ユーザーガイド

AWS Security Hub

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Security Hub : ユーザーガイド

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは、Amazon の所有物ではない製品またはサービスに関連づけて使用してはならず、どんな形であれ、お客様に混乱を招くような方法、あるいは Amazon の信用を傷つけたり失わせたりするような方法で使用することはできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

Security Hub と Security Hub CSPM とは 1
AWS Security Hub とは 2
機能 2
統合 3
AWS リージョン パブリックプレビューで をサポート 3
アクセシビリティ 4
料金 5
入門 5
Security Hub を有効にする 6
レコメンデーション 14
概念 16
OCSF の検出結果 17
カバレッジの検出結果 18
Security Hub CSPM のカバレッジ結果 18
GuardDuty のカバレッジ結果 18
Amazon Inspector のカバレッジ結果 19
Macie のカバレッジ結果 19
露出の検出結果 20
サポート リソース 20
サポートされている特性 21
露出の検出結果の生成 22
露出検出結果の重要度レベルの決定 27
露出の検出結果の確認 27
露出の検出結果の修正 30
攻撃シーケンスの検出結果 86
攻撃シーケンスの検出結果の確認 87
攻撃シーケンスの検出結果の修正 88
自動化ルール 88
主な機能強化 89
外部統合 89
OCSF でサポートされている基準 89
の OCSF フィールド `AutomationRulesFindingFieldsUpdate` 90
サードパーティ統合 3
KMS キーを作成する 90

Jira Cloud ... 93
ServiceNow ... 98
ダッシュボード ... 101
公開概要ウィジェット ... 102
脅威の概要ウィジェット ... 102
セキュリティカバレッジウィジェット ... 103
Security Hub でのリソースの詳細の表示 ... 103
潜在的な攻撃パスグラフ ... 104
Security Hub を無効にする ... 105
AWS Security Hub CSPM ... 106
Security Hub CSPM の利点 ... 107
Security Hub CSPM へのアクセス ... 108
関連サービス ... 109
Security Hub CSPM の無料トライアル、使用状況、料金 ... 110
使用状況の詳細と見積もりコストの表示 ... 110
料金詳細 ... 111
概念 ... 111
Security Hub CSPM の有効化 ... 117
必要なアクセス許可を確認する ... 117
Organizations との統合による Security Hub CSPM の有効化 ... 117
Security Hub CSPM を手動で有効にする ... 119
次のステップ: 姿勢管理と統合 ... 121
AWS Configの設定 ... 121
ローカル設定 ... 126
中央設定 ... 127
複数のアカウントの管理 ... 172
を使用したアカウントの管理 AWS Organizations ... 172
招待によるアカウントの手動での管理 ... 173
マルチアカウント環境の推奨事項 ... 173
を使用したアカウントの管理 AWS Organizations ... 175
招待によるアカウントの管理 ... 191
管理者アカウントとメンバーアカウントによって許可されるアクション ... 205
データに対するアカウントアクションの影響 ... 212
リージョン間のデータの集約 ... 215
集計されるデータのタイプ ... 216
管理者アカウントとメンバーアカウントの集計 ... 217

中央設定と集約 218
集約の有効化 219
集約設定の確認 221
集約設定の更新 222
集約の停止 224
[Standards] (標準) 226
標準リファレンス 227
標準を有効にする 324
標準の詳細の確認 330
自動有効化標準を無効にする 333
セキュリティ標準の無効化 335
コントロール 337
統合コントロールビュー 338
コントロールのセキュリティスコアの概要 339
コントロールリファレンスガイド 340
コントロールを設定するアクセス許可 1196
コントロールの有効化 1197
コントロールを無効化する 1205
セキュリティチェックとセキュリティスコア 1217
コントロールのカテゴリ 1293
コントロールの詳細の確認 1297
コントロールのフィルタリングとソート 1299
コントロールパラメータ 1301
コントロールの検出結果の確認と管理 1315
統合 1341
統合のリストの確認 1342
統合先からの検出結果のフローの有効化 1343
統合先からの検出結果フローの無効化 1344
統合先からの検出結果の表示 1345
AWS のサービス 統合 1346
サードパーティ統合 1368
カスタム製品の統合 1402
結果 1404
検出結果プロバイダーの BatchImportFindings 1406
お客様の BatchUpdateFindings 1410
検出結果の詳細と履歴の確認 1413

検出結果のフィルタリング 1418
結果をグループ化する 1421
結果のワークフローステータスを設定する 1421
カスタムアクションに結果を送信する 1425
検出結果形式: ASFF 1425
Insights 1721
インサイトの確認と対応 1722
マネージド型インサイト 1725
カスタムインサイト 1736
オートメーション 1744
自動化ルール 1745
自動応答および自動修復 1770
[要約] ダッシュボード 1787
リスク概要ウィジェット 1788
脅威の概要ウィジェット 1788
セキュリティカバレッジウィジェット 1788
[概要] ダッシュボードで利用できるウィジェット 1788
ダッシュボードのフィルタリング 1792
ダッシュボードのカスタマイズ 1794
リージョンの制限 1795
クロスリージョン集約の制限 1795
リージョン別の統合の可用性 1796
リージョン別の標準の有無 1798
リージョン別のコントロールの可用性 1799
コントロールの地域制限 1799
CloudFormation を使用したリソースの作成 2041
Security Hub CSPM と AWS CloudFormation テンプレート 2041
の詳細 AWS CloudFormation 2042
お知らせのサブスクライブ 2042
Amazon SNS メッセージ形式 2048
Security Hub CSPM の無効化 2050
セキュリティ 2053
データ保護 2053
Identity and Access Management 2055
対象者 2055
アイデンティティを使用した認証 2056

ポリシーを使用したアクセスの管理 2059
Security Hub と IAM の連携方法 2062
アイデンティティベースのポリシーの例 2070
サービスにリンクされた役割 2077
AWS 管理ポリシー 2080
トラブルシューティング 2090
コンプライアンス検証 2094
耐障害性 2095
インフラストラクチャセキュリティ 2095
VPC エンドポイントAWS PrivateLink 2096
Security Hub VPC エンドポイントに関する考慮事項 2096
Security Hub 用のインターフェイス VPC エンドポイントの作成 2096
Security Hub 用の VPC エンドポイントポリシーの作成 2096
共有サブネット 2097
API コールのログ作成 2098
CloudTrail の Security Hub CSPM 情報 2098
例: Security Hub CSPM ログファイルエントリ 2099
リソースのタグ付け 2101
タグ付けの基本 2101
IAMポリシーでタグを使用する 2103
リソースに タグを追加する 2104
リソースのタグを編集する 2106
リソースのタグを確認する 2108
リソースからのタグの削除 2111
クォータ 2113
最大クォータ 2113
レートクォータ 2113
ドキュメント履歴 2114
..... mmccxx

Security Hub と Security Hub CSPM とは

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

AWS Security Hub と AWS Security Hub CSPM は、クラウド環境を保護する AWS のサービス ものです。サービスは互いに褒め合います。これらを組み合わせると、 AWS 環境のセキュリティ体制に関する貴重なインサイトが得られます。

Security Hub CSPM は、セキュリティ体制を包括的に把握し、セキュリティ業界標準とベストプラクティスに照らしてクラウド環境を評価するのに役立ちます。Security Hub は、重要なセキュリティ問題の優先順位付けと対応に役立つ統一されたエクスペリエンスを提供します。Security Hub CSPM の検出結果は Security Hub に自動的にルーティングされ、Amazon Inspector などの他のセキュリティサービスの検出結果と相関して公開されます。これにより、環境内の最も重要なリスクを特定できます。Security Hub には自動化されたワークフロー機能も用意されており、Security Hub CSPM の検出結果を運用ワークフローに組み込むのに役立ちます。

ベストプラクティスとして、両方のサービスを有効にすることをお勧めします。設定ミスの特定とセキュリティ体制の評価が主な目的である場合、Security Hub を有効にせずに Security Hub CSPM を有効にできます。ただし、Security Hub CSPM を有効にせずに Security Hub を有効にした場合、Security Hub は Security Hub CSPM の検出結果を使用して AWS 、環境のリスクと露出に関する情報を提供することはできません。最適なエクスペリエンスを得るには、Security Hub と Security Hub CSPM を有効にするだけでなく、Amazon GuardDuty、Amazon Inspector、Amazon Macie などの他のセキュリティサービスを有効にすることをお勧めします。

AWS Security Hub とは

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

AWS Security Hub は、重要なセキュリティ問題を優先し、大規模な対応を支援する統合クラウドセキュリティソリューションです。Security Hub は、体制管理、脆弱性管理 (Amazon Inspector)、機密データ (Macie)、脅威検出 (GuardDuty) など、複数のソースからのセキュリティシグナルを自動的に関連付けて強化することで、セキュリティの問題を検出します。これにより、セキュリティチームは自動分析とコンテキストインサイトを通じて、クラウド環境でアクティブなリスクに優先順位を付けることができます。直感的な視覚化により、Security Hub は複雑なセキュリティシグナルを実用的なインサイトに変換し、セキュリティについて情報に基づいた意思決定を迅速に行うことができます。Security Hub には、リスクの修復、チームの生産性の向上、運用の中断の最小化に役立つ自動対応ワークフローも含まれています。

機能

統合セキュリティソリューション

統合されたクラウドセキュリティソリューションで一元管理することで、クラウド環境全体の可視性を高めます。

実用的なセキュリティインサイト

高度な分析を通じて実用的なセキュリティインサイトを取得し、環境に関連するセキュリティリスクについて学習します。

応答時間の短縮

自動化されたワークフローと統合されたチケット発行システムで応答時間を合理化します。

露出の検出結果

Security Hub は、Security Hub CSPM コントロールチェック、Amazon Inspector などの検出結果を関連付け AWS のサービス て、 AWS リソースに関連する露出を検出します。

結果は Open Cybersecurity Schema Framework (OCSF) でフォーマットされています

Security Hub は OCSF で検出結果を生成し、Security Hub CSPM などから OCSF で検出結果を受け取ります AWS のサービス。

- Amazon GuardDuty
- Amazon Macie
- Amazon Inspector

ダッシュボード

Security Hub コンソールは、公開、脅威、セキュリティカバレッジ、リソースの包括的なビューと、潜在的な攻撃者が公開結果に関連するリソースにアクセスして制御する方法を示す攻撃パスグラフと呼ばれるインタラクティブな視覚化を提供します。

サードパーティー製品との統合

Security Hub 統合を使用すると、セキュリティ体制を強化できます。たとえば、 Jira Cloudまたはを使用する場合ServiceNow ITSM、この機能を使用して検出結果からチケットを作成できます。

統合

Security Hub は以下と統合されています AWS のサービス。

- AWS Security Hub CSPM
- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie

AWS リージョン パブリックプレビューで をサポート

Security Hub は、このパブリックプレビューリリース AWS リージョン で以下をサポートしています。

- アジアパシフィック (東京)
- アジアパシフィック (ソウル)
- アジアパシフィック (大阪)

- アジアパシフィック (ムンバイ)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- カナダ (中部)
- 欧州 (フランクフルト)
- 欧州 (ストックホルム)
- 欧州 (アイルランド)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- 欧州 (ロンドン)
- 欧州 (パリ)
- 南米 (サンパウロ)
- 米国東部 (バージニア北部)
- 米国東部 (オハイオ)

以下はオプトインです。オプトインにアクセスするには AWS リージョン、オプトインを有効にする必要があります。

- アフリカ (ケープタウン)
- アジアパシフィック (香港)
- アジアパシフィック (ジャカルタ)
- 欧州 (ミラノ)
- 中東 (バーレーン)

詳細については AWS リージョン、 およびアベイラビリティーゾーンユーザーガイドの「オプトインステータス」を参照してください。 AWS リージョン

アクセシビリティ

Security Hub は、上記の AWS リージョン で利用できます。組織内の個々のアカウントまたはアカウントに対して Security Hub を有効にできます。Security Hub には、以下を通じてアクセスできます。

Security Hub コンソール

Security Hub コンソールは、 AWS リソースの作成と管理に使用できるブラウザベースのインターフェイスです。このコンソールでは、アカウント、データ、リソースにアクセスできます。

Security Hub API

Security Hub API を使用すると、アカウント、データ、リソースにプログラムでアクセスできます。HTTPS リクエストは Security Hub に直接送信できます。

AWS CLI

を使用するとAWS CLI、システムコマンドラインでコマンドを実行してタスクを実行し、タスクを実行するスクリプトを構築できます。場合によっては、 AWS CLI Security Hub コンソールよりも の方が便利です。

AWS SDKs

AWS SDKsは、さまざまなプログラミング言語とプラットフォーム (C++、Go、Java、.NET、Python) 用のライブラリとサンプルコードで構成されています。これらは、任意の言語で Security Hub やその他の へのプログラム AWS のサービス によるアクセスを提供し、エラーの管理、リクエストの署名、リクエストの再試行などのタスクの管理に役立ちます。

料金

Security Hub の使用に料金はかかりません。Security Hub は、このパブリックプレビュー中は無料です。

Security Hub の開始方法

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

このセクションのトピックでは、Security Hub の使用を開始する方法について説明します。

Security Hub を有効にする

> **Note**
> Security Hub はプレビューリリースであり、変更される可能性があります。

任意の に対して Security Hub を有効にできます AWS アカウント。このトピックの手順では、 AWS 組織管理アカウント、委任管理者アカウント、スタンドアロンアカウントから Security Hub を有効にする方法について説明します。

> **Note**
> Security Hub を有効にすると、環境内の露出がすぐに分析されます。ただし、リソースの公開結果を受信するまで最大 6 時間待つことができます。

組織の Security Hub を有効にする

このセクションの手順では、 AWS 組織管理アカウントの Security Hub を有効にする方法について説明します。この手順では、Security Hub CSPM の委任管理者を設定し、Security Hub で組織の委任管理者を設定できるステップが含まれていることを前提としています。Security Hub での委任管理者の設定の詳細については、「Security Hub での委任管理者アカウントの設定」を参照してください。

有効化中に Security Hub の委任管理者を設定する場合は、AWS Organizations コンソールでリソースポリシーを作成し、委任管理者が組織に代わってアクションを実行できるようにする必要があります。委任管理者アカウントには、次のサンプルリソースポリシーを使用できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::delegated-administrator-account-id:root"
      },
      "Action": [
```

```
        "organizations:AttachPolicy",
        "organizations:CreatePolicy",
        "organizations:DetachPolicy",
        "organizations:DeletePolicy",
        "organizations:UpdatePolicy",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:DisablePolicyType",
        "organizations:EnablePolicyType"
      ],
      "Resource": "*"
    }
  ]
}
```

委任管理者を設定しない場合は、後で委任管理者を設定できます。詳細については、「Security Hub での委任管理者アカウントの設定」を参照してください。トピックには、Security Hub コンソールの全般ページから組織の委任管理者を設定する方法を説明する手順が含まれています。

次の手順では、Security Hub で組織の委任管理者アカウントを設定する方法について説明します。

AWS 組織管理アカウントの Security Hub を有効にするには

1. AWS 組織管理 AWS アカウントの認証情報を使用してアカウントにサインインします。https://console.aws.amazon.com/securityhub/v2/home で Security Hub コンソールを開きます。
2. Security Hub ホームページから、Security Hub を選択します。[開始する] を選択します。
3. （オプション) 委任管理者アカウントの場合、提供されたオプションに基づいて委任管理者を設定します。ベストプラクティスとして、一貫したガバナンスのために、セキュリティサービス全体で同じ委任管理者を使用することをお勧めします。委任管理者アカウントの設定の詳細については、Security Hub の「委任管理者アカウントの設定」を参照してください。
4. （オプション) アカウントを有効にするには、チェックボックスをオンにして AWS アカウントの Security Hub を有効にします。
5. コピーしてアタッチを選択して組織設定を開きます。Organizations コンソールで、委任された管理者 AWS Organizationsの下にある委任を選択し、リソースポリシーを貼り付けます。ポリシーの作成を選択します。
6. Security Hub コンソールに移動します。[設定] を選択します。

Security Hub を有効にすると、AWSServiceRoleForSecurityHubV2 というサービスにリンクされたロールがアカウントに作成され、サービスにリンクされたレコーダーがアカウントに追加されます。サービスにリンクされたレコーダーは、 AWS サービス固有のリソースの設定データを記録できるサービスによって管理される AWS Config レコーダーの一種です。サービスにリンクされたレコーダーを使用すると、Security Hub は、露出分析カバレッジに必要なリソース設定項目を取得するためのイベント駆動型のアプローチを可能にします。サービスにリンクされたレコーダーは、 AWS アカウント および ごとに設定されます AWS リージョン。

> **Note**
>
> 委任管理者を設定すると、委任管理者は Security Hub のメンバーアカウントを有効または無効にするポリシーを作成して適用できます。詳細については、「メンバーアカウントを管理する委任管理者としてのポリシーの作成」を参照してください。

委任管理者の Security Hub を有効にする

AWS 組織管理アカウントが組織の委任管理者を設定する場合、委任管理者はアカウントの Security Hub を有効にする必要があります。以下の手順は、委任管理者がアカウントの Security Hub を有効にしていない場合にのみ、委任管理者が完了する必要があります。委任管理者の設定については、Security Hub の「委任管理者アカウントの設定」を参照してください。

委任管理者アカウントの Security Hub を有効にするには

1. 委任された管理者認証情報を使用して AWS アカウントにサインインし、https://console.aws.amazon.com/securityhub/v2/home で Security Hub コンソールを開きます。
2. Security Hub ホームページから Security Hub を選択し、開始方法を選択します。
3. [有効化] を選択します。
4. (オプション) タグでは、キーと値のペアをアカウント設定に追加するかどうかを決定します。
5. [Go to Security Hub] (Security Hub に移動) を選択します。

Security Hub を有効にすると、AWSServiceRoleForSecurityHubV2 というサービスにリンクされたロールがアカウントに作成され、サービスにリンクされたレコーダーがアカウントに追加されます。サービスにリンクされたレコーダーは、 AWS サービス固有のリソースの設定データを記録できるサービスによって管理される AWS Config レコーダーの一種です。サービスにリンクされたレコーダーを使用すると、Security Hub は、露出分析カバレッジに必要なリソース設定項目を取得するため

のイベント駆動型のアプローチを可能にします。サービスにリンクされたレコーダーは、 AWS アカウント および ごとに設定されます AWS リージョン。

> **Note**
>
> 組織の委任管理者は、Security Hub のメンバーアカウントを有効または無効にするポリシーを作成して適用できます。詳細については、「メンバーアカウントを管理するための委任管理者としてのポリシーの作成」を参照してください。

スタンドアロンアカウントの Security Hub を有効にする

次の手順では、スタンドアロンアカウントで Security Hub を有効にする方法について説明します。Security Hub を有効にできるスタンドアロンアカウントには、組織内に AWS アカウント ない と組織 AWS アカウント 内の の 2 種類があります。 AWS 組織 AWS アカウント 内の は、委任管理者が に AWS Organizations ポリシー AWS アカウント をアタッチする にすることができます AWS アカウント。詳細については、「 AWS Organizations ユーザーガイド」の「Security Hub ポリシー」を参照してください。

スタンドアロンアカウントの Security Hub を有効にするには

1. 認証情報を使用して AWS アカウントにサインインし、https://console.aws.amazon.com/securityhub/v2/home で Security Hub コンソールを開きます。
2. Security Hub ホームページから Security Hub を選択し、開始方法を選択します。
3. [有効化] を選択します。

Security Hub を有効にすると、AWSServiceRoleForSecurityHubV2 というサービスにリンクされたロールがアカウントに作成され、サービスにリンクされたレコーダーがアカウントに追加されます。サービスにリンクされたレコーダーは、 AWS サービス固有のリソースの設定データを記録できるサービスによって管理される AWS Config レコーダーの一種です。サービスにリンクされたレコーダーを使用すると、Security Hub は、露出分析カバレッジに必要なリソース設定項目を取得するためのイベント駆動型のアプローチを可能にします。サービスにリンクされたレコーダーは、 AWS アカウント および ごとに設定されます AWS リージョン。

Security Hub での委任管理者アカウントの設定

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

AWS 組織管理アカウントから、組織の委任管理者を設定できます。ベストプラクティスとして、一貫したガバナンスのために、セキュリティサービス全体で同じ委任管理者を使用することをお勧めします。このセクションの手順では、2 つの方法で組織の委任管理者を設定する方法について説明します。最初の方法は、Security Hub CSPM で委任管理者を設定していない AWS 組織管理アカウントの場合です。2 番目の方法は、Security Hub を有効にしたが、有効化中に委任管理者の設定をスキップした AWS 組織管理アカウントの場合です。

考慮事項

Security Hub CSPM の委任管理者とは異なる Security Hub の委任管理者を設定するシナリオが発生する場合があります。Security Hub CSPM で委任管理者を設定している場合は、次の点を考慮してください。

- AWS 組織管理アカウントが Security Hub CSPM の委任管理者として設定されている場合、このアカウントを Security Hub の委任管理者として設定することはできません。ただし、組織 AWS アカウント 内の別の を Security Hub の委任管理者として指定することはできます。セキュリティサービス全体で一貫したガバナンスを実現するには、Security Hub CSPM と Security Hub の委任管理者と同じアカウント (AWS 組織管理アカウント以外) を使用することをお勧めします。
- AWS 組織管理アカウント以外のアカウントが Security Hub CSPM の委任管理者として設定されている場合、このアカウントは自動的に Security Hub の委任管理者になります。このシナリオでは、Security Hub は、この特定の のみを委任管理者として AWS アカウント 使用できます。

> **Note**
>
> Security Hub CSPM 委任管理者として組織管理アカウント以外のアカウントを使用している場合、Security Hub CSPM コンソールまたは AWS Organizations API を使用してアカウントを削除すると、Security Hub からも削除されます。同様に、Security Hub コンソールまたは AWS Organizations API を使用して Security Hub 委任管理者を削除すると、Security Hub CSPM から削除されます。委任された管理者が Security Hub CSPM から削除されると、中央設定は自動的にオプトアウトします。

次の手順では、Security Hub CSPM の委任管理者を設定しておらず、Security Hub の委任管理者を設定していることを前提としています。

Security Hub で委任管理者を設定するには

1. 組織管理 AWS アカウントの認証情報を使用してアカウントにサインインし、https://console.aws.amazon.com/securityhub/v2/home で Security Hub コンソールを開きます。
2. Security Hub ホームページから Security Hub を選択し、開始方法を選択します。
3. 委任された管理者で、設定 を選択します。ポップアップウィンドウで、 AWS アカウント 必要な の 12 桁の AWS アカウント 番号を入力するか、推奨アカウント (他のセキュリティサービスで委任管理者を使用する場合) を選択して、組織の委任管理者として を設定します。[保存] を選択します。
4. (オプション) アカウントを有効にするには、 の Security Hub を有効にするボックスを選択します AWS アカウント。
5. コピーしてアタッチを選択して組織設定を開きます。Organizations コンソールで、委任された管理者 AWS Organizationsの下にある委任を選択し、リソースポリシーを貼り付けます。ポリシーの作成を選択します。
6. Security Hub コンソールに移動します。[設定] を選択します。

> **Note**
>
> 委任された管理者を設定した後、そのアカウントは Security Hub を有効にし、メンバーアカウントから結果を受信するようにポリシーを設定する必要があります。

次の手順では、Security Hub を有効にしたが、有効化中に委任管理者の設定をスキップすることを前提としています。Security Hub コンソールの一般ページから委任管理者を設定できます。

全般ページから Security Hub コンソールで委任管理者を設定するには

1. 組織管理 AWS アカウントの認証情報を使用してアカウントにサインインし、https://console.aws.amazon.com/securityhub/v2/home で Security Hub コンソールを開きます。
2. ナビゲーションペインから、全般を選択します。
3. 委任された管理者で、設定 を選択します。ポップアップウィンドウで、組織の委任管理者として設定 AWS アカウント する の 12 桁の AWS アカウント 番号を入力します。または、他の

AWS セキュリティサービスで委任管理者を設定する AWS アカウント 場合は、推奨 を選択します。[保存] を選択します。

この手順を完了したら、Security Hub の委任ポリシーステートメントをコピーし、 AWS Organizations ポリシーの委任管理者にアタッチする必要があります。これにより、Security Hub の委任管理者は Security Hub でアクションを実行できます。このポリシーステートメントがないと、委任管理者は組織の Security Hub を設定できません。詳細については、「Security Hub の委任ポリシーステートメントのアタッチ」を参照してください。

Security Hub の委任ポリシーステートメントのアタッチ

組織管理アカウントから、Security Hub の委任ポリシーステートメントをコピーし、 AWS Organizations ポリシーの委任管理者にアタッチする必要があります。これにより、Security Hub の委任管理者は Security Hub でアクションを実行できます。このポリシーステートメントがないと、委任管理者は組織の Security Hub を設定できません。このポリシーは、Security Hub コンソールの全般ページからコピーできます。これを行うと、 AWS Organizations コンソールの設定ページが表示され、 AWS Organizations ポリシーの委任管理者を編集できます。このトピックでは、Security Hub でポリシーをコピーする方法について説明します。 AWS Organizations ポリシーの委任管理者を更新する方法については、「 AWS Organizations ユーザーガイド」の「 でリソースベースの委任ポリシーを更新する AWS Organizations」を参照してください。

Security Hub の委任ポリシーステートメントをアタッチするには

1. 組織管理 AWS アカウントの認証情報を使用してアカウントにサインインし、https://console.aws.amazon.com/securityhub/v2/home で Security Hub コンソールを開きます。
2. ナビゲーションペインから、全般を選択します。
3. Security Hub の委任ポリシーステートメントで、コピーしてアタッチを選択します。「設定」ページが表示され AWS Organizations 、 AWS Organizations ポリシーの委任管理者を編集して、委任ポリシーステートメントを含めることができます。ポリシーステートメントをコピーする前に表示する場合は、ポリシーの詳細を選択します。

> **Note**
>
> 委任管理者を設定すると、委任管理者は memeber アカウントの有効化と無効化を許可するポリシーを作成して適用できます。次のトピックの手順では、このポリシーを設定する方法について説明します。

メンバーアカウントを管理するための委任管理者としてのポリシーの作成

組織の委任管理者は、メンバーアカウントを有効または無効にできるポリシーを作成して適用できます。Security Hub コンソールの設定画面から、設定済みのすべてのポリシーにアクセスできます。次の手順では、このポリシーを作成する方法について説明します。

> **Note**
>
> ステップ 6. は、このポリシーが親ポリシーとどのように相互作用するかを記述できるオプションのステップです。ポリシーの継承の詳細については、AWS Organizations 「 ユーザーガイド」の「管理ポリシーの継承について」を参照してください。

メンバーアカウントの有効化と無効化を許可するポリシーを作成するには

1. 認証情報を使用してサインインし、https://console.aws.amazon.com/securityhub/v2/home?region=us-east-1 で Security Hub コンソールを開きます。
2. ナビゲーションペインで、設定 を選択し、設定 を選択します。
3. [Create policy] (ポリシーの作成) を選択します。
4. 詳細 にポリシーの名前を入力し、ポリシーのオプションの説明を入力するかどうかを決定します。
5. リージョンの場合は、すべてのリージョンを有効にする、すべてのリージョンを無効にする、またはリージョンを指定するを選択します。すべてのリージョンを有効にするを選択すると、新しいリージョンを自動的に有効にするかどうかを判断できます。すべてのリージョンを無効にするを選択すると、新しいリージョンを自動的に無効にするかどうかを判断できます。リージョンを指定するを選択した場合は、有効または無効にするリージョンを選択する必要があります。
6. (オプション) 詳細設定については、 のガイダンスを参照してください AWS Organizations。
7. (オプション) タグでは、キーと値のペアをポリシーに追加するかどうかを決定します。最大 50 個のタグを追加できます。
8. [次へ] を選択します。
9. 変更を確認し、適用を選択します。ターゲットアカウントは、ポリシーに基づいて設定されます。有効なポリシーをアカウントレベルで表示するには、設定ページの組織タブでアカウントを選択できます。

Security Hub での委任管理者アカウントの削除

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

Security Hub コンソールで委任管理者アカウントはいつでも削除できます。ただし、このアクションは、委任された管理者を Security Hub から削除するだけでなく、Security Hub CSPM も削除します。このアクションは、セキュリティアカウントでこのオペレーションを確認した場合にのみ実行することをお勧めします。

> **Note**
>
> Security Hub CSPM 委任管理者として組織管理アカウント以外のアカウントを使用している場合、CSPM コンソールまたは AWS Organizations API を使用してアカウントを削除すると、Security Hub からも削除されます。
> 同様に、Security Hub コンソールまたは AWS Organizations API を使用して Security Hub 委任管理者を削除すると、Security Hub CSPM からも削除されます。委任された管理者が CSPM から削除されると、中央設定は自動的にオプトアウトされます。

委任管理者アカウントを削除するには

1. 組織管理 AWS アカウントの認証情報を使用してアカウントにサインインし、https://console.aws.amazon.com/securityhub/v2/home?region=us-east-1 で Security Hub コンソールを開きます。
2. ナビゲーションペインから、全般を選択します。
3. 委任管理者で、委任管理者の削除を選択します。ポップアップウィンドウで確認と入力し、削除を選択します。

Security Hub の推奨事項

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

の次のセキュリティサービスは、検出結果を OCSF 形式で Security Hub AWS に送信します。Security Hub を有効にしたら、セキュリティを強化 AWS のサービス するためにこれらを有効にすることをお勧めします。

Security Hub CSPM

Security Hub CSPM を有効にすると、 のセキュリティ状態が包括的に表示されます AWS。これにより、セキュリティ業界標準とベストプラクティスに照らして環境を評価することができます。Security Hub CSPM を有効にしなくても Security Hub の使用を開始できますが、Security Hub は Security Hub CSPM からのセキュリティシグナルを関連付けて体制管理を改善するため、Security Hub CSPM を有効にすることをお勧めします。

Security Hub CSPM を有効にする場合は、アカウントの AWS Foundational Security Best Practices 標準を有効にすることもお勧めします。この標準は、 AWS アカウント および リソースがセキュリティのベストプラクティスから逸脱した場合を検出する一連のコントロールで構成されています。アカウントの AWS Foundational Security Best Practices 標準を有効にすると、 AWS Security Hub CSPM は、次のリソースタイプのコントロールを含むすべてのコントロールを自動的に有効にします。

- アカウントコントロール
- DynamoDB コントロール
- Amazon EC2 コントロール
- IAM コントロール
- AWS Lambda コントロール
- Amazon RDS コントロール
- Amazon S3 コントロール

このリストのいずれかのコントロールを無効にすることができます。ただし、これらのコントロールのいずれかを無効にすると、サポートされているリソースの公開結果を受け取ることはできません。Foundational Security Best Practices 標準に適用されるコントロールの詳細については、 AWS AWS 「 Foundational Security Best Practices v1.0.0 (FSBP) standard」を参照してください。

GuardDuty

GuardDuty を有効にすると、Security Hub コンソールのダッシュボードですべての脅威とセキュリティカバレッジの検出結果を表示できます。GuardDuty を有効にすると、GuardDuty は OCSF 形式で Security Hub へのデータの送信を自動的に開始します。

Amazon Inspector

Amazon Inspector を有効にすると、Security Hub コンソールのダッシュボードですべての露出とセキュリティカバレッジの検出結果を表示できます。Amazon Inspector を有効にすると、Amazon Inspector は OCSF 形式で Security Hub へのデータの送信を自動的に開始します。

Amazon EC2 スキャンと Lambda 標準スキャンをアクティブ化することをお勧めします。Amazon EC2 スキャンをアクティブ化すると、Amazon Inspector はアカウントの Amazon EC2 インスタンスをスキャンして、パッケージの脆弱性とネットワーク到達可能性の問題を確認します。Lambda 標準スキャンをアクティブ化すると、Amazon Inspector は Lambda 関数をスキャンして、パッケージの依存関係におけるソフトウェアの脆弱性を確認します。詳細については、Amazon Inspector ユーザーガイド」の「スキャンタイプのアクティブ化」を参照してください。

Macie

Macie を有効にすると、Amazon S3 バケットの追加露出を検出できます。Macie が Amazon S3 バケットインベントリを毎日評価できるように、機密データ自動検出を設定することをお勧めします。

Security Hub の概念

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

以下の用語と概念は、露出の検出結果を管理する方法を理解するのに役立ちます。

露出

アカウントの潜在的なセキュリティシナリオで、脆弱性、悪用可能なリソース、または設定ミスが原因である可能性があります。

露出の検出結果

環境に存在する露出を記述する検出結果のタイプ。露出の検出結果には、特性とシグナルが含まれます。シグナルには、1 つ以上のタイプの露出特性を含めることができます。Security Hub は、Security Hub CSPM コントロールの検出結果や Amazon Inspector AWS のサービスなどの他の からのシグナルが露出の存在を示すと、露出の検出結果を生成します。リソースには、最大 1 つの露出検出結果を含めることができます。Security Hub は、リソースが公開されると公開結果

を生成します。リソースに露出特性がない場合、または不十分な特性がある場合、Security Hub はそのリソースの露出結果を生成しません。

Signal

露出検出結果に寄与する検出結果。シグナルは、寄与する検出結果と呼ばれます。シグナルは、Security Hub CSPM AWS Config、または Amazon Inspector AWS のサービスなどの他の から発信できます。

特性

露出の検出結果につながるセキュリティ偏差。特性タイプには、設定ミス、到達可能性、機密データ、脆弱性などがあります。特性は 1 つのシグナルに関連付けられ、シグナルには複数の特性を含めることができます。例えば、Security Hub CSPM コントロールは、カスタマー管理ポリシーが管理アクセスコントロールを許可していることを示します。このシグナルには、設定ミスの特性が含まれています。

Security Hub での OCSF の検出結果

> **Note**
> Security Hub はプレビューリリースであり、変更される可能性があります。

Security Hub のすべての検出結果は、Open Cybersecurity Schema Framework (OCSF) でフォーマットされています。Security Hub は、 の検出結果をアクティブな検出結果と見なす`activity_name != Close`します。アクティブな検出結果は、90 日以内に更新されない場合に自動的に削除されます。Security Hub は、 の検出結果を`Activity_name = Close`クローズド検出結果と見なします。クローズされた検出結果は、14 日以内に更新されない場合、自動的に削除されます。Security Hub は、検出結果の最新の値を使用して検出結果を更新するタイミングを決定します`modified_time_dt`。検出結果の保持期間が終了すると、Security Hub は検出結果を完全に削除します。検出結果プロバイダーは、検出結果を更新するときに `finding.info.modified_time_dt`フィールドの値を変更することができます。他の`Activity_name`値の詳細については、OCSF スキーマの「脆弱性の検出結果https://schema.ocsf.io/1.5.0/classes/vulnerability_finding」を参照してください。

Security Hub でのカバレッジの検出結果

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

Security Hub のカバレッジ検出結果は、どの AWS セキュリティ機能が有効で、スタンドアロンアカウントまたは組織の AWS 環境全体でカバレッジにギャップがある可能性があるかを可視化します。追加のセキュリティ機能を有効にすると、Security Hub の検出機能が強化されます。Coverage Findings は、アカウントに対して有効になっている GuardDuty、Amazon Inspector、Macie、および Security Hub CSPM の機能を評価します。これらの検出結果は、Security Hub ダッシュボードにウィジェットとして表示され、特定のセキュリティ機能別により詳細なビューにドリルダウンできます。委任管理者の場合、このウィジェットには、Security Hub が有効なすべてのアカウントのカバレッジ内訳が表示されます。

制限

- メンバーアカウントの場合、カバレッジ情報はリンクされた 間で集計されますが AWS リージョン、そのメンバーアカウントに対してのみ集計されます。
- Security Hub にオンボーディングされていないアカウントではカバレッジ情報が表示されない
- カバレッジは、 AWS のサービス サービス内の特定の機能が有効になっているかどうかではなく、 AWS が有効になっているかどうかのみを示します。

Security Hub CSPM のカバレッジ結果

Security Hub CSPM Coverage Findings は、アカウントで認定された体制管理セキュリティ標準が有効になっているかどうかを評価します。Security Hub CSPM Standard を有効にすると、 AWS Control Tower および リソースタグ付け標準を除き、 が対象になります。

Security Hub CSPM を有効にすると、デフォルトで有効になっている標準が検出されるまでに最大 24 時間かかることがあります。

GuardDuty のカバレッジ結果

GuardDuty カバレッジの検出結果は、GuardDuty が有効になっているかどうか、および でどの GuardDuty 機能が有効になっているかを評価します AWS アカウント。

- Malware Protection for Amazon EC2 – Amazon EC2 インスタンスをスキャンしてマルウェアの可能性がないか調べます
- Amazon EKS Protection – Amazon EKS クラスター内の脅威について Kubernetes 監査ログをモニタリングします
- Lambda Protection – Lambda 関数の呼び出しを分析して潜在的な脅威がないか調べます
- Amazon S3 Protection – Amazon S3 バケットへの潜在的な脅威に関するデータイベントを分析します
- Amazon RDS Protection – Amazon RDS データベースへの脅威を監視します
- Runtime Monitoring – Amazon EC2 インスタンスのランタイム動作をリアルタイムでモニタリングします。

GuardDuty カバレッジの更新が組織内のすべてのメンバーアカウントに反映されるまでに、最大 24 時間かかることがあります。

Amazon Inspector のカバレッジ結果

Amazon Inspector Coverage Findings はAmazon Inspector が有効になっているかどうか、およびアカウントで有効になっている機能を評価します。

- Amazon EC2 スキャン – Amazon EC2 インスタンスの脆弱性をスキャンします
- Amazon ECR スキャン – Amazon ECR のコンテナイメージの脆弱性をスキャンします
- Lambda 標準スキャン – Lambda 関数の脆弱性をスキャンします
- Lambda コードスキャン – Lambda コード関数をスキャンしてコードの脆弱性を確認します
- Amazon Inspector コードセキュリティ – ファーストパーティーアプリケーションのソースコード、サードパーティーアプリケーションの依存関係、Infrastructure as Code の脆弱性をスキャンします。

Macie のカバレッジ結果

Macie Coverage Findings は、Macie が有効になっているかどうかを示す評価です AWS アカウント。

Macie 自動機密データ検出の更新が組織内のすべてのメンバーアカウントに反映されるまでに、最大 24 時間かかることがあります。

Security Hub での露出の検出結果

> **Note**
> Security Hub はプレビューリリースであり、変更される可能性があります。

Security Hub は AWS のサービス、Security Hub CSPM コントロールチェックや Amazon Inspector などの他の の検出結果を関連付けて、 AWS リソースに関連する露出を検出します。露出検出結果は、脆弱性、悪用可能なリソース、または設定ミスによる環境内の潜在的な露出を説明する検出結果の一種です。最も重要な露出を優先して解決することで、環境に対する潜在的な攻撃を防ぐことができます。Security Hub コンソールで、Security Hub CSPM および Security Hub API オペレーションを使用してプログラムで公開結果にアクセスできます。

Security Hub での公開結果でサポートされているリソースタイプ

> **Note**
> Security Hub はプレビューリリースであり、変更される可能性があります。

Security Hub は、次の AWS リソースタイプの公開結果を生成します。

- `AWS::DynamoDB::Table`
- `AWS::EC2::Instance`
- `AWS::ECS::Service`
- `AWS::EKS::Cluster`
- `AWS::IAM::User`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::S3::Bucket`

Security Hub は、リソースごとに 1 つの公開結果を生成します。リソースに露出特性がない場合、または不十分な特性がある場合、Security Hub はそのリソースの露出結果を生成しません。

Security Hub でサポートされている特性タイプ

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

Security Hub は、 AWS Security Hub CSPM コントロールの検出結果と AWS のサービス Amazon Inspector などのサポートされている他の によって生成された検出結果に、リソースの公開特性が含まれている場合に、公開検出結果を生成します。次の表は、サポートされている特性タイプに関する情報を示しています。

特性タイプ	説明	ソース	影響を受けるリソース
設定ミス	リソースの設定ミスを示します。	Security Hub CSPM コントロールの検出結果。	すべてのリソースタイプ。
到達可能性	リソースへのオープンネットワークパスを示します。	Security Hub CSPM コントロールの検出結果と Amazon Inspector ネットワーク到達可能性の検出結果。	Amazon EC2 インスタンス
機密データ	リソースに機密データが含まれていることを示します。	Macie 機密データの検出結果。	Amazon S3 バケット
脆弱性	リソースが共通脆弱性識別子 (CVEs) に公開されていることを示します。	Amazon Inspector パッケージの脆弱性の検出結果。	Amazon EC2 インスタンス、Amazon ECS サービス、Amazon EKS クラス

特性タイプ	説明	ソース	影響を受けるリソース
			ター、Lambda 関数

各特性は、リソースに影響を与える露出に関する詳細を提供する複数のタイトルに関連付けることができます。たとえば、EC2 露出検出結果の詳細に脆弱性特性の Exploit Available タイトルが表示される場合があります。

露出の検出結果の生成

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

Security Hub は 6 時間ごとに公開結果を生成します。各 6 時間の間に、Security Hub はリソースの利用可能な露出特性を考慮します。リソース ID ごとに最大 1 つの露出結果を生成します。検出結果の一意性は、ID AWS リージョン、タイプ、アカウントによって決まります。つまり、同じ ID を持つ 2 つのリソースを持つことができますが、リソースは異なるリソースタイプになります。この露出検出結果は、リソースに適用されるすべての適用可能な露出特性を集計します。

リソースに露出特性がない場合、または不十分な特性がある場合、Security Hub はそのリソースの露出結果を生成しません。Security Hub は、公開結果をサポートしていないリソースタイプの公開結果を発行しません。リソースに多数の特性と特性の組み合わせがある場合、Security Hub は公開結果を生成します。特性の数と組み合わせによって、露出検出結果の重要度レベルも決まります。

サンプル露出の検出結果

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

Security Hub は、Open Cybersecurity Schema Framework (OCSF) の公開結果を正規化します。

OCSF スキーマのサンプル

次のサンプル OCSF スキーマでは、 `related_events`パラメータに、結果の寄与など、公開結果に固有の詳細が含まれています。寄与結果とは、露出結果に関連する特性とシグナルです。1 つの寄与結果には、1 つ以上の特性を含めることができます。`observables` パラメータは、寄与する検出結果に関連付けられたリソースを識別します。これは、公開結果に関連付けられたリソースを識別する `resources`パラメータとは異なる場合があります。

