュリティスコアが更新されるまで、最大 24 時間かかります。さらに、新しい集約リージョンの有効化や、リンクされたリージョンの更新を行うと、既存のセキュリティスコアがリセットされます。Security Hub では、更新されたリージョンのデータを含む新しいセキュリティスコアを生成するまでに、最大 24 時間かかります。

セキュリティスコアの計算方法

セキュリティスコアは、有効になっているコントロールのうち、合格の状態にあるコントロールの割合を示します。スコアは、小数点以下を最も近い整数に四捨五入したパーセンテージで表示されます。

Security Hub は、有効なすべての標準でセキュリティスコアの要約を計算します。Security Hub では、有効な標準ごとにセキュリティ スコアも計算されます。スコアの計算に使用可能なコントロー

ルには、[合格]、[失敗]、および [不明] のステータスが付いたコントロールが含まれます。ステータスが [データなし] のコントロールはスコア計算から除外されます。

Security Hub は、コントロールステータスを計算するときに、アーカイブされた検出結果と抑制された検出結果を無視します。これはセキュリティスコアに影響する可能性があります。例えば、あるコントロールで失敗した検出結果をすべて抑制すると、そのステータスは「合格」になり、セキュリティスコアが向上する可能性があります。コントロールステータスの詳細については、コンプライアンスステータスとコントロールステータス を参照してください。

スコアリングの例:

標準	合格コントロール	失敗コントロール	未知のコントロール	標準スコア
AWS Foundational Security Best Practices v1.0.0	168	22	0	88%
CIS AWS Foundations Benchmark v1.4.0	8	29	0	22%
CIS AWS Foundations Benchmark v1.2.0	6	35	0	15%
NIST 特別刊行物 800-53 リビジョン 5	159	56	0	74%
PCI DSS v3.2.1	28	17	0	62%

セキュリティスコアの概要を計算する際、Security Hub は各コントロールを標準全体で一度だけカウントします。例えば、有効な 3 つの標準に適用されるコントロールを有効にした場合、スコアの対象となるのは有効な 1 つのコントロールとしてのみカウントされます。

この例の場合、有効になっている標準全体で有効になっているコントロールの総数は 528 ですが、Security Hub は各固有のコントロールをスコア対象として、1 回だけカウントします。有効になっている固有のコントロール数は 528 よりもおそらく少ないはずです。有効になっている固有のコントロール数が 515 で、通過した固有のコントロール数が 357 であると仮定すると、概要スコアは 69% になります。このスコアは、通過した固有のコントロール数を、有効なコントロールの総数で割って計算されます。

現在のリージョンのアカウントで有効化した標準が 1 つのみの場合でも、概要スコアが標準セキュリティスコアと異なる可能性があります。これは、管理者アカウントにサインインしており、メンバーアカウントが追加の標準または異なる標準を有効化している場合に発生することがあります。また、集約リージョンのスコアを表示しており、リンクされたリージョンで追加の標準または異なる標準が有効化されている場合にも発生することがあります。

管理者アカウントのセキュリティスコア

管理者アカウントにログインしている場合、概要セキュリティスコアと標準スコアは、管理者アカウントおよびメンバーアカウントのすべてのコントロールステータスを考慮したものになります。

1 つのメンバーアカウントでコントロールのステータスが [失敗] の場合、管理者アカウントのステータスは [失敗] となり、管理者アカウントのスコアに影響を与えます。

管理者アカウントにログインしていて、集約リージョンを考慮したものになっている場合、セキュリティスコアは、すべてのメンバーアカウントおよびリンクされているすべてのリージョンを考慮したものになります。

集約リージョンを設定している場合のセキュリティスコア

集約 を設定している場合 AWS リージョン、セキュリティスコアの概要と標準スコアは、すべてのコントロールステータスを考慮します。
リンクされたリージョン。

制御のステータスが 1 つのリンクされたリージョンでも [失敗] の場合、そのステータスは集約リージョンで [失敗] となり、集約リージョンスコアに影響を与えます。

管理者アカウントにログインしていて、集約リージョンを考慮したものになっている場合、セキュリティスコアは、すべてのメンバーアカウントおよびリンクされているすべてのリージョンを考慮したものになります。

Security Hub 標準のリファレンス

AWS Security Hub は現在、このセクションで説明されているセキュリティ標準をサポートしています。

標準を選択すると、その標準の詳細と適用されるコントロールが表示されます。

Security Hub の標準とコントロールは、規制のフレームワークや監査への準拠を保証するものではありません。コントロールは、 AWS アカウント とリソースの現在の状態をモニタリングする方法を提供します。

サポートされている標準

- AWS Foundational Security Best Practices (FSBP) 標準
- CIS AWS Foundations Benchmark
- 米国国立標準技術研究所 (NIST) SP 800-53 Rev. 5
- Payment Card Industry Data Security Standard (PCI DSS)
- AWS リソースタグ付け標準
- サービスマネージドスタンダード

AWS Foundational Security Best Practices (FSBP) 標準

AWS Foundational Security Best Practices 標準は、 AWS アカウント および 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場合に検出する一連のコントロールです。

この標準により、 AWS アカウント と のすべての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する領域をすばやく特定できます。組織のセキュリティ体制を改善および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、リソースに対するセキュリティのベストプラクティスが含まれます。また、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、「the section called “コントロールのカテゴリ”」を参照してください。

FSBP 標準に適用されるコントロール。

[Account.1] のセキュリティ連絡先情報を に提供する必要があります AWS アカウント

[ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります

[ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります

[APIGateway.1] API Gateway REST と WebSocket API 実行の口グ記録を有効にする必要があります

[APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります

[APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります

[APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります

[APIGateway.5] API Gateway REST API のキャッシュデータは、保管中に暗号化する必要があります

[APIGateway.8] API Gateway ルートには認証タイプを指定する必要があります

[APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります

〔AppSync.2] フィールドレベルの口グ記録を有効にする AWS AppSync 必要があります

〔AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください

〔AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要があります

〔AutoScaling.2] Amazon EC2 Auto Scaling グループは複数のアベイラビリティーゾーンをカバーする必要があります

〔AutoScaling.3] Auto Scaling グループの起動設定では、インスタンスメタデータサービスバージョン 2 (IMDSv2) を要求するように EC2 インスタンスを設定する必要がありますIMDSv2

[Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません

〔AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります

〔AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります

[EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします

[EC2.19] セキュリティグループは、リスクの高いポートへの無制限アクセスを許可してはいけません

[EC2.20] AWS Site-to-Site VPN 接続の両方の VPN トンネルが稼働している必要があります

[EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります

[EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします

[EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします

[EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします

[EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります

[ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります

[ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります

[ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります

[ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。

[ECS.2] ECS サービスには、パブリック IP アドレスを自動で割り当てないでください

[ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください

[ECS.4] ECS コンテナは、非特権として実行する必要があります

[ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。

[ECS.8] シークレットは、コンテナ環境の変数として渡さないでください

[ECS.9] ECS タスク定義には口グ設定が必要です。

[ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。

[ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります

[EFS .1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS

[EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります

[EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります

[EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります

[EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません

[EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります

[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。

[EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります

[EKS.8] EKS クラスターでは、監査口グ記録が有効になっている必要があります

〔ElastiCache.1] ElastiCache Redis クラスターでは自動バックアップを有効にする必要があります

〔ElastiCache.2]Redis キャッシュクラスター ElastiCache では、マイナーバージョン自動アップグレードを有効にする必要があります

Redis ElastiCache レプリケーショングループの [ElastiCache.3] では、自動フェイルオーバーを有効にする必要があります

〔ElastiCache.4] ElastiCache for Redis レプリケーショングループは保管時に暗号化する必要があります

Redis ElastiCache レプリケーショングループの [ElastiCache.5] は転送中に暗号化する必要があります

〔ElastiCache.6]バージョン ElastiCache 6.0 より前の Redis レプリケーショングループでは、Redis AUTH を使用する必要があります

〔ElastiCache.7] ElastiCache クラスターはデフォルトのサブネットグループを使用しないでください

〔ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります

〔ElasticBeanstalk.2] Elastic Beanstalk マネージドプラットフォームの更新を有効にする必要があります

〔ElasticBeanstalk.3] Elastic Beanstalk はログを にストリーミングする必要があります CloudWatch

[ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります

[ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager

[ELB.3] Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります

[ELB.4] Application Load Balancer は、http ヘッダーを削除するように設定する必要があります

[ELB.5] アプリケーションおよび Classic Load Balancer のログ記録を有効にする必要があります

[ELB.6] Application、Gateway、Network Load Balancer では、削除保護を有効にする必要があります

[ELB.7] Classic Load Balancers は、Connection Draining を有効にする必要があります

[ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な AWS Config設定を持つ事前定義されたセキュリティポリシーを使用する必要があります

[ELB.9] Classic Load Balancer では、クロスゾーンロードバランシングが有効になっている必要があります

[ELB.10] Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります

[ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります

[ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります

[ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります

[EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります

[EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります

[ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります

[ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります

[ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります

[ES.4] Logs への Elasticsearch CloudWatch ドメインエラーのログ記録を有効にする必要があります

[ES.5] Elasticsearch ドメインで監査ログ記録が有効になっている必要があります

[ES.6] Elasticsearch ドメインには少なくとも 3 つのデータノードが必要です

[ES.7] Elasticsearch ドメインは、少なくとも 3 つの専用マスターノードを設定する必要があります。

[ES.8] Elasticsearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります

〔EventBridge.3] EventBridge カスタムイベントバスには、リソースベースのポリシーがアタッチされている必要があります

[FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります

[FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります

〔GuardDuty.1] GuardDuty を有効にする必要があります

[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください

[IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください

[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります

[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません

[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります

[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります

[IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です

[IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります

[IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません

[Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります

[KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください

[KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください

[KMS.3] 意図せずに削除 AWS KMS keys しないでください

[Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります

[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります

[Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります

[Macie.1] Amazon Macie を有効にする必要があります

[Macie.2] Macie 自動機密データ検出を有効にする必要があります

[MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch

[MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります

[MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります

[Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります

[Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります

[Neptune.3] Neptune DB クラススナップショットはパブリックにしないでください

[Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります

[Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります

[Neptune.6] Neptune DB クラススナップショットは、保管中に暗号化する必要があります

[Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります

[Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります

〔NetworkFirewall.2] Network Firewall のログ記録を有効にする必要があります

〔NetworkFirewall.3] Network Firewall ポリシーには、少なくとも 1 つのルールグループが関連付けられている必要があります

〔NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、フルパケットに対してドロップまたは転送する必要があります

〔NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、フラグメント化されたパケットに対してドロップまたは転送する必要があります

〔NetworkFirewall.6] ステートレス Network Firewall ルールグループは空にしないでください

〔NetworkFirewall.9] Network Firewall ファイアウォールでは、削除保護を有効にする必要があります

[Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります

[Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません

[Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります

[Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります

[Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります

[Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です

[Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります

[Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります

[Opensearch.10] OpenSearch ドメインには最新のソフトウェア更新がインストールされている必要があります

[PCA.1] AWS Private CA ルート認証機関を無効にする必要があります

[Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります

[RDS.1] RDS スナップショットはプライベートである必要があります

[RDS.2] RDS DB インスタンスは、 PubliclyAccessible AWS Config設定によって決定されるパブリックアクセスを禁止する必要があります

[RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。

[RDS.4] RDS クラスタースナップショットとデータベーススナップショットは保管中に暗号化する必要があります

[RDS.5] RDS DB インスタンスは、複数のアベイラビリティーゾーンで設定する必要があります

[RDS.6] RDS DB インスタンスの拡張モニタリングを設定する必要があります

[RDS.7] RDS クラスターでは、削除保護が有効になっている必要があります

[RDS.8] RDS DB インスタンスで、削除保護が有効になっている必要があります

[RDS.9] RDS DB インスタンスはログを CloudWatch Logs に発行する必要があります

[RDS.10] IAM 認証は RDS インスタンス用に設定する必要があります

[RDS.11] RDS インスタンスでは、自動バックアップが有効になっている必要があります

[RDS.12] IAM 認証は RDS クラスター用に設定する必要があります

[RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります

[RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります

[RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります

[RDS.16] タグをスナップショットにコピーするように RDS DB クラスターを設定する必要があります

[RDS.17] RDS DB インスタンスは、タグをスナップショットにコピーするように設定する必要があります

[RDS.18] RDS インスタンスは VPC 内にデプロイする必要があります

[RDS.19] 重大なクラスターイベントについて、既存の RDS イベント通知サブスクリプションを設定する必要があります

[RDS.20] 重大なデータベースインスタンスイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります

[RDS.21] 重大なデータベースパラメータグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります

[RDS.22] 重大なデータベースセキュリティグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります

[RDS.23] RDS インスタンスはデータベースエンジンのデフォルトポートを使用しないようにする必要があります

[RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります

[RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります

[RDS.27] RDS DB クラスターは保管中に暗号化する必要があります

[RDS.34] Aurora MySQL DB クラスターは監査ログを CloudWatch Logs に発行する必要があります

[RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります

[PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります

[Redshift.2] Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります

[Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります

[Redshift.4] Amazon Redshift クラスターでは、監査ログ記録が有効になっている必要があります

[Redshift.6] Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります

[Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります

[Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください

[Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください

[Redshift.10] Redshift クラスターは保存時に暗号化する必要があります

[Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります

[S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります

[S3.2] S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります

[S3.3] S3 汎用バケットはパブリック書き込みアクセスをブロックする必要があります

[S3.5] S3 汎用バケットでは、SSL を使用するリクエストが必要です

[S3.6] S3 汎用バケットポリシーでは、他の へのアクセスを制限する必要があります AWS アカウント

[S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります

[S3.9] S3 汎用バケットでは、サーバーアクセスのログ記録を有効にする必要があります

[S3.12] ACLs を使用しないでください S3

[S3.13] S3 汎用バケットにはライフサイクル設定が必要です

[S3.19] S3 アクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります

〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません

〔SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります

〔SageMaker.3] SageMaker ユーザーはノートブックインスタンスへのルートアクセスを許可されない

〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります

〔SecretsManager.1] Secrets Manager シークレットでは、自動ローテーションを有効にする必要があります

〔SecretsManager.2] 自動ローテーションで設定された Secrets Manager シークレットは正常にローテーションする必要があります

〔SecretsManager.3] 未使用の Secrets Manager シークレットを削除する

〔SecretsManager.4] Secrets Manager のシークレットは、指定された日数内にローテーションする必要があります

〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります

[SQS.1] Amazon SQS キューは保管中に暗号化する必要があります

[SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager

[SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります

[SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります

[SSM.4] SSM ドキュメントはパブリックにしないでください

〔StepFunctions.1] Step Functions ステートマシンでは ログ記録が有効になっている必要があります

[Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください

[WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります

[WAF.2] AWS WAF クラシックリージョンルールには少なくとも 1 つの条件が必要です

[WAF.3] AWS WAF クラシックリージョンルールグループには、少なくとも 1 つのルールが必要です

[WAF.4] AWS WAF クラシックリージョンウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

[WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です

[WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です

[WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

[WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

[WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります

CIS AWS Foundations Benchmark

Center for Internet Security (CIS) AWS Foundations Benchmark 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、明確で step-by-step 実装、評価の手順を提供します。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、このベンチマークのコントロールは、組織が使用する特定のシステムの保護に役立ちます。

AWS Security Hub は、CIS AWS Foundations Benchmark v3.0.0、1.4.0、および v1.2.0 をサポートしています。

このページには、各バージョンがサポートするセキュリティコントロールが一覧表示され、バージョンの比較が表示されます。

CIS AWS Foundations Benchmark v3.0.0

Security Hub は、CIS AWS Foundations Benchmark のバージョン 3.0.0 をサポートしています。

Security Hub は CIS Security Software Certification の要件を満たしており、以下の CIS Benchmarks で CIS Security Software Certification を受けています:

- CIS Benchmark for CIS AWS Foundations Benchmark、v3.0.0、レベル 1
- CIS Benchmark for CIS AWS Foundations Benchmark、v3.0.0、レベル 2

CIS AWS Foundations Benchmark v3.0.0 に適用されるコントロール

[Account.1] のセキュリティ連絡先情報を に提供する必要があります AWS アカウント

〔CloudTrail.1] CloudTrail 読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン追跡を有効にして設定する必要があります

〔CloudTrail.2] 保管時の暗号化を有効にする CloudTrail 必要があります

〔CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります

〔CloudTrail.7] S3 バケットで CloudTrail S3 バケットアクセスログ記録が有効になっていることを確認する

[Config.1] AWS Config を有効にし、サービスにリンクされたロールをリソース記録に使用する必要があります

[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします

[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします

[EC2.7] EBS のデフォルト暗号化を有効にすることをお勧めします

[EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします

[EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります

[EC2.53] EC2 セキュリティグループは、0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可しないでください

[EC2.54] EC2 セキュリティグループは、::/0 からリモートサーバー管理ポートへの入力を許可しないでください

[EFS .1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS

[IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください

[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります

[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません

[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります

[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります

[IAM.9] ルートユーザーに対して MFA を有効にする必要があります

[IAM.15] 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します

[IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています

[IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support

[IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります

[IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります

[IAM.27] IAM ID には AWSCloudShellFullAccess ポリシーをアタッチしないでください

[IAM.28] IAM Access Analyzer の外部アクセスアナライザーを有効にする必要があります

[KMS.4] AWS KMS キーローテーションを有効にする必要があります

[RDS.2] RDS DB インスタンスは、 PubliclyAccessible AWS Config設定によって決定されるパブリックアクセスを禁止する必要があります

[RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。

[RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります

[S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります

[S3.5] S3 汎用バケットでは、SSL を使用するリクエストが必要です

[S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります

[S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります

[S3.22] S3 汎用バケットは、オブジェクトレベルの書き込みイベントをログに記録する必要があります

[S3.23] S3 汎用バケットは、オブジェクトレベルの読み取りイベントをログに記録する必要があります

CIS AWS Foundations Benchmark v1.4.0

Security Hub は CIS AWS Foundations Benchmark の v1.4.0 をサポートしています。

CIS AWS Foundations Benchmark v1.4.0 に適用されるコントロール

〔CloudTrail.1] CloudTrail 読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン追跡を有効にして設定する必要があります

〔CloudTrail.2] 保管時の暗号化を有効にする CloudTrail 必要があります

〔CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります

〔CloudTrail.5] CloudTrail 証跡は Amazon CloudWatch Logs と統合する必要があります

〔CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットがパブリックにアクセスできないようにする

〔CloudTrail.7] S3 バケットで CloudTrail S3 バケットアクセスログ記録が有効になっていることを確認する

〔CloudWatch.1] 「ルート」ユーザーの使用に対してログメトリクスフィルターとアラームが存在する必要があります

〔CloudWatch.4] IAM ポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.5] CloudTrail AWS Configログメトリクスフィルターとアラームが設定変更用に存在することを確認する

〔CloudWatch.6] AWS Management Console 認証の失敗に対してログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.7] カスタマーマネージドキーの無効化またはスケジュールされた削除のためのログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.8] S3 バケットポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.9] AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.10] セキュリティグループの変更に対するログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.11] ネットワークアクセスコントロールリスト (NACL) の変更に対するログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.12] ネットワークゲートウェイの変更に対するログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.13] ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.14] VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認する

[Config.1] AWS Config を有効にし、サービスにリンクされたロールをリソース記録に使用する必要があります

[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします

[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします

[EC2.7] EBS のデフォルト暗号化を有効にすることをお勧めします

[EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります

[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください

[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります

[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません

[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります

[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります

[IAM.9] ルートユーザーに対して MFA を有効にする必要があります

[IAM.15] 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します

[IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています

[IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support

[IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります

[KMS.4] AWS KMS キーローテーションを有効にする必要があります

[RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。

[S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります

[S3.5] S3 汎用バケットでは、SSL を使用するリクエストが必要です

[S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります

[S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります

Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0

Security Hub は、CIS AWS Foundations Benchmark のバージョン 1.2.0 をサポートしています。

Security Hub は CIS Security Software Certification の要件を満たしており、以下の CIS Benchmarks で CIS Security Software Certification を受けています:

- CIS Benchmark for CIS AWS Foundations Benchmark、v1.2.0、レベル 1
- CIS Benchmark for CIS AWS Foundations Benchmark、v1.2.0、レベル 2

CIS AWS Foundations Benchmark v1.2.0 に適用されるコントロール

〔CloudTrail.1] CloudTrail 読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン追跡を有効にして設定する必要があります

〔CloudTrail.2] 保管時の暗号化を有効にする CloudTrail 必要があります

〔CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります

〔CloudTrail.5] CloudTrail 証跡は Amazon CloudWatch Logs と統合する必要があります

〔CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットがパブリックにアクセスできないようにする

〔CloudTrail.7] S3 バケットで CloudTrail S3 バケットアクセスログ記録が有効になっていることを確認する

〔CloudWatch.1] 「ルート」ユーザーの使用に対してログメトリクスフィルターとアラームが存在する必要があります

〔CloudWatch.2] 不正な API コールに対してログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.3] MFA を使用しない マネジメントコンソールサインインのログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.4] IAM ポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.5] CloudTrail AWS Configログメトリクスフィルターとアラームが設定変更用に存在することを確認する

〔CloudWatch.6] AWS Management Console 認証の失敗に対してログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.7] カスタマーマネージドキーの無効化またはスケジュールされた削除のためのログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.8] S3 バケットポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.9] AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.10] セキュリティグループの変更に対するログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.11] ネットワークアクセスコントロールリスト (NACL) の変更に対するログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.12] ネットワークゲートウェイの変更に対するログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.13] ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認する

〔CloudWatch.14] VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認する

[Config.1] AWS Config を有効にし、サービスにリンクされたロールをリソース記録に使用する必要があります

[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします

[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします

[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります

[EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります

[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください

[IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください

[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります

[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません

[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります

[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります

[IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります

[IAM.9] ルートユーザーに対して MFA を有効にする必要があります

[IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します

[IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します

[IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します

[IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します

[IAM.15] 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します

[IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています

[IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します

[IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support

[KMS.4] AWS KMS キーローテーションを有効にする必要があります

CIS AWS Foundations Benchmark のバージョン比較

このセクションでは、Center for Internet Security (CIS) AWS Foundations Benchmark v3.0.0、v1.4.0、および v1.2.0 の違いを要約します。

Security Hub は CIS AWS Foundations Benchmark の各バージョンをサポートしていますが、v3.0.0 を使用してセキュリティのベストプラクティスを最新の状態に保つことをお勧めします。複数のバージョンの標準を同時に有効にすることができます。詳細については、「セキュリティ標準の有効化および無効化」を参照してください。v3.0.0 にアップグレードする場合は、古いバージョンを無効にする前に最初に有効にすることをお勧めします。Security Hub と の統合を使用して複数の AWS

Organizations を一元管理 AWS アカウント し、すべてのアカウントで v3.0.0 をバッチで有効にする場合は、中央設定 を使用できます。

各バージョンの CIS 要件へのコントロールのマッピング

CIS AWS Foundations Benchmark がサポートする各バージョンのコントロールについて説明します。

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
[Account.1] のセキュリティ連絡先情報を に提供する必要があります AWS アカウント	1.2	1.2	1.18
〔CloudTrail.1] CloudTrail 読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン追跡を有効にして設定する必要があります	3.1	3.1	2.1
〔CloudTrail.1] CloudTrail 読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン追跡を有効にして設定する必要があります	3.1	3.1	2.1
〔CloudTrail.2] 保管時の暗号化を有効にする CloudTrail 必要があります	3.5	37	2.7
〔CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります	3.2	3.2	2.2
〔CloudTrail.5] CloudTrail 証跡は Amazon CloudWatch Logs と統合する必要があります	サポート対象外 — CIS はこの要件を削除しました	3.4	2.4

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
〔CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットがパブリックにアクセスできないようにする	サポート対象外 — CIS はこの要件を削除しました	3.3	2.3
〔CloudTrail.7] S3 バケットで CloudTrail S3 バケットアクセスログ記録が有効になっていることを確認する	3.4	3.6	2.6
〔CloudWatch.1] 「ルート」ユーザーの使用に対してログメトリクスフィルターとアラームが存在する必要があります	サポート対象外 – 手動チェック	4.3	3.3
〔CloudWatch.2] 不正な API コールに対してログメトリクスフィルターとアラームが存在することを確認する	サポート対象外 – 手動チェック	サポート対象外 – 手動チェック	3.1
〔CloudWatch.3] MFA を使用しない マネジメントコンソールサインインのログメトリクスフィルターとアラームが存在することを確認する	サポート対象外 – 手動チェック	サポート対象外 – 手動チェック	3.2
〔CloudWatch.4] IAM ポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認する	サポート対象外 – 手動チェック	4.4	3.4
〔CloudWatch.5] CloudTrail AWS Configログメトリクスフィルターとアラームが設定変更用に存在することを確認する	サポート対象外 – 手動チェック	4.5	3.5

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
〔CloudWatch.6] AWS Management Console 認証の失敗に対してログメトリクスフィルターとアラームが存在することを確認する	サポート対象外 – 手動チェック	4.6	3.6
〔CloudWatch.7] カスタマーマネージドキーの無効化またはスケジュールされた削除のためのログメトリクスフィルターとアラームが存在することを確認する	サポート対象外 – 手動チェック	4.7	37
〔CloudWatch.8] S3 バケットポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認する	サポート対象外 – 手動チェック	4.8	3.8
〔CloudWatch.9] AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する	サポート対象外 – 手動チェック	4.9	3.9
〔CloudWatch.10] セキュリティグループの変更に対するログメトリクスフィルターとアラームが存在することを確認する	サポート対象外 – 手動チェック	4.10	3.10
〔CloudWatch.11] ネットワークアクセスコントロールリスト (NACL) の変更に対するログメトリクスフィルターとアラームが存在することを確認する	サポート対象外 – 手動チェック	4.11	3.11
〔CloudWatch.12] ネットワークゲートウェイの変更に対するログメトリクスフィルターとアラームが存在することを確認する	サポート対象外 – 手動チェック	4.12	3.12

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
〔CloudWatch.13] ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認する	サポート対象外 – 手動チェック	4.13	3.13
〔CloudWatch.14] VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認する	サポート対象外 – 手動チェック	4.14	3.14
[Config.1] AWS Config を有効にし、サービスにリンクされたロールをリソース記録に使用する必要があります	3.3	3.5	2.5
[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします	5.4	5.3	4.3
[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします	37	3.9	2.9
[EC2.7] EBS のデフォルト暗号化を有効にすることをお勧めします	2.2.1	2.2.1	サポートされていません
[EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします	5.6	サポートされません	サポートされません

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります	サポート対象外 — 要件 5.2 および 5.3 に置き換えられました	サポート対象外 — 要件 5.2 および 5.3 に置き換えられました	4.1
[EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります	サポート対象外 — 要件 5.2 および 5.3 に置き換えられました	サポート対象外 — 要件 5.2 および 5.3 に置き換えられました	4.2
[EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります	5.1	5.1	サポートされていません
[EC2.53] EC2 セキュリティグループは、0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可しないでください	5.2	サポートされません	サポートされません
[EC2.54] EC2 セキュリティグループは、::/0 からリモートサーバー管理ポートへの入力を許可しないでください	5.3	サポートされません	サポートされません
[EFS .1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS	2.4.1	サポートされません	サポートされません
[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください	サポートされません	1.16	1.22

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
[IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください	1.15	サポートされていません	1.16
[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります	1.14	1.14	1.4
[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません	1.4	1.4	1.12
[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります	1.10	1.10	1.2
[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります	1.6	1.6	1.14
[IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります	サポート対象外 – [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります代わりに「」を参照してください。	サポート対象外 – [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります代わりに「」を参照してください。	1.3
[IAM.9] ルートユーザーに対して MFA を有効にする必要があります	1.5	1.5	1.13
[IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します	サポート対象外 — CIS はこの要件を削除しました	サポート対象外 — CIS はこの要件を削除しました	1.5

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
[IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します	サポート対象外 — CIS はこの要件を削除しました	サポート対象外 — CIS はこの要件を削除しました	1.6
[IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します	サポート対象外 — CIS はこの要件を削除しました	サポート対象外 — CIS はこの要件を削除しました	1.7
[IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します	サポート対象外 — CIS はこの要件を削除しました	サポート対象外 — CIS はこの要件を削除しました	1.8
[IAM.15] 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します	1.8	1.8	1.9
[IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています	1.9	1.9	1.10
[IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します	サポート対象外 — CIS はこの要件を削除しました	サポート対象外 — CIS はこの要件を削除しました	1.11
[IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support	1.17	1.17	1.2

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
[IAM.20] ルートユーザーの使用を避けます	サポート対象外 — CIS はこの要件を削除しました	サポート対象外 — CIS はこの要件を削除しました	1.1
[IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります	1.12	1.12	サポート対象外 — CIS が新しいバージョンでこの要件を追加しました
[IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります	1.19	サポート対象外 — CIS が新しいバージョンでこの要件を追加しました	サポート対象外 — CIS が新しいバージョンでこの要件を追加しました
[IAM.27] IAM ID には AWSCloudShellFullAccess ポリシーをアタッチしないでください	1.22	サポート対象外 — CIS が新しいバージョンでこの要件を追加しました	サポート対象外 — CIS が新しいバージョンでこの要件を追加しました
[IAM.28] IAM Access Analyzer の外部アクセスアナライザーを有効にする必要があります	1.20	サポート対象外 — CIS が新しいバージョンでこの要件を追加しました	サポート対象外 — CIS が新しいバージョンでこの要件を追加しました
[KMS.4] AWS KMS キーローテーションを有効にする必要があります	3.6	3.8	2.8
[Macie.1] Amazon Macie を有効にする必要があります	サポート対象外 – 手動チェック	サポート対象外 – 手動チェック	サポート対象外 – 手動チェック

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
[RDS.2] RDS DB インスタンスは、PubliclyAccessible AWS Config設定によって決定されるパブリックアクセスを禁止する必要があります	2.3.3	サポート対象外 — CIS が新しいバージョンでこの要件を追加しました	サポート対象外 — CIS が新しいバージョンでこの要件を追加しました
[RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。	2.3.1	2.3.1	サポート対象外 — CIS が新しいバージョンでこの要件を追加しました
[RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります	2.3.2	サポート対象外 — CIS が新しいバージョンでこの要件を追加しました	サポート対象外 — CIS が新しいバージョンでこの要件を追加しました
[S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります	2.1.4	2.1.5	サポート対象外 — CIS が新しいバージョンでこの要件を追加しました
[S3.5] S3 汎用バケットでは、SSL を使用するリクエストが必要です	2.1.1	2.1.2	サポート対象外 — CIS が新しいバージョンでこの要件を追加しました
[S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります	2.1.4	2.1.5	サポート対象外 — CIS が新しいバージョンでこの要件を追加しました

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
[S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります	2.1.2	2.1.3	サポート対象外 — CIS が新しいバージョンでこの要件を追加しました

CIS AWS ARNs

CIS AWS Foundations Benchmark の 1 つ以上のバージョンを有効にすると、 AWS Security Finding 形式 (ASFF) で結果の受信が開始されます。ASFF では、各バージョンは次の Amazon リソースネーム (ARN) を使用します。

CIS AWS Foundations Benchmark v3.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/3.0.0
```

CIS AWS Foundations Benchmark v1.4.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/1.4.0
```

CIS AWS Foundations Benchmark v1.2.0

```
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

Security Hub API の GetEnabledStandardsオペレーションを使用して、有効な標準の ARN を確認できます。

上記の値は 用ですStandardsArn。ただし、 は、BatchEnableStandardsリージョンで を呼び出して標準をサブスクライブするときに Security Hub が作成する標準サブスクリプションリソースStandardsSubscriptionArnを指します。

> **Note**
>
> CIS AWS Foundations Benchmark のバージョンを有効にすると、Security Hub は、他の有効な標準で有効になっているコントロールと同じ AWS Config サービスにリンクされたルールを使用するコントロールの検出結果を生成するまでに最大 18 時間かかる場合があります。詳細については、「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。

統合統制結果を有効にすると、検出結果フィールドは異なります。違いについての詳細は ASFF フィールドと値への統合の影響 を参照してください。サンプルコントロールの検出結果については、「」を参照してくださいコントロールの検出結果のサンプル。

Security Hub でサポートされていない CIS 要件

前の表で説明したように、Security Hub は CIS AWS Foundations Benchmark のすべてのバージョンですべての CIS 要件をサポートしているわけではありません。サポートされていない要件の多くは、 AWS リソースの状態を確認することで手動でのみ評価できます。

米国国立標準技術研究所 (NIST) SP 800-53 Rev. 5

NIST SP 800-53 Rev. 5 は、米国商務省の一機関である米国国立標準技術研究所 (NIST) が開発した、サイバーセキュリティおよびコンプライアンスのフレームワークです。このコンプライアンスフレームワークは、情報システムと重要なリソースの可用性、機密性、完全性の保護に役立ちます。米国連邦政府機関および請負業者は、システムを保護するために NIST SP 800-53 に準拠する必要がありますが、民間企業はサイバーセキュリティリスクを軽減するための指針となるフレームワークとして、自主的に NIST SP 800-53 を使用することができます。

Security Hub は、一部の NIST SP 800-53 要件をサポートするコントロールを提供します。これらのコントロールは、自動化されたセキュリティチェックによって評価されます。Security Hub コントロールは、手動での確認が必要な NIST SP 800-53 の要件をサポートしていません。また、Security Hub コントロールは、各コントロールの詳細に関連する要件としてリストされている、自動化された NIST SP 800-53 の要件のみをサポートします。詳細を表示するには、次のリストからコントロールを選択します。コントロールの詳細に記載されていない関連要件は、現在 Security Hub ではサポートされていません。

他のフレームワークとは異なり、NIST SP 800-53 は、その要件をどのように評価すべきかについて、指示を与えるものではありません。その代わりに、フレームワークはガイドラインを提供しています。また、Security Hub NIST SP 800-53 コントロールは、サービスでガイドラインが理解されていることを示しています。

Security Hub と の統合を使用して複数のアカウント AWS Organizations を一元管理し、すべてのアカウントで NIST SP 800-53 をバッチで有効にする場合は、管理者アカウントから Security Hub マルチアカウントスクリプトを実行できます。

NIST SP 800-53 Rev. 5 の詳細については、「NIST Computer Security Resource Center」を参照してください。

NIST SP 800-53 Rev. 5 に適用されるコントロール

[Account.1] のセキュリティ連絡先情報を に提供する必要があります AWS アカウント

[Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります

[ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります

[APIGateway.1] API Gateway REST と WebSocket API 実行の口グ記録を有効にする必要があります

[APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります

[APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります

[APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります

[APIGateway.5] API Gateway REST API のキャッシュデータは、保管中に暗号化する必要があります

[APIGateway.8] API Gateway ルートには認証タイプを指定する必要があります

[APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります

〔AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください

〔AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要があります

〔AutoScaling.2] Amazon EC2 Auto Scaling グループは複数のアベイラビリティーゾーンをカバーする必要があります

〔AutoScaling.3] Auto Scaling グループの起動設定では、インスタンスメタデータサービスバージョン 2 (IMDSv2) を要求するように EC2 インスタンスを設定する必要がありますIMDSv2

[Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません

〔AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります

〔AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります

[Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります

〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります

〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です

〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります

〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります

〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります

〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります

〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります

〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります

〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください

〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません

〔CloudTrail.1] CloudTrail 読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン追跡を有効にして設定する必要があります

〔CloudTrail.2] 保管時の暗号化を有効にする CloudTrail 必要があります

〔CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります

〔CloudTrail.5] CloudTrail 証跡は Amazon CloudWatch Logs と統合する必要があります

〔CloudWatch.15] CloudWatch アラームには、指定されたアクションが設定されている必要があります

〔CloudWatch.16] CloudWatch ロググループは、指定された期間保持する必要があります

〔CloudWatch.17] CloudWatch アラームアクションを有効にする必要があります

〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください

〔CodeBuild.2] CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください

〔CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります

〔CodeBuild.4] CodeBuild プロジェクト環境にはログ記録 AWS Config設定が必要です

[Config.1] AWS Config を有効にし、サービスにリンクされたロールをリソース記録に使用する必要があります

〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります

[DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります

[DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。

[DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。

[DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。

[DMS.9] DMS エンドポイントは SSL を使用する必要があります。

[DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります

[DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります

[DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります

[DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります

[DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です

[DocumentDB.3] Amazon DocumentDB 手動クラススナップショットはパブリックにできません

[DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります

[DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります

[DynamoDB.1] DynamoDB テーブルは、需要に応じて容量をオートスケーリングする必要があります

[DynamoDB.2] DynamoDB テーブルでは point-in-time リカバリを有効にする必要があります

[DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります

[DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります

[DynamoDB.6] DynamoDB テーブルで、削除保護が有効になっている必要があります

[DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります

[EC2.1] Amazon EBS スナップショットはパブリックに復元できないようにすることをお勧めします

[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします

[EC2.3] アタッチされた Amazon EBS ボリュームは、保管時に暗号化することをお勧めします

[EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります

[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします

[EC2.7] EBS のデフォルト暗号化を有効にすることをお勧めします

[EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします

[EC2.9] Amazon EC2 インスタンスは、パブリック IPv4 アドレスを未設定にすることをお勧めします

[EC2.10] Amazon EC2 サービス用に作成された VPC エンドポイントを使用するようにAmazon EC2 を設定することをお勧めします

[EC2.12] 未使用の Amazon EC2 EIP を削除することをお勧めします

[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります

[EC2.15] Amazon EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないことをお勧めします

[EC2.16] 未使用のネットワークアクセスコントロールリストを削除することをお勧めします

[EC2.17] Amazon EC2 インスタンスが複数の ENI を使用しないようにすることをお勧めします

[EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします

[EC2.19] セキュリティグループは、リスクの高いポートへの無制限アクセスを許可してはいけません

[EC2.20] AWS Site-to-Site VPN 接続の両方の VPN トンネルが稼働している必要があります

[EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります

[EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします

[EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします

[EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします

[EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします

[EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります

[ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります

[ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります

[ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります

[ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。

[ECS.2] ECS サービスには、パブリック IP アドレスを自動で割り当てないでください

[ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください

[ECS.4] ECS コンテナは、非特権として実行する必要があります

[ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。

[ECS.8] シークレットは、コンテナ環境の変数として渡さないでください

[ECS.9] ECS タスク定義にはログ設定が必要です。

[ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。

[ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります

[EFS .1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS

[EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります

[EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります

[EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります

[EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません

[EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります

[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。

[EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります

[EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります

〔ElastiCache.1] ElastiCache Redis クラスターでは自動バックアップを有効にする必要があります

〔ElastiCache.2]Redis キャッシュクラスター ElastiCache では、マイナーバージョン自動アップグレードを有効にする必要があります

Redis ElastiCache レプリケーショングループの [ElastiCache.3] では、自動フェイルオーバーを有効にする必要があります

〔ElastiCache.4] ElastiCache for Redis レプリケーショングループは保管時に暗号化する必要があります

Redis ElastiCache レプリケーショングループの [ElastiCache.5] は転送中に暗号化する必要があります

〔ElastiCache.6]バージョン ElastiCache 6.0 より前の Redis レプリケーショングループでは、Redis AUTH を使用する必要があります

〔ElastiCache.7] ElastiCache クラスターはデフォルトのサブネットグループを使用しないでください

〔ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります

〔ElasticBeanstalk.2] Elastic Beanstalk マネージドプラットフォームの更新を有効にする必要があります

[ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります

[ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager

[ELB.3] Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります

[ELB.4] Application Load Balancer は、http ヘッダーを削除するように設定する必要があります

[ELB.5] アプリケーションおよび Classic Load Balancer のログ記録を有効にする必要があります

[ELB.6] Application、Gateway、Network Load Balancer では、削除保護を有効にする必要があります

[ELB.7] Classic Load Balancers は、Connection Draining を有効にする必要があります

[ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な AWS Config設定を持つ事前定義されたセキュリティポリシーを使用する必要があります

[ELB.9] Classic Load Balancer では、クロスゾーンロードバランシングが有効になっている必要があります

[ELB.10] Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります

[ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります

[ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります

[ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります

[ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります

[EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります

[EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります

[ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります

[ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります

[ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります

[ES.4] Logs への Elasticsearch CloudWatch ドメインエラーのログ記録を有効にする必要があります

[ES.5] Elasticsearch ドメインで監査ログ記録が有効になっている必要があります

[ES.6] Elasticsearch ドメインには少なくとも 3 つのデータノードが必要です

[ES.7] Elasticsearch ドメインは、少なくとも 3 つの専用マスターノードを設定する必要があります。

[ES.8] Elasticsearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります

〔EventBridge.3] EventBridge カスタムイベントバスには、リソースベースのポリシーがアタッチされている必要があります

〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります

[FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります

[FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります

〔GuardDuty.1] GuardDuty を有効にする必要があります

[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください

[IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください

[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります

[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません

[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります

[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります

[IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です

[IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります

[IAM.9] ルートユーザーに対して MFA を有効にする必要があります

[IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります

[IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません

[Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります

[KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください

[KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください

[KMS.3] 意図せずに削除 AWS KMS keys しないでください

[KMS.4] AWS KMS キーローテーションを有効にする必要があります

[Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります

[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります

[Lambda.3] Lambda 関数は VPC 内に存在する必要があります

[Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります

[Macie.1] Amazon Macie を有効にする必要があります

[Macie.2] Macie 自動機密データ検出を有効にする必要があります

[MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります

[MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります

[MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch

[MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります

[MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります

[MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。

[Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります

[Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります

[Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください

[Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります

[Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります

[Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります

[Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります

[Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります

[Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります

〔NetworkFirewall.1] Network Firewall ファイアウォールは複数のアベイラビリティーゾーンにデプロイする必要があります

〔NetworkFirewall.2] Network Firewall のログ記録を有効にする必要があります

〔NetworkFirewall.3] Network Firewall ポリシーには、少なくとも 1 つのルールグループが関連付けられている必要があります

〔NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、フルパケットに対してドロップまたは転送する必要があります

〔NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、フラグメント化されたパケットに対してドロップまたは転送する必要があります

〔NetworkFirewall.6] ステートレス Network Firewall ルールグループは空にしないでください

〔NetworkFirewall.9] Network Firewall ファイアウォールでは、削除保護を有効にする必要があります

[Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります

[Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません

[Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります

[Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります

[Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります

[Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です

[Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります

[Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります

[Opensearch.10] OpenSearch ドメインには最新のソフトウェア更新がインストールされている必要があります

[Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です

[PCA.1] AWS Private CA ルート認証機関を無効にする必要があります

[RDS.1] RDS スナップショットはプライベートである必要があります

[RDS.2] RDS DB インスタンスは、 PubliclyAccessible AWS Config設定によって決定されるパブリックアクセスを禁止する必要があります

[RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。

[RDS.4] RDS クラスタースナップショットとデータベーススナップショットは保管中に暗号化する必要があります

[RDS.5] RDS DB インスタンスは、複数のアベイラビリティーゾーンで設定する必要があります

[RDS.6] RDS DB インスタンスの拡張モニタリングを設定する必要があります

[RDS.7] RDS クラスターでは、削除保護が有効になっている必要があります

[RDS.8] RDS DB インスタンスで、削除保護が有効になっている必要があります

[RDS.9] RDS DB インスタンスはログを CloudWatch Logs に発行する必要があります

[RDS.10] IAM 認証は RDS インスタンス用に設定する必要があります

[RDS.11] RDS インスタンスでは、自動バックアップが有効になっている必要があります

[RDS.12] IAM 認証は RDS クラスター用に設定する必要があります

[RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります

[RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります

[RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります

[RDS.16] タグをスナップショットにコピーするように RDS DB クラスターを設定する必要があります

[RDS.17] RDS DB インスタンスは、タグをスナップショットにコピーするように設定する必要があります

[RDS.18] RDS インスタンスは VPC 内にデプロイする必要があります

[RDS.19] 重大なクラスターイベントについて、既存の RDS イベント通知サブスクリプションを設定する必要があります

[RDS.20] 重大なデータベースインスタンスイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります

[RDS.21] 重大なデータベースパラメータグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります

[RDS.22] 重大なデータベースセキュリティグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります

[RDS.23] RDS インスタンスはデータベースエンジンのデフォルトポートを使用しないようにする必要があります

[RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります

[RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります

[RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります

[RDS.27] RDS DB クラスターは保管中に暗号化する必要があります

[RDS.34] Aurora MySQL DB クラスターは監査ログを CloudWatch Logs に発行する必要があります

[RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります

[PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります

[Redshift.2] Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります

[Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります

[Redshift.4] Amazon Redshift クラスターでは、監査ログ記録が有効になっている必要があります

[Redshift.6] Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります

[Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります

[Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください

[Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください

[Redshift.10] Redshift クラスターは保存時に暗号化する必要があります

[Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります

[S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります

[S3.2] S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります

[S3.3] S3 汎用バケットはパブリック書き込みアクセスをブロックする必要があります

[S3.5] S3 汎用バケットでは、SSL を使用するリクエストが必要です

[S3.6] S3 汎用バケットポリシーでは、他の へのアクセスを制限する必要があります AWS アカウント

[S3.7] S3 汎用バケットはクロスリージョンレプリケーションを使用する必要があります

[S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります

[S3.9] S3 汎用バケットでは、サーバーアクセスのログ記録を有効にする必要があります

[S3.10] バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です

[S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります

[S3.12] ACLs を使用しないでください S3

[S3.13] S3 汎用バケットにはライフサイクル設定が必要です

[S3.14] S3 汎用バケットではバージョニングを有効にする必要があります

[S3.15] S3 汎用バケットでは、オブジェクトロックを有効にする必要があります

[S3.17] S3 汎用バケットは、保管時に で暗号化する必要があります AWS KMS keys

[S3.19] S3 アクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります

[S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります

〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません

〔SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります

〔SageMaker.3] SageMaker ユーザーはノートブックインスタンスへのルートアクセスを許可されない

〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります

〔SecretsManager.1] Secrets Manager シークレットでは、自動ローテーションを有効にする必要があります

〔SecretsManager.2] 自動ローテーションで設定された Secrets Manager シークレットは正常にローテーションする必要があります

〔SecretsManager.3] 未使用の Secrets Manager シークレットを削除する

〔SecretsManager.4] Secrets Manager のシークレットは、指定された日数内にローテーションする必要があります

〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります

[SNS.1] SNS トピックは、保管時に を使用して暗号化する必要があります AWS KMS

[SQS.1] Amazon SQS キューは保管中に暗号化する必要があります

[SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager

[SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります

[SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります

[SSM.4] SSM ドキュメントはパブリックにしないでください

[Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください

[WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります

[WAF.2] AWS WAF クラシックリージョンルールには少なくとも 1 つの条件が必要です

[WAF.3] AWS WAF クラシックリージョンルールグループには、少なくとも 1 つのルールが必要です

[WAF.4] AWS WAF クラシックリージョンウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

[WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です

[WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です

[WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

[WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

[WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります

[WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります

Payment Card Industry Data Security Standard (PCI DSS)

Security Hub の Payment Card Industry Data Security Standard (PCI DSS) は、カード所有者データの処理について、一連の AWS セキュリティのベストプラクティスを提供します。この標準を使用して、カード所有者データを処理するリソースのセキュリティ上の脆弱性を発見できます。Security Hub は現在、アカウントレベルでコントロールをスコープします。カード所有者データを保存、処理、送信するリソースを持つすべてのアカウントで、これらのコントロールを有効にすることをお勧めします。

この標準は Security AWS Assurance Services LLC (AWS SAS) によって検証されました。SAS は、PCI DSS ガイダンスと PCI DSS Security Standards Council (QSAs) のチームです。 AWS SAS は、自動チェックが顧客による PCI DSS 評価の準備に役立つことを確認しました。

このページには、セキュリティコントロール ID とタイトルが一覧表示されます。 AWS GovCloud (US) Region および中国リージョンでは、標準固有のコントロール IDs とタイトルが使用されます。セキュリティコントロール ID とタイトルを標準固有のコントロール ID とタイトルにマッピングする方法については、「統合がコントロール ID とタイトルに与える影響」を参照してください。

PCI DSS に適用されるコントロール

〔AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要があります

〔CloudTrail.2] 保管時の暗号化を有効にする CloudTrail 必要があります

〔CloudTrail.3] 少なくとも 1 つの CloudTrail 証跡を有効にする必要があります

〔CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります

〔CloudTrail.5] CloudTrail 証跡は Amazon CloudWatch Logs と統合する必要があります

〔CloudWatch.1] 「ルート」ユーザーの使用に対してログメトリクスフィルターとアラームが存在する必要があります

〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください

〔CodeBuild.2] CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください

[Config.1] AWS Config を有効にし、サービスにリンクされたロールをリソース記録に使用する必要があります

[DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります

[EC2.1] Amazon EBS スナップショットはパブリックに復元できないようにすることをお勧めします

[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします

[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします

[EC2.12] 未使用の Amazon EC2 EIP を削除することをお勧めします

[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります

[ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります

[ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります

[ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります

〔GuardDuty.1] GuardDuty を有効にする必要があります

[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください

[IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください

[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません

[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります

[IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります

[IAM.9] ルートユーザーに対して MFA を有効にする必要があります

[IAM.10] IAM ユーザーのパスワードポリシーには強力な AWS Config設定が必要です

[IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります

[KMS.4] AWS KMS キーローテーションを有効にする必要があります

[Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります

[Lambda.3] Lambda 関数は VPC 内に存在する必要があります

[Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります

[Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません

[RDS.1] RDS スナップショットはプライベートである必要があります

[RDS.2] RDS DB インスタンスは、 PubliclyAccessible AWS Config設定によって決定されるパブリックアクセスを禁止する必要があります

[PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります

[S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります

[S3.2] S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります

[S3.3] S3 汎用バケットはパブリック書き込みアクセスをブロックする必要があります

[S3.5] S3 汎用バケットでは、SSL を使用するリクエストが必要です

[S3.7] S3 汎用バケットはクロスリージョンレプリケーションを使用する必要があります

〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません

[SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager

[SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります

[SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります

AWS リソースタグ付け標準

このセクションでは、 AWS リソースタグ付け標準について説明します。

> **Note**
>
> AWS リソースタグ付け標準は、カナダ西部 (カルガリー) 、中国、および では使用できません AWS GovCloud (US)。

AWS リソースタグ付け標準とは

タグは、 AWS リソースを整理するためのメタデータとして機能するキーと値のペアです。ほとんどのリソースでは、 AWS リソースの作成時または作成後にタグを追加するオプションがあります。リソースの例としては、Amazon CloudFront ディストリビューション、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、 のシークレットなどがあります AWS Secrets Manager。

タグは、リソースの管理、識別、整理、検索、フィルタリングに役立ちます。

各タグは 2 つの部分で構成されます。

- タグキー (例: `CostCenter`、`Environment` または `Project`)。タグキーでは、大文字と小文字が区別されます。
- タグ値 (`111122223333`や などProduction) 。タグキーと同様に、タグ値は大文字と小文字が区別されます。

タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。

AWS リソースにタグを追加する手順については、「Security Hub ユーザーガイド」の AWS 「リソースにタグを追加する方法」を参照してください。 AWS

AWS Security Hub によって開発された AWS Resource Tagging Standard は、 AWS いずれかのリソースにタグキーがないかどうかをすばやく特定するのに役立ちます。`requiredTagKeys` パラメータをカスタマイズして、コントロールがチェックする特定のタグキーを指定できます。特定のタグが指定されていない場合、コントロールは少なくとも 1 つのタグキーの存在をチェックするだけです。

AWS リソースタグ付け標準を有効にすると、 AWS Security Finding 形式 (ASFF) で結果の受信が開始されます。

> **Note**
>
> AWS Resource Tagging Standard を有効にすると、Security Hub が他の有効な標準で有効になっているコントロールと同じ AWS Config サービスにリンクされたルールを使用するコン

トロールの検出結果を生成するまでに、最大 18 時間かかる場合があります。詳細については、「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。

この標準には、次の Amazon リソースネーム (ARN) があります: `arn:aws:securityhub:region::standards/aws-resource-tagging-standard/v/1.0.0`。

Security Hub API の GetEnabledStandardsオペレーションを使用して、有効な標準の ARN を確認することもできます。

AWS リソースタグ付け標準のコントロール

Resource AWS Tagging Standard には、次のコントロールが含まれています。コントロールを選択すると、その詳細な説明が表示されます。

- [ACM.3] ACM 証明書にはタグを付ける必要があります
- 〔AppSync.4] AWS AppSync GraphQL APIsにはタグを付ける必要があります
- [Athena.2] Athena データカタログにはタグを付ける必要があります
- [Athena.3] Athena ワークグループにはタグを付ける必要があります
- 〔AutoScaling.10] EC2 Auto Scaling グループにタグを付ける必要があります
- [Backup.2] AWS Backup 復旧ポイントにタグを付ける必要があります
- [Backup.3] AWS Backup ボールトにはタグを付ける必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [Backup.5] AWS Backup バックアップ計画にはタグを付ける必要があります
- 〔CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CloudTrail.9] CloudTrail 証跡にはタグを付ける必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- [Detective.1] Detective の動作グラフにはタグを付ける必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにタグを付ける必要があります

- [DynamoDB.5] DynamoDB テーブルにはタグを付ける必要があります
- [EC2.33] EC2 トランジットゲートウェイアタッチメントにはタグを付ける必要があります
- [EC2.34] EC2 トランジットゲートウェイルートテーブルにタグを付ける必要があります
- [EC2.35] EC2 ネットワークインターフェイスにタグを付ける必要があります
- [EC2.36] EC2 カスタマーゲートウェイにはタグを付ける必要があります
- [EC2.37] EC2 Elastic IP アドレスにタグを付ける必要があります
- [EC2.38] EC2 インスタンスにはタグを付ける必要があります
- [EC2.39] EC2 インターネットゲートウェイにはタグを付ける必要があります
- [EC2.40] EC2 NAT ゲートウェイにタグを付ける必要があります
- [EC2.41] EC2 ネットワーク ACLs にはタグを付ける必要があります
- [EC2.42] EC2 ルートテーブルにはタグを付ける必要があります
- [EC2.43] EC2 セキュリティグループにタグを付ける必要があります
- [EC2.44] EC2 サブネットにはタグを付ける必要があります
- [EC2.45] EC2 ボリュームにはタグを付ける必要があります
- [EC2.46] Amazon VPCsにはタグを付ける必要があります
- [EC2.47] Amazon VPC エンドポイントサービスにはタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります
- [EC2.49] Amazon VPC ピアリング接続にはタグを付ける必要があります
- [EC2.50] EC2 VPN ゲートウェイにはタグを付ける必要があります
- [EC2.52] EC2 トランジットゲートウェイにはタグを付ける必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.13] ECS サービスはタグ付けする必要があります
- [ECS.14] ECS クラスターにはタグを付ける必要があります
- [ECS.15] ECS タスク定義にはタグを付ける必要があります
- [EFS .5] EFS アクセスポイントにはタグを付ける必要があります
- [EKS.6] EKS クラスターにはタグを付ける必要があります
- [EKS.7] EKS ID プロバイダーの設定にはタグを付ける必要があります
- [ES.9] Elasticsearch ドメインにはタグを付ける必要があります
- 〔EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります

- [Glue.1] AWS Glue ジョブにはタグを付ける必要があります
- 〔GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- 〔GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- 〔GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [IAM.23] IAM Access Analyzer アナライザーにはタグを付ける必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーはタグ付けする必要があります
- [IoT.1] AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [Kinesis.2] Kinesis ストリームにはタグを付ける必要があります
- [Lambda.6] Lambda 関数にはタグを付ける必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります
- 〔NetworkFirewall.7] Network Firewall ファイアウォールにはタグを付ける必要があります
- 〔NetworkFirewall.8] Network Firewall ファイアウォールポリシーにはタグを付ける必要があります
- [Opensearch.9] OpenSearch ドメインにはタグを付ける必要があります
- [RDS.28] RDS DB クラスターにはタグを付ける必要があります
- [RDS.29] RDS DB クラスタースナップショットにはタグを付ける必要があります
- [RDS.30] RDS DB インスタンスにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [RDS.32] RDS DB スナップショットにはタグを付ける必要があります
- [RDS.33] RDS DB サブネットグループにタグを付ける必要があります
- [Redshift.11] Redshift クラスターにはタグを付ける必要があります
- [Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります
- [Redshift.13] Redshift クラスタースナップショットにはタグを付ける必要があります
- [Redshift.14] Redshift クラスターサブネットグループにタグを付ける必要があります

- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- 〔SecretsManager.5] Secrets Manager のシークレットにはタグを付ける必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- [SNS.3] SNS トピックにはタグを付ける必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- 〔StepFunctions.2] Step Functions アクティビティにはタグを付ける必要があります
- [Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります

サービスマネージドスタンダード

サービスマネージド標準は、別の が AWS のサービス 管理するセキュリティ標準です。例えば、サービスマネージドスタンダード： AWS Control Tower は、 が AWS Control Tower 管理するサービスマネージドスタンダードです。サービスマネージドスタンダードは、 AWS Security Hub が管理するセキュリティ標準とは次の点で異なります。

- 標準の作成と削除 — 管理サービスのコンソールまたは API、または AWS CLIを使用して、サービスマネージドスタンダードを作成および削除します。いずれかの方法で管理サービスで標準を作成するまでは、その標準は Security Hub コンソールに表示されず、Security Hub API または AWS CLIからもアクセスできません。
- コントロールの自動有効化なし – サービスマネージドスタンダードを作成したとき、Security Hub および管理サービスは、標準に適用されるコントロールの自動有効化を行いません。また、Security Hub が標準で新しいコントロールをリリースするとき、それが自動有効化されることもありません。これは Security Hub が管理する標準からの逸脱です。Security Hub でコントロールを設定する通常の方法の詳細については、「セキュリティコントロールの表示と管理」を参照してください。
- コントロールの有効化と無効化 — ドリフトを防ぐために、管理サービスでコントロールを有効または無効にすることをお勧めします。
- コントロールの可用性 – 管理サービスは、サービスマネージドスタンダードの一部として使用できるコントロールを選択します。使用可能なコントロールには、既存の Security Hub コントロールのすべて、またはサブセットを含めることができます。

管理サービスがサービスマネージドスタンダードを作成し、そのコントロールを使用できるようになった後は、Security Hub コンソール、Security Hub API、または AWS CLIで、コントロールの検出

結果、コントロールステータス、標準セキュリティスコアにアクセス表示できます。この情報の一部または全部は、管理サービスで使用することもできます。

以下のリストからサービスマネージドスタンダードを選択すると、その詳細が表示されます。

サービスマネージドスタンダード

- サービスマネージドスタンダード： AWS Control Tower

サービスマネージドスタンダード： AWS Control Tower

このセクションでは、サービスマネージドスタンダード: について説明します AWS Control Tower。

サービスマネージドスタンダード AWS Control Towerとは

この標準は、 AWS Security Hub および のユーザー向けに設計されています AWS Control Tower。これにより、 AWS Control Tower サービスの Security Hub の検出コントロール AWS Control Tower とともに、 のプロアクティブコントロールを設定できます。

プロアクティブコントロールは、ポリシー違反や設定ミスにつながる可能性のあるアクションにフラグを付けるため、 がコンプライアンス AWS アカウント を維持するのに役立ちます。検出コントロールは、 AWS アカウント内のリソースのコンプライアンス違反 (設定ミスなど) を検出します。AWS 環境のプロアクティブコントロールと検出コントロールを有効にすることで、開発のさまざまな段階でセキュリティ体制を強化できます。

> **Tip**
>
> サービスマネージド標準は、 AWS Security Hub が管理する標準とは異なります。例えば、サービスマネージドスタンダードの作成および削除は、管理サービスで行う必要があります。詳細については、「サービスマネージドスタンダード」を参照してください。

Security Hub コンソールと API では、サービスマネージドスタンダード: AWS Control Tower と他の Security Hub 標準を表示できます。

標準の作成

この標準は、 で標準を作成する場合にのみ使用できます AWS Control Tower。 AWS Control Tower は、次のいずれかの方法を使用して、該当するコントロールを最初に有効にしたときに標準を作成します。

- AWS Control Tower コンソール
- AWS Control Tower API (EnableControl API を呼び出す)
- AWS CLI (enable-control コマンドを実行する)

Security Hub コントロールは、 AWS Control Tower コンソールで SH.*ControlID* (SH..1 など) として識別されますCodeBuild。

標準を作成するときに、Security Hub をまだ有効にしていない場合は、Security Hub AWS Control Tower も有効にします。

を設定していない場合、Security Hub コンソール AWS Control Tower、Security Hub API、またはでこの標準を表示またはアクセスすることはできません AWS CLI。をセットアップした場合でも AWS Control Tower、前述の方法のいずれか AWS Control Tower を使用して で標準を作成しないと、Security Hub でこの標準を表示またはアクセスすることはできません。

この標準は、 を含む AWS リージョンAWS Control Tower が利用可能な でのみ使用できます AWS GovCloud (US)。

標準のコントロールの有効化と無効化

AWS Control Tower コンソールで標準を作成したら、両方のサービスで標準とその使用可能なコントロールを表示できます。

最初に標準を作成すると、これに自動的に有効化されたコントロールはありません。さらに、Security Hub が新しいコントロールを追加すると、サービスマネージドスタンダード: に対してそれらが自動的に有効になることはありません AWS Control Tower。次のいずれかの方法 AWS Control Tower を使用して、 で標準のコントロールを有効または無効にする必要があります。

- AWS Control Tower コンソール
- AWS Control Tower API (EnableControlおよび DisableControl APIs)
- AWS CLI (コマンドenable-controlと disable-control コマンドを実行します)

でコントロールの有効化ステータスを変更すると AWS Control Tower、その変更は Security Hub にも反映されます。

ただし、 で有効になっている Security Hub でコントロールを無効にすると、コントロールドリフト AWS Control Tower が発生します。のコントロールステータスは と AWS Control Tower 表示されますDrifted。このドリフトは、 AWS Control Tower コンソールで OU の再登録を選択するか、前述

の方法のいずれか AWS Control Tower を使用して でコントロールを無効化および再有効化することで解決できます。

で有効化アクションと無効化アクションを完了すると、制御ドリフトを回避 AWS Control Tower できます。

でコントロールを有効または無効にすると AWS Control Tower、アクションはアカウントとリージョン全体に適用されます。Security Hub でコントロールを有効または無効にした場合 (標準では推奨されません)、アクションは現在のアカウントとリージョンにのみ適用されます。

> **Note**
>
> 中央設定は、サービスマネージドスタンダード: の管理には使用できません AWS Control Tower。中央設定を使用する場合は、 AWS Control Tower サービスのみを使用して、一元管理アカウントに対してこの標準のコントロールを有効または無効にできます。

有効化ステータスとコントロールステータスの表示

次のいずれかの方法を使用して、コントロールの有効化ステータスを表示できます。

- Security Hub コンソール、Security Hub API、または AWS CLI
- AWS Control Tower コンソール
- AWS Control Tower 有効なコントロールのリストを表示する API (`ListEnabledControls` API を呼び出す)
- AWS CLI 有効になっているコントロールのリストを表示するには (`list-enabled-controls` コマンドを実行)

で無効にしたコントロール AWS Control Tower は、Security Hub `Disabled`でそのコントロールを明示的に有効にしない限り、Security Hub で有効化ステータスが になります。

Security Hub は、ワークフローステータスおよびコントロール検出結果のコンプライアンスステータスに基づき、コントロールステータスを計算します。有効化ステータスとコントロールステータスの詳細については、「コントロールの詳細の表示」 を参照してください。

コントロールのステータスに基づいて、Security Hub はサービスマネージドスタンダード: のセキュリティスコアを計算します AWS Control Tower。このスコアは Security Hub のみで確認できます。また、Security Hub で表示できるのは統制結果のみです。標準セキュリティスコアとコントロールの検出結果は、 では使用できません AWS Control Tower。

> **Note**
>
> サービスマネージドスタンダード: のコントロールを有効にすると AWS Control Tower、Security Hub が既存の AWS Config サービスにリンクされたルールを使用するコントロールの検出結果を生成するまでに最大 18 時間かかる場合があります。Security Hub で他の標準やコントロールを有効にしている場合、既存のサービスリンクルールが存在する可能性があります。詳細については、「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。

標準を削除する

次のいずれかの方法を使用して、該当するすべてのコントロールを無効にする AWS Control Tower ことで、 でこの標準を削除できます。

- AWS Control Tower コンソール
- AWS Control Tower API (`DisableControl` API を呼び出す)
- AWS CLI (`disable-control` コマンドを実行する)

すべてのコントロールを無効にすることにより、 AWS Control Tower のすべてのマネージドアカウントと管理対象リージョンの標準が削除されます。で標準を削除すると AWS Control Tower 、Security Hub コンソールの標準ページから削除され、Security Hub API または を使用して標準にアクセスできなくなります AWS CLI。

> **Note**
>
> Security Hub で標準のすべてのコントロールを無効にしても、標準が無効化または削除されることはありません。

Security Hub サービスを無効にする AWS Control Tower と、サービスマネージドスタンダード および有効化したその他の標準が削除されます。

サービスマネージドスタンダードの検出結果フィールド形式： AWS Control Tower

サービスマネージドスタンダード: を作成し、そのコントロールを有効にする AWS Control Tower と、Security Hub でコントロールの検出結果を受信し始めます。Security Hub は、AWS Security

Finding 形式 (ASFF) で統制結果をレポートします。これらは、この標準の Amazon リソースネーム (ARN) および GeneratorId の ASFF 値です。

- 標準 ARN — *arn:aws:us-east-1*:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0
- GeneratorId – service-managed-aws-control-tower/v/1.0.0/*CodeBuild.1*

サービスマネージドスタンダード: の検出結果のサンプルについては AWS Control Tower、「」を参照してくださいコントロールの検出結果のサンプル。

サービスマネージドスタンダードに適用されるコントロール： AWS Control Tower

サービスマネージドスタンダード: AWS Foundational Security Best Practices (FSBP) 標準の一部であるコントロールのサブセット AWS Control Tower をサポートします。次の表からコントロールを選択すると、失敗した結果の修正手順など、そのコントロールに関する情報が表示されます。

次のリストは、サービスマネージドスタンダードで使用可能なコントロールを示しています AWS Control Tower。コントロールに対するリージョンの制限は、FSBP 標準のコロラリーコントロールに対するリージョンの制限と一致します。このリストには、標準に依存しないセキュリティコントロール ID が表示されます。 AWS Control Tower コンソールでは、コントロール IDs は SH.***ControlID*** (SH..1 など) としてフォーマットされますCodeBuild。Security Hub では、[統合されたコントロールの検出結果] が無効になっている場合、ProductFields.ControlId フィールドに標準ベースのコントロール ID が使用されます。標準ベースのコントロール ID は CT としてフォーマットされます***ControlId*** (例えば、CT..1)CodeBuild。

- [Account.1] のセキュリティ連絡先情報を に提供する必要があります AWS アカウント
- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [APIGateway.1] API Gateway REST と WebSocket API 実行のログ記録を有効にする必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります
- [APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります

- [APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります
- [APIGateway.5] API Gateway REST API のキャッシュデータは、保管中に暗号化する必要があります
- [APIGateway.8] API Gateway ルートには認証タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- 〔AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- 〔AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要があります
- 〔AutoScaling.2] Amazon EC2 Auto Scaling グループは複数のアベイラビリティーゾーンをカバーする必要があります
- 〔AutoScaling.3] Auto Scaling グループの起動設定では、インスタンスメタデータサービスバージョン 2 (IMDSv2) を要求するように EC2 インスタンスを設定する必要がありますIMDSv2
- [Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません
- 〔AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります
- 〔AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります
- 〔CloudTrail.1] CloudTrail 読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン追跡を有効にして設定する必要があります
- 〔CloudTrail.2] 保管時の暗号化を有効にする CloudTrail 必要があります
- 〔CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります
- 〔CloudTrail.5] CloudTrail 証跡は Amazon CloudWatch Logs と統合する必要があります
- 〔CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットがパブリックにアクセスできないようにする
- 〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください
- 〔CodeBuild.2] CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください
- 〔CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- 〔CodeBuild.4] CodeBuild プロジェクト環境にはログ記録 AWS Config設定が必要です

- [DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラススナップショットはパブリックにできません
- [DynamoDB.1] DynamoDB テーブルは、需要に応じて容量をオートスケーリングする必要があります
- [DynamoDB.2] DynamoDB テーブルでは point-in-time リカバリを有効にする必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [EC2.1] Amazon EBS スナップショットはパブリックに復元できないようにすることをお勧めします
- [EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします
- [EC2.3] アタッチされた Amazon EBS ボリュームは、保管時に暗号化することをお勧めします
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします
- [EC2.7] EBS のデフォルト暗号化を有効にすることをお勧めします
- [EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.9] Amazon EC2 インスタンスは、パブリック IPv4 アドレスを未設定にすることをお勧めします
- [EC2.10] Amazon EC2 サービス用に作成された VPC エンドポイントを使用するようにAmazon EC2 を設定することをお勧めします
- [EC2.15] Amazon EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないことをお勧めします
- [EC2.16] 未使用のネットワークアクセスコントロールリストを削除することをお勧めします
- [EC2.17] Amazon EC2 インスタンスが複数の ENI を使用しないようにすることをお勧めします
- [EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします

- [EC2.19] セキュリティグループは、リスクの高いポートへの無制限アクセスを許可してはいけません
- [EC2.20] AWS Site-to-Site VPN 接続の両方の VPN トンネルが稼働している必要があります
- [EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。
- [ECS.2] ECS サービスには、パブリック IP アドレスを自動で割り当てないでください
- [ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください
- [ECS.4] ECS コンテナは、非特権として実行する必要があります
- [ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。
- [ECS.8] シークレットは、コンテナ環境の変数として渡さないでください
- [ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。
- [ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります
- [EFS .1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります

- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- Redis ElastiCache レプリケーショングループの [ElastiCache.3] では、自動フェイルオーバーを有効にする必要があります
- 〔ElastiCache.4] ElastiCache for Redis レプリケーショングループは保管時に暗号化する必要があります
- Redis ElastiCache レプリケーショングループの [ElastiCache.5] は転送中に暗号化する必要があります
- 〔ElastiCache.6]バージョン ElastiCache 6.0 より前の Redis レプリケーショングループでは、Redis AUTH を使用する必要があります
- 〔ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります
- 〔ElasticBeanstalk.2] Elastic Beanstalk マネージドプラットフォームの更新を有効にする必要があります
- [ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.3] Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります
- [ELB.4] Application Load Balancer は、http ヘッダーを削除するように設定する必要があります
- [ELB.5] アプリケーションおよび Classic Load Balancer のログ記録を有効にする必要があります
- [ELB.6] Application、Gateway、Network Load Balancer では、削除保護を有効にする必要があります
- [ELB.7] Classic Load Balancers は、Connection Draining を有効にする必要があります
- [ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な AWS Config設定を持つ事前定義されたセキュリティポリシーを使用する必要があります
- [ELB.9] Classic Load Balancer では、クロスゾーンロードバランシングが有効になっている必要があります

- [ELB.10] Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります
- [ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります
- [ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります
- [ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります
- [ES.4] Logs への Elasticsearch CloudWatch ドメインエラーのログ記録を有効にする必要があります
- [ES.5] Elasticsearch ドメインで監査ログ記録が有効になっている必要があります
- [ES.6] Elasticsearch ドメインには少なくとも 3 つのデータノードが必要です
- [ES.7] Elasticsearch ドメインは、少なくとも 3 つの専用マスターノードを設定する必要があります。
- [ES.8] Elasticsearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- 〔EventBridge.3] EventBridge カスタムイベントバスには、リソースベースのポリシーがアタッチされている必要があります
- 〔GuardDuty.1] GuardDuty を有効にする必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります

- [IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [KMS.3] 意図せずに削除 AWS KMS keys しないでください
- [KMS.4] AWS KMS キーローテーションを有効にする必要があります
- [Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります
- [Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります
- [Lambda.3] Lambda 関数は VPC 内に存在する必要があります
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- 〔NetworkFirewall.3] Network Firewall ポリシーには、少なくとも 1 つのルールグループが関連付けられている必要があります

- 〔NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、フルパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、フラグメント化されたパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.6] ステートレス Network Firewall ルールグループは空にしないでください
- [Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [RDS.1] RDS スナップショットはプライベートである必要があります
- [RDS.2] RDS DB インスタンスは、 PubliclyAccessible AWS Config設定によって決定されるパブリックアクセスを禁止する必要があります
- [RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。
- [RDS.4] RDS クラスタースナップショットとデータベーススナップショットは保管中に暗号化する必要があります
- [RDS.5] RDS DB インスタンスは、複数のアベイラビリティーゾーンで設定する必要があります
- [RDS.6] RDS DB インスタンスの拡張モニタリングを設定する必要があります
- [RDS.8] RDS DB インスタンスで、削除保護が有効になっている必要があります
- [RDS.9] RDS DB インスタンスはログを CloudWatch Logs に発行する必要があります
- [RDS.10] IAM 認証は RDS インスタンス用に設定する必要があります
- [RDS.11] RDS インスタンスでは、自動バックアップが有効になっている必要があります
- [RDS.12] IAM 認証は RDS クラスター用に設定する必要があります
- [RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります

- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります
- [RDS.17] RDS DB インスタンスは、タグをスナップショットにコピーするように設定する必要があります
- [RDS.18] RDS インスタンスは VPC 内にデプロイする必要があります
- [RDS.19] 重大なクラスターイベントについて、既存の RDS イベント通知サブスクリプションを設定する必要があります
- [RDS.20] 重大なデータベースインスタンスイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります
- [RDS.21] 重大なデータベースパラメータグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります
- [RDS.22] 重大なデータベースセキュリティグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります
- [RDS.23] RDS インスタンスはデータベースエンジンのデフォルトポートを使用しないようにする必要があります
- [RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります
- [Redshift.2] Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります
- [Redshift.4] Amazon Redshift クラスターでは、監査ログ記録が有効になっている必要があります
- [Redshift.6] Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります
- [Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります
- [Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください
- [Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります
- [S3.2] S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります
- [S3.3] S3 汎用バケットはパブリック書き込みアクセスをブロックする必要があります
- [S3.5] S3 汎用バケットでは、SSL を使用するリクエストが必要です

- [S3.6] S3 汎用バケットポリシーでは、他の へのアクセスを制限する必要があります AWS アカウント
- [S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります
- [S3.9] S3 汎用バケットでは、サーバーアクセスのログ記録を有効にする必要があります
- [S3.12] ACLs を使用しないでください S3
- [S3.13] S3 汎用バケットにはライフサイクル設定が必要です
- [S3.17] S3 汎用バケットは、保管時に で暗号化する必要があります AWS KMS keys
- 〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません
- 〔SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- 〔SageMaker.3] SageMaker ユーザーはノートブックインスタンスへのルートアクセスを許可されない
- 〔SecretsManager.1] Secrets Manager シークレットでは、自動ローテーションを有効にする必要があります
- 〔SecretsManager.2] 自動ローテーションで設定された Secrets Manager シークレットは正常にローテーションする必要があります
- 〔SecretsManager.3] 未使用の Secrets Manager シークレットを削除する
- 〔SecretsManager.4] Secrets Manager のシークレットは、指定された日数内にローテーションする必要があります
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [SSM.4] SSM ドキュメントはパブリックにしないでください
- [WAF.2] AWS WAF クラシックリージョンルールには少なくとも 1 つの条件が必要です
- [WAF.3] AWS WAF クラシックリージョンルールグループには、少なくとも 1 つのルールが必要です
- [WAF.4] AWS WAF クラシックリージョンウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

この標準の詳細については、「AWS Control Tower ユーザーガイド」の「Security Hub controls」(Security Hub コントロール) を参照してください。

セキュリティ標準の表示と管理

セキュリティ標準には、規制フレームワーク、業界のベストプラクティス、または企業ポリシーへの準拠を判断するための一連の要件が含まれています。 は、これらの要件をコントロールに AWS Security Hub マッピングし、コントロールでセキュリティチェックを実行して、標準の要件が満たされているかどうかを評価します。コントロールは 1 つ以上の標準で有効になっている場合があります。[統合されたコントロールの検出結果] を有効にすると、コントロールが複数の有効化された標準の一部である場合でも、Security Hub はセキュリティチェックあたり 1 つの検出結果を生成します。詳細については、「統合されたコントロールの検出結果」を参照してください。

利用可能な標準とそれらに適用されるコントロールの一覧については、標準リファレンス を参照してください。Security Hub コンソールの [セキュリティ基準] ページには、Security Hub でサポートされているすべてのセキュリティ標準とその有効化ステータスも表示されます。アカウントで有効になっている各セキュリティ標準 (または との統合を使用する場合は、組織内の少なくとも 1 つのアカウント) について AWS Organizations、次の情報を表示できます。

- 中央設定を使用する場合の、さまざまな Security Hub 設定ポリシーにおける標準の有効化ステータス
- 無効になっている標準の説明
- 標準で現在有効になっているコントロールのリストと、検出結果のコンプライアンスステータスに基づくコントロールの全体的なステータス
- 標準に適用されているが、現在無効になっているコントロールのリスト
- 標準のセキュリティスコア

Security Hub は、各標準のセキュリティスコアを生成します。管理者アカウントには、そのメンバーアカウント全体の、集約されたセキュリティスコアとコントロールステータスが表示されます。集約リージョンを設定すると、セキュリティスコアに、リンクされているリージョンすべてのコントロールのコンプライアンスステータスが反映されます。詳細については、「セキュリティスコアの計算方法」を参照してください。

トピック

セキュリティ標準の有効化および無効化

Security Hub で利用可能な各セキュリティ標準を有効化または無効化できます。

セキュリティ標準を有効にする前に、リソース記録を有効に AWS Config して設定していることを確認してください。確認されていない場合、標準に適用されるコントロールの検出結果を Security Hub が生成できない可能性があります。詳細については、「の設定 AWS Config」を参照してください。

> **Note**
>
> 標準を有効または無効にする手順は、中央設定を使用するかどうかによって異なります。このセクションでは、その違いについて説明します。Security Hub と を統合するユーザーは、中央設定を使用できます AWS Organizations。マルチアカウント、マルチリージョン環境で標準を有効または無効にするプロセスを簡略化するために、中央設定を使用することをお勧めします。

セキュリティ標準の有効化

セキュリティ標準を有効にすると、その標準に適用されるすべてのコントロールが自動的に有効になります。Security Hub は、標準に適用されるコントロールの検出結果の生成も開始します。

それぞれの標準で有効または無効にするコントロールを選択することができます。コントロールを無効にすると、コントロールの検出結果の生成が停止し、セキュリティスコアの計算時にコントロールが無視されます。

Security Hub を有効にすると、Security Hub は、Security Hub コンソールの [Summary] (概要) ページまたは [Security standards] (セキュリティ標準) ページへの最初のアクセスから 30 分以内に最初の標準のセキュリティスコアを計算します。中国リージョンおよび AWS GovCloud (US) Regionでは、最初のセキュリティスコアが作成されるまで、最大 24 時間かかる場合があります。スコアは、これらのページにアクセスしたときに有効になっている標準に対してのみ生成されます。さらに、スコアが表示されるように AWS Config リソース記録を設定する必要があります。最初のスコア生成の後、Security Hub はセキュリティスコアを 24 時間毎に更新します。Security Hub には、セキュリ

ティスコアが最後に更新されたときの時刻が表示されます。アカウントで現在有効になっている標準のリストを表示するには、GetEnabledStandards API を呼び出します。

複数のアカウントおよびリージョンで標準を有効にする

複数のアカウントおよび でセキュリティ標準を有効にするには AWS リージョン、中央設定 を使用する必要があります。

中央設定を使用する場合、委任管理者は 1 つ以上の標準を有効にする Security Hub 設定ポリシーを作成できます。そして、設定ポリシーを特定のアカウントや組織単位 (OU)、またはルートに関連付けることができます。設定ポリシーは、ホームリージョン (集約リージョンとも呼ばれる) およびリンクされているすべてのリージョンで有効になります。

設定ポリシーではカスタマイズが可能です。例えば、1 つの OU で AWS Foundational Security Best Practices (FSBP) のみを有効にし、別の OU で FSBP と Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 を有効にできます。指定された標準を有効にする設定ポリシーの作成手順については、「Security Hub 設定ポリシーの作成と関連付け」を参照してください。

中央設定を使用する場合、Security Hub は新規または既存のアカウントの標準を自動的に有効にしません。代わりに、設定ポリシーを作成するときに、委任管理者がさまざまなアカウントでどの標準を有効にするかを定義します。Security Hub では、FSBP のみを有効にする推奨設定ポリシーが提供されています。詳細については、「設定ポリシーのタイプ」を参照してください。

> **Note**
>
> 委任管理者は、サービスマネージドスタンダード: 以外の標準 AWS Control Towerを有効にする設定ポリシーを作成できます。この標準は、 AWS Control Tower サービスでのみ有効にできます。中央設定を使用する場合、この標準のコントロールは、 AWS Control Towerで一元管理されたアカウントに対してのみ有効または無効にできます。

委任管理者ではなく一部のアカウントに独自の標準を設定させたい場合は、委任管理者がそれらのアカウントをセルフマネージドとして指定できます。セルフマネージドアカウントは、リージョンごとに標準を個別に設定する必要があります。

1 つのアカウントおよびリージョンで標準を有効にする

中央設定を使用していない場合、またはセルフマネージドアカウントの場合、設定ポリシーを使用して複数のアカウントおよびリージョンで標準を一元的に有効にすることはできません。ただし、次の手順を使用して、1 つのアカウントおよびリージョンで標準を有効にすることができます。

Security Hub console

1 つのアカウントおよびリージョンで標準を有効にするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. 標準を有効にするリージョンで Security Hub を使用していることを確認します。
3. Security Hub ナビゲーションペインで、[Security standards] (セキュリティ標準) を選択します。
4. 有効にする標準に対して、[Enable] (有効化) を選択します。これでその標準内に存在するすべてのコントロールも有効になります。
5. 標準を有効にするリージョンごとに、これらの手順を繰り返します。

Security Hub API

1 つのアカウントおよびリージョンで標準を有効にするには

1. BatchEnableStandards API を呼び出します。
2. 有効化する標準の Amazon リソースネーム (ARN) を提供します。標準 ARN を取得するには、DescribeStandards API を呼び出します。
3. 標準を有効にするリージョンごとに、これらの手順を繰り返します。

AWS CLI

1 つのアカウントおよびリージョンで標準を有効にするには

1. batch-enable-standards コマンドを実行します。
2. 有効化する標準の Amazon リソースネーム (ARN) を提供します。標準 ARN を取得するには、describe-standards コマンドを実行します。

```
aws securityhub batch-enable-standards --standards-subscription-requests
 '{"StandardsArn": "standard ARN"}'
```

例

```
aws securityhub batch-enable-standards --standards-subscription-requests
 '{"StandardsArn":"arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"}'
```

3. 標準を有効にするリージョンごとに、これらの手順を繰り返します。

デフォルトのセキュリティ標準を自動的に有効にする

中央設定を使用しない場合、Security Hub は、新しいアカウントが組織に参加したときに、そのアカウントのデフォルトのセキュリティ標準を自動的に有効にします。デフォルトの標準に含まれるすべてのコントロールも自動的に有効になります。現在、自動的に有効になるデフォルトのセキュリティ標準は、 AWS Foundational Security Best Practices (FSBP) と Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 です。新規アカウントの標準を手動で有効にしたい場合は、標準の自動有効化をオフにできます。

中央設定を使用する場合は、デフォルトの標準を有効にする設定ポリシーを作成し、このポリシーをルートに関連付けることができます。組織アカウントと OU は、別のポリシーに関連付けられている場合やセルフマネージドの場合を除き、すべてこの構成ポリシーを継承します。

標準の自動有効化をオフにする

以下の手順は、 と統合している AWS Organizations が、中央設定を使用しない場合にのみ適用されます。Organizations 統合を使用しない場合は、Security Hub を最初に有効にするときにデフォルトの標準をオフにするか、標準を無効にするためのステップを使用することができます。

Security Hub console

標準の自動有効化をオフにするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   管理者アカウントの認証情報を使用してサインインします。
2. Security Hub のナビゲーションペインの [設定] で、[設定] を選択します。
3. [アカウント] セクションで、[デフォルトの標準を自動的に有効にする] をオフにします。

Security Hub API

標準の自動有効化をオフにするには

1. Security Hub 管理者アカウントで、UpdateOrganizationConfiguration API を呼び出します。
2. 新規メンバーアカウントで、標準の自動有効化をオフにするには、`AutoEnableStandards` を `NONE` に等しい値に設定します。

AWS CLI

標準の自動有効化をオフにするには

1. update-organization-configuration コマンドを実行します。
2. `auto-enable-standards` パラメータを含めて、新規メンバーアカウントでの標準の自動有効化をオフにします。

```
aws securityhub update-organization-configuration --auto-enable-standards
```

セキュリティ標準の無効化

Security Hub でセキュリティ標準を無効にすると、次のようになります。

- その標準に適用されるすべてのコントロールも、他の標準と関連付けられていない限り無効になります。
- 無効化されたコントロールのチェックは実行されなくなります。また、無効化されたコントロールの追加の検出結果は生成されません。
- 無効化されたコントロールの既存の検出結果は、約 3～5 日後に自動的にアーカイブされます。
- 無効化されたコントロールに対して Security Hub が作成した AWS Config ルールは削除されます。

  これは通常、標準を無効にしてから数分以内に発生しますが、時間がかかる場合があります。AWS Config ルールを削除する最初のリクエストが失敗した場合、Security Hub は 12 時間ごとに再試行します。ただし、Security Hub を無効にした場合、または他の標準を有効にしていない場合、Security Hub はこのリクエストを再試行できません。つまり、 AWS Config ルールは削除できません。これが発生し、 AWS Config ルールを削除する必要がある場合は、 にお問い合わせください AWS Support。

複数のアカウントおよびリージョンで標準を無効にする

複数のアカウントおよびリージョンでセキュリティ標準を無効にするには、中央設定を使用する必要があります。

中央設定を使用する場合、委任管理者は 1 つ以上の標準を無効にする設定ポリシーを作成できます。そして、設定ポリシーを特定のアカウントや OU、またはルートに関連付けることができます。

設定ポリシーは、ホームリージョン (集約リージョンとも呼ばれる) およびリンクされているすべてのリージョンで有効になります。

設定ポリシーではカスタマイズが可能です。例えば、ある OU では Payment Card Industry Data Security Standard (PCI DSS) を無効にするように選択し、別の OU では PCI DSS と米国国立標準技術研究所 (NIST) SP 800-53 Rev. 5 の両方を無効にするように選択することができます。指定された標準を無効にする設定ポリシーの作成手順については、「Security Hub 設定ポリシーの作成と関連付け」を参照してください。

> **Note**
>
> 委任管理者は、サービスマネージドスタンダード: 以外の標準 AWS Control Towerを無効にする設定ポリシーを作成できます。この標準は、 AWS Control Tower サービスでのみ無効にできます。中央設定を使用する場合、この標準のコントロールは、 AWS Control Towerで一元管理されたアカウントに対してのみ有効または無効にできます。

委任管理者ではなく一部のアカウントに独自の標準を設定させたい場合は、委任管理者がそれらのアカウントをセルフマネージドとして指定できます。セルフマネージドアカウントは、リージョンごとに標準を個別に設定する必要があります。

1 つのアカウントおよびリージョンで標準を無効にする

中央設定を使用していない場合、またはセルフマネージドアカウントの場合、設定ポリシーを使用して複数のアカウントおよびリージョンで標準を一元的に無効にすることはできません。ただし、次の手順を使用して、1 つのアカウントおよびリージョンで標準を無効にすることができます。

Security Hub console

1 つのアカウントおよびリージョンで標準を無効にするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. 標準を無効にするリージョンで Security Hub を使用していることを確認します。
3. Security Hub ナビゲーションペインで、[Security standards] (セキュリティ標準) を選択します。
4. 無効にする標準に対して、[Disable] (無効化) を選択します。
5. 標準を無効にするリージョンごとに、これらの手順を繰り返します。

Security Hub API

1 つのアカウントおよびリージョンで標準を無効にするには

1. BatchDisableStandards API を呼び出します。
2. 無効化する各標準に対し、標準サブスクリプションの ARN を提供します。有効な標準のサブスクリプション ARN を取得するには、GetEnabledStandards API を呼び出します。
3. 標準を無効にするリージョンごとに、これらの手順を繰り返します。

AWS CLI

1 つのアカウントおよびリージョンで標準を無効にするには

1. batch-disable-standards コマンドを実行します。
2. 無効化する各標準に対し、標準サブスクリプションの ARN を提供します。有効な標準のサブスクリプション ARN を取得するには、get-enabled-standards コマンドを実行します。

```
aws securityhub batch-disable-standards --standards-subscription-arns "standard
 subscription ARN"
```

例

```
aws securityhub batch-disable-standards --standards-subscription-arns
 "arn:aws:securityhub:us-west-1:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0"
```

3. 標準を無効にするリージョンごとに、これらの手順を繰り返します。

標準の詳細の表示

AWS Security Hub コンソールでは、標準の詳細ページに次の情報が含まれます。

- 標準セキュリティスコアと、その標準で有効化されたコントロールのセキュリティチェックの視覚的要約。と統合すると AWS Organizations、少なくとも 1 つの組織アカウントで有効になっているコントロールが有効と見なされます。
- 標準に適用されるコントロールを有効または無効にする設定。

- 標準に適用されるコントロールのリスト。コントロールは、有効化のステータスに基づき、いくつかのタブに分かれています。[すべて有効] 列のコントロールの数は、[失敗]、[不明]、[データなし]、[合格] の各列におけるコントロールの合計です。

Security Hub API および を使用して AWS CLI 、標準の詳細を取得することもできます。次のセクションでは、標準の詳細を取得する方法について説明します。

有効化された標準の詳細ページの表示 (コンソール)

[セキュリティ基準] ページから、有効化された標準の詳細ページを表示できます。

管理者アカウントにサインインしている場合、1 つ以上のメンバーアカウントで有効化されたすべての標準の詳細を確認できます。

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. Security Hub ナビゲーションペインで、[Security standards] (セキュリティ標準) を選択します。
3. 詳細を表示したい標準で、[View results] (結果の表示) を選択します。

標準セキュリティスコアとセキュリティチェックの概要

標準の詳細ページの上部には、標準のセキュリティスコアが表示されます。スコアは、有効化された (データのある) 標準のコントロールに対して、合格の状態にあるコントロールの割合を示します。

Security Hub は、Security Hub コンソールの [Summary] (概要) ページまたは [Security standards] (セキュリティ標準) ページへの最初のアクセスから 30 分以内に最初のセキュリティスコアを計算します。スコアは、これらのページにアクセスしたときに有効になっている標準に対してのみ生成されます。現在有効になっている標準のリストを表示するには、`GetEnabledStandards` API オペレーションを使用します。また、スコアを表示するには、 AWS Config リソースレコードを設定する必要があります。最初のスコア生成の後、Security Hub はセキュリティスコアを 24 時間毎に更新します。Security Hub には、セキュリティスコアが最後に更新されたときの時刻が表示されます。詳細については、「the section called “セキュリティスコアの決定”」を参照してください。

> **Note**
>
> 中国リージョンおよび AWS GovCloud (US) Regionでは、最初のセキュリティスコアが作成されるまで、最大 24 時間かかる場合があります。

スコアの隣には、標準で有効化されているコントロールのセキュリティチェックの概要図が表示されます。この図には、不合格となったセキュリティチェックと合格したセキュリティチェックの割合が表示されます。図を一時停止すると、ポップアップに次の情報が表示されます。

- 各重要度のコントロールの不合格になったセキュリティチェックの数
- ステータスが [不明] になっているコントロールのセキュリティチェックの数
- 合格したセキュリティチェックの数

管理者アカウントの場合、標準のスコアと図は、管理者アカウントとメンバーアカウントの両方を合わせて集計されます。

集約リージョンを設定している場合を除き、[Security standards] (セキュリティ標準) の詳細ページにあるデータはすべて現在のリージョンに固有のものとなります。集約リージョンを設定している場合、セキュリティスコアは、リージョン全体に適用され、リンクされたすべてのリージョンの検出結果を含みます。標準の詳細ページにあるコントロールのコンプライアンスステータスには、リンクされたリージョンの結果も反映されており、セキュリティチェックの数には、リンクされたリージョンの結果が含まれています。

有効化された標準のコントロールの表示

標準の詳細ページに移動すると、その標準に適用されるセキュリティコントロールのリストが表示されます。このリストは、コントロールの現在のコンプライアンスステータスと、各コントロールに割り当てられた重要度に基づいてソートされます。Security Hub では 24 時間ごとにコントロールステータスとセキュリティチェック数が更新されます。各タブのタイムスタンプは、コントロールステータスとセキュリティチェック数が最後に更新された日時を示します。詳細については、「the section called “コンプライアンスステータスとコントロールステータス”」を参照してください。

管理者アカウントの場合、コントロールコンプライアンスのステータスとセキュリティチェック数は、管理者アカウントとメンバーアカウントの両方を合わせて集計されます。

[すべて有効] タブには、標準で現在有効になっているコントロールがすべて一覧表示されます。管理者アカウントの場合、[すべて有効] タブには、アカウントまたは 1 つ以上のメンバーアカウントの標準で有効になっているコントロールが含まれています。

[失敗]、[不明]、[データなし]、[合格] タブでは、[すべて有効] タブからのコントロールは特定のステータスの有効なコントロールのみを含むようにフィルタリングされます。

[無効] タブには、標準で無効になっているコントロールの一覧が含まれます。管理者アカウントの場合、[無効] タブには、アカウントまたはすべてのメンバーアカウントの標準で無効になっているコントロールが含まれています。

各コントロールについて、タブには次の情報が表示されます。

- コントロールのステータス (「the section called “コンプライアンスステータスとコントロールステータス”」を参照)
- コントロールに関連付けられた重要度
- コントロール ID とタイトル
- アクティブな検出結果の合計数のうち、不合格となったアクティブな検出結果の数。該当する場合は、[Failed checks] (不合格になったチェック) 列に、ステータスが [Unknown] (不明) の結果の数も表示されます。

各タブの検索フィルターに加えて、以下のフィールドに基づきリストをソートできます。

- コンプライアンス状況
- 重要度
- ID
- [Title] (タイトル)
- 不合格のチェック

任意の列を使用して各リストをソートできます。デフォルトでは、[All enabled] (すべて有効) タブは、不合格になったコントロールがリストの上部に表示されるようにソートされます。これにより、修復が必要な問題にすぐに焦点を当てることができます。

他のタブでは、コントロールはデフォルトで重要度の降順でソートされます。言い換えると、非常事態のコントロールが最初にあり、次に重要度が高、中、低のコントロールが続きます。

お好みのアクセス方法を選択し、以下の手順に従って、有効な標準で利用できるコントロールを表示します。これらの手順の代わりに、 DescribeStandardsControl API オペレーションを使用することもできます。

Security Hub console

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. ナビゲーションペインで、[セキュリティ基準] を選択します。

3. 標準の [結果を表示する] を選択します。ページの下部に、標準に適用されるコントロール (タブ区切り) が一覧表示されます。

Security Hub API

1. ListSecurityControlDefinitions を実行し、標準 Amazon リソースネーム (ARN) を提供して、その標準のコントロール ID 一覧を取得します。標準 ARN を取得するには、DescribeStandards を実行します。標準 ARN を提供しない場合、この API はすべての Security Hub コントロール ID を返します。この API は、標準固有のコントロール ID ではなく、標準に依存しないセキュリティコントロール ID を返します。

   リクエストの例:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. ListStandardsControlAssociations を実行して、アカウントで有効にした各標準でコントロールが有効になっているかどうかを確認します。
3. SecurityControlId または SecurityControlArn を提供してコントロールを特定します。ページ分割パラメータはオプションです。

   リクエストの例:

   ```
   {
       SecurityControlId: Config.1
       NextToken: lkeyusdlk-sdlflsnd-ladfterb
       MaxResults: 5
   }
   ```

AWS CLI

1. list-security-control-definitions コマンドを実行し、1 つ以上の標準 ARN を提供してコントロール ID のリストを取得します。標準 ARN を取得するには、describe-standards コマンドを実行します。標準 ARN を提供しない場合、このコマンドはすべての Security Hub コントロール ID を返します。このコマンドは、標準固有のコントロール ID ではなく、標準に依存しないセキュリティコントロール ID を返します。

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. list-standards-control-associations コマンドを実行して、アカウントで有効にした各標準でコントロールが有効になっているかどうかを確認します。
3. security-control-id または security-control-arn を提供してコントロールを特定します。

   コマンドの例:

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id Config.1
```

コントロールリストのダウンロード

コントロールリストの現在のページを .csv ファイルにダウンロードできます。

コントロールリストをフィルタリングした場合、ダウンロードされたファイルには、フィルター設定に一致するコントロールのみが含まれます。

特定のコントロールをリストから選択した場合、ダウンロードされたファイルにはそのコントロールのみが含まれます。

コントロールリストの現在のページ、または現在選択されているコントロールをダウンロードするには、[ダウンロード] を選択します。

特定の標準コントロールの有効化と無効化

で標準を有効にすると AWS Security Hub、その標準に適用されるすべてのコントロールがその標準で自動的に有効になります (ただし、サービスマネージド標準は例外です)。その後、標準内の特定のコントロールを無効化または再有効化できます。ただし、有効なすべての標準でコントロールの有効化ステータスを一致させることをお勧めします。

> **Note**
>
> Security Hub の中央設定を使用する場合、委任管理者は、有効なすべての標準で組織アカウントのコントロールを有効または無効にできます。コントロールの有効化ステータスが標準間で統一されるように、この方法を使用することをお勧めします。ただし、委任管理者は、

アカウントをセルフマネージドとして指定できます。これにより、特定の標準のコントロールを有効または無効にすることができます。詳細については、「中央設定の仕組み」を参照してください。

標準の詳細ページには、その標準に適用されるコントロールの一覧と、その標準で現在有効化されているコントロールと無効化されているコントロールに関する情報が含まれます。

また、標準の詳細ページで、特定の標準のコントロールを有効または無効にすることもできます。コントロールは、 と のそれぞれで個別に有効 AWS アカウント または無効にする必要があります AWS リージョン。コントロールを有効または無効にした場合、現在のアカウントとリージョンにのみ影響します。

Security Hub コンソール、Security Hub API、または を使用して、各リージョンでコントロールを有効または無効にできます AWS CLI。集約リージョンを設定すると、リンクされたすべてのリージョンのコントロールが表示されます。リンクされたリージョンでコントロールを使用できるが、集約リージョンでは使用できない場合は、集約リージョンからそのコントロールを有効または無効にすることはできません。マルチアカウントおよびマルチリージョンコントロールの無効化スクリプトについては、「マルチアカウント環境で Security Hub コントロールを無効にする」を参照してください。

特定の標準のコントロールを有効にする

標準のコントロールを有効にするには、まず、そのコントロールが適用される標準を少なくとも 1 つ有効にする必要があります。標準の有効化の詳細については「セキュリティ標準の有効化および無効化」を参照してください。標準でコントロールを有効にすると、 はそのコントロールの検出結果の生成 AWS Security Hub を開始します。Security Hub では、全体のセキュリティスコアと標準セキュリティスコアの計算にコントロールステータスを含みます。コントロールを複数の標準で有効にしている場合でも、コントロール検出結果を統合して有効にすると、標準全体のセキュリティチェックごとに 1 つの検出結果を受け取ることができます。詳細については、統合コントロールの検出結果を参照してください。

標準でコントロールを有効にするには、そのコントロールが現在のリージョンで使用可能である必要があります。詳細については、「リージョン別のコントロールの可用性」を参照してください。

以下の手順に従って、特定の標準で Security Hub コントロールを有効にします。以下の手順の代わりに、`UpdateStandardsControl` API アクションを使用して特定の標準のコントロールを有効にすることもできます。すべての標準でコントロールを有効にする手順については、「1 つのアカウントおよびリージョンのすべての標準でコントロールを有効にする」を参照してください。

Security Hub console

特定の標準のコントロールを有効にするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. ナビゲーションペインで、[セキュリティ基準] を選択します。
3. 該当する標準の [結果を表示する] を選択します。
4. コントロールを選択します。
5. [コントロールの有効化] を選択します (このオプションは、既に有効になっているコントロールには表示されません)。[有効化] を選択して確定します。

Security Hub API

特定の標準のコントロールを有効にするには

1. ListSecurityControlDefinitions を実行して標準 ARN を提供すると、特定の標準で利用できるコントロールのリストが表示されます。標準 ARN を取得するには、DescribeStandards を実行します。この API は、標準固有のコントロール ID ではなく、標準に依存しないセキュリティコントロール ID を返します。

   リクエストの例:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. ListStandardsControlAssociations を実行し、特定のコントロール ID を提供すると、各標準のコントロールの現在の有効化ステータスが返されます。

   リクエストの例:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. BatchUpdateStandardsControlAssociations を実行します。コントロールを有効にする標準の ARN を指定します。
4. AssociationStatus パラメータを ENABLED と等しい値に設定します。

リクエストの例:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}]
}
```

AWS CLI

特定の標準のコントロールを有効にするには

1. list-security-control-definitions コマンドを実行して標準 ARN を提供すると、特定の標準で利用できるコントロールのリストが表示されます。標準 ARN を取得するには、describe-standards を実行します。このコマンドは、標準固有のコントロール ID ではなく、標準に依存しないセキュリティコントロール ID を返します。

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. list-standards-control-associations コマンドを実行し、特定のコントロール ID を提供すると、各標準のコントロールの現在の有効化ステータスが返されます。

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. batch-update-standards-control-associations コマンドを実行します。コントロールを有効にする標準の ARN を指定します。
4. AssociationStatus パラメータを ENABLED と等しい値に設定します。

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]'
```

特定の標準のコントロールを無効にする

標準のコントロールを無効にすると、Security Hub はそのコントロールの検出結果の生成を停止します。コントロールステータスは、標準のセキュリティスコアの計算には使用されなくなりました。

コントロールを無効にする方法の 1 つは、コントロールが適用されるすべての標準を無効にすることです。標準を無効にすると、その標準に適用されるすべてのコントロールが無効になります (ただし、それらのコントロールは他の標準では有効のままです)。標準の無効化の詳細については、「the section called “標準の有効化および無効化”」を参照してください。

適用される標準を無効化することでコントロールを無効にすると、以下のようになります。

- その標準では、コントロールのセキュリティチェックは実行されなくなります。つまり、コントロールのステータスは標準のセキュリティスコアに影響しません (Security Hub では、他の標準で有効になっているコントロールのセキュリティチェックを引き続き実行します)。
- そのコントロールに対して追加の結果が生成されません。
- 既存の検出結果は 3～5 日後に自動的にアーカイブされます (これはベストエフォートであり保証されないことに注意してください)。
- Security Hub が作成した関連 AWS Config ルールは削除されます。

標準を無効化すると、Security Hub ではどのコントロールが無効にされたかを追跡しません。その後、標準を再度有効化すると、適用されるすべてのコントロールが自動的に有効になります。また、コントロールの無効化は 1 回限りのアクションになります。コントロールを無効にしてから、以前に無効になっていた標準を有効にしたとします。標準にそのコントロールが含まれている場合、コントロールはその標準で有効になります。Security Hub で標準を有効にすると、その標準に適用されるすべてのコントロールが自動的に有効になります。

適用される標準を無効化してコントロールを無効にするのではなく、1 つ以上の特定の標準でコントロールを無効にするだけで済みます。

検出結果のノイズを減らすには、環境に関係のないコントロールを無効にするとよいでしょう。無効にするコントロールに関する推奨事項については、「無効にする可能性のある Security Hub コントロール」を参照してください。

特定の標準でコントロールを無効化するには、次の手順に従います。以下の手順の代わりに、`UpdateStandardsControl` API アクションを使用して特定の標準のコントロールを無効にすることもできます。すべての標準でコントロールを無効にする手順については、「すべての標準におけるコントロールの有効化と無効化」を参照してください。

Security Hub console

特定の標準のコントロールを無効にするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. ナビゲーションペインで、[セキュリティ基準] を選択します。該当する標準の [結果を表示する] を選択します。
3. コントロールを選択します。
4. [コントロールの無効化] を選択します (このオプションは、既に無効になっているコントロールには表示されません)。
5. コントロールを無効にする理由を入力し、[無効化] を選択して確定します。

Security Hub API

特定の標準のコントロールを無効にするには

1. ListSecurityControlDefinitions を実行して標準 ARN を提供すると、特定の標準で利用できるコントロールのリストが表示されます。標準 ARN を取得するには、DescribeStandards を実行します。この API は、標準固有のコントロール ID ではなく、標準に依存しないセキュリティコントロール ID を返します。

   リクエストの例:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. ListStandardsControlAssociations を実行し、特定のコントロール ID を提供すると、各標準のコントロールの現在の有効化ステータスが返されます。

   リクエストの例:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. BatchUpdateStandardsControlAssociations を実行します。コントロールを無効にする標準の ARN を指定します。

4. AssociationStatus パラメータを DISABLED と等しい値に設定します。既に無効化されているコントロールに対してこれらの手順を実行すると、API は HTTP ステータスコード 200 の応答を返します。

   リクエストの例:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED",  "UpdatedReason": "Not applicable to
 environment"}]
}
```

AWS CLI

特定の標準のコントロールを無効にするには

1. list-security-control-definitions コマンドを実行して標準 ARN を提供すると、特定の標準で利用できるコントロールのリストが表示されます。標準 ARN を取得するには、describe-standards を実行します。このコマンドは、標準固有のコントロール ID ではなく、標準に依存しないセキュリティコントロール ID を返します。

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. list-standards-control-associations コマンドを実行し、特定のコントロール ID を提供すると、各標準のコントロールの現在の有効化ステータスが返されます。

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. batch-update-standards-control-associations コマンドを実行します。コントロールを無効にする標準の ARN を指定します。

4. AssociationStatus パラメータを DISABLED と等しい値に設定します。既に有効化されているコントロールに対してこれらの手順を実行すると、コマンドは HTTP ステータスコード 200 の応答を返します。