```
{
    "activity_id": 1,
    "activity_name": "Create",
    "category_name": "Findings",
    "category_uid": 2,
    "class_name": "Detection Finding",
    "class_uid": 2004,
    "cloud": {
        "account": {
            "uid": "123456789012",
            "name": "production-application"
        },
        "cloud_partition": "aws",
        "provider": "AWS",
        "region": "us-east-1"
    },
    "finding_info": {
        "analytic": {
            "name": "Exposure",
            "type": "Rule",
            "type_id": 1,
            "uid": "0.0.1"
        },
        "created_time_dt": "2024-11-15T21:39:26.337224100Z",
        "desc": "Publicly invocable Lambda function executed outside of VPC has
 vulnerability with known exploit that can be exploited from remote network",
        "finding.info.modified_time_dt": "2024-11-15T21:39:26.337224100Z",
        "related_events_count": 3,
        "related_events": [
            {
                "tags": [
                    {
                        "name": "Vulnerability",
                        "values": [
                            "Attack Vector Network",
                            "EPSS Level >= High",
                            "EPSS Level >= Medium",
```

```
                            "Exploit Available",
                            "No Privileges Required",
                            "No User Interaction Required",
                            "Vulnerable"
                        ]
                    }
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/inspector"
                },
                "observables": [
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
                    }
                ],
                "type": "Finding",
                "title": "CVE-2023-33246 - org.apache.rocketmq:rocketmq-controller",
                "uid": "arn:aws:inspector2:us-
east-1:123456789012:finding/1234567890abcdef0"
            },
            {
                "tags": [
                    {
                        "name": "Reachability",
                        "values": [
                            "Publicly Invocable"
                        ]
                    }
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
                },
                "observables": [
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
                    }
                ],
                "type": "Finding",
```

```
                "title":  "Lambda function policies should prohibit public access",
                "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
            },
            {
                "tags": [
                    {
                        "name": "Misconfiguration",
                        "values": [
                            "Deployed outside VPC"
                        ]
                    }
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
                },
                "observables": [
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
                    }
                ],
                "type": "Finding",
                "title": "Lambda functions should be in a VPC",
                "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.3/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            }
        ],
        "title": "Publicly invocable Lambda function executed outside of VPC has
 vulnerability with known exploit that can be exploited from remote network",
        "types": [
            "Exposure/Potential Impact/Resource Hijacking"
        ],
        "uid": "arn:aws:securityhub:us-
east-1:123456789012:risk:1234f781c7ae7507f01e2fb460f15ca8fe7f9c95e257698a092cb74a4ea84a42"
    },
    "metadata": {
        "product": {
            "name": "Security Hub Exposure Analysis",
            "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub-risk",
            "vendor_name": "Amazon"
        },
```

```
        "processed_time_dt": "2024-11-15T21:39:58.819Z",
        "profiles": [
            "cloud",
            "datetime"
        ],
        "version": "1.4.0-dev"
    },
    "resources": [
        {
            "cloud_partition": "aws",
            "region": "us-east-1",
            "tags": [
                {
                    "name": "aws:cloudformation:stack-name",
                    "value": "VeepLambdaRule3"
                },
                {
                    "name": "aws:cloudformation:stack-id",
                    "value": "arn:aws:cloudformation:us-east-1:123456789012:stack/
VeepLambdaRule3/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
                },
                {
                    "name": "aws:cloudformation:logical-id",
                    "value": "lambdar3function94D10D40"
                }
            ],
            "type": "AwsLambdaFunction",
            "uid": "arn:aws:lambda:us-east-1:123456789012:application-function"
        }
    ],
    "severity": "Critical",
    "severity_id": 5,
    "status": "New",
    "status_id": 1,
    "time": 1731706766337,
    "time_dt": "2024-11-15T21:39:26.337224100Z",
    "type_name": "Detection Finding: Create",
    "type_uid": 200401,
    "vendor_attributes": {
        "severity_id": 5,
        "severity": "Critical"
    }
}
```

露出検出結果の重要度レベルの決定

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

Security Hub は、各露出検出結果にデフォルトの重要度 `CRITICAL`、`HIGH`、、`MEDIUM`または を割り当てます`LOW`。重要度が の露出検出`INFORMATIONAL`結果は公開されません。Security Hub は、いくつかの要因を使用して、露出検出結果のデフォルトの重要度レベルを決定します。

- 認識 — 露出が理論的ではなく、公開されている、または自動化されたエクスプロイトがある程度。これは、EC2 インスタンスと Lambda 関数の公開結果に適用されます。
- 検出の容易さ – ポートスキャンやインターネット検索などの自動ツールが、リスクのあるリソースを検出できるかどうか。
- 悪用の容易さ – 脅威アクターが公開を悪用できる容易さ。たとえば、オープンなネットワークパスや誤って設定されたメタデータが存在する場合、脅威アクターはより簡単に公開を悪用できます。
- エクスプロイトの可能性 – 今後 30 日間にエクスポージャーが悪用される可能性。この要素は、Exploit Protection Scoring System (EPSS) に対応し、Amazon EC2 インスタンスと Lambda 関数の公開結果に適用されます。
- 影響 — エクスプロイトが実行された場合の損害。たとえば、公開すると、説明責任の喪失、可用性の喪失、データ公開による機密性の喪失、データ破損による整合性の喪失につながる可能性があります。

露出の検出結果の確認

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

AWS Security Hub コンソールと API を使用して、すべての公開結果を確認できます。Security Hub コンソールの「露出」ページには、アクティブな露出の検出結果がすべて表示されます。露出の検出結果は重要度を下げて一覧表示されます。フィルターの追加検索バーを使用してフィルターを追加および削除することで、露出の検出結果をフィルタリングできます。露出の検出結果を Group by

ドロップダウンでグループ化できます。クイックフィルターメニューを使用して、露出の検出結果をフィルタリングすることもできます。

露出検出結果の詳細

露出検出結果の多くの詳細を表示できます。Security Hub コンソールでは、これらの詳細はタブに分割されます。概要タブには、露出検出結果のスナップショットが表示されます。特性タブには、露出検出結果に関連する特性とシグナルが一覧表示されます。リソースタブには、公開結果に関連付けられたリソースとリソースタグの詳細が表示されます。次のリストでは、露出検出結果の詳細について説明します。

- 検出結果のタイトル — 露出検出結果のタイトル。
- 重要度レベル – 露出検出結果の重要度レベル。Security Hub は、リソースの特性の数と組み合わせを使用して、露出検出結果の重要度レベルを決定します。重要度レベルは、`CRITICAL`、`HIGH`、`MEDIUM`、または ですLOW。Security Hub は、重要度が の公開結果を発行しませんINFORMATIONAL。は、`Severity`Security Hub コンソールまたは BatchUpdateFindingsV2 API オペレーションを使用して更新できます。
- 説明 – 露出の検出結果の説明。
- Type – 露出検出結果タイプの名前。たとえば、名前は のようになりますExposure/Potential Impact/Resource Hijacking。
- アカウント – 露出の検出結果が生成された AWS アカウント の ID。
- Age – 露出検出結果がアクティブであった期間を示します。
- 作成日時 – 露出検出結果が作成された日時を示すタイムスタンプ。
- 変更された時間 – 露出の検出結果が最後に更新された日時を示すタイムスタンプ。
- リージョン – 露出検出結果が生成された AWS リージョン 場所。
- 製品名 – 露出結果を生成した製品の名前。
- 会社名 – 公開結果を生成した会社名。
- アクティビティ名 – アクティビティの名前。
- Status – この露出検出結果のステータス。
- 検出結果 ID – 露出検出結果に関連付けられた一意の識別子。
- 潜在的な攻撃経路 (コンソールのみ) – インタラクティブな視覚化は、潜在的な攻撃者が公開結果に関連するリソースにアクセスして制御する方法を示しています。詳細については、潜在的な攻撃パスグラフを使用して Security Hub で公開情報を表示するを参照してください。

- 特性 – 露出検出結果に関連する特性タイプと特性タイトルを識別します。Security Hub コンソールでは、特性タイプまたはシグナル別に特性を表示できます。これにより、関連する公開のコンテキストで寄与した検出結果を分析できます。
- リソース – 露出検出結果に関連付けられたリソースを識別します。

露出検出結果の詳細の確認

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

このトピックでは、Security Hub コンソールと API で公開結果の詳細を確認する方法について説明します。

Security Hub コンソールでの公開結果の詳細の確認

Security Hub コンソールで公開結果の詳細を表示するには

1. 認証情報を使用してサインインし、https://console.aws.amazon.com/securityhub/v2/home?region=us-east-1 で Security Hub コンソールを開きます。
2. ナビゲーションペインから、露出を選択します。
3. 詳細を表示する露出検出結果を選択します。

API を使用した露出検出結果の詳細の確認

`GetFindingsV2` API または を使用して、露出の検出結果を確認できます AWS CLI。EC2 インスタンスの露出結果のみを返す`Exposure/EC2`場合は、 `FindingProviderFieldsTypes`パラメータと のフィルター値を指定して結果をフィルタリングできます。他のフィールドでフィルタリングして結果を絞り込むことができます。

コマンドの例

以下は、アカウントで最近生成された 10 件の公開結果を取得する AWS CLI 例です。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
aws securityhub get-findings-v2 \
                    --max-results '10' \
```

```
                    --filter '{"CompositeFilters": [{"StringFilters":
[{"FieldName":"finding_info.title","Filter":
{"Value":"GuardDuty","Comparison":"PREFIX"}} ]}]}'
```

露出の検出結果の修正

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

このセクションのトピックでは、さまざまな の修復リスクについて説明します AWS のサービス。

OCSF 形式の `Remediation`フィールドには、 `remediation`と の 2 つのフィールドが含まれます`references`。 https://docs.aws.amazon.com/securityhub/latest/userguide/security-hub-v2-ocsf-findings.html

```
"Remediation": {
     "Recommendation": {
      "remediation":{"desc":"String",
      "references":["string array"]}
     }
},
```

> **Note**
>
> 以下のセクションで提供される修復ガイダンスでは、他の AWS リソースで追加の相談が必要になる場合があります。

DynamoDB テーブルの露出の修正

AWS Security Hub は、DynamoDB テーブルの公開結果を生成できます。

Security Hub コンソールでは、公開結果に関連する DynamoDB テーブルとその識別情報が、結果の詳細のリソースセクションに一覧表示されます。プログラムにより、Security Hub API の GetFindingsV2オペレーションを使用してリソースの詳細を取得できます。

露出検出結果に関連するリソースを特定したら、不要なリソースを削除できます。不要なリソースを削除すると、露出プロファイルと AWS コストを削減できます。リソースが不可欠な場合は、以下の

推奨される修復手順に従ってリスクを軽減します。修復トピックは、特性のタイプに基づいて分割されます。

1 つの公開結果には、複数の修復トピックで特定された問題が含まれます。逆に、1 つの修復トピックだけに対処することで、露出の検出結果に対処し、その重要度レベルを下げることができます。リスク修復へのアプローチは、組織の要件とワークロードによって異なります。

> **Note**
>
> このトピックで提供される修復ガイダンスでは、他の AWS リソースで追加の相談が必要になる場合があります。

目次

- DynamoDB の設定ミス特性
  - DynamoDB テーブルでpoint-in-timeリカバリが無効になっている
  - DynamoDB テーブルはバックアッププランの対象ではありません
  - DynamoDB テーブルの削除保護が無効になっている

DynamoDB の設定ミス特性

DynamoDB テーブルの設定ミスの特性と修復手順について説明します。

DynamoDB テーブルでpoint-in-timeリカバリが無効になっている

DynamoDB point-in-timeリカバリを有効にする

DynamoDB point-in-timeリカバリは、DynamoDB テーブルデータの継続的な自動バックアップを提供します。DynamoDB テーブルを特定の時点に復元する方法については、「Amazon DynamoDB ユーザーガイド」の「DynamoDB テーブルを特定の時点に復元する」を参照してください。DynamoDB

DynamoDB テーブルはバックアッププランの対象ではありません

AWS Backup は、DynamoDB を含むサービス間でバックアップを設定、管理、自動化するための一元化された AWS サービスを提供します。バックアッププランがない場合、テーブルにはカスタマイズ可能な保持期間を持つスケジュールされた自動バックアップがないため、重大なセキュリティリスクが発生します。攻撃者は、テーブルデータを悪意のある方法で破損または削除する可能性があります。適切なバックアップがないと、Point-in-Timeリカバリウィンドウ (有効になっている場合) を超

えるリカバリオプションがないため、永続的なデータ損失が発生する可能性があります。データ保護のベストプラクティスに従って、DynamoDB テーブルをバックアッププランでカバーすることをお勧めします。

バックアッププランの作成

バックアッププランを作成する前に、データの適切なバックアップ頻度と保持期間を決定します。バックアッププランの作成方法については、「Amazon DynamoDB ユーザーガイド」の「バックアッププランにリソースを割り当てる」を参照してください。

DynamoDB テーブルの削除保護が無効になっている

削除保護により、DynamoDB テーブルが誤って削除されるのを防ぎます。削除保護を無効にすると、DynamoDB テーブルはコンソールアクション、API コール、CLI コマンド、または自動プロセスによる意図しない削除に対して脆弱になります。これにより、 AWS 環境にアクセスできる権限のないエンティティがテーブルを意図的に削除し、サービスの中断や永続的なデータ損失が発生する可能性があるため、 AWS 環境がデータ損失にさらされる可能性があります。データ保護のベストプラクティスに従って、DynamoDB テーブルのデータ保護を有効にすることをお勧めします。

削除保護の有効化

複数のテーブルを管理する場合は、 を使用してテーブルプロパティ AWS CloudFormation を一括で更新することを検討してください。 AWS CloudFormation テンプレートを変更して `DeletionProtectionEnabled`プロパティを含めたり、スタックを更新したりできます。修復が完了したら、テーブル設定タブの追加情報ドロップダウンで削除保護が有効になっていることを確認します。

EC2 インスタンスの露出の修正

AWS Security Hub は、Amazon Elastic Compute Cloud (EC2) インスタンスの公開結果を生成できます。

Security Hub コンソールでは、公開結果に関連する EC2 インスタンスとその識別情報が、検出結果の詳細のリソースセクションに一覧表示されます。プログラムでは、Security Hub API の GetFindingsV2オペレーションを使用してリソースの詳細を取得できます。

露出検出結果に関連するリソースを特定したら、不要なリソースを削除できます。不要なリソースを削除すると、露出プロファイルと AWS コストを削減できます。リソースが不可欠な場合は、以下の推奨される修復手順に従ってリスクを軽減します。修復トピックは、特性のタイプに基づいて分割されます。

1 つの公開結果には、複数の修復トピックで特定された問題が含まれます。逆に、1 つの修復トピックだけに対処することで、露出の検出結果に対処し、その重要度レベルを下げることができます。リスク修復へのアプローチは、組織の要件とワークロードによって異なります。

> **Note**
>
> このトピックで提供される修復ガイダンスでは、他の AWS リソースで追加の相談が必要になる場合があります。

目次

- EC2 インスタンスの設定ミス特性
  - EC2 インスタンスは、バージョン 1 を使用して IMDS へのアクセスを許可します
  - Amazon EC2 インスタンスに関連付けられた IAM ロールには管理アクセスポリシーがあります
  - Amazon EC2 インスタンスに関連付けられた IAM ロールにはサービス管理者ポリシーがあります
  - Amazon EC2 インスタンスに、SSH または RDP アクセスを許可するセキュリティグループまたはネットワーク ACL がある
  - Amazon EC2 インスタンスにオープンセキュリティグループがある
  - Amazon EC2 インスタンスにパブリック IP アドレスがある
- EC2 インスタンスの到達可能性特性
  - EC2 インスタンスにはインターネット経由でアクセスできます。
  - Amazon EC2 インスタンスは Amazon VPC 内で到達可能
- EC2 インスタンスの脆弱性特性
  - EC2 インスタンスには、悪用の可能性が高いネットワークで悪用可能なソフトウェアの脆弱性があります
  - Amazon EC2 インスタンスにソフトウェアの脆弱性がある

EC2 インスタンスの設定ミス特性

EC2 インスタンスの設定ミスの特徴と推奨される修復手順は次のとおりです。

EC2 インスタンスは、バージョン 1 を使用して IMDS へのアクセスを許可します

インスタンスメタデータは、実行中のインスタンスを設定または管理するためにアプリケーションが使用できる Amazon EC2 インスタンスに関するデータです。インスタンスメタデータサービス

(IMDS) は、インスタンス上のコードによって、インスタンスメタデータに安全にアクセスするために使用されるインスタンス上のコンポーネントです。IMDS が適切に保護されていない場合、一時的な認証情報やその他の機密設定データにアクセスできるため、潜在的な攻撃ベクトルになる可能性があります。IMDSv2 は、セッション指向認証による悪用に対する保護を強化し、メタデータリクエストにセッショントークンを必要とし、セッション期間を制限します。標準のセキュリティ原則に従って、 では、IMDSv2 を使用し、IMDSv1 を無効にするように Amazon EC2 インスタンスを設定する AWS ことをお勧めします。 IMDSv2 IMDSv1

アプリケーションの互換性をテストする

IMDSv2 を実装する前に、インスタンスをテストして IMDSv2 との互換性を確認します。一部のアプリケーションまたはスクリプトでは、コア機能に IMDSv1 が必要で、追加の設定が必要になる場合があります。アプリケーションの互換性をテストするためのツールと推奨パスの詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の「インスタンスメタデータサービスバージョン 2 の使用への移行」を参照してください。

IMDSv2 を使用するようにインスタンスを更新する

IMDSv2 を使用するように既存のインスタンスを変更します。詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の「既存のインスタンスのインスタンスメタデータオプションを変更する」を参照してください。

Auto Scaling グループのインスタンスに更新を適用する

インスタンスが Auto Scaling グループの一部である場合は、起動テンプレートまたは起動設定を新しい設定で更新し、インスタンスの更新を実行します。

Amazon EC2 インスタンスに関連付けられた IAM ロールには管理アクセスポリシーがあります

管理アクセスポリシーは、Amazon EC2 インスタンスに AWS のサービス および リソースへの広範なアクセス許可を提供します。これらのポリシーには通常、インスタンス機能に必要のないアクセス許可が含まれます。Amazon EC2 インスタンスで (インスタンスプロファイルにアタッチされたロールが必要とする最小限のアクセス許可のセットではなく) IAM アイデンティティに管理アクセスポリシーを提供することで、Amazon EC2 インスタンスが侵害された場合に攻撃の範囲を広げることができます。インスタンスが侵害された場合、攻撃者はこれらの過剰なアクセス許可を利用して、環境を横切って移動したり、データにアクセスしたり、リソースを操作したりする可能性があります。標準のセキュリティ原則に従って、最小権限を付与することをお勧めします。つまり、タスクの実行に必要なアクセス許可のみを付与します。

管理ポリシーの確認と識別

IAM ダッシュボードで、ロール名を持つロールを見つけます。IAM ロールにアタッチされているアクセス許可ポリシーを確認します。ポリシーが AWS マネージドポリシーの場合は、`AdministratorAccess`または を探します`IAMFullAccess`。それ以外の場合は、ポリシードキュメントで、`"Effect": "Allow", "Action": "*"`、、および を含むステートメントを探します`"Resource": "*"`。

最小特権アクセスの実装

管理ポリシーを、インスタンスが機能するために必要な特定のアクセス許可のみを付与するポリシーに置き換えます。IAM ロールのセキュリティのベストプラクティスの詳細については、AWS Identity and Access Management 「 ユーザーガイド」の「セキュリティのベストプラクティス」の「最小特権のアクセス許可を適用する」を参照してください。不要なアクセス許可を特定するには、IAM Access Analyzer を使用して、アクセス履歴に基づいてポリシーを変更する方法を理解します。詳細については、「 AWS Identity and Access Management ユーザーガイド」の「外部アクセスと未使用のアクセスの検出結果」を参照してください。または、新しい IAM ロールを作成して、既存のロールを使用して他のアプリケーションに影響を与えないようにすることもできます。このシナリオでは、新しい IAM ロールを作成し、新しい IAM ロールをインスタンスに関連付けます。インスタンスの IAM ロールを置き換える手順については、「Amazon Elastic Compute Cloud ユーザーガイド」の「インスタンスに IAM ロールをアタッチする」を参照してください。

安全な設定に関する考慮事項

インスタンスにサービスレベルの管理権限が必要な場合は、リスクを軽減するためにこれらの追加のセキュリティコントロールを実装することを検討してください。

- 安全な設定に関する考慮事項
  - 多要素認証 (MFA) – MFA は、追加の形式の認証を要求することで、セキュリティレイヤーを追加します。これにより、認証情報が侵害された場合でも、不正アクセスを防ぐことができます。詳細については、AWS Identity and Access Management 「 ユーザーガイド」の「多要素認証 (MFA) を要求する」を参照してください。
  - IAM 条件 – 条件要素を設定すると、ソース IP や MFA の経過時間などの要因に基づいて、管理アクセス許可をいつ、どのように使用できるかを制限できます。詳細については、「 AWS Identity and Access Management ユーザーガイド」の「IAM ポリシーの条件を使用してアクセスをさらに制限する」を参照してください。
  - アクセス許可の境界 — アクセス許可の境界は、ロールが持つことができる最大アクセス許可を確立し、管理アクセスを持つロールのガードレールを提供します。詳細については、「 ユー

ザーガイド」の「アクセス許可の境界を使用してアカウント内のアクセス許可管理を委任する」を参照してください。 AWS Identity and Access Management

自動スケーリンググループのインスタンスに更新を適用する

AWS 自動スケーリンググループの Amazon EC2 インスタンスの場合、新しいインスタンスプロファイルを使用して起動テンプレートまたは起動設定を更新し、インスタンスの更新を実行します。起動テンプレートの更新の詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の「起動テンプレートの変更 (起動テンプレートのバージョンの管理)」を参照してください。詳細については、「インスタンスの更新を使用して Auto Scaling グループのインスタンスを更新する」を参照してください。Auto Scaling グループで IAM ロールを使用する方法の詳細については、Amazon EC2 Auto Scaling ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションの IAM ロールAuto Scaling Amazon EC2」を参照してください。

Amazon EC2 インスタンスに関連付けられた IAM ロールにはサービス管理者ポリシーがあります

サービスアクセスポリシーは、Amazon EC2 インスタンスに AWS サービスとリソースへの広範なアクセス許可を提供します。これらのポリシーには通常、インスタンス機能に必要のないアクセス許可が含まれます。インスタンスプロファイルにアタッチされたロールが必要とする最小限のアクセス許可セットではなく、IAM ID に Amazon EC2 インスタンスの管理アクセスポリシーを提供することで、インスタンスが侵害された場合に攻撃の範囲を広げることができます。標準のセキュリティ原則に従って、最小権限を付与することをお勧めします。つまり、タスクの実行に必要なアクセス許可のみを付与します。

管理ポリシーの確認と識別

IAM ダッシュボードで、ロール名を持つロールを見つけます。IAM ロールにアタッチされているアクセス許可ポリシーを確認します。ポリシーが AWS マネージドポリシーの場合は、`AdministratorAccess`または を探します`IAMFullAccess`。それ以外の場合は、ポリシードキュメントで、`"Effect": "Allow", "Action": "*"`、、および を含むステートメントを探します`"Resource": "*"`。

最小特権アクセスの実装

サービス管理者ポリシーを、インスタンスが機能するために必要な特定のアクセス許可のみを付与するポリシーに置き換えます。IAM ロールのセキュリティのベストプラクティスの詳細については、AWS Identity and Access Management 「 ユーザーガイド」の「セキュリティのベストプラクティス」の「最小特権のアクセス許可を適用する」を参照してください。不要なアクセス許可を特定するには、IAM Access Analyzer を使用して、アクセス履歴に基づいてポリシーを変更する方法を

理解します。詳細については、「 AWS Identity and Access Management ユーザーガイド」の「外部アクセスと未使用のアクセスの検出結果」を参照してください。または、新しい IAM ロールを作成して、既存のロールを使用している他のアプリケーションに影響を与えないようにすることもできます。このシナリオでは、新しい IAM ロールを作成し、新しい IAM ロールをインスタンスに関連付けます。インスタンスの IAM ロールの置き換えについては、「Amazon Elastic Compute Cloud ユーザーガイド」の「インスタンスに IAM ロールをアタッチする」を参照してください。

安全な設定に関する考慮事項

インスタンスにサービスレベルの管理権限が必要な場合は、リスクを軽減するためにこれらの追加のセキュリティコントロールを実装することを検討してください。

安全な設定に関する考慮事項

インスタンスにサービスレベルの管理権限が必要な場合は、リスクを軽減するためにこれらの追加のセキュリティコントロールを実装することを検討してください。

- 多要素認証 (MFA) – MFA は、追加の形式の認証を要求することで、セキュリティレイヤーを追加します。これにより、認証情報が侵害された場合でも、不正アクセスを防ぐことができます。詳細については、「 AWS Identity and Access Management ユーザーガイド」の「多要素認証 (MFA) を要求する」を参照してください。
- IAM 条件 – 条件要素を設定すると、ソース IP や MFA の経過時間などの要因に基づいて、管理アクセス許可をいつ、どのように使用できるかを制限できます。詳細については、「 AWS Identity and Access Management ユーザーガイド」の「IAM ポリシーの条件を使用してアクセスをさらに制限する」を参照してください。
- アクセス許可の境界 – アクセス許可の境界は、ロールが持つことができる最大アクセス許可を確立し、管理アクセスを持つロールのガードレールを提供します。詳細については、「 ユーザーガイド」の「アクセス許可の境界を使用してアカウント内のアクセス許可管理を委任する」を参照してください。 AWS Identity and Access Management

Auto Scaling グループのインスタンスに更新を適用する

AWS 自動スケーリンググループの Amazon EC2 インスタンスの場合、新しいインスタンスプロファイルを使用して起動テンプレートまたは起動設定を更新し、インスタンスの更新を実行します。起動テンプレートの更新については、「Amazon Elastic Compute Cloud ユーザーガイド」の「起動テンプレートの変更 (起動テンプレートのバージョンの管理) 」を参照してください。詳細については、「インスタンスの更新を使用して Auto Scaling グループのインスタンスを更新する」を参照してください。Auto Scaling グループで IAM ロールを使用する方法の詳細については、Amazon EC2

Auto Scaling ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションの IAM ロールAuto Scaling Amazon EC2」を参照してください。

Amazon EC2 インスタンスに、SSH または RDP アクセスを許可するセキュリティグループまたはネットワーク ACL がある

SSH や RDP などのリモートアクセスプロトコルを使用すると、ユーザーは外部の場所から Amazon EC2 インスタンスに接続および管理できます。セキュリティグループがインターネットからのこれらのプロトコルへの無制限アクセスを許可すると、インスタンスへのインターネットアクセスを許可することで、Amazon EC2 インスタンスのアタックサーフェスが増加します。標準のセキュリティ原則に従って、 では、リモートアクセスを信頼できる特定の IP アドレスまたは範囲に制限 AWS することをお勧めします。