```
aws securityhub  --region us-east-1 batch-update-standards-control-
associations --standards-control-association-updates '[{"SecurityControlId":
 "CloudTrail.1", "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "AssociationStatus": "DISABLED",
 "UpdatedReason": "Not applicable to environment"}]'
```

Security Hub コントロールのリファレンス

このコントロールリファレンスでは、使用可能な AWS Security Hub コントロールのリストと、各コントロールに関する詳細情報へのリンクを提供します。概要テーブルには、コントロールがコントロール ID のアルファベット順に表示されます。Security Hub でアクティブに使用されているコントロールのみがここに含まれています。廃止されたコントロールはこのリストから除外されます。このテーブルには、各コントロールの以下の情報が表示されます。

- セキュリティコントロール ID – この ID は標準全体に適用され、コントロールが関連付けられている AWS のサービス とリソースを示します。Security Hub コンソールには、アカウントで [統合されたコントロールの検出結果] が有効か無効かに関係なく、セキュリティコントロール ID が表示されます。ただし、Security Hub の検出結果がセキュリティコントロール ID を参照するのは、アカウントで [統合されたコントロールの検出結果] が有効になっている場合のみです。アカウントで [統合されたコントロールの検出結果] が無効になっている場合、一部のコントロール ID はコントロールの検出結果に含まれる標準によって異なります。標準固有のコントロール ID をセキュリティコントロール ID にマッピングする方法については、「統合がコントロール ID とタイトルに与える影響」を参照してください。

  セキュリティコントロールの自動化を設定するときは、タイトルや説明ではなく、コントロール ID に基づいてフィルタリングすることをお勧めします。Security Hub はコントロールのタイトルや説明を更新することがありますが、コントロール ID は変わりません。

  コントロール ID は数字が飛ばされることがあります。これらは将来のコントロール用のプレースホルダーです。
- 適用される標準 — コントロールが適用される標準を示します。コントロールを選択すると、サードパーティのコンプライアンスフレームワークにおける特定の要件が表示されます。
- セキュリティコントロールタイトル — このタイトルはあらゆる標準に適用されます。Security Hub コンソールには、アカウントで [統合されたコントロールの検出結果] が有効か無効かに関係なく、セキュリティコントロールタイトルが表示されます。ただし、Security Hub 検出結果がセ

キュリティコントロールタイトルを参照するのは、アカウントで [統合されたコントロールの検出結果] が有効になっている場合のみです。アカウントで [統合されたコントロールの検出結果] が無効になっている場合、一部のコントロールタイトルはコントロールの検出結果に含まれる標準によって異なります。標準固有のコントロール ID をセキュリティコントロール ID にマッピングする方法については、「統合がコントロール ID とタイトルに与える影響」を参照してください。

- 重要度 — コントロールの重要度は、セキュリティの観点からその重要性を示します。Security Hub がコントロールの重要度を決定する方法の詳細については、「コントロール結果への重要度の割り当て」を参照してください。
- スケジュールタイプ — コントロールがいつ評価されるかを示します。詳細については、「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。
- カスタムパラメータをサポート — コントロールが 1 つ以上のパラメータのカスタム値をサポートしているかどうかを示します。コントロールを選択すると、パラメータの詳細が表示されます。詳細については、「カスタムコントロールパラメータ」を参照してください。

詳細を表示するコントロールを選択します。コントロールはサービス名のアルファベット順にリストされています。

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Account.1	のセキュリティ連絡先情報を提供する必要があります AWS アカウント	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
Account.2	AWS アカウント は AWS Organizations 組織の一部である必要があります	NIST SP 800-53 Rev. 5	HIGH	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ACM.1	インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 はい	変更によるトリガーと定期的なトリガー
ACM.2	ACM が管理する RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります	AWS Foundational Security Best Practices v1.0.0	HIGH	 いいえ	変更によってトリガーされる
ACM.3	ACM 証明書にはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
APIGateway.1	API Gateway REST と WebSocket API 実行のログ記録を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
APIGateway.2	API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
APIGateway.3	API Gateway REST API ステージでは、AWS X-Ray トレースを有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
APIGateway.4	API Gateway は、WAF ウェブ ACL に関連付けられている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
APIGateway.5	API Gateway REST API のキャッシュデータは、保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
APIGateway.8	API Gateway ルートには認証タイプを指定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 はい	定期的
APIGateway.9	API Gateway V2 ステージにアクセスログ記録を設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
AppSync.2	AWS AppSync フィールドレベルのログ記録を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0	中	 はい	変更によってトリガーされる
AppSync.4	AWS AppSync GraphQL APIsにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
AppSync.5	AWS AppSync GraphQL APIs は API キーで認証しないでください	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Athena.2	Athena データカタログにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
Athena.3	Athena ワークグループにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
AutoScaling.1	ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要があります	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
AutoScaling.2	Amazon EC2 Auto Scaling グループは、複数のアベイラビリティーゾーンをカバーする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
AutoScaling.3	Auto Scaling グループの起動設定は、EC2 インスタンスを、インスタンスメタデータサービスバージョン 2 (IMDSv2) を必要とするように設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
Autoscaling.5	Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
AutoScaling.6	Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
AutoScaling.9	EC2 Auto Scaling グループは EC2 起動テンプレートを使用する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
AutoScaling.10	EC2 Auto Scaling グループにタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
Backup.1	AWS Backup 復旧ポイントは保管時に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
バックアップ.2	AWS Backup 復旧ポイントにタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
バックアップ.3	AWS Backup ボールトにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
バックアップ.4	AWS Backup レポートプランにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
バックアップ.5	AWS Backup バックアッププランにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudFormation.2	CloudFormation スタックにはタグを付ける必要があります	AWS リソースタグ付け標準	低	 はい	変更によってトリガーされる
CloudFront.1	CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
CloudFront.3	CloudFront ディストリビューションには転送中の暗号化が必要です	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
CloudFront.4	CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
CloudFront.5	CloudFront ディストリビューションではログ記録が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudFront.6	CloudFront ディストリビューションでは WAF が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
CloudFront.7	CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
CloudFront.8	CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
CloudFront.9	CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
CloudFront.10	CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください。	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudFront.12	CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしないでください	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	HIGH	 いいえ	定期的
CloudFront.13	CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります	AWS Foundational Security Best Practices v1.0.0	中	 いいえ	変更によってトリガーされる
CloudFront.14	CloudFront ディストリビューションにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
CloudTrail.1	CloudTrail 読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン証跡を有効にして設定する必要があります	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0、AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudTrail.2	CloudTrail は保管時の暗号化を有効にする必要があります	CIS AWS Foundations Benchmark v1.2.0、 AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
CloudTrail.3	少なくとも 1 つの CloudTrail 証跡を有効にする必要があります	PCI DSS v3.2.1	HIGH	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudTrail.4	CloudTrail ログファイルの検証を有効にする必要があります	CIS AWS Foundations Benchmark v1.2.0、 AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	低	 いいえ	定期的
CloudTrail.5	CloudTrail 証跡は Amazon CloudWatch Logs と統合する必要があります	CIS AWS Foundations Benchmark v1.2.0、 AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	低	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudTrail.6	CloudTrail ログの保存に使用される S3 バケットがパブリックアクセス可能でないことを確認する	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0	重大	 いいえ	変更によるトリガーと定期的なトリガー
CloudTrail.7	S3 バケットで CloudTrail S3 バケットアクセスのログ記録が有効になっていることを確認する	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0	低	 いいえ	定期的
CloudTrail.9	CloudTrail 証跡にはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
CloudWatch.1	「ルート」ユーザーの使用に対するログメトリックフィルターとアラームが存在する必要があります	CIS AWS Foundations Benchmark v1.2.0、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0	低	 いいえ	定期的
CloudWatch.2	不正な API コールに対するログメトリクスフィルターとアラームが存在することを確認する	CIS AWS Foundations Benchmark v1.2.0	低	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudWatch.3	MFA を使用しないマネジメントコンソールサインインに対してログメトリクスフィルターとアラームが存在することを確認します	CIS AWS Foundations Benchmark v1.2.0	低	 いいえ	定期的
CloudWatch.4	MFA なしの IAM ポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認します。	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0	低	 いいえ	定期的
CloudWatch.5	CloudTrail 設定変更のログメトリクスフィルターとアラームが存在することを確認する	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0	低	 いいえ	定期的
CloudWatch.6	AWS Management Console 認証の失敗に対してログメトリクスフィルターとアラームが存在することを確認する	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0	低	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudWatch.7	カスタマー作成の CMK の無効化またはスケジュールされた削除に対してログメトリクスフィルターとアラームが存在することを確認します	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0	低	 いいえ	定期的
CloudWatch.8	S3 バケットの変更に対してログメトリクスフィルターとアラームが存在することを確認します	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0	低	 いいえ	定期的
CloudWatch.9	AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0	低	 いいえ	定期的
CloudWatch.10	セキュリティグループの変更に対するメトリクスフィルターとアラームが存在することを確認します	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0	低	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudWatch.11	ネットワークアクセスコントロールリスト (NACL) への変更に対するログメトリクスとアラームが存在することを確認します	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0	低	 いいえ	定期的
CloudWatch.12	ネットワークゲートウェイへの変更に対するログメトリクスとアラームが存在することを確認します	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0	低	 いいえ	定期的
CloudWatch.13	ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認します	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0	低	 いいえ	定期的
CloudWatch.14	VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認します	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0	低	 いいえ	定期的
CloudWatch.15	CloudWatch アラームには、指定されたアクションが設定されている必要があります	NIST SP 800-53 Rev. 5	HIGH	 はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudWatch.16	CloudWatch ロググループは、指定された期間保持する必要があります	NIST SP 800-53 Rev. 5	中	 はい	定期的
CloudWatch.17	CloudWatch アラームアクションを有効にする必要があります	NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
CodeArtifact.1	CodeArtifact リポジトリにはタグを付ける必要があります	AWS リソースタグ付け標準	低	 はい	変更によってトリガーされる
CodeBuild.1	CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	 いいえ	変更によってトリガーされる
CodeBuild.2	CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CodeBuild.3	CodeBuild S3 ログは暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
CodeBuild.4	CodeBuild プロジェクト環境にはログ記録設定が必要です	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
Config.1	AWS Config を有効にし、サービスにリンクされたロールをリソース記録に使用する必要があります	CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1	中	 いいえ	定期的
DataFirehose.1	Firehose 配信ストリームは保管時に暗号化する必要があります	AWS Foundational Security Best Practices NIST SP 800-53 Rev. 5	中	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Detective.1	検出動作グラフにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
DMS.1	Database Migration Service のレプリケーションインスタンスは、パブリックではない必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	 いいえ	定期的
DMS.2	DMS 証明書にはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
DMS.3	DMS イベントサブスクリプションにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
DMS.4	DMS レプリケーションインスタンスにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
DMS.5	DMS レプリケーションサブネットグループにタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
DMS.6	DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
DMS.7	ターゲットデータベースの DMS レプリケーションタスクでは、ログ記録が有効になっている必要があります。	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
DMS.8	ソースデータベースの DMS レプリケーションタスクでは、ログ記録が有効になっている必要があります。	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
DMS.9	DMS エンドポイントは SSL を使用する必要があります。	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
DMS.10	Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
DMS.11	MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
DMS.12	Redis の DMS エンドポイントでは TLS が有効になっている必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
DocumentDB.1	Amazon DocumentDB クラスターは、保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	中	 いいえ	変更によってトリガーされる
DocumentDB.2	Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	中	 はい	変更によってトリガーされる
DocumentDB.3	Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	重大	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
DocumentDB.4	Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
DocumentDB.5	Amazon DocumentDB では、削除保護が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
DynamoDB.1	DynamoDB テーブルは、需要に応じて容量をオートスケーリングする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✓ はい	定期的
DynamoDB.2	DynamoDB テーブルでは point-in-time リカバリを有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
DynamoDB.3	DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	✗ いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
DynamoDB 4	DynamoDB テーブルはバックアッププランに含まれている必要があります	NIST SP 800-53 Rev. 5	中	 はい	定期的
DynamoDB 5	DynamoDB テーブルにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
DynamoDB 6	DynamoDB テーブルで、削除保護が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
DynamoDB 7	DynamoDB Accelerator クラスターは転送中に暗号化する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
EC2.1	EBS スナップショットをパブリックに復元可能であってはなりません	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.2	VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにする必要があります	CIS AWS Foundations Benchmark v1.2.0、 AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
EC2.3	アタッチされた EBS ボリュームは、保管時に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
EC2.4	停止した EC2 インスタンスは、指定した期間後に削除する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 はい	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.6	すべての VPC で VPC フローログ記録を有効にする必要があります	CIS AWS Foundations Benchmark v1.2.0、 AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
EC2.7	EBS のデフォルト暗号化を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	中	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.8	EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
EC2.9	EC2 インスタンスは、パブリック IPv4 アドレスを未設定にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
EC2.10	Amazon EC2 サービス用に作成された VPC エンドポイントを使用するように Amazon EC2 を設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
EC2.12	未使用の EC2 EIP を削除する必要があります	PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.13	セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないでください	CIS AWS Foundations Benchmark v1.2.0、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	HIGH	いいえ	変更によってトリガーされる
EC2.14	セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないでください	CIS AWS Foundations Benchmark v1.2.0	HIGH	いいえ	変更によってトリガーされる
EC2.15	EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
EC2.16	未使用のネットワークアクセスコントロールリストを削除する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.17	EC2 インスタンスは複数の ENI を使用しないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
EC2.18	セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可する必要があります。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 はい	変更によってトリガーされる
EC2.19	セキュリティグループは、リスクの高いポートへの無制限アクセスを許可しないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	重大	 いいえ	変更によってトリガーされる
EC2.20	AWS Site-to-Site VPN 接続の両方の VPN トンネルが稼働している必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.21	ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
EC2.22	未使用の EC2 セキュリティグループを削除する必要があります	サービスマネージドスタンダード： AWS Control Tower	中	 いいえ	定期的
EC2.23	EC2 Transit Gateway は VPC アタッチメントリクエストを自動的に受け付けないようにする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
EC2.24	EC2 準仮想化インスタンスタイプは使用しないでください	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.25	EC2 起動テンプレートはパブリック IP をネットワークインターフェイスに割り当ててはなりません	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
EC2.28	EBS ボリュームはバックアッププランに入っている必要があります	NIST SP 800-53 Rev. 5	低	 はい	定期的
EC2.33	EC2 トランジットゲートウェイアタッチメントにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EC2.34	EC2 Transit Gateway ルートテーブルにタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EC2.35	EC2 ネットワークインターフェイスにタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.36	EC2 カスタマーゲートウェイにタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EC2.37	EC2 Elastic IP アドレスにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EC2.38	EC2 インスタンスにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EC2.39	EC2 インターネットゲートウェイにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EC2.40	EC2 NAT ゲートウェイにタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EC2.41	EC2 ネットワーク ACLsタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.42	EC2 ルートテーブルにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EC2.43	EC2 セキュリティグループにタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EC2.44	EC2 サブネットにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EC2.45	EC2 ボリュームにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EC2.46	Amazon VPCsにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EC2.47	Amazon VPC エンドポイントサービスにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.48	Amazon VPC フローログにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EC2.49	Amazon VPC ピアリング接続にはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EC2.50	EC2 VPN ゲートウェイにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EC2.51	EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
EC2.52	EC2 トランジットゲートウェイにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EC2.53	EC2 セキュリティグループは、0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可しないでください	CIS AWS Foundations Benchmark v3.0.0	HIGH	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.54	EC2 セキュリティグループは、::/0 からリモートサーバー管理ポートへの入力を許可しないでください	CIS AWS Foundations Benchmark v3.0.0	HIGH	 いいえ	定期的
ECR.1	ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	定期的
ECR.2	ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
ECR.3	ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ECR.4	ECR パブリックリポジトリにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
ECS.1	Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
ECS.2	Amazon ECS サービスには、パブリック IP アドレスを自動で割り当てないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
ECS.3	ECS タスク定義では、ホストのプロセス名前空間を共有しないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ECS.4	ECS コンテナは、非特権として実行する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
ECS.5	ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
ECS.8	シークレットは、コンテナ環境の変数として渡さないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
ECS.9	ECS タスク定義にはログ設定が必要です。	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ECS.10	ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
ECS.12	ECS クラスターはコンテナインサイトを使用する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
ECS.13	ECS サービスにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
ECS.14	ECS クラスターにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
ECS.15	ECS タスク定義にはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EFS.1	Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
EFS.2	Amazon EFS ボリュームは、バックアッププランに含める必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
EFS.3	EFS アクセスポイントは、ルートディレクトリを適用する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
EFS.4	EFS アクセスポイントは、ユーザー ID を適用する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EFS .5	EFS アクセスポイントにタグを付ける必要があります	AWS リソースタグ付け標準	低	 はい	変更によってトリガーされる
EFS .6	EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません	AWS 基本的なセキュリティのベストプラクティス	中	 いいえ	定期的
EKS.1	EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	HIGH	 いいえ	定期的
EKS.2	EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
EKS.3	EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EKS.6	EKS クラスターにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EKS.7	EKS ID プロバイダー設定にはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EKS.8	EKS クラスターでは、監査ログ記録が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
ElastiCache.1	ElastiCache Redis クラスターでは自動バックアップが有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	HIGH	 はい	定期的
ElastiCache.2	ElastiCache for Redis キャッシュクラスターでは、マイナーバージョンの自動アップグレードを有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	HIGH	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ElastiCache.3	ElastiCache レプリケーショングループで自動フェイルオーバーが有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
ElastiCache.4	ElastiCache レプリケーショングループで encryption-at-rest が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
ElastiCache.5	ElastiCache レプリケーショングループで encryption-in-transit が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
ElastiCache.6	ElastiCache 以前の Redis バージョンのレプリケーショングループでは、Redis AUTH が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
ElastiCache.7	ElastiCache クラスターはデフォルトのサブネットグループを使用しないでください	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	HIGH	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ElasticBeanstalk.1	Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
ElasticBeanstalk.2	Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 はい	変更によってトリガーされる
ElasticBeanstalk.3	Elastic Beanstalk は口グを にストリーミングする必要があります CloudWatch	AWS Foundational Security Best Practices v1.0.0	HIGH	 はい	変更によってトリガーされる
ELB.1	Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	中	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ELB.2	SSL/HTTPS リスナーを使用する Classic Load Balancer は、AWS Certificate Manager によって提供される証明書を使用する必要があります。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
ELB.3	Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
ELB.4	Application Load Balancer は、http ヘッダーを削除するように設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
ELB.5	アプリケーションおよび Classic Load Balancer のログ記録を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ELB.6	Application、Gateway、Network Load Balancer では、削除保護を有効にする必要があります	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
ELB.7	Classic Load Balancer は、Connection Draining を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
ELB.8	SSL リスナーを使用する Classic Load Balancer は、強力な設定を持つ事前定義されたセキュリティポリシーを使用する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
ELB.9	Classic Load Balancer では、クロスゾーンロードバランシングが有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ELB.10	Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 はい	変更によってトリガーされる
ELB.12	Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
ELB.13	Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 はい	変更によってトリガーされる
ELB.14	Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ELB.16	Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります	NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
EMR.1	Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	定期的
EMR.2	Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	重大	 いいえ	定期的
ES.1	Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	中	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ES.2	Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	 いいえ	定期的
ES.3	Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
ES.4	Logs への Elasticsearch CloudWatch ドメインエラーのログ記録を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
ES.5	Elasticsearch ドメインで監査ログ記録が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ES.6	Elasticsearch ドメインには少なくとも 3 つのデータノードが必要です	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
ES.7	Elasticsearch ドメインは、少なくとも 3 つの専用マスターノードを設定する必要があります。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
ES.8	Elasticsearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
ES.9	Elasticsearch ドメインにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EventBridge.2	EventBridge イベントバスにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
EventBridge.3	EventBridge カスタムイベントバスには、リソースベースのポリシーがアタッチされている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
EventBridge.4	EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります	NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
FSx.1	FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
FSx.2	FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Glue.1	AWS Glue ジョブにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
GlobalAccelerator.1	Global Accelerator アクセラレーターにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
GuardDuty.1	GuardDuty を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	HIGH	 いいえ	定期的
GuardDuty.2	GuardDuty フィルターにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
GuardDuty.3	GuardDuty IPSetsにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
GuardDuty.4	GuardDuty ディテクターにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.1	IAM ポリシーでは、完全な「*」管理権限を許可してはなりません	CIS AWS Foundations Benchmark v1.2.0、 AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
IAM.2	IAM ユーザーには IAM ポリシーをアタッチしてはなりません	CIS AWS Foundations Benchmark v1.2.0、 AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.3	IAM ユーザーのアクセスキーは 90 日以内ごとに更新する必要があります	CIS AWS Foundations Benchmark v1.2.0、 AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
IAM.4	IAM ルートユーザーのアクセスキーが存在してはいけません	CIS AWS Foundations Benchmark v1.2.0、 AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	重大	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.5	MFA は、コンソールパスワードを持つすべての IAM ユーザーに対して有効にする必要があります	CIS AWS Foundations Benchmark v1.2.0、 AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
IAM.6	ルートユーザーに対してハードウェア MFA を有効にする必要があります	CIS AWS Foundations Benchmark v1.2.0、 AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	重大	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.7	IAM ユーザーのパスワードポリシーには強力な設定が必要です	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 はい	定期的
IAM.8	未使用の IAM ユーザー認証情報は削除する必要があります	CIS AWS Foundations Benchmark v1.2.0、 AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
IAM.9	ルートユーザーに対して MFA を有効にする必要があります	CIS AWS Foundations Benchmark v1.2.0、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	重大	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.10	IAM ユーザーのパスワードポリシーには強力な設定が必要です	PCI DSS v3.2.1	中	 いいえ	定期的
IAM.11	IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認する	CIS AWS Foundations Benchmark v1.2.0	中	 いいえ	定期的
IAM.12	IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認する	CIS AWS Foundations Benchmark v1.2.0	中	 いいえ	定期的
IAM.13	IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認する	CIS AWS Foundations Benchmark v1.2.0	中	 いいえ	定期的
IAM.14	IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認する	CIS AWS Foundations Benchmark v1.2.0	中	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.15	IAM パスワードポリシーにおいて、14 文字以上のパスワードが要求されるようにする	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0	中	 いいえ	定期的
IAM.16	IAM パスワードポリシーはパスワードの再使用を禁止しています	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0	低	 いいえ	定期的
IAM.17	IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認する	CIS AWS Foundations Benchmark v1.2.0	低	 いいえ	定期的
IAM.18	でインシデントを管理するためのサポートロールが作成されていることを確認します。 AWS Support	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0	低	 いいえ	定期的
IAM.19	すべての IAM ユーザーに対して MFA を有効にする必要があります	PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	中	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.21	作成する IAM カスタマー管理ポリシーにはサービスのワイルドカードアクションを許可しないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
IAM.22	45 日間未使用の IAM ユーザー認証情報は削除する必要があります	CIS AWS Foundations Benchmark v1.4.0	中	 いいえ	定期的
IAM.23	IAM Access Analyzer アナライザーにはタグを付ける必要があります	AWS リソースタグ付け標準	低	 はい	変更によってトリガーされる
IAM.24	IAM ロールにはタグを付ける必要があります	AWS リソースタグ付け標準	低	 はい	変更によってトリガーされる
IAM.25	IAM ユーザーはタグ付けする必要があります	AWS リソースタグ付け標準	低	 はい	変更によってトリガーされる
IAM.26	IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります	CIS AWS Foundations Benchmark v3.0.0	中	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.27	IAM ID には AWSCloudShellFullAccess ポリシーをアタッチしないでください	CIS AWS Foundations Benchmark v3.0.0	中	 いいえ	変更によってトリガーされる
IAM.28	IAM Access Analyzer の外部アクセスアナライザーを有効にする必要があります	CIS AWS Foundations Benchmark v3.0.0	HIGH	 いいえ	定期的
IoT.1	AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
IoT.2	AWS IoT Core 緩和アクションにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
IoT.3	AWS IoT Core ディメンションにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
IoT.4	AWS IoT Core オーソライザーにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IoT.5	AWS IoT Core ロールエイリアスにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
IoT.6	AWS IoT Core ポリシーにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
Kinesis.1	Kinesis Streams は、保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
Kinesis.2	Kinesis ストリームにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
KMS.1	IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
KMS.2	IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用ないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
KMS.3	AWS KMS keys 意図せずに削除しないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	重大	 いいえ	変更によってトリガーされる
KMS.4	AWS KMS key ローテーションを有効にする必要があります	CIS AWS Foundations Benchmark v1.2.0、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	中	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Lambda.1	Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	 いいえ	変更によってトリガーされる
Lambda.2	Lambda 関数はサポートされているランタイムを使用する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
Lambda.3	Lambda 関数は VPC 内に存在する必要があります	PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
Lambda.5	VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Lambda.6	Lambda 関数にはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
Macie.1	Amazon Macie を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
Macie.2	Macie 自動機密データ検出を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	HIGH	 いいえ	定期的
MSK.1	MSK クラスターはブローカーノード間の転送時に暗号化される必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
MSK.2	MSK クラスターでは、拡張モニタリングを設定する必要があります	NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
MQ.2	ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
MQ.3	Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
MQ.4	Amazon MQ ブローカーにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
MQ.5	ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります	NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	低	 いいえ	変更によってトリガーされる
MQ.6	RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。	NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	低	 いいえ	変更によってトリガーされる
Neptune.1	Neptune DB クラスターは、保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Neptune.2	Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	中	 いいえ	変更によってトリガーされる
Neptune.3	Neptune DB クラスタースナップショットはパブリックにしないでください	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	重大	 いいえ	変更によってトリガーされる
Neptune.4	Neptune DB クラスターでは、削除保護が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	低	 いいえ	変更によってトリガーされる
Neptune.5	Neptune DB クラスターでは、自動バックアップが有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	中	 はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Neptune.6	Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	中	 いいえ	変更によってトリガーされる
Neptune.7	Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	中	 いいえ	変更によってトリガーされる
Neptune.8	Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	低	 いいえ	変更によってトリガーされる
Neptune.9	Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります	NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
NetworkFirewall.1	Network Firewall ファイアウォールを複数のアベイラビリティーゾーンにデプロイする必要があります	NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
NetworkFirewall.2	Network Firewall ログ記録を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
NetworkFirewall.3	Network Firewall ポリシーには、1 つ以上のルールグループが関連付けられている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
NetworkFirewall.4	Network Firewall ポリシーのデフォルトのステートレスアクションは、完全なパケットに対してドロップまたは転送される必要があります。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
NetworkFirewall.5	Network Firewall ポリシーのデフォルトのステートレスアクションは、断片化されたパケットに対してドロップまたは転送される必要があります。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
NetworkFirewall.6	ステートレスネットワークファイアウォールのルールグループを空にしないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
NetworkFirewall.7	Network Firewall ファイアウォールにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
NetworkFirewall.8	Network Firewall ファイアウォールポリシーにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
NetworkFirewall.9	Network Firewall は削除保護を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Opensearch.1	OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
Opensearch.2	OpenSearch ドメインはパブリックアクセス可能であってはなりません	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	 いいえ	変更によってトリガーされる
Opensearch.3	OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Opensearch.4	OpenSearch CloudWatch ログへのドメインエラーのログ記録を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
Opensearch.5	OpenSearch ドメインでは監査ログ記録が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
Opensearch.6	OpenSearch ドメインには少なくとも 3 つのデータノードが必要です	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
Opensearch.7	OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Opensearch.8	OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
Opensearch.9	OpenSearch ドメインにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
Opensearch.10	OpenSearch ドメインには最新のソフトウェア更新がインストールされている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
Opensearch.11	OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です	NIST SP 800-53 Rev. 5	中	 いいえ	定期的
PCA.1	AWS Private CA ルート認証機関を無効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	低	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.1	RDS スナップショットはプライベートである必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	 いいえ	変更によってトリガーされる
RDS.2	RDS DB インスタンスは、 PubliclyAccessible 設定によって決定されるパブリックアクセスを禁止する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	 いいえ	変更によってトリガーされる
RDS.3	RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.4	RDS クラスタースナップショットとデータベーススナップショットは保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
RDS.5	RDS DB インスタンスは、複数のアベイラビリティーゾーンで設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
RDS.6	RDS DB インスタンスの拡張モニタリングを設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	 はい	変更によってトリガーされる
RDS.7	RDS クラスターでは、削除保護が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.8	RDS DB インスタンスで、削除保護が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
RDS.9	RDS DB インスタンスはログを CloudWatch Logs に発行する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
RDS.10	IAM 認証は RDS インスタンス用に設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
RDS.11	Amazon RDS インスタンスでは、自動バックアップが有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.12	IAM 認証は RDS クラスター用に設定する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
RDS.13	RDS 自動マイナーバージョンアップグレードを有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
RDS.14	Amazon Aurora クラスターはバックトラッキングを有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 はい	変更によってトリガーされる
RDS.15	RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
RDS.16	タグをスナップショットにコピーするように RDS DB クラスターを設定する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.17	RDS DB インスタンスは、タグをスナップショットにコピーするように設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
RDS.18	RDS インスタンスは VPC 内にデプロイする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
RDS.19	重大なクラスターイベントについて、既存の RDS イベント通知サブスクリプションを設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
RDS.20	重大なデータベースインスタンスイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.21	重大なデータベースパラメータグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
RDS.22	重大なデータベースセキュリティグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
RDS.23	RDS インスタンスはデータベースエンジンのデフォルトポートを使用しないようにする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
RDS.24	RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.25	RDS データベースインスタンスはカスタム管理者ユーザー名を使用する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
RDS.26	RDS DB インスタンスはバックアッププランで保護する必要があります	NIST SP 800-53 Rev. 5	中	 はい	定期的
RDS.27	RDS DB クラスターは保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード： AWS Control Tower	中	 いいえ	変更によってトリガーされる
RDS.28	RDS DB クラスターにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
RDS.29	RDS DB クラスタースナップショットにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.30	RDS DB インスタンスにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
RDS.31	RDS DB セキュリティグループにタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
RDS.32	RDS DB スナップショットにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
RDS.33	RDS DB サブネットグループにタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
RDS.34	Aurora MySQL DB クラスターは監査ログを CloudWatch ログに発行する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
RDS.35	RDS DB クラスターではマイナーバージョンの自動アップグレードを有効にしておく必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Redshift.1	Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	 いいえ	変更によってトリガーされる
Redshift.2	Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
Redshift.3	Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 はい	変更によってトリガーされる
Redshift.4	Amazon Redshift クラスターでは、監査ログ記録が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Redshift.6	Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
Redshift.7	Redshift クラスターは拡張 VPC ルーティングを使用する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
Redshift.8	Amazon Redshift クラスターでデフォルトの管理者ユーザー名を使用しないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
Redshift.9	Redshift クラスターでは、デフォルトのデータベース名を使用しないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Redshift.10	Redshift クラスターは保存時に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
Redshift.11	Redshift クラスターにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
Redshift.12	Redshift イベントサブスクリプション通知にはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
Redshift.13	Redshift クラスタースナップショットにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
Redshift.14	Redshift クラスターサブネットグループにタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Redshift.15	Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります	AWS 基本的なセキュリティのベストプラクティス	HIGH	 いいえ	定期的
Route53.1	Route 53 ヘルスチェックにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
Route53.2	Route 53 のパブリックホストゾーンは DNS クエリを ログに記録する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
S3.1	S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	中	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
S3.2	S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	 いいえ	変更によるトリガーと定期的なトリガー
S3.3	S3 汎用バケットはパブリック書き込みアクセスをブロックする必要があります	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	 いいえ	変更によるトリガーと定期的なトリガー
S3.5	S3 汎用バケットでは、SSL の使用をリクエストする必要があります	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
S3.6	S3 汎用バケットポリシーでは、他の へのアクセスを制限する必要があります AWS アカウント	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
S3.7	S3 汎用バケットはクロスリージョンレプリケーションを使用する必要があります	PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
S3.8	S3 汎用バケットはパブリックアクセスをブロックする必要があります	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
S3.9	S3 汎用バケットでは、サーバーアクセスのログ記録を有効にする必要があります	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
S3.10	バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です	NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
S3.11	S3 汎用バケットでは、イベント通知を有効にする必要があります	NIST SP 800-53 Rev. 5	中	 はい	変更によってトリガーされる
S3.12	ACLs は、S3 汎用バケットへのユーザーアクセスを管理するために使用しないでください	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
S3.13	S3 汎用バケットにはライフサイクル設定が必要です	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	 はい	変更によってトリガーされる
S3.14	S3 汎用バケットではバージョニングを有効にする必要があります	NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
S3.15	S3 汎用バケットでは、オブジェクトロックを有効にする必要があります	NIST SP 800-53 Rev. 5	中	 はい	変更によってトリガーされる
S3.17	S3 汎用バケットは、保管時に で暗号化する必要があります AWS KMS keys	サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
S3.19	S3 アクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	重大	 いいえ	変更によってトリガーされる
S3.20	S3 汎用バケットでは MFA 削除が有効になっている必要があります	CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
S3.22	S3 汎用バケットはオブジェクトレベルの書き込みイベントをログに記録する必要があります	CIS AWS Foundations Benchmark v3.0.0	中	 いいえ	定期的
S3.23	S3 汎用バケットは、オブジェクトレベルの読み取りイベントをログに記録する必要があります	CIS AWS Foundations Benchmark v3.0.0	中	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
SageMaker.1	Amazon SageMaker Notebook インスタンスは、インターネットに直接アクセスできません	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	HIGH	 いいえ	定期的
SageMaker.2	SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
SageMaker.3	ユーザーは SageMaker ノートブックインスタンスへのルートアクセスを禁止されます	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる
SageMaker.4	SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	 いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
SecretsManager.1	Secrets Manager のシークレットは、自動ローテーションを有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 はい	変更によってトリガーされる
SecretsManager.2	自動ローテーションを設定した Secrets Manager のシークレットは正常にローテーションする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
SecretsManager.3	未使用の Secrets Manager のシークレットを削除します	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 はい	定期的
SecretsManager.4	Secrets Manager のシークレットは、指定された日数以内にローテーションする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 はい	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
SecretsManager.5	Secrets Manager のシークレットにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
ServiceCatalog.1	Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	HIGH	 いいえ	定期的
SES.1	SES 連絡先リストにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
SES.2	SES 設定セットにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
SNS.1	SNS トピックは、保管時に を使用して暗号化する必要があります AWS KMS	NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
SNS.3	SNS トピックにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
SQS.1	Amazon SQS キューは保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
SQS.2	SQS キューにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
SSM.1	EC2 インスタンスはによって管理する必要があります AWS Systems Manager	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
SSM.2	Systems Manager によって管理される EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	HIGH	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
SSM.3	Systems Manager によって管理される EC2 インスタンスの関連付けコンプライアンスステータスは、COMPLIANT である必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	低	 いいえ	変更によってトリガーされる
SSM.4	SSM ドキュメントはパブリックにしないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	重大	 いいえ	定期的
StepFunctions.1	Step Functions ステートマシンでは、ログ記録がオンになっている必要があります	AWS 基本的なセキュリティのベストプラクティス	中	 はい	変更によってトリガーされる
StepFunctions.2	Step Functions アクティビティにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる
Transfer.1	Transfer Family ワークフローにはタグを付ける必要があります	AWS リソースタグ付け標準	低	あり	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Transfer.2	Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
WAF.1	AWS WAF Classic グローバルウェブ ACL ログ記録を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	定期的
WAF.2	AWS WAF Classic リージョンルールには少なくとも 1 つの条件が必要です	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
WAF.3	AWS WAF Classic リージョンルールグループには、少なくとも 1 つのルールが必要です	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
WAF.4	AWS WAF Classic リージョンウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
WAF.6	AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
WAF.7	AWS WAF Classic グローバルルールグループには、少なくとも 1 つのルールが必要です	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
WAF.8	AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
WAF.10	AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる
WAF.11	AWS WAF ウェブ ACL ログ記録を有効にする必要があります	NIST SP 800-53 Rev. 5	低	 いいえ	定期的
WAF.12	AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	 いいえ	変更によってトリガーされる

トピック

- AWS アカウント コントロール
- AWS Certificate Manager コントロール
- Amazon API Gateway コントロール
- AWS AppSync コントロール
- Amazon Athena コントロール
- AWS Backup コントロール
- AWS CloudFormation コントロール
- Amazon CloudFront コントロール
- AWS CloudTrail コントロール
- Amazon CloudWatch コントロール

- AWS CodeArtifact コントロール
- AWS CodeBuild コントロール
- AWS Config コントロール
- Amazon Data Firehose コントロール
- Amazon Detective コントロール
- AWS Database Migration Service コントロール
- Amazon DocumentDB コントロール
- Amazon DynamoDB コントロール
- Amazon Elastic Container Registry のコントロール
- Amazon ECS コントロール
- Amazon Elastic Compute Cloud コントロール
- Amazon EC2 Auto Scaling コントロール
- Amazon EC2 Systems Manager コントロール
- Amazon Elastic File System のコントロール
- Amazon Elastic Kubernetes Service コントロール
- Amazon ElastiCache コントロール
- AWS Elastic Beanstalk コントロール
- Elastic Load Balancing のコントロール
- Amazon EMR コントロール
- Elasticsearch コントロール
- Amazon EventBridge コントロール
- Amazon FSx コントロール
- AWS Global Accelerator コントロール
- AWS Glue コントロール
- Amazon GuardDuty コントロール
- AWS Identity and Access Management コントロール
- AWS IoT コントロール
- Amazon Kinesis のコントロール
- AWS Key Management Service コントロール
- AWS Lambda コントロール

- Amazon Macie コントロール
- Amazon MSK コントロール
- Amazon MQ コントロール
- Amazon Neptune コントロール
- AWS Network Firewall コントロール
- Amazon OpenSearch Service コントロール
- AWS Private Certificate Authority コントロール
- Amazon Relational Database Service コントロール
- Amazon Redshift のコントロール
- Amazon Route 53 のコントロール
- Amazon Simple Storage Service コントロール
- Amazon SageMaker コントロール
- AWS Secrets Manager コントロール
- AWS Service Catalog コントロール
- Amazon Simple Email Service コントロール
- Amazon Simple Notification Service コントロール
- Amazon Simple Queue Service コントロール
- AWS Step Functions コントロール
- AWS Transfer Family コントロール
- AWS WAF コントロール

AWS アカウント コントロール

これらのコントロールは に関連しています AWS アカウント。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Account.1] のセキュリティ連絡先情報を に提供する必要があります AWS アカウント

関連する要件: NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 識別 > リソース設定

重要度: 中

リソースタイプ: `AWS::::Account`

AWS Config ルール: `security-account-information-provided`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Amazon Web Services (AWS) アカウントにセキュリティの連絡先情報があるかどうかを確認します。アカウントにセキュリティの連絡先情報が提供されていない場合、コントロールは失敗します。

代替のセキュリティ連絡先では AWS 、利用できなくなった場合に、アカウントに関する問題について別のユーザーに連絡することができます。通知は AWS Support、 または他の AWS のサービスチームから、 AWS アカウント の使用に関連するセキュリティ関連のトピックについて行うことができます。

修正

代替連絡先をセキュリティ連絡先として に追加するには AWS アカウント、「請求情報とコスト管理ユーザーガイド」の「代替連絡先の追加、変更、または削除」を参照してください。 AWS

[Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります

カテゴリ: 保護 > セキュアなアクセス管理 > アクセスコントロール

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

重要度: 高

リソースタイプ: `AWS::::Account`

AWS Config ルール: `account-part-of-organizations`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロール AWS アカウント は、 が を通じて管理される組織の一部であるかどうかをチェックします AWS Organizations。アカウントが組織の一部ではない場合、コントロールは失敗します。

Organizations は、 でワークロードをスケーリングする際に、環境を一元管理するのに役立ちます AWS。特定のセキュリティ要件があるワークロードの分離や、HIPAA または PCI といったフレーム

ワークへの準拠のため、 AWS アカウント を複数使用できます。組織を作成することで、複数のアカウントを 1 つのユニットとして管理し AWS のサービス、、リソース、リージョンへのアクセスを一元管理できます。

修正

新しい組織を作成して自動的に追加 AWS アカウント するには、「 AWS Organizations ユーザーガイド」の「組織の作成」を参照してください。既存の組織にアカウントを追加するには、「 ユーザーガイド」の「組織 AWS アカウント への の招待」を参照してください。 AWS Organizations

AWS Certificate Manager コントロール

これらのコントロールは ACM リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります

関連する要件: NIST.800-53.r5 SC-28(3)、NIST.800-53.r5 SC-7(16)

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::ACM::Certificate`

AWS Config ルール : `acm-certificate-expiration-check`

スケジュールタイプ： 変更がトリガーされ、定期的に行われる

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`daysToExpiration`	ACM 証明書を更新する必要がある日数	整数	`14 ~ 365`	`30`

このコントロールは、 AWS Certificate Manager (ACM) 証明書が指定された期間内に更新されているかどうかをチェックします。インポートした証明書と ACM によって提供された証明書の両方をチェックします。指定された期間内に証明書が更新されない場合、コントロールは失敗します。更新期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 30 日を使用します。

ACM は DNS 検証を使用する証明書を自動的に更新できます。E メール検証を使用する証明書の場合、ドメイン検証 E メールに応答する必要があります。ACM は、ユーザーがインポートした証明書を自動的に更新しません。インポートした証明書を手動で更新する必要があります。

修正

ACM は、Amazon 発行の SSL/TLS 証明書のマネージド更新が可能です。つまり、ACM は証明書を自動的に更新するか (DNS 検証を使用している場合)、有効期限が近づくと E メール通知を送信します。これらのサービスは、パブリック ACM 証明書とプライベート ACM 証明書の両方に対して提供されます。

E メールで検証されたドメイン

証明書の有効期限まで 45 日間の時点で、ACM はドメイン所有者にドメイン名ごとに E メールを送信します。ドメインを検証して更新を完了するには、E メール通知に応答する必要があります。

詳細については、「AWS Certificate Manager ユーザーガイド」の「E メールで検証されたドメインの更新」を参照してください。

DNS によって検証されたドメイン

ACM は DNS 検証を使用する証明書を自動的に更新します。有効期限の 60 日前に、ACM は証明書が更新できることを確認します。

ドメイン名を検証できない場合、ACM は手動検証が必要である旨の通知を送信します。これらの通知は、有効期限の 45 日、30 日、7 日、1 日前に送信されます。

詳細については、「AWS Certificate Manager ユーザーガイド」の「DNS によって検証されたドメインの更新」を参照してください。

[ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります

カテゴリ: 識別 > インベントリ > インベントリサービス

重要度: 高

リソースタイプ: `AWS::ACM::Certificate`

AWS Config ルール : `acm-certificate-rsa-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 によって管理される RSA 証明書が、少なくとも 2,048 ビットのキー長 AWS Certificate Manager を使用しているかどうかをチェックします。キーの長さが 2,048 ビットより小さい場合、コントロールは失敗します。

暗号化の強度はキーサイズと直接相関します。コンピューティング能力が低下し、サーバーがより高度になるため、 AWS リソースを保護するために 2,048 ビット以上のキー長をお勧めします。

修正

ACM が発行する RSA 証明書における最小のキーの長さは、既に 2,048 ビットです。ACM で新しい RSA 証明書を発行する手順については、「AWS Certificate Manager ユーザーガイド」の「証明書の発行と管理」を参照してください。

ACM では短いキーの長さで証明書をインポートできますが、この制御を行うには少なくとも 2,048 ビットのキーを使用する必要があります。証明書をインポートした後で、キーの長さを変更することはできません。代わりに、キーの長さが 2,048 ビット未満の証明書を削除する必要があります。ACM への証明書のインポートに関する詳細については、「AWS Certificate Manager ユーザーガイド」の「証明書をインポートするための前提条件」を参照してください。

[ACM.3] ACM 証明書にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::ACM::Certificate`

AWS Config ルール: `tagged-acm-certificate` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、 AWS Certificate Manager (ACM) 証明書にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。証明書にタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、証明書にキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

ACM 証明書にタグを追加するには、「 AWS Certificate Manager ユーザーガイド」の AWS Certificate Manager 「証明書のタグ付け」を参照してください。

Amazon API Gateway コントロール

これらのコントロールは API Gateway リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[APIGateway.1] API Gateway REST と WebSocket API 実行の口グ記録を有効にする必要があります

関連する要件: NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > 口グ記録

重要度: 中

リソースタイプ: `AWS::ApiGateway::Stage`、`AWS::ApiGatewayV2::Stage`

AWS Config ルール : `api-gw-execution-logging-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`loggingLevel`	ログ記録レベル	列挙型	`ERROR`, `INFO`	`No default value`

このコントロールは、Amazon API Gateway REST または WebSocket API のすべてのステージで口グ記録が有効になっているかどうかをチェックします。API のすべてのステージ

で、`loggingLevel` が `ERROR` でも `INFO` でもない場合、コントロールは失敗します。特定のログタイプを有効にする必要があることを示すカスタムパラメータ値を指定しない限り、ログ記録レベルが `ERROR` または `INFO` であれば、Security Hub は成功の検出結果を生成します。

API Gateway REST または WebSocket API ステージでは、関連するログを有効にする必要があります。API Gateway REST および WebSocket API 実行ログは、API Gateway REST および API WebSocket ステージに対して行われたリクエストの詳細なレコードを提供します。ステージには、API 統合バックエンドレスポンス、Lambda オーソライザーレスポンス、統合 AWS エンドポイント`requestId`の が含まれます。

修正

REST および WebSocket API オペレーションのログ記録を有効にするには、 CloudWatch 「API Gateway デベロッパーガイド」の「API Gateway コンソールを使用した API ログ記録の設定」を参照してください。

[APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります

関連する要件: NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::ApiGateway::Stage`

AWS Config ルール : `api-gw-ssl-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon API Gateway REST API ステージに SSL 証明書が設定されているかどうかをチェックします。バックエンドシステムは、これらの証明書を使用して、API Gateway からの受信リクエストであることを認証します。

API Gateway からのリクエストをバックエンドシステムが認証できるようにするには、API Gateway REST API ステージを SSL 証明書を設定する必要があります。

修正

API Gateway REST API SSL 証明書を生成し設定する方法の詳細については、「API Gateway 開発者ガイド」の「バックエンド認証用 SSL 証明書の生成と設定」を参照してください。

[APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります

関連する要件: NIST.800-53.r5 CA-7

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::ApiGateway::Stage`

AWS Config ルール : `api-gw-xray-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon API Gateway REST API ステージで AWS X-Ray アクティブトレースが有効になっているかどうかをチェックします。

X-Ray アクティブトレースを使用すると、基盤となるインフラストラクチャのパフォーマンスの変化に対してより迅速に対応できます。パフォーマンスの変化により、API が利用できなくなる可能性があります。X-Ray アクティブトレースは、API Gateway REST API オペレーションと接続サービスを介して流れるユーザーリクエストのリアルタイムメトリクスを提供します。

修正

API Gateway REST API オペレーションの X-Ray アクティブトレースを有効にする方法の詳細については、[AWS X-Ray 開発者ガイド]の[AWS X-Rayの Amazon API Gateway アクティブトレースサポート]を参照してください。

[APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります

関連する要件: NIST.800-53.r5 AC-4(21)

カテゴリ: 保護 > 保護サービス

重要度: 中

リソースタイプ: `AWS::ApiGateway::Stage`

AWS Config ルール : `api-gw-associated-with-waf`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、API Gateway ステージが AWS WAF ウェブアクセスコントロールリスト (ACL) を使用しているかどうかをチェックします。 AWS WAF ウェブ ACL が REST API Gateway ステージにアタッチされていない場合、このコントロールは失敗します。

AWS WAF は、ウェブアプリケーションと APIsから保護するのに役立つウェブアプリケーションファイアウォールです。これにより、ユーザーが定義するカスタマイズ可能なウェブセキュリティルールと条件に基づいて、ウェブリクエストを許可、ブロック、またはカウントする一連のルールである ACL を設定することができます。API Gateway ステージが AWS WAF ウェブ ACL に関連付けられていることを確認し、悪意のある攻撃から保護します。

修正

API Gateway コンソールを使用して AWS WAF リージョンウェブ ACL を既存の API Gateway API ステージに関連付ける方法については、「API Gateway デベロッパーガイド」のAPIs 「 AWS WAF を使用して API を保護する」を参照してください。

[APIGateway.5] API Gateway REST API のキャッシュデータは、保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ: `AWS::ApiGateway::Stage`

AWS Config ルール: `api-gw-cache-encrypted` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、キャッシュが有効になっている API Gateway REST API ステージ内のすべてのメソッドが暗号化されているかどうかをチェックします。API Gateway REST API ステージ内のメソッドのキャッシュ機能が設定されており、そのキャッシュが暗号化されていない場合、コントロールは失敗します。Security Hub は、特定のメソッドのキャッシュが有効になっている場合にのみ、そのメソッドの暗号化を評価します。

保管中のデータを暗号化すると、ディスクに保存されているデータが、 に対して認証されていないユーザーによってアクセスされるリスクが軽減されます AWS。これにより、権限のないユーザーによるデータへのアクセスを制限するために、別の一連のアクセスコントロールが追加されます。例えば、データを読み取る前にデータを復号化するには、API の許可が必要です。

API Gateway REST API キャッシュは、セキュリティを強化するために、保管中に暗号化する必要があります。

修正

ステージの API キャッシュを設定するには、「API Gateway デベロッパーガイド」の「Amazon API Gateway のキャッシュを有効にする」を参照してください。[キャッシュ設定] で、[キャッシュデータを暗号化する] を選択します。

[APIGateway.8] API Gateway ルートには認証タイプを指定する必要があります

関連する要件: NIST.800-53.r5 AC-3、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::ApiGatewayV2::Route`

AWS Config ルール: `api-gwv2-authorization-type-configured`

スケジュールタイプ: 定期的

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`authorizationType`	API ルートの認証タイプ	列挙型	`AWS_IAM`, `CUSTOM`, `JWT`	デフォルト値なし

このコントロールは、Amazon API Gateway ルートに認証タイプが設定されているかどうかを確認します。API Gateway ルートで認証タイプが指定されていない場合、コントロールは失敗します。`authorizationType` パラメータで指定された認証タイプをルートが使用する場合にのみコントロールを成功させたい場合は、必要に応じてカスタムパラメータ値を指定できます。

API Gateway は API へのアクセスを制御し管理する複数のメカニズムをサポートしています。認証タイプを指定することで、API へのアクセスを許可されたユーザーまたはプロセスのみに制限できます。

修正

HTTP API の認証タイプを設定するには、「API Gateway デベロッパーガイド」の「API Gateway での HTTP API へのアクセスの制御と管理」を参照してください。 WebSocket APIs WebSocket 「API Gateway デベロッパーガイド」の「API Gateway での API へのアクセスの制御と管理」を参照してください。

[APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります

関連する要件: NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::ApiGatewayV2::Stage`

AWS Config ルール: `api-gwv2-access-logs-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon API Gateway V2 ステージのアクセスログが設定されているかどうかをチェックします。アクセスログ設定が定義されていない場合、このコントロールは失敗します。

API Gateway アクセスログは、誰が API にアクセスしたかや、発信者が API にアクセスした方法に関する詳細情報を提供します。これらのログは、セキュリティ監査やアクセス監査、証拠調査などのアプリケーションに役立ちます。トラフィックパターンの分析や問題のトラブルシューティングを行うには、これらのアクセスログを有効にします。

その他のベストプラクティスについては、「API Gateway デベロッパーガイド」の「REST API のモニタリング」を参照してください。

修正

アクセスログを設定するには、CloudWatch 「API Gateway デベロッパーガイド」の「API Gateway コンソールを使用した API ログの設定」を参照してください。

AWS AppSync コントロール

これらのコントロールは AWS AppSync リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔AppSync.2] フィールドレベルのログ記録を有効にする AWS AppSync 必要があります

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::AppSync::GraphQLApi`

AWS Config ルール : `appsync-logging-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値	
`fieldLoggingLevel`	フィールドのログ記録レベル	列挙型	`ERROR`, `ALL`	`No default value`	

このコントロールは、 AWS AppSync API でフィールドレベルのログ記録が有効になっているかどうかをチェックします。フィールドリゾルバーのログレベルが [なし] に設定されている場合、コント

ロールは失敗します。特定のログタイプを有効にする必要があることを示すカスタムパラメータ値を指定しない限り、フィールドリゾルバーのログレベルが ERROR または ALL であれば、Security Hub は成功の検出結果を生成します。

ログおよびメトリクスを使用して、GraphQL クエリを特定、トラブルシューティング、最適化できます。 AWS AppSync GraphQL のログ記録を有効にすると、API リクエストとレスポンスに関する詳細情報を取得し、問題を特定して対応し、規制要件に準拠できます。

修正

のログ記録を有効にするには AWS AppSync、「 AWS AppSync デベロッパーガイド」の「セットアップと設定」を参照してください。

〔AppSync.4] AWS AppSync GraphQL APIsにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::AppSync::GraphQLApi`

AWS Config ルール: `tagged-appsync-graphqlapi` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、 AWS AppSync GraphQL API にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。GraphQL API にタグキーがな

い場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、GraphQL API にキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS AppSync GraphQL API にタグを追加するには、「 API リファレンスTagResource」の「」を参照してください。 AWS AppSync

〔AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理 > パスワードレス認証

重要度: 高

リソースタイプ: `AWS::AppSync::GraphQLApi`

AWS Config ルール : appsync-authorization-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `AllowedAuthorizationTypes: AWS_LAMBDA, AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS` (カスタマイズ不可)

このコントロールは、アプリケーションが API キーを使用して AWS AppSync GraphQL API とやり取りしているかどうかをチェックします。 AWS AppSync GraphQL API が API キーで認証されている場合、コントロールは失敗します。

API キーは、認証されていない GraphQL エンドポイントを作成するときに AWS AppSync サービスによって生成されるアプリケーション内のハードコードされた値です。この API キーが侵害されると、エンドポイントは意図しないアクセスに対して脆弱になります。一般にアクセス可能なアプリケーションやウェブサイトをサポートしている場合を除き、API キーを認証に使用することはお勧めしません。

修正

AWS AppSync GraphQL API の認証オプションを設定するには、「 AWS AppSync デベロッパーガイド」の「認証と認証」を参照してください。

Amazon Athena コントロール

これらのコントロールは Athena リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Athena.1] Athena ワークグループは、保管中に暗号化する必要があります

> **Important**
>
> Security Hub は 2024 年 4 月にこのコントロールを廃止しました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

重要度: 中

リソースタイプ: `AWS::Athena::WorkGroup`

AWS Config ルール : athena-workgroup-encrypted-at-rest

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Athena ワークグループが保管中に暗号化されているかどうかをチェックします。Athena ワークグループが保管中に暗号化されていない場合、コントロールは失敗します。

Athena では、チーム、アプリケーション、またはさまざまなワークロードのクエリを実行するためのワークグループを作成できます。各ワークグループには、すべてのクエリで暗号化を有効にする設定があります。Amazon Simple Storage Service (Amazon S3) マネージドキーによるサーバー側の暗号化、 AWS Key Management Service （ AWS KMS) キーによるサーバー側の暗号化、またはカスタマーマネージド KMS キーによるクライアント側の暗号化を使用するオプションがあります。保管中のデータとは、永続的な不揮発性ストレージに任意の期間保管されているデータを指します。暗号化は、このようなデータの機密性を保護し、権限のないユーザーがデータにアクセスするリスクを低減するのに役立ちます。

修正

Athena ワークグループの保管中の暗号化を有効にするには、「Amazon Athena ユーザーガイド」の「ワークグループの編集」を参照してください。[クエリ結果の設定] セクションで [クエリ結果の暗号化] をクリックします。

[Athena.2] Athena データカタログにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::Athena::DataCatalog`

AWS Config ルール: `tagged-athena-datacatalog` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、Amazon Athena データカタログにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。データカタログにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、データカタログにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Athena データカタログにタグを追加するには、「Amazon Athena ユーザーガイド」の「Athena リソースのタグ付け」を参照してください。 Amazon Athena

[Athena.3] Athena ワークグループにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::Athena::WorkGroup`

AWS Config ルール: `tagged-athena-workgroup` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、Amazon Athena ワークグループに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。ワークグループにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、ワークグループにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責

任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Athena ワークグループにタグを追加するには、「Amazon Athena ユーザーガイド」の「個々のワークグループでのタグの追加と削除」を参照してください。 Amazon Athena

AWS Backup コントロール

これらのコントロールは AWS Backup リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります

関連する要件: NIST.800-53.r5 CP-9(8)、NIST.800-53.r5 SI-12

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::Backup::RecoveryPoint`

AWS Config ルール : `backup-recovery-point-encrypted`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS Backup リカバリポイントが保管中に暗号化されているかどうかを確認します。復旧ポイントが保管時に暗号化されていない場合、コントロールは失敗します。

AWS Backup 復旧ポイントとは、バックアッププロセスの一部として作成されるデータの特定のコピーまたはスナップショットを指します。データがバックアップされた特定の瞬間を表し、元のデータが失われたり、破損したり、アクセス不能になったりした場合の復元ポイントとして機能します。バックアップ復旧ポイントを暗号化すると、不正アクセスに対する保護をさらに強化することができます。暗号化は、バックアップデータの機密性、完全性、およびセキュリティを保護するためのベストプラクティスです。

修正

AWS Backup 復旧ポイントを暗号化するには、「 AWS Backup デベロッパーガイド」の「 でのバックアップの暗号化 AWS Backup」を参照してください。

[Backup.2] AWS Backup 復旧ポイントにタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::Backup::RecoveryPoint`

AWS Configルール: `tagged-backup-recoverypoint` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーで	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	は、大文字と小文字が区別されます。			

このコントロールは、 AWS Backup 復旧ポイントにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。復旧ポイントにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、復旧ポイントにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS Backup 復旧ポイントにタグを追加するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。

2. ナビゲーションペインで、[バックアッププラン] を選択します。
3. リストからバックアッププランを選択します。
4. Backup プランタグ セクションで、タグの管理 を選択します。
5. タグのキーと値を入力します。追加のキーと値のペアに新しいタグを追加を選択します。
6. タグの追加を完了したら、[Save (保存)] を選択します。

[Backup.3] AWS Backup ボールトにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::Backup::BackupVault`

AWS Configルール: `tagged-backup-backupvault` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、ボール AWS Backup トにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。復旧ポイントにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、復旧ポイントにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS Backup ボールトにタグを追加するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアップボールト] を選択します。
3. リストからバックアップボールトを選択します。
4. バックアップボールトタグ セクションで、タグの管理 を選択します。
5. タグのキーと値を入力します。キーと値のペアを追加するには、新しいタグを追加 を選択します。
6. タグの追加を完了したら、[Save (保存)] を選択します。

[Backup.4] AWS Backup レポートプランにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::Backup::ReportPlan`

AWS Configルール: `tagged-backup-reportplan` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、 AWS Backup レポートプランにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。レポートプランにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、レポートプランにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベ

ストプラクティスの詳細については、「」の「AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS Backup レポートプランにタグを追加するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアップボールト] を選択します。
3. リストからバックアップボールトを選択します。
4. バックアップボールトタグ セクションで、タグの管理 を選択します。
5. [新しいタグを追加] をクリックします。タグのキーと値を入力します。追加のキーと値のペアについても同じ手順を繰り返します。
6. タグの追加を完了したら、[Save (保存)] を選択します。

[Backup.5] AWS Backup バックアップ計画にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::Backup::BackupPlan`

AWS Configルール: `tagged-backup-backupplan` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーで	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	は、大文字と小文字が区別されます。			

このコントロールは、 AWS Backup バックアッププランにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。バックアッププランにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、バックアッププランにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS Backup バックアッププランにタグを追加するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。

2. ナビゲーションペインで、[バックアップボールト] を選択します。
3. リストからバックアップボールトを選択します。
4. バックアップボールトタグ セクションで、タグの管理 を選択します。
5. [新しいタグを追加] をクリックします。タグのキーと値を入力します。追加のキーと値のペアについても同じ手順を繰り返します。
6. タグの追加を完了したら、[Save (保存)] を選択します。

AWS CloudFormation コントロール

これらのコントロールは CloudFormation リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔CloudFormation.1] CloudFormation スタックは Simple Notification Service (SNS) と統合する必要があります

> **Important**
>
> Security Hub は 2024 年 4 月にこのコントロールを廃止しました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

関連する要件: NIST.800-53.r5 SI-4(12)、NIST.800-53.r5 SI-4(5)

カテゴリ: 検出 > 検出サービス > アプリケーションモニタリング

重要度: 低

リソースタイプ: `AWS::CloudFormation::Stack`

AWS Config ルール : `cloudformation-stack-notification-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon Simple Notification Service の通知が AWS CloudFormation スタックに統合されているかどうかをチェックします。SNS 通知がスタックに関連付けられていない場合、CloudFormation スタックのコントロールは失敗します。

CloudFormation スタックで SNS 通知を設定すると、スタックで発生したイベントや変更を利害関係者にすぐに通知できます。

修正

CloudFormation スタックと SNS トピックを統合するには、「ユーザーガイド」の「スタックの直接更新」を参照してください。 AWS CloudFormation

〔CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::CloudFormation::Stack`

AWS Config ルール: `tagged-cloudformation-stack` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、 AWS CloudFormation スタックにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。スタックにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、スタックにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

CloudFormation スタックにタグを追加するには、AWS CloudFormation 「 API リファレンスCreateStack」の「」を参照してください。

Amazon CloudFront コントロール

これらのコントロールは CloudFront リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります

関連する要件: NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)

カテゴリ: 保護 > セキュアなアクセス管理 > パブリックアクセスが不可能なリソース

重要度: 高

リソースタイプ: `AWS::CloudFront::Distribution`

AWS Config ルール : `cloudfront-default-root-object-configured`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon CloudFront ディストリビューションがデフォルトのルートオブジェクトである特定のオブジェクトを返すように設定されているかどうかを確認します。 CloudFront ディストリビューションにデフォルトのルートオブジェクトが設定されていない場合、コントロールは失敗します。

ユーザーは、ディストリビューション内のオブジェクトではなく、ディストリビューションのルート URL を要求することがあります。この場合、デフォルトのルートオブジェクトを指定することで、ウェブディストリビューションのコンテンツの漏洩を防止できます。

修正

CloudFront ディストリビューションのデフォルトのルートオブジェクトを設定するには、「Amazon CloudFront デベロッパーガイド」の「デフォルトのルートオブジェクトを指定する方法」を参照してください。

〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です

関連する要件: NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::CloudFront::Distribution`

AWS Config ルール : `cloudfront-viewer-policy-https`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon CloudFront ディストリビューションでビューワーが HTTPS を直接使用する必要があるかどうか、またはリダイレクトを使用するかどうかをチェックします。`ViewerProtocolPolicy` が `defaultCacheBehavior` または `cacheBehaviors` の `allow-all` に設定されている場合、コントロールは失敗します。

HTTPS (TLS) を使用すると、潜在的な攻撃者がネットワークトラフィックを傍受または操作するために または同様の攻撃を使用すること person-in-the-middleを防ぐことができます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。転送中のデータの暗号化は、パフォーマンスに影響する可能性があります。TLS のパフォーマンスプロファイルと TLS の影響を把握するには、この機能を使用してアプリケーションをテストする必要があります。

修正

転送中の CloudFront ディストリビューションを暗号化するには、「Amazon CloudFront デベロッパーガイド」の「ビューワーと 間の通信に HTTPS を要求する CloudFront」を参照してください。

〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 低

リソースタイプ: `AWS::CloudFront::Distribution`

AWS Config ルール : `cloudfront-origin-failover-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon CloudFront ディストリビューションに 2 つ以上のオリジンを持つオリジングループが設定されているかどうかをチェックします。

CloudFront オリジンフェイルオーバーは可用性を高めることができます。オリジンフェイルオーバーは、プライマリオリジンが使用できない場合、または特定の HTTP レスポンスステータスコードを返した場合に、自動的にセカンダリーオリジンにトラフィックをリダイレクトします。

修正

CloudFront ディストリビューションのオリジンフェイルオーバーを設定するには、「Amazon CloudFront デベロッパーガイド」の「オリジングループの作成」を参照してください。

〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります

関連する要件: NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::CloudFront::Distribution`

AWS Config ルール : `cloudfront-accesslogs-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、ディス CloudFront トリビューションでサーバーアクセスのログ記録が有効になっているかどうかをチェックします。ディストリビューションでアクセスのログ記録が有効でない場合、コントロールは失敗します。

CloudFront アクセスログは、 が CloudFront 受け取るすべてのユーザーリクエストに関する詳細情報を提供します。各ログには、リクエストが受信された日時、リクエストを行ったビューワーの IP アドレス、リクエストソース、ビューワーからのリクエストポート番号などの情報が含まれます。

これらのログは、セキュリティ監査やアクセス監査、証拠調査などのアプリケーションに役立ちます。アクセスログの分析方法に関するその他のガイダンスについては、「Amazon Athena ユーザーガイド」の「Amazon CloudFront ログのクエリ」を参照してください。 Amazon Athena

修正

CloudFront ディストリビューションのアクセスログを設定するには、「Amazon CloudFront デベロッパーガイド」の「標準ログ (アクセスログ) の設定と使用」を参照してください。

〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります

関連する要件: NIST.800-53.r5 AC-4(21)

カテゴリ: 保護 > 保護サービス

重要度: 中

リソースタイプ: `AWS::CloudFront::Distribution`

AWS Config ルール : `cloudfront-associated-with-waf`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 CloudFront ディストリビューションが AWS WAF Classic または AWS WAF ウェブ ACLs に関連付けられているかどうかをチェックします。ディストリビューションがウェブ ACL に関連付けられていない場合、コントロールは失敗します。

AWS WAF は、ウェブアプリケーションと APIsから保護するのに役立つウェブアプリケーションファイアウォールです。これで、ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる一連のルールを設定することができます。このルールは、ユーザーが定義するカスタマイズ可能なウェブセキュリティルールと条件に基づいて、ウェブリクエストを許可、ブロック、またはカウントします。悪意のある攻撃から保護するために、 CloudFront ディストリビューションが AWS WAF ウェブ ACL に関連付けられていることを確認します。

修正

AWS WAF ウェブ ACL を CloudFront ディストリビューションに関連付けるには、「Amazon CloudFront デベロッパーガイド」の「 AWS WAF を使用してコンテンツへのアクセスを制御する」を参照してください。

〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります

関連する要件: NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5

SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::CloudFront::Distribution`

AWS Config ルール : `cloudfront-custom-ssl-certificate`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 CloudFront ディストリビューションが CloudFront が提供するデフォルトの SSL/TLS 証明書を使用しているかどうかをチェックします。このコントロールは、 CloudFront ディストリビューションがカスタム SSL/TLS 証明書を使用している場合に成功します。 CloudFront ディストリビューションがデフォルトの SSL/TLS 証明書を使用している場合、このコントロールは失敗します。

カスタム SSL/TLS を使用すると、ユーザーは代替ドメイン名を使用してコンテンツにアクセスできます。カスタム証明書は AWS Certificate Manager (推奨)、または IAM で保存できます。

修正

カスタム SSL/TLS 証明書を使用して CloudFront ディストリビューションの代替ドメイン名を追加するには、「Amazon CloudFront デベロッパーガイド」の「代替ドメイン名の追加」を参照してください。

〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 低

リソースタイプ: `AWS::CloudFront::Distribution`

AWS Config ルール : `cloudfront-sni-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon CloudFront ディストリビューションがカスタム SSL/TLS 証明書を使用していて、SNI を使用して HTTPS リクエストを処理するように設定されているかどうかを確認します。カスタム SSL/TLS 証明書が関連付けられているものの、SSL/TLS サポートメソッドが専用 IP アドレスである場合、このコントロールは失敗します。

Server Name Indication (SNI) は、2010 年以降にリリースされたブラウザとクライアントでサポートされている TLS プロトコルを拡張したものです。SNI を使用して HTTPS リクエストを処理する CloudFront ように を設定すると、 は代替ドメイン名を各エッジロケーションの IP アドレスに CloudFront 関連付けます。ビューワーがコンテンツに対して HTTPS リクエストを送信すると、DNS は、正しいエッジロケーションの IP アドレスにリクエストをルーティングします。ドメイン名の IP アドレスが SSL/TLS ハンドシェイクネゴシエーション中に決定されます。IP アドレスはディストリビューション専用にはなりません。

修正

SNI を使用して HTTPS リクエストを処理するように CloudFront ディストリビューションを設定するには、「 CloudFront デベロッパーガイド」の「SNI を使用して HTTPS リクエストを処理する (ほとんどのクライアントで動作)」を参照してください。

〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります

関連する要件: NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::CloudFront::Distribution`

AWS Config ルール : `cloudfront-traffic-to-origin-encrypted`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon CloudFront ディストリビューションがカスタムオリジンへのトラフィックを暗号化しているかどうかをチェックします。このコントロールは、オリジンプロトコルポリシーが「http-only」を許可する CloudFront ディストリビューションでは失敗します。ディストリビューションのオリジンプロトコルポリシーが「match-viewer」で、ビューワープロトコルポリシーが「allow-all」である場合にも、このコントロールは失敗します。

HTTPS (TLS) は、ネットワークトラフィックの傍受や操作を防止するために使用できます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。

修正

CloudFront 接続の暗号化を要求するようにオリジンプロトコルポリシーを更新するには、「Amazon CloudFront デベロッパーガイド」の「 CloudFront とカスタムオリジン間の通信に HTTPS を要求する」を参照してください。

〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください

関連する要件: NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::CloudFront::Distribution`

AWS Config ルール : `cloudfront-no-deprecated-ssl-protocols`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon CloudFront ディストリビューションが CloudFront エッジロケーションとカスタムオリジン間の HTTPS 通信に非推奨の SSL プロトコルを使用しているかどうかを確認します。 CloudFront ディストリビューションに `OriginSslProtocols`が含まれている場合、このコントロールは失敗`CustomOriginConfig`します`SSLv3`。

2015 年、Internet Engineering Task Force (IETF) は、SSL 3.0 はプロトコルの安全性が不十分であることから廃止すべきであると、正式に発表しました。カスタムオリジンへの HTTPS 通信には、TLSv1.2 以降を使用することが推奨されます。

修正

CloudFront ディストリビューションのオリジン SSL プロトコルを更新するには、「Amazon CloudFront デベロッパーガイド」の CloudFront 「 とカスタムオリジン間の通信に HTTPS を要求する」を参照してください。

〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません

関連する要件: NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 識別 > リソース設定

重要度: 高

リソースタイプ: `AWS::CloudFront::Distribution`

AWS Config ルール: `cloudfront-s3-origin-non-existent-bucket`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Amazon CloudFront ディストリビューションが存在しない Amazon S3 オリジンを指しているかどうかをチェックします。オリジンが存在しないバケットを指すように設定されている場合、ディス CloudFront トリビューションのコントロールは失敗します。このコントロールは、静的ウェブサイトホスティングのない S3 バケットが S3 オリジンである CloudFront ディストリビューションにのみ適用されます。

アカウント内の CloudFront ディストリビューションが存在しないバケットを指すように設定されている場合、悪意のある第三者が参照先のバケットを作成し、ディストリビューションを通じて独自のコンテンツを提供できます。ルーティング動作に関係なくすべてのオリジンをチェックして、ディストリビューションが適切なオリジンをポイントしていることを確認することをお勧めします。

修正

新しいオリジンを指すように CloudFront ディストリビューションを変更するには、「Amazon CloudFront デベロッパーガイド」の「ディストリビューションの更新」を参照してください。

〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります

カテゴリ: 保護 > セキュアなアクセス管理 > パブリックアクセスが不可能なリソース

重要度: 中

リソースタイプ: `AWS::CloudFront::Distribution`

AWS Config ルール : `cloudfront-s3-origin-access-control-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon S3 オリジンを持つ Amazon CloudFront ディストリビューションにオリジンアクセスコントロール (OAC) が設定されているかどうかを確認します。OAC が CloudFront ディストリビューション用に設定されていない場合、コントロールは失敗します。

S3 バケットを CloudFront ディストリビューションのオリジンとして使用する場合は、OAC を有効にできます。これにより、指定された CloudFront ディストリビューションを介してのみバケット内のコンテンツへのアクセスが許可され、バケットまたは別のディストリビューションからの直接アクセスが禁止されます。はオリジンアクセスアイデンティティ (OAI) CloudFront をサポートしていますが、OAC には追加機能があり、OAI を使用するディストリビューションは OAC に移行できます。OAI は S3 オリジンに安全にアクセスする方法を提供しますが、きめ細かなポリシー設定や、AWS 署名バージョン 4 (SigV4) を必要とする で POST メソッドを使用する HTTP/HTTPS リクエストのサポート AWS リージョン がないなどの制限があります。OAI は による暗号化もサポートしていません AWS Key Management Service。OAC は、IAM サービスプリンシパルを使用して S3 オリジンで認証するという AWS ベストプラクティスに基づいています。

修正

S3 オリジンを持つ CloudFront ディストリビューションの OAC を設定するには、Amazon S3オリジンへのアクセスの制限」を参照してください。 CloudFront

〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::CloudFront::Distribution`

AWS Config ルール : `tagged-cloudfront-distribution` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon CloudFront ディストリビューションにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。ディストリビューションにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、ディストリビューションがどのキーでもタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

CloudFront ディストリビューションにタグを追加するには、「Amazon デベロッパーガイド」の「Amazon CloudFront ディストリビューションのタグ付け」を参照してください。 CloudFront

AWS CloudTrail コントロール

これらのコントロールは CloudTrail リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔CloudTrail.1] CloudTrail 読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン追跡を有効にして設定する必要があります

関連する要件： CIS AWS Foundations Benchmark v1.2.0/2.1、 CIS AWS Foundations Benchmark v1.4.0/3.1、 CIS AWS Foundations Benchmark v3.0.0/3.1、 NIST.800-53.r5 AC-2(4)、 NIST.800-53.r5 AC-4(26)、 NIST.800-53.r5 AC-6(9)、 NIST.800-53.r5 AU-10、 NIST.800-53.r5 AU-12、 NIST.800-53.r5 AU-2、 NIST.800-53.r5 AU-3、 NIST.800-53.r5 AU-6(3)、 NIST.800-53.r5 AU-6(4)、 NIST.800-53.r5 AU-14(1)、 NIST.800-53.r5 CA-7、 NIST.800-53.r5 SC-7(9)、 NIST.800-53.r5 SI-3 (8)、 NIST.800-53.r5 SI-4 (20)、 NIST.800-53.r5 SI-7(8)、 NIST.800-53.r5 SA-8 (22)

カテゴリ: 識別 > ログ記録

重要度: 高

リソースタイプ: `AWS::::Account`

AWS Config ルール: `multi-region-cloudtrail-enabled`

スケジュールタイプ: 定期的

パラメータ:

- `readWriteType`: `ALL` (カスタマイズ不可)

  `includeManagementEvents`: `true` (カスタマイズ不可)

このコントロールは、読み取りおよび書き込み管理イベントをキャプチャするマルチリージョン AWS CloudTrail 証跡が少なくとも 1 つあるかどうかをチェックします。が無効になっているか、読み取りおよび書き込み管理イベントをキャプチャする CloudTrail 証跡が少なくとも 1 つない場合、コントロール CloudTrail は失敗します。

AWS CloudTrail は、アカウントの AWS API コールを記録し、ログファイルを配信します。記録された情報には、次の情報が含まれます。

- API 発信者の ID
- API コールの時刻
- API 発信者の送信元 IP アドレス
- パラメータのリクエスト
- によって返されるレスポンス要素 AWS のサービス

CloudTrail は、、 AWS Management Console SDK、コマンドラインツールからの AWS API コールなど、 アカウントの API コールの履歴を提供します。 AWS SDKs 履歴には、 AWS のサービス などの上位レベルの API コールも含まれます AWS CloudFormation。

によって生成された AWS API コール履歴 CloudTrail により、セキュリティ分析、リソース変更の追跡、コンプライアンス監査が可能になります。マルチリージョン追跡には、次の利点もあります。

- マルチリージョン追跡により、使用していないリージョンで発生する予期しないアクティビティを検出できます。
- マルチリージョン追跡では、グローバルサービスイベントのログ記録がデフォルトで追跡に対して確実に有効になっています。グローバルサービスイベントのログ記録は、 AWS グローバルサービスによって生成されたイベントを記録します。
- マルチリージョンの証跡の場合、すべての読み取りおよび書き込みオペレーションの管理イベントにより、 は 内のすべてのリソースの管理オペレーション CloudTrail を記録します AWS アカウント。

デフォルトでは、 を使用して作成された CloudTrail 証跡はマルチリージョンの証跡 AWS Management Console です。

修正

で新しいマルチリージョン証跡を作成するには CloudTrail、「 ユーザーガイド」の「証跡の作成AWS CloudTrail 」を参照してください。以下の値を使用します。

フィールド	値
追加設定、ログファイル検証	有効
ログイベント、管理イベント、API アクティビティを選択	[読み取り] と [書き込み] 除外にするチェックボックスはオフにしてください。

既存の追跡を更新するには、「AWS CloudTrail ユーザーガイド」の「証跡の更新」を参照してください。[管理イベント] の [API アクティビティ] で、[読み取り] と [書き込み] を選択します。

〔CloudTrail.2] 保管時の暗号化を有効にする CloudTrail 必要があります

関連する要件： PCI DSS v3.2.1/3.4、CIS AWS Foundations Benchmark v1.2.0/2.7、CIS AWS Foundations Benchmark v1.4.0/3.7、CIS AWS Foundations Benchmark v3.0.0/3.5、NIST.800-53.r5 AU-9、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC SC-7 SI-7-

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::CloudTrail::Trail`

AWS Config ルール: `cloud-trail-encryption-enabled`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロール CloudTrail は、 がサーバー側の暗号化 (SSE) AWS KMS key 暗号化を使用するように設定されているかどうかをチェックします。`KmsKeyId` が定義されていない場合、コントロールは失敗します。

機密性の高い CloudTrail ログファイルのセキュリティを強化するには、保管時の暗号化のためにログファイルに AWS KMS keys (SSE-KMS) によるサーバー側の暗号化を使用する必要があります。

CloudTrail デフォルトでは、 によってバケット CloudTrail に配信されるログファイルは、Amazon S3-managedの暗号化キー (SSE-S3) による Amazon サーバー側の暗号化によって暗号化されることに注意してください。

修正

CloudTrail ログファイルの SSE-KMS 暗号化を有効にするには、「 ユーザーガイド」の「KMS キーを使用するように証跡を更新するAWS CloudTrail 」を参照してください。

〔CloudTrail.3] 少なくとも 1 つの CloudTrail 証跡を有効にする必要があります

関連する要件: PCI DSS v3.2.1/10.1、PCI DSS v3.2.1/10.2.1、PCI DSS v3.2.1/10.2.2、PCI DSS v3.2.1/10.2.3、PCI DSS v3.2.1/10.2.4、PCI DSS v3.2.1/10.2.5、PCI DSS v3.2.1/10.2.6、PCI DSS v3.2.1/10.2.7、PCI DSS v3.2.1/10.3.1、PCI DSS v3.2.1/10.3.2、PCI DSS v3.2.1/10.3.3、PCI DSS v3.2.1/10.3.4、PCI DSS v3.2.1/10.3.5、PCI DSS v3.2.1/10.3.6

カテゴリ: 識別 > ログ記録

重要度: 高

リソースタイプ: `AWS::::Account`

AWS Config ルール: `cloudtrail-enabled`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、 で証 AWS CloudTrail 跡が有効になっているかどうかをチェックします AWS アカウント。アカウントに少なくとも 1 つの CloudTrail 証跡が有効になっていない場合、コントロールは失敗します。

ただし、一部の AWS サービスでは、すべての APIs とイベントのログ記録が有効になっていません。以外の追加の監査証跡を実装 CloudTrail し、CloudTrail サポートされているサービスと統合 の各サービスのドキュメントを確認する必要があります。

修正

の使用を開始 CloudTrail して証跡を作成するには、 AWS CloudTrail ユーザーガイドの「 の開始方法 AWS CloudTrail」チュートリアルを参照してください。

〔CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります

関連する要件： PCI DSS v3.2.1/10.5.2、PCI DSS v3.2.1/10.5.5、CIS AWS Foundations Benchmark v1.2.0/2.2、CIS AWS Foundations Benchmark v1.4.0/3.2、CIS AWS Foundations Benchmark v3.0.0/3.2、NIST.800-53.r5 AU-9、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-7(1)、NIST.800-53.r5 SI-7(3)、NIST.800-53.r5 SI-7(7)

カテゴリ: データ保護 > データの整合性

重要度: 低

リソースタイプ: `AWS::CloudTrail::Trail`

AWS Config ルール: `cloud-trail-log-file-validation-enabled`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、証跡でログファイルの CloudTrail整合性検証が有効になっているかどうかをチェックします。

CloudTrail ログファイルの検証では、Amazon S3 に CloudTrail 書き込む各ログのハッシュを含むデジタル署名されたダイジェストファイルが作成されます。これらのダイジェストファイルを使用して、ログの CloudTrail 配信後にログファイルが変更、削除、または変更されていないかどうかを判断できます。

Security Hub では、すべての追跡でファイルの検証を有効にすることを推奨します。ログファイルの検証により、 CloudTrail ログの整合性チェックが追加されます。

修正

CloudTrail ログファイルの検証を有効にするには、「 ユーザーガイド」の「 のログファイルの整合性の検証 CloudTrailを有効にするAWS CloudTrail 」を参照してください。

〔CloudTrail.5] CloudTrail 証跡は Amazon CloudWatch Logs と統合する必要があります

関連する要件： PCI DSS v3.2.1/10.5.3、 CIS AWS Foundations Benchmark v1.2.0/2.4、 CIS AWS Foundations Benchmark v1.4.0/3.4、 NIST.800-53.r5 AC-2(4)、 NIST.800-53.r5 AC-4(26)、 NIST.800-53.r5 AC-6(9)、 NIST.800-53.r5 AU-10、 NIST.800-53.r5 AU-12、 NIST.800-53.r5 AU-2、

NIST.800-53.r5 AU-3、 NIST.800-53.r5 AU-6(1)、 NIST.800-53.r5 AU-6(3)、 NIST.800-53.r5 AU-6(4)、 NIST.800-53.r5 AU-6(5)、 NIST.800-53.r5 AU-7(1)、 NIST.800-53.r5 CA-7、 NIST.800-53.r5 SC-7(9)、 NIST.800-53.r5 SI-20、 NIST.800-53.r5 SI-3 (8)、 NIST.800-53.r5 SI-4 (20)、 NIST.800-53.r5 SI-4 (5)、 NIST.800-53.r5 SI-7 (8)

カテゴリ: 識別 > ログ記録

重要度: 低

リソースタイプ: `AWS::CloudTrail::Trail`

AWS Config ルール: cloud-trail-cloud-watch-logs-enabled

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、証 CloudTrail 跡が CloudWatch ログにログを送信するように設定されているかどうかを確認します。追跡の `CloudWatchLogsLogGroupArn` プロパティが空の場合、コントロールは失敗します。

CloudTrail は、特定のアカウントで行われた AWS API コールを記録します。記録された情報には、以下が含まれます。

- API 発信者のアイデンティティ
- API コールの時刻
- API 発信者の送信元 IP アドレス
- リクエストパラメータ
- によって返されるレスポンス要素 AWS のサービス

CloudTrail はログファイルのストレージと配信に Amazon S3 を使用します。長期分析のために、指定された S3 バケットに CloudTrail ログをキャプチャできます。リアルタイム分析を実行するには、ログ CloudTrail を CloudWatch ログに送信するように を設定できます。

アカウントのすべてのリージョンで有効になっている証跡の場合、 はそれらのすべてのリージョンのログファイルを Logs CloudWatch ロググループ CloudTrail に送信します。

Security Hub では、 CloudTrail ログを Logs CloudWatch に送信することをお勧めします。この推奨事項は、アカウントアクティビティが確実にキャプチャおよびモニタリングされ、適切なアラームが

出されることを確認する目的であることにご注意ください CloudWatch ログを使用して、 でこれをセットアップできます AWS のサービス。この推奨事項は、別のソリューションの使用を除外するものではありません。

Logs CloudWatch に CloudTrail ログを送信すると、ユーザー、API、リソース、および IP アドレスに基づいて、リアルタイムおよび過去のアクティビティログ記録が容易になります。この方法を使用して、異常または機密性の高いアカウントアクティビティに対してアラームと通知を確立できます。

修正

CloudWatch ログ CloudTrail と統合するには、「 AWS CloudTrail ユーザーガイド」の CloudWatch 「ログへのイベントの送信」を参照してください。

〔CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットがパブリックにアクセスできないようにする

関連する要件： CIS AWS Foundations Benchmark v1.2.0/2.3、CIS AWS Foundations Benchmark v1.4.0/3.3

カテゴリ: 識別 > ログ記録

重要度: 非常事態

リソースタイプ: `AWS::S3::Bucket`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的および変更がトリガーされた場合

パラメータ: なし

CloudTrail は、アカウントで行われたすべての API コールのレコードを記録します。これらのログファイルは S3 バケットに保存されます。CIS では、ログへのパブリックアクセスを防ぐために CloudTrail ログを記録する S3 バケットに適用される S3 バケットポリシーまたはアクセスコントロールリスト (ACL) を推奨しています CloudTrail 。 CloudTrail ログコンテンツへのパブリックアクセスを許可すると、攻撃者は影響を受けるアカウントの使用または設定の弱点を特定するのに役立ちます。

このチェックを実行するために、Security Hub はまずカスタムロジックを使用して、 CloudTrail ログが保存されている S3 バケットを探します。次に、 AWS Config マネージドルールを使用して、バケットがパブリックにアクセス可能であることを確認します。

ログを単一の集中管理 S3 バケットに集約する場合、Security Hub は、集中管理された S3 バケットがあるアカウントとリージョンに対してのみチェックを実行します。他のアカウントとリージョンでは、コントロールステータスは [No data] (データなし) となります。

バケットがパブリックアクセス可能な場合、チェックにより結果 (失敗) が生成されます。

修正

CloudTrail S3 バケットへのパブリックアクセスをブロックするには、「Amazon Simple Storage Service ユーザーガイド」のS3 バケットのブロックパブリックアクセス設定の構成」を参照してください。4 つの Amazon S3 パブリックアクセスブロック設定をすべて選択します。

〔CloudTrail.7] S3 バケットで CloudTrail S3 バケットアクセスログ記録が有効になっていることを確認する

関連する要件： CIS AWS Foundations Benchmark v1.2.0/2.6、CIS AWS Foundations Benchmark v1.4.0/3.6、CIS AWS Foundations Benchmark v3.0.0/3.4

カテゴリ: 識別 > ログ記録

重要度: 低

リソースタイプ: `AWS::S3::Bucket`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的

パラメータ: なし

S3 バケットアクセスログ記録により、S3 バケットに対して行われたリクエストごとのアクセスレコードを含むログが生成されます。アクセスログレコードには、リクエストのタイプ、リクエストに指定されたリソース、リクエストが処理された日時など、リクエストの詳細が記録されます。

CIS では、 CloudTrail S3 バケットでバケットアクセスのログ記録を有効にすることをお勧めします。

ターゲット S3 バケットで S3 バケットのログ記録を有効にすることで、ターゲットバケット内のオブジェクトに影響を与える可能性のあるすべてのイベントをキャプチャできます。ログを別のバケットに配置するように設定すると、ログ情報にアクセスできるようになり、セキュリティおよびインシデント対応のワークフローで役立ちます。

このチェックを実行するために、Security Hub はまずカスタムロジックを使用して CloudTrail ログが保存されているバケットを検索し、次に AWS Config マネージドルールを使用してログ記録が有効になっているかどうかを確認します。

が複数の から 1 つの送信先 Amazon S3 バケット AWS アカウント にログファイルを CloudTrail 配信する場合、Security Hub は、そのバケットが配置されているリージョンの送信先バケットに対してのみこのコントロールを評価します。これにより、結果が効率化されます。ただし、ログを送信先バケットに配信するすべてのアカウント CloudTrail で を有効にする必要があります。宛先バケットを保持しているアカウントを除くすべてのアカウントの制御ステータスは「データなし」です。

バケットがパブリックアクセス可能な場合、チェックにより結果 (失敗) が生成されます。

修正

CloudTrail S3 バケットのサーバーアクセスログ記録を有効にするには、Amazon S3 サーバーアクセスログ記録の有効化」を参照してください。

〔CloudTrail.9] CloudTrail 証跡にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::CloudTrail::Trail`

AWS Config ルール: `tagged-cloudtrail-trail` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS CloudTrail 証跡にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。証跡にタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、証跡にキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

CloudTrail 証跡にタグを追加するには、 AWS CloudTrail API リファレンスAddTagsの「」を参照してください。

Amazon CloudWatch コントロール

これらのコントロールは CloudWatch リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔CloudWatch.1]「ルート」ユーザーの使用に対してログメトリクスフィルターとアラームが存在する必要があります

関連する要件： PCI DSS v3.2.1/7.2.1、CIS AWS Foundations Benchmark v1.2.0/1.1、CIS AWS Foundations Benchmark v1.2.0/3.3、CIS AWS Foundations Benchmark v1.4.0/1.7、CIS AWS Foundations Benchmark v1.4.0/4.3

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的

パラメータ: なし

ルートユーザーは、 AWS アカウントのすべてのリソースとサービスに完全かつ無制限にアクセスできます。日常的なタスクにはルートユーザーを使用しないことが強く推奨されます。ルートユーザーの使用を最小限にし、アクセス管理の最小特権の原則を採用することにより、高い権限を持つ認証情報の意図しない変更や偶発的な開示のリスクが軽減されます。

ベストプラクティスは、アカウントおよびサービスの管理タスクを実行するときに必要となる場合のみ、ルートユーザー認証情報を使用することです。 AWS Identity and Access Management (IAM) ポリシーをグループとロールに直接適用しますが、ユーザーには適用されません。日常的に使用する管理者を設定する方法のチュートリアルについては、「IAM ユーザーガイド」の「最初の IAM 管理者のユーザーおよびグループの作成」を参照してください。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 1.7 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 証跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡であ

る可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
チェックの結果、以下の場合は結果 FAILED となります。

- 追跡が設定されていません。
- 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。

チェックの結果、以下の場合はコントロール状況が NO_DATA になります。

- マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

  組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任された管理者アカウントでのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは NO_DATA になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、ListSubscriptionsByTopic を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 WARNING を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS ア

ラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。

2. すべての に適用される CloudTrail 証跡を作成します AWS リージョン。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 証跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。

3. メトリクスのフィルターを作成します。手順については、「Amazon ユーザーガイド」の「ログググループのメトリクスフィルターを作成する」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}`
メトリクス名前空間	**LogMetrics**
メトリクス値	**1**
デフォルト値	**0**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon ユーザーガイド」の「ロググループメトリクスフィルターに基づく CloudWatch アラームの作成」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が の場合	以上
条件は...	**1**

〔CloudWatch.2] 不正な API コールに対してログメトリクスフィルターとアラームが存在することを確認する

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.1

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ:
`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的

パラメータ: なし

CloudTrail ログを Logs に送信し、対応するメトリクスフィルターとアラームを確立することで、API CloudWatch コールをリアルタイムでモニタリングできます。

CIS では、不正な API コールに対するメトリクスフィルターとアラームを作成することを推奨しています。不正な API コールをモニタリングすることでアプリケーションエラーを明らかにし、悪意のあるアクティビティを検出するのにかかる時間を短縮できる可能性があります。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.2 のコントロール 3.1 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 証跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
> チェックの結果、以下の場合は結果 `FAILED` となります。
>
> - 追跡が設定されていません。

- 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。

チェックの結果、以下の場合はコントロール状況が NO_DATA になります。

- マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

  組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任された管理者アカウントでのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは NO_DATA になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、ListSubscriptionsByTopic を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 WARNING を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての に適用される CloudTrail 証跡を作成します AWS リージョン。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

CloudTrail 証跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。

3. メトリクスのフィルターを作成します。手順については、「Amazon ユーザーガイド」の「ロググループのメトリクスフィルターを作成する」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.errorCode="*UnauthorizedOperation") \|\| ($.errorCode="AccessDenied*")}`
メトリクス名前空間	**LogMetrics**
メトリクス値	**1**
デフォルト値	**0**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon ユーザーガイド」の「ロググループメトリクスフィルターに基づく CloudWatch アラームの作成」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が である場合	以上
条件は...	**1**

〔CloudWatch.3] MFA を使用しない マネジメントコンソールサインインのログメトリクスフィルターとアラームが存在することを確認する

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.2

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ:
AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的

パラメータ: なし

CloudTrail ログを Logs に送信し、対応するメトリクスフィルターとアラームを確立することで、API CloudWatch コールをリアルタイムでモニタリングできます。

CIS では、MFA で保護されていないコンソールログインに対するメトリクスフィルターとアラームを作成することを推奨しています。単一要素のコンソールログインをモニタリングすることにより、MFA によって保護されていないアカウントへの可視性が向上します。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.2 のコントロール 3.2 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 証跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
> チェックの結果、以下の場合は結果 FAILED となります。
>
> - 追跡が設定されていません。
> - 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。
>
> チェックの結果、以下の場合はコントロール状況が NO_DATA になります。
>
> - マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
> - マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任された管理者アカウントでのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは `NO_DATA` になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、`ListSubscriptionsByTopic` を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての に適用される CloudTrail 証跡を作成します AWS リージョン。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 証跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon ユーザーガイド」の「ロググループのメトリクスフィルターを作成する」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") && ($.userIdentity.type = "IAMUser") && ($.responseElements.ConsoleLogin = "Success") }`
メトリクス名前空間	**LogMetrics**
メトリクス値	**1**
デフォルト値	**0**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon ユーザーガイド」の「ロググループメトリクスフィルターに基づく CloudWatch アラームの作成」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が の場合	以上
条件は...	**1**

〔CloudWatch.4] IAM ポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認する

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.4、CIS AWS Foundations Benchmark v1.4.0/4.4

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ:
AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、 CloudTrail ログを Logs に送信し、対応するメトリクスフィルターとアラームを確立することで、API CloudWatch コールをリアルタイムでモニタリングするかどうかをチェックします。

CIS では、IAM ポリシーに加えられた変更に対するメトリクスフィルターとアラームを作成することを推奨しています。これらの変更をモニタリングすることで、認証と認可の管理が損なわれないようにできます。

Note

Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 証跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
チェックの結果、以下の場合は結果 FAILED となります。

- 追跡が設定されていません。
- 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。

チェックの結果、以下の場合はコントロール状況が NO_DATA になります。

- マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任された管理者アカウントでのみ管理できます。組織の

証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは NO_DATA になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、ListSubscriptionsByTopic を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 WARNING を生成します。

修正

Note

これらの修復手順で推奨されるフィルターパターンは、CIS ガイダンスのフィルターパターンとは異なります。推奨フィルターは IAM API 呼び出しからのイベントのみを対象としています。

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての に適用される CloudTrail 証跡を作成します AWS リージョン。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 証跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon ユーザーガイド」の「ロググループのメトリクスフィルターを作成する」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventSource=iam.amazonaws.com) && (($.eventName=DeleteGroupPolicy) || ($.eventName=DeleteRolePolicy) \|\| ($.eventName=DeleteUserPolicy) || ($.eventName=PutGroupPolicy) \|\| ($.eventName=PutRolePolicy) || ($.eventName=PutUserPolicy) \|\| ($.eventName=CreatePolicy) || ($.eventName=DeletePolicy) \|\| ($.eventName=CreatePolicyVersion) || ($.eventName=DeletePolicyVersion) \|\| ($.eventName=AttachRolePolicy) || ($.eventName=DetachRolePolicy) \|\| ($.eventName=AttachUserPolicy) || ($.eventName=DetachUserPolicy) \|\| ($.eventName=AttachGroupPolicy) || ($.eventName=DetachGroupPolicy))}`
メトリクス名前空間	**LogMetrics**
メトリクス値	**1**
デフォルト値	**0**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon ユーザーガイド」の「ロググループメトリクスフィルターに基づく CloudWatch アラームの作成」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が の場合	以上
条件は...	**1**

〔CloudWatch.5] CloudTrail AWS Configログメトリクスフィルターとアラームが設定変更用に存在することを確認する

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.5、CIS AWS Foundations Benchmark v1.4.0/4.5

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的

パラメータ: なし

CloudTrail ログを Logs に送信し、対応するメトリクスフィルターとアラームを確立することで、API CloudWatch コールをリアルタイムでモニタリングできます。

CIS では、設定の変更 CloudTrailに対するメトリクスフィルターとアラームを作成することをお勧めします。これらの変更をモニタリングすることで、アカウント内のアクティビティを継続的に可視化できます。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 4.5 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

Note

Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 証跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
チェックの結果、以下の場合は結果 `FAILED` となります。

- 追跡が設定されていません。
- 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。

チェックの結果、以下の場合はコントロール状況が `NO_DATA` になります。

- マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

  組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任された管理者アカウントでのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは `NO_DATA` になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、`ListSubscriptionsByTopic` を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての に適用される CloudTrail 証跡を作成します AWS リージョン。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 証跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon ユーザーガイド」の「ログググループのメトリクスフィルターを作成する」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventName=CreateTrail) \|\| ($.eventName=UpdateTrail) || ($.eventName=DeleteTrail) \|\| ($.eventName=StartLogging) || ($.eventName=StopLogging)}`
メトリクス名前空間	**`LogMetrics`**
メトリクス値	**`1`**
デフォルト値	**`0`**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon ユーザーガイド」の「ロググループメトリクスフィルターに基づく CloudWatch アラームの作成」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が である場合	以上
条件は...	**1**

〔CloudWatch.6] AWS Management Console 認証の失敗に対してログメトリクスフィルターとアラームが存在することを確認する

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.6、CIS AWS Foundations Benchmark v1.4.0/4.6

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的

パラメータ: なし

CloudTrail ログを Logs に送信し、対応するメトリクスフィルターとアラームを確立することで、API CloudWatch コールをリアルタイムでモニタリングできます。

CIS では、コンソール認証の試行の失敗に対するメトリクスフィルターとアラームを作成することを推奨しています。コンソールログインの失敗をモニタリングすることにより、認証情報へのブルートフォース攻撃の試行の検出にかかるリードタイムを短縮できる可能性があり、ソース IP などの、他のイベント相関で使用できるインジケータが得られる可能性もあります。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 4.6 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロー

ルは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 証跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
> チェックの結果、以下の場合は結果 `FAILED` となります。
>
> - 追跡が設定されていません。
> - 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。
>
> チェックの結果、以下の場合はコントロール状況が `NO_DATA` になります。
>
> - マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
> - マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。
>
>   組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任された管理者アカウントでのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは `NO_DATA` になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。
>
> アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、`ListSubscriptionsByTopic` を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての に適用される CloudTrail 証跡を作成します AWS リージョン。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 証跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon ユーザーガイド」の「ログググループのメトリクスフィルターを作成する」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventName=ConsoleLogin) && ($.errorMessage="Failed authentication")}`
メトリクス名前空間	**`LogMetrics`**
メトリクス値	**`1`**
デフォルト値	**`0`**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon ユーザーガイド」の「ロググループメトリクスフィルターに基づく CloudWatch アラームの作成」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的

フィールド	値
your-metric-name が の場合	以上
条件は...	**1**

〔CloudWatch.7] カスタマーマネージドキーの無効化またはスケジュールされた削除のためのログメトリクスフィルターとアラームが存在することを確認する

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.7、CIS AWS Foundations Benchmark v1.4.0/4.7

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的

パラメータ: なし

CloudTrail ログを Logs に送信し、対応するメトリクスフィルターとアラームを確立することで、API CloudWatch コールをリアルタイムでモニタリングできます。

CIS では、状態が無効またはスケジュールされた削除に変更されたカスタマーマネージドキーに対するメトリクスフィルターとアラームを作成することを推奨しています。無効になっているか、または削除されたキーで暗号化されたデータには、アクセスできなくなります。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 4.7 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。`ExcludeManagementEventSources` が `kms.amazonaws.com` を含む場合も、コントロールは失敗します。

Note

Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 証跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
チェックの結果、以下の場合は結果 `FAILED` となります。

- 追跡が設定されていません。
- 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。

チェックの結果、以下の場合はコントロール状況が `NO_DATA` になります。

- マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

  組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任された管理者アカウントでのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは `NO_DATA` になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、`ListSubscriptionsByTopic` を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての に適用される CloudTrail 証跡を作成します AWS リージョン。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 証跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon ユーザーガイド」の「ログググループのメトリクスフィルターを作成する」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventSource=kms.amazonaws.com) && (($.eventName=DisableKey) || ($.eventName=ScheduleKeyDeletion))}`
メトリクス名前空間	**`LogMetrics`**
メトリクス値	**`1`**
デフォルト値	**`0`**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon ユーザーガイド」の「ロググループメトリクスフィルターに基づく CloudWatch アラームの作成」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的

フィールド	値
your-metric-name が の場合	以上
条件は...	**1**

〔CloudWatch.8] S3 バケットポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認する

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.8、CIS AWS Foundations Benchmark v1.4.0/4.8

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的

パラメータ: なし

CloudTrail ログを Logs に送信し、対応するメトリクスフィルターとアラームを確立することで、API CloudWatch コールをリアルタイムでモニタリングできます。

CIS では、S3 バケットポリシーの変更に対するメトリクスフィルターとアラームを作成することを推奨しています。これらの変更をモニタリングすることで、機密性の高い S3 バケットの過剰な権限のあるポリシーを検出して修正するまでの時間を短縮できます。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 4.8 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

Note

Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 証跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
チェックの結果、以下の場合は結果 FAILED となります。

- 追跡が設定されていません。
- 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。

チェックの結果、以下の場合はコントロール状況が NO_DATA になります。

- マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

  組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任された管理者アカウントでのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは NO_DATA になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、ListSubscriptionsByTopic を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 WARNING を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての に適用される CloudTrail 証跡を作成します AWS リージョン。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 証跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon ユーザーガイド」の「ログググループのメトリクスフィルターを作成する」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventSource=s3.amazonaws.com) && (($.eventName=PutBucketAcl) || ($.eventName=PutBucketPolicy) \|\| ($.eventName=PutBucketCors) || ($.eventName=PutBucketLifecycle) \|\| ($.eventName=PutBucketReplication) || ($.eventName=DeleteBucketPolicy) \|\| ($.eventName=DeleteBucketCors) || ($.eventName=DeleteBucketLifecycle) \|\| ($.eventName=DeleteBucketReplication))}`
メトリクス名前空間	**LogMetrics**
メトリクス値	**1**

フィールド	値
デフォルト値	**0**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon ユーザーガイド」の「ロググループメトリクスフィルターに基づく CloudWatch アラームの作成」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が であるたびに、	以上
条件は...	**1**

〔CloudWatch.9] AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.9、CIS AWS Foundations Benchmark v1.4.0/4.9

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的

パラメータ: なし

CloudTrail ログを Logs に送信し、対応するメトリクスフィルターとアラームを確立することで、API CloudWatch コールをリアルタイムでモニタリングできます。

CIS では、 AWS Config 構成設定の変更に対するメトリクスフィルターとアラームを作成することを推奨しています。これらの変更をモニタリングすることで、アカウント内の設定項目を継続的に可視化できます。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 4.9 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 証跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
> チェックの結果、以下の場合は結果 FAILED となります。
>
> - 追跡が設定されていません。
> - 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。
>
> チェックの結果、以下の場合はコントロール状況が NO_DATA になります。
>
> - マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
> - マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。
>
>   組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任された管理者アカウントでのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは NO_DATA になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。
>
> アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、ListSubscriptionsByTopic を呼び出すことで Amazon SNS トピックにアク

セスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 WARNING を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての に適用される CloudTrail 証跡を作成します AWS リージョン。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 証跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon ユーザーガイド」の「ログググループのメトリクスフィルターを作成する」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventSource=config.amazonaws.com) && (($.eventName=StopConfigurationRecorder) || ($.eventName=DeleteDeliveryChannel) \|\| ($.eventName=PutDeliveryChannel) || ($.eventName=PutConfigurationRecorder))}`
メトリクス名前空間	**`LogMetrics`**
メトリクス値	**`1`**
デフォルト値	**`0`**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon ユーザーガイド」の「ロググループメトリクスフィルターに基づく CloudWatch アラームの作成」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が の場合	以上
条件は...	**1**

〔CloudWatch.10] セキュリティグループの変更に対するログメトリクスフィルターとアラームが存在することを確認する

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.10、CIS AWS Foundations Benchmark v1.4.0/4.10

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的

パラメータ: なし

CloudTrail ログを Logs に送信し、対応するメトリクスフィルターとアラームを確立することで、API CloudWatch コールをリアルタイムでモニタリングできます。セキュリティグループは、VPC の入力トラフィックと出力トラフィックを制御するステートフルパケットフィルターです。

CIS では、セキュリティグループの変更に対するメトリクスフィルターとアラームを作成することを推奨しています。これらの変更をモニタリングすることにより、リソースやサービスが意図せずに公開されないようにできます。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 4.10 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 証跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
> チェックの結果、以下の場合は結果 FAILED となります。
>
> - 追跡が設定されていません。
> - 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。
>
> チェックの結果、以下の場合はコントロール状況が NO_DATA になります。
>
> - マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
> - マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。
>
>   組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任された管理者アカウントでのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは NO_DATA になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。
>
> アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、ListSubscriptionsByTopic を呼び出すことで Amazon SNS トピックにアク

セスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての に適用される CloudTrail 証跡を作成します AWS リージョン。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 証跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon ユーザーガイド」の「ログググループのメトリクスフィルターを作成する」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventName=AuthorizeSecurityGroupIngress) \|\| ($.eventName=AuthorizeSecurityGroupEgress) || ($.eventName=RevokeSecurityGroupIngress) \|\| ($.eventName=RevokeSecurityGroupEgress) || ($.eventName=CreateSecurityGroup) \|\| ($.eventName=DeleteSecurityGroup)}`
メトリクス名前空間	**`LogMetrics`**

フィールド	値
メトリクス値	**1**
デフォルト値	**0**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon ユーザーガイド」の「ロググループメトリクスフィルターに基づく CloudWatch アラームの作成」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が である場合	以上
条件は...	**1**

〔CloudWatch.11] ネットワークアクセスコントロールリスト (NACL) の変更に対するログメトリクスフィルターとアラームが存在することを確認する

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.11、CIS AWS Foundations Benchmark v1.4.0/4.11

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的

パラメータ: なし

CloudTrail ログを Logs に送信し、対応するメトリクスフィルターとアラームを確立することで、API CloudWatch コールをリアルタイムでモニタリングできます。NACL は、VPC 内のサブネッ

トの入力トラフィックと出力トラフィックを制御するためのステートレスパケットフィルターとして使用されます。

CIS では、NACL の変更に対するメトリクスフィルターとアラームを作成することを推奨しています。これらの変更をモニタリングすることで、 AWS リソースやサービスが意図せずに公開されないようにすることができます。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 4.11 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 証跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
> チェックの結果、以下の場合は結果 `FAILED` となります。
>
> - 追跡が設定されていません。
> - 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。
>
> チェックの結果、以下の場合はコントロール状況が `NO_DATA` になります。
>
> - マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
> - マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。
>
> 組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任された管理者アカウントでのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは `NO_DATA` になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者の

アカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、`ListSubscriptionsByTopic` を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての に適用される CloudTrail 証跡を作成します AWS リージョン。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 証跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon ユーザーガイド」の「ロググループのメトリクスフィルターを作成する」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventName=CreateNetworkAcl) \|\| ($.eventName=CreateNetworkAclEntry) || ($.eventName=DeleteNetworkAcl) \|\| ($.eventName=DeleteNetworkAclEntry) || ($.eventName=ReplaceNetworkAclEntry) \|\| ($.eventN`

フィールド	値
	ame=ReplaceNetworkAclAssoci ation)}
メトリクス名前空間	**LogMetrics**
メトリクス値	**1**
デフォルト値	**0**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon ユーザーガイド」の「ロググループメトリクスフィルターに基づく CloudWatch アラームの作成」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が である場合	以上
条件は...	**1**

〔CloudWatch.12] ネットワークゲートウェイの変更に対するログメトリクスフィルターとアラームが存在することを確認する

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.12、CIS AWS Foundations Benchmark v1.4.0/4.12

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的

パラメータ: なし

CloudTrail ログを Logs に送信し、対応するメトリクスフィルターとアラームを確立することで、API CloudWatch コールをリアルタイムでモニタリングできます。ネットワークゲートウェイは、VPC の外部にある送信先との間でトラフィックを送受信する必要があります。

CIS では、ネットワークゲートウェイの変更に対するメトリクスフィルターとアラームを作成することを推奨しています。これらの変更をモニタリングすることにより、すべての入力トラフィックと出力トラフィックが制御されたパスを通じて VPC 境界を通過するようになります。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.2 のコントロール 4.12 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 証跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
> チェックの結果、以下の場合は結果 `FAILED` となります。
>
> - 追跡が設定されていません。
> - 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。
>
> チェックの結果、以下の場合はコントロール状況が `NO_DATA` になります。
>
> - マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
> - マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。
>
> 組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任された管理者アカウントでのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは `NO_DATA` になります。メンバーアカウントでは、Security Hub はメンバー所有のリ

ソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、`ListSubscriptionsByTopic` を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての に適用される CloudTrail 証跡を作成します AWS リージョン。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 証跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon ユーザーガイド」の「ログググループのメトリクスフィルターを作成する」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventName=CreateCustomerGateway) \|\| ($.eventName=DeleteCustomerGateway) || ($.eventName=AttachInternetGateway) \|\| ($.eventName=CreateInternetGateway) || ($.eventName=Delet`

フィールド	値
	eInternetGateway) || ($.eventName=DetachInternetGateway)}
メトリクス名前空間	**LogMetrics**
メトリクス値	**1**
デフォルト値	**0**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon ユーザーガイド」の「ロググループメトリクスフィルターに基づく CloudWatch アラームの作成」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が である場合	以上
条件は...	**1**

〔CloudWatch.13] ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認する

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.13、CIS AWS Foundations Benchmark v1.4.0/4.13

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、 CloudTrail ログを Logs に送信し、対応するメトリクスフィルターとアラームを確立することで、API CloudWatch コールをリアルタイムでモニタリングするかどうかをチェックします。ルーティングテーブルは、サブネット間およびネットワークゲートウェイへのネットワークトラフィックをルーティングします。

CIS では、ルートテーブルの変更に対するメトリクスフィルターとアラームを作成することを推奨しています。これらの変更をモニタリングすることで、すべての VPC トラフィックが確実に想定どおりのパスを通過するようにできます。

Note

Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 証跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
チェックの結果、以下の場合は結果 `FAILED` となります。

- 追跡が設定されていません。
- 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。

チェックの結果、以下の場合はコントロール状況が `NO_DATA` になります。

- マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

  組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任された管理者アカウントでのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは `NO_DATA` になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、`ListSubscriptionsByTopic` を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

> **Note**
>
> これらの修復手順で推奨されるフィルターパターンは、CIS ガイダンスのフィルターパターンとは異なります。推奨フィルターは Amazon Elastic Compute Cloud (EC2) 呼び出しからのイベントのみを対象としています。

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての に適用される CloudTrail 証跡を作成します AWS リージョン。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 証跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon ユーザーガイド」の「ロググループのメトリクスフィルターを作成する」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventSource=ec2.amazonaws.com) && (($.eventName=CreateRoute) || ($.eventName=Creat`

フィールド	値
	`eRouteTable) || ($.eventN ame=ReplaceRoute) \|\| ($.eventN ame=ReplaceRouteTableAssoci ation) || ($.eventName=Delet eRouteTable) \|\| ($.eventN ame=DeleteRoute) || ($.eventN ame=DisassociateRouteTable))}`
メトリクス名前空間	**`LogMetrics`**
メトリクス値	**`1`**
デフォルト値	**`0`**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon ユーザーガイド」の「ロググループメトリクスフィルターに基づく CloudWatch アラームの作成」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
`your-metric-name` が である場合	以上
条件は...	**`1`**

〔CloudWatch.14] VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認する

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.14、CIS AWS Foundations Benchmark v1.4.0/4.14

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ:
AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的

パラメータ: なし

CloudTrail ログを Logs に送信し、対応するメトリクスフィルターとアラームを確立することで、API CloudWatch コールをリアルタイムでモニタリングできます。1 つのアカウントに複数の VPC を含めることができるのに加えて、2 つの VPC 間にピア接続を作成し、ネットワークトラフィックを VPC 間でルーティングすることができます。

CIS では、VPC の変更に対するメトリクスフィルターとアラームを作成することを推奨しています。これらの変更をモニタリングすることで、認証と認可の管理が損なわれないようにできます。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 4.14 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 証跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
> チェックの結果、以下の場合は結果 FAILED となります。
>
> - 追跡が設定されていません。
> - 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。
>
> チェックの結果、以下の場合はコントロール状況が NO_DATA になります。
>
> - マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。

- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

  組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任された管理者アカウントでのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは `NO_DATA` になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、`ListSubscriptionsByTopic` を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての に適用される CloudTrail 証跡を作成します AWS リージョン。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 証跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon ユーザーガイド」の「ロググループのメトリクスフィルターを作成する」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventName=CreateVpc) \|\| ($.eventName=DeleteVpc) || ($.eventName=ModifyVpcAttribute) \|\| ($.eventName=AcceptVpcPeeringConnection) || ($.eventName=CreateVpcPeeringConnection) \|\| ($.eventName=DeleteVpcPeeringConnection) || ($.eventName=RejectVpcPeeringConnection) \|\| ($.eventName=AttachClassicLinkVpc) || ($.eventName=DetachClassicLinkVpc) \|\| ($.eventName=DisableVpcClassicLink) || ($.eventName=EnableVpcClassicLink)}`
メトリクス名前空間	**LogMetrics**
メトリクス値	**1**
デフォルト値	**0**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon ユーザーガイド」の「ロググループメトリクスフィルターに基づく CloudWatch アラームの作成」を参照してください。 CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が の場合	以上
条件は...	**1**

〔CloudWatch.15] CloudWatch アラームには、指定されたアクションが設定されている必要があります

カテゴリ: 検出 > 検出サービス

関連する要件: NIST.800-53.r5 AU-6(1)、NIST.800-53.r5 AU-6(5)、NIST.800-53.r5 CA-7、NIST.800-53.r5 IR-4(1)、NIST.800-53.r5 IR-4(5)、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-20、NIST.800-53.r5 SI-4(12)、NIST.800-53.r5 SI-4(5)

重要度: 高

リソースタイプ: `AWS::CloudWatch::Alarm`

AWS Config ルール： `cloudwatch-alarm-action-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`alarmActionRequired`	パラメータが `true` に設定されていて、アラームの状態が ALARM に変わるとアラームがアクションを起こす場合に、コントロールが PASSED 検出結果を生成します。	ブール値	カスタマイズ不可	`true`
`insufficientDataActionRequired`	パラメータが `true` に設定されていて、アラームの状態が INSUFFICIENT_DATA に変わるとアラームがアクションを起こす場合に、コントロールが PASSED 検出結果を生成します。	ブール値	`true` 、、または `false`	`false`
`okActionRequired`	パラメータが `true` に設定されていて、アラームの状態が	ブール値	`true` 、、または `false`	`false`

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	OK に変わるとアラームがアクションを起こす場合に、コントロールが PASSED 検出結果を生成します。			

このコントロールは、Amazon CloudWatch アラームに ALARM状態に設定されたアクションが少なくとも 1 つあるかどうかをチェックします。ALARM 状態に対して設定されたアクションがアラームにない場合、コントロールは失敗します。必要に応じて、カスタムパラメータ値を含めて、INSUFFICIENT_DATA 状態または OK 状態のアラームアクションを要求することもできます。

> **Note**
>
> Security Hub は、 CloudWatch メトリクスアラームに基づいてこのコントロールを評価します。メトリクスアラームは、指定されたアクションが設定された複合アラームの一部である場合があります。コントロールは、次の場合にFAILED結果を生成します。
>
> - 指定されたアクションは、メトリクスアラーム用に設定されていません。
> - メトリクスアラームは、指定されたアクションが設定された複合アラームの一部です。

このコントロールは、 CloudWatch アラームにアラームアクションが設定されているかどうかに重点を置き、CloudWatch.17 は CloudWatch アラームアクションのアクティベーションステータスに重点を置いています。

CloudWatch アラームアクションを使用して、モニタリング対象のメトリクスが定義されたしきい値を超過したときに自動的にアラートを受け取ることをお勧めします。アラームをモニタリングすることで、異常なアクティビティを特定し、アラームが特定の状態になったときのセキュリティや運用上の問題に迅速に対応できます。アラームアクションの最も一般的なタイプは、Amazon Simple Notification Service (Amazon SNS) トピックにメッセージを送信して、1 人または複数のユーザーに通知することです。

修正

CloudWatch アラームでサポートされるアクションの詳細については、「Amazon ユーザーガイド」の「アラームアクション」を参照してください。 CloudWatch

〔CloudWatch.16] CloudWatch ロググループは、指定された期間保持する必要があります

カテゴリ: 識別 > ログ記録

関連する要件: NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-11、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-12

重要度: 中

リソースタイプ: `AWS::Logs::LogGroup`

AWS Config ルール： `cw-loggroup-retention-period-check`

スケジュールタイプ: 定期的

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値	
`minRetentionTime`	CloudWatch ロググループの最小保持期間	列挙型	`365, 400, 545, 731, 1827, 3653`	`365`	

このコントロールは、Amazon CloudWatch ロググループに少なくとも指定された日数の保持期間があるかどうかをチェックします。保持期間が指定された日数未満の場合、コントロールは失敗します。保持期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 365 日を使用します。

CloudWatch ログは、すべてのシステム、アプリケーション、および からのログを、高度にスケーラブルな単一のサービス AWS のサービス に一元化します。 CloudWatch Logs を使用して、Amazon Elastic Compute Cloud (EC2) インスタンス、Amazon Route 53 AWS CloudTrail、およびその他のソースからログファイルをモニタリング、保存、およびアクセスできます。ログを少なくとも 1 年間保存することで、ログ保持標準への準拠に役立ちます。

修正

ログ保持設定を構成するには、「Amazon CloudWatch ユーザーガイド」の CloudWatch 「ログのログデータ保持の変更」を参照してください。

〔CloudWatch.17] CloudWatch アラームアクションを有効にする必要があります

カテゴリ: 検出 > 検出サービス

関連する要件: NIST.800-53.r5 AU-6(1)、NIST.800-53.r5 AU-6(5)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-4(12)

重要度: 高

リソースタイプ: `AWS::CloudWatch::Alarm`

AWS Config ルール： `cloudwatch-alarm-action-enabled-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 CloudWatch アラームアクションが有効になっているかどうかをチェックします (`ActionEnabled`true に設定する必要があります)。アラームの CloudWatch アラームアクションが非アクティブ化されると、コントロールは失敗します。

> **Note**
>
> Security Hub は、 CloudWatch メトリクスアラームに基づいてこのコントロールを評価します。メトリクスアラームは、アラームアクションが有効になっている複合アラームの一部である場合があります。コントロールは、次の場合に`FAILED`結果を生成します。
>
> - 指定されたアクションは、メトリクスアラーム用に設定されていません。
> - メトリクスアラームは、アラームアクションが有効になっている複合アラームの一部です。

このコントロールは CloudWatch アラームアクションのアクティベーションステータスに焦点を当て、CloudWatch.15 は CloudWatch アラームでALARMアクションが設定されているかどうかに焦点を当てます。

アラームアクションは、モニタリング対象のメトリクスが定義されたしきい値を超えると自動的に警告します。アラームアクションが非アクティブ化されている場合、アラームの状態が変わってもアクションは実行されず、モニタリング対象メトリクスの変更に関する警告は表示されません。セキュリティや運用上の問題に迅速に対応できるように、 CloudWatch アラームアクションをアクティブ化することをお勧めします。

修正

CloudWatch アラームアクションを有効にするには (コンソール)

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。
2. ナビゲーションペインの [アラーム] で、[すべてのアラーム] を選択します。
3. アクションをアクティブにするアラームを選択します。
4. [アクション] で、[アラームアクション — 新規] を選択し、[有効化] を選択します。

CloudWatch アラームアクションのアクティブ化の詳細については、「Amazon ユーザーガイド」の「アラームアクション」を参照してください。 CloudWatch

AWS CodeArtifact コントロール

これらのコントロールは CodeArtifact リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::CodeArtifact::Repository`

AWS Config ルール: `tagged-codeartifact-repository` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、 AWS CodeArtifact リポジトリにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。リポジトリにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、リポジトリにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

CodeArtifact リポジトリにタグを追加するには、「 ユーザーガイド」の「 でリポジトリにタグ CodeArtifactAWS CodeArtifact を付ける」を参照してください。

AWS CodeBuild コントロール

これらのコントロールは CodeBuild リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください

関連する要件: PCI DSS v3.2.1/8.2.1、NIST.800-53.r5 SA-3

カテゴリ: 保護 > セキュアな開発

重要度: 非常事態

リソースタイプ: `AWS::CodeBuild::Project`

AWS Config ルール : `codebuild-project-source-repo-url-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS CodeBuild プロジェクトの Bitbucket ソースリポジトリ URL に個人用アクセストークンまたはユーザー名とパスワードが含まれているかどうかをチェックします。Bitbucket ソースリポジトリ URL に個人用アクセストークンまたはユーザー名とパスワードが含まれている場合、コントロールは失敗します。

> **Note**
>
> このコントロールは、 CodeBuild ビルドプロジェクトのプライマリソースとセカンダリソースの両方を評価します。プロジェクトソースの詳細については、「 AWS CodeBuild ユーザーガイド」の「複数の入力ソースと出力アーティファクトのサンプル」を参照してください。

サインイン認証情報は、クリアテキストで保存または送信したり、ソースリポジトリ URL に表示されたりしないでください。個人用のアクセストークンやサインイン認証情報の代わりに、 のソースプロバイダーにアクセスし CodeBuild、Bitbucket リポジトリの場所へのパスのみを含むようにソースリポジトリ URL を変更する必要があります。個人アクセストークンまたはサインイン認証情報を使用すると、意図しないデータ漏えいや不正アクセスにつながる可能性があります。

修正

OAuth を使用するように CodeBuild プロジェクトを更新できます。

CodeBuild プロジェクトソースから基本認証/ (GitHub) Personal Access Token を削除するには

1. https://console.aws.amazon.com/codebuild/ で CodeBuild コンソールを開きます。
2. 個人用のアクセストークンまたはユーザー名とパスワードを含むビルドプロジェクトを選択します。
3. [Edit] (編集) から、[Source] (ソース) を選択します。
4. GitHub / Bitbucket から切断を選択します。
5. OAuth を使用して接続 を選択し、/ Bitbucket に接続 GitHub を選択します。
6. プロンプトが表示されたら、[authorize as appropriate] (必要に応じて認可)を選択します。
7. 必要に応じて、[Repository URL] (リポジトリ URL) と [additional configuration] (追加の設定) を再設定します。
8. [Update source] (ソースの更新) を選択します。

詳細については、「 ユーザーガイド」のCodeBuild 「ユースケースベースのサンプルAWS CodeBuild 」を参照してください。

〔CodeBuild.2] CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください

関連する要件: PCI DSS v3.2.1/8.2.1、NIST.800-53.r5 IA-5(7)、NIST.800-53.r5 SA-3

カテゴリ: 保護 > セキュアな開発

重要度: 非常事態

リソースタイプ: `AWS::CodeBuild::Project`

AWS Config ルール : `codebuild-project-envvar-awscred-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、プロジェクトに環境変数 AWS_ACCESS_KEY_ID と AWS_SECRET_ACCESS_KEY が含まれているかどうかをチェックします。

認証情報 AWS_ACCESS_KEY_ID および AWS_SECRET_ACCESS_KEY はクリアテキストで保存しないでください。これは、意図しないデータ漏えいや不正アクセスに認証情報が公開される可能性があるためです。

修正

CodeBuild プロジェクトから環境変数を削除するには、「 AWS CodeBuild ユーザーガイド」の「 でビルドプロジェクトの設定を変更する AWS CodeBuild」を参照してください。[環境変数] に何も選択されていないことを確認します。

機密性の高い値を持つ環境変数を AWS Systems Manager Parameter Store または に保存し AWS Secrets Manager 、ビルド仕様から取得できます。手順については、「AWS CodeBuild ユーザーガイド」の「環境」セクションで、「重要」ラベルの付いたボックスを参照してください。

〔CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 低

リソースタイプ: AWS::CodeBuild::Project

AWS Config ルール : codebuild-project-s3-logs-encrypted

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS CodeBuild プロジェクトの Amazon S3 ログが暗号化されているかどうかを確認します。 CodeBuild プロジェクトの S3 ログの暗号化が非アクティブ化されると、コントロールは失敗します。

保管中のデータの暗号化は、データ周辺にアクセス管理のレイヤーを追加するために推奨されるベストプラクティスです。保管中のログを暗号化すると、 によって認証されていないユーザーがディス

クに保存されているデータにアクセスするリスクが軽減 AWS されます。権限のないユーザーがデータにアクセスできる能力を制限するための一連のアクセスコントロールが追加されます。

修正

CodeBuild プロジェクト S3 ログの暗号化設定を変更するには、「 AWS CodeBuild ユーザーガイド」の「 でビルドプロジェクトの設定を変更する AWS CodeBuild」を参照してください。

〔CodeBuild.4] CodeBuild プロジェクト環境にはログ記録 AWS Config設定が必要です

関連する要件: NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 AU-9(7)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::CodeBuild::Project`

AWS Config ルール : `codebuild-project-logging-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 CodeBuild プロジェクト環境に S3 または ログに対して少なくとも 1 つの CloudWatch ログオプションが有効になっているかどうかをチェックします。 CodeBuild プロジェクト環境で少なくとも 1 つのログオプションが有効になっていない場合、このコントロールは失敗します。

セキュリティの観点から、ログ記録はセキュリティインシデントが発生した場合に、将来的に証拠の取り組みを可能にするために重要な機能です。 CodeBuild プロジェクトの異常を脅威検出と相関させることで、それらの脅威検出の精度に対する信頼を高めることができます。

修正

CodeBuild プロジェクトログの設定方法の詳細については、 CodeBuild ユーザーガイドの「ビルドプロジェクトの作成 (コンソール) 」を参照してください。

〔CodeBuild.5] CodeBuild プロジェクト環境では特権モードを有効にしないでください

> **Important**
>
> Security Hub は 2024 年 4 月にこのコントロールを廃止しました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(10)、NIST.800-53.r5 AC-6(2)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 高

リソースタイプ: `AWS::CodeBuild::Project`

AWS Config ルール : `codebuild-project-environment-privileged-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS CodeBuild プロジェクト環境の特権モードが有効か無効かをチェックします。 CodeBuild プロジェクト環境で特権モードが有効になっている場合、コントロールは失敗します。

デフォルトでは、Docker コンテナはどのデバイスにもアクセスを許可できません。権限モードは、ビルドプロジェクトの Docker コンテナにすべてのデバイスへのアクセスを許可します。Docker コンテナ内で Docker デーモンの実行を許可するには、`privilegedMode` に `true` の値を設定します。Docker デーモンは、Docker API リクエストをリッスンし、イメージ、コンテナ、ネットワーク、ボリュームなどの Docker オブジェクトを管理します。このパラメータは、ビルドプロジェクトを使用して Docker イメージをビルドする場合にのみ、true に設定する必要があります。それ以外の場合、Docker API およびコンテナの基盤となるハードウェアへの意図しないアクセスを防ぐため、この設定を無効にする必要があります。`privilegedMode` を `false` に設定すると、重要なリソースを改ざんや削除から保護するのに役立ちます。

修正

CodeBuild プロジェクト環境設定を構成するには、「 CodeBuild ユーザーガイド」の「ビルドプロジェクトの作成 (コンソール) 」を参照してください。[環境] セクションでは、[特権付与] 設定を選択しないでください。

AWS Config コントロール

これらのコントロールは AWS Config リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Config.1] AWS Config を有効にし、サービスにリンクされたロールをリソース記録に使用する必要があります

関連する要件： CIS AWS Foundations Benchmark v1.2.0/2.5、CIS AWS Foundations Benchmark v1.4.0/3.5、CIS AWS Foundations Benchmark v3.0.0/3.3、NIST.800-53.r5 CM-3、NIST.800-53.r5 CM-6(1)、NIST.800-53.r5 CM-8、NIST.800-53.r5 CM-8(2)、PCI DSS v3.2.1/10.5.2、PCI DSS v3.2.1/1.5

カテゴリ: 識別 > インベントリ

重要度: 中

リソースタイプ: `AWS::::Account`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的

パラメータ: なし

このコントロール AWS Config は、現在の のアカウントで が有効になっているかどうかを確認し AWS リージョン、現在のリージョンで有効になっているコントロールに対応するすべてのリソースを記録し、サービスにリンクされた AWS Config ロール を使用します。サービスにリンクされたロールを使用しない場合、他のロールには がリソースを正確に記録するために必要なアクセス許可がないため、コントロール AWS Config は失敗します。

この AWS Config サービスは、アカウントでサポートされている AWS リソースの設定管理を実行し、ログファイルを配信します。記録された情報には、設定項目 (AWS リソース) 、設定項目間の

関係、およびリソース内の設定変更が含まれます。グローバルリソースは、どのリージョンでも利用できるリソースです。

コントロールは次のように評価されます。

- 現在のリージョンが集約リージョン として設定されている場合、コントロールは AWS Identity and Access Management (IAM) グローバルリソースが記録されているPASSED場合にのみ結果を生成します (それらを必要とするコントロールを有効にしている場合) 。
- 現在のリージョンがリンクされたリージョンとして設定されている場合、コントロールは IAM グローバルリソースが記録されているかどうかを評価しません。
- 現在のリージョンがアグリゲータにない場合、またはクロスリージョン集約がアカウントで設定されていない場合、コントロールは IAM グローバルリソースが記録されている場合にのみPASSED結果を生成します (それらを必要とするコントロールを有効にしている場合) 。

コントロールの結果は、 でリソースの状態の変化を毎日記録するか継続的に記録するかによって影響を受けません AWS Config。ただし、新しいコントロールの自動有効化を設定している場合、または新しいコントロールを自動的に有効にする中央設定ポリシーがある場合、新しいコントロールがリリースされると、このコントロールの結果が変わる可能性があります。このような場合、すべてのリソースを記録しない場合は、新しいコントロールに関連付けられているリソースの記録を設定して、PASSED結果を受け取る必要があります。

Security Hub のセキュリティチェックは、すべてのリージョン AWS Config で を有効にし、それを必要とするコントロールのリソース記録を設定する場合にのみ、意図したとおりに機能します。

> **Note**
>
> Config.1 では AWS Config 、Security Hub を使用するすべてのリージョンで が有効になっている必要があります。
> Security Hub はリージョンサービスであるため、このコントロールに対して実行されるチェックでは、アカウントの現在のリージョンのみが評価されます。
> リージョン内の IAM グローバルリソースに対するセキュリティチェックを許可するには、そのリージョン内の IAM グローバルリソースを記録する必要があります。IAM グローバルリソースが記録されていないリージョンには、IAM グローバルリソースをチェックするコントロールのデフォルトのPASSED結果が表示されます。IAM グローバルリソースは 間で同じであるため AWS リージョン、IAM グローバルリソースはホームリージョンでのみ記録することをお勧めします (クロスリージョン集約がアカウントで有効になっている場合) 。IAM リソースは、グローバルリソース記録が有効になっているリージョンでのみ記録されます。

AWS Config がサポートするグローバルに記録された IAM リソースタイプは、IAM ユーザー、グループ、ロール、カスタマー管理ポリシーです。グローバルリソースの記録がオフになっているリージョンでは、これらのリソースタイプをチェックする Security Hub コントロールを無効にすることをお勧めします。詳細については、「無効にする可能性のある Security Hub コントロール」を参照してください。

修正

コントロールごとに記録する必要があるリソースのリストについては、「」を参照してくださいAWS Config コントロールの検出結果を生成するために必要な リソース。

アグリゲータの一部ではないホームリージョンおよびリージョンで、現在のリージョンで有効になっているコントロールに必要なすべてのリソースを記録します。これには、IAM グローバルリソースを必要とするコントロールを有効にしている場合、IAM グローバルリソースが含まれます。

リンクされたリージョンでは、現在のリージョンで有効になっているコントロールに対応するすべてのリソース AWS Config を記録する限り、任意の記録モードを使用できます。リンクされたリージョンで、IAM グローバルリソースの記録を必要とするコントロールが有効になっている場合、FAILED検出結果を受け取ることはできません (他のリソースの記録で十分です) 。

リソースを記録するように有効に AWS Config して設定するには、「 AWS Config デベロッパーガイドAWS Config 」の「コンソールでのセットアップ」を参照してください。テンプレートを使用してこのプロセス AWS CloudFormation を自動化することもできます。詳細については、「 ユーザーガイド」のAWS CloudFormation StackSets 「サンプルテンプレートAWS CloudFormation 」を参照してください。

Amazon Data Firehose コントロール

これらのコントロールは Amazon Data Firehose リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります

関連する要件： NIST.800-53.r5 AC-3、NIST.800-53.r5 AU-3、NIST.800-53.r5 SC-12、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::KinesisFirehose::DeliveryStream`

AWS Config ルール: `kinesis-firehose-delivery-stream-encrypted`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Amazon Data Firehose 配信ストリームが保管時にサーバー側の暗号化で暗号化されているかどうかをチェックします。Firehose 配信ストリームがサーバー側の暗号化で保管中に暗号化されていない場合、このコントロールは失敗します。

サーバー側の暗号化は、Amazon Data Firehose 配信ストリームの機能で、 AWS Key Management Service () で作成されたキーを使用して、保管中のデータを自動的に暗号化しますAWS KMS。データは Data Firehose ストリームストレージレイヤーに書き込まれる前に暗号化され、ストレージから取得された後に復号されます。これにより、規制要件に準拠し、データのセキュリティを強化できます。

修正

Firehose 配信ストリームでサーバー側の暗号化を有効にするには、「Amazon Data Firehose デベロッパーガイド」の「Amazon Data Firehoseでのデータ保護」を参照してください。

Amazon Detective コントロール

これらのコントロールは Detective リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Detective.1] Detective の動作グラフにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::Detective::Graph`

AWS Config ルール: `tagged-detective-graph` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、Amazon Detective 動作グラフに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。動作グラフにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、動作グラフにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Detective 動作グラフにタグを追加するには、「Amazon Detective 管理ガイド」の「動作グラフにタグを追加する」を参照してください。

AWS Database Migration Service コントロール

これらのコントロールは AWS DMS リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.6、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 非常事態

リソースタイプ: `AWS::DMS::ReplicationInstance`

AWS Config ルール: `dms-replication-not-public`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、 AWS DMS レプリケーションインスタンスがパブリックかどうかをチェックします。これを行うために、`PubliclyAccessible` フィールドの値を調査します。

プライベートレプリケーションインスタンスには、レプリケーションネットワーク外からアクセスできないプライベート IP アドレスがあります。ソースデータベースとターゲットデータベースが同じネットワーク内にある場合、レプリケーションインスタンスにはプライベート IP アドレスが必要です。ネットワークは、VPN、または VPC ピアリングを使用して AWS Direct Connectレプリケーション インスタンスの VPC にも接続する必要があります。パブリックおよびプライベートレプリ

ケーションインスタンスの詳細については、「AWS Database Migration Service ユーザーガイド」の「パブリックおよびプライベートレプリケーションインスタンス」を参照してください。

また、 AWS DMS インスタンス設定へのアクセスが許可されたユーザーのみに制限されていることを確認する必要があります。これを行うには、ユーザーの IAM アクセス許可を制限して、 AWS DMS 設定とリソースを変更します。

修正

DMS レプリケーションインスタンスのパブリックアクセス設定は、作成後に変更できません。パブリックアクセス設定を変更するには、現在のインスタンスを削除してから再作成します。[パブリックアクセス可能] オプションは選択しないでください。

[DMS.2] DMS 証明書にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::DMS::Certificate`

AWS Config ルール: `tagged-dms-certificate` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS DMS 証明書にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。証明書にタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータ

が指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、証明書にキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

DMS 証明書にタグを追加するには、「 AWS Database Migration Service ユーザーガイド」の「 でのリソースのタグ付け AWS Database Migration Service」を参照してください。

[DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: AWS::DMS::EventSubscription

AWS Config ルール: tagged-dms-eventsubscription (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS DMS イベントサブスクリプションにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。イベントサブスクリプションにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、イベントサブスクリプションにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

DMS イベントサブスクリプションにタグを追加するには、「 AWS Database Migration Service ユーザーガイド」の「 でのリソースのタグ付け AWS Database Migration Service」を参照してください。

[DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::DMS::ReplicationInstance`

AWS Config ルール: `tagged-dms-replicationinstance` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS DMS レプリケーションインスタンスにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。レプリケーションインスタンスにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、レプリケーションインスタンスにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの

識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

DMS レプリケーションインスタンスにタグを追加するには、 AWS Database Migration Service ユーザーガイドの「 でのリソースのタグ付け AWS Database Migration Service」を参照してください。

[DMS.5] DMS レプリケーションサブネットグループにタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::DMS::ReplicationSubnetGroup`

AWS Config ルール: `tagged-dms-replicationsubnetgroup` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS DMS レプリケーションサブネットグループに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。レプリケーションサブネットグループにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、レプリケーションサブネットグループにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

DMS レプリケーションサブネットグループにタグを追加するには、「 AWS Database Migration Service ユーザーガイド」の「 でのリソースのタグ付け AWS Database Migration Service」を参照してください。

[DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。

関連する要件: NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 中

リソースタイプ: `AWS::DMS::ReplicationInstance`

AWS Config ルール : `dms-auto-minor-version-upgrade-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS DMS レプリケーションインスタンスで自動マイナーバージョンアップグレードが有効になっているかどうかを確認します。このコントロールは、DMS レプリケーションインスタンスのマイナーバージョンの自動アップグレードが有効になっているかどうかを確認します。

DMS では、サポートされている各レプリケーションエンジンへのマイナーバージョン自動アップグレードが提供されるため、レプリケーションインスタンス を維持できます up-to-date。マイナーバージョンには、ソフトウェアの新機能、バグ修正、セキュリティパッチ、およびパフォーマンスの向上を含む可能性があります。DMS レプリケーションインスタンスでマイナーバージョン自動アップグレードを有効にすると、マイナーアップグレードはメンテナンス期間中に自動的に適用され、[変更を今すぐ適用] オプションが選択されている場合はすぐに適用されます。

修正

DMS レプリケーションインスタンスのマイナーバージョン自動アップグレードを有効にするには、「AWS Database Migration Service ユーザーガイド」の「レプリケーションインスタンスの変更」を参照してください。

[DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。

関連する要件: NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::DMS::ReplicationTask`

AWS Config ルール : `dms-replication-task-targetdb-logging`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、DMS レプリケーションタスク `TARGET_APPLY` および `TARGET_LOAD` の `LOGGER_SEVERITY_DEFAULT` の最小重要度レベルでログ記録が有効になっているかどうかを確認します。これらのタスクでロギングが有効になっていない場合や、最小重大度レベルが `LOGGER_SEVERITY_DEFAULT` よりも低い場合、コントロールは失敗します。

DMS は、移行プロセス中に Amazon CloudWatch を使用して情報をログに記録します。ロギングタスク設定を使用して、ログ記録するコンポーネントアクティビティとログに記録する情報量を指定できます。次のタスクにはロギングを指定する必要があります。

- `TARGET_APPLY` - データおよびデータ定義言語 (DDL) ステートメントがターゲットデータベースに適用されます。
- `TARGET_LOAD` — データはターゲットデータベースにロードされます。

ロギングは、モニタリング、トラブルシューティング、監査、パフォーマンス分析、エラー検出、リカバリのほか、履歴分析やレポート作成を可能にするため、DMS のレプリケーションタスクにおいて重要な役割を果たします。これにより、データの整合性と規制要件の遵守を維持しながら、データベース間のデータレプリケーションを正常に行うことができます。これらのコンポーネントでは、トラブルシューティング時に `DEFAULT` 以外のログレベルが必要になることは、ほぼありません。 AWS Supportにより特に変更の要求がない限り、これらのコンポーネントには `DEFAULT` と同

じログレベルを維持するようにしてください。DEFAULT の最低限のロギングレベルでは、情報メッセージ、警告、エラーメッセージが確実にログに書き込まれます。このコントロールは、前述のレプリケーションタスクのログレベルが、LOGGER_SEVERITY_DEFAULT、LOGGER_SEVERITY_DEBUG または LOGGER_SEVERITY_DETAILED_DEBUG のいずれかのログレベルであるかどうかを確認します。

修正

ターゲットデータベースの DMS レプリケーションタスクのログ記録を有効にするには、「 AWS Database Migration Service ユーザーガイド」の AWS DMS 「タスクログの表示と管理」を参照してください。

[DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。

関連する要件: NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: AWS::DMS::ReplicationTask

AWS Config ルール : dms-replication-task-sourcedb-logging

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、DMS レプリケーションタスク SOURCE_CAPTURE および SOURCE_UNLOAD の LOGGER_SEVERITY_DEFAULT の最小重要度レベルでログ記録が有効になっているかどうかを確認します。これらのタスクでロギングが有効になっていない場合や、最小重大度レベルが LOGGER_SEVERITY_DEFAULT よりも低い場合、コントロールは失敗します。

DMS は、移行プロセス中に Amazon CloudWatch を使用して情報をログに記録します。ロギングタスク設定を使用して、ログ記録するコンポーネントアクティビティとログに記録する情報量を指定できます。次のタスクにはロギングを指定する必要があります。

- SOURCE_CAPTURE— 進行中のレプリケーションまたは変更データキャプチャ (CDC) データがソースデータベースまたはサービスからキャプチャされ、SORTER サービスコンポーネントに渡されます。
- SOURCE_UNLOAD— 全ロード中に、データがソースデータベースまたはサービスからアンロードされます。

ロギングは、モニタリング、トラブルシューティング、監査、パフォーマンス分析、エラー検出、リカバリのほか、履歴分析やレポート作成を可能にするため、DMS のレプリケーションタスクにおいて重要な役割を果たします。これにより、データの整合性と規制要件の遵守を維持しながら、データベース間のデータレプリケーションを正常に行うことができます。これらのコンポーネントでは、トラブルシューティング時に DEFAULT 以外のログレベルが必要になることは、ほぼありません。 AWS Supportにより特に変更の要求がない限り、これらのコンポーネントには DEFAULT と同じログレベルを維持するようにしてください。DEFAULT の最低限のロギングレベルでは、情報メッセージ、警告、エラーメッセージが確実にログに書き込まれます。このコントロールは、前述のレプリケーションタスクのログレベルが、LOGGER_SEVERITY_DEFAULT、LOGGER_SEVERITY_DEBUG または LOGGER_SEVERITY_DETAILED_DEBUG のいずれかのログレベルであるかどうかを確認します。

修正

ソースデータベースの DMS レプリケーションタスクのログ記録を有効にするには、「 AWS Database Migration Service ユーザーガイド」の AWS DMS 「タスクログの表示と管理」を参照してください。

[DMS.9] DMS エンドポイントは SSL を使用する必要があります。

関連する要件: NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: AWS::DMS::Endpoint

AWS Config ルール : dms-endpoint-ssl-configured

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS DMS エンドポイントが SSL 接続を使用しているかどうかをチェックします。エンドポイントが SSL を使用していない場合、コントロールは失敗します。

SSL/TLS 接続は、DMS レプリケーションインスタンスとデータベースの間の接続を暗号化することによって、セキュリティレイヤーを 1 つ提供します。証明書を使用すると、想定されるデータベースへの接続が確立されていることを検証することによって、追加のセキュリティレイヤーが提供されます。これを行うには、プロビジョニングしたすべての DB インスタンスに自動インストールされたサーバー証明書を確認します。DMS エンドポイントで SSL 接続を有効にすることで、移行中のデータの機密性を保護できます。

修正

SSL 接続を新規または既存の DMS エンドポイントに追加するには、「AWS Database Migration Service ユーザーガイド」の「AWS Database Migration Serviceでの SSL の使用」を参照してください。

[DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります

関連する要件： NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-17、NIST.800-53.r5 IA-2、NIST.800-53.r5 IA-5

カテゴリ: 保護 > セキュアなアクセス管理 > パスワードレス認証

重要度: 中

リソースタイプ: `AWS::DMS::Endpoint`

AWS Config ルール : `dms-neptune-iam-authorization-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon Neptune データベースの AWS DMS エンドポイントが IAM 認証で設定されているかどうかをチェックします。DMS エンドポイントで IAM 認証が有効になっていない場合、コントロールは失敗します。

AWS Identity and Access Management (IAM) は、 全体できめ細かなアクセスコントロールを提供します AWS。IAM では、どの のサービスやリソースにどの条件でアクセスできるかを指定できま

す。IAM ポリシーでは、ワークフォースとシステムへのアクセス許可を管理して、最小特権のアクセス許可を確保します。Neptune データベースの AWS DMS エンドポイントで IAM 認証を有効にすると、 `ServiceAccessRoleARN`パラメータで指定されたサービスロールを使用して、IAM ユーザーに認証権限を付与できます。

修正

Neptune データベースの DMS エンドポイントで IAM 認証を有効にするには、「 ユーザーガイド」の「 のターゲットとして Amazon Neptune AWS Database Migration Service AWS Database Migration Service を使用する」を参照してください。

[DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります

関連する要件： NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-6、NIST.800-53.r5 IA-2、NIST.800-53.r5 IA-5

カテゴリ: 保護 > セキュアなアクセス管理 > パスワードレス認証

重要度: 中

リソースタイプ: `AWS::DMS::Endpoint`

AWS Config ルール : `dms-mongo-db-authentication-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、MongoDB の AWS DMS エンドポイントが認証メカニズムで設定されているかどうかをチェックします。エンドポイントに認証タイプが設定されていない場合、コントロールは失敗します。

AWS Database Migration Service はMongoDB の 2 つの認証方法をサポートします。MongoDB バージョン 2.x の場合は MONGODB-CR、MongoDB バージョン 3.x 以降の場合は SCRAM-SHA-1 です。これらの認証方法は、ユーザーがパスワードを使用してデータベースにアクセスする場合に MongoDB パスワードを認証および暗号化するために使用されます。 AWS DMS エンドポイントでの認証により、承認されたユーザーのみがデータベース間で移行されるデータにアクセスして変更できるようになります。適切な認証を行わないと、権限のないユーザーは移行プロセス中に機密データにアクセスできる可能性があります。これにより、データ侵害、データ損失、またはその他のセキュリティインシデントが発生する可能性があります。

修正

MongoDB の DMS エンドポイントで認証メカニズムを有効にするには、「 ユーザーガイド」の「 のソースとして MongoDB AWS DMS AWS Database Migration Service を使用する」を参照してください。

[DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります

関連する要件： NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-13

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::DMS::Endpoint`

AWS Config ルール : `dms-redis-tls-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Redis の AWS DMS エンドポイントが TLS 接続で設定されているかどうかをチェックします。エンドポイントで TLS が有効になっていない場合、コントロールは失敗します。

TLS は、データがインターネット経由でアプリケーションまたはデータベース間で送信されるときに end-to-end セキュリティを提供します。DMS エンドポイントに SSL 暗号化を設定すると、移行プロセス中にソースデータベースとターゲットデータベース間の暗号化された通信が可能になります。これにより、悪意のある攻撃者による機密データの傍受や傍受を防ぐことができます。SSL 暗号化を使用しないと、機密データにアクセスされ、データ侵害、データ損失、またはその他のセキュリティインシデントが発生する可能性があります。

修正

Redis の DMS エンドポイントで TLS 接続を有効にするには、「 AWS Database Migration Service ユーザーガイド」の「 のターゲットとして Redis AWS Database Migration Service を使用する」を参照してください。

Amazon DocumentDB コントロール

これらのコントロールは Amazon DocumentDB リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール : `docdb-cluster-encrypted`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon DocumentDB クラスターが保管中に暗号化されているかどうかをチェックします。Amazon DocumentDB クラスターが保管中に暗号化されていない場合、コントロールは失敗します。

保管中のデータとは、永続的な不揮発性ストレージに任意の期間保管されているデータを指します。暗号化は、このようなデータの機密性を保護し、権限のないユーザーがデータにアクセスするリスクを低減するのに役立ちます。Amazon DocumentDB クラスター内のデータは、セキュリティを強化するために、保管中に暗号化する必要があります。Amazon DocumentDB は、256 ビット高度暗号化標準 (AES-256) を使用し、 AWS Key Management Service (AWS KMS) に保存されている暗号化キーを使用してデータを暗号化します。

修正

Amazon DocumentDB クラスターを作成するときに、保管中の暗号化を有効にできます。クラスターを作成した後で暗号化設定を変更することはできません。詳細については、「Amazon DocumentDB デベロッパーガイド」の「Enabling encryption at rest for an Amazon DocumentDB cluster」を参照してください。

[DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です

関連する要件: NIST.800-53.r5 SI-12

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

重要度: 中

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール : `docdb-cluster-backup-retention-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値	
`minimumBackupRetentionPeriod`	最小バックアップ保持期間 (日数)	整数	7 ~ 35	7	

このコントロールは、Amazon DocumentDB クラスターのバックアップ保持期間が指定された時間枠以上であるかどうかをチェックします。バックアップ保持期間が指定された時間枠未満の場合、コントロールは失敗します。バックアップ保持期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 7 日を使用します。

バックアップは、セキュリティインシデントからの迅速な復元と、システムの耐障害性の強化に役立ちます。Amazon DocumentDB クラスターのバックアップを自動化すると、システムを特定の時点に復元し、ダウンタイムとデータ損失を最小限に抑えることができます。Amazon DocumentDB では、クラスターのデフォルトのバックアップ保持期間は 1 日です。このコントロールを成功させるには、この値を 7 日から 35 日までの値に増やす必要があります。

修正

Amazon DocumentDB クラスターのバックアップ保持期間を変更するには、「Amazon DocumentDB デベロッパーガイド」の「Amazon DocumentDB クラスターの変更」を参照してください。[バックアップ] で、バックアップ保持期間を選択します。

[DocumentDB.3] Amazon DocumentDB 手動クラススナップショットはパブリックにできません

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 非常事態

リソースタイプ: `AWS::RDS::DBClusterSnapshot`、`AWS::RDS:DBSnapshot`

AWS Config ルール : `docdb-cluster-snapshot-public-prohibited`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon DocumentDB の手動クラススナップショットがパブリックかどうかをチェックします。手動クラススナップショットがパブリックの場合、コントロールは失敗します。

Amazon DocumentDB 手動クラススナップショットは、意図しない限りパブリックにしないでください。暗号化されていない手動スナップショットをパブリックとして共有すると、すべての AWS アカウントでこのスナップショットを使用できるようになります。パブリックスナップショットは、意図しないデータ漏えいにつながる可能性があります。

> **Note**
>
> このコントロールは手動クラススナップショットを評価します。Amazon DocumentDB 自動クラススナップショットを共有することはできません。ただし、自動スナップショットをコピーして手動スナップショットを作成し、そのコピーを共有できます。

修正

Amazon DocumentDB 手動クラススナップショットへのパブリックアクセスを削除するには、「Amazon DocumentDB デベロッパーガイド」の「スナップショットの共有」を参照してください。プログラムでは、Amazon DocumentDB のオペレーション `modify-db-snapshot-attribute` を使用できます。`attribute-name` を `restore` として、`values-to-remove` を `all` として設定します。

[DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります

関連する要件: NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール : `docdb-cluster-audit-logging-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon DocumentDB クラスターが監査ログを Amazon CloudWatch Logs に発行するかどうかをチェックします。クラスターが監査ログを CloudWatch Logs に発行しない場合、コントロールは失敗します。

Amazon DocumentDB (MongoDB 互換) を使用すると、クラスター内で実行されたイベントを監査できます。ログに記録されるイベントの例としては、認証の成功と失敗、データベース内のコレクションの削除、インデックスの作成などがあります。デフォルトでは、監査が Amazon DocumentDB 上で無効化されているため、この機能を有効化する必要があります。

修正

Amazon DocumentDB 監査ログを CloudWatch ログに発行するには、Amazon DocumentDB デベロッパーガイド」の「監査の有効化」を参照してください。

[DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

カテゴリ: 保護 > データ保護 > データ削除保護

重要度: 中

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール : `docdb-cluster-deletion-protection-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon DocumentDB クラスターで削除保護が有効になっているかどうかを確認します。クラスターで削除保護が有効になっていない場合、コントロールは失敗します。

クラスターの削除保護を有効にすることで、偶発的なデータベース削除や権限のないユーザーによる削除に対して保護の強化を提供します。削除保護が有効の間、Amazon DocumentDB クラスターは削除できません。削除リクエストを成功させるには、まず削除保護を無効にする必要があります。Amazon DocumentDB コンソールを使用してクラスターを作成する場合は、デフォルトで削除保護が有効になっています。

修正

既存の Amazon DocumentDB クラスターの削除保護を有効にするには、「Amazon DocumentDB デベロッパーガイド」の「Amazon DocumentDB クラスターの変更」を参照してください。[クラスターの変更] セクションで、[削除保護の有効化]を選択します。

Amazon DynamoDB コントロール

これらのコントロールは DynamoDB リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[DynamoDB.1] DynamoDB テーブルは、需要に応じて容量をオートスケーリングする必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-2(2)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::DynamoDB::Table`

AWS Config ルール: dynamodb-autoscaling-enabled

スケジュールタイプ: 定期的

パラメータ:

パラメータ	説明	[Type] (タイプ)	有効なカスタム値	Security Hub のデフォルト値
`minProvisionedReadCapacity`	DynamoDB 自動スケーリング用にプロビジョニングされた読み込みキャパシティユニットの最小数	整数	`1~40000`	デフォルト値なし
`targetReadUtilization`	読み込みキャパシティのターゲット使用率 (%)	整数	`20~90`	デフォルト値なし
`minProvisionedWriteCapacity`	DynamoDB 自動スケーリング用にプロビジョニングされた書き込みキャパシティユニットの最小数	整数	`1~40000`	デフォルト値なし
`targetWriteUtilization`	書き込みキャパシティのターゲット使用率 (%)	整数	`20~90`	デフォルト値なし

このコントロールは、Amazon DynamoDB テーブルが必要に応じて読み取りおよび書き込み容量をスケーリングできるかどうかをチェックします。テーブルで自動スケーリングが設定されたオンデマンドキャパシティモードまたはプロビジョンモードを使用しない場合、コントロールは失敗します。デフォルトでは、このコントロールは、特定のレベルの読み込みまたは書き込みキャパシティに関係なく、これらのモードのいずれかを設定するだけで済みます。必要に応じて、特定のレベルの読み込みおよび書き込みキャパシティ、またはターゲット使用率を必要とするカスタムパラメータ値を指定できます。