1. セキュリティグループルールを変更する

   Amazon EC2 インスタンスへのアクセスを特定の信頼された IP アドレスに制限します。SSH および RDP アクセスを特定の信頼できる IP アドレスに制限するか、CIDR 表記を使用して IP 範囲 (198.168.1.0/24 など) を指定します。セキュリティグループルールを変更するには、「Amazon Elastic Compute Cloud ユーザーガイド」の「セキュリティグループルールの設定」を参照してください。

Amazon EC2 インスタンスにオープンセキュリティグループがある

セキュリティグループはAmazon EC2 インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックを制御します。任意の IP アドレスからの無制限のアクセスを許可するオープンセキュリティグループは、インスタンスを不正アクセスにさらす可能性があります。標準のセキュリティ原則に従って、 はセキュリティグループアクセスを特定の IP アドレスとポートに制限 AWS することをお勧めします。

セキュリティグループのルールを確認し、現在の設定を評価する

などの幅広い IP 範囲からオープンおよびアクセス可能なポートを評価します(`0.0.0.0/0 or ::/0`)。セキュリティグループの詳細を表示する手順については、「Porting Assistant for .NET API Reference」の「DescribeSecurityGroups」を参照してください。

セキュリティグループルールを変更する

セキュリティグループのルールを変更して、特定の信頼された IP アドレスまたは範囲へのアクセスを制限します。セキュリティグループルールを更新するときは、必要なソース IP 範囲ごとにルー

ルを作成するか、特定のポートへのアクセスを制限することで、異なるネットワークセグメントのアクセス要件を分離することを検討してください。セキュリティグループルールを変更するには、Amazon EC2 ユーザーガイド」の「セキュリティグループルールの設定」を参照してください。

Amazon EC2 インスタンスにパブリック IP アドレスがある

パブリック IP アドレスを持つ Amazon EC2 インスタンスは、インターネットからパブリックにアクセスできます。外部顧客にサービスを提供するインスタンスにはパブリック IP アドレスが必要になる場合がありますが、これは不正なプリンシパルを攻撃することで潜在的なものとして使用できます。は、標準のセキュリティ原則に従って、可能な場合はリソースの公開を制限することを AWS 推奨しています。

インスタンスをプライベートサブネットに移動する

インスタンスが直接インターネットアクセスを必要としない場合は、VPC 内のプライベートサブネットに移動することを検討してください。これにより、パブリック IP アドレスが削除され、VPC 内の他のリソースと通信できるようになります。詳細については、 AWS ナレッジセンターのAmazon EC2 インスタンスを別のサブネット、アベイラビリティーゾーン、または VPC に移動するにはどうすればよいですか？」を参照してください。

パブリック IP アドレスなしで起動するようにインスタンスを設定する

インスタンスがパブリック IP アドレスを必要としないパブリックサブネットで起動された場合、パブリック IP アドレスの自動割り当てを防ぐために起動設定を変更できます。これは、サブネットレベルまたは個々のインスタンスを起動するときに無効にできます。詳細については、Amazon Virtual Private Cloud ユーザーガイド」の「サブネットの IP アドレス属性の変更」および「Amazon Elastic Compute Cloud ユーザーガイド」の「Amazon EC2instance IP アドレス指定」を参照してください。

代替アクセス方法

代替アクセス方法には、次のオプションを検討してください。

- アウトバウンドインターネット接続に NAT ゲートウェイを使用する –

  インターネットへのアクセス (更新のダウンロードなど) を必要とするプライベートサブネット内のインスタンスの場合、パブリック IP アドレスを割り当てる代わりに NAT ゲートウェイを使用することを検討してください。NAT Gateway を使用すると、プライベートサブネットのインスタンスは、インターネットからのインバウンド接続を防止しながら、インターネットへのアウトバウ

ンド接続を開始できます。詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「NAT ゲートウェイ」を参照してください。 Amazon Virtual Private Cloud

- Elastic Load Balancing を使用する – ウェブアプリケーションを実行しているインスタンスの場合は、Elastic Load Balancer (LB) の使用を検討してください。LBs は、LB がパブリックサブネットで実行され、インターネットトラフィックを処理する間に、インスタンスがプライベートサブネットで実行されるように設定できます。詳細については、ELB ユーザーガイドのElastic Load Balancing AWSとは」を参照してください。LB の維持戦略を選択する方法については、「規範ガイダンス」の「ロードバランサーサブネット」を参照してください。 AWS

EC2 インスタンスの到達可能性特性

EC2 インスタンスの到達可能性特性と推奨される修復手順は次のとおりです。

EC2 インスタンスにはインターネット経由でアクセスできます。

インターネットゲートウェイ (Application Load Balancer または Classic Load Balancer の背後にあるインスタンスを含む) 、VPC ピアリング接続、または VPN 仮想ゲートウェイを介してインターネットから到達可能なポートを持つ Amazon EC2 インスタンスは、インスタンスをインターネットに公開することがあります。標準のセキュリティ原則に従い、インバウンドトラフィックを必要なソースとポートのみに制限して、最小特権のネットワークアクセスコントロールを実装することをお勧めします。

セキュリティグループルールの変更または削除

リソースタブで、Amazon EC2 セキュリティグループのリソースを開きます。インスタンスが機能するためにインターネットアクセスが必要かどうかを確認します。無制限のアクセスを許可するインバウンドセキュリティグループルールを変更または削除します (`0.0.0.0/0` または `::/0`) 。特定の IP 範囲またはセキュリティグループに基づいて、より制限の厳しいルールを実装します。制限されたパブリックアクセスが必要な場合は、インスタンスの 関数に必要な特定のポートとプロトコルへのアクセスを制限します。セキュリティグループルールを管理する手順については、Amazon EC2 ユーザーガイド」の「セキュリティグループルールの設定」を参照してください。

ネットワーク ACLs を更新する

インスタンスのサブネットに関連付けられたネットワークアクセスコントロールリスト (ACLs) を確認して変更します。ACL 設定がセキュリティグループの変更と一致しており、意図せずにパブリックアクセスを許可していないことを確認します。ネットワーク ACLs「Amazon VPC ユーザーガイド」の「ネットワーク ACLs」を参照してください。

代替アクセス方法

代替アクセス方法には、次のオプションを検討してください。

- アウトバウンドインターネット接続に NAT Gateway を使用する – インターネットへのアクセスを必要とする (更新をダウンロードするなど) プライベートサブネット内のインスタンスの場合、パブリック IP アドレスを割り当てる代わりに NAT Gateway を使用することを検討してください。NAT Gateway を使用すると、プライベートサブネットのインスタンスはインターネットからのインバウンド接続を防止しながら、インターネットへのアウトバウンド接続を開始できます。
- Systems Manager Session Manager を使用する – Session Manager は、インバウンドポート、SSH キーの管理、踏み台ホストの維持を必要とせずに、Amazon EC2 インスタンスへの安全なシェルアクセスを提供します。
- WAF と Elastic Load Balancing または Application Load Balancer を使用する – ウェブアプリケーションを実行しているインスタンスの場合は、LB を AWS ウェブアプリケーションファイアウォール (WAF) と組み合わせて使用することを検討してください。LBs は、LB がパブリックサブネットで実行され、インターネットトラフィックを処理する間に、インスタンスがプライベートサブネットで実行されるように設定できます。WAF をロードバランサーに追加すると、ウェブエクスプロイトやボットに対する保護を強化できます。

Amazon EC2 インスタンスは Amazon VPC 内で到達可能

Amazon Virtual Private Cloud (Amazon VPC) を使用すると、定義された仮想ネットワークで AWS リソースを起動できます。インスタンス間の無制限のアクセスを許可する Amazon VPC ネットワーク設定は、インスタンスが侵害された場合に攻撃の範囲を広げる可能性があります。セキュリティのベストプラクティスに従って、 はサブネットおよびセキュリティグループレベルでのネットワークセグメンテーションと最小特権のアクセスコントロールの実装 AWS を推奨します。

Amazon VPC ネットワーク接続パターンを確認する

公開結果で、ARN のセキュリティグループ ID を特定します。相互に通信する必要があるインスタンスとポートを特定します。Amazon VPC フローログを使用して Amazon VPC 内の既存のトラフィックパターンを分析し、使用されているポートを特定できます。

セキュリティグループルールを変更する

セキュリティグループのルールを変更して、特定の信頼された IP アドレスまたは範囲へのアクセスを制限します。たとえば、VPC CIDR 範囲全体 (10.0.0.0/16 など) からのすべてのトラフィックを許可する代わりに、特定のセキュリティグループまたは IP 範囲へのアクセスを制限します。セキュ

リティグループルールを更新するときは、必要なソース IP 範囲ごとにルールを作成するか、特定のポートへのアクセスを制限することで、異なるネットワークセグメントのアクセス要件を分離することを検討してください。セキュリティグループルールを変更するには、「Amazon EC2Userユーザーガイド」の「セキュリティグループルールの設定」を参照してください。

セキュリティ要件または機能に基づいて Amazon VPC リソースをサブネットに整理することを検討してください。たとえば、ウェブサーバーとデータベースサーバーを別々のサブネットに配置します。詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「VPC のサブネット」を参照してください。 Amazon Virtual Private Cloud

サブネットレベルの保護用にネットワーク ACLs を設定する

ネットワークアクセスコントロールリスト (NACLsは、サブネットレベルで追加のセキュリティレイヤーを提供します。セキュリティグループとは異なり、NACLs はステートレスであり、インバウンドルールとアウトバウンドルールの両方を明示的に定義する必要があります。詳細については、Amazon Virtual Private Cloud ユーザーガイド」の「ネットワークアクセスコントロールリストを使用してサブネットトラフィックを制御する」を参照してください。

その他の考慮事項

Amazon VPC へのアクセスを制限するときは、次の点を考慮してください。

- 制限付きルーティングによる Transit Gateway または Amazon VPC ピアリング – アーキテクチャで通信する必要がある複数の VPCs を使用している場合は、 AWS Transit Gateway と Amazon VPC ピアリングを使用して Amazon VPCs 間の接続を提供しながら、どのサブネットが相互に通信できるかを制御できるようにすることを検討してください。詳細については、「Amazon VPC Transit Gateway と VPC ピアリング接続の使用を開始する」を参照してください。 https://docs.aws.amazon.com/vpc/latest/peering/working-with-vpc-peering.html
- サービスエンドポイントとプライベートリンク – Amazon VPC エンドポイントを使用して、トラフィックを AWS ネットワーク内に保持し、インターネット経由ではなく AWS リソースと通信できます。これにより、同じサービスにアクセスするインスタンス間の直接接続の必要性が軽減されます。VPC エンドポイントの詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「Amazon VPC エンドポイントとは」を参照してください。 Amazon Virtual Private Cloud 他の Amazon VPCs、 の使用を検討してください AWS PrivateLink。

EC2 インスタンスの脆弱性特性

EC2 インスタンスの脆弱性特性と推奨される修復手順は次のとおりです。

EC2 インスタンスには、悪用の可能性が高いネットワークで悪用可能なソフトウェアの脆弱性があります

EC2 インスタンスにインストールされているソフトウェアパッケージは、共通脆弱性識別子 (CVEs) に公開できます。重要な CVEs AWS 、環境に重大なセキュリティリスクをもたらします。認可されていないプリンシパルは、これらのパッチが適用されていない脆弱性を悪用して、データの機密性、完全性、可用性を侵害したり、他のシステムにアクセスしたりする可能性があります。エクスプロイトコードはすでに公開されており、攻撃者や自動スキャンツールによってアクティブに使用されている可能性があるため、エクスプロイトの可能性の高い重大な脆弱性は即時のセキュリティ脅威を表します。インスタンスを保護するために、これらの脆弱性にパッチを適用することをお勧めします。

影響を受けるインスタンスを更新する

特性の脆弱性タブの「リファレンス」セクションを確認します。ベンダーのドキュメントには、特定の修復ガイダンスが含まれている場合があります。これらの一般的なガイドラインを使用して、適切な修復に従ってください。

Systems Manager Patch Manager を使用して、オペレーティングシステムとアプリケーションの両方にパッチを適用します。Patch Manager は、オペレーティングシステムとソフトウェアパッチを自動的に大規模なインスタンスグループに選択してデプロイするのに役立ちます。Patch Manager を設定していない場合は、影響を受ける各インスタンスのオペレーティングシステムを手動で更新します。

ベンダーの推奨手順に従って、影響を受けるアプリケーションを最新の安全なバージョンに更新します。複数のインスタンスでアプリケーションの更新を管理するには、Systems Manager ステートマネージャーを使用してソフトウェアを一貫した状態に保つことを検討してください。更新が利用できない場合は、パッチがリリースされるか、アプリケーションへのネットワークアクセスの制限や脆弱な機能の無効化などのその他の緩和策が行われるまで、脆弱なアプリケーションを削除または無効化することを検討してください。

Amazon Inspector の検出結果に記載されている特定の修復アドバイスに従ってください。これには、セキュリティグループルールの変更、インスタンス設定の変更、アプリケーション設定の調整が含まれる場合があります。

インスタンスが Auto Scaling グループの一部であるかどうかを確認します。AMI 置換パッチ適用は、Auto Scaling グループに新しい Amazon EC2 インスタンスをデプロイするように設定された AMI ID を更新することで、イミュータブルなインフラストラクチャで行われます。カスタム/ゴールデン AMI を使用している場合は、新しい AMI でインスタンスを作成し、インスタンスをカスタマイズして新しいゴールデン AMI を作成します。詳細については、「AMI の更新パッチ適用 (Auto Scaling グループのパッチ適用された AMIs を使用)」を参照してください。

今後の考慮事項

今後の発生を防ぐには、脆弱性管理プログラムの実装を検討してください。Amazon Inspector は、インスタンスで CVEs を自動的にスキャンするように設定できます。Amazon Inspector は、自動修復のために Security Hub と統合することもできます。Systems Manager メンテナンスウィンドウを使用して定期的なパッチ適用スケジュールを実装し、インスタンスの中断を最小限に抑えることを検討してください。

Amazon EC2 インスタンスにソフトウェアの脆弱性がある

Amazon EC2instancesにインストールされているソフトウェアパッケージは、共通脆弱性識別子 (CVEs) に公開される可能性があります。重要でない CVEsは、重要な CVEs と比較して重要度や悪用可能性が低いセキュリティの弱点を表します。これらの脆弱性は差し迫ったリスクが少なくなりますが、攻撃者はパッチが適用されていないこれらの脆弱性を悪用してデータの機密性、完全性、可用性を侵害したり、他のシステムにアクセスしたりできます。セキュリティのベストプラクティスに従って、 は、インスタンスを攻撃から保護するために、これらの脆弱性にパッチを適用 AWSすることをお勧めします。

影響を受けるインスタンスを更新する

AWS Systems Manager Patch Manager を使用して、オペレーティングシステムにパッチを適用します。Patch Manager は、オペレーティングシステムとソフトウェアパッチを自動的に選択して大規模なインスタンスグループにデプロイするのに役立ちます。Patch Manager を設定していない場合は、影響を受ける各インスタンスのオペレーティングシステムを手動で更新します。

ベンダーの推奨手順に従って、影響を受けるアプリケーションを最新の安全なバージョンに更新します。複数のインスタンスでアプリケーションの更新を管理するには、 AWS Systems Manager ステートマネージャーを使用してソフトウェアを一貫した状態に保つことを検討してください。更新が利用できない場合は、パッチがリリースされるか、アプリケーションへのネットワークアクセスの制限や脆弱な機能の無効化などのその他の緩和策が行われるまで、脆弱なアプリケーションを削除または無効化することを検討してください。

Amazon Inspector の検出結果に記載されている特定の修復アドバイスに従ってください。これには、セキュリティグループルールの変更、インスタンス設定の変更、アプリケーション設定の調整が含まれる場合があります。

インスタンスが Auto Scaling グループの一部であるかどうかを確認します。AMI 置換パッチ適用は、Auto Scaling グループに新しい Amazon EC2 インスタンスをデプロイするように設定された AMI ID を更新することで、イミュータブルなインフラストラクチャで行われます。カスタム/ゴー

ルデン AMI を使用している場合は、新しい AMI でインスタンスを作成し、インスタンスをカスタマイズして新しいゴールデン AMI を作成します。詳細については、「AMI の更新パッチ適用 (Auto Scaling グループのパッチ適用された AMIs を使用)」を参照してください。

今後の考慮事項

今後の発生を防ぐには、脆弱性管理プログラムの実装を検討してください。Amazon Inspector は、インスタンスで CVEs を自動的にスキャンするように設定できます。Amazon Inspector は、自動修復のために Security Hub と統合することもできます。Systems Manager メンテナンスウィンドウを使用して定期的なパッチ適用スケジュールを実装し、インスタンスの中断を最小限に抑えることを検討してください。

Amazon ECS サービスの露出の修正

AWS Security Hub は、Amazon Elastic Container Service (Amazon ECS) サービスの公開結果を生成できます。

露出検出結果に関連する Amazon ECS サービスとその識別情報は、検出結果の詳細のリソースセクションに一覧表示されます。これらのリソースの詳細は、Security Hub コンソールで取得することも、Security Hub API の GetFindingsV2オペレーションを使用してプログラムで取得することもできます。

露出検出結果に関連するリソースを特定したら、不要なリソースを削除できます。不要なリソースを削除すると、露出プロファイルと AWS コストを削減できます。リソースが不可欠な場合は、以下の推奨される修復手順に従ってリスクを軽減します。修復トピックは、特性のタイプに基づいて分割されます。

1 つの公開結果には、複数の修復トピックで特定された問題が含まれます。逆に、1 つの修復トピックだけに対処することで、露出の検出結果に対処し、その重要度レベルを下げることができます。リスク修復へのアプローチは、組織の要件とワークロードによって異なります。

> **Note**
>
> このトピックで提供される修復ガイダンスでは、他の AWS リソースで追加の相談が必要になる場合があります。

目次

- Amazon ECS サービスの設定ミスの特性

- Amazon ECS サービスは、昇格された権限で設定されたタスク定義を使用します。
- Amazon ECS サービスには、IAM ロールを引き受けることができるコンテナがあります
- Amazon ECS サービスは、コンテナがルートファイルシステムにアクセスできるようにするタスク定義を使用します。
- Amazon ECS サービスは、ホストのプロセス名前空間を共有するように設定されたタスク定義を使用します。
- Amazon ECS サービスは、環境変数でクリアテキスト認証情報で設定されたタスク定義を使用します。
- Amazon ECS サービスにオープンセキュリティグループがある
- Amazon ECS サービスにパブリック IP アドレスがある
- Amazon ECS サービスは、ホストネットワークモードが有効に設定されたタスク定義を使用します。
- Amazon ECS サービスに関連付けられた IAM ロールには管理アクセスポリシーがあります
- Amazon ECS サービスの脆弱性特性
  - Amazon ECS サービスには、悪用の可能性の高いネットワークで悪用可能なソフトウェアの脆弱性を持つコンテナがあります。
  - Amazon ECS サービスにソフトウェアの脆弱性があるコンテナがある

Amazon ECS サービスの設定ミスの特性

Amazon ECS サービスの設定ミスの特徴と推奨される修復手順は次のとおりです。

Amazon ECS サービスは、昇格された権限で設定されたタスク定義を使用します。

昇格された権限を持つ Amazon ECS コンテナは、ホストシステムと同様の機能を持ち、ホストリソースやその他のコンテナへのアクセスを許可する可能性があります。この設定により、侵害されたコンテナを使用して意図した範囲外のリソースにアクセスまたは変更するリスクが高まり、コンテナのエスケープ、基盤となるホストへの不正アクセス、同じホスト上の他のコンテナに影響を与える違反につながる可能性があります。標準のセキュリティ原則に従って、 AWS は最小権限を付与することをお勧めします。つまり、タスクの実行に必要なアクセス許可のみを付与します。

タスク定義の確認と変更

公開で、タスク定義 ARN を識別します。Amazon ECS コンソールでタスク定義を開きます。タスク定義で、コンテナ定義で true に設定されている特権フラグを探します。特権モードが必要ない場合は、特権フラグなしで新しいタスク定義リビジョンを作成します。特権モードが必要な場合は、不正

な変更を防ぐために読み取り専用ファイルシステムを使用するようにコンテナを設定することを検討してください。

Amazon ECS サービスには、IAM ロールを引き受けることができるコンテナがあります

IAM ロールを使用すると、Amazon ECS タスクは一時的な認証情報を使用して他の AWS サービスに安全にアクセスできます。コンテナが他の AWS リソースとやり取りする必要がある Amazon ECS タスクには、タスク実行ロールが必要になる場合があります。これはコンテナの機能に必要になる場合がありますが、ロールが正しく設定されていないと、コンテナが侵害された場合に攻撃者が悪用する可能性のある過剰な権限が付与され、 AWS リソースへの不正アクセス、データの盗難、インフラストラクチャの不正な変更が許可される可能性があります。標準のセキュリティ原則に従って、 AWS は最小特権アクセスを実装し、Amazon ECS タスクにアタッチされた IAM ロールを確認することをお勧めします。

アタッチされたロールを確認する

IAM ダッシュボードに移動し、識別されたロールを選択します。IAM ロールにアタッチされているアクセス許可ポリシーを確認します。タスクが他の AWS サービスとやり取りする必要がある場合は、タスク実行ロールを保持し、最小特権のアクセス許可の適用を検討してください。それ以外の場合は、実行ロールなしで新しいタスク定義リビジョンを作成します。

Amazon ECS サービスは、コンテナがルートファイルシステムにアクセスできるようにするタスク定義を使用します。

ホストルートファイルシステムにアクセスできる Amazon ECS コンテナは、ホストシステムで重要なファイルを読み取ったり、変更したり、実行したりする可能性があります。この設定により、侵害されたコンテナを使用して意図した範囲外のリソースにアクセスまたは変更し、ホストファイルシステムで機密データを公開するリスクが高まります。標準のセキュリティ原則に従って、 AWS は最小権限を付与することをお勧めします。つまり、タスクの実行に必要なアクセス許可のみを付与します。

ホストファイルシステムアクセスを持つコンテナの確認と変更

公開結果で、タスク定義 ARN を特定します。Amazon ECS コンソールでタスク定義を開きます。ホストパスマッピングを定義するタスク定義のボリュームセクションを探します。タスク定義を確認して、コンテナ機能にホストファイルシステムアクセスが必要かどうかを確認します。 ホストファイルシステムアクセスが必要ない場合は、新しいタスク定義リビジョンを作成し、ホストパスを使用するボリューム定義を削除します。ホストファイルシステムへのアクセスが必要な場合は、不正な変更を防ぐために読み取り専用ファイルシステムを使用するようにコンテナを設定することを検討してください。

Amazon ECS サービスは、ホストのプロセス名前空間を共有するように設定されたタスク定義を使用します。

公開された名前空間で実行されている Amazon ECS コンテナは、ホストシステムリソースやその他のコンテナ名前空間にアクセスする可能性があります。この設定により、侵害されたコンテナが分離境界からエスケープでき、プロセス、ネットワークインターフェイス、または意図した範囲外のその他のリソースにアクセスする可能性があります。プロセス ID (PID) 名前空間は、プロセス間を分離します。これにより、システムプロセスが可視化されることを防ぎ、PID 1 を含む PID の再利用が可能になります。ホストの PID 名前空間がコンテナと共有されている場合、コンテナは、ホストシステム上のすべてのプロセスを参照できるようになります。これにより、ホストとコンテナ間をプロセスレベルで分離するメリットが減ります。これらの要因により、ホスト自体でプロセスを操作して終了する機能など、プロセスへの不正アクセスが発生する可能性があります。は、標準のセキュリティ原則に従って、コンテナに対して適切な名前空間分離を維持する AWS ことを推奨します。

公開された名前空間でタスク定義を更新する

公開のリソースタブを開き、公開された名前空間を持つタスク定義を特定します。Amazon ECS コンソールでタスク定義を開きます。ホストの値を持つ pidMode 設定を探します。これにより、プロセス ID 名前空間がホストと共有されます。タスク定義から pidMode: ホスト設定を削除して、コンテナが適切な名前空間分離で実行されるようにします。

Amazon ECS サービスは、環境変数でクリアテキスト認証情報で設定されたタスク定義を使用します。

環境変数にクリアテキスト認証情報を持つ Amazon ECS コンテナは、攻撃者がタスク定義、コンテナ環境、またはコンテナログにアクセスした場合に侵害される可能性のある機密認証情報を公開します。これにより、漏洩した認証情報が他の AWS サービスやリソースへのアクセスに使用される可能性があるため、重大なセキュリティリスクが発生します。

クリアテキスト認証情報を置き換える

公開結果で、クリアテキスト認証情報を使用してタスク定義を特定します。Amazon ECS コンソールでタスク定義を開きます。 AWS アクセスキー、データベースパスワード、API トークンなどの機密値を含む環境変数をコンテナ定義で探します。

認証情報を渡すには、次の代替方法を検討してください。

- AWS アクセスキーを使用する代わりに、IAM タスク実行ロールとタスクロールを使用して、コンテナにアクセス許可を付与します。
- Secrets Manager に認証情報をシーク AWS レットとして保存し、タスク定義で参照します。

タスク定義の更新

認証情報を安全に処理するタスク定義の新しいリビジョンを作成します。次に、新しいタスク定義リビジョンを使用するように Amazon ECS サービスを更新します。

Amazon ECS サービスにオープンセキュリティグループがある

セキュリティグループは、Amazon ECS タスクの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックを制御します。任意の IP アドレスからの無制限のアクセスを許可するオープンセキュリティグループは、コンテナを不正アクセスにさらし、自動スキャンツールやターゲットを絞った攻撃にさらされるリスクを高める可能性があります。標準のセキュリティ原則に従って、 はセキュリティグループアクセスを特定の IP アドレスとポートに制限 AWS することをお勧めします。

セキュリティグループのルールを確認し、現在の設定を評価する

Amazon ECS セキュリティグループのリソースを開きます。などの幅広い IP 範囲からオープンおよびアクセス可能なポートを評価します(`0.0.0.0/0 or ::/0`)。

セキュリティグループルールを変更する

セキュリティグループのルールを変更して、特定の信頼された IP アドレスまたは範囲へのアクセスを制限します。セキュリティグループルールを更新するときは、必要なソース IP 範囲ごとにルールを作成するか、特定のポートへのアクセスを制限することで、異なるネットワークセグメントのアクセス要件を分離することを検討してください。

セキュリティグループルールを変更する

代替アクセス方法については、次のオプションを検討してください。

- Session Manager は、インバウンドポート、SSH キーの管理、踏み台ホストの維持を必要とせずに、Amazon EC2 インスタンスへの安全なシェルアクセスを提供します。
- NACLsは、サブネットレベルで追加のセキュリティレイヤーを提供します。セキュリティグループとは異なり、NACLs はステートレスであり、インバウンドルールとアウトバウンドルールの両方を明示的に定義する必要があります。

Amazon ECS サービスにパブリック IP アドレスがある

タスクにパブリック IP アドレスが割り当てられている Amazon ECS サービスは、インターネットから直接アクセスできます。これは、公開する必要があるサービスで必要になる場合がありますが、攻撃対象領域が増加し、不正アクセスの可能性が高まります。

パブリック IP アドレスを持つサービスを特定する

公開結果で、タスクにパブリック IP アドレスが割り当てられている Amazon ECS サービスを特定します。サービス`assignPublicIp`設定`ENABLED`で の値を持つ 設定を探します。

タスク定義の更新

パブリック IP アドレスを無効にするタスク定義の新しいリビジョンを作成します。次に、新しいタスク定義リビジョンを使用するように Amazon ECS サービスを更新します。

プライベートネットワークアクセスパターンを実装する

ウェブアプリケーションを実行しているインスタンスの場合は、Load Balancer (LB) の使用を検討してください。LBs は、LB がパブリックサブネットで実行され、インターネットトラフィックを処理する間、インスタンスがプライベートサブネットで実行されるように設定できます。

Amazon ECS サービスは、ホストネットワークモードが有効に設定されたタスク定義を使用します。

ホストネットワークモードで実行されている Amazon ECS コンテナは、ネットワーク名前空間をホストと共有し、ホストのネットワークインターフェイス、ポート、ルーティングテーブルに直接アクセスできるようにします。この設定は、コンテナによって提供されるネットワーク分離をバイパスし、コンテナで実行されているサービスを外部ネットワークに直接公開し、コンテナがホストネットワーク設定を変更できるようにします。は、標準のセキュリティ原則に従って、コンテナの適切なネットワーク分離を維持する AWS ことを推奨します。

ホストネットワークモードを無効にする

公開結果で、ホストネットワーキングモードでタスク定義を特定します。Amazon ECS コンソールでタスク定義を開きます。タスク定義でホストの値を持つ networkMode 設定を探します。

ホストネットワークモードを無効にするには、次のオプションを検討してください。

- `awsvpc` ネットワークモードは、各タスクに独自の Elastic Network Interface を提供することで、最も強力なレベルのネットワーク分離を提供します。
- `bridge` ネットワークモードは、ポートマッピングが特定のコンテナポートをホストに公開できるようにしながら、分離を提供します。

タスク定義の更新

更新されたネットワークモード設定を使用して、タスク定義の新しいリビジョンを作成します。次に、新しいタスク定義リビジョンを使用するように Amazon ECS サービスを更新します。

Amazon ECS サービスに関連付けられた IAM ロールには管理アクセスポリシーがあります

Amazon ECS タスクに管理アクセスポリシーがアタッチされた IAM ロールは、コンテナオペレーションに通常必要な範囲を超える広範なアクセス許可を提供します。この設定により、侵害されたコンテナを使用して AWS 環境全体のリソースにアクセスまたは変更するリスクが高まります。標準のセキュリティ原則に従って、 は、タスクが機能するために必要なアクセス許可のみを付与して、最小特権アクセスを実装 AWS することをお勧めします。

管理ポリシーの確認と識別

リソース ID で、IAM ロール名を指定します。IAM ダッシュボードに移動し、識別されたロールを選択します。IAM ロールにアタッチされているアクセス許可ポリシーを確認します。ポリシーが AWS 管理ポリシーの場合は、 を探します`AdministratorAccess`。それ以外の場合は、ポリシードキュメントで、ステートメントが`"Effect": "Allow", "Action": "*", and "Resource": "*"`一緒にあるステートメントを探します。

最小特権アクセスの実装

管理ポリシーを、インスタンスが機能するために必要な特定のアクセス許可のみを付与するポリシーに置き換えます。不要なアクセス許可を特定するには、IAM Access Analyzer を使用して、アクセス履歴に基づいてポリシーを変更する方法を理解します。または、新しい IAM ロールを作成して、既存のロールを使用している他のアプリケーションに影響を与えないようにすることもできます。このシナリオでは、新しい IAM ロールを作成し、新しい IAM ロールをインスタンスに関連付けます。

安全な設定に関する考慮事項

インスタンスにサービスレベルの管理権限が必要な場合は、リスクを軽減するためにこれらの追加のセキュリティコントロールを実装することを検討してください。

- MFA は、追加の形式の認証を要求することで、セキュリティレイヤーを追加します。これにより、認証情報が侵害された場合でも、不正アクセスを防ぐことができます。
- 条件要素を設定すると、ソース IP や MFA の経過時間などの要因に基づいて、管理アクセス許可をいつ、どのように使用できるかを制限できます。

タスク定義の更新

新規または更新された IAM ロールを参照するタスク定義の新しいリビジョンを作成します。次に、新しいタスク定義リビジョンを使用するように Amazon ECS サービスを更新します。

Amazon ECS サービスの脆弱性特性

Amazon ECS の到達可能性特性と推奨される修復手順は次のとおりです。

Amazon ECS サービスには、悪用の可能性の高いネットワークで悪用可能なソフトウェアの脆弱性を持つコンテナがあります。

1. 露出を理解する

   パッケージ脆弱性の検出結果は、共通脆弱性識別子 (CVEs) にさらされる AWS 環境内のソフトウェアパッケージを識別します。攻撃者は、こうしたパッチが適用されていない脆弱性を利用し、データの機密性、完全性、可用性を侵害したり、他のシステムにアクセスしたりする可能性があります。ECR コンテナイメージには、パッケージの脆弱性の検出結果を含めることができます。
2. 露出を修正する
   a. パッケージバージョンを更新する

      Lambda 関数のパッケージ脆弱性の検出結果を確認します。Amazon Inspector の提案に従ってパッケージバージョンを更新します。詳細については、Amazon Inspector ユーザーガイド」の「Amazon Inspector の検出結果の詳細の表示」を参照してください。 Amazon Inspector Amazon Inspector コンソールの検出結果の詳細の修復セクションには、パッケージを更新するために実行できるコマンドが表示されます。
   b. ベースコンテナイメージを更新する

      ベースコンテナイメージを定期的に再構築および更新して、コンテナを最新の状態に保ちます。イメージを再構築するときは、アタックサーフェスを減らすために不要なコンポーネントを含めないでください。コンテナイメージを再構築する手順については、「イメージを頻繁に再構築する」を参照してください。

Amazon ECS サービスにソフトウェアの脆弱性があるコンテナがある

Amazon ECS コンテナにインストールされているソフトウェアパッケージは、共通脆弱性識別子 (CVEs) に公開される可能性があります。優先度の低い脆弱性は、優先度の高い脆弱性と比較して重要度または悪用可能性が低いセキュリティの弱点を表します。これらの脆弱性は即時のリスクが低くなりますが、攻撃者はパッチが適用されていないこれらの脆弱性を悪用してデータの機密性、完全性、可用性を侵害したり、他のシステムにアクセスしたりする可能性があります。

影響を受けるコンテナイメージを更新する

特性の脆弱性タブのリファレンスセクションを確認します。ベンダーのドキュメントには、特定の修復ガイダンスが含まれている場合があります。

以下の一般的なガイドラインに従って、適切な修復を適用します。

- 影響を受けるパッケージのパッチ適用されたバージョンを使用するようにコンテナイメージを更新します。
- アプリケーションの影響を受ける依存関係を最新の安全なバージョンに更新します。

コンテナイメージを更新したら、コンテナレジストリにプッシュし、新しいイメージを使用するように Amazon ECS タスク定義を更新します。

今後の考慮事項

コンテナイメージのセキュリティ体制をさらに強化するには、Amazon ECS タスクとコンテナセキュリティのベストプラクティスに従うことを検討してください。Amazon Inspector は、コンテナの CVEs を自動的にスキャンするように設定できます。Amazon Inspector は、自動修復のために Security Hub と統合することもできます。Systems Manager メンテナンスウィンドウを使用して定期的なパッチ適用スケジュールを実装し、コンテナの中断を最小限に抑えることを検討してください。

Amazon EKS クラスターの公開の修正

AWS Security Hub は、Amazon Elastic Kubernetes Service (Amazon EKS) クラスターの公開結果を生成できます。

露出検出結果に関連する Amazon EKS クラスターとその識別情報は、検出結果の詳細のリソースセクションに一覧表示されます。これらのリソースの詳細は、Security Hub コンソールで取得することも、Security Hub API の GetFindingsV2オペレーションを使用してプログラムで取得することもできます。

露出検出結果に関連するリソースを特定したら、不要なリソースを削除できます。不要なリソースを削除すると、露出プロファイルと AWS コストを削減できます。リソースが不可欠な場合は、以下の推奨される修復手順に従ってリスクを軽減します。修復トピックは、特性のタイプに基づいて分割されます。

1 つの公開結果には、複数の修復トピックで特定された問題が含まれます。逆に、1 つの修復トピックだけに対処することで、露出の検出結果に対処し、その重要度レベルを下げることができます。リスク修復へのアプローチは、組織の要件とワークロードによって異なります。

> **Note**
>
> このトピックで提供される修復ガイダンスでは、他の AWS リソースで追加の相談が必要になる場合があります。

目次

- Amazon EKS クラスターの設定ミス特性
  - Amazon EKS クラスターがパブリックアクセスを許可する
  - Amazon EKS クラスターがサポートされていない Kubernetes バージョンを使用している
  - Amazon EKS クラスターが暗号化されていない Kubernetes シークレットを使用する
- Amazon EKS クラスターの脆弱性特性
  - Amazon EKS クラスターには、悪用の可能性の高いネットワークで悪用可能なソフトウェアの脆弱性があるコンテナがあります。
  - Amazon EKS クラスターにソフトウェアの脆弱性があるコンテナがある

Amazon EKS クラスターの設定ミス特性

Amazon EKS クラスターの設定ミスの特徴と推奨される修復手順は次のとおりです。

Amazon EKS クラスターがパブリックアクセスを許可する

Amazon EKS クラスターエンドポイントは、クラスターの Kubernetes API サーバーとの通信に使用するエンドポイントです。デフォルトでは、このエンドポイントはインターネットに公開されています。パブリックエンドポイントは、攻撃対象領域と Kubernetes API サーバーへの不正アクセスのリスクを高め、攻撃者がクラスターリソースにアクセスまたは変更したり、機密データにアクセスしたりできる可能性があります。セキュリティのベストプラクティスに従って、 は EKS クラスターエンドポイントへのアクセスを必要な IP 範囲のみに制限 AWS することをお勧めします。

エンドポイントアクセスの変更

露出検出結果で、 リソースを開きます。これにより、影響を受ける Amazon EKS クラスターが開きます。プライベートアクセス、パブリックアクセス、またはその両方を使用するようにクラスターを

設定できます。プライベートアクセスでは、クラスターの VPC 内で発生する Kubernetes API リクエストは、プライベート VPC エンドポイントを使用します。パブリックアクセスでは、クラスターの VPC の外部から送信される Kubernetes API リクエストは、パブリックエンドポイントを使用します。

クラスターへのパブリックアクセスの変更または削除

既存のクラスターのエンドポイントアクセスを変更するには、「Amazon Elastic Kubernetes Service ユーザーガイド」の「クラスターエンドポイントアクセスの変更」を参照してください。特定の IP 範囲またはセキュリティグループに基づいて、より制限の厳しいルールを実装します。制限されたパブリックアクセスが必要な場合は、特定の CIDR ブロック範囲へのアクセスを制限するか、プレフィックスリストを使用します。

Amazon EKS クラスターがサポートされていない Kubernetes バージョンを使用している

Amazon EKS は、各 Kubernetes バージョンを一定期間サポートします。サポートされていない Kubernetes バージョンでクラスターを実行すると、CVE パッチが古いバージョンでリリースされなくなるため、環境がセキュリティの脆弱性にさらされる可能性があります。サポートされていないバージョンには、攻撃者が悪用する可能性のある既知のセキュリティ脆弱性が含まれており、新しいバージョンで使用できるセキュリティ機能がない可能性があります。セキュリティのベストプラクティスに従って、 AWS では Kubernetes バージョンを更新することをお勧めします。

Kubernetes バージョンを更新する

露出検出結果で、 リソースを開きます。これにより、影響を受ける Amazon EKS クラスターが開きます。クラスターを更新する前に、Amazon Elastic Kubernetes Service ユーザーガイドの標準サポートで利用可能なバージョンで、現在サポートされている Kubernetes バージョンのリストを確認してください。

Amazon EKS クラスターが暗号化されていない Kubernetes シークレットを使用する

Kubernetes シークレットは、デフォルトでは API サーバーの基盤となるデータストア (etcd) に暗号化されずに保存されます。API アクセスを持つユーザー、または etcd へのアクセス権を持つユーザーは、シークレットを取得または変更できます。これを防ぐには、保管中の Kubernetes シークレットを暗号化する必要があります。Kubernetes シークレットが暗号化されていない場合、 etcd が侵害されると不正アクセスに対して脆弱になります。シークレットにはパスワードや API トークンなどの機密情報が含まれていることが多いため、シークレットが公開されると、他のアプリケーションやデータへの不正アクセスにつながる可能性があります。セキュリティのベストプラクティスに従って、 は Kubernetes シークレットに保存されているすべての機密情報を暗号化 AWS することをお勧めします。

Kubernetes シークレットの暗号化

Amazon EKS は、エンベロープ暗号化による KMS キーを使用した Kubernetes シークレットの暗号化をサポートしています。EKS クラスターの Kubernetes シークレットの暗号化を有効にするには、「Amazon EKS ユーザーガイド」の「既存のクラスターで KMS を使用して Kubernetes シークレットを暗号化する」を参照してください。

Amazon EKS クラスターの脆弱性特性

Amazon EKS クラスターの脆弱性特性は次のとおりです。

Amazon EKS クラスターには、悪用の可能性の高いネットワークで悪用可能なソフトウェアの脆弱性があるコンテナがあります。

EKS クラスターにインストールされているソフトウェアパッケージは、共通脆弱性識別子 (CVEs) に公開できます。重要な CVEs AWS 、環境に重大なセキュリティリスクをもたらします。認可されていないユーザーは、これらのパッチが適用されていない脆弱性を悪用して、データの機密性、完全性、可用性を侵害したり、他のシステムにアクセスしたりする可能性があります。エクスプロイトコードはすでに公開されており、攻撃者や自動スキャンツールによってアクティブに使用されている可能性があるため、エクスプロイトの可能性の高い重大な脆弱性は即時のセキュリティ脅威を表します。セキュリティのベストプラクティスに従って、 は、インスタンスを攻撃から保護するために、これらの脆弱性にパッチを適用 AWS することをお勧めします。

影響を受けるインスタンスを更新する

コンテナイメージを、特定された脆弱性のセキュリティ修正を含む新しいバージョンに更新します。これには通常、更新されたベースイメージまたは依存関係を使用してコンテナイメージを再構築し、新しいイメージを Amazon EKS クラスターにデプロイする必要があります。

Amazon EKS クラスターにソフトウェアの脆弱性があるコンテナがある

Amazon EKS クラスターにインストールされているソフトウェアパッケージは、共通脆弱性識別子 (CVEs) に公開される可能性があります。重要でない CVEsは、重要な CVEs と比較して重要度や悪用可能性が低いセキュリティの弱点を表します。これらの脆弱性は差し迫ったリスクが少なくなりますが、攻撃者はパッチが適用されていないこれらの脆弱性を悪用してデータの機密性、完全性、可用性を侵害したり、他のシステムにアクセスしたりできます。セキュリティのベストプラクティスに従って、 は、インスタンスを攻撃から保護するために、これらの脆弱性にパッチを適用 AWS することをお勧めします。

影響を受けるインスタンスを更新する

コンテナイメージを、特定された脆弱性のセキュリティ修正を含む新しいバージョンに更新します。これには通常、更新されたベースイメージまたは依存関係を使用してコンテナイメージを再構築し、新しいイメージを Amazon EKS クラスターにデプロイする必要があります。

IAM ユーザーの露出の修正

AWS Security Hub は、 AWS Identity and Access Management (IAM) ユーザーの公開結果を生成できます。

Security Hub コンソールでは、公開結果に関与した IAM ユーザーとその識別情報が、検出結果の詳細のリソースセクションに一覧表示されます。プログラムにより、Security Hub API の GetFindingsV2オペレーションを使用してリソースの詳細を取得できます。

露出検出結果に関連するリソースを特定したら、不要なリソースを削除できます。不要なリソースを削除すると、露出プロファイルと AWS コストを削減できます。リソースが不可欠な場合は、以下の推奨される修復手順に従ってリスクを軽減します。修復トピックは、特性のタイプに基づいて分割されます。

1 つの公開結果には、複数の修復トピックで特定された問題が含まれます。逆に、1 つの修復トピックだけに対処することで、露出の検出結果に対処し、その重要度レベルを下げることができます。リスク修復へのアプローチは、組織の要件とワークロードによって異なります。

> **Note**
>
> このトピックで提供される修復ガイダンスでは、他の AWS リソースで追加の相談が必要になる場合があります。

IAM ベストプラクティスでは、個々の IAM ユーザーを作成する代わりに、IAM ロールを作成するか、ID プロバイダーとのフェデレーションを使用して にアクセス AWS することをお勧めします。これが組織やユースケースのオプションである場合は、IAM ユーザーを使用する代わりに、ロールまたはフェデレーションに切り替えることをお勧めします。詳細については、『IAM ユーザーガイド』のIAM ユーザーを参照してください。

目次

- IAM ユーザーの設定ミスの特性
  - IAM ユーザーが管理アクセス権を持つポリシーを持っている
  - IAM ユーザーで MFA が有効になっていない
  - IAM ユーザーには、 への管理アクセス権を持つポリシーがあります。 AWS のサービス

- IAM ユーザーの AWS アカウントには弱いパスワードポリシーがあります
- IAM ユーザーに未使用の認証情報がある
- IAM ユーザーがローテーションされていないアクセスキーを持っている
- IAM ユーザーには、KMS キー復号化への無制限アクセスを許可するポリシーがあります

IAM ユーザーの設定ミスの特性

IAM ユーザーの設定ミスの特徴と推奨される修復手順は次のとおりです。

IAM ユーザーが管理アクセス権を持つポリシーを持っている

IAM ポリシーは、リソースにアクセスするときに IAM ユーザーに一連の権限を付与します。管理ポリシーは、IAM ユーザーに AWS サービスとリソースへの広範なアクセス許可を付与します。ユーザーが必要とする最小限のアクセス許可のセットではなく、完全な管理者権限を提供することで、認証情報が侵害された場合に攻撃の範囲を広げることができます。標準のセキュリティ原則に従って、AWS は最小権限を付与することをお勧めします。つまり、タスクの実行に必要なアクセス許可のみを付与します。

1. 管理ポリシーの確認と識別 – リソース ID で、IAM ロール名を識別します。IAM ダッシュボードに移動し、識別されたロールを選択します。IAM ユーザーにアタッチされているアクセス許可ポリシーを確認します。ポリシーが AWS マネージドポリシーの場合は、`AdministratorAccess`または を探します`IAMFullAccess`。それ以外の場合は、ポリシードキュメントで、 `"Action": "*"`を超える `"Effect":"Allow"`ステートメントを持つステートメントを探します`"Resource": "*"`。
2. 最小特権アクセスの実装 – サービス管理ポリシーを、ユーザーが機能するために必要な特定のアクセス許可のみを付与するポリシーに置き換えます。IAM ポリシーのセキュリティのベストプラクティスの詳細については、「 AWS Identity and Access Management ユーザーガイド」の「最小特権のアクセス許可を適用する」を参照してください。不要なアクセス許可を特定するには、IAM Access Analyzer を使用して、アクセス履歴に基づいてポリシーを変更する方法を理解します。詳細については、「 AWS Identity and Access Management ユーザーガイド」の「外部アクセスと未使用のアクセスの検出結果」を参照してください。
3. 安全な設定に関する考慮事項 – インスタンスにサービス管理アクセス許可が必要な場合は、リスクを軽減するために、以下の追加のセキュリティコントロールを実装することを検討してください。
   - 多要素認証 (MFA) – MFA は、追加の形式の認証を要求することで、セキュリティレイヤーを追加します。これにより、認証情報が侵害された場合でも、不正アクセスを防ぐことができま

す。詳細については、 AWS Identity and Access Management ユーザーガイドの「多要素認証 (MFA) を要求する」を参照してください。

- IAM 条件 – 条件要素を設定すると、ソース IP や MFA の経過時間などの要因に基づいて、管理アクセス許可をいつどのように使用できるかを制限できます。詳細については、「 AWS Identity and Access Management ユーザーガイド」の「IAM ポリシーの条件を使用してアクセスをさらに制限する」を参照してください。
- アクセス許可の境界 – アクセス許可の境界は、ロールが持つことができる最大アクセス許可を確立し、管理アクセスを持つロールのガードレールを提供します。詳細については、「 ユーザーガイド」の「アクセス許可の境界を使用してアカウント内のアクセス許可管理を委任する」を参照してください。 AWS Identity and Access Management

IAM ユーザーで MFA が有効になっていない

多要素認証 (MFA) は、ユーザー名とパスワードに更なる保護手段を追加します。MFA が有効で、IAM ユーザーが AWS ウェブサイトにサインインすると、 AWS MFA デバイスからユーザー名、パスワード、認証コードの入力を求められます。認証プリンシパルは、時間的制約のあるキーを発行するデバイスを所有し、認証情報に関する知識がある必要があります。MFA を使用しない場合、ユーザーのパスワードが侵害されると、攻撃者はユーザーのアクセス AWS 許可へのフルアクセスを取得します。標準のセキュリティ原則に従って、 は AWS Management Console アクセス権を持つすべてのアカウントとユーザーに対して MFA を有効にする AWS ことをお勧めします。

MFA タイプを確認する

AWS は、次の MFA タイプをサポートしています。

- パスキーとセキュリティキー
- 仮想認証アプリケーション
- ハードウェア TOTP トークン

物理デバイスによる認証は通常、より厳格なセキュリティ保護を提供しますが、任意のタイプの MFA の使用は、MFA を無効にするよりも安全です。

MFA の有効化

要件に合った MFA タイプを有効にするには、AWS IAM ユーザーガイドの「IAM での多要素認証」を参照してください。 実装する特定の MFA タイプのステップに従います。多くのユーザーを管理する組織では、MFA に機密リソースへのアクセスを要求することで、MFA の使用を強制できます。

IAM ユーザーには、 への管理アクセス権を持つポリシーがあります。 AWS のサービス

サービス管理者ポリシーは、IAM ユーザーに特定の AWS サービス内のすべてのアクションを実行するアクセス許可を付与します。これらのポリシーには通常、ユーザーがジョブ機能を実行するために必要ではないアクセス許可が含まれます。IAM ユーザーに必要な最小限のアクセス許可のセットではなく、サービス管理者権限を付与すると、認証情報が侵害された場合に攻撃の範囲が広がります。標準のセキュリティ原則に従って、 AWS は最小権限を付与することをお勧めします。つまり、タスクの実行に必要なアクセス許可のみを付与します。

サービス管理者ポリシーの確認と識別

リソース ID で、IAM ロール名を指定します。IAM ダッシュボードに移動し、識別されたロールを選択します。IAM ユーザーにアタッチされているアクセス許可ポリシーを確認します。ポリシーが AWS 管理ポリシーの場合は、 `AdministratorAccess`または を探します`IAMFullAccess`。それ以外の場合は、ポリシードキュメントで、「」というステートメントを持つステートメントを探します`Effect": "Allow" with "Action": "*" over "Resource": "*"`。

最小特権アクセスの実装

サービス管理ポリシーを、ユーザーが機能するために必要な特定のアクセス許可のみを付与するポリシーに置き換えます。不要なアクセス許可を特定するには、IAM Access Analyzer を使用して、アクセス履歴に基づいてポリシーを変更する方法を理解します。

安全な設定に関する考慮事項

インスタンスにサービス管理権限が必要な場合は、これらの追加のセキュリティコントロールを実装して露出を軽減することを検討してください。

- MFA は、追加の形式の認証を要求することで、セキュリティレイヤーを追加します。これにより、認証情報が侵害された場合でも、不正アクセスを防ぐことができます。
- 条件要素を使用して、ソース IP や MFA の経過時間などの要因に基づいて、管理アクセス許可をいつ、どのように使用できるかを制限します。
- アクセス許可の境界を使用して、ロールが持つことができる最大アクセス許可を確立し、管理アクセスを持つロールのガードレールを提供します。

IAM ユーザーの AWS アカウントには弱いパスワードポリシーがあります

パスワードポリシーは、IAM ユーザーパスワードの複雑さを最小限に抑えることで、不正アクセスから保護するのに役立ちます。強力なパスワードポリシーがないと、パスワード推測やブルートフォース攻撃によってユーザーアカウントが侵害されるリスクが高くなります。標準のセキュリティ

原則に従って、 は強力なパスワードポリシーを実装して、ユーザーが推測が難しい複雑なパスワードを作成することを AWS 推奨しています。

強力なパスワードポリシーを設定する

IAM ダッシュボードに移動し、アカウント設定に移動します。最小長、必要な文字タイプ、パスワードの有効期限設定など、アカウントの現在のパスワードポリシー設定を確認します。

パスワードポリシーを設定するときは、少なくとも以下のベストプラクティスに従う AWS ことをお勧めします。

- 少なくとも 1 つの大文字が必要です。
- 少なくとも 1 つの小文字が必要です。
- 少なくとも 1 つの記号が必要です。
- 少なくとも 1 つの数字が必要です。
- 8 文字以上が必要です。

セキュリティに関するその他の考慮事項

強力なパスワードポリシーに加えて、以下の追加のセキュリティ対策を検討してください。

- MFA は、追加の形式の認証を要求することで、セキュリティレイヤーを追加します。これにより、認証情報が侵害された場合でも、不正アクセスを防ぐことができます。
- ソース IP や MFA の経過時間などの要因に基づいて、管理アクセス許可をいつどのように使用できるかを制限する条件要素を設定します。

IAM ユーザーに未使用の認証情報がある

90 日以上非アクティブのままになっているパスワードやアクセスキーなどの未使用の認証情報は、AWS 環境にセキュリティ上のリスクをもたらします。これらの未使用の認証情報は、攻撃者の潜在的な攻撃ベクトルを作成し、組織全体の攻撃対象領域を増やします。セキュリティのベストプラクティスに従って、 AWS では、攻撃対象領域を減らすために、90 日以上使用されていない認証情報を無効化または削除することをお勧めします。

未使用の認証情報の無効化または削除

公開結果で、 リソースを開きます。これにより、ユーザーの詳細ウィンドウが開きます。未使用の認証情報に対してアクションを実行する前に、環境への潜在的な影響を評価します。適切な評価なしで認証情報を削除すると、バックグラウンドプロセス、スケジュールされたジョブなどが中断される

可能性があります。未使用の認証情報を削除する影響を確認するために、永続的な削除の前に短い非アクティブ化期間を検討してください。

認証情報タイプに基づいて適切なアクションを実行します。

- 未使用のコンソールパスワードの場合は、まずパスワードを変更し、一時的に無効にすることを検討してください。問題が発生しない場合は、永続的な非アクティブ化または削除に進みます。
- 未使用のアクセスキーについては、まずキーを非アクティブ化することを検討してください。影響を受けるシステムがないことを確認したら、永続的な非アクティブ化または削除に進みます。
- 未使用のユーザーの場合、完全な削除の前に制限ポリシーをアタッチしてユーザーを一時的に非アクティブ化することを検討してください。

IAM ユーザーがローテーションされていないアクセスキーを持っている

アクセスキーは、 AWS リソースへのプログラムによるアクセスを可能にするアクセスキー ID とシークレットアクセスキーで構成されます。アクセスキーを長期間変更しないと、不正アクセスのリスクが高まります。セキュリティのベストプラクティスに従って、攻撃者が侵害された認証情報を使用する機会を最小限に抑えるために、 は 90 日ごとにアクセスキーをローテーション AWS することをお勧めします。

アクセスキーのローテーション

公開結果で、 リソースを開きます。これにより、ユーザーの詳細ウィンドウが開きます。アクセスキーをローテーションするには、「IAM ユーザーガイド」の「IAM ユーザーのアクセスキーを管理する」を参照してください。

IAM ユーザーには、KMS キー復号化への無制限アクセスを許可するポリシーがあります

AWS KMS を使用すると、データの保護に使用される暗号化キーを作成および管理できます。すべての KMS AWS KMS キーに対して無制限の復号アクセス許可 (`kms:Decrypt`や などkms:ReEncryptFrom) を許可する IAM ポリシーは、IAM ユーザーの認証情報が侵害された場合、不正なデータアクセスにつながる可能性があります。攻撃者がこれらの認証情報にアクセスすると、機密データを含む環境内の暗号化されたデータを復号化する可能性があります。セキュリティのベストプラクティスに従って、 AWS KMS は、復号化のアクセス許可を、ユーザーが職務機能に必要な特定のキーのみに制限することで、最小特権の実装 AWS を推奨します。

最小特権アクセスの実装

露出検出結果で、 リソースを開きます。これにより、IAM ポリシーウィンドウが開きます。KMS で、リソース仕様が `KMS:*`の kms:Decrypt または `kms:ReEncryptFrom` または を許可するアクセ

ス許可を探します"*"。ポリシーを更新して、 AWS KMS 復号のアクセス許可を必要な特定のキーのみに制限します。ポリシーを変更して、"*"リソースを必要な AWS KMS キーの特定の ARNs に置き換えます。

安全な設定に関する考慮事項

これらのアクセス許可を使用できるタイミングをさらに制限するための条件を追加することを検討してください。たとえば、復号オペレーションを特定の VPC エンドポイントまたはソース IP 範囲に制限できます。特定の KMS キーを使用できるユーザーをさらに制限するようにキーポリシーを設定することもできます。

Lambda 関数の公開の修正

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

AWS Security Hub は、 AWS Lambda (Lambda) 関数の公開結果を生成できます。

Security Hub コンソールでは、公開結果に関連する Lambda 関数とその識別情報が、検出結果の詳細のリソースセクションに一覧表示されます。プログラムでは、Security Hub API の GetFindingsV2オペレーションを使用してリソースの詳細を取得できます。

露出検出結果に関連するリソースを特定したら、不要なリソースを削除できます。不要なリソースを削除すると、露出プロファイルと AWS コストを削減できます。リソースが不可欠な場合は、以下の推奨される修復手順に従ってリスクを軽減します。修復トピックは、特性のタイプに基づいて分割されます。

1 つの公開結果には、複数の修復トピックで特定された問題が含まれます。逆に、1 つの修復トピックだけに対処することで、露出の検出結果に対処し、その重要度レベルを下げることができます。リスク修復へのアプローチは、組織の要件とワークロードによって異なります。

> **Note**
>
> このトピックで提供される修復ガイダンスでは、他の AWS リソースで追加の相談が必要になる場合があります。

> **Note**
>
> このトピックで提供される修復ガイダンスでは、他の AWS リソースで追加の相談が必要になる場合があります。

目次

- Lambda 関数の設定ミスの特性
  - Lambda 関数がサポートされていないランタイムを実行しています
  - Lambda 関数が Amazon VPC の外部にデプロイされる
  - Lambda 関数は IAM ロールを引き受けることができます
  - Lambda 関数に関連付けられた IAM ロールには管理アクセスポリシーがあります
  - Lambda 関数に関連付けられた IAM ロールには、 AWS サービスへの管理アクセス権を持つポリシーがあります
- Lambda 関数の到達可能性特性
  - Lambda 関数はパブリックに呼び出すことができます
- Lambda 関数の脆弱性特性
  - Lambda 関数にネットワークが爆発するソフトウェアの脆弱性がある
  - Lambda 関数にはソフトウェア脆弱性があります

Lambda 関数の設定ミスの特性

Lambda 関数の設定ミスの特徴と推奨される修復手順は次のとおりです。

Lambda 関数がサポートされていないランタイムを実行しています

Lambda を使用すると、開発者はマネージド環境でコードを実行するランタイムを通じてサーバーをプロビジョニングまたは管理することなくコードを実行できます。Lambda は、マネージドランタイムとそれに対応するコンテナベースイメージにパッチとセキュリティ更新プログラムを自動的に適用します。ランタイムバージョンがサポートされなくなった場合、セキュリティ更新、バグ修正、またはテクニカルサポートは受け取られなくなります。非推奨のランタイムで実行されている関数にはセキュリティの脆弱性があり、証明書の有効期限切れなどの問題により最終的に機能停止する可能性があります。さらに、サポートされていないランタイムは、利用可能なパッチなしで新しく検出されたセキュリティエクスプロイトに対して脆弱になる可能性があります。セキュリティのベストプラク

ティスに従って、Lambda 関数にはパッチが適用され、サポートされているランタイムを使用することをお勧めします。

関数ランタイムをアップグレードする

公開のリソースタブで、ハイパーリンクを使用してリソースを開きます。これにより、Lambda 関数ウィンドウが開きます。関数をサポートされているランタイムにアップグレードするには、ランタイム管理設定を構成します。関数を最新のランタイムバージョンに自動的に更新することを選択できますが、このオプションを選択する前に、自動アップグレードが実行中のアプリケーションに影響を与える可能性があるかどうかを評価してください。詳細については、「Lambda がランタイムバージョンの更新を管理する方法を理解する」を参照してください。

Lambda 関数が Amazon VPC の外部にデプロイされる

デフォルトでは、Lambda 関数はパブリックインターネットにアクセスできるようにデプロイされます。このデフォルト設定により、Lambda 関数は AWS サービスエンドポイントと外部 APIs にアクセスできますが、潜在的なセキュリティリスクにさらされます。インターネットアクセスのある関数は、データの流出、不正なサーバーとの通信、または侵害された場合の外部アクターのエントリポイントになるために使用できます。Amazon VPC は、定義されたプライベートネットワーク内のリソースとのみ通信するように Lambda 関数を制限することで、ネットワークを分離します。標準のセキュリティ原則に従って、ネットワーク分離によるセキュリティを向上させるために、VPC 内に Lambda 関数をデプロイすることをお勧めします。

VPC に関数をアタッチする

公開結果で、ハイパーリンクを使用してリソースを開きます。これにより、Lambda 関数ウィンドウが開きます。ネットワークアクセスを制限して Lambda 関数を保護するには、適切なネットワークコントロールが設定されている VPC にアタッチします。関数を VPC にアタッチする前に、必要な AWS サービスアクセスを計画してください。NAT ゲートウェイまたは VPC エンドポイントのないプライベートサブネットの関数は AWS サービス APIs に到達できないためです。アカウントの Amazon VPC に Lambda 関数をアタッチする方法については、「 の Amazon VPC に Lambda 関数をアタッチする AWS アカウント」を参照してください。関数がプライベートサブネット内からサービスにアクセスする必要がある場合は、インターネットアクセスなしで AWS サービス接続に VPC エンドポイントを使用することを検討してください。プライベートサブネットからのアウトバウンドインターネット接続が必要な場合は、NAT ゲートウェイを設定します。

Lambda 関数は IAM ロールを引き受けることができます

Lambda 関数は、IAM ロールを使用して AWS サービスとやり取りします。これらのロールは、実行中に AWS リソースにアクセスするためのアクセス許可を Lambda 関数に付与します。これらのロー

ルは、Lambda 関数がタスクを実行するために必要になる場合がありますが、これらのロールは最小特権の原則に従う必要があります。標準のセキュリティ原則に従って、 は、関数の意図した機能に基づいて、ロールにアタッチされたアクセス許可が適切かどうかを確認する AWS ことをお勧めします。

1. アタッチされた IAM ロールが必要かどうかを判断する

   Lambda 関数で IAM 実行ロールを設定する必要があるかどうかを確認します。ほとんどの Lambda 関数には、CloudWatch へのログの書き込みなど、基本的な操作権限が必要です。関数の実行ロールにアタッチされているアクセス許可を確認し、関数に IAM ロールが必要かどうかを判断します。Lambda 実行ロールの詳細については、「 デベロッパーガイド」の「実行ロールを使用した Lambda 関数のアクセス許可の定義」を参照してください。 AWS Lambda

2. 最小特権アクセスの実装

   過度に寛容なポリシーを、関数が動作するために必要な特定のアクセス許可のみを付与するポリシーに置き換えます。IAM ロールのセキュリティのベストプラクティスについては、「 AWS Identity and Access Management ユーザーガイド」の「最小特権のアクセス許可を適用する」を参照してください。不要なアクセス許可を特定するには、IAM Access Analyzer を使用して、アクセス履歴に基づいてポリシーを変更する方法を理解します。詳細については、「 AWS Identity and Access Management ユーザーガイド」の「外部アクセスと未使用のアクセスの検出結果」を参照してください。または、新しい IAM ロールを作成して、既存のロールを使用している他の Lambda 関数に影響を与えないようにすることもできます。このシナリオでは、新しい IAM ロールを作成し、新しい IAM ロールをインスタンスに関連付けます。関数の IAM ロールを置き換える手順については、「 AWS Lambda デベロッパーガイド」の「関数の実行ロールを更新する」を参照してください。

Lambda 関数に関連付けられた IAM ロールには管理アクセスポリシーがあります

管理アクセスポリシーは、Lambda 関数に AWS サービスとリソースへの広範なアクセス許可を提供します。これらのポリシーには通常、機能に必要のないアクセス許可が含まれます。実行ロールに必要な最小限のアクセス許可のセットではなく、Lambda 関数の管理アクセスポリシーを IAM アイデンティティに提供すると、関数が侵害された場合に攻撃の範囲を広げることができます。標準のセキュリティ原則に従って、 AWS は最小権限を付与することをお勧めします。つまり、タスクの実行に必要なアクセス許可のみを付与します。

1. 管理ポリシーの確認と識別

公開結果で、ロール名を特定します。IAM ダッシュボードに移動し、前に特定したロール名を持つロールを見つけます。IAM ロールにアタッチされているアクセス許可ポリシーを確認します。ポリシーが AWS マネージドポリシーの場合は、 `AdministratorAccess`または を探します`IAMFullAccess`。それ以外の場合は、ポリシードキュメントで、 ステートメント`"Effect": "Allow", "Action": "*"`と ステートメントが`"Resource": "*"`一緒にあるステートメントを探します。

2. 最小特権アクセスの実装

   管理ポリシーを、関数の動作に必要な特定のアクセス許可のみを付与するポリシーに置き換えます。IAM ロールのセキュリティのベストプラクティスの詳細については、「 AWS Identity and Access Management ユーザーガイド」の「最小特権のアクセス許可を適用する」を参照してください。不要なアクセス許可を特定するには、IAM Access Analyzer を使用して、アクセス履歴に基づいてポリシーを変更する方法を理解します。詳細については、「 AWS Identity and Access Management ユーザーガイド」の「外部アクセスと未使用のアクセスの検出結果」を参照してください。または、新しい IAM ロールを作成して、既存のロールを使用して他の Lambda 関数に影響を与えないようにすることもできます。このシナリオでは、新しい IAM ロールを作成します。次に、新しいロールをインスタンスに関連付けます。関数の IAM ロールの置き換えについては、「 AWS Lambda デベロッパーガイド」の「関数の実行ロールの更新」を参照してください。

3. 安全な設定に関する考慮事項

   インスタンスに管理アクセス許可が必要な場合は、リスクを軽減するために、これらの追加のセキュリティコントロールを実装することを検討してください。

   - 多要素認証 (MFA) – MFA は、追加の形式の認証を要求することで、セキュリティレイヤーを追加します。これにより、認証情報が侵害された場合でも、不正アクセスを防ぐことができます。詳細については、「 AWS Identity and Access Management ユーザーガイド」の「多要素認証 (MFA) を要求する」を参照してください。
   - IAM 条件 – 条件要素を設定すると、ソース IP や MFA の経過時間などの要因に基づいて、管理アクセス許可をいつどのように使用できるかを制限できます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの条件を使用してアクセスをさらに制限する」を参照してください。
   - アクセス許可の境界 – アクセス許可の境界は、ロールが持つことができる最大アクセス許可を確立し、管理アクセスを持つロールのガードレールを提供します。詳細については、「 ユーザーガイド」の「アクセス許可の境界を使用してアカウント内のアクセス許可管理を委任する」を参照してください。 AWS Identity and Access Management

Lambda 関数に関連付けられた IAM ロールには、 AWS サービスへの管理アクセス権を持つポリシーがあります

サービス管理者ポリシーにより、Lambda 関数は特定の AWS サービス内のすべてのアクションを実行できます。これらのポリシーは通常、関数のオペレーションに必要な以上のアクセス許可を付与します。サービス管理者ポリシーを持つ Lambda 関数が侵害された場合、攻撃者はこれらのアクセス許可を使用して、 AWS 環境内の機密データまたはサービスにアクセスまたは変更する可能性があります。標準のセキュリティ原則に従って、最小権限を付与することをお勧めします。つまり、タスクの実行に必要なアクセス許可のみを付与します。

1. 管理ポリシーの確認と識別

   公開結果で、ARN 内のロール名を特定します。IAM ダッシュボードに移動し、ロール名を見つけます。ロールにアタッチされているアクセス許可ポリシーを確認します。ポリシーが AWS マネージドポリシーの場合は、 `AdministratorAccess`または を探します`IAMFullAccess`。それ以外の場合は、ポリシードキュメントで、 ステートメント`"Effect": "Allow", "Action": "*"`と `"Resource": "*"` ステートメントを持つステートメントを探します。

2. 最小特権アクセスの実装

   管理ポリシーを、関数の動作に必要な特定のアクセス許可のみを付与するポリシーに置き換えます。詳細については、「AWS Identity and Access Management ユーザーガイド」の「最小特権アクセス許可を適用する」を参照してください。不要なアクセス許可を特定するには、IAM Access Analyzer を使用して、アクセス履歴に基づいてポリシーを変更する方法を理解します。詳細については、「 AWS Identity and Access Management ユーザーガイド」の「外部アクセスと未使用のアクセスの検出結果」を参照してください。または、新しい IAM ロールを作成して、既存のロールを使用している他の Lambda 関数に影響を与えないようにすることもできます。このシナリオでは、新しい IAM ロールを作成し、新しい IAM ロールをインスタンスに関連付けます。関数の IAM ロールを置き換える手順については、「 AWS Lambda デベロッパーガイド」の「関数の実行ロールを更新する」を参照してください。

3. 安全な設定に関する考慮事項

   インスタンスにサービスレベルの管理権限が必要な場合は、リスクを軽減するためにこれらの追加のセキュリティコントロールを実装することを検討してください。

   - 多要素認証 (MFA) – MFA は、追加の形式の認証を要求することで、セキュリティレイヤーを追加します。これにより、認証情報が侵害された場合でも、不正アクセスを防ぐことができます。詳細については、「 AWS Identity and Access Management ユーザーガイド」の「多要素認証 (MFA) を要求する」を参照してください。