需要に応じて容量をスケーリングすると、スロットリング例外を回避し、アプリケーションの可用性を維持するのに役立ちます。オンデマンドキャパシティモードの DynamoDB テーブルは、DynamoDB スループットのデフォルトテーブルクォータによってのみ制限されます。これらのクォータを引き上げるには、トラフィックパターンに応じてプロビジョニングされたスループット容量を自動スケーリングで調整するプロビジョニングモードの AWS Support.DynamoDB テーブルでサポートチケットを提出できます。DynamoDB リクエストスロットリングの詳細については、「Amazon DynamoDB 開発者ガイド」の「リクエストのスロットリングとバーストキャパシティ」を参照してください。

修正

キャパシティモードで既存テーブルの DynamoDB オートスケーリングを有効にするには、「Amazon DynamoDB 開発者ガイド」の「既存のテーブルでの DynamoDB Auto Scaling の有効化」を参照してください。

[DynamoDB.2] DynamoDB テーブルでは point-in-time リカバリを有効にする必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

重要度: 中

リソースタイプ: `AWS::DynamoDB::Table`

AWS Config ルール : `dynamodb-pitr-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon DynamoDB テーブルで point-in-time リカバリ (PITR) が有効になっているかどうかをチェックします。

バックアップは、セキュリティインシデントからより迅速に復元するために役立ちます。また、システムの耐障害性を強化します。DynamoDB point-in-time リカバリは、DynamoDB テーブルのバックアップを自動化します。偶発的な削除や書き込み操作から回復する時間が短縮されます。PITR を有効にした DynamoDB テーブルは、過去 35 日間の任意の時点に復元できます。

修正

DynamoDB テーブルを特定の時点に復元するには、「Amazon DynamoDB 開発者ガイド」の「DynamoDB テーブルをある時点に復元する」を参照してください。

[DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::DAX::Cluster`

AWS Config ルール: `dax-encryption-enabled`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Amazon DynamoDB Accelerator (DAX) クラスターが保管中に暗号化されているかどうかをチェックします。DAX クラスターが保管中に暗号化されていない場合、コントロールは失敗します。

保管中のデータを暗号化すると、ディスクに保存されているデータが、 に対して認証されていないユーザーによってアクセスされるリスクが軽減されます AWS。暗号化により、権限のないユーザーがデータにアクセスする能力を制限するために、別の一連のアクセスコントロールが追加されます。例えば、データを読み取る前にデータを復号化するには、API の許可が必要です。

修正

クラスターが作成された後は、保管中の暗号化を有効または無効にすることはできません。保管中の暗号化を有効にするにはクラスターを再作成する必要があります。保管中の暗号化が有効な DAX クラスターを作成する方法の詳細については、「Amazon DynamoDB 開発者ガイド」の「AWS Management Consoleを使用して保管中の暗号化を有効にする」を参照してください。

[DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

重要度: 中

リソースタイプ: `AWS::DynamoDB::Table`

AWS Config ルール： `dynamodb-resources-protected-by-backup-plan`

スケジュールタイプ: 定期的

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`backupVaultLockCheck`	パラメータが に設定`true`され、リソースが AWS Backup ボールトロックを使用する場合、コントロールは`PASSED`結果を生成します。	ブール値	`true` 、、または `false`	デフォルト値なし

このコントロールは、`ACTIVE` 状態の Amazon DynamoDB テーブルがバックアッププランの対象になっているかどうかを評価します。DynamoDB テーブルがバックアッププランの対象になっていない場合、コントロールは失敗します。`backupVaultLockCheck` パラメータを に設定する

とtrue、DynamoDB テーブルが AWS Backup ロックされたボールトにバックアップされている場合にのみコントロールが成功します。

AWS Backup は、 全体のデータのバックアップを一元化および自動化するのに役立つフルマネージドバックアップサービスです AWS のサービス。を使用すると AWS Backup、データのバックアップ頻度やバックアップの保持期間など、バックアップ要件を定義するバックアッププランを作成できます。バックアッププランに DynamoDB テーブルを含めると、意図しない損失や削除からデータを保護できます。

修正

AWS Backup バックアッププランに DynamoDB テーブルを追加するには、「 AWS Backup デベロッパーガイド」の「バックアッププランへのリソースの割り当て」を参照してください。

[DynamoDB.5] DynamoDB テーブルにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::DynamoDB::Table`

AWS Config ルール: `tagged-dynamodb-table` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、Amazon DynamoDB テーブルに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。テーブルにタグキーがな

い場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、テーブルにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

DynamoDB テーブルにタグを追加するには、「Amazon DynamoDB デベロッパーガイド」の「DynamoDB でのリソースのタグ付け」を参照してください。 DynamoDB

[DynamoDB.6] DynamoDB テーブルで、削除保護が有効になっている必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

カテゴリ: 保護 > データ保護 > データ削除保護

重要度: 中

リソースタイプ: AWS::DynamoDB::Table

AWS Config ルール： dynamodb-table-deletion-protection-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon DynamoDB テーブルで削除保護が有効になっているかどうかをチェックします。DynamoDB テーブルで削除保護が有効になっていない場合、コントロールは失敗します。

削除保護プロパティを使用すると、DynamoDB テーブルを誤って削除しないように保護できます。テーブルに対してこのプロパティを有効にすると、管理者が通常のテーブル管理オペレーションを行うときにテーブルが誤って削除されるのを防ぐことができます。これにより、通常業務が中断されるのを防ぐことができます。

修正

DynamoDB テーブルの削除保護を有効にするには、「Amazon DynamoDB 開発者ガイド」の「削除保護の使用」を参照してください。

[DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります

関連する要件： NIST.800-53.r5 AC-17、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::DynamoDB::Table`

AWS Config ルール： dax-tls-endpoint-encryption

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Amazon DynamoDB Accelerator (DAX) クラスターが転送中に暗号化され、エンドポイントの暗号化タイプが TLS に設定されているかどうかをチェックします。DAX クラスターが転送中に暗号化されていない場合、コントロールは失敗します。

HTTPS (TLS) を使用すると、潜在的な攻撃者がネットワークトラフィックを傍受 person-in-the-middle または操作するために または同様の攻撃を使用することを防ぐことができます。DAX クラスターへのアクセスには、TLS 経由の暗号化された接続のみを許可する必要があります。ただし、転送中のデータを暗号化すると、パフォーマンスに影響する可能性があります。TLS のパフォーマンスプロファイルと影響を理解するには、暗号化を有効にしてアプリケーションをテストする必要があります。

修正

DAX クラスターの作成後に TLS 暗号化設定を変更することはできません。既存の DAX クラスターを暗号化するには、転送中の暗号化を有効にして新しいクラスターを作成し、アプリケーションのトラフィックをそのクラスターに移動してから、古いクラスターを削除します。詳細については、「Amazon DynamoDB ディベロッパーガイド」の「削除保護の使用」を参照してください。

Amazon Elastic Container Registry のコントロール

これらのコントロールは Amazon ECR リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります

関連する要件: NIST.800-53.r5 RA-5

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 高

リソースタイプ: `AWS::ECR::Repository`

AWS Config ルール: `ecr-private-image-scanning-enabled`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、プライベート Amazon ECR リポジトリでイメージスキャニングが設定されているかどうかをチェックします。プライベート ECR リポジトリがプッシュ時スキャンまたは連続スキャン用に設定されていない場合、コントロールは失敗します。

ECR イメージスキャニングは、コンテナイメージ内のソフトウェアの脆弱性を特定するのに役立ちます。ECR リポジトリでイメージスキャンを設定すると、保存されているイメージの整合性と安全性を検証するレイヤーが追加されます。

修正

ECR リポジトリのイメージスキャニングを設定する方法については、「Amazon Elastic Container Registry User Guide」(Amazon Elastic Container Registry ユーザーガイド) の「Image scanning」(イメージスキャニング) を参照してください。

[ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-8(1)

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 中

リソースタイプ: `AWS::ECR::Repository`

AWS Config ルール : `ecr-private-tag-immutability-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、プライベート ECR リポジトリでタグのイミュータビリティが有効になっているかどうかをチェックします。プライベート ECR リポジトリでタグのイミュータビリティが無効になっていると、このコントロールは失敗します。このルールは、タグのイミュータビリティが有効で、かつ値が `IMMUTABLE` に設定されていると成功します。

Amazon ECR のタグのイミュータビリティにより、ユーザーは、イメージの説明タグを信頼性の高いメカニズムとして使用し、イメージを追跡して一意に識別することができます。イミュータブルなタグは静的です。つまり、各タグは一意のイメージを参照します。静的タグを使用すると、常に同じイメージがデプロイされるので、信頼性とスケーラビリティが向上します。設定すると、タグのイミュータビリティにより、タグが上書きされなくなり、アタックサーフェスが減少します。

修正

イミュータブル (変更不可能) なタグが設定されたリポジトリを作成する場合、または既存のリポジトリのイメージタグのイミュータビリティ (変更不可能性) を更新するには、Amazon Elastic Container Registry ユーザーガイドの「イメージタグの変更可能性」を参照してください。

[ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 識別 > リソース設定

重要度: 中

リソースタイプ: `AWS::ECR::Repository`

AWS Config ルール : `ecr-private-lifecycle-policy-configured`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon ECR リポジトリに少なくとも 1 つのライフサイクルポリシーが設定されているかどうかをチェックします。ECR リポジトリにライフサイクルポリシーが設定されていない場合、このコントロールは失敗します。

Amazon ECR ライフサイクルポリシーを使用すると、リポジトリ内のイメージのライフサイクル管理を有効にすることができます。ライフサイクルポリシーを設定することで、未使用イメージのクリーンアップと、年数またはカウントに基づいたイメージの有効期限を自動化することができます。これらのタスクを自動化することで、リポジトリで古いイメージを意図せずに使用することを回避できます。

修正

ライフサイクルポリシーを設定するには、「Amazon Elastic Container Registry ユーザーガイド」の「ライフサイクルポリシーのプレビューを作成する」を参照してください。

[ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::ECR::PublicRepository`

AWS Config ルール: `tagged-ecr-publicrepository` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon ECR パブリックリポジトリに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。パブリックリポジトリにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、パブリックリポジトリにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

ECR パブリックリポジトリにタグを追加するには、「Amazon Elastic Container Registry ユーザーガイド」の「Amazon ECR パブリックリポジトリのタグ付け」を参照してください。

Amazon ECS コントロール

これらのコントロールは Amazon ECS リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 高

リソースタイプ: `AWS::ECS::TaskDefinition`

AWS Config ルール : `ecs-task-definition-user-for-host-mode-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `SkipInactiveTaskDefinitions`: `true` (カスタマイズ不可)

このコントロールは、ホストネットワークモードを使用するアクティブな Amazon ECS タスク定義に `privileged` または `user` コンテナの定義もあるかどうかをチェックします。ホストネットワークモードとコンテナ定義が `privileged=false`、空で、`user=root`、または空のタスク定義では、制御に失敗します。

このコントロールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

この制御の目的は、ホストネットワークモードを使用するタスクを実行するときに、アクセスが意図的に定義されるようにすることです。タスク定義に昇格されたアクセス権限がある場合は、その構成を選択したことによるものです。このコントロールは、タスク定義でホストネットワークが有効になっていても、お客様が昇格されたアクセス権限を選択していない場合に、予期しない権限の昇格の有無をチェックします。

修正

タスク定義を更新する方法については、「Amazon Elastic Container Service 開発者ガイド」の「タスク定義の更新」を参照してください。

タスク定義を更新しても、以前のタスク定義から起動された実行中のタスクは更新されません。実行中のタスクを更新するには、新しいタスク定義を使用してタスクを再デプロイする必要があります。

[ECS.2] ECS サービスには、パブリック IP アドレスを自動で割り当てないでください

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 高

リソースタイプ: `AWS::ECS::Service`

AWS Configルール: `ecs-service-assign-public-ip-disabled` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `exemptEcsServiceArns` (カスタマイズ不可)。Security Hub は、このパラメータを設定しません。このルールから除外する Amazon ECS サービスの ARN カンマ区切りリスト。

  Amazon ECS サービスで `AssignPublicIP` が `ENABLED` に設定されていて、このパラメータリストで指定されている場合、このルールは `COMPLIANT` が使用されます。

Amazon ECS サービスで AssignPublicIP が ENABLED に設定されていて、このパラメータリストで指定されていない場合、このルールは NON_COMPLIANT が使用されます。

このコントロールは、Amazon ECS サービスがパブリック IP アドレスの自動割り当てが設定されているかどうかをチェックします。AssignPublicIP が ENABLED の場合、このコントロールは失敗します。AssignPublicIP が DISABLED の場合、このコントロールは成功です。

パブリック IP アドレスは、インターネットから到達可能な IP アドレスです。パブリック IP アドレスを使用して Amazon ECS インスタンスを起動すると、Amazon ECS インスタンスにインターネットから到達することができます。Amazon ECS サービスは、コンテナアプリケーションサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスができないようにする必要があります。

修正

パブリック IP の自動割り当てを無効にするには、「Amazon Elastic Container Service 開発者ガイド」の「サービスに VPC とセキュリティグループ設定を設定するには」を参照してください。

[ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 識別 > リソース設定

重要度: 高

リソースタイプ: AWS::ECS::TaskDefinition

AWS Configルール： ecs-task-definition-pid-mode-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon ECS のタスク定義が、ホストのプロセス名前空間をそのコンテナと共有するように設定されているかどうかをチェックします。タスク定義が、ホストのプロセス名前空間を、そこで実行されているコンテナと共有している場合、このコントロールは失敗します。このコントロールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

プロセス ID (PID) 名前空間は、プロセス間を分離します。これにより、システムプロセスが可視化されることを防ぎ、PID 1 を含む PID の再利用が可能になります。ホストの PID 名前空間がコンテ

ナと共有されている場合、コンテナは、ホストシステム上のすべてのプロセスを参照できるようになります。これにより、ホストとコンテナ間をプロセスレベルで分離するメリットが減ります。このような状況は、ホストそれ自体で行われているプロセスへの、不正アクセス (プロセスの操作や終了など) につながる可能性があります。ユーザーは、ホストのプロセス名前空間を、そこで実行されているコンテナと共有すべきではありません。

修正

タスク定義上で `pidMode` を設定する方法については、「Amazon Elastic Container Service デベロッパーガイド」の「タスク定義パラメータ」を参照してください。

[ECS.4] ECS コンテナは、非特権として実行する必要があります

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理 > ルートユーザーのアクセス制限

重要度: 高

リソースタイプ: `AWS::ECS::TaskDefinition`

AWS Configルール: ecs-containers-nonprivileged

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon ECS のタスク定義の、コンテナ定義の `privileged` パラメータが `true` に設定されているかどうかをチェックします。このパラメータの値が `true` である場合、このコントロールは失敗します。このコントロールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

昇格された特権を、ECS タスク定義から削除することが推奨されます。この特権パラメータが `true` の場合、このコンテナには、ホストコンテナインスタンスに対する昇格された特権が付与されます (ルートユーザーと同様)。

修正

タスク定義上で `privileged` を設定する方法については、「Amazon Elastic Container Service デベロッパーガイド」の「詳細コンテナ定義パラメータ」を参照してください。

[ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 高

リソースタイプ: `AWS::ECS::TaskDefinition`

AWS Configルール: ecs-containers-readonly-access

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon ECS コンテナが、マウントされたルートファイルシステムへの読み取り専用アクセスに制限されているかどうかをチェックします。`readonlyRootFilesystem` パラメータが `false` に設定されているか、タスク定義内のコンテナ定義にパラメータが存在しない場合、コントロールは失敗します。このコントロールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

このオプションを有効にすると、ファイルシステムフォルダとディレクトリに対する明示的な読み取り/書き込み権限がない限り、コンテナインスタンスのファイルシステムへの改ざんや書き込みができないため、セキュリティ攻撃ベクトルを減らすことができます。このコントロールは、最小特権の原則にも準拠しています。

修正

コンテナ定義をルート filesystems への読み取り専用アクセスに制限します

1. Amazon ECS クラシックコンソール (https://console.aws.amazon.com/ecs/) を開きます。
2. 左側のナビゲーションペインで、[タスク定義] をクリックします。
3. 更新の必要なコンテナ定義を含むタスク定義をクリックします。それぞれ、以下のステップを完了します。
    - ドロップダウンから、[JSON を使用した新しいリビジョンの作成] を選択します。
    - `readonlyRootFilesystem` パラメータを追加し、タスク定義内のコンテナ定義で `true` に設定します。

- [Create] (作成) を選択します。

[ECS.8] シークレットは、コンテナ環境の変数として渡さないでください

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアな開発 > 認証情報がハードコーディングされていない

重要度: 高

リソースタイプ: `AWS::ECS::TaskDefinition`

AWS Configルール: ecs-no-environment-secrets

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- secretKeys = `AWS_ACCESS_KEY_ID`、`AWS_SECRET_ACCESS_KEY`、`ECS_ENGINE_AUTH_DATA` (カスタマイズ不可)

このコントロールは、コンテナ定義の `environment` パラメータにある、任意の変数のキー値に、`AWS_ACCESS_KEY_ID`、`AWS_SECRET_ACCESS_KEY`、`ECS_ENGINE_AUTH_DATA` のいずれかが含まれているかどうかをチェックします。任意のコンテナ定義内の単一の環境変数が、`AWS_ACCESS_KEY_ID`、`AWS_SECRET_ACCESS_KEY`、`ECS_ENGINE_AUTH_DATA` のいずれかである場合、このコントロールは失敗します。このコントロールは、Amazon S3 など、他のロケーションから渡される環境変数は対象としません。このコントロールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

AWS Systems Manager Parameter Store は、組織のセキュリティ体制の改善に役立ちます。シークレットと認証情報は、コンテナインスタンスに直接渡したり、コードにハードコーディングしたりするのではなく、Parameter Store を使用して保存することが推奨されます。

修正

SSM を使用してパラメータを作成する方法については、「AWS Systems Manager ユーザーガイド」の「Systems Manager パラメータを作成する」を参照してください。シークレットを指定するタスク定義の作成に関する詳細は、「Amazon Elastic Container Service デベロッパーガイド」の「Secrets Manager を使用した機密データの指定」を参照してください。

[ECS.9] ECS タスク定義にはログ設定が必要です。

関連する要件: NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 高

リソースタイプ: `AWS::ECS::TaskDefinition`

AWS Configルール： ecs-task-definition-log-configuration

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、最新のアクティブな Amazon ECS タスク定義にロギング設定が指定されているかどうかを確認します。タスク定義に `logConfiguration` プロパティが定義されていない場合、または少なくとも 1 つのコンテナ定義で `logDriver` の値が null の場合、コントロールは失敗します。

ログ記録は Amazon ECS の信頼性、可用性、パフォーマンスの維持に有益です。タスク定義からデータを収集すると可視性が得られ、プロセスのデバッグやエラーの根本原因の特定に役立ちます。ECS タスク定義で定義する必要のないロギングソリューション (サードパーティのロギングソリューションなど) を使用している場合は、ログを無効にできますが、無効にする前に、ログが適切に取得、保存されていることを確認してください。

修正

Amazon ECS タスク定義のログ設定を定義するには、「Amazon Elastic Container Service デベロッパーガイド」の「タスク定義でログ設定を指定する」を参照してください。

[ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。

関連する要件: NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 中

リソースタイプ: `AWS::ECS::Service`

AWS Configルール : `ecs-fargate-latest-platform-version`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `latestLinuxVersion: 1.4.0` (カスタマイズ不可)
- `latestWindowsVersion: 1.0.0` (カスタマイズ不可)

このコントロールは、Amazon ECS Fargate サービスが最新バージョンの Fargate プラットフォームで実行されているかどうかをチェックします。プラットフォームが最新バージョンでない場合、このコントロールは失敗します。

AWS Fargate プラットフォームバージョンは、カーネルとコンテナランタイムバージョンの組み合わせである Fargate タスクインフラストラクチャの特定のランタイム環境を指します。新しいプラットフォームのバージョンは、ランタイム環境の進化に伴ってリリースされます。例えば、新しいバージョンは、カーネルやオペレーティングシステムの更新、新機能、バグ修正、セキュリティ更新があったときなどにリリースされます。セキュリティの更新やパッチは、 Fargate のタスクに自動的にデプロイされます。プラットフォームバージョンに影響するセキュリティ問題が見つかった場合、はプラットフォームバージョンを AWS パッチします。

修正

プラットフォームバージョンを含む既存サービスの更新方法については、「Amazon Elastic Container Service デベロッパーガイド」の「サービスの更新」を参照してください。

[ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります

関連する要件: NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::ECS::Cluster`

AWS Configルール : `ecs-container-insights-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、ECS クラスターが Container Insights を使用しているかどうかをチェックします。クラスターで Container Insights がセットアップされていない場合、このコントロールは失敗します。

モニタリングは、Amazon ECS クラスターの信頼性、可用性、パフォーマンスを維持する上で欠かせない要素です。 CloudWatch Container Insights を使用して、コンテナ化されたアプリケーションおよびマイクロサービスからメトリクスとログを収集、集約、要約します。 は、CPU、メモリ、ディスク、ネットワークなどの多くのリソースのメトリクス CloudWatch を自動的に収集します。Container Insights では、問題の迅速な特定と解決に役立つ、コンテナの再起動失敗などの診断情報も提供されます。Container Insights が収集するメトリクスに CloudWatch アラームを設定することもできます。

修正

Container Insights を使用するには、「Amazon CloudWatch ユーザーガイド」の「サービスの更新」を参照してください。

[ECS.13] ECS サービスはタグ付けする必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::ECS::Service`

AWS Configルール: `tagged-ecs-service` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーで	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	は、大文字と小文字が区別されます。			

このコントロールは、Amazon ECS サービスにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。サービスにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、サービスがキーでタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

ECS サービスにタグを追加するには、「Amazon Elastic Container Service デベロッパーガイド」の「Amazon ECS リソースのタグ付け」を参照してください。

[ECS.14] ECS クラスターにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::ECS::Cluster`

AWS Configルール: `tagged-ecs-cluster` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon ECS クラスターにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。クラスターにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、クラスターにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できま

す。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

ECS クラスターにタグを追加するには、「Amazon Elastic Container Service デベロッパーガイド」の「Amazon ECS リソースのタグ付け」を参照してください。

[ECS.15] ECS タスク定義にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::ECS::TaskDefinition`

AWS Configルール: `tagged-ecs-taskdefinition` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon ECS タスク定義に、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。タスク定義にタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、タスク定義にキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

ECS タスク定義にタグを追加するには、「Amazon Elastic Container Service デベロッパーガイド」の「Amazon ECS リソースのタグ付け」を参照してください。

Amazon Elastic Compute Cloud コントロール

これらのコントロールは Amazon EC2 リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[EC2.1] Amazon EBS スナップショットはパブリックに復元できないようにすることをお勧めします

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 非常事態

リソースタイプ: `AWS::::Account`

AWS Config ルール: `ebs-snapshot-public-restorable-check`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Amazon Elastic Block Store スナップショットがパブリックではないかどうかをチェックします。Amazon EBS スナップショットを誰でも復元できる場合、コントロールは失敗します。

EBS スナップショットは、特定の時点の EBS ボリュームのデータを Amazon S3 にバックアップするために使用されます。スナップショットを使用して、EBS ボリュームを以前の状態に復元できます。スナップショットのパブリックへの共有は滅多に認められていません。一般的に、スナップショットを公開する決定は、誤って行われたか、影響を完全に理解せずに行われています。このチェックは、そのような共有がすべて完全に計画され、意図的であったことを確認するのに役立ちます。

パブリック EBS スナップショットをプライベートにするには、「Amazon EC2 ユーザーガイド」の「スナップショットの共有」を参照してください。 Amazon EC2 [アクション、権限の変更] で、[非公開] を選択します。

[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします

関連する要件： PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/2.1、CIS AWS Foundations Benchmark v1.2.0/4.3、CIS AWS Foundations Benchmark v1.4.0/5.3、CIS AWS Foundations Benchmark v3.0.0/5.4、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(1 SC-7 SC-7 SC-76

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ: `AWS::EC2::SecurityGroup`

AWS Config ルール : `vpc-default-security-group-closed`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、VPC のデフォルトのセキュリティグループがインバウンドとアウトバウンドのいずれかのトラフィックを許可しているかをチェックします。セキュリティグループがインバウンドまたはアウトバウンドのトラフィックを許可している場合、このコントロールは失敗します。

デフォルトのセキュリティグループのルールでは、同じセキュリティグループに割り当てられているネットワークインターフェイス (および関連するインスタンス) からのすべてのアウトバウンドトラフィックとインバウンドトラフィックを許可します。デフォルトのセキュリティグループを使用しないことをお勧めします。デフォルトのセキュリティグループは削除できないため、デフォルトのセキュリティグループルール設定を変更して、インバウンドトラフィックとアウトバウンドトラフィックを制限する必要があります。これにより、デフォルトのセキュリティグループが EC2 インスタンスなどのリソースに対して誤って設定されている場合に、意図しないトラフィックが防止されます。

修正

この問題を解決するには、まず新しい最小特権のセキュリティグループを作成することから始めます。手順については、「Amazon VPC ユーザーガイド」の「セキュリティグループの作成」を参照してください。次に、新しいセキュリティグループを EC2 インスタンスに割り当てます。手順については、Amazon EC2 ユーザーガイド」の「インスタンスのセキュリティグループを変更する」を参照してください。

新しいセキュリティグループをリソースに割り当てた後、デフォルトのセキュリティグループからすべてのインバウンドルールとアウトバウンドルールを削除します。手順については、「Amazon VPC ユーザーガイド」の「セキュリティグループのルールの削除」を参照してください。

[EC2.3] アタッチされた Amazon EBS ボリュームは、保管時に暗号化することをお勧めします

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::EC2::Volume`

AWS Config ルール : `encrypted-volumes`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、添付済みの EBS ボリュームが暗号化されているかどうかをチェックします。このチェックに合格するには、EBS ボリュームが使用中であり、暗号化されている必要があります。EBS ボリュームが添付済みでない場合、このチェックは対象外です。

EBS ボリュームの機密データのセキュリティを強化するには、保管中の EBS 暗号化を有効にする必要があります。Amazon EBS 暗号化は、EBS リソースに対して、独自のキー管理インフラストラクチャの構築、保守、および保護を必要としない、簡単な暗号化ソリューションを提供します。暗号化されたボリュームとスナップショットを作成する際に、KMS キー を使用します。

Amazon EBS 暗号化の詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EBS 暗号化」を参照してください。 Amazon EC2

修正

暗号化されていない既存のボリュームまたはスナップショットを暗号化する直接的な方法はありません。新しいボリュームまたはスナップショットは、作成時にのみ暗号化できます。

暗号化をデフォルトで有効にした場合、Amazon EBS は Amazon EBS 暗号化のデフォルトキーを使用して、作成された新しいボリュームまたはスナップショットを暗号化します。デフォルトで暗号化

を有効にしていない場合でも、個々のボリュームまたはスナップショットを作成するときに暗号化を有効にすることができます。どちらの場合も、Amazon EBS 暗号化のデフォルトキーを上書きし、対称カスタマーマネージドキーを選択できます。

詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EBS ボリュームAmazon EC2の作成」および「Amazon EBS スナップショットのコピー」を参照してください。

[EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 識別 > インベントリ

重要度: 中

リソースタイプ: `AWS::EC2::Instance`

AWS Config ルール: `ec2-stopped-instance`

スケジュールタイプ: 定期的

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`AllowedDays`	失敗の検出結果が生成される前に、EC2 インスタンスが停止状態になっても許容される日数。	整数	`1~365`	`30`

このコントロールは、許可されている日数よりも長く停止している Amazon EC2 インスタンスがあるかどうかをチェックします。EC2 インスタンスが最大許容期間よりも長く停止すると、コントロールは失敗します。最大許容期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 30 日を使用します。

EC2 インスタンスが長期間実行されていないと、インスタンスがアクティブに保守 (分析、パッチ適用、更新) されていないため、セキュリティリスクが発生します。後で起動すると、適切なメンテナ

ンスが行われないと、 AWS 環境で予期しない問題が発生する可能性があります。EC2 インスタンスを非アクティブ状態で長期間安全に維持するには、メンテナンスのために定期的に起動し、メンテナンス後に停止します。これは自動化されたプロセスであるべきです。

修正

非アクティブな EC2 インスタンスを終了するには、「Amazon EC2 ユーザーガイド」の「インスタンスの終了」を参照してください。 Amazon EC2

[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします

関連する要件： CIS AWS Foundations Benchmark v1.2.0/2.9、CIS AWS Foundations Benchmark v1.4.0/3.9、CIS AWS Foundations Benchmark v3.0.0/3.7、PCI DSS v3.2.1/10.3.3、PCI DSS v3.2.1/10.3.4、PCI DSS v3.2.1/10.3.5、NIST.800-53.r5 AC-4(26)10.3.6、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3 AU-6 AU-6 CA-7 SI-7

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::EC2::VPC`

AWS Config ルール: `vpc-flow-logs-enabled`

スケジュールタイプ: 定期的

パラメータ:

- `trafficType`: `REJECT` (カスタマイズ不可)

このコントロールは、Amazon VPC フローログが見つかり、VPC に対して有効になっているかどうかをチェックします。トラフィックタイプは `Reject` に設定されています。

VPC フローログ機能を使用して、VPC のネットワークインターフェイスとの間で行き来する IP アドレストラフィックに関する情報をキャプチャします。フローログを作成したら、そのデータを CloudWatch Logs で表示および取得できます。コストを削減するために、フローログを Amazon S3 に送信することもできます。

Security Hub では、VPC のパケット拒否のフローログ記録を有効にすることを推奨します。フローログは、VPC を通過するネットワークトラフィックを可視化し、セキュリティワークフロー中の異常なトラフィックを検出したりインサイトを提供できます。

デフォルトでは、レコードには送信元、送信先、プロトコルなど、IP アドレスフローのさまざまなコンポーネントの値が含まれています。ログフィールドの詳細と説明については、「Amazon VPC ユーザーガイド」の「VPC フローログ」を参照してください。

修正

VPC フローログを作成するには、「Amazon VPC ユーザーガイド」の「VPC フローログを作成する」を参照してください。Amazon VPC コンソールを開いたら、[お客様の VPC] を選択します。[フィルター] で、[拒否] または [すべて] を選択します。

[EC2.7] EBS のデフォルト暗号化を有効にすることをお勧めします

関連する要件： CIS AWS Foundations Benchmark v1.4.0/2.2.1、CIS AWS Foundations Benchmark v3.0.0/2.2.1、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::::Account`

AWS Config ルール: `ec2-ebs-encryption-by-default`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Amazon Elastic Block Store (Amazon EBS) でアカウントレベルの暗号化がデフォルトで有効になっているかどうかをチェックします。アカウントレベルの暗号化が有効になっていない場合、コントロールは失敗します。

アカウントで暗号化が有効になっている場合、Amazon EBS ボリュームとスナップショットのコピーは保管中に暗号化されます。これにより、データの保護レイヤーが追加されます。詳細については、「Amazon EC2 ユーザーガイド」の「デフォルトで暗号化」を参照してください。

次のインスタンスタイプでは暗号化がサポートされないことに注意してください: R1、C1、および M1。

修正

Amazon EBS ボリュームのデフォルトの暗号化を設定するには、「Amazon EC2 ユーザーガイド」の「デフォルトでの暗号化」を参照してください。 Amazon EC2

[EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします

関連する要件： CIS AWS Foundations Benchmark v3.0.0/5.6、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

カテゴリ： 保護 > ネットワークセキュリティ

重要度: 高

リソースタイプ: `AWS::EC2::Instance`

AWS Config ルール : `ec2-imdsv2-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、EC2 インスタンスメタデータバージョンが、インスタンスメタデータサービスバージョン 2 (IMDSv2) で設定されているかどうかをチェックします。IMDSv2 で `HttpTokens` が必須に設定されている場合、コントロールは成功します。`HttpTokens` が `optional` に設定されている場合、コントロールは失敗します。

インスタンスメタデータは、実行中のインスタンスを設定または管理するために使用します。IMDS は、一時的で頻繁にローテーションされる認証情報へのアクセスを提供します。これらの認証情報を使用すると、機密認証情報を手動でまたはプログラムでインスタンスにハードコーディングや、配信する必要がなくなります。IMDS は、すべての EC2 インスタンスにローカルに添付されます。これは、特別な「リンクローカル」IP アドレス 169.254.169.254 で実行されます。この IP アドレスは、インスタンスで実行されるソフトウェアによってのみアクセスできます。

IMDS のバージョン 2 では、次の種類の脆弱性に対する新しい保護が追加されています。これらの脆弱性は IMDS へのアクセスに利用される可能性があります。

- ウェブサイトアプリケーションのファイアウォールを開く
- リバースプロキシを開く
- サーバー側リクエスト偽造 (SSRF) の脆弱性

- レイヤー 3 ファイアウォールおよびネットワークアドレス変換 (NAT) を開く

Security Hub では、EC2 インスタンスを IMDSv2 で設定することを推奨します。

修正

IMDSv2 で EC2 インスタンスを設定するには、「Amazon EC2 ユーザーガイド」のIMDSv2を要求する推奨パス」を参照してください。 IMDSv2 Amazon EC2

[EC2.9] Amazon EC2 インスタンスは、パブリック IPv4 アドレスを未設定にすることをお勧めします

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 高

リソースタイプ: `AWS::EC2::Instance`

AWS Config ルール : `ec2-instance-no-public-ip`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、EC2 インスタンスにパブリック IP アドレスがあるかどうかをチェックします。EC2 インスタンスの設定項目に `publicIp` フィールドが存在する場合、コントロールは失敗します。このコントロールは、IPv4 アドレスにのみ適用されます。

パブリック IPv4 アドレスは、インターネットから到達可能な IP アドレスです。パブリック IP アドレスを使用してインスタンスを起動すると、EC2 インスタンスはインターネットから到達可能です。プライベート IPv4 アドレスは、インターネットから到達できない IP アドレスです。プライベート IPv4 アドレスは、同じ VPC 内の EC2 インスタンス間または接続されたプライベートネットワークの通信に使用できます。

IPv6 アドレスはグローバルに一意であるため、インターネットから到達できます。ただし、デフォルトではすべてのサブネットで IPv6 アドレス指定属性が false に設定されています。VPC での IPv6

の詳細については、「Amazon VPC ユーザーガイド」の「VPC での IP アドレス指定」を参照してください。

パブリック IP アドレスで EC2 インスタンスを維持する正当なユースケースがある場合は、このコントロールの結果を抑制できます。フロントエンドアーキテクチャオプションの詳細については、「AWS アーキテクチャのブログ」または「This Is My Architecture series (マイアーキテクチャシリーズ)」を参照してください。

修正

デフォルト以外の VPC を使用し、デフォルトでインスタンスがパブリック IP アドレスに割り当てられないようにします。

デフォルトの VPC で EC2 インスタンスを起動すると、パブリック IP アドレスが割り当てられます。EC2 インスタンスをデフォルト以外の VPC で起動すると、サブネット設定によって、パブリック IP アドレスを受信するかどうかが決まります。サブネットには、サブネット内の新しい EC2 インスタンスがパブリック IPv4 アドレスプールからパブリック IP アドレスを受け取るかどうかを判断する属性があります。

EC2 インスタンスから自動で割り当てられたパブリック IP アドレスを手動でインスタンスに関連付ける、または、関連付け解除することはできません。EC2 インスタンスがパブリック IP アドレスを受信するかどうかをコントロールするには、以下のいずれかのの方法を使用します。

- サブネットのパブリック IP アドレス指定属性を変更する。詳細については、「Amazon VPC ユーザーガイド」の「サブネットのパブリック IPv4 アドレス指定属性の変更」を参照してください。
- 起動時にパブリック IP アドレス指定属性機能を有効または無効にします。これにより、サブネットのパブリック IP アドレス指定属性が上書きされます。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの起動時にパブリック IPv4 アドレスを割り当てる」を参照してください。 Amazon EC2

詳細については、「Amazon EC2 ユーザーガイド」の「パブリック IPv4 アドレスと外部 DNS ホスト名」を参照してください。

EC2 インスタンスが Elastic IP アドレスに関連付けられている場合、EC2 インスタンスはインターネットからアクセスできます。インスタンスまたはネットワークインターフェイスから Elastic IP アドレスの関連付けをいつでも解除できます。Elastic IP アドレスの関連付けを解除するには、「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスの関連付けを解除する」を参照してください。 Amazon EC2

[EC2.10] Amazon EC2 サービス用に作成された VPC エンドポイントを使用するようにAmazon EC2 を設定することをお勧めします

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)

カテゴリ: 保護 > セキュアなネットワーク設定 > API プライベートアクセス

重要度: 中

リソースタイプ: `AWS::EC2::VPC`

AWS Config ルール: `service-vpc-endpoint-enabled`

スケジュールタイプ: 定期的

パラメータ:

- `serviceName`: `ec2` (カスタマイズ不可)

このコントロールは、Amazon EC2 のサービスエンドポイントが各 VPC に対して作成しているかどうかをチェックします。VPC に Amazon EC2 サービス用に作成した VPC エンドポイントがない場合、コントロールは失敗します。

このコントロールは、単一のアカウントのリソースを評価します。アカウント外のリソースは記述できません。 AWS Config と Security Hub はクロスアカウントチェックを行わないため、アカウント間で共有されている VPCsの検出`FAILED`結果が表示されます。Security Hub では、これらの `FAILED` 結果を抑制することを推奨します。

VPC のセキュリティ体制を強化するために、インターフェイス VPC エンドポイントを使用するように Amazon EC2 を設定できます。インターフェイスエンドポイントは AWS PrivateLink、Amazon EC2 API オペレーションにプライベートにアクセスできるテクノロジーである を利用しています。これは、VPC と Amazon EC2 間のすべてのネットワークトラフィックを Amazon ネットワークに限定します。エンドポイントは同じリージョンでのみサポートされるため、別のリージョンの VPC とサービス間にエンドポイントを作成することはできません。これにより、他のリージョンへの意図しない Amazon EC2 API コールを防ぐことができます。

Amazon EC2 用の VPC エンドポイントの作成の詳細については、Amazon EC2 ユーザーガイド」の「Amazon EC2 とインターフェイス VPC エンドポイントAmazon EC2」を参照してください。

修正

Amazon VPC コンソールから Amazon EC2 へのインターフェイスエンドポイントを作成するには、「AWS PrivateLink ガイド」の「VPC エンドポイントを作成する」を参照してください。[サービス名] で [com.amazonaws.*region*.ec2] を選択します。

また、エンドポイントポリシーを作成し、VPC エンドポイントにアタッチして Amazon EC2 API へのアクセスを制御することもできます。VPC エンドポイントポリシーの作成手順については、「Amazon EC2 ユーザーガイド」の「エンドポイントポリシーの作成」を参照してください。 Amazon EC2

[EC2.12] 未使用の Amazon EC2 EIP を削除することをお勧めします

関連する要件: PCI DSS v3.2.1/2.4、NIST.800-53.r5 CM-8(1)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 低

リソースタイプ: `AWS::EC2::EIP`

AWS Config ルール : `eip-attached`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、VPC に割り当てられた Elastic IP (EIP) アドレスが、 EC2 インスタンスまたは使用中の Elastic Network Interface (ENI) にアタッチされているかどうかを確認します。

検出に失敗した場合は、未使用の EC2 EIP がある可能性があります。

これにより、カード所有者データ環境 (CDE) 内の EIP のアセットインベントリを正確な状態に維持できます。

未使用の EIP をリリースするには、「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスを解放する」を参照してください。 Amazon EC2

[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります

関連する要件： CIS AWS Foundations Benchmark v1.2.0/4.1、PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/2.2.2、NIST.800-53.r5 AC-4、NIST.800-53.r5

AC-4(21)、NIST.800-53.r5 CM-7、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(SC-7 SC-72

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ: `AWS::EC2::SecurityGroup`

AWS Config ルール : `restricted-ssh`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon EC2 セキュリティグループが 0.0.0.0/0 または ::/0 からポート 22 への入力を許可しているかどうかをチェックします。セキュリティグループが 0.0.0.0/0 または ::/0 からポート 22 への入力を許可している場合、コントロールは失敗します。

セキュリティグループは、 AWS リソースへの入力および出力ネットワークトラフィックのステートフルフィルタリングを提供します。セキュリティグループはポート 22 への無制限の入力を許可しません。SSH などのリモートコンソールサービスへの自由な接続を制限することにより、サーバーがリスクにさらされることを軽減できます。

修正

ポート 22 への進入を禁止するには、VPC に関連付けられている各セキュリティグループにそのようなアクセスを許可するルールを削除します。手順については、「Amazon EC2 ユーザーガイド」の「セキュリティグループルールの更新」を参照してください。 Amazon EC2 Amazon EC2 コンソールでセキュリティグループを選択したら、アクション、インバウンドルールの編集 を選択します。ポート 22 へのアクセスを許可するルールを削除します。

[EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります

関連する要件： CIS AWS Foundations Benchmark v1.2.0/4.2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ: `AWS::EC2::SecurityGroup`

AWS Config ルール： `restricted-common-ports` (作成されたルールは `restricted-rdp`)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon EC2 セキュリティグループが 0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しているかどうかをチェックします。セキュリティグループが 0.0.0.0/0 または ::/0 からポート 3389 への入力を許可している場合、コントロールは失敗します。

セキュリティグループは、 AWS リソースへの入力および出力ネットワークトラフィックのステートフルフィルタリングを提供します。セキュリティグループはポート 3389 への無制限の入力を許可しません。RDP などのリモートコンソールサービスへの自由な接続を制限することにより、サーバーがリスクにさらされることを軽減できます。

修正

ポート 3389 への進入を禁止するには、VPC に関連付けられている各セキュリティグループにそのようなアクセスを許可するルールを削除します。手順については、「Amazon VPC ユーザーガイド」の「セキュリティグループのルールの更新」を参照してください。Amazon VPC コンソールでセキュリティグループを選択したら、[アクション、インバウンドルールの編集] を選択します。ポート 3389 へのアクセスを許可するルールを削除します。

[EC2.15] Amazon EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないことをお勧めします

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ： 保護 > ネットワークセキュリティ

重要度: 中

リソースタイプ: `AWS::EC2::Subnet`

AWS Config ルール : `subnet-auto-assign-public-ip-disabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon Virtual Private Cloud (Amazon VPC) サブネット内のパブリック IP の割り当ての `MapPublicIpOnLaunch` が `FALSE` に設定されているかチェックします。フラグが `FALSE` に設定されている場合、コントロールは成功します。

すべてのサブネットには、サブネット内に作成されたネットワークインターフェイスが自動的にパブリック IPv4 アドレスを受信するかどうかを判断する属性があります。この属性が有効になっているサブネットで起動されるインスタンスには、プライマリアネットワークインターフェイスに割り当てられるパブリック IP アドレスが割り当てられます。

修正

パブリック IP アドレスを割り当てないようにサブネットを設定するには、「Amazon VPC ユーザーガイド」の「サブネットのパブリック IPv4 アドレス指定属性の変更」を参照してください。[パブリック IPv4 アドレスの自動割り当てを有効にする] チェックボックスをオフにします。

[EC2.16] 未使用のネットワークアクセスコントロールリストを削除することをお勧めします

関連する要件: NIST.800-53.r5 CM-8(1)

カテゴリ： 保護 > ネットワークセキュリティ

重要度: 低

リソースタイプ: `AWS::EC2::NetworkAcl`

AWS Config ルール : `vpc-network-acl-unused-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Virtual Private Cloud (VPC) に未使用のネットワークアクセスコントロールリスト (ネットワーク ACLsがあるかどうかを確認します。ネットワーク ACL がサブネットに関連付けられていない場合、コントロールは失敗します。コントロールは、未使用のデフォルトネットワーク ACL の検出結果を生成しません。

コントロールは、リソース `AWS::EC2::NetworkAcl` の項目設定をチェックして、ネットワーク ACL の関係を判断します。

唯一の関係がネットワーク ACL の VPC である場合、コントロールは失敗します。

他の関係がリスト済みの場合、コントロールは成功します。

修正

未使用のネットワーク ACL を削除する方法については、「Amazon VPC ユーザーガイド」の「ネットワーク ACL の削除」を参照してください。デフォルトのネットワーク ACL またはサブネットに関連付けられた ACL は削除できません。

[EC2.17] Amazon EC2 インスタンスが複数の ENI を使用しないようにすることをお勧めします

関連する要件: NIST.800-53.r5 AC-4(21)

カテゴリ： 保護 > ネットワークセキュリティ

重要度: 低

リソースタイプ: `AWS::EC2::Instance`

AWS Config ルール : `ec2-instance-multiple-eni-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `Adapterids` - EC2 インスタンスに添付済みのネットワークインターフェイス ID のリスト (カスタマイズ不可)

このコントロールは、EC2 インスタンスが複数の Elastic Network Interface (ENI) または Elastic Fabric Adapter (EFA) を使用しているかどうかをチェックします。このコントロールは、単一のネットワークアダプタが使用されている場合に成功します。コントロールには、許可された ENI を識別するためのオプションのパラメータリストが含まれています。Amazon EKS クラスターに属する EC2 インスタンスが複数の ENI を使用している場合も、このコントロールは失敗します。EC2 インスタンスに Amazon EKS クラスターの一部として複数の ENI が必要な場合は、これらのコントロールの検出結果を抑制できます。

複数の ENI の使用は、デュアルホームインスタンス (複数のサブネットを持つインスタンス) を引き起こす可能性があります。これにより、ネットワークセキュリティの複雑性が増し、意図しないネットワークパスとアクセスが導入する可能性があります。

修正

EC2 インスタンスからネットワークインターフェイスをデタッチするには、「Amazon EC2 ユーザーガイド」の「インスタンスからネットワークインターフェイスをデタッチする」を参照してください。 Amazon EC2

[EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします

関連する要件: NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(5)

カテゴリ: 保護 > セキュアなネットワーク設定 > セキュリティグループの設定

重要度: 高

リソースタイプ: `AWS::EC2::SecurityGroup`

AWS Config ルール : `vpc-sg-open-only-to-authorized-ports`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`authorizedTcpPorts`	許可されている TCP ポートのリスト	IntegerList（最大 32 項目）	`1-65535`	`[80,443]`
`authorizedUdpPorts`	許可されている UDP ポートのリスト	IntegerList（最大 32 項目）	`1-65535`	デフォルト値なし

このコントロールは、Amazon EC2 セキュリティグループが、許可されていないポートからの無制限の着信トラフィックを許可しているかどうかをチェックします。コントロールのステータスは次のように決定されます。

- `authorizedTcpPorts` のデフォルト値を使用する場合、セキュリティグループがポート 80 およびポート 443 以外のポートからの無制限の着信トラフィックを許可すると、コントロールは失敗します。
- `authorizedTcpPorts` または `authorizedUdpPorts` にカスタム値を指定した場合、セキュリティグループがリストにないポートからの無制限の着信トラフィックを許可すると、コントロールは失敗します。
- パラメータを使用しない場合、無制限のインバウンドトラフィックルールを持つセキュリティグループに対してコントロールが失敗します。

セキュリティグループは、 AWSへの入力および出力ネットワークトラフィックのステートフルフィルタリングを提供します。セキュリティグループのルールは、最小特権アクセスのプリンシパルに従う必要があります。無制限アクセス (/0 サフィックスを持つ IP アドレス) は、ハッキング、 denial-of-service 攻撃、データ損失などの悪意のあるアクティビティの機会を増やします。ポートが特別に許可されていない限り、ポートは無制限アクセスを拒否する必要があります。

修正

セキュリティグループを変更するには、「Amazon VPC ユーザーガイド」の「セキュリティグループの操作」を参照してください。

[EC2.19] セキュリティグループは、リスクの高いポートへの無制限アクセスを許可してはいけません

関連する要件: NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-7、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(5)

カテゴリ: 保護 > 制限付きネットワークアクセス

重要度: 非常事態

リソースタイプ: `AWS::EC2::SecurityGroup`

AWS Config ルール： `restricted-common-ports` (作成されたルールは `vpc-sg-restricted-common-ports`)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: `"blockedPorts": "20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,560` (カスタマイズ不可)

このコントロールは、指定した高リスクと見なされるポートに Amazon EC2 セキュリティグループの無制限の受信トラフィックがアクセス可能かどうかをチェックします。セキュリティグループ内のルールがこれらのポートへの「0.0.0.0/0」または「::/0」からの入力トラフィックを許可している場合、このコントロールは失敗します。

セキュリティグループは、 AWS リソースへの入力および出力ネットワークトラフィックのステートフルフィルタリングを提供します。無制限アクセス (0.0.0.0/0) は、ハッキング、 denial-of-service 攻撃、データ損失などの悪意のあるアクティビティの機会を増やします。どのセキュリティグループでも、以下のポートへの無制限の入力アクセスを許可してはいけません。

- 20、21 (FTP)
- 22 (SSH)
- 23 (Telnet)
- 25 (SMTP)
- 110 (POP3)
- 135 (RPC)
- 143 (IMAP)
- 445 (CIFS)
- 1433、1434 (MSSQL)
- 3000 (Go、Node.js、および Ruby のウェブ開発フレームワーク)
- 3306 (mySQL)
- 3389 (RDP)
- 4333 (ahsp)
- 5000 (Python ウェブ開発フレームワーク)
- 5432 (postgresql)
- 5500 (fcp-addr-srvr1)
- 5601 (OpenSearch ダッシュボード)
- 8080 (proxy)
- 8088 (レガシー HTTP ポート)

- 8888 (代替 HTTP ポート)
- 9200 または 9300 (OpenSearch)

修正

セキュリティグループからルールを削除するには、「Amazon EC2 ユーザーガイド」の「セキュリティグループからルールを削除する」を参照してください。 Amazon EC2

[EC2.20] AWS Site-to-Site VPN 接続の両方の VPN トンネルが稼働している必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ :`AWS::EC2::VPNConnection`

AWS Config ルール : `vpc-vpn-2-tunnels-up`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

VPN トンネルは、顧客ネットワークから AWS Site-to-Site VPN 接続 AWS との間でデータを渡すことができる暗号化されたリンクです。各 VPN 接続には、高可用性のために同時に使用できる 2 つの VPN トンネルが含まれています。 AWS VPC とリモートネットワーク間の安全で可用性の高い接続を確認するには、両方の VPN トンネルが VPN 接続用に稼働していることを確認することが重要です。

このコントロールは、 AWS Site-to-Site VPN によって提供される両方の VPN トンネルが UP ステータスであることを確認します。一方または両方のトンネルのステータスが DOWN の場合、コントロールは失敗します。

修正

VPN トンネルオプションを変更するには、「Site-to-Site VPN ユーザーガイド」の「Site-to-Site VPN トンネルオプションの変更」を参照してください。 AWS

[EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります

関連する要件： CIS AWS Foundations Benchmark v1.4.0/5.1、CIS AWS Foundations Benchmark v3.0.0/5.1、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-7、NIST.800-53.r5 SC-7SC-7(21)、NIST.800-53.r5 SC-7(5)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ :`AWS::EC2::NetworkAcl`

AWS Config ルール : `nacl-no-unrestricted-ssh-rdp`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、ネットワークアクセスコントロールリスト (ネットワーク ACL) が SSH/RDP イングレストラフィックのデフォルトの TCP ポートへの無制限アクセスを許可しているかどうかをチェックします。ネットワーク ACL インバウンドエントリが TCP ポート 22 または 3389 に対してソース CIDR ブロック「0.0.0.0/0」または「::/0」を許可している場合、コントロールは失敗します。コントロールは、デフォルトのネットワーク ACL の検出結果を生成しません。

ポート 22 (SSH) やポート 3389 (RDP) などのリモートサーバー管理ポートへのアクセスは、VPC 内のリソースへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

修正

ネットワーク ACL トラフィックルールを編集するには、「Amazon VPC ユーザーガイドACLs の操作」を参照してください。

[EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします

> **Important**
>
> 特定の標準から廃止 – Security Hub は、2023 年 9 月 20 日に AWS Foundational Security Best Practices 標準および NIST SP 800-53 Rev. 5 からこのコントロールを削除しま

した。このコントロールは、引き続きサービスマネージドスタンダード: の一部です AWS Control Tower。この コントロールでは、セキュリティグループが EC2 インスタンス、または Elastic Network Interface にアタッチされている場合に、合格の検出結果を生成します。ただし、特定のユースケースでは、セキュリティグループがアタッチされていなくてもセキュリティ上のリスクはありません。他の EC2 コントロール (EC2.2、EC2.13、EC2.14、EC2.18、EC2.19 など) を使用すると、セキュリティグループをモニタリングできます。

カテゴリ: 識別 > インベントリ

重要度: 中

リソースタイプ:`AWS::EC2::NetworkInterface`、`AWS::EC2::SecurityGroup`

AWS Config ルール: `ec2-security-group-attached-to-eni-periodic`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、セキュリティグループが Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは Elastic Network Interface にアタッチされているかどうかを確認します。セキュリティグループが Amazon EC2 インスタンスまたは Elastic Network Interface に関連付けられていない場合、コントロールは失敗します。

修正

セキュリティグループを作成、割り当て、削除するには、「Amazon EC2 ユーザーガイド」の「セキュリティグループ」を参照してください。

[EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします

関連する要件: NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ :`AWS::EC2::TransitGateway`

AWS Config ルール : ec2-transit-gateway-auto-vpc-attach-disabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、EC2 中継ゲートウェイが共有 VPC アタッチメントを自動的に受け入れているかどうかをチェックします。中継ゲートウェイが共有 VPC アタッチメントリクエストを自動的に受け入れていると、このコントロールは失敗します。

AutoAcceptSharedAttachments をオンにすると、中継ゲートウェイは、リクエストまたはアタッチメントの発信元であるアカウントを確認せずに、クロスアカウント VPC アタッチメントリクエストを自動的に受け入れるように設定されます。認可および認証のベストプラクティスに従うため、この機能はオフにして、認証された VPC アタッチメントリクエストのみを受け入れることが推奨されます。

修正

中継ゲートウェイを変更するには、「Amazon VPC デベロッパーガイド」の「中継ゲートウェイの変更」を参照してください。

[EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします

関連する要件: NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 中

リソースタイプ :AWS::EC2::Instance

AWS Config ルール : ec2-paravirtual-instance-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、EC2 インスタンスの仮想化タイプが準仮想化かどうかをチェックします。EC2 インスタンスの virtualizationType が paravirtual に設定されている場合、このコントロールは失敗します。

Linux Amazon マシンイメージ (AMI)では、2 つの仮想化タイプ、準仮想化 (PV) とハードウェア仮想化 (HVM) のうち、いずれかを使用します。PV AMI と HVM AMI の主な違いは、起動の方法と、パ

フォーマンス向上のための特別なハードウェア拡張機能 (CPU、ネットワーク、ストレージ) を利用できるかどうかという点です。

従来、PV のゲストは HVM のゲストよりも多くの場合にパフォーマンスが向上しました。ただし、HVM 仮想化の機能強化や HVM AMI で PV ドライバが利用可能になったことにより、このようなパフォーマンスの向上はなくなりました。詳細については、Amazon EC2 ユーザーガイド」の「Linux AMI 仮想化タイプ」を参照してください。

修正

EC2 インスタンスを新しいインスタンスタイプに更新するには、「Amazon EC2 ユーザーガイド」の「インスタンスタイプを変更する」を参照してください。 Amazon EC2

[EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 高

リソースタイプ :`AWS::EC2::LaunchTemplate`

AWS Config ルール : `ec2-launch-template-public-ip-disabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon EC2 起動テンプレートが起動の際にネットワークインターフェイスにパブリック IP アドレスを割り当てる設定になっていないかをチェックします。EC2 起動テンプレートがネットワークインターフェイスにパブリック IP アドレスを割り当てる設定になっている場合、またはパブリック IP アドレスを持つネットワークインターフェイスが 1 つ以上ある場合、コントロールは失敗します。

パブリック IP アドレスは、インターネットから到達可能な IP アドレスです。パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイス

に関連付けられたリソースは、インターネットからアクセスできる可能性があります。EC2 リソースへのパブリックアクセスを可能にすべきではありません。ワークロードへの意図しないアクセスが可能になるおそれがあるためです。

修正

EC2 起動テンプレートを更新するには、「Amazon EC2 Auto Scaling ユーザーガイド」の「デフォルトのネットワークインターフェイス設定を変更する」を参照してください。

[EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

重要度: 低

リソースタイプ: `AWS::EC2::Volume`

AWS Config ルール： `ebs-resources-protected-by-backup-plan`

スケジュールタイプ: 定期的

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`backupVaultLockCheck`	パラメータが に設定`true`され、リソースが AWS Backup ボールトロックを使用する場合、コントロールは`PASSED`結果を生成します。	ブール値	`true` 、、または `false`	デフォルト値なし

このコントロールは、`in-use` 状態の Amazon EBS ボリュームがバックアッププランの対象になっているかどうかを評価します。EBS ボリュームがバックアッププランの対象でない場合、コントロールは失敗します。`backupVaultLockCheck` パラメータを に設定すると`true`、EBS ボリュー

ムが AWS Backup ロックされたボールトにバックアップされている場合にのみコントロールが成功します。

バックアップは、セキュリティインシデントからより迅速に復元するために役立ちます。また、システムの耐障害性を強化します。バックアッププランに Amazon EBS ボリュームを含めると、意図しない損失や削除からデータを保護できます。

修正

Amazon EBS ボリュームを AWS Backup バックアッププランに追加するには、「 AWS Backup デベロッパーガイド」の「バックアッププランへのリソースの割り当て」を参照してください。

[EC2.33] EC2 トランジットゲートウェイアタッチメントにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::TransitGatewayAttachment`

AWS Config ルール: `tagged-ec2-transitgatewayattachment` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon EC2 トランジットゲートウェイアタッチメントに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。Transit Gateway アタッチメントにタグキーがない場合、またはパラメータ で指定されたすべてのキーがな

い場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、トランジットゲートウェイアタッチメントにどのキーもタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EC2 Transit Gateway アタッチメントにタグを追加するには、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付けるAmazon EC2」を参照してください。

[EC2.34] EC2 トランジットゲートウェイルートテーブルにタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::TransitGatewayRouteTable`

AWS Config ルール: `tagged-ec2-transitgatewayroutetable` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon EC2 トランジットゲートウェイルートテーブルに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。Transit Gateway ルートテーブルにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、トランジットゲートウェイルートテーブルにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC AWSとは」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベ

ストプラクティスの詳細については、「」の「AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EC2 Transit Gateway ルートテーブルにタグを追加するには、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付けるAmazon EC2」を参照してください。

[EC2.35] EC2 ネットワークインターフェイスにタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::NetworkInterface`

AWS Config ルール: `tagged-ec2-networkinterface` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon EC2 ネットワークインターフェイスに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。ネットワークインターフェイスにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、ネットワークインターフェイスにキーが

タグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EC2 ネットワークインターフェイスにタグを追加するには、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付けるAmazon EC2」を参照してください。

[EC2.36] EC2 カスタマーゲートウェイにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::CustomerGateway`

AWS Config ルール: `tagged-ec2-customergateway` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon EC2 カスタマーゲートウェイに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。カスタマーゲートウェイにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、カスタマーゲートウェイにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EC2 カスタマーゲートウェイにタグを追加するには、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付けるAmazon EC2」を参照してください。

[EC2.37] EC2 Elastic IP アドレスにタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::EIP`

AWS Config ルール: `tagged-ec2-eip` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon EC2 Elastic IP アドレスに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。Elastic IP アドレスにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、Elastic IP アドレスにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセス

コントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EC2 Elastic IP アドレスにタグを追加するには、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付けるAmazon EC2」を参照してください。

[EC2.38] EC2 インスタンスにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::Instance`

AWS Config ルール: `tagged-ec2-instance` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーで	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	は、大文字と小文字が区別されます。			

このコントロールは、Amazon EC2 インスタンスにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。インスタンスにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、インスタンスにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EC2 インスタンスにタグを追加するには、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付けるAmazon EC2」を参照してください。

[EC2.39] EC2 インターネットゲートウェイにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::InternetGateway`

AWS Config ルール: `tagged-ec2-internetgateway` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon EC2 インターネットゲートウェイに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。インターネットゲートウェイにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、インターネットゲートウェイにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できま

す。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EC2 インターネットゲートウェイにタグを追加するには、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付けるAmazon EC2」を参照してください。

[EC2.40] EC2 NAT ゲートウェイにタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::NatGateway`

AWS Config ルール: `tagged-ec2-natgateway` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon EC2 ネットワークアドレス変換 (NAT) ゲートウェイに、パラメータ で定義された特定のキーを持つタグがあるかどうかを確認しますrequiredTagKeys。NAT ゲートウェイにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、NAT ゲートウェイにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EC2 NAT ゲートウェイにタグを追加するには、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付けるAmazon EC2」を参照してください。

[EC2.41] EC2 ネットワーク ACLs にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::NetworkAcl`

AWS Config ルール: `tagged-ec2-networkacl` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon EC2 ネットワークアクセスコントロールリスト (ネットワーク ACL) に、パラメータ で定義された特定のキーを持つタグがあるかどうかを確認しますrequiredTagKeys。ネットワーク ACL にタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、ネットワーク ACL にキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベ

ストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EC2 ネットワーク ACL にタグを追加するには、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付けるAmazon EC2」を参照してください。

[EC2.42] EC2 ルートテーブルにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::RouteTable`

AWS Config ルール: `tagged-ec2-routetable` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon EC2 ルートテーブルに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。ルートテーブルにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、ルートテーブルにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EC2 ルートテーブルにタグを追加するには、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付けるAmazon EC2」を参照してください。

[EC2.43] EC2 セキュリティグループにタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::SecurityGroup`

AWS Config ルール: `tagged-ec2-securitygroup` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon EC2 セキュリティグループにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。セキュリティグループにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、セキュリティグループにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EC2 セキュリティグループにタグを追加するには、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付けるAmazon EC2」を参照してください。

[EC2.44] EC2 サブネットにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::Subnet`

AWS Config ルール: `tagged-ec2-subnet` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon EC2 サブネットにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。サブネットにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、サブネットにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセス

コントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EC2 サブネットにタグを追加するには、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付けるAmazon EC2」を参照してください。

[EC2.45] EC2 ボリュームにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::Volume`

AWS Config ルール: `tagged-ec2-subnet` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーで	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	は、大文字と小文字が区別されます。			

このコントロールは、Amazon EC2 ボリュームにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。ボリュームにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、ボリュームにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EC2 ボリュームにタグを追加するには、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付けるAmazon EC2」を参照してください。

[EC2.46] Amazon VPCsにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::VPC`

AWS Config ルール: `tagged-ec2-vpc` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon Virtual Private Cloud (Amazon VPC) に、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。Amazon VPC にタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、Amazon VPC にキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できま

す。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

VPC にタグを追加するには、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付けるAmazon EC2」を参照してください。

[EC2.47] Amazon VPC エンドポイントサービスにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::VPCEndpointService`

AWS Config ルール: `tagged-ec2-vpcendpointservice` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon VPC エンドポイントサービスに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。エンドポイントサービスにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、エンドポイントサービスがキーでタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Amazon VPC エンドポイントサービスにタグを追加するには、「 AWS PrivateLink ガイド」の「エンドポイントサービスの設定」セクションの「タグの管理」を参照してください。 https://docs.aws.amazon.com/vpc/latest/privatelink/configure-endpoint-service.html

[EC2.48] Amazon VPC フローログにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: AWS::EC2::FlowLog

AWS Config ルール: `tagged-ec2-flowlog` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon VPC フローログに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。フローログにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、フローログにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベ

ストプラクティスの詳細については、「」の「AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Amazon VPC フローログにタグを追加するには、「Amazon VPC ユーザーガイド」の「フローログにタグを付ける」を参照してください。

[EC2.49] Amazon VPC ピアリング接続にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::VPCPeeringConnection`

AWS Config ルール: `tagged-ec2-vpcpeeringconnection` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon VPC ピアリング接続に、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。ピアリング接続にタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、ピアリング接続にキーのタグが付けられていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Amazon VPC ピアリング接続にタグを追加するには、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付ける」を参照してください。 Amazon EC2

[EC2.50] EC2 VPN ゲートウェイにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::VPNGateway`

AWS Config ルール: `tagged-ec2-vpngateway` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon EC2 VPN ゲートウェイにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。VPN ゲートウェイにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、VPN ゲートウェイにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EC2 VPN ゲートウェイにタグを追加するには、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付けるAmazon EC2」を参照してください。

[EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります

関連する要件: NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 AU-9(7)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 低

リソースタイプ: `AWS::EC2::ClientVpnEndpoint`

AWS Config ルール： `ec2-client-vpn-connection-log-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS Client VPN エンドポイントでクライアント接続のログ記録が有効になっているかどうかをチェックします。エンドポイントでクライアント接続ログ記録が有効になっていない場合、コントロールは失敗します。

Client VPN エンドポイントにより、リモートクライアントは AWSの仮想プライベートクラウド (VPC) 内のリソースに安全に接続できます。接続ログにより、VPN エンドポイントでのユーザーアクティビティを追跡し、可視化することができます。接続ログを有効にすると、ロググループ内のログストリームの名前を指定できます。ログストリームを指定しない場合、クライアント VPN サービスによって自動的に作成されます。

修正

接続ログ記録を有効にするには、「AWS Client VPN 管理者ガイド」の「既存のクライアント VPN エンドポイントの接続ログを有効にする」を参照してください。

[EC2.52] EC2 トランジットゲートウェイにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EC2::TransitGateway`

AWS Config ルール: `tagged-ec2-transitgateway` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、Amazon EC2 トランジットゲートウェイにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。Transit Gateway にタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、トランジットゲートウェイにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できま

す。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EC2 トランジットゲートウェイにタグを追加するには、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付けるAmazon EC2」を参照してください。

[EC2.53] EC2 セキュリティグループは、0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可しないでください

関連する要件： CIS AWS Foundations Benchmark v3.0.0/5.2

カテゴリ: 保護 > セキュアなネットワーク設定 > セキュリティグループの設定

重要度: 高

リソースタイプ: `AWS::EC2::SecurityGroup`

AWS Config ルール: `vpc-sg-port-restriction-check`

スケジュールタイプ: 定期的

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`ipType`	IP バージョン	文字列	カスタマイズ不可	`IPv4`

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`restrictPorts`	イングレストラフィックを拒否するポートのリスト	IntegerList	カスタマイズ不可	`22,3389`

このコントロールは、Amazon EC2 セキュリティグループが 0.0.0.0/0 からリモートサーバー管理ポート (ポート 22 および 3389) への入力を許可しているかどうかをチェックします。セキュリティグループが 0.0.0.0/0 からポート 22 または 3389 への入力を許可している場合、コントロールは失敗します。

セキュリティグループは、 AWS リソースへの入出力ネットワークトラフィックをステートフルにフィルタリングします。TDP (6)、UDP (17)、または ALL (-1) プロトコルのいずれかを使用して、ポート 22 への SSH やポート 3389 への RDP などのリモートサーバー管理ポートへの無制限の進入アクセスをセキュリティグループで許可しないことをお勧めします。これらのポートへのパブリックアクセスを許可すると、リソースアタックサーフェスが増加し、リソースが侵害されるリスクが高まります。

修正

指定されたポートへの進入トラフィックを禁止するように EC2 セキュリティグループルールを更新するには、「Amazon EC2 ユーザーガイド」の「セキュリティグループルールの更新」を参照してください。 Amazon EC2 Amazon EC2 コンソールでセキュリティグループを選択したら、アクション、インバウンドルールの編集 を選択します。ポート 22 またはポート 3389 へのアクセスを許可するルールを削除します。

[EC2.54] EC2 セキュリティグループは、::/0 からリモートサーバー管理ポートへの入力を許可しないでください

関連する要件： CIS AWS Foundations Benchmark v3.0.0/5.3

カテゴリ: 保護 > セキュアなネットワーク設定 > セキュリティグループの設定

重要度: 高

リソースタイプ: `AWS::EC2::SecurityGroup`

AWS Config ルール: `vpc-sg-port-restriction-check`

スケジュールタイプ: 定期的

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`ipType`	IP バージョン	文字列	カスタマイズ不可	`IPv6`
`restrictPorts`	イングレストラフィックを拒否するポートのリスト	IntegerList	カスタマイズ不可	`22,3389`

このコントロールは、Amazon EC2 セキュリティグループが ::/0 からリモートサーバー管理ポート (ポート 22 および 3389) への入力を許可しているかどうかをチェックします。セキュリティグループが ::/0 からポート 22 または 3389 への入力を許可している場合、コントロールは失敗します。

セキュリティグループは、 AWS リソースへの入出力ネットワークトラフィックをステートフルにフィルタリングします。TDP (6)、UDP (17)、または ALL (-1) プロトコルのいずれかを使用して、ポート 22 への SSH やポート 3389 への RDP などのリモートサーバー管理ポートへの無制限の進入アクセスをセキュリティグループで許可しないことをお勧めします。これらのポートへのパブリックアクセスを許可すると、リソースアタックサーフェスが増加し、リソースが侵害されるリスクが高まります。

修正

指定されたポートへの進入トラフィックを禁止するように EC2 セキュリティグループルールを更新するには、「Amazon EC2 ユーザーガイド」の「セキュリティグループルールの更新」を参照してください。 Amazon EC2 Amazon EC2 コンソールでセキュリティグループを選択したら、アクション、インバウンドルールの編集 を選択します。ポート 22 またはポート 3389 へのアクセスを許可するルールを削除します。

Amazon EC2 Auto Scaling コントロール

これらのコントロールは Amazon EC2 Auto Scaling リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要があります

関連する要件: PCI DSS v3.2.1/2.2、NIST.800-53.r5 CA-7、NIST.800-53.r5 CP-2(2)、NIST.800-53.r5 SI-2

カテゴリ: 識別 > インベントリ

重要度: 低

リソースタイプ: `AWS::AutoScaling::AutoScalingGroup`

AWS Config ルール : `autoscaling-group-elb-healthcheck-required`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、ロードバランサーに関連付けられている Amazon EC2 Auto Scaling グループが Elastic Load Balancing (ELB) ヘルスチェックを使用しているかどうかをチェックします。Auto Scaling グループが ELB ヘルスチェックを使用しない場合、コントロールは失敗します。

ELB ヘルスチェックは、Auto Scaling グループがロードバランサーによって提供される追加のテストに基づいてインスタンスのヘルスを判断できるようにするのに役立ちます。Elastic Load Balancing ヘルスチェックを使用すると、EC2 Auto Scaling グループを使用するアプリケーションの可用性もサポートできます。

修正

Elastic Load Balancing ヘルスチェックを追加するには、「Amazon EC2 Auto Scaling ユーザーガイド」の「Elastic Load Balancing のヘルスチェックを追加する」を参照してください。

〔AutoScaling.2] Amazon EC2 Auto Scaling グループは複数のアベイラビリティーゾーンをカバーする必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-2(2)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::AutoScaling::AutoScalingGroup`

AWS Config ルール : autoscaling-multiple-az

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値	
minAvailabilityZones	アベイラビリティーゾーンの最小数	列挙型	2, 3, 4, 5, 6	2	

このコントロールは、Amazon EC2 Auto Scaling グループが少なくとも指定された数のアベイラビリティーゾーン (AZ) にまたがっているかどうかをチェックします。Auto Scaling グループが少なくとも指定された数の AZ にまたがっていない場合、コントロールは失敗します。AZ の最小数に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 2 つの AZ を使用します。

複数の AZ にまたがらない Auto Scaling グループは、設定された単一の AZ が使用できなくなった場合、埋め合わせとなる別の AZ ではインスタンスを起動できません。ただし、バッチジョブや AZ 内の転送コストを最小限に抑える必要がある場合など、一部のユースケースでは、単一のアベイラビリティーゾーンを持つ Auto Scaling グループが推奨されることがあります。このような場合は、このコントロールを無効にしたり、検出結果を抑制したりすることができます。

修正

既存の Auto Scaling グループに AZ を追加するには、「Amazon EC2 Auto Scaling ユーザーガイド」の「アベイラビリティーゾーンを追加および削除する」を参照してください。

〔AutoScaling.3] Auto Scaling グループの起動設定では、インスタンスメタデータサービスバージョン 2 (IMDSv2) を要求するように EC2 インスタンスを設定する必要がありますIMDSv2

関連する要件: NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ: `AWS::AutoScaling::LaunchConfiguration`

AWS Config ルール : `autoscaling-launchconfig-requires-imdsv2`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon EC2 Auto Scaling グループが起動するすべてのインスタンスで IMDSv2 が有効になっているかどうかをチェックします。インスタンスメタデータサービス (IMDS) のバージョンが起動設定に含まれていない場合、または IMDSv1 と IMDSv2 の両方が有効になっている場合、コントロールは失敗します。

IMDS は、インスタンスに関するデータで、実行中のインスタンスを設定または管理するために使用します。

IMDS のバージョン 2 では、EC2 インスタンスの保護を強化するために、IMDSv1 では利用できなかった新しい保護が追加されています。

修正

Auto Scaling グループは、一度に 1 つの起動設定に関連付けられます。起動設定は、作成後に変更することはできません。Auto Scaling グループの起動設定を変更するには、新しい起動設定のベースとして、既存の起動設定を IMDSv2 を有効にした上で使用します。詳細については、「Amazon EC2 ユーザーガイド」の「新しいインスタンスのインスタンスメタデータオプションを設定する」を参照してください。 Amazon EC2

〔AutoScaling.4] Auto Scaling グループの起動設定には、メタデータレスポンスホップ制限が 1 より大きくないようにしてください

> **Important**
>
> Security Hub は 2024 年 4 月にこのコントロールを廃止しました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ: `AWS::AutoScaling::LaunchConfiguration`

AWS Config ルール : `autoscaling-launch-config-hop-limit`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

これにより、メタデータトークンが移動できる、ネットワークホップの数をチェックします。メタデータの応答ホップ制限が 1 を越えるとコントロールは失敗します。

Instance Metadata Service (IMDS) は、Amazon EC2 インスタンスに関するメタデータ情報を提供するものであり、アプリケーションの設定に役立ちます。メタデータサービスの HTTP PUT 応答を EC2 インスタンスのみに制限することで、IMDS を不正使用から保護します。

IP パケットの Time To Live (TTL) フィールドは、ホップごとに 1 ずつ削減されます。この削減により、パケットを EC2 外に移動させないようにすることができます。IMDSv2 は、オープンルーター、レイヤー 3 ファイアウォール、VPN、トンネル、または NAT デバイスとして誤って構成された可能性のある EC2 インスタンスを保護し、権限のないユーザーがメタデータを取得できないようにします。IMDSv2 では、デフォルトのメタデータ応答ホップ制限が 1 に設定されているため、シークレットトークンを含む PUT 応答は、インスタンスの外に移動することができません。ただし、この値が 1 より大きい場合、トークンは EC2 インスタンスから移動することができます。

修正

既存の起動設定のメタデータレスポンスホップ制限を変更するには、「Amazon EC2 ユーザーガイド」の「既存のインスタンスのインスタンスメタデータオプションの変更」を参照してください。
Amazon EC2

[Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 高

リソースタイプ: `AWS::AutoScaling::LaunchConfiguration`

AWS Config ルール : `autoscaling-launch-config-public-ip-disabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Auto Scaling グループに関連付けられた起動設定が、グループのインスタンスにパブリック IP アドレスを割り当てるかどうかをチェックします。関連付けられた起動設定が、パブリック IP アドレスを割り当てている場合に、このコントロールは失敗します。

Auto Scaling グループの起動設定の Amazon EC2 インスタンスには、限定されたエッジケースを除き、パブリック IP アドレスを関連付けないでください。Amazon EC2 インスタンスは、インターネットに直接公開されるのではなく、ロードバランサーを介した場合のみアクセスできるようにする必要があります。

修正

Auto Scaling グループは、一度に 1 つの起動設定に関連付けられます。起動設定は、作成後に変更することはできません。Auto Scaling グループの起動設定を変更するには、新しい起動設定のベースとして既存の起動設定を使用します。次に、Auto Scaling グループを新しい起動設定を使用するように更新します。 step-by-step 手順については、「Amazon EC2 Auto Scaling ユーザーガイド」の「Auto Scaling グループの起動設定を変更する」を参照してください。 Amazon EC2 Auto Scaling 新しい起動設定を作成する際、[追加設定] にある [高度な詳細] の [IP アドレスタイプ] で、[どのインスタンスにもパブリック IP アドレスを割り当てない] を選択します。

起動設定を変更すると、Auto Scaling は、新しいインスタンスを新しい設定オプションで起動します。既存のインスタンスは影響を受けません。既存のインスタンスを更新するには、インスタンスの更新を行うか、終了ポリシーに基づいて自動スケーリングで古いインスタンスを新しいインスタンスに徐々に置き換えるようにすることをお勧めします。Auto Scaling インスタンスの更新についての詳細は、「Amazon EC2 Auto Scaling ユーザーガイド」の「Auto Scaling インスタンスの更新」を参照してください。

〔AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-2(2)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::AutoScaling::AutoScalingGroup`

AWS Config ルール : `autoscaling-multiple-instance-types`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon EC2 Auto Scaling グループが複数のインスタンスタイプを使用しているかどうかをチェックします。Auto Scaling グループで 1 つのインスタンスタイプしか定義されていない場合、そのコントロールは失敗します。

複数のアベイラビリティーゾーンで実行されている複数のインスタンスタイプ間でアプリケーションをデプロイすることで、可用性を向上させることができます。Security Hub では、選択したアベイラビリティーゾーンに十分なインスタンス容量がない場合に Auto Scaling グループが別のインスタンスタイプを起動できるよう、複数のインスタンスタイプを使用することが推奨されます。

修正

複数のインスタンスタイプで Auto Scaling グループを作成するには、「Amazon EC2 Auto Scaling ユーザーガイド」の「複数のインスタンスタイプと購入オプションを使用する Auto Scaling グループ」を参照してください。

〔AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 識別 > リソース設定

重要度: 中

リソースタイプ: `AWS::AutoScaling::AutoScalingGroup`

AWS Config ルール : `autoscaling-launch-template`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon EC2 Auto Scaling グループが、EC2 起動テンプレートから作成されたものかどうかを確認します。Amazon EC2 Auto Scaling グループが起動テンプレートを使用して作成されていない場合、または混合インスタンスポリシーで起動テンプレートが指定されていない場合、このコントロールは失敗します。

EC2 Auto Scaling グループは、EC2 起動テンプレートまたは起動設定のいずれかから作成できます。ただし、起動テンプレートを使用して Auto Scaling グループを作成することで、最新の機能や改善点に確実にアクセスできます。

修正

EC2 起動テンプレートを使用して Auto Scaling グループを作成するには、「Amazon EC2 Auto Scalingユーザーガイド」の「起動テンプレートを使用して Auto Scaling グループを作成する」を参照してください。起動設定を起動テンプレートに置き換える方法については、「Amazon EC2 ユーザーガイド」の「起動設定を起動テンプレートに置き換える」を参照してください。 Amazon EC2

〔AutoScaling.10] EC2 Auto Scaling グループにタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::AutoScaling::AutoScalingGroup`

AWS Config ルール: `tagged-autoscaling-autoscalinggroup` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーで	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	は、大文字と小文字が区別されます。			

このコントロールは、Amazon EC2 Auto Scaling グループにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。Auto Scaling グループにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、Auto Scaling グループにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Auto Scaling グループにタグを追加するには、「Amazon EC2 Auto Scaling ユーザーガイド」の「Auto Scaling グループとインスタンスのタグ付け」を参照してください。 Amazon EC2 Auto Scaling

Amazon EC2 Systems Manager コントロール

これらのコントロールは、 によって管理される Amazon EC2 インスタンスに関連しています AWS Systems Manager。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager

関連する要件: PCI DSS v3.2.1/2.4、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-8、NIST.800-53.r5 CM-8(1)、NIST.800-53.r5 CM-8(2)、NIST.800-53.r5 CM-8(3)、NIST.800-53.r5 SA-15(2)、NIST.800-53.r5 SA-15(8)、NIST.800-53.r5 SA-3、NIST.800-53.r5 SI-2(3)

カテゴリ: 識別 > インベントリ

重要度: 中

評価されたリソース: `AWS::EC2::Instance`

必要な AWS Config 記録リソース： `AWS::EC2::Instance`、`AWS::SSM::ManagedInstanceInventory`

AWS Config ルール : `ec2-instance-managed-by-systems-manager`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、アカウントで停止および実行中の EC2 インスタンスが によって管理されているかどうかを確認します AWS Systems Manager。Systems Manager は、インフラストラクチャの表示と制御 AWS のサービス に使用できる です AWS 。

セキュリティとコンプライアンスを維持するために、Systems Manager は停止中および実行中のマネージドインスタンスをスキャンします。マネージドインスタンスとは、Systems Manager で使用するために設定されたマシンです。Systems Manager が検出したポリシー違反について報告または是正処置を講じます。Systems Manager は、マネージドインスタンスの設定と維持管理にも役立ちます。

詳細については、「AWS Systems Manager ユーザーガイド」を参照してください。

修正

Systems Manager を使用して EC2 インスタンスを管理するには、「AWS Systems Manager ユーザーガイド」の「Amazon EC2 ホスト管理」を参照してください。[設定オプション] セクションでは、デフォルトの選択肢をそのまま使用することも、希望の設定に合わせて必要に応じて変更することもできます。

[SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります

関連する要件: PCI DSS v3.2.1/6.2、NIST.800-53.r5 CM-8(3)、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(3)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)

カテゴリ: 検出 > 検出サービス

重要度: 高

リソースタイプ: `AWS::SSM::PatchCompliance`

AWS Config ルール : `ec2-managedinstance-patch-compliance-status-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、インスタンスへのパッチインストール後、Systems Manager パッチコンプライアンスのコンプライアンスステータスが、`COMPLIANT` と `NON_COMPLIANT` のどちらであるかをチェックします。コンプライアンスステータスが `NON_COMPLIANT` の場合、コントロールは失敗します。このコントロールは、Systems Manager Patch Manager によって管理されているインスタンスのみをチェックします。

組織の要求に応じて EC2 インスタンスにパッチを適用すると、 AWS アカウントのアタックサーフェスが低減されます。

修正

Systems Manager では、パッチポリシーを使用して、マネージドインスタンスのパッチ適用を設定することを推奨しています。次の手順で説明するように、Systems Manager のドキュメントを使用してインスタンスにパッチを適用することもできます。

非準拠のパッチを修正するには

1. https://console.aws.amazon.com/systems-manager/ で AWS Systems Manager コンソールを開きます。
2. [ノード管理] で、[コマンドを実行する] を選択し、[コマンドを実行する] を選択します。
3. AWS-RunPatchBaseline のオプションを選択します。
4. [Operation] (オペレーション) を [Install] (インストール) に変更します。
5. [インスタンスを手動で選択する] を選択し、非準拠のインスタンスを選択します。
6. [実行] を選択します。
7. コマンドの完了後に、パッチを適用したインスタンスの新しいコンプライアンスステータスをモニタリングするには、ナビゲーションペインで [コンプライアンス] を選択します。

[SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります

関連する要件: PCI DSS v3.2.1/2.4、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-8、NIST.800-53.r5 CM-8(1)、NIST.800-53.r5 CM-8(3)、NIST.800-53.r5 SI-2(3)

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::SSM::AssociationCompliance`

AWS Config ルール : ec2-managedinstance-association-compliance-status-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS Systems Manager 関連付けコンプライアンスのステータスが `COMPLIANT`であるか、インスタンスで関連付けが実行され`NON_COMPLIANT`た後であるかをチェックします。関連付けのコンプライアンスステータスが `NON_COMPLIANT` の場合、コントロールは失敗します。

State Manager の関連付けは、マネージドインスタンスに割り当てられる設定です。この設定では、インスタンスで維持する状態を定義します。例えば、関連付けでは、アンチウイルスソフトウェアを

インスタンス上にインストールして実行する必要があること、または特定のポートを閉じる必要があることを指定できます。

State Manager の関連付けを 1 つまたは複数作成することで、コンプライアンスステータス情報をすぐに表示できるようになります。コンプライアンスステータスは、コンソールで、または AWS CLI コマンドや対応する Systems Manager API アクションに応答して表示できます。関連付けでは、設定コンプライアンスはコンプライアンスステータスを表示します (`Compliant` または `Non-compliant`)。また、関連付けに割り当てられた `Critical` または `Medium` などの重要度レベルを表示します。

State Manager 関連付けのコンプライアンスの詳細については、「AWS Systems Manager ユーザーガイド」の「State Manager 関連付けのコンプライアンスについて」を参照してください。

修正

失敗した関連付けは、ターゲットや SSM ドキュメント名など、さまざまなものに関連している可能性があります。この問題を修正するには、まず関連付けの履歴を表示し、関連付けを特定して調査する必要があります。関連付けの履歴を表示するには、「AWS Systems Manager ユーザーガイド」の「関連付けの履歴の表示」を参照してください。

調査後、関連付けを編集して特定された問題を修正できます。関連付けを編集して、新しい名前やスケジュール、重要度レベル、ターゲットを指定できます。関連付けを編集すると、 は新しいバージョン AWS Systems Manager を作成します。関連付けの編集については、「AWS Systems Manager ユーザーガイド」の「関連付けの編集と新しいバージョンの作成」を参照してください。

[SSM.4] SSM ドキュメントはパブリックにしないでください

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 非常事態

リソースタイプ: `AWS::SSM::Document`

AWS Config ルール: `ssm-document-not-public`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、アカウントが所有する AWS Systems Manager ドキュメントがパブリックかどうかをチェックします。所有者 `Self` の SSM ドキュメントがパブリックの場合、このコントロールは失敗します。

パブリックの SSM ドキュメントは、ドキュメントへの意図しないアクセスを許可する場合があります。パブリック SSM ドキュメントは、アカウント、リソース、および内部プロセスに関する貴重な情報を公開する可能性があります。

ユースケースでパブリック共有が必要な場合を除き、`Self` が所有する Systems Manager ドキュメントのパブリック共有設定をブロックすることを推奨します。

修正

SSM ドキュメントのパブリック共有をブロックするには、「AWS Systems Manager ユーザーガイド」の「SSM ドキュメントのパブリック共有をブロックする」を参照してください。

Amazon Elastic File System のコントロール

これらのコントロールは Amazon EFS リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[EFS .1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS

関連する要件： CIS AWS Foundations Benchmark v3.0.0/2.4.1、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::EFS::FileSystem`

AWS Config ルール: `efs-encrypted-check`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Amazon Elastic File System が を使用してファイルデータを暗号化するように設定されているかどうかをチェックします AWS KMS。次の場合、チェックは失敗します。

- `DescribeFileSystems` レスポンスで `Encrypted` は、`false` に設定されている。
- `DescribeFileSystems` レスポンスの `KmsKeyId` キーが `efs-encrypted-check` の `KmsKeyId` パラメータと一致しない。

このコントロールでは、`efs-encrypted-check` の `KmsKeyId` パラメータを使用しないことに注意してください。`Encrypted` の値のみをチェックします。

Amazon EFS で機密データのセキュリティを強化するには、暗号化されたファイルシステムを作成する必要があります。Amazon EFS は保管時のファイルシステムの暗号化をサポートします。Amazon EFS ファイルシステムを作成する場合、保管中のデータの暗号化を有効にすることができます。Amazon EFS 暗号化の詳細については、「Amazon Elastic File System ユーザーガイド」の「Amazon EFS でのデータ暗号化」を参照してください。

修正

新しい Amazon EFS ファイルシステムを暗号化する方法の詳細については、「Amazon Elastic File System ユーザーガイド」の「保管中のデータの暗号化」を参照してください。

[EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > バックアップ

重要度: 中

リソースタイプ: `AWS::EFS::FileSystem`

AWS Config ルール: `efs-in-backup-plan`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup のバックアッププランに追加されているかどうかをチェックします。Amazon EFS ファイルシステムがバックアッププランに含まれていない場合、コントロールは失敗します。

バックアッププランに EFS ファイルシステムを組み込むと、データの削除やデータの損失からデータを保護できます。

修正

既存の Amazon EFS ファイルシステムの自動バックアップを有効にするには、AWS Backup デベロッパーガイドの「開始方法 4: Amazon EFS 自動バックアップの作成」を参照してください。

[EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります

関連する要件: NIST.800-53.r5 AC-6(10)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::EFS::AccessPoint`

AWS Config ルール : `efs-access-point-enforce-root-directory`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon EFS アクセスポイントが、ルートディレクトリを適用するように設定されているかどうかをチェックします。`Path` の値が `/` (ファイルシステムのデフォルトのルートディレクトリ) に設定されていると、このコントロールは失敗します。

ルートディレクトリを適用すると、アクセスポイントを使用する NFS クライアントは、ファイルシステムのルートディレクトリではなく、アクセスポイントに設定されているルートディレクトリを使用します。アクセスポイントのルートディレクトリを適用すると、アクセスポイントのユーザーを、指定されたサブディレクトリのファイルにのみアクセスさせ、データアクセスを制限することができます。

修正

EFS アクセスポイントのルートディレクトリを適用する方法については、Amazon Elastic File System ユーザーガイドの「アクセスポイントでルートディレクトリを適用する」を参照してください。

[EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります

関連する要件: NIST.800-53.r5 AC-6(2)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::EFS::AccessPoint`

AWS Config ルール : `efs-access-point-enforce-user-identity`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon EFS アクセスポイントが、ユーザーアイデンティティを適用するように設定されているかどうかをチェックします。EFS アクセスポイントの作成中に POSIX ユーザー ID が定義されていない場合、このコントロールは失敗します。

Amazon EFS アクセスポイントは、EFS ファイルシステムへのアプリケーション固有のエントリポイントです。これにより、共有データセットへのアプリケーションアクセスが管理しやすくなります。アクセスポイントを使用すると、アクセスポイントを介したすべてのファイルシステム要求に対してユーザーアイデンティティ (ユーザーの POSIX グループなど) を適用できます。また、ファイルシステムに対して別のルートディレクトリを適用し、このディレクトリまたはそのサブディレクトリ内のデータに対してのみ、クライアントにアクセスを許可することもできます。

修正

Amazon EFS アクセスポイントのユーザーアイデンティティを適用する方法については、Amazon Elastic File System ユーザーガイドの「アクセスポイントを使用したユーザ ID の適用」を参照してください。

[EFS .5] EFS アクセスポイントにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EFS::AccessPoint`

AWS Configルール: `tagged-efs-accesspoint` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon EFS アクセスポイントにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。アクセスポイントにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、アクセスポイントにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベ

ストプラクティスの詳細については、「」の「AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EFS アクセスポイントにタグを追加するには、「Amazon Elastic File System ユーザーガイド」の「Amazon EFS リソースのタグ付け」を参照してください。 Amazon Elastic File System

[EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 中

リソースタイプ: `AWS::EFS::FileSystem`

AWS Config ルール: `efs-mount-target-public-accessible`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Amazon EFS マウントターゲットがプライベートサブネットに関連付けられているかどうかをチェックします。マウントターゲットがパブリックサブネットに関連付けられている場合、コントロールは失敗します。

デフォルトでは、ファイルシステムは、それを作成した Virtual Private Cloud (VPC) からのみアクセスできます。インターネットからアクセスできないプライベートサブネットに EFS マウントターゲットを作成することをお勧めします。これにより、ファイルシステムへのアクセスが許可されたユーザーのみに限定され、不正アクセスや攻撃に対して脆弱になることはありません。

修正

マウントターゲットの作成後に EFS マウントターゲットとサブネットの関連付けを変更することはできません。既存のマウントターゲットを別のサブネットに関連付けるには、プライベートサブネットに新しいマウントターゲットを作成し、古いマウントターゲットを削除する必要があります。マウントターゲットの管理の詳細については、「Amazon Elastic File System ユーザーガイド」の「マウントターゲットとセキュリティグループの作成と管理」を参照してください。 Amazon Elastic File System

Amazon Elastic Kubernetes Service コントロール

これらのコントロールは Amazon EKS リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 高

リソースタイプ: `AWS::EKS::Cluster`

AWS Config ルール: `eks-endpoint-no-public-access`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Amazon EKS クラスターエンドポイントがパブリックにアクセス可能かどうかをチェックします。EKS クラスターにパブリックにアクセス可能なエンドポイントがある場合、コントロールは失敗します。

新しいクラスターを作成すると、Amazon EKS によって、マネージド型 Kubernetes API サーバー用にエンドポイントが作成されます。このエンドポイントは、ユーザーがクラスターとの通信に使用します。デフォルトでは、この API サーバーエンドポイントはインターネットで公開されています。API サーバーへのアクセスは、 AWS Identity and Access Management (IAM) とネイティブ Kubernetes ロールベースアクセスコントロール (RBAC) の組み合わせを使用して保護されます。エンドポイントへのパブリックアクセスを削除することで、意図しない公開やクラスターへのアクセスを防ぐことができます。

修正

既存の EKS クラスターのエンドポイントアクセスを変更するには、「Amazon EKS ユーザーガイド」の「クラスターエンドポイントのアクセスの変更」を参照してください。新しい EKS クラスターの作成時に、エンドポイントアクセスを設定できます。新しい Amazon EKS クラスターを作成する手順については、「Amazon EKS ユーザーガイド」の「Amazon EKS クラスターの作成」を参照してください。

[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 高

リソースタイプ: `AWS::EKS::Cluster`

AWS Config ルール : `eks-cluster-supported-version`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `oldestVersionSupported`: `1.26` (カスタマイズ不可)

このコントロールは、Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、サポートされている Kubernetes バージョンで実行されているかどうかをチェックします。EKS クラスターがサポートされていないバージョンで実行されている場合、このコントロールは失敗します。

アプリケーションが Kubernetes の特定のバージョンを必要としない場合は、EKS がクラスター用にサポートしている、Kubernetes の使用可能な最新バージョンを使用することが推奨されます。サポートされるバージョンの詳細については、「Amazon EKS ユーザーガイド」の「Amazon EKS Kubernetes リリースカレンダー」と「Amazon EKS のバージョンのよくある質問」を参照してください。

修正

EKS クラスターの更新方法については、「Amazon EKS ユーザーガイド」の「Amazon EKS クラスターの Kubernetes バージョンの更新」を参照してください。

[EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります

関連する要件： NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-12、NIST.800-53.r5 SC-13、NIST.800-53.r5 SI-28

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::EKS::Cluster`

AWS Config ルール: `eks-secrets-encrypted`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Amazon EKS クラスターが暗号化された Kubernetes シークレットを使用しているかどうかをチェックします。クラスターの Kubernetes シークレットが暗号化されていない場合、コントロールは失敗します。

シークレットを暗号化するときは、 AWS Key Management Service （ AWS KMS) キーを使用して、クラスターの etcd に保存されている Kubernetes シークレットをエンベロープ暗号化できます。この暗号化は、EBS クラスターの一部として etcd に保存されているすべてのデータ (シークレットを含む) に対してデフォルトで有効になっている EBS ボリューム暗号化に追加されます。EKS クラスターにシークレット暗号化を使用すると、ユーザーが定義して管理する KMS キーで Kubernetes シークレットを暗号化することで、Kubernetes アプリケーションの多層防御戦略をデプロイできます。

修正

EKS クラスターでシークレット暗号化を有効にするには、「Amazon EKS ユーザーガイド」の「既存のクラスターでシークレット暗号化を有効にする」を参照してください。

[EKS.6] EKS クラスターにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EKS::Cluster`

AWS Configルール: `tagged-eks-cluster` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon EKS クラスターにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。クラスターにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、クラスターにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベ

ストプラクティスの詳細については、「」の「AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EKS クラスターにタグを追加するには、「Amazon EKS ユーザーガイド」の「Amazon EKS リソースのタグ付け」を参照してください。

[EKS.7] EKS ID プロバイダーの設定にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::EKS::IdentityProviderConfig`

AWS Configルール: `tagged-eks-identityproviderconfig` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon EKS ID プロバイダー設定に、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。設定にタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、設定にキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EKS ID プロバイダー設定にタグを追加するには、「Amazon EKS ユーザーガイド」の「Amazon EKS リソースのタグ付け」を参照してください。

[EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります

関連する要件: NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 AU-9(7)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::EKS::Cluster`

AWS Config ルール: `eks-cluster-logging-enabled`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Amazon EKS クラスターで監査ログ記録が有効になっているかどうかをチェックします。クラスターで監査ログ記録が有効になっていない場合、コントロールは失敗します。

EKS コントロールプレーンのログ記録は、EKS コントロールプレーンからアカウントの Amazon CloudWatch Logs に直接監査ログと診断ログを提供します。必要なログタイプを選択すると、ログはログストリームとして 内の各 EKS クラスターのグループに送信されます CloudWatch。ログ記録により、EKS クラスターのアクセスとパフォーマンスを可視化できます。EKS クラスターの EKS コントロールプレーンログを CloudWatch Logs に送信することで、監査と診断目的のオペレーションを一元的に記録できます。

修正

EKS クラスターの監査ログを有効にするには、「Amazon EKS ユーザーガイド」の「コントロールプレーンログの有効化と無効化」を参照してください。

Amazon ElastiCache コントロール

これらのコントロールは ElastiCache リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔ElastiCache.1] ElastiCache Redis クラスターでは自動バックアップを有効にする必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

重要度: 高

リソースタイプ: `AWS::ElastiCache::CacheCluster`

AWS Config ルール： `elasticache-redis-cluster-automatic-backup-check`

スケジュールタイプ: 定期的

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
snapshotRetentionPeriod	最小スナップショット保持期間 (日数)	整数	1～35	1

このコントロールは、Amazon ElastiCache for Redis クラスターに自動バックアップがスケジュールされているかどうかを評価します。Redis クラスターの SnapshotRetentionLimit が指定された期間未満の場合、コントロールは失敗します。スナップショット保持期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 1 日を使用します。

Amazon ElastiCache for Redis クラスターはデータをバックアップできます。バックアップを使用して、クラスターを復元したり、新しいクラスターをシードしたりできます。バックアップは、クラスター内の全データとクラスターのメタデータで構成されます。すべてのバックアップは、耐久性のあるストレージを提供する Amazon Simple Storage Service (Amazon S3) に書き込まれます。新しい Redis クラスターを作成し、バックアップのデータを挿入することでデータを復元できます。バックアップは、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、および ElastiCache API を使用して管理できます。

修正

ElastiCache for Redis クラスターで自動バックアップをスケジュールするには、「Amazon ElastiCache ユーザーガイド」の「自動バックアップのスケジュール」を参照してください。

〔ElastiCache.2]Redis キャッシュクラスター ElastiCache では、マイナーバージョン自動アップグレードを有効にする必要があります

関連する要件: NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 高

リソースタイプ: AWS::ElastiCache::CacheCluster

AWS Config ルール: elasticache-auto-minor-version-upgrade-check

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、 ElastiCache for Redis がキャッシュクラスターにマイナーバージョンアップグレードを自動的に適用するかどうかを評価します。 ElastiCache for Redis キャッシュクラスターにマイナーバージョンアップグレードが自動的に適用されていない場合、このコントロールは失敗します。

`AutoMinorVersionUpgrade` は、新しいマイナーキャッシュエンジンバージョンが利用可能になったときにキャッシュクラスターを自動的にアップグレードするために ElastiCache 、 for Redis で有効にできる機能です。これらのアップグレードには、セキュリティパッチとバグ修正を含む場合があります。パッチのインストール up-to-date を維持することは、システムを保護する上で重要なステップです。

修正

既存の ElastiCache for Redis キャッシュクラスターに自動マイナーバージョンアップグレードを適用するには、「Amazon ElastiCache ユーザーガイド」の「エンジンバージョンのアップグレード」を参照してください。

Redis ElastiCache レプリケーショングループの [ElastiCache.3] では、自動フェイルオーバーを有効にする必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::ElastiCache::ReplicationGroup`

AWS Config ルール: `elasticache-repl-grp-auto-failover-enabled`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは ElastiCache 、 for Redis レプリケーショングループで自動フェイルオーバーが有効になっているかどうかを確認します。Redis レプリケーショングループで自動フェイルオーバーが有効になっていない場合、このコントロールは失敗します。

レプリケーショングループで自動フェイルオーバーを有効にすると、プライマリノードのロールは、いずれかのリードレプリカに自動的にフェイルオーバーされます。このフェイルオーバーとレプリカの昇格により、昇格の完了後すぐに新しいプライマリへの書き込みを再開できるため、障害発生時も全体のダウンタイムを短縮できます。

修正

既存の ElastiCache for Redis レプリケーショングループの自動フェイルオーバーを有効にするには、「Amazon ElastiCache ユーザーガイド」の「 ElastiCache クラスターの変更」を参照してください。 ElastiCache コンソールを使用する場合は、自動フェイルオーバーを有効に設定します。

〔ElastiCache.4] ElastiCache for Redis レプリケーショングループは保管時に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::ElastiCache::ReplicationGroup`

AWS Config ルール: `elasticache-repl-grp-encrypted-at-rest`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは ElastiCache 、 for Redis レプリケーショングループが保管中に暗号化されているかどうかを確認します。 ElastiCache for Redis レプリケーショングループが保管中に暗号化されていない場合、このコントロールは失敗します。

保管中のデータを暗号化すると、認証されていないユーザーがディスクに保存しているデータにアクセスするリスクが低減されます。 ElastiCache for Redis レプリケーショングループは、セキュリティを強化するために保管時に暗号化する必要があります。

修正

for Redis レプリケーショングループで保管時の暗号化を設定するには、「Amazon ユーザーガイド ElastiCache 」の「保管時の暗号化の有効化」を参照してください。 ElastiCache

Redis ElastiCache レプリケーショングループの [ElastiCache.5] は転送中に暗号化する必要があります

関連する要件: NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::ElastiCache::ReplicationGroup`

AWS Config ルール: `elasticache-repl-grp-encrypted-in-transit`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは ElastiCache 、 for Redis レプリケーショングループが転送中に暗号化されているかどうかを確認します。 ElastiCache for Redis レプリケーショングループが転送中に暗号化されていない場合、このコントロールは失敗します。

転送中のデータを暗号化することで、権限のないユーザーがネットワークトラフィックを盗聴するリスクが軽減されます。 ElastiCache for Redis レプリケーショングループで転送中の暗号化を有効にすると、クラスター内のノード間やクラスターとアプリケーション間など、ある場所から別の場所に移動するたびにデータが暗号化されます。

修正

for Redis レプリケーショングループで転送時の暗号化を設定するには、「Amazon ユーザーガイド ElastiCache 」の「転送時の暗号化の有効化」を参照してください。 ElastiCache

〔ElastiCache.6]バージョン ElastiCache 6.0 より前の Redis レプリケーショングループでは、Redis AUTH を使用する必要があります

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::ElastiCache::ReplicationGroup`

AWS Config ルール: `elasticache-repl-grp-redis-auth-enabled`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは ElastiCache 、 for Redis レプリケーショングループで Redis AUTH が有効になっているかどうかを確認します。Redis バージョンのノードが ElastiCache 6.0 未満で使用されていない場合、 for Redis レプリケーショングループのコントロール`AuthToken`は失敗します。

Redis 認証トークンまたはパスワードを使用すると、Redis はクライアントにコマンドの実行を許可する前にパスワードを要求するため、データのセキュリティが向上します。Redis 6.0 以降のバージョンでは、ロールベースのアクセス制御 (RBAC) の使用をお勧めします。RBAC は 6.0 より前のバージョンの Redis ではサポートされていないため、このコントロールは RBAC 機能を使用できないバージョンのみを評価します。

修正

ElastiCache for Redis レプリケーショングループで Redis AUTH を使用するには、「Amazon ElastiCache ユーザーガイド」の「既存の for Redis クラスターの AUTH トークンの変更 ElastiCache 」を参照してください。

〔ElastiCache.7] ElastiCache クラスターはデフォルトのサブネットグループを使用しないでください

関連する要件: NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(5)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ: `AWS::ElastiCache::CacheCluster`

AWS Config ルール: `elasticache-subnet-group-check`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、 ElastiCache クラスターにカスタムサブネットグループが設定されているかどうかを確認します。に値 がある場合、 ElastiCache クラスターのコントロールCacheSubnetGroupNameは失敗しますdefault。

ElastiCache クラスターを起動するときに、デフォルトのサブネットグループがまだ存在しない場合は作成されます。デフォルトグループは、デフォルトの仮想プライベートクラウド (VPC) のサブネットを使用します。クラスターが存在するサブネットや、クラスターがサブネットから継承するネットワークの制限機能がより強力な、カスタムサブネットグループを使用することをお勧めします。

修正

ElastiCache クラスターの新しいサブネットグループを作成するには、「Amazon ユーザーガイド」の「サブネットグループの作成」を参照してください。 ElastiCache

AWS Elastic Beanstalk コントロール

これらのコントロールは Elastic Beanstalk リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります

関連する要件: NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2

カテゴリ: 検出 > 検出サービス > アプリケーションモニタリング

重要度: 低

リソースタイプ: `AWS::ElasticBeanstalk::Environment`

AWS Config ルール : `beanstalk-enhanced-health-reporting-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS Elastic Beanstalk 環境で拡張ヘルスレポートが有効になっているかどうかをチェックします。

Elastic Beanstalk 拡張ヘルスレポートにより、基盤となるインフラストラクチャの健全性の変化に対するより迅速な対応が可能になります。これらの変更は、アプリケーションの可用性を低下させる可能性があります。

Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。サポートされている Amazon マシンイメージ (AMI) に含まれる Elastic Beanstalk ヘルスエージェントは、環境 EC2 インスタンスのログとメトリクスを評価します。

詳細については、「AWS Elastic Beanstalk 開発者ガイド」の「拡張ヘルスレポートおよびモニタリング」を参照してください。

修正

拡張ヘルスレポートを有効にする手順については、「AWS Elastic Beanstalk 開発者ガイド」の「Elastic Beanstalk コンソールを使用した拡張ヘルスレポートの有効化」を参照してください。

〔ElasticBeanstalk.2] Elastic Beanstalk マネージドプラットフォームの更新を有効にする必要があります

関連する要件: NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 高

リソースタイプ: `AWS::ElasticBeanstalk::Environment`

AWS Config ルール : `elastic-beanstalk-managed-updates-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`UpdateLevel`	バージョン更新レベル	列挙型	`minor`, `patch`	デフォルト値なし

このコントロールは、Elastic Beanstalk 環境でマネージドプラットフォームの更新が有効になっているかどうかをチェックします。マネージドプラットフォームの更新が有効になっていない場合、コントロールは失敗します。デフォルトでは、何らかのプラットフォーム更新が有効になっていればコントロールは成功します。必要に応じて、特定の更新レベルを要求するカスタムパラメータ値を指定できます。

マネージドプラットフォームの更新を有効にすると、環境で使用可能な最新のプラットフォームの修正、更新、および機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムを保護する上で重要なステップです。

修正

マネージドプラットフォームの更新を有効にするには、「AWS Elastic Beanstalk 開発者ガイド」の「マネージドプラットフォームの更新でマネージドプラットフォームの更新を設定するには」を参照してください。

〔ElasticBeanstalk.3] Elastic Beanstalk はログを にストリーミングする必要があります CloudWatch

カテゴリ: 識別 > ログ記録

重要度: 高

リソースタイプ: `AWS::ElasticBeanstalk::Environment`

AWS Config ルール : `elastic-beanstalk-logs-to-cloudwatch`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`RetentionInDays`	有効期限が切れるまでログイベントを保持する日数	列挙型	1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365 ,	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
			400, 545, 731, 1827, 3653	

このコントロールは、Elastic Beanstalk 環境がログを CloudWatch Logs に送信するように設定されているかどうかを確認します。Elastic Beanstalk 環境がログを CloudWatch Logs に送信するように設定されていない場合、コントロールは失敗します。有効期限が切れる前の指定された日数だけログが保持される場合にのみコントロールを成功させたい場合は、必要に応じて `RetentionInDays` パラメータにカスタム値を指定できます。

CloudWatch は、アプリケーションとインフラストラクチャリソースのさまざまなメトリクスを収集してモニタリングするのに役立ちます。を使用して CloudWatch 、特定のメトリクスに基づいてアラームアクションを設定することもできます。Elastic Beanstalk 環境の可視性を高めるため CloudWatch に、Elastic Beanstalk を と統合することをお勧めします。Elastic Beanstalk のログには、eb-activity.log、その環境の nginx または Apache プロキシサーバーからのアクセスログ、および環境に固有のログが含まれます。

修正

Elastic Beanstalk を CloudWatch ログと統合するには、「 AWS Elastic Beanstalk デベロッパーガイド」の「インスタンスログを CloudWatch ログにストリーミングする」を参照してください。

Elastic Load Balancing のコントロール

これらのコントロールは Elastic Load Balancing リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります

関連する要件: PCI DSS v3.2.1/2.3、PCI DSS v3.2.1/4.1、NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5

SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)

カテゴリ: 検出 > 検出サービス

重要度: 中

リソースタイプ: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config ルール: `alb-http-to-https-redirection-check`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、HTTP から HTTPS へのリダイレクトが Application Load Balancer のすべての HTTP リスナーで設定されているかどうかを確認します。HTTP から HTTPS へのリダイレクトが設定されていない Application Load Balancer の HTTP リスナーがある場合、コントロールは失敗します。

Application Load Balancer の使用を開始する前に、1 つ以上のリスナーを追加する必要があります。リスナーとは、設定したプロトコルとポートを使用して接続リクエストをチェックするプロセスです。リスナーは、HTTP プロトコルと HTTPS プロトコルの両方をサポートします。HTTPS リスナーを使用して、暗号化と復号化の作業をロードバランサーにオフロードできます。転送中の暗号化を強制するには、Application Load Balancer でリダイレクトアクションを使用して、クライアントの HTTP リクエストをポート 443 の HTTPS リクエストにリダイレクトする必要があります。

詳細については、「Application Load Balancer ユーザーガイド」の「Application Load Balancer のリスナー」を参照してください。

修正

HTTP リクエストを HTTPS にリダイレクトするには、Application Load Balancer のリスナールールを追加するか、既存のルールを編集する必要があります。

新しいルールを追加する手順については、「Application Load Balancer ユーザーガイド」の「ルールの追加」を参照してください。[プロトコル: ポート] で [HTTP] を選択し、**80** と入力します。[アクションの追加、リダイレクト先] で [HTTPS] を選択し、**443** と入力します。

既存のルールを編集する手順については、「Application Load Balancer ユーザーガイド」の「ルールの編集」を参照してください。[プロトコル: ポート] で [HTTP] を選択し、**80** と入力します。[アクションの追加、リダイレクト先] で [HTTPS] を選択し、**443** と入力します。

[ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager

関連する要件: NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(5)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config ルール : `elb-acm-certificate-required`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

Classic Load Balancer が AWS Certificate Manager (ACM) によって提供される HTTPS/SSL 証明書を使用しているかどうかをチェックします。HTTPS/SSL リスナーで構成された Classic Load Balancer が ACM によって提供される証明書を使用しない場合、コントロールは失敗します。

証明書の作成には、ACM または SSL や TLS プロトコルをサポートする OpenSSL などのツールを使用できます。Security Hub では、ACM を使用して、ロードバランサーの証明書を作成またはインポートすることを推奨します。

ACM は Classic Load Balancer と統合して、ロードバランサーに証明書をデプロイできます。また、これらの証明書は自動的に更新する必要があります。

修正

ACM SSL/TLS 証明書を Classic Load Balancer に関連付ける方法については、ナレッジセンターの記事「 AWS ACM SSL/TLS 証明書を Classic Load Balancer、Application Load Balancer、または Network Load Balancer と関連付ける方法を教えてください」を参照してください。

[ELB.3] Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります

関連する要件: NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5

SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config ルール : `elb-tls-https-listeners-only`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Classic Load Balancer リスナーがフロントエンド (クライアントからロードバランサー) 接続に HTTPS または TLS プロトコルを使用するよう設定されているかどうかをチェックします。このコントロールは、Classic Load Balancer にリスナーが有効な場合に適用されます。Classic Load Balancer にリスナーが設定されていない場合、コントロールは結果を報告しません。

Classic Load Balancer のリスナーがフロントエンド接続に TLS または HTTPS が設定されている場合、コントロールは成功します。

リスナーがフロントエンド接続に TLS または HTTPS が設定されていない場合、コントロールは失敗します。

ロードバランサーの使用を開始する前に、1 つまたは複数のリスナーを追加する必要があります。リスナーとは、設定したプロトコルとポートを使用して接続リクエストをチェックするプロセスです。リスナーは、HTTP プロトコルと HTTPS/TLS プロトコルの両方をサポートします。ロードバランサーが転送中に暗号化と復号化を行うため、常に HTTPS または TLS リスナーを使用する必要があります。

修正

この問題を修正するには、TLS または HTTPS プロトコルを使用するようにリスナーを更新します。

すべての非準拠リスナーを TLS/HTTPS リスナーに変更するには

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. ナビゲーションペインの [Load Balancing] で、[Load Balancers] を選択します。
3. Classic Load Balancer を選択します。

4. [Listeners] タブで、[Edit] を選択します。
5. すべてのリスナーについて、[Load Balancer Protocol] (ロードバランサーのプロトコル) が HTTPS または SSL に設定されていない場合は、設定を HTTPS または SSL に変更します。
6. 変更されたすべてのリスナーに対して、[証明書] タブで [デフォルトの変更] を選択します。
7. [ACM 証明書と IAM 証明書]の場合は、証明書を選択します。
8. [デフォルトとして保存] を選択します。
9. すべてのリスナーを更新したら、[Save] (保存) を選択します。

[ELB.4] Application Load Balancer は、http ヘッダーを削除するように設定する必要があります

関連する要件: NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8(2)

カテゴリ： 保護 > ネットワークセキュリティ

重要度: 中

リソースタイプ: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config ルール : `alb-http-drop-invalid-header-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは AWS 、Application Load Balancer を評価して、無効な HTTP ヘッダーを削除するように設定されていることを確認します。`routing.http.drop_invalid_header_fields.enabled` の値が `false` に設定されている場合、コントロールは失敗します。

デフォルトでは、Application Load Balancer は、無効な HTTP ヘッダー値を削除するように設定されていません。これらのヘッダー値を削除すると、HTTP desync 攻撃を防ぐことができます。

ELB.12 が有効になっている場合、このコントロールを無効にできます。

修正

この問題を修正するには、無効なヘッダーフィールドを削除するようにロードバランサーを設定します。

ロードバランサーで無効なヘッダーフィールドを削除するように設定するには

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. ナビゲーションペインで、[Load Balancers] (ロードバランサー) を選択します。
3. Application Load Balancer を選択します。
4. [Actions] (アクション) で、[Edit attributes] (属性の編集) を選択します。
5. [Drop Invalid Header Fields] (無効なヘッダーフィールドを削除) で、[Enable] (有効) を選択します。
6. [Save] (保存) を選択します。

[ELB.5] アプリケーションおよび Classic Load Balancer のログ記録を有効にする必要があります

関連する要件: NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::ElasticLoadBalancing::LoadBalancer`、`AWS::ElasticLoadBalancingV2::LoadBalance`

AWS Config ルール : `elb-logging-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

Application Load Balancer と Classic Load Balancer でログ記録が有効になっているかどうかをチェックします。`access_logs.s3.enabled` が `false` の場合、コントロールは失敗します。

Elastic Load Balancing は、ロードバランサーに送信されるリクエストに関する詳細情報をキャプチャしたアクセスログを提供します。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。これらのアクセスログを使用して、トラフィックパターンの分析や、問題のトラブルシューティングを行うことができます。

詳細については、「Classic Load Balancer ユーザーガイド」の「Classic Load Balancerのアクセスログ」を参照してください。

修正

アクセスログを有効にするには、「Application Load Balancer ユーザーガイド」の「ステップ 3: アクセスログの設定」を参照してください。

[ELB.6] Application、Gateway、Network Load Balancer では、削除保護を有効にする必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config ルール : `elb-deletion-protection-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Application、Gateway、または Network Load Balancer で削除保護が有効になっているかどうかをチェックします。削除保護が無効になっている場合、コントロールは失敗します。

削除保護を有効にして、Application、Gateway、または Network Load Balancer を削除から保護します。

修正

ロードバランサーが誤って削除されるのを防ぐために、削除保護を有効にできます。デフォルトでは、ロードバランサーで削除保護が無効になっています。

ロードバランサーの削除保護を有効にした場合、ロードバランサーを削除する前に無効にする必要があります。

Application Load Balancer の削除保護を有効にするには、「Application Load Balancer ユーザーガイド」の「削除保護」を参照してください。Gateway Load Balancer の削除保護を有効にするに

は、Gateway Load Balancer のユーザーガイドの「削除保護」を参照してください。 Network Load Balancer の削除保護を有効にするには、「Network Load Balancer ユーザーガイド」の「削除保護」を参照してください。

[ELB.7] Classic Load Balancers は、Connection Draining を有効にする必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: リカバリ > 耐障害性

重要度: 中

リソースタイプ: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Configルール: `elb-connection-draining-enabled` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Classic Load Balancers で Connection Draining が有効になっているかどうかをチェックします。

Classic Load Balancers で Connection Draining を有効にすることで、ロードバランサーは、登録解除中のインスタンスまたは異常の発生したインスタンスへのリクエストの送信を確実に停止します。既存の接続を開いたままにします。これは、Auto Scaling グループのインスタンスで、接続が突然切断されないようにするために特に役立ちます。

修正

Classic Load Balancers で Connection Draining を有効にするには、Classic Load Balancer のユーザーガイドの「Classic Load Balancer の Connection Draining の設定」を参照してください。

[ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な AWS Config設定を持つ事前定義されたセキュリティポリシーを使用する必要があります

関連する要件: NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config ルール : `elb-predefined-security-policy-ssl-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `predefinedPolicyName`: `ELBSecurityPolicy-TLS-1-2-2017-01` (カスタマイズ不可)

このコントロールは、Classic Load Balancer の HTTPS/SSL リスナーが事前定義されたポリシー `ELBSecurityPolicy-TLS-1-2-2017-01` を使用しているかどうかをチェックします。Classic Load Balancer の HTTPS/SSL リスナーが `ELBSecurityPolicy-TLS-1-2-2017-01` を使用しない場合、コントロールは失敗します。

セキュリティポリシーは、SSL プロトコル、暗号、およびサーバーの優先順位オプションを組み合わせたものです。事前定義されたポリシーは、クライアントとロードバランサー間の SSL ネゴシエーションでサポートする暗号、プロトコル、および優先順位をコントロールします。

`ELBSecurityPolicy-TLS-1-2-2017-01` を使用すると、SSL および TLS の特定のバージョンを無効にする必要があるコンプライアンスとセキュリティ標準に準拠することに役立ちます。詳細については、「Classic Load Balancer ユーザーガイド」の「Classic Load Balancer の事前定義された SSL セキュリティポリシー」を参照してください。

修正

Classic Load Balancer で定義済みのセキュリティポリシー `ELBSecurityPolicy-TLS-1-2-2017-01` を使用する方法については、「Classic Load Balancer ユーザーガイド」の「セキュリティ設定の構成」を参照してください。

[ELB.9] Classic Load Balancer では、クロスゾーンロードバランシングが有効になっている必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config ルール : `elb-cross-zone-load-balancing-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、クロスゾーンロードバランシングが Classic Load Balancer (CLB) に対して有効になっているかどうかをチェックします。クロスゾーンロードバランシングが CLB に対して有効になっていない場合、コントロールは失敗します。

ロードバランサノードは、アベイラビリティーゾーン内の登録済みターゲット全体にのみトラフィックを分散します。クロスゾーンロードバランシングが無効の場合、各ロードバランサーノードは、そのアベイラビリティーゾーンの登録済みターゲットにのみトラフィックを分散します。登録済みターゲット数がアベイラビリティーゾーン間で同じでない場合、トラフィックは均等に分散されず、あるゾーンのインスタンスは、別のゾーンのインスタンスと比較して過剰に使用される可能性があります。クロスゾーンロードバランシングを有効にすると、Classic Load Balancer の各ロードバランサーノードは、有効なすべてのアベイラビリティーゾーンに登録済みのインスタンスにリクエストを均等に分散します。詳細については、「Elastic Load Balancing ユーザーガイド」の「クロスゾーンロードバランシング」を参照してください。

修正

Classic Load Balancer でクロスゾーンロードバランシングを有効にするには、「Classic Load Balancer ユーザーガイド」の「クロスゾーンロードバランシングを有効にする」を参照してください。

[ELB.10] Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config ルール : clb-multiple-az

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
minAvailabilityZones	アベイラビリティーゾーンの最小数	列挙型	2, 3, 4, 5, 6	2

このコントロールは、Classic Load Balancer が少なくとも指定された数のアベイラビリティーゾーン (AZ) にまたがるように設定されているかどうかをチェックします。Classic Load Balancer が少なくとも指定された数の AZ にまたがっていない場合、コントロールは失敗します。AZ の最小数に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 2 つの AZ を使用します。

Classic Load Balancer は、単一のアベイラビリティーゾーンまたは複数のアベイラビリティーゾーンにある Amazon EC2 インスタンスに受信リクエストを配信するように設定できます。複数のアベイラビリティーゾーンにまたがらない Classic Load Balancer は、単独で構成されたアベイラビリティーゾーンが使用できなくなった場合、別のアベイラビリティーゾーンのターゲットにトラフィックをリダイレクトすることはできません。

修正

Classic Load Balancer にアベイラビリティーゾーンを追加するには、「Classic Load Balancer のユーザーガイド」の「Classic Load Balancer でのサブネットの追加もしくは削除」を参照してください。

[ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります

関連する要件: NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ： 保護 > データ保護 > データの整合性

重要度: 中

リソースタイプ: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config ルール : `alb-desync-mode-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `desyncMode`: `defensive, strictest` (カスタマイズ不可)

このコントロールは、Application Load Balancer が防御モードまたは最も厳密な非同期緩和モードに設定されているかどうかをチェックします。Application Load Balancer が防御モードまたは最も厳密な非同期緩和モードに設定されていない場合、このコントロールは失敗します。

HTTP 非同期の問題はリクエストスマグリングにつながり、アプリケーションがリクエストキューやキャッシュポイズニングに対して脆弱になる可能性があります。そしてこうした脆弱性は、認証情報スタッフィングや不正なコマンドの実行につながります。防御モードまたは最も厳密な非同期緩和モードで構成された Application Load Balancer は、HTTP 非同期に起因するセキュリティ上の問題からアプリケーションを保護します。

修正

Application Load Balancer の非同期緩和モードの更新方法については、「Application Load Balancer ユーザーガイド」の「Desync mitigation mode」(非同期緩和モード) を参照してください。

[ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config ルール : `elbv2-multiple-az`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`minAvailabilityZones`	アベイラビリティーゾーンの最小数	列挙型	`2, 3, 4, 5, 6`	`2`

このコントロールは、Elastic Load Balancer V2 (アプリケーション、ネットワーク、または Gateway Load Balancer) に少なくとも指定された数のアベイラビリティーゾーン (AZ) のインスタンスが登録されているかどうかをチェックします。Elastic Load Balancer V2 で、少なくとも指定された数の AZ にインスタンスが登録されていない場合、コントロールは失敗します。AZ の最小数に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 2 つの AZ を使用します。

Elastic Load Balancing は、受信したトラフィックを複数のアベイラビリティーゾーンの複数のターゲット (EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散させます。Elastic Load Balancing は、受信トラフィックの時間的な変化に応じて、ロードバランサーをスケーリングします。サービスの可用性を確保するため、2 つ以上のアベイラビリティーゾーンを設定することが推奨されます。それにより、Elastic Load Balancer はアベイラビリティーゾーンを使用できなくなったときに、別のアベイラビリティーゾーンにトラフィックを転送することができます。複数のアベイラビリティーゾーンを設定しておくと、アプリケーションの単一障害点を回避できます。

修正

アベイラビリティーゾーンを Application Load Balancer に追加する方法については、「Application Load Balancer ユーザーガイド」の「Application Load Balancer のアベイラビリティーゾーン」参照してください。アベイラビリティーゾーンを Network Load Balancer に追加する方法については、「Network Load Balancer ユーザーガイド」の「Network Load Balancer」を参照してください。アベイラビリティーゾーンを Gateway Load Balancer に追加する方法については、「Gateway Load Balancer ユーザーガイド」の「Create a Gateway Load Balancer」(Gateway Load Balancer の作成) を参照してください。

[ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります

関連する要件: NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ： 保護 > データ保護 > データの整合性

重要度: 中

リソースタイプ: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config ルール : `clb-desync-mode-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `desyncMode: defensive, strictest` (カスタマイズ不可)

このコントロールは、Classic Load Balancer が防御モードまたは最も厳密な非同期緩和モードで設定されているかどうかをチェックします。Classic Load Balancer が防御モードまたは最も厳密な非同期緩和モードに設定されていない場合、このコントロールは失敗します。

HTTP 非同期の問題はリクエストスマグリングにつながり、アプリケーションがリクエストキューやキャッシュポイズニングに対して脆弱になる可能性があります。そしてこうした脆弱性は、認証情報の乗っ取りや不正なコマンドの実行につながります。防御モードまたは最も厳密な非同期緩和モードで構成された Classic Load Balancer は、HTTP 非同期に起因するセキュリティ上の問題からアプリケーションを保護します。

修正

Classic Load Balancer の非同期緩和モードの更新方法については、「Classic Load Balancer ユーザーガイド」の「非同期緩和モードの変更」を参照してください。

[ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります

関連する要件: NIST.800-53.r5 AC-4(21)

カテゴリ: 保護 > 保護サービス

重要度: 中

リソースタイプ: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config ルール : `alb-waf-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Application Load Balancer が AWS WAF Classic または AWS WAF ウェブアクセスコントロールリスト (ウェブ ACL) に関連付けられているかどうかをチェックします。 AWS WAF 設定の `Enabled` フィールドが `false` に設定されている場合、コントロールは失敗します。

AWS WAF は、ウェブアプリケーションと APIsから保護するのに役立つウェブアプリケーションファイアウォールです。では AWS WAF、ウェブ ACL を設定できます。これは、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいて、ウェブリクエストを許可、ブロック、またはカウントする一連のルールです。悪意のある攻撃から保護するために、 AWS WAF ウェブ ACL に Application Load Balancer を関連付けることをお勧めします。

修正

Application Load Balancer をウェブ ACL に関連付けるには、「 デベロッパーガイド」の「ウェブ ACL と AWS リソースの関連付けまたは関連付け解除」を参照してください。 AWS WAF

Amazon EMR コントロール

これらのコントロールは Amazon EMR リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ: `AWS::EMR::Cluster`

AWS Config ルール: `emr-master-no-public-ip`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Amazon EMR クラスターのマスターノードにパブリック IP アドレスが設定されているかどうかをチェックします。マスターノードインスタンスのいずれかにパブリック IP アドレスが関連付けられている場合、コントロールは失敗します。

パブリック IP アドレスは、インスタンスの `NetworkInterfaces` 設定の `PublicIp` フィールドで指定されます。このコントロールは、`RUNNING` または `WAITING` 状態にある Amazon EMR クラスターのみをチェックします。

修正

起動中に、デフォルトサブネットまたはデフォルト以外のサブネット内のインスタンスがパブリック IPv4 アドレスを割り当てられるかどうかをコントロールできます。デフォルトでは、デフォルトサブネットのこの属性は `true` に設定されています。Amazon EC2 起動インスタンスウィザードによって作成された場合を除き、デフォルト以外のサブネットで IPv4 パブリックアドレス属性は `false` に設定されています。その場合、属性は `true` に設定されます。

起動後に、インスタンスからパブリック IPv4 アドレスの割り当てを手動で解除することはできません。

失敗した検出結果を修正するには、IPv4 パブリックアドレス属性が `false` に設定されているプライベートサブネットを使用して、VPC で新しいクラスターを起動する必要があります。手順については、「Amazon EMR 管理ガイド」の「VPC でクラスターを起動する」を参照してください。

[EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなアクセス管理 > パブリックアクセスが不可能なリソース

重要度: 非常事態

リソースタイプ: `AWS::::Account`

AWS Config ルール: `emr-block-public-access`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、アカウントに Amazon EMR ブロックパブリックアクセスが設定されているかどうかをチェックします。ブロックパブリックアクセス設定が有効になっていない場合、またはポート 22 以外のポートが許可されている場合、コントロールは失敗します。

Amazon EMR のブロックパブリックアクセスは、クラスターのセキュリティ設定でポートのパブリック IP アドレスからのインバウンドトラフィックが許可されている場合に、ユーザーがパブリックサブネットでクラスターを起動するのを防止します。 AWS アカウント のユーザーがクラスターを起動すると、Amazon EMR はクラスターのセキュリティグループのポートルールをチェックし、インバウンドトラフィックルールと比較します。セキュリティグループに、パブリック IP アドレス IPv4 0.0.0.0/0 または IPv6 ::/0 に対してポートを開くインバウンドルールがあり、それらのポートがアカウントで適切に指定されていない場合、Amazon EMR はユーザーにクラスターの作成を許可しません。

> **Note**
>
> ブロックパブリックアクセスはデフォルトで有効になっています。アカウントの保護を強化するには、これを有効のままにしておくことが推奨されます。

修正

Amazon EMR のブロックパブリックアクセスを設定するには、「Amazon EMR 管理ガイド」の「Amazon EMR のパブリックアクセスブロックの使用」を参照してください。

Elasticsearch コントロール

これらのコントロールは Elasticsearch リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります

関連する要件: PCI DSS v3.2.1/3.4、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::Elasticsearch::Domain`

AWS Config ルール: `elasticsearch-encrypted-at-rest`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Elasticsearch ドメインで保管中の暗号化設定が有効になっているかどうかをチェックします。保管時の暗号化が有効になっていない場合、チェックは失敗します。

の機密データのセキュリティを強化するには OpenSearch、保管時に暗号化 OpenSearch されるように を設定する必要があります。Elasticsearch ドメインは、保管中のデータの暗号化を提供します。この機能は、 AWS KMS を使用して暗号化キーを保存および管理します。暗号化の実行には、256 ビットキーを使用した Advanced Encryption Standard アルゴリズム (AES-256) を使用します。

保管時の OpenSearch 暗号化の詳細については、「Amazon OpenSearch Service デベロッパーガイド」の「Amazon Service の保管中のデータの暗号化」を参照してください。 OpenSearch

`t.small` や `t.medium` などの特定のインスタンスタイプでは、保管中のデータの暗号化がサポートされていません。詳細については、「Amazon OpenSearch Service デベロッパーガイド」の「サポートされているインスタンスタイプ」を参照してください。

修正

新規および既存の Elasticsearch ドメインの保管時の暗号化を有効にするには、「Amazon OpenSearch Service デベロッパーガイド」の「保管中のデータの暗号化の有効化」を参照してください。

[ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5

AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > VPC 内のリソース

重要度: 非常事態

リソースタイプ: `AWS::Elasticsearch::Domain`

AWS Config ルール: `elasticsearch-in-vpc-only`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Elasticsearch ドメインが VPC 内にあるかどうかをチェックします。このコントロールは、パブリックアクセスの可能性を判断するための VPC サブネットルーティング設定を評価しません。Elasticsearch ドメインがパブリックサブネットに添付済みでないことを確認する必要があります。「Amazon Service デベロッパーガイド」の「リソースベースのポリシー」を参照してください。 OpenSearch また、推奨されるベストプラクティスに従って VPC が確実に設定されていることを確認する必要があります。「Amazon VPC ユーザーガイド」の「VPC 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。

VPC 内にデプロイされた Elasticsearch ドメインは、パブリックインターネットを経由することなく、プライベート AWS ネットワーク経由で VPC リソースと通信できます。この設定では、転送中のデータへのアクセスを制限することにより、セキュリティ体制が向上します。VPC は、ネットワーク ACL やセキュリティグループを含む Elasticsearch ドメインへのアクセスを保護するための多数のネットワークコントロールを提供します。Security Hub では、これらのコントロールを有効に利用するために、パブリック Elasticsearch ドメインを VPC に移行することを推奨します。

修正

パブリックエンドポイントを使用してドメインを作成する場合、後で VPC 内にドメインを配置することはできません。代わりに、新規のドメインを作成して、データを移行する必要があります。逆の場合も同様です。VPC 内にドメインを作成する場合、パブリックエンドポイントを持つことはできません。代わりに、別のドメインを作成するか、このコントロールを無効にする必要があります。

「Amazon OpenSearch Service デベロッパーガイド」の「VPC 内で Amazon Service ドメインを起動する」を参照してください。 OpenSearch

[ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります

関連する要件: NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::Elasticsearch::Domain`

AWS Config ルール : `elasticsearch-node-to-node-encryption-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Elasticsearch ドメインで node-to-node 暗号化が有効になっているかどうかをチェックします。Elasticsearch ドメインで node-to-node 暗号化が有効になっていない場合、コントロールは失敗します。このコントロールは、Elasticsearch バージョンが node-to-node 暗号化チェックをサポートしていない場合にも、失敗した検出結果を生成します。

HTTPS (TLS) を使用すると、潜在的な攻撃者が または同様の攻撃を使用してネットワークトラフィックを盗聴 person-in-the-middle または操作するのを防ぐことができます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。Elasticsearch ドメインの node-to-node 暗号化を有効にすると、クラスター内通信が転送中に暗号化されます。

この設定には、パフォーマンス上のペナルティが発生する可能性があります。このオプションを有効にする前に、パフォーマンスのトレードオフを認識してテストする必要があります。

修正

新規および既存のドメインで node-to-node 暗号化を有効にする方法については、「Amazon Service node-to-nodeデベロッパーガイド」の「暗号化の有効化」を参照してください。 OpenSearch

[ES.4] Logs への Elasticsearch CloudWatch ドメインエラーのログ記録を有効にする必要があります

関連する要件: NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5

AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 - ログ記録

重要度: 中

リソースタイプ: `AWS::Elasticsearch::Domain`

AWS Config ルール : `elasticsearch-logs-to-cloudwatch`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `logtype = 'error'` (カスタマイズ不可)

このコントロールは、Elasticsearch ドメインがエラーログを CloudWatch ログに送信するように設定されているかどうかを確認します。

Elasticsearch ドメインのエラーログを有効にし、それらのログを Logs CloudWatch に送信して保持と応答を行う必要があります。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

修正

ログ発行を有効にする方法については、Amazon OpenSearch Service デベロッパーガイドの「ログ発行の有効化 (コンソール)」を参照してください。

[ES.5] Elasticsearch ドメインで監査ログ記録が有効になっている必要があります

関連する要件: NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::Elasticsearch::Domain`

AWS Config ルール: `elasticsearch-audit-logging-enabled` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `cloudWatchLogsLogGroupArnList` (カスタマイズ不可)。Security Hub は、このパラメータを設定しません。監査ログ用に設定する必要がある CloudWatch Logs ロググループのカンマ区切りリスト。

  このルールは`NON_COMPLIANT`、Elasticsearch ドメインの CloudWatch ロググループがこのパラメータリストで指定されていない場合に になります。

このコントロールは、Elasticsearch ドメインで監査ログ記録が有効になっているかどうかをチェックします。Elasticsearch ドメインで監査ログ記録が有効になっていない場合、このコントロールは失敗します。

監査ログは高度なカスタマイズが可能です。これにより、認証の成功と失敗、 へのリクエスト、インデックスの変更、受信検索クエリなど OpenSearch、Elasticsearch クラスターでのユーザーアクティビティを追跡できます。

修正

監査ログを有効にする詳細な手順については、「Amazon OpenSearch Service デベロッパーガイド」の「監査ログの有効化」を参照してください。

[ES.6] Elasticsearch ドメインには少なくとも 3 つのデータノードが必要です

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::Elasticsearch::Domain`

AWS Config ルール: `elasticsearch-data-node-fault-tolerance` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Elasticsearch ドメインに少なくとも 3 つのデータノードが設定されていること、また zoneAwarenessEnabled が true かどうかをチェックします。

Elasticsearch ドメインでは、高可用性と耐障害性のために少なくとも 3 つのデータノードが必要です。少なくとも 3 つのデータノードを持つ Elasticsearch ドメインをデプロイすると、ノードに障害が発生した場合のクラスター操作が確保されます。

修正

Elasticsearch ドメインのデータノードの数を変更するには

1. https://console.aws.amazon.com/aos/ で Amazon OpenSearch Service コンソールを開きます。
2. [ドメイン] で、編集するドメインの名前を選択します。
3. [Edit domain] (ドメインの編集) を選択します。
4. [Data nodes] (データノード) で、[Number of nodes] (ノード数) に 3 以上の数値を設定します。

   3 つのアベイラビリティーゾーンのデプロイは、3 の倍数に設定してアベイラビリティーゾーン間で均等に配信されるようにします。
5. [Submit] (送信) を選択します。

[ES.7] Elasticsearch ドメインは、少なくとも 3 つの専用マスターノードを設定する必要があります。

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: AWS::Elasticsearch::Domain

AWS Configルール: elasticsearch-primary-node-fault-tolerance (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Elasticsearch ドメインに少なくとも 3 つの専用プライマリノードが設定されているかどうかを確認します。ドメインが専用プライマリノードを使用しない場合、このコントロー

ルは失敗します。Elasticsearch ドメインに 5 つの専用プライマリノードがある場合、このコントロールは成功します。ただし、可用性リスクを軽減するために 3 つ以上のプライマリノードを使用する必要がない場合があり、追加コストが発生する可能性があります。

Elasticsearch ドメインでは、高可用性と耐障害性を実現するために、少なくとも 3 つの専用プライマリノードが必要です。データノードのブルー/グリーンデプロイ中に、管理すべきノードが他にもあるため、専用のプライマリノードリソースに負荷がかかる可能性があります。少なくとも 3 つの専用プライマリノードを持つ Elasticsearch ドメインをデプロイすると、ノードに障害が発生した場合に十分なプライマリノードリソース容量とクラスターオペレーションが確保されます。

修正

OpenSearch ドメイン内の専用プライマリノードの数を変更するには

1. https://console.aws.amazon.com/aos/ で Amazon OpenSearch Service コンソールを開きます。
2. [ドメイン] で、編集するドメインの名前を選択します。
3. [Edit domain] (ドメインの編集) を選択します。
4. [Dedicated master nodes] (専用マスターノード) で、[Instance type] (インスタンスタイプ) に目的のインスタンスタイプを設定します。
5. [Number of master nodes] (マスターノードの数) を 3 以上に設定します。
6. [Submit] (送信) を選択します。

[ES.8] Elasticsearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります

関連する要件: NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::Elasticsearch::Domain`

AWS Config ルール: `elasticsearch-https-required` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Elasticsearch ドメインエンドポイントが最新の TLS セキュリティポリシーを使用するように設定されているかどうかをチェックします。Elasticsearch ドメインエンドポイントがサポートされている最新のポリシーを使用するように設定されていない場合、または HTTPs は失敗します。現在サポートされている最新の TLS セキュリティポリシーは ですPolicy-Min-TLS-1-2-PFS-2023-10。

HTTPS (TLS) を使用すると、潜在的な攻撃者がネットワークトラフィックを傍受または操作するために または同様の攻撃を使用すること person-in-the-middleを防ぐことができます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。転送中のデータの暗号化は、パフォーマンスに影響する可能性があります。TLS のパフォーマンスプロファイルと TLS の影響を把握するには、この機能を使用してアプリケーションをテストする必要があります。TLS 1.2 は、以前の TLS バージョンに比べて、いくつかのセキュリティ機能の強化を提供します。

修正

TLS 暗号化を有効にするには、 UpdateDomainConfig API オペレーションを使用して DomainEndpointOptions オブジェクトを設定します。これにより、 が設定されますTLSSecurityPolicy。

[ES.9] Elasticsearch ドメインにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: AWS::Elasticsearch::Domain

AWS Config ルール: tagged-elasticsearch-domain (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
requiredTagKeys	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーで	StringList	AWS 要件を満たすタグのリスト	No default value

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	は、大文字と小文字が区別されます。			

このコントロールは、Elasticsearch ドメインにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。ドメインにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、ドメインにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Elasticsearch ドメインにタグを追加するには、「Amazon OpenSearch Service デベロッパーガイド」の「タグの使用」を参照してください。

Amazon EventBridge コントロール

これらのコントロールは EventBridge リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::Events::EventBus`

AWS Config ルール : `tagged-events-eventbus` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon EventBridge イベントバスにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。イベントバスにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、イベントバスにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの

識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EventBridge イベントバスにタグを追加するには、「Amazon ユーザーガイド」の「Amazon EventBridge タグ」を参照してください。 EventBridge

〔EventBridge.3] EventBridge カスタムイベントバスには、リソースベースのポリシーがアタッチされている必要があります

関連する要件: NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(3)

カテゴリ: 保護 > セキュアなアクセス管理 > パブリックアクセスが不可能なリソース

重要度: 低

リソースタイプ: `AWS::Events::EventBus`

AWS Config ルール : `custom-schema-registry-policy-attached`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon EventBridge カスタムイベントバスにリソースベースのポリシーがアタッチされているかどうかを確認します。カスタムイベントバスにリソースベースのポリシーがない場合、このコントロールは失敗します。

デフォルトでは、 EventBridge カスタムイベントバスにはリソースベースのポリシーがアタッチされていません。これにより、アカウント内のプリンシパルはイベントバスにアクセスできます。リソースベースのポリシーをイベントバスにアタッチすることで、イベントバスへのアクセスを特定のアカウントに制限したり、別のアカウントのエンティティへのアクセスを意図的に許可したりできます。

修正

リソースベースのポリシーを EventBridge カスタムイベントバスにアタッチするには、「Amazon ユーザーガイド」の「イベントバスのアクセス許可の管理」を参照してください。 EventBridge

〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::Events::Endpoint`

AWS Config ルール : `global-endpoint-event-replication-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon EventBridge グローバルエンドポイントでイベントレプリケーションが有効になっているかどうかを確認します。グローバルエンドポイントでイベントレプリケーションが有効になっていない場合、コントロールは失敗します。

グローバルエンドポイントによりアプリケーションをリージョンフォールトトレラントにできます。開始するには、エンドポイントに Amazon Route 53 ヘルスチェックを割り当てます。フェイルオーバーが開始されると、ヘルスチェックは「異常」状態を報告します。フェイルオーバーの開始から数分以内に、すべてのカスタムイベントがセカンダリリージョンのイベントバスにルーティングされ、そのイベントバスによって処理されます。グローバルエンドポイントを使用する場合、イベントレプリケーションを有効にできます。イベントレプリケーションは、マネージドルールを使用して、す

べてのカスタムイベントをプライマリリージョンとセカンダリリージョンのイベントバスに送信します。グローバルエンドポイントを設定する場合は、イベントレプリケーションを有効にすることをお勧めします。イベントレプリケーションは、グローバルエンドポイントが正しく設定されていることを確認するのに役立ちます。フェイルオーバーイベントから自動的にリカバリするには、イベントレプリケーションが必要です。イベントレプリケーションを有効にしていない場合は、イベントがプライマリリージョンにルーティングされる前に、Route 53 ヘルスチェックを手動で「正常」にリセットする必要があります。

> **Note**
>
> カスタムイベントバスを使用している場合、フェイルオーバーが正常に機能するためには、各リージョンに同じ名前と同じアカウントを持つカスタムイベントバスが必要です。イベントレプリケーションを有効にすると、月額のコストが増加する可能性があります。料金の詳細については、「Amazon の EventBridge 料金」を参照してください。

修正

EventBridge グローバルエンドポイントのイベントレプリケーションを有効にするには、「Amazon ユーザーガイド」の「グローバルエンドポイントの作成」を参照してください。 EventBridge イベントレプリケーションの場合は、[イベントレプリケーションが有効] を選択します。

Amazon FSx コントロール

これらのコントロールは Amazon FSx リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::FSx::FileSystem`

AWS Config ルール : `fsx-openzfs-copy-tags-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon FSx for OpenZFS ファイルシステムがタグをバックアップとボリュームにコピーするように設定されているかどうかをチェックします。OpenZFS ファイルシステムがタグをバックアップとボリュームにコピーするように設定されていない場合、コントロールは失敗します。

IT アセットの身分証明書とインベントリはガバナンスとセキュリティの重要な側面です。タグは、AWS リソースを目的、所有者、環境などさまざまな方法で分類するのに役立ちます。割り当てたタグに基づいて特定のリソースをすばやく識別できるため、これは同じ型のリソースが多い場合に役立ちます。

修正

タグをバックアップとボリュームにコピーするように FSx for OpenZFS ファイルシステムを設定するには、「Amazon FSx OpenZFS ユーザーガイド」の「ファイルシステムの更新」を参照してください。

[FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります

関連する要件： NIST.800-53.r5 CP-9、NIST.800-53.r5 CM-8

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::FSx::FileSystem`

AWS Config ルール : `fsx-lustre-copy-tags-to-backups`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon FSx for Lustre ファイルシステムがタグをバックアップとボリュームにコピーするように設定されているかどうかをチェックします。Lustre ファイルシステムがバックアップとボリュームにタグをコピーするように設定されていない場合、コントロールは失敗します。

IT アセットの身分証明書とインベントリはガバナンスとセキュリティの重要な側面です。タグは、AWS リソースを目的、所有者、環境などさまざまな方法で分類するのに役立ちます。割り当てたタ

グに基づいて特定のリソースをすばやく識別できるため、これは同じ型のリソースが多い場合に役立ちます。

修正

タグをバックアップにコピーするように FSx for Lustre ファイルシステムを設定するには、「Amazon FSx OpenZFS FSx OpenZFS ユーザーガイド」の「ファイルシステムの更新」を参照してください。

AWS Global Accelerator コントロール

これらのコントロールは Global Accelerator リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::GlobalAccelerator::Accelerator`

AWS Config ルール: `tagged-globalaccelerator-accelerator` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS Global Accelerator アクセラレーターにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。アクセラレーターにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、アクセラレーターがどのキーでもタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Global Accelerator グローバルアクセラレーターにタグを追加するには、「 デベロAWS Global Accelerator ッパーガイド」の「 でのタグ付け AWS Global Accelerator」を参照してください。

AWS Glue コントロール

これらのコントロールは AWS Glue リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Glue.1] AWS Glue ジョブにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::Glue::Job`

AWS Config ルール：`tagged-glue-job` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、 AWS Glue ジョブにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。ジョブにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、ジョブにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオ

ペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS Glue ジョブにタグを追加するには、「 ユーザーガイドAWS 」の「 のタグ AWS GlueAWS Glue 」を参照してください。

Amazon GuardDuty コントロール

これらのコントロールは GuardDuty リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔GuardDuty.1] GuardDuty を有効にする必要があります

関連する要件: PCI DSS v3.2.1/11.4、NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AU-6(1)、NIST.800-53.r5 AU-6(5)、NIST.800-53.r5 CA-7、NIST.800-53.r5 CM-8(3)、NIST.800-53.r5 RA-3(4)、NIST.800-53.r5 SA-11(1)、NIST.800-53.r5 SA-11(6)、NIST.800-53.r5 SA-15(2)、NIST.800-53.r5 SA-15(8)、NIST.800-53.r5 SA-8(19)、NIST.800-53.r5 SA-8(21)、NIST.800-53.r5 SA-8(25)、NIST.800-53.r5 SC-5、NIST.800-53.r5 SC-5(1)、NIST.800-53.r5 SC-5(3)、NIST.800-53.r5 SI-20、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-4(1)、NIST.800-53.r5 SI-4(13)、NIST.800-53.r5 SI-4(2)、NIST.800-53.r5 SI-4(22)、NIST.800-53.r5 SI-4(25)、NIST.800-53.r5 SI-4(4)、NIST.800-53.r5 SI-4(5)

カテゴリ: 検出 > 検出サービス

重要度: 高

リソースタイプ: `AWS::::Account`

AWS Config ルール: guardduty-enabled-centralized

スケジュールタイプ: 定期的

パラメータ: なし

このコントロール GuardDuty は、 GuardDuty アカウントとリージョンで Amazon が有効になっているかどうかをチェックします。

サポートされているすべての AWS リージョン GuardDuty で を有効にすることを強くお勧めします。これにより、アクティブ GuardDuty に使用されていないリージョンでも、不正または異常なアクティビティに関する検出結果を生成できます。これにより、 GuardDuty は IAM などのグローバル AWS のサービス の CloudTrail イベントをモニタリングすることもできます。

修正

この問題を修正するには、 を有効にします GuardDuty。

を使用して複数のアカウント AWS Organizations を管理する方法など GuardDuty、 を有効にする方法の詳細については、「Amazon ユーザーガイド」の GuardDuty「 の開始方法」を参照してください。 GuardDuty

〔GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::GuardDuty::Filter`

AWS Config ルール: `tagged-guardduty-filter` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーで	StringList	AWS 要件を満たすタグのリスト	`No default value`

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	は、大文字と小文字が区別されます。			

このコントロールは、Amazon GuardDuty フィルターにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。フィルターにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、フィルターにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

GuardDuty フィルターにタグを追加するには、「Amazon GuardDuty API リファレンスTagResource」の「」を参照してください。

〔GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::GuardDuty::IPSet`

AWS Config ルール: `tagged-guardduty-ipset` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、Amazon GuardDuty IPSet にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。IPSet にタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、IPSet にキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できま

す。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

GuardDuty IPSet にタグを追加するには、「Amazon API リファレンス GuardDuty TagResource」の「」を参照してください。

〔GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::GuardDuty::Detector`

AWS Config ルール: `tagged-guardduty-detector` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、Amazon GuardDuty ディテクターにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。ディテクターにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、ディテクターがキーでタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

GuardDuty ディテクターにタグを追加するには、「Amazon GuardDuty API リファレンスTagResource」の「」を参照してください。

AWS Identity and Access Management コントロール

これらのコントロールは IAM リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください

関連する要件： PCI DSS v3.2.1/7.2.1、CIS AWS Foundations Benchmark v1.2.0/1.22、CIS AWS Foundations Benchmark v1.4.0/1.16、NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.8000-5 AC-6、NIST. AC-6 AC-68

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 高

リソースタイプ: `AWS::IAM::Policy`

AWS Config ルール : iam-policy-no-statements-with-admin-access

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `excludePermissionBoundaryPolicy: true` (カスタマイズ不可)

このコントロールは、IAM ポリシー (カスタマー管理ポリシーとも呼ばれます) のデフォルトバージョンに、`"Action": "*"` が `"Resource": "*"` に対して規定された `"Effect": "Allow"` ステートメントを持つ管理者アクセス権があるかどうかをチェックします。このようなステートメントを含む IAM ポリシーがある場合、コントロールは失敗します。

コントロールは、作成したカスタマーマネージドポリシーのみをチェックします。インラインポリシーと AWS 管理ポリシーはチェックされません。

IAM ポリシーは、ユーザー、グループ、またはロールに付与される権限のセットを定義します。標準のセキュリティアドバイスに従って、 は最小権限を付与 AWS することをお勧めします。これは、タスクの実行に必要なアクセス許可のみを付与することを意味します。ユーザーが必要とする最小限の許可セットではなく、完全な管理者権限を提供すると、リソースが不要なアクションにさらされる可能性があります。

完全な管理者権限を許可するのではなく、ユーザーが何をする必要があるのかを決定し、ユーザーが、それらのタスクのみを実行できるポリシーを作成します。最小限の許可セットから開始し、必要に応じて追加許可を付与する方がより安全です。あまりにも寛大な許可から始めて、後でそれらを強化しようとしないでください。

`"Effect": "Allow"` および `"Action": "*"` が `"Resource": "*"` に対して規定されたステートメントを持つ IAM ポリシーは削除する必要があります。

> **Note**
>
> AWS Config Security Hub を使用するすべてのリージョンで を有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。グローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

IAM ポリシーを変更して、完全な「*」管理者権限を許可しないようにする方法については、「IAM ユーザーガイド」の「IAM ポリシーの編集」を参照してください。

[IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください

関連する要件： PCI DSS v3.2.1/7.2.1、CIS AWS Foundations Benchmark v3.0.0/1.15、CIS AWS Foundations Benchmark v1.2.0/1.16、NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(3)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 低

リソースタイプ: `AWS::IAM::User`

AWS Config ルール : `iam-user-no-policies-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、IAM ユーザーにポリシーが添付済みかどうかをチェックします。IAM ユーザーにポリシーが添付されている場合、コントロールは失敗します。代わりに、IAM ユーザーは、IAM グループまたはロールから許可を継承するか、ロールを引き受ける必要があります。

デフォルトでは、IAM ユーザー、グループ、ロールは AWS リソースにアクセスできません。IAM ポリシーで、ユーザー、グループ、またはロールに権限を付与します。IAM ポリシーはグループとロールには直接適用しますが、ユーザーには直接適用しないことを推奨します。グループレベルまた

はロールレベルで権限を割り当てると、ユーザー数が増えるにつれてアクセス管理の複雑さが軽減されます。アクセス管理の複雑さを軽減することで、プリンシパルが誤って過剰な権限を受け取ったり保持する機会を減らすことができます。

> **Note**
>
> Amazon Simple Email Service が作成した IAM ユーザーは、インラインポリシーを使用して自動作成されます。Security Hub は、これらのユーザーをこのコントロールから自動的に除外します。
> AWS Config Security Hub を使用するすべてのリージョンで を有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。グローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

この問題を解決するには、IAM グループを作成し、ポリシーをこのグループにアタッチします。続いて、ユーザーをこのグループに追加します。ポリシーは、グループ内の各ユーザーに適用されます。ユーザーに直接添付されているポリシーを削除するには、IAM ユーザーガイドの「IAM ID のアクセス許可の追加および削除」を参照してください。

[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.14、CIS AWS Foundations Benchmark v1.4.0/1.14、CIS AWS Foundations Benchmark v1.2.0/1.4、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-2(3)、NIST.800-53.r5 AC-3(15)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::IAM::User`

AWS Config ルール: `access-keys-rotated`

スケジュールタイプ: 定期的

パラメータ:

- `maxAccessKeyAge: 90` (カスタマイズ不可)

このコントロールは、アクティブなアクセスキーが 90 日以内にローテーションされているかどうかをチェックします。

アカウントのすべてのアクセスキーを生成したり削除したりしないことを強く推奨します。代わりに、1 つ以上の IAM ロールを作成するか、 経由でフェデレーションを使用することが推奨されます AWS IAM Identity Center。これらの方法を使用して、ユーザーが AWS Management Console およびにアクセスすることを許可できます AWS CLI。

各アプローチにはそれぞれのユースケースがあります。フェデレーションは、既存の中央ディレクトリを保有する企業や、現在の制限 IAM ユーザーよりも多くを必要とする予定の企業にとって一般的に適しています。 AWS 環境の外部で実行されるアプリケーションには、 AWS リソースへのプログラムによるアクセスのためのアクセスキーが必要です。

ただし、プログラムによるアクセスを必要とするリソースが 内で実行されている場合 AWS、ベストプラクティスは IAM ロールを使用することです。ロールを使用すると、アクセスキー ID とシークレットアクセスキーを設定にハードコーディングすることなく、リソースへのアクセスを許可できます。

アクセスキーとアカウントの保護の詳細については、「」の AWS 「アクセスキーを管理するためのベストプラクティス」を参照してくださいAWS 全般のリファレンス。また、ブログ記事「プログラムによるアクセス AWS アカウント を使用する際の の保護に関するガイドライン」も参照してください。

アクセスキーが既に存在する場合、Security Hub では 90 日ごとにアクセスキーをローテーションすることを推奨します。アクセスキーをローテーションすることにより、侵害されたアカウントや終了したアカウントに関連付けられているアクセスキーが使用される可能性が低くなります。また、紛失した、クラックされた、盗まれた古いキーでデータにアクセスできないようにします。アクセスキーをローテーションしたら、必ずアプリケーションを更新してください。

アクセスキーは、アクセスキー ID とシークレットアクセスキーで構成されます。これは AWSへのプログラムによるリクエストの署名に使用されます。ユーザーは、、Tools for Windows AWS CLI、PowerShell AWS SDKs、または個々の の API オペレーションを使用した直接 HTTP 呼び出し AWS から をプログラムで呼び出すために、独自のアクセスキーが必要です AWS のサービス。

組織が AWS IAM Identity Center (IAM Identity Center) を使用している場合、ユーザーは Active Directory、組み込みの IAM Identity Center ディレクトリ、または IAM Identity Center に接続された別の ID プロバイダー (IdP) にサインインできます。その後、アクセスキーを必要とせずに AWS

CLI コマンドを実行したり AWS API オペレーションを呼び出すことができる IAM ロールにマッピングできます。詳細については、「 ユーザーガイド」の AWS CLI 「 を使用するための の設定 AWS IAM Identity CenterAWS Command Line Interface 」を参照してください。

> **Note**
>
> AWS Config Security Hub を使用するすべてのリージョンで を有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。グローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

90 日以上経過したアクセスキーをローテーションするには、「IAM ユーザーガイド」の「アクセスキーのローテーション」を参照してください。[アクセスキーの有効期間] が 90 日を超えるすべてのユーザーに対する指示に従ってください。

[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.4、CIS AWS Foundations Benchmark v1.4.0/1.4、CIS AWS Foundations Benchmark v1.2.0/1.12、PCI DSS v3.2.1/2.1、PCI DSS v3.2.1/2.2、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(AC-61

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 非常事態

リソースタイプ: `AWS::::Account`

AWS Config ルール: `iam-root-access-key-check`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、ルートユーザーアクセスキーが存在するかどうかをチェックします。

ルートユーザーは、 の最も特権のあるユーザーです AWS アカウント。 AWS アクセスキーは、特定のアカウントへのプログラムによるアクセスを提供します。

Security Hub では、ルートユーザーに関連付けられたすべてのアクセスキーの削除を推奨します。これにより、お使いのアカウントの侵害に使用できるベクトルが制限されます。また、最小特権のロールベースのアカウントの作成と使用が促進されます。

修正

ルートユーザーアクセスキーを削除するには、「IAM ユーザーガイドの「ルートユーザーのアクセスキーの削除」を参照してください。の からルートユーザーアクセスキーを削除するには AWS GovCloud (US)、 AWS アカウント 「 ユーザーガイド」のAWS GovCloud (US) 「アカウントルートユーザーアクセスキーの削除AWS GovCloud (US) 」を参照してください。

[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.10、CIS AWS Foundations Benchmark v1.4.0/1.10、CIS AWS Foundations Benchmark v1.2.0/1.2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 IA-2(1)、NIST.800-53.r5 IA-2(2)、NIST.800-53.r5 IA-2(6)、NIST.800-53.r5 IA-2(8)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::IAM::User`

AWS Config ルール: `mfa-enabled-for-iam-console-access`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、コンソールパスワードを使用するすべての IAM ユーザーに対して AWS 多要素認証 (MFA) が有効になっているかどうかをチェックします。

多要素認証 (MFA) は、ユーザー名とパスワードに更なる保護手段を追加します。MFA を有効にすると、ユーザーが AWS ウェブサイトにサインインすると、ユーザー名とパスワードの入力を求められます。さらに、 AWS MFA デバイスから認証コードの入力を求められます。

コンソールパスワードを使用するすべてのアカウントにおいて、MFA を有効にすることを推奨します。MFA は、コンソールアクセスのセキュリティを強化するために設計されています。認証プリン

シパルは、時間的制約のあるキーを発行するデバイスを所有し、認証情報に関する知識がある必要があります。

> **Note**
>
> AWS Config Security Hub を使用するすべてのリージョンで を有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。グローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

IAM ユーザーを MFA に追加するには、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。

対象となるお客様には、MFA セキュリティキーを無料で提供しています。資格があるかどうかを確認し、無料のキーを注文します。

[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.6、CIS AWS Foundations Benchmark v1.4.0/1.6、CIS AWS Foundations Benchmark v1.2.0/1.14、PCI DSS v3.2.1/8.3.1、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 IA-2(1)、NIST.800-53.r5 IA-2(2)、NIST.800-53.r5 IA-2IA-2(8)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 非常事態

リソースタイプ: `AWS::::Account`

AWS Config ルール: `root-account-hardware-mfa-enabled`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロール AWS アカウント は、 がハードウェア多要素認証 (MFA) デバイスを使用してルートユーザーの認証情報でサインインできるかどうかを確認します。MFA が有効になっていない場合や、仮想 MFA デバイスにルートユーザー認証情報によるサインインが許可されている場合、コントロールは失敗します。

仮想 MFA はハードウェア MFA デバイスと同じレベルのセキュリティを提供しない可能性があります。ハードウェアの購入承認の待機中、またはハードウェアの到着を待つ間にのみ、仮想 MFA デバイスの使用を推奨します。詳細については、「IAM ユーザーガイド」の「仮想多要素認証 (MFA) デバイスの有効化 (コンソール)」を参照してください。

タイムベースドワンタイムパスワード (TOTP) トークンと、ユニバーサルセカンドファクター (U2F) トークンの両方が、ハードウェア MFA オプションとして実行可能です。

修正

ルートユーザーのハードウェア MFA デバイスを追加するには、IAM ユーザーガイドの AWS アカウント「ルートユーザーのハードウェア 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。

対象となるお客様には、MFA セキュリティキーを無料で提供しています。資格があるかどうかを確認し、無料のキーを注文します。

[IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-2(3)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 IA-5(1)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::::Account`

AWS Config ルール: `iam-password-policy`

スケジュールタイプ: 定期的

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`RequireUppercaseCharacters`	パスワードには少なくとも 1 つの大文字が必要です	ブール値	`true` 、、または `false`	`true`

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
RequireLowercaseCharacters	パスワードには少なくとも 1 つの小文字が必要です	ブール値	true 、、または false	true
RequireSymbols	パスワードには少なくとも 1 つの記号が必要です	ブール値	true 、、または false	true
RequireNumbers	パスワードには少なくとも 1 つの数字が必要です	ブール値	true 、、または false	true
MinimumPasswordLength	パスワードに含まれる文字の最小数	整数	8～128	8
PasswordReusePrevention	古いパスワードを再使用できるようになるまでのパスワードローテーション回数	整数	12～24	デフォルト値なし
MaxPasswordAge	パスワードが有効期限切れになるまでの日数	整数	1～90	デフォルト値なし

このコントロールは、IAM ユーザーのアカウントパスワードポリシーが強力な設定を使用しているかどうかをチェックします。パスワードポリシーが強力な設定を使用していない場合、コントロールは失敗します。カスタムパラメータ値を指定しない限り、Security Hub は前の表に記載されているデフォルト値を使用します。PasswordReusePrevention パラメータおよび MaxPasswordAge パラメータにはデフォルト値がないため、これらのパラメータを除外した場合、Security Hub はこのコントロールを評価する際にパスワードローテーションの回数とパスワードの有効期間を無視します。

にアクセスするには AWS Management Console、IAM ユーザーにパスワードが必要です。ベストプラクティスとして、Security Hub では IAM ユーザーを作成する代わりに、フェデレーションの使用を強く推奨します。フェデレーションでは、ユーザーは既存の企業認証情報を使用して、 AWS Management Consoleにログインできます。 AWS IAM Identity Center (IAM Identity Center) を使用してユーザーを作成またはフェデレーションし、アカウントに IAM ロールを引き受けます。

アイデンティティプロバイダーと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「アイデンティティプロバイダーとフェデレーション」を参照してください。IAM Identity Center の詳細については、AWS IAM Identity Center ユーザーガイドを参照してください。

IAM ユーザーを使用する必要がある場合は、Security Hub では、強力なユーザーパスワードの作成を強制することを推奨します。にパスワードポリシーを設定 AWS アカウント して、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を指定できます。パスワードポリシーを作成または変更する場合、パスワードポリシーの設定の多くは、ユーザーが次回パスワードを変更するときに適用されます。ただし、一部の設定は即座に適用されます。

修正

パスワードポリシーの更新については、「IAM ユーザーガイド」の「IAM ユーザーのアカウントパスワードポリシーの設定」を参照してください。

[IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります

関連する要件： PCI DSS v3.2.1/8.1.4、CIS AWS Foundations Benchmark v1.2.0/1.3、NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-2(3)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::IAM::User`

AWS Config ルール: `iam-user-unused-credentials-check`

スケジュールタイプ: 定期的

パラメータ:

- `maxCredentialUsageAge`: `90` (カスタマイズ不可)

このコントロールは、IAM ユーザーが 90 日間使用されていないパスワードまたはアクティブなアクセスキーを持っているかどうかをチェックします。

IAM ユーザーは、パスワードやアクセスキーなど、さまざまなタイプの認証情報を使用して AWS リソースにアクセスできます。

Security Hub では、90 日以上使用されていないすべての認証情報を削除または非アクティブ化することを推奨します。不要な認証情報を無効化または削除することにより、侵害または放棄されたアカウントに関連付けられている認証情報が使用される可能性が少なくなります。

> **Note**
>
> AWS Config Security Hub を使用するすべてのリージョンで を有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。グローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

IAM コンソールでユーザー情報を表示すると、[アクセスキーの有効期間]、[パスワードの有効期間]、[最終アクティビティ] の列が表示されます。これらの列の値のいずれかが 90 日より大きい場合は、それらのユーザーの認証情報を非アクティブにします。

認証情報レポートを使用してユーザーアカウントをモニタリングし、90 日以上アクティビティのないアカウントを特定することもできます。IAM コンソールから認証情報レポートを `.csv` 形式でダウンロードできます。

非アクティブなアカウント、または未使用の認証情報を特定したら、それらを非アクティブ化します。手順については、「IAM ユーザーガイド」の「IAM ユーザーパスワードの作成、変更、削除 (コンソール)」を参照してください。

[IAM.9] ルートユーザーに対して MFA を有効にする必要があります

関連する要件： PCI DSS v3.2.1/8.3.1、CIS AWS Foundations Benchmark v3.0.0/1.5、CIS AWS Foundations Benchmark v1.4.0/1.5、CIS AWS Foundations Benchmark v1.2.0/1.13、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 IA-2(1)、NIST.800-53.r5 IA-2(2)、NIST.800-53.r5 IA-2IA-2(8)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 非常事態

リソースタイプ: `AWS::::Account`

AWS Config ルール: `root-account-mfa-enabled`

スケジュールタイプ: 定期的

パラメータ: なし

ルートユーザーは、 AWS アカウントのすべてのサービスとリソースへの完全なアクセス権を持ちます。MFA は、ユーザー名とパスワードに更なる保護手段を追加します。MFA を有効にすると、ユーザーが にサインインすると AWS Management Console、ユーザー名とパスワードと AWS MFA デバイスからの認証コードの入力を求められます。

ルートユーザーに仮想 MFA を使用する場合、CIS は個人用デバイスではないデバイスを使用することを推奨しています。代わりに、各個人のデバイスとは独立して課金およびセキュリティ保護を維持できるように管理している、専用のモバイルデバイス (タブレットまたは電話) を使用してください。これにより、デバイスの紛失、デバイスの下取り、またはデバイスを所有する個人の離職のために MFA へのアクセスが失われるリスクが軽減されます。

修正

ルートユーザーの MFA を有効にするには、「 アカウント管理リファレンスガイド」の AWS アカウント 「ルートユーザーの MFA を有効にする」を参照してください。 AWS

[IAM.10] IAM ユーザーのパスワードポリシーには強力な AWS Config設定が必要です

関連する要件: PCI DSS v3.2.1/8.1.4、PCI DSS v3.2.1/8.2.3、PCI DSS v3.2.1/8.2.4、PCI DSS v3.2.1/8.2.5

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::::Account`

AWS Config ルール: `iam-password-policy`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、IAM ユーザーのアカウントパスワードポリシーが次の最低限の PCI DSS 設定を使用しているかどうかをチェックします。

- `RequireUppercaseCharacters` - パスワードには少なくとも 1 つの大文字が必要。(デフォルト = `true`)
- `RequireLowercaseCharacters` - パスワードには少なくとも 1 つの小文字が必要。(デフォルト = `true`)

- `RequireNumbers` - パスワードには少なくとも 1 つの数字が必要。(デフォルト = `true`)
- `MinimumPasswordLength` - パスワードの最小文字数。(デフォルト = 7 以上)
- `PasswordReusePrevention` - パスワードの再利用を許可するまでのパスワードの数。(デフォルト = 4)
- MaxPasswordAge - パスワードの有効期限が切れるまでの日数。(デフォルト = 90)

修正

推奨される設定を使用するようにパスワードポリシーを更新するには、「IAM ユーザーガイドの「IAM ユーザー用のアカウントパスワードポリシーの設定」を参照してください。

[IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/1.5

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::::Account`

AWS Config ルール: `iam-password-policy`

スケジュールタイプ: 定期的

パラメータ: なし

パスワードポリシーは、パスワードの複雑さの要件をある程度強制します。IAM パスワードポリシーを使用して、パスワードで異なる文字セットを使用するようにします。

CIS では、パスワードポリシーで少なくとも 1 文字の大文字を要求することを推奨しています。パスワードの複雑さに関するポリシーを設定すると、ブルートフォースのログイン試行に対するアカウントの耐障害性が高まります。

修正

パスワードポリシーの変更については、「IAM ユーザーガイド」の「IAM ユーザーのアカウントパスワードポリシーの設定」を参照してください。[パスワードの強度] で、[ラテンアルファベット (A–Z) の少なくとも 1 つの大文字が必要] を選択します。

[IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/1.6

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::::Account`

AWS Config ルール: `iam-password-policy`

スケジュールタイプ: 定期的

パラメータ: なし

パスワードポリシーは、パスワードの複雑さの要件をある程度強制します。IAM パスワードポリシーを使用して、パスワードで異なる文字セットを使用するようにします。CIS では、パスワードポリシーで少なくとも 1 文字の小文字を要求することを推奨しています。パスワードの複雑さに関するポリシーを設定すると、ブルートフォースのログイン試行に対するアカウントの耐障害性が高まります。

修正

パスワードポリシーの変更については、「IAM ユーザーガイド」の「IAM ユーザーのアカウントパスワードポリシーの設定」を参照してください。[パスワードの強度] で、[ラテンアルファベット (A–Z) の少なくとも 1 つの小文字が必要] を選択します。

[IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/1.7

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::::Account`

AWS Config ルール: `iam-password-policy`

スケジュールタイプ: 定期的

パラメータ: なし

パスワードポリシーは、パスワードの複雑さの要件をある程度強制します。IAM パスワードポリシーを使用して、パスワードで異なる文字セットを使用するようにします。

CIS では、パスワードポリシーで少なくとも 1 文字の記号を要求することを推奨しています。パスワードの複雑さに関するポリシーを設定すると、ブルートフォースのログイン試行に対するアカウントの耐障害性が高まります。

修正

パスワードポリシーの変更については、「IAM ユーザーガイド」の「IAM ユーザーのアカウントパスワードポリシーの設定」を参照してください。[パスワードの強度] で、[少なくとも 1 つの英数字以外の文字が必要] を選択します。

[IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/1.8

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::::Account`

AWS Config ルール: `iam-password-policy`

スケジュールタイプ: 定期的

パラメータ: なし

パスワードポリシーは、パスワードの複雑さの要件をある程度強制します。IAM パスワードポリシーを使用して、パスワードで異なる文字セットを使用するようにします。

CIS では、パスワードポリシーで少なくとも 1 文字の数字を要求することを推奨しています。パスワードの複雑さに関するポリシーを設定すると、ブルートフォースのログイン試行に対するアカウントの耐障害性が高まります。

修正

パスワードポリシーの変更については、「IAM ユーザーガイド」の「IAM ユーザーのアカウントパスワードポリシーの設定」を参照してください。[パスワードの強度] で、[少なくとも 1 つの数字が必要] を選択します。

[IAM.15] 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します

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.8、CIS AWS Foundations Benchmark v1.4.0/1.8、CIS AWS Foundations Benchmark v1.2.0/1.9

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::::Account`

AWS Config ルール: `iam-password-policy`

スケジュールタイプ: 定期的

パラメータ: なし

パスワードポリシーは、パスワードの複雑さの要件をある程度強制します。IAM パスワードポリシーを使用して、パスワードが指定された長さ以上になるようにします。

CIS では、パスワードポリシーで 14 文字以上の長さを要求することを推奨しています。パスワードの複雑さに関するポリシーを設定すると、ブルートフォースのログイン試行に対するアカウントの耐障害性が高まります。

修正

パスワードポリシーの変更については、「IAM ユーザーガイド」の「IAM ユーザーのアカウントパスワードポリシーの設定」を参照してください。[パスワードの最小文字数] で、**14** またはそれ以上の数字を入力します。

[IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.9、CIS AWS Foundations Benchmark v1.4.0/1.9、CIS AWS Foundations Benchmark v1.2.0/1.10

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 低

リソースタイプ: `AWS::::Account`

AWS Config ルール: `iam-password-policy`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、記憶するパスワードの数が 24 に設定されているかどうかをチェックします。値が 24 でない場合、コントロールは失敗します。

IAM パスワードポリシーにより、同じユーザーによる特定のパスワードの再使用を防ぐことができます。

CIS では、パスワードポリシーでパスワードの再使用を禁止することを推奨しています。パスワードの再使用を禁止すると、ブルートフォースのログイン試行に対するアカウントの耐障害性が高まります。

修正

パスワードポリシーの変更については、「IAM ユーザーガイド」の「IAM ユーザーのアカウントパスワードポリシーの設定」を参照してください。[パスワードの再利用を禁止] で、**24** と入力します。

[IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/1.11

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 低

リソースタイプ: `AWS::::Account`

AWS Config ルール: `iam-password-policy`

スケジュールタイプ: 定期的

パラメータ: なし

IAM パスワードポリシーでは、指定された日数後にパスワードをローテーションするか、または有効期限切れにすることを要求できます。

CIS では、パスワードポリシーでパスワードを 90 日以内に有効期限切れにすることを推奨しています。パスワードの有効期間を短くすると、ブルートフォースのログイン試行に対するアカウントの耐障害性が高まります。定期的なパスワード変更の要求は、以下のシナリオでも役立ちます。

- パスワードはユーザーが知らない間に、盗まれたり漏洩したりする可能性があります。これは、システムの侵害、ソフトウェアの脆弱性、または内部の脅威によって起こりえます。
- 特定の企業や政府のウェブフィルターまたはプロキシサーバーは、暗号化されている場合でもトラフィックを傍受し記録できます。
- 多くの人々が仕事、E メール、個人用など多くのシステムで同じパスワードを使用しています。
- 侵害されたエンドユーザーのワークステーションに、キーストロークロガーが設置されている可能性があります。

修正

パスワードポリシーの変更については、「IAM ユーザーガイド」の「IAM ユーザーのアカウントパスワードポリシーの設定」を参照してください。[パスワードの有効期間をオンにする] で、**90** またはそれより小さい数字を入力します。

[IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.17、CIS AWS Foundations Benchmark v1.4.0/1.17、CIS AWS Foundations Benchmark v1.2.0/1.20

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 低

リソースタイプ: `AWS::::Account`

AWS Config ルール: `iam-policy-in-use`

スケジュールタイプ: 定期的

パラメータ:

- `policyARN`: `arn:`*`partition`*`:iam::aws:policy/AWSSupportAccess` (カスタマイズ不可)
- `policyUsageType`: `ANY` (カスタマイズ不可)

AWS は、インシデントの通知と対応、テクニカルサポート、カスタマーサービスに使用できるサポートセンターを提供します。

IAM ロールを作成して、認可済みのユーザーが AWS サポートでインシデントを管理できるようにします。アクセスコントロールの最小権限を実装することで、IAM ロールには、 でインシデント

を管理するためにサポートセンターへのアクセスを許可する適切な IAM ポリシーが必要です AWS Support。

> **Note**
>
> AWS Config Security Hub を使用するすべてのリージョンで を有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。グローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

この問題を修正するには、認可済みのユーザーに AWS Support インシデントの管理を許可するロールを作成します。

AWS Support アクセスに使用するロールを作成するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. IAM ナビゲーションペインで [Roles] (ロール) を選択し、続いて [Create role] (ロールの作成) を選択します。
3. [Role type] (ロールタイプ) で、[Another AWS アカウント] を選択します。
4. アカウント ID には、リソースへのアクセスを許可する の AWS アカウント ID を入力します。AWS アカウント

   このロールを引き受けるユーザーまたはグループが同じアカウントに属している場合は、ローカルアカウント番号を入力します。

   > **Note**
   >
   > 指定したアカウントの管理者は、そのアカウントのすべての ユーザーに、このロールを引き受けるアクセス許可を付与できます。そのためには、管理者から `sts:AssumeRole` アクションの許可を付与するユーザーまたはグループにポリシーを添付します。そのポリシーで、リソースはロール ARN である必要があります。

5. [Next: Permissions] (次へ: 許可) を選択します。
6. マネージドポリシー `AWSSupportAccess` を検索します。
7. `AWSSupportAccess` マネージドポリシーのチェックボックスを選択します。

8. [Next: Tags] (次へ: タグ) を選択します。
9. (オプション) ロールにメタデータを追加するには、キーバリューのペアとしてタグをアタッチします。

   IAM でのタグの使用の詳細については、「IAM ユーザーガイド」の「Tagging IAM users and roles」(IAM ユーザーとロールのタグ付け) を参照してください。
10. [Next: Review] (次へ: レビュー) を選択します。
11. [Role name] (ロール名) に、ロールの名前を入力します。

    ロール名は 内で一意である必要があります AWS アカウント。大文字と小文字は区別されません。
12. (オプション) [Role description] (ロールの説明) に、新しいロールの説明を入力します。
13. ロールを確認し、[Create role] (ロールの作成) を選択します。

[IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります

関連する要件: PCI DSS v3.2.1/8.3.1、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 IA-2(1)、NIST.800-53.r5 IA-2(2)、NIST.800-53.r5 IA-2(6)、NIST.800-53.r5 IA-2(8)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::IAM::User`

AWS Config ルール: `iam-user-mfa-enabled`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、IAM ユーザーが多要素認証 (MFA) を有効にしているかどうかを確認します。

> **Note**
>
> AWS Config Security Hub を使用するすべてのリージョンで を有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。グ

ローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

IAM ユーザーに MFA を追加するには、「IAM ユーザーガイド」の「AWSユーザーの MFA デバイスの有効化」を参照してください。

[IAM.20] ルートユーザーの使用を避けます

> **Important**
>
> Security Hub は 2024 年 4 月にこのコントロールを廃止しました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

関連する要件： CIS AWS Foundations Benchmark v1.2.0/1.1

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 低

リソースタイプ: `AWS::IAM::User`

AWS Config ルール: `use-of-root-account-test` (カスタム Security Hub ルール)

スケジュールタイプ: 定期的

パラメータ: なし

このコントロール AWS アカウント は、 にルートユーザーの使用に制限があるかどうかをチェックします。このコントロールは、以下のリソースを評価します。

- Amazon Simple Notification Service (Amazon SNS)のトピック
- AWS CloudTrail 証跡
- CloudTrail 証跡に関連付けられたメトリクスフィルター
- フィルターに基づく Amazon CloudWatch アラーム

チェックの結果、以下の記述の 1 つ以上が真であれば `FAILED` と判定されます:

- アカウントに証 CloudTrail 跡が存在しません。
- CloudTrail 証跡は有効になっていますが、読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン証跡では設定されていません。
- CloudTrail 証跡は有効になっていますが、 CloudWatch ロググループに関連付けられていません。
- Center for Internet Security (CIS) が規定する正確なメトリックフィルターが使用されていません。規定のメトリックフィルターは `'{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}'` です。
- メトリクスフィルターに基づく CloudWatch アラームがアカウントに存在しません。
- CloudWatch 関連付けられた SNS トピックに通知を送信するように設定された アラームは、アラーム条件に基づいてトリガーされません。
- SNS トピックが、SNS トピックにメッセージを送信するための制約に準拠していません。
- SNS トピックに 1 人以上のサブスクライバーが存在しません。

チェックの結果、以下の条件の 1 つ以上に当てはまれば、`NO_DATA` コントロールステータスになります:

- マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

チェックの結果、以下の条件の 1 つ以上に当てはまれば、`WARNING` コントロールステータスになります:

- 現在のアカウントは、 CloudWatch アラームで参照される SNS トピックを所有していません。
- `ListSubscriptionsByTopic` SNS API を呼び出しても、現在のアカウントは SNS トピックにアクセスできません。

> **Note**
>
> 組織内の多数のアカウントからのイベントを記録するには、組織の証跡を使用することをお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS

Organizations 管理アカウントまたは CloudTrail 委任された管理者アカウントでのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは NO_DATA になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

ベストプラクティスは、アカウントおよびサービスの管理タスクを実行するときに必要となる場合のみ、ルートユーザー認証情報を使用することです。IAM ポリシーは直接ユーザーに適用するのではなく、グループとロールに適用します。日常的に使用する管理者を設定する方法については、「IAM ユーザーガイド」の「最初の IAM 管理者のユーザーおよびグループの作成」を参照してください。

修正

この問題を修正するステップには、Amazon SNS トピック、 CloudTrail証跡、メトリクスフィルター、メトリクスフィルターのアラームの設定が含まれます。

Amazon SNS トピックを作成するには

1. Amazon SNS コンソール (https://console.aws.amazon.com/sns/v3/home) を開きます。
2. すべての CIS アラームを受信する Amazon SNS トピックを作成します。

   トピックに少なくとも 1 人の受信者を作成します。詳細については、「Amazon Simple Notification Service 開発者ガイド」の「Amazon SNS の開始方法」を参照してください。

次に、すべてのリージョン CloudTrail に適用される をアクティブに設定します。これを行うには、the section called “〔CloudTrail.1] CloudTrail 読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン追跡を有効にして設定する必要があります” の修正ステップに従います。

CloudTrail 証跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。そのロググループに対してメトリクスフィルターを作成します。

最後に、メトリクスフィルターとアラームを作成します。

メトリクスフィルターとアラームを作成するには

1. https://console.aws.amazon.com/cloudwatch/ で CloudWatch コンソールを開きます。

2. ナビゲーションペインで、[ロググループ] を選択します。
3. 作成した証 CloudTrail 跡に関連付けられている CloudWatch ログロググループのチェックボックスをオンにします。
4. [Actions] (アクション) から、[Create Metric Filter] (メトリクスフィルターの作成) を選択します。
5. [Define pattern] (パターンを定義) で、以下の操作を行います。

   a. 次のパターンをコピーして、[Filter Pattern] (フィルターパターン) フィールドに貼り付けます。

   ```
   {$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS &&
    $.eventType !="AwsServiceEvent"}
   ```

   b. [Next] (次へ) を選択します。
6. [Assign Metric] (メトリクスの割り当て) で、以下の操作を行います。

   a. [Filter name] (フィルター名) に、メトリクスフィルターの名前を入力します。
   b. [Metric namespace] (メトリクス名前空間) に **LogMetrics** と入力します。

      すべての CIS ログメトリクスフィルターに同じ名前空間を使用した場合、すべての CIS Benchmark メトリクスがグループ化されます。
   c. [Metric Name] (メトリクス名) に、メトリクスの名前を入力します。メトリクスの名前を忘れないでください。アラームの作成時にメトリクスを選択する必要があります。
   d. [Metric value] (メトリクス値) に **1** と入力します。
   e. [Next] (次へ) を選択します。
7. [Review and create] (確認して作成) で、新しいメトリクスフィルター用に入力した情報を確認します。その後、[Create metric filter] (メトリクスフィルターの作成) を選択します。
8. ナビゲーションペインで [Log groups] (ロググループ)を選択し、[Metric filters] (メトリクスフィルター) で作成したフィルターを選択します。
9. フィルターのチェックボックスをオンにします。[アラームを作成] を選択します。
10. [Specify metric and conditions] (メトリクスと条件の指定) で、以下の操作を行います。

    a. [Conditions] (条件) の [Threshold] (しきい値) で、[Static] (静的) を選択します。
    b. [Define the alarm condition] (アラーム条件を定義) で、[Greater/Equal] (より大きい/等しい) を選択します。
    c. [Define the threshold value] (しきい値の定義) で、**1** を入力します。

d. [Next] (次へ) を選択します。

11. [Configure actions] (アクションの設定) で、次の作業を行います。

    a. [Alarm state trigger] (アラーム状態トリガー) で、[In alarm] (アラーム状態) を選択します。

    b. [Select an SNS topic] (SNS トピックの選択) で、[Select an existing SNS topic] (既存の SNS トピックの選択) を選択します。

    c. [Send a notification to] (通知の送信先) で、前の手順で作成した SNS トピックの名前を入力します。

    d. [Next] (次へ) を選択します。

12. [Add name and description] (名前と説明を追加) に、アラームの [Name] (名前)と [Description] (説明)を **`CIS-1.1-RootAccountUsage`** のように入力します。続いて、[Next] (次へ) を選択します。

13. [Preview and create] (プレビューと作成) で、アラームの設定を確認します。次に [Create alarm] (アラームの作成) を選択します。

[IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません

関連する要件: NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(10)、NIST.800-53.r5 AC-6(2)、NIST.800-53.r5 AC-6(3)

カテゴリ: 検出 > セキュアなアクセス管理

重要度: 低

リソースタイプ: `AWS::IAM::Policy`

AWS Config ルール : `iam-policy-no-statements-with-full-access`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `excludePermissionBoundaryPolicy`: `True` (カスタマイズ不可)

このコントロールは、作成した IAM アイデンティティベースのポリシーに、ワイルドカード (*) を使用して、任意のサービスに対してすべてのアクションに許可を付与する許可ステートメントがあ

るかどうかをチェックします。ポリシーステートメントに、"Effect": "Allow" と "Action": "Service:*" が含まれている場合、コントロールは失敗します。

例えば、ポリシーに次のような記述があると、結果は失敗となります。

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:*",
  "Resource": "*"
}
```