- IAM 条件 – 条件要素を設定すると、ソース IP や MFA の経過時間などの要因に基づいて、管理アクセス許可をいつどのように使用できるかを制限できます。詳細については、「 AWS Identity and Access Management ユーザーガイド」の「IAM ポリシーの条件を使用してアクセスをさらに制限する」を参照してください。
- アクセス許可の境界 – アクセス許可の境界は、ロールが持つことができる最大アクセス許可を確立し、管理アクセスを持つロールのガードレールを提供します。詳細については、「 AWS Identity and Access Management ユーザーガイド」の「アクセス許可の境界を使用してアクセス許可の管理を委任する」を参照してください。

Lambda 関数の到達可能性特性

Lambda 関数の到達可能性特性と推奨される修復手順は次のとおりです。

Lambda 関数はパブリックに呼び出すことができます

Lambda リソースベースのポリシーは、関数を呼び出すことができるユーザーを決定します。プリンシパルとして「*」を含むリソースポリシーを持つ関数 (またはプリンシパルをまったく含まない) では、認証された AWS ユーザーが呼び出すことができます。これにより、特に機密データの処理、リソースの変更、またはアクセス許可の昇格を行う関数に重大なリスクが生じます。許可されていないユーザーは、この設定を悪用して、望ましくない操作を実行したり、データを公開したり、リソースを操作したり、関数機能を悪用したりする可能性があります。セキュリティのベストプラクティスに従って、Lambda 関数へのアクセスを承認されたプリンシパルのみに制限することをお勧めします。

関数のリソースベースのポリシーを変更する

公開のリソースタブで、ハイパーリンクを使用してリソースを開きます。これにより、Lambda 関数ウィンドウが開きます。リソースベースのポリシーで、承認された AWS アカウント IDsまたは特定の IAM プリンシパル (ユーザー、ロール、またはサービス) のみを指定して、Lambda 関数へのアクセスを制限します。リソースベースのポリシーは、プログラムでのみ変更できます。

Lambda 関数の脆弱性特性

Lambda 関数の脆弱性特性と推奨される修復手順は次のとおりです。

Lambda 関数にネットワークが爆発するソフトウェアの脆弱性がある

Lambda 関数コードで使用されるソフトウェアパッケージには、悪用される可能性が高い共通脆弱性識別子 (CVEs) を含めることができます。重要な CVEs AWS 、環境に重大なセキュリティリスクをもたらします。攻撃者は、こうしたパッチが適用されていない脆弱性を利用し、データの機密性、完

全性、可用性を侵害したり、他のシステムにアクセスしたりする可能性があります。エクスプロイトコードはすでに公開されており、攻撃者や自動スキャンツールによってアクティブに使用されている可能性があるため、エクスプロイトの可能性の高い重大な脆弱性は即時のセキュリティ脅威を表します。セキュリティのベストプラクティスに従って、これらの脆弱性にパッチを適用して、 関数を攻撃から保護することをお勧めします。

影響を受ける関数を更新する

特性の脆弱性タブの「リファレンス」セクションを確認してください。ベンダーのドキュメントには、特定の修復ガイダンスが含まれている場合があります。ベンダーが推奨する手順に従って、脆弱なライブラリを最新の安全なバージョンに更新します。通常、修復ワークフローは、zip ファイルをアップロードするか、コンテナイメージで Lambda 関数を作成することによって Lambda パッケージをデプロイしたかによって異なります。ライブラリを更新したら、固定バージョンを使用するように Lambda 関数コードを更新します。その後、更新されたバージョンをデプロイします。

Lambda 関数にはソフトウェア脆弱性があります

Lambda 関数は、多くの場合、重要な CVEs と比較して重要度や脆弱性が低いセキュリティの脆弱性を含む可能性のあるサードパーティーのライブラリと依存関係を使用します。これらの重要でない脆弱性はすぐには悪用できないかもしれませんが、他の脆弱性と連鎖して関数を侵害する可能性があるセキュリティ上の弱点を表しています。時間の経過とともに、これらの脆弱性のリスクを高める新しいエクスプロイト手法も出現する可能性があります。標準的なセキュリティ原則に従って、安全な環境を維持するために、これらの脆弱性にパッチを適用することをお勧めします。

特性の脆弱性タブの「リファレンス」セクションを確認してください。ベンダーのドキュメントには、特定の修復ガイダンスが含まれている場合があります。ベンダーが推奨する手順に従って、脆弱なライブラリを最新の安全なバージョンに更新します。通常、修復ワークフローは、zip ファイルをアップロードするか、コンテナイメージで Lambda 関数を作成することによって Lambda パッケージをデプロイしたかによって異なります。ライブラリを更新したら、固定バージョンを使用するように Lambda 関数コードを更新します。その後、更新されたバージョンをデプロイします。

Amazon RDS 関数の公開の修正

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

AWS Security Hub は、Amazon RDS 関数の公開結果を生成できます。

Security Hub コンソールでは、公開結果に関連する Amazon RDS 関数とその識別情報が、検出結果の詳細のリソースセクションに一覧表示されます。プログラムにより、Security Hub API の GetFindingsV2オペレーションを使用してリソースの詳細を取得できます。

公開結果に関連するリソースを特定したら、不要なリソースを削除できます。不要なリソースを削除すると、露出プロファイルと AWS コストを削減できます。リソースが不可欠な場合は、以下の推奨される修復手順に従ってリスクを軽減します。修復トピックは、特性のタイプに基づいて分割されます。

1 つの公開結果には、複数の修復トピックで特定された問題が含まれます。逆に、1 つの修復トピックだけに対処することで、露出の検出結果に対処し、その重要度レベルを下げることができます。リスク修復へのアプローチは、組織の要件とワークロードによって異なります。

> **Note**
>
> このトピックで提供される修復ガイダンスでは、他の AWS リソースで追加の相談が必要になる場合があります。

目次

- Amazon RDS 関数の設定ミス特性
  - Amazon RDS DB インスタンスはパブリックアクセスで設定されています
  - Amazon RDS DB クラスターには、パブリックに共有されているスナップショットがあります
  - Amazon RDS DB インスタンスには、保管時に暗号化されていないスナップショットがあります
  - Amazon RDS DB クラスターには、保管時に暗号化されていないスナップショットがあります
  - Amazon RDS DB インスタンスにオープンセキュリティグループがある
  - Amazon RDS DB インスタンスで IAM データベース認証が無効になっている
  - Amazon RDS DB インスタンスはデフォルトの管理者ユーザー名を使用します
  - Amazon RDS DB クラスターはデフォルトの管理者ユーザー名を使用します
  - Amazon RDS DB インスタンスで自動マイナーバージョンアップグレードが無効になっている
  - Amazon RDS DB インスタンスの自動バックアップが無効になっている
  - Amazon RDS DB インスタンスの削除保護が無効になっている
  - Amazon RDS DB クラスターの削除保護が無効になっている
  - Amazon RDS DB インスタンスは、データベースエンジンのデフォルトポートを使用します。
  - Amazon RDS DB インスタンスはバックアッププランの対象ではありません

Amazon RDS 関数の設定ミス特性

以下に、Amazon RDS 関数の設定ミスの特性と修復手順について説明します。

Amazon RDS DB インスタンスはパブリックアクセスで設定されています

パブリックアクセスを持つ Amazon RDS インスタンスは、エンドポイントを介してインターネット経由でアクセスできる可能性があります。インスタンス機能にはパブリックアクセスが必要になる場合がありますが、この設定は、権限のないユーザーがデータベースにアクセスしようとする潜在的な攻撃ベクトルとして使用できます。パブリックにアクセス可能なデータベースは、ポートスキャン、ブルートフォース攻撃、悪用の試みにさらされる可能性があります。標準のセキュリティ原則に従って、データベースリソースの公開を制限することをお勧めします。

1. パブリックアクセス設定を変更する

   公開結果で、ハイパーリンクを使用してリソースを開きます。これにより、影響を受ける DB インスタンスが開きます。DB インスタンスがアプリケーションアーキテクチャに基づいてパブリックアクセシビリティを必要とするかどうかを評価します。詳細については、「Amazon RDS でのパブリックアクセスまたはプライベートアクセスの設定」を参照してください。

Amazon RDS DB クラスターには、パブリックに共有されているスナップショットがあります

パブリックスナップショットには誰でもアクセスできるため AWS アカウント、機密データが権限のないユーザーに公開される可能性があります。 AWS アカウント には、これらのパブリックスナップショットをコピーして DB インスタンスを作成するアクセス許可があり、データ侵害や不正なデータアクセスにつながる可能性があります。セキュリティのベストプラクティスに従って、Amazon RDS スナップショットへのアクセスを信頼できる組織 AWS アカウント と組織のみに制限することをお勧めします。

1. プライベートアクセス用に Amazon RDS スナップショットを設定する

公開結果で、ハイパーリンクを使用してリソースを開きます。スナップショット共有設定を変更する方法については、「Amazon Aurora ユーザーガイド」の「スナップショットの共有」を参照してください。 スナップショットの共有を停止する方法については、「Amazon Aurora ユーザーガイド」の「スナップショットの共有の停止」を参照してください。

Amazon RDS DB インスタンスには、保管時に暗号化されていないスナップショットがあります

暗号化されていない Amazon RDS DB インスタンススナップショットは、ストレージレイヤーへの不正アクセスが取得されると、機密データを公開する可能性があります。暗号化を行わないと、ス

ナップショット内のデータが不正アクセスによって公開される可能性があります。これにより、データ侵害やコンプライアンス違反のリスクが生じます。セキュリティのベストプラクティスに従って、データの機密性を維持するために、すべてのデータベースリソースとそのバックアップを暗号化することをお勧めします。

公開結果で、ハイパーリンクを使用してリソースを開きます。これにより、影響を受けるスナップショットが開きます。暗号化されていない既存のスナップショットを直接暗号化することはできません。代わりに、暗号化されていないスナップショットの暗号化されたコピーを作成します。詳細な手順については、「Amazon Aurora ユーザーガイド」の「DB クラスタースナップショットのコピーと Amazon RDS リソースの暗号化」を参照してください。

Amazon RDS DB クラスターには、保管時に暗号化されていないスナップショットがあります

暗号化されていない Amazon RDS DB クラスタースナップショットは、ストレージレイヤーへの不正アクセスが取得されると、機密データを公開する可能性があります。暗号化を行わないと、スナップショット内のデータが不正アクセスによって公開される可能性があります。これにより、データ侵害やコンプライアンス違反のリスクが生じます。セキュリティのベストプラクティスに従って、データの機密性を維持するために、すべてのデータベースリソースとそのバックアップを暗号化することをお勧めします。

1. スナップショットの暗号化されたコピーを作成する

公開結果で、ハイパーリンクを使用してリソースを開きます。これにより、影響を受けるスナップショットが開きます。暗号化されていない既存のスナップショットを直接暗号化することはできません。代わりに、暗号化されていないスナップショットの暗号化されたコピーを作成します。詳細な手順については、「Amazon Aurora ユーザーガイド」の「DB クラスタースナップショットのコピーと Amazon RDS リソースの暗号化」を参照してください。

Amazon RDS DB インスタンスにオープンセキュリティグループがある

セキュリティグループは、Amazon RDS インスタンスの仮想ファイアウォールとして機能し、インバウンドトラフィックとアウトバウンドトラフィックを制御します。任意の IP アドレスからの無制限のアクセスを許可するオープンセキュリティグループは、データベースインスタンスを不正アクセスや潜在的な攻撃にさらす可能性があります。標準のセキュリティ原則に従って、最小特権の原則を維持するために、セキュリティグループアクセスを特定の IP アドレスとポートに制限することをお勧めします。

セキュリティグループのルールを確認し、現在の設定を評価する

公開結果で、DB インスタンスのセキュリティグループのリソースを開きます。などの幅広い IP 範囲からオープンおよびアクセス可能なポートを評価します(`0.0.0.0/0 or ::/0`)。セキュ

リティグループの詳細の表示については、Amazon Elastic Compute Cloud API リファレンスの「DescribeSecurityGroups」を参照してください。

セキュリティグループルールを変更する

セキュリティグループのルールを変更して、特定の信頼された IP アドレスまたは範囲へのアクセスを制限します。セキュリティグループルールを更新するときは、必要なソース IP 範囲ごとにルールを作成するか、特定のポートへのアクセスを制限することで、異なるネットワークセグメントのアクセス要件を分離することを検討してください。セキュリティグループルールを変更するには、Amazon EC2 ユーザーガイド」の「セキュリティグループルールの設定」を参照してください。既存の Amazon RDS データベースインスタンスのデフォルトポートを変更するには、「Amazon Aurora ユーザーガイド」の「コンソール、CLI、API を使用した DB クラスターの変更」を参照してください。

Amazon RDS DB インスタンスで IAM データベース認証が無効になっている

IAM データベース認証を使用すると、データベースパスワードの代わりに IAM 認証情報を使用して Amazon RDS データベースを認証できます。これにより、一元化されたアクセス管理、一時的な認証情報、データベースパスワードをアプリケーションコードに保存することの排除など、いくつかのセキュリティ上の利点があります。IAM データベース認証では、パスワードではなく、認証トークンを使用したデータベースインスタンスへの認証が可能です。その結果、データベースインスタンスとの間のネットワークトラフィックは SSL を使用して暗号化されます。IAM 認証がない場合、データベースは通常パスワードベースの認証に依存しているため、パスワードの再利用やパスワードの不足につながる可能性があります。セキュリティのベストプラクティスに従って、IAM データベース認証を有効にすることをお勧めします。

IAM データベース認証を有効にする

公開結果で、ハイパーリンクを使用してリソースを開きます。これにより、影響を受ける DB インスタンスが開きます。データベースオプションで IAM データベース認証を有効にできます。詳細については、「Amazon RDS ユーザーガイド」の「IAM データベース認証の有効化と無効化」を参照してください。IAM 認証を有効にしたら、パスワードベースの認証ではなく IAM 認証を使用するように DB インスタンスを更新します。

Amazon RDS DB インスタンスはデフォルトの管理者ユーザー名を使用します

DB インスタンスにデフォルトのユーザー名 (例: 「admin」、「root」) を使用すると、ブルートフォース攻撃の対象となることが広く知られており、セキュリティリスクが高まります。デフォルトのユーザー名は予測可能で、権限のないユーザーがデータベースにアクセスすることを容易にし

ます。デフォルトのユーザー名では、攻撃者はデータベースにアクセスするために両方を必要とするのではなく、パスワードを取得するだけで済みます。セキュリティのベストプラクティスに従って、データベースインスタンスに一意の管理者ユーザー名を使用して、不明瞭さによるセキュリティを強化し、不正アクセスのリスクを軽減することをお勧めします。

一意の管理者ユーザー名を設定する

公開結果で、ハイパーリンクを使用してリソースを開きます。これにより、影響を受ける DB インスタンスが開きます。アプリケーションに最適なバックアップ頻度、保持期間、ライフサイクルルールを検討してください。

Amazon RDS DB クラスターはデフォルトの管理者ユーザー名を使用します

DB インスタンスにデフォルトのユーザー名 (例: 「admin」、「root」) を使用すると、ブルートフォース攻撃の対象となることが広く知られており、セキュリティリスクが高まります。デフォルトのユーザー名は予測可能で、権限のないユーザーがデータベースにアクセスすることを容易にします。デフォルトのユーザー名では、攻撃者はデータベースにアクセスするために両方を必要とするのではなく、パスワードを取得するだけで済みます。セキュリティのベストプラクティスに従って、データベースインスタンスに一意の管理者ユーザー名を使用して、不明瞭さによるセキュリティを強化し、不正アクセスのリスクを軽減することをお勧めします。

一意の管理者ユーザー名を設定する

公開結果で、ハイパーリンクを使用してリソースを開きます。これにより、影響を受ける DB インスタンスが開きます。既存の Amazon RDS DB インスタンスの管理者ユーザー名を変更することはできません。一意の管理者名を作成するには、カスタムユーザー名で新しい DB インスタンスを作成し、データを移行する必要があります。

Amazon RDS DB インスタンスで自動マイナーバージョンアップグレードが無効になっている

自動マイナーバージョンアップグレードにより、Amazon RDS インスタンスは利用可能になったときにマイナーエンジンバージョンアップグレードを自動的に受け取ることができます。これらのアップグレードには、多くの場合、データベースのセキュリティと安定性を維持するのに役立つ重要なセキュリティパッチとバグ修正が含まれます。データベースは、新しいマイナーバージョンで修正された既知のセキュリティ脆弱性で実行されるリスクがあります。自動更新がない場合、データベースインスタンスは新しい CVEsを蓄積する可能性があります。セキュリティのベストプラクティスに従って、すべての Amazon RDS インスタンスに対してマイナーバージョンの自動アップグレードを有効にすることをお勧めします。

自動マイナーバージョンアップグレードを有効にする

公開結果で、ハイパーリンクを使用してリソースを開きます。これにより、影響を受ける DB インスタンスが開きます。自動マイナーアップグレード設定は、メンテナンスとバックアップタブで表示できます。詳細については、「Amazon RDS for MySQL の自動マイナーバージョンアップグレード」を参照してください。データベースアクティビティが少ない期間にメンテナンスウィンドウが発生するように設定することもできます。

Amazon RDS DB インスタンスの自動バックアップが無効になっている

自動バックアップは、Amazon RDS インスタンスのpoint-in-timeリカバリを提供するため、データベースを保持期間内の任意の時点に復元できます。自動バックアップを無効にすると、悪意のある削除、データ破損、またはその他のデータ損失シナリオが発生した場合に、データが失われるリスクがあります。ランサムウェア攻撃、データベーステーブルの削除、破損などの悪意のあるアクティビティが発生した場合、インシデントが発生する前の時点に復元できるため、インシデントからの復旧にかかる時間が短縮されます。セキュリティのベストプラクティスに従って、すべての本番データベースに対して適切な保持期間を持つ自動バックアップを有効にすることをお勧めします。

Amazon RDS DB インスタンスの削除保護が無効になっている

データベース削除保護は、データベースインスタンスの削除を防ぐのに役立つ機能です。削除保護を無効にすると、十分なアクセス許可を持つユーザーがデータベースを削除できるため、データ損失やアプリケーションのダウンタイムが発生する可能性があります。攻撃者はデータベースを削除し、サービスの中断、データ損失、復旧時間の増加につながる可能性があります。セキュリティのベストプラクティスに従って、RDS DB インスタンスの削除保護を有効にして、悪意のある削除を防ぐことをお勧めします。

Amazon RDS DB クラスターの削除保護を有効にする

公開結果で、ハイパーリンクを使用してリソースを開きます。これにより、影響を受ける DB クラスターが開きます。

Amazon RDS DB クラスターの削除保護が無効になっている

データベース削除保護は、データベースインスタンスの削除を防ぐのに役立つ機能です。削除保護を無効にすると、十分なアクセス許可を持つユーザーがデータベースを削除できるため、データ損失やアプリケーションのダウンタイムが発生する可能性があります。攻撃者はデータベースを削除し、サービスの中断、データ損失、復旧時間の増加につながる可能性があります。セキュリティのベストプラクティスに従って、RDS DB クラスターの削除保護を有効にして、悪意のある削除を防ぐことをお勧めします。

Amazon RDS DB クラスターの削除保護を有効にする

公開結果で、ハイパーリンクを使用してリソースを開きます。これにより、影響を受ける DB クラスターが開きます。

Amazon RDS DB インスタンスは、データベースエンジンのデフォルトポートを使用します。

データベースエンジンにデフォルトポートを使用する Amazon RDS インスタンスでは、これらのデフォルトポートが広く知られており、多くの場合、自動スキャンツールのターゲットになっているため、セキュリティリスクが増加する可能性があります。デフォルト以外のポートを使用するように DB インスタンスを変更すると、あいまいさによるセキュリティレイヤーが追加されるため、権限のないユーザーがデータベースに対して自動攻撃やターゲットを絞った攻撃を実行することが難しくなります。通常、デフォルトのポートは権限のない人物によってスキャンされ、DB インスタンスがターゲットになる可能性があります。セキュリティのベストプラクティスに従って、デフォルトポートをカスタムポートに変更して、自動攻撃やターゲットを絞った攻撃のリスクを減らすことをお勧めします。

公開結果で、ハイパーリンクを使用してリソースを開きます。これにより、影響を受ける DB インスタンスが開きます。

アプリケーション接続文字列を更新する

ポートを変更したら、Amazon RDS インスタンスに接続するすべてのアプリケーションとサービスを更新して、新しいポート番号を使用します。

Amazon RDS DB インスタンスはバックアッププランの対象ではありません

AWS Backup は、データのバックアップを一元化および自動化するフルマネージドバックアップサービスです AWS のサービス。DB インスタンスがバックアッププランの対象でない場合、悪意のある削除、データ破損、またはその他のデータ損失シナリオが発生した場合、データが失われるリスクがあります。ランサムウェア攻撃、データベーステーブルの削除、破損などの悪意のあるアクティビティが発生した場合、インシデントが発生する前の時点に復元できるため、インシデントからの復旧にかかる時間が短縮されます。セキュリティのベストプラクティスに従って、データ保護を確保するために Amazon RDS インスタンスをバックアッププランに含めることをお勧めします。

DB インスタンスのバックアッププランを作成して割り当てる

公開結果で、ハイパーリンクを使用してリソースを開きます。これにより、影響を受ける DB インスタンスが開きます。アプリケーションに最適なバックアップ頻度、保持期間、ライフサイクルルールを検討してください。

Amazon S3 バケットの露出の修正

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

AWS Security Hub は、Amazon Simple Storage Service (S3) バケットの公開結果を生成できます。

Security Hub コンソールでは、公開結果に関連する Amazon S3 バケットとその識別情報が、検出結果の詳細のリソースセクションに一覧表示されます。プログラムにより、Security Hub API の GetFindingsV2オペレーションを使用してリソースの詳細を取得できます。

露出検出結果に関連するリソースを特定したら、不要なリソースを削除できます。不要なリソースを削除すると、露出プロファイルと AWS コストを削減できます。リソースが不可欠な場合は、以下の推奨される修復手順に従ってリスクを軽減します。修復トピックは、特性のタイプに基づいて分割されます。

1 つの公開結果には、複数の修復トピックで特定された問題が含まれます。逆に、1 つの修復トピックだけに対処することで、露出の検出結果に対処し、その重要度レベルを下げることができます。リスク修復へのアプローチは、組織の要件とワークロードによって異なります。

> **Note**
>
> このトピックで提供される修復ガイダンスでは、他の AWS リソースで追加の相談が必要になる場合があります。

目次

- Amazon S3 バケットの設定ミス特性
  - Amazon S3 バケットのバージョニングが無効になっている
  - Amazon S3 バケットでオブジェクトロックが無効になっている
  - Amazon S3 バケットは保管時に AWS KMS キーで暗号化されません
  - バージョニングされた Amazon S3 バケットで多要素認証 (MFA) 削除が無効になっている
  - Amazon S3 バケットは、他の AWS アカウントのプリンシパルにバケットのアクセス許可の変更を許可します。
- Amazon S3 バケットの到達可能性特性

- Amazon S3 バケットにはパブリックアクセスがあります
- Amazon S3 バケットにはパブリック読み取りアクセスがあります
- Amazon S3 バケットには書き込みアクセス権があります
- Amazon S3 アクセスポイントでパブリックアクセス設定が有効になっている
- Amazon S3 バケットの機密データ特性
  - Amazon S3 バケットの機密データ特性

Amazon S3 バケットの設定ミス特性

Amazon S3 バケットの設定ミスの特徴と推奨される修復手順は次のとおりです。

Amazon S3 バケットのバージョニングが無効になっている

Amazon S3 バージョニングは、オブジェクトの複数のバリアントを同じバケットに保持するのに役立ちます。バージョニングを無効にすると、Amazon S3 は各オブジェクトの最新バージョンのみを保存します。つまり、オブジェクトが誤って、または悪意のある方法で削除または上書きされた場合、復元することはできません。バージョニングが有効なバケットは、データの不正な変更や削除が発生する可能性のある、偶発的な削除、アプリケーションの障害、ランサムウェア攻撃などのセキュリティインシデントに対する保護を提供します。セキュリティのベストプラクティスに従って、重要なデータを含むバケットに対してバージョニングを有効にすることをお勧めします。このデータが失われた場合、再作成は困難または不可能になります。

1. バージョニングを有効にする – バケットで Amazon S3 バージョニングを有効にするには、「Amazon Simple Storage Service ユーザーガイド」の「バケットでのバージョニングの有効化」を参照してください。バージョニングを有効にするときは、ストレージを管理するライフサイクルルールの実装を検討してください。バージョニングはオブジェクトの複数のコピーを保持するためです。

Amazon S3 バケットでオブジェクトロックが無効になっている

Amazon S3 オブジェクトロックは、Amazon S3 オブジェクトの write-once-read-many (WORM) モデルを提供し、一定期間または無期限に削除または上書きされるのを防ぎます。オブジェクトロックを無効にすると、オブジェクトがランサムウェアによる偶発的または悪意のある削除、変更、または暗号化に対して脆弱になる可能性があります。オブジェクトロックは、イミュータブルなデータストレージを要求する規制要件に準拠し、データの暗号化を試みる可能性のあるランサムウェアなどの高度な脅威から保護するために特に重要です。オブジェクトロックを有効にすると、データ保護の追加レイヤーとして保持ポリシーを適用し、重要なデータのイミュータブルなバックアップ戦略を作成で

きます。セキュリティのベストプラクティスに従って、オブジェクトの悪意のある変更を防ぐためにオブジェクトロックを有効にすることをお勧めします。

1. オブジェクトロックは新しいバケットの作成時にのみ有効にできるため、オブジェクトロックを有効にして新しいバケットを作成する必要があります。大規模な移行の場合は、バッチオペレーションを使用してオブジェクトを新しいバケットにコピーすることを検討してください。オブジェクトをロックする前に、バケットで Amazon S3 バージョニングとオブジェクトロックも有効にする必要があります。オブジェクトロックは新しいバケットでのみ有効にできるため、オブジェクトロックが有効になっている新しいバケットに既存のデータを移行する必要があります。Amazon S3 オブジェクトロックの設定 – バケットでオブジェクトロックを設定する方法については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3Object Lock ConfiguringAmazon」を参照してください。オブジェクトロックを設定したら、環境に応じて適切な保持モードを選択します。

Amazon S3 バケットは保管時に AWS KMS キーで暗号化されません

Amazon S3 は、Amazon S3 マネージドキーによるサーバー側の暗号化を、すべての新しいバケットのデフォルトの暗号化レベルとして適用します。Amazon S3 マネージドキーは強力な暗号化保護を提供しますが、 AWS Key Management Service キーと同じレベルのアクセスコントロールおよび監査機能を提供するわけではありません。KMS キーを使用する場合、オブジェクトへのアクセスには、Amazon S3 バケットとオブジェクトを暗号化した KMS キーの両方に対するアクセス許可が必要です。これは、暗号化されたオブジェクトにアクセスできるユーザーをきめ細かく制御し、暗号化キーの使用状況を包括的に監査する必要がある機密データにとって特に重要です。セキュリティのベストプラクティスに従って、KMS キーを使用して機密データを含むバケットを暗号化するか、厳格なコンプライアンス要件がある環境で使用することをお勧めします。

1. Amazon S3 バケットキーを設定する

   新しいオブジェクトに Amazon S3 バケットキーを使用するようにバケットを設定するには、「Amazon Simple Storage Service ユーザーガイド」の「SSE-KMS で Amazon S3 バケットキーを使用するようにバケットを設定する」を参照してください。既存のオブジェクトを暗号化する方法については、 AWS ストレージブログのAmazon S3バッチオペレーションによるオブジェクトの暗号化」を参照してください。

AWS KMS 暗号化を実装するときは、次の点を考慮してください。

- キー管理 – AWS マネージドキーとカスタマーマネージドキー (CMK) のどちらを使用するかを決定します。CMKsは、キーのライフサイクルと使用状況を完全に制御します。これら 2 種類の

キーの違いの詳細については、「 AWS Key Management Service デベロッパーガイド」のAWS「KMS キー」を参照してください。

- キーローテーション – 追加のセキュリティ対策として、KMS キーの自動キーローテーションを有効にします。詳細については、「 AWS Key Management Service デベロッパーガイド」の「自動キーローテーションを有効にする」を参照してください。

バージョニングされた Amazon S3 バケットで多要素認証 (MFA) 削除が無効になっている

多要素認証 (MFA) 削除は、Amazon S3 バケットのセキュリティを強化します。破壊的な Amazon S3 オペレーションには多要素認証が必要です。MFA 削除を無効にすると、適切なアクセス許可を持つユーザーは、追加の認証チャレンジなしで、バケットのオブジェクトバージョンを完全に削除したり、バージョニングを停止したりできます。MFA 削除を有効にすると、データの不正または偶発的な削除から保護し、ランサムウェア攻撃、内部脅威、運用エラーに対する保護を強化できます。MFA 削除は、不正な削除から保護する必要がある重要なデータやコンプライアンスに敏感なデータを含むバケットにとって特に重要です。セキュリティのベストプラクティスに従って、Amazon S3 バケットの MFA を有効にすることをお勧めします。

1. MFA タイプを確認する

   AWS は、次の MFA タイプをサポートしています。物理デバイスによる認証は通常、より厳格なセキュリティ保護を提供しますが、任意のタイプの MFA の使用は、MFA を無効にするよりも安全です。

2. リソースポリシーレベルで MFA を適用する

   バケットポリシーで `aws:MultiFactorAuthAge`条件キーを使用して、機密性の高いオペレーションに MFA を要求します。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「MFA の要求」を参照してください。

3. MFA を有効にする

   MFA 削除を有効にするには、まず Amazon S3 バケットでバージョニングが有効になっていることを確認します。MFA 削除は、バージョニングが有効になっているバケットでのみサポートされます。Amazon S3 バージョニングを有効にする方法については、「Amazon Simple Storage Service ユーザーガイド」の「バケットでのバージョニングの有効化」を参照してください。MFA 削除は Amazon S3 コンソールでは有効にできません。Amazon S3 API または を使用する必要があります AWS CLI。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「MFA 削除の設定」を参照してください。

Amazon S3 バケットは、他の AWS アカウントのプリンシパルにバケットのアクセス許可の変更を許可します。

Amazon S3 バケットポリシーは、バケットとオブジェクトへのアクセスを制御します。バケットポリシーが他の AWS アカウントのプリンシパルにバケットのアクセス許可の変更を許可する場合、権限のないユーザーはバケットを再設定できます。外部プリンシパル認証情報が侵害された場合、認証されていないユーザーはバケットを制御し、データ侵害やサービスの中断につながる可能性があります。標準のセキュリティ原則に従って、 AWS では、アクセス許可管理アクションを信頼できるプリンシパルのみに制限することをお勧めします。

1. バケットポリシーの確認と識別

   公開で、ARN フィールドで Amazon S3 バケットを識別します。Amazon S3 コンソールでバケットを選択し、アクセス許可タブに移動してバケットポリシーを確認します。バケットにアタッチされているアクセス許可ポリシーを確認します。プリンシパルステートメントで示されているように、 `s3:PutBucketPolicy`, `s3:PutBucketAcl`, `s3:DeleteBucketPolicy`, `s3:*` などのアクションを付与するポリシーステートメントや、アカウント外のプリンシパルへのアクセスを許可するポリシーステートメントを探します。

2. バケットポリシーを変更する

   バケットポリシーを変更して、他の AWS アカウントに付与されたアクションを削除または制限します。

   - 外部アカウントに許可管理アクションを付与するポリシーステートメントを削除します。
   - クロスアカウントアクセスが必要な場合は、広範なアクセス許可(`s3:*`)を、バケットアクセス許可管理を含まない特定のアクションに置き換えます。

   バケットポリシーの変更については、Amazon S3 ユーザーガイド」の「Amazon S3 コンソールを使用したバケットポリシーの追加」を参照してください。 Amazon S3

Amazon S3 バケットの到達可能性特性

Amazon S3 バケットの到達可能性特性と推奨される修復手順は次のとおりです。

Amazon S3 バケットにはパブリックアクセスがあります

デフォルトでは、Amazon S3 バケットとオブジェクトはプライベートですが、さまざまな設定で公開できます。バケットポリシー、アクセスポイントポリシー、またはオブジェクトのアクセス許可を変更してパブリックアクセスを許可すると、機密データが公開されるリスクがあります。

1. バケットを評価する

   組織のポリシー、コンプライアンス要件、またはデータ分類に基づいて、バケットをプライベートにできるかどうかを評価します。パブリックまたは他の にバケットアクセスを許可する予定がない場合は AWS アカウント、残りの修復手順に従ってください。

2. バケットをプライベートに設定する

   Amazon S3 バケットのプライベートアクセスを設定するには、次のいずれかのオプションを選択します。

   - アカウントレベル – アカウントレベルの設定を使用してアカウント内のすべてのバケットのパブリックアクセスをブロックするには、「Amazon Simple Storage Service ユーザーガイド」の「アカウントのパブリックアクセスブロックの設定」を参照してください。
   - バケットレベル – 特定のバケットのパブリックアクセスをブロックするには、yourAmazon S3buckets」を参照してください。
   - バケット ACL またはポリシー – バケットアクセスコントロールリスト (ACL)、バケットポリシー、マルチリージョンアクセスポイント (MRAP) ポリシー、またはアクセスポイントポリシーを変更してバケットへのパブリックアクセスを削除するには、Amazon Simple Storage Service ユーザーガイドの「バケットアクセスの確認と変更」を参照してください。アカウントレベルまたはバケットレベルでパブリックアクセスをブロックする場合、それらのブロックはパブリックアクセスを許可するポリシーよりも優先されます。

Amazon S3 バケットにはパブリック読み取りアクセスがあります

パブリック読み取りアクセスを持つ Amazon S3 バケットを使用すると、インターネット上のすべてのユーザーがバケットの内容を表示できます。これはパブリックにアクセス可能なウェブサイトまたは共有リソースで必要になる場合がありますが、バケットに機密データが含まれている場合、セキュリティリスクが発生する可能性があります。パブリック読み取りアクセスは、不正な表示とダウンロードにつながる可能性があり、機密データがそれらのバケットに保存されると、データ侵害につながる可能性があります。は、標準のセキュリティ原則に従って、Amazon S3 バケットへのアクセスを必要なユーザーとシステムに制限 AWS することをお勧めします。

1. バケットレベルでパブリックアクセスをブロックする

   Amazon S3 には、バケットポリシーや ACLs。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 ストレージへのパブリックアクセスをブロックする」を参照してください。パブリックアクセスをブロックしたら、バケットのアクセスコントロール設定を確認して、アクセス要件と一致していることを確認します。次に、Amazon S3 バケット

ポリシーを確認して、バケットにアクセスできるユーザーを明示的に定義します。バケットポリシーの例については、Amazon S3 バケットポリシーの例」を参照してください。