"Effect": "Allow" と "NotAction": "*service*:*" を使用する場合も、コントロールは失敗します。その場合、 NotAction要素は、 で指定されたアクションを除き AWS のサービス、 内のすべてのアクションへのアクセスを提供しますNotAction。

このコントロールは、カスタマー管理 IAM ポリシーにのみ適用されます。 AWSによって管理される IAM ポリシーには適用されません。

にアクセス許可を割り当てるときは AWS のサービス、IAM ポリシーで許可されている IAM アクションの範囲を設定することが重要です。IAM アクションは、必要なアクションのみに制限する必要があります。これは、最小特権の許可のプロビジョンに役立ちます。ポリシーが許可を必要としない IAM プリンシパルに添付済みの場合、過度に許可されたポリシーは特権エスカレーションにつながる可能性があります。

場合によっては、DescribeFlowLogs や DescribeAvailabilityZones のような類似のプレフィックスを持つ IAM アクションを許可する必要があります。これらの承認済みのケースでは、共通プレフィクスにサフィックス付きワイルドカードを追加することができます。例えば、ec2:Describe* です。

プレフィクスが付いた IAM アクションとサフィックス付きワイルドカードを使用する場合、このコントロールは成功します。例えば、ポリシー内の次のステートメントでは、結果が成功になります。

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:Describe*",
  "Resource": "*"
```

```
}
```

この方法で関連する IAM アクションをグループ化することで、IAM ポリシーのサイズ制限を超えないようにすることもできます。

> **Note**
>
> AWS Config Security Hub を使用するすべてのリージョンで を有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。グローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

この問題を修正するには、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します。IAM ポリシーを編集する方法の詳細は、「IAM ユーザーガイド」の「IAM ポリシーの編集」を参照してください。

[IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.12、CIS AWS Foundations Benchmark v1.4.0/1.12

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::IAM::User`

AWS Config ルール: `iam-user-unused-credentials-check`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、IAM ユーザーが 45 日以上使用されていないパスワードまたはアクティブなアクセスキーを持っていないかどうかをチェックします。そのためには、 AWS Config ルールの `maxCredentialUsageAge`パラメータが 45 以上であるかどうかをチェックします。

ユーザーは、パスワードやアクセスキーなど、さまざまなタイプの認証情報を使用して AWS リソースにアクセスできます。

CIS では、45 日以上使用されていないすべての認証情報を削除または非アクティブ化することが推奨されています。不要な認証情報を無効化または削除することにより、侵害または放棄されたアカウントに関連付けられている認証情報が使用される可能性が少なくなります。

このコントロールの AWS Config ルールは、 GetCredentialReportおよび GenerateCredentialReport API オペレーションを使用します。これらは 4 時間ごとにのみ更新されます。IAM ユーザーへの変更がこのコントロールから確認できるようになるまでに、最大 4 時間かかる場合があります。

> **Note**
>
> AWS Config Security Hub を使用するすべてのリージョンで を有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。グローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

IAM コンソールでユーザー情報を表示すると、[アクセスキーの有効期間]、[パスワードの有効期間]、[最終アクティビティ] の列が表示されます。これらの列の値のいずれかが 45 日より大きい場合は、それらのユーザーの認証情報を非アクティブにします。

認証情報レポートを使用してユーザーアカウントをモニタリングし、45 日以上アクティビティのないアカウントを特定することもできます。IAM コンソールから認証情報レポートを `.csv` 形式でダウンロードできます。

非アクティブなアカウント、または未使用の認証情報を特定したら、それらを非アクティブ化します。手順については、「IAM ユーザーガイド」の「IAM ユーザーパスワードの作成、変更、削除 (コンソール)」を参照してください。

[IAM.23] IAM Access Analyzer アナライザーにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::AccessAnalyzer::Analyzer`

AWS Config ルール: `tagged-accessanalyzer-analyzer` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) によって管理されるアナライザーに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。アナライザーにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、アナライザーにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベ

ストプラクティスの詳細については、「」の「AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

アナライザーにタグを追加するには、AWS 「IAM Access Analyzer API リファレンスTagResource」の「」を参照してください。

[IAM.24] IAM ロールにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::IAM::Role`

AWS Config ルール: `tagged-iam-role` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS Identity and Access Management (IAM) ロールにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。ロールにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、ロールにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

IAM ロールにタグを追加するには、「IAM ユーザーガイド」の「IAM リソースのタグ付け」を参照してください。

[IAM.25] IAM ユーザーはタグ付けする必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::IAM::User`

AWS Config ルール: `tagged-iam-user` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS Identity and Access Management (IAM) ユーザーにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。ユーザーにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、ユーザーがどのキーでもタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

IAM ユーザーにタグを追加するには、「IAM ユーザーガイド」の「IAM リソースのタグ付け」を参照してください。

[IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.19

カテゴリ： 識別 > コンプライアンス

重要度: 中

リソースタイプ: `AWS::IAM::ServerCertificate`

AWS Config ルール: `iam-server-certificate-expiration-check`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、IAM で管理されているアクティブな SSL/TLS サーバー証明書の有効期限が切れているかどうかをチェックします。期限切れの SSL/TLS サーバー証明書が削除されない場合、コントロールは失敗します。

でウェブサイトまたはアプリケーションへの HTTPS 接続を有効にするには AWS、SSL/TLS サーバー証明書が必要です。IAM または AWS Certificate Manager (ACM) を使用して、サーバー証明書を保存およびデプロイできます。ACM でサポートされていない で HTTPS 接続をサポートする必要がある場合にのみ、IAM AWS リージョン を証明書マネージャーとして使用します。IAM はプライベートキーを安全に暗号化し、暗号化されたバージョンを IAM SSL 証明書ストレージに保存します。IAM はすべての リージョンでのサーバー証明書のデプロイをサポートしていますが、 で使用するには外部プロバイダーから証明書を取得する必要があります AWS。ACM 証明書を IAM にアップロードすることはできません。さらに、IAM コンソールから証明書を管理することはできません。期限切れの SSL/TLS 証明書を削除すると、無効な証明書が誤ってリソースにデプロイされ、基盤となるアプリケーションまたはウェブサイトの信頼性が損なわれるリスクがなくなります。

修正

IAM からサーバー証明書を削除するには、「IAM ユーザーガイド」の「IAM でのサーバー証明書の管理」を参照してください。

[IAM.27] IAM ID には AWSCloudShellFullAccess ポリシーをアタッチしないでください

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.22

カテゴリ： 保護 > 安全なアクセス管理 > 安全な IAM ポリシー

重要度: 中

リソースタイプ： `AWS::IAM::Role`、`AWS::IAM::User`、 `AWS::IAM::Group`

AWS Config ルール: `iam-policy-blacklisted-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- policyArns」 : 「arn:aws:iam::aws:policy/AWSCloudShellFullAccess,arn:aws-cn:iam::aws:policy/AWSCloudShellFullAccess, arn:aws-us-gov:iam::aws:policy/AWSCloudShellFullAccess」

このコントロールは、IAM アイデンティティ (ユーザー、ロール、またはグループ) に AWS 管理ポリシーが`AWSCloudShellFullAccess`アタッチされているかどうかを確認します。IAM ID にポリシーがア`AWSCloudShellFullAccess`タッチされている場合、コントロールは失敗します。

AWS CloudShell は、 に対して CLI コマンドを実行する便利な方法を提供します AWS のサービス。AWS 管理ポリシー`AWSCloudShellFullAccess`は、 へのフルアクセスを提供します。これにより CloudShell、ユーザーのローカルシステムと CloudShell 環境間のファイルのアップロードおよびダウンロード機能が可能になります。 CloudShell 環境内では、ユーザーは sudo アクセス許可を持ち、インターネットにアクセスできます。その結果、この管理ポリシーを IAM アイデンティティにアタッチすることで、ファイル転送ソフトウェアをインストールし、 から外部のインターネットサーバー CloudShell にデータを移動できるようになります。最小特権の原則に従い、IAM ID に狭いアクセス許可をアタッチすることをお勧めします。

修正

IAM ID から`AWSCloudShellFullAccess`ポリシーをデタッチするには、「IAM ユーザーガイド」の「IAM ID アクセス許可の追加と削除」を参照してください。

[IAM.28] IAM Access Analyzer の外部アクセスアナライザーを有効にする必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.20

カテゴリ： 検出 > 検出サービス > 特権使用量のモニタリング

重要度: 高

リソースタイプ: `AWS::AccessAnalyzer::Analzyer`

AWS Config ルール: `iam-external-access-analyzer-enabled`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロール AWS アカウント は、 で IAM Access Analyzer の外部アクセスアナライザーが有効になっているかどうかをチェックします。現在選択されている で外部アクセスアナライザーが有効になっていない場合、コントロールは失敗します AWS リージョン。

IAM Access Analyzer の外部アクセスアナライザーは、Amazon Simple Storage Service (Amazon S3) バケットや IAM ロールなど、外部エンティティと共有されている組織やアカウント内のリソースを識別するのに役立ちます。これにより、リソースやデータへの意図しないアクセスを防ぐことができます。IAM Access Analyzer はリージョン別であり、各リージョンで有効にする必要があります。外部プリンシパルと共有されているリソースを識別するために、アクセスアナライザーはロジックベースの推論を使用して環境内のリソースベースのポリシーを分析します AWS 。外部アクセスアナライザーを有効にすると、組織全体またはアカウント用のアナライザーが作成されます。

修正

特定のリージョンで外部アクセスアナライザーを有効にするには、IAM ユーザーガイドの「IAM Access Analyzer の有効化」を参照してください。リソースへのアクセスをモニタリングする各リージョンでアナライザーを有効にする必要があります。

AWS IoT コントロール

これらのコントロールは AWS IoT リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[IoT.1] AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::IoT::SecurityProfile`

AWS Config ルール: `tagged-iot-securityprofile` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS IoT Core セキュリティプロファイルにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。セキュリティプロファイルにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、セキュリティプロファイルにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できま

す。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS IoT Core セキュリティプロファイルにタグを追加するには、「 AWS IoT デベロッパーガイド」の「 AWS IoT リソースのタグ付け」を参照してください。

[IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::IoT::MitigationAction`

AWS Config ルール: `tagged-iot-mitigationaction` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS IoT Core 緩和アクションにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。緩和アクションにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、緩和アクションにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS IoT Core 緩和アクションにタグを追加するには、「 AWS IoT デベロッパーガイド」の「 AWS IoT リソースのタグ付け」を参照してください。

[IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::IoT::Dimension`

AWS Config ルール: `tagged-iot-dimension` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS IoT Core ディメンションにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。ディメンションにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、ディメンションにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベ

ストプラクティスの詳細については、「」の「AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS IoT Core ディメンションにタグを追加するには、「AWS IoT デベロッパーガイド」の「AWS IoT リソースのタグ付け」を参照してください。

[IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::IoT::Authorizer`

AWS Config ルール: `tagged-iot-authorizer` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS IoT Core オーソライザーにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。オーソライザーにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、オーソライザーがキーでタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS IoT Core オーソライザーにタグを追加するには、「 AWS IoT デベロッパーガイド」の「 AWS IoT リソースのタグ付け」を参照してください。

[IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::IoT::RoleAlias`

AWS Config ルール: `tagged-iot-rolealias` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS IoT Core ロールエイリアスにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。ロールエイリアスにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、ロールエイリアスにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS IoT Core ロールエイリアスにタグを追加するには、「 AWS IoT デベロッパーガイド」の「 AWS IoT リソースのタグ付け」を参照してください。

[IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::IoT::Policy`

AWS Config ルール: `tagged-iot-policy` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS IoT Core ポリシーにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。ポリシーにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、ポリシーにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責

任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC AWSとは」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS IoT Core ポリシーにタグを追加するには、「 AWS IoT デベロッパーガイド」の「 AWS IoT リソースのタグ付け」を参照してください。

Amazon Kinesis のコントロール

これらのコントロールは Kinesis リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::Kinesis::Stream`

AWS Config ルール : `kinesis-stream-encrypted`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon Kinesis Streams が保管中にサーバー側の暗号化を使用して暗号化されているかどうかをチェックします。Amazon Kinesis Streams が、保管中にサーバー側の暗号化を使用して暗号化されていない場合、このコントロールは失敗します。

サーバー側の暗号化は、 AWS KMS keyを使用してデータを保管中になる前に自動的に暗号化する、Amazon Kinesis Data Streams の機能です。データは、Kinesis ストリームストレージレイヤーに書き込まれる前に暗号化され、ストレージから取得された後で復号されます。これにより、Amazon Kinesis Data Streams サービス内に保管中のデータは暗号化されます。

修正

Kinesis Streams でサーバー側の暗号化を有効にする方法については、「Amazon Kinesis Data Streams デベロッパーガイド」の「サーバー側の暗号化を使用する」を参照してください。

[Kinesis.2] Kinesis ストリームにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::Kinesis::Stream`

AWS Configルール: `tagged-kinesis-stream` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon Kinesis データストリームに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。データストリームにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、データストリームにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Kinesis データストリームにタグを追加するには、Amazon Kinesis デベロッパーガイド」の「Amazon Kinesis Data Streams でのストリームのタグ付け」を参照してください。 Amazon Kinesis

AWS Key Management Service コントロール

これらのコントロールは AWS KMS リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください

関連する要件: NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(3)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::IAM::Policy`

AWS Config ルール : `iam-customer-policy-blocked-kms-actions`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt` (カスタマイズ不可)
- `excludePermissionBoundaryPolicy: True` (カスタマイズ不可)

IAM カスタマー管理ポリシーのデフォルトバージョンで、プリンシパルがすべてのリソースで復 AWS KMS 号アクションを使用できるかどうかをチェックします。ポリシーがすべての KMS キーに対して `kms:Decrypt` または `kms:ReEncryptFrom` のアクションを許可するのに十分にオープンな場合、このコントロールは失敗します。

コントロールはリソース要素の KMS キーのみをチェックし、ポリシーの Condition 要素の条件は考慮しません。このコントロールは、添付済みのカスタマーマネージドポリシーと添付されていないカスタマーマネージドポリシーの両方を評価します。インラインポリシーや AWS 管理ポリシーはチェックされません。

を使用すると AWS KMS、KMS キーを使用できるユーザーを制御し、暗号化されたデータにアクセスできます。IAM ポリシーは、アイデンティティ (ユーザー、グループ、またはロール) がどのリソースに対してどのアクションを実行できるかを定義します。セキュリティのベストプラクティスに従って、 では最小特権を許可することを AWS 推奨しています。つまり、ID に付与するのは `kms:Decrypt` または `kms:ReEncryptFrom` 許可と、タスクの実行に必要なキーのみにする必要があります。そうでない場合、ユーザーはデータに適さないキーを使用する可能性があります。

すべてのキーに対する許可を付与する代わりに、ユーザーが暗号化されたデータにアクセスするために必要な最小限のキーのセットを決定します。次に、ユーザーがそれらのキーのみを使用できるよう

にするポリシーを設計します。例えば、すべての KMS キーに kms:Decrypt 許可を付与しないでください。代わりに、アカウントの特定のリージョン内のキーのみに kms:Decrypt を許可します。最小特権のプリンシパルを採用することで、意図しないデータ開示のリスクを減らすことができます。

修正

IAM カスタマー管理ポリシーを変更するには、「IAM ユーザーガイド」の「カスタマー管理ポリシーの編集」を参照してください。Resource フィールドのポリシーを編集する際、復号化アクションを許可する特定の 1 つまたは複数キーの Amazon リソースネーム (ARN) を指定します。

[KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください

関連する要件: NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(3)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ :

- AWS::IAM::Group
- AWS::IAM::Role
- AWS::IAM::User

AWS Config ルール : iam-inline-policy-blocked-kms-actions

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt (カスタマイズ不可)

このコントロールは、IAM アイデンティティ (ロール、ユーザー、またはグループ) に埋め込まれているインラインポリシーが、すべての KMS キーに対する復 AWS KMS 号化および再暗号化

アクションを許可しているかどうかをチェックします。ポリシーがすべての KMS キーに対して `kms:Decrypt` または `kms:ReEncryptFrom` のアクションを許可するのに十分にオープンな場合、このコントロールは失敗します。

コントロールはリソース要素の KMS キーのみをチェックし、ポリシーの Condition 要素の条件は考慮しません。

を使用すると AWS KMS、KMS キーを使用できるユーザーを制御し、暗号化されたデータにアクセスできます。IAM ポリシーは、アイデンティティ (ユーザー、グループ、またはロール) がどのリソースに対してどのアクションを実行できるかを定義します。セキュリティのベストプラクティスに従って、 では最小特権を許可することを AWS 推奨しています。つまり、ID には必要な許可のみを、タスクの実行に必要なキーにのみ付与する必要があります。そうでない場合、ユーザーはデータに適さないキーを使用する可能性があります。

すべてのキーに対する許可を付与する代わりに、ユーザーが暗号化されたデータにアクセスするために必要なキーの最小セットを決定します。次に、ユーザーがそれらのキーのみを使用できるようにするポリシーを設計します。例えば、すべての KMS キーに `kms:Decrypt` 許可を付与しないでください。代わりに、アカウントの特定リージョンでの特定のキーにのみ許可を付与してください。最小特権のプリンシパルを採用することで、意図しないデータ開示のリスクを減らすことができます。

修正

IAM インラインポリシーを変更するには、「IAM ユーザーガイド」の「インラインポリシーの編集」を参照してください。`Resource` フィールドのポリシーを編集する際、復号化アクションを許可する特定の 1 つまたは複数キーの Amazon リソースネーム (ARN) を指定します。

[KMS.3] 意図せずに削除 AWS KMS keys しないでください

関連する要件: NIST.800-53.r5 SC-12、NIST.800-53.r5 SC-12(2)

カテゴリ: 保護 > データ保護 > データ削除保護

重要度: 非常事態

リソースタイプ: `AWS::KMS::Key`

AWS Config ルール: `kms-cmk-not-scheduled-for-deletion-2` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、KMS キーの削除がスケジュール済みかどうかをチェックします。KMS キーの削除がスケジュール済みの場合、コントロールは失敗します。

KMS キーは、一度削除すると復元できません。KMS キーで暗号化されたデータも、KMS キーが削除された場合は永久に回復できません。削除予定の KMS キーで、意味のあるデータが暗号化されている場合、意図的に暗号化消去を実行しない限り、データの復号化または新しい KMS キーでデータの再暗号化を検討してください。

KMS キーの削除がスケジュール済みで、誤ってスケジュールされた場合、削除の取り消し時間を確保するために、強制的に待ち時間が適用されます。デフォルトの待機期間は 30 日間ですが、KMS キーの削除がスケジュールされている場合は 7 日以内に短縮できます。待機期間中、スケジュール済みの削除はキャンセルすることができ、KMS キーは削除されません。

KMS キーの削除の詳細については、「AWS Key Management Service 開発者ガイド」の「KMS キーの削除」を参照してください。

修正

スケジュール済み KMS キーの削除をキャンセルには、「AWS Key Management Service デベロッパーガイド」の「キー削除のスケジュールとキャンセル (コンソール)」内にある「キーの削除をキャンセルするには」を参照してください。

[KMS.4] AWS KMS キーローテーションを有効にする必要があります

関連する要件： PCI DSS v3.2.1/3.6.4、CIS AWS Foundations Benchmark v3.0.0/3.6、CIS AWS Foundations Benchmark v1.4.0/3.8、CIS AWS Foundations Benchmark v1.2.0/2.8、NIST.800-53.r5 SC-12、NIST.800-53.r5 SC-12(2)、NIST.800-53.r5 SC-28(3)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::KMS::Key`

AWS Config ルール: `cmk-backing-key-rotation-enabled`

スケジュールタイプ: 定期的

パラメータ: なし

AWS KMS では、 に保存されているキーマテリアルであり、KMS キーのキー ID AWS KMS に関連付けられているバッキングキーをローテーションできます。バッキングキーは、暗号化や復号化などの暗号化オペレーションを実行するために使用されます。現在、キーの自動ローテーションでは以前のすべてのバッキングキーが保持されるため、暗号化したデータは透過的に復号化できます。

CIS では、KMS キーのローテーションを有効にすることを推奨しています。新しいキーで暗号化されたデータは、漏洩した可能性がある以前のキーではアクセスできないため、暗号化キーをローテーションすることで、漏洩したキーにより起こる可能性のある被害を減らすことができます。

修正

KMS キーローテーションを有効にするには、「AWS Key Management Service デベロッパーガイド」の「自動キーローテーションを有効または無効にする方法」を参照してください。

AWS Lambda コントロール

これらのコントロールは Lambda リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 非常事態

リソースタイプ: `AWS::Lambda::Function`

AWS Config ルール : `lambda-function-public-access-prohibited`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Lambda 関数リソースベースポリシーがアカウントの外部からのパブリックアクセスを禁止しているかどうかをチェックします。パブリックアクセスが許可されている場合、コントロールは失敗します。Lambda 関数が Amazon S3 から呼び出され、ポリシーが `AWS:SourceAccount` などパブリックアクセスを制限する条件が含まれていない場合も、コントロールは失敗します。より細かくアクセスするには、バケットポリシーで他の S3 条件を `AWS:SourceAccount` と併用することをおすすめします。

Lambda 関数は、関数コードへの意図しないアクセスを許可する可能性があるため、パブリックからアクセスできない必要があります。

修正

この問題を修正するには、関数のリソースベースのポリシーを更新して許可を削除するか、`AWS:SourceAccount` 条件を追加します。リソースベースのポリシーは、Lambda API または からのみ更新できます AWS CLI。

まず、Lambda コンソールでリソースベースのポリシーを確認します。`"*"` や `{ "AWS": "*" }` など、ポリシーをパブリックにする `Principal` フィールド値を持つポリシーステートメントを特定します。

ポリシーはコンソールから編集できません。関数から許可を削除するには、 AWS CLIから `remove-permission` コマンドを作動します。

```
$ aws lambda remove-permission --function-name <function-name> --statement-
id <statement-id>
```

`<function-name>` を Lambda 関数の名前で置き換え、*`<statement-id>`* を削除するステートメントのステートメント ID (`Sid`) に置き換えます。

[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)

カテゴリ: 保護 > セキュアな開発

重要度: 中

リソースタイプ: `AWS::Lambda::Function`

AWS Config ルール : `lambda-function-settings-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `runtime`: `dotnet8, dotnet6, java21, java17, java11, java8.al2, nodejs20.x, nodejs18.x, nodejs16.x, python3.12, python3.11, python3.10, python3.9, python3.8, ruby3.3, ruby3.2` (カスタマイズ不可)

このコントロールは、 AWS Lambda 関数のランタイム設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかをチェックします。Lambda 関数がサポートされているランタイムを使用していない場合、以前にパラメータで説明したようにコントロールは失敗します。Security Hub は、パッケージタイプが `Image` の関数を無視します。

Lambda ランタイムは、メンテナンスとセキュリティの更新の対象となる OS、プログラミング言語、およびソフトウェアライブラリの組み合わせを中心に構築されています。ランタイムコンポーネントがセキュリティアップデートでサポート対象外となった場合、Lambda はこのランタイムを非推奨にします。非推奨のランタイムを使用する関数を作成することはできませんが、この関数は呼び出しイベントを処理するために引き続き使用できます。Lambda 関数が最新であり、非推奨のランタイム環境を使用しないようにすることをお勧めします。サポートされているランタイムのリストについては、「 AWS Lambda デベロッパーガイド」の「Lambda ランタイム」を参照してください。

修正

サポートされているランタイムおよび非推奨スケジュールの詳細については、「AWS Lambda デベロッパーガイド」の「ランタイムの非推奨化に関するポリシー」を参照してください。ランタイムを最新バージョンに移行するときは、言語の発行元からの構文とガイダンスに従ってください。また、ランタイム更新を適用して、ランタイムバージョンの非互換性がまれに発生する場合にワークロードに影響を与えるリスクを軽減することをお勧めします。

[Lambda.3] Lambda 関数は VPC 内に存在する必要があります

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5

SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 低

リソースタイプ: `AWS::Lambda::Function`

AWS Config ルール: `lambda-inside-vpc`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Lambda 関数が Virtual Private Cloud (VPC) にデプロイされているかどうかをチェックします。Lambda 関数が VPC にデプロイされていない場合、コントロールは失敗します。Security Hub は、パブリック到達可能性を判断するために VPC サブネットルーティング設定を評価しません。Lambda@Edge リソースに関する失敗の結果が表示される場合があります。

VPC にリソースをデプロイすると、ネットワーク設定のセキュリティと制御が強化されます。このようなデプロイでは、複数のアベイラビリティーゾーンにわたってスケーラビリティと高い耐障害性も提供されます。VPC デプロイをカスタマイズして、さまざまなアプリケーション要件を満たすことができます。

修正

VPC のプライベートサブネットに接続する既存の機能を設定するには、「AWS Lambda デベロッパーガイド」の「VPC アクセスの設定」を参照してください。可用性を高めるためにプライベートサブネットを少なくとも 2 つ選択し、機能の接続要件を満たすセキュリティグループを少なくとも 1 つ選択することをお勧めします。

[Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::Lambda::Function`

AWS Config ルール : `lambda-vpc-multi-az-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`availabilityZones`	アベイラビリティーゾーンの最小数	列挙型	`2, 3, 4, 5, 6`	`2`

このコントロールは、仮想プライベートクラウド (VPC) に接続する AWS Lambda 関数が、少なくとも指定された数のアベイラビリティーゾーン (AZsで動作しているかどうかを確認します。少なくとも指定された数の AZ で関数が動作していない場合、コントロールは失敗します。AZ の最小数に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 2 つの AZ を使用します。

複数の AZs にリソースをデプロイすることは、アーキテクチャ内で高可用性を確保するための AWS ベストプラクティスです。可用性は、機密性、完全性、可用性から成り立つセキュリティモデルの 3 要素における中心的な柱です。VPC に接続するすべての Lambda 関数には、1 つのゾーンで障害が発生しても運用が完全に中断されないように、マルチ AZ 配置がある必要があります。

修正

お客様のアカウントで VPC に接続するように関数を設定する場合は、複数のアベイラビリティーゾーン (AZ) でサブネットを指定することで、高可用性を確保します。手順については、「AWS Lambda デベロッパーガイド」の「VPC アクセスの設定」を参照してください。

Lambda は、複数のアベイラビリティーゾーン (AZ) で他の関数を自動的に実行し、1 つのゾーンでサービスの中断が発生した場合にも、関数をイベントの処理に使用できることを保証します。

[Lambda.6] Lambda 関数にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::Lambda::Function`

AWS Config ルール: `tagged-lambda-function` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS Lambda 関数にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。関数にタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、関数にキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Lambda 関数にタグを追加するには、「 AWS Lambda デベロッパーガイド」の「Lambda 関数でのタグの使用」を参照してください。

Amazon Macie コントロール

これらのコントロールは Macie リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Macie.1] Amazon Macie を有効にする必要があります

関連する要件: NIST.800-53.r5 CA-7、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 RA-5、NIST.800-53.r5 SA-8(19)、NIST.800-53.r5 SI-4

カテゴリ: 検出 > 検出サービス

重要度: 中

リソースタイプ: `AWS::::Account`

AWS Config ルール: `macie-status-check`

スケジュールタイプ: 定期的

このコントロールは、アカウントで Amazon Macie が有効になっているかどうかをチェックします。アカウントに対して Macie が有効になっていない場合、コントロールは失敗します。

Amazon Macie は、機械学習とパターンマッチングを使用して機密データを検出し、データセキュリティリスクを可視化し、それらのリスクに対する自動保護を可能にします。Macie は、Amazon Simple Storage Service (Amazon S3) バケットのセキュリティとアクセスコントロールを自動的かつ

継続的に評価し、検出結果を生成して、Amazon S3 データのセキュリティまたはプライバシーに関する潜在的な問題について通知します。また、Macie は、Amazon S3 に保存している個人を特定できる情報 (PII) などの機密データを詳細に把握できるよう、そのようなデータの検出とレポートを自動化します。詳細については、「Amazon Macie ユーザーガイド」を参照してください。

修正

Macie を有効にするには、「Amazon Macie ユーザーガイド」の「Macie を有効化する」を参照してください。

[Macie.2] Macie 自動機密データ検出を有効にする必要があります

関連する要件: NIST.800-53.r5 CA-7、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 RA-5、NIST.800-53.r5 SA-8(19)、NIST.800-53.r5 SI-4

カテゴリ: 検出 > 検出サービス

重要度: 高

リソースタイプ: `AWS::::Account`

AWS Config ルール: `macie-auto-sensitive-data-discovery-check`

スケジュールタイプ: 定期的

このコントロールは、Amazon Macie 管理者アカウントで機密データの自動検出が有効になっているかどうかをチェックします。Macie 管理者アカウントで機密データの自動検出が有効になっていない場合、コントロールは失敗します。このコントロールは管理者アカウントにのみ適用されます。

Macie は、Amazon Simple Storage Service (Amazon S3) バケット内の個人を特定できる情報 (PII) などの機密データの検出と報告を自動化します。機密データの自動検出により、Macie はバケットインベントリを継続的に評価し、サンプリング技術を使用してバケットから代表的な S3 オブジェクトを特定して選択します。その後、Macie は選択したオブジェクトを分析し、機密データを検査します。分析が進むにつれて、Macie は S3 データに関して提供する統計、インベントリデータ、およびその他の情報を更新します。Macie は、検出した機密データを報告する検出結果も生成します。

修正

S3 バケット内のオブジェクトを分析するための機密データ自動検出ジョブを作成および設定するには、Amazon Macie ユーザーガイド」の「アカウントの機密データ自動検出の設定」を参照してください。

Amazon MSK コントロール

これらのコントロールは、Amazon Managed Streaming for Apache Kafka (Amazon MSK) リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります

関連する要件: NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::MSK::Cluster`

AWS Config ルール : `msk-in-cluster-node-require-tls`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon MSK クラスターがクラスターのブローカーノード間で HTTPS (TLS) で転送中に暗号化されているかどうかをチェックします。クラスターブローカーノード接続でプレーンテキスト通信が有効になっていると、コントロールは失敗します。

HTTPS は、TLS を使用してデータを移動するため、セキュリティをさらに強化します。また、潜在的な攻撃者がネットワークトラフィックを傍受または操作するために person-in-the-middle または同様の攻撃を使用することを防ぐのに役立ちます。デフォルトでは、Amazon MSK は転送中のデータを TLS で暗号化します。ただし、このデフォルトはクラスターの作成時に上書きできます。ブローカーノード接続には、HTTPS (TLS) 経由の暗号化接続を使用することをお勧めします。

修正

MSK クラスターの暗号化設定を更新するには、「Amazon Managed Streaming for Apache Kafka デベロッパーガイド」の「クラスターのセキュリティ設定の更新」を参照してください。

[MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります

関連する要件: NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::MSK::Cluster`

AWS Config ルール : `msk-enhanced-monitoring-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon MSK クラスターに、少なくとも `PER_TOPIC_PER_BROKER` のモニタリングレベルで指定された拡張モニタリングが設定されているかどうかをチェックします。クラスターのモニタリングレベルが `DEFAULT` または `PER_BROKER` に設定されている場合、コントロールは失敗します。

`PER_TOPIC_PER_BROKER` モニタリングレベルでは、MSK クラスターのパフォーマンスをより詳細に把握できる他、CPU やメモリ使用量などのリソース使用率に関連するメトリクスも表示されます。これにより、個々のトピックおよびブローカーのパフォーマンスボトルネックやリソース使用パターンを特定できるようになります。この可視性により、Kafka ブローカーのパフォーマンスを最適化できます。

修正

MSK クラスターの拡張モニタリングを設定するには、以下の手順を実行します。

1. https://console.aws.amazon.com/msk/home?region=us-east-1#/home/ で Amazon MSK コンソールを開きます。
2. ナビゲーションペインで [クラスター] を選択します。次に、クラスターを選択します。
3. [アクション] で [モニタリングを編集] を選択します。
4. [拡張トピックレベルモニタリング] のオプションを選択します。
5. [変更の保存] を選択します。

モニタリングレベルの詳細については、「Amazon Managed Streaming for Apache Kafka デベロッパーガイド」の「クラスターのセキュリティ設定の更新」を参照してください。

Amazon MQ コントロール

これらのコントロールは Amazon MQ リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch

関連する要件： NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-12、NIST.800-53.r5 SI-4

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::AmazonMQ::Broker`

AWS Config ルール : `mq-cloudwatch-audit-log-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon MQ ActiveMQ ブローカーが監査ログを Amazon CloudWatch Logs にストリーミングするかどうかをチェックします。ブローカーが監査ログを CloudWatch Logs にストリーミングしない場合、コントロールは失敗します。

ActiveMQ ブローカーログを CloudWatch Logs に発行することで、セキュリティ関連情報の可視性を高める CloudWatch アラームとメトリクスを作成できます。

修正

ActiveMQ ブローカーログを CloudWatch ログにストリーミングするには、Amazon MQ デベロッパーガイド」の「Amazon MQ for ActiveMQ ログの設定」を参照してください。 Amazon MQ

[MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります

関連する要件： NIST.800-53.r5 CM-3、NIST.800-53.r5 SI-2

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 低

リソースタイプ: `AWS::AmazonMQ::Broker`

AWS Config ルール : `mq-auto-minor-version-upgrade-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon MQ ブローカーで自動マイナーバージョンアップグレードが有効になっているかどうかをチェックします。ブローカーで自動マイナーバージョンアップグレードが有効になっていない場合、コントロールは失敗します。

Amazon MQ が新しいブローカーエンジンバージョンをリリースしてサポートしているため、変更は既存のアプリケーションと下位互換性があり、既存の機能を非推奨にしません。ブローカーエンジンの自動バージョン更新により、セキュリティリスクからの保護、バグの修正、機能の向上に役立ちます。

> **Note**
>
> 自動マイナーバージョンアップグレードに関連付けられたブローカーが最新のパッチにあり、サポートされなくなった場合は、アップグレードを手動で実行する必要があります。

修正

MQ ブローカーの自動マイナーバージョンアップグレードを有効にするには、Amazon MQ デベロッパーガイド」の「マイナーエンジンバージョンの自動アップグレード」を参照してください。

[MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::AmazonMQ::Broker`

AWS Config ルール: `tagged-amazonmq-broker` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、Amazon MQ ブローカーにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。ブローカーにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、ブローカーがキーでタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Amazon MQ ブローカーにタグを追加するには、Amazon MQ デベロッパーガイド」の「リソースのタグ付け」を参照してください。

[MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 低

リソースタイプ: `AWS::AmazonMQ::Broker`

AWS Config ルール : `mq-active-deployment-mode`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon MQ ActiveMQ ブローカーのデプロイモードがアクティブ/スタンバイに設定されているかどうかを確認します。単一インスタンスブローカー (デフォルトで有効) がデプロイモードに設定されている場合、コントロールは失敗します。

アクティブ/スタンバイデプロイにより、 AWS リージョン内の Amazon MQ ActiveMQ ブローカーの可用性が高くなります。アクティブ/スタンバイのデプロイモードには、2 つの異なるアベイラビリティーゾーンの 2 つのブローカーインスタンスが冗長ペアとして設定されています。これらのブローカーはアプリケーションと同期して通信するため、障害発生時のダウンタイムやデータ損失を減らすことができます。

修正

アクティブ/スタンバイデプロイモードで新しい ActiveMQ ブローカーを作成するには、「Amazon MQ デベロッパーガイド」の「ActiveMQ ブローカーの作成と設定」を参照してください。[デプロイモード] で、[アクティブ/スタンバイブローカー] を選択します。既存のブローカーのデプロイモードは変更できません。代わりに、新しいブローカーを作成し、古いブローカーから設定をコピーする必要があります。

[MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 低

リソースタイプ: `AWS::AmazonMQ::Broker`

AWS Config ルール : `mq-rabbit-deployment-mode`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon MQ RabbitMQ ブローカーのデプロイモードがクラスターデプロイに設定されているかどうかを確認します。単一インスタンスブローカー (デフォルトで有効) がデプロイモードに設定されている場合、コントロールは失敗します。

クラスターデプロイにより、 AWS リージョン内の Amazon MQ RabbitMQ ブローカーの可用性が高くなります。クラスターデプロイは、3 つの RabbitMQ ブローカーノードを論理的にグループ化したもので、それぞれに独自の Amazon Elastic Block Store (Amazon EBS) ボリュームと 1 つの共有状態があります。クラスターデプロイは、データがクラスター内の全ノードに確実に複製され、障害発生時のダウンタイムとデータ損失が減少するようにします。

修正

クラスターデプロイモードで新しい RabbitMQ ブローカーを作成するには、「Amazon MQ デベロッパーガイド」の「RabbitMQ ブローカーの作成と接続」を参照してください。[デプロイモード] で、[クラスターデプロイ] を選択します。既存のブローカーのデプロイモードは変更できません。代わりに、新しいブローカーを作成し、古いブローカーから設定をコピーする必要があります。

Amazon Neptune コントロール

これらのコントロールは Neptune リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール : `neptune-cluster-encrypted`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Neptune DB クラスターが保管中に暗号化されているかどうかをチェックします。Neptune DB クラスターが保管中に暗号化されていない場合、コントロールは失敗します。

保管中のデータとは、永続的な不揮発性ストレージに任意の期間保管されているデータを指します。暗号化は、このようなデータの機密性を保護し、権限のないユーザーがデータにアクセスするリスクを低減するのに役立ちます。Neptune DB クラスターを暗号化することで、データとメタデータを不正アクセスから保護します。また、本番ファイルシステムの data-at-rest 暗号化に関するコンプライアンス要件を満たします。

修正

Neptune DB クラスターを作成するときに、保管中の暗号化を有効にできます。クラスターを作成した後で暗号化設定を変更することはできません。詳細については、「Neptune ユーザーガイド」の「Encrypting Neptune resources at rest」を参照してください。

[Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります

関連する要件: NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(1)、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 AU-6(5)、NIST.800-53.r5 AU-7(1)、NIST.800-53.r5 AU-9(7)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-20、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-4(5)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール : `neptune-cluster-cloudwatch-log-export-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Neptune DB クラスターが監査ログを Amazon CloudWatch Logs に発行するかどうかをチェックします。Neptune DB クラスターが監査ログを CloudWatch Logs に発行しない場合、コントロールは失敗します。 は に設定`EnableCloudWatchLogsExport`する必要がありま す`Audit`。

Amazon Neptune と Amazon CloudWatch は統合されているため、パフォーマンスメトリクスを収集して分析できます。Neptune は にメトリクスを自動的に送信 CloudWatch し、 CloudWatch アラームもサポートします。監査ログは高度なカスタマイズが可能です。データベースを監査すると、データに対する各操作をモニタリングし、どのデータベースクラスターがどのようにアクセスされたかに関する情報などを監査証跡に記録できます。Neptune DB クラスターのモニタリングに役立つ CloudWatch ように、これらのログを に送信することをお勧めします。

修正

Neptune 監査ログを CloudWatch ログに発行するには、「Neptune ユーザーガイド」の「Amazon CloudWatch Logs への Neptune ログの発行」を参照してください。 [Log exports] セクションで、[Audit] を選択します。

[Neptune.3] Neptune DB クラススナップショットはパブリックにしないでください

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 非常事態

リソースタイプ: `AWS::RDS::DBClusterSnapshot`

AWS Config ルール : neptune-cluster-snapshot-public-prohibited

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Neptune の手動 DB クラススナップショットがパブリックかどうかをチェックします。Neptune の手動 DB クラススナップショットがパブリックの場合、コントロールは失敗します。

Neptune DB クラスターの手動スナップショットは、意図しない限りパブリックにしないでください。暗号化されていない手動スナップショットをパブリックとして共有すると、すべての AWS アカウントでこのスナップショットを使用できるようになります。パブリックスナップショットは、意図しないデータ漏えいにつながる可能性があります。

修正

Neptune の手動 DB クラススナップショットからパブリックアクセスを削除するには、「Neptune ユーザーガイド」の「Sharing a DB cluster snapshot」を参照してください。

[Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

カテゴリ: 保護 > データ保護 > データ削除保護

重要度: 低

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール : neptune-cluster-deletion-protection-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Neptune DB クラスターの削除保護が有効になっているかどうかをチェックします。Neptune DB クラスターで削除保護が有効になっていない場合、コントロールは失敗します。

クラスターの削除保護を有効にすることで、偶発的なデータベース削除や権限のないユーザーによる削除に対して保護の強化を提供します。削除保護が有効の間、Neptune DB クラスターは削除できません。削除リクエストを成功させるには、まず削除保護を無効にする必要があります。

修正

既存の Neptune DB クラスターの削除保護を有効にするには、「Amazon Aurora ユーザーガイド」の「コンソール、CLI、API を使用した DB クラスターの変更」を参照してください。

[Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります

関連する要件: NIST.800-53.r5 SI-12

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

重要度: 中

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール : `neptune-cluster-backup-retention-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値	
`minimumBackupRetentionPeriod`	最小バックアップ保持期間 (日数)	整数	7 ~ 35	7	

このコントロールは、Neptune DB クラスターで自動バックアップが有効になっているかどうか、およびバックアップ保持期間が指定された時間枠以上であるかどうかをチェックします。Neptune DB クラスターのバックアップが有効になっていない場合や、保持期間が指定された時間枠未満の場合、コントロールは失敗します。バックアップ保持期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 7 日を使用します。

バックアップは、セキュリティインシデントからの迅速な復元と、システムの耐障害性の強化に役立ちます。Neptune DB クラスターのバックアップを自動化すると、システムを特定の時点に復元し、ダウンタイムとデータ損失を最小限に抑えることができます。

修正

Neptune DB クラスターの自動バックアップを有効にしてバックアップ保持期間を設定するには、「Amazon RDS ユーザーガイド」の「自動バックアップの有効化」を参照してください。[バックアップ保持期間] で 7 以上の値を選択します。

[Neptune.6] Neptune DB クラススナップショットは、保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-7(18)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::RDS::DBClusterSnapshot`

AWS Config ルール : `neptune-cluster-snapshot-encrypted`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Neptune DB クラススナップショットが保管中に暗号化されているかどうかをチェックします。Neptune DB クラスターが保管中に暗号化されていない場合、コントロールは失敗します。

保管中のデータとは、永続的な不揮発性ストレージに任意の期間保管されているデータを指します。暗号化は、このようなデータの機密性を保護し、権限のないユーザーがデータにアクセスするリスクを低減するのに役立ちます。Neptune DB クラススナップショット内のデータは、セキュリティを強化するために、保管中に暗号化する必要があります。

修正

既存の Neptune DB クラススナップショットは暗号化できません。代わりに、スナップショットを新しい DB クラスターに復元し、このクラスターで暗号化を有効にする必要があります。これで、

暗号化されたクラスターから、暗号化されたスナップショットを作成できます。手順については、「Neptune ユーザーガイド」の「Restoring from a DB cluster snapshot」と「Creating a DB cluster snapshot in Neptune」を参照してください。

[Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理 > パスワードレス認証

重要度: 中

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール : `neptune-cluster-iam-database-authentication`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Neptune DB クラスターで IAM データベース認証が有効になっているかどうかをチェックします。Neptune DB クラスターで IAM データベース認証が有効になっていない場合、コントロールは失敗します。

Amazon Neptune データベースクラスターの IAM データベース認証では、認証は IAM を使用して外部で管理されるため、ユーザー認証情報をデータベース設定内に保存する必要がなくなります。IAM データベース認証が有効になっている場合、各リクエストは署名バージョン AWS 4 を使用して署名する必要があります。

修正

デフォルトでは、Neptune DB クラスターの作成時、IAM データベース認証は無効になっています。有効にするには、「Neptune ユーザーガイド」の「Enabling IAM database authentication in Neptune」を参照してください。

[Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール : neptune-cluster-copy-tags-to-snapshot-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、スナップショットの作成時に、すべてのタグをスナップショットにコピーするように Neptune DB クラスターが設定されているかどうかをチェックします。Neptune DB クラスターがタグをスナップショットにコピーするように設定されていない場合、コントロールは失敗します。

IT アセットの身分証明書とインベントリはガバナンスとセキュリティの重要な側面です。スナップショットは、親 Amazon RDS データベースクラスターと同じ方法でタグ付けする必要があります。タグをコピーすると、DB スナップショットと親データベースクラスターのメタデータが確実に一致し、また、DB スナップショットと親 DB インスタンスのアクセスポリシーが確実に一致するようになります。

修正

Neptune DB クラスターのスナップショットにタグをコピーするには、「Neptune ユーザーガイド」の「Copying tags in Neptune」を参照してください。

[Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール : neptune-cluster-multi-az-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon Neptune DB クラスターで、複数のアベイラビリティーゾーン (AZ) にリードレプリカインスタンスがあるかどうかをチェックします。クラスターが 1 つの AZ にのみデプロイされている場合、コントロールは失敗します。

AZ が使用できなくなった場合や、定期的なメンテナンスイベントでは、リードレプリカがプライマリインスタンスのフェイルオーバーターゲットとして機能します。つまり、プライマリインスタンスが失敗した場合、Neptune はリードレプリカをプライマリインスタンスに昇格します。対照的に、DB クラスターにリードレプリカインスタンスが含まれていない場合、プライマリインスタンスが再作成されるまで障害が発生しても、DB クラスターは使用できないままになります。プライマリインスタンスの再作成は、リードレプリカの昇格よりもかなり時間がかかります。高可用性を確保するために、プライマリインスタンスと同じ DB インスタンスクラスを持ち、プライマリインスタンスとは異なる AZ に配置する 1 つ以上のリードレプリカインスタンスを作成することをお勧めします。

修正

Neptune DB クラスターを複数の AZ にデプロイするには、「Neptune ユーザーガイド」の「Neptune DB クラスター内のリードレプリカ DB インスタンス」を参照してください。

AWS Network Firewall コントロール

これらのコントロールは Network Firewall リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔NetworkFirewall.1] Network Firewall ファイアウォールは複数のアベイラビリティーゾーンにデプロイする必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::NetworkFirewall::Firewall`

AWS Config ルール : `netfw-multi-az-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 で管理されるファイアウォール AWS Network Firewall が複数のアベイラビリティーゾーン (AZsにデプロイされているかどうかを評価します。ファイアウォールが 1 つの AZ にのみデプロイされている場合、コントロールは失敗します。

AWS グローバルインフラストラクチャには複数の が含まれています AWS リージョン。AZ は、低レイテンシー、高スループット、高冗長性のネットワークで接続されている、各リージョン内の物理的に独立し隔離されたロケーションです。Network Firewall ファイアウォールを複数の AZ にデプロイすることで、AZ 間でトラフィックを分散およびシフトできるため、可用性の高いソリューションを設計できるようになります。

修正

Network Firewall ファイアウォールを複数の AZ にデプロイする

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、ネットワークファイアウォールの下にあるファイアウォールを選択します。
3. [ファイアウォール] ページで、編集するファイアウォールを選択します。
4. ファイアウォールの詳細ページで、[ファイアウォールの詳細] タブを選択します。
5. [関連付けられたポリシーと VPC] セクションで、[編集] を選択します。
6. 新しい AZ を追加するには、[新しいサブネットを追加] を選択します。使用する AZ とサブネットを選択します。少なくとも 2 つの AZ を選択するようにします。
7. [保存] を選択します。

〔NetworkFirewall.2] Network Firewall のログ記録を有効にする必要があります

関連する要件: NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 AU-9(7)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::NetworkFirewall::LoggingConfiguration`

AWS Config ルール: `netfw-logging-enabled`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、 AWS Network Firewall ファイアウォールでログ記録が有効になっているかどうかをチェックします。少なくとも 1 つのログタイプでログ記録が有効になっていない場合、またはログ記録先が存在しない場合、コントロールは失敗します。

ログ記録はファイアウォールの信頼性、可用性、パフォーマンスの維持に有益です。Network Firewall でログを記録すると、ステートフルエンジンがパケットフローを受信した時間、パケットフローに関する詳細情報、パケットフローに対して実行されたステートフルルールアクションなど、ネットワークトラフィックに関する詳細情報が得られます。

修正

ファイアウォールのログ記録を有効にするには、「AWS Network Firewall 開発者ガイド」の「Updating a firewall's logging configuration」を参照してください。

〔NetworkFirewall.3] Network Firewall ポリシーには、少なくとも 1 つのルールグループが関連付けられている必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config ルール : `netfw-policy-rule-group-associated`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Network Firewall ポリシーに、ステートフルなルールグループかステートレスなルールグループのいずれかが関連付けられているかどうかをチェックします。ステートレスまたはステートフルなルールグループが割り当てられていない場合、このコントロールは失敗します。

ファイアウォールポリシーは、ファイアウォールが Amazon Virtual Private Cloud (Amazon VPC) のトラフィックをモニタリングおよび処理する方法を定義します。ステートレスおよびステートフルのルールグループの設定は、パケットとトラフィックフローのフィルタリングに役立ち、デフォルトのトラフィック処理を定義します。

修正

Network Firewall ポリシーにルールグループを追加する方法については、「AWS Network Firewall デベロッパーガイド」の「Updating a firewall policy」(ファイアウォールポリシーの更新) を参照してください。ルールグループの作成および管理方法については、「AWS Network Firewallのルールグループ」を参照してください。

〔NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、フルパケットに対してドロップまたは転送する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config ルール : `netfw-policy-default-action-full-packets`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `statelessDefaultActions: aws:drop,aws:forward_to_sfe` (カスタマイズ不可)

このコントロールは、Network Firewall ポリシーの完全なパケットに対するデフォルトのステートレスアクションが、ドロップまたは転送かどうかをチェックします。`Drop` または `Forward` が選択されている場合、コントロールはパスします。`Pass` が選択されている場合、このコントロールは失敗します。

ファイアウォールポリシーは、ファイアウォールが Amazon VPC のトラフィックをモニタリングおよび処理する方法を定義します。ステートレスおよびステートフルのルールグループを設定し、パケットとトラフィックフローをフィルタリングします。`Pass` をデフォルトに設定すると、意図しないトラフィックが許可される可能性があります。

修正

ファイアウォール ポリシーを変更する方法については、「AWS Network Firewall デベロッパーガイド」の「ファイアウォールポリシーの更新」 を参照してください。[ステートレスデフォルトアク

ション] で、[編集] を選択します。続いて、[アクション] として、[ドロップ] または [ステートフルルールグループに転送] を選択します。

〔NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、フラグメント化されたパケットに対してドロップまたは転送する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config ルール : `netfw-policy-default-action-fragment-packets`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe` (カスタマイズ不可)

このコントロールは、Network Firewall ポリシーの断片化されたパケットに対するデフォルトのステートレスアクションが、ドロップまたは転送かどうかをチェックします。`Drop` または `Forward` が選択されている場合、コントロールはパスします。`Pass` が選択されている場合、このコントロールは失敗します。

ファイアウォールポリシーは、ファイアウォールが Amazon VPC のトラフィックをモニタリングおよび処理する方法を定義します。ステートレスおよびステートフルのルールグループを設定し、パケットとトラフィックフローをフィルタリングします。`Pass` をデフォルトに設定すると、意図しないトラフィックが許可される可能性があります。

修正

ファイアウォール ポリシーを変更する方法については、「AWS Network Firewall デベロッパーガイド」の「ファイアウォールポリシーの更新」 を参照してください。[ステートレスデフォルトアクション] で、[編集] を選択します。続いて、[アクション] として、[ドロップ] または [ステートフルルールグループに転送] を選択します。

〔NetworkFirewall.6] ステートレス Network Firewall ルールグループは空にしないでください

関連する要件: NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(5)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ: `AWS::NetworkFirewall::RuleGroup`

AWS Config ルール : `netfw-stateless-rule-group-not-empty`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 のステートレスルールグループにルール AWS Network Firewall が含まれているかどうかを確認します。ルールグループにルールが含まれない場合、コントロールは失敗します。

ルールグループには、ファイアウォールが VPC 内のトラフィックを処理する方法を定義するルールが含まれています。ファイアウォールポリシーに空のステートレスルールグループが存在する場合、ルールグループがトラフィックを処理するという印象を与える可能性があります。ただし、ステートレスルールグループが空の場合、トラフィックは処理されません。

修正

ネットワークファイアウォールのルールグループにルールを追加するには、「AWS Network Firewall デベロッパーガイド」の「ステートフルルールグループの更新」を参照してください。ファイアウォールの詳細ページの [ステートレスルールグループ] で、[編集] を選択してルールを追加します。

〔NetworkFirewall.7] Network Firewall ファイアウォールにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::NetworkFirewall::Firewall`

AWS Config ルール: `tagged-networkfirewall-firewall` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS Network Firewall ファイアウォールにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。ファイアウォールにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、ファイアウォールにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベ

ストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Network Firewall ファイアウォールにタグを追加するには、「 AWS Network Firewall デベロッパーガイド」の「 AWS Network Firewall リソースのタグ付け」を参照してください。

〔NetworkFirewall.8] Network Firewall ファイアウォールポリシーにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config ルール: `tagged-networkfirewall-firewallpolicy` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS Network Firewall ファイアウォールポリシーにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。ファイアウォールポリシーにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コ

ントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、ファイアウォールポリシーにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Network Firewall ポリシーにタグを追加するには、「 AWS Network Firewall デベロッパーガイド」の「 AWS Network Firewall リソースのタグ付け」を参照してください。

〔NetworkFirewall.9] Network Firewall ファイアウォールでは、削除保護を有効にする必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

カテゴリ： 保護 > ネットワークセキュリティ

重要度: 中

リソースタイプ: `AWS::NetworkFirewall::Firewall`

AWS Config ルール : `netfw-deletion-protection-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS Network Firewall ファイアウォールで削除保護が有効になっているかどうかをチェックします。ファイアウォールで削除保護が有効になっていないと、コントロールは失敗します。

AWS Network Firewall は、仮想プライベートクラウド (VPCs。削除防止設定は、ファイアウォールが誤って削除されないように保護するものです。

修正

既存の Network Firewall ファイアウォールで削除保護を有効にするには、「AWS Network Firewall デベロッパーガイド」の「ファイアウォールの更新」を参照してください。[変更保護] で [有効化] を選択します。 UpdateFirewallDeleteProtection API を呼び出して `DeleteProtection`フィールドをに設定することで、削除保護を有効にすることもできます`true`。

Amazon OpenSearch Service コントロール

これらのコントロールは OpenSearch サービスリソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::OpenSearch::Domain`

AWS Config ルール : opensearch-encrypted-at-rest

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 OpenSearch ドメインで encryption-at-rest 設定が有効になっているかどうかをチェックします。保管中の暗号化が有効になっていない場合、チェックは失敗します。

機密データのセキュリティを強化するには、 OpenSearch サービスドメインを保管時に暗号化するように設定する必要があります。保管中のデータの暗号化を設定すると、 は暗号化キー AWS KMS を保存および管理します。暗号化を実行するために、 は 256 ビットキー (AES-256) で Advanced Encryption Standard アルゴリズム AWS KMS を使用します。

保管時の OpenSearch サービス暗号化の詳細については、Amazon Service デベロッパーガイドの「Amazon OpenSearch Service の保管中のデータの暗号化 OpenSearch 」を参照してください。

修正

新規および既存の OpenSearch ドメインの保管時の暗号化を有効にするには、「Amazon OpenSearch Service デベロッパーガイド」の「保管中のデータの暗号化を有効にする」を参照してください。

[Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > VPC 内のリソース

重要度: 非常事態

リソースタイプ: `AWS::OpenSearch::Domain`

AWS Config ルール : opensearch-in-vpc-only

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 OpenSearch ドメインが VPC 内にあるかどうかをチェックします。このコントロールは、パブリックアクセスの可能性を判断するための VPC サブネットルーティング設定を評価しません。

OpenSearch ドメインがパブリックサブネットにアタッチされていないことを確認する必要があります。「Amazon OpenSearch Service デベロッパーガイド」の「リソースベースのポリシー」を参照してください。また、推奨されるベストプラクティスに従って VPC が確実に設定されていることを確認する必要があります。「Amazon VPC ユーザーガイド」の「VPC 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。

OpenSearch VPC 内にデプロイされた ドメインは、パブリックインターネットを経由することなく、プライベート AWS ネットワーク経由で VPC リソースと通信できます。この設定では、転送中のデータへのアクセスを制限することにより、セキュリティ体制が向上します。VPCs、ネットワーク ACL やセキュリティグループなど、 OpenSearch ドメインへのアクセスを保護するための多数のネットワークコントロールを提供します。Security Hub では、パブリック OpenSearch ドメインを VPCsに移行してこれらのコントロールを利用することをお勧めします。

修正

パブリックエンドポイントを使用してドメインを作成する場合、後で VPC 内にドメインを配置することはできません。代わりに、新規のドメインを作成して、データを移行する必要があります。逆の場合も同様です。VPC 内にドメインを作成する場合、パブリックエンドポイントを持つことはできません。代わりに、別のドメインを作成するか、このコントロールを無効にする必要があります。

手順については、「Amazon OpenSearch Service デベロッパーガイド」の「VPC 内で Amazon Service ドメインを起動する」を参照してください。 OpenSearch

[Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります

関連する要件: NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::OpenSearch::Domain`

AWS Config ルール : opensearch-node-to-node-encryption-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 OpenSearch ドメインで node-to-node 暗号化が有効になっているかどうかをチェックします。ドメインで node-to-node 暗号化が無効になっている場合、このコントロールは失敗します。

HTTPS (TLS) を使用すると、潜在的な攻撃者が または同様の攻撃を使用してネットワークトラフィックを盗聴 person-in-the-middle または操作するのを防ぐことができます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。 OpenSearch ドメインの node-to-node 暗号化を有効にすると、クラスター内通信が転送中に暗号化されます。

この設定には、パフォーマンス上のペナルティが発生する可能性があります。このオプションを有効にする前に、パフォーマンスのトレードオフを認識してテストする必要があります。

修正

OpenSearch ドメインで node-to-node 暗号化を有効にするには、「Amazon OpenSearch Service デベロッパーガイド」の node-to-node 「暗号化の有効化」を参照してください。

[Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります

関連する要件: NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::OpenSearch::Domain`

AWS Config ルール : opensearch-logs-to-cloudwatch

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `logtype = 'error'` (カスタマイズ不可)

このコントロールは、 OpenSearch ドメインがエラーログを CloudWatch ログに送信するように設定されているかどうかをチェックします。ドメインで へのエラーログ記録が有効になっていない場合、このコントロール CloudWatch は失敗します。

OpenSearch ドメインのエラーログを有効にし、保持と応答 CloudWatch のためにログに送信する必要があります。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

修正

ログ発行を有効にするには、Amazon OpenSearch Service デベロッパーガイドの「ログ発行の有効化 (コンソール)」を参照してください。

[Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります

関連する要件: NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::OpenSearch::Domain`

AWS Config ルール : opensearch-audit-logging-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `cloudWatchLogsLogGroupArnList` (カスタマイズ不可) – Security Hub は、このパラメータを設定しません。監査ログ用に設定する必要がある CloudWatch Logs ロググループのカンマ区切りリスト。

このルールは`NON_COMPLIANT`、ドメインの CloudWatch ロググループがこのパラメータリストで指定されていない場合に になります OpenSearch。

このコントロールは、 OpenSearch ドメインで監査ログ記録が有効になっているかどうかをチェックします。 OpenSearch ドメインで監査ログ記録が有効になっていない場合、このコントロールは失敗します。

監査ログは高度なカスタマイズが可能です。これにより、認証の成功と失敗、 へのリクエスト、インデックスの変更、受信検索クエリなどOpenSearch、OpenSearch クラスターでのユーザーアクティビティを追跡できます。

修正

監査ログを有効にする手順については、「Amazon OpenSearch Service デベロッパーガイド」の「監査ログの有効化」を参照してください。

[Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::OpenSearch::Domain`

AWS Config ルール : `opensearch-data-node-fault-tolerance`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 OpenSearch ドメインが少なくとも 3 つのデータノードで構成され、`zoneAwarenessEnabled` が であるかどうかをチェックします`true`。`instanceCount` が 3 未満または が の場合、 OpenSearch ドメインに対してこのコントロール`zoneAwarenessEnabled`は失敗します`false`。

OpenSearch 高可用性と耐障害性を実現するために、ドメインには少なくとも 3 つのデータノードが必要です。少なくとも 3 つのデータノードを持つ OpenSearch ドメインをデプロイすると、ノードに障害が発生した場合にクラスターオペレーションが保証されます。

修正

OpenSearch ドメイン内のデータノードの数を変更するには

1. AWS コンソールにサインインし、https://console.aws.amazon.com/aos/ で Amazon OpenSearch Service コンソールを開きます。
2. [My domains] (ドメイン) で、編集するドメインの名前を選択し、[Edit] (編集) を選択します。
3. [Data nodes] (データノード) で、[Number of nodes] (ノード数) を 3 以上の数値に設定します。3 つのアベイラビリティーゾーンに展開する場合は、アベイラビリティーゾーン間で均等に分配されるように 3 の倍数に設定します。
4. [送信] を選択します。

[Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理 > 機密性の高い API オペレーションアクションを制限する

重要度: 高

リソースタイプ: `AWS::OpenSearch::Domain`

AWS Config ルール : `opensearch-access-control-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 OpenSearch ドメインできめ細かなアクセスコントロールが有効になっているかどうかをチェックします。きめ細かなアクセスコントロールが有効でない場合、このコントロールは失敗します。きめ細かなアクセスコントロールでは`update-domain-config`、 OpenSearch パラメータ`advanced-security-options`で を有効にする必要があります。

きめ細かなアクセスコントロールは、Amazon OpenSearch Service 上のデータへのアクセスを制御する追加の方法を提供します。

修正

きめ細かなアクセスコントロールを有効にするには、「Amazon OpenSearch Service デベロッパーガイド」の「Amazon Service でのきめ細かなアクセスコントロール」を参照してください。 OpenSearch

[Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります

関連する要件: NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::OpenSearch::Domain`

AWS Config ルール : `opensearch-https-required`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `tlsPolicies: Policy-Min-TLS-1-2-PFS-2023-10` (カスタマイズ不可)

このコントロールは、Amazon OpenSearch Service ドメインエンドポイントが最新の TLS セキュリティポリシーを使用するように設定されているかどうかをチェックします。 OpenSearch ドメインエンドポイントがサポートされている最新のポリシーを使用するように設定されていない場合、または HTTPsは失敗します。

HTTPS (TLS) を使用すると、潜在的な攻撃者がネットワークトラフィックを傍受 person-in-the-middle または操作するために または同様の攻撃を使用することを防ぐことができます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。転送中のデータの暗号化は、パフォーマンスに影響する可能性があります。TLS のパフォーマンスプロファイルと TLS の影響を把

握するには、この機能を使用してアプリケーションをテストする必要があります。TLS 1.2 は、以前の TLS バージョンに比べて、いくつかのセキュリティ機能の強化を提供します。

修正

TLS 暗号化を有効にするには、 UpdateDomainConfig API オペレーションを使用します。の値を指定するように DomainEndpointOptionsフィールドを設定しますTLSSecurityPolicy。詳細については、「Amazon OpenSearch Service デベロッパーガイド」の「N ode-to-node 暗号化」を参照してください。

[Opensearch.9] OpenSearch ドメインにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::OpenSearch::Domain`

AWS Config ルール: `tagged-opensearch-domain` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、Amazon OpenSearch Service ドメインにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。ドメインにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタ

グキーの存在のみをチェックし、ドメインにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

OpenSearch サービスドメインにタグを追加するには、「Amazon OpenSearch Service デベロッパーガイド」の「タグの使用」を参照してください。

[Opensearch.10] OpenSearch ドメインには最新のソフトウェア更新がインストールされている必要があります

関連する要件: NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 低

リソースタイプ: `AWS::OpenSearch::Domain`

AWS Config ルール : `opensearch-update-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon OpenSearch Service ドメインに最新のソフトウェア更新がインストールされているかどうかをチェックします。ソフトウェアアップデートが利用可能で、ドメインにインストールされていない場合、コントロールは失敗します。

OpenSearch サービスソフトウェアの更新により、環境で使用できる最新のプラットフォームの修正、更新、機能が提供されます。パッチのインストール up-to-date を継続することで、ドメインのセキュリティと可用性を維持できます。必要なアップデートに関するアクションを実行しない場合、サービスソフトウェアは (通常 2 週間後に) 自動的に更新されます。サービスの中断を最小限に抑えるため、ドメインへのトラフィックが少ない時間帯にアップデートをスケジュールすることをお勧めします。

修正

OpenSearch ドメインのソフトウェア更新をインストールするには、「Amazon OpenSearch Service デベロッパーガイド」の「更新の開始」を参照してください。

[Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です

関連する要件： NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-2、NIST.800-53.r5 SC-5、NIST.800-53.r5 SC-36、NIST.800-53.r5 SI-13

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::OpenSearch::Domain`

AWS Config ルール : `opensearch-primary-node-fault-tolerance`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon OpenSearch Service ドメインに少なくとも 3 つの専用プライマリノードが設定されているかどうかを確認します。ドメインの専用プライマリノードが 3 つ未満の場合、コントロールは失敗します。

OpenSearch サービスは、クラスターの安定性を高めるために専用のプライマリノードを使用します。専用プライマリノードはクラスター管理タスクを実行しますが、データを保持したり、データのアップロードリクエストに応答したりしません。スタンバイでマルチ AZ を使用することをお勧めします。スタンバイでは、各本番 OpenSearch ドメインに 3 つの専用プライマリノードが追加されます。

修正

OpenSearch ドメインのプライマリノードの数を変更するには、「Amazon OpenSearch Service デベロッパーガイド」の「Amazon Service ドメインの作成と管理」を参照してください。
OpenSearch

AWS Private Certificate Authority コントロール

これらのコントロールは AWS Private CA リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[PCA.1] AWS Private CA ルート認証機関を無効にする必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 低

リソースタイプ: `AWS::ACMPCA::CertificateAuthority`

AWS Config ルール: `acm-pca-root-ca-disabled`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロール AWS Private CA は、無効になっているルート認証機関 (CA) があるかどうかをチェックします。ルート CA が有効になっている場合、コントロールは失敗します。

では AWS Private CA、ルート CA と下位 CA を含む CAs階層を作成できます。特に本番環境では、日常的なタスクでのルート CA の使用を最小限に抑える必要があります。ルート CA は、中間 CA 認定を交付するためにのみ使用する必要があります。これにより、中間 CA が エンドエンティティ証明書を発行する毎日のタスクを実行しながら、ルート CA を害のない方法で保存することができます。

修正

ルート CA を無効にするには、「AWS Private Certificate Authority ユーザーガイド」の「CA ステータスの更新」を参照してください。

Amazon Relational Database Service コントロール

これらのコントロールは Amazon RDS リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[RDS.1] RDS スナップショットはプライベートである必要があります

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 非常事態

リソースタイプ: `AWS::RDS::DBClusterSnapshot`、`AWS::RDS::DBSnapshot`

AWS Config ルール : `rds-snapshots-public-prohibited`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon RDS スナップショットがパブリックかどうかをチェックします。RDS スナップショットがパブリックである場合、このコントロールは失敗します。このコントロールは、RDS インスタンス、Aurora DB インスタンス、Neptune DB インスタンス、Amazon DocumentDB クラスターを評価します。

RDS スナップショットは、特定の時点で RDS インスタンスのデータをバックアップするために使用されます。これらは、RDS インスタンスを以前の状態に復元するために使用できます。

RDS スナップショットは、意図しない限りパブリックにしないでください。暗号化されていない手動スナップショットをパブリックとして共有すると、このスナップショットをすべての AWS アカウ

ントが使用できるようになります。これにより、RDS インスタンスの意図しないデータ漏えいが発生する可能性があります。

パブリックアクセスを許可するように設定を変更した場合、 AWS Config ルールは最大 12 時間変更を検出できない場合があります。 AWS Config ルールが変更を検出するまで、設定がルールに違反していてもチェックは成功します。

DB スナップショットの共有の詳細については、「Amazon RDS ユーザーガイド」の「DB スナップショットの共有」を参照してください。

修正

RDS スナップショットからパブリックアクセスを削除するには、「Amazon RDS ユーザーガイド」の「スナップショットの共有」を参照してください。[DB スナップショットの可視性] で、[プライベート] を選択します。

[RDS.2] RDS DB インスタンスは、 PubliclyAccessible AWS Config設定によって決定されるパブリックアクセスを禁止する必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/2.3.3、PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7 (1) SC-7 SC-7 SC-7 SC-7

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 非常事態

リソースタイプ: `AWS::RDS::DBInstance`

AWS Config ルール : `rds-instance-public-access-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、インスタンス設定項目内の `PubliclyAccessible` フィールドを評価して、Amazon RDS インスタンスがパブリックにアクセスできるかどうかをチェックします。

Neptune DB インスタンスと Amazon DocumentDB クラスターには、`PubliclyAccessible` フラグがないため、評価できません。ただし、このコントロールでは、これらのリソースに関する結果を生成できます。これらの結果を抑制できます。

RDS インスタンス設定 の PubliclyAccessible 値は、DB インスタンスがパブリックにアクセスできるかどうかを示します。DB インスタンスが PubliclyAccessible で設定されている場合、パブリックに解決可能な DNS 名を持つインターネット向けインスタンスであり、パブリック IP アドレスに解決されます。DB インスタンスがパブリックにアクセスできない場合、それはプライベート IP アドレスに解決される DNS 名を持つ内部インスタンスとなります。

RDS インスタンスのパブリックアクセスを可能にする意図がない限り、RDS インスタンスを PubliclyAccessible 値に設定しないでください。この設定を行った場合、データベースインスタンスへの不要なトラフィックが許可される可能性があります。

修正

RDS DB インスタンスからパブリックアクセスを削除するには、「Amazon RDS ユーザーガイド」の「Amazon RDS DB インスタンスを変更する」を参照してください。[パブリックアクセス] で [いいえ] を選択します。

[RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。

関連する要件： CIS AWS Foundations Benchmark v3.0.0/2.3.1、CIS AWS Foundations Benchmark v1.4.0/2.3.1、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: AWS::RDS::DBInstance

AWS Config ルール : rds-storage-encrypted

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon RDS DB インスタンスに対してストレージの暗号化が有効になっているかどうかをチェックします。

このコントロールは、RDS DB インスタンスを対象としています。ただし、Aurora DB インスタンス、Neptune DB インスタンス、および Amazon DocumentDB クラスターの結果を生成することもできます。これらの結果が役に立たない場合は、それらを抑制できます。

RDS DB インスタンスの機密データのセキュリティを強化するには、RDS DB インスタンスを保管中に暗号化するように設定する必要があります。保管中の Amazon RDS DB インスタンスとスナップショットを暗号化するには、RDS DB インスタンスの暗号化オプションを有効にします。保管中に暗号化されるデータには、DB インスタンス、自動バックアップ、リードレプリカ、スナップショットの基本的なストレージが含まれます。

RDS の暗号化された DB インスタンスでは、RDS DB インスタンスをホストしているサーバーでデータを暗号化するために、オープン標準の AES-256 暗号化アルゴリズムを使用します。データが暗号化されると、Amazon RDS はパフォーマンスの影響を最小限に抑えながら、データへのアクセスと復号化の認証を透過的に処理します。暗号化を使用するために、データベースのクライアントアプリケーションを変更する必要はありません。

Amazon RDS 暗号化は、現在すべてのデータベースエンジンおよびストレージタイプに使用できます。Amazon RDS 暗号化は、ほとんどの DB インスタンスクラスで使用できます。Amazon RDS 暗号化をサポートしていない DB インスタンスクラスの詳細については、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースの暗号化」を参照してください。

修正

Amazon RDS での DB インスタンスの暗号化の詳細については、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースの暗号化」を参照してください。

[RDS.4] RDS クラスタースナップショットとデータベーススナップショットは保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::RDS::DBClusterSnapshot`、 `AWS::RDS::DBSnapshot`

AWS Config ルール : `rds-snapshot-encrypted`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、RDS DB スナップショットが暗号化されているかどうかをチェックします。RDS DB スナップショットが暗号化されていない場合、コントロールは失敗します。

このコントロールは、RDS DB インスタンスを対象としています。ただし、Aurora DB インスタンス、Neptune DB インスタンス、および Amazon DocumentDB クラスターのスナップショットに関する結果を生成することもできます。これらの結果が役に立たない場合は、それらを抑制できます。

保管中のデータを暗号化すると、認証されていないユーザーがディスクに保存しているデータにアクセスするリスクが低減されます。RDS スナップショット内のデータは、セキュリティを強化するために、保管中に暗号化する必要があります。

修正

RDS スナップショットを暗号化するには、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースの暗号化」を参照してください。RDS DB インスタンスを暗号化するとき、暗号化されたデータにはインスタンスの基盤となるストレージ、自動バックアップ、リードレプリカ、スナップショットが含まれます。

RDS DB インスタンスを暗号化できるのは作成時のみであり、DB インスタンスの作成後には暗号化できません。ただし、暗号化されていないスナップショットのコピーは暗号化できるので、暗号化されていない DB インスタンスに効果的に暗号化を追加できます。つまり、DB インスタンスのスナップショットを作成し、そのスナップショットの暗号化済みコピーを作成します。この暗号化されたスナップショットから DB インスタンスを復元することで、元の DB インスタンスの暗号化されたコピーを作成できます。

[RDS.5] RDS DB インスタンスは、複数のアベイラビリティーゾーンで設定する必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::RDS::DBInstance`

AWS Config ルール : `rds-multi-az-support`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、RDS DB インスタンスの高可用性が有効になっているかどうかをチェックします。

RDS DB インスタンスは、複数のアベイラビリティーゾーン (AZ) に対して設定する必要があります。これにより、保存されたデータの可用性が保証されます。マルチ AZ 配置では、AZ の可用性に問題が発生した場合や、RDS の定期メンテナンス中に自動フェイルオーバーを実行できます。

修正

DB インスタンスを複数の AZ にデプロイするには、「Amazon RDS ユーザーガイド」の「DB インスタンスをマルチ AZ DB インスタンスのデプロイに変更する」を参照してください。

[RDS.6] RDS DB インスタンスの拡張モニタリングを設定する必要があります

関連する要件: NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::RDS::DBInstance`

AWS Config ルール : `rds-enhanced-monitoring-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値	
`monitoringInterval`	モニタリングメトリクスの収集間隔の秒数	列挙型	`1`, `5`, `10`, `15`, `30`, `60`	デフォルト値なし	

このコントロールは、Amazon Relational Database Service (Amazon RDS) DB インスタンスに対して拡張モニタリングが有効になっているかどうかをチェックします。インスタンスで拡張モニタリン

グが有効になっていない場合、コントロールは失敗します。monitoringInterval パラメータにカスタム値を指定したときは、指定された間隔でインスタンスの拡張モニタリングメトリクスが収集された場合にのみコントロールが成功します。

Amazon RDS では、拡張モニタリングによって、基盤となるインフラストラクチャのパフォーマンスの変化に対してより迅速にレスポンスできます。これらのパフォーマンスの変化により、データの可用性が低下する可能性があります。拡張モニタリングが有効になっている場合、RDS DB インスタンスが実行される OS のリアルタイムメトリクスを提供します。エージェントがインスタンスにインストールされています。エージェントは、ハイパーバイザーレイヤーから得られるよりも正確にメトリクスを取得できます。

拡張モニタリングのメトリクスは、DB インスタンス上のさまざまなプロセスやスレッドがどのように CPU を使用しているかを表示するときに便利です。詳細については、「Amazon RDS ユーザーガイド」の「拡張モニタリング」を参照してください。

修正

DB インスタンスで拡張モニタリングを有効にする手順の詳細については、「Amazon RDS ユーザーガイド」の「拡張モニタリングの設定と有効化」を参照してください。

[RDS.7] RDS クラスターでは、削除保護が有効になっている必要があります

関連する要件: NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

カテゴリ: 保護 > データ保護 > データ削除保護

重要度: 低

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール : `rds-cluster-deletion-protection-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、RDS DB クラスターで削除保護が有効になっているかどうかをチェックします。RDS DB クラスターで削除保護が有効になっていない場合、コントロールは失敗します。

このコントロールは、RDS DB インスタンスを対象としています。ただし、Aurora DB インスタンス、Neptune DB インスタンス、および Amazon DocumentDB クラスターの結果を生成することもできます。これらの結果が役に立たない場合は、それらを抑制できます。

クラスターの削除保護を有効にすることで、偶発的なデータベース削除や不正なエンティティによる削除に対して保護の強化を提供します。

削除保護が有効になっている場合、RDS クラスターは削除できません。削除リクエストが成功するには、削除保護を無効にする必要があります。

修正

RDS DB クラスターの削除保護を有効にするには、「Amazon RDS ユーザーガイド」の「コンソール、CLI、API を使用した DB クラスターの変更」を参照してください。[削除保護] で [削除保護の有効化] を選択します。

[RDS.8] RDS DB インスタンスで、削除保護が有効になっている必要があります

関連する要件: NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: 保護 > データ保護 > データ削除保護

重要度: 低

リソースタイプ: `AWS::RDS::DBInstance`

AWS Config ルール : `rds-instance-deletion-protection-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `databaseEngines`: `mariadb,mysql,custom-oracle-ee,oracle-ee-cdb,oracle-se2-cdb,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web` (カスタマイズ不可)

このコントロールは、リストされたデータベースエンジンのいずれかを使用する RDS DB インスタンスで削除保護が有効になっているかどうかをチェックします。RDS DB インスタンスで削除保護が有効になっていない場合、コントロールは失敗します。

インスタンス削除保護を有効にすると、偶発的なデータベース削除や不正なエンティティによる削除に対する保護の強化を提供します。

削除保護が有効になっている間は、RDS DB インスタンスを削除できません。削除リクエストが成功するには、削除保護を無効にする必要があります。

修正

RDS DB インスタンスの削除保護を有効にするには、「Amazon RDS ユーザーガイド」の「Amazon RDS DB インスタンスを変更する」を参照してください。[削除保護] で [削除保護の有効化] を選択します。

[RDS.9] RDS DB インスタンスはログを CloudWatch Logs に発行する必要があります

関連する要件: NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::RDS::DBInstance`

AWS Config ルール : `rds-logging-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon RDS DB インスタンスが Amazon CloudWatch Logs に次のログを発行するように設定されているかどうかをチェックします。インスタンスが次のログを CloudWatch Logs に発行するように設定されていない場合、コントロールは失敗します。

- Oracle: (アラート、監査、トレース、リスナー)
- PostgreSQL: (Postgresql、アップグレード)
- MySQL : (監査、エラー、一般、 SlowQuery)
- MariaDB : (監査、エラー、一般、 SlowQuery)
- SQL Server: (エラー、エージェント)
- Aurora: (監査、エラー、一般、 SlowQuery)
- Aurora-MySQL : (監査、エラー、一般、 SlowQuery)
- Aurora-PostgreSQL: (Postgresql、アップグレード)。

RDS データベースでは、関連するログを有効にする必要があります。データベースログ記録は、RDS に対して行われたリクエストの詳細な記録を提供します。データベースログは、セキュリティとアクセス監査に役立ち、可用性の問題を診断するのに役立ちます。

修正

RDS データベースログを CloudWatch Logs に発行するには、「Amazon RDS ユーザーガイド」の「ログに発行する CloudWatch ログの指定」を参照してください。

[RDS.10] IAM 認証は RDS インスタンス用に設定する必要があります

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理 > パスワードレス認証

重要度: 中

リソースタイプ: `AWS::RDS::DBInstance`

AWS Config ルール : `rds-instance-iam-authentication-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、RDS DB インスタンスで IAM データベース認証が有効になっているかどうかをチェックします。RDS DB インスタンスに IAM 認証が設定されていない場合、コントロールは失敗します。このコントロールは、`mysql`、`postgres`、`aurora`、`aurora-mysql`、`aurora-postgresql` および `mariadb` のエンジンタイプの RDS インスタンスのみを評価します。また、RDS インスタンスが結果を生成するには、`available`、`backing-up`、`storage-optimization`、`storage-full` のいずれかの状態になっている必要があります。

IAM データベース認証では、パスワードではなく、認証トークンを使用したデータベースインスタンスへの認証が可能です。データベースに出入りするネットワークトラフィックは、SSL を使用して暗号化されます。詳細については、「Amazon Aurora ユーザーガイド」の「IAM データベース認証」を参照してください。

修正

RDS DB インスタンスで IAM データベース認証を有効にするには、「Amazon RDS ユーザーガイド」の「IAM データベース認証の有効化と無効化」を参照してください。

[RDS.11] RDS インスタンスでは、自動バックアップが有効になっている必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

重要度: 中

リソースタイプ: `AWS::RDS::DBInstance`

AWS Config ルール : db-instance-backup-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値	
`backupRetentionMinimum`	最小バックアップ保持期間 (日数)	整数	`7 ~ 35`	`7`	
`checkReadReplicas`	リードレプリカに対して RDS DB インスタンスでバックアップが有効になっているかどうかを確認します	ブール値	カスタマイズ不可	`false`	

このコントロールは、Amazon Relational Database Service インスタンスで自動バックアップが有効に設定されていて、バックアップ保持期間が指定された時間枠以上であるかどうかをチェックします。リードレプリカは評価から除外されます。インスタンスのバックアップが有効になっていない場合や、保持期間が指定された時間枠未満の場合、コントロールは失敗します。バックアップ保持期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 7 日を使用します。

バックアップは、セキュリティインシデントからより迅速に復元し、システムの耐障害性を強化するのに役立ちます。Amazon RDS により、毎日のフルインスタンスボリュームスナップショットを設定することができます。Amazon RDS の自動バックアップの詳細については、「Amazon RDS ユーザーガイド」の「バックアップの使用」を参照してください。

修正

RDS DB インスタンスの自動バックアップを有効化するには、「Amazon RDS ユーザーガイド」の「自動バックアップの有効化」を参照してください。

[RDS.12] IAM 認証は RDS クラスター用に設定する必要があります

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理 > パスワードレス認証

重要度: 中

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール : `rds-cluster-iam-authentication-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon RDS DB クラスターで IAM データベース認証が有効になっているかどうかをチェックします。

IAM データベース認証では、データベースインスタンスへパスワードなしの認証が許可されています。認証には、認証トークンが使用されます。データベースに出入りするネットワークトラフィックは、SSL を使用して暗号化されます。詳細については、「Amazon Aurora ユーザーガイド」の「IAM データベース認証」を参照してください。

修正

DB クラスターで IAM 認証を有効にするには、「Amazon Aurora ユーザーガイド」の「IAM データベース認証の有効化と無効化」を参照してください。

[RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/2.3.2、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 高

リソースタイプ: `AWS::RDS::DBInstance`

AWS Config ルール : `rds-automatic-minor-version-upgrade-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、RDS データベースインスタンスでマイナーバージョン自動アップグレードが有効になっているかどうかをチェックします。

マイナーバージョン自動アップグレードを有効にすると、リレーショナルデータベース管理システム (RDBMS) に最新のマイナーバージョンの更新がインストールされます。これらのアップグレードには、セキュリティパッチとバグ修正を含む場合があります。パッチのインストールを最新の状態に保つことは、システムを保護する上で重要なステップです。

修正

既存の DB インスタンスの自動マイナーバージョンアップグレードを有効にするには、「Amazon RDS ユーザーガイド」の「Amazon RDS DB インスタンスを変更する」を参照してください。[マイナーバージョン自動アップグレード] で [はい] を選択します。

[RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

重要度: 中

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール : `aurora-mysql-backtracking-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値	
`BacktrackWindowInHours`	Aurora MySQL クラスターをバックトラックする時間数	ダブル	`0.1~72`	デフォルト値なし	

このコントロールは、Amazon Aurora クラスターでバックトラックが有効になっているかどうかをチェックします。クラスターでバックトラックが有効になっていない場合、コントロールは失敗します。`BacktrackWindowInHours` パラメータにカスタム値を指定したときは、指定された時間、クラスターがバックトラックされた場合にのみコントロールが成功します。

バックアップは、セキュリティインシデントからより迅速に復元するために役立ちます。また、システムの耐障害性を強化します。Aurora バックトラッキングによって、データベースを特定の時点に復元する時間が短縮されます。復元を実行する場合にデータベースの復元は必要ありません。

修正

Aurora バックトラックを有効にするには、「Amazon Aurora ユーザーガイド」の「バックトラックの設定」を参照してください。

既存のクラスターではバックトラッキングを有効にできないことに注意してください。代わりに、バックトラッキングが有効になっているクローンを作成できます。Aurora でのバックトラック制限の詳細については、「バックトラックの概要」の制限事項の一覧を参照してください。

[RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール : rds-cluster-multi-az-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、RDS DB クラスターで高可用性が有効になっているかどうかをチェックします。RDS DB クラスターが複数のアベイラビリティーゾーン (AZ) にデプロイされていない場合、コントロールは失敗します。

RDS DB クラスターは、保存されたデータの可用性を確保するために、複数の AZ に対して設定する必要があります。複数の AZ にデプロイすると、AZ の可用性に問題が発生した場合や、RDS の定期メンテナンスイベント中に自動フェイルオーバーを実行できます。

修正

DB クラスターを複数の AZ にデプロイするには、「Amazon RDS ユーザーガイド」の「DB インスタンスをマルチ AZ DB インスタンスのデプロイに変更する」を参照してください。

Aurora グローバルデータベースでは、修正の手順が異なります。Aurora グローバルデータベースに複数のアベイラビリティーゾーンを設定するには、DB クラスターを選択します。次に、[アクション] と [リーダーの追加] を選択し、複数の AZ を指定します。詳細については、「Amazon Aurora ユーザーガイド」の「Aurora レプリカを DB クラスターに追加する」を参照してください。

[RDS.16] タグをスナップショットにコピーするように RDS DB クラスターを設定する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 識別 > インベントリ

重要度: 低

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール: `rds-cluster-copy-tags-to-snapshots-enabled` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、スナップショットの作成時に、すべてのタグをスナップショットにコピーするように RDS DB クラスターが設定されているかどうかをチェックします。

IT アセットの身分証明書とインベントリはガバナンスとセキュリティの重要な側面です。すべての RDS DB クラスタを可視化することで、それらのセキュリティ体制を評価し、潜在的な弱点に対してアクションを起こせるようにする必要があります。スナップショットは、親 RDS データベースクラスターと同じ方法でタグ付けする必要があります。この設定を有効にすると、スナップショットが親データベースクラスターのタグを継承します。

修正

RDS DB クラスターのスナップショットにタグを自動的にコピーするには、「Amazon Aurora ユーザーガイド」の「コンソール、CLI、API を使用して DB クラスターを変更する」を参照してください。[タグをスナップショットへコピー] を選択します。

[RDS.17] RDS DB インスタンスは、タグをスナップショットにコピーするように設定する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 識別 > インベントリ

重要度: 低

リソースタイプ: `AWS::RDS::DBInstance`

AWS Config ルール: `rds-instance-copy-tags-to-snapshots-enabled` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、スナップショットの作成時に、すべてのタグをスナップショットにコピーするように RDS DB インスタンスが構成されているかどうかをチェックします。

IT アセットの身分証明書とインベントリはガバナンスとセキュリティの重要な側面です。すべての RDS DB インスタンスを可視化することで、それらのセキュリティ体制を評価し、潜在的な弱点に対してアクションを起こせるようにする必要があります。スナップショットは、親 RDS データベースインスタンスと同じ方法でタグ付けする必要があります。この設定を有効にすると、スナップショットが親データベースインスタンスのタグを継承します。

修正

RDS DB インスタンスのスナップショットにタグを自動的にコピーするには、「Amazon RDS ユーザーガイド」の「Amazon RDS DB インスタンスを変更する」を参照してください。[タグをスナップショットへコピー] を選択します。

[RDS.18] RDS インスタンスは VPC 内にデプロイする必要があります

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > VPC 内のリソース

重要度: 高

リソースタイプ: `AWS::RDS::DBInstance`

AWS Config ルール: `rds-deployed-in-vpc` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon RDS インスタンスが EC2-VPC にデプロイされているかどうかをチェックします。

VPC は、RDS リソースへのアクセスを保護するための多数のネットワークコントロールを提供します。これらのコントロールには、VPC エンドポイント、ネットワーク ACL、セキュリティグループが含まれます。これらのコントロールを利用するには、EC2-VPC 上に RDS インスタンスを作成することが推奨されます。

修正

RDS インスタンスを VPC に移動する方法については、「Amazon RDS ユーザーガイド」の「DB インスタンスの VPC を更新する」を参照してください。

[RDS.19] 重大なクラスターイベントについて、既存の RDS イベント通知サブスクリプションを設定する必要があります

関連する要件: NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2

カテゴリ: 検出 > 検出サービス > アプリケーションモニタリング

重要度: 低

リソースタイプ: `AWS::RDS::EventSubscription`

AWS Config ルール: `rds-cluster-event-notifications-configured` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、データベースクラスターの既存の Amazon RDS イベントサブスクリプションに、次のソースタイプ、イベントカテゴリのキーと値のペアに対して有効な通知があるかどうかをチェックします。

```
DBCluster: ["maintenance","failure"]
```

アカウントに既存のイベントサブスクリプションがない場合、コントロールはパスします。

RDS イベント通知は Amazon SNS を使用して、RDS リソースの可用性または設定の変更を通知します。これらの通知により、迅速な対応が実現します。RDS イベント通知の詳細については、「Amazon RDS ユーザーガイド」の「Amazon RDS イベント通知の使用」を参照してください。

修正

RDS クラスターイベント通知にサブスクライブするには、「アマゾン RDS ユーザーガイド」の「Amazon RDS イベント通知にサブスクライブする」を参照してください。以下の値を使用します。

フィールド	値
ソースタイプ	クラスター
含めるクラスター	すべてのクラスター
含めるイベントカテゴリ	[Specific event categories] (特定のイベントカテゴリ) または [All event categories] (すべてのイベントカテゴリ) を選択します

[RDS.20] 重大なデータベースインスタンスイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります

関連する要件: NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2

カテゴリ: 検出 > 検出サービス > アプリケーションモニタリング

重要度: 低

リソースタイプ: `AWS::RDS::EventSubscription`

AWS Config ルール: `rds-instance-event-notifications-configured` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、データベースインスタンスの既存の Amazon RDS イベントサブスクリプションに、次のソースタイプ、イベントカテゴリのキーと値のペアに対して有効な通知があるかどうかをチェックします。

```
DBInstance: ["maintenance","configuration change","failure"]
```

アカウントに既存のイベントサブスクリプションがない場合、コントロールはパスします。

RDS イベント通知は Amazon SNS を使用して、RDS リソースの可用性または設定の変更をユーザーに知らせます。これらの通知により、迅速な対応が実現します。RDS イベント通知の詳細については、「Amazon RDS ユーザーガイド」の「Amazon RDS イベント通知の使用」を参照してください。

修正

RDS インスタンスイベント通知にサブスクライブするには、「Amazon RDS ユーザーガイド」の「Amazon RDS イベント通知にサブスクライブする」を参照してください。以下の値を使用します。

フィールド	値
ソースタイプ	インスタンス
含めるインスタンス	すべてのインスタンス

フィールド	値
含めるイベントカテゴリ	[Specific event categories] (特定のイベントカテゴリ) または [All event categories] (すべてのイベントカテゴリ) を選択します

[RDS.21] 重大なデータベースパラメータグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります

関連する要件: NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2

カテゴリ: 検出 > 検出サービス > アプリケーションモニタリング

重要度: 低

リソースタイプ: `AWS::RDS::EventSubscription`

AWS Config ルール: `rds-pg-event-notifications-configured` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、次のソースタイプ、イベントカテゴリのキーバリューペアに対して通知が有効になっている Amazon RDS イベントサブスクリプションが存在するかどうかをチェックします。アカウントに既存のイベントサブスクリプションがない場合、コントロールはパスします。

```
DBParameterGroup: ["configuration change"]
```

RDS イベント通知は Amazon SNS を使用して、RDS リソースの可用性または設定の変更をユーザーに知らせます。これらの通知により、迅速な対応が実現します。RDS イベント通知の詳細については、「Amazon RDS ユーザーガイド」の「Amazon RDS イベント通知の使用」を参照してください。

修正

RDS データベースパラメータグループイベント通知にサブスクライブするには、「Amazon RDS ユーザーガイド」の「Amazon RDS イベント通知にサブスクライブする」を参照してください。以下の値を使用します。

フィールド	値
ソースタイプ	パラメータグループ
含めるパラメータグループ	すべてのパラメータグループ
含めるイベントカテゴリ	[Specific event categories] (特定のイベントカテゴリ) または [All event categories] (すべてのイベントカテゴリ) を選択します

[RDS.22] 重大なデータベースセキュリティグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります

関連する要件: NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2

カテゴリ: 検出 > 検出サービス > アプリケーションモニタリング

重要度: 低

リソースタイプ: `AWS::RDS::EventSubscription`

AWS Config ルール: `rds-sg-event-notifications-configured` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、次のソースタイプ、イベントカテゴリのキーバリューペアに対して通知が有効になっている Amazon RDS イベントサブスクリプションが存在するかどうかをチェックします。アカウントに既存のイベントサブスクリプションがない場合、コントロールはパスします。

```
DBSecurityGroup: ["configuration change","failure"]
```

RDS イベント通知は Amazon SNS を使用して、RDS リソースの可用性または設定の変更をユーザーに知らせます。これらの通知により、迅速なレスポンスが可能になります。RDS イベント通知の詳細については、「Amazon RDS ユーザーガイド」の「Amazon RDS イベント通知の使用」を参照してください。

修正

RDS インスタンスイベント通知にサブスクライブするには、「Amazon RDS ユーザーガイド」の「Amazon RDS イベント通知にサブスクライブする」を参照してください。以下の値を使用します。

フィールド	値
ソースタイプ	セキュリティグループ
含めるセキュリティグループ	すべてのセキュリティグループ
含めるイベントカテゴリ	[Specific event categories] (特定のイベントカテゴリ) または [All event categories] (すべてのイベントカテゴリ) を選択します

[RDS.23] RDS インスタンスはデータベースエンジンのデフォルトポートを使用しないようにする必要があります

関連する要件: NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(5)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 低

リソースタイプ: `AWS::RDS::DBInstance`

AWS Config ルール: `rds-no-default-ports` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、RDS クラスターまたはインスタンスがデータベースエンジンのデフォルトポート以外のポートを使用しているかどうかをチェックします。RDS クラスターまたはインスタンスがデフォルトポートを使用する場合、このコントロールは失敗します。

既知のポートを使用して RDS クラスターまたはインスタンスをデプロイすると、攻撃者はクラスターまたはインスタンスに関する情報を推測できる可能性があります。攻撃者は、この情報を他の情

報と組み合わせ、RDS クラスターまたはインスタンスに接続したり、ユーザーのアプリケーションに関する追加情報を取得できます。

ポートを変更する場合は、古いポートへの接続に使用された既存の接続文字列も更新する必要があります。また、ユーザーは DB インスタンスのセキュリティグループをチェックして、新しいポートでの接続を許可するイングレスルールが確実に含まれていることを確認する必要があります。

修正

既存の RDS DB インスタンスのデフォルトポートを変更するには、「Amazon RDS ユーザーガイド」の「Amazon RDS DB インスタンスを変更する」を参照してください。既存の RDS DB クラスターのデフォルトポートを変更するには、「Amazon Aurora ユーザーガイド」の「コンソール、CLI、API を使用した DB クラスターの変更」を参照してください。データベースポートについて、ポート値をデフォルト以外の値に変更します。

[RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 識別 > リソース設定

重要度: 中

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール : `rds-cluster-default-admin-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon RDS データベースクラスターが管理者ユーザーネームをデフォルト値から変更したかどうかをチェックします。このコントロールは、Neptune (Neptune DB) または docdb (DocumentDB) タイプのエンジンには適用されません。管理者ユーザーネームがデフォルト値に設定されている場合、このルールは失敗します。

Amazon RDS データベースを作成するときは、デフォルトの管理者ユーザーネームを一意の値に変更する必要があります。デフォルトのユーザーネームはパブリックナレッジであり、RDS データベースの作成時に変更する必要があります。デフォルトのユーザーネームを変更すると、意図しないアクセスのリスクが軽減されます。

修正

Amazon RDS データベースクラスターに関連付けられている管理者ユーザーネームを変更するには、新しい RDS データベースクラスターを作成し、データベースの作成時に、デフォルトの管理者ユーザーネームを変更します。

[RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 識別 > リソース設定

重要度: 中

リソースタイプ: `AWS::RDS::DBInstance`

AWS Config ルール : `rds-instance-default-admin-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールでは、Amazon Relational Database Service (Amazon RDS) のデータベースインスタンスの管理者ユーザーネームがデフォルト値から変更されたかどうかをチェックします。このコントロールは、Neptune (Neptune DB) または docdb (DocumentDB) タイプのエンジンには適用されません。管理者ユーザーネームがデフォルト値に設定されている場合、このコントロールは失敗します。

Amazon RDS データベースのデフォルトの管理ユーザーネームは、パブリックナレッジです。Amazon RDS データベースを作成するときは、意図しないアクセスのリスクを減らすために、デフォルトの管理ユーザーネームを一意の値に変更する必要があります。

修正

RDS データベースインスタンスに関連付けられている管理ユーザーネームを変更するには、始めに新しい RDS データベースインスタンスを作成します。データベースの作成時に、デフォルトの管理ユーザーネームを変更します。

[RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

重要度: 中

リソースタイプ: `AWS::RDS::DBInstance`

AWS Config ルール： `rds-resources-protected-by-backup-plan`

スケジュールタイプ: 定期的

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値	
`backupVaultLockCheck`	パラメータが true に設定され、リソースが AWS Backup ボールトロックを使用する場合、コントロールはPASSED結果を生成します。	ブール値	`true` 、、または `false`	デフォルト値なし	

このコントロールは、Amazon RDS DB インスタンスがバックアッププランの対象かどうかを評価します。RDS DB インスタンスがバックアッププランの対象となっていない場合、このコントロールは失敗します。`backupVaultLockCheck` パラメータを に設定すると`true`、インスタンスが AWS Backup ロックされたボールトにバックアップされている場合にのみコントロールが成功します。

AWS Backup は、 全体のデータのバックアップを一元化および自動化するフルマネージドバックアップサービスです AWS のサービス。では AWS Backup、バックアッププランと呼ばれるバックアップポリシーを作成できます。これらのプランを使用して、データのバックアップ頻度やバックアップを保持する期間など、バックアップ要件を定義できます。バックアッププランに RDS DB インスタンスを含めると、意図しない損失や削除からデータを保護できます。

修正

RDS DB インスタンスを AWS Backup バックアッププランに追加するには、「 AWS Backup デベロッパーガイド」の「バックアッププランへのリソースの割り当て」を参照してください。

[RDS.27] RDS DB クラスターは保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール： `rds-cluster-encrypted-at-rest`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、RDS DB クラスターが保管中に暗号化されているかどうかをチェックします。RDS DB クラスターが保管中に暗号化されていない場合、コントロールは失敗します。

保管中のデータとは、永続的な不揮発性ストレージに任意の期間保管されているデータを指します。暗号化は、このようなデータの機密性を保護し、権限のないユーザーがデータにアクセスするリスクを低減するのに役立ちます。RDS DB クラスターを暗号化することで、データとメタデータを不正アクセスから保護します。また、本番ファイルシステムの data-at-rest 暗号化に関するコンプライアンス要件を満たします。

修正

RDS DB クラスターを作成するときに、保管中の暗号化を有効にできます。クラスターを作成した後で暗号化設定を変更することはできません。詳細については、「Amazon Aurora ユーザーガイド」の「Amazon Aurora DB クラスターの暗号化」を参照してください。

[RDS.28] RDS DB クラスターにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール：`tagged-rds-dbcluster` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon RDS DB クラスターに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。DB クラスターにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、DB クラスターにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC AWSとは」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベ

ストプラクティスの詳細については、「」の「AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

RDS DB クラスターにタグを追加するには、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースのタグ付け」を参照してください。

[RDS.29] RDS DB クラススナップショットにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::RDS::DBClusterSnapshot`

AWS Config ルール：`tagged-rds-dbclustersnapshot` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon RDS DB クラススナップショットに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。DB クラススナップショットにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、DB クラススナップショットにキー

がタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

RDS DB クラスタースナップショットにタグを追加するには、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースのタグ付け」を参照してください。

[RDS.30] RDS DB インスタンスにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::RDS::DBInstance`

AWS Config ルール : `tagged-rds-dbinstance` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon RDS DB インスタンスにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。DB インスタンスにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、DB インスタンスにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

RDS DB インスタンスにタグを追加するには、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースのタグ付け」を参照してください。

[RDS.31] RDS DB セキュリティグループにタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::RDS::DBSecurityGroup`

AWS Config ルール：`tagged-rds-dbsecuritygroup` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon RDS DB セキュリティグループに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。DB セキュリティグループにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、DB セキュリティグループにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの

識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

RDS DB セキュリティグループにタグを追加するには、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースのタグ付け」を参照してください。

[RDS.32] RDS DB スナップショットにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::RDS::DBSnapshot`

AWS Config ルール : `tagged-rds-dbsnapshot` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon RDS DB スナップショットに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。DB スナップショットにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、DB スナップショットにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

RDS DB スナップショットにタグを追加するには、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースのタグ付け」を参照してください。

[RDS.33] RDS DB サブネットグループにタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::RDS::DBSubnetGroup`

AWS Config ルール：`tagged-rds-dbsubnetgroups` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon RDS DB サブネットグループに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。DB サブネットグループにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、DB サブネットグループにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの

識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

RDS DB サブネットグループにタグを追加するには、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースのタグ付け」を参照してください。

[RDS.34] Aurora MySQL DB クラスターは監査ログを CloudWatch Logs に発行する必要があります

関連する要件: NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ロギング

重要度: 中

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール： `rds-aurora-mysql-audit-logging-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon Aurora MySQL DB クラスターが監査ログを Amazon CloudWatch Logs に発行するように設定されているかどうかをチェックします。クラスターが監査ログを CloudWatch Logs に発行するように設定されていない場合、コントロールは失敗します。このコントロールは、Aurora Serverless v1 DB クラスターの結果を生成しません。

監査ログには、ログイン試行、データ変更、スキーマ変更、セキュリティとコンプライアンスの目的で監査の対象となる可能性のあるその他のイベントなど、データベースアクティビティのレコードが記録されます。Amazon Logs のロググループに監査ログを発行するように Aurora MySQL DB CloudWatch クラスターを設定すると、ログデータのリアルタイム分析を実行できます。CloudWatch ログは、耐久性の高いストレージにログを保持します。また、 でアラームを作成し、メトリクスを表示することもできます CloudWatch。

> **Note**
>
> 監査ログを CloudWatch Logs に発行するもう 1 つの方法は、高度な監査を有効にし、クラスターレベルの DB パラメータを に設定`server_audit_logs_upload`することです1。`server_audit_logs_upload parameter` のデフォルト値は `0` です。ただし、このコントロールを渡すには、代わりに以下の修正手順を使用することをおすすめします。

修正

Aurora MySQL DB クラスター監査ログを CloudWatch ログに発行するには、「Amazon Aurora ユーザーガイド」の「Amazon Aurora MySQL ログを Amazon CloudWatch Logsに発行する」を参照してください。

[RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります

関連する要件: NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 中

リソースタイプ: `AWS::RDS::DBCluster`

AWS Config ルール： `rds-cluster-auto-minor-version-upgrade-enable`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon RDS マルチ AZ DB クラスターで自動マイナーバージョンアップグレードが有効になっているかどうかを確認します。マルチ AZ DB クラスターで自動マイナーバージョンアップグレードが有効になっていない場合、コントロールは失敗します。

RDS には、マルチ AZ DB クラスターを最新の状態に保つことができるように、自動マイナーバージョンアップグレードが用意されています。マイナーバージョンには、ソフトウェアの新機能、バグ修正、セキュリティパッチ、およびパフォーマンスの向上を含む可能性があります。RDS データベースクラスターでマイナーバージョンの自動アップグレードを有効にすると、新しいバージョンが利用可能になった時点で、クラスターとクラスター内のインスタンスがマイナーバージョンへ自動更新を受け取ります。更新はメンテナンスの時間帯に自動で適用されます。

修正

マルチ AZ DB クラスターで自動マイナーバージョンアップグレードを有効にするには、「Amazon RDS ユーザーガイド」の「マルチ AZ DB クラスターの変更」を参照してください。

Amazon Redshift のコントロール

これらのコントロールは Amazon Redshift リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 非常事態

リソースタイプ: `AWS::Redshift::Cluster`

AWS Config ルール : `redshift-cluster-public-access-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon Redshift クラスターがパブリックにアクセス可能かどうかをチェックします。このコントロールは、クラスター設定項目の `PubliclyAccessible` フィールドを評価します。

Amazon Redshift クラスター設定の `PubliclyAccessible` 属性は、クラスターがパブリックにアクセス可能かどうかを示します。クラスターが `PubliclyAccessible` を `true` に設定して構成されている場合、パブリックに解決可能な DNS 名を持つインターネット向けインスタンスであり、パブリック IP アドレスに解決されます。

クラスターがパブリックにアクセスできない場合、プライベート IP アドレスに解決される DNS 名を持つ内部インスタンスです。クラスターをパブリックにアクセスさせる意図がない限り、クラスターは `PubliclyAccessible` を `true` に設定しないでください。

修正

Amazon Redshift クラスターを更新してパブリックアクセスを無効にするには、「Amazon Redshift 管理ガイド」の「クラスターの変更」を参照してください。[Publicly Accessible] を [No] に設定します。

[Redshift.2] Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります

関連する要件: NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ： `AWS::Redshift::Cluster` `AWS::Redshift::ClusterParameterGroup`

AWS Config ルール : redshift-require-tls-ssl

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon Redshift クラスターへの接続において、転送中に暗号化を使用する必要があるかどうかをチェックします。Amazon Redshift クラスターパラメータ require_SSL が True に設定されていない場合、チェックは失敗します。

TLS を使用すると、潜在的な攻撃者がネットワークトラフィックを傍受 person-in-the-middle または操作するために または同様の攻撃を使用することを防ぐことができます。TLS 経由の暗号化された接続のみを許可する必要があります。転送中のデータの暗号化は、パフォーマンスに影響する可能性があります。TLS のパフォーマンスプロファイルと TLS の影響を把握するには、この機能を使用してアプリケーションをテストする必要があります。

修正

Amazon Redshift パラメータグループを更新して暗号化を要求するには、「Amazon Redshift 管理ガイド」の「パラメータグループの変更」を参照してください。require_sslを True に設定します。

[Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

重要度: 中

リソースタイプ: AWS::Redshift::Cluster

AWS Config ルール : redshift-backup-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値	
`MinRetentionPeriod`	最小スナップショット保持期間 (日数)	整数	`7~35`	`7`	

このコントロールは、Amazon Redshift クラスターで自動スナップショットが有効になっているかどうか、および保持期間が指定された時間枠以上であるかどうかをチェックします。クラスターの自動スナップショットが有効になっていない場合や、保持期間が指定された時間枠未満の場合、コントロールは失敗します。スナップショット保持期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 7 日を使用します。

バックアップは、セキュリティインシデントからより迅速に復元するために役立ちます。これにより、システムの耐障害性が強化されます。Amazon Redshift は、デフォルトで定期的にスナップショットを作成します。このコントロールは、自動スナップショットが有効で、少なくとも 7 日間保持されているかどうかをチェックします。Amazon Redshift の自動スナップショットの詳細については、「Amazon Redshift 管理ガイド」の「自動スナップショット」を参照してください。

修正

Amazon Redshift クラスターのスナップショット保持期間を更新するには、「Amazon Redshift 管理ガイド」の「クラスターの変更」を参照してください。[Backup] (バックアップ) の場合、[Snapshot retention] (スナップショットの保持) を 7 以上の値に設定します。

[Redshift.4] Amazon Redshift クラスターでは、監査ログ記録が有効になっている必要があります

関連する要件: NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::Redshift::Cluster`

AWS Config ルール: `redshift-cluster-audit-logging-enabled` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `loggingEnabled = true` (カスタマイズ不可)

このコントロールは、Amazon Redshift クラスターで監査ログ記録が有効になっているかどうかをチェックします。

Amazon Redshift 監査ログ記録は、ユーザーのクラスター内の接続とユーザーアクティビティに関する追加情報を提供します。このデータは、Amazon S3 内で保存および保護することができ、セキュリティ監査や調査に役立ちます。詳細については、「Amazon Redshift 管理ガイド」の「データベース監査ログ記録」を参照してください。

修正

Amazon Redshift クラスターの監査ログを設定するには、「Amazon Redshift 管理ガイド」の「コンソールを使用して監査を設定する」を参照してください。

[Redshift.6] Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 中

リソースタイプ: `AWS::Redshift::Cluster`

AWS Config ルール : `redshift-cluster-maintenancesettings-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `allowVersionUpgrade = true` (カスタマイズ不可)

このコントロールは、Amazon Redshift クラスターで自動メジャーバージョンアップグレードが有効になっているかどうかをチェックします。

自動メジャーバージョンアップグレードを有効にすることで、メンテナンスウィンドウ中に Amazon Redshift クラスターの最新のメジャーバージョンの更新がインストールされます。これらのアップデートには、セキュリティパッチやバグ修正が含まれる場合があります。パッチのインストールを最新の状態に保つことは、システムを保護する上で重要なステップです。

修正

この問題を から修正するには AWS CLI、Amazon Redshift `modify-cluster` コマンドを使用して `--allow-version-upgrade` 属性を設定します。

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

clustername は Amazon Redshift クラスターの名前です。

[Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります

関連する要件: NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > API プライベートアクセス

重要度: 中

リソースタイプ: `AWS::Redshift::Cluster`

AWS Config ルール : redshift-enhanced-vpc-routing-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon Redshift クラスターで `EnhancedVpcRouting` が有効かどうかをチェックします。

拡張 VPC ルーティングは、クラスターとデータリポジトリ間のすべての `COPY` および `UNLOAD` トラフィックが VPC を経由するよう強制します。その後、セキュリティグループやネットワークアクセスコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用して、ネットワークトラフィックをモニタリングすることもできます。

修正

詳細な修正手順については、「Amazon Redshift 管理ガイド」の「拡張された VPC ルーティングの有効化」を参照してください。

[Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 識別 > リソース設定

重要度: 中

リソースタイプ: `AWS::Redshift::Cluster`

AWS Config ルール : `redshift-default-admin-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon Redshift クラスターが、管理者ユーザーネームをデフォルト値から変更したかどうかをチェックします。Redshift クラスターの管理者ユーザーネームが `awsuser` に設定されている場合、このコントロールは失敗します。

Amazon RDS クラスターを作成するときは、デフォルトの管理者ユーザーネームを一意の値に変更する必要があります。デフォルトのユーザーネームはパブリックナレッジであり、設定時に変更する必要があります。デフォルトのユーザーネームを変更すると、意図しないアクセスのリスクが軽減されます。

修正

Amazon Redshift クラスターの管理者ユーザーネームは、作成後に変更することはできません。DB クラスターを新たに作成するには、「こちら」の手順に従います。

[Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 識別 > リソース設定

重要度: 中

リソースタイプ: `AWS::Redshift::Cluster`

AWS Config ルール : `redshift-default-db-name-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon Redshift クラスターが、データベース名をデフォルト値から変更したかどうかをチェックします。Redshift クラスターのデータベース名が dev に設定されている場合、このコントロールは失敗します。

Redshift クラスターを作成するときは、デフォルトのデータベース名を一意の値に変更する必要があります。デフォルトの名前は一般に知られているため、設定時に変更する必要があります。よく知られた名前は、IAM ポリシー条件などで使用されると偶発的なアクセスにつながる可能性があります。

修正

Amazon Redshift クラスターのデータベース名は、作成後に変更することはできません。新規クラスターの作成方法については、「Amazon Redshift の入門ガイド」の「Amazon Redshift の開始方法」を参照してください。

[Redshift.10] Redshift クラスターは保存時に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::Redshift::Cluster`

AWS Config ルール : `redshift-cluster-kms-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon Redshift クラスターが保管時に暗号化されているかどうかをチェックします。Redshift クラスターが保存時に暗号化されていない場合、または暗号化キーがルールパラメータで指定されたキーと異なる場合、コントロールは失敗します。

Amazon Redshift では、クラスターに対してデータベースの暗号化を有効にして、保管中のデータを保護できます。クラスターに対して暗号化を有効にすると、クラスターとそのスナップショットのデータブロックとシステムメタデータが暗号化されます。保管中のデータの暗号化は、データにアクセス管理のレイヤーを追加できるため、推奨されるベストプラクティスです。保管中の Redshift クラスターを暗号化すると、認証されていないユーザーがディスクに保存しているデータにアクセスするリスクが低減されます。

修正

KMS 暗号化を使用するように Redshift クラスターを変更するには、Amazon Redshift 管理ガイドの「クラスターの暗号化の変更」を参照してください。

[Redshift.11] Redshift クラスターにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::Redshift::Cluster`

AWS Config ルール: `tagged-redshift-cluster` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、Amazon Redshift クラスターにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。クラスターにタグキーがな

い場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、クラスターにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Redshift クラスターにタグを追加するには、「Amazon Redshift 管理ガイド」の「Amazon Redshift でのリソースのタグ付け」を参照してください。

[Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: AWS::Redshift::EventSubscription

AWS Config ルール: tagged-redshift-eventsubscription (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、Amazon Redshift クラスタースナップショットに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。クラスタースナップショットにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、クラスタースナップショットにキーのタグが付けられていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベ

ストプラクティスの詳細については、「」の「AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Redshift イベント通知サブスクリプションにタグを追加するには、「Amazon Redshift 管理ガイド」の「Amazon Redshift でのリソースのタグ付け」を参照してください。

[Redshift.13] Redshift クラススナップショットにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::Redshift::ClusterSnapshot`

AWS Config ルール: `tagged-redshift-clustersnapshot` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、Amazon Redshift クラススナップショットに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。クラススナップショットにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、クラススナップショットにキーのタ

グが付けられていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Redshift クラススナップショットにタグを追加するには、「Amazon Redshift 管理ガイド」の「Amazon Redshift でのリソースのタグ付け」を参照してください。

[Redshift.14] Redshift クラスターサブネットグループにタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::Redshift::ClusterSubnetGroup`

AWS Config ルール: `tagged-redshift-clustersubnetgroup` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、Amazon Redshift クラスターサブネットグループに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。クラスターサブネットグループにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、クラスターサブネットグループにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Redshift クラスターサブネットグループにタグを追加するには、「Amazon Redshift 管理ガイド」の「Amazon Redshift でのリソースのタグ付け」を参照してください。

[Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります

カテゴリ: 保護 > セキュアなネットワーク設定 > セキュリティグループの設定

重要度: 高

リソースタイプ: `AWS::Redshift::Cluster`

AWS Config ルール: `redshift-unrestricted-port-access`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Amazon Redshift クラスターに関連付けられたセキュリティグループに、インターネット (0.0.0.0/0 または ::/0) からクラスターポートへのアクセスを許可する進入ルールがあるかどうかをチェックします。セキュリティグループの進入ルールがインターネットからのクラスターポートへのアクセスを許可している場合、コントロールは失敗します。

Redshift クラスターポート (/0 サフィックスを持つ IP アドレス) への無制限のインバウンドアクセスを許可すると、不正アクセスやセキュリティインシデントが発生する可能性があります。セキュリティグループを作成し、インバウンドルールを設定するときは、最小特権アクセスのプリンシパルを適用することをお勧めします。

修正

Redshift クラスターポートの進入を制限オリジンに制限するには、「Amazon VPC ユーザーガイド」の「セキュリティグループルールの操作」を参照してください。ポート範囲が Redshift クラスターポートと一致し、IP ポート範囲が 0.0.0.0/0 であるルールを更新します。

Amazon Route 53 のコントロール

これらのコントロールは Route 53 のリソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::Route53::HealthCheck`

AWS Config ルール：`tagged-route53-healthcheck` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon Route 53 ヘルスチェックに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。ヘルスチェックにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、ヘルスチェックがどのキーでもタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオ

ペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Route 53 ヘルスチェックにタグを追加するには、Amazon Route 53 デベロッパーガイドの「ヘルスチェックの命名とタグ付け」を参照してください。

[Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを口グに記録する必要があります

関連する要件: NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > 口グ記録

重要度: 中

リソースタイプ: `AWS::Route53::HostedZone`

AWS Config ルール : `route53-query-logging-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

Amazon Route 53 パブリックホストゾーンで DNS クエリログ記録が有効になっているかどうかを確認します。このコントロールは Amazon Route 53 パブリックホストゾーンで DNS クエリログ記録が有効になっているかどうかを確認します。

Route 53 ホストゾーンの DNS クエリを記録することで、DNS のセキュリティとコンプライアンスの要件に対応し、可視性を高めます。ログには、クエリされたドメインまたはサブドメイン、クエリ

の日時、DNS レコードタイプ (A や AAAA など)、DNS 応答コード (`NoError` または `ServFail`) などの情報が含まれます。DNS クエリログ記録が有効になっている場合、Route 53 はログファイルを Amazon CloudWatch Logs に発行します。

修正

Route 53 パブリックホストゾーンの DNS クエリをログ記録するには、「Amazon Route 53 デベロッパーガイド」の「DNS クエリのログ記録の設定」を参照してください。

Amazon Simple Storage Service コントロール

これらのコントロールは Amazon S3 リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります

> **Important**
>
> 2024 年 3 月 12 日、このコントロールのタイトルは表示されているタイトルに変更されました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

関連する要件： CIS AWS Foundations Benchmark v3.0.0/2.1.4、 CIS AWS Foundations Benchmark v1.4.0/2.1.5、 PCI DSS v3.2.1/1.2.1、 PCI DSS v3.2.1/1.3.1、 PCI DSS v3.2.1/1.3.2、 PCI DSS v3.2.1/1.3.4、 PCI DSS v3.2.1/1.3.6、 NIST.800-53.r5 AC-21、 NIST.800-53.r5 AC-3、 NIST.800-53.r5 AC-3(7)、 NIST.800-53.r5 AC-4、 NIST.800-53.r5 AC-4(21)、 NIST.800-53.r5 AC-6、 NIST.800-53.r5 SC-7、 NIST.800-53.r5 SC-7(11)、 NIST.800-53.r5 SC-7(16)、 NIST.800-53.r5 SC-7(20)、 NIST.800-53.r5 SC-7(21)、 NIST.800-53.r5 SC-7(3)、 NIST.800-53.r5 SC-7(4)、 NIST.800-53.r5 SC-7 (9)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ: `AWS::::Account`

AWS Config ルール: `s3-account-level-public-access-blocks-periodic`

スケジュールタイプ: 定期的

パラメータ:

- `ignorePublicAcls`: `true` (カスタマイズ不可)
- `blockPublicPolicy`: `true` (カスタマイズ不可)
- `blockPublicAcls`: `true` (カスタマイズ不可)
- `restrictPublicBuckets`: `true` (カスタマイズ不可)

このコントロールは、前述の Amazon S3 ブロックパブリックアクセス設定が S3 汎用バケットのアカウントレベルで設定されているかどうかを確認します。1 つ以上のブロックパブリックアクセス設定が に設定されている場合、コントロールは失敗しますfalse。

いずれかの設定が `false` に設定されているか、またはいずれかが設定されていない場合、コントロールは失敗します。

Amazon S3 パブリックアクセスブロックは、 全体 AWS アカウント または個々の S3 バケットレベルでコントロールを提供し、オブジェクトがパブリックアクセスされないように設計されています。パブリックアクセスは、アクセスコントロールリスト (ACL)、バケットポリシー、またはその両方からバケットおよびオブジェクトに付与されます。

S3 バケットをパブリックにアクセスできるように意図する場合を除き、アカウントレベルの Amazon S3 ブロックパブリックアクセス機能を設定する必要があります。

詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 ブロックパブリックアクセスの使用」を参照してください。

修正

の Amazon S3 パブリックアクセスブロックを有効にするには AWS アカウント、Amazon Simple Storage Service ユーザーガイドの「アカウントのパブリックアクセスブロック設定の構成」を参照してください。

[S3.2] S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります

> **Important**
>
> 2024 年 3 月 12 日、このコントロールのタイトルは表示されているタイトルに変更されました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.6、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 非常事態

リソースタイプ: `AWS::S3::Bucket`

AWS Config ルール : `s3-bucket-public-read-prohibited`

スケジュールタイプ: 定期的および変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon S3 汎用バケットがパブリック読み取りアクセスを許可するかどうかをチェックします。これにより、ブロックパブリックアクセス設定、バケットポリシー、およびバケットアクセスコントロールリスト (ACL) を評価します。バケットがパブリック読み取りアクセスを許可すると、コントロールは失敗します。

ユースケースによっては、インターネット上のすべてのユーザーが S3 バケットからの読み取りが必要な場合があります。しかし、そのような状況は稀です。データの整合性とセキュリティを確保するために、S3 バケットをパブリックに読み取り可能にしないでください。

修正

Amazon S3 バケットで公開読み取りアクセスをブロックするには、「Amazon Simple Storage Service ユーザーガイド」の「S3 バケットのブロックパブリックアクセス設定の構成」を参照してください。

[S3.3] S3 汎用バケットはパブリック書き込みアクセスをブロックする必要があります

> **Important**
>
> 2024 年 3 月 12 日、このコントロールのタイトルは表示されているタイトルに変更されました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 非常事態

リソースタイプ: `AWS::S3::Bucket`

AWS Config ルール : `s3-bucket-public-write-prohibited`

スケジュールタイプ: 定期的および変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon S3 汎用バケットがパブリック書き込みアクセスを許可するかどうかをチェックします。これにより、ブロックパブリックアクセス設定、バケットポリシー、およびバケットアクセスコントロールリスト (ACL) を評価します。バケットがパブリック書き込みアクセスを許可すると、コントロールは失敗します。

ユースケースによっては、インターネット上の全員が S3 バケットに書き込むことができる必要があります。しかし、そのような状況は稀です。データの整合性とセキュリティを確保するため、S3 バケットはパブリックに書き込み可能にしないでください。

修正

Amazon S3 バケットで公開書き込みアクセスをブロックするには、「Amazon Simple Storage Service ユーザーガイド」の「S3 バケットのブロックパブリックアクセス設定の構成」を参照してください。

[S3.5] S3 汎用バケットでは、SSL を使用するリクエストが必要です

> **Important**
>
> 2024 年 3 月 12 日、このコントロールのタイトルは表示されているタイトルに変更されました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

関連する要件： CIS AWS Foundations Benchmark v3.0.0/2.1.1、CIS AWS Foundations Benchmark v1.4.0/2.1.2、PCI DSS v3.2.1/4.1、NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23(3)、NIST.800-53 SC-23 SC-7 SC-8 SC-8 SC-8 SI-7

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::S3::Bucket`

AWS Config ルール : `s3-bucket-ssl-requests-only`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon S3 汎用バケットに SSL の使用リクエストを要求するポリシーがあるかどうかをチェックします。バケットポリシーで SSL を使用するリクエストが必要ない場合、コントロールは失敗します。

S3 バケットには、条件キー `aws:SecureTransport` によって示される S3 リソースポリシーで HTTPS 経由のデータ送信のみを受け入れるために、すべてのリクエスト (`Action: S3:*`) を要求するポリシーを備える必要があります。

修正

Amazon S3 バケットポリシーを更新して安全でないトランスポートを拒否するには、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。

以下のポリシーに、同様のポリシーステートメントを追加します。`DOC-EXAMPLE-BUCKET` を変更するバケットの名前で置き換えます。

```
{
    "Id": "ExamplePolicy",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
```

```
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            },
           "Principal": "*"
        }
    ]
}
```

詳細については、「 AWS 公式ナレッジセンター」のAWS Config 「ルール s3-bucket-ssl-requests-only? に準拠するためにどの S3 バケットポリシーを使用すべきか」を参照してください。

[S3.6] S3 汎用バケットポリシーでは、他の へのアクセスを制限する必要があります AWS アカウント

> **Important**
>
> 2024 年 3 月 12 日、このコントロールのタイトルは表示されているタイトルに変更されました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなアクセス管理 > 機密性の高いAPIオペレーションアクションを制限する

重要度: 高

リソースタイプ: `AWS::S3::Bucket`

AWS Config ルール: `s3-bucket-blacklisted-actions-prohibited`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- `blacklistedactionpatterns`: `s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl` (カスタマイズ不可)

このコントロールは、Amazon S3 汎用バケットポリシーが、プリンシパルが AWS アカウント S3 バケット内のリソースに対して拒否されたアクションを実行することを他の に禁止しているかどうかをチェックします。バケットポリシーが別の のプリンシパルに対して前述のアクションを 1 つ以上許可している場合、コントロールは失敗します AWS アカウント。

最小特権アクセスの実装は、セキュリティリスクおよびエラーの影響や悪意ある行動を減らす上での基礎となります。もしS3 バケットポリシーで外部アカウントからのアクセスを許可している場合、内部脅威または攻撃者によるデータの漏えいにつながる可能性があります。

`blacklistedactionpatterns` パラメータを使用すると、S3 バケットのルールを正常に評価できます。パラメータは、外部アカウントに対して `blacklistedactionpatterns` リストに含まれていないアクションパターンのアクセス許可を付与します。

修正

Amazon S3 バケットポリシーを更新してアクセス許可を削除するには、「Amazon Simple Storage Service ユーザーガイド」の「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。

[バケットポリシーを編集] ページのポリシー編集テキストボックスで、以下のいずれかのアクションを実行します。

- 拒否されたアクションへのアクセス許可を別の AWS アカウント に付与するステートメントを削除する。
- 許可済みの拒否されたアクションをステートメントから削除する。

[S3.7] S3 汎用バケットはクロスリージョンレプリケーションを使用する必要があります

> **Important**
>
> 2024 年 3 月 12 日、このコントロールのタイトルは表示されているタイトルに変更されました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

関連する要件: PCI DSS v3.2.1/2.2、NIST.800-53.r5 AU-9(2)、NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-36(2)、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 低

リソースタイプ: `AWS::S3::Bucket`

AWS Config ルール: `s3-bucket-cross-region-replication-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon S3 汎用バケットでクロスリージョンレプリケーションが有効になっているかどうかをチェックします。バケットでクロスリージョンレプリケーションが有効になっていない場合、コントロールは失敗します。

レプリケーションは、同じ または異なる のバケット間でオブジェクトを自動的に非同期コピーします AWS リージョン。レプリケーションは、新しく作成されたオブジェクトと、レプリケート元バケットからレプリケート先バケットへのオブジェクトの更新をコピーします。 AWS ベストプラクティスでは、同じ AWS アカウント が所有するレプリケート元バケットとレプリケート先バケットのレプリケーションを推奨しています。可用性に加えて、他のシステム強化構成も考慮する必要があります。

修正

Amazon S3 バケットのレプリケーションを有効にするには、「Amazon Simple Storage Service ユーザーガイド」の「同じアカウントが所有するレプリケート元バケットとレプリケート先バケットのレプリケーションの設定」を参照してください。[ソースバケット] で、[バケット内のすべてのオブジェクトに適用] を選択します。

[S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/2.1.4、CIS AWS Foundations Benchmark v1.4.0/2.1.5、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(1)、NIST.800-53.r5 SC-7 SC-7 SC-7 SC-7 SC-7 SC-77

カテゴリ: 保護 > セキュアなアクセス管理 > アクセスコントロール

重要度: 高

リソースタイプ: `AWS::S3::Bucket`

AWS Config ルール : s3-bucket-level-public-access-prohibited

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

- excludedPublicBuckets (カスタマイズ不可) - 既知の許可されているパブリック S3 バケット名のカンマ区切りリスト

このコントロールは、Amazon S3 汎用バケットがバケットレベルでパブリックアクセスをブロックしているかどうかをチェックします。次のいずれかの設定が に設定されている場合、コントロールは失敗しますfalse。

- ignorePublicAcls
- blockPublicPolicy
- blockPublicAcls
- restrictPublicBuckets

S3 バケットレベルのブロックパブリックアクセスは、オブジェクトがパブリックアクセスできないようにコントロールを提供します。パブリックアクセスは、アクセスコントロールリスト (ACL)、バケットポリシー、またはその両方からバケットおよびオブジェクトに付与されます。

S3 バケットをパブリックにアクセスできるように意図する場合を除き、バケットレベルの Amazon S3 ブロックパブリックアクセス機能を設定する必要があります。

修正

バケットレベルでパブリックアクセスを削除する方法については、「Amazon S3 ユーザーガイド」の「Amazon S3 ストレージへのパブリックアクセスのブロック」を参照してください。

[S3.9] S3 汎用バケットでは、サーバーアクセスのログ記録を有効にする必要があります

> **Important**
>
> 2024 年 3 月 12 日、このコントロールのタイトルは表示されているタイトルに変更されました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

関連する要件: NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::S3::Bucket`

AWS Config ルール : `s3-bucket-logging-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon S3 汎用バケットでサーバーアクセスログ記録が有効になっているかどうかをチェックします。サーバーアクセスのログ記録が有効になっていない場合、コントロールは失敗します。ログ記録を有効にすると、Amazon S3 は、ソースバケットのアクセスログを選択されたターゲットバケットに配信します。ターゲットバケットはソースバケット AWS リージョン と同じ にあり、デフォルトの保持期間を設定していない必要があります。ターゲットのログ記録バケットは、サーバーアクセスのログ記録を有効にする必要がないため、このバケットの結果は非表示にします。

サーバーアクセスのログ記録には、バケットに対するリクエストの詳細を提供します。サーバーアクセスログは、セキュリティとアクセス監査に役立ちます。詳細については、「Amazon S3 のセキュリティベストプラクティス: Amazon S3 サーバーアクセスログを有効にします」を参照してください。

修正

Amazon S3 のサーバーアクセスのログ記録を有効にするには、「Amazon S3 ユーザーガイド」の「Amazon S3 サーバーアクセスログの有効化」を参照してください。

[S3.10] バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です

> **Important**
>
> 2024 年 3 月 12 日、このコントロールのタイトルは表示されているタイトルに変更されました。Security Hub は 2024 年 4 月にこのコントロールを AWS Foundational Security Best

Practices 標準から廃止しましたが、NIST SP 800-53 Rev. 5 標準にまだ含まれています。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::S3::Bucket`

AWS Config ルール : `s3-version-lifecycle-policy-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon S3 汎用バージョニングバケットにライフサイクル設定があるかどうかをチェックします。バケットにライフサイクル設定がない場合、コントロールは失敗します。

オブジェクトの存続期間中に Amazon S3 が実行するアクションを定義するのに役立つように、S3 バケットのライフサイクル設定を作成することをお勧めします。 Amazon S3

修正

Amazon S3 バケットでのライフサイクルの設定の詳細については、「バケットのライフサイクル設定の指定」と「ストレージのライフサイクルの管理」を参照してください。

[S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります

Important

2024 年 3 月 12 日、このコントロールのタイトルは表示されているタイトルに変更されました。Security Hub は 2024 年 4 月に AWS Foundational Security Best Practices 標準からこのコントロールを廃止しましたが、NIST SP 800-53 Rev. 5 標準には含まれています。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

関連する要件: NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-4(4)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::S3::Bucket`

AWS Config ルール : `s3-event-notifications-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`eventTypes`	推奨される S3 イベントタイプのリスト	EnumList（最大 28 項目）	`s3:IntelligentTiering`, `s3:LifecycleExpiration:*`, `s3:LifecycleExpiration:Delete`, `s3:LifecycleExpiration:DeleteMarkerCreated`, `s3:LifecycleTransition`, `s3:ObjectAcl:Put`, `s3:ObjectCreated:*`	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
			, s3:ObjectCreated:CompleteMultipartUpload, s3:ObjectCreated:Copy, s3:ObjectCreated:Post, s3:ObjectCreated:Put, s3:ObjectRemoved:* , s3:ObjectRemoved:Delete, s3:ObjectRemoved:DeleteMarkerCreated , s3:ObjectRestore:* , s3:ObjectRestore:Completed,	

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
			s3:ObjectRestore:Delete, s3:ObjectRestore:Post, s3:ObjectTagging:*, s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replication:*, s3:Replication:OperationFailedReplication, s3:Replication:OperationMissedThreshold, s3:Replic	

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
			`ation:OperationNotTracked, s3:ReplicationOperationReplicatedAfterThreshold, s3:TestEvent`	

このコントロールは、Amazon S3 汎用バケットで Amazon S3イベント通知が有効になっているかどうかをチェックします。バケットで S3 イベント通知が有効になっていない場合、コントロールは失敗します。`eventTypes` パラメータにカスタム値を指定すると、指定されたタイプのイベントでイベント通知が有効になっている場合にのみコントロールが成功します。

S3 イベント通知を有効にすると、S3 バケットに影響を与える特定のイベントが発生したときにアラートを受け取ります。例えば、オブジェクトの作成、オブジェクトの削除、オブジェクトの復元を通知を受けることができます。これらの通知により、不正なデータアクセスにつながる可能性のある偶発的または意図的な変更を関連チームに警告することができます。

修正

S3 バケットおよびオブジェクトの変更を、検出する方法の詳細については、「Amazon S3 ユーザーガイド」の「Amazon S3 イベント通知」を参照してください。

[S3.12] ACLs を使用しないでください S3

> **Important**
>
> 2024 年 3 月 12 日、このコントロールのタイトルは表示されているタイトルに変更されました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理 > アクセスコントロール

重要度: 中

リソースタイプ: `AWS::S3::Bucket`

AWS Config ルール : `s3-bucket-acl-prohibited`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon S3 汎用バケットがアクセスコントロールリスト (ACL) を持つユーザーアクセス許可を付与しているかどうかをチェックします。ACL がバケットへのユーザーアクセスを管理するように設定されている場合、コントロールは失敗します。

ACL は、IAM よりも前のレガシーアクセスコントロールメカニズムです。ACLs の代わりに、S3 バケットポリシーまたは AWS Identity and Access Management (IAM) ポリシーを使用して S3 バケットへのアクセスを管理することをお勧めします。

修正

このコントロールに合格するには、S3 バケットの ACL を無効にする必要があります。手順については、「Amazon Simple Storage Service ユーザーガイド」の「オブジェクトの所有権の制御とバケットの ACL の無効化」を参照してください。

S3 バケットポリシーを作成するには、「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。S3 バケットに IAM ユーザーポリシーを作成するには、「ユーザーポリシーを使用したバケットへのアクセスの制御」を参照してください。

[S3.13] S3 汎用バケットにはライフサイクル設定が必要です

> **Important**
>
> 2024 年 3 月 12 日、このコントロールのタイトルは表示されているタイトルに変更されました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: 保護 > データ保護

重要度: 低

リソースタイプ: `AWS::S3::Bucket`

AWS Config ルール : `s3-lifecycle-policy-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`targetTransitionDays`	オブジェクトが、その作成後、指定されたストレージクラスに移行するまでの日数	整数	`1~36500`	デフォルト値なし
`targetExpirationDays`	オブジェクトが作成されてから削除されるまでの日数	整数	`1~36500`	デフォルト値なし
`targetTransitionStorageClass`	送信先 S3 ストレージクラスのタイプ	列挙型	`STANDARD_IA, INTELLIGENT_TIERING, ONEZONE_IA, GLACIER, GLACIER_IR, DEEP_ARCHIVE`	デフォルト値なし

このコントロールは、Amazon S3 汎用バケットにライフサイクル設定があるかどうかをチェックします。バケットにライフサイクル設定がない場合、コントロールは失敗します。前述の 1 つ以上のパラメータにカスタム値を指定したときは、指定されたストレージクラス、削除時間、または移行時間がポリシーに含まれている場合にのみコントロールが成功します。

S3 バケットのライフサイクル設定を作成すると、オブジェクトの存続期間中に Amazon S3 が実行するアクションが定義されます。例えば、オブジェクトを別のストレージクラスに移行させる、アーカイブする、あるいは指定した期間後に削除する、といったことが可能です。

修正

Amazon S3 バケットでライフサイクルポリシーを設定する方法の詳細については、「Amazon S3 ユーザーガイド」の「バケットのライフサイクル設定の指定」および「ストレージのライフサイクルの管理」を参照してください。

[S3.14] S3 汎用バケットではバージョニングを有効にする必要があります

> **Important**
>
> 2024 年 3 月 12 日、このコントロールのタイトルは表示されているタイトルに変更されました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

カテゴリ: 保護 > データ保護 > データ削除保護

関連する要件: NIST.800-53.r5 AU-9(2)、NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

重要度: 低

リソースタイプ: `AWS::S3::Bucket`

AWS Config ルール : `s3-bucket-versioning-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon S3 汎用バケットでバージョニングが有効になっているかどうかをチェックします。バケットのバージョニングが停止されている場合、コントロールは失敗します。

バージョニングにより、同じ S3 バケット内でオブジェクトの複数のバリアントを保持します。バージョニングを使用して、S3 バケットに保存されたオブジェクトの旧バージョンを保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションとアプリケーション障害から復旧できます。

> **Tip**
>
> バージョニングが原因でバケット内のオブジェクトの数が増加すると、ルールに基づいてバージョニングされたオブジェクトを自動的にアーカイブまたは削除するようにライフサイクル設定を設定できます。詳細については、「バージョニングされたオブジェクトの Amazon S3 ライフサイクル管理」を参照してください。

修正

S3 バケットでバージョニングを使用するには、「Amazon S3 ユーザーガイド」の「バケットでのバージョニングの有効化」を参照してください。

[S3.15] S3 汎用バケットでは、オブジェクトロックを有効にする必要があります

> **Important**
>
> 2024 年 3 月 12 日、このコントロールのタイトルは表示されているタイトルに変更されました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

カテゴリ: 保護 > データ保護 > データ削除保護

関連する要件: NIST.800-53.r5 CP-6(2)

重要度: 中

リソースタイプ: `AWS::S3::Bucket`

AWS Config ルール： `s3-bucket-default-lock-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
mode	S3 Object Lock の保持モード	列挙型	GOVERNANCE , COMPLIANCE	デフォルト値なし

このコントロールは、Amazon S3 汎用バケットでオブジェクトロックが有効になっているかどうかをチェックします。オブジェクトロックがバケットに対して有効になっていない場合、コントロールは失敗します。mode パラメータにカスタム値を指定したときは、S3 Object Lock が指定された保持モードを使用する場合にのみコントロールが成功します。

S3 オブジェクトロックを使用して、 write-once-read-many (WORM) モデルを使用してオブジェクトを保存できます。Object Lock により、S3 バケットのオブジェクトが削除または上書きされることを、一定期間または無期限に防止できます。S3 Object Lock を使用して、WORM ストレージを必要とする規制要件を満たしたり、オブジェクトの変更や削除に対する保護レイヤーを追加したりできます。

修正

新規および既存の S3 バケットの Object Lock を設定するには、「Amazon S3 ユーザーガイド」の「オブジェクトロックの設定」を参照してください。

[S3.17] S3 汎用バケットは、保管時に で暗号化する必要があります AWS KMS keys

> **Important**
>
> 2024 年 3 月 12 日、このコントロールのタイトルは表示されているタイトルに変更されました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

関連する要件: NIST.800-53.r5 SC-12(2)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 SI-7(6)、NIST.800-53.r5 AU-9

重要度: 中

リソースタイプ: `AWS::S3::Bucket`

AWS Config ルール： `s3-default-encryption-kms`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon S3 汎用バケットが AWS KMS key (SSE-KMS または DSSE-KMS) で暗号化されているかどうかをチェックします。バケットがデフォルトの暗号化 (SSE-S3) で暗号化されている場合、コントロールは失敗します。

サーバー側の暗号化 (SSE)とは、データを受信するアプリケーションまたはサービスによって、送信先でデータを暗号化することです。特に指定しない限り、デフォルトでは、S3 バケットはサーバー側の暗号化に Amazon S3 マネージドキー (SSE-S3) を使用します。ただし、コントロールを強化するために、代わりに AWS KMS keys (SSE-KMS または DSSE-KMS) によるサーバー側の暗号化を使用するようにバケットを設定することもできます。Amazon S3 は、 AWS データセンターのディスクにデータを書き込むときにオブジェクトレベルでデータを暗号化し、アクセス時に復号します。

修正

SSE-KMS を使用して S3 バケットを暗号化するには、「Amazon S3 ユーザーガイド」の AWS KMS 「 (SSE-KMS) によるサーバー側の暗号化の指定」を参照してください。 Amazon S3 DSSE-KMS を使用して S3 バケットを暗号化するには、「Amazon S3 ユーザーガイド」の AWS KMS keys 「 (DSSE-KMS) による二層式サーバー側の暗号化の指定」を参照してください。 Amazon S3

[S3.19] S3 アクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなアクセス管理 > パブリックアクセスが不可能なリソース

重要度: 非常事態

リソースタイプ: `AWS::S3::AccessPoint`

AWS Config ルール： s3-access-point-public-access-blocks

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon S3 アクセスポイントでブロックパブリックアクセス設定が有効になっているかどうかをチェックします。アクセスポイントのブロックパブリックアクセス設定が有効になっていない場合、コントロールは失敗します。

Amazon S3 パブリックアクセスブロック機能は、アカウント、バケット、アクセスポイントの 3 つのレベルで S3 リソースへのアクセスを管理するのに役立ちます。各レベルの設定は個別に構成できるため、データに対して異なるレベルのパブリックアクセス制限を設定できます。アクセスポイントの設定で、より高いレベル (アカウントレベルまたはアクセスポイントに割り当てられたバケット) のより制限的な設定を個別にオーバーライドすることはできません。むしろ、アクセスポイントレベルの設定は付加的です。つまり、他のレベルの設定を補完し、連携して機能します。S3 アクセスポイントをパブリックにアクセス可能にする予定がない限り、ブロックパブリックアクセス設定を有効にする必要があります。

修正

Amazon S3 は、現在、アクセスポイントの作成後におけるアクセスポイントのブロックパブリックアクセス設定の変更をサポートしていません。デフォルトでは、新しいアクセスポイントを作成すると、すべてのブロックパブリックアクセス設定が有効になります。これらの設定を特に無効にする必要がある場合を除いて、すべての設定を有効にしておくことをお勧めします。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「アクセスポイントへのパブリックアクセスの管理」を参照してください。

[S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/2.1.2、CIS AWS Foundations Benchmark v1.4.0/2.1.3、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

カテゴリ: 保護 > データ保護 > データ削除保護

重要度: 低

リソースタイプ: `AWS::S3::Bucket`

AWS Config ルール： s3-bucket-mfa-delete-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon S3 汎用バージョニングバケットで多要素認証 (MFA) 削除が有効になっているかどうかをチェックします。バケットで MFA 削除が有効になっていない場合、コントロールは失敗します。コントロールは、ライフサイクル設定を持つバケットの検出結果を生成しません。

Amazon S3 バケットで S3 バージョニングを行うときに、MFA 削除が有効になるようにバケットを設定すれば、セキュリティをさらに強化できます。この設定を行うと、バケット所有者は、特定のバージョンを削除したりバケットのバージョニング状態を変更したりするリクエストに、2 つの認証形式を含めることが必要になります。MFA 削除は、セキュリティ認証情報に不正なアクセスがあった場合にセキュリティを強化します。また、MFA 削除は、削除アクションを開始したユーザーに MFA コードを使って MFA デバイスの物理的所有を証明するように要求したり、削除アクションに摩擦とセキュリティのレイヤーをさらに追加したりすることで、バケットの偶発的な削除を防ぎます。

> **Note**
>
> MFA 削除機能には、依存関係としてバケットのバージョニングが必要です。バケットのバージョニングとは、同じバケット内で S3 オブジェクトの複数のバリエーションを保持する方法です。さらに、ルートユーザーとしてログインしているバケット所有者のみが、MFA 削除を有効にして、S3 バケットで削除アクションを実行できます。

修正

S3 バージョニングを有効にして、バケットで MFA 削除を設定するには、「Amazon Simple Storage Service ユーザーガイド」の「MFA 削除の設定」を参照してください。

[S3.22] S3 汎用バケットは、オブジェクトレベルの書き込みイベントをログに記録する必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/3.8

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::::Account`

AWS Config ルール： `cloudtrail-all-write-s3-data-event-check`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロール AWS アカウント は、 に、Amazon S3 バケットのすべての書き込みデータイベントを記録する AWS CloudTrail マルチリージョン証跡が少なくとも 1 つあるかどうかをチェックします。 Amazon S3 アカウントに S3 バケットの書き込みデータイベントをログに記録するマルチリージョンの証跡がない場合、コントロールは失敗します。

、、 などの S3 オブジェクトレベルのオペレーションは`GetObject`、`DeleteObject`、`PutObject`データイベントと呼ばれます。デフォルトでは、 CloudTrail はデータイベントをログに記録しませんが、S3 バケットのデータイベントをログに記録するように証跡を設定できます。書き込みデータイベントのオブジェクトレベルのログ記録を有効にすると、S3 バケット内の個々のオブジェクト (ファイル) アクセスをログに記録できます。オブジェクトレベルのログ記録を有効にすると、Amazon CloudWatch Events を使用して、データコンプライアンス要件を満たす、包括的なセキュリティ分析を実行する、 でのユーザー動作の特定のパターンをモニタリングする AWS アカウント、S3 バケット内のオブジェクトレベルの API アクティビティに対してアクションを実行するのに役立ちます。このコントロールは、すべての S3 バケットの書き込み専用またはすべてのタイプのデータイベントをログに記録するマルチリージョン証跡を設定すると、`PASSED`結果を生成します。

修正

S3 バケットのオブジェクトレベルのログ記録を有効にするには、「Amazon Simple Storage Service ユーザーガイド」のS3 バケットとオブジェクトの CloudTrail イベントログ記録を有効にする」を参照してください。

[S3.23] S3 汎用バケットは、オブジェクトレベルの読み取りイベントをログに記録する必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/3.9

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::::Account`

AWS Config ルール： cloudtrail-all-read-s3-data-event-check

スケジュールタイプ: 定期的

パラメータ: なし

このコントロール AWS アカウント は、 に Amazon S3 バケットのすべての読み取りデータイベントを記録する AWS CloudTrail マルチリージョン証跡が少なくとも 1 つあるかどうかをチェックします。 Amazon S3 アカウントに S3 バケットの読み取りデータイベントをログに記録するマルチリージョンの証跡がない場合、コントロールは失敗します。

、、 などの S3 オブジェクトレベルのオペレーションはGetObjectDeleteObjectPutObject、データイベントと呼ばれます。デフォルトでは、 CloudTrail はデータイベントをログに記録しませんが、S3 バケットのデータイベントをログに記録するように証跡を設定できます。読み取りデータイベントのオブジェクトレベルのログ記録を有効にすると、S3 バケット内の個々のオブジェクト (ファイル) アクセスをログに記録できます。オブジェクトレベルのログ記録を有効にすると、Amazon CloudWatch Events を使用して、データコンプライアンス要件を満たす、包括的なセキュリティ分析を実行する、 でのユーザー動作の特定のパターンをモニタリングする AWS アカウント、S3 バケット内のオブジェクトレベルの API アクティビティに対してアクションを実行するのに役立ちます。このコントロールは、すべての S3 バケットの読み取り専用またはすべてのタイプのデータイベントをログに記録するマルチリージョン証跡を設定すると、PASSED結果を生成します。

修正

S3 バケットのオブジェクトレベルのログ記録を有効にするには、「Amazon Simple Storage Service ユーザーガイド」のS3 バケットとオブジェクトの CloudTrail イベントログ記録の有効化」を参照してください。

Amazon SageMaker コントロール

これらのコントロールは SageMaker リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、NIST.800-53.r5 AC-21、NIST.800-53.r5

AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ: `AWS::SageMaker::NotebookInstance`

AWS Config ルール: `sagemaker-notebook-no-direct-internet-access`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、 SageMaker ノートブックインスタンスで直接インターネットアクセスが無効になっているかどうかをチェックします。ノートブックインスタンスで `DirectInternetAccess`フィールドが有効になっている場合、コントロールは失敗します。

VPC なしで SageMaker インスタンスを設定すると、デフォルトでインスタンスで直接インターネットアクセスが有効になります。VPC ありでインスタンスを設定し、デフォルト設定を [無効化 - VPC 経由でインターネットにアクセスする] に変更する必要があります。ノートブックからモデルをトレーニングまたはホストするには、インターネットアクセスが必要です。インターネットアクセスを有効にするには、VPC にインターフェイスエンドポイント (AWS PrivateLink) または NAT ゲートウェイのいずれかと、アウトバウンド接続を許可するセキュリティグループが必要です。ノートブックインスタンスを VPC 内のリソースに接続する方法の詳細については、「Amazon SageMaker デベロッパーガイド」の「ノートブックインスタンスを VPC 内のリソースに接続する」を参照してください。また、 SageMaker 設定へのアクセスが許可されたユーザーのみに制限されていることを確認する必要があります。ユーザーが SageMaker 設定とリソースを変更できるようにする IAM アクセス許可を制限します。

修正

ノートブックインスタンスを作成した後は、インターネットアクセスの設定を変更することはできません。代わりに、インターネットアクセスがブロックされているインスタンスを停止して削除し、再作成できます。直接インターネットアクセスを許可するノートブックインスタンスを削除するには、「Amazon SageMaker デベロッパーガイド」の「ノートブックインスタンスを使用してモデルを構築する: クリーンアップ」を参照してください。インターネットアクセスを拒否するノート

ブックインスタンスを再作成するには、「ノートブックインスタンスを作成する」を参照してください。[ネットワーク] の [直接インターネットアクセス] で、[無効化 - VPC 経由でインターネットにアクセスする] を選択します。

〔SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > VPC 内のリソース

重要度: 高

リソースタイプ: `AWS::SageMaker::NotebookInstance`

AWS Config ルール : `sagemaker-notebook-instance-inside-vpc`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon SageMaker ノートブックインスタンスがカスタム Virtual Private Cloud (VPC) 内で起動されているかどうかを確認します。このコントロールは、 SageMaker ノートブックインスタンスがカスタム VPC 内で起動されない場合、または SageMaker サービス VPC 内で起動された場合に失敗します。

サブネットは、ある範囲の IP アドレスが示す VPC 内の領域です。インフラストラクチャの安全なネットワーク保護を確保するために、リソースは可能な限りカスタム VPC 内に保管することをお勧めします。Amazon VPC は、 専用の仮想ネットワークです AWS アカウント。Amazon VPC を使用すると、 SageMaker Studio インスタンスとノートブックインスタンスのネットワークアクセスとインターネット接続を制御できます。

修正

ノートブックインスタンスを作成した後は、VPC の設定を変更することはできません。代わりに、インスタンスを停止して削除し、再作成できます。手順については、「Amazon SageMaker デベ

ロッパーガイド」の「ノートブックインスタンスを使用してモデルを構築する: クリーンアップ」を参照してください。

〔SageMaker.3] SageMaker ユーザーはノートブックインスタンスへのルートアクセスを許可されない

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(10)、NIST.800-53.r5 AC-6(2)

カテゴリ: 保護 > セキュアなアクセス管理 > ルートユーザーのアクセス制限

重要度: 高

リソースタイプ: `AWS::SageMaker::NotebookInstance`

AWS Config ルール : `sagemaker-notebook-instance-root-access-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon SageMaker Notebook インスタンスのルートアクセスが有効になっているかどうかをチェックします。 SageMaker ノートブックインスタンスのルートアクセスが有効になっている場合、コントロールは失敗します。

最小特権のプリンシパルに従い、意図せずに権限を過剰にプロビジョニングしないために、ルートアクセスをインスタンスリソースに制限することが、推奨されるセキュリティ上のベストプラクティスです。

修正

SageMaker ノートブックインスタンスへのルートアクセスを制限するには、「Amazon SageMaker デベロッパーガイド」の SageMaker「ノートブックインスタンスへのルートアクセスを制御する」を参照してください。

〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります

関連する要件： NIST.800-53.r5 CP-10、NIST.800-53.r5 SC-5、NIST.800-53.r5 SC-36、NIST.800-53.r5 SA-13

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::SageMaker::EndpointConfig`

AWS Config ルール: `sagemaker-endpoint-config-prod-instance-count`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、Amazon SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数が 1 より大きいかどうかをチェックします。エンドポイントの本番稼働用バリアントの初期インスタンスが 1 つしかない場合、コントロールは失敗します。

インスタンス数が 1 を超える本番稼働用バリアントは、 によって管理されるマルチ AZ インスタンスの冗長性を許可しますSageMaker。複数のアベイラビリティーゾーンにリソースをデプロイすることは、アーキテクチャ内で高可用性を実現するための AWS ベストプラクティスです。高可用性は、セキュリティインシデントからの回復に役立ちます。

> **Note**
>
> このコントロールは、インスタンスベースのエンドポイント設定にのみ適用されます。

修正

エンドポイント設定のパラメータの詳細については、「Amazon SageMaker デベロッパーガイド」の「エンドポイント設定の作成」を参照してください。

AWS Secrets Manager コントロール

これらのコントロールは Secrets Manager リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔SecretsManager.1] Secrets Manager シークレットでは、自動ローテーションを有効にする必要があります

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)

カテゴリ: 保護 > セキュアな開発

重要度: 中

リソースタイプ: `AWS::SecretsManager::Secret`

AWS Config ルール : `secretsmanager-rotation-enabled-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`maximumAllowedRotationFrequency`	シークレットローテーション頻度の許容最大日数	整数	`1~365`	デフォルト値なし

このコントロール AWS Secrets Manager は、 に保存されているシークレットが自動ローテーションで設定されているかどうかをチェックします。シークレットが自動ローテーションで構成されていない場合、コントロールは失敗します。`maximumAllowedRotationFrequency` パラメータにカスタム値を指定したときは、指定された時間帯内にシークレットが自動的にローテーションされた場合にのみコントロールが成功します。

Secrets Manager は、組織のセキュリティ体制を向上するのに役立ちます。シークレットとは、データベース認証情報、パスワード、サードパーティーの API キーなどが含まれます。Secrets Manager を使用することで、シークレットを一元的に保存、シークレットの自動暗号化、シークレットへのアクセスコントロール、シークレットを安全かつ自動的にローテーションすることができます。

Secrets Manager はシークレットをローテーションできます。ローテーションを使用して、長期のシークレットを短期のシークレッに置き換えることができます。シークレットをローテーションすることで、権限のないユーザーが侵害されたシークレットを使用できる期間を制限することができます。このため、シークレットは頻繁にローテーションする必要があります。ローテーションの詳細については、「 AWS Secrets Manager ユーザーガイド」の「シー AWS Secrets Manager クレットのローテーション」を参照してください。

修正

Secrets Manager シークレットの自動ローテーションを有効にするには、「 AWS Secrets Manager ユーザーガイド」の「コンソールを使用して AWS Secrets Manager シークレットの自動ローテーションを設定する」を参照してください。ローテーション用の AWS Lambda 関数を選択して設定する必要があります。

〔SecretsManager.2] 自動ローテーションで設定された Secrets Manager シークレットは正常にローテーションする必要があります

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)

カテゴリ: 保護 > セキュアな開発

重要度: 中

リソースタイプ: `AWS::SecretsManager::Secret`

AWS Config ルール : `secretsmanager-scheduled-rotation-success-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS Secrets Manager シークレットがローテーションスケジュールに基づいて正常にローテーションされたかどうかをチェックします。`RotationOccurringAsScheduled` が `false` の場合、コントロールは失敗します。コントロールは、ローテーションがオンになっているシークレットのみを評価します。

Secrets Manager は、組織のセキュリティ体制を向上するのに役立ちます。シークレットとは、データベース認証情報、パスワード、サードパーティーの API キーなどが含まれます。Secrets Manager を使用することで、シークレットを一元的に保存、シークレットの自動暗号化、シークレットへのアクセスコントロール、シークレットを安全かつ自動的にローテーションすることができます。

Secrets Manager はシークレットをローテーションできます。ローテーションを使用して、長期のシークレットを短期のシークレッに置き換えることができます。シークレットをローテーションすることで、権限のないユーザーが侵害されたシークレットを使用できる期間を制限することができます。このため、シークレットは頻繁にローテーションする必要があります。

シークレットが自動的にローテーションされるように設定することに加えて、これらのシークレットがローテーションスケジュールに基づいて正常にローテーションするように設定する必要があります。

ローテーションの詳細については、「AWS Secrets Manager ユーザーガイド」の「AWS Secrets Manager シークレットのローテーション」を参照してください。

修正

自動ローテーションが失敗した場合、Secrets Manager の設定でエラーが発生している可能性があります。Secrets Manager でシークレットをローテーションさせるには、シークレットを所有するデータベースまたはサービスとの対話方法を定義する Lambda 関数を使用する必要があります。

シークレットのローテーションに関連する一般的なエラーの診断と修正については、「 AWS Secrets Manager ユーザーガイド」の「シークレットの AWS Secrets Manager ローテーションのトラブルシューティング」を参照してください。

〔SecretsManager.3] 未使用の Secrets Manager シークレットを削除する

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::SecretsManager::Secret`

AWS Config ルール: `secretsmanager-secret-unused`

スケジュールタイプ: 定期的

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`unusedForDays`	シークレットを未使用のままにできる最大日数	整数	`1~365`	`90`

このコントロールは、シー AWS Secrets Manager クレットが指定された期間内にアクセスされたかどうかをチェックします。指定された時間枠を過ぎてもシークレットが使用されない場合、コントロールは失敗します。アクセス期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 90 日を使用します。

未使用のシークレットを削除することは、シークレットをローテーションするのと同様に重要です。未使用のシークレットは、これらのシークレットにアクセスする必要のない以前のユーザーによって悪用される可能性があります。また、より多くのユーザーがシークレットへのアクセスすると、誰かが誤って処理して権限のないエンティティに漏洩する可能性があるため、不正使用のリスクが高まります。未使用のシークレットを削除することで、必要としないユーザーからのシークレットへのアクセスを取り消すことができます。また、Secrets Manager の使用コスト削減にも役立ちます。したがって、未使用のシークレットを定期的に削除することが不可欠です。

修正

非アクティブな Secrets Manager シークレットを削除するには、「AWS Secrets Manager ユーザーガイド」の「AWS Secrets Manager シークレットの削除」を参照してください。

〔SecretsManager.4] Secrets Manager のシークレットは、指定された日数内にローテーションする必要があります

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ: `AWS::SecretsManager::Secret`

AWS Config ルール: `secretsmanager-secret-periodic-rotation`

スケジュールタイプ: 定期的

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`maxDaysSinceRotation`	シークレットを未変更のままにできる最大日数	整数	`1~180`	`90`

このコントロールは、シー AWS Secrets Manager クレットが指定された時間枠内に少なくとも 1 回ローテーションされているかどうかをチェックします。シークレットを少なくともこの頻度でロー

テーションしないと、コントロールは失敗します。ローテーション期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 90 日を使用します。

シークレットをローテーションすることで、 AWS アカウントでユーザーのシークレットが不正に使用されるリスクを減らすのに役立ちます。例えば、データベース認証情報、パスワード、サードパーティーの API キーおよび任意のテキストなどがあります。シークレットを長期間変更しない場合、シークレットが侵害される可能性が高くなります。

より多くのユーザーがシークレットへのアクセスすると、誰かが操作を誤り、権限のないエンティティに漏洩する可能性があります。シークレットは、ログとキャッシュデータを介して漏洩する可能性があります。これらはデバッグ目的で共有でき、デバッグ完了後に変更または取り消されることはありません。これらすべての理由から、シークレットは頻繁にローテーションする必要があります。

AWS Secrets Managerでシークレットの自動ローテーションを設定できます。自動ローテーションにより、長期のシークレットを短期のシークレットに置き換えることが可能となり、侵害されるリスクを大幅に減少させるのに役立ちます。Secrets Manager のシークレットの自動ローテーションを設定することをお勧めします。詳細については、「AWS Secrets Manager ユーザーガイド」の「AWS Secrets Manager シークレットのローテーション」を参照してください。

修正

Secrets Manager シークレットの自動ローテーションを有効にするには、「 AWS Secrets Manager ユーザーガイド」の「コンソールを使用して AWS Secrets Manager シークレットの自動ローテーションを設定する」を参照してください。ローテーション用の AWS Lambda 関数を選択して設定する必要があります。

〔SecretsManager.5] Secrets Manager のシークレットにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::SecretsManager::Secret`

AWS Config ルール: `tagged-secretsmanager-secret` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS Secrets Manager シークレットにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。シークレットにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタグキーの存在のみをチェックし、シークレットにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグ`aws:`は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。ABAC は、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Secrets Manager シークレットにタグを追加するには、AWS Secrets Manager 「 ユーザーガイド」の「タグシーク AWS Secrets Manager レット」を参照してください。

AWS Service Catalog コントロール

これらのコントロールは Service Catalog リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります

関連する要件： NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-6、NIST.800-53.r5 CM-8、NIST.800-53.r5 SC-7

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 高

リソースタイプ: `AWS::ServiceCatalog::Portfolio`

AWS Config ルール : `servicecatalog-shared-within-organization`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 と AWS Organizations の統合が有効になっているときに、 が組織内のポートフォリオ AWS Service Catalog を共有するかどうかをチェックします。ポートフォリオが組織内で共有されていない場合、コントロールは失敗します。

Organizations 内でのみポートフォリオを共有すると、ポートフォリオが間違った と共有されないようになります AWS アカウント。Service Catalog ポートフォリオを組織内のアカウントと共有するために、Security Hub では `ORGANIZATION_MEMBER_ACCOUNT`の代わりに を使用することをお勧めします`ACCOUNT`。これにより、組織全体のアカウントに付与されるアクセスを管理できるため、管理が簡素化されます。Service Catalog ポートフォリオを外部アカウントと共有する必要がある場合は、このコントロールの検出結果を自動的に抑制するか、無効にすることができます。

修正

Organizations とのポートフォリオ共有を有効にするには、「Service Catalog 管理者ガイド」の「との共有 AWS Organizations」を参照してください。

Amazon Simple Email Service コントロール

これらのコントロールは Amazon SES リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[SES.1] SES 連絡先リストにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::SES::ContactList`

AWS Configルール: `tagged-ses-contactlist` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon SES 連絡先リストに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。連絡先リストにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しま

すrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、連絡先リストにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Amazon SES 連絡先リストにタグを追加するには、TagResourceAmazon SESv2 リファレンス」の「」を参照してください。

[SES.2] SES 設定セットにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: AWS::SES::ConfigurationSet

AWS Configルール: tagged-ses-configurationset (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、Amazon SES 設定セットに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。設定セットにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、設定セットにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Amazon SES 設定セットにタグを追加するには、TagResourceAmazon SESv2 リファレンス」の「」を参照してください。

Amazon Simple Notification Service コントロール

これらのコントロールは Amazon SNS リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[SNS.1] SNS トピックは、保管時に を使用して暗号化する必要があります AWS KMS

> **Important**
>
> Security Hub は 2024 年 4 月にこのコントロールを AWS Foundational Security Best Practices 標準から廃止しましたが、NIST SP 800-53 Rev. 5 標準にまだ含まれています。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::SNS::Topic`

AWS Config ルール : `sns-encrypted-kms`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon SNS トピックが AWS Key Management Service () で管理されるキーを使用して保管時に暗号化されているかどうかをチェックしますAWS KMS。SNS トピックがサーバー側の暗号化 (SSE) に KMS キーを使用しない場合、コントロールは失敗します。デフォルトでは、SNS はディスク暗号化を使用してメッセージとファイルを保存します。このコントロールに合

格するには、代わりに暗号化に KMS キーを使用する必要があります。これにより、セキュリティレイヤーが追加され、アクセスコントロールの柔軟性が向上します。

保管中のデータを暗号化すると、ディスクに保存されているデータが、 に対して認証されていないユーザーによってアクセスされるリスクが軽減されます AWS。データを読み取り前に復号化するには、API アクセス許可が必要です。セキュリティを強化するために、SNS トピックを KMS キーで暗号化することをお勧めします。

修正

SNS トピックの SSE を有効にするには、Amazon SNS トピックのサーバー側の暗号化 (SSE) を有効にする」を参照してください。 SSE を使用する前に、トピックの暗号化とメッセージの暗号化と復号を許可する AWS KMS key ポリシーも設定する必要があります。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の AWS KMS 「アクセス許可の設定」を参照してください。

[SNS.2] トピックに送信される通知メッセージでは、配信ステータスのログ記録を有効にする必要があります

> **Important**
>
> Security Hub は 2024 年 4 月にこのコントロールを廃止しました。詳細については、「Security Hub コントロールの変更ログ」を参照してください。

関連する要件: NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::SNS::Topic`

AWS Config ルール : `sns-topic-message-delivery-notification-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、エンドポイントの Amazon SNS トピックに送信される通知メッセージの配信ステータスで、ログ記録が有効になっているかどうかをチェックします。メッセージの配信ステータス通知が有効になっていない場合、このコントロールは失敗します。

ログ記録は、サービスの信頼性、可用性、パフォーマンスを維持するための重要な要素です。メッセージの配信ステータスをログ記録することで、以下のようなオペレーション上のインサイトを得ることができます。

- メッセージが Amazon SNS エンドポイントに配信されたかどうかを知ることができます。
- Amazon SNS エンドポイントから Amazon SNS に送信された応答を識別します。
- メッセージの滞留時間 (メッセージの発行から Amazon SNS エンドポイントに渡されるまでの時間) を決定する。

修正

トピックの配信ステータスロギングを設定する方法については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS メッセージ配信ステータス」を参照してください。

[SNS.3] SNS トピックにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::SNS::Topic`

AWS Config ルール: `tagged-sns-topic` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、Amazon SNS トピックにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。トピックにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、トピックにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

SNS トピックにタグを追加するには、Amazon SNS トピックタグの設定」を参照してください。

Amazon Simple Queue Service コントロール

これらのコントロールは Amazon SQS リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[SQS.1] Amazon SQS キューは保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ： 保護 > データ保護 > の暗号化 data-at-rest

重要度: 中

リソースタイプ: `AWS::SQS::Queue`

AWS Config ルール: `sqs-queue-encrypted` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon SQS キューが保管中に暗号化されるかどうかをチェックします。キューが SQS マネージドキー (SSE-SQS) または () キー AWS Key Management Service (SSE-KMS AWS KMS) で暗号化されていない場合、コントロールは失敗します。

保管中のデータを暗号化すると、認証されていないユーザーがディスクに保存されているデータにアクセスするリスクが低減されます。サーバー側の暗号化 (SSE) は、SQS 管理の暗号化キー (SSE-SQS) または AWS KMS キー (SSE-KMS) を使用して SQS キュー内のメッセージの内容を保護します。

修正

SQS キューの SSE を設定するには、「Amazon Simple Queue Service デベロッパーガイド」の「キューのサーバー側の暗号化 (SSE) の設定 (コンソール)」を参照してください。

[SQS.2] SQS キューにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::SQS::Queue`

AWS Config ルール: `tagged-sqs-queue` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、Amazon SQS キューにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。キューにタグキーがない場合、またはパラメータで指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、キューにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Amazon SQS コンソールを使用して既存のキューにタグを追加するには、「Amazon Simple Queue Service デベロッパーガイド」のAmazon SQS キューのコスト配分タグの設定 (コンソール) 」を参照してください。

AWS Step Functions コントロール

これらのコントロールは、Step Functions リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔StepFunctions.1] Step Functions ステートマシンではログ記録が有効になっている必要があります

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::StepFunctions::StateMachine`

AWS Config ルール : `step-functions-state-machine-logging-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`logLevel`	最小ログ記録レベル	列挙型	`ALL`, `ERROR`, `FATAL`	デフォルト値なし

このコントロールは、 AWS Step Functions ステートマシンでログ記録が有効になっているかどうかをチェックします。ステートマシンでログ記録が有効になっていない場合、コントロールは失敗します。`logLevel` パラメータにカスタム値を指定したときは、ステートマシンで指定されたログ記録レベルがオンになっている場合にのみコントロールが成功します。

モニタリングは、Step Functions の信頼性、可用性、パフォーマンスを維持するのに役立ちます。マルチポイント障害をより簡単にデバッグできるように、 AWS のサービス 使用する からモニタリングデータを収集する必要があります。Step Functions ステートマシンにログ記録設定を定義しておくと、Amazon CloudWatch Logs で実行履歴と結果を追跡できます。オプションで、エラーまたは致命的なイベントのみを追跡できます。

修正

Step Functions ステートマシンのログ記録を有効にするには、「AWS Step Functions デベロッパーガイド」の「ログ記録の設定」を参照してください。

〔StepFunctions.2] Step Functions アクティビティにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::StepFunctions::Activity`

AWS Config ルール : `tagged-stepfunctions-activity` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	デフォルト値なし

このコントロールは、 AWS Step Functions アクティビティにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。アクティビティにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredTagKeys`。パラメータが指定されていない場合、コントロール`requiredTagKeys`はタ

グキーの存在のみをチェックし、アクティビティがキーでタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「」の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Step Functions アクティビティにタグを追加するには、「 AWS Step Functions デベロッパーガイド」の「Step Functions でのタグ付け」を参照してください。

AWS Transfer Family コントロール

これらのコントロールは、Transfer Family リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ: `AWS::Transfer::Workflow`

AWS Config ルール: `tagged-transfer-workflow` (カスタム Security Hub ルール)

スケジュールタイプ: 変更がトリガーされた場合

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList	AWS 要件を満たすタグのリスト	`No default value`

このコントロールは、 AWS Transfer Family ワークフローにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。ワークフローにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredTagKeys。パラメータが指定されていない場合、コントロールrequiredTagKeysはタグキーの存在のみをチェックし、ワークフローにキーがタグ付けされていない場合は失敗します。自動的に適用され、 で始まるシステムタグaws:は無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。また、タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用すると、属性ベースのアクセスコントロール (ABAC) を認証戦略として実装できます。これは、タグに基づいてアクセス許可を定義します。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルには、単一の ABAC ポリシーまたは個別のポリシーセットを作成できます。これらの ABAC ポリシーを設計して、プリンシパルの タグがリソースタグと一致するときにオペレーションを許可できます。詳細については、IAM ユーザーガイドの「 の ABAC とは AWS」を参照してください。

> **Note**
>
> 個人を特定できる情報 (PII) やその他の機密情報や機密情報をタグに追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベ

ストプラクティスの詳細については、「」の「AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Transfer Family ワークフローにタグを追加するには (コンソール)

1. AWS Transfer Family コンソールを開きます。
2. ナビゲーションペインで、ワークフロー を選択します。次に、タグ付けするワークフローを選択します。
3. タグの管理 を選択し、タグを追加します。

[Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください

関連する要件： NIST.800-53.r5 CM-7、NIST.800-53.r5 IA-5、NIST.800-53.r5 SC-8

カテゴリ： 保護 > データ保護 > の暗号化 data-in-transit

重要度: 中

リソースタイプ: `AWS::Transfer::Server`

AWS Config ルール: `transfer-family-server-no-ftp`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、 AWS Transfer Family サーバーがエンドポイント接続に FTP 以外のプロトコルを使用しているかどうかをチェックします。サーバーがクライアントに FTP プロトコルを使用してサーバーのエンドポイントに接続すると、コントロールは失敗します。

FTP (File Transfer Protocol) は、暗号化されていないチャネルを介してエンドポイント接続を確立し、これらのチャネルを介して送信されるデータは傍受を受けやすくなります。SFTP (SSH File Transfer Protocol)、FTPS (File Transfer Protocol Secure)、または AS2 (適用性ステートメント 2) を使用すると、転送中のデータを暗号化することでセキュリティをさらに強化できます。また、潜在的

な攻撃者がネットワークトラフィックを盗聴または操作するために person-in-the-middle または同様の攻撃を使用することを防ぐのに役立ちます。

修正

Transfer Family サーバーのプロトコルを変更するには、「 ユーザーガイド」の「ファイル転送プロトコルの編集AWS Transfer Family 」を参照してください。

AWS WAF コントロール

これらのコントロールは AWS WAF リソースに関連しています。

これらのコントロールは、すべての で利用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります

関連する要件: NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::WAF::WebACL`

AWS Config ルール: `waf-classic-logging-enabled`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、 AWS WAF グローバルウェブ ACL でログ記録が有効になっているかどうかをチェックします。ウェブ ACL のログ記録が有効でない場合、このコントロールは失敗します。

ログ記録は、 の信頼性、可用性、パフォーマンスを AWS WAF グローバルに維持する上で重要な部分です。これは、多くの組織でビジネスおよびコンプライアンス要件であり、アプリケーションの動作をトラブルシューティングできます。また、 AWS WAFに添付済みのウェブ ACL によって分析されるトラフィックに関する詳細情報も提供します。

修正

AWS WAF ウェブ ACL のログ記録を有効にするには、「 AWS WAF デベロッパーガイド」の「ウェブ ACL トラフィック情報のログ記録」を参照してください。

[WAF.2] AWS WAF クラシックリージョンルールには少なくとも 1 つの条件が必要です

関連する要件: NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ: `AWS::WAFRegional::Rule`

AWS Config ルール : `waf-regional-rule-not-empty`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS WAF リージョンルールに少なくとも 1 つの条件があるかどうかをチェックします。ルールに条件が 1 つもない場合、このコントロールは失敗します。

WAF リージョンルールには、複数の条件を含めることが可能です。このルールの条件によってトラフィックの検査が許可され、定義されたアクション (許可、ブロック、カウント) が実行されます。条件が 1 つもないと、トラフィックは検査なしで通過します。条件がないにもかかわらず、許可、ブロック、カウントを示す名前またはタグが付いている WAF リージョンルールは、上記いずれかのアクションが行われているという誤解を生む可能性があります。

修正

空のルールに条件を追加する方法については、には、「AWS WAF デベロッパーガイド」の「ルールの条件の追加と削除」を参照してください。

[WAF.3] AWS WAF クラシックリージョンルールグループには、少なくとも 1 つのルールが必要です

関連する要件: NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ: `AWS::WAFRegional::RuleGroup`

AWS Config ルール : `waf-regional-rulegroup-not-empty`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS WAF リージョンルールグループに少なくとも 1 つのルールがあるかどうかを確認します。ルールグループにルールが 1 つもない場合、このコントロールは失敗します。

WAF リージョンルールグループには、複数のルールを含めることができます。このルールの条件によってトラフィックの検査が許可され、定義されたアクション (許可、ブロック、カウント) が実行されます。ルールが 1 つもないと、トラフィックは検査なしで通過します。ルールはないにもかかわらず、許可、ブロック、カウントを示す名前またはタグが付いている WAF リージョンルールグループは、上記いずれかのアクションが行われているという誤解を生む可能性があります。

修正

空のルールグループにルールとルール条件を追加するには、「 AWS WAF デベロッパーガイド」の AWS WAF 「 Classic ルールグループへのルールの追加と削除」および「ルール内の条件の追加と削除」を参照してください。

[WAF.4] AWS WAF クラシックリージョンウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ: `AWS::WAFRegional::WebACL`

AWS Config ルール : `waf-regional-webacl-not-empty`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS WAF Classic Regional ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれているかどうかをチェックします。ウェブ ACL に WAF ルールまたはルールグループが含まれていない場合、このコントロールは失敗します。

WAF リージョンウェブ ACL には、ウェブリクエストを検査および制御する、ルールおよびルールグループのコレクションを含めることができます。ウェブ ACL が空の場合、ウェブトラフィックは、デフォルトのアクションに応じて WAF による検出または処理なしに通過できます。

修正

空の AWS WAF Classic Regional Web ACL にルールまたはルールグループを追加するには、「AWS WAF デベロッパーガイド」の「Web ACL の編集」を参照してください。

[WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ: `AWS::WAF::Rule`

AWS Config ルール : `waf-global-rule-not-empty`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS WAF グローバルルールに条件が含まれているかどうかをチェックします。ルールに条件が 1 つもない場合、このコントロールは失敗します。

WAF グローバルルールには、複数の条件を含めることが可能です。ルールの条件によってトラフィックの検査が可能になり、定義されたアクション (許可、ブロック、カウント) を実行できます。条件が 1 つもないと、トラフィックは検査なしで通過します。条件はないにもかかわらず、許可、ブロック、カウントを示す名前またはタグが付いている WAF グローバルルールは、上記いずれかのアクションが行われているという誤解を生む可能性があります。

修正

ルールの作成方法および条件の追加方法については、「AWS WAF デベロッパーガイド」の「ルールの作成と条件の追加」を参照してください。

[WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ: `AWS::WAF::RuleGroup`

AWS Config ルール : `waf-global-rulegroup-not-empty`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS WAF グローバルルールグループに少なくとも 1 つのルールがあるかどうかを確認します。ルールグループにルールが 1 つもない場合、このコントロールは失敗します。

WAF グローバルルールグループには、複数のルールを含めることができます。このルールの条件によってトラフィックの検査が許可され、定義されたアクション (許可、ブロック、カウント) が実行されます。ルールが 1 つもないと、トラフィックは検査なしで通過します。ルールはないにもかかわらず、許可、ブロック、カウントを示す名前またはタグが付いている WAF グローバルルールグループは、上記いずれかのアクションが行われているという誤解を生む可能性があります。

修正

ルールグループにルールを追加する手順については、「 デベロッパーガイド」の AWS WAF 「 Classic ルールグループの作成」を参照してください。 AWS WAF

[WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

関連する要件: NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ: `AWS::WAF::WebACL`

AWS Config ルール : waf-global-webacl-not-empty

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS WAF グローバルウェブ ACL に少なくとも 1 つの WAF ルールまたは WAF ルールグループが含まれているかどうかをチェックします。ウェブ ACL に WAF ルールまたはルールグループが含まれていない場合、このコントロールは失敗します。

WAF グローバルウェブ ACL には、ウェブリクエストを検査および制御するルールおよびルールグループのコレクションを含めることができます。ウェブ ACL が空の場合、ウェブトラフィックは、デフォルトのアクションに応じて WAF による検出または処理なしに通過できます。

修正

空の AWS WAF グローバルウェブ ACL にルールまたはルールグループを追加するには、「 AWS WAF デベロッパーガイド」の「ウェブ ACL の編集」を参照してください。フィルター で、グローバル (CloudFront) を選択します。

[WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ: AWS::WAFv2::WebACL

AWS Config ルール : wafv2-webacl-not-empty

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS WAF V2 ウェブアクセスコントロールリスト (ウェブ ACL) に少なくとも 1 つのルールまたはルールグループが含まれているかどうかをチェックします。ウェブ ACL にルールまたはルールグループが含まれていない場合、このコントロールは失敗します。

ウェブ ACL を使用すると、保護されたリソースが応答するすべての HTTP(S) ウェブリクエストをきめ細かく制御できます。ウェブ ACL には、ウェブリクエストを検査および制御するルールおよ

びルールグループのコレクションを含める必要があります。ウェブ ACL が空の場合、ウェブトラフィックは、デフォルトのアクション AWS WAF に応じて、 によって検出または処理されることなく通過できます。

修正

ルールまたはルールグループを空の WAFV2 ウェブ ACL に追加するには、「AWS WAF デベロッパーガイド」の「ウェブ ACL の編集」を参照してください。

[WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります

関連する要件: NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 低

リソースタイプ: `AWS::WAFv2::WebACL`

AWS Config ルール： `wafv2-logging-enabled`

スケジュールタイプ: 定期的

パラメータ: なし

このコントロールは、 AWS WAF V2 ウェブアクセスコントロールリスト (ウェブ ACL) のログ記録が有効になっているかどうかをチェックします。ウェブ ACL のログ記録が無効の場合、このコントロールは失敗します。

ログ記録は、 の信頼性、可用性、パフォーマンスを維持します AWS WAF。また、多くの組織において、ログ記録はビジネスおよびコンプライアンス要件となっています。ウェブ ACL で分析されたトラフィックをログに記録することで、アプリケーションの挙動のトラブルシューティングができます。

修正

AWS WAF ウェブ ACL のログ記録を有効にするには、「 AWS WAF デベロッパーガイド」の「ウェブ ACL のログ記録の管理」を参照してください。

[WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります

関連する要件: NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::WAFv2::RuleGroup`

AWS Config ルール： `wafv2-rulegroup-logging-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS WAF ルールまたはルールグループで Amazon CloudWatch メトリクスが有効になっているかどうかをチェックします。ルールまたはルールグループで CloudWatch メトリクスが有効になっていない場合、コントロールは失敗します。

AWS WAF ルールとルールグループで CloudWatch メトリクスを設定すると、トラフィックフローを可視化できます。どの ACL ルールがトリガーされ、どのリクエストが受け入れられブロックされたかを確認できます。この可視性は、関連リソースでの悪意のあるアクティビティを特定するのに役立ちます。

修正

AWS WAF ルールグループで CloudWatch メトリクスを有効にするには、 UpdateRuleGroup API を呼び出します。 AWS WAF ルールで CloudWatch メトリクスを有効にするには、ACL API UpdateWebを呼び出します。`CloudWatchMetricsEnabled` フィールドは `true` に設定されます。AWS WAF コンソールを使用してルールまたはルールグループを作成すると、 CloudWatch メトリクスは自動的に有効になります。

セキュリティコントロールの表示と管理

コントロールは、組織が情報の機密性、完全性、可用性を保護する際に役立つセキュリティ標準内の保護手段です。Security Hub では、コントロールは特定の AWS リソースに関連しています。

統合コントロールビュー

Security Hub コンソールの「コントロール」ページには、現在の で使用可能なすべてのコントロールが表示されます AWS リージョン（ セキュリティ標準「」ページにアクセスして、有効な標準を選択することで、標準のコンテキストでコントロールを表示できます ）。セキュリティハブは、どの標準でも一貫したセキュリティコントロール ID、タイトル、説明をコントロールに割り当てます。コントロール IDsには、関連する番号 AWS のサービス と一意の番号 (.3 など) CodeBuildが含まれます。

次の情報は、Security Hub コンソールの [コントロール] ページにあります。

- データを含む有効なコントロールの総数に対する合格したコントロールの割合に基づく、総合的なセキュリティスコア
- 有効になっているすべてのコントロールにおけるセキュリティチェックの不合格の割合
- さまざまな重大度のコントロールに対するセキュリティチェックの合格と不合格の数
- コントロールのリストは、有効化のステータスに基づき、いくつかのタブに分かれています。有効になっている標準のいずれにも適用されない使用可能なコントロールは、[無効] 列に表示されます。現在のリージョンでは利用できないコントロールなど、未処理のコントロールは [データなし] 列に表示されます。[すべて] 列のコントロールの数は、[失敗]、[不明]、[合格]、[無効]、[データなし] の各列におけるコントロールの合計と等しくなります。

[コントロール] ページでコントロールを選択して詳細を確認し、コントロールが生成した検出結果に対してアクションを実行することができます。このページでは、現在の AWS アカウント と でセキュリティコントロールを有効または無効にすることもできます AWS リージョン。[コントロール] ページからの有効化および無効化アクションは、すべての標準に適用されます。詳細については、「すべての標準におけるコントロールの有効化と無効化」を参照してください。

管理者アカウントの場合、[コントロール] ページには、メンバーアカウント全体のコントロールのステータスが反映されます。少なくとも 1 つのメンバーアカウントでコントロールチェックが失敗した場合、[コントロール] ページの [失敗] タブにコントロールが表示されます。集約リージョンを設定している場合、[コントロール] ページには、リンクされているすべてのリージョンのコントロールステータスが反映されます。リンクされた少なくとも 1 つのリージョンでコントロールチェックが失敗した場合、そのコントロールは [コントロール] ページの [失敗] タブに表示されます。

統合コントロールビューでは、ワークフローに影響を与える可能性のある AWS Security Finding 形式 (ASFF) のコントロール検出結果フィールドが変更されます。詳細については、「統合コントロールビュー — ASFF の変更」を参照してください。

コントロールの総合セキュリティスコア

[コントロール] ページには、全体的なセキュリティスコアが 0～100% で表示されます。総合的なセキュリティスコアは、データを含む有効なコントロールの総数に対する合格したコントロールの割合に基づき計算されます。

> **Note**
>
> コントロールの全体的なセキュリティスコアを表示するには、Security Hub へのアクセスに使用する IAM ロールに **`BatchGetControlEvaluations`** の呼び出し権限を追加する必要があります。この権限は、特定の標準のセキュリティスコアを表示する場合には必要ありません。

Security Hub を有効にすると、Security Hub は、Security Hub コンソールの [概要] ページまたは [セキュリティ基準] ページへの最初のアクセスから 30 分以内に最初のセキュリティスコアを計算します。中国リージョンおよび AWS GovCloud (US) Regionでは、最初のセキュリティスコアが作成されるまで、最大 24 時間かかる場合があります。スコアは、これらのページにアクセスしたときに有効になっている標準に対してのみ生成されます。現在有効になっている標準のリストを表示するには、`GetEnabledStandards` API オペレーションを使用します。また、スコアを表示するには、AWS Config リソースレコードを設定する必要があります。全体的なセキュリティスコアは、標準のセキュリティスコアの平均値です。

最初のスコア生成の後、Security Hub はセキュリティスコアを 24 時間ごとに更新します。Security Hub には、セキュリティスコアが最後に更新されたときの時刻が表示されます。

集約リージョンを設定している場合、全体のセキュリティスコアには、リンクされたリージョン全体の検出結果が反映されます。

トピック

- コントロールのカテゴリ
- すべての標準におけるコントロールの有効化と無効化
- 有効な標準で新しいコントロールを自動的に有効化する
- カスタムコントロールパラメータ
- 無効にする可能性のある Security Hub コントロール
- コントロールの詳細の表示

- コントロールリストのフィルタリングとソート
- 統制結果の表示とアクションの実行

コントロールのカテゴリ

各コントロールにはカテゴリが割り当てられます。コントロールのカテゴリは、コントロールが適用されるセキュリティ機能を反映します。

カテゴリ値には、カテゴリ、カテゴリ内のサブカテゴリ、およびオプションでサブカテゴリ内の分類子が含まれます。例:

- 識別 > インベントリ
- 保護 > データ保護 > 転送中のデータの暗号化

ここでは、使用可能なカテゴリ、サブカテゴリ、および分類子の説明を示します。

識別

システム、アセット、データ、機能に対するサイバーセキュリティのリスクを管理するための組織の理解を深めます。

インベントリ

サービスは正しいリソースタグ付け戦略を実装していますか? タグ付け戦略にはリソース所有者が含まれていますか?

どのようなリソースをサービスで使用していますか? これらは、このサービスの承認されたリソースですか?

承認されたインベントリを可視化していますか? 例えば、Amazon EC2 Systems Manager やサービスカタログなどのサービスを使用しますか?

ログ記録

サービスに関連するすべてのログ記録を安全に有効化していますか? ログファイルの例は次のとおりです。

- Amazon VPC フローログ
- Elastic Load Balancing のアクセスログ

- Amazon CloudFront ログ
- Amazon CloudWatch Logs
- Amazon Relational Database Service のログ記録
- Amazon OpenSearch Service スローインデックスログ
- X-Ray トレース
- AWS Directory Service ログ
- AWS Config 項目
- スナップショット

保護

重要なインフラストラクチャサービスを確実に提供し、安全なコーディング手法を確保するための適切な保護策を開発および実施します。

安全なアクセス管理

サービスは、IAM ポリシーまたはリソースポリシーで最小特権プラクティスを使用していますか?

パスワードとシークレットは十分に複雑なものですか? 適切にローテーションしていますか?

サービスで多要素認証 (MFA) を使用しますか?

このサービスはルートユーザーを回避しますか?

リソースベースのポリシーはパブリックアクセスを許可しますか?

セキュアなネットワーク設定

サービスは、パブリックおよび安全でないリモートネットワークアクセスを回避しますか?

サービスは VPC を適切に使用しますか? 例えば、ジョブは VPC で実行する必要がありますか?

サービスは、機密性の高いリソースを適切にセグメント化および分離しますか?

データ保護

保管中のデータの暗号化 - サービスは保管中のデータを暗号化しますか?

転送中のデータの暗号化 - サービスで転送中のデータを暗号化していますか?

データの整合性 - サービスでデータの整合性を検証していますか?

データの削除保護 - サービスはデータの誤削除を防止しますか?

データの管理/使用状況 - 機密データの場所を証跡するために Amazon Macie などのサービスを使用していますか?

API の保護

サービスは、サービス API オペレーション AWS PrivateLink を保護するために を使用していますか ?

保護サービス

適切な保護サービスが提供されていますか? 保護サービスは正しい範囲をカバーしていますか?

保護サービスは、サービスに対する攻撃や侵害を回避するのに役立ちます。の保護サービスの例としては AWS AWS Control Tower、、 AWS WAF AWS Shield Advanced、Vanta、Secrets Manager、IAM Access Analyzer、 などがあります AWS Resource Access Manager。

安全な開発

安全なコーディングプラクティスを使用していますか?

Open Web Application Security Project (OWASP) Top 10 などの脆弱性を回避していますか?

検出

サイバーセキュリティイベントの発生を特定するための適切なアクティビティを開発および実施します。

検出サービス

正しい検出サービスは提供されていますか?

保護サービスは正しい範囲をカバーしていますか?

AWS 検出サービスの例としては、Amazon GuardDuty、 AWS Security Hub、Amazon Inspector 、Amazon Detective、Amazon CloudWatch アラーム AWS IoT Device Defender、 などがあります AWS Trusted Advisor。

応答

検出されたサイバーセキュリティイベントに関するアクションを実行するための適切なアクティビティを開発および実施します。

レスポンスアクション

- セキュリティイベントに迅速に対応していますか?
- 重要または重要度が高い結果が実際にありますか?

フォレンジック

- サービスのフォレンジックデータを安全に取得できますか? 例えば、True ポジティブの結果に関連する Amazon EBS スナップショットを取得していますか?
- フォレンジックアカウントを設定していますか?

復旧

耐障害性に関する計画を保持し、サイバーセキュリティイベントで損なわれた機能やサービスを復元するための適切なアクティビティを開発および実施します。

耐障害性

- サービスの設定は、スムーズなフェイルオーバー、伸縮自在なスケーリング、高可用性をサポートしていますか?
- バックアップを確立していますか?

すべての標準におけるコントロールの有効化と無効化

AWS Security Hub は、有効なコントロールの検出結果を生成し、セキュリティスコアを計算するときに有効なすべてのコントロールを考慮します。すべてのセキュリティ標準でコントロールを有効または無効にしたり、有効化ステータスを標準ごとに異なる方法で設定したりできます。有効なすべての標準でコントロールの有効化ステータスを一致させる前者のオプションを使用することをお勧めします。このセクションでは、標準全体でコントロールを有効および無効にする方法について説明します。1 つまたは複数の特定の標準でコントロールを有効または無効にするには、「特定の標準コントロールの有効化と無効化」を参照してください。

集約リージョンを設定すると、Security Hub コンソールには、リンクされたすべてのリージョンのコントロールが表示されます。リンクされたリージョンでコントロールを使用できるが、集約リージョンでは使用できない場合は、集約リージョンからそのコントロールを有効または無効にすることはできません。

> **Note**
>
> コントロールを有効または無効にする手順は、中央設定を使用するかどうかによって異なります。このセクションでは、その違いについて説明します。Security Hub と を統合するユーザーは、中央設定を使用できます AWS Organizations。マルチアカウント、マルチリージョン環境でコントロールを有効または無効にするプロセスを簡略化するために、中央設定を使用することをお勧めします。

コントロールの有効化

標準でコントロールを有効にすると、Security Hub はそのコントロールのセキュリティチェックを開始し、コントロールの検出結果を生成します。

Security Hub では、全体のセキュリティスコアと標準セキュリティスコアの計算にコントロールステータスを含みます。[統合されたコントロールの検出結果] を有効にすると、コントロールを複数の標準で有効にしている場合でも、セキュリティチェックの検出結果を 1 つ受け取ります。詳細については、統合コントロールの検出結果を参照してください。

複数のアカウントおよびリージョンのすべての標準でコントロールを有効にする

複数のアカウントおよび でセキュリティコントロールを有効にするには AWS リージョン、中央設定 を使用する必要があります。

中央設定を使用する場合、委任管理者は、有効な標準全体で指定されたコントロールを有効にする Security Hub 設定ポリシーを作成できます。そして、設定ポリシーを特定のアカウントや組織単位 (OU)、またはルートに関連付けることができます。設定ポリシーは、ホームリージョン (集約リージョンとも呼ばれる) およびリンクされているすべてのリージョンで有効になります。

設定ポリシーではカスタマイズが可能です。例えば、ある OU ではすべてのコントロールを有効にし、別の OU では Amazon Elastic Compute Cloud (EC2) コントロールのみを有効にすることができます。詳細度のレベルは、組織のセキュリティカバレッジについて目指す目標によって異なります。標準全体で指定されたコントロールを有効にする設定ポリシーの作成手順については、「Security Hub 設定ポリシーの作成と関連付け」を参照してください。

> **Note**
>
> 委任管理者は、サービスマネージドスタンダード: AWS Control Towerを除くすべての標準でコントロールを管理するための設定ポリシーを作成できます。この標準のコントロールは、AWS Control Tower サービスで設定する必要があります。

委任管理者ではなく一部のアカウントに独自のコントロールを設定させたい場合は、委任管理者がそれらのアカウントをセルフマネージドとして指定できます。セルフマネージドアカウントは、リージョンごとにコントロールを個別に設定する必要があります。

1 つのアカウントおよびリージョンのすべての標準でコントロールを有効にする

中央設定を使用していない場合、またはセルフマネージドアカウントの場合、設定ポリシーを使用して複数のアカウントおよびリージョンでコントロールを一元的に有効にすることはできません。ただし、次の手順を使用して、1 つのアカウントおよびリージョンでコントロールを有効にすることができます。

Security Hub console

1 つのアカウントおよびリージョンの標準全体でコントロールを有効にするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. ナビゲーションペインで [コントロール] を選択します。
3. [無効] タブを選択します。
4. コントロールの横にあるオプションを選択します。
5. [コントロールの有効化] を選択します (このオプションは、既に有効になっているコントロールには表示されません)。
6. コントロールを有効にするリージョンごとに、これらの手順を繰り返します。

Security Hub API

1 つのアカウントおよびリージョンの標準全体でコントロールを有効にするには

1. ListStandardsControlAssociations API を呼び出します。セキュリティコントロール ID を指定します。

   リクエストの例:

```
{
    "SecurityControlId": "IAM.1"
}
```

2. BatchUpdateStandardsControlAssociations API を呼び出します。コントロールが有効になっていない標準の Amazon リソースネーム (ARN) を指定します。標準 ARN を取得するには、DescribeStandards を実行します。
3. AssociationStatus パラメータを ENABLED と等しい値に設定します。既に有効化されているコントロールに対してこれらの手順を実行すると、API は HTTP ステータスコード 200 の応答を返します。

   リクエストの例:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]
}
```

4. コントロールを有効にするリージョンごとに、これらの手順を繰り返します。

AWS CLI

1 つのアカウントおよびリージョンの標準全体でコントロールを有効にするには

1. list-standards-control-associations コマンドを実行します。セキュリティコントロール ID を指定します。

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. batch-update-standards-control-associations コマンドを実行します。コントロールが有効になっていない標準の Amazon リソースネーム (ARN) を指定します。標準 ARN を取得するには、describe-standards コマンドを実行します。
3. AssociationStatus パラメータを ENABLED と等しい値に設定します。既に有効化されているコントロールに対してこれらの手順を実行すると、コマンドは HTTP ステータスコード 200 の応答を返します。

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0", "AssociationStatus": "ENABLED"}]'
```

4. コントロールを有効にするリージョンごとに、これらの手順を繰り返します。

有効な標準で新しいコントロールを自動的に有効化する

Security Hub は定期的に新しいセキュリティコントロールをリリースし、1 つ以上の標準に追加しています。有効化した標準で新しいコントロールを自動的に有効化するかどうかは、ユーザーが選択できます。

> **Note**
>
> 新しいコントロールを自動的に有効にするには、中央設定を使用することをお勧めします。設定ポリシーに無効にするコントロールのリストが含まれている場合 (プログラム上、これは `DisabledSecurityControlIdentifiers` パラメータを反映しています)、Security Hub は、他のすべてのコントロール (新しくリリースされたコントロールを含む) を標準全体で自動的に有効にします。ポリシーに有効にするコントロールのリストが含まれている場合 (これは `EnabledSecurityControlIdentifiers` パラメータを反映しています)、Security Hub は、他のすべてのコントロール (新しくリリースされたコントロールを含む) を標準全体で自動的に無効にします。詳細については、「Security Hub 設定ポリシーの仕組み」を参照してください。

お好みのアクセス方法を選択し、次の手順に従って、有効な標準の新しいコントロールを自動的に有効化します。以下の手順は、中央設定を使用しない場合にのみ適用されます。

Security Hub console

新しいコントロールを自動的に有効化するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. ナビゲーションペインで、[Settings] (設定)、[General] (一般) タブの順に選択します。

3. [コントロール] で [編集] を選択します。
4. [有効になっている標準で新しいコントロールを自動的に有効にする] をオンにします。
5. [保存] を選択します。

Security Hub API

新しいコントロールを自動的に有効化するには

1. UpdateSecurityHubConfiguration API を呼び出します。
2. 有効な標準で新しいコントロールを自動的に有効にするには、`AutoEnableControls` を `true` に設定します。新しいコントロールを自動的に有効化しない場合は、`AutoEnableControls` を false に設定します。

AWS CLI

新しいコントロールを自動的に有効化するには

1. update-security-hub-configuration コマンドを実行します。
2. 有効な標準で新しいコントロールを自動的に有効にするには、`--auto-enable-controls` を指定します。新しいコントロールを自動的に有効化しない場合は、`--no-auto-enable-controls` を指定します。

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

コマンドの例

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

コントロールを無効化する

すべての標準でコントロールを無効化すると、次のようになります。

- コントロールのセキュリティチェックは実行されなくなります。
- そのコントロールに対して追加の結果が生成されません。

- 既存の検出結果は 3～5 日後に自動的にアーカイブされます (これはベストエフォートである点に注意してください)。
- Security Hub が作成した関連 AWS Config ルールはすべて削除されます。

すべての標準でコントロールを無効にするのではなく、1 つ以上の特定の標準でコントロールを無効にするだけで済みます。これを行うと、Security Hub は、無効にした標準のコントロールのセキュリティチェックを実行しなくなるため、それらの標準のセキュリティスコアには影響しません。ただし、Security Hub は AWS Config ルールを保持し、他の標準で有効になっている場合は、コントロールのセキュリティチェックを続行します。これは概要セキュリティスコアに影響する可能性があります。特定の標準でコントロールを設定する手順については、「特定の標準コントロールの有効化と無効化」を参照してください。

検出結果のノイズを減らすには、環境に関係のないコントロールを無効にするとよいでしょう。無効にするコントロールに関する推奨事項については、「無効にする可能性のある Security Hub コントロール」を参照してください。

標準を無効にすると、その標準に適用されるすべてのコントロールが無効になります (ただし、それらのコントロールは他の標準では有効のままです)。標準の無効化の詳細については、「the section called “標準の有効化および無効化”」を参照してください。

標準を無効にすると、Security Hub はどの該当するコントロールが無効になったかを追跡しません。その後、同じ標準を再度有効にすると、その標準に適用されるすべてのコントロールが自動的に有効になります。さらに、コントロールを無効にすることは永続的なアクションではありません。コントロールを無効にしてから、以前に無効になっていた標準を有効にしたとします。標準にそのコントロールが含まれている場合、コントロールはその標準で有効になります。Security Hub で標準を有効にすると、その標準に適用されるすべてのコントロールが自動的に有効になります。特定のコントロールを無効にすることを選択できます。

複数のアカウントおよびリージョンのすべての標準でコントロールを無効にする

複数のアカウントおよび でセキュリティコントロールを無効にするには AWS リージョン、中央設定 を使用する必要があります。

中央設定を使用する場合、委任管理者は、有効な標準全体で指定されたコントロールを無効にする Security Hub 設定ポリシーを作成できます。そして、設定ポリシーを特定のアカウント、OU、またはルートに関連付けることができます。設定ポリシーは、ホームリージョン (集約リージョンとも呼ばれる) およびリンクされているすべてのリージョンで有効になります。

設定ポリシーではカスタマイズが可能です。例えば、1 つの OU のすべての AWS CloudTrail コントロールを無効にすることや、別の OU のすべての IAM コントロールを無効にすることを選択できます。詳細度のレベルは、組織のセキュリティカバレッジについて目指す目標によって異なります。標準全体で指定されたコントロールを無効にする設定ポリシーの作成手順については、「Security Hub 設定ポリシーの作成と関連付け」を参照してください。

> **Note**
>
> 委任管理者は、サービスマネージドスタンダード: AWS Control Towerを除くすべての標準でコントロールを管理するための設定ポリシーを作成できます。この標準のコントロールは、AWS Control Tower サービスで設定する必要があります。

委任管理者ではなく一部のアカウントに独自のコントロールを設定させたい場合は、委任管理者がそれらのアカウントをセルフマネージドとして指定できます。セルフマネージドアカウントは、リージョンごとにコントロールを個別に設定する必要があります。

1 つのアカウントおよびリージョンのすべての標準でコントロールを無効にする

中央設定を使用していない場合、またはセルフマネージドアカウントの場合、設定ポリシーを使用して複数のアカウントおよびリージョンでコントロールを一元的に無効にすることはできません。ただし、次の手順を使用して、1 つのアカウントおよびリージョンでコントロールを無効にすることができます。

Security Hub console

1 つのアカウントおよびリージョンの標準全体でコントロールを無効にするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. ナビゲーションペインで [コントロール] を選択します。
3. コントロールの横にあるオプションを選択します。
4. [コントロールの無効化] を選択します (このオプションは、既に無効になっているコントロールには表示されません)。
5. コントロールを無効にする理由を選択し、[無効化] を選択して確定します。
6. コントロールを無効にするリージョンごとに、これらの手順を繰り返します。

Security Hub API

1 つのアカウントおよびリージョンの標準全体でコントロールを無効にするには

1. ListStandardsControlAssociations API を呼び出します。セキュリティコントロール ID を指定します。

   リクエストの例:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. BatchUpdateStandardsControlAssociations API を呼び出します。コントロールが有効になっている標準の ARN を指定します。標準 ARN を取得するには、DescribeStandards を実行します。
3. AssociationStatus パラメータを DISABLED と等しい値に設定します。既に無効化されているコントロールに対してこれらの手順を実行すると、API は HTTP ステータスコード 200 の応答を返します。

   リクエストの例:

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-
   benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not
    applicable to environment"}, {"SecurityControlId": "IAM.1", "StandardsArn":
    "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/
   v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
    environment"}}]
   }
   ```

4. コントロールを無効にするリージョンごとに、これらの手順を繰り返します。

AWS CLI

1 つのアカウントおよびリージョンの標準全体でコントロールを無効にするには

1. list-standards-control-associations コマンドを実行します。セキュリティコントロール ID を指定します。

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. batch-update-standards-control-associations コマンドを実行します。コントロールが有効になっている標準の ARN を指定します。標準 ARN を取得するには、describe-standards コマンドを実行します。
3. AssociationStatus パラメータを DISABLED と等しい値に設定します。既に無効化されているコントロールに対してこれらの手順を実行すると、コマンドは HTTP ステータスコード 200 の応答を返します。

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable
 to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":
 "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/v/1.4.0",
 "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}]'
```

4. コントロールを無効にするリージョンごとに、これらの手順を繰り返します。

有効な標準で新しいコントロールを自動的に有効化する

AWS Security Hub は定期的に新しいコントロールをリリースし、1 つ以上の標準に追加します。有効化した標準で新しいコントロールを自動的に有効化するかどうかは、ユーザーが選択できます。

> **Note**
>
> 中央設定を使用していて、無効にする特定のコントロールのリストを設定ポリシーに含めている場合 (プログラム上、これは DisabledSecurityControlIdentifiers パラメータを反映しています)、Security Hub は、他のすべてのコントロール (新しくリリースされたコントロールを含む) を標準全体で自動的に有効にします。詳細については、「Security Hub 設定ポリシーの仕組み」を参照してください。

新しいセキュリティコントロールを自動的に有効にするには、Security Hub の中央設定を使用することをお勧めします。標準全体で無効にするコントロールのリストが含まれた設定ポリシーを作成でき

ます。新しくリリースされたものも含め、他のすべてのコントロールはデフォルトで有効になっています。また、標準全体で有効にするコントロールのリストが含まれたポリシーを作成することもできます。新しくリリースされたものも含め、他のすべてのコントロールはデフォルトで無効になっています。詳細については、「中央設定の仕組み」を参照してください。

Security Hub では、有効化されていない標準に新しいコントロールが追加された場合、そのコントロールを有効化しません。

以下の手順は、中央設定を使用しない場合にのみ適用されます。

お好みのアクセス方法を選択し、次の手順に従って、有効な標準の新しいコントロールを自動的に有効化します。

Security Hub console

新しいコントロールを自動的に有効化するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. ナビゲーションペインで、[Settings] (設定)、[General] (一般) タブの順に選択します。
3. [コントロール] で [編集] を選択します。
4. [有効になっている標準で新しいコントロールを自動的に有効にする] をオンにします。
5. [保存] を選択します。

Security Hub API

新しいコントロールを自動的に有効化するには

1. `UpdateSecurityHubConfiguration` を実行します。
2. 有効な標準で新しいコントロールを自動的に有効にするには、`AutoEnableControls` を `true` に設定します。新しいコントロールを自動的に有効化しない場合は、`AutoEnableControls` を false に設定します。

AWS CLI

新しいコントロールを自動的に有効化するには

1. `update-security-hub-configuration` コマンドを実行します。

2. 有効な標準で新しいコントロールを自動的に有効にするには、--auto-enable-controls を指定します。新しいコントロールを自動的に有効化しない場合は、--no-auto-enable-controls を指定します。

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

コマンドの例

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

新しいコントロールを自動的に有効化しない場合は、手動で有効化する必要があります。手順については、「the section called “すべての標準におけるコントロールの有効化と無効化”」を参照してください。

カスタムコントロールパラメータ

Security Hub コントロールの中には、コントロールの評価方法に影響するパラメータを使用するものがあります。通常、このようなコントロールは、Security Hub が定義するデフォルトのパラメータ値と照らし合わせて評価されます。ただし、これらのコントロールのサブセットについては、パラメータ値をカスタマイズすることができます。コントロールのパラメータ値をカスタマイズした場合、Security Hub は、指定された値に対するコントロールの評価を開始します。コントロールの基になるリソースがカスタム値を満たした場合、Security Hub は PASSED 検出結果を生成します。リソースがカスタム値を満たさなかった場合、Security Hub は FAILED 検出結果を生成します。

コントロールパラメータをカスタマイズすることで、ビジネス要件やセキュリティの期待と一致するように、Security Hub によって推奨および監視されるセキュリティベストプラクティスを改良できます。コントロールの検出結果を抑制する代わりに、1 つ以上のパラメータをカスタマイズして、セキュリティニーズに合った検出結果を取得することができます。

カスタムコントロールパラメータのサンプルユースケースを以下に示します。

- 〔CloudWatch.16] – CloudWatch ロググループは、指定された期間保持する必要があります

  保持期間を指定できます。
- [IAM.7] – IAM ユーザーのパスワードポリシーには強力な設定が必要です

  パスワード強度に関するパラメータを指定できます。

- [EC2.18] – セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可する必要があります

  無制限の着信トラフィックを許可するように承認するポートを指定できます。
- [Lambda.5] – VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります

  成功の検出結果を生成するアベイラビリティーゾーンの最小数を指定できます。

このセクションでは、コントロールパラメータをカスタマイズして管理する方法について説明します。

カスタムコントロールパラメータの仕組み

コントロールは、1 つまたは複数のカスタマイズ可能なパラメータを持つことができます。それぞれのコントロールパラメータで使用可能なデータ型には以下が含まれます。

- ブール値
- ダブル
- 列挙型
- EnumList
- 整数
- IntegerList
- 文字列
- StringList

一部のコントロールは、許容パラメータ値も指定された範囲に収まらないと有効になりません。このような場合は、Security Hub が許容範囲を提供します。

Security Hub はデフォルトのパラメータ値を選択し、場合によっては更新することもあります。コントロールパラメータをカスタマイズしても、その値は、変更しない限りパラメータに指定した値のままです。つまり、パラメータのカスタム値が Security Hub で定義されている現在のデフォルト値と一致する場合でも、パラメータはデフォルトの Security Hub 値の更新の追跡を停止します。コントロール「[ACM.1] – インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります」の例を以下に示します。

```
{
```

```
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 30
            }
        }
    }
}
```

前の例では、daysToExpiration パラメータのカスタム値は 30 です。このパラメータの現在のデフォルト値も 30 です。Security Hub がデフォルト値を 14 に変更しても、この例のパラメータはその変更を追跡しません。30 の値は保持されます。

パラメータのデフォルトの Security Hub 値の更新を追跡する場合は、ValueType フィールドを CUSTOM ではなく DEFAULT に設定します。詳細については、「1 つのアカウントおよびリージョンでデフォルトのパラメータ値に戻す」を参照してください。

パラメータ値を変更する場合は、新しい値に基づいてコントロールを評価する新しいセキュリティチェックもトリガーします。そして、Security Hub が新しい値に基づいて新しいコントロール検出結果を生成します。コントロール検出結果の定期更新時には、Security Hub は新しいパラメータ値も使用します。コントロールのパラメータ値を変更しても、そのコントロールを含む標準を有効にしていない場合、Security Hub は新しい値を使用したセキュリティチェックを行いません。新しいパラメータ値に基づいてコントロールを評価するには、Security Hub の関連標準を少なくとも 1 つ有効にする必要があります。

カスタムパラメータ値は、有効になっている標準全体に適用されます。現在のリージョンでサポートされていないコントロールのパラメータはカスタマイズできません。個々のコントロールに関するリージョンの制限のリストについては、「コントロールの地域制限」を参照してください。

コントロールパラメータのカスタマイズ

コントロールパラメータをカスタマイズする手順は、中央設定を使用するかどうかによって異なります。中央設定は、委任された Security Hub 管理者が組織内の AWS リージョン、アカウント、組織単位 (OUs) 全体で Security Hub 機能を管理するために使用できる機能です。

組織が中央設定を使用している場合、委任管理者は、カスタムコントロールパラメータを含む設定ポリシーを作成できます。これらのポリシーは、一元管理されるメンバーアカウントや OU に関連付けることができ、自分のホームリージョンおよびリンクされているすべてのリージョンで有効にな

ります。委任管理者は 1 つ以上のアカウントをセルフマネージドとして指定することもできます。これにより、アカウント所有者は各リージョンで独自のパラメータを個別に設定できるようになります。組織で中央設定を使用していない場合は、アカウントおよびリージョンごとにコントロールパラメータを個別にカスタマイズする必要があります。

複数のアカウントおよびリージョンのコントロールパラメータをカスタマイズする

中央設定を使用すると、複数のアカウントおよびリージョンで一元管理されるアカウントや OU のコントロールパラメータをカスタマイズできます。組織のさまざまな部分でコントロールパラメータ値を整合させることができるため、中央設定を使用することをお勧めします。例えば、すべてのテストアカウントが特定のパラメータ値を使用し、すべての本番稼働用アカウントが異なる値を使用する場合があります。

中央設定を使用する組織の委任 Security Hub 管理者の場合は、希望する方法を選択し、手順に従って複数のアカウントおよびリージョンのコントロールパラメータをカスタマイズします。

Security Hub console

複数のアカウントおよびリージョンのコントロールパラメータをカスタマイズするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   ホームリージョンにサインインしていることを確認します。
2. ナビゲーションペインで、[設定]、[設定] の順に選択します。
3. [Policies] タブを選択します。
4. カスタムパラメータを含む新しい設定ポリシーを作成するには、[ポリシーの作成] を選択します。既存の設定ポリシーでカスタムパラメータを指定するには、ポリシーを選択し、[編集] を選択します。

   カスタムパラメータを使用して新しい設定ポリシーを作成するには

   1. [カスタムポリシー] セクションで、有効にするセキュリティ標準およびコントロールを選択します。
   2. [コントロールパラメータをカスタマイズする] を選択します。
   3. コントロールを選択し、1 つ以上のパラメータにカスタム値を指定します。
   4. その他のコントロールのパラメータをカスタマイズするには、[その他のコントロールをカスタマイズする] を選択します。
   5. [アカウント] セクションで、ポリシーを適用するアカウントまたは OU を選択します。

6. [次へ] をクリックします。
7. [ポリシーを作成して適用] を選択します。ホームリージョンおよびリンクされているすべてのリージョンで、このアクションにより、この設定ポリシーに関連付けられているアカウントおよび OU の既存の構成設定がオーバーライドされます。アカウントと OU は、直接適用するか親から継承することによって、設定ポリシーに関連付けることができます。

既存の設定ポリシーでカスタムパラメータを追加または編集するには

1. [コントロール] セクションの [カスタムポリシー] で、必要な新しいカスタムパラメータ値を指定します。
2. このポリシーでコントロールパラメータをカスタマイズするのが初めての場合は、[コントロールパラメータをカスタマイズする] を選択し、カスタマイズするコントロールを選択します。その他のコントロールのパラメータをカスタマイズするには、[その他のコントロールをカスタマイズする] を選択します。
3. [アカウント] セクションで、ポリシーを適用するアカウントまたは OU を確認します。
4. [次へ] をクリックします。
5. 変更内容を見直し、それらが正しいことを確認します。完了したら、[ポリシーを保存して適用] を選択します。ホームリージョンおよびリンクされているすべてのリージョンで、このアクションにより、この設定ポリシーに関連付けられているアカウントおよび OU の既存の構成設定がオーバーライドされます。アカウントと OU は、直接適用するか親から継承することによって、設定ポリシーに関連付けることができます。

Security Hub API

複数のアカウントおよびリージョンのコントロールパラメータをカスタマイズするには

カスタムパラメータを使用して新しい設定ポリシーを作成するには

1. ホームリージョンの委任管理者アカウントから CreateConfigurationPolicy API を呼び出します。
2. `SecurityControlCustomParameters` オブジェクトには、カスタマイズする各コントロールの識別子を指定します。
3. `Parameters` オブジェクトには、カスタマイズする各パラメータの名前を指定します。カスタマイズする各パラメータで、`ValueType` に `CUSTOM` を指定します。`Value` には、パラメータのデータ型とカスタム値を指定します。`ValueType` が `CUSTOM` の場合、`Value` フィールドを空にすることはできません。コントロールがサポートす

るパラメータをリクエストで省略した場合、そのパラメータは現在の値を保持します。GetSecurityControlDefinition API を呼び出すことで、コントロールでサポートされているパラメータ、データ型、有効な値を確認できます。

既存の設定ポリシーでカスタムパラメータを追加または編集するには

1. ホームリージョンの委任管理者アカウントから UpdateConfigurationPolicy API を呼び出します。
2. `Identifier` フィールドには、更新する設定ポリシーの Amazon リソースネーム (ARN) または ID を指定します。
3. `SecurityControlCustomParameters` オブジェクトには、カスタマイズする各コントロールの識別子を指定します。
4. `Parameters` オブジェクトには、カスタマイズする各パラメータの名前を指定します。カスタマイズする各パラメータで、`ValueType` に `CUSTOM` を指定します。`Value` には、パラメータのデータ型とカスタム値を指定します。コントロールがサポートするパラメータをリクエストで省略した場合、そのパラメータは現在の値を保持します。GetSecurityControlDefinition API を呼び出すことで、コントロールでサポートされているパラメータ、データ型、有効な値を確認できます。

新しい設定ポリシーを作成する API リクエストの例:

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"},
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"}
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
```

```
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

AWS CLI

複数のアカウントおよびリージョンのコントロールパラメータをカスタマイズするには

カスタムパラメータを使用して新しい設定ポリシーを作成するには

1. ホームリージョンの委任管理者アカウントから create-configuration-policy コマンドを実行します。
2. `SecurityControlCustomParameters` オブジェクトには、カスタマイズする各コントロールの識別子を指定します。
3. `Parameters` オブジェクトには、カスタマイズする各パラメータの名前を指定します。カスタマイズする各パラメータで、`ValueType` に `CUSTOM` を指定します。`Value` には、パラメータのデータ型とカスタム値を指定します。`ValueType` が `CUSTOM` の場合、`Value` フィールドを空にすることはできません。コントロールがサポートするパラメータをリクエストで省略した場合、そのパラメータは現在の値を保持します。get-security-control-definition コマンドを実行することで、コントロールでサポートされているパラメータ、データ型、有効な値を確認できます。

既存の設定ポリシーでパラメータを追加または編集するには

1. 既存の設定ポリシーでカスタム入力パラメータを追加または更新するには、ホームリージョンの委任管理者アカウントから update-configuration-policy コマンドを実行します。
2. `identifier` フィールドには、更新するポリシーの Amazon リソースネーム (ARN) または ID を指定します。

3. SecurityControlCustomParameters オブジェクトには、カスタマイズする各コントロールの識別子を指定します。
4. Parameters オブジェクトには、カスタマイズする各パラメータの名前を指定します。カスタマイズする各パラメータで、ValueType に CUSTOM を指定します。Value には、パラメータのデータ型とカスタム値を指定します。コントロールがサポートするパラメータをリクエストで省略した場合、そのパラメータは現在の値を保持します。get-security-control-definition コマンドを実行することで、コントロールでサポートされているパラメータ、データ型、有効な値を確認できます。

新しい設定ポリシーを作成するコマンドの例:

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": "Integer": 15}}}]}}}'
```

1 つのアカウントおよびリージョンでコントロールパラメータをカスタマイズする

中央設定を使用していない場合、またはセルフマネージドアカウントがある場合は、一度に 1 つのリージョンでアカウントのコントロールパラメータをカスタマイズできます。

希望する方法を選択し、手順に従ってコントロールパラメータをカスタマイズします。変更は、現在のリージョンのアカウントにのみ適用されます。別のリージョンでコントロールパラメータをカスタマイズするには、パラメータをカスタマイズする別のアカウントおよびリージョンごとに以下の手順を繰り返します。同じコントロールでも、リージョンごとに異なるパラメータ値を使用できます。

Security Hub console

1 つのアカウントおよびリージョンでコントロールパラメータをカスタマイズするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

2. ナビゲーションペインで [コントロール] を選択します。テーブルで、カスタムパラメータをサポートしていて、パラメータを変更したいコントロールを選択します。[カスタムパラメータ] 列に、どのコントロールがカスタムパラメータをサポートしているかが示されます。
3. コントロールの詳細ページで、[パラメータ] タブを選択し、[編集] を選択します。
4. 必要なパラメータ値を指定します。
5. 必要に応じて、[変更の理由] セクションで、パラメータをカスタマイズする理由を選択します。
6. [保存] を選択します。

Security Hub API

1 つのアカウントおよびリージョンでコントロールパラメータをカスタマイズするには

1. UpdateSecurityControl API を呼び出します。
2. `SecurityControlId` には、カスタマイズするコントロールの ID を指定します。
3. `Parameters` オブジェクトには、カスタマイズする各パラメータの名前を指定します。カスタマイズする各パラメータで、`ValueType` に `CUSTOM` を指定します。`Value` には、パラメータのデータ型とカスタム値を指定します。コントロールがサポートするパラメータをリクエストで省略した場合、そのパラメータは現在の値を保持します。GetSecurityControlDefinition API を呼び出すことで、コントロールでサポートされているパラメータ、データ型、有効な値を確認できます。
4. 必要に応じて、`LastUpdateReason` に、コントロールパラメータをカスタマイズする理由を入力します。

API リクエストの例:

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 15
            }
        }
    },
    "LastUpdateReason": "Internal compliance requirement"
```

```
}
```

AWS CLI

1 つのアカウントおよびリージョンでコントロールパラメータをカスタマイズするには

1. update-security-control コマンドを実行します。
2. `security-control-id` には、カスタマイズするコントロールの ID を指定します。
3. `parameters` オブジェクトには、カスタマイズする各パラメータの名前を指定します。カスタマイズする各パラメータで、`ValueType` に `CUSTOM` を指定します。`Value` には、パラメータのデータ型とカスタム値を指定します。コントロールがサポートするパラメータをリクエストで省略した場合、そのパラメータは現在の値を保持します。get-security-control-definition コマンドを実行することで、コントロールでサポートされているパラメータ、データ型、有効な値を確認できます。
4. 必要に応じて、`last-update-reason` に、コントロールパラメータをカスタマイズする理由を入力します。

コマンドの例:

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer":
 15}}}' \
--last-update-reason "Internal compliance requirement"
```

コントロールパラメータのステータスをチェックする

コントロールパラメータの変更のステータスを検証してチェックすることは重要です。これにより、コントロールが期待どおりに機能し、意図したセキュリティ値を提供することを確認できます。パラメータの更新が成功したことを検証するには、Security Hub コンソールでコントロールの詳細を確認します。コンソールで、コントロールを選択して詳細を表示します。[パラメータ] タブに、パラメータ変更のステータスが表示されます。

プログラム上では、パラメータの更新リクエストが有効な場合、BatchGetSecurityControls 操作を受けて `UpdateStatus` フィールドの値が `UPDATING` になります。つまり、更新は有効でも、検出

結果には更新されたパラメータ値がまだ含まれていない可能性があります。UpdateState の値が READY に変わると、更新されたパラメータ値が検出結果に含まれ始めます。

UpdateSecurityControl 操作は、無効なパラメータ値に対して InvalidInputException レスポンスを返します。このレスポンスにより、失敗の理由に関するさらなる詳細が提供されます。例えば、パラメータの有効範囲外の値を指定した可能性があります。あるいは、正しいデータ型を使用していない値を指定しました。有効な入力内容でリクエストを再送信します。パラメータの更新に失敗した場合、Security Hub はパラメータの現在の値を保持します。

パラメータ値を更新しようとしたときに内部障害が発生した場合、有効にすると Security Hub は自動的に再試行 AWS Config します。詳細については、「の設定 AWS Config」を参照してください。

コントロールパラメータの確認

アカウント内の個々のコントロールパラメータの現在の値を確認できます。中央設定を使用する場合、委任 Security Hub 管理者は、設定ポリシーで指定されているパラメータ値を確認することもできます。

希望する方法を選択し、手順に従って現在のコントロールパラメータ値を確認します。

Security Hub console

現在のパラメータ値を確認するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. ナビゲーションペインで [コントロール] を選択します。コントロールを選択します。
3. [パラメータ] タブを選択します。このタブに、コントロールの現在のパラメータ値が表示されます。

Security Hub API

現在のパラメータ値を確認するには

BatchGetSecurityControls API を呼び出し、1 つ以上のセキュリティコントロール ID または ARN を指定します。レスポンス内の Parameters オブジェクトに、指定されたコントロールの現在のパラメータ値が表示されます。

API リクエストの例:

```
{
    "SecurityControlIds": ["APIGateway.1", "CloudWatch.15", "IAM.7"]
```

```
}
```

AWS CLI

現在のパラメータ値を確認するには

batch-get-security-controls コマンドを実行し、1 つ以上のセキュリティコントロール ID または ARN を指定します。レスポンス内の `Parameters` オブジェクトに、指定されたコントロールの現在のパラメータ値が表示されます。

コマンドの例:

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

希望する方法を選択し、中央設定ポリシーの現在のパラメータ値を表示します。

Security Hub console

設定ポリシーの現在のパラメータ値を確認するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   ホームリージョンの委任 Security Hub 管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで、[設定]、[設定] の順に選択します。
3. [ポリシー] タブで、設定ポリシーを選択し、[詳細を表示] を選択します。すると、現在のパラメータ値を含むポリシーの詳細が表示されます。

Security Hub API

設定ポリシーの現在のパラメータ値を確認するには

1. ホームリージョンの委任管理者アカウントから GetConfigurationPolicy API を呼び出します。
2. 詳細を確認したい設定ポリシーの ARN または ID を指定します。レスポンスに、現在のパラメータ値が含まれています。

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

設定ポリシーの現在のパラメータ値を確認するには

1. ホームリージョンの委任管理者アカウントから get-configuration-policy コマンドを実行します。
2. 詳細を確認したい設定ポリシーの ARN または ID を指定します。レスポンスに、現在のパラメータ値が含まれています。

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

コントロール検出結果には現在のパラメータ値も表示されます。AWS Security Finding Format (ASFF) 構文 では、これらの値は `Compliance` オブジェクトの `Parameters` フィールドに表示されます。Security Hub コンソールで検出結果を表示するには、ナビゲーションペインで [検出結果] を選択します。検出結果をプログラムで確認するには、GetFindings 操作を使用します。

> **Note**
>
> カスタムコントロールパラメータ機能のリリース後、Security Hub は、`Parameters` ASFF フィールドが含まれるように既存のコントロール検出結果を更新します。これには最大で 24 時間かかる場合があります。

デフォルトのコントロールパラメータ値に戻す

コントロールパラメータには、Security Hub が定義するデフォルト値を設定できます。進化するセキュリティベストプラクティスを反映させるため、パラメータのデフォルト値を更新する場合があり

ます。コントロールパラメータにカスタム値を指定していない場合、コントロールは、これらの更新を自動的に追跡し、新しいデフォルト値を使用します。

コントロールのデフォルトパラメータ値を使用するように戻すことができます。これを行う方法は、中央設定を使用するかどうかによって異なります。

> **Note**
>
> すべてのコントロールパラメータにデフォルトの Security Hub 値があるわけではありません。このような場合は、`ValueType` を `DEFAULT` に設定しても、Security Hub が使用する特定のデフォルト値は存在しません。より正確に言えば、Security Hub は、カスタム値がないときはパラメータを無視します。

複数のアカウントおよびリージョンでデフォルトのパラメータ値に戻す

中央設定を使用すると、複数のアカウントおよびリージョンで一元管理されるアカウントや OU のコントロールパラメータを元に戻すことができます。

希望する方法を選択し、手順に従って、中央設定を使用して複数のアカウントおよびリージョンでデフォルトのパラメータ値に戻します。

Security Hub console

複数のアカウントおよびリージョンでデフォルトのパラメータ値に戻すには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。

   ホームリージョンの Security Hub 委任管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで、[設定]、[設定] の順に選択します。
3. [Policies] タブを選択します。
4. ポリシーを選択し、[編集] を選択します。
5. [カスタムポリシー] の [コントロール] セクションに、カスタムパラメータを指定したコントロールのリストが表示されます。
6. 元に戻すパラメータ値が 1 つ以上あるコントロールを見つけます。そして、[削除] を選択してデフォルト値に戻します。
7. [アカウント] セクションで、ポリシーを適用するアカウントまたは OU を確認します。

8. [次へ] をクリックします。
9. 変更内容を見直し、それらが正しいことを確認します。完了したら、[ポリシーを保存して適用] を選択します。ホームリージョンおよびリンクされているすべてのリージョンで、このアクションにより、この設定ポリシーに関連付けられているアカウントおよび OU の既存の構成設定がオーバーライドされます。アカウントと OU は、直接適用するか親から継承することによって、設定ポリシーに関連付けることができます。

Security Hub API

複数のアカウントおよびリージョンでデフォルトのパラメータ値に戻すには

1. ホームリージョンの委任管理者アカウントから UpdateConfigurationPolicy API を呼び出します。
2. `Identifier` フィールドには、更新するポリシーの Amazon リソースネーム (ARN) または ID を指定します。
3. `SecurityControlCustomParameters` オブジェクトには、1 つ以上のパラメータを元に戻す各コントロールの識別子を指定します。
4. `Parameters` オブジェクトでは、元に戻すパラメータごとに、`ValueType` フィールドに `DEFAULT` を指定します。`ValueType` を `DEFAULT` に設定すると、`Value` フィールドに値を指定する必要がなくなります。リクエストに値が含まれている場合、Security Hub はその値を無視します。コントロールがサポートするパラメータをリクエストで省略した場合、そのパラメータは現在の値を保持します。

> **Warning**
>
> `SecurityControlCustomParameters` フィールドでコントロールオブジェクトを省略すると、Security Hub は、そのコントロールのすべてのカスタムパラメータをデフォルト値に戻します。`SecurityControlCustomParameters` のリストが完全に空の場合は、すべてのコントロールのカスタムパラメータがデフォルト値に戻ります。

API リクエストの例:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
    "Name": "TestConfigurationPolicy",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Revert ACM.1 parameter to default value",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"},
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"}
                ],
             "SecurityControlsConfiguration": {
                "DisbledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "DEFAULT"
                             }
                         }
                    }
                ]
             }
        }
    }
}
```

AWS CLI

複数のアカウントおよびリージョンでデフォルトのパラメータ値に戻すには

1. ホームリージョンの委任管理者アカウントから update-configuration-policy コマンドを実行します。
2. `identifier` フィールドには、更新するポリシーの Amazon リソースネーム (ARN) または ID を指定します。
3. `SecurityControlCustomParameters` オブジェクトには、1 つ以上のパラメータを元に戻す各コントロールの識別子を指定します。

4. Parameters オブジェクトでは、元に戻すパラメータごとに、ValueType フィールドに DEFAULT を指定します。ValueType を DEFAULT に設定すると、Value フィールドに値を指定する必要がなくなります。リクエストに値が含まれている場合、Security Hub はその値を無視します。コントロールがサポートするパラメータをリクエストで省略した場合、そのパラメータは現在の値を保持します。

> **Warning**
>
> SecurityControlCustomParameters フィールドでコントロールオブジェクトを省略すると、Security Hub は、そのコントロールのすべてのカスタムパラメータをデフォルト値に戻します。SecurityControlCustomParameters のリストが完全に空の場合は、すべてのコントロールのカスタムパラメータがデフォルト値に戻ります。

コマンドの例:

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--name "TestConfigurationPolicy" \
--description "Updated configuration policy" \
--updated-reason "Revert ACM.1 parameter to default value"
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "DEFAULT"}}}]}}}'
```

1 つのアカウントおよびリージョンでデフォルトのパラメータ値に戻す

中央設定を使用していない場合、またはセルフマネージドアカウントがある場合は、一度に 1 つのリージョンでアカウントのデフォルトパラメータ値を使用するように戻すことができます。

希望する方法を選択し、手順に従って 1 つのリージョンでアカウントのデフォルトのパラメータ値に戻します。別のリージョンでデフォルトのパラメータ値に戻すには、それぞれのリージョンでこれらの手順を繰り返します。

> **Note**
>
> Security Hub を無効にすると、カスタムコントロールパラメータがリセットされます。その後、Security Hub を再度有効にすると、すべてのコントロールがデフォルトのパラメータ値を使用して起動します。

Security Hub console

1 つのアカウントおよびリージョンでデフォルトのパラメータ値に戻すには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. ナビゲーションペインで [コントロール] を選択します。デフォルトのパラメータ値に戻すコントロールを選択します。
3. `Parameters` タブで、コントロールパラメータの横にある [カスタマイズ済み] を選択します。そして、[カスタマイズを削除] を選択します。これで、このパラメータはデフォルトの Security Hub 値を使用し、デフォルト値の今後の更新を追跡するようになります。
4. 元に戻すパラメータ値ごとに、上記のステップを繰り返します。

Security Hub API

1 つのアカウントおよびリージョンでデフォルトのパラメータ値に戻すには

1. UpdateSecurityControl API を呼び出します。
2. `SecurityControlId` には、パラメータを元に戻すコントロールの ARN または ID を指定します。
3. `Parameters` オブジェクトでは、元に戻すパラメータごとに、`ValueType` フィールドに `DEFAULT` を指定します。`ValueType` を `DEFAULT` に設定すると、`Value` フィールドに値を指定する必要がなくなります。リクエストに値が含まれている場合、Security Hub はその値を無視します。
4. 必要に応じて、`LastUpdateReason` に、デフォルトのパラメータ値に戻す理由を入力します。

API リクエストの例:

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "DEFAULT"
        },
    "LastUpdateReason": "New internal requirement"
}
```

AWS CLI

1 つのアカウントおよびリージョンでデフォルトのパラメータ値に戻すには

1. update-security-control コマンドを実行します。
2. `security-control-id` には、パラメータを元に戻すコントロールの ARN または ID を指定します。
3. `parameters` オブジェクトでは、元に戻すパラメータごとに、`ValueType` フィールドに `DEFAULT` を指定します。`ValueType` を `DEFAULT` に設定すると、`Value` フィールドに値を指定する必要がなくなります。リクエストに値が含まれている場合、Security Hub はその値を無視します。
4. 必要に応じて、`last-update-reason` に、デフォルトのパラメータ値に戻す理由を入力します。

コマンドの例:

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

カスタムパラメータをサポートするコントロール

カスタムパラメータをサポートするセキュリティコントロールのリストについては、Security Hub コンソールの [コントロール] ページまたは「Security Hub コントロールのリファレンス」を参照して

ください。このリストをプログラムで取得するには、ListSecurityControlDefinitions 操作を使用します。レスポンスで、CustomizableProperties オブジェクトによって、どのコントロールがカスタマイズ可能なパラメータをサポートしているかが示されます。

無効にする可能性のある Security Hub コントロール

検出結果のノイズを減らし、コストを抑えるために、一部の AWS Security Hub コントロールを無効にすることをお勧めします。

グローバルリソースを処理するコントロール

一部の はグローバルリソース AWS のサービス をサポートしています。つまり、任意の からリソースにアクセスできます AWS リージョン。のコストを節約するために AWS Config、1 つのリージョンを除くすべてのリージョンでグローバルリソースの記録を無効にすることができます。ただし、これを行った後、Security Hub は引き続きコントロールが有効になっているすべてのリージョンでセキュリティチェックを実行し、リージョンごとにアカウントごとのチェック数に基づいて料金を請求します。したがって、検出結果のノイズを減らし、Security Hub のコストを節約するには、グローバルリソースを記録するリージョンを除くすべてのリージョンで、グローバルリソースを含むコントロールを無効にする必要もあります。

コントロールにグローバルリソースが含まれるが、1 つのリージョンでのみ使用可能な場合、そのリージョンでコントロールを無効にすると、基盤となるリソースに関する結果を取得できなくなります。この場合、コントロールを有効にしておくことをお勧めします。クロスリージョン集約を使用する場合、コントロールが利用可能なリージョンは、集約リージョンまたはリンクされたリージョンのいずれかである必要があります。以下のコントロールにはグローバルリソースが含まれますが、1 つのリージョンでのみ使用できます。

- すべての CloudFront コントロール — 米国東部 (バージニア北部) でのみ使用可能
- GlobalAccelerator.1 – 米国西部 (オレゴン) でのみ使用可能
- Route53.2 – 米国東部 (バージニア北部) でのみ使用可能
- WAF.1、WAF.6、WAF.7、および WAF.8 – 米国東部 (バージニア北部) でのみ使用可能

> **Note**
>
> 中央設定を使用する場合、Security Hub はホームリージョンを除くすべてのリージョンでグローバルリソースを含むコントロールを自動的に無効にします。設定ポリシーを有効にして選択したその他のコントロールは、使用可能なすべてのリージョンで有効になります。これ

らのコントロールの検出結果を 1 つのリージョンのみに制限するには、 AWS Config レコーダーの設定を更新し、ホームリージョンを除くすべてのリージョンでグローバルリソースの記録をオフにします。中央設定を使用する場合、ホームリージョンおよびリンクされたリージョンで利用できないコントロールのカバレッジがありません。中央設定の詳細については、「中央設定の仕組み」を参照してください。

定期的なスケジュールタイプを持つコントロールの場合、課金を防ぐには Security Hub でコントロールを無効にする必要があります。 AWS Config パラメータを `includeGlobalResourceTypes`に設定`false`しても、定期的な Security Hub コントロールには影響しません。

以下は、グローバルリソースを含む Security Hub コントロールのリストです。

- [Account.1] のセキュリティ連絡先情報を に提供する必要があります AWS アカウント
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります

- 〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.10] IAM ユーザーのパスワードポリシーには強力な AWS Config設定が必要です
- [IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します
- [IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します
- [IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します
- [IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します
- [IAM.15] 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します
- [IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています
- [IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します
- [IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります

- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーはタグ付けする必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID には AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります

CloudTrail ログ記録を処理するコントロール

このコントロールは、 AWS Key Management Service （ AWS KMS) を使用して AWS CloudTrail 証跡ログを暗号化します。集中ログ記録アカウントでこれらの追跡をログ記録する場合、このコントロールは集中ログ記録が行われるアカウントとリージョンを有効化するだけで済みます。

> **Note**
>
> 中央設定を使用した場合、コントロールの有効化ステータスは、ホームリージョンおよびリンクされたリージョンで統一されます。一部のリージョンでコントロールを無効にして、他のリージョンで有効にすることはできません。この場合は、以下のコントロールの検出結果を抑制し、検出結果のノイズを減らします。

- 〔CloudTrail.2] 保管時の暗号化を有効にする CloudTrail 必要があります

CloudWatch アラームを処理するコントロール

Amazon CloudWatch アラームの代わりに Amazon を使用して GuardDuty 異常検出を行う場合は、CloudWatch アラームに焦点を当てたこれらのコントロールを無効にすることができます。

- 〔CloudWatch.1] 「ルート」ユーザーの使用に対してログメトリクスフィルターとアラームが存在する必要があります
- 〔CloudWatch.2] 不正な API コールに対してログメトリクスフィルターとアラームが存在することを確認する
- 〔CloudWatch.3] MFA を使用しない マネジメントコンソールサインインのログメトリクスフィルターとアラームが存在することを確認する
- 〔CloudWatch.4] IAM ポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認する
- 〔CloudWatch.5] CloudTrail AWS Configログメトリクスフィルターとアラームが設定変更用に存在することを確認する
- 〔CloudWatch.6] AWS Management Console 認証の失敗に対してログメトリクスフィルターとアラームが存在することを確認する
- 〔CloudWatch.7] カスタマーマネージドキーの無効化またはスケジュールされた削除のためのログメトリクスフィルターとアラームが存在することを確認する
- 〔CloudWatch.8] S3 バケットポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認する
- 〔CloudWatch.9] AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する
- 〔CloudWatch.10] セキュリティグループの変更に対するログメトリクスフィルターとアラームが存在することを確認する
- 〔CloudWatch.11] ネットワークアクセスコントロールリスト (NACL) の変更に対するログメトリクスフィルターとアラームが存在することを確認する
- 〔CloudWatch.12] ネットワークゲートウェイの変更に対するログメトリクスフィルターとアラームが存在することを確認する
- 〔CloudWatch.13] ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認する
- 〔CloudWatch.14] VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認する

コントロールの詳細の表示

AWS Security Hub コントロールごとに、便利な詳細のページを表示できます。

コントロールの詳細ページの上部に、以下のようなコントロールの概要が表示されます。

- [有効化ステータス] — ページの上部に、少なくとも 1 つのメンバーアカウントで、少なくとも 1 つの標準に対してコントロールが有効になっているかどうかが表示されます。集約リージョンを設定した場合、そのコントロールは、少なくとも 1 つのリージョンで少なくとも 1 つの標準に対して有効になっていれば有効になります。コントロールが無効になっている場合は、このページから有効化できます。コントロールが有効になっている場合は、このページから無効化できます。詳細については、「the section called “すべての標準におけるコントロールの有効化と無効化”」を参照してください。
- [コントロールステータス] - これは、コントロールの検出結果のコンプライアンスステータスに基づき、コントロールのパフォーマンスを要約します。Security Hub は通常、Security Hub コンソールの [Summary] (概要) ページまたは [Security standards] (セキュリティ標準) ページへの最初のアクセスから 30 分以内に最初のコントロールステータスを生成します。ステータスは、これらのページにアクセスしたときに有効になっているコントロールでのみ使用できます。`UpdateStandardsControl` API オペレーションを使用して、コントロールを有効または無効にします。さらに、コントロールステータスが表示されるように AWS Config リソース記録を設定する必要があります。最初のコントロールステータスが生成された後、Security Hub は、過去 24 時間の結果に基づき、24 時間おきにコントロールステータスを更新します。Security Hub によって、標準の詳細ページおよびコントロールの詳細ページに、ステータスが最後に更新された日時を示すタイムスタンプが表示されます。

  管理者アカウントには、管理者アカウントとメンバーアカウントを横断して集約されたコントロールステータスが表示されます。集約リージョンを設定すると、コントロールステータスには、リンクされたすべてのリージョンの検出結果が含まれます。コントロールステータスの詳細については、the section called “コンプライアンスステータスとコントロールステータス” を参照してください。

> **Note**
>
> 有効にしてから、最初のコントロールステータスのコントロールが中国リージョンと AWS GovCloud (US) Regionで生成されるまで、最大で 24 時間かかります。

[標準と要件] タブには、コントロールが有効化できる標準と、さまざまなコンプライアンスフレームワークからのコントロールに関連する要件が一覧表示されます。

詳細ページの下部には、そのコントロールのアクティブな結果に関する情報が表示されます。コントロールの結果は、コントロールに対するセキュリティチェックによって生成されます。コントロール結果リストには、アーカイブされた結果は含まれません。

結果リストで使用されるタブには、リストのさまざまなサブセットが表示されます。ほとんどのタブの結果リストには、ワークフローステータスが NEW、NOTIFIED、または RESOLVED である結果が表示されます。ワークフローが SUPPRESSED の結果は、別のタブに表示されます。

各検出結果について、リストからコンプライアンスステータスや関連リソースなどの検出結果の詳細にアクセスできます。各結果のワークフローステータスを設定し、結果をカスタムアクションに送信することもできます。詳細については、「the section called “統制結果の表示とアクションの実行”」を参照してください。

コントロールの詳細の表示

お好みのアクセス方法を選択し、以下の手順に従ってコントロールの詳細を表示します。詳細は現在のアカウントとリージョンに適用されます。また、以下の内容を含みます。

- コントロールのタイトルと説明
- 失敗したコントロールの検出結果を修正する手順へのリンク
- コントロールの重要度
- コントロールの有効化ステータス
- (コンソール上) コントロールの最近の検出結果のリスト。Security Hub API または を使用する場合は AWS CLI、 `GetFindings`を使用してコントロールの検出結果を取得します。

Security Hub console

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. ナビゲーションペインで [コントロール] を選択します。
3. コントロールを選択します。

Security Hub API

1. `ListSecurityControlDefinitions` を実行し、1 つ以上の標準 ARN を提供して、その標準におけるコントロール ID のリストを取得します。標準 ARN を取得するに

は、DescribeStandards を実行します。標準 ARN を提供しない場合、この API はすべての Security Hub コントロール ID を返します。この API は、これらの機能リリース以前に存在していた標準ベースのコントロール ID ではなく、標準に依存しないセキュリティコントロール ID を返します。

リクエストの例:

```
{
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
}
```

2. を実行してBatchGetSecurityControls、現在の AWS アカウント と の 1 つ以上のコントロールに関する詳細を取得します AWS リージョン。

   リクエストの例:

```
{
    "SecurityControlIds": ["Config.1", "IAM.1"]
}
```

AWS CLI

1. list-security-control-definitions コマンドを実行し、1 つ以上の標準 ARN を提供してコントロール ID のリストを取得します。標準 ARN を取得するには、describe-standards コマンドを実行します。標準 ARN を提供しない場合、このコマンドはすべての Security Hub コントロール ID を返します。このコマンドは、これらの機能リリース以前に存在していた標準ベースのコントロール ID ではなく、標準に依存しないセキュリティコントロール ID を返します。

```
aws securityhub --region us-east-1 list-security-control-definitions --standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0"
```

2. batch-get-security-controls コマンドを実行し、 AWS アカウント および AWS リージョンにおける 1 つ以上のコントロールの詳細を取得します。

```
aws securityhub --region us-east-1 batch-get-security-controls --security-
control-ids '["Config.1", "IAM.1"]'
```

コントロールリストのフィルタリングとソート

[コントロール] ページには、コントロールのリストが表示されます。リストのフィルタリングまたはソートを実行し、特定のコントロールのサブセットに注目します。

- [すべて有効] (少なくとも 1 つの有効な標準で有効になっているコントロール)
- [失敗] (Failed ステータスのコントロール)
- [不明] (Unknown ステータスのコントロール)
- [合格] (Passed ステータスのコントロール)
- [無効] (すべての標準で無効になっているコントロール)
- [データなし] (検出結果のないコントロール)
- [すべて] (すべてのコントロール。有効と無効の両方で、コントロールステータスや検出結果の数は考慮しない)

コントロールステータスの詳細については、コンプライアンスステータスとコントロールステータスを参照してください。

AWS Organizations との統合を使用していて、管理者アカウントにログイン AWS Security Hub している場合、すべて有効タブには、少なくとも 1 つのメンバーアカウントで有効になっているコントロールが含まれます。集約リージョンを設定している場合、[すべて有効] タブには、リンクされているリージョンの少なくとも 1 つで有効化されたコントロールが表示されます。

デフォルトでは、[失敗] タブが表示されます。各タブのコントロールは、デフォルトで [重要] から [低] まで、重要度別にソートされています。コントロール ID、コンプライアンスステータス、重要度、失敗したチェックの数でコントロールをソートすることもできます。検索バーでは、特定のコントロールを検索できます。

> **Tip**
>
> コントロール検出結果に基づいてワークフローを自動化している場合は、Title や Description より SecurityControlId または SecurityControlArn ASFF フィールドをフィルターとして使用することをお勧めします。前者のフィールドは変更される可能性がありますが、コントロール ID と ARN は静的な識別子です。

コントロールの横にあるオプションを選択すると、コントロールが現在有効になっている標準を表示するサイドパネルが表示されます。また、コントロールが現在無効になっている標準も確認できます。このパネルから、すべての標準でコントロールを無効化することでコントロールを無効にできます。標準全体に関わるコントロールの有効化と無効化の詳細については、「すべての標準におけるコントロールの有効化と無効化」を参照してください。管理者アカウントの場合、サイドパネルに表示される情報には、すべてのメンバーアカウントが反映されます。

Security Hub API で、`ListSecurityControlDefinitions` を実行してコントロール ID のリストを取得します。関心のあるコントロール IDs を取得したら、`BatchGetSecurityControls`を実行して、現在の AWS アカウント と のコントロールのサブセットに関するデータを取得します AWS リージョン。

統制結果の表示とアクションの実行

コントロールの詳細ページには、コントロールのアクティブな検出結果のリストが表示されます。このリストには、アーカイブされた結果は含まれていません。

コントロールの詳細ページは、検出結果の集約をサポートしています。集約リージョンを設定している場合、コントロール詳細ページのコントロールステータスおよびセキュリティチェックのリストには、リンクされているすべての AWS リージョンのチェックが含まれます。

リストには、結果をフィルタリングおよびソートするためのツールが用意されており、急を要する結果から重点的に取り組むことができます。検出結果には、関連するサービスコンソールにおけるリソースの詳細へのリンクが含まれている場合があります。 AWS Config ルールに基づくコントロールの場合、ルールと設定タイムラインの詳細を表示できます。

AWS Security Hub API を使用して検出結果のリストを取得することもできます。詳細については、「the section called “結果の詳細の確認”」を参照してください。

トピック

- 統制結果および結果リソースに関する詳細の表示
- コントロールの検出結果のサンプル
- コントロールの検出結果リストのフィルタリング、ソート、ダウンロード
- 統制結果に対するアクションをとる

統制結果および結果リソースに関する詳細の表示

AWS Security Hub では、各コントロールの検出結果について、調査に役立つ以下の詳細を提供します。

- ユーザーが検出結果に加えた変更の履歴
- 検出結果の .json ファイル
- 検出結果に関連するリソースに関する情報
- 検出結果に関連する設定ルール
- ユーザーが検出結果に追加したメモ

次のセクションでは、これらの詳細にアクセスする方法について説明します。

検出結果の履歴

検出結果の履歴は、過去 90 日間に検出結果に加えられた変更を追跡できる Security Hub の機能です。

検出結果の履歴は、コントロールの検出結果といった Security Hub の検出結果に使用できます。詳細については、「結果履歴の確認」を参照してください。

結果の完全な .json の表示

結果の .json 全文を表示してダウンロードすることができます。

.json を表示するには、[Finding .json] (.json を検索する) 列で、アイコンを選択します。

[Finding JSON] (JSON を検索する) パネルで、.json をダウンロードするため、[Download] (ダウンロード) を選択します。

結果リソースに関する情報を表示する

[Resource] (リソース) 列には、リソースタイプとリソース識別子が含まれています。

リソースに関する情報を表示するには、リソース識別子を選択します。 AWS アカウントの場合は、アカウントが組織メンバーアカウントの場合、情報にはアカウント ID とアカウント名の両方が含まれます。手動で招待されたアカウントの場合は、情報にはアカウント ID のみが含まれます。

元のサービスでリソースを表示する許可が付与されている場合、リソース識別子にサービスへのリンクが表示されます。例えば、 AWS ユーザーの場合、リソースの詳細には、IAM でユーザーの詳細を表示するリンクが表示されます。

リソースが別のアカウントにある場合は、Security Hub がメッセージ通知を表示します。

結果リソースの設定タイムラインの表示

調査の一つの手段として、 AWS Configでリソースの設定タイムラインを確認します。

結果リソースの設定タイムラインを表示する許可がある場合、結果リストにはタイムラインへのリンクが表示されます。

リソースが別のアカウントにある場合は、Security Hub によって表示されるメッセージで通知されます。

の設定タイムラインに移動するには AWS Config

1. [Investigate] (調査) 列で、アイコンを選択します。
2. メニューで、[Configuration timeline] (設定タイムライン) を選択します。設定タイムラインへのアクセス権がない場合、リンクは表示されません。

検出結果リソースの AWS Config ルールの表示

コントロールが AWS Config ルールに基づいている場合は、 AWS Config ルールの詳細を表示することもできます。 AWS Config ルール情報は、チェックが成功または失敗した理由をよりよく理解するのに役立ちます。

コントロールの AWS Config ルールを表示するアクセス許可がある場合、結果リストには の AWS Config ルールへのリンクが表示されます AWS Config。

リソースが別のアカウントにある場合は、Security Hub によって表示されるメッセージで通知されます。

AWS Config ルールに移動するには

1. [Investigate] (調査) 列で、アイコンを選択します。
2. メニューで、[Config rule] (Config ルール) を選択します。 AWS Config ルールにアクセスできない場合、Config ルールはリンクされません。

結果に関するメモの表示

結果に関連するメモがある場合、[Updated] (更新) 列にはノートアイコンが表示されます。

結果に関連付けられているメモを表示するには

[Updated] (更新) 列で、ノートアイコンを選択します。

コントロールの検出結果のサンプル

コントロールの検出結果の形式は、[統合されたコントロールの検出結果] を有効にしているかどうかによって異なります。この機能を有効にすると、コントロールが複数の有効化された標準に適用される場合でも、Security Hub はコントロールチェックに対して単一の検出結果を生成します。詳細については、「統合されたコントロールの検出結果」を参照してください。

次のセクションでは、コントロールの検出結果のサンプルを示しています。アカウントで [統合されたコントロールの検出結果] が無効になっている場合は各 Security Hub 標準の検出結果が、有効になっている場合は標準全体にわたるコントロールの検出結果のサンプルが含まれます。

> **Note**
>
> 検出結果は、中国リージョンと AWS GovCloud (US) リージョンのさまざまなフィールドと値を参照します。詳細については、「ASFF フィールドと値への統合の影響」を参照してください。

[統合されたコントロールの検出結果] が無効

- AWS Foundational Security Best Practices (FSBP) 標準のサンプル結果
- Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 の検出結果の例
- Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 の検出結果の例
- Center for Internet Security (CIS) AWS Foundations Benchmark v3.0.0 の検出結果例
- 米国国立標準技術研究所 (NIST) SP 800-53 (リビジョン 5) の検出結果のサンプル
- Payment Card Industry Data Security Standard (PCI DSS) の検出結果のサンプル
- Resource Tagging Standard AWS のサンプル結果
- サービスマネージドスタンダードの検出結果の例： AWS Control Tower

[統合されたコントロールの検出結果] が有効

- 標準全体の検出結果のサンプル

FSBP の検出結果のサンプル


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.076Z",
  "LastObservedAt": "2021-09-28T16:10:06.956Z",
  "CreatedAt": "2020-08-06T02:18:23.076Z",
  "UpdatedAt": "2021-09-28T16:10:00.093Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-
practices/v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0",
    "ControlId": "CloudTrail.2",
```

```
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/aws-foundation-best-practices/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
```

```
      "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
    ]
  }
}
```

CIS AWS Foundations Benchmark v3.0.0 のサンプル結果

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2024-04-18T07:46:18.193Z",
  "LastObservedAt": "2024-04-23T07:47:01.137Z",
  "CreatedAt": "2024-04-18T07:46:18.193Z",
  "UpdatedAt": "2024-04-23T07:46:46.165Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.2.1 EBS default encryption should be enabled",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
 the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
 at EBS volume creation is supported.",
  "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/EC2.7/remediation"
    }
```

```
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/3.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0",
    "ControlId": "2.2.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2843ed9e",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v3.0.0/2.2.1"
    ],
    "SecurityControlId": "EC2.7",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
```

```
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  },
  "ProcessedAt": "2024-04-23T07:47:07.088Z"
}
```

CIS AWS Foundations Benchmark v1.4.0 のサンプル結果

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/1.4.0/3.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2022-10-21T22:14:48.913Z",
  "LastObservedAt": "2022-12-22T22:24:56.980Z",
  "CreatedAt": "2022-10-21T22:14:48.913Z",
  "UpdatedAt": "2022-12-22T22:24:52.409Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
```

```
  "Description": "AWS CloudTrail is a web service that records AWS API calls for an
 account and makes those logs available to users and resources in accordance with IAM
 policies. AWS Key Management Service (KMS) is a managed service that helps create
 and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail logs
 can be configured to leverage server side encryption (SSE) and AWS KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0",
    "ControlId": "3.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-855f82d1",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/1.4.0/3.7",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-1"
    }
```

```
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  }
}
```

CIS AWS Foundations Benchmark v1.2.0 のサンプル結果

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/
rule/2.7",
  "AwsAccountId": "123456789012",
  "Types": [
```

```
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2020-08-29T04:10:06.337Z",
  "LastObservedAt": "2021-09-28T16:10:05.350Z",
  "CreatedAt": "2020-08-29T04:10:06.337Z",
  "UpdatedAt": "2021-09-28T16:10:00.087Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS Key Management Service (KMS) is a managed service that helps
 create and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail
 logs can be configured to leverage server side encryption (SSE) and KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsGuideArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0",
    "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
    "RuleId": "2.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/cis-aws-
foundations-benchmark/v/1.2.0/2.7",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
```

```
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  }
}
```

NIST SP 800-53 Rev. 5 の検出結果のサンプル

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-53/v/5.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2023-02-17T14:22:46.726Z",
  "LastObservedAt": "2023-02-17T14:22:50.846Z",
  "CreatedAt": "2023-02-17T14:22:46.726Z",
  "UpdatedAt": "2023-02-17T14:22:46.726Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to fix this issue, consult the AWS Security Hub
 NIST 800-53 R5 documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-53/v/5.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-53/v/5.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.9/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
```

```
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/
v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",

      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",

      "Partition": "aws",

      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
        "NIST.800-53.r5 AU-9",
        "NIST.800-53.r5 CA-9(1)",
        "NIST.800-53.r5 CM-3(6)",
        "NIST.800-53.r5 SC-13",
        "NIST.800-53.r5 SC-28",
        "NIST.800-53.r5 SC-28(1)",
        "NIST.800-53.r5 SC-7(10)",
        "NIST.800-53.r5 SI-7(6)"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-53/v/5.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
```

```
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2023-02-17T14:22:53.572Z"
}
```

PCI DSS の検出結果のサンプル

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "pci-dss/v/3.2.1/PCI.CloudTrail.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.089Z",
  "LastObservedAt": "2021-09-28T16:10:06.942Z",
  "CreatedAt": "2020-08-06T02:18:23.089Z",
  "UpdatedAt": "2021-09-28T16:10:00.090Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest using AWS KMS
 CMKs",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption by checking if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
```

```
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/pci-dss/v/3.2.1",
    "ControlId": "PCI.CloudTrail.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/pci-dss/
v/3.2.1/PCI.CloudTrail.1",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "PCI DSS 3.4"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/pci-dss/v/3.2.1"
    }]
  },
```

```
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
    ]
  }
}
```

Resource Tagging Standard AWS のサンプル結果

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "security-control/EC2.44",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-02-19T21:00:32.206Z",
  "LastObservedAt": "2024-04-29T13:01:57.861Z",
  "CreatedAt": "2024-02-19T21:00:32.206Z",
  "UpdatedAt": "2024-04-29T13:01:41.242Z",
  "Severity": {
    "Label": "LOW",
    "Normalized": 1,
    "Original": "LOW"
  },
  "Title": "EC2 subnets should be tagged",
  "Description": "This control checks whether an Amazon EC2 subnet has tags with the
 specific keys defined in the parameter requiredTagKeys. The control fails if the
```

```
 subnet doesn't have any tag keys or if it doesn't have all the keys specified in
 the parameter requiredTagKeys. If the parameter requiredTagKeys isn't provided, the
 control only checks for the existence of a tag key and fails if the subnet isn't
 tagged with any key. System tags, which are automatically applied and begin with aws:,
 are ignored.",
  "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/EC2.44/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-tagged-ec2-subnet-6ceafede",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "No tags are present.",
    "Resources:0/Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
    "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
securityhub/arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsEc2Subnet",
      "Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/subnet-1234567890abcdef0",
      "Partition": "aws",
      "Region": "eu-central-1",
      "Details": {
        "AwsEc2Subnet": {
          "AssignIpv6AddressOnCreation": false,
          "AvailabilityZone": "eu-central-1b",
          "AvailabilityZoneId": "euc1-az3",
          "AvailableIpAddressCount": 4091,
          "CidrBlock": "10.24.34.0/23",
          "DefaultForAz": true,
          "MapPublicIpOnLaunch": true,
          "OwnerId": "123456789012",
          "State": "available",
          "SubnetArn": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
          "SubnetId": "subnet-1234567890abcdef0",
```

```
          "VpcId": "vpc-021345abcdef6789"
        }
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.44",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/aws-resource-tagging-standard/v/1.0.0"
      }
    ],
    "SecurityControlParameters": [
      {
        "Name": "requiredTagKeys",
        "Value": [
          "peepoo"
        ]
      }
    ],
            },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "LOW",
      "Original": "LOW"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2024-04-29T13:02:03.259Z"
}
```

サービスマネージドスタンダードの検出結果の例： AWS Control Tower

> **Note**
>
> この標準は、 で標準を作成した AWS Control Tower ユーザーのみが使用できます AWS Control Tower。詳細については、「サービスマネージドスタンダード： AWS Control Tower」を参照してください。


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-
control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-11-17T01:25:30.296Z",
  "LastObservedAt": "2022-11-17T01:25:45.805Z",
  "CreatedAt": "2022-11-17T01:25:30.296Z",
  "UpdatedAt": "2022-11-17T01:25:30.296Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CT.CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "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/CloudTrail.2/remediation"
    }
```

```
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/service-managed-aws-control-tower/
v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0",
    "ControlId": "CT.CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/service-
managed-aws-control-tower/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-
aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
```

```
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}
```

標準全体の検出結果サンプル ([統合されたコントロールの検出結果] が有効な場合)

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "security-control/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-10-06T02:18:23.076Z",
  "LastObservedAt": "2022-10-28T16:10:06.956Z",
  "CreatedAt": "2022-10-06T02:18:23.076Z",
  "UpdatedAt": "2022-10-28T16:10:00.093Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": "40",
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
```

```
  },
  "ProductFields": {
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  }
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
        "PCI DSS v3.2.1/3.4",
        "CIS AWS Foundations Benchmark v1.2.0/2.7",
        "CIS AWS Foundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
       { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
       { "StandardsId": "standards/pci-dss/v/3.2.1"},
       { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
       { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
       { "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
```

```
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}
```

コントロールの検出結果リストのフィルタリング、ソート、ダウンロード

フィルタリングタブを使用して、コンプライアンスステータスに基づいてコントロールの検出結果のリストをフィルタリングできます。他の検出結果フィールドの値に基づいてリストをフィルタリングし、リストから検出結果をダウンロードすることもできます。

統制結果リストのフィルタリングとソート

[All checks] (すべてのチェック) タブには、ワークフローステータスが NEW、NOTIFIED、または RESOLVED のアクティブな結果がすべて一覧表示されます。デフォルトでは、失敗した結果が、リストの先頭に表示されるようにリストがソートされます。このようなソート順で表示し、対処が必要な検出結果に優先順位を付けることができます。

[Failed] (失敗)、[Unknown] (不明)、および [Passed] (成功) のタブにあるリストは、Compliance.Status の値に基づいてフィルタリングされます。リストには、ワークフローステータスが NEW、NOTIFIED、または RESOLVED のアクティブな結果のみが含まれます。

[抑制済み] タブには、ワークフローステータスが [SUPPRESSED] のアクティブな検出結果のリストが表示されます。

各タブの組み込みフィルターに加えて、次のフィールドの値を使用してリストをフィルタリングできます。

- アカウント ID
- ワークフローステータス
- コンプライアンス状況
- リソース ID
- リソースタイプ

任意の列を使用して各リストをソートできます。

統制結果リストのダウンロード

[セキュリティ標準] に移動して標準を選択すると、標準のコントロールのリストが表示されます。リストからコントロールを選択すると、コントロールの結果のリストを含むコントロールの詳細ページが表示されます。ここから、統制結果を .csv 形式でダウンロードできます。

検出結果リストをフィルタリングする場合は、ダウンロードにはフィルターに一致するコントロールのみが含まれます。

リストから特定の検出結果を選択する場合は、ダウンロードには選択した検出結果のみが含まれます。

検出結果をダウンロードするには [Download now] (今すぐダウンロード) を選択します。検出結果の現在のページがダウンロードされます。

統制結果に対するアクションをとる

調査の現在のステータスを反映するには、ワークフローステータスを設定します。詳細については、「the section called “結果のワークフローステータスを設定する”」を参照してください。

では AWS Security Hub、選択した検出結果を Amazon のカスタムアクションに送信することもできます EventBridge。詳細については、「the section called “カスタムアクションに結果を送信する”」を参照してください。

[概要] ダッシュボードの使用

AWS Security Hub コンソールの [概要] ページのダッシュボードは、追加の分析ツールや複雑なクエリを使用しなくても、AWS 環境内のセキュリティ上の懸念事項を特定するのに役立ちます。ダッシュボードのレイアウトをカスタマイズしたり、ウィジェットを追加または削除したり、データをフィルタリングして特に関心のある分野に焦点を当てることができます。フィルター条件をフィルターセットとして保存して、後で特定の種類のデータをすばやく取得することもできます。

ダッシュボードをカスタマイズしたり、データをフィルタリングしたりすると、Security Hub では自動的にその設定が保存され、後で使用できるようになります。また、この設定は Security Hub アカウントのユーザーごとに個別に保存されます。つまり、ユーザーごとにダッシュボードのレイアウト、ウィジェット、フィルターセットを設定できます。

[概要] ダッシュボードを開くたびに、Security Hub はほとんどのダッシュボードデータを自動的に更新します。ただし、一部のデータはそれほど頻繁には更新されません。例えば、セキュリティスコアとコントロールステータスは 24 時間ごとに更新されます。

Security Hub にクロスリージョン集約リージョンを設定した場合、ダッシュボードデータには集約リージョンとすべてのリンクされたリージョンの検出結果が含まれます。組織の Security Hub 委任管理者である場合、データには管理者アカウントとメンバーアカウントの検出結果が含まれます。オプションで、アカウント別にデータをフィルタリングすることができます。メンバーアカウントまたはスタンドアロンアカウントの場合、データにはそのアカウントの検出結果のみが含まれます。

[概要] ダッシュボードで利用できるウィジェット

[概要] ダッシュボードには、AWS ユーザーのセキュリティ運用と経験に基づいて、最新のクラウドセキュリティ脅威の状況を反映したウィジェットが表示されます。ウィジェットには、デフォルトで表示されるものもあれば、表示されないものもあります。ウィジェットを追加または削除することで、ダッシュボードの表示をカスタマイズできます。

ウィジェットを追加するには、[概要] ページの右上にある [ウィジェットを追加] を選択します。検索バーに、ウィジェットのタイトルを入力します。ウィジェットをダッシュボードにドラッグアンドドロップします。

デフォルトで表示されるウィジェット

デフォルトでは、[概要] ダッシュボードには以下のウィジェットが表示されます。

セキュリティ標準

最新の概要セキュリティスコアと Security Hub 標準ごとのセキュリティスコアが表示されます。セキュリティスコア (0～100%) は、有効になっているすべてのコントロールに対する合格したコントロールの割合を表します。スコアの詳細については、「セキュリティスコアの計算方法」を参照してください。このウィジェットは、全体的なセキュリティ体制を把握するのに役立ちます。

最も検出結果の多いアセット

検出結果が最も多いリソース、アカウント、アプリケーションの概要を示します。リストは、検出結果の数によって降順にソートされます。ウィジェットの各タブには、そのカテゴリの上位 6 つの項目が重大度とリソースタイプ別にグループ化されて表示されます。[合計検出結果] 列で数値を選択すると、Security Hub にはアセットの検出結果を表示するページが開きます。このウィジェットは、どのコアアセットに潜在的なセキュリティ脅威があるかをすばやく特定するのに役立ちます。

リージョン別の検出結果

Security Hub が有効になっている AWS リージョンごとの検出結果の総数を、重大度でグループ化して表示します。このウィジェットは、特定のリージョンに影響を与える可能性のあるセキュリティ問題を特定するのに役立ちます。集約リージョンでダッシュボードを開くと、このウィジェットはリンクされたリージョンごとに発生する可能性のあるセキュリティ問題をモニタするのに役立ちます。

最も一般的な脅威タイプ

AWS 環境内で最も一般的な 10 種類の脅威の内訳を示します。これには、権限のエスカレーションや、公開されている認証情報の使用、悪意のある IP アドレスでの通信などの脅威が含まれます。

このデータを表示するには、Amazon GuardDuty が有効になっている必要があります。有効になっている場合は、このウィジェットで脅威の種類を選択して GuardDuty コンソールを開き、この脅威に関連する検出結果を確認します。このウィジェットは、他のセキュリティ問題との関連で潜在的な脅威を評価するのに役立ちます。

エクスプロイトを伴うソフトウェアの脆弱性

AWS 環境内に存在し、エクスプロイトが確認されているソフトウェアの脆弱性の概要を表示します。また、修正できる脆弱性と修正できない脆弱性の内訳を確認することもできます。

このデータを表示するには、Amazon Inspector が有効になっている必要があります。有効になっている場合は、このウィジェットで統計を選択して Amazon Inspector コンソールを開き、脆弱

性に関する詳細を確認します。このウィジェットは、他のセキュリティ問題との関連でソフトウェアの脆弱性を評価するのに役立ちます。

時間の経過に伴う新しい検出結果の数

過去 90 日間の新しい日次検出結果の数の傾向を示します。データを重大度別またはプロバイダー別に分類して、さらに詳しい情報を得ることができます。このウィジェットは、過去 90 日間の特定の時期に検出結果の数が急増または減少したかどうかを把握するのに役立ちます。

最も検出結果の多いリソース

最も多くの検出結果が得られたリソースの概要を、Amazon Simple Storage Service (Amazon S3) バケット、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、AWS Lambda 関数の各リソースタイプ別に分類して表示します。

ウィジェットの各タブは、上記のリソースタイプの 1 つに焦点を当て、最も多くの検出結果を生成した 10 個のリソースインスタンスを一覧表示します。特定のリソースの検出結果を確認するには、リソースインスタンスを選択します。このウィジェットは、共通 AWS リソースに関連するセキュリティ検出結果をトリアージするのに役立ちます。

デフォルトでは非表示のウィジェット

[概要] ダッシュボードでは以下のウィジェットも使用できますが、デフォルトでは非表示になっています。

最も検出結果の多い AMI

最も多くの検出結果が得られた 10 個の Amazon マシンイメージ (AMI) のリストを表示します。このデータは、アカウントで Amazon EC2 が有効になっている場合にのみ利用できます。どの AMI が潜在的なセキュリティリスクをもたらすかを特定するのに役立ちます。

最も検出結果の多い IAM プリンシパル

最も多くの検出結果が得られた 10 人の AWS Identity and Access Management (IAM) ユーザーのリストを表示します。このウィジェットは、管理タスクや請求タスクを実行するのに役立ちます。Security Hub の使用状況に最も影響を与えているユーザーが表示されます。

最も検出結果の多いアカウント (重大度別)

最も多くの検出結果が得られた 10 個のアカウントのグラフを、重大度別にグループ化して表示します。このウィジェットは、分析と対策の取り組みをどのアカウントに集中させるかを判断するのに役立ちます。

最も検出結果の多いアカウント (リソースタイプ別)

最も多くの結果が得られた 10 個のアカウントのグラフを、リソースタイプ別にグループ化して表示します。このウィジェットは、どのアカウントとリソースタイプを分析と対策で優先するかについて判断するのに役立ちます。

インサイト

Security Hub が管理する 5 つのインサイトと、それらによって生成された検出結果の数を一覧表示します。インサイトは、注意が必要な特定のセキュリティ領域を識別します。

AWS 統合から得られた最新の検出結果の数

統合 AWS のサービスの Security Hub で得られた検出結果の数を表示します。また、各統合サービスから最近の検出結果を取得した日時も表示されます。このウィジェットは、複数の AWS のサービスの検出結果データを統合して表示します。ドリルダウンするには、統合サービスを選択します。これにより、そのサービスのコンソールが Security Hub で開きます。

[概要] ダッシュボードのフィルタリング

[概要] ダッシュボードのデータを整理し、自分にとって最も関連性の高いセキュリティデータのみ表示するには、ダッシュボードをフィルタリングします。例えば、アプリケーションチームのメンバーであれば、本稼働環境にある重要なアプリケーション専用のビューを作成できます。セキュリティチームのメンバーであれば、重大度の高い検出結果に焦点を当てるのに役立つ専用ビューを作成するとよいでしょう。[概要] ダッシュボードのデータをフィルタリングするには、ダッシュボードの上にあるフィルターボックスにフィルター条件を入力します。フィルター条件を適用すると、その条件は [インサイト] ウィジェットと [セキュリティ基準] ウィジェット内のデータを除く、ダッシュボード上のすべてのデータに適用されます。

以下のフィールドを使用してデータをフィルタリングできます。

- アカウント名
- アカウント ID
- アプリケーションの Amazon リソースネーム (ARN)
- アプリケーション名
- 製品名 (AWS のサービスまたは Security Hub に検出結果を送信するサードパーティー製品)
- レコードの状態
- リージョン

- リソースタグ
- 緊急度
- ワークフローステータス

デフォルトでは、`Workflow status` が `NOTIFIED` または `NEW`、`Record state` が `ACTIVE` という条件を使用してダッシュボードデータをフィルタリングします。これらの条件は、ダッシュボードの上、フィルターボックスの下に表示されます。これらの条件を削除するには、削除する条件のフィルタートークンで [X] を選択します。

再使用するフィルター条件を適用する場合は、フィルターセットとして保存できます。フィルターセットは一連のフィルター条件であり、[概要] ダッシュボードでデータを確認するときに再適用するために作成し保存します。

> **Note**
>
> アプリケーション ARN、アプリケーション名、リソースタグの各フィールドはフィルターセットの一部として保存できません。

フィルターセットの作成と保存

フィルターセットを作成して保存するには、以下の手順に従います。

フィルターセットを作成して保存するには

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。
2. ナビゲーションペインで 概要 を選択します。
3. [概要] ダッシュボードの上にあるフィルターボックスに、フィルターセットのフィルター条件を入力します。
4. [フィルターをクリア] メニューで、[新しいフィルターセットを保存] を選択します。
5. [フィルターセットを保存] ダイアログボックスで、フィルターセットの名前を入力します。
6. (オプション) [概要] ページを開くたびにこのフィルターセットをデフォルトで使用するには、このオプションを選択してデフォルトビューとして設定します。
7. [Save (保存)] を選択します。

作成して保存したフィルターセットを切り替えるには、[概要] ダッシュボードの上にある [フィルターセットを選択] メニューを使用します。フィルタセットを選択すると、Security Hub はフィルタセットの条件をダッシュボード上のデータに適用します。

フィルターセットの更新または削除

既存のフィルターセットを更新または削除するには、以下の手順を実行します。現在 [概要] ダッシュボードのデフォルトビューとして設定されているフィルターセットを削除すると、デフォルトビューはデフォルトの Security Hub ビューにリセットされます。

フィルターセットを更新または削除するには

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。
2. ナビゲーションペインで 概要 を選択します。
3. [概要] ページの上にある [フィルターセットを選択] メニューで、フィルターセットを選択します。
4. [フィルターをクリア] メニューで、以下のいずれかを実行します。
   - フィルターセットを更新するには、[現在のフィルターセットを更新] を選択します。次に、表示されるダイアログボックスに変更内容を入力します。
   - フィルターセットを削除するには、[現在のフィルターセットを削除] を選択します。次に、表示されたダイアログボックスで、[削除] を選択します。

[概要] ダッシュボードのカスタマイズ

[概要] ダッシュボードはいくつかの方法でカスタマイズできます。ダッシュボードにウィジェットを追加したり、削除したりできます。ダッシュボード上のウィジェットの配置やサイズを変更することもできます。

ダッシュボードをカスタマイズすると、Security Hub は変更をすぐに適用し、新しいダッシュボード設定を保存します。変更内容は、すべての AWS リージョンおよびブラウザでのダッシュボードの表示に適用されます。

[概要] ダッシュボードをカスタマイズするには

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。
2. ナビゲーションペインで 概要 を選択します。

3. 次のいずれかを実行します。

   - ウィジェットを追加するには、ページの右上隅の [ウィジェットを追加] を選択します。検索バーに、追加するウィジェットのタイトルを入力します。次に、ウィジェットを目的の位置にドラッグします。
   - ウィジェットを削除するには、ウィジェットの右上隅にある 3 つのドットを選択します。
   - ウィジェットを移動するには、ウィジェットの左上隅にあるハンドルを選択し、ウィジェットを目的の位置にドラッグします。
   - ウィジェットのサイズを変更するには、ウィジェットの右下隅にあるリサイズハンドルを選択します。ウィジェットの端を、希望のサイズになるまでドラッグします。

後で元の設定に戻すには、ページ上部の [デフォルトのレイアウトにリセット] を選択します。

AWS CloudFormation を使用した Security Hub リソースの作成

AWS Security Hub AWS CloudFormationと統合します。これはリソースのモデル化と設定を支援するサービスで、 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ます。 AWS 必要なすべてのリソース (自動化ルールなど) を記述したテンプレートを作成し、 AWS CloudFormation それらのリソースを自動的にプロビジョニングして構成します。

を使用すると AWS CloudFormation、テンプレートを再利用して Security Hub リソースを一貫して繰り返し設定できます。リソースを一度記述すれば、 AWS アカウント 同じリソースを複数のリージョンやリージョンで何度もプロビジョニングできます。

Security Hub AWS CloudFormation とテンプレート

Security Hub 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 テンプレートがどう機能するのか理解しておく必要があります。テンプレートは、JSON または YAML 形式のテキストファイルです。これらのテンプレートには、 AWS CloudFormation スタックにプロビジョニングするリソースが記述されています。

JSON や YAML に慣れていない場合は、 AWS CloudFormation Designer を使用してテンプレートを使い始めることができます。 AWS CloudFormation 詳細については、「Designer とは AWS CloudFormation」を参照してください。 『AWS CloudFormation ユーザーガイド』の。

次の種類の Security Hub AWS CloudFormation リソースのテンプレートを作成できます。

- Security Hub を有効にする
- 組織の委任されたSecurity Hub 管理者の指定
- セキュリティ標準の有効化
- カスタムインサイトの作成
- 自動化ルールの作成
- サードパーティ製品インテグレーションの購読

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情報については、「AWS CloudFormation ユーザーガイド」の「AWS Security Hub リソースタイプのリファレンス」を参照してください。

詳細はこちら AWS CloudFormation

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ースユーザーガイド

Amazon Simple Notification Service を使用した Security Hub の発表のサブスクライブ

このセクションでは、Amazon Simple Notification Service (Amazon SNS) を使用して AWS Security Hub の発表をサブスクライブし、Security Hub に関する通知を受け取る方法について説明します。

サブスクライブした後、次のイベントに関する通知を受信するようになります (各イベントに対応する `AnnouncementType` を以下に示します)。

- `GENERAL` — Security Hub サービスに関する一般的な通知。
- `UPCOMING_STANDARDS_CONTROLS` — 指定された Security Hub コントロールまたは標準がまもなくリリースされる予定です。このタイプの発表は、リリースに先立って対応と修正のワークフローを準備するのに役立ちます。
- `NEW_REGIONS` – 新たに AWS リージョン で Security Hub がサポートされます。
- `NEW_STANDARDS_CONTROLS` — 新しい Security Hub コントロールまたは標準が追加されました。
- `UPDATED_STANDARDS_CONTROLS` — 既存の Security Hub コントロールまたは標準が更新されました。
- `RETIRED_STANDARDS_CONTROLS` — 既存の Security Hub コントロールまたは標準が廃止されました。
- `UPDATED_ASFF` — AWS Security Finding 形式 (ASFF) の構文、フィールド、または値が更新されました。
- `NEW_INTEGRATION` — 他の AWS サービスまたはサードパーティー製品との新しい統合を利用できるようになりました。
- `NEW_FEATURE` — Security Hub の新しい機能を利用できるようになりました。
- `UPDATED_FEATURE` — Security Hub の既存の機能が更新されました。

Amazon SNS がサポートするすべての形式で通知を使用できます。Security Hub が利用可能なすべての AWS リージョン で、Security Hub の発表をサブスクライブできます。

Amazon SNS トピックにサブスクライブするには、ユーザーは、`Subscribe` 許可が必要です。これは、Amazon SNS ポリシー、IAM ポリシー、またはその両方で実現できます。詳細については、「IAM and Amazon SNS policies together」(IAM と Amazon SNS のポリシーを一緒に) の「Amazon Simple 通知サービス デベロッパーガイド」を参照してください。

> **Note**
>
> Security Hub は、 全体の Security Hub サービスの更新に関する Amazon SNS の発表をサブスクライブしている AWS アカウント に送信します。Security Hub アカウント内の結果に関する通知を受け取るには、「結果の詳細と履歴の管理と確認」を参照してください。

Amazon SNS トピックについて Amazon Simple Queue Service (Amazon SQS) キューをサブスクライブできますが、同じリージョンにある Amazon SNS トピックの Amazon リソースネーム (ARN) を使用する必要があります。詳細については、「Amazon Simple Queue Service デベロッパーガイド」の「チュートリアル: Amazon SNS トピックへの Amazon SQS キューのサブスクライブ」を参照してください。

通知を受信したときに AWS Lambda 関数を使用してイベントを呼び出すこともできます。サンプル関数コードなどの詳細については、「AWS Lambda デベロッパーガイド」の「チュートリアル: Amazon Simple Notification Service での AWS Lambda の使用」を参照してください。

各リージョンの Amazon SNS トピックの ARN は次のとおりです。

AWS リージョン	Amazon SNS トピックの ARN
米国東部 (オハイオ)	`arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements`
米国東部 (バージニア北部)	`arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements`
米国西部 (北カリフォルニア)	`arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements`
米国西部 (オレゴン)	`arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`

AWS リージョン	Amazon SNS トピックの ARN
アフリカ (ケープタウン)	arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements
アジアパシフィック (香港)	arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements
アジアパシフィック (ハイデラバード)	arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements
アジアパシフィック (ジャカルタ)	arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements
アジアパシフィック (ムンバイ)	arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements
アジアパシフィック (大阪)	arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements
アジアパシフィック (ソウル)	arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements
アジアパシフィック (シンガポール)	arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements
アジアパシフィック (シドニー)	arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements

AWS リージョン	Amazon SNS トピックの ARN
アジアパシフィック (東京)	arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements
カナダ (中部)	arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements
中国 (北京)	arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements
中国 (寧夏)	arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements
ヨーロッパ (フランクフルト)	arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements
欧州 (アイルランド)	arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements
ヨーロッパ (ロンドン)	arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements
ヨーロッパ (ミラノ)	arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements
欧州 (パリ)	arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements

AWS リージョン	Amazon SNS トピックの ARN
欧州 (スペイン)	arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements
欧州 (ストックホルム)	arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements
欧州 (チューリッヒ)	arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements
イスラエル (テルアビブ)	arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements
中東 (バーレーン)	arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements
中東 (アラブ首長国連邦)	arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements
南米 (サンパウロ)	arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements
AWS GovCloud (米国東部)	arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements
AWS GovCloud (米国西部)	arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements

メッセージは通常、パーティション内のリージョン間で同じであるため、各パーティションの 1 つのリージョンにサブスクライブすれば、そのパーティションのすべてのリージョンに影響する発表を受け取ることができます。メンバーアカウントに関連する発表は、管理者アカウントではレプリケートされません。その結果、管理者アカウントを含む各アカウントには、各発表のコピーが 1 つだけ存在することになります。Security Hub の発表をサブスクライブするために使用するアカウントを決定できます。

Security Hub の発表をサブスクライブするコストの詳細については、「Amazon SNS 料金」を参照してください。

Security Hub の発表のサブスクライブ (コンソール)

1. Amazon SNS コンソール (https://console.aws.amazon.com/sns/v3/home) を開きます。
2. リージョンのリストで、Security Hub の発表をサブスクライブするリージョンを選択します。この例では、`us-west-2` リージョンを使用します。
3. ナビゲーションペインで、[Subscriptions] (サブスクリプション) を選択して、[Create subscription] (サブスクリプションの作成) を選択します。
4. [Topic ARN] (トピック ARN) ボックスにトピック ARN を入力します。例えば、`arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements` です。
5. [Protocol] (プロトコル) で、Security Hub の発表を受け取る方法を選択します。[Email] (E メール) を選択した場合、[Endpoint] (エンドポイント) で、発表の受信に使用する E メールアドレスを入力します。
6. [Create subscription] (サブスクリプションの作成) を選択します。
7. サブスクリプションを確認します。例えば、E メールプロトコルを選択した場合、指定した E メールに Amazon SNS からサブスクリプションの確認メッセージが送信されます。

Security Hub の発表のサブスクライブ (AWS CLI)

1. 次のコマンドを実行します。

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. サブスクリプションを確認します。例えば、E メールプロトコルを選択した場合、指定した E メールに Amazon SNS からサブスクリプションの確認メッセージが送信されます。

Amazon SNS メッセージ形式

以下の例は、新しいセキュリティコントロールの導入に関する Amazon SNS からの Security Hub の発表を示しています。メッセージの内容は発表のタイプによって異なりますが、形式はすべての発表タイプで同じです。オプションで、発表に関する詳細を指定する Link フィールドを含めることができます。

例: 新しいコントロールに関する Security Hub の発表 (E メールプロトコル)

```
{
"AnnouncementType":"NEW_STANDARDS_CONTROLS",
"Title":"[New Controls] 36 new Security Hub controls added to the AWS Foundational
 Security Best Practices standard",
"Description":"We have added 36 new controls to the AWS Foundational Security Best
 Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3,
 AutoScaling.4, AutoScaling.6), AWS CloudFormation (CloudFormation.1), Amazon
 CloudFront (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23,
 EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon
 Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12),
 Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes
 Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon
 Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3, NetworkFirewall.4,
 NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift
 (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
 (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
 Foundational Security Best Practices standard in an account and configured Security
 Hub to automatically enable new controls, these controls are enabled by default.
 Availability of controls can vary by Region. "
}
```

例: 新しいコントロールに関する Security Hub の発表 (E メール JSON プロトコル)

```
{
  "Type" : "Notification",
  "MessageId" : "d124c9cf-326a-5931-9263-92a92e7af49f",
  "TopicArn" : "arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements",
  "Message" : "{\"AnnouncementType\":\"NEW_STANDARDS_CONTROLS\",\"Title\":\"[New
 Controls] 36 new Security Hub controls added to the AWS Foundational Security Best
 Practices standard\",\"Description\":\"We have added 36 new controls to the AWS
 Foundational Security Best Practices standard. These include controls for Amazon
 Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), AWS CloudFormation
```

```
 (CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud
 (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR)
 (ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5,
 ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon
 Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12,
 ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3,
 NetworkFirewall.4, NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7),
 Amazon Redshift (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
 (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
 Foundational Security Best Practices standard in an account and configured SSecurity
 Hub to automatically enable new controls, these controls are enabled by default.
 Availability of controls can vary by Region. \"}",
  "Timestamp" : "2022-08-04T19:11:12.652Z",
  "SignatureVersion" : "1",
  "Signature" :
 "HTHgNFRYMetCvisulgLM4CVySvK9qCXFPHQDxYl9tuCFQuIrd7YO4m4YFR28XKMgzqrF20YP
+EilipUm2SOTpEEtOTekU5bn74+YmNZfwr4aPFx0vUuQCVOshmHl37hjkiLjhCg/t53QQiLfP7MH
+MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUsOG8yiJVCBEJhJ1yS
+gkwJdhRk2UQab9RcAmE6COK3hRWcjDwqTXz5nR6Ywv1ZqZfLIl7gYKslt+jsyd/k+7kOqGmOJRDr7qhE7H
+7vaGRLOptsQnbW8VmeYnDbahEO8FV+Mp1rpV+7Qg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-56e67fcb41f6fec09b0196692625d385.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements:9d0230d7-d582-451d-9f15-0c32818bf61f"
}
```

AWS Security Hub のセキュリティ

AWS では、クラウドのセキュリティが最優先事項です。セキュリティを最も重視する組織の要件を満たすために構築された AWS のデータセンターとネットワークアーキテクチャは、お客様に大きく貢献します。

セキュリティは、AWS と顧客の間の責任共有です。責任共有モデルでは、この責任が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して説明されています。

- クラウドのセキュリティ - AWS は、AWS クラウドで AWS のサービスを実行するインフラストラクチャを保護する責任を負います。また、AWS は、使用するサービスを安全に提供します。AWS 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が定期的にセキュリティの有効性をテストおよび検証しています。AWS Security Hub 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、「コンプライアンスプログラムによる対象範囲内の AWS のサービス」を参照してください。
- クラウド内のセキュリティ - ユーザーの責任は、使用する AWS のサービスに応じて異なります。また、ユーザーは、データの機密性、企業要件、および適用法令と規制などのその他要因に対する責任も担います。

このドキュメントは、Security Hub を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。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 Security Hub を設定する方法を説明します。Security Hub リソースのモニタリングやセキュリティ確保に役立つ他の AWS サービスの使用方法についても説明します。

トピック

AWS Security Hub でのデータ保護

AWS責任共有モデルは、AWS Security Hub でのデータ保護に適用されます。このモデルで説明されているように、AWS は、AWS クラウド のすべて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があります。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。

データを保護するため、AWS アカウント の認証情報を保護し、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セットアップ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を各ユーザーに付与できます。また、次の方法でデータを保護することをおすすめします。

- 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 が必須です。TLS 1.3 が推奨されます。
- AWS CloudTrail で API とユーザーアクティビティロギングをセットアップします。
- AWS のサービス内でデフォルトである、すべてのセキュリティ管理に加え、AWS の暗号化ソリューションを使用します。
- 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 により AWS にアクセスするときに FIPS 140-2 検証済み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。

顧客の E メールアドレスなどの機密情報やセンシティブ情報は、タグや [Name] (名前) フィールドなどの自由形式の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、AWS CLI、または AWS SDK を利用して Security Hub または他の AWS のサービス のサービスを使用する場合も同様です。タグまたは名前に使用する自由記入欄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。

Security Hub はマルチテナント型サービスを提供します。データ保護を確実に行うために、Security Hub は保管中のデータとコンポーネントサービス間で転送中のデータを暗号化します。

AWS の Identity and Access Management AWS Security Hub

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、誰を認可する (Security Hub リソースの使用を許可する) 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、Security Hub で行う作業によって異なります。

サービスユーザー - ユーザーがジョブを実行するために Security Hub 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そのユーザーに提供されます。作業を行うためにさらに多くの Security Hub の機能を使用する場合、追加の許可が必要になる可能性があります。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。Security Hub の機能にアクセスできない場合は、「AWS Security Hub 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 - お客様が社内の Security Hub リソースを担当している場合は、通常 Security Hub に完全にアクセスすることができます。サービスユーザーがどの Security Hub 機能およびリソースにアクセスする必要があるかを決定するのは管理者の仕事です。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確認して、IAM の基本概念を理解してください。お客様の会社で Security Hub で IAM を利用する方法の詳細については、「と IAM の AWS Security Hub 連携方法」を参照してください。

IAM 管理者 - IAM 管理者は、Security Hub へのアクセスを管理するポリシーの作成方法を詳しく確認する必要がある場合があります。IAM で使用できる Security Hub 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、「Security Hub のアイデンティティベースのポリシーの例」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 AWS のサービス およびリソースへの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のユーザー、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。

と IAM の AWS Security Hub 連携方法

AWS Identity and Access Management (IAM) を使用して へのアクセスを管理する前に AWS Security Hub、Security Hub で使用できる IAM 機能を確認してください。

で使用できる IAM の機能 AWS Security Hub

IAM 機能	Security Hub 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	いいえ
ポリシー条件キー	あり
アクセスコントロールリスト (ACL)	なし
属性ベースのアクセス制御 (ABAC) – ポリシー内のタグ	あり
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

IAM 機能	Security Hub のサポート
サービスリンクロール	あり

Security Hub およびその他の がほとんどの IAM 機能と AWS のサービス 連携する方法の概要については、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。

Security Hub の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。

Security Hub はアイデンティティベースのポリシーをサポートしています。詳細については、「Security Hub のアイデンティティベースのポリシーの例」を参照してください。

Security Hub の Resource=based ポリシー

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。

Security Hub では、リソースベースのポリシーはサポートされていません。IAM ポリシーを Security Hub リソースに直接アタッチすることはできません。

Security Hub のポリシーアクション

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。

Security Hub 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を使用します。

```
securityhub:
```

例えば、Security Hub API の EnableSecurityHubオペレーションに対応するアクションである Security Hub を有効にするアクセス許可をユーザーに付与するには、ポリシーに securityhub:EnableSecurityHubアクションを含めます。ポリシーステートメントには、Action または NotAction 要素を含める必要があります。Security Hub では、このサービスで実行できるタスクを記述する独自のアクションのセットを定義します。

```
"Action": "securityhub:EnableSecurityHub"
```

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。例:

```
"Action": [
      "securityhub:EnableSecurityHub",
      "securityhub:BatchEnableStandards"
```

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もできます。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": "securityhub:Get*"
```

ただしベストプラクティスとして、最小特権 の原則に準拠したポリシーを作成してください。別の言い方をすると、特定タスクの実行にのみ必要とされる権限のみが含まれたポリシーを作成してください。

、、BatchGetStandardsControlAssociationsおよび にアクセスするにはBatchGetSecurityControls、ユーザーが DescribeStandardsControlオペレーションにアクセスできる必要がありますListStandardsControlAssociations。

、、および にアクセスするにはBatchUpdateStandardsControlAssociations、ユーザーが UpdateStandardsControlsオペレーションにアクセスできる必要がありますUpdateSecurityControl。

Security Hub アクションのリストについては、「サービス認証リファレンス」の「 で定義されるアクション AWS Security Hub」を参照してください。Security Hub アクションを指定するポリシーの例については、「」を参照してくださいSecurity Hub のアイデンティティベースのポリシーの例。

リソース

ポリシーリソースに対するサポート	なし

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": "*"
```

Security Hub では、次のリソースタイプを定義します。

- [Hub] (ハブ)
- 製品
- クロスリージョンアグリゲータとも呼ばれるアグリゲータの検索
- 自動化ルール
- 設定ポリシー

ARN を使用して、ポリシーでこれらのタイプのリソースを指定できます。

Security Hub リソースタイプのリストと各リソースの ARN 構文については、「サービス認証リファレンス」の「 で定義されるリソースタイプ AWS Security Hub」を参照してください。リソースのタイプごとに指定できるアクションについては、「サービス認証リファレンス」の「 で定義されるアクション AWS Security Hub」を参照してください。リソースを指定するポリシーの例については、Security Hub のアイデンティティベースのポリシーの例を参照してください。

Security Hub のポリシー条件キー

サービス固有のポリシー条件キーのサポート	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。

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。

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 IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。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。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。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。

Security Hub の条件キーのリストについては、「サービス認証リファレンス」の「 の条件キー AWS Security Hub」を参照してください。条件キーを使用できるアクションとリソースについては、「 で定義されるアクション AWS Security Hub」を参照してください。条件キーを使用するポリシーの例については、「Security Hub のアイデンティティベースのポリシーの例」を参照してください。

Security Hub ACLs)

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。

Security Hub は ACLsをサポートしていません。つまり、ACL を Security Hub リソースにアタッチすることはできません。

Security Hub での属性ベースのアクセスコントロール (ABAC)

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。

Security Hub リソースにタグをアタッチできます。ポリシーの `Condition`要素でタグ情報を指定することで、 リソースへのアクセスを制御することもできます。

Security Hub 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 Security Hub リソースのタグ付け。タグに基づいてリソースへのアクセスを制御するアイデンティティベースのポリシーの例については、Security Hub のアイデンティティベースのポリシーの例をご参照ください。

Security Hub で一時的なセキュリティ認証情報を使用する

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。

一時的な認証情報を使用して、フェデレーションでサインインする、IAM ロールを引き受ける、またはクロスアカウントロールを引き受けることができます。一時的なセキュリティ認証情報を取得するには、 AssumeRoleや などの AWS STS API オペレーションを呼び出しますGetFederationToken。

Security Hub は、一時的な認証情報の使用をサポートしています。

Security Hub の転送アクセスセッション

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。

例えば、Security Hub を と AWS Organizations 統合 AWS のサービス し、Organizations 内の組織の委任された Security Hub 管理者アカウントを指定すると、Security Hub はダウンストリームに FAS リクエストを行います。

その他のタスクでは、Security Hub はサービスにリンクされたロールを使用してユーザーに代わってアクションを実行します。このロールの詳細については、Security Hub のサービスにリンクされたロールを参照してください。

Security Hub のサービスロール

Security Hub はサービスロールを引き受けたり使用したりしません。ユーザーに代わってアクションを実行するために、Security Hub はサービスにリンクされたロールを使用します。このロールの詳細については、Security Hub のサービスにリンクされたロール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、Security Hub の使用で運用上の問題が発生する可能性があります。Security Hub 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。

Security Hub のサービスにリンクされたロール

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。

Security Hub は、サービスにリンクされたロールを使用してユーザーに代わってアクションを実行します。このロールの詳細については、Security Hub のサービスにリンクされたロールを参照してください。