2. 代替アクセス方法

   パブリック読み取りアクセスが必要な場合は、次のより安全な代替方法を検討してください。

   - CloudFront – オリジンアクセスアイデンティティ (OAI) またはオリジンアクセスコントロール (OAC) で CloudFront を使用して、プライベート Amazon S3 バケットからの読み取りアクセスを許可します。別の方法として、Amazon S3 バケットへの直接アクセスを制限しながら、CloudFront を介してコンテンツをパブリックにアクセスできるようにします。詳細については、「Amazon Amazon S3オリジンへのアクセスの制限」を参照してください。 Amazon CloudFront
   - 署名付き URLs – 特定のオブジェクトへの一時的なアクセスには、署名付き URLs を使用します。詳細については、AWSAmazon S3Userユーザーガイドの URLs を使用したオブジェクトの共有」を参照してください。

Amazon S3 バケットには書き込みアクセス権があります

パブリック書き込みアクセスを持つ Amazon S3 バケットを使用すると、インターネット上のすべてのユーザーがバケット内のオブジェクトをアップロード、変更、または削除できます。これにより、悪意のあるファイルのアップロード、既存のファイルの変更、データの削除など、重大なセキュリティリスクが発生します。パブリック書き込みアクセスは、攻撃者が悪用する可能性のあるセキュリティの脆弱性を作成します。標準のセキュリティ原則に従って、 AWS は Amazon S3 バケットへの書き込みアクセスを必要なユーザーとシステムのみに制限することをお勧めします。

1. アカウントおよびバケットレベルでパブリックアクセスをブロックする

   Amazon S3 には、バケットポリシーや ACLs。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 ストレージへのパブリックアクセスをブロックする」を参照してください。

2. バケットポリシーの変更

   パブリック書き込みアクセスを削除するより詳細なアプローチについては、バケットポリシーを確認してください。`s3:PutObject`、、`s3:DeleteObject`または を検索できます`s3:*`。バケットポリシーの管理の詳細については、Amazon Simple Storage Service ユーザーガイドの「Amazon Amazon S3のバケットポリシー」を参照してください。

3. 代替アクセス方法 パブリック読み取りアクセスが必要な場合は、次のより安全な代替方法を検討してください。

- CloudFront – オリジンアクセスアイデンティティ (OAI) またはオリジンアクセスコントロール (OAC) で CloudFront を使用して、プライベート Amazon S3 バケットからの読み取りアクセスを許可します。別の方法として、Amazon S3 バケットへの直接アクセスを制限しながら、CloudFront を介してコンテンツをパブリックにアクセスできるようにします。詳細については、「Amazon CloudFront デベロッパーガイド」の「Restricting access to an Amazon S3 origin」(Amazon S3 オリジンへのアクセスを制限する) を参照してください。
- 署名付き URLs – 特定のオブジェクトへの一時的なアクセスには、署名付き URLs を使用します。詳細については、「Amazon Simple Storage Service ユーザーガイド」のURLs を使用したオブジェクトの共有」を参照してください。

Amazon S3 アクセスポイントでパブリックアクセス設定が有効になっている

Amazon S3 アクセスポイントは、Amazon S3 バケット内の共有データセットへのカスタマイズされたアクセスを提供します。アクセスポイントのパブリックアクセスを有効にすると、インターネット上の誰でもデータにアクセスできます。は、標準のセキュリティ原則に従って、Amazon S3 アクセスポイントへのパブリックアクセスを制限することを AWS 推奨しています。

1. パブリックアクセスブロックを有効にして新しいアクセスポイントを作成する

   Amazon S3 では、アクセスポイントの作成後にアクセスポイントのパブリックアクセス設定を変更することはできません。アクセスポイントの作成の詳細については、Amazon S3 ユーザーガイド」の「汎用バケットのアクセスポイントへのパブリックアクセスの管理」を参照してください。アクセスポイントへのパブリックアクセスの管理の詳細については、Amazon S3 ユーザーガイド」の「汎用バケットのアクセスポイントの作成」を参照してください。

Amazon S3 バケットの機密データ特性

Amazon S3 バケットの機密データ特性と推奨される修復手順は次のとおりです。

Amazon S3 バケットの機密データ特性

Macie が Amazon S3 バケット内の機密データを識別すると、即時の対応が必要な潜在的なセキュリティとコンプライアンスの露出を示します。

機密データには以下が含まれます。

- 認証情報
- 個人を特定できる情報

- 財務情報
- 保護が必要な機密コンテンツ

機密データが設定ミスや不正アクセスによって公開されると、コンプライアンス違反、データ侵害、なりすまし窃盗、または財務上の損失につながる可能性があります。セキュリティのベストプラクティスに従って、 は Amazon S3 バケット内のデータの適切な分類と機密データの継続的なモニタリング AWS を推奨します。

機密データのコントロールを実装する

露出の検出結果で、Open リソース を選択します。検出された機密データのタイプとバケット内の場所を確認します。Macie の検出結果の解釈については、Amazon Macie Macie ユーザーガイド」の「Macie の検出結果のタイプ」を参照してください。

検出された機密データのタイプに基づいて、適切なセキュリティコントロールを実装します。

- バケットへのアクセスを制限する – バケットのアクセス許可を確認して、最小特権の原則に従っていることを確認します。IAM ポリシー、バケットポリシー、および ACLsを使用してアクセスを制限します。詳細については、Amazon S3 Identity and Access Management」を参照してください。
- サーバー側の暗号化を有効にする – KMS キーによるサーバー側の暗号化を有効にして、保護を強化します。詳細については、Amazon Simple Storage Service ユーザーガイド AWS の「KMS キーによるサーバー側の暗号化の使用 (SSE-KMS)」を参照してください。
- Use AWS Glue DataBrew – データの準備とクリーニングGlue DataBrewに使用します。詳細については、「 AWS Glue DataBrew デベロッパーガイド」の「 とは AWS Glue DataBrew」を参照してください。

Security Hub での攻撃シーケンスの検出結果

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

攻撃シーケンスは、セキュリティ上の脅威の一種です。GuardDuty は、イベントが疑わしいアクティビティのパターンと一致すると、攻撃シーケンスの検出結果を生成します。GuardDuty を有効にすると、Security Hub コンソールでこのタイプの検出結果にアクセスできます。これにより、コン

ソールを切り替えることなく、すべてのセキュリティ脅威を調査および修正できます。Security Hub コンソールの脅威画面から攻撃シーケンスの検出結果を確認できます。

攻撃シーケンスの検出結果の確認

> **Note**
> Security Hub はプレビューリリースであり、変更される可能性があります。

Security Hub コンソールの脅威画面から攻撃シーケンスの検出結果を確認できます。次のトピックでは、攻撃シーケンスの検出結果の詳細を確認する方法について説明します。

攻撃シーケンスの検出結果の詳細の確認

> **Note**
> Security Hub はプレビューリリースであり、変更される可能性があります。

このトピックでは、Security Hub コンソールと API で攻撃シーケンスの検出結果の詳細を確認する方法について説明します。

Security Hub コンソールでの攻撃シーケンスの詳細の確認

以下に、Security Hub コンソールで攻撃シーケンスの詳細を確認する方法について説明します。

コンソールで攻撃シーケンスの検出結果を確認するには

1. 認証情報を使用してサインインし、https://console.aws.amazon.com/securityhub/v2/home?region=us-east-1 で Security Hub コンソールを開きます。
2. ナビゲーションペインから、脅威を選択します。
3. 攻撃シーケンスの検出結果のリストから、詳細を表示する攻撃シーケンスの検出結果を選択します。

API を使用した攻撃シーケンスの検出結果の詳細の確認

`GetFindingsV2` API または を使用して、攻撃シーケンスの検出結果を確認できます AWS CLI。アタックシーケンスの結果のみを返す`TTPs/AttackSequence`場合は、

FindingProviderFieldsパラメータと のフィルター値を指定して結果をフィルタリングできます。他のフィールドでフィルタリングして結果を絞り込むことができます。

コマンドの例

以下は、アカウントで最近生成された 10 件の攻撃シーケンスの検出結果を取得する AWS CLI 例です。この例は Linux、macOS、Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ文字 (\) が使用されます。

```
$ aws securityhub get-findings-v2 \
--filters '{"FindingProviderFieldsTypes":[{"Value": "TTPs/
AttackSequence","Comparison":"PREFIX"}]}' \
--sort-criteria '{ "Field": "LastObservedAt", "SortOrder": "desc"}' \
--max-items 10
```

攻撃シーケンスの検出結果の修正

> **Note**
> Security Hub はプレビューリリースであり、変更される可能性があります。

攻撃シーケンスの検出結果の修正については、「Amazon GuardDuty ユーザーガイド」の「検出された GuardDuty セキュリティの検出結果の修正」を参照してください。 Amazon GuardDuty

Security Hub のオートメーションルール

> **Note**
> Security Hub はプレビューリリースであり、変更される可能性があります。

Security Hub オートメーションルールは、Security Hub CSPM オートメーションルールのより拡張可能で設定可能なバージョンです。Security Hub は、検出結果固有の自動化システムからより広範な設定プラットフォームに進化しました。Security Hub CSPM は ASFF をサポートしていますが、Security Hub は OCSF のサポートを導入し、より多くの設定の基盤を確立します。Security Hub の自動化ルールの主な機能の 1 つは、アグリゲータ設定との統合です。これにより、リンクされていないリージョンエクスペリエンスを AWS リージョン 1 つずつ柔軟にセットアップ AWS リージョン しながら、リンクされたセットに設定を微調整してきめ細かくデプロイできます。

オートメーションルール AWS リージョン、コネクタ、アグリゲータなど、 AWS アカウント および の Security Hub リソースは、以下のシナリオでは機能しなくなります。

- スタンドアロン が委任された管理者を持つ AWS 組織のメンバー AWS アカウント になる
- AWS 組織管理アカウントは、組織の委任管理者を削除し、新しい委任管理者を設定します。
- 委任管理者またはスタンドアロンのアグリゲータ設定 AWS アカウント が変更され、リンクされていないリージョンがリンクされたリージョンになります。

これらのシナリオでは、メンバーアカウントは AWS CLI でのみこれらのリソースをリスト、取得、削除オペレーションで管理できます。リンクされていないリージョンがリンクされたリージョンにされた場合でも、委任された管理者アカウントまたはスタンドアロン AWS アカウントは、リスト、取得、削除オペレーションを通じて、リンクされたリージョン内の古いリソースを管理できます。

主な機能強化

Security Hub CSPM の自動化ルールはリージョン別であり、作成された AWS リージョン の検出結果にのみ適用されます。Security Hub のオートメーションルールは、 AWS リージョン （アグリゲーションリージョン) で 1 回設定し、アグリゲータ V2 設定を介してすべての設定済み AWS リージョン （リンクされたリージョン) に適用できます。この機能の利点の 1 つは、セキュリティ検出結果をセットアップ AWS リージョン するだけで、複数の で自動化および修復できることです AWS リージョン。つまり、リンクされたリージョンで結果が生成された場合、集約リージョンの設定に基づいて自動的に修正できます。

外部統合

Security Hub のオートメーションルールは、ITSM チケット作成のアクションタイプをサポートしています。これにより、選択した OCSF の検出結果を 1 つ以上の設定された ITSM 統合に直接ルーティングできます。OCSF の検出結果が条件に一致する場合は、 Jira Cloudまたは でチケットを作成できますServiceNow ITSM。詳細については、「Security Hub のサードパーティー統合」を参照してください。

OCSF でサポートされている基準

Security Hub CSPM は、Security Hub が OCSF フィールドと一致する間、検出結果の ASFF フィールドの評価をサポートします。たとえば、V2 自動化ルールで使用される `Criteria`パラメータでサポートされているフィルターのセットは、 で使用される `Criteria`パラメータでサポートされているフィルターのセットと一致します`GetFindingsV2`。つまり、V2 の検出結果の取得に使用されるフィルターは、検出結果に一致する V2 自動化ルールで使用できます。

の OCSF フィールド AutomationRulesFindingFieldsUpdate

Security Hub CSPM AutomationRulesFindingFieldsUpdateで を更新できるフィールドのリストが Security Hub で変更されました。更新できるフィールドAutomationRulesFindingFieldsUpdateV2のリストには、以下が含まれます。

- Comment
- SeverityId
- StatusId

Security Hub のサードパーティー統合

> **Note**
> Security Hub はプレビューリリースであり、変更される可能性があります。

AWS Security Hub のサードパーティー統合により、セキュリティ体制を強化できます。この機能を使用すると、Security Hub からの結果を消費する統合を有効にし、Security Hub に運用、調査、対応ツールを組み込むことができます。現在、Security Hub は Jira Cloudおよび との統合をサポートしていますServiceNow。

認証情報を暗号化する KMS キーを作成する

このセクションの統合手順では、 AWS 所有キーまたはカスタマーマネージドキーを使用して認証情報を暗号化するオプションを提供します。 AWS 所有キーは、認証情報を暗号化する AWS サービスが KMS キーを所有および管理 AWS アカウント するため、 にない KMS キーです。認証情報の暗号化に使用される KMS キーを完全に制御する場合は、カスタマーマネージドキーを作成します。カスタマーマネージドキーは、所有および管理している KMS キーです。

Security Hub 暗号化オペレーションアクセス

このポリシーステートメントにより、Security Hub は暗号化オペレーションに AWS KMS キーを使用できます。これにより、Security Hub は、このキーを使用してクライアントシークレットを保護することができます。アクセス許可は、ソース ARN と暗号化コンテキストをチェックする条件ブロックを介して、特定の Security Hub コネクタに関連するオペレーションに制限されます。

```
{
```

```
    "Sid": "Allow Security Hub access to the customer managed key",
    "Effect": "Allow",
    "Principal": {
        "Service": "connector.securityhub.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:ReEncrypt*"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:securityhub:${Region}:${AccountId}:connectorv2/*"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:securityhub:connectorV2Arn":
 "arn:aws:securityhub:${Region}:${AccountId}:connectorv2/*",
            "kms:EncryptionContext:aws:securityhub:providerName":
 "${CloudProviderName}"
        }
    }
}
```

> **Note**
>
> *CloudProviderName* には、 JIRA_CLOUDまたは と入力しますSERVICENOW。*Region* と *AccountId* には、 AWS リージョン と AWS アカウント ID を入力します。

Security Hub キーの読み取りアクセス

このポリシーステートメントにより、Security Hub は DescribeKeyオペレーションを許可して KMS キーに関するメタデータを読み取ることができます。このアクセス許可は、Security Hub がキーのステータスと設定を検証するために必要です。アクセスは、ソース ARN 条件を通じて特定の Security Hub コネクタに制限されます。

```
{
    "Sid": "Allow Security Hub read access to the customer managed key",
    "Effect": "Allow",
    "Principal": {
        "Service": "connector.securityhub.amazonaws.com"
```

```
    },
    "Action": [
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:securityhub:${Region}:${AccountId}:connectorv2/*"
        }
    }
}
```

> **Note**
>
> *Region* と *AccountId* には、 AWS リージョン と AWS アカウント ID を入力します。

Security Hub オペレーションの IAM プリンシパルアクセス

このポリシーステートメントは、指定された IAM ロールに、CreateConnectorV2 および CreateTicketV2 APIs。条件により、これらのオペレーションは指定されたリージョンの Security Hub サービスを介してのみ実行できます。

```
{
    "Sid": "Allow permissions to access key through Security Hub",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::${AccountId}:role/${RoleName}"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:ReEncrypt*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": [
                "securityhub.${Region}.amazonaws.com"
            ]
        },
        StringLike": {
```

```
            "kms:EncryptionContext:aws:securityhub:providerName": "SERVICENOW"
        }
    }
}

{
    "Sid": "Allow read permissions to access key through Security Hub",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::${AccountId}:role/${RoleName}"
    },
    "Action": [
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": [
                "securityhub.${Region}.amazonaws.com"
            ]
        }
    }
}
```

> **Note**
>
> *RoleName* には、Security Hub を呼び出す IAM ロールの名前を入力します。*Region* と *AccountId* には、 AWS リージョン と AWS アカウント ID を入力します。

AWS Security Hub の統合 Jira Cloud

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

このトピックでは、Security Hub コンソールにアクセスして の統合を設定する方法について説明しますJira Cloud。このトピックの手順を完了する前に、Jira Cloudサブスクリプションプランを購入す

る必要があります。サブスクリプションプランの詳細については、 Atlassianウェブサイトの「料金表」を参照してください。

組織内のアカウントでは、委任された管理者のみが統合を設定できます。委任管理者は、メンバーアカウントの調査結果にチケット作成機能を手動で使用できます。さらに、委任管理者は自動化ルールを使用して、メンバーアカウントに関連付けられた検出結果のチケットを自動的に作成できます。自動化ルールを定義する場合、委任管理者はすべてのメンバーアカウントまたは特定のメンバーアカウントを含む条件を設定できます。委任管理者の設定については、Security Hub の「委任管理者アカウントの設定」を参照してください。

組織内にないアカウントでは、この機能のすべての側面を使用できます。

前提条件

の統合を設定する前に、次の前提条件を満たす必要がありますJira Cloud。そうしないと、 Jira Cloudと Security Hub の統合は機能しません。

1. AWS Security Hub for Jira Cloudアプリをインストールする

次の手順では、アプリをインストールする方法について説明します。

1. 管理者としてAtlassianサイトにサインインします。
2. 設定 を選択し、アプリ を選択します。
3. マーケットプレイスページが表示されたら、「新しいアプリの検索」を選択します。アプリページに移動した場合は、アプリを探索を選択し、AWS Security Hub for Jira Cloudを検索します。次に、今すぐ取得を選択します。

2. プロジェクトを作成する

このステップは、プロジェクトを作成していない場合に必要です。プロジェクトの作成方法については、 Jira Cloud Supportドキュメントの「新しいプロジェクトを作成する」を参照してください。

プロジェクトを作成するための要件

新しいプロジェクトを作成するときは、必ず以下を実行してください。

- プロジェクトテンプレートのソフトウェア開発を選択します。
- プロジェクトタイプの会社管理を選択します。

- プロジェクトキーを書き留めます。

3. Jira Cloud アプリケーション用の AWS Security Hub にソフトウェア開発プロジェクトを追加する

次の手順では、Jira Cloudアプリケーション用 Security Hub にソフトウェア開発プロジェクトを追加する方法について説明します。

1. 管理者としてAtlassianサイトにサインインします。
2. 設定 を選択し、アプリ を選択します。
3. アプリケーションのリストから、AWS Security Hub for Jira Cloud を選択します。
4. コネクタ設定タブを選択します。
5. 有効なプロジェクト で、Jira プロジェクトの追加 を選択します。
   a. ドロップダウンから、すべて追加を選択するか、プロジェクトを選択します。複数のプロジェクトを追加するが、すべてのプロジェクトを追加するわけではない場合は、このステップを繰り返します。
   b. [保存] を選択します。

Installation Manager タブから、正常にインストールされたプロジェクトを確認できます。Installation Manager タブからフィールド、画面、ステータス、ワークフローの設定を確認することもできます。

> **Note**
> Installation Manager タブを選択すると、選択したすべてのプロジェクトが正常にインストールされたことを確認できます。

の詳細についてはJira Cloud、 Altlassianウェブサイトの「 Jira Cloudリソース」を参照してください。

レコメンデーション

以下は、 の統合を設定する前に考慮すべき推奨事項ですJira Cloud。

- で専用システムアカウントを作成しますJira Cloud。
- Jira Cloud インスタンスごとに 1 つのシステムアカウントを使用します。

の統合を設定する Jira Cloud

Security Hub は自動的に で問題を作成しますJira Cloud.。この統合により、Security Hub の検出結果を に送信できるためJira Cloud、運用ワークフローの一部として管理できます。たとえば、調査と修復が必要な問題に所有権を割り当てることができます。Security Hub の検出結果を送信するJira Cloudプロジェクトごとに、次の手順を完了する必要があります。

> **Note**
>
> Jira Cloud コネクタを作成すると、現在の から AWS リージョン にリダイレクトされるため`"https://3rdp.oauth.console.api.aws"`、コネクタの登録を完了できます。その後、コネクタ AWS リージョン が作成される に戻ります。

の統合を設定するには Jira Cloud

1. 認証情報を使用して AWS アカウントにサインインし、https://console.aws.amazon.com/securityhub/v2/home?region=us-east-1 で Security Hub コンソールを開きます。
2. ナビゲーションペインから、管理を選択し、統合を選択します。
3. [Add]Jira Cloud (追加) を選択します。
4. 詳細 には、統合の一意のわかりやすい名前を入力し、統合のオプションの説明を入力するかどうかを決定します。
5. セキュリティ設定では、Security Hub でJira Cloud認証情報を暗号化する方法を決定します。サービス所有キーを選択した場合、 AWS 所有キーを使用してデータを暗号化します。カスタマイズされたキーを選択した場合は、既存のカスタマイズされたキーの ARN を入力するか、キーの作成を選択して新しい AWS KMS キーを作成する必要があります。KMS キーの作成方法については、「対称暗号化 KMS キーの作成」を参照してください。

   > **Note**
   >
   > この設定を完了すると、これらの設定を変更することはできません。ただし、カスタマイズキーを選択した場合、カスタマイズしたキーポリシーはいつでも編集できます。

6. (オプション) タグの場合は、タグを作成して統合に追加します。最大 50 個のタグを追加できます。

7. 認可で、コネクタの作成と認可を選択します。ポップアップが表示され、承認の完了を許可するを選択します。認可が完了すると、認可が成功したことを通知するチェックボックスが表示されます。
8. 設定 にプロジェクト Jira Cloud ID を入力します。
9. 設定の完了 を選択します。設定が完了したら、設定済み統合タブで設定済み統合を表示できます。

Jira Cloud 統合のチケットの作成

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

との統合を作成したらJira Cloud、検出結果のチケットを作成できます。

> **Note**
>
> 検出結果は、ライフサイクル全体で常に 1 つのチケットに関連付けられます。最初の作成後の結果に対するそれ以降のすべての更新は、同じチケットに送信されます。自動化ルールに関連付けられたコネクタが変更された場合、更新されたコネクタは、ルール基準に一致する新規および受信の検出結果にのみ使用されます。

検出結果のチケットを作成するには

1. 認証情報を使用して AWS アカウントにサインインし、https://console.aws.amazon.com/securityhub/v2/home?region=us-east-1 で Security Hub コンソールを開きます。
2. ナビゲーションペインのインベントリで、検出結果を選択します。
3. 検出結果を選択します。検出結果で、チケットの作成を選択します。
4. 統合 でドロップダウンメニューを開き、統合を選択します。この統合は、Jira Cloudプロジェクトを設定したときに以前に作成した統合です。検出結果を送信する統合を選択します。
5. [作成] を選択します。

Jira Cloud 統合のチケットの表示

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

検出結果のチケットを作成したら、Jira Cloudインスタンスでチケットを開くことができます。

Jira Cloud インスタンスで結果を表示するには

1. 認証情報を使用して AWS アカウントにサインインし、https://console.aws.amazon.com/securityhub/v2/home?region=us-east-1 で Security Hub コンソールを開きます。
2. ナビゲーションペインのインベントリで、検出結果を選択します。
3. チケットを作成した結果を選択します。
4. 結果で、チケット ID を選択してJira Cloudインスタンスのチケットを表示するか、JSON を表示します。

の統合 ServiceNow

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

このトピックでは、Security Hub コンソールにアクセスして の統合を設定する方法について説明しますServiceNow ITSM。このトピックの手順を完了する前に、この統合を追加するServiceNow ITSM前に へのサブスクリプションが必要です。詳細については、 ServiceNowウェブサイトの料金ページを参照してください。

組織内のアカウントでは、委任された管理者のみが統合を設定できます。委任管理者は、メンバーアカウントの結果にチケット作成機能を手動で使用できます。さらに、委任管理者は自動化ルールを使用して、メンバーアカウントに関連付けられた検出結果のチケットを自動的に作成できます。自動化ルールを定義する場合、委任管理者はすべてのメンバーアカウントまたは特定のメンバーアカウントを含む条件を設定できます。委任管理者の設定については、Security Hub の「委任管理者アカウントの設定」を参照してください。

組織内にないアカウントでは、この機能のすべての側面を使用できます。

前提条件

の統合を設定する前に、次の前提条件を満たす必要がありますServiceNow ITSM。そうしないと、ServiceNow ITSMと Security Hub の統合は機能しません。

1. IT Service Management (ITSM) 用の Security Hubfindings 統合をインストールする

次の手順では、Security Hub プラグインをインストールする方法について説明します。

1. ServiceNow ITSM インスタンスにサインインし、アプリケーションナビゲーターを開きます。
2. ServiceNow ストアに移動します。
3. IT Service Management (ITSM) の Security Hub の検出結果統合を検索し、Get を選択してアプリケーションをインストールします。

> **Note**
>
> Security Hub アプリケーションの設定で、新しい Security Hub の検出結果がServiceNow ITSM環境に送信されたときに実行するアクションを選択します。Do nothing、Create incident、Create problem、またはその両方 (incident/problem

2. インバウンド OAuth リクエストのクライアント認証情報許可タイプを設定する

このグラントタイプは、インバウンド OAuth リクエスト用に設定する必要があります。詳細については、「 サポートウェブページ」の「インバウンド OAuth のクライアント認証情報付与タイプがサポートされています」を参照してください。 ServiceNow

3. OAuth アプリケーションの作成

OAuth アプリケーションを作成済みの場合は、この前提条件をスキップできます。OAuth アプリケーションの作成については、OAuth のセットアップ」を参照してください。

の統合を設定する ServiceNow ITSM

Security Hub は、 でインシデントまたは問題を自動的に作成できますServiceNow ITSM。

の統合を設定するには ServiceNow ITSM

1. 認証情報を使用して AWS アカウントにサインインし、https://console.aws.amazon.com/securityhub/v2/home?region=us-east-1 で Security Hub コンソールを開きます。

2. ナビゲーションペインから、管理を選択し、統合を選択します。
3. でServiceNow ITSM、統合の追加を選択します。
4. 詳細 には、統合の名前を入力し、統合のオプションの説明を入力するかどうかを決定します。
5. セキュリティ設定では、Security Hub でJira Cloud認証情報を暗号化する方法を決定します。サービス所有キーを選択した場合、 AWS 所有キーを使用してデータを暗号化します。カスタマイズされたキーを選択した場合は、既存のカスタマイズされたキーの ARN を入力するか、キーの作成を選択して新しい AWS KMS キーを作成する必要があります。KMS キーの作成方法については、「対称暗号化 KMS キーの作成」を参照してください。

   > **Note**
   > この設定を完了すると、これらの設定を変更することはできません。ただし、カスタマイズキーを選択した場合、カスタマイズしたキーポリシーはいつでも編集できます。

6. 認可には、ServiceNow ITSMURL、クライアント ID、クライアントシークレットを入力します。
7. タグ では、統合にオプションのタグを作成して追加するかどうかを決定します。
8. 設定の完了 を選択します。設定が完了したら、設定済み統合タブで設定済み統合を表示できます。

ServiceNow ITSM 統合のチケットの作成

> **Note**
> Security Hub はプレビューリリースであり、変更される可能性があります。

との統合を作成したらServiceNow ITSM、検出結果のチケットを作成できます。

> **Note**
> 検出結果は、ライフサイクル全体で常に 1 つのチケットに関連付けられます。最初の作成後の結果に対するそれ以降のすべての更新は、同じチケットに送信されます。自動化ルールに関連付けられたコネクタが変更された場合、更新されたコネクタは、ルール条件に一致する新規および受信の検出結果にのみ使用されます。

検出結果のチケットを作成するには

1. 認証情報を使用して AWS アカウントにサインインし、https://console.aws.amazon.com/securityhub/v2/home?region=us-east-1 で Security Hub コンソールを開きます。
2. ナビゲーションペインのインベントリで、検出結果を選択します。
3. 検出結果を選択します。検出結果で、チケットの作成を選択します。
4. 統合 でドロップダウンメニューを開き、統合を選択します。
5. [作成] を選択します。

ServiceNow ITSM 統合のチケットの表示

> **Note**
> Security Hub はプレビューリリースであり、変更される可能性があります。

検出結果のチケットを作成したら、ServiceNow ITSMインスタンスでチケットを開くことができます。

ServiceNow ITSM インスタンスで検出結果を表示するには

1. 認証情報を使用して AWS アカウントにサインインし、https://console.aws.amazon.com/securityhub/v2/home?region=us-east-1 で Security Hub コンソールを開きます。
2. ナビゲーションペインのインベントリで、検出結果を選択します。
3. チケットを作成した結果を選択します。
4. 結果で、チケット ID を選択してServiceNow ITSMインスタンスのチケットを表示するか、JSON を表示します。

Security Hub の概要ダッシュボードの操作

> **Note**
> Security Hub はプレビューリリースであり、変更される可能性があります。

このトピックでは、Security Hub コンソールの概要ダッシュボードについて説明します。このページでは、複数のセキュリティウィジェットにわたる露出、脅威、上位リソース、セキュリティサービスカバレッジの概要を示します。これらのウィジェットは、セキュリティ機能別に重要度とアカウント別に露出と脅威を視覚化するのに役立ちます。このページを開くたびに、データは自動的に更新されます。

このページをカスタマイズするには、さまざまなセキュリティウィジェットを追加および削除し、フィルター条件を設定して各ウィジェット内の特定のデータを取得します。このページのカスタマイズは、今後の使用のために保存されます。アカウントが組織の委任管理者アカウントである場合、カスタマイズはメンバーアカウントのカスタマイズとは別に保存されます。

> **Note**
>
> 保存されたフィルター、カスタムウィジェット、またはその他の関連する自由形式のテキストフィールドに、機密、機密、または個人を特定できる情報 (PII) を含めないことをお勧めします。

アカウントが組織の委任管理者アカウントである場合、データにはアカウントとメンバーアカウントの結果が含まれます。アカウントがメンバーアカウントまたはスタンドアロンアカウントの場合、データにはアカウントの結果のみが含まれます。Security Hub でクロスリージョン集約を設定すると、このページには集約の結果が表示されます。

公開概要ウィジェット

このウィジェットには、すべての露出が重要度別に表示されます。環境内の各露出の頻度を確認できます。重要度が高い露出が最初に表示されます。エクスポージャーは、Security Hub や Amazon Inspector AWS のサービスなどの他の の検出結果と特性の分析に基づいています。このウィジェットの露出のリストは、重要な検出結果の数が最も多い 8 つの最も高い露出に制限されています。2 つ以上の露出に同じ数の重要な検出結果がある場合、リストはより最近の重要な検出結果の背後にある検出結果を自動的にグループ化します。

脅威の概要ウィジェット

このウィジェットには、すべての脅威が重要度別に表示されます。重要度の高い脅威が最初に表示されます。脅威は一連のイベントに関連しており、環境内の潜在的な脅威を特定します。また、GuardDuty を起点としています。このウィジェットの脅威のリストは、重要度が最も高い 8 つの脅威に限定されます。2 つ以上の脅威の重要度が同じ場合、リストはより最近の検出結果の背後に

ある検出結果を自動的にグループ化します。このウィジェットでデータを受信するには、GuardDuty を有効にする必要があります。

セキュリティカバレッジウィジェット

このウィジェットは、セキュリティカバレッジの概要を示し、サポートされているサービスのカバレッジ結果に基づいています。合格、不合格、または使用できないカバレッジチェックが表示されます。利用不可は、カバレッジチェックを完了できないことを示します。これは、削除されたリソースまたはサーバー障害が原因である可能性があります。

カバレッジチェックの割合は、合格と不合格のチェックの数を示します。たとえば、1 つのカバレッジチェックが成功し、1 つのカバレッジチェックが失敗します。これは、50% のチェックが成功し、50% のチェックが失敗したことを示します。場合によっては、パーセンテージは最も近い整数に四捨五入されます。

GuardDuty、Amazon Inspector、Macie などのセキュリティサービスとは異なり、Security Hub CSPM はアカウントごとに 1 つのカバレッジ検出結果を発行します。これは、少なくとも 1 つの標準が有効になっている場合の PASS など、有効な標準に応じて PASS/FAIL です。Security Hub CSPM のカバレッジ率は、Security Hub CSPM カバレッジの検出結果の総数に渡された Security Hub CSPM カバレッジの検出結果の数です。

> **Note**
>
> 保存されたフィルター、カスタムウィジェット、またはその他の関連する自由形式のテキストフィールドに、機密、機密、または個人を特定できる情報 (PII) を含めないことをお勧めします。

Security Hub でのリソースの詳細の表示

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

リソースページは、アカウント全体の一般的なリソースを追跡します。Security Hub コンソールのリソースページにアクセスするには、ナビゲーションペインのリソースを選択します。リソースタイプを選択すると、リソースタイプに関連付けられているすべてのリソースを確認できます。リソースに関連付けられている検出結果を確認できます。

> **Note**
>
> 委任管理者は、メンバーアカウントに関連付けられているすべてのリソースを表示できます。ホームを設定した場合は AWS リージョン、リンクされた AWS リージョン からホーム内のすべてのリソースを表示できます AWS リージョン。

リソースを選択すると、そのリソースの詳細を確認できます。これらの詳細には、リソース名、ID、ARN、タイプ、カテゴリが含まれます。リソースに関連付けられたアカウント ID、リソースが作成された日時 (タイムスタンプ) 、リソースが作成された場所 () を確認できますAWS リージョン。コピーできる JSON スニペットで追加の詳細を確認することもできます。

概要タブから検出結果タブに切り替えると、リソースに関連付けられている検出結果を確認できます。検出結果タブには、各検出結果の名前、各検出結果のタイプ、各検出結果の重要度が表示されます。検出結果を異なるフィールドでグループ化し、フィルターを使用して検出結果を検索できます。検出結果を選択した場合は、検出結果の概要を確認できます。これには、コンプライアンスに関する情報と、検出結果に関連する問題の修正方法が含まれます。リソースに戻る場合は、リソースを開くを選択して、リソースタイプのコンソールでリソースを確認できます。たとえば、リソースが IAM リソースの場合、IAM コンソールでリソースを開くことができます。

リソースページには、リソースを整理および検索するさまざまな方法が用意されています。リソースはタイプ別にグループ化できます。たとえば、アカウント ID、検出結果タイプ、リソースカテゴリ AWS リージョン、リソース名、リソースタイプでリソースをグループ化できます。フィルターを使用して検出結果を検索できます。クイックフィルターは、カテゴリ、アカウント、検出結果タイプ別にリソースを確認するのに役立ちます。

リソースページの利点は、セキュリティ体制のモニタリング、リソースの整理、リソースの詳細の確認に役立つことです。

潜在的な攻撃パスグラフを使用した Security Hub での公開の表示

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

潜在的な攻撃パスグラフは、潜在的な攻撃者が公開結果に関連するリソースにアクセスして制御する方法を示すインタラクティブな視覚化です。このグラフには、Security Hub コンソールと Exposures

画面からのみアクセスできます。露出検出結果の詳細を表示すると、概要タブには潜在的な攻撃パスと呼ばれるセクションが含まれます。

概要タブのこのセクションでは、潜在的な攻撃パスグラフで AWS リソースを選択してドラッグできます。ズームインアイコンとズームアウトアイコンを使用して、攻撃パスグラフの特定領域に集中できます。全画面表示アイコンを使用して、全画面表示モードの内外で攻撃パスグラフを展開できます。凡例は、プライマリリソース、関連リソース、寄与する特性数を色別にコードし、攻撃パスグラフに特性カテゴリと特性の数を表示します。リソースの詳細を表示するには、リソースを選択し、リソースの詳細を表示を選択します。リソースに関連付けられた ID と AWS アカウント 番号をコピーすることもできます。到達可能性特性を持つ露出の検出結果は、パブリックインターネットと折りたたまれたネットワークパスを攻撃パスグラフに表示します。この詳細を表示するには、折りたたまれたネットワークパスノードを選択します。

Security Hub を無効にする

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

アカウントが組織の一部でない場合は、Security Hub コンソールで Security Hub をいつでも無効にできます。Security Hub を無効にすると、 は結果の取り込みを停止します。また、既存の検出結果と設定にアクセスできなくなります。次の手順では、Security Hub を無効にする方法について説明します。

Security Hub を無効にするには

1. 認証情報を使用して AWS アカウントにサインインし、https://console.aws.amazon.com/securityhub/v2/home で Security Hub コンソールを開きます。
2. ナビゲーションペインから、全般を選択します。
3. Security Hub で、Disable を選択します。ポップアップウィンドウで、Disable と入力し、Disable を選択します。

AWS Security Hub CSPM の概要

AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM) は、 のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスに照らして AWS 環境を評価するのに役立ちます。

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

組織のセキュリティ状態を管理するために、Security Hub CSPM は複数のセキュリティ標準をサポートしています。これには AWS、 によって開発された AWS Foundational Security Best Practices (FSBP) 標準、Center for Internet Security (CIS)、Payment Card Industry Data Security Standard (PCI DSS)、米国国立標準技術研究所 (NIST) などの外部コンプライアンスフレームワークが含まれます。セキュリティ標準ごとに複数のセキュリティ管理が含まれており、それぞれがセキュリティのベストプラクティスを表しています。Security Hub CSPM は、セキュリティコントロールに対してチェックを実行し、セキュリティのベストプラクティスに対するコンプライアンスを評価するのに役立つコントロールの検出結果を生成します。

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

Security Hub CSPM には、セキュリティ問題の優先順位付けと修復に役立つ自動化機能が用意されています。たとえば、自動化ルールを使用して、セキュリティチェックが失敗した場合に重要な結果を自動的に更新できます。Amazon EventBridge との統合を活用して、特定の結果に対する自動応答をトリガーすることもできます。

トピック

- Security Hub CSPM の利点
- Security Hub CSPM へのアクセス
- 関連サービス
- Security Hub CSPM 無料トライアルと料金
- Security Hub CSPM の概念と用語

- Security Hub CSPM の有効化
- Security Hub CSPM での管理者アカウントとメンバーアカウントの管理
- Security Hub CSPM でのクロスリージョン集約について
- Security Hub CSPM のセキュリティ標準について
- Security Hub CSPM のセキュリティコントロールについて
- Security Hub CSPM の統合について
- Security Hub CSPM での検出結果の作成と更新
- Security Hub CSPM でのインサイトの表示
- Security Hub CSPM の検出結果を自動的に変更して処理する
- Security Hub CSPM でのダッシュボードの操作
- Security Hub CSPM のリージョン制限
- CloudFormation を使用した Security Hub CSPM リソースの作成
- Amazon SNS で Security Hub CSPM の発表をサブスクライブする
- Security Hub CSPM の無効化

Security Hub CSPM の利点

Security Hub CSPM が AWS 環境全体のコンプライアンスとセキュリティ体制のモニタリングに役立つ主な方法をいくつか紹介します。

検出結果の収集と優先順位付けの労力削減

Security Hub CSPM は、統合製品と AWS パートナー製品からアカウント全体のセキュリティ結果を収集 AWS のサービス して優先順位付けする労力を削減します。Security Hub CSPM は、標準の検出結果形式である AWS Security Finding Format (ASFF) を使用して検出結果データを処理します。これにより、無数の情報源からの検出結果を複数の形式で管理する必要がなくなります。また、Security Hub CSPM はプロバイダー間で検出結果を関連付けて、最も重要な検出結果を優先できるようにします。

ベストプラクティスと標準に対する自動セキュリティチェック

Security Hub CSPM は、 AWS ベストプラクティスと業界標準に基づいて、アカウントレベルの継続的な設定とセキュリティチェックを自動的に実行します。Security Hub CSPM は、これらのチェックの結果を使用してセキュリティスコアを計算し、注意が必要な特定のアカウントとリソースを特定します。

アカウントとプロバイダーでの結果の統合ビュー

Security Hub CSPM は、アカウントとプロバイダー製品間でセキュリティ検出結果を統合し、Security Hub CSPM コンソールに結果を表示します。Security Hub CSPM API AWS CLI、または SDKs を使用して検出結果を取得することもできます。現在のセキュリティ状態を全体的に把握して傾向をとらえ、潜在的な問題を特定し、必要な修復手順を実行することができます。

検出結果の更新と修復を自動化する機能

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

Security Hub CSPM へのアクセス

Security Hub CSPM はほとんどの で使用できます AWS リージョン。Security Hub CSPM が現在利用可能なリージョンのリストについては、のAWS 「Security Hub CSPM エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。の 管理 AWS リージョン の詳細についてはAWS アカウント、「 AWS アカウント管理 リファレンスガイド」の AWS リージョン 「アカウントで使用できる の指定」を参照してください。

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

Security Hub CSPM コンソール

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

Security Hub CSPM API

Security Hub CSPM API を使用すると、Security Hub CSPM アカウント、データ、リソースにプログラムでアクセスできます。API を使用すると、HTTPS リクエストを Security Hub CSPM に直接送信できます。API の詳細については、AWS Security Hub CSPM API リファレンスを参照してください。

AWS CLI

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

AWS SDKs

AWS はSDKs を提供します。SDKs は、任意の言語で Security Hub CSPM やその他の への便利 AWS のサービス でプログラムによるアクセスを提供します。SDK は、暗号署名によるリクエスト、エラーの管理、リクエストの自動再試行などのタスクも処理します。 AWS SDKs」を参照してください。 AWS

> **Important**
>
> Security Hub CSPM は、Security Hub CSPM を有効にした後に生成された検出結果のみを検出して統合します。Security Hub CSPM を有効にする前に生成されたセキュリティ検出結果を遡及的に検出して統合することはありません。
> Security Hub CSPM は、アカウントで Security Hub CSPM を有効にしたリージョンでのみ検出結果を受信して処理します。
> CIS AWS Foundations Benchmark セキュリティチェックに完全に準拠するには、サポートされているすべての AWS リージョンで Security Hub CSPM を有効にする必要があります。

関連サービス

AWS 環境をさらに保護するには、Security Hub CSPM AWS のサービス と組み合わせて他の を使用することを検討してください。一部の は検出結果を Security Hub CSPM AWS のサービスに送信し、Security Hub CSPM は検出結果を標準形式に正規化します。一部の AWS のサービスは、Security Hub CSPM から結果を受け取ることもできます。

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

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

び AWS リソースを指します。Security Hub CSPM コントロールのリストについては、「」を参照してくださいSecurity Hub CSPM のコントロールリファレンス。ほとんどのコントロール結果を生成するには、Security Hub CSPM AWS Config の でリソースを有効に AWS Config して記録する必要があります。詳細については、「を有効にして設定する前に考慮すべき点 AWS Config」を参照してください。

Security Hub CSPM 無料トライアルと料金

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

無料トライアル中に Security Hub CSPM を使用すると、 AWS Config Security Hub CSPM がアイテムなど、操作する他の のサービスの使用に対して課金されます。Security Hub CSPM セキュリティ標準によってのみアクティブ化された AWS Config ルールには課金されません。

無料トライアルが終了するまで、Security Hub CSPM の使用に対して料金は発生しません。

使用状況の詳細と見積もりコストの表示

Security Hub CSPM は、Security Hub CSPM の使用にかかる推定 30 日間のコストを含む使用状況情報を提供します。使用状況の詳細には、無料トライアルの残り時間が含まれます。使用状況情報は、無料トライアル終了後の Security Hub CSPM のコストを理解するのに役立ちます。使用状況に関する情報は、無料トライアルの終了後にも確認できます。

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

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

推定月額コストは、30 日間に予測された検出結果とセキュリティチェックに対するアカウントの Security Hub CSPM の使用状況に基づきます。

使用状況情報と推定コストは、現在のアカウントと現在のリージョンについてのみ発生します。集約リージョンでは、使用情報と見積コストには、リンクされたリージョンは含まれません。リンクされたリージョンの詳細については、「the section called “集計されるデータのタイプ”」を参照してください。

料金詳細

取り込まれた検出結果とセキュリティチェックに対して Security Hub CSPM が請求する方法の詳細については、「Security Hub CSPM の料金」を参照してください。

Security Hub CSPM の概念と用語

AWS Security Hub CSPM では、一般的な AWS 概念と用語に基づいて構築し、これらの追加用語を使用します。

アカウント

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

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

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

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

詳細については、「Security Hub CSPM での管理者アカウントとメンバーアカウントの管理」を参照してください。

管理者アカウント

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

アカウントには次のいずれかの方法で管理者アカウントが付与されます:

- アカウントは、Security Hub CSPM で他のアカウントを関連付けるように招待します。このような招待されたアカウントが招待を承諾すると、そのアカウントはメンバーアカウントになり、招待したアカウントは管理者アカウントになります。

- アカウントは、組織管理アカウントによって Security Hub CSPM 管理者アカウントとして指定されます。Security Hub CSPM 管理者アカウントは、任意の組織アカウントをメンバーアカウントとして有効にし、他のアカウントをメンバーアカウントとして招待することもできます。

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

集約リージョン

集約リージョンを設定すると、複数の のセキュリティ検出結果を AWS リージョン 1 つの画面で表示できます。

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

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

詳細については、「the section called “リージョン間のデータの集約”」を参照してください。

アーカイブ済みの結果

レコード状態 (`RecordState`) が である検出結果`ARCHIVED`。結果がアーカイブされる場合、結果プロバイダーでは結果の関連性がなくなったとみなしているということを意味します。レコードの状態は、調査結果の調査のステータスを追跡するワークフローのステータスとは異なります。

検出結果プロバイダーは、Security Hub CSPM API の BatchImportFindingsオペレーションを使用して、作成した検出結果をアーカイブできます。Security Hub CSPM は、特定の基準を満たすコントロールの検出結果を自動的にアーカイブします。詳細については、「コントロールの検出結果の生成、更新、アーカイブ」を参照してください。

Security Hub CSPM コンソールでは、デフォルトのフィルター設定により、アーカイブされた検出結果が検出結果リストとテーブルから除外されます。アーカイブされた検出結果を含めるように設定を更新できます。Security Hub CSPM API の GetFindingsオペレーションを使用して検出結果を取得すると、そのオペレーションはアーカイブされた検出結果とアクティブな検出結果の両方を取得します。アーカイブされた結果を除外するには、結果をフィルタリングします。例:

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

```
        "Value": "ARCHIVED"
    }
],
```

AWS Security Finding 形式 (ASFF)

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

コントロール

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

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

カスタムアクション

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

委任管理者アカウント (Organizations)

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

Security Hub CSPM では、Security Hub CSPM 管理者アカウントは Security Hub CSPM の委任管理者アカウントでもあります。組織管理アカウントが最初に Security Hub CSPM 管理者アカウントを指定すると、Security Hub CSPM は Organizations を呼び出して、そのアカウントを委任管理者アカウントにします。

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

結果

セキュリティチェックまたはセキュリティ関連の検出の監視可能なレコード。Security Hub CSPM は、コントロールのセキュリティチェックを完了した後に検出結果を生成および更新します。これらはコントロールの検出結果と呼ばれます。検出結果は、他の AWS のサービス およびサードパーティー製品との統合からも得られます。

詳細については、「the section called “結果”」を参照してください。

クロスリージョン集約

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

詳細については、「the section called “リージョン間のデータの集約”」を参照してください。

結果の取り込み

他の AWS サービスやサードパーティーのパートナープロバイダーから Security Hub CSPM に結果をインポートすること。

結果取り込みイベントには、新しい結果と既存の結果の更新が含まれます。

インサイト

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

リンクされたリージョン

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

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

詳細については、「the section called “リージョン間のデータの集約”」を参照してください。

メンバーアカウント

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

アカウントは次のいずれかの方法でメンバーアカウントになります。

- 別のアカウントからの招待を承諾する。
- 組織アカウントの場合、Security Hub CSPM 管理者アカウントはアカウントをメンバーアカウントとして有効にします。

関連する要件

コントロールにマッピングされる一連の業界または規制要件。

ルール

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

セキュリティチェック

1 つのリソースに対するルールの特定のポイントインタイム評価。`PASSED`、`FAILED`、`WARNING`、または `NOT_AVAILABLE` の状態を特定します。セキュリティチェックを実行すると、結果が生成されます。

Security Hub CSPM 管理者アカウント

組織の Security Hub CSPM メンバーシップを管理する組織アカウント。

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

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

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

セキュリティ標準

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

緊急度

Security Hub CSPM コントロールに割り当てられた重要度は、コントロールの重要性を識別します。コントロールの重要度は、[Critical] (重要)、[High] (高)、[Medium] (中)、[Low] (低) または [Informational] (情報) のいずれかです。コントロールの結果に割り当てられる重要度は、そのコントロール自体の重要度と同等です。Security Hub CSPM がコントロールに重要度を割り当てる方法については、「」を参照してください[コントロールの検出結果の重要度レベル](#)。

ワークフローステータス

結果の調査ステータス。これは 属性を使用して追跡されます`Workflow.Status`。

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

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

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

```
"WorkflowStatus": [
    {
        "Comparison": "EQUALS",
        "Value": "RESOLVED"
    }
],
```

Security Hub CSPM コンソールには、検出結果のワークフローステータスを設定するオプションがあります。お客様 (または結果プロバイダーの結果をお客様に代わって更新する SIEM、チケッ

ト発行、インシデント管理、または SOAR ツール) は、BatchUpdateFindings を使用してワークフローステータスを更新することもできます。

Security Hub CSPM の有効化

Security Hub CSPM AWS を有効にするには、 AWS Organizations と統合するか、手動で 2 つの方法があります。

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

必要なアクセス許可を確認する

アマゾン ウェブ サービス (AWS) にサインアップしたら、Security Hub CSPM がその機能を使用できるようにする必要があります。Security Hub CSPM を有効にするには、まず Security Hub CSPM コンソールと API オペレーションへのアクセスを許可するアクセス許可を設定する必要があります。これを行う AWS には、 AWS Identity and Access Management (IAM) を使用して というマネージドポリシーを AWS IAM ID `AWSSecurityHubFullAccess`にアタッチします。

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

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

Organizations との統合による Security Hub CSPM の有効化

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

ご希望の方法を選択し、手順に従って委任管理者を指定します。

Security Hub CSPM console

オンボーディング時に委任 Security Hub CSPM 管理者を指定するには

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

2. 「Security Hub CSPM に移動」を選択します。組織の管理アカウントにサインインするよう求めるメッセージが表示されます。
3. [委任された管理者アカウント] セクションの [委任された管理者を指定] ページで、委任された管理者アカウントを指定します。委任された管理者には、他の AWS セキュリティおよびコンプライアンスサービスと同一の設定を選択することをお勧めします。
4. [委任された管理者を設定] を選択します。

Security Hub CSPM API

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

AWS CLI

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

コマンドの例:

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

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

中央設定

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

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

- Security Hub CSPM が有効か無効か
- どのセキュリティ基準を有効または無効にするか
- どのセキュリティコントロールを有効または無効にするか

- コントロール選択用のパラメータをカスタマイズするかどうか

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

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

中央設定を使用しない場合は、主にアカウントとリージョンごとに Security Hub CSPM を個別に設定する必要があります。これはローカル設定と呼ばれます。ローカル設定では、委任管理者は、現在のリージョンの新しい組織アカウントで Security Hub CSPM と制限された一連のセキュリティ標準を自動的に有効にできます。ローカル設定は、既存の組織アカウントや、現在のリージョン以外のリージョンには適用されません。また、ローカル設定では設定ポリシーの使用もサポートされていません。

Security Hub CSPM を手動で有効にする

スタンドアロンアカウントがある場合、または と統合していない場合は、Security Hub CSPM を手動で有効にする必要があります AWS Organizations。スタンドアロンアカウントは と統合できず AWS Organizations 、手動有効化を使用する必要があります。

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

任意の方法を選択し、手順に従って Security Hub CSPM を有効にします。コンソールから Security Hub CSPM を有効にすると、サポートされているセキュリティ標準を有効にするオプションもあります。

Security Hub CSPM console

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. Security Hub CSPM コンソールを初めて開くときは、「Security Hub CSPM に移動」を選択します。
3. ウェルカムページには、Security Standards セクションに、Security Hub CSPM がサポートするセキュリティ標準が記載されています。

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

標準またはその個々のコントロールは、いつでも有効または無効にできます。セキュリティ標準の管理の詳細については、「Security Hub CSPM のセキュリティ標準について」を参照してください。

4. [Enable Security Hub] (Security Hub の有効化) を選択します。

Security Hub CSPM API

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

- AWS 基本的なセキュリティのベストプラクティス
- Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0

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

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

AWS CLI

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

- AWS 基本的なセキュリティのベストプラクティス
- Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0

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

例

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

マルチアカウント有効化スクリプト

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

GitHub の Security Hub CSPM マルチアカウント有効化スクリプトを使用すると、アカウントとリージョン間で Security Hub CSPM を有効にできます。スクリプトを使用することで、メンバーアカウントへの招待の送信と AWS Configの有効化のプロセスも自動化されます。

このスクリプトは、すべてのリージョンで、グローバル AWS Config リソースを含むすべてのリソースのリソース記録を自動的に有効にします。グローバルリソースの記録を 1 つのリージョンに制限するものではありません。コストを削減するには、グローバルリソースを 1 つのリージョンにのみ記録することをお勧めします。中央設定またはクロスリージョン集約を使用する場合、これはホームリージョンである必要があります。詳細については、「でのリソースの記録 AWS Config」を参照してください。

アカウントとリージョン全体で Security Hub CSPM を無効にするための対応するスクリプトがあります。

次のステップ: 姿勢管理と統合

Security Hub CSPM を有効にしたら、セキュリティ標準とコントロールを有効にしてセキュリティ体制をモニタリングすることをお勧めします。コントロールを有効にすると、Security Hub CSPM はセキュリティチェックの実行と、 AWS 環境の設定ミスの検出に役立つコントロールの検出結果の生成を開始します。コントロールの検出結果を受け取るには、Security Hub CSPM AWS Config のを有効にして設定する必要があります。詳細については、「Security Hub CSPM AWS Config の有効化と設定」を参照してください。

Security Hub CSPM を有効にした後、Security Hub CSPM と他の AWS のサービス およびサードパーティーソリューションとの統合を活用して、Security Hub CSPM で検出結果を確認することもできます。Security Hub CSPM は、さまざまなソースから結果を集約し、一貫した形式で取り込みます。詳細については、「Security Hub CSPM の統合について」を参照してください。

Security Hub CSPM AWS Config の有効化と設定

AWS Security Hub CSPM は、 AWS Config ルールを使用してセキュリティチェックを実行し、ほとんどのコントロールの検出結果を生成します。 AWS Config は、 内の AWS リソースの設定の詳細

なビューを提供します AWS アカウント。ルールを使用してリソースのベースライン設定を確立し、設定レコーダーを使用して、特定のリソースがルールの条件に違反しているかどうかを検出します。AWS Config マネージドルールと呼ばれる一部のルールは、 によって事前定義および開発されています AWS Config。その他のルールは AWS Config 、Security Hub CSPM が開発するカスタムルールです。

AWS Config Security Hub CSPM がコントロールに使用する ルールは、サービスにリンクされたルールと呼ばれます。サービスにリンクされたルールを使用すると、Security Hub CSPM AWS のサービス などの がアカウントに AWS Config ルールを作成できます。

Security Hub CSPM でコントロールの検出結果を受信するには、アカウント AWS Config で を有効にし、有効なコントロールが評価するリソースの記録を有効にする必要があります。このページでは、Security Hub CSPM AWS Config で を有効にし、リソース記録を有効にする方法について説明します。

を有効にして設定する前に考慮すべき点 AWS Config

Security Hub CSPM でコントロールの検出結果を受信するには、Security Hub CSPM AWS Config が有効になってい AWS リージョン る各 でアカウントが を有効にしている必要があります。マルチアカウント環境で Security Hub CSPM を使用する場合は、管理者アカウントとすべてのメンバーアカウントの各リージョンで を有効にする AWS Config 必要があります。

Security Hub CSPM 標準とコントロールを有効にする AWS Config 前に、 でリソース記録を有効にすることを強くお勧めします。これにより、コントロールの検出結果が正確になります。

でリソース記録を有効にするには AWS Config、設定レコーダーにアタッチされている AWS Identity and Access Management (IAM) ロールにリソースを記録するのに十分なアクセス許可が必要です。さらに、リソースを記録するアクセス許可が AWS Config に付与されないように、IAM ポリシーや で管理 AWS Organizations されているポリシーがないことを確認してください。Security Hub CSPM コントロールチェックは、リソースの設定を直接評価し、 AWS Organizations ポリシーを考慮しません。 AWS Config 録画の詳細については、「 AWS Config デベロッパーガイド」の「設定レコーダーの使用」を参照してください。

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

- 標準を有効にした日。
- 標準を有効にした翌日。
- 標準を有効にしてから 3 日後。

- 標準を有効にしてから 7 日後、その後は 7 日ごとに継続します。

中央設定を使用する場合、Security Hub CSPM は、1 つ以上の標準を有効にする設定ポリシーをアカウント、組織単位 (OUs)、またはルートに関連付けるたびに、サービスにリンクされた AWS Config ルールの作成も試みます。

でのリソースの記録 AWS Config

有効にするときは AWS Config、設定レコーダーに記録する AWS AWS Config リソースを指定する必要があります。サービスにリンクされたルールを通じて、設定レコーダーは Security Hub CSPM がリソース設定の変更を検出できるようにします。

Security Hub CSPM が正確なコントロール結果を生成するには、有効なコントロールに対応するリソースの の記録 AWS Config を有効にする必要があります。これは主に、リソースの記録を必要とする変更トリガースケジュールタイプで有効になっているコントロールです。定期的なスケジュールタイプの一部のコントロールでは、リソースの記録も必要です。これらのコントロールとその対応するリソースのリストについては、「」を参照してください[コントロールの検出結果に必要な AWS Config リソース](#)。

> **Warning**
>
> Security Hub CSPM コントロールの記録 AWS Config を正しく設定しないと、特に次のインスタンスで、コントロールの検出結果が不正確になる可能性があります。
>
> - 特定のコントロールのリソースを記録したことがないか、そのタイプのリソースを作成する前にリソースの記録を無効にしました。このような場合、記録を無効にした後にコントロールの範囲内でリソースを作成している場合でも、問題のコントロール`WARNING`の検出結果を受け取ります。この`WARNING`検出結果は、リソースの設定状態を実際に評価しないデフォルトの検出結果です。
> - 特定のコントロールによって評価されるリソースの記録を無効にします。この場合、コントロールが新規または更新されたリソースを評価していない場合でも、Security Hub CSPM は記録を無効にする前に生成されたコントロール結果を保持します。Security Hub CSPM は、検出結果のコンプライアンスステータスも に変更します`WARNING`。これらの保持された検出結果は、リソースの現在の設定状態を正確に反映していない可能性があります。

デフォルトでは、 AWS リージョン は、実行中の で検出されたサポートされているすべてのリージョンリソース AWS Config を記録します。すべての Security Hub CSPM コントロールの検出結果を受信するには、グローバルリソースを記録する AWS Config ように も設定する必要があります。コストを削減するには、グローバルリソースを 1 つのリージョンにのみ記録することをお勧めします。中央設定またはクロスリージョン集約を使用する場合、このリージョンはホームリージョンである必要があります。

では AWS Config、リソースの状態の変化を継続的に記録するか、毎日記録するかを選択できます。日次記録を選択した場合、リソース状態に変更があった場合、 は 24 時間ごとにリソース設定データを AWS Config 配信します。変化がなければ、データは配信されません。これにより、変更によってトリガーされるコントロールの Security Hub CSPM 検出結果の生成が 24 時間完了するまで遅延する可能性があります。

AWS Config 録画の詳細については、「 AWS Config デベロッパーガイド」のAWS 「リソースの記録」を参照してください。

を有効にして設定する方法 AWS Config

リソース記録は、次のいずれかの方法で有効化 AWS Config および有効化できます。

- AWS Config コンソール – AWS Config コンソールを使用して AWS Config 、アカウントの を有効にできます。手順については、「 AWS Config デベロッパーガイド」の「 コンソール AWS Config でのセットアップ」を参照してください。
- AWS CLI または SDKs – AWS Command Line Interface () を使用して AWS Config 、 アカウントの を有効にできますAWS CLI。手順については、「 AWS Config デベロッパーガイド」の「 AWS Config でのセットアップ AWS CLI」を参照してください。 AWS ソフトウェア開発キット (SDK) は、多くのプログラミング言語でも使用できます。 SDKs
- CloudFormation テンプレート – 多くのアカウント AWS Config で を有効にするには、Enable AWS Configという名前の AWS CloudFormation テンプレートを使用することをお勧めします。このテンプレートにアクセスするには、「 AWS CloudFormation ユーザーガイド」のAWS CloudFormation StackSet サンプルテンプレート」を参照してください。

  デフォルトでは、このテンプレートは IAM グローバルリソースの記録を除外します。記録コストを節約するために、IAM グローバルリソースの記録を 1 AWS リージョン つのみ有効にしてください。クロスリージョン集約を有効にしている場合は、Security Hub CSPM ホームリージョンである必要があります。それ以外の場合は、Security Hub CSPM が利用可能な任意のリージョンで、IAM グローバルリソースの記録をサポートできます。1 つの StackSet を実行して、IAM グローバルリソースを含むすべてのリソースをホームリージョンまたは他の選択したリージョンに記

録することをお勧めします。次に、2 番目の StackSet を実行して、他のリージョンの IAM グローバルリソースを除くすべてのリソースを記録します。

- GitHub スクリプト – Security Hub CSPM は、Security Hub CSPM と をリージョン間で複数のアカウント AWS Config に対して有効にする GitHub スクリプトを提供します。このスクリプトは、と統合していない場合や AWS Organizations、組織の一部ではないメンバーアカウントがある場合に便利です。

詳細については、 AWS セキュリティブログのブログ記事「Optimize AWS Config for AWS Security Hub CSPM to effectively manage your cloud security posture」を参照してください。

Config.1 コントロール

Security Hub CSPM では、 が無効になっている場合、Config.1 コントロール AWS Config はアカウントに`FAILED`結果を生成します。また、 AWS Config が有効になっていてもリソース記録が有効になっていない場合、アカウントに`FAILED`結果を生成します。

AWS Config が有効になっていてリソース記録が有効になっているが、有効なコントロールがチェックするタイプのリソースに対してリソース記録が有効になっていない場合、Security Hub CSPM は Config.1 コントロール`FAILED`の結果を生成します。この`FAILED`検出結果に加えて、Security Hub CSPM は、有効なコントロールと、コントロールがチェックするリソースのタイプに関する`WARNING`検出結果を生成します。たとえば、KMS.5 コントロールを有効にし、リソース記録が有効になっていない場合 AWS KMS keys、Security Hub CSPM は Config.1 コントロール`FAILED`の結果を生成します。Security Hub CSPM は、KMS.5 コントロールと KMS キーの検出`WARNING`結果も生成します。

Config.1 コントロールの検出`PASSED`結果を受信するには、有効なコントロールに対応するすべてのリソースタイプのリソース記録を有効にします。また、組織に必要ないコントロールも無効にします。これにより、セキュリティコントロールチェックで設定ギャップがなくなります。また、誤って設定されたリソースに関する正確な検出結果を確実に受け取るのに役立ちます。

お客様が組織の委任 Security Hub CSPM 管理者である場合、アカウントとメンバーアカウントに対して AWS Config 記録を正しく設定する必要があります。クロスリージョン集約を使用する場合は、ホームリージョンとすべてのリンクされたリージョンで AWS Config 録音を正しく設定する必要があります。グローバルリソースをリンクされたリージョンに記録する必要はありません。

サービスにリンクされたルールの生成

サービスにリンクされた AWS Config ルールを使用するコントロールごとに、Security Hub CSPM は必要なルールのインスタンスを AWS 環境に作成します。

これらのサービスにリンクされたルールは、Security Hub CSPM に固有です。Security Hub CSPM は、同じルールの他のインスタンスがすでに存在する場合でも、これらのサービスにリンクされたルールを作成します。サービスにリンクされたルールは、元のルール名の`securityhub`前に を追加し、ルール名の後に一意の識別子を追加します。たとえば、 AWS Config マネージドルール の場合`vpc-flow-logs-enabled`、サービスにリンクされたルール名は ですsecurityhub-vpc-flow-logs-enabled-12345。

コントロールの評価に使用できる AWS Config マネージドルールの数にはクォータがあります。Security Hub CSPM が作成する AWS Config ルールは、これらのクォータにはカウントされません。アカウントのマネージドルール AWS Config のクォータにすでに達している場合でも、セキュリティ標準を有効にできます。 AWS Config ルールのクォータの詳細については、「 AWS Config デベロッパーガイド」の「 のサービス制限 AWS Config」を参照してください。

コストに関する考慮事項

Security Hub CSPM は、 AWS Config 設定項目を更新することで、`AWS::Config::ResourceCompliance`設定レコーダーのコストに影響を与える可能性があります。更新は、 AWS Config ルールに関連付けられた Security Hub CSPM コントロールがコンプライアンス状態を変更する、有効または無効になる、またはパラメータが更新されるたびに発生する可能性があります。Security Hub CSPM にのみ AWS Config 設定レコーダーを使用し、他の目的でこの設定項目を使用しない場合は、その記録をオフにすることをお勧めします AWS Config。これにより、 AWS Config コストを削減できます。Security Hub CSPM で動作するには、`AWS::Config::ResourceCompliance`セキュリティチェックを記録する必要はありません。

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

Security Hub CSPM のローカル設定について

ローカル設定は、Security Hub CSPM で AWS 組織を設定するデフォルトの方法です。中央設定にオプトインして有効にしない場合、組織はデフォルトでローカル設定を使用します。

ローカル設定では、委任 Security Hub CSPM 管理者アカウントは設定の制御が制限されています。委任管理者が適用できる唯一の設定は、新しい組織アカウントで Security Hub CSPM とデフォルトのセキュリティ標準を自動的に有効にすることです。これらの設定は、委任管理者アカウントを指定したリージョンにのみ適用されます。デフォルトのセキュリティ標準は、 AWS Foundational Security Best Practices (FSBP) と Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 です。ローカル設定は、既存の組織アカウントや、委任管理者アカウントが指定されたリージョン以外のリージョンには適用されません。

1 つのリージョンで新しい組織アカウントで Security Hub CSPM とデフォルト標準を有効にするだけでなく、標準とコントロールを含む他の Security Hub CSPM 設定をリージョンとアカウントごとに個別に設定する必要があります。これは重複するプロセスであるため、次のいずれかに当てはまる場合は、マルチアカウント環境に中央設定を使用することをお勧めします。

- 組織のさまざまな部分で異なる設定 (例えば、チームごとに異なる有効な標準やコントロール) が必要です。
- 複数のリージョンで運用しており、これらのリージョン全体でサービスを設定する時間と複雑さを軽減したいと考えています。
- 新しいアカウントが組織に加わるときに、特定の設定を使用するようにします。
- 組織アカウントは、親アカウントまたはルートから特定の設定を継承します。

中央設定の詳細については、「Security Hub CSPM の中央設定について」を参照してください。

Security Hub CSPM の中央設定について

中央設定は、複数の AWS アカウント と にまたがる AWS Security Hub CSPM のセットアップと管理に役立つ Security Hub CSPM 機能です AWS リージョン。中央設定を使用するには、まず Security Hub CSPM と を統合する必要があります AWS Organizations。組織を作成し、組織の委任 Security Hub CSPM 管理者アカウントを指定することで、サービスを統合できます。

委任 Security Hub CSPM 管理者アカウントから、リージョン間で組織のアカウントと組織単位 (OUs) に対して Security Hub CSPM を有効にできます。リージョン間でアカウントと OUs の個々のセキュリティ標準とセキュリティコントロールを有効、設定、無効にすることもできます。これらの設定は、ホームリージョンと呼ばれる 1 つのプライマリリージョンから、わずか数ステップで設定できます。

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

一元管理アカウントを設定するには、委任管理者は Security Hub CSPM 設定ポリシーを使用します。設定ポリシーにより、委任管理者は Security Hub CSPM を有効または無効にするか、どの標準とコントロールを有効または無効にするかを指定できます。また、特定のコントロールのパラメータをカスタマイズするためにも使用できます。

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

> **Tip**
>
> 中央設定を使用しない場合は、主にアカウントとリージョンごとに Security Hub CSPM を個別に設定する必要があります。これはローカル設定と呼ばれます。ローカル設定では、委任管理者は、現在のリージョンの新しい組織アカウントで Security Hub CSPM と制限された一連のセキュリティ標準を自動的に有効にできます。ローカル設定は、既存の組織アカウントや、現在のリージョン以外のリージョンには適用されません。また、ローカル設定では設定ポリシーの使用もサポートされていません。

このセクションでは、中央設定の概要について説明します。

中央設定を使用する利点

中央設定には、次のような利点があります。

Security Hub CSPM サービスと機能の設定を簡素化する

中央設定を使用する場合、Security Hub CSPM は組織のセキュリティのベストプラクティスを設定するプロセスをガイドします。また、作成された設定ポリシーは、指定したアカウントと OU に自動的にデプロイされます。新しいセキュリティコントロールを自動的に有効にするなど、既存の Security Hub CSPM 設定がある場合は、設定ポリシーの開始点として使用できます。さらに、Security Hub CSPM コンソールの設定ページには、設定ポリシーと、各ポリシーを使用するアカウントと OUs のリアルタイム概要が表示されます。

複数のアカウントやリージョンにまたがる設定

中央設定を使用して、複数のアカウントとリージョンにわたって Security Hub CSPM を設定できます。これにより、組織の各部署で一貫した設定と適切なセキュリティ対策が確保されます。

さまざまなアカウントや OU で異なる設定に対応

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

設定のずれを防ぐ

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

中央設定をいつ使用するのか?