Security Hub のアイデンティティベースのポリシーの例

デフォルトでは、ユーザーおよびロールには、Security Hub リソースを作成または変更する許可はありません。AWS Management Console、AWS CLI、または AWS API を使用してタスクを実行することもできません。IAM 管理者は、指定されたリソースで特定の API 操作を実行するための許可をユーザーとロールに付与する IAM ポリシーを作成する必要があります。続いて、管理者はそれらのアクセス許可が必要なユーザーまたはグループにそのポリシーをアタッチします。

JSON ポリシードキュメントのこれらの例を使用して、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「JSON タブでのポリシーの作成」を参照してください。

トピック

ポリシーのベストプラクティス

ID ベースのポリシーは、あるユーザーがアカウント内で Security Hub リソースを作成、アクセス、または削除できるどうかを決定します。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 マネージドポリシーを使用して開始し、最小特権の権限に移行する – ユーザーとワークロードへの権限の付与を開始するには、多くの一般的なユースケースのために権限を付与する AWS マネージドポリシーを使用します。これらは AWS アカウントで使用できます。ユースケースに応じた AWS カスタマーマネージドポリシーを定義することで、権限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「AWS ジョブ機能の管理ポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで権限を設定するときは、タスクの実行に必要な権限のみを付与します。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、最小特権権限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 でのポリシーと権限」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。また、AWS CloudFormation などの特定の AWS のサービス を介して使用する場合、条件を使用して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。詳細については、「IAM ユーザーガイド」の「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 - AWS アカウント内の IAM ユーザーまたはルートユーザーを要求するシナリオがある場合は、セキュリティを強化するために MFA をオンにします。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。

Security Hub コンソールの使用

AWS Security Hub コンソールにアクセスするには、最小限の許可セットが必要です。これらの許可は、AWS アカウント の Security Hub リソースの一覧と詳細を表示できるものである必要があります。最小限必要なアクセス許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) ではコンソールが意図したとおりに機能しません。

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権限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を許可します。

これらのユーザーとロールが Security Hub コンソールを使用できるようにするには、次の AWS 管理ポリシーもエンティティにアタッチします。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」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
```

```
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

例 : ユーザーにそれぞれのアクセス権限の表示を許可する

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 か AWS API を使用してプログラム的に、このアクションを完了する権限が含まれています。

```
{
    "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": "*"
```

```
        }
    ]
}
```

例: ユーザーに設定ポリシーの作成と管理を許可する

この例では、ユーザーが設定ポリシーを作成、表示、更新、削除できるようにする IAM ポリシーを作成する方法を示します。このポリシー例では、ポリシーの関連付けの開始、停止、および表示もユーザーに許可します。この IAM ポリシーが機能するには、ユーザーは組織の委任 Security Hub 管理者である必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateConfigurationPolicy",
                "securityhub:UpdateConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetConfigurationPolicy",
                "securityhub:ListConfigurationPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:DeleteConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicyAssociation",
            "Effect": "Allow",
```

```
            "Action": [
                "securityhub:BatchGetConfigurationPolicyAssociations",
                "securityhub:GetConfigurationPolicyAssociation",
                "securityhub:ListConfigurationPolicyAssociations"
            ],
            "Resource": "*"
        },
        {
            "Sid": "UpdateConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:StartConfigurationPolicyAssociation",
                "securityhub:StartConfigurationPolicyDisassociation"
            ],
            "Resource": "*"
        }
    ]
}
```

例: ユーザーに結果の表示を許可する

この例では、Security Hub の検出結果の表示をユーザーに許可する IAM ポリシーを作成する方法を示します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

例: ユーザーに自動化ルールの作成と管理を許可する

この例では、ユーザーが Security Hub 自動化ルールを作成、表示、更新、削除できるようにする IAM ポリシーを作成する方法を示します。この IAM ポリシーが機能するには、ユーザーが Security

Hub 管理者である必要があります。例えば、ユーザーに自動化ルールの表示のみを許可するなど、アクセス許可を制限するには、作成、更新、削除のアクセス許可を削除できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateAutomationRule",
                "securityhub:BatchUpdateAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetAutomationRules",
                "securityhub:ListAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchDeleteAutomationRules"
            ],
            "Resource": "*"
        }
    ]
}
```

Security Hub のサービスにリンクされたロール

AWS Security Hub は、 という名前の 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AWSServiceRoleForSecurityHub。このサービスにリンクされたロールは、Security Hub に直接リンクされた IAM ロールです。これは Security Hub によって事前定義されており、Security Hub がユーザーに代わって他の を呼び出しAWS のサービス、AWS リソースをモニタリングするために必要なすべてのアクセス許可が含まれています。Security Hub

は、Security Hub AWS リージョンが利用可能なすべての で、この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を使用することで、必要な許可を手動で追加する必要がなくなるため、Security Hub の設定が簡単になります。Security Hub は、サービスにリンクされたロールの許可を定義します。その許可が特別に定義されていない限り、Security Hub のみがそのロールを引き受けます。定義される許可には、信頼ポリシーや許可ポリシーなどがあり、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスにリンクされたロールの詳細を表示するには、Security Hub コンソールの [設定] ページで [一般] を選択し、次に [サービス権限の表示] を選択します。

Security Hub のサービスにリンクされたロールの削除は、それが有効になっているすべてのリージョンで Security Hub を無効にした後でのみ行うことができます。これにより、アクセスに必要な許可を誤って削除してしまうことがなくなり、Security Hub リソースは保護されます。

サービスにリンクされたロールをサポートするその他のサービスについては、「IAM ユーザーガイド」の「IAM と連携する AWS のサービス」を参照の上、[Service-Linked Role] (サービスにリンクされたロール) 列が [Yes] (はい) になっているサービスを確認してください。サービスのサービスにリンクされたロールに関するドキュメントを表示するには、[YES] (はい) となっているリンクを選択します。

トピック

- Security Hub のサービスにリンクされたロールの許可
- Security Hub のサービスにリンクされたロールの作成
- Security Hub 向けのサービスにリンクされたロールの編集
- Security Hub 向けのサービスにリンクされたロールの削除

Security Hub のサービスにリンクされたロールの許可

Security Hub では、`AWSServiceRoleForSecurityHub` 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。これは AWS Security Hub がリソースにアクセスする際に必要となる、サービスにリンクされたロールです。サービスにリンクされたロールにより、Security Hub が他の AWS のサービス から検出結果を受け取り、コントロールのセキュリティチェックを実行するために必要な AWS Config インフラストラクチャを構成できるようになります。

`AWSServiceRoleForSecurityHub` サービスにリンクされたロールは、ロールの引き受けについて以下のサービスを信頼します。

- securityhub.amazonaws.com

AWSServiceRoleForSecurityHub サービスにリンクされたロールは、マネージドポリシーである AWSSecurityHubServiceRolePolicy を使用します。

IAM アイデンティティ (ロール、グループ、ユーザーなど) に、サービスにリンクされたロールの作成、編集、削除を許可する設定をする必要があります。AWSServiceRoleForSecurityHub サービスにリンクされたロールを適切に作成するには、Security Hub を使用する IAM アイデンティティに、必要な許可が付与されている必要があります。必要なアクセス許可を付与するには、次のポリシーをロール、グループ、またはユーザーにアタッチします。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Security Hub のサービスにリンクされたロールの作成

Security Hub を初めて有効にする場合や、過去に Security Hub を有効にしていなかったサポート対象リージョンで Security Hub を有効にする場合は、AWSServiceRoleForSecurityHub 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。IAM コンソール、IAM CLI、あるいは IAM API を使って、AWSServiceRoleForSecurityHub サービスにリンクされたロールを手動で作成することもできます。

> **Important**
>
> Security Hub 管理者アカウント用に作成されたサービスにリンクされたロールは、Security Hub メンバーアカウントには適用されません。

IAM ロールを手動で作成する方法の詳細は、「IAM ユーザーガイド」の「サービスにリンクされたロールを作成する」を参照してください。

Security Hub 向けのサービスにリンクされたロールの編集

Security Hub では、AWSServiceRoleForSecurityHub サービスにリンクされたロールの編集は許可されていません。サービスにリンクされた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 を使用してロールの説明の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの編集」を参照してください。

Security Hub 向けのサービスにリンクされたロールの削除

サービスにリンクされたロールを必要とする機能またはサービスが不要になった場合には、その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。

> **Important**
>
> AWSServiceRoleForSecurityHub のサービスにリンクされたロールを削除するには、まずそれが有効になっているすべてのリージョンで Security Hub を無効にしておく必要があります。
> サービスにリンクされたロールを削除しようとしたときに、Security Hub が無効になっていない場合、削除することはできません。詳細については、「Security Hub を無効にする」を参照してください。

Security Hub を無効にすると、AWSServiceRoleForSecurityHub のサービスにリンクされたロールは自動的に削除されません。Security Hub を再度有効にすると、既存の AWSServiceRoleForSecurityHub サービスにリンクされたロールが使用されるようになります。

IAM を使用してサービスにリンクされたロールを手動で削除するには

AWSServiceRoleForSecurityHub サービスにリンクされたロールを削除するには、IAM コンソール、IAM CLI、または IAM API を使用します。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの削除」を参照してください。

AWSAWS Security Hub の マネージドポリシー

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対する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、ロールへの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。 は、新しい AWS のサービス 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 マネージドポリシー」を参照してください。

AWS 管理ポリシー: AWSSecurityHubFullAccess

AWSSecurityHubFullAccess ポリシーは IAM アイデンティティにアタッチできます。

このポリシーにより、プリンシパルが Security Hub のすべてのアクションに完全にアクセスすることが許可される、管理者許可が付与されます。このポリシーは、アカウントの Security Hub を手動で有効にする前に、プリンシパルに添付する必要があります。例えば、これらの許可を持つプリンシパルは、結果のステータスを表示および更新できます。カスタムインサイトを設定し、統合を有効にできます。これにより、標準とコントロールを有効または無効にすることができます。管理者アカウントのプリンシパルは、メンバーアカウントを管理することもできます。

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。

- securityhub - すべての Security Hub アクションへの完全なアクセスをプリンシパルに許可します。

- guardduty — プリンシパルが Amazon のアカウントステータスに関する情報を取得できるようにします GuardDuty。
- iam - サービスにリンクされたロールの作成をプリンシパルに許可します。
- inspector – Amazon Inspector のアカウントステータスに関する情報の取得をプリンシパルに許可します。
- pricing — プリンシパルが AWS のサービス および 製品の料金表を取得できるようにします。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecurityHubAllowAll",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Sid": "SecurityHubServiceLinkedRole",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        },
        {
            "Sid": "OtherServicePermission",
            "Effect": "Allow",
            "Action": [
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "inspector2:BatchGetAccountStatus",
                "pricing:GetProducts"
            ],
            "Resource": "*",
        }
    ]
}
```

Security Hub マネージドポリシー: AWSSecurityHubReadOnlyAccess

AWSSecurityHubReadOnlyAccess ポリシーは IAM アイデンティティにアタッチできます。

このポリシーは、ユーザーが Security Hub の情報を確認できるようにするための読み取り専用の許可を付与します。このポリシーが添付されたプリンシパルは、Security Hub で更新を実行できません。例えば、これらの許可を持つプリンシパルは、アカウントに関連付けられた結果のリストを表示できますが、結果のステータスを変更することはできません。インサイトの結果を表示することはできますが、カスタムインサイトを作成したり設定したりすることはできません。コントロールや製品統合を設定することはできません。

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。

- securityhub - ユーザーは、アイテムのリストまたはアイテムに関する詳細を返すアクションを実行することができます。これには、Get、List、または Describe で始まる API オペレーションが含まれます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSSecurityHubReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "securityhub:Get*",
                "securityhub:List*",
                "securityhub:BatchGet*",
                "securityhub:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS マネージドポリシー: AWSSecurityHubOrganizationsAccess

AWSSecurityHubOrganizationsAccess ポリシーは IAM ID にアタッチできます。

このポリシーは AWS Organizations 、Security Hub と Organizations の統合をサポートするために必要な管理アクセス許可を に付与します。

これらの許可により、組織管理アカウントで Security Hub の委任された管理者アカウントを指定できます。また、委任された Security Hub 管理者アカウントで、組織アカウントをメンバーアカウントとして有効にすることもできます。

このポリシーでは、Organizations に対する許可のみが提供されます。組織管理アカウントと委任された Security Hub 管理者アカウントには、Security Hub の関連するアクションに対する許可も必要です。これらの許可は、AWSSecurityHubFullAccess マネージドポリシーを使用して付与することができます。

許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- organizations:ListAccounts - 組織に属するアカウントリストの取得をプリンシパルに許可します。
- organizations:DescribeOrganization - 組織に関する情報の取得をプリンシパルに許可します。
- organizations:ListRoots - 組織ルートの一覧表示をプリンシパルに許可します。
- organizations:ListDelegatedAdministrators - 組織の委任管理者の一覧表示をプリンシパルに許可します。
- organizations:ListAWSServiceAccessForOrganization – 組織が使用する を一覧表示することをプリンシパル AWS のサービス に許可します。
- organizations:ListOrganizationalUnitsForParent - 親 OU の子組織単位 (OU) の一覧表示をプリンシパルに許可します。
- organizations:ListAccountsForParent - 親 OU の子アカウントの一覧表示をプリンシパルに許可します。
- organizations:DescribeAccount - 組織内のアカウントに関する情報の取得をプリンシパルに許可します。
- organizations:DescribeOrganizationalUnit - 組織内の OU に関する情報の取得をプリンシパルに許可します。
- organizations:DescribeOrganization - 組織設定に関する情報の取得を、プリンシパルに許可します。
- organizations:EnableAWSServiceAccess - Security Hub と Organizations の統合の有効化を、プリンシパルに許可します。

- organizations:RegisterDelegatedAdministrator - Security Hub の委任された管理者アカウントを指定することを、プリンシパルに許可します。
- organizations:DeregisterDelegatedAdministrator - Security Hub の委任された管理者アカウントを削除することを、プリンシパルに許可します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OrganizationPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:ListRoots",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAccountsForParent",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganizationalUnit"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationPermissionsEnable",
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "securityhub.amazonaws.com"
                }
            }
        },
        {
            "Sid": "OrganizationPermissionsDelegatedAdmin",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator"
            ],
```

```
            "Resource": "arn:aws:organizations::*:account/o-*/*",
            "Condition": {
            "StringEquals": {
                "organizations:ServicePrincipal": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

AWS 管理ポリシー: AWSSecurityHubServiceRolePolicy

IAM エンティティに AWSSecurityHubServiceRolePolicy をアタッチすることはできません。このポリシーは、ユーザーに代わって Security Hub がアクションを実行することを許可するサービスにリンクされたロールに添付されます。詳細については、「the section called “サービスにリンクされたロール”」を参照してください。

このポリシーは、サービスにリンクされたロールに管理許可を付与し、Security Hub コントロールのセキュリティチェックを実行できるようにします。

許可の詳細

このポリシーには以下を実行するための許可が含まれています。

- cloudtrail – CloudTrail 証跡に関する情報を取得します。
- cloudwatch – 現在の CloudWatch アラームを取得します。
- logs – CloudWatch ログのメトリクスフィルターを取得します。
- sns - SNS トピックのサブスクリプションリストを取得します。
- config – 設定レコーダー、リソース、および AWS Config ルールに関する情報を取得します。また、サービスにリンクされたロールに AWS Config ルールの作成と削除、およびルールに対する評価の実行も許可します。
- iam - アカウントの認証情報レポートの取得と生成を実行します。
- organizations — 組織のアカウントおよび組織単位 (OU) 情報を取得します。
- securityhub — Security Hub サービス、標準およびコントロールの設定方法に関する情報を取得します。
- tag— リソースタグに関する情報を取得します。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecurityHubServiceRolePermissions",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:GetEventSelectors",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "logs:DescribeMetricFilters",
                "sns:ListSubscriptionsByTopic",
                "config:DescribeConfigurationRecorders",
                "config:DescribeConfigurationRecorderStatus",
                "config:DescribeConfigRules",
                "config:DescribeConfigRuleEvaluationStatus",
                "config:BatchGetResourceConfig",
                "config:SelectResourceConfig",
                "iam:GenerateCredentialReport",
                "organizations:ListAccounts",
                "config:PutEvaluations",
                "tag:GetResources",
                "iam:GetCredentialReport",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListChildren",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "securityhub:BatchDisableStandards",
                "securityhub:BatchEnableStandards",
                "securityhub:BatchUpdateStandardsControlAssociations",
                "securityhub:BatchGetSecurityControls",
                "securityhub:BatchGetStandardsControlAssociations",
                "securityhub:CreateMembers",
                "securityhub:DeleteMembers",
                "securityhub:DescribeHub",
                "securityhub:DescribeOrganizationConfiguration",
                "securityhub:DescribeStandards",
                "securityhub:DescribeStandardsControls",
                "securityhub:DisassociateFromAdministratorAccount",
                "securityhub:DisassociateMembers",
                "securityhub:DisableSecurityHub",
                "securityhub:EnableSecurityHub",
```

```
                "securityhub:GetEnabledStandards",
                "securityhub:ListStandardsControlAssociations",
                "securityhub:ListSecurityControlDefinitions",
                "securityhub:UpdateOrganizationConfiguration",
                "securityhub:UpdateSecurityControl",
                "securityhub:UpdateSecurityHubConfiguration",
                "securityhub:UpdateStandardsControl",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SecurityHubServiceRoleConfigPermissions",
            "Effect": "Allow",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:GetComplianceDetailsByConfigRule"
            ],
            "Resource": "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
        },
        {
            "Sid": "SecurityHubServiceRoleOrganizationsPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "securityhub.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

AWS マネージドポリシーに対する Security Hub の更新

Security Hub の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。このページの変更に関する自動通知について

は、Security Hub の [Document history] (ドキュメントの履歴) 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
AWSSecurityHubFullAccess – 既存のポリシーの更新	Security Hub は、 AWS のサービス および 製品の料金詳細を取得するようにポリシーを更新しました。	2024 年 4 月 24 日
AWSSecurityHubReadOnlyAccess – 既存のポリシーの更新	Security Hub は、 `Sid`フィールドを追加してこの管理ポリシーを更新しました。	2024 年 2 月 22 日
AWSSecurityHubFullAccess – 既存のポリシーの更新	Security Hub はポリシーを更新し、アカウントで Amazon GuardDuty と Amazon Inspector が有効になっているかどうかを判断できるようにしました。これにより、お客様は複数の からセキュリティ関連情報をまとめることができます AWS のサービス。	2023 年 11 月 16 日
AWSSecurityHubOrganizationsAccess – 既存のポリシーの更新	Security Hub は、 AWS Organizations 委任管理者機能への読み取り専用アクセスを許可する追加の権限を付与するようにポリシーを更新しました。これには、ルート、組織単位 (OU)、アカウント、組織構造、およびサービスアクセスなどの詳細が含まれます。	2023 年 11 月 16 日

変更	説明	日付
AWSSecurityHubServiceRolePolicy – 既存ポリシーへの更新	Security Hub で `BatchGetSecurityControls` 、`DisassociateFromAdministratorAccount` 、および `UpdateSecurityControl` アクセス許可が追加され、カスタマイズ可能なセキュリティコントロールプロパティの読み取りおよび更新を行うようになりました。	2023 年 11 月 26 日
AWSSecurityHubServiceRolePolicy – 既存ポリシーへの更新	Security Hub は、`tag:GetResources` 調査結果に関連するリソースタグを読み取る権限を追加しました。	2023 年 11 月 7 日
AWSSecurityHubServiceRolePolicy – 既存ポリシーへの更新	Security Hub は、コントロールの有効化ステータスに関する情報を取得する `BatchGetStandardsControlAssociations` アクセス許可を標準に追加しました。	2023 年 9 月 27 日
AWSSecurityHubServiceRolePolicy – 既存ポリシーへの更新	Security Hub に AWS Organizations 、データを取得し、標準やコントロールなどの Security Hub 設定を読み取って更新するための新しいアクセス許可が追加されました。	2023 年 9 月 20 日

変更	説明	日付
AWSSecurityHubServiceRolePolicy - 既存のポリシーを更新する	Security Hub が既存の config:DescribeConfigRuleEvaluationStatus 許可をポリシー内の別のステートメントに移動しました。これにより、config:DescribeConfigRuleEvaluationStatus 許可がすべてのリソースに適用されます。	2023 年 3 月 17 日
AWSSecurityHubServiceRolePolicy - 既存のポリシーを更新する	Security Hub が既存の config:PutEvaluations 許可をポリシー内の別のステートメントに移動しました。これにより、config:PutEvaluations 許可がすべてのリソースに適用されます。	2021 年 7 月 14 日
AWSSecurityHubServiceRolePolicy - 既存のポリシーを更新する	Security Hub は、サービスにリンクされたロールから評価結果を AWS Configに送信することを許可する新しい許可を追加しました。	2021 年 6 月 29 日
AWSSecurityHubServiceRolePolicy – マネージドポリシーのリストに追加されました	Security Hub サービスにリンクされたロール AWSSecurityHubServiceRolePolicyで使用される マネージドポリシー に関する情報を追加しました。	2021 年 6 月 11 日

変更	説明	日付
AWSSecurityHubOrganizationsAccess – 新しいポリシー	Security Hub に、Security Hub と Organizations との統合に必要な許可を付与する新しいポリシーが追加されました。	2021 年 3 月 15 日
Security Hub で変更の追跡が開始されました	Security Hub が AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 3 月 15 日

AWS Security Hub ID とアクセスのトラブルシューティング

次の情報は、Security Hub 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

- Security Hub でアクションを実行することが認可されていない
- iam を実行する権限がありません。PassRole
- Security Hub にプログラム的にアクセスしたい
- 管理者として Security Hub へのアクセスを他のユーザーに許可したい
- 自分の 以外のユーザーに Security Hub リソース AWS アカウント へのアクセスを許可したい

Security Hub でアクションを実行することが認可されていない

がアクションを実行する権限がないと AWS Management Console 通知した場合は、管理者に連絡してサポートを依頼する必要があります。管理者は、サインイン認証情報を提供した担当者です。

以下の例のエラーは、mateojackson ユーザーがコンソールを使用して、######の詳細を表示しようとしているが、 securityhub:*GetWidget* アクセス許可がない場合に発生します。

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

この場合、Mateo は、`securityhub:GetWidget` アクションを使用して `my-example-widget` リソースへのアクセスが許可されるように、管理者にポリシーの更新を依頼します。

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 Security Hub にロールを渡すことができ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 Security Hub 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。

Security Hub にプログラム的にアクセスしたい

ユーザーが の AWS 外部で を操作する場合は、プログラムによるアクセスが必要です AWS Management Console。プログラムによるアクセスを許可する方法は、 にアクセスするユーザーのタイプによって異なります AWS。

ユーザーにプログラマチックアクセス権を付与するには、以下のいずれかのオプションを選択します。

プログラマチックアクセス権を必要とするユーザー	目的	方法
ワークフォースアイデンティティ (IAM Identity Center で管理されているユーザー)	一時的な認証情報を使用して、、 AWS SDKs AWS CLI、または AWS APIs。	使用するインターフェイス用の手引きに従ってください。 • については AWS CLI、「 ユーザーガイド」の AWS CLI 「 を使用するための の設定 AWS IAM Identity CenterAWS Command Line Interface 」を参照してください。 • AWS SDKs 、ツール、AWS APIs「 SDK とツールのリファレンスガイド」の「IAM Identity Center 認証」を参照してください。AWS SDKs
IAM	一時的な認証情報を使用して、、 AWS SDKs AWS CLI、または AWS APIs。	「IAM ユーザーガイド」の「 AWS リソースでの一時的な認証情報の使用」の手順に従います。
IAM	(非推奨) 長期認証情報を使用して、、AWS SDKs AWS CLI、または AWS APIs。	使用するインターフェイス用の手引きに従ってください。 • については AWS CLI、「 AWS Command Line Interface ユーザーガイド」の「IAM ユーザー認証情報を使用した認証」を参照してください。 • AWS SDKs「 SDK とツールのリファレンスガイド」の「長期的な認証情報を使

プログラマチックアクセス権を必要とするユーザー	目的	方法
		用した認証」を参照してください。 AWS SDKs • AWS APIsユーザーガイド」の「IAM ユーザーのアクセスキーの管理」を参照してください。

管理者として Security Hub へのアクセスを他のユーザーに許可したい

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。

自分の 以外のユーザーに Security Hub 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。

- Security Hub でこれらの機能がサポートされるかどうかを確認するには、「と IAM の AWS Security Hub 連携方法」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。

AWS Security Hub のコンプライアンス検証

サードパーティーの監査者は、複数の AWS Security Hub コンプライアンスプログラムの一環として AWS のセキュリティとコンプライアンスを評価します。これらのプログラムには、SOC、PCI、FedRAMP、HIPAA などが含まれます。

特定のコンプライアンスプログラムの対象範囲に含まれる AWS のサービスのリストについては、「コンプライアンスプログラムによる対象範囲内の AWS のサービス」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。

AWS Artifact 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。詳細については、「AWS Artifact のレポートのダウンロード」を参照してください。

Security Hub を使用する際のユーザーのコンプライアンス責任は、ユーザーのデータの機密性や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。AWS では、コンプライアンスに役立つ以下のリソースを提供しています。

- 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、機密性とコンプライアンスに焦点を当てたベースライン環境を AWS にデプロイするためのステップが示されています。
- AWS コンプライアンスのリソース - ワークブックとお客様の業界や所在地に適用される場合があるガイドのコレクション。

- AWS Config - この AWS のサービスでは、自社プラクティス、業界ガイドライン、および規制に対するリソースの設定の準拠状態を評価します。
- AWS Security Hub - この AWS サービスでは、AWS 内のセキュリティ状態を包括的に表示しており、セキュリティ業界の標準およびベストプラクティスへの準拠を確認するのに役立ちます。

AWS Security Hub の耐障害性

AWS のグローバルインフラストラクチャは AWS リージョン とアベイラビリティーゾーンを中心として構築されます。リージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立および隔離されたアベイラビリティーゾーンがあります。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 と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。

AWS Security Hub 内のインフラストラクチャセキュリティ

マネージドサービスである AWS Security Hub 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 AWS がインフラストラクチャ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 フレームワーク」の「インフラストラクチャ保護」を参照してください。

AWS が公開した API コールを使用して、ネットワーク経由で Security Hub 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 が必須です。TLS 1.3 が推奨されます。
- DHE (Ephemeral Diffie-Hellman) や ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) などの Perfect Forward Secrecy (PFS) を使用した暗号スイート。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 ServiceAWS 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。

AWS Security Hub とインターフェース VPC エンドポイント (AWS PrivateLink)

VPC と AWS Security Hub とのプライベート接続を確立するには、インターフェイス VPC エンドポイントを作成します。インターフェイスエンドポイントは AWS PrivateLink テクノロジーを利用しています。このテクノロジーは Security Hub API にプライベートにアクセスでき、インターネットゲートウェイ、NAT デバイス、VPN 接続、AWS Direct Connect 接続のいずれも必要としません。VPC のインスタンスは、パブリック IP アドレスがなくても Security Hub API と通信できます。VPC と Security Hub との間のトラフィックは、Amazon 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 つ以上の Elastic Network Interface によって表されます。

詳細については、「AWS PrivateLink 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。

Security Hub VPC エンドポイントに関する考慮事項

Security Hub 用のインターフェース VPC エンドポイントを設定する前に、「AWS PrivateLink 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」の内容を確認してください。

Security Hub では、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ています。

> **Note**
>
> Security Hub では、アジアパシフィック (大阪) リージョンで VPC エンドポイントがサポートされていません。

Security Hub 用のインターフェイス VPC エンドポイントの作成

Security Hub サービス用の VPC エンドポイントを作成するには、Amazon VPC コンソールまたは AWS Command Line Interface (AWS CLI) を使用できます。詳細については、「AWS PrivateLink 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。

Security Hub 用の VPC エンドポイントを作成するには、次のサービス名を使用します。

- com.amazonaws.*region*.securityhub

エンドポイントのプライベート DNS を有効にすると、リージョンのデフォルト DNS 名 (`securityhub.us-east-1.amazonaws.com` など) を使用して、Security Hub への API リクエストを実行できるようになります。

詳細については、「AWS PrivateLink 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。

Security Hub 用の VPC エンドポイントポリシーの作成

VPC エンドポイントに Security Hub へのアクセスをコントロール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、「AWS PrivateLink 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: Security Hub アクションの VPC エンドポイントポリシー

以下は、Security Hub のエンドポイントポリシーの例です。このポリシーは、エンドポイントに添付されると、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 Security Hub アクションへのアクセスが許可されます。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

共有サブネット

自分と共有されているサブネットで VPC エンドポイントを作成、説明、変更、または削除することはできません。ただし、VPC エンドポイントを使用することはできます。VPC 共有の詳細については、「Amazon VPC ユーザーガイド」の「VPC を他のアカウントと共有する」を参照してください。

AWS CloudTrail を使用した AWS Security Hub API コールのログ記録

AWS Security Hub は AWS CloudTrail という、Security Hub のユーザー、ロール、または AWS サービスによって実行されたアクションを記録するサービスと統合しています。CloudTrail は、Security Hub の API コールをイベントとしてキャプチャします。キャプチャされたコールには、Security Hub コンソールからのコールと、Security Hub API オペレーションへのコードコールが含まれます。追跡を作成すると、Security Hub のイベントなどを含んだ Amazon S3 バケットへの CloudTrail イベントの継続的な送信を有効にすることができます。追跡を設定しない場合でも、CloudTrail コンソールの [Event history] (イベント履歴) で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、Security Hub に対して実行されたリクエストや、そのリクエストが発信された IP アドレス、リクエストの実行者、リクエストの実行日時、およびその他の詳細情報を特定できます。

設定や有効化の方法など、CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

CloudTrail での Security Hub 情報

CloudTrail は、AWS アカウントを作成すると、その中で有効になります。サポートされているイベントアクティビティが Security Hub で発生すると、そのアクティビティは [Event history] (イベント履歴) の他の AWS サービスのイベントと共に、CloudTrail イベントに記録されます。最近のイベントは、アカウントで表示、検索、ダウンロードできます。詳細については、「CloudTrail イベント履歴でのイベントの表示」を参照してください。

Security Hub のイベントなど、アカウントのイベントを継続的に記録する場合は、追跡を作成します。追跡を有効にすることで、CloudTrail でログファイルを Amazon S3 バケットに送信できるようになります。デフォルトでは、コンソールで追跡を作成すると、すべての AWS リージョンに追跡が適用されます。追跡は、AWS パーティション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、CloudTrail ログで収集したイベントデータをより詳細に分析し、それに基づく対応するためにその他の AWS サービスを設定できます。詳細については、次を参照してください:

- 「証跡作成の概要」
- CloudTrail がサポートされているサービスと統合
- CloudTrail の Amazon SNS 通知の設定

- 「複数のリージョンから CloudTrail ログファイルを受け取る」および「複数のアカウントから CloudTrail ログファイルを受け取る」

Security Hub では、すべての Security Hub API アクションを CloudTrail ログのイベントとしてログ記録することができます。Security Hub オペレーションのリストを表示するには、「Security Hub API リファレンス」を参照してください。

次のアクションのアクティビティが CloudTrail にログ記録されると、`responseElements` の値は `null` に設定されます。これにより、機密性の高い情報が CloudTrail ログに含まれることがなくなります。

- `BatchImportFindings`
- `GetFindings`
- `GetInsights`
- `GetMembers`
- `UpdateFindings`

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報から以下を判断することができます。

- リクエストが、ルートと AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して送信されたか
- リクエストの送信に使用された一時的なセキュリティ認証情報に、ロールとフェデレーティッドユーザーのどちらが使用されたか
- 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 要素」を参照してください。

例: Security Hub ログファイルのエントリ

追跡は、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するように設定できるものです。CloudTrail のログファイルは、単一か複数のログエントリを含みます。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、リクエストのパラメータなどの情報が含まれます。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、CreateInsight アクションを示す CloudTrail ログエントリです。この例では、Test Insight というインサイトが作成されます。ResourceId 属性は、[Group by] (グループ化の条件) アグリゲータとして指定され、このインサイトに対するオプションのフィルターは指定されません。インサイトの詳細については、「AWS Security Hub のインサイト」を参照してください。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJK6U5DS22IAVUI7BW",
        "arn": "arn:aws:iam::012345678901:user/TestUser",
        "accountId": "012345678901",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "TestUser"
    },
    "eventTime": "2018-11-25T01:02:18Z",
    "eventSource": "securityhub.amazonaws.com",
    "eventName": "CreateInsight",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
    "requestParameters": {
        "Filters": {},
        "ResultField": "ResourceId",
        "Name": "Test Insight"
    },
    "responseElements": {
        "InsightArn": "arn:aws:securityhub:us-west-2:0123456789010:insight/custom/
f4c4890b-ac6b-4c26-95f9-e62cc46f3055"
    },
    "requestID": "c0fffccd-f04d-11e8-93fc-ddcd14710066",
    "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "012345678901"
}
```

AWS Security Hub リソースのタグ付け

タグは、特定のタイプの AWS セキュリティハブリソースなど、AWS リソースをオプションで定義および割り当てることができるラベルです。タグを使用することで、目的、所有者、環境、その他の条件など、さまざまな方法でリソースを特定、分類および管理できます。例えば、タグを使用して、リソースを区別したり、特定のコンプライアンス要件やワークフローをサポートするリソースを識別したり、コストを割り当てたりできます。

タグは、自動化ルール、設定ポリシー、Hub リソースという種類の Security Hub リソースに割り当てることができます。

トピック

タグ付けの基本

リソースには、最大 50 個のタグを含めることができます。タグはそれぞれ、1 つの必須タグキーとオプションの 1 つのタグ値で構成されており、どちらもお客様側が定義します。タグキーは、より具体的なタグ値のカテゴリとして機能する一般的なラベルです。タグ値は、タグキーの記述子として機能します。

例えば、環境ごとに異なる自動化ルール (テスト用と本番用の自動化ルール) を作成する場合、それらのルールに `Environment` タグキーを割り当てます。関連するタグ値は、テストアカウントに関連付けられているルール用の `Test` でも、本番用アカウントと OU に関連するルール用の `Prod` でもかまいません。

AWS Security Hub リソースにタグを定義して割り当てる場合は、次のことに注意してください。

- 各リソースには、最大 50 個のタグを設定できます。
- リソースごとに、各タグ キーは一意である必要があり、タグ値は 1 つだけ持つことができます。

- タグのキーと値では、大文字と小文字が区別されます。ベスト プラクティスとして、タグを大文字にする戦略を定義し、その戦略をリソース全体で一貫して実装することをお勧めします。
- タグキーは最大 128 文字 (UTF-8) です。タグ値には最大 256 文字の UTF-8 文字を含めることができます。文字には、文字、数字、スペース、または次の記号を使用できます: _ 。 : / = + - @
- aws: プレフィックスは、AWS が使用するために留保されています。定義したどのタグキーや値にも使用できません。さらに、このプレフィックスを使用するタグキーまたは値を変更または削除することはできません。このプレフィックスを使用するタグは、リソースあたりのタグ数のクォータ (50 個) にはカウントされません。
- 割り当てたタグは、自分の AWS アカウントだけが使用でき、割り当てた AWS リージョンでしか使用できません。
- Security Hub を使用してリソースにタグを割り当てると、タグは該当する AWS リージョンの Security Hub に直接保存されているリソースにのみ適用されます。これは、Security Hub が他の AWS のサービスで作成、使用、管理する関連サポートリソースには適用されません。例えば、Amazon Simple Storage Service (Amazon S3) に関連する検出結果を更新する自動化ルールにタグを割り当てた場合、タグは指定されたリージョンの Security Hub 自動化ルールにのみ適用されます。S3 バケットには適用されません。関連するリソースにもタグを割り当てるには、リソースを格納する AWS Resource Groups または AWS のサービスを使用できます。例えば、S3 バケットの場合は Amazon S3 を使用します。関連するリソースにタグを割り当てると、Security Hub リソースのサポートリソースを特定しやすくなります。
- リソースを削除すると、リソースに関連付けられているすべてのタグも削除されます。

> **Important**
>
> 機密データやその他の重要なデータをタグに保存しないでください。タグは、AWS Billing and Cost Management を含む多くの AWS のサービス からアクセスできます。それらは機密データに使用することを目的としていません。

Security Hub リソースのタグを追加および管理するには、Security Hub コンソール、Security Hub API、または AWS Resource Groups Tagging API を使用します。Security Hub を使用すると、リソースの作成時にタグをリソースに追加できます。また、既存のリソースごとにタグを追加、管理することもできます。リソースグループを使用すると、Security Hub を含む複数の AWS のサービスにまたがる複数の既存リソースに対し、タグを一括で追加、管理できます。

その他のタグ付けに関するヒント、ベストプラクティスについては、「Tagging AWS Resources User Guide」の「Tagging your AWS resources」を参照してください。

IAMポリシーでタグを使用する

リソースのタグ付けを開始した後、タグベースのリソースレベルのアクセス許可を AWS Identity and Access Management (IAM) ポリシーで定義できます。この方法でタグを使用すると、AWS アカウント 内のどのユーザーとロールがリソースの作成とタグ付けの権限を持つか、どのユーザーとロールがより一般的にタグの追加、編集、削除の権限を持つかを詳細に制御できます。タグに基づいてアクセスを制御するには、IAM ポリシーの条件の要素でタグ関連の条件キーを使用します。

例えば、リソースの `Owner` タグの値がユーザー名となっている場合、すべての AWS Security Hub リソースに対して、ユーザーにフルアクセスを許可する IAM ポリシーを作成できます。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

タグをベースにしてリソースレベルでアクセス許可を定義した場合、そのアクセス許可は即座に反映されます。つまり、リソースが作成されるとすぐにリソースの安全性が増し、新しいリソースにタグの使用をすぐに強制できるようになります。リソースレベルのアクセス許可を使用して、新しいリソースと既存のリソースに、どのタグキーと値を関連付けるかを制御することもできます。詳細については、IAM ユーザーガイドのタグを使用したAWSリソースへのアクセスのコントロールを参照してください。

AWS Security Hub リソースへのタグの追加

ここの AWS Security Hub リソースにタグを追加するには、Security Hub コンソールまたは Security Hub API を使用します。コンソールは Hub リソースへのタグの追加をサポートしていません。

複数の Security Hub リソースに同時にタグを追加するには、AWS Resource Groups Tagging API のタグ付けオペレーションを使用します。

> **Important**
>
> リソースにタグを追加すると、リソースへのアクセスに影響を与える可能性があります。リソースにタグを追加する前に、タグを使用してリソースへのアクセスを管理する可能性のある AWS Identity and Access Management (IAM) ポリシーを必ず確認してください。

Console

リソースにタグを追加

自動化ルールまたは設定ポリシーを作成すると、Security Hub コンソールにタグを追加するオプションが表示されます。タグキーとタグ値はタグセクションで指定できます。

Security Hub API & AWS CLI

リソースにタグを追加

リソースを作成して 1 つ以上のタグをプログラムで追加するには、作成するリソースのタイプに適した操作を使用します。

- 設定ポリシーを作成して 1 つまたは複数のタグを追加するには、CreateConfigurationPolicy API を呼び出すか、AWS CLI を使用している場合は create-configuration-policy コマンドを実行します。
- 自動化ルールを作成して 1 つ以上のタグを追加するには、CreateAutomationRule API を呼び出すか、AWS CLI を使用している場合は create-automation-rule コマンドを実行します。
- Security Hub を有効にして Hub リソースに 1 つ以上のタグを追加するには、EnableSecurityHub API を呼び出すか、AWS Command Line Interface (AWS CLI) を使用している場合は enable-security-hub コマンドを実行します。

リクエストでは、`tags` パラメータを使用して、リソースに追加する各タグのタグキーとオプションのタグ値を指定します。`tags` パラメータは、オブジェクトの配列を指定します。各オブジェクトはタグキーとそれに関連するタグ値を指定します。

既存のリソースに 1 つ以上のタグを追加するには、Security Hub API の TagResource オペレーションを使用するか、AWS CLIを使用している場合は tag-resource コマンドを実行します。リクエストでは、タグを追加するリソースの Amazon リソースネーム (ARN) を指定します。`tags` パラメータを使用して、追加する各タグのタグキー (`key`) とオプションのタグ値 (`value`) を指定し

ます。tags パラメータは、オブジェクトの配列、各タグキーに 1 つのオブジェクト、および関連するタグ値を指定します。

例えば、次の AWS CLI コマンドは、タグ値が Prod の Environment タグキーを指定した設定ポリシーに追加します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

CLI コマンドの例:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Prod
```

実行する条件は以下のとおりです。

- resource-arn ではタグを追加する設定ポリシーの ARN を指定します。
- *Environment* はルールに追加するタグのタグキーです。
- *Prod* は指定されたタグキー (*Environment*) のタグ値です。

次の例では、コマンドは設定ポリシーに複数のタグを追加します。

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Prod key=CostCenter,value=12345 key=Owner,value=jane-
doe
```

tags配列内の各オブジェクトには、keyvalueとの引数の両方が必要です。ただし、value引数の値は空の文字列とすることができます。タグ値をタグキーに関連付けない場合、value引数の値を指定しないでください。例えば、次のコマンドは、関連するタグ値を含まない Owner タグキーを追加します。

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Owner,value=
```

タグ付けオペレーションが成功すると、Security Hub は空の HTTP 200 レスポンスを返します。それ以外の場合、Security Hub は HTTP 4xx またはオペレーションが失敗した理由を示す 500 レスポンスを返します。

AWS Security Hub リソースのタグを確認する

Security Hub コンソールまたは Security Hub API を使用して、Security Hub 自動化ルールまたは設定ポリシーのタグ (タグキーとタグ値の両方) を確認できます。コンソールは Hub リソースのタグの確認をサポートしていません。

複数の Security Hub リソースのタグを同時に確認するには、AWS Resource Groups Tagging API のタグ付けオペレーションを使用します。

Console

リソースのタグを確認するには

1. Security Hub 管理者の認証情報を使用して、https://console.aws.amazon.com/securityhub/ で AWS Security Hub コンソールを開きます。
2. タグを追加するリソースのタイプに応じて、次のいずれかを実行します。
   - 自動化ルールのタグを確認するには、ナビゲーションペインで [自動化] を選択します。次に、自動化ルールを選択します。
   - 設定ポリシーのタグを確認するには、ナビゲーションペインで [設定] を選択します。次に、[ポリシー] タブで設定ポリシーの横にあるオプションを選択します。サイドパネルが開き、ポリシーに割り当てられたタグの数が表示されます。[タグ] ヘッダーを展開すると、タグキーとタグ値が表示されます。

Tags セクションには、現在リソースに割り当てられているすべてのタグが一覧表示されます。

Security Hub API & AWS CLI

リソースのタグを確認する

既存のリソースのタグを取得して確認するには、ListTagsForResource API を呼び出します。リクエストでは、`resourceArn` パラメータを使用してリソースの Amazon リソースネーム (ARN) を指定します。

AWS CLI を使用している場合は、list-tags-for-resourceコマンドを実行し、resource-arn パラメータを使用してリソースの ARN を指定します。例:

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

操作が成功すると、Security Hub は tags 配列を返します。配列内の各オブジェクトは、現在リソースに割り当てられているタグ (タグキーとタグ値の両方) を指定します。例:

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Prod"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

ここでEnvironment、CostCenter、Ownerは、リソースに割り当てられるタグキーです。Prodは、Environmentタグキーに関連付けられているタグ値です。 12345は、CostCenterタグキーに関連付けられているタグ値です。Ownerタグキーには、関連するタグ値はありません。

タグの付いたすべての Security Hub リソースと、それらのリソースのそれぞれに割り当てられたすべてのタグのリストを取得するには、AWS Resource Groups Tagging API の GetResources オペレーションを使用します。リクエストでは、ResourceTypeFilters パラメータの値を securityhub に設定します。AWS CLI を使用してこれを行うには、get-resourcesコマンドを実行し、resource-type-filters パラメータの値を securityhub に設定します。例:

```
$ aws resourcegroupstaggingapi get-resources -\-resource-type-filters "securityhub"
```

オペレーションが成功すると、Resource Groups は ResourceTagMappingList 配列を返します。この配列には、タグが付いている Security Hub リソースごとに 1 つのオブジェクトが含まれ

ます。各オブジェクトで Security Hub リソースの ARN と、リソースに割り当てられるタグキーと値を指定します。

AWS Security Hub リソースのタグを編集する

AWS Security Hub リソースのタグ (タグキーまたはタグ値) を編集するには、Security Hub API を使用します。現在、Security Hub コンソールはタグ編集をサポートしていません。

複数の Security Hub リソースのタグを同時に編集するには、AWS Resource Groups Tagging API のタグ付けオペレーションを使用します。

> **Important**
>
> リソースのタグを編集すると、リソースへのアクセスに影響する可能性があります。タグの名前 (キー) や値を編集する前に、タグを使用してリソースへのアクセスを制御する可能性のある AWS Identity and Access Management IAM ポリシーがあれば、必ず確認してください。

Security Hub API & AWS CLI

リソースのタグを編集する

リソースのタグをプログラムで編集すると、既存のタグが新しい値で上書きされます。したがって、タグを編集する最適な方法は、タグキーまたはタグ値を編集するのか、またはその両方を編集するのかによって異なります。タグキーを編集するには、現在のタグを削除して新しいタグを追加します。

タグキーに関連付けられているタグ値のみを編集または削除するには、Security Hub API の TagResource オペレーションを使用して既存の値を上書きします。AWS CLI を使用している場合は、tag-resource コマンドを実行します。リクエストでは、タグ値を編集または削除するリソースの Amazon リソースネーム (ARN) を指定します。

タグ値を編集するには、`tags` パラメータを使用して、タグ値を変更したいタグキーを指定します。キーには新しいタグ値も指定する必要があります。例えば、次の AWS CLI コマンドは、特定の自動化ルールに割り当てられている `Environment` タグキーのタグ値を `Prod` から `Test` に変更します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Test
```

実行する条件は以下のとおりです。

- `resource-arn` では設定ポリシーの ARN を指定します。
- *`Environment`*は、変更するタグ値に関連付けられているタグキーです。
- *`Test`*は、指定したタグキー (*`Environment`*) に使用する新しいタグ値です。

タグキーからタグ値を削除するには、`tags`パラメーターのキーの`value`引数の値を指定しないでください。例:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Owner,value=
```

オペレーションが成功すると、Security Hub は空の HTTP 200 レスポンスを返します。それ以外の場合、Security Hub は HTTP 4xx またはオペレーションが失敗した理由を示す 500 レスポンスを返します。

AWS Security Hub リソースからのタグの削除

AWS Security Hub リソースからタグを削除するには、Security Hub API を使用します。現在、Security Hub コンソールはタグの削除をサポートしていません。

複数の Security Hub リソースからタグを同時に削除するには、AWS Resource Groups Tagging API のタグ付けオペレーションを使用します。

> **Important**
>
> リソースからタグを削除すると、リソースへのアクセスに影響を与える可能性があります。タグを削除する前に、タグを使用してリソースへのアクセスを管理する可能性のある AWS Identity and Access Management (IAM) ポリシーを必ず確認してください。

Security Hub API & AWS CLI

リソースからタグを削除する

リソースから 1 つ以上のタグをプログラムで削除するには、Security Hub API の UntagResource オペレーションを使用します。リクエストで、resourceArnパラメーターを使用して、タグを削除するリソースの Amazon リソースネーム (ARN) を指定します。tagKeysパラメータを使用して、削除するタグのタグキーを指定します。複数のタグを削除するには、削除する各タグのtagKeysパラメーターと引数をアンパサンド (&) で区切って追加します (例:tagKeys=*key1*&tagKeys=*key2*)。リソースから特定のタグ値 (タグキーではない) のみを削除するには、タグを削除する代わりにタグを編集します。

AWS CLI を使用している場合は、untag-resource コマンドを実行して 1 つ以上のタグをリソースから削除します。resource-arn パラメータには、タグを削除するリソースの ARN を指定します。tag-keysパラメータを使用して、削除するタグのタグキーを指定します。例えば、次のコマンドは、指定した設定ポリシーから Environment タグ (タグキーとタグ値の両方) を削除します。

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

ここで resource-arn ではタグを削除する設定ポリシーの ARN を指定し、*Environment* は削除するタグのタグキーです。

リソースから複数のタグを削除するには、追加の各タグ キーを tag-keys パラメーターの引数として追加します。例:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment Owner
```

オペレーションが成功すると、Security Hub は空の HTTP 200 レスポンスを返します。それ以外の場合、Security Hub は HTTP 4xx またはオペレーションが失敗した理由を示す 500 レスポンスを返します。

Security Hub クォータ

AWS アカウント には、AWS のサービス ごとに特定のデフォルトのクォータ (以前は [limits] (制限) と呼ばれていました) があります。これらのクォータは、アカウントのサービスリソースまたはオペレーションの最大数です。このトピックは、ご利用のアカウントの AWS Security Hub のリソースとオペレーションに適用されるクォータとリンクしています。特に明記されていない限り、クォータはそれぞれの AWS リージョン のアカウントに適用されます。

クォータによっては、引き上げることができないものもあります。クォータの引き上げをリクエストするには、[Service Quotas console] (Service Quotas コンソール) を使用します。クォータの引き上げをリクエストする方法についての説明は、Service Quotas ユーザーガイド の「クォータ引き上げリクエスト」を参照してください。Service Quotas コンソールでクォータが使用できない場合は、AWS Support Center Console の [サービス制限の引き上げフォーム] を使用して、クォータの引き上げをリクエストします。

最大クォータ

Security Hub のリソースに適用されるクォータのリストについては、AWS 全般のリファレンス の「AWS Security Hub エンドポイントとクォータ」を参照してください。

レートクォータ

Security Hub API オペレーションに適用されるクォータのリストについては、「AWS Security Hub API リファレンス」を参照してください。

クロスリージョン集約 を設定している場合、`BatchImportFindings` と `BatchUpdateFindings` への 1 回の呼び出しが、リンクされたリージョンと集約リージョンに影響を及ぼします。`GetFindings` オペレーションは、リンクされたリージョンと集約リージョンから結果を取得します。ただし、`BatchEnableStandards` と `UpdateStandardsControl` オペレーションはリージョンに固有です。

Security Hub 地域制限

一部の AWS Security Hub 機能は、特定の でのみ使用できます AWS リージョン。以下のセクションでは、これらのリージョン制限を示します。

Security Hub を利用できるリージョンのリストについては、「AWS 全般のリファレンス」の「AWS Security Hub エンドポイントとクォータ」を参照してください。

クロスリージョン集約の制限

では AWS GovCloud (US)、クロスリージョン集約は、 の検出結果、検出結果の更新、インサイトに対して AWS GovCloud (US) のみ使用できます。具体的には、 (米国東部) と AWS GovCloud (AWS GovCloud 米国西部) の間の結果、結果の更新、インサイトのみを集約できます。

中国リージョンでは、クロスリージョン集約は、中国リージョンの結果、結果の更新、インサイトにのみ使用できます。具体的には、中国 (北京) と中国 (寧夏) の間の結果、結果の更新、インサイトのみを集約できます。

デフォルトで無効になっているリージョンは、集約リージョンとして使用できません。デフォルトで無効になっているリージョンのリストについては、「AWS 全般のリファレンス」の「リージョンを有効にする」を参照してください。

リージョン別の統合の可用性

一部のリージョンでは統合を利用できない場合があります。特定のリージョンで統合を使用できない場合は、そのリージョンを選択したとき、そのリージョンは Security Hub コンソールの [Integrations] (統合) ページに表示されません。

中国 (北京) および中国 (寧夏) でサポートされている統合

中国 (北京) および中国 (寧夏) リージョンは、以下の AWS サービスとの統合のみをサポートしています。

- AWS Firewall Manager
- Amazon GuardDuty
- AWS Identity and Access Management Access Analyzer

- Amazon Inspector
- AWS IoT Device Defender
- AWS Systems Manager Explorer
- AWS Systems Manager OpsCenter
- AWS Systems Manager パッチマネージャー

中国 (北京) および中国 (寧夏) リージョンは、以下のサードパーティーの統合のみをサポートしています。

- Cloud Custodian
- FireEye Helix
- Helecloud
- IBM QRadar
- PagerDuty
- Palo Alto Networks Cortex XSOAR
- Palo Alto Networks VM-Series
- Prowler
- RSA Archer
- Splunk Enterprise
- Splunk Phantom
- ThreatModeler

AWS GovCloud（米国東部) および AWS GovCloud（米国西部) でサポートされている統合

AWS GovCloud（米国東部) および AWS GovCloud（米国西部) リージョンは、サービスとの AWS 以下の統合のみをサポートします。

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty

- AWS Health
- IAM Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender

AWS GovCloud（米国東部）および AWS GovCloud（米国西部）リージョンでは、以下のサードパーティー統合 のみがサポートされています。

- Atlassian Jira Service Management
- Atlassian Jira Service Management Cloud
- Atlassian OpsGenie
- Caveonix Cloud
- Cloud Custodian
- Cloud Storage Security Antivirus for Amazon S3
- CrowdStrike Falcon
- FireEye Helix
- Forcepoint CASB
- Forcepoint DLP
- Forcepoint NGFW
- Fugue
- Kion
- MicroFocus ArcSight
- NETSCOUT Cyber Investigator
- PagerDuty
- Palo Alto Networks – Prisma Cloud Compute
- Palo Alto Networks – Prisma Cloud Enterprise
- Palo Alto Networks – VM-Series (AWS GovCloud（米国西部）でのみ使用可能)
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer

- SecureCloudDb
- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

リージョン別の標準の有無

サービスマネージドスタンダード: AWS Control Tower は、 を含む AWS Control Tower がサポートするリージョンでのみ使用できます AWS GovCloud (US)。が AWS Control Tower サポートするリージョンのリストについては、 AWS Control Tower ユーザーガイドの「 の AWS リージョン 仕組み AWS Control Tower」を参照してください。

AWS リソースタグ付け標準は、カナダ西部 (カルガリー) 、中国、および では使用できません AWS GovCloud (US)。

その他のセキュリティ標準は、Security Hub が利用できる全リージョンで利用可能です。

リージョン別のコントロールの可用性

Security Hub コントロールは、一部のリージョンで利用できない場合があります。各リージョンで使用できないコントロールのリストについては、「コントロールの地域制限」を参照してください。サインインしているリージョンで使用できない場合、そのコントロールは Security Hub コンソールのコントロールリストに表示されません。ただし、集約リージョンにサインインしている場合は例外です。その場合は、集約リージョンまたは 1 つ以上のリンクされたリージョンで利用できるコントロールが表示されます。

コントロールの地域制限

AWS Security Hub コントロールは、すべての で利用できるとは限りません AWS リージョン。このページには、特定のリージョンで利用できないコントロールが表示されます。サインインしているリージョンで使用できない場合、そのコントロールは Security Hub コンソールのコントロールリストに表示されません。ただし、集約リージョンにサインインしている場合は例外です。その場合は、集約リージョンまたは 1 つ以上のリンクされたリージョンで利用できるコントロールが表示されます。

目次

- 中東 (アラブ首長国連邦)
- 南米 (サンパウロ)
- AWS GovCloud （ 米国東部 ）
- AWS GovCloud （ 米国西部 ）

米国東部 (バージニア北部)

以下のコントロールは米国東部 (バージニア北部) ではサポートされていません。

- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- 〔ElastiCache.4] ElastiCache for Redis レプリケーショングループは保管時に暗号化する必要があります
- Redis ElastiCache レプリケーショングループの [ElastiCache.5] は転送中に暗号化する必要があります
- 〔ElastiCache.6]バージョン ElastiCache 6.0 より前の Redis レプリケーショングループでは、Redis AUTH を使用する必要があります
- 〔ElastiCache.7] ElastiCache クラスターはデフォルトのサブネットグループを使用しないでください
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です

- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください

米国東部 (オハイオ)

米国東部 (オハイオ) では、以下のコントロールはサポートされていません。

- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります

- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です

- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

米国西部 (北カリフォルニア)

米国西部 (北カリフォルニア) では、以下のコントロールはサポートされていません。

- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります

- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラススナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを ログに記録する必要があります

- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

米国西部 (オレゴン)

米国西部 (オレゴン) では、以下のコントロールはサポートされていません。

- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません

- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です

- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

アフリカ (ケープタウン)

アフリカ (ケープタウン) では、以下のコントロールはサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [APIGateway.1] API Gateway REST と WebSocket API 実行の口グ記録を有効にする必要があります
- 〔AppSync.2] フィールドレベルのログ記録を有効にする AWS AppSync 必要があります
- 〔AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションでは口グ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります

- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください
- 〔CodeBuild.2] CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.3] アタッチされた Amazon EBS ボリュームは、保管時に暗号化することをお勧めします
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.12] 未使用の Amazon EC2 EIP を削除することをお勧めします
- [EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります

- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS .1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.4] Application Load Balancer は、http ヘッダーを削除するように設定する必要があります
- [ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な AWS Config設定を持つ事前定義されたセキュリティポリシーを使用する必要があります
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります
- 〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- 〔GuardDuty.1] GuardDuty を有効にする必要があります
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support

- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IoT.1] AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.1] RDS スナップショットはプライベートである必要があります
- [RDS.9] RDS DB インスタンスはログを CloudWatch Logs に発行する必要があります
- [RDS.10] IAM 認証は RDS インスタンス用に設定する必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります

- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを ログに記録する必要があります
- 〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります

アジアパシフィック (香港)

アジアパシフィック (香港) では、以下のコントロールはサポートされていません。

- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります

- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります

- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- 〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.10] IAM 認証は RDS インスタンス用に設定する必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを ログに記録する必要があります
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です

- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

アジアパシフィック (ハイデラバード)

以下のコントロールはアジアパシフィック (ハイデラバード) ではサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.1] API Gateway REST と WebSocket API 実行の口グ記録を有効にする必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります
- [APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります
- [APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります
- [APIGateway.8] API Gateway ルートには認証タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- 〔AppSync.2] フィールドレベルのログ記録を有効にする AWS AppSync 必要があります
- 〔AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- [Athena.2] Athena データカタログにはタグを付ける必要があります
- [Athena.3] Athena ワークグループにはタグを付ける必要があります
- 〔AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要があります
- [Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.2] AWS Backup 復旧ポイントにタグを付ける必要があります
- [Backup.3] AWS Backup ボールトにはタグを付ける必要があります

- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [Backup.5] AWS Backup バックアップ計画にはタグを付ける必要があります
- 〔CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットがパブリックにアクセスできないようにする
- 〔CloudTrail.7] S3 バケットで CloudTrail S3 バケットアクセスログ記録が有効になっていることを確認する
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください
- 〔CodeBuild.2] CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください

- 〔CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- 〔CodeBuild.4] CodeBuild プロジェクト環境にはログ記録 AWS Config設定が必要です
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [Detective.1] Detective の動作グラフにはタグを付ける必要があります
- [DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります

- [EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.34] EC2 トランジットゲートウェイルートテーブルにタグを付ける必要があります
- [EC2.40] EC2 NAT ゲートウェイにタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。
- [ECS.9] ECS タスク定義にはログ設定が必要です。
- [EFS .1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります

- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EFS .5] EFS アクセスポイントにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [ELB.5] アプリケーションおよび Classic Load Balancer のログ記録を有効にする必要があります
- [ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- 〔ElastiCache.1] ElastiCache Redis クラスターでは自動バックアップを有効にする必要があります
- 〔ElastiCache.6]バージョン ElastiCache 6.0 より前の Redis レプリケーショングループでは、Redis AUTH を使用する必要があります
- 〔ElastiCache.7] ElastiCache クラスターはデフォルトのサブネットグループを使用しないでください
- 〔ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります
- 〔ElasticBeanstalk.2] Elastic Beanstalk マネージドプラットフォームの更新を有効にする必要があります
- 〔ElasticBeanstalk.3] Elastic Beanstalk はログを にストリーミングする必要があります CloudWatch
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります
- [ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります
- [ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります
- [ES.4] Logs への Elasticsearch CloudWatch ドメインエラーのログ記録を有効にする必要があります

- 〔EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります
- 〔EventBridge.3] EventBridge カスタムイベントバスには、リソースベースのポリシーがアタッチされている必要があります
- 〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.1] AWS Glue ジョブにはタグを付ける必要があります
- 〔GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- 〔GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- 〔GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーはタグ付けする必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID には AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [IoT.1] AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります

- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 自動機密データ検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラススナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラススナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります

- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.1] Network Firewall ファイアウォールは複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.2] Network Firewall のログ記録を有効にする必要があります
- 〔NetworkFirewall.3] Network Firewall ポリシーには、少なくとも 1 つのルールグループが関連付けられている必要があります
- 〔NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、フルパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、フラグメント化されたパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.6] ステートレス Network Firewall ルールグループは空にしないでください
- 〔NetworkFirewall.9] Network Firewall ファイアウォールでは、削除保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインにはタグを付ける必要があります
- [Opensearch.10] OpenSearch ドメインには最新のソフトウェア更新がインストールされている必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.2] RDS DB インスタンスは、 PubliclyAccessible AWS Config設定によって決定されるパブリックアクセスを禁止する必要があります
- [RDS.7] RDS クラスターでは、削除保護が有効になっている必要があります

- [RDS.9] RDS DB インスタンスはログを CloudWatch Logs に発行する必要があります
- [RDS.12] IAM 認証は RDS クラスター用に設定する必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります
- [RDS.16] タグをスナップショットにコピーするように RDS DB クラスターを設定する必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [RDS.28] RDS DB クラスターにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [RDS.34] Aurora MySQL DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります
- [Redshift.2] Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります
- [Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります
- [Redshift.6] Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります
- [Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.6] S3 汎用バケットポリシーでは、他の へのアクセスを制限する必要があります AWS アカウント

- [S3.17] S3 汎用バケットは、保管時に で暗号化する必要があります AWS KMS keys
- 〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません
- 〔SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- 〔SageMaker.3] SageMaker ユーザーはノートブックインスタンスへのルートアクセスを許可されない
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SNS.3] SNS トピックにはタグを付ける必要があります
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- 〔StepFunctions.1] Step Functions ステートマシンではログ記録が有効になっている必要があります
- [Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.2] AWS WAF クラシックリージョンルールには少なくとも 1 つの条件が必要です
- [WAF.3] AWS WAF クラシックリージョンルールグループには、少なくとも 1 つのルールが必要です
- [WAF.4] AWS WAF クラシックリージョンウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります

アジアパシフィック (ジャカルタ)

以下のコントロールはアジアパシフィック (ジャカルタ) ではサポートされていません。

- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.1] API Gateway REST と WebSocket API 実行の口グ記録を有効にする必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります
- [APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります
- [APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります
- [APIGateway.8] API Gateway ルートには認証タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- 〔AppSync.2] フィールドレベルの口グ記録を有効にする AWS AppSync 必要があります
- 〔AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- 〔AutoScaling.3] Auto Scaling グループの起動設定では、インスタンスメタデータサービスバージョン 2 (IMDSv2) を要求するように EC2 インスタンスを設定する必要がありますIMDSv2
- 〔AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります
- 〔AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります
- [Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません

- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.2] AWS Backup 復旧ポイントにタグを付ける必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [Backup.5] AWS Backup バックアップ計画にはタグを付ける必要があります
- 〔CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CloudWatch.17] CloudWatch アラームアクションを有効にする必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください
- 〔CodeBuild.2] CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください

- 〔CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- 〔CodeBuild.4] CodeBuild プロジェクト環境にはログ記録 AWS Config設定が必要です
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [Detective.1] Detective の動作グラフにはタグを付ける必要があります
- [DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります

- [EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.2] ECS サービスには、パブリック IP アドレスを自動で割り当てないでください
- [ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください
- [ECS.4] ECS コンテナは、非特権として実行する必要があります
- [ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。
- [ECS.8] シークレットは、コンテナ環境の変数として渡さないでください
- [ECS.9] ECS タスク定義には ログ設定が必要です。
- [ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。
- [ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります
- [EFS .1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS

- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります
- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります
- [ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- 〔ElastiCache.1] ElastiCache Redis クラスターでは自動バックアップを有効にする必要があります
- 〔ElastiCache.6]バージョン ElastiCache 6.0 より前の Redis レプリケーショングループでは、Redis AUTH を使用する必要があります
- 〔ElastiCache.7] ElastiCache クラスターはデフォルトのサブネットグループを使用しないでください
- 〔ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります
- 〔ElasticBeanstalk.2] Elastic Beanstalk マネージドプラットフォームの更新を有効にする必要があります
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります
- [ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります
- [ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります
- 〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります

- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.1] AWS Glue ジョブにはタグを付ける必要があります
- 〔GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- 〔GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- 〔GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IoT.1] AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 自動機密データ検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラススナップショットはパブリックにしないでください

- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.1] Network Firewall ファイアウォールは複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.3] Network Firewall ポリシーには、少なくとも 1 つのルールグループが関連付けられている必要があります
- 〔NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、フルパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、フラグメント化されたパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.6] ステートレス Network Firewall ルールグループは空にしないでください
- [Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.9] RDS DB インスタンスはログを CloudWatch Logs に発行する必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります

- [RDS.16] タグをスナップショットにコピーするように RDS DB クラスターを設定する必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります
- [Redshift.2] Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります
- [Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります
- [Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります
- [Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを口グに記録する必要があります
- [S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります
- [S3.13] S3 汎用バケットにはライフサイクル設定が必要です
- 〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません
- 〔SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- 〔SageMaker.3] SageMaker ユーザーはノートブックインスタンスへのルートアクセスを許可されない
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SNS.3] SNS トピックにはタグを付ける必要があります
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります

- [SQS.2] SQS キューにはタグを付ける必要があります
- [SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.2] AWS WAF クラシックリージョンルールには少なくとも 1 つの条件が必要です
- [WAF.3] AWS WAF クラシックリージョンルールグループには、少なくとも 1 つのルールが必要です
- [WAF.4] AWS WAF クラシックリージョンウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります

アジアパシフィック (ムンバイ)

アジアパシフィック (ムンバイ) では、以下のコントロールはサポートされていません。

- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります

- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch

- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを口グに記録する必要があります
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ロク記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

アジアパシフィック (メルボルン)

以下のコントロールはアジアパシフィック (メルボルン) ではサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります
- [APIGateway.8] API Gateway ルートには認証タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- 〔AppSync.2] フィールドレベルのログ記録を有効にする AWS AppSync 必要があります

- 〔AppSync.4] AWS AppSync GraphQL APIsにはタグを付ける必要があります
- 〔AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- [Athena.2] Athena データカタログにはタグを付ける必要があります
- [Athena.3] Athena ワークグループにはタグを付ける必要があります
- 〔AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要があります
- [Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.2] AWS Backup 復旧ポイントにタグを付ける必要があります
- [Backup.3] AWS Backup ボールトにはタグを付ける必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [Backup.5] AWS Backup バックアップ計画にはタグを付ける必要があります
- 〔CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません

- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください
- 〔CodeBuild.2] CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください
- 〔CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- 〔CodeBuild.4] CodeBuild プロジェクト環境にはログ記録 AWS Config設定が必要です
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [Detective.1] Detective の動作グラフにはタグを付ける必要があります
- [DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です

- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.1] Amazon EBS スナップショットはパブリックに復元できないようにすることをお勧めします
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.9] Amazon EC2 インスタンスは、パブリック IPv4 アドレスを未設定にすることをお勧めします
- [EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.33] EC2 トランジットゲートウェイアタッチメントにはタグを付ける必要があります
- [EC2.34] EC2 トランジットゲートウェイルートテーブルにタグを付ける必要があります
- [EC2.40] EC2 NAT ゲートウェイにタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります

- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.52] EC2 トランジットゲートウェイにはタグを付ける必要があります
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。
- [ECS.9] ECS タスク定義にはログ設定が必要です。
- [EFS .1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります
- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EFS .5] EFS アクセスポイントにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [EKS.6] EKS クラスターにはタグを付ける必要があります
- [EKS.7] EKS ID プロバイダーの設定にはタグを付ける必要があります
- [EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります
- [ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- 〔ElastiCache.1] ElastiCache Redis クラスターでは自動バックアップを有効にする必要があります
- 〔ElastiCache.2]Redis キャッシュクラスター ElastiCache では、マイナーバージョン自動アップグレードを有効にする必要があります

- Redis ElastiCache レプリケーショングループの [ElastiCache.3] では、自動フェイルオーバーを有効にする必要があります
- 〔ElastiCache.4] ElastiCache for Redis レプリケーショングループは保管時に暗号化する必要があります
- Redis ElastiCache レプリケーショングループの [ElastiCache.5] は転送中に暗号化する必要があります
- 〔ElastiCache.6]バージョン ElastiCache 6.0 より前の Redis レプリケーショングループでは、Redis AUTH を使用する必要があります
- 〔ElastiCache.7] ElastiCache クラスターはデフォルトのサブネットグループを使用しないでください
- 〔ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります
- 〔ElasticBeanstalk.2] Elastic Beanstalk マネージドプラットフォームの更新を有効にする必要があります
- 〔ElasticBeanstalk.3] Elastic Beanstalk はログを にストリーミングする必要があります CloudWatch
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります
- [ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります
- [ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります
- [ES.4] Logs への Elasticsearch CloudWatch ドメインエラーのログ記録を有効にする必要があります
- 〔EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります
- 〔EventBridge.3] EventBridge カスタムイベントバスには、リソースベースのポリシーがアタッチされている必要があります
- 〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります

- [Glue.1] AWS Glue ジョブにはタグを付ける必要があります
- 〔GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- 〔GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- 〔GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.10] IAM ユーザーのパスワードポリシーには強力な AWS Config設定が必要です
- [IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します
- [IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します
- [IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します
- [IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します
- [IAM.15] 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します
- [IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています
- [IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します
- [IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーはタグ付けする必要があります

- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID には AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [IoT.1] AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 自動機密データ検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラススナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラススナップショットは、保管中に暗号化する必要があります

- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.1] Network Firewall ファイアウォールは複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.2] Network Firewall のログ記録を有効にする必要があります
- 〔NetworkFirewall.3] Network Firewall ポリシーには、少なくとも 1 つのルールグループが関連付けられている必要があります
- 〔NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、フルパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、フラグメント化されたパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.6] ステートレス Network Firewall ルールグループは空にしないでください
- 〔NetworkFirewall.9] Network Firewall ファイアウォールでは、削除保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインにはタグを付ける必要があります
- [Opensearch.10] OpenSearch ドメインには最新のソフトウェア更新がインストールされている必要があります

- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.1] RDS スナップショットはプライベートである必要があります
- [RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。
- [RDS.7] RDS クラスターでは、削除保護が有効になっている必要があります
- [RDS.12] IAM 認証は RDS クラスター用に設定する必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります
- [RDS.16] タグをスナップショットにコピーするように RDS DB クラスターを設定する必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [RDS.28] RDS DB クラスターにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [RDS.34] Aurora MySQL DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを ログに記録する必要があります
- [S3.14] S3 汎用バケットではバージョニングを有効にする必要があります
- [S3.15] S3 汎用バケットでは、オブジェクトロックを有効にする必要があります
- 〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません
- 〔SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- 〔SageMaker.3] SageMaker ユーザーはノートブックインスタンスへのルートアクセスを許可されない

- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SNS.1] SNS トピックは、保管時に を使用して暗号化する必要があります AWS KMS
- [SNS.3] SNS トピックにはタグを付ける必要があります
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [SSM.4] SSM ドキュメントはパブリックにしないでください
- 〔StepFunctions.1] Step Functions ステートマシンでは口グ記録が有効になっている必要があります
- 〔StepFunctions.2] Step Functions アクティビティにはタグを付ける必要があります
- [Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります

アジアパシフィック (大阪)

アジアパシフィック (大阪) では、以下のコントロールはサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.1] API Gateway REST と WebSocket API 実行の口グ記録を有効にする必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります
- [APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります
- [APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります
- [Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- 〔CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションでは口グ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません

- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CloudWatch.15] CloudWatch アラームには、指定されたアクションが設定されている必要があります
- 〔CloudWatch.16] CloudWatch ロググループは、指定された期間保持する必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください
- 〔CodeBuild.2] CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください
- 〔CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- 〔CodeBuild.4] CodeBuild プロジェクト環境にはログ記録 AWS Config設定が必要です
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [Detective.1] Detective の動作グラフにはタグを付ける必要があります
- [DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラススナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります

- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.2] DynamoDB テーブルでは point-in-time リカバリを有効にする必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.1] Amazon EBS スナップショットはパブリックに復元できないようにすることをお勧めします
- [EC2.3] アタッチされた Amazon EBS ボリュームは、保管時に暗号化することをお勧めします
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.7] EBS のデフォルト暗号化を有効にすることをお勧めします
- [EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.9] Amazon EC2 インスタンスは、パブリック IPv4 アドレスを未設定にすることをお勧めします
- [EC2.10] Amazon EC2 サービス用に作成された VPC エンドポイントを使用するようにAmazon EC2 を設定することをお勧めします
- [EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.15] Amazon EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないことをお勧めします
- [EC2.16] 未使用のネットワークアクセスコントロールリストを削除することをお勧めします
- [EC2.17] Amazon EC2 インスタンスが複数の ENI を使用しないようにすることをお勧めします
- [EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします
- [EC2.20] AWS Site-to-Site VPN 接続の両方の VPN トンネルが稼働している必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします

- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.52] EC2 トランジットゲートウェイにはタグを付ける必要があります
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。
- [ECS.2] ECS サービスには、パブリック IP アドレスを自動で割り当てないでください
- [ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください
- [ECS.4] ECS コンテナは、非特権として実行する必要があります
- [ECS.8] シークレットは、コンテナ環境の変数として渡さないでください
- [ECS.9] ECS タスク定義にはログ設定が必要です。
- [ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。
- [ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります
- [EFS .1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager

- [ELB.3] Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります
- [ELB.4] Application Load Balancer は、http ヘッダーを削除するように設定する必要があります
- [ELB.6] Application、Gateway、Network Load Balancer では、削除保護を有効にする必要があります
- [ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な AWS Config設定を持つ事前定義されたセキュリティポリシーを使用する必要があります
- [ELB.9] Classic Load Balancer では、クロスゾーンロードバランシングが有効になっている必要があります
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- 〔ElastiCache.1] ElastiCache Redis クラスターでは自動バックアップを有効にする必要があります
- 〔ElastiCache.7] ElastiCache クラスターはデフォルトのサブネットグループを使用しないでください
- 〔ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります
- 〔ElasticBeanstalk.2] Elastic Beanstalk マネージドプラットフォームの更新を有効にする必要があります
- 〔ElasticBeanstalk.3] Elastic Beanstalk はログを にストリーミングする必要があります CloudWatch
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります
- [ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります
- [ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- 〔GuardDuty.1] GuardDuty を有効にする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません

- [IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IoT.1] AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [KMS.3] 意図せずに削除 AWS KMS keys しないでください
- [Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります
- [Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります
- [Lambda.3] Lambda 関数は VPC 内に存在する必要があります
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります

- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- [Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.1] RDS スナップショットはプライベートである必要があります
- [RDS.4] RDS クラススナップショットとデータベーススナップショットは保管中に暗号化する必要があります
- [RDS.6] RDS DB インスタンスの拡張モニタリングを設定する必要があります
- [RDS.7] RDS クラスターでは、削除保護が有効になっている必要があります
- [RDS.8] RDS DB インスタンスで、削除保護が有効になっている必要があります
- [RDS.9] RDS DB インスタンスはログを CloudWatch Logs に発行する必要があります
- [RDS.10] IAM 認証は RDS インスタンス用に設定する必要があります
- [RDS.12] IAM 認証は RDS クラスター用に設定する必要があります
- [RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります

- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります
- [Redshift.2] Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります
- [Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります
- [Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを ログに記録する必要があります
- [S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります
- [S3.15] S3 汎用バケットでは、オブジェクトロックを有効にする必要があります
- [S3.17] S3 汎用バケットは、保管時に で暗号化する必要があります AWS KMS keys
- 〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔SecretsManager.1] Secrets Manager シークレットでは、自動ローテーションを有効にする必要があります
- 〔SecretsManager.2] 自動ローテーションで設定された Secrets Manager シークレットは正常にローテーションする必要があります
- 〔SecretsManager.3] 未使用の Secrets Manager シークレットを削除する
- 〔SecretsManager.4] Secrets Manager のシークレットは、指定された日数内にローテーションする必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SNS.1] SNS トピックは、保管時に を使用して暗号化する必要があります AWS KMS
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります

- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.3] AWS WAF クラシックリージョンルールグループには、少なくとも 1 つのルールが必要です
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります

アジアパシフィック (ソウル)

アジアパシフィック (ソウル) では、以下のコントロールはサポートされていません。

- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります

- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを ログに記録する必要があります

- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

アジアパシフィック (シンガポール)

アジアパシフィック (シンガポール) では、以下のコントロールはサポートされていません。

- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません

- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります

- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

アジアパシフィック (シドニー)

アジアパシフィック (シドニー) では、以下のコントロールはサポートされていません。

- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります

- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを ログに記録する必要があります
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

アジアパシフィック (東京)

アジアパシフィック (東京) では、以下のコントロールはサポートされていません。

- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません

- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

カナダ (中部)

カナダ (中部) では、以下のコントロールはサポートされていません。

- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です

- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションでは口グ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります

- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを ログに記録する必要があります
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

中国 (北京)

中国 (北京) では、以下のコントロールはサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [ACM.3] ACM 証明書にはタグを付ける必要があります

- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります
- [APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります
- [APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります
- 〔AppSync.4] AWS AppSync GraphQL APIsにはタグを付ける必要があります
- [Athena.2] Athena データカタログにはタグを付ける必要があります
- [Athena.3] Athena ワークグループにはタグを付ける必要があります
- 〔AutoScaling.10] EC2 Auto Scaling グループにタグを付ける必要があります
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.2] AWS Backup 復旧ポイントにタグを付ける必要があります
- [Backup.3] AWS Backup ボールトにはタグを付ける必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [Backup.5] AWS Backup バックアップ計画にはタグを付ける必要があります
- 〔CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください

- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CloudTrail.9] CloudTrail 証跡にはタグを付ける必要があります
- 〔CloudWatch.15] CloudWatch アラームには、指定されたアクションが設定されている必要があります
- 〔CloudWatch.16] CloudWatch ロググループは、指定された期間保持する必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [Detective.1] Detective の動作グラフにはタグを付ける必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにタグを付ける必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.5] DynamoDB テーブルにはタグを付ける必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.15] Amazon EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないことをお勧めします

- [EC2.16] 未使用のネットワークアクセスコントロールリストを削除することをお勧めします
- [EC2.20] AWS Site-to-Site VPN 接続の両方の VPN トンネルが稼働している必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.33] EC2 トランジットゲートウェイアタッチメントにはタグを付ける必要があります
- [EC2.34] EC2 トランジットゲートウェイルートテーブルにタグを付ける必要があります
- [EC2.35] EC2 ネットワークインターフェイスにタグを付ける必要があります
- [EC2.36] EC2 カスタマーゲートウェイにはタグを付ける必要があります
- [EC2.37] EC2 Elastic IP アドレスにタグを付ける必要があります
- [EC2.38] EC2 インスタンスにはタグを付ける必要があります
- [EC2.39] EC2 インターネットゲートウェイにはタグを付ける必要があります
- [EC2.40] EC2 NAT ゲートウェイにタグを付ける必要があります
- [EC2.41] EC2 ネットワーク ACLs にはタグを付ける必要があります
- [EC2.42] EC2 ルートテーブルにはタグを付ける必要があります
- [EC2.43] EC2 セキュリティグループにタグを付ける必要があります
- [EC2.44] EC2 サブネットにはタグを付ける必要があります
- [EC2.45] EC2 ボリュームにはタグを付ける必要があります
- [EC2.46] Amazon VPCsにはタグを付ける必要があります
- [EC2.47] Amazon VPC エンドポイントサービスにはタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります
- [EC2.49] Amazon VPC ピアリング接続にはタグを付ける必要があります
- [EC2.50] EC2 VPN ゲートウェイにはタグを付ける必要があります
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.52] EC2 トランジットゲートウェイにはタグを付ける必要があります
- [EC2.53] EC2 セキュリティグループは、0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可しないでください
- [EC2.54] EC2 セキュリティグループは、::/0 からリモートサーバー管理ポートへの入力を許可しないでください

- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。
- [ECS.13] ECS サービスはタグ付けする必要があります
- [ECS.14] ECS クラスターにはタグを付ける必要があります
- [ECS.15] ECS タスク定義にはタグを付ける必要があります
- [EFS .5] EFS アクセスポイントにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [EKS.6] EKS クラスターにはタグを付ける必要があります
- [EKS.7] EKS ID プロバイダーの設定にはタグを付ける必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- 〔ElastiCache.1] ElastiCache Redis クラスターでは自動バックアップを有効にする必要があります
- 〔ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります
- 〔ElasticBeanstalk.2] Elastic Beanstalk マネージドプラットフォームの更新を有効にする必要があります
- 〔ElasticBeanstalk.3] Elastic Beanstalk はログを にストリーミングする必要があります CloudWatch
- [EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります
- [ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります
- [ES.4] Logs への Elasticsearch CloudWatch ドメインエラーのログ記録を有効にする必要があります
- [ES.9] Elasticsearch ドメインにはタグを付ける必要があります
- 〔EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります
- 〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります

- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.1] AWS Glue ジョブにはタグを付ける必要があります
- 〔GuardDuty.1] GuardDuty を有効にする必要があります
- 〔GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- 〔GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- 〔GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.23] IAM Access Analyzer アナライザーにはタグを付ける必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーはタグ付けする必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID には AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [IAM.28] IAM Access Analyzer の外部アクセスアナライザーを有効にする必要があります
- [IoT.1] AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [Kinesis.2] Kinesis ストリームにはタグを付ける必要があります
- [Lambda.6] Lambda 関数にはタグを付ける必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 自動機密データ検出を有効にする必要があります

- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.1] Network Firewall ファイアウォールは複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.2] Network Firewall のログ記録を有効にする必要があります
- 〔NetworkFirewall.3] Network Firewall ポリシーには、少なくとも 1 つのルールグループが関連付けられている必要があります
- 〔NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、フルパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、フラグメント化されたパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.6] ステートレス Network Firewall ルールグループは空にしないでください
- 〔NetworkFirewall.7] Network Firewall ファイアウォールにはタグを付ける必要があります
- 〔NetworkFirewall.8] Network Firewall ファイアウォールポリシーにはタグを付ける必要があります
- 〔NetworkFirewall.9] Network Firewall ファイアウォールでは、削除保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります

- [Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインにはタグを付ける必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [PCA.1] AWS Private CA ルート認証機関を無効にする必要があります
- [RDS.7] RDS クラスターでは、削除保護が有効になっている必要があります
- [RDS.10] IAM 認証は RDS インスタンス用に設定する必要があります
- [RDS.12] IAM 認証は RDS クラスター用に設定する必要があります
- [RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります
- [RDS.16] タグをスナップショットにコピーするように RDS DB クラスターを設定する必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [RDS.28] RDS DB クラスターにはタグを付ける必要があります
- [RDS.29] RDS DB クラススナップショットにはタグを付ける必要があります
- [RDS.30] RDS DB インスタンスにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります

- [RDS.32] RDS DB スナップショットにはタグを付ける必要があります
- [RDS.33] RDS DB サブネットグループにタグを付ける必要があります
- [RDS.34] Aurora MySQL DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.11] Redshift クラスターにはタグを付ける必要があります
- [Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります
- [Redshift.13] Redshift クラススナップショットにはタグを付ける必要があります
- [Redshift.14] Redshift クラスターサブネットグループにタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを口グに記録する必要があります
- [S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります
- [S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります
- [S3.14] S3 汎用バケットではバージョニングを有効にする必要があります
- [S3.22] S3 汎用バケットは、オブジェクトレベルの書き込みイベントを口グに記録する必要があります
- [S3.23] S3 汎用バケットは、オブジェクトレベルの読み取りイベントを口グに記録する必要があります
- 〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- 〔SecretsManager.3] 未使用の Secrets Manager シークレットを削除する
- 〔SecretsManager.4] Secrets Manager のシークレットは、指定された日数内に口ーテーションする必要があります

- 〔SecretsManager.5] Secrets Manager のシークレットにはタグを付ける必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SNS.3] SNS トピックにはタグを付ける必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- 〔StepFunctions.2] Step Functions アクティビティにはタグを付ける必要があります
- [Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.3] AWS WAF クラシックリージョンルールグループには、少なくとも 1 つのルールが必要です
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります

中国 (寧夏)

中国 (寧夏) では、以下のコントロールはサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [ACM.3] ACM 証明書にはタグを付ける必要があります
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります
- [APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります

- [APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります
- 〔AppSync.4] AWS AppSync GraphQL APIsにはタグを付ける必要があります
- [Athena.2] Athena データカタログにはタグを付ける必要があります
- [Athena.3] Athena ワークグループにはタグを付ける必要があります
- 〔AutoScaling.10] EC2 Auto Scaling グループにタグを付ける必要があります
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.2] AWS Backup 復旧ポイントにタグを付ける必要があります
- [Backup.3] AWS Backup ボールトにはタグを付ける必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [Backup.5] AWS Backup バックアップ計画にはタグを付ける必要があります
- 〔CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります

- 〔CloudTrail.9] CloudTrail 証跡にはタグを付ける必要があります
- 〔CloudWatch.15] CloudWatch アラームには、指定されたアクションが設定されている必要があります
- 〔CloudWatch.16] CloudWatch ロググループは、指定された期間保持する必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [Detective.1] Detective の動作グラフにはタグを付ける必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにタグを付ける必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.5] DynamoDB テーブルにはタグを付ける必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.15] Amazon EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないことをお勧めします
- [EC2.16] 未使用のネットワークアクセスコントロールリストを削除することをお勧めします
- [EC2.20] AWS Site-to-Site VPN 接続の両方の VPN トンネルが稼働している必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします

- [EC2.33] EC2 トランジットゲートウェイアタッチメントにはタグを付ける必要があります
- [EC2.34] EC2 トランジットゲートウェイルートテーブルにタグを付ける必要があります
- [EC2.35] EC2 ネットワークインターフェイスにタグを付ける必要があります
- [EC2.36] EC2 カスタマーゲートウェイにはタグを付ける必要があります
- [EC2.37] EC2 Elastic IP アドレスにタグを付ける必要があります
- [EC2.38] EC2 インスタンスにはタグを付ける必要があります
- [EC2.39] EC2 インターネットゲートウェイにはタグを付ける必要があります
- [EC2.40] EC2 NAT ゲートウェイにタグを付ける必要があります
- [EC2.41] EC2 ネットワーク ACLs にはタグを付ける必要があります
- [EC2.42] EC2 ルートテーブルにはタグを付ける必要があります
- [EC2.43] EC2 セキュリティグループにタグを付ける必要があります
- [EC2.44] EC2 サブネットにはタグを付ける必要があります
- [EC2.45] EC2 ボリュームにはタグを付ける必要があります
- [EC2.46] Amazon VPCsにはタグを付ける必要があります
- [EC2.47] Amazon VPC エンドポイントサービスにはタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります
- [EC2.49] Amazon VPC ピアリング接続にはタグを付ける必要があります
- [EC2.50] EC2 VPN ゲートウェイにはタグを付ける必要があります
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.52] EC2 トランジットゲートウェイにはタグを付ける必要があります
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。
- [ECS.13] ECS サービスはタグ付けする必要があります
- [ECS.14] ECS クラスターにはタグを付ける必要があります
- [ECS.15] ECS タスク定義にはタグを付ける必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります

- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EFS .5] EFS アクセスポイントにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [EKS.6] EKS クラスターにはタグを付ける必要があります
- [EKS.7] EKS ID プロバイダーの設定にはタグを付ける必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- 〔ElastiCache.1] ElastiCache Redis クラスターでは自動バックアップを有効にする必要があります
- 〔ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります
- 〔ElasticBeanstalk.2] Elastic Beanstalk マネージドプラットフォームの更新を有効にする必要があります
- 〔ElasticBeanstalk.3] Elastic Beanstalk はログを にストリーミングする必要があります CloudWatch
- [EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります
- [ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります
- [ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります
- [ES.4] Logs への Elasticsearch CloudWatch ドメインエラーのログ記録を有効にする必要があります
- [ES.9] Elasticsearch ドメインにはタグを付ける必要があります
- 〔EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります
- 〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります

- [Glue.1] AWS Glue ジョブにはタグを付ける必要があります
- 〔GuardDuty.1] GuardDuty を有効にする必要があります
- 〔GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- 〔GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- 〔GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.23] IAM Access Analyzer アナライザーにはタグを付ける必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーはタグ付けする必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID には AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [IAM.28] IAM Access Analyzer の外部アクセスアナライザーを有効にする必要があります
- [IoT.1] AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [Kinesis.2] Kinesis ストリームにはタグを付ける必要があります
- [Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります
- [Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります
- [Lambda.3] Lambda 関数は VPC 内に存在する必要があります
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Lambda.6] Lambda 関数にはタグを付ける必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 自動機密データ検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch

- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります
- [Neptune.3] Neptune DB クラススナップショットはパブリックにしないでください
- 〔NetworkFirewall.1] Network Firewall ファイアウォールは複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.2] Network Firewall のログ記録を有効にする必要があります
- 〔NetworkFirewall.3] Network Firewall ポリシーには、少なくとも 1 つのルールグループが関連付けられている必要があります
- 〔NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、フルパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、フラグメント化されたパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.6] ステートレス Network Firewall ルールグループは空にしないでください
- 〔NetworkFirewall.7] Network Firewall ファイアウォールにはタグを付ける必要があります
- 〔NetworkFirewall.8] Network Firewall ファイアウォールポリシーにはタグを付ける必要があります
- 〔NetworkFirewall.9] Network Firewall ファイアウォールでは、削除保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインにはタグを付ける必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です

- [PCA.1] AWS Private CA ルート認証機関を無効にする必要があります
- [RDS.7] RDS クラスターでは、削除保護が有効になっている必要があります
- [RDS.9] RDS DB インスタンスはログを CloudWatch Logs に発行する必要があります
- [RDS.10] IAM 認証は RDS インスタンス用に設定する必要があります
- [RDS.12] IAM 認証は RDS クラスター用に設定する必要があります
- [RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.28] RDS DB クラスターにはタグを付ける必要があります
- [RDS.29] RDS DB クラススナップショットにはタグを付ける必要があります
- [RDS.30] RDS DB インスタンスにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [RDS.32] RDS DB スナップショットにはタグを付ける必要があります
- [RDS.33] RDS DB サブネットグループにタグを付ける必要があります
- [RDS.34] Aurora MySQL DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります
- [Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.11] Redshift クラスターにはタグを付ける必要があります
- [Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります
- [Redshift.13] Redshift クラススナップショットにはタグを付ける必要があります
- [Redshift.14] Redshift クラスターサブネットグループにタグを付ける必要があります

- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを口グに記録する必要があります
- [S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります
- [S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります
- [S3.14] S3 汎用バケットではバージョニングを有効にする必要があります
- 〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- 〔SecretsManager.3] 未使用の Secrets Manager シークレットを削除する
- 〔SecretsManager.4] Secrets Manager のシークレットは、指定された日数内にローテーションする必要があります
- 〔SecretsManager.5] Secrets Manager のシークレットにはタグを付ける必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SNS.3] SNS トピックにはタグを付ける必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- 〔StepFunctions.2] Step Functions アクティビティにはタグを付ける必要があります
- [Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL 口グ記録を有効にする必要があります
- [WAF.3] AWS WAF クラシックリージョンルールグループには、少なくとも 1 つのルールが必要です
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です

- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります

ヨーロッパ (フランクフルト)

ヨーロッパ (フランクフルト) では、以下のコントロールはサポートされていません。

- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります

- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを ログに記録する必要があります
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

ヨーロッパ (アイルランド)

ヨーロッパ (アイルランド) では、以下のコントロールはサポートされていません。

- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります

- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを ログに記録する必要があります
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

ヨーロッパ (ロンドン)

ヨーロッパ (ロンドン) では、以下のコントロールはサポートされていません。

- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません

- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

ヨーロッパ (ミラノ)

ヨーロッパ (ミラノ) では、以下のコントロールはサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります

- [APIGateway.1] API Gateway REST と WebSocket API 実行のログ記録を有効にする必要があります
- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください
- 〔CodeBuild.2] CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります

- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.3] アタッチされた Amazon EBS ボリュームは、保管時に暗号化することをお勧めします
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.12] 未使用の Amazon EC2 EIP を削除することをお勧めします
- [EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります
- [EFS .1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.4] Application Load Balancer は、http ヘッダーを削除するように設定する必要があります
- [ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な AWS Config設定を持つ事前定義されたセキュリティポリシーを使用する必要があります
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります

- 〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- 〔GuardDuty.1] GuardDuty を有効にする必要があります
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IoT.1] AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [KMS.3] 意図せずに削除 AWS KMS keys しないでください
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります

- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- [Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.1] RDS スナップショットはプライベートである必要があります
- [RDS.4] RDS クラスタースナップショットとデータベーススナップショットは保管中に暗号化する必要があります
- [RDS.9] RDS DB インスタンスはログを CloudWatch Logs に発行する必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [Redshift.2] Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります
- [Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを ログに記録する必要があります
- 〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります

- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります

ヨーロッパ (パリ)

ヨーロッパ (パリ) では、以下のコントロールはサポートされていません。

- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります

- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを ログに記録する必要があります

- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

欧州 (スペイン)

以下のコントロールは欧州 (スペイン) ではサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.1] API Gateway REST と WebSocket API 実行の口グ記録を有効にする必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります
- [APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります
- [APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります
- [APIGateway.8] API Gateway ルートには認証タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- 〔AppSync.2] フィールドレベルのログ記録を有効にする AWS AppSync 必要があります
- 〔AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください

- [Athena.2] Athena データカタログにはタグを付ける必要があります
- [Athena.3] Athena ワークグループにはタグを付ける必要があります
- 〔AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要があります
- [Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.2] AWS Backup 復旧ポイントにタグを付ける必要があります
- [Backup.3] AWS Backup ボールトにはタグを付ける必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [Backup.5] AWS Backup バックアップ計画にはタグを付ける必要があります
- 〔CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションでは口グ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります

- 〔CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットがパブリックにアクセスできないようにする
- 〔CloudTrail.7] S3 バケットで CloudTrail S3 バケットアクセスログ記録が有効になっていることを確認する
- 〔CloudWatch.16] CloudWatch ロググループは、指定された期間保持する必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください
- 〔CodeBuild.2] CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください
- 〔CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- 〔CodeBuild.4] CodeBuild プロジェクト環境にはログ記録 AWS Config設定が必要です
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [Detective.1] Detective の動作グラフにはタグを付ける必要があります
- [DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります

- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラススナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.1] DynamoDB テーブルは、需要に応じて容量をオートスケーリングする必要があります
- [DynamoDB.2] DynamoDB テーブルでは point-in-time リカバリを有効にする必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.1] Amazon EBS スナップショットはパブリックに復元できないようにすることをお勧めします
- [EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします
- [EC2.3] アタッチされた Amazon EBS ボリュームは、保管時に暗号化することをお勧めします
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします
- [EC2.7] EBS のデフォルト暗号化を有効にすることをお勧めします
- [EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.9] Amazon EC2 インスタンスは、パブリック IPv4 アドレスを未設定にすることをお勧めします
- [EC2.10] Amazon EC2 サービス用に作成された VPC エンドポイントを使用するようにAmazon EC2 を設定することをお勧めします
- [EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.15] Amazon EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないことをお勧めします

- [EC2.16] 未使用のネットワークアクセスコントロールリストを削除することをお勧めします
- [EC2.17] Amazon EC2 インスタンスが複数の ENI を使用しないようにすることをお勧めします
- [EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします
- [EC2.20] AWS Site-to-Site VPN 接続の両方の VPN トンネルが稼働している必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.34] EC2 トランジットゲートウェイルートテーブルにタグを付ける必要があります
- [EC2.40] EC2 NAT ゲートウェイにタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。
- [ECS.9] ECS タスク定義にはログ設定が必要です。
- [EFS .1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります
- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります

- [EFS .5] EFS アクセスポイントにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.3] Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります
- [ELB.4] Application Load Balancer は、http ヘッダーを削除するように設定する必要があります
- [ELB.5] アプリケーションおよび Classic Load Balancer の口グ記録を有効にする必要があります
- [ELB.6] Application、Gateway、Network Load Balancer では、削除保護を有効にする必要があります
- [ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な AWS Config設定を持つ事前定義されたセキュリティポリシーを使用する必要があります
- [ELB.9] Classic Load Balancer では、クロスゾーンロードバランシングが有効になっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- 〔ElastiCache.1] ElastiCache Redis クラスターでは自動バックアップを有効にする必要があります
- 〔ElastiCache.6]バージョン ElastiCache 6.0 より前の Redis レプリケーショングループでは、Redis AUTH を使用する必要があります
- 〔ElastiCache.7] ElastiCache クラスターはデフォルトのサブネットグループを使用しないでください
- 〔ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります

- 〔ElasticBeanstalk.2] Elastic Beanstalk マネージドプラットフォームの更新を有効にする必要があります
- 〔ElasticBeanstalk.3] Elastic Beanstalk はログを にストリーミングする必要があります CloudWatch
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります
- [ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります
- [ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります
- [ES.4] Logs への Elasticsearch CloudWatch ドメインエラーのログ記録を有効にする必要があります
- 〔EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります
- 〔EventBridge.3] EventBridge カスタムイベントバスには、リソースベースのポリシーがアタッチされている必要があります
- 〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.1] AWS Glue ジョブにはタグを付ける必要があります
- 〔GuardDuty.1] GuardDuty を有効にする必要があります
- 〔GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- 〔GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- 〔GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります

- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーはタグ付けする必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID には AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [IoT.1] AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [KMS.4] AWS KMS キーローテーションを有効にする必要があります
- [Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります
- [Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります
- [Lambda.3] Lambda 関数は VPC 内に存在する必要があります
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 自動機密データ検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch

- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.1] Network Firewall ファイアウォールは複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.2] Network Firewall のログ記録を有効にする必要があります
- 〔NetworkFirewall.3] Network Firewall ポリシーには、少なくとも 1 つのルールグループが関連付けられている必要があります
- 〔NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、フルパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、フラグメント化されたパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.6] ステートレス Network Firewall ルールグループは空にしないでください
- 〔NetworkFirewall.9] Network Firewall ファイアウォールでは、削除保護を有効にする必要があります

- [Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインにはタグを付ける必要があります
- [Opensearch.10] OpenSearch ドメインには最新のソフトウェア更新がインストールされている必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.1] RDS スナップショットはプライベートである必要があります
- [RDS.2] RDS DB インスタンスは、 PubliclyAccessible AWS Config設定によって決定されるパブリックアクセスを禁止する必要があります
- [RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。
- [RDS.4] RDS クラスタースナップショットとデータベーススナップショットは保管中に暗号化する必要があります
- [RDS.5] RDS DB インスタンスは、複数のアベイラビリティーゾーンで設定する必要があります
- [RDS.6] RDS DB インスタンスの拡張モニタリングを設定する必要があります
- [RDS.7] RDS クラスターでは、削除保護が有効になっている必要があります
- [RDS.8] RDS DB インスタンスで、削除保護が有効になっている必要があります
- [RDS.9] RDS DB インスタンスはログを CloudWatch Logs に発行する必要があります
- [RDS.10] IAM 認証は RDS インスタンス用に設定する必要があります
- [RDS.11] RDS インスタンスでは、自動バックアップが有効になっている必要があります
- [RDS.12] IAM 認証は RDS クラスター用に設定する必要があります
- [RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります

- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります
- [RDS.16] タグをスナップショットにコピーするように RDS DB クラスターを設定する必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [RDS.28] RDS DB クラスターにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [RDS.34] Aurora MySQL DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります
- [Redshift.2] Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります
- [Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります
- [Redshift.6] Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります
- [Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを ログに記録する必要があります
- [S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります
- [S3.5] S3 汎用バケットでは、SSL を使用するリクエストが必要です
- [S3.6] S3 汎用バケットポリシーでは、他の へのアクセスを制限する必要があります AWS アカウント
- [S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります
- [S3.9] S3 汎用バケットでは、サーバーアクセスのログ記録を有効にする必要があります

- [S3.15] S3 汎用バケットでは、オブジェクトロックを有効にする必要があります
- [S3.17] S3 汎用バケットは、保管時に で暗号化する必要があります AWS KMS keys
- 〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません
- 〔SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- 〔SageMaker.3] SageMaker ユーザーはノートブックインスタンスへのルートアクセスを許可されない
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- 〔SecretsManager.2] 自動ローテーションで設定された Secrets Manager シークレットは正常にローテーションする必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SNS.1] SNS トピックは、保管時に を使用して暗号化する必要があります AWS KMS
- [SNS.3] SNS トピックにはタグを付ける必要があります
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- 〔StepFunctions.1] Step Functions ステートマシンではログ記録が有効になっている必要があります
- [Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.2] AWS WAF クラシックリージョンルールには少なくとも 1 つの条件が必要です

- [WAF.3] AWS WAF クラシックリージョンルールグループには、少なくとも 1 つのルールが必要です
- [WAF.4] AWS WAF クラシックリージョンウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります

ヨーロッパ (ストックホルム)

ヨーロッパ (ストックホルム) では、以下のコントロールはサポートされていません。

- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません

- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラススナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります

- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを口グに記録する必要があります
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

欧州 (チューリッヒ)

以下のコントロールは欧州 (チューリッヒ) ではサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [APIGateway.1] API Gateway REST と WebSocket API 実行のログ記録を有効にする必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります
- [APIGateway.8] API Gateway ルートには認証タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- 〔AppSync.2] フィールドレベルのログ記録を有効にする AWS AppSync 必要があります
- 〔AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください

- [Athena.2] Athena データカタログにはタグを付ける必要があります
- [Athena.3] Athena ワークグループにはタグを付ける必要があります
- 〔AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要があります
- [Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.2] AWS Backup 復旧ポイントにタグを付ける必要があります
- [Backup.3] AWS Backup ボールトにはタグを付ける必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [Backup.5] AWS Backup バックアップ計画にはタグを付ける必要があります
- 〔CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションでは口グ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります

- 〔CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットがパブリックにアクセスできないようにする
- 〔CloudTrail.7] S3 バケットで CloudTrail S3 バケットアクセスログ記録が有効になっていることを確認する
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください
- 〔CodeBuild.2] CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください
- 〔CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- 〔CodeBuild.4] CodeBuild プロジェクト環境にはログ記録 AWS Config設定が必要です
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [Detective.1] Detective の動作グラフにはタグを付ける必要があります
- [DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です

- [DocumentDB.3] Amazon DocumentDB 手動クラススナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.1] DynamoDB テーブルは、需要に応じて容量をオートスケーリングする必要があります
- [DynamoDB.2] DynamoDB テーブルでは point-in-time リカバリを有効にする必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします
- [EC2.3] アタッチされた Amazon EBS ボリュームは、保管時に暗号化することをお勧めします
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします
- [EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.9] Amazon EC2 インスタンスは、パブリック IPv4 アドレスを未設定にすることをお勧めします
- [EC2.10] Amazon EC2 サービス用に作成された VPC エンドポイントを使用するようにAmazon EC2 を設定することをお勧めします
- [EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.15] Amazon EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないことをお勧めします
- [EC2.16] 未使用のネットワークアクセスコントロールリストを削除することをお勧めします
- [EC2.17] Amazon EC2 インスタンスが複数の ENI を使用しないようにすることをお勧めします
- [EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします

- [EC2.20] AWS Site-to-Site VPN 接続の両方の VPN トンネルが稼働している必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。
- [ECS.9] ECS タスク定義には ログ設定が必要です。
- [EFS .1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります
- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EFS .5] EFS アクセスポイントにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります

- [ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.3] Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります
- [ELB.4] Application Load Balancer は、http ヘッダーを削除するように設定する必要があります
- [ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な AWS Config設定を持つ事前定義されたセキュリティポリシーを使用する必要があります
- [ELB.9] Classic Load Balancer では、クロスゾーンロードバランシングが有効になっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- 〔ElastiCache.1] ElastiCache Redis クラスターでは自動バックアップを有効にする必要があります
- 〔ElastiCache.6]バージョン ElastiCache 6.0 より前の Redis レプリケーショングループでは、Redis AUTH を使用する必要があります
- 〔ElastiCache.7] ElastiCache クラスターはデフォルトのサブネットグループを使用しないでください
- 〔ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります
- 〔ElasticBeanstalk.2] Elastic Beanstalk マネージドプラットフォームの更新を有効にする必要があります
- 〔ElasticBeanstalk.3] Elastic Beanstalk はログを にストリーミングする必要があります CloudWatch
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります
- [ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります
- [ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります
- [ES.4] Logs への Elasticsearch CloudWatch ドメインエラーのログ記録を有効にする必要があります

- 〔EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります
- 〔EventBridge.3] EventBridge カスタムイベントバスには、リソースベースのポリシーがアタッチされている必要があります
- 〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.1] AWS Glue ジョブにはタグを付ける必要があります
- 〔GuardDuty.1] GuardDuty を有効にする必要があります
- 〔GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- 〔GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- 〔GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーはタグ付けする必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID には AWSCloudShellFullAccess ポリシーをアタッチしないでください

- [IoT.1] AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 自動機密データ検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラススナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラススナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります

- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.1] Network Firewall ファイアウォールは複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.2] Network Firewall のログ記録を有効にする必要があります
- 〔NetworkFirewall.3] Network Firewall ポリシーには、少なくとも 1 つのルールグループが関連付けられている必要があります
- 〔NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、フルパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、フラグメント化されたパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.6] ステートレス Network Firewall ルールグループは空にしないでください
- 〔NetworkFirewall.9] Network Firewall ファイアウォールでは、削除保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインにはタグを付ける必要があります
- [Opensearch.10] OpenSearch ドメインには最新のソフトウェア更新がインストールされている必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.1] RDS スナップショットはプライベートである必要があります

- [RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。
- [RDS.5] RDS DB インスタンスは、複数のアベイラビリティーゾーンで設定する必要があります
- [RDS.8] RDS DB インスタンスで、削除保護が有効になっている必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.16] タグをスナップショットにコピーするように RDS DB クラスターを設定する必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります
- [Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを口グに記録する必要があります
- [S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります
- [S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります
- 〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません
- 〔SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- 〔SageMaker.3] SageMaker ユーザーはノートブックインスタンスへのルートアクセスを許可されない
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- 〔SecretsManager.2] 自動口ーテーションで設定された Secrets Manager シークレットは正常に口ーテーションする必要があります

- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SNS.1] SNS トピックは、保管時に を使用して暗号化する必要があります AWS KMS
- [SNS.3] SNS トピックにはタグを付ける必要があります
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- 〔StepFunctions.1] Step Functions ステートマシンではログ記録が有効になっている必要があります
- [Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.2] AWS WAF クラシックリージョンルールには少なくとも 1 つの条件が必要です
- [WAF.3] AWS WAF クラシックリージョンルールグループには、少なくとも 1 つのルールが必要です
- [WAF.4] AWS WAF クラシックリージョンウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります

イスラエル (テルアビブ)

イスラエル (テルアビブ) では、以下のコントロールはサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [APIGateway.8] API Gateway ルートには認証タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- 〔AppSync.2] フィールドレベルのログ記録を有効にする AWS AppSync 必要があります
- 〔AppSync.4] AWS AppSync GraphQL APIsにはタグを付ける必要があります
- 〔AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- [Athena.2] Athena データカタログにはタグを付ける必要があります
- [Athena.3] Athena ワークグループにはタグを付ける必要があります
- [Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.2] AWS Backup 復旧ポイントにタグを付ける必要があります
- [Backup.3] AWS Backup ボールトにはタグを付ける必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [Backup.5] AWS Backup バックアップ計画にはタグを付ける必要があります
- 〔CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります

- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください
- 〔CodeBuild.2] CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください
- 〔CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- 〔CodeBuild.4] CodeBuild プロジェクト環境にはログ記録 AWS Config設定が必要です
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [Detective.1] Detective の動作グラフにはタグを付ける必要があります
- [DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります

- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラススナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.3] アタッチされた Amazon EBS ボリュームは、保管時に暗号化することをお勧めします
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします
- [EC2.10] Amazon EC2 サービス用に作成された VPC エンドポイントを使用するようにAmazon EC2 を設定することをお勧めします
- [EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします
- [EC2.20] AWS Site-to-Site VPN 接続の両方の VPN トンネルが稼働している必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.33] EC2 トランジットゲートウェイアタッチメントにはタグを付ける必要があります
- [EC2.34] EC2 トランジットゲートウェイルートテーブルにタグを付ける必要があります

- [EC2.40] EC2 NAT ゲートウェイにタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.52] EC2 トランジットゲートウェイにはタグを付ける必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。
- [ECS.9] ECS タスク定義にはログ設定が必要です。
- [EFS .1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります
- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EFS .5] EFS アクセスポイントにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [EKS.6] EKS クラスターにはタグを付ける必要があります
- [EKS.7] EKS ID プロバイダーの設定にはタグを付ける必要があります
- [EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります
- [ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager

- [ELB.4] Application Load Balancer は、http ヘッダーを削除するように設定する必要があります
- [ELB.6] Application、Gateway、Network Load Balancer では、削除保護を有効にする必要があります
- [ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な AWS Config設定を持つ事前定義されたセキュリティポリシーを使用する必要があります
- [ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- 〔ElastiCache.1] ElastiCache Redis クラスターでは自動バックアップを有効にする必要があります
- 〔ElastiCache.2]Redis キャッシュクラスター ElastiCache では、マイナーバージョン自動アップグレードを有効にする必要があります
- Redis ElastiCache レプリケーショングループの [ElastiCache.3] では、自動フェイルオーバーを有効にする必要があります
- 〔ElastiCache.4] ElastiCache for Redis レプリケーショングループは保管時に暗号化する必要があります
- Redis ElastiCache レプリケーショングループの [ElastiCache.5] は転送中に暗号化する必要があります
- 〔ElastiCache.6]バージョン ElastiCache 6.0 より前の Redis レプリケーショングループでは、Redis AUTH を使用する必要があります
- 〔ElastiCache.7] ElastiCache クラスターはデフォルトのサブネットグループを使用しないでください
- 〔ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります
- 〔ElasticBeanstalk.2] Elastic Beanstalk マネージドプラットフォームの更新を有効にする必要があります
- 〔ElasticBeanstalk.3] Elastic Beanstalk はログを にストリーミングする必要があります CloudWatch
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります

- [ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります
- [ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります
- [ES.4] Logs への Elasticsearch CloudWatch ドメインエラーのログ記録を有効にする必要があります
- 〔EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります
- 〔EventBridge.3] EventBridge カスタムイベントバスには、リソースベースのポリシーがアタッチされている必要があります
- 〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- 〔GuardDuty.1] GuardDuty を有効にする必要があります
- 〔GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- 〔GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- 〔GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.10] IAM ユーザーのパスワードポリシーには強力な AWS Config設定が必要です
- [IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します

- [IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します
- [IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します
- [IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します
- [IAM.15] 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します
- [IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています
- [IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します
- [IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.23] IAM Access Analyzer アナライザーにはタグを付ける必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーはタグ付けする必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID には AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [IAM.28] IAM Access Analyzer の外部アクセスアナライザーを有効にする必要があります
- [IoT.1] AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [Kinesis.2] Kinesis ストリームにはタグを付ける必要があります
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください

- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.1] Network Firewall ファイアウォールは複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.2] Network Firewall のログ記録を有効にする必要があります
- 〔NetworkFirewall.3] Network Firewall ポリシーには、少なくとも 1 つのルールグループが関連付けられている必要があります
- 〔NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、フルパケットに対してドロップまたは転送する必要があります

- 〔NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、フラグメント化されたパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.6] ステートレス Network Firewall ルールグループは空にしないでください
- 〔NetworkFirewall.9] Network Firewall ファイアウォールでは、削除保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインにはタグを付ける必要があります
- [Opensearch.10] OpenSearch ドメインには最新のソフトウェア更新がインストールされている必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [PCA.1] AWS Private CA ルート認証機関を無効にする必要があります
- [RDS.1] RDS スナップショットはプライベートである必要があります
- [RDS.4] RDS クラスタースナップショットとデータベーススナップショットは保管中に暗号化する必要があります
- [RDS.7] RDS クラスターでは、削除保護が有効になっている必要があります
- [RDS.8] RDS DB インスタンスで、削除保護が有効になっている必要があります
- [RDS.12] IAM 認証は RDS クラスター用に設定する必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります
- [RDS.16] タグをスナップショットにコピーするように RDS DB クラスターを設定する必要があります

- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [RDS.28] RDS DB クラスターにはタグを付ける必要があります
- [RDS.29] RDS DB クラススナップショットにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [RDS.34] Aurora MySQL DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります
- [Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください
- [Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください
- [Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを口グに記録する必要があります
- [S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります
- [S3.2] S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります
- [S3.3] S3 汎用バケットはパブリック書き込みアクセスをブロックする必要があります
- [S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります
- [S3.9] S3 汎用バケットでは、サーバーアクセスのログ記録を有効にする必要があります
- 〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません
- 〔SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- 〔SageMaker.3] SageMaker ユーザーはノートブックインスタンスへのルートアクセスを許可されない

- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- 〔SecretsManager.1] Secrets Manager シークレットでは、自動ローテーションを有効にする必要があります
- 〔SecretsManager.2] 自動ローテーションで設定された Secrets Manager シークレットは正常にローテーションする必要があります
- 〔SecretsManager.3] 未使用の Secrets Manager シークレットを削除する
- 〔SecretsManager.4] Secrets Manager のシークレットは、指定された日数内にローテーションする必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SNS.1] SNS トピックは、保管時に を使用して暗号化する必要があります AWS KMS
- [SNS.3] SNS トピックにはタグを付ける必要があります
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [SSM.4] SSM ドキュメントはパブリックにしないでください
- 〔StepFunctions.1] Step Functions ステートマシンでは口グ記録が有効になっている必要があります
- 〔StepFunctions.2] Step Functions アクティビティにはタグを付ける必要があります
- [Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.2] AWS WAF クラシックリージョンルールには少なくとも 1 つの条件が必要です

- [WAF.3] AWS WAF クラシックリージョンルールグループには、少なくとも 1 つのルールが必要です
- [WAF.4] AWS WAF クラシックリージョンウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります
- [WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります

中東 (バーレーン)

中東 (バーレーン) では、以下のコントロールはサポートされていません。

- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません

- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラススナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.20] AWS Site-to-Site VPN 接続の両方の VPN トンネルが稼働している必要があります
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- 〔ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります
- 〔ElasticBeanstalk.3] Elastic Beanstalk はログを にストリーミングする必要があります CloudWatch
- 〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります

- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- 〔GuardDuty.1] GuardDuty を有効にする必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.7] RDS クラスターでは、削除保護が有効になっている必要があります
- [RDS.12] IAM 認証は RDS クラスター用に設定する必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります
- [RDS.16] タグをスナップショットにコピーするように RDS DB クラスターを設定する必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [Redshift.6] Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを ログに記録する必要があります
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります

- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

中東 (アラブ首長国連邦)

中東 (UAE) では、以下のコントロールはサポートされていません。

- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [APIGateway.1] API Gateway REST と WebSocket API 実行のログ記録を有効にする必要があります
- [APIGateway.8] API Gateway ルートには認証タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- 〔AppSync.2] フィールドレベルのログ記録を有効にする AWS AppSync 必要があります
- 〔AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- [Athena.2] Athena データカタログにはタグを付ける必要があります
- [Athena.3] Athena ワークグループにはタグを付ける必要があります
- 〔AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要があります
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.2] AWS Backup 復旧ポイントにタグを付ける必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [Backup.5] AWS Backup バックアップ計画にはタグを付ける必要があります
- 〔CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります

- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CloudTrail.1] CloudTrail 読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン追跡を有効にして設定する必要があります
- 〔CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットがパブリックにアクセスできないようにする
- 〔CloudWatch.15] CloudWatch アラームには、指定されたアクションが設定されている必要があります
- 〔CloudWatch.16] CloudWatch ロググループは、指定された期間保持する必要があります
- 〔CloudWatch.17] CloudWatch アラームアクションを有効にする必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください
- 〔CodeBuild.2] CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください
- 〔CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります

- 〔CodeBuild.4] CodeBuild プロジェクト環境にはログ記録 AWS Config設定が必要です
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [Detective.1] Detective の動作グラフにはタグを付ける必要があります
- [DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.3] アタッチされた Amazon EBS ボリュームは、保管時に暗号化することをお勧めします

- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします
- [EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.12] 未使用の Amazon EC2 EIP を削除することをお勧めします
- [EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。
- [ECS.9] ECS タスク定義にはログ設定が必要です。
- [EFS .1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります

- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります
- [ELB.3] Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります
- [ELB.9] Classic Load Balancer では、クロスゾーンロードバランシングが有効になっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- 〔ElastiCache.1] ElastiCache Redis クラスターでは自動バックアップを有効にする必要があります
- 〔ElastiCache.2]Redis キャッシュクラスター ElastiCache では、マイナーバージョン自動アップグレードを有効にする必要があります
- Redis ElastiCache レプリケーショングループの [ElastiCache.3] では、自動フェイルオーバーを有効にする必要があります
- 〔ElastiCache.4] ElastiCache for Redis レプリケーショングループは保管時に暗号化する必要があります
- Redis ElastiCache レプリケーショングループの [ElastiCache.5] は転送中に暗号化する必要があります
- 〔ElastiCache.6]バージョン ElastiCache 6.0 より前の Redis レプリケーショングループでは、Redis AUTH を使用する必要があります
- 〔ElastiCache.7] ElastiCache クラスターはデフォルトのサブネットグループを使用しないでください
- 〔ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります

- 〔ElasticBeanstalk.2] Elastic Beanstalk マネージドプラットフォームの更新を有効にする必要があります
- 〔ElasticBeanstalk.3] Elastic Beanstalk はログを にストリーミングする必要があります CloudWatch
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- 〔EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります
- 〔EventBridge.3] EventBridge カスタムイベントバスには、リソースベースのポリシーがアタッチされている必要があります
- 〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- 〔GuardDuty.1] GuardDuty を有効にする必要があります
- 〔GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- 〔GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- 〔GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.18] でインシデントを管理するためのサポートロールが作成されていることを確認する AWS Support
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります

- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーはタグ付けする必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID には AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [IoT.1] AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [KMS.4] AWS KMS キーローテーションを有効にする必要があります
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 自動機密データ検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラススナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラススナップショットは、保管中に暗号化する必要があります

- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.1] Network Firewall ファイアウォールは複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.2] Network Firewall のログ記録を有効にする必要があります
- 〔NetworkFirewall.3] Network Firewall ポリシーには、少なくとも 1 つのルールグループが関連付けられている必要があります
- 〔NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、フルパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、フラグメント化されたパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.6] ステートレス Network Firewall ルールグループは空にしないでください
- 〔NetworkFirewall.7] Network Firewall ファイアウォールにはタグを付ける必要があります
- 〔NetworkFirewall.8] Network Firewall ファイアウォールポリシーにはタグを付ける必要があります
- 〔NetworkFirewall.9] Network Firewall ファイアウォールでは、削除保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります

- [Opensearch.9] OpenSearch ドメインにはタグを付ける必要があります
- [Opensearch.10] OpenSearch ドメインには最新のソフトウェア更新がインストールされている必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.1] RDS スナップショットはプライベートである必要があります
- [RDS.2] RDS DB インスタンスは、 PubliclyAccessible AWS Config設定によって決定されるパブリックアクセスを禁止する必要があります
- [RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。
- [RDS.5] RDS DB インスタンスは、複数のアベイラビリティーゾーンで設定する必要があります
- [RDS.6] RDS DB インスタンスの拡張モニタリングを設定する必要があります
- [RDS.8] RDS DB インスタンスで、削除保護が有効になっている必要があります
- [RDS.11] RDS インスタンスでは、自動バックアップが有効になっている必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.16] タグをスナップショットにコピーするように RDS DB クラスターを設定する必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください
- [Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを口グに記録する必要があります
- [S3.2] S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります
- [S3.3] S3 汎用バケットはパブリック書き込みアクセスをブロックする必要があります
- [S3.5] S3 汎用バケットでは、SSL を使用するリクエストが必要です
- [S3.6] S3 汎用バケットポリシーでは、他の へのアクセスを制限する必要があります AWS アカウント

- [S3.14] S3 汎用バケットではバージョニングを有効にする必要があります
- 〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません
- 〔SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- 〔SageMaker.3] SageMaker ユーザーはノートブックインスタンスへのルートアクセスを許可されない
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- 〔SecretsManager.1] Secrets Manager シークレットでは、自動ローテーションを有効にする必要があります
- 〔SecretsManager.2] 自動ローテーションで設定された Secrets Manager シークレットは正常にローテーションする必要があります
- 〔SecretsManager.3] 未使用の Secrets Manager シークレットを削除する
- 〔SecretsManager.4] Secrets Manager のシークレットは、指定された日数内にローテーションする必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SNS.1] SNS トピックは、保管時に を使用して暗号化する必要があります AWS KMS
- [SNS.3] SNS トピックにはタグを付ける必要があります
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager
- 〔StepFunctions.1] Step Functions ステートマシンではログ記録が有効になっている必要があります
- [Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.2] AWS WAF クラシックリージョンルールには少なくとも 1 つの条件が必要です

- [WAF.3] AWS WAF クラシックリージョンルールグループには、少なくとも 1 つのルールが必要です
- [WAF.4] AWS WAF クラシックリージョンウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります

南米 (サンパウロ)

南米 (サンパウロ) では、以下のコントロールはサポートされていません。

- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません

- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IoT.1] AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [RDS.7] RDS クラスターでは、削除保護が有効になっている必要があります
- [RDS.12] IAM 認証は RDS クラスター用に設定する必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります

- [RDS.16] タグをスナップショットにコピーするように RDS DB クラスターを設定する必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを口グに記録する必要があります
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL 口グ記録を有効にする必要があります
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

AWS GovCloud （ 米国東部 ）

（ AWS GovCloud 米国東部) では、以下のコントロールはサポートされていません。

- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [ACM.3] ACM 証明書にはタグを付ける必要があります
- [Account.1] のセキュリティ連絡先情報を に提供する必要があります AWS アカウント
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります
- [APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります

- [APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります
- [APIGateway.8] API Gateway ルートには認証タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- 〔AppSync.2] フィールドレベルのログ記録を有効にする AWS AppSync 必要があります
- 〔AppSync.4] AWS AppSync GraphQL APIsにはタグを付ける必要があります
- 〔AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- [Athena.2] Athena データカタログにはタグを付ける必要があります
- [Athena.3] Athena ワークグループにはタグを付ける必要があります
- 〔AutoScaling.2] Amazon EC2 Auto Scaling グループは複数のアベイラビリティーゾーンをカバーする必要があります
- 〔AutoScaling.3] Auto Scaling グループの起動設定では、インスタンスメタデータサービスバージョン 2 (IMDSv2) を要求するように EC2 インスタンスを設定する必要がありますIMDSv2
- 〔AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります
- 〔AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります
- 〔AutoScaling.10] EC2 Auto Scaling グループにタグを付ける必要があります
- [Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません
- [Backup.2] AWS Backup 復旧ポイントにタグを付ける必要があります
- [Backup.3] AWS Backup ボールトにはタグを付ける必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [Backup.5] AWS Backup バックアップ計画にはタグを付ける必要があります
- 〔CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションでは口グ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります

- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください
- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CloudTrail.9] CloudTrail 証跡にはタグを付ける必要があります
- 〔CloudWatch.15] CloudWatch アラームには、指定されたアクションが設定されている必要があります
- 〔CloudWatch.16] CloudWatch ロググループは、指定された期間保持する必要があります
- 〔CloudWatch.17] CloudWatch アラームアクションを有効にする必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください
- 〔CodeBuild.2] CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください
- 〔CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- 〔CodeBuild.4] CodeBuild プロジェクト環境にはログ記録 AWS Config設定が必要です
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [Detective.1] Detective の動作グラフにはタグを付ける必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにタグを付ける必要があります

- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.1] DynamoDB テーブルは、需要に応じて容量をオートスケーリングする必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.5] DynamoDB テーブルにはタグを付ける必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.15] Amazon EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないことをお勧めします
- [EC2.16] 未使用のネットワークアクセスコントロールリストを削除することをお勧めします
- [EC2.17] Amazon EC2 インスタンスが複数の ENI を使用しないようにすることをお勧めします
- [EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします

- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.33] EC2 トランジットゲートウェイアタッチメントにはタグを付ける必要があります
- [EC2.34] EC2 トランジットゲートウェイルートテーブルにタグを付ける必要があります
- [EC2.35] EC2 ネットワークインターフェイスにタグを付ける必要があります
- [EC2.36] EC2 カスタマーゲートウェイにはタグを付ける必要があります
- [EC2.37] EC2 Elastic IP アドレスにタグを付ける必要があります
- [EC2.38] EC2 インスタンスにはタグを付ける必要があります
- [EC2.39] EC2 インターネットゲートウェイにはタグを付ける必要があります
- [EC2.40] EC2 NAT ゲートウェイにタグを付ける必要があります
- [EC2.41] EC2 ネットワーク ACLs にはタグを付ける必要があります
- [EC2.42] EC2 ルートテーブルにはタグを付ける必要があります
- [EC2.43] EC2 セキュリティグループにタグを付ける必要があります
- [EC2.44] EC2 サブネットにはタグを付ける必要があります
- [EC2.45] EC2 ボリュームにはタグを付ける必要があります
- [EC2.46] Amazon VPCsにはタグを付ける必要があります
- [EC2.47] Amazon VPC エンドポイントサービスにはタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります
- [EC2.49] Amazon VPC ピアリング接続にはタグを付ける必要があります
- [EC2.50] EC2 VPN ゲートウェイにはタグを付ける必要があります
- [EC2.52] EC2 トランジットゲートウェイにはタグを付ける必要があります
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります

- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。
- [ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください
- [ECS.4] ECS コンテナは、非特権として実行する必要があります
- [ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。
- [ECS.8] シークレットは、コンテナ環境の変数として渡さないでください
- [ECS.9] ECS タスク定義には ログ設定が必要です。
- [ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。
- [ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります
- [ECS.13] ECS サービスはタグ付けする必要があります
- [ECS.14] ECS クラスターにはタグを付ける必要があります
- [ECS.15] ECS タスク定義にはタグを付ける必要があります
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります
- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EFS .5] EFS アクセスポイントにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [EKS.6] EKS クラスターにはタグを付ける必要があります
- [EKS.7] EKS ID プロバイダーの設定にはタグを付ける必要があります
- [EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な AWS Config設定を持つ事前定義されたセキュリティポリシーを使用する必要があります

- [ELB.10] Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります
- [ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- 〔ElastiCache.1] ElastiCache Redis クラスターでは自動バックアップを有効にする必要があります
- 〔ElastiCache.2]Redis キャッシュクラスター ElastiCache では、マイナーバージョン自動アップグレードを有効にする必要があります
- Redis ElastiCache レプリケーショングループの [ElastiCache.3] では、自動フェイルオーバーを有効にする必要があります
- 〔ElastiCache.4] ElastiCache for Redis レプリケーショングループは保管時に暗号化する必要があります
- Redis ElastiCache レプリケーショングループの [ElastiCache.5] は転送中に暗号化する必要があります
- 〔ElastiCache.6]バージョン ElastiCache 6.0 より前の Redis レプリケーショングループでは、Redis AUTH を使用する必要があります
- 〔ElastiCache.7] ElastiCache クラスターはデフォルトのサブネットグループを使用しないでください
- 〔ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります
- 〔ElasticBeanstalk.2] Elastic Beanstalk マネージドプラットフォームの更新を有効にする必要があります
- 〔ElasticBeanstalk.3] Elastic Beanstalk はログを にストリーミングする必要があります CloudWatch
- [EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります
- [ES.4] Logs への Elasticsearch CloudWatch ドメインエラーのログ記録を有効にする必要があります
- [ES.9] Elasticsearch ドメインにはタグを付ける必要があります

- 〔EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります
- 〔EventBridge.3] EventBridge カスタムイベントバスには、リソースベースのポリシーがアタッチされている必要があります
- 〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.1] AWS Glue ジョブにはタグを付ける必要があります
- 〔GuardDuty.1] GuardDuty を有効にする必要があります
- 〔GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- 〔GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- 〔GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.23] IAM Access Analyzer アナライザーにはタグを付ける必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーはタグ付けする必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.28] IAM Access Analyzer の外部アクセスアナライザーを有効にする必要があります
- [IoT.1] AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります

- [Kinesis.2] Kinesis ストリームにはタグを付ける必要があります
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Lambda.6] Lambda 関数にはタグを付ける必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 自動機密データ検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラススナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラススナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.1] Network Firewall ファイアウォールは複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.2] Network Firewall のログ記録を有効にする必要があります
- 〔NetworkFirewall.3] Network Firewall ポリシーには、少なくとも 1 つのルールグループが関連付けられている必要があります

- 〔NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、フルパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、フラグメント化されたパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.6] ステートレス Network Firewall ルールグループは空にしないでください
- 〔NetworkFirewall.7] Network Firewall ファイアウォールにはタグを付ける必要があります
- 〔NetworkFirewall.8] Network Firewall ファイアウォールポリシーにはタグを付ける必要があります
- 〔NetworkFirewall.9] Network Firewall ファイアウォールでは、削除保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインにはタグを付ける必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [PCA.1] AWS Private CA ルート認証機関を無効にする必要があります
- [RDS.12] IAM 認証は RDS クラスター用に設定する必要があります
- [RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります

- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [RDS.28] RDS DB クラスターにはタグを付ける必要があります
- [RDS.29] RDS DB クラスタースナップショットにはタグを付ける必要があります
- [RDS.30] RDS DB インスタンスにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [RDS.32] RDS DB スナップショットにはタグを付ける必要があります
- [RDS.33] RDS DB サブネットグループにタグを付ける必要があります
- [RDS.34] Aurora MySQL DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります
- [Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください
- [Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.11] Redshift クラスターにはタグを付ける必要があります
- [Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります
- [Redshift.13] Redshift クラスタースナップショットにはタグを付ける必要があります
- [Redshift.14] Redshift クラスターサブネットグループにタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリを ログに記録する必要があります
- [S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります
- [S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります
- [S3.10] バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です
- [S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります
- [S3.12] ACLs を使用しないでください S3

- [S3.13] S3 汎用バケットにはライフサイクル設定が必要です
- [S3.14] S3 汎用バケットではバージョニングを有効にする必要があります
- [S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります
- 〔SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできません
- 〔SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- 〔SageMaker.3] SageMaker ユーザーはノートブックインスタンスへのルートアクセスを許可されない
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- 〔SecretsManager.3] 未使用の Secrets Manager シークレットを削除する
- 〔SecretsManager.4] Secrets Manager のシークレットは、指定された日数内にローテーションする必要があります
- 〔SecretsManager.5] Secrets Manager のシークレットにはタグを付ける必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SNS.3] SNS トピックにはタグを付ける必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SSM.4] SSM ドキュメントはパブリックにしないでください
- 〔StepFunctions.1] Step Functions ステートマシンでは口グ記録が有効になっている必要があります
- 〔StepFunctions.2] Step Functions アクティビティにはタグを付ける必要があります
- [Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL 口グ記録を有効にする必要があります
- [WAF.2] AWS WAF クラシックリージョンルールには少なくとも 1 つの条件が必要です
- [WAF.3] AWS WAF クラシックリージョンルールグループには、少なくとも 1 つのルールが必要です

- [WAF.4] AWS WAF クラシックリージョンウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります
- [WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります

AWS GovCloud （米国西部）

（ AWS GovCloud 米国西部) では、以下のコントロールはサポートされていません。

- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [ACM.3] ACM 証明書にはタグを付ける必要があります
- [Account.1] のセキュリティ連絡先情報を に提供する必要があります AWS アカウント
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります
- [APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります
- [APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります
- [APIGateway.8] API Gateway ルートには認証タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- 〔AppSync.2] フィールドレベルのログ記録を有効にする AWS AppSync 必要があります
- 〔AppSync.4] AWS AppSync GraphQL APIsにはタグを付ける必要があります
- 〔AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- [Athena.2] Athena データカタログにはタグを付ける必要があります

- [Athena.3] Athena ワークグループにはタグを付ける必要があります
- 〔AutoScaling.2] Amazon EC2 Auto Scaling グループは複数のアベイラビリティーゾーンをカバーする必要があります
- 〔AutoScaling.3] Auto Scaling グループの起動設定では、インスタンスメタデータサービスバージョン 2 (IMDSv2) を要求するように EC2 インスタンスを設定する必要がありますIMDSv2
- 〔AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります
- 〔AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります
- 〔AutoScaling.10] EC2 Auto Scaling グループにタグを付ける必要があります
- [Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません
- [Backup.2] AWS Backup 復旧ポイントにタグを付ける必要があります
- [Backup.3] AWS Backup ボールトにはタグを付ける必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [Backup.5] AWS Backup バックアップ計画にはタグを付ける必要があります
- 〔CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- 〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります
- 〔CloudFront.3] CloudFront ディストリビューションには転送中の暗号化が必要です
- 〔CloudFront.4] CloudFront ディストリビューションにはオリジンフェイルオーバーが設定されている必要があります
- 〔CloudFront.5] CloudFront ディストリビューションではログ記録を有効にする必要があります
- 〔CloudFront.6] CloudFront ディストリビューションでは WAF を有効にする必要があります
- 〔CloudFront.7] CloudFront ディストリビューションはカスタム SSL/TLS 証明書を使用する必要があります
- 〔CloudFront.8] CloudFront ディストリビューションは SNI を使用して HTTPS リクエストを処理する必要があります
- 〔CloudFront.9] CloudFront ディストリビューションはカスタムオリジンへのトラフィックを暗号化する必要があります
- 〔CloudFront.10] CloudFront ディストリビューションでは、エッジロケーションとカスタムオリジン間で非推奨の SSL プロトコルを使用しないでください

- 〔CloudFront.12] CloudFront ディストリビューションは存在しない S3 オリジンを指してはいけません
- 〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります
- 〔CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- 〔CloudTrail.9] CloudTrail 証跡にはタグを付ける必要があります
- 〔CloudWatch.15] CloudWatch アラームには、指定されたアクションが設定されている必要があります
- 〔CloudWatch.16] CloudWatch ロググループは、指定された期間保持する必要があります
- 〔CloudWatch.17] CloudWatch アラームアクションを有効にする必要があります
- 〔CodeArtifact.1]CodeArtifact リポジトリにはタグを付ける必要があります
- 〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください
- 〔CodeBuild.2] CodeBuild プロジェクト環境変数にはクリアテキスト認証情報を含めないでください
- 〔CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- 〔CodeBuild.4] CodeBuild プロジェクト環境にはログ記録 AWS Config設定が必要です
- 〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [Detective.1] Detective の動作グラフにはタグを付ける必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります

- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります
- [DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.1] DynamoDB テーブルは、需要に応じて容量をオートスケーリングする必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.5] DynamoDB テーブルにはタグを付ける必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります
- [EC2.15] Amazon EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないことをお勧めします
- [EC2.16] 未使用のネットワークアクセスコントロールリストを削除することをお勧めします
- [EC2.17] Amazon EC2 インスタンスが複数の ENI を使用しないようにすることをお勧めします
- [EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.33] EC2 トランジットゲートウェイアタッチメントにはタグを付ける必要があります
- [EC2.34] EC2 トランジットゲートウェイルートテーブルにタグを付ける必要があります
- [EC2.35] EC2 ネットワークインターフェイスにタグを付ける必要があります

- [EC2.36] EC2 カスタマーゲートウェイにはタグを付ける必要があります
- [EC2.37] EC2 Elastic IP アドレスにタグを付ける必要があります
- [EC2.38] EC2 インスタンスにはタグを付ける必要があります
- [EC2.39] EC2 インターネットゲートウェイにはタグを付ける必要があります
- [EC2.40] EC2 NAT ゲートウェイにタグを付ける必要があります
- [EC2.41] EC2 ネットワーク ACLs にはタグを付ける必要があります
- [EC2.42] EC2 ルートテーブルにはタグを付ける必要があります
- [EC2.43] EC2 セキュリティグループにタグを付ける必要があります
- [EC2.44] EC2 サブネットにはタグを付ける必要があります
- [EC2.45] EC2 ボリュームにはタグを付ける必要があります
- [EC2.46] Amazon VPCsにはタグを付ける必要があります
- [EC2.47] Amazon VPC エンドポイントサービスにはタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります
- [EC2.49] Amazon VPC ピアリング接続にはタグを付ける必要があります
- [EC2.50] EC2 VPN ゲートウェイにはタグを付ける必要があります
- [EC2.52] EC2 トランジットゲートウェイにはタグを付ける必要があります
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。
- [ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください
- [ECS.4] ECS コンテナは、非特権として実行する必要があります
- [ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。
- [ECS.8] シークレットは、コンテナ環境の変数として渡さないでください
- [ECS.9] ECS タスク定義にはログ設定が必要です。

- [ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。
- [ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります
- [ECS.13] ECS サービスはタグ付けする必要があります
- [ECS.14] ECS クラスターにはタグを付ける必要があります
- [ECS.15] ECS タスク定義にはタグを付ける必要があります
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります
- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EFS .5] EFS アクセスポイントにはタグを付ける必要があります
- [EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません
- [EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [EKS.6] EKS クラスターにはタグを付ける必要があります
- [EKS.7] EKS ID プロバイダーの設定にはタグを付ける必要があります
- [EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります
- [ELB.10] Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります
- [ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- 〔ElastiCache.1] ElastiCache Redis クラスターでは自動バックアップを有効にする必要があります
- 〔ElastiCache.2]Redis キャッシュクラスター ElastiCache では、マイナーバージョン自動アップグレードを有効にする必要があります

- Redis ElastiCache レプリケーショングループの [ElastiCache.3] では、自動フェイルオーバーを有効にする必要があります
- 〔ElastiCache.4] ElastiCache for Redis レプリケーショングループは保管時に暗号化する必要があります
- Redis ElastiCache レプリケーショングループの [ElastiCache.5] は転送中に暗号化する必要があります
- 〔ElastiCache.6]バージョン ElastiCache 6.0 より前の Redis レプリケーショングループでは、Redis AUTH を使用する必要があります
- 〔ElastiCache.7] ElastiCache クラスターはデフォルトのサブネットグループを使用しないでください
- 〔ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります
- 〔ElasticBeanstalk.2] Elastic Beanstalk マネージドプラットフォームの更新を有効にする必要があります
- 〔ElasticBeanstalk.3] Elastic Beanstalk はログを にストリーミングする必要があります CloudWatch
- [EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります
- [ES.4] Logs への Elasticsearch CloudWatch ドメインエラーのログ記録を有効にする必要があります
- [ES.9] Elasticsearch ドメインにはタグを付ける必要があります
- 〔EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります
- 〔EventBridge.3] EventBridge カスタムイベントバスには、リソースベースのポリシーがアタッチされている必要があります
- 〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります
- 〔GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.1] AWS Glue ジョブにはタグを付ける必要があります
- 〔GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- 〔GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります

- 〔GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.23] IAM Access Analyzer アナライザーにはタグを付ける必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーはタグ付けする必要があります
- [IAM.28] IAM Access Analyzer の外部アクセスアナライザーを有効にする必要があります
- [IoT.1] AWS IoT Core セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [Kinesis.2] Kinesis ストリームにはタグを付ける必要があります
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Lambda.6] Lambda 関数にはタグを付ける必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 自動機密データ検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch
- [MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります

- [Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.1] Network Firewall ファイアウォールは複数のアベイラビリティーゾーンにデプロイする必要があります
- 〔NetworkFirewall.2] Network Firewall のログ記録を有効にする必要があります
- 〔NetworkFirewall.3] Network Firewall ポリシーには、少なくとも 1 つのルールグループが関連付けられている必要があります
- 〔NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、フルパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、フラグメント化されたパケットに対してドロップまたは転送する必要があります
- 〔NetworkFirewall.6] ステートレス Network Firewall ルールグループは空にしないでください
- 〔NetworkFirewall.7] Network Firewall ファイアウォールにはタグを付ける必要があります
- 〔NetworkFirewall.8] Network Firewall ファイアウォールポリシーにはタグを付ける必要があります
- 〔NetworkFirewall.9] Network Firewall ファイアウォールでは、削除保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインでは、保管時の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch ログへの OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録が有効になっている必要があります

- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインでは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインにはタグを付ける必要があります
- [Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です
- [PCA.1] AWS Private CA ルート認証機関を無効にする必要があります
- [RDS.12] IAM 認証は RDS クラスター用に設定する必要があります
- [RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [RDS.28] RDS DB クラスターにはタグを付ける必要があります
- [RDS.29] RDS DB クラスタースナップショットにはタグを付ける必要があります
- [RDS.30] RDS DB インスタンスにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにタグを付ける必要があります
- [RDS.32] RDS DB スナップショットにはタグを付ける必要があります
- [RDS.33] RDS DB サブネットグループにタグを付ける必要があります
- [RDS.34] Aurora MySQL DB クラスターは監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります
- [Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください
- [Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください

- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.11] Redshift クラスターにはタグを付ける必要があります
- [Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります
- [Redshift.13] Redshift クラススナップショットにはタグを付ける必要があります
- [Redshift.14] Redshift クラスターサブネットグループにタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります
- [S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります
- [S3.10] バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です
- [S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります
- [S3.12] ACLs を使用しないでください S3
- [S3.13] S3 汎用バケットにはライフサイクル設定が必要です
- [S3.14] S3 汎用バケットではバージョニングを有効にする必要があります
- [S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります
- 〔SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- 〔SageMaker.3] SageMaker ユーザーはノートブックインスタンスへのルートアクセスを許可されない
- 〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- 〔SecretsManager.3] 未使用の Secrets Manager シークレットを削除する
- 〔SecretsManager.4] Secrets Manager のシークレットは、指定された日数内にローテーションする必要があります
- 〔SecretsManager.5] Secrets Manager のシークレットにはタグを付ける必要があります
- 〔ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります

- [SNS.3] SNS トピックにはタグを付ける必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SSM.4] SSM ドキュメントはパブリックにしないでください
- 〔StepFunctions.1] Step Functions ステートマシンでは ログ記録が有効になっている必要があります
- 〔StepFunctions.2] Step Functions アクティビティにはタグを付ける必要があります
- [Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [WAF.1] AWS WAF クラシックグローバルウェブ ACL ログ記録を有効にする必要があります
- [WAF.2] AWS WAF クラシックリージョンルールには少なくとも 1 つの条件が必要です
- [WAF.3] AWS WAF クラシックリージョンルールグループには、少なくとも 1 つのルールが必要です
- [WAF.4] AWS WAF クラシックリージョンウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります
- [WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります

Security Hub を無効にする

> **Note**
>
> 中央設定を使用すると、AWS Security Hub 委任管理者は、特定のアカウントや組織単位 (OU) で Security Hub を無効にする設定ポリシーを作成し、他のアカウントや OU では有効のままにすることができます。設定ポリシーは、ホームリージョンとすべてのリンクされたリージョンで有効になります。詳細については、「中央設定の仕組み」を参照してください。

Security Hub を無効にするには、Security Hub コンソール、Security Hub API または AWS CLI を使用します。

アカウントで Security Hub を無効にすると、次のようになります。

- そのアカウントの新しい検出結果は処理されません。
- 90 日後、既存の結果とインサイト、および Security Hub の構成設定は削除され、回復できなくなります。

  既存の結果を保存する場合は、Security Hub を無効にする前にそれらをエクスポートする必要があります。詳細については、「the section called “アカウントアクションが Security Hub データに及ぼす影響”」を参照してください。
- 有効な標準およびコントロールはすべて無効になります。

次の場合は、Security Hub を無効にできません。

- アカウントが組織の委任された Security Hub 管理者アカウントである場合。中央設定を使用する場合、Security Hub を無効にする設定ポリシーを、委任管理者アカウントに関連付けることはできません。関連付けは他のアカウントでは成功する可能性がありますが、Security Hub ではこのようなポリシーは委任管理者アカウントに適用されません。
- アカウントが招待による Security Hub 管理者アカウントであり、有効になっているメンバーアカウントがある場合。Security Hub を無効にするには、すべてのメンバーアカウントの関連付けを解除する必要があります。「the section called “メンバーアカウントの関連付けを解除する”」を参照してください。

メンバーアカウントで Security Hub を無効にするには、そのアカウントの関連付けを管理者アカウントから解除する必要があります。組織アカウントの場合、メンバーアカウントの関連付けを解除できるのは管理者アカウントのみです。詳細については、「the section called “組織メンバーアカウントの関連付けを解除する”」を参照してください。手動で招待されたアカウントの場合は、管理者アカウントまたはメンバーアカウントのいずれかでメンバーアカウントの関連付けを解除できます。詳細については、「the section called “メンバーアカウントの関連付けを解除する”」または「the section called “管理者アカウントから関連付けを解除する”」を参照してください。特定のメンバーアカウントで Security Hub を無効にするポリシーを作成できるため、中央設定を使用する場合は関連付けを解除する必要はありません。

アカウントで Security Hub を無効にすると、現在のリージョンでのみ無効になります。ただし、中央設定を使用して特定のアカウントで Security Hub を無効にすると、ホームリージョンとすべてのリンクされたリージョンで無効になります。

ご希望の方法を選択し、手順に従って Security Hub を無効にします。

Security Hub console

Security Hub を無効にするには

1. AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。
2. ナビゲーションペインで [設定] を選択します。
3. [Settings] (設定) ページで [General] (全般) を選択します。
4. [Disable AWS Security Hub] (AWS Security Hub を無効化) で、[Disable AWS Security Hub] (AWS Security Hub を無効化) を選択します。次に [Disable AWS Security Hub] (AWS Security Hub を無効化) を再度選択します。

Security Hub API

Security Hub を無効にするには

`DisableSecurityHub` API を呼び出します。

AWS CLI

Security Hub を無効にするには

`disable-security-hub` コマンドを実行します。

コマンドの例:

```
aws securityhub disable-security-hub
```

Security Hub コントロールの変更ログ

次の変更ログは、既存の AWS Security Hub セキュリティコントロールへの重要な変更を追跡します。これにより、コントロールの全体的なステータスとその検出結果のコンプライアンスステータスが変更される可能性があります。Security Hub がコントロールステータスをどのように評価するかは、「コンプライアンスステータスとコントロールステータス」を参照してください。 AWS リージョン コントロールが利用可能なすべての に影響を与えるには、このログへの入力から数日かかる場合があります。

このログは、2023 年 4 月以降に発生した変更を追跡します。

コントロールを選択すると、その詳細が表示されます。タイトルの変更は、各コントロールの 90 日間の詳細な説明に記載されています。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 6 月 25 日	[Config.1] AWS Config を有効にし、サービスにリンクされたロールをリソース記録に使用する必要があります	このコントロール AWS Config は、 が有効になっているかどうか、サービスにリンクされたロールを使用しているかどうか、有効なコントロールのリソースを記録します。Security Hub は、コントロールが評価する内容を反映するようにコントロールタイトルを更新しました。
2024 年 6 月 14 日	[RDS.34] Aurora MySQL DB クラスターは監査ログを CloudWatch Logs に発行する必要があります	このコントロールは、Amazon Aurora MySQL DB クラスターが監査ログを Amazon CloudWatch Logs に発行するよ

変更日	コントロール ID とタイトル	変更点の説明
		うに設定されているかどうかをチェックします。Security Hub は、Aurora Serverless v1 DB クラスターの検出結果を生成しないようにコントロールを更新しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 6 月 10 日	[Config.1] AWS Config を有効にし、サービスにリンクされたロールをリソース記録に使用する必要があります	このコントロール AWS Config は、 が有効で、 AWS Config リソース記録が有効になっているかどうかをチェックします。以前は、コントロールは、すべてのリソースの記録を設定した場合にのみPASSED検出結果を生成していました。Security Hub は、有効なコントロールに必要なリソースの記録が有効になっている場合にPASSED検出結果を生成するようにコントロールを更新しました。また、サービスにリンクされたロールが使用されているかどうかを確認する AWS Config ようにコントロールが更新されました。これにより、必要なリソースを記録するためのアクセス許可が提供されます。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 5 月 8 日	[S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります	このコントロールは、Amazon S3 汎用バージョニングバケットで多要素認証 (MFA) 削除が有効になっているかどうかをチェックします。以前は、コントロールはライフサイクル設定を持つバケットFAILEDの結果を生成していました。ただし、ライフサイクル設定を持つバケットでは、バージョニングによる MFA 削除を有効にすることはできません。Security Hub は、ライフサイクル設定を持つバケットの検出結果を生成しないようにコントロールを更新しました。コントロールの説明が更新され、現在の動作が反映されました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 5 月 2 日	[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。	Security Hub は、Amazon EKS クラスターを実行できる、サポートされている最も古いバージョンの Kubernetes を更新し、検出結果を生成しました。現在サポートされている最も古いバージョンは Kubernetes 1.26 です。
2024 年 4 月 30 日	〔CloudTrail.3] 少なくとも 1 つの CloudTrail 証跡を有効にする必要があります	コントロールタイトルを から CloudTrail に変更しました。少なくとも 1 つの CloudTrail 証跡を有効にする必要があります。このコントロールは、 で少なくとも 1 つの CloudTrail 証跡が有効になっている場合 AWS アカウント 、現在PASSED検出結果を生成します。タイトルと説明は、現在の動作を正確に反映するように変更されました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 29 日	〔AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要があります	Classic Load Balancer に関連付けられた Auto Scaling グループがロードバランサーのヘルスチェックを使用するようにコントロールタイトルを変更し、ロードバランサーに関連付けられた Auto Scaling グループが ELB ヘルスチェックを使用するように変更しました。このコントロールは現在、Application、Gateway、Network、Classic Load Balancer を評価します。タイトルと説明は、現在の動作を正確に反映するように変更されました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 19 日	〔CloudTrail.1] CloudTrail 読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン追跡を有効にして設定する必要があります	コントロール AWS CloudTrail は、読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン証跡が有効で設定されているかどうかを確認します。以前は、証跡が読み取り/書き込み管理イベントをキャプチャしていない場合でも、アカウントが少なくとも 1 つのマルチリージョン証跡 CloudTrail を有効にして設定したときに、コントロールが誤ってPASSED検出結果を生成していました。コントロールは、 CloudTrail が有効で、読み取りおよび書き込み管理イベントをキャプチャする少なくとも 1 つのマルチリージョン追跡で設定されている場合にのみ、PASSED結果を生成するようになりました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 10 日	[Athena.1] Athena ワークグループは保管時に暗号化する必要があります	Security Hub はこのコントロールを廃止し、すべての標準から削除しました。Athena ワークグループは、Amazon Simple Storage Service (Amazon S3) バケットにログを送信します。Amazon S3 では、新規および既存の S3 バケットで S3 マネージドキー (SS3-S3) によるデフォルトの暗号化を提供するようになりました。
2024 年 4 月 10 日	〔AutoScaling.4] Auto Scaling グループの起動設定では、メタデータレスポンスホップ制限が 1 より大きくなってはなりません	Security Hub はこのコントロールを廃止し、すべての標準から削除しました。Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのメタデータレスポンスホップ制限は、ワークロードによって異なります。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 10 日	〔CloudFormation.1] CloudFormation スタックは Simple Notification Service (SNS) と統合する必要があります	Security Hub はこのコントロールを廃止し、すべての標準から削除しました。 AWS CloudFormation スタックと Amazon SNS トピックの統合は、セキュリティのベストプラクティスではなくなりました。重要な CloudFormation スタックを SNS トピックと統合することは便利ですが、すべてのスタックに必須ではありません。
2024 年 4 月 10 日	〔CodeBuild.5] CodeBuild プロジェクト環境では特権モードを有効にしないでください	Security Hub はこのコントロールを廃止し、すべての標準から削除しました。プロジェクトで CodeBuild 特権モードを有効にしても、顧客環境に追加のリスクは生じません。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 10 日	[IAM.20] ルートユーザーの使用を避ける	Security Hub はこのコントロールを廃止し、すべての標準から削除しました。このコントロールの目的は、別のコントロール でカバーされています〔CloudWatch.1]「ルート」ユーザーの使用に対してログメトリクスフィルターとアラームが存在する必要があります。
2024 年 4 月 10 日	[SNS.2] トピックに送信される通知メッセージの配信ステータスのログ記録を有効にする必要があります	Security Hub はこのコントロールを廃止し、すべての標準から削除しました。SNS トピックの配信ステータスのログ記録は、セキュリティのベストプラクティスではなくなりました。重要な SNS トピックの配信ステータスのログ記録は便利ですが、すべてのトピックで必須ではありません。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 10 日	[S3.10] バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です	Security Hub は AWS 、 Foundational Security Best Practices と Service-Managed Standard: からこのコントロールを削除しました AWS Control Tower。このコントロールの目的は、 [S3.13] S3 汎用バケットにはライフサイクル設定が必要です と の 2 つの他のコントロールでカバーされています[S3.14] S3 汎用バケットではバージョニングを有効にする必要があります。このコントロールは、NIST SP 800-53 Rev. 5 の一部です。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 10 日	[S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります	Security Hub は AWS 、 Foundational Security Best Practices と Service-Managed Standard: からこのコントロールを削除しました AWS Control Tower。S3 バケットのイベント通知が役立つ場合もありますが、これは一般的なセキュリティのベストプラクティスではありません。このコントロールは、NIST SP 800-53 Rev. 5 の一部です。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 10 日	[SNS.1] SNS トピックは、保管時に を使用して暗号化する必要があります AWS KMS	Security Hub は AWS 、 Foundational Security Best Practices と Service-Managed Standard: からこのコントロールを削除しました AWS Control Tower。SNS はすでにデフォルトでトピックを暗号化しているため、 を使用してトピック AWS KMS を暗号化することは、セキュリティのベストプラクティスとして推奨されなくなりました。このコントロールは、NIST SP 800-53 Rev. 5 の一部です。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 8 日	[ELB.6] Application、Gateway、Network Load Balancer では、削除保護を有効にする必要があります	Application Application Load Balancer の削除保護を有効にする必要があるコントロールタイトルを Application、Gateway、Network Load Balancer で削除保護を有効にする必要があるコントロールタイトルに変更しました。このコントロールは現在、Application、Gateway、Network Load Balancer を評価します。タイトルと説明は、現在の動作を正確に反映するように変更されました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 22 日	[Opensearch.8] OpenSearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります	コントロールタイトルを「接続」から OpenSearch 「ドメインへの暗号化」から OpenSearch 「ドメインへの接続」は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります」に変更しました。以前は、コントロールは OpenSearch ドメインへの接続が TLS 1.2 を使用しているかどうかのみを確認していました。OpenSearch ドメインが最新の TLS セキュリティポリシーを使用して暗号化されている場合、コントロールは検出PASSED結果を生成するようになりました。コントロールのタイトルと説明が更新され、現在の動作が反映されました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 22 日	[ES.8] Elasticsearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります	コントロールタイトルを Connections から Elasticsearch ドメインに変更しました。TLS 1.2 を使用して暗号化する必要があります。Elasticsearch ドメインへの接続は、最新の TLS セキュリティポリシーを使用して暗号化する必要があります。以前は、コントロールは Elasticsearch ドメインへの接続が TLS 1.2 を使用しているかどうかのみを確認していました。このコントロールは、Elasticsearch ドメインが最新の TLS セキュリティポリシーを使用して暗号化されている場合に検出PASSED結果を生成するようになりました。コントロールのタイトルと説明が更新され、現在の動作が反映されました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 12 日	[S3.1] S3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります	タイトルをS3 パブリックアクセスブロック設定を有効にする」からS3 汎用バケットでは、パブリックアクセスブロック設定を有効にする必要があります」に変更しました。Security Hub は、新しい S3 バケットタイプを考慮してタイトルを変更しました。
2024 年 3 月 12 日	[S3.2] S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります	タイトルを S3 バケットから変更した場合、S3 汎用バケットへのパブリック読み取りアクセスを禁止する必要があります。パブリック読み取りアクセスをブロックする必要がありますS3。Security Hub は、新しい S3 バケットタイプを考慮してタイトルを変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 12 日	[S3.3] S3 汎用バケットはパブリック書き込みアクセスをブロックする必要があります	タイトルを S3 バケットから変更した場合、S3 汎用バケットへのパブリック書き込みアクセスを禁止する必要があります。パブリック書き込みアクセスをブロックする必要がありますS3。Security Hub は、新しい S3 バケットタイプを考慮してタイトルを変更しました。
2024 年 3 月 12 日	[S3.5] S3 汎用バケットでは、SSL を使用するリクエストが必要です	タイトルを S3 バケットから変更した場合、Secure Socket Layer を使用するリクエストを S3 汎用バケットに要求する場合は、SSL を使用するリクエストが必要です。Security Hub は、新しい S3 バケットタイプを考慮してタイトルを変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 12 日	[S3.6] S3 汎用バケットポリシーでは、他の へのアクセスを制限する必要があります AWS アカウント	バケットポリシー AWS アカウント で他の に付与された S3 アクセス許可のタイトルを変更した場合は、S3 汎用バケットポリシーで他の へのアクセスを制限する必要がありますS3 AWS アカウント。Security Hub は、新しい S3 バケットタイプを考慮してタイトルを変更しました。
2024 年 3 月 12 日	[S3.7] S3 汎用バケットはクロスリージョンレプリケーションを使用する必要があります	タイトルをS3 バケットではクロスリージョンレプリケーションを有効にする必要があります」からS3 汎用バケットではクロスリージョンレプリケーションを使用する必要があります」に変更しました。Security Hub は、新しい S3 バケットタイプを考慮してタイトルを変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 12 日	[S3.7] S3 汎用バケットはクロスリージョンレプリケーションを使用する必要があります	タイトルをS3 バケットではクロスリージョンレプリケーションを有効にする必要があります」からS3 汎用バケットではクロスリージョンレプリケーションを使用する必要があります」に変更しました。Security Hub は、新しい S3 バケットタイプを考慮してタイトルを変更しました。
2024 年 3 月 12 日	[S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります	タイトルをS3 パブリックアクセスブロック」設定からS3 汎用バケットはパブリックアクセスをブロックする」に変更しました。Security Hub は、新しい S3 バケットタイプを考慮してタイトルを変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 12 日	[S3.9] S3 汎用バケットでは、サーバーアクセスのログ記録を有効にする必要があります	タイトルをS3 バケットサーバーのアクセスログ記録を有効にする必要があります」からS3 汎用バケットのサーバーアクセスログ記録を有効にする必要があります」に変更しました。Security Hub は、新しい S3 バケットタイプを考慮してタイトルを変更しました。
2024 年 3 月 12 日	[S3.10] バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です	タイトルをバージョニングが有効になっている S3 バケットに変更しました。ライフサイクルポリシーは、バージョニングが有効になっている S3 汎用バケットに設定されている必要があります。ライフサイクル設定はです。Security Hub は、新しい S3 バケットタイプを考慮してタイトルを変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 12 日	[S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります	タイトルをS3 バケットではイベント通知が有効になっている必要があります」からS3 汎用バケットではイベント通知が有効になっている必要があります」に変更しました。Security Hub は、新しい S3 バケットタイプを考慮してタイトルを変更しました。
2024 年 3 月 12 日	[S3.12] ACLs を使用しないでください S3	タイトルをS3 アクセスコントロールリスト (ACL)」から「ACL へのユーザーアクセスの管理ACLsACLsS3 汎用バケット へのユーザーアクセスの管理」に変更しました。Security Hub は、新しい S3 バケットタイプを考慮してタイトルを変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 12 日	[S3.13] S3 汎用バケットにはライフサイクル設定が必要です	タイトルをS3 バケット」から「S3 汎用バケット」にライフサイクルポリシーを設定する必要がありますS3「」に変更しました。Security Hub は、新しい S3 バケットタイプを考慮してタイトルを変更しました。
2024 年 3 月 12 日	[S3.14] S3 汎用バケットではバージョニングを有効にする必要があります	タイトルをS3 バケットはバージョニングを使用する」からS3 汎用バケットではバージョニングが有効になっている必要があります」に変更しました。Security Hub は、新しい S3 バケットタイプを考慮してタイトルを変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 12 日	[S3.15] S3 汎用バケットでは、オブジェクトロックを有効にする必要があります	タイトルを S3 バケットから S3 汎用バケットにオブジェクトロックを使用するように設定し、オブジェクトロックを有効にする必要がありますS3。Security Hub は、新しい S3 バケットタイプを考慮してタイトルを変更しました。
2024 年 3 月 12 日	[S3.17] S3 汎用バケットは、保管時に で暗号化する必要があります AWS KMS keys	タイトルをS3 バケットは保管時に で暗号化 AWS KMS keysする必要があります」からS3 汎用バケットは保管時に で暗号化する必要があります AWS KMS keys」に変更しました。Security Hub は、新しい S3 バケットタイプを考慮してタイトルを変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 7 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub で、パラメータ`ruby3.3`として `nodejs20.x` およびがサポートされるようになりました。
2024 年 2 月 22 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub では、パラメータとして `dotnet8` がサポートされるようになりました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 2 月 5 日	[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。	Security Hub は、Amazon EKS クラスターを実行できる、サポートされている最も古いバージョンの Kubernetes を更新し、検出結果を生成しました。現在サポートされている最も古いバージョンは Kubernetes 1.25 です。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 1 月 10 日	〔CodeBuild.1] CodeBuild Bitbucket ソースリポジトリ URLsには機密認証情報を含めないでください	タイトルを CodeBuild GitHub または Bitbucket ソースリポジトリ URLsしました。OAuth から CodeBuild Bitbucket ソースリポジトリ URLs に機密認証情報を含めないでください。Security Hub では、他の接続方法も安全である可能性があるため、OAuth に関する言及を削除しました。Security Hub では、 GitHub ソースリポジトリ URL に個人用のアクセストークンまたはユーザー名とパスワードを持つことができなくなる GitHub ため、 への言及を削除しました。 URLs

変更日	コントロール ID とタイトル	変更点の説明
2024 年 1 月 8 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。廃止されたランタイムであるため、Security Hub ではパラメータとして `go1.x` および `java8` がサポートされなくなりました。
2023 年 12 月 29 日	[RDS.8] RDS DB インスタンスで、削除保護が有効になっている必要があります	RDS.8 は、サポートされているデータベースエンジンのいずれかを使用する Amazon RDS DB インスタンスで削除保護が有効になっているかどうかをチェックします。Security Hub では `custom-oracle-ee`、`oracle-ee-cdb` 、および `oracle-se2-cdb` がデータベースエンジンとしてサポートされるようになりました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 12 月 22 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub では、パラメータとして `java21` および `python3.12` がサポートされるようになりました。Security Hub では、パラメータとして `ruby2.7` がサポートされなくなりました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 12 月 15 日	〔CloudFront.1] CloudFront ディストリビューションにはデフォルトのルートオブジェクトが設定されている必要があります	CloudFront.1 は、Amazon CloudFront ディストリビューションにデフォルトのルートオブジェクトが設定されているかどうかを確認します。Security Hub では、このコントロールの重大度が CRITICAL から HIGH に下げられました。これは、デフォルトルートオブジェクトを追加することがユーザーのアプリケーションと特定の要件に依存する推奨事項であるためです。
2023 年 12 月 5 日	[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります	コントロールタイトルが「セキュリティグループでは 0.0.0.0/0 からポート 22 へのイングレスは許可しない必要があります」から「セキュリティグループでは 0.0.0.0/0 または ::/0 からポート 22 へのイングレスは許可しない必要があります」に変更されました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 12 月 5 日	[EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります	コントロールタイトルが「セキュリティグループでは 0.0.0.0/0 からポート 3389 へのイングレスは許可されないことを確認します」から「セキュリティグループでは 0.0.0.0/0 または ::/0 からポート 3389 へのイングレスは許可しない必要があります」に変更されました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 12 月 5 日	[RDS.9] RDS DB インスタンスはログを CloudWatch Logs に発行する必要があります	コントロールタイトルを「データベースログ記録を有効にする必要があります」から「RDS DB インスタンスはログを CloudWatch に発行する必要があります」に変更しました。Security Hub は、このコントロールがログが Amazon CloudWatch Logs に発行されているかどうかのみをチェックし、RDS ログが有効になっているかどうかをチェックしないことを特定しました。このコントロールは、RDS DB インスタンスがログを CloudWatch Logs に発行するように設定されている場合、PASSED結果を生成します。コントロールタイトルは、現在の動作を反映して更新されました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 11 月 17 日	[EC2.19] セキュリティグループは、リスクの高いポートへの無制限アクセスを許可してはいけません	EC2.19 は、指定した高リスクと見なされるポートにセキュリティグループの無制限の受信トラフィックがアクセス可能かどうかをチェックします。Security Hub では、セキュリティグループルールのソースとして提供される場合、マネージド型プレフィックスリストを考慮するようにこのコントロールが更新されました。コントロールは、プレフィックスリストに文字列「0.0.0.0/0」または「::/0」が含まれている場合、FAILED 検出結果を生成します。
2023 年 11 月 16 日	〔CloudWatch.15] CloudWatch アラームには、指定されたアクションが設定されている必要があります	コントロールタイトルが、CloudWatch アラームに ALARM 状態用に設定されたアクションが必要から、 CloudWatch アラームに指定されたアクションが設定されたことに変更されました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 11 月 16 日	〔CloudWatch.16] CloudWatch ロググループは、指定された期間保持する必要があります	CloudWatch ロググループのコントロールタイトルを少なくとも 1 年間保持し、CloudWatch ロググループを指定された期間 にわたって保持するように変更しました。
2023 年 11 月 16 日	[Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります	コントロールタイトルが「VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります」から「VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります」に変更されました。
2023 年 11 月 16 日	〔AppSync.2] フィールドレベルのログ記録を有効にする AWS AppSync 必要があります	コントロールタイトルが「AWS AppSync は、リクエストレベルとフィールドレベルのログ記録をオンにする必要があります」から「AWS AppSync はフィールドレベルのログ記録を有効にする必要があります」に変更されました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 11 月 16 日	[EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります	コントロールタイトルが Amazon Elastic MapReduce クラスターマスターノードにパブリック IP アドレスがあってはなりません。Amazon EMR クラスタープライマリノードにパブリック IP アドレスがあってはなりません。
2023 年 11 月 16 日	[Opensearch.2] OpenSearch ドメインはパブリックアクセス可能であってはなりません	コントロールタイトルをOpenSearch ドメインから VPC に変更し、OpenSearchドメインをパブリックアクセス可能な にすることはできません。
2023 年 11 月 16 日	[ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります	コントロールタイトルが「Elasticsearch ドメインは VPC 内に含まれている必要があります」から「Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります」に変更されました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 10 月 31 日	[ES.4] Logs への Elasticsearch CloudWatch ドメインエラーのログ記録を有効にする必要があります	ES.4 は、Elasticsearch ドメインが Amazon CloudWatch Logs にエラーログを送信するように設定されているかどうかを確認します。コントロールは、以前に、 ログに送信するようにログが設定された Elasticsearch CloudWatch ドメインPASSEDの結果を生成しました。Security Hub は、エラーログを CloudWatch Logs に送信するように設定された Elasticsearch ドメインPASSEDのみの結果を生成するようにコントロールを更新しました。コントロールも更新され、エラーログをサポートしない Elasticsearch バージョンを評価から除外するようになりました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 10 月 16 日	[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります	EC2.13 は、セキュリティグループがポート 22 への無制限のイングレスアクセスを許可しているかどうかをチェックします。Security Hub では、セキュリティグループルールのソースとして提供される場合、マネージド型プレフィックスリストを考慮するようにこのコントロールが更新されました。コントロールは、プレフィックスリストに文字列「0.0.0.0/0」または「::/0」が含まれている場合、FAILED 検出結果を生成します。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 10 月 16 日	[EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります	EC2.14 は、セキュリティグループがポート 3389 への無制限のイングレスアクセスを許可しているかどうかをチェックします。Security Hub では、セキュリティグループルールのソースとして提供される場合、マネージド型プレフィックスリストを考慮するようにこのコントロールが更新されました。コントロールは、プレフィックスリストに文字列「0.0.0.0/0」または「::/0」が含まれている場合、FAILED 検出結果を生成します。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 10 月 16 日	[EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします	EC2.18 は、使用中のセキュリティグループが、無制限の受信トラフィックを許可しているかどうかをチェックします。Security Hub では、セキュリティグループルールのソースとして提供される場合、マネージド型プレフィックスリストを考慮するようにこのコントロールが更新されました。コントロールは、プレフィックスリストに文字列「0.0.0.0/0」または「::/0」が含まれている場合、FAILED 検出結果を生成します。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 10 月 16 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub では、パラメータとして `python3.11` がサポートされるようになりました。
2023 年 10 月 4 日	[S3.7] S3 汎用バケットはクロスリージョンレプリケーションを使用する必要があります	Security Hub は、S3 `CROSS-REGION` バケットで同じリージョンのレプリケーションではなくクロスリージョンレプリケーションを有効にするために、`ReplicationType` という値を持つパラメータが追加されました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 9 月 27 日	[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。	Security Hub は、Amazon EKS クラスターを実行できる、サポートされている最も古いバージョンの Kubernetes を更新し、検出結果を生成しました。現在サポートされている最も古いバージョンは Kubernetes 1.24 です。
2023 年 9 月 20 日	CloudFront.2 – CloudFront ディストリビューションではオリジンアクセスアイデンティティを有効にする必要があります	Security Hub はこのコントロールを廃止し、すべての標準から削除しました。代わりに、「〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります」を参照してください。オリジンのアクセスコントロールは、現在のセキュリティのベストプラクティスです。このコントロールは 90 日後にドキュメントから削除されます。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 9 月 20 日	[EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします	Security Hub は AWS 、 Foundational Security Best Practices (FSBP) および米国国立標準技術研究所 (NIST) SP 800-53 Rev. 5 からこのコントロールを削除しました。これはまだサービスマネージドスタンダードの一部です AWS Control Tower。この コントロールでは、セキュリティグループが EC2 インスタンス、または Elastic Network Interface にアタッチされている場合に、合格の検出結果を生成します。ただし、特定のユースケースでは、セキュリティグループがアタッチされていなくてもセキュリティ上のリスクはありません。他の EC2 コントロール (EC2.2、EC2.13、EC2.14、EC2.18、EC2.19 など) を使用すると、セキュリティグルー

変更日	コントロール ID とタイトル	変更点の説明
		プをモニタリングできます。
2023 年 9 月 20 日	EC2.29 — EC2 インスタンスは VPC で起動することをお勧めします	Security Hub はこのコントロールを廃止し、すべての標準から削除しました。Amazon EC2 では、EC2-Classic インスタンスが VPC に移行されました。このコントロールは 90 日後にドキュメントから削除されます。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 9 月 20 日	S3.4 - S3 バケットでは、サーバー側の暗号化を有効にする必要があります	Security Hub はこのコントロールを廃止し、すべての標準から削除しました。Amazon S3 では、新規および既存の S3 バケットで S3 マネージドキー (SS3-S3) によるデフォルトの暗号化を提供するようになりました。SS3-S3 または SS3-KMS のサーバー側の暗号化を使用して暗号化された既存のバケットの場合、暗号化設定は変更されません。このコントロールは 90 日後にドキュメントから削除されます。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 9 月 14 日	[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします	コントロールタイトルを「VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックとアウトバウンドトラフィックを許可しないようにする必要があります」から「VPC のデフォルトのセキュリティグループ (複数可) では、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにする必要があります」に変更しました。
2023 年 9 月 14 日	[IAM.9] ルートユーザーに対して MFA を有効にする必要があります	コントロールタイトルを「ルートユーザーに対して仮想 MFA を有効にする必要があります」から「ルートユーザーに対して MFA を有効にする必要があります」に変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 9 月 14 日	[RDS.19] 重大なクラスターイベントについて、既存の RDS イベント通知サブスクリプションを設定する必要があります	コントロールタイトルを「重大なクラスターイベントについて、RDS イベント通知のサブスクリプションを設定する必要があります」から「重大なクラスターイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります」に変更しました。
2023 年 9 月 14 日	[RDS.20] 重大なデータベースインスタンスイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります	コントロールタイトルを「重大なデータベースインスタンスイベントに対して RDS イベント通知サブスクリプションを設定する必要があります」から「重大なデータベースインスタンスイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります」に変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 9 月 14 日	[WAF.2] AWS WAF クラシックリージョンルールには少なくとも 1 つの条件が必要です	コントロールタイトルを「WAF リージョンルールには、1 つ以上の条件が必要です」から「AWS WAF Classic リージョンルールには、1 つ以上の条件が必要です」に変更しました。
2023 年 9 月 14 日	[WAF.3] AWS WAF クラシックリージョンルールグループには、少なくとも 1 つのルールが必要です	コントロールタイトルを「WAF リージョンルールグループには、1 つ以上の条件が必要です」から「AWS WAF Classic リージョンルールグループには、1 つ以上の条件が必要です」に変更しました。
2023 年 9 月 14 日	[WAF.4] AWS WAF クラシックリージョンウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です	コントロールタイトルを「WAF リージョンウェブ ACL には、1 つ以上のルールまたはルールグループが必要です」から「AWS WAF Classic リージョンウェブ ACL には、1 つ以上のルールまたはルールグループが必要です」に変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 9 月 14 日	[WAF.6] AWS WAF クラシックグローバルルールには少なくとも 1 つの条件が必要です	コントロールタイトルを「WAF グローバルルールには、1 つ以上の条件が必要です」から「AWS WAF Classic グローバルルールには、1 つ以上の条件が必要です」に変更しました。
2023 年 9 月 14 日	[WAF.7] AWS WAF クラシックグローバルルールグループには、少なくとも 1 つのルールが必要です	コントロールタイトルを「WAF グローバルルールグループには、1 つ以上の条件が必要です」から「AWS WAF Classic グローバルルールグループには、1 つ以上の条件が必要です」に変更しました。
2023 年 9 月 14 日	[WAF.8] AWS WAF クラシックグローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です	コントロールタイトルを「WAF グローバルウェブ ACL には、1 つ以上のルールまたはルールグループが必要です」から「AWS WAF Classic グローバルウェブ ACL には、1 つ以上のルールまたはルールグループが必要です」に変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 9 月 14 日	[WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です	コントロールタイトルを「WAFv2 ウェブ ACL には、1 つ以上のルールまたはルールグループが必要です」から「AWS WAF ウェブ ACL には、1 つ以上のルールまたはルールグループが必要です」に変更しました。
2023 年 9 月 14 日	[WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります	コントロールタイトルを「AWS WAF v2 ウェブ ACL ログ記録を有効にする必要があります」から「AWS WAF ウェブ ACL ログ記録を有効にする必要があります」に変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 7 月 20 日	S3.4 - S3 バケットでは、サーバー側の暗号化を有効にする必要があります	S3.4 は、Amazon S3 バケットでサーバー側の暗号化が有効になっているか、または S3 バケットポリシーでサーバー側の暗号化なしの `PutObject` リクエストを明示的に拒否しているかどうかをチェックします。Security Hub はこのコントロールを更新し、KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS) を追加しました。S3 バケットが SSE-S3、SSE-KMS、または DSSE-KMS で暗号化されている場合、このコントロールは合格の検出結果を生成します。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 7 月 17 日	[S3.17] S3 汎用バケットは、保管時に で暗号化する必要があります AWS KMS keys	S3.17 は Amazon S3 バケットが AWS KMS keyで暗号化されているかどうかをチェックします。Security Hub はこのコントロールを更新し、KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS) を追加しました。S3 バケットが SSE-KMS または DSSE-KMS で暗号化されている場合、このコントロールは合格の検出結果を生成します。
2023 年 6 月 9 日	[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。	EKS.2 は、Amazon EKS クラスターがサポートされている Kubernetes バージョンで実行されているかどうかをチェックします。サポートされている最も古いバージョンは現在のところ、1.23 です。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 6 月 9 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub では、パラメータとして `ruby3.2` がサポートされるようになりました。
2023 年 6 月 5 日	[APIGateway.5] API Gateway REST API のキャッシュデータは、保管中に暗号化する必要があります	APIGateway.5. は、Amazon API Gateway REST API ステージのすべてのメソッドが保存時に暗号化されているかどうかをチェックします。Security Hub を更新し、特定のメソッドのキャッシュが有効になっている場合にのみ、そのメソッドの暗号化を評価するようにしました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 5 月 18 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub では、パラメータとして `java17` がサポートされるようになりました。
2023 年 5 月 18 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub では、パラメータとして `nodejs12.x` がサポートされなくなりました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 4 月 23 日	[ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。	ECS.10 は、Amazon ECS Fargate サービスが最新の Fargate プラットフォームバージョンで実行されているかどうかをチェックします。お客様は、ECS から直接、または を使用して Amazon ECS をデプロイできます CodeDeploy。Security Hub は、 を使用して ECS Fargate サービスをデプロイするときに、合格の検出結果を生成するようにこのコントロールを更新しました。CodeDeploy

変更日	コントロール ID とタイトル	変更点の説明
2023 年 4 月 20 日	[S3.6] S3 汎用バケットポリシーでは、他の へのアクセスを制限する必要があります AWS アカウント	S3.6 は、Amazon Simple Storage Service (Amazon S3) バケットポリシーによって、他の のプリンシパルが S3 バケット内のリソースに対して AWS アカウント 拒否されたアクションを実行できないかどうかを確認します。Security Hub では、このコントロールが更新され、バケットポリシーの条件を考慮するようになりました。
2023 年 4 月 18 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub では、パラメータとして `python3.10` がサポートされるようになりました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 4 月 18 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub では、パラメータとして `dotnetcore3.1` がサポートされなくなりました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 4 月 17 日	[RDS.11] RDS インスタンスでは、自動バックアップが有効になっている必要があります	RDS.11 は、Amazon RDS インスタンスで自動バックアップが有効になっているかどうか、およびバックアップ保持期間が 7 日以上であるかどうかをチェックします。Security Hub では、このコントロールが更新され、リードレプリカを評価から除外するようになりました。すべてのエンジンがリードレプリカの自動バックアップをサポートしているわけではないためです。また、RDS には、リードレプリカの作成時にバックアップ保持期間を指定するオプションはありません。リードレプリカは、デフォルトでバックアップ保持期間 `0` で作成されます。

AWS Security Hub ユーザーガイドのドキュメント履歴

次の表に、 AWS Security Hub のドキュメントの更新を示します。

> **Note**
>
> セキュリティコントロールリリースの場合、指定された日付はすべてのアカウントとリージョンでコントロールが利用可能になる日付です。コントロールがすべてのアカウントとリージョンに反映されるまで、1～2 週間かかることがあります。

変更	説明	日付
CIS AWS Foundations Benchmark v3.0.0 のリリース	Security Hub は、Center for Internet Security (CIS) AWS Foundations Benchmark v3.0.0 をリリースしました。このリリースには、以下の新しいコントロールと、いくつかの既存のコントロールへのマッピングが含まれています。 • the section called “[EC2.53] EC2 セキュリティグループは、0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可しないでください” • the section called “[EC2.54] EC2 セキュリティグループは、::/0 からリモートサーバー管理ポートへの入力を許可しないでください” • the section called “[IAM.26] IAM で管理されている期限	2024 年 5 月 13 日

切れの SSL/TLS 証明書は削除する必要があります”

- the section called “[IAM.27] IAM ID には AWSCloudShellFullAccess ポリシーをアタッチしないでください”
- the section called “[IAM.28] IAM Access Analyzer の外部アクセスアナライザーを有効にする必要があります”
- the section called “[S3.22] S3 汎用バケットは、オブジェクトレベルの書き込みイベントをログに記録する必要があります”
- the section called “[S3.23] S3 汎用バケットは、オブジェクトレベルの読み取りイベントをログに記録する必要があります”

新しいセキュリティコントロール	次の新しい Security Hub コントロールが使用できます。 • the section called “〔DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります” • the section called “[DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証を有効にする必要があります” • the section called “[DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムを有効にする必要があります” • the section called “[DMS.12] Redis の DMS エンドポイントでは TLS を有効にする必要があります” • the section called “[DynamoDB.7] DynamoDB Accelerator クラスターは転送中に暗号化する必要があります” • the section called “[EFS .6] EFS マウントターゲットをパブリックサブネットに関連付けるべきではありません” • the section called “[EKS.3] EKS クラスターは暗号化された Kubernetes シークレッ	2024 年 5 月 3 日

トを使用する必要があります”

- the section called “[FSx.2] FSx for Lustre ファイルシステムは、タグをバックアップにコピーするように設定する必要があります”
- the section called “[MQ.2] ActiveMQ ブローカーは監査ログを にストリーミングする必要があります CloudWatch”
- the section called “[MQ.3] Amazon MQ ブローカーでは、マイナーバージョンの自動アップグレードを有効にする必要があります”
- the section called “[Opensearch.11] OpenSearch ドメインには、少なくとも 3 つの専用プライマリノードが必要です”
- the section called “[Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの進入を許可する必要があります”
- the section called “〔SageMaker.4] SageMaker エンドポイントの本番稼働用バリアントの初期インスタンス数は 1 より大きい必要があります”

	• the section called “〔Service Catalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります” • the section called “[Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください”	
AWS リソースタグ付け標準	Security Hub の AWS Resource Tagging Standard が、標準に適用される新しいコントロールとともに一般公開されました。	2024 年 4 月 30 日
既存の マネージドポリシーの更新	Security Hub は、 AWS のサービス と 製品の料金詳細を取得`AmazonSecurityHubFullAccess` するために、という名前の AWS マネージドポリシーを更新しました。	2024 年 4 月 24 日
コントロールパラメータのコンテキスト内設定	中央設定を使用する場合、Security Hub コンソールのコントロールの詳細ページから、コンテキスト でコントロールパラメータを設定できるようになりました。	2024 年 3 月 29 日
既存の マネージドポリシーの更新	Security Hub は、 という名前の AWS マネージドポリシーを更新`AWSSecurityHubReadOnlyAccess` し、`Sid`フィールドを追加しました。	2024 年 2 月 22 日

新しいセキュリティコントロール	コントロール [Macie.2] Macie 自動機密データ検出を有効にすることができるようになりました。このコントロールのリージョン制限については、「リージョン別のコントロールの可用性」を参照してください。	2024 年 2 月 19 日
カナダ西部 (カルガリー) で利用可能になった Security Hub	Security Hub をカナダ西部 (カルガリー) でご利用いただけるようになりました。このリージョンでは、特定のセキュリティコントロールを除き、すべての Security Hub 機能を利用できるようになりました。詳細については、「リージョン別のコントロールの可用性」を参照してください。	2023 年 12 月 20 日

新しいセキュリティコントロール	次の新しい Security Hub コントロールが使用できます。 • the section called “[Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります” • the section called “[DynamoDB.6] DynamoDB テーブルで、削除保護が有効になっている必要があります” • the section called “[EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります” • the section called “[EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります” • the section called “[EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります” • the section called “[FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります” • the section called “[Macie.1] Amazon Macie を有効にする必要があります”	2023 年 12 月 14 日

- the section called “[MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります”
- the section called “[Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります”
- the section called “〔NetworkFirewall.1] Network Firewall ファイアウォールは複数のアベイラビリティーゾーンにデプロイする必要があります”
- the section called “〔NetworkFirewall.2] Network Firewall のログ記録を有効にする必要があります”
- the section called “[Opensearch.10] OpenSearch ドメインには最新のソフトウェア更新がインストールされている必要があります”
- the section called “[PCA.1] AWS Private CA ルート認証機関を無効にする必要があります”
- the section called “[S3.19] S3 アクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります”

	• the section called “[S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります”	
検出結果の強化	Security Hub は、新しい検出結果フィールド `AwsAccountName` 、`ApplicationArn` 、 `ApplicationName` を AWS Security Finding 形式 (ASFF) に追加しました。	2023 年 11 月 27 日
[概要] ダッシュボードの機能強化	Security Hub コンソールの [概要] ページで、より多くのダッシュボードウィジェットにアクセスでき、ダッシュボードのフィルターセットを保存して特定のセキュリティ問題にすばやく焦点を当てたり、ダッシュボードレイアウトをカスタマイズしたりできるようになりました。	2023 年 11 月 27 日
中央設定	中央設定が利用可能になりました。Security Hub 委任管理者は、中央設定を使用して、複数の組織アカウント、組織単位 (OU)、リージョンで Security Hub、標準、およびコントロールを設定できます。	2023 年 11 月 27 日

マネージドポリシーの更新	Security Hub でカスタマイズ可能なセキュリティコントロールプロパティを読み取りおよび更新できる新しいアクセス許可が `AWSSecurityHubServiceRolePolicy` 管理ポリシーに追加されました。	2023 年 11 月 26 日
カスタムコントロールパラメータ	Security Hub コントロールの選択でパラメータ値をカスタマイズできるようになりました。これにより、特定のコントロールの検出結果をビジネス要件やセキュリティ上の期待とより関連性のあるものにすることができます。	2023 年 11 月 26 日
マネージドポリシーの更新	Security Hub は`AWSSecurityHubFullAccess` 、Security Hub 機能と との統合をそれぞれ使用できるようにする および `AWSSecurityHubOrganizationsAccess` マネージドポリシーを更新しました AWS Organizations。	2023 年 11 月 16 日

サービスマネージドスタンダードに追加された既存のセキュリティコントロール：AWS Control Tower	以下の既存の Security Hub コントロールがサービスマネージドスタンダードに追加されました AWS Control Tower。 • ACM.2 • AppSync.5 • CloudTrail.6 • DMS.9 • DocumentDB.3 • DynamoDB.3 • EC2.23 • EKS.1 • ElastiCache.3 • ElastiCache.4 • ElastiCache.5 • ElastiCache.6 • EventBridge.3 • KMS.4 • Lambda.3 • MQ.5 • MQ.6 • MSK.1 • RDS.12 • RDS.15 • S3.17	2023 年 11 月 14 日

マネージドポリシーの更新	Security Hub は、検出結果に関連するリソースタグを読み取ることができる新しいタグ付け権限を管理ポリシー`AWSSecurityHubServiceRolePolicy` に追加しました。	2023 年 11 月 7 日

新しいセキュリティコントロール	次の新しい Security Hub コントロールが使用できます。 • the section called “〔AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください” • the section called “[DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。” • the section called “[DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。” • the section called “[DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。” • the section called “[DMS.9] DMS エンドポイントは SSL を使用する必要があります。” • the section called “[DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません”	2023 年 10 月 10 日

- the section called “[DocumentDB.4] Amazon DocumentDB クラスターは監査ログを CloudWatch Logs に発行する必要があります”
- the section called “[DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります”
- the section called “[ECS.9] ECS タスク定義にはログ設定が必要です。”
- the section called “〔EventBridge.3] EventBridge カスタムイベントバスには、リソースベースのポリシーがアタッチされている必要があります”
- the section called “〔EventBridge.4] EventBridge グローバルエンドポイントでは、イベントレプリケーションを有効にする必要があります”
- the section called “[MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります”
- the section called “[MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります”

- the section called “[MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。”
- the section called “〔NetworkFirewall.9] Network Firewall ファイアウォールでは、削除保護を有効にする必要があります”
- the section called “[RDS.34] Aurora MySQL DB クラスターは監査ログを CloudWatch Logs に発行する必要があります”
- the section called “[RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります”
- the section called “[Route53 .2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります”
- the section called “[WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります”

マネージドポリシーの更新	Security Hub は、アカウントと組織単位 (OU) の情報を取得できるようにする新しい組織アクションを `AWSSecurityHubServiceRolePolicy` マネージドポリシーに追加しました。また、Security Hub が標準やコントロールはなどのサービス設定を読み取って更新できるようにする新しい Security Hub アクションも追加しました。	2023 年 9 月 27 日

サービスマネージドスタンダードに追加された既存のセキュリティコントロール：AWS Control Tower	以下の既存の Security Hub コントロールがサービスマネージドスタンダードに追加されました AWS Control Tower。 • the section called “[Athena.1] Athena ワークグループは、保管中に暗号化する必要があります” • the section called “[DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります” • the section called “[DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です” • the section called “[Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります” • the section called “[Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります” • the section called “[Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください” • the section called “[Neptune.4] Neptune DB クラスター	2023 年 9 月 26 日

では、削除保護が有効になっている必要があります”

- the section called “[Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります”
- the section called “[Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります”
- the section called “[Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります”
- the section called “[Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります”
- the section called “[RDS.27] RDS DB クラスターは保管中に暗号化する必要があります”

で利用可能な統合コントロールビューと統合コントロールの検出結果 AWS GovCloud (US)	統合されたコントロールビューと統合されたコントロールの検出結果が AWS GovCloud (US) Regionで利用できるようになりました。Security Hub コンソールの [コントロール] ページには、標準全体のすべてのコントロールが表示されます。各コントロールは、標準全体で同じコントロール ID を持ちます。統合されたコントロールの検出結果を有効にすると、コントロールが複数の有効な標準に適用される場合でも、セキュリティチェックごとに 1 つの検出結果を受け取ります。	2023 年 9 月 6 日
統合されたコントロールビューと統合されたコントロールの検出結果が中国リージョンで利用可能に	統合されたコントロールビューと統合されたコントロールの検出結果が中国リージョンで利用できるようになりました。Security Hub コンソールの [コントロール] ページには、標準全体のすべてのコントロールが表示されます。各コントロールは、標準全体で同じコントロール ID を持ちます。統合されたコントロールの検出結果を有効にすると、コントロールが複数の有効な標準に適用される場合でも、セキュリティチェックごとに 1 つの検出結果を受け取ります。	2023 年 8 月 28 日

Security Hub をイスラエル (テルアビブ) リージョンでご利用いただけます	Security Hub をイスラエル (テルアビブ) でご利用いただけるようになりました。このリージョンでは、特定のセキュリティコントロールを除き、すべての Security Hub 機能を利用できるようになりました。詳細については、「リージョン別のコントロールの可用性」を参照してください。	2023 年 8 月 8 日

新しいセキュリティコントロール	次の新しい Security Hub コントロールが使用できます。 • the section called “[Athena.1] Athena ワークグループは、保管中に暗号化する必要があります” • the section called “[DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります” • the section called “[DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です” • the section called “[Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります” • the section called “[Neptune.2] Neptune DB クラスターは監査ログを CloudWatch Logs に発行する必要があります” • the section called “[Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください” • the section called “[Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります”	2023 年 7 月 28 日

	• the section called “[Neptune .5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります” • the section called “[Neptune .6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります” • the section called “[Neptune .7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります” • the section called “[Neptune .8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります” • the section called “[RDS.27] RDS DB クラスターは保管中に暗号化する必要があります”	
自動化ルール基準の新しい演算子	自動化ルールのマッピングおよび文字列条件に対して、CONTAINS 比較演算子と NOT_CONTAINS 比較演算子を使用できるようになりました。	2023 年 7 月 25 日
自動化ルール	Security Hub は、指定した条件に基づいて検出結果を自動的に更新する自動化ルールの提供を開始しました。	2023 年 6 月 13 日

新しいサードパーティー統合	Snyk は、Security Hub に検出結果を送信する新しいサードパーティーの統合です。	2023 年 6 月 12 日

サービスマネージドスタンダードに追加された既存のセキュリティコントロール：AWS Control Tower	以下の既存の Security Hub コントロールがサービスマネージドスタンダードに追加されました AWS Control Tower。 • the section called “[Account.1] のセキュリティ連絡先情報を に提供する必要があります AWS アカウント” • the section called “[APIGateway.8] API Gateway ルートには認証タイプを指定する必要があります” • the section called “[APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります” • the section called “〔CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります” • the section called “[EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします” • the section called “[ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります” • the section called “[Redshift.10] Redshift クラスターは	2023 年 6 月 12 日

保存時に暗号化する必要があります”

- the section called “〔SageMaker.2〕 SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります”
- the section called “〔SageMaker.3〕 SageMaker ユーザーはノートブックインスタンスへのルートアクセスを許可されない”
- the section called “[WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です”

新しいセキュリティコントロール	次の新しい Security Hub コントロールが使用できます。 • the section called “[ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります” • the section called “〔AppSync.2] フィールドレベルのログ記録を有効にする AWS AppSync 必要があります” • the section called “〔CloudFront.13] CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります” • the section called “〔Elastic Beanstalk.3] Elastic Beanstalk はログを にストリーミングする必要があります CloudWatch” • the section called “[S3.17] S3 汎用バケットは、保管時に で暗号化する必要があります AWS KMS keys” • the section called “〔StepFunctions.1] Step Functions ステートマシンでは ログ記録が有効になっている必要があります”	2023 年 6 月 6 日

Security Hub をアジアパシフィック (メルボルン) でご利用いただけます	Security Hub をアジアパシフィック (メルボルン) でご利用いただけるようになりました。このリージョンでは、特定のセキュリティコントロールを除き、すべての Security Hub 機能を利用できるようになりました。詳細については、「リージョン別のコントロールの可用性」を参照してください。	2023 年 5 月 25 日
検出結果の履歴	Security Hub では、過去 90 日間の検出結果の履歴を追跡できるようになりました。	2023 年 5 月 4 日

新しいセキュリティコントロール	次の新しい Security Hub コントロールが使用できます。 • the section called “[EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります” • the section called “[ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります” • the section called “[Redshift.10] Redshift クラスターは保存時に暗号化する必要があります” • the section called “[S3.15] S3 汎用バケットでは、オブジェクトロックを有効にする必要があります”	2023 年 3 月 29 日
統合されたコントロールの検出結果のサポートを拡大	AWS v2.0.0 の自動セキュリティレスポンスで、統合統制結果がサポートされるようになりました。	2023 年 3 月 24 日
Security Hub が新しい で利用可能に AWS リージョン	Security Hub は現在、アジアパシフィック (ハイデラバード)、欧州 (スペイン)、欧州 (チューリッヒ) でご利用いただけます。これらのリージョンでは、利用できるコントロールに制限があります。	2023 年 3 月 21 日

マネージドポリシーの更新	Security Hub で、AWSSecurityHubServiceRolePolicy マネージドポリシーの既存の権限が更新されました。	2023 年 3 月 17 日

NIST 800-53 標準の新しいセキュリティコントロール	Security Hub に次のセキュリティコントロールが追加されました。NIST 800-53 標準に適用できます。 • the section called “[Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります” • the section called “〔CloudWatch.15] CloudWatch アラームには、指定されたアクションが設定されている必要があります” • the section called “〔CloudWatch.16] CloudWatch ロググループは、指定された期間保持する必要があります” • the section called “〔CloudWatch.17] CloudWatch アラームアクションを有効にする必要があります” • the section called “[DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります” • the section called “ [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします”	2023 年 3 月 3 日

	• EC2.29 — EC2 インスタンスは VPC で起動する必要があります (廃止) • the section called “[RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります” • the section called “[S3.14] S3 汎用バケットではバージョニングを有効にする必要があります” • the section called “[WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります”	
米国国立標準技術研究所 (NIST) 800-53 リビジョン 5	Security Hub は NIST 800-53 リビジョン 5 標準をサポートするようになりました。これには、200 を超える適用可能なセキュリティコントロールがあります。	2023 年 2 月 28 日

統合コントロールビューとコントロールの検出結果	統合されたコントロールビューのリリースに伴い、Security Hub コンソールの [コントロール] ページに、標準全体のすべてのコントロールが表示されます。各コントロールは、標準全体で同じコントロール ID を持ちます。統合されたコントロールの検出結果を有効にすると、コントロールが複数の有効な標準に適用される場合でも、セキュリティチェックごとに 1 つの検出結果を受け取ります。	2023 年 2 月 23 日

新しいセキュリティコントロール	次の新しい Security Hub コントロールが使用できます。一部、リージョン別の制限があるコントロールがあります。 • the section called “〔ElastiCache.1] ElastiCache Redis クラスターでは自動バックアップを有効にする必要があります” • the section called “〔ElastiCache.2]Redis キャッシュクラスター ElastiCache では、マイナーバージョン自動アップグレードを有効にする必要があります” • the section called “Redis ElastiCache レプリケーショングループの [ElastiCache.3] では、自動フェイルオーバーを有効にする必要があります” • the section called “〔ElastiCache.4] ElastiCache for Redis レプリケーショングループは保管時に暗号化する必要があります” • the section called “Redis ElastiCache レプリケーショングループの [ElastiCache.5] は転送中に暗号化する必要があります” • the section called “〔ElastiCache.6]バージョン ElastiCache 6.0 より前の	2023 年 2 月 16 日

	Redis レプリケーショングループでは、Redis AUTH を使用する必要があります” • the section called “〔ElastiCache.7] ElastiCache クラスターはデフォルトのサブネットグループを使用しないでください”	
新しい ASFF フィールド	Security Hub は、 AWS SecProductFieldsurity Finding 形式 (ASFF) ReasonCode に ProductFields.ArchivalReasons:0/Description と .Archival Reasons:0/ を追加しました。	2023 年 2 月 8 日
新しい ASFF フィールド	Security Hub は、Compliance.AssociatedStandards and Compliance. SecurityControlId を AWS Security Finding 形式 (ASFF) に追加しました。	2023 年 1 月 31 日
脆弱性の詳細が公開されました	Amazon Inspector が Security Hub に送信する結果について、Security Hub コンソールで脆弱性の詳細を確認できるようになりました。	2023 年 1 月 14 日
Security Hub が中東 (UAE) で利用可能に	Security Hub が中東 (UAE) で利用可能になりました。一部、リージョン別の制限があるコントロールがあります。	2023 年 1 月 12 日

MetricStream とのサードパーティ統合を追加	Security Hub は、中国と を除くすべてのリージョンMetric Streamで とのサードパーティー統合をサポートするようになりました AWS GovCloud (US)。	2023 年 1 月 11 日
組織アカウント上限の引き上げ	Security Hub は、リージョンごとの各 Security Hub 管理者アカウントにつき、最大 11,000 のメンバーアカウントをサポートするようになりました。	2022 年 12 月 27 日
ElasticBeanstalk.3 ロールバック	Security Hub は、すべてのリージョンで FSBP 標準から にログをストリーミングする必要があるコントロール [ElasticBeanstalk.3] CloudWatch をロールバックしました。	2022 年 12 月 21 日
Security Hub で新しいセキュリティコントロールを追加	新しい Security Hub コントロールは、FSBP 標準を有効にしているお客様が使用できます。一部、リージョン別の制限があるコントロールがあります。	2022 年 12 月 15 日

今後予定されている機能についてのガイダンス	Security Hub は、統合されたコントロールビューと統合された統制結果という、2 つの新機能をリリースする予定です。これらの今後予定されている機能は、統制結果フィールドや値に依存する既存のワークフローに影響を与える可能性があります。	2022 年 12 月 9 日
Amazon Security Lake の統合の提供を開始	Security Lake は Security Hub の検出結果を受け取ることで、Security Hub と統合されるようになりました。	2022 年 11 月 29 日
サービスマネージドスタンダードのサポート： AWS Control Tower	Security Hub は、Service -Managed Standard: AWS Control Tower. AWS Control Tower manages という新しいセキュリティ標準をサポートしています。	2022 年 11 月 28 日
CIS AWS Foundations Benchmark v1.4.0 が中国リージョンで利用可能に	Security Hub は、中国リージョンで CIS AWS Foundations Benchmark v1.4.0 をサポートするようになりました。	2022 年 11 月 18 日
Jira Service Management Cloud の統合の提供を開始	Jira Service Management Cloud は、中国リージョンを除くすべての利用可能なリージョンで、Security Hub の検出結果を受け取るようになりました。	2022 年 11 月 17 日

AWS IoT Device Defender 統合が利用可能に	AWS IoT Device Defender は、利用可能なすべてのリージョンで結果を Security Hub に送信するようになりました。	2022 年 11 月 17 日
CIS AWS Foundations Benchmark v1.4.0 のサポート	Security Hub では、CIS AWS Foundations Benchmark v1.4.0 をサポートするセキュリティコントロールが提供されるようになりました。この標準は、中国リージョンを除くすべての利用可能なリージョンで利用できます。	2022 年 11 月 9 日
での Security Hub の発表のサポート AWS GovCloud (US)	(米国東部) および (AWS GovCloud 米国西部) の Amazon Simple Notification Service (Amazon SNS) で Security Hub の発表をサブスクライブして、Security Hub AWS GovCloud に関する通知を受信できるようになりました。	2022 年 10 月 3 日
AWS Security Hub が新しいセキュリティコントロールを追加	新しい Security Hub コントロール AutoScaling.9 は、FSBP 標準を有効にしているお客様が利用できます。コントロールにはリージョン別の制限がある場合があります。	2022 年 9 月 1 日

Security Hub の発表のサブスクライブ	Amazon Simple Notification Service (Amazon SNS) を使用して Security Hub の発表をサブスクライブし、Security Hub に関する通知を受け取ることができるようになりました。	2022 年 8 月 29 日
クロスリージョン集約のためのリージョン拡張	クロスリージョン集約を AWS GovCloud (US)の結果、結果の更新、インサイトに使用できるようになりました。	2022 年 8 月 2 日
新しいサードパーティー製品の統合	Fortinet - FortiCNP は Security Hub の結果を受信するサードパーティー統合です。JFrog は Security Hub に結果を送信するサードパーティー統合です。	2022 年 7 月 26 日
EC2.27 は廃止されました	Security Hub は EC2.27 を廃止しました - EC2 インスタンスの実行には、 Foundational Security Best Practices (FSBP) 標準の以前のコントロールであるキーペア を使用しないでください。 AWS	2022 年 7 月 20 日
Lambda.2 は python3.6 をサポートしなくなりました	Security Hub は Lambda.2 のパラメータとして python3.6 をサポートしなくなりました。- Lambda 関数は、Foundational Security Best Practices (FSBP) 標準のコントロールであるサポートされているランタイム を使用する必要があります。 AWS	2022 年 7 月 19 日

AWS Security Hub で新しいセキュリティコントロールを追加	新しい Security Hub コントロールは、FSBP 標準を有効にしているお客様が使用できます。一部、リージョン別の制限があるコントロールがあります。	2022 年 6 月 22 日
AWS Security Hub が新しいリージョンをサポート	Security Hub をアジアパシフィック (ジャカルタ) でご利用いただけるようになりました。このリージョンでは、一部のコントロールが使用できません。	2022 年 6 月 7 日
AWS Security Hub と の統合を改善 AWS Config	Security Hub ユーザーは、AWS Config ルール評価の結果を Security Hub の結果として表示できます。	2022 年 6 月 6 日
自動で有効化された標準をオプトアウトする機能が追加されました	と統合しているユーザーの場合 AWS Organizations、この機能により Security Hub 管理者アカウントにログインし、自動有効化標準から新しいメンバーアカウントをオプトアウトできます。	2022 年 4 月 25 日
クロスリージョン集約が拡張されました	コントロールステータスとセキュリティスコアにクロスリージョン集約が追加されました。	2022 年 4 月 20 日
CompanyName と ProductName が最上位の属性になりました	カスタムインテグレーションに関連付けられた会社名および製品名を設定するための、新しいトップレベル属性が追加されました	2022 年 4 月 1 日

AWS Foundational Security Best Practices 標準に新しいコントロールを追加	AWS Foundational Security Best Practices 標準に 5 個の新しいコントロールが追加されました。	2022 年 3 月 31 日
新しいリソースの詳細オブジェクトが ASFF に追加されました	`AwsRdsDbSecurityGroup` リソースタイプが ASFF に追加されました。	2022 年 3 月 25 日
ASFF に新しいリソースの詳細が追加されました	その他の詳細が `AwsAutoScalingScalingGroup` 、`AwsElbLoadBalancer` 、`AwsRedshiftCluster` 、`AwsCodeBuildProject` に追加されました。	2022 年 3 月 25 日
AWS Foundational Security Best Practices 標準に新しいコントロールを追加	AWS Foundational Security Best Practices 標準に 15 個の新しいコントロールが追加されました。	2022 年 3 月 16 日
AWS Foundational Security Best Practices 標準と Payment Card Industry Data Security Standard (PCI DSS) に新しいコントロールを追加しました。	Amazon OpenSearch Service、Amazon RDS、Amazon EC2、Elastic Load Balancing、および の新しいコントロール CloudFront を AWS Foundational Security Best Practices 標準に追加しました。また、PCI DSS に OpenSearch Service の 2 つの新しいコントロールを追加しました。	2022 年 2 月 15 日
ASFF に新しいフィールドを追加	次の新しいフィールドが追加されました: `Sample`。	2022 年 1 月 26 日

との統合を追加 AWS Health	AWS Health は service-to-service 、イベントメッセージングを使用して結果を Security Hub に送信します。	2022 年 1 月 19 日
との統合を追加 AWS Trusted Advisor	Trusted Advisor は、チェックの結果を Security Hub の検出結果として Security Hub に送信します。Security Hub は、 AWS 基本的なセキュリティのベストプラクティスチェックの結果を に送信します Trusted Advisor。	2022 年 1 月 18 日
ASFF のリソースの詳細オブジェクトを更新	`MixedInstancesPolicy` および `AvailabilityZones` が `AwsAutoScalingAutoScalingGroup` に追加されました。`MetadataOptions` が `AwsAutoScalingLaunchConfiguration` に追加されました。`BucketVersioningConfiguration` が `AwsS3Bucket` に追加されました。	2021 年 12 月 20 日
ASFF ドキュメントの出力を更新	ASFF 属性の説明は、以前は 1 つのトピックにまとめられていました。各最上位レベルのオブジェクトと各リソースの詳細オブジェクトが、独自のトピックに移動されました。ASFF 構文のトピックには、これらのトピックへのリンクが含まれています。	2021 年 12 月 20 日

の ASFF に新しいリソース詳細オブジェクトを追加 AWS Network Firewall	に AWS Network Firewall、、、および のリソース詳細オブジェクトを追加`AwsNetworkFirewallFirewall` `AwsNetworkFireFirewallPolicy` しました`AwsNetworkFirewallRuleGroup` 。	2021 年 12 月 20 日
Amazon Inspector の新しいバージョンのサポートの追加	Security Hub が Amazon Inspector Classic だけでなく Amazon Inspector の新バージョンとも統合されました。Amazon Inspector が Security Hub に結果を送信します。	2021 年 11 月 29 日
EC2.19 の重要度を変更	EC2.19 (セキュリティグループが、リスクの高いポートへの無制限アクセスを許可しない) の重要度 が「高」から「重大」に変更されました。	2021 年 11 月 17 日
Sonrai Dig との新しい統合	Security Hub で Sonrai Dig との統合が可能となりました。Sonrai Dig はクラウド環境を監視して、セキュリティリスクを特定します。Sonrai Dig は結果を Security Hub に送信します。	2021 年 11 月 12 日

CIS 2.1 および . CloudTrail1 コントロールのチェックを更新	CIS 2.1 および .1 では、少なくとも 1 つのマルチリージョン CloudTrail 証跡が設定されていること CloudTrail の確認に加えて、少なくとも 1 つのマルチリージョン CloudTrail 証跡で `ExcludeManagementEventSources` パラメータが空であることを確認します。	2021 年 11 月 9 日
VPC エンドポイントのサポートを追加	Security Hub が と統合 AWS PrivateLink され、VPC エンドポイントがサポートされるようになりました。	2021 年 11 月 3 日
AWS Foundational Security Best Practices 標準にコントロールを追加	Elastic Load Balancing (ELB.2 および ELB.8) と AWS Systems Manager (SSM.4) の新しいコントロールを追加しました。	2021 年 11 月 2 日
EC2.19 コントロールのチェックにポートを追加	EC2.19 では、セキュリティグループが次のポートへの無制限の入力アクセスを許可しないこともチェックするようになりました: 3000 (Go、Node.js、および Ruby の ウェブ開発フレームワーク)、5000 (Python ウェブ開発フレームワーク)、8088 (レガシー HTTP ポート)、8888 (代替 HTTP ポート)	2021 年 10 月 27 日

Logz.io クラウド SIEM との統合を追加	Logz.io は、セキュリティチームがリアルタイムでセキュリティの脅威を検出、分析、対応できるように、ログとイベントデータの高度な相関を提供する Cloud SIEM のプロバイダです。Logz.io は、Security Hub から結果を受け取ります。	2021 年 10 月 25 日
リージョン間の結果集約のサポートを追加	クロスリージョン集約では、リージョンを変更しなくても、すべての結果を確認できます。管理者アカウントによって、集約リージョンとリンクされたリージョンが選択されます。管理者アカウントとそのメンバーアカウントの結果が、リンクされたリージョンから集約リージョンに集約されます。	2021 年 10 月 20 日
ASFF のリソースの詳細オブジェクトを更新	ビューワーの証明書の詳細が `AwsCloudFrontDistribution` に追加されました。その他の詳細が `AwsCodeBuildProject` に追加されました。ロードバランサーの属性が `AwsElbV2LoadBalancer` に追加されました。S3 バケット所有者のアカウント識別子が `AwsS3Bucket` に追加されました。	2021 年 10 月 8 日

新しいリソースの詳細オブジェクトを ASFF に追加	次の新しいリソースの詳細オブジェクトが ASFF に追加されました: `AwsEc2VpcEndpointService` 、`AwsEcrRepository` 、`AwsEksCluster` 、`AwsOpenSearchServiceDomain` 、`AwsWafRateBasedRule` 、`AwsWafRegionalRateBasedRule` 、`AwsXrayEncryptionConfig`	2021 年 10 月 8 日
Lambda.2 コントロールから非推奨のランタイムを削除	AWS Foundational Security Best Practices 標準で、 は [Lambda.2] Lambda 関数から`dotnetcore2.1` ランタイムを削除し、サポートされているランタイム を使用する必要があります。	2021 年 10 月 6 日
Check Point 統合の新しい名前	Check Point Dome9 Arc との統合が Check Point CloudGuard Posture Management になりました。統合 ARN は変更されませんでした。	2021 年 10 月 1 日
Alcide との統合を削除	Alcide kAudit との統合は中止されます。	2021 年 9 月 30 日
EC2.19 の重要度を変更	「[EC2.19] セキュリティグループが、リスクの高いポートへの無制限アクセスを許可しない」の重要度が「中」から「高」に変更されました。	2021 年 9 月 30 日

との統合 AWS Organizations が中国リージョンでサポートされるようになりました	Security Hub と Organizations の統合が中国 (北京) と中国 (寧夏) でサポートされるようになりました。	2021 年 9 月 20 日
S3.1 および PCI.S3.6 コントロールの新しい AWS Config ルール	S3.1 と PCI.S3.6 の両方で、Amazon S3 ブロックパブリックアクセスの設定が有効になっていることが確認されます。これらのコントロールの AWS Config ルールが から `s3-account-level-public-access-blocks` に変更されましたs3-account-level-public-access-blocks-periodic 。	2021 年 9 月 14 日
Lambda.2 コントロールから非推奨のランタイムを削除	AWS Foundational Security Best Practices 標準で、 は [Lambda.2] Lambda 関数から `nodejs10.x` および `ruby2.5`ランタイムを削除し、サポートされているランタイム を使用する必要があります。	2021 年 9 月 13 日
CIS 2.2 コントロールの重要度を変更	CIS AWS Foundations Benchmark 標準では、2.2 の重要度。– CloudTrail ログファイルの検証が有効になっていることを確認します。	2021 年 9 月 13 日

AWS Foundational Security Best Practices 標準で ECS.1、Lambda.2、SSM.1 を更新	AWS Foundational Security Best Practices 標準では、ECS.1 に に設定されたSkipInactiveTaskDefinitions パラメータが追加されましたtrue。これにより、コントロールはアクティブなタスク定義のみをチェックします。Lambda.2 では、Python 3.9 がランタイムのリストに追加されました。SSM.1 は、停止中および実行中の両方のインスタンスをチェックするようになりました。	2021 年 9 月 7 日
PCI.Lambda.2 コントロールによって Lambda @Edge リソースを除外	Payment Card Industry Data Security Standard (PCI DSS) では、PCI.Lambda.2 コントロールによって Lambda @Edge リソースが除外されるようになりました。	2021 年 9 月 7 日
HackerOne Vulnerability Intelligence との統合を追加	Security Hub で HackerOne Vulnerability Intelligence との統合が可能になりました。この統合によって、結果が Security Hub に送信されるようになります。	2021 年 9 月 7 日

ASFF のリソースの詳細オブジェクトを更新	AwsKmsKey には、KeyRotationStatus が追加されました。AwsS3Bucket には、AccessControlList 、BucketLoggingConfiguration 、BucketNotificationConfiguration 、および BucketWebsiteConfiguration が追加されました。	2021 年 9 月 2 日
新しいリソースの詳細オブジェクトを ASFF に追加	次の新しいリソースの詳細オブジェクトが ASFF に追加されました: AwsAutoScalingLaunchConfiguration 、AwsEc2VpnConnection 、および AwsEcrContainerImage 。	2021 年 9 月 2 日
ASFF で Vulnerabilities オブジェクトに詳細を追加	Cvss では、Adjustments と Source が追加されました。VulnerablePackages では、ファイルパスとパッケージマネージャーが追加されました。	2021 年 9 月 2 日
Systems Manager Explorer と OpsCenter 統合が中国リージョンでサポートされるようになりました	Security Hub と SSM Explorer および の統合 OpsCenter が、中国 (北京) および中国 (寧夏) でサポートされるようになりました。	2021 年 8 月 31 日

Lambda.4 コントロールの廃止	Security Hub では、コントロール「[Lambda.4] Lambda 関数にはデッドレターキューが設定されている必要があります」が廃止されます。このコントロールが使用停止されると、コンソールに表示されなくなり、Security Hub はそのコントロールに対するチェックを実行しません。	2021 年 8 月 31 日
PCI.EC2.3 コントロールの廃止	Security Hub では、コントロール「[PCI.EC2.3] 未使用の EC2 セキュリティグループを削除する必要があります」が廃止されます。このコントロールが使用停止されると、コンソールに表示されなくなり、Security Hub はそのコントロールに対するチェックを実行しません。	2021 年 8 月 27 日
Security Hub によるカスタムアクションへの結果の送信方法の変更	カスタムアクションに結果を送信するとき、Security Hub が個別のSecurity Hub Findings - Custom Action イベントの各結果を送信するようになりました。	2021 年 8 月 20 日

カスタム Lambda ランタイムの新しいコンプライアン状況理由コードを追加	新しい LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE コンプライアンス状況理由コードが追加されました。この理由コードは、Security Hub がカスタム Lambda ランタイムに対してチェックを実行できなかったことを示しています。	2021 年 8 月 20 日
AWS Firewall Manager 統合が中国リージョンでサポートされるようになりました	Security Hub と Firewall Managerの統合が中国 (北京) および中国 (寧夏) でサポートされるようになりました。	2021 年 8 月 19 日
Caveonix Cloud および Forcepoint Cloud Security Gateway との新しい統合	Security Hub で Caveonix Cloud および Forcepoint Cloud Security Gateway との統合が可能になりました。両方の統合によって、結果が Security Hub に送信されるようになります。	2021 年 8 月 10 日

ASFF に新しい CompanyName 、ProductName 、および Region 属性を追加	ASFF の最上位レベルに CompanyName 、ProductName 、および Region フィールドが追加されました。これらのフィールドは自動的に入力され、カスタム製品統合を除き、BatchImportFindings または BatchUpdateFindings を使用して更新することはできません。コンソールでは、検索フィルターによってこれらの新しいフィールドが使用されます。API では、CompanyName および ProductName フィルターによって ProductFields の属性が使用されます。	2021 年 7 月 23 日
ASFF のリソースの詳細オブジェクトを追加および更新	新しい AwsRdsEventSubscription リソースタイプと新しいリソースの詳細が追加されました。AwsEcsService リソースタイプのリソースの詳細が追加されました。AwsElasticsearchDomain リソースの詳細オブジェクトに属性が追加されました	2021 年 7 月 23 日

AWS Foundational Security Best Practices 標準にコントロールを追加	Amazon API Gateway (APIGateway.5),、Amazon EC2 (EC2.19)、Amazon ECS (ECS.2)、Elastic Load Balancing (ELB.7)、Amazon OpenSearch Service (ES.5 から ES.8)、Amazon RDS (RDS.16 から RDS.23)、Amazon Redshift (Redshift.4)、および Amazon SQS (SQS.1) の新しいコントロールを追加しました。	2021 年 7 月 20 日
サービスにリンクされたロールマネージドポリシー内の許可を移動	マネージドポリシー `AWSSecurityHubServiceRolePolicy` 内の `config:PutEvaluations` 許可が移動され、すべてのリソースに適用されるようになりました。	2021 年 7 月 14 日
AWS Foundational Security Best Practices 標準にコントロールを追加	Amazon API Gateway (APIGateway.4),、Amazon CloudFront （ CloudFront.5 および CloudFront.6)、Amazon EC2 (EC2.17 および EC2.18)、Amazon ECS (ECS.1)、Amazon OpenSearch Service (ES.4) AWS Identity and Access Management 、(IAM.21)、Amazon RDS (RDS.15)、および Amazon S3 (S3.8) の新しいコントロールを追加しました。	2021 年 7 月 8 日

統制結果の新しいコンプライアンス状況の理由コードを追加	INTERNAL_SERVICE_ERROR は、不明なエラーが発生したことを示します。SNS_TOPIC_CROSS_ACCOUNT は、SNS トピックが別のアカウントによって所有されていることを示します。SNS_TOPIC_INVALID は、関連付けられた SNS トピックが無効であることを示します。	2021 年 7 月 6 日
との統合を追加 AWS Chatbot	との統合を追加しました AWS Chatbot。Security Hub は結果を に送信します AWS Chatbot。	2021 年 6 月 30 日
サービスにリンクされたロールマネージドポリシーに新しい許可を追加	マネージドポリシー AWSSecurityHubServiceRolePolicy に新しい許可が追加され、サービスにリンクされたロールで AWS Configに評価結果を提供できるようになりました。	2021 年 6 月 29 日

ASFF の新規および更新されたリソース詳細オブジェクト	ECS クラスタおよび ECS タスク定義の新しいリソースの詳細オブジェクトが追加されました。EC2 インスタンスオブジェクトが更新されて、関連付けられているネットワークインターフェイスが一覧表示されるようになりました。API Gateway V2 のステージのクライアント証明書 ID が追加されました。S3 バケットのライフサイクル設定が追加されました。	2021 年 6 月 24 日
集約されたコントロールステータスと標準のセキュリティスコアの計算を更新	Security Hub で 24 時間ごとに全体的なコントロールステータスと標準のセキュリティスコアが計算されるようになりました。管理者アカウントの場合、アカウントごとに各コントロールが有効または無効かどうかがスコアに反映されるようになりました。	2021 年 6 月 23 日
中断されているアカウントの Security Hub の処理に関する情報を更新	AWSで中断されているアカウントを Security Hub が処理する方法に関する情報が追加されました。	2021 年 6 月 23 日

個々の管理者アカウントの有効化/無効化されたコントロールを表示するタブを追加	管理者アカウントの場合、標準の詳細ページのメインタブに、アカウント間で集約された情報が表示されます。新しい [Enabled for this account] (このアカウントでは有効) および [Disabled for this account] (このアカウントでは無効) タブには、個々の管理者アカウントに対して有効または無効になっているアカウントが一覧表示されます。	2021 年 6 月 23 日
Lambda.2 のパラメータに java8.al2 を追加	AWS Foundational Security Best Practices 標準java8.al2 で、がLambda.2コントロールでサポートされているランタイムに追加されました。	2021 年 6 月 8 日
MicroFocus ArcSight と の Cyber investigator との新しい統合	Security Hub からの結果を、MicroFocus ArcSight および"" Cyber investigator. MicroFocus ArcSight receives との統合を追加しました。NETSCOUT Cyber Investigator が結果を Security Hub に送信します。	2021 年 6 月 7 日
AWSSecurityHubServiceRolePolicy の詳細を追加	マネージドポリシーセクションが更新され、既存のマネージドポリシー AWSSecurityHubServiceRolePolicy の詳細が追加されました。これは Security Hub サービスにリンクされたロールによって使用されます。	2021 年 6 月 4 日

Jira サービス管理との新しい統合	AWS Service Management Connector for Jira は検出結果を Jira に送信し、それを使用して Jira の問題を作成します。Jira 問題が更新されると、Security Hub の対応する結果も更新されます。	2021 年 5 月 26 日
アジアパシフィック (大阪) リージョンでサポートされているコントロールリストを更新	CIS AWS Foundations 標準と Payment Card Industry Data Security Standard (PCI DSS) を更新し、アジアパシフィック (大阪) でサポートされていないコントロールを示しました。	2021 年 5 月 21 日
Sysdig Secure for cloud との新しい統合	Sysdig Secure for cloud との統合が追加されました。この統合によって、結果が Security Hub に送信されるようになります。	2021 年 5 月 14 日

AWS Foundational Security Best Practices 標準にコントロールを追加	Amazon API Gateway (APIGateway.2 と APIGateway.3), AWS CloudTrail 、（ CloudTrail.4 と CloudTrail.5)、Amazon EC2 (EC2.15 と EC2.16)、 AWS Elastic Beanstalk（ ElasticBeanstalk.1 と ElasticBeanstalk.2) AWS Lambda 、(Lambda.4)、Amazon RDS (RDS.12 – RDS.14)、Amazon Redshift (Redshift.7) AWS Secrets Manager 、 (SecretsManager.3 と SecretsManager.4)、および AWS WAF (WAF.1) の新しいコントロールを追加しました。	2021 年 5 月 10 日
GuardDuty および Amazon RDS コントロールの更新	`GuardDuty.1` および `PCI.GuardDuty.1` の重要度が「中」から「高」に変更されました。`databaseEngines` パラメータが `RDS.8` に追加されました。	2021 年 5 月 4 日
新しいリソースの詳細を ASFF に追加	`Resources.Details` で、Amazon EC2 ネットワーク ACL、Amazon EC2 サブネット、 AWS Elastic Beanstalk 環境の新しいリソースの詳細オブジェクトが追加されました。	2021 年 5 月 3 日

Amazon EventBridge ルールのフィルター値を提供するコンソールフィールドを追加	Security Hub EventBridge ルールの新しい定義済みフィルターパターンには、フィルター値を指定するために使用できるコンソールフィールドが用意されています。	2021 年 4 月 30 日
AWS Systems Manager Explorer および との統合を追加 OpsCenter	Security Hub は、Systems Manager Explorer および との統合をサポートするようになりました OpsCenter。この統合によって、Security Hub から結果を受け取り、Security Hub でこれらの結果が更新されます。	2021 年 4 月 26 日
製品統合の新しいタイプ	新しい統合タイプ、`UPDATE_FINDINGS_IN_SECURITY_HUB` は、製品統合によって Security Hub から受け取った結果が更新されることを示します。	2021 年 4 月 22 日
「マスターアカウント」という用語を「管理者アカウント」に変更	「マスターアカウント」という用語が「管理者アカウント」に変更されました。この用語は、Security Hub コンソールと API でも変更されます。	2021 年 4 月 22 日
HTTP を Websocket に置き換えるように APIGateway.1 を更新	APIGateway.1 のタイトル、説明、および修正が更新されました。コントロールは、HTTP API 実行ログではなく Websocket API 実行ログをチェックするようになりました。	2021 年 4 月 9 日

Amazon GuardDuty の統合が北京と寧夏でサポートされるようになりました	Security Hub と の統合 GuardDuty が、中国 (北京) および中国 (寧夏) リージョンでサポートされるようになりました。	2021 年 4 月 5 日
Lambda.2 コントロールのサポートされているランタイムに nodejs14.x を追加	Foundational Security Best Practices 標準の Lambda.2 コントロールでは、nodejs14.x ランタイムがサポートされるようになりました。	2021 年 3 月 30 日
Security Hub をアジアパシフィック (大阪) で開始	Security Hub がアジアパシフィック (大阪) リージョン でご利用いただけるようになりました。	2021 年 3 月 29 日
結果の詳細に結果プロバイダーフィールドを追加	結果の詳細パネルの新しい [Finding Provider Fields] (結果プロバイダフィールド) セクションには、信頼度、重大度、関連する結果、重要度、およびタイプの結果プロバイダー値が含まれています。	2021 年 3 月 24 日
Amazon Macie から機密性の高い結果を受け取るオプションを追加	Macie との統合について、機密性の高い結果を Security Hub に送信するように構成できるようになりました。	2021 年 3 月 23 日

アカウント管理 AWS Organizations のための への移行	メンバーアカウントを持つ既存の管理者アカウントを持つ顧客の場合、 は、招待によるアカウントの管理から Organizations を使用したアカウントの管理への変更方法に関する新しい情報を追加しました。	2021 年 3 月 22 日
Amazon S3 パブリックアクセスブロックの設定に関する情報の ASFF の新しいオブジェクト	`Resources` では、新しい `AwsS3AccountPublicAccessBlock` リソースタイプと詳細オブジェクトによって、アカウントの Amazon S3 パブリックアクセスブロック設定に関する情報が提供されます。`AwsS3Bucket` リソースの詳細オブジェクトでは、`PublicAccessBlockConfiguration` オブジェクトによって、S3 バケットのパブリックアクセスブロック設定が提供されます。	2021 年 3 月 18 日
ASFF の新しいオブジェクトを使用して、結果プロバイダーによる特定のフィールドの更新を許可	ASFF の新しい `FindingProviderFields` オブジェクトが `BatchImportFindings` で使用され、`Confidence`、`Criticality`、`RelatedFindings`、`Severity`、`Types` の値が指定されます。元のフィールドは、`BatchUpdateFindings` を使用してのみ更新されます。	2021 年 3 月 18 日

ASFF のリソースの新規 DataClassification オブジェクト	ASFF の新規 Resources.DataClassification オブジェクトは、リソースで検出された機密データに関する情報を提供するために使用されます。	2021 年 3 月 18 日
使用可能なコンプライアンス状況コードに CONFIG_RETURNS_NOT_APPLICABLE 値を追加	NOT_AVAILABLE コンプライアンス状況について、理由コード RESOURCE_NO_LONGER_EXISTS が削除され、理由コード CONFIG_RETURNS_NOT_APPLICABLE が追加されました。	2021 年 3 月 16 日
と統合するための新しいマネージドポリシー AWS Organizations	新しいマネージドポリシー、AWSSecurityHubOrganizationsAccess によって、組織管理アカウントおよび委任された Security Hub 管理者アカウントに必要な組織の許可が提供されます。	2021 年 3 月 15 日
マネージドポリシーとサービスにリンクされたロール情報が「セキュリティ」の章に移動	マネージドポリシーに関する情報が改訂され、拡張されます。マネージドポリシー情報とサービスにリンクされたロールに関する情報は、「セキュリティ」の章に移動しました。	2021 年 3 月 15 日

SecureCloudDB との新しい統合	サードパーティー統合のリストに SecureCloudDB を追加しました。 SecureCloudDB は、内部および外部のセキュリティ体制とアクティビティを包括的に可視化するクラウドネイティブデータベースセキュリティツールです。 SecureCloudDB は結果を Security Hub に送信します。	2021 年 3 月 4 日
CIS 1.1 および CIS 3.1 ~ CIS 3.14 コントロールの重要度を改訂	CIS 1.1 および CIS 3.1 ~ CIS 3.14 コントロールの重要度が「低」に変更されます。	2021 年 3 月 3 日
RDS.11 コントロールを削除	Foundational Security Best Practices 標準から RDS.11 コントロールを削除	2021 年 3 月 3 日
Turbot の統合を更新	結果を送受信するように Turbot 統合が更新されます。	2021 年 2 月 26 日
Foundational Security Best Practices 標準にコントロールを追加	Amazon API Gateway (APIGateway.1),Amazon EC2 (EC2.9 および EC2.10)、Amazon Elastic File System (EFS .2)、Amazon OpenSearch Service (ES.2 および ES.3)、Elastic Load Balancing (ELB.6)、および AWS Key Management Service（ AWS KMS) (KMS.3) の新しいコントロールを追加しました。	2021 年 2 月 11 日

DescribeProducts API にオプションの ProductArn フィルターを追加	DescribeProducts API オペレーションにオプションの ProductArn パラメータが含まれるようになりました。ProductArn パラメータは、特定の製品の統合を識別して詳細を返すために使用されます。	2021 年 2 月 3 日
クラウドストレージセキュリティからの Amazon S3 用アンチウイルスとの新しい統合	Amazon S3 用アンチウイルスとの統合により、ウイルススキャン結果が結果として Security Hub に送信されます。	2021 年 1 月 27 日
管理者アカウントのセキュリティスコア計算プロセスを更新しました	管理者アカウントの場合、Security Hub は別のプロセスを使用してセキュリティスコアを計算します。新しいプロセスにより、メンバーアカウントでは有効になっているが、管理者アカウントでは無効になっているコントロールがスコアに含まれるようになります。	2021 年 1 月 21 日
ASFF の新しいフィールドとオブジェクト	新しい Action オブジェクトが追加され、リソースに対して発生したアクションを追跡します。フィールドが AwsEc2NetworkInterface オブジェクトに追加され、DNS 名と IP アドレスを追跡します。新しい AwsSsmPatchCompliance オブジェクトがリソースの詳細に追加されました。	2021 年 1 月 21 日

Foundational Security Best Practices 標準にコントロールを追加	Amazon CloudFront（CloudFront.1 から CloudFront.4)、Amazon DynamoDB (DynamoDB.1 から DynamoDB.3),、Elastic Load Balancing (ELB.3 から ELB.5)、Amazon RDS (RDS.9 から RDS.11)、Amazon Redshift (Redshift.1 から Redshift.3 と Redshift.6)、および Amazon SNS (SNS.1) の新しいコントロールを追加しました。	2021 年 1 月 15 日
ワークフローステータスは、レコードの状態またはコンプライアン状況に基づいてリセットされます	Security Hub は、アーカイブされた結果がアクティブになった場合、結果のコンプライアンス状況が PASSED から FAILED、WARNING、NOT_AVAILABLE のいずれかに変化した場合、ワークフローステータスを NOTIFIED または RESOLVED から NEW に自動的にリセットします。このような変更は、追加の調査が必要であることを示しています。	2021 年 1 月 7 日
コントロールベースの結果の ProductFields の情報を追加	コントロールから生成される結果について、 AWS Security Finding 形式の ProductFields オブジェクトのコンテンツに関する情報が追加されました。	2020 年 12 月 29 日

マネージド型インサイトの更新	インサイト 5 のタイトルが変更されました。疑わしいアクティビティにかかわっている IAM ユーザーをチェックする新しいインサイト 32 が追加されました。	2020 年 12 月 22 日
IAM.7 および Lambda.1 コントロールの更新	AWS Foundational Security Best Practices 標準で、IAM.7 のパラメータを更新しました。Lambda.1 のタイトルと説明が更新されました。	2020 年 12 月 22 日
ServiceNow ITSM との統合の拡張	ServiceNow ITSM 統合により、Security Hub の検出結果を受信すると、ユーザーはインシデントまたは問題を自動的に作成できます。このようなインシデントまたは問題が更新されると、Security Hub の結果も更新されます。	2020 年 12 月 11 日
AWS Audit Manager との新しい統合	Security Hub で Audit Manager AWS との統合が可能になりました。統合により、Audit Manager は Security Hub からコントロールベースの結果を受け取ることができます。	2020 年 12 月 8 日
Aqua Security Kube-Bench との新しい統合	Security Hub に Aqua Security Kube-Bench との統合が追加されました。この統合によって、結果が Security Hub に送信されるようになります。	2020 年 11 月 24 日

Cloud Custodian が、中国リージョンで利用可能になります	Cloud Custodian との統合が中国 (北京) および中国 (寧夏) リージョンで利用可能になりました。	2020 年 11 月 24 日
追加フィールドを更新するために BatchImportFindings を使用できるようになります	これまでは、BatchImportFindings を使用して Confidence 、Criticality 、RelatedFindings 、Severity、および Types フィールドを更新できませんでした。今後は、これらのフィールドが BatchUpdateFindings によって更新されていない場合は、BatchImportFindings によって更新できます。フィールドが BatchUpdateFindings によって更新された場合、BatchImportFindings では更新できません。	2020 年 11 月 24 日
Security Hub が と統合されました AWS Organizations	お客様が Organizations アカウント設定を使用して、メンバーアカウントを管理できるようになりました。組織管理アカウントは、Security Hub で有効にする組織アカウントを決定する Security Hub 管理者アカウントを指定します。手動招待プロセスは、組織に含まれていないアカウントでも使用できます。	2020 年 11 月 23 日

大量のコントロールの個々の結果リストを削除	コントロールの結果リストでは、結果が非常に多い場合、[Findings] (結果) のページ形式が使用されなくなりました。	2020 年 11 月 19 日
新しいサードパーティの統合と更新されたサードパーティの統合	Security Hub は、cloudtamer.io、3CORESec、Prowler、Kubernetes StackRox Security との統合をサポートするようになりました。IBM QRadar は結果を送信しなくなりました。結果を受け取ることはできます。	2020 年 10 月 30 日
コントロールの詳細ページから結果のリストをダウンロードするオプションが追加されました。	コントロールの詳細ページで、新しい [Download] (ダウンロード) オプションを使用すると、検索リストを .csv ファイル形式でダウンロードできます。ダウンロードされたリストは、リストに含まれるすべてのフィルターを優先します。特定の結果を選択した場合、ダウンロードされたリストにはそれらの結果のみが含まれます。	2020 年 10 月 26 日

標準の詳細ページからコントロールのリストをダウンロードするオプションが追加されました。	標準の詳細ページで、新しいオプションの [Download] (ダウンロード) オプションを使用すると、コントロールリストを .csv ファイルにダウンロードできます。ダウンロードされたリストは、リストに含まれるすべてのフィルターを優先します。特定のコントロールを選択した場合、ダウンロードされたファイルにはそのコントロールのみが含まれます。	2020 年 10 月 26 日
新しいパートナーの統合と更新されたパートナーの統合	Security Hub が と統合されました ThreatModeler。新しい製品名を反映するように、次のパートナーの統合が更新されました。Twistlock Enterprise Edition は Palo Alto Networks - Prisma Cloud Compute になりました。Palo Alto Networks ではさらに、Demisto が Cortex XSOAR に名称変更されると共に、Redlock が Prisma Cloud Enterprise に名称変更され、機能強化されました。	2020 年 10 月 23 日
Security Hub を中国 (北京) および中国 (寧夏) で開始	Security Hub が中国 (北京) および中国 (寧夏) リージョンで利用可能になりました。	2020 年 10 月 21 日

ASFF 属性およびサードパーティー統合のフォーマットを改訂	ASFF の属性およびパートナーの統合のリストでテーブルの代わりにリストベースの形式が使用されるようになりました。ASFF の構文、属性、およびタイプ分類が別々のトピックになりました。	2020 年 10 月 15 日
標準の詳細ページを再設計	有効な標準の標準の詳細ページに、コントロールのタブ付きリストが表示されるようになりました。タブは、コントロールステータスに基づいてコントロールリストをフィルタリングします。	2020 年 10 月 7 日
Events CloudWatch を に置き換えました EventBridge	Amazon CloudWatch Events への参照を Amazon に置き換えました EventBridge。	2020 年 10 月 1 日
、Alcide kAudit AWS、Palo Alto Networks VM シリーズ用の Blue Hexagon との新しい統合。	Security Hub は、、Alcide kAudit AWS、Palo Alto Networks VM シリーズ用の Blue Hexagon と統合されました。Blue Hexagon for AWS と kAudit は、結果を Security Hub に送信します。VM-Series は、Security Hub から結果を受け取ります。	2020 年 9 月 30 日

ASFF の新規および更新されたリソース詳細オブジェクト	AwsApiGatewayRestApi 、AwsApiGatewayStage 、AwsApiGatewayV2Api 、AwsApiGatewayV2Stage 、AwsCertificateManagerCertificate 、AwsElbLoadBalancer 、AwsIamGroup 、AwsRedshiftCluster の新しい Resources.Details オブジェクトが追加されました。AwsCloudFrontDistribution 、AwsIamRole 、AwsIamAccessKey オブジェクトに詳細が追加されました。	2020 年 9 月 30 日
ASFF のリソースの新しい ResourceRole 属性で、リソースがアクターであるか、ターゲットであるかを追跡します。	リソースの ResourceRole 属性は、リソースが結果アクティビティの対象であるか、検索アクティビティの被対象であるかを示します。有効な値は ACTOR および TARGET です。	2020 年 9 月 30 日
利用可能な AWS サービス統合に AWS Systems Manager Patch Manager を追加	AWS Systems Manager Patch Manager が Security Hub と統合されました。Patch Manager は、お客様のフリート内のインスタンスがパッチコンプライアンス標準に準拠していない場合、結果を Security Hub に送信します。	2020 年 9 月 22 日

AWS Foundational Security Best Practices 標準に新しいコントロールを追加	Amazon EC2 (EC2.7 と EC2.8)、Amazon EMR (EMR.1)、IAM (IAM.8)、Amazon RDS (RDS.4 から RDS.8)、Amazon S3 (S3.6)、AWS Secrets Manager および (SecretsManager.1 と .2) のサービスに新しいコントロールを追加 SecretsManagerしました。	2020 年 9 月 15 日
IAM ポリシーの新しいコンテキストキーによって BatchUpdateFindings フィールドへのアクセスを制御	IAM ポリシーを設定して、BatchUpdateFindings の使用時に、フィールドとフィールド値へのアクセスを制限できるようになりました。	2020 年 9 月 10 日
メンバーアカウントの BatchUpdateFindings へのアクセスを拡張	デフォルトでは、メンバーアカウントは管理者アカウントBatchUpdateFindings と同じアクセス権を持つようになりました。	2020 年 9 月 10 日
Foundational Security Best Practices Standard AWS KMS の の新しいコントロール	Foundational Security Best Practices 標準に 2 つの新しいコントロール (KMS.1 と KMS.2) が追加されました。新しいコントロールは、IAM ポリシーが復 AWS KMS 号アクションへのアクセスを制限するかどうかをチェックします。	2020 年 9 月 9 日

コントロールのアカウントレベルの結果を削除	Security Hub でコントロールのアカウントレベルの結果が生成されなくなりました。生成されるのはリソースレベルの結果のみです。	2020 年 9 月 1 日
ASFF の新しい PatchSummary オブジェクト	ASFF に `PatchSummary` オブジェクトが追加されました。`PatchSummary` オブジェクトは、選択したコンプライアンス標準に関連するリソースのパッチコンプライアンスに関する情報を提供します。	2020 年 9 月 1 日
コントロールの詳細ページを再設計	コントロールの詳細ページが再設計されました。統制結果リストには、コンプライアンスステータスに基づいてリストをすばやくフィルタリングできるタブがあります。また、非表示の結果をすばやく確認することもできます。各エントリは、検出結果リソース、 AWS Config ルール、および検出結果ノートに関する追加の詳細へのアクセスを提供します。	2020 年 8 月 28 日
結果の新しいフィルターオプション	結果フィルターでは、is not フィルターを使用すると、フィールド値がフィルター値と等しくない結果を検索できます。does not start with を使用すると、指定したフィルター値でフィールド値が開始しない結果を検索できます。	2020 年 8 月 28 日

ASFF の新規リソース詳細オブジェクト	次のリソースタイプの新しい Resources.Details オブジェクトが追加されました: AwsDynamoDbTable 、AwsEc2Eip 、AwsIamPolicy 、AwsIamUser 、AwsRdsDbCluster 、AwsRdsDbClusterSnapshot 、AwsRdsDbSnapshot 、AwsSecretsManagerSecret	2020 年 8 月 18 日
RSA Archer との新しい統合	Security Hub が RSA Archer と統合されました。RSA Archer は、Security Hub から結果を受け取ります。	2020 年 8 月 18 日
の新しい説明フィールド AwsKmsKey	Resources.Details の AwsKmsKey オブジェクトに Description フィールドが追加されました。	2020 年 8 月 18 日
にフィールドを追加 AwsRdsDbInstance	Resources.Details の AwsRdsDbInstance オブジェクトに複数の属性が追加されました。	2020 年 8 月 18 日

Security Hub によるコントロールの全体的なステータスを特定する方法を更新	結果がないコントロールの場合、ステータスは [Unknown] (不明) の代わりに [No data] (データなし) となります。コントロールステータスには、アカウントレベルの結果とリソースレベルの結果の両方が含まれます。コントロールステータスでは、非表示の結果を無視することを除き、結果のワークフローステータスが使用されません。	2020 年 8 月 13 日
Security Hub による標準のセキュリティスコアの計算方法を更新	標準のセキュリティスコアを計算するときに、Security Hub は、ステータスが [No Data] (データなし) のコントロールを無視するようになりました。セキュリティスコアは、データがないコントロールを除いた、有効なコントロールに対する合格コントロールの割合です。	2020 年 8 月 13 日
有効な標準で新しいコントロールを自動的に有効にする新しいオプション	有効な標準の新しいコントロールを自動的に有効にする [Settings] (設定) オプションが追加されました。`UpdateSecurityHubConfiguration` API オペレーションを使用しても、このオプションを設定できます。	2020 年 7 月 31 日

Payment Card Industry Data Security Standard (PCI DSS) 標準の新しいコントロール	PCI DSS 標準に新しいコントロールが追加されました。新しいコントロールの識別子は、PCI.DMS.1、PCI.EC2.5、PCI.EC2.6、PCI.ELBV2.1、PCI.GuardDuty.1、PCI.IAM.7、PCI.IAM.8、PCI.S3.5、PCI.S3.6、PCISageMaker.1、PCI.SSM.2、PCI.SSM.3 です。	2020 年 7 月 29 日
Foundational Security Best Practices 標準の新しいコントロールと更新	Foundational Security Best Practices 標準に新しいコントロールが追加されました。新しいコントロールの識別子は、 AutoScaling.1、DMS.1、EC2.4、EC2.6、S3.5、SSM.3 です。ACM.1 のタイトルが更新され、daysToExpiration パラメータの値が 30 に変更されました。	2020 年 7 月 29 日
ASFF の新しい Vulnerabilities オブジェクト	Vulnerabilities オブジェクトが追加されました。このオブジェクトは、結果に関連付けられた脆弱性に関する情報を提供します。	2020 年 7 月 1 日
Auto Scaling グループ、EC2 ボリューム、および EC2 VPC の ASFF の新しい Resource.Details オブジェクト	AwsAutoScalingAutoScalingGroup 、AWSEc2Volume 、および AwsEc2Vpc オブジェクトが Resource.Details に追加されました。	2020 年 7 月 1 日

ASFF の新しい NetworkPath オブジェクト	NetworkPath オブジェクトが追加されました。このオブジェクトは、結果に関連するネットワークパスに関する情報を提供します。	2020 年 7 月 1 日
Compliance.Status が PASSED のときに結果を自動的に解決	コントロールの結果については、Compliance.Status が PASSED の場合、Security Hub では自動的に Workflow.Status が RESOLVED に設定されます。	2020 年 6 月 24 日
AWS Command Line Interface 例	いくつかの Security Hub タスクの AWS CLI 構文と例を追加しました。これには、Security Hub の有効化、インサイトの管理、標準とコントロールの管理、製品統合の管理、Security Hub の無効化が含まれます。	2020 年 6 月 24 日
ASFF の新しい Severity.Original 属性	Severity.Original 属性が追加されました。この属性は、結果プロバイダーからの元の重要度です。これにより、廃止された Severity.Product 属性が置き換えられます。	2020 年 5 月 20 日
コントロールのステータスの詳細に関する ASFF の新しい Compliance.StatusReasons オブジェクト	Compliance.StatusReasons オブジェクトが追加されました。このオブジェクトは、コントロールの現在のステータスに関する追加のコンテキストを提供します。	2020 年 5 月 20 日

新しい AWS Foundational Security Best Practices 標準	新しい AWS Foundational Security Best Practices 標準を追加しました。これは、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場合に検出する一連のコントロールです。	2020 年 4 月 22 日
結果のワークフローステータスを更新する新しいコンソールオプション	Security Hub のコンソールまたは API を使用して結果のワークフローステータスを設定する方法の情報が追加されました。	2020 年 4 月 16 日
結果のお客様による更新の新しい BatchUpdateFindings API	BatchUpdateFindings を使用して結果の調査プロセスに関連する情報を更新する方法の情報が追加されました。BatchUpdateFindings は UpdateFindings に置き換えられますが、これは非推奨です。	2020 年 4 月 16 日

AWS Security Finding 形式 (ASFF) の更新	複数の新しいリソースタイプが追加されました。Label オブジェクトに新しい Severity 属性が追加されました。Label は Normalized フィールドを置き換えることを目的としています。結果の調査プロセスを追跡する新しい Workflow オブジェクトが追加されました。Workflow には、既存の Status 属性を置き換える Workflowstate 属性が含まれています。	2020 年 3 月 12 日
[Integrations] (統合) ページを更新	[Integrations] (統合) ページの変更を反映するように更新されました。各統合について、統合カテゴリと、Security Hub との結果の送受信について、各統合でいずれの操作が実行されるが示されます。また、各統合を有効にするために必要な特定の手順も示されています。	2020 年 2 月 26 日
新しいサードパーティー製品の統合	Cloud Custodian、FireEye Helix、Forcepoint CASB、Forcepoint DLP、Forcepoint NGFW、Rackspace Cloud Native Security、および Vectra.ai Cognito Detect という新しい製品統合が追加されました。	2020 年 2 月 21 日

Payment Card Industry Data Security Standard (PCI DSS) の新しいセキュリティ標準	Payment Card Industry Data Security Standard (PCI DSS) の Security Hub セキュリティ標準が追加されました。この標準が有効な場合、Security Hub は PCI DSS の要件に関連するコントロールに対して自動チェックを実行します。	2020 年 2 月 13 日
AWS Security Finding 形式 (ASFF) の更新	標準コントロールの関連要件のフィールドが追加されました。新しいリソースタイプと新しいリソースの詳細が追加されました。ASFF で、最大 32 のリソースを指定できるようになりました。	2020 年 2 月 5 日
個々のセキュリティ標準コントロールを無効にする新しいオプション	個々のセキュリティ標準コントロールを有効にするかどうかを制御する方法に関する情報が追加されました。	2020 年 1 月 15 日
用語と概念の更新	一部の説明が更新され、「用語と概念」に新しい用語が追加されました。	2019 年 9 月 21 日
AWS Security Hub の一般提供リリース	プレビュー期間中の Security Hub の改善を反映するためにコンテンツが更新されました。	2019 年 6 月 25 日
CIS AWS Foundations チェックの修復手順を追加	AWS Security Hub でサポートされているセキュリティ標準に修復手順を追加しました。	2019 年 4 月 15 日

AWS Security Hub のプレビューリリース	「AWS Security Hub ユーザーガイド」のプレビューリリースバージョンが公開されました。	2018 年 11 月 18 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。