中央設定は、複数の Security Hub CSPM アカウントを含む AWS 環境に最も有益です。これは、複数のアカウントの Security Hub CSPM を一元管理できるように設計されています。

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

中央設定に関する用語と概念

以下の主要な用語と概念を理解することは、Security Hub CSPM 中央設定の使用に役立ちます。

中央設定

組織の委任 Security Hub CSPM 管理者アカウントが、複数のアカウントとリージョンにわたって Security Hub CSPM サービス、セキュリティ標準、セキュリティコントロールを設定するのに役立つ Security Hub CSPM 機能。これらの設定を構成するために、委任管理者は組織内の一元管理アカウント用の Security Hub CSPM 設定ポリシーを作成および管理します。セルフマネージド型アカウントは、リージョンごとに独自の設定を個別に行うことができます。中央設定を使用するには、Security Hub CSPM と を統合する必要があります AWS Organizations。

ホームリージョン

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

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

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

リンクされたリージョン

ホームリージョンから設定 AWS リージョン 可能な 。設定ポリシーは、ホームリージョンの委任管理者によって作成されます。ポリシーは、ホームリージョンとリンクされたすべてのリージョンで有効になります。リンクされたリージョンの指定はオプションです。

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

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

[Target] (ターゲット)

AWS アカウント、組織単位 (OU)、または組織ルート。

Security Hub CSPM 設定ポリシー

委任管理者が一元管理ターゲット用に設定できる Security Hub CSPM 設定のコレクション。これには、以下が含まれます。

- Security Hub CSPM を有効または無効にするかどうか。
- 1 つ以上のセキュリティ標準を有効にするかどうか。
- 有効になっている標準でどのセキュリティコントロールを有効にするか。委任管理者は、有効にする必要がある特定のコントロールのリストを提供することでこれを行うことができます。Security Hub CSPM は、他のすべてのコントロール (リリース時の新しいコントロールを含む) を無効にします。または、委任管理者は無効にする必要がある特定のコントロールのリストを提供でき、Security Hub CSPM は他のすべてのコントロール (リリース時の新しいコントロールを含む) を有効にします。
- オプションで、有効な複数の標準で有効になっているコントロールを選択してパラメータをカスタマイズできます。

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

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

推奨される設定ポリシーでは、Security Hub CSPM、 AWS Foundational Security Best Practices (FSBP) 標準、および既存のすべての FSBP コントロールと新しい FSBP コントロールが有効になっています。パラメータを受け入れるコントロールは、デフォルト値を使用します。推奨される設定ポリシーは、組織全体に適用されます。

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

ローカル設定

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

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

手動アカウント管理

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

中央設定 API

Security Hub CSPM 委任 Security Hub CSPM 管理者のみがホームリージョンで使用して、一元管理されたアカウントの設定ポリシーを管理できる Security Hub CSPM オペレーション。オペレーションは次のとおりです。

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

アカウント固有の API

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

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

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

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

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

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

組織単位 (OU)

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

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

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

一元管理型

委任管理者のみが設定ポリシーを使用して複数のリージョンにわたり設定できるターゲット。

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

セルフマネージド型

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

委任管理者アカウントで、ターゲットがセルフマネージド型かどうかを指定します。委任管理者は、ターゲットにセルフマネージド型の動作を適用できます。また、アカウントや OU は親からセルフマネージド型の動作を継承することもできます。

委任管理者アカウントは、それ自体がセルフマネージド型アカウントである可能性があります。委任管理者アカウントは、ターゲットのステータスをセルフマネージド型から一元管理型、または逆に変更できます。

設定ポリシーの関連付け

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

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

関連付けは、別の設定が適用または継承されるまで発生します。

適用された設定ポリシー

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

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

継承された設定ポリシー

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

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

ルート

AWS Organizations および Security Hub CSPM では、組織内の最上位の親ノード。委任された管理者が設定ポリシーをルートに適用すると、そのポリシーは組織内のすべてのアカウントと OU に関連付けられます。ただし、アプリケーションまたは継承によって別のポリシーが使用されている場合や、セルフマネージド型として指定されている場合は除きます。管理者がルートをセルフマネージド型として指定した場合、アプリケーションまたは継承で設定ポリシーを使用する場

合を除き、組織内のすべてのアカウントと OU はセルフマネージド型になります。ルートがセルフマネージド型で、現在設定ポリシーが存在しない場合、組織内のすべての新規アカウントで現在の設定が保持されます。

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

Security Hub CSPM で中央設定を有効にする

委任 AWS Security Hub CSPM 管理者アカウントは、中央設定を使用して、複数のアカウントと組織単位 (OUs) の Security Hub CSPM、標準、コントロールを設定できます AWS リージョン。

中央設定の利点とその仕組みについては、「Security Hub CSPM の中央設定について」を参照してください。

このセクションでは、中央設定の前提条件と使用開始方法について説明します。

中央設定の前提条件

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

Organizations との統合

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

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

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

> **Important**
>
> 中央設定を使用する場合、Security Hub CSPM コンソールまたは Security Hub CSPM APIs を使用して、委任管理者アカウントを変更または削除することはできません。Organizations

管理アカウントが AWS Organizations APIs を使用して Security Hub CSPM 委任管理者を変更または削除する場合、Security Hub CSPM は自動的に中央設定を停止します。設定ポリシーの関連付けも解除され、削除されます。メンバーアカウントには、委任管理者が変更または削除される前の設定が保持されます。

ホームリージョンの指定

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

> **Note**
>
> ホームリージョンは、 AWS をオプトインリージョンとして指定したリージョンにすることはできません。オプトインリージョンは、デフォルトでは無効となっています。オプトインリージョンのリストについては、「AWS アカウント管理リファレンスガイド」の「Considerations before enabling and disabling Regions」を参照してください。

必要に応じて、ホームリージョンから設定可能なリンクされたリージョンを 1 つ以上指定できます。

委任管理者は、ホームリージョンからのみ設定ポリシーを作成および管理できます。設定ポリシーは、ホームリージョンとリンクされたすべてのリージョンで有効になります。これらのリージョンのサブセットにのみ適用され、他のリージョンには適用されない設定ポリシーは作成できません。ただし、グローバルリソースが関与するコントロールは例外です。中央設定を使用する場合、Security Hub CSPM は、ホームリージョンを除くすべてのリージョンでグローバルリソースを含むコントロールを自動的に無効にします。詳細については、「グローバルリソースを使用するコントロール」を参照してください。

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

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

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

中央設定を有効にする手順

ご希望の方法を選択し、手順に従って組織の中央設定を有効化します。

Security Hub CSPM console

中央設定を有効化するには (コンソール)

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

   Security Hub CSPM にオンボーディングする場合は、「Security Hub CSPM に移動」を選択します。
3. [委任された管理者を指定] ページで、委任管理者アカウントを選択するか、アカウント ID を入力します。該当する場合は、他の AWS セキュリティおよびコンプライアンスサービスに設定したのと同じ委任管理者を選択することをお勧めします。[委任された管理者を設定] を選択します。
4. [組織を一元化] ページの [リージョン] セクションで、ホームリージョンを選択します。続行するには、ホームリージョンにサインインする必要があります。クロスリージョン集約の集約リージョンを既に設定している場合、そのリージョンがホームリージョンとして表示されます。ホームリージョンを変更するには、[リージョンの設定を編集] を選択します。これにより、ご希望のホームリージョンを選択して、このワークフローに戻ることができます。
5. ホームリージョンにリンクするリージョンを少なくとも 1 つ選択してください。必要に応じて、将来サポートされるリージョンをホームリージョンに自動的にリンクするかどうかを選択します。ここで選択したリージョンは、委任管理者がホームリージョンから設定できます。設定ポリシーは、ホームリージョンとすべてのリンクされたリージョンで有効になります。
6. [確認して続行] を選択します。
7. 中央設定を使用できるようになりました。続けてコンソールのプロンプトに従い、最初の設定ポリシーを作成します。設定ポリシーを作成する準備がまだ整っていない場合は、[まだ設定する準備ができていません] を選択します。ポリシーは、後でナビゲーションペインで [設

定]、[設定] の順に選択して作成できます。設定ポリシーの作成手順については、「設定ポリシーの作成と関連付け」を参照してください。

Security Hub CSPM API

中央設定を有効化するには (API)

1. 委任管理者アカウントの認証情報を使用して、ホームリージョンから UpdateOrganizationConfiguration API を呼び出します。
2. `AutoEnable` フィールドは `false` に設定されます。
3. `OrganizationConfiguration` オブジェクト内の `ConfigurationType` フィールドを `CENTRAL` に設定します。このアクションには以下の影響があります。
   - すべてのリンクされたリージョンで、呼び出し元のアカウントを Security Hub CSPM 委任管理者として指定します。
   - すべてのリンクされたリージョンの委任管理者アカウントで Security Hub CSPM を有効にします。
   - 呼び出し元のアカウントを、Security Hub CSPM を使用し、組織に属する新規および既存のアカウントの Security Hub CSPM 委任管理者として指定します。これはホームリージョンとすべてのリンクされたリージョンで発生します。呼び出し元アカウントは、Security Hub CSPM が有効になっている設定ポリシーに関連付けられている場合にのみ、新しい組織アカウントの委任管理者として設定されます。呼び出し元アカウントは、Security Hub CSPM が既に有効になっている場合にのみ、既存の組織アカウントの委任管理者として設定されます。
   - すべてのリンクされたリージョンで AutoEnable を `false` に設定し、ホームリージョンとすべてのリンクされたリージョンで AutoEnableStandards を `NONE` に設定します。これらのパラメータは、中央設定を使用する場合、ホームリージョンとリンクされたリージョンには関係ありませんが、設定ポリシーを使用して、組織アカウントで Security Hub CSPM とデフォルトのセキュリティ標準を自動的に有効にできます。
4. 中央設定を使用できるようになりました。委任管理者は、組織内で Security Hub CSPM を設定する設定ポリシーを作成できます。設定ポリシーの作成手順については、「設定ポリシーの作成と関連付け」を参照してください。

API リクエストの例:

```
{
```

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

AWS CLI

中央設定を有効化するには (AWS CLI)

1. 委任管理者アカウントの認証情報を使用して、ホームリージョンから update-organization-configuration コマンドを実行します。
2. `no-auto-enable` パラメータを指定します。
3. `organization-configuration` オブジェクト内の `ConfigurationType` フィールドを `CENTRAL` に設定します。このアクションには以下の影響があります。
   - すべてのリンクされたリージョンで、呼び出し元のアカウントを Security Hub CSPM 委任管理者として指定します。
   - すべてのリンクされたリージョンの委任管理者アカウントで Security Hub CSPM を有効にします。
   - 呼び出し元のアカウントを、Security Hub CSPM を使用し、組織に属する新規および既存のアカウントの Security Hub CSPM 委任管理者として指定します。これはホームリージョンとすべてのリンクされたリージョンで発生します。呼び出しアカウントは、新しい組織アカウントが Security Hub が有効になっている設定ポリシーに関連付けられている場合にのみ、その委任管理者として設定されます。呼び出し元アカウントは、Security Hub CSPM が既に有効になっている場合にのみ、既存の組織アカウントの委任管理者として設定されます。
   - すべてのリンクされたリージョンで自動有効化オプションを no-auto-enable に設定し、ホームリージョンとすべてのリンクされたリージョンで auto-enable-standards を `NONE` に設定します。これらのパラメータは、中央設定を使用する場合、ホームリージョンとリンクされたリージョンには関係ありませんが、設定ポリシーを使用して、組織アカウントで Security Hub CSPM とデフォルトのセキュリティ標準を自動的に有効にできます。
4. 中央設定を使用できるようになりました。委任管理者は、組織内で Security Hub CSPM を設定する設定ポリシーを作成できます。設定ポリシーの作成手順については、「設定ポリシーの作成と関連付け」を参照してください。

コマンドの例:

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

一元管理ターゲットと自己管理ターゲット

中央設定を有効にすると、委任 AWS Security Hub CSPM 管理者は、各組織アカウント、組織単位 (OU)、ルートを一元管理型またはセルフマネージド型として指定できます。ターゲットの管理タイプによって、Security Hub の CSPM 設定を指定する方法が決まります。

中央設定の利点とその仕組みについては、「Security Hub CSPM の中央設定について」を参照してください。

このセクションでは、一元管理型とセルフマネージド型の指定の違いと、アカウント、OU、またはルートの管理タイプを選択する方法について説明します。

セルフマネージド型

セルフマネージドアカウント、OU、またはルートの所有者は、それぞれの設定を個別に設定する必要があります AWS リージョン。委任管理者は、セルフマネージドターゲットの設定ポリシーを作成できません。

一元管理型

ホームリージョンとリンクされたリージョン全体で一元管理されたアカウント、OUs、またはルートの設定を設定できるのは、委任 Security Hub CSPM 管理者のみです。設定ポリシーは、一元管理型アカウントおよび OU に関連付けることができます。

委任管理者は、ターゲットのステータスをセルフマネージド型と一元管理型の間で切り替えることができます。デフォルトでは、Security Hub CSPM API を使用して中央設定を開始すると、すべてのアカウントと OU が自己管理されます。コンソールでは、管理タイプは最初の設定ポリシーによって異なります。最初のポリシーに関連付けられるアカウントと OU は、一元管理型です。その他のアカウントと OU は、デフォルトではセルフマネージド型になります。

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

一元管理アカウントをセルフマネージドアカウントに変更した場合、設定ポリシーを通じてアカウントに適用された設定はそのまま残ります。たとえば、一元管理アカウントは、最初は Security Hub CSPM を有効にし、 AWS Foundational Security Best Practices を有効にし、CloudTrail.1. その後、アカウントをセルフマネージドとして指定すると、すべての設定は変更されません。ただし、アカウント所有者は今後アカウントの設定を個別に変更できます。

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

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

セルフマネージドアカウントで設定を行うオプション

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

セルフマネージドアカウントの所有者は、各リージョンで Security Hub CSPM API の次のオペレーションを呼び出して、設定を構成することができます。

- `EnableSecurityHub` および `DisableSecurityHub` を使用して、Security Hub CSPM サービスを有効または無効にします (セルフマネージドアカウントに委任 Security Hub CSPM 管理者がいる場合、アカウント所有者が Security Hub CSPM を無効にする前に、管理者はアカウントの関連付けを解除する必要があります)。
- 標準を有効または無効にする `BatchEnableStandards` または `BatchDisableStandards`
- コントロールを有効または無効にする `BatchUpdateStandardsControlAssociations` または `UpdateStandardsControl`

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

Security Hub CSPM API アクションの詳細については、AWS Security Hub CSPM API リファレンスを参照してください。

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

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

ターゲットの管理タイプの選択

任意の方法を選択し、手順に従って、 AWS Security Hub CSPM でアカウントまたは OU を一元管理または自己管理として指定します。

Security Hub CSPM console

アカウントまたは OU の管理タイプを選択するには

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

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

Security Hub CSPM API

アカウントまたは OU の管理タイプを選択するには

1. ホームリージョンの Security Hub CSPM 委任管理者アカウントから StartConfigurationPolicyAssociation API を呼び出します。
2. アカウントまたは OU で独自の設定を制御する場合は、`ConfigurationPolicyIdentifier` フィールドに `SELF_MANAGED_SECURITY_HUB` と入力します。委任された管理者がアカウントまたは OU の設定を制御する場合は、関連する設定ポリシーの Amazon リソースネーム (ARN) または ID を指定します。

3. `Target` フィールドに、管理タイプを変更するターゲットの AWS アカウント ID、OU ID、またはルート ID を指定します。これにより、セルフマネージド型の動作または指定した設定ポリシーがターゲットに関連付けられます。ターゲットの子アカウントは、セルフマネージド型の動作または設定ポリシーを継承できます。

セルフマネージド型アカウントを指定する API リクエストの例:

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

AWS CLI

アカウントまたは OU の管理タイプを選択するには

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

セルフマネージド型アカウントを指定するコマンドの例:

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

Security Hub CSPM の設定ポリシーの仕組み

委任 AWS Security Hub CSPM 管理者は、組織の Security Hub CSPM、セキュリティ標準、セキュリティコントロールを設定する設定ポリシーを作成できます。設定ポリシーを作成した後に、委任管理者はそれを特定のアカウント、組織単位 (OU)、またはルートに関連付けることができます。その後、ポリシーは、指定されたアカウント、OU またはルートで有効になります。

中央設定の利点とその仕組みについては、「Security Hub CSPM の中央設定について」を参照してください。

このセクションでは、設定ポリシーの詳細な概要を示します。

ポリシーに関する考慮事項

Security Hub CSPM で設定ポリシーを作成する前に、次の詳細を考慮してください。

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

用するコントロールは例外です。Security Hub CSPM は、ホームリージョンを除くすべてのリージョンで、グローバルリソースを含むコントロールを自動的に無効にします。

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

ポリシーがホームリージョンまたは 1 つ以上のリンクされたリージョンで利用できないコントロールを設定する場合、Security Hub CSPM は使用できないリージョンでコントロール設定をスキップしますが、コントロールが利用可能なリージョンで設定を適用します。ホームリージョンまたはリンクされたリージョンのいずれかで利用できないコントロールがカバーされなくなります。

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

設定ポリシーのタイプ

各設定ポリシーでは、次の設定を指定します。

- Security Hub CSPM を有効または無効にします。
- 1 つ以上のセキュリティ標準を有効にします。
- 有効な標準でどのセキュリティコントロールが有効になっているかを示します。これを行うには、有効にする必要がある特定のコントロールのリストを指定します。Security Hub CSPM は、リリース時に新しいコントロールを含め、他のすべてのコントロールを無効にします。または、無効にする必要がある特定のコントロールのリストを指定することもできます。Security Hub CSPM は、リリース時に新しいコントロールを含む他のすべてのコントロールを有効にします。
- オプションで、有効な標準全体で有効になっているコントロールを選択してパラメータをカスタマイズできます。

中央設定ポリシーには AWS Config レコーダー設定は含まれません。Security Hub CSPM がコントロール結果を生成するには、必要なリソースの記録を個別に有効に AWS Config してオンにする必要

があります。詳細については、「を有効にして設定する前に考慮すべき点 AWS Config」を参照してください。

中央設定を使用する場合、Security Hub CSPM は、ホームリージョンを除くすべてのリージョンでグローバルリソースを含むコントロールを自動的に無効にします。設定ポリシーを通じて有効を選択したその他のコントロールは、利用可能なすべてのリージョンで有効になります。これらのコントロールの検出結果を 1 つのリージョンのみに制限するには、 AWS Config レコーダー設定を更新し、ホームリージョンを除くすべてのリージョンでグローバルリソース記録をオフにします。

グローバルリソースを含む有効なコントロールがホームリージョンでサポートされていない場合、Security Hub CSPM は、コントロールがサポートされているリンクされた 1 つのリージョンでコントロールを有効にしようとします。中央設定では、ホームリージョンまたはリンクされたリージョンで利用できないコントロールのカバレッジがありません。

グローバルリソースを含むコントロールのリストについては、「グローバルリソースを使用するコントロール」を参照してください。

推奨される設定ポリシー

Security Hub CSPM コンソールで初めて設定ポリシーを作成する場合は、Security Hub CSPM 推奨ポリシーを選択できます。

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

カスタム設定ポリシー

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

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

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

アプリケーションと継承によるポリシーの関連付け

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

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

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

適用は継承よりも優先されます。つまり、委任管理者がアカウントまたは OU に直接適用した設定ポリシーまたはセルフマネージド型指定を継承によって上書きされることはありません。

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

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

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

次の図は、中央設定におけるポリシーの適用と継承の仕組みを示しています。

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

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

設定ポリシーのテスト

設定ポリシーの仕組みを確実に理解するには、1 つのポリシーを作成し、テストアカウントまたは OU に関連付けることをお勧めします。

設定ポリシーをテストするには

1. カスタム設定ポリシーを作成し、Security Hub CSPM の有効化、標準、およびコントロールの指定された設定が正しいことを確認します。手順については、「設定ポリシーの作成と関連付け」を参照してください。
2. 子アカウントや OU を持たないテストアカウントまたは OU に設定ポリシーを適用します。
3. テストアカウントまたは OU が、ホームリージョンとリンクされているすべてのリージョンで設定ポリシーを想定どおりに使用していることを確認します。また、組織内の他のすべてのアカウントと OU が引き続きセルフマネージドされ、各地域で独自の設定を変更できることを確認できます。

1 つのアカウントまたは OU で設定ポリシーをテストした後に、その設定ポリシーを他のアカウントや OU に関連付けることができます。

設定ポリシーの作成と関連付け

委任 AWS Security Hub CSPM 管理者アカウントは、指定されたアカウントと組織単位 (OUs) で Security Hub CSPM、標準、コントロールを設定する方法を指定する設定ポリシーを作成できます。設定ポリシーは、委任管理者が少なくとも 1 つのアカウントまたは組織単位 (OU)、またはルートに関連付けた後にのみ有効になります。委任管理者は、アカウント、OU、またはルートにセルフマネージド型の設定を関連付けることもできます。

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

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

> **Note**
>
> 中央設定を使用する場合、Security Hub CSPM は、ホームリージョンを除くすべてのリージョンでグローバルリソースを含むコントロールを自動的に無効にします。設定ポリシーを通じて有効を選択したその他のコントロールは、利用可能なすべてのリージョンで有効になります。これらのコントロールの結果を 1 つのリージョンのみに制限するには、 AWS Config レコーダー設定を更新し、ホームリージョンを除くすべてのリージョンでグローバルリソース記録をオフにします。
> グローバルリソースを含む有効なコントロールがホームリージョンでサポートされていない場合、Security Hub CSPM は、コントロールがサポートされているリンクされた 1 つのリージョンでコントロールを有効にしようとします。中央設定では、ホームリージョンまたはリンクされたリージョンで利用できないコントロールのカバレッジがありません。
> グローバルリソースを含むコントロールのリストについては、「グローバルリソースを使用するコントロール」を参照してください。

Security Hub CSPM console

設定ポリシーを作成して関連付けるには

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

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

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

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

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

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

   - 設定ポリシーをルートに適用する場合は、[すべてのアカウント] を選択します。これには、別のポリシーが適用されていない、または継承されていない組織内のすべてのアカウントと OU が含まれます。
   - 設定ポリシーを特定のアカウントまたは OU に適用する場合は、[特定のアカウント] を選択します。アカウント ID を入力するか、組織構造からアカウントと OU を選択します。ポリシーは、作成時に最大 15 個のターゲット (アカウント、OU、またはルート) に適用できます。さらに多く指定するには、作成後にポリシーを編集し、他のターゲットに適用します。

- [委任された管理者のみ] を選択すると、現在の委任管理者アカウントに設定ポリシーが適用されます。

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

Security Hub CSPM API

設定ポリシーを作成して関連付けるには

1. ホームリージョンの Security Hub CSPM 委任管理者アカウントから CreateConfigurationPolicy API を呼び出します。
2. `Name` には、設定ポリシーの一意の名前を入力します。オプションで、`Description` に設定ポリシーの説明を入力します。
3. `ServiceEnabled` フィールドで、この設定ポリシーで Security Hub CSPM を有効または無効にするかどうかを指定します。
4. `EnabledStandardIdentifiers` フィールドで、この設定ポリシーで有効にする Security Hub CSPM 標準を指定します。
5. `SecurityControlsConfiguration` オブジェクトで、この設定ポリシーで有効または無効にするコントロールを指定します。`EnabledSecurityControlIdentifiers` を選択すると、指定したコントロールが有効になります。有効になっている標準に含まれるその他のコントロール (新しくリリースされたコントロールを含む) は無効になります。`DisabledSecurityControlIdentifiers` を選択すると、指定したコントロールが無効になります。有効になっている標準に含まれるその他のコントロール (新しくリリースされたコントロールを含む) が有効になります。
6. オプションで、`SecurityControlCustomParameters` フィールドに、パラメータをカスタマイズする有効なコントロールを指定します。`ValueType` フィールドに `CUSTOM` を指定し、`Value` フィールドにカスタムパラメータ値を指定します。値は正しいデータ型で、Security Hub CSPM で指定された有効な範囲内である必要があります。カスタムパラ

メータ値をサポートするコントロールのみ選択します。詳細については、「Security Hub CSPM のコントロールパラメータについて」を参照してください。

7. アカウントまたは OUs に設定ポリシーを適用するには、ホームリージョンの Security Hub CSPM 委任管理者アカウントから StartConfigurationPolicyAssociation API を呼び出します。
8. `ConfigurationPolicyIdentifier` フィールドに、ポリシーの Amazon リソースネーム (ARN) または 一意識別子 (UUID) を入力します。ARN と UUID は `CreateConfigurationPolicy` API によって返されます。セルフマネージド設定の場合、`ConfigurationPolicyIdentifier` フィールドは `SELF_MANAGED_SECURITY_HUB` に等しくなります。
9. `Target` フィールドには、この設定ポリシーを適用する OU、アカウント、またはルート ID を指定します。各 API リクエストに指定できるターゲットは 1 つのみです。選択したターゲットの子アカウントと OU は、セルフマネージド型であるか、別の設定ポリシーを使用している場合を除き、自動的にこの設定ポリシーを継承します。

設定ポリシーを作成する API リクエストの例:

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

```
                                    }
                                }
                            }
                        }
                    ]
                }
            }
        }
    }
```

設定ポリシーを関連付ける API リクエストの例:

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

AWS CLI

設定ポリシーを作成して関連付けるには

1. ホームリージョンの Security Hub CSPM 委任管理者アカウントから create-configuration-policy コマンドを実行します。
2. `name` には、設定ポリシーの一意の名前を入力します。オプションで、`description` に設定ポリシーの説明を入力します。
3. `ServiceEnabled` フィールドで、この設定ポリシーで Security Hub CSPM を有効または無効にするかどうかを指定します。
4. `EnabledStandardIdentifiers` フィールドで、この設定ポリシーで有効にする Security Hub CSPM 標準を指定します。
5. `SecurityControlsConfiguration` フィールドで、この設定ポリシーで有効または無効にするコントロールを指定します。`EnabledSecurityControlIdentifiers` を選択すると、指定したコントロールが有効になります。有効になっている標準に含まれるその他のコントロール (新しくリリースされたコントロールを含む) は無効になります。`DisabledSecurityControlIdentifiers` を選択すると、指定したコントロールが無効になります。有効になっている標準に適用されるその他のコントロール (新しくリリースされたコントロールを含む) が有効になります。

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

設定ポリシーを作成するコマンドの例:

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

設定ポリシーを関連付けるコマンドの例:

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

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

設定ポリシーのステータスと詳細の確認

委任 AWS Security Hub CSPM 管理者は、組織の設定ポリシーとその詳細を表示できます。これには、ポリシーが関連付けられているアカウントと組織単位 (OU) が含まれます。

中央設定の利点とその仕組みについては、「Security Hub CSPM の中央設定について」を参照してください。

任意の方法を選択し、その手順に従って設定ポリシーを表示します。

Security Hub CSPM console

設定ポリシーを表示するには (コンソール)

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

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

Security Hub CSPM API

すべての設定ポリシーの概要リストを表示するには、Security Hub CSPM API の ListConfigurationPoliciesオペレーションを使用します。を使用する場合は AWS CLI、 list-configuration-policies コマンドを実行します。委任 Security Hub CSPM 管理者アカウントは、ホームリージョンで オペレーションを呼び出す必要があります。

```
$ aws securityhub list-configuration-policies \
--max-items 5 \
```

```
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf
```

特定の設定ポリシーの詳細を表示するには、GetConfigurationPolicy オペレーションを使用します。を使用する場合は AWS CLI、 を実行しますget-configuration-policy。委任管理者アカウントは、ホームリージョンでオペレーションを呼び出す必要があります。詳細を表示する設定ポリシーの Amazon リソースネーム (ARN) または ID を指定します。

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

すべての設定ポリシーとそのアカウント関連付けの概要リストを表示するには、ListConfigurationPolicyAssociations オペレーションを使用します。を使用する場合は AWS CLI、 list-configuration-policy-associations コマンドを実行します。委任管理者アカウントは、ホームリージョンでオペレーションを呼び出す必要があります。オプションで、ページ分割パラメータを指定したり、特定のポリシー ID、関連付けタイプ、または関連付けステータスで結果をフィルタリングしたりできます。

```
$ aws securityhub list-configuration-policy-associations \
--filters '{"AssociationType": "APPLIED"}'
```

特定のアカウントの関連付けを表示するには、GetConfigurationPolicyAssociationオペレーションを使用します。を使用する場合は AWS CLI、 get-configuration-policy-association コマンドを実行します。委任管理者アカウントは、ホームリージョンでオペレーションを呼び出す必要があります。`target` の場合、アカウント番号、OU ID、またはルート ID を指定します。

```
$ aws securityhub get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

設定ポリシーの関連付けステータスの確認

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

- `BatchGetConfigurationPolicyAssociations`
- `GetConfigurationPolicyAssociation`
- `ListConfigurationPolicyAssociations`
- `StartConfigurationPolicyAssociation`

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

の値は、ポリシーの関連付けが保留中か、特定のアカウントの成功または失敗の状態かAssociationStatusを示します。ステータスが PENDING から SUCCESS または FAILED に変わるまで、最大 24 時間かかることがあります。ステータスが の場合、設定ポリシーで指定されたすべての設定がアカウントに関連付けられているSUCCESSことを意味します。ステータスが の場合、設定ポリシーで指定された 1 つ以上の設定がアカウントとの関連付けに失敗したFAILEDことを意味します。FAILED ステータスにかかわらず、アカウントはポリシーに従って部分的に設定できます。たとえば、Security Hub CSPM を有効にし、 AWS 基本的なセキュリティのベストプラクティスを有効にし、CloudTrail.1. 最初の 2 つの設定は成功する可能性がありますが、CloudTrail.1 設定は失敗する可能性があります。この例では、一部の設定が正しく設定されていてFAILEDも、関連付けステータスは です。

親 OU またはルートの関連付けステータスは、子のステータスによって異なります。すべての子の関連付けステータスが SUCCESS の場合、親の関連付けステータスは SUCCESS です。1 人以上の子の関連付けステータスが FAILED の場合、親の関連付けステータスは FAILED です。

の値は、関連するすべてのリージョンのポリシーの関連付けステータスAssociationStatusによって異なります。ホームリージョンとリンクされているすべてのリージョンで関連付けが成功すると、AssociationStatus の値は SUCCESS になります。これらの 1 つ以上のリージョンで関連付けに失敗すると、AssociationStatus の値は FAILED になります。

以下の動作は、AssociationStatus の値にも影響します。

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

新しいリンクされたリージョンを追加すると、Security Hub CSPM は、新しいリージョンの PENDING、SUCCESS、または FAILED状態にある既存の関連付けをレプリケートします。

関連付けステータスが であってもSUCCESS、ポリシーの一部である標準の有効化ステータスは不完全な状態に移行する可能性があります。その場合、Security Hub CSPM は標準のコントロールの結果を生成できません。詳細については、「標準のステータスの確認」を参照してください。

関連付けの失敗のトラブルシューティング

AWS Security Hub CSPM では、以下の一般的な理由で設定ポリシーの関連付けが失敗することがあります。

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

設定ポリシーの更新

設定ポリシーを作成した後、委任 AWS Security Hub CSPM 管理者アカウントはポリシーの詳細とポリシーの関連付けを更新できます。ポリシーの詳細が更新されると、設定ポリシーに関連付けられているアカウントは、更新されたポリシーの使用を自動的に開始します。

中央設定の利点とその仕組みについては、「Security Hub CSPM の中央設定について」を参照してください。

委任管理者は、次のポリシー設定を更新できます。

- Security Hub CSPM を有効または無効にします。
- 1 つ以上のセキュリティ標準を有効にします。
- 有効な標準でどのセキュリティコントロールが有効になっているかを示します。これを行うには、有効にする必要がある特定のコントロールのリストを指定します。Security Hub CSPM は、リリース時に新しいコントロールを含め、他のすべてのコントロールを無効にします。または、無効にする必要がある特定のコントロールのリストを指定することもできます。Security Hub CSPM は、リリース時に新しいコントロールを含む他のすべてのコントロールを有効にします。
- オプションで、有効な標準全体で有効になっているコントロールを選択してパラメータをカスタマイズできます。

任意の方法を選択し、その手順に従って設定ポリシーを更新します。

> **Note**
>
> 中央設定を使用する場合、Security Hub CSPM は、ホームリージョンを除くすべてのリージョンでグローバルリソースを含むコントロールを自動的に無効にします。設定ポリシーを通じて有効を選択したその他のコントロールは、利用可能なすべてのリージョンで有効になります。これらのコントロールの検出結果を 1 つのリージョンのみに制限するには、 AWS Config レコーダー設定を更新し、ホームリージョンを除くすべてのリージョンでグローバルリソース記録をオフにします。
> グローバルリソースを含む有効なコントロールがホームリージョンでサポートされていない場合、Security Hub CSPM は、コントロールがサポートされているリンクされた 1 つのリージョンでコントロールを有効にしようとします。中央設定では、ホームリージョンまたはリンクされたリージョンで利用できないコントロールのカバレッジがありません。
> グローバルリソースを含むコントロールのリストについては、「グローバルリソースを使用するコントロール」を参照してください。

Console

設定ポリシーを更新するには

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

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

2. ナビゲーションペインで、[設定]、[設定] の順に選択します。
3. [Policies] タブを選択します。
4. 編集する設定ポリシーを選択したら、[編集] を選択します。必要に応じて、ポリシーの設定を編集します。ポリシーの設定を変更せずにそのまま維持する場合は、このセクションはそのままにします。
5. [次へ] を選択します。必要に応じて、ポリシーの関連付けを編集します。ポリシーの関連付けを変更せずにそのまま維持する場合は、このセクションはそのままにします。更新時に、ポリシーを最大 15 個のターゲット (アカウント、OU、またはルート) に関連付けるか、関連付けを解除できます。
6. [次へ] を選択します。
7. 更新内容を確認して [保存] を選択して適用します。ホームリージョンとリンクされたリージョンでは、このアクションは、この設定ポリシーに関連付けられているアカウントの既存の設定よりも優先されます。アカウントは、アプリケーションを通じて設定ポリシーに関連付けることも、親ノードから継承することもできます。

API

設定ポリシーを更新するには

1. 設定ポリシーの設定を更新するには、ホームリージョンの Security Hub CSPM 委任管理者アカウントから UpdateConfigurationPolicy API を呼び出します。
2. 更新する設定ポリシーの Amazon リソースネーム (ARN) または ID を指定します。
3. `ConfigurationPolicy` の下のフィールドに、更新された値を入力します。オプションで、更新の理由も指定できます。
4. この設定ポリシーに新しい関連付けを追加するには、ホームリージョンの Security Hub CSPM 委任管理者アカウントから StartConfigurationPolicyAssociation API を呼び出します。1 つ以上の現在の関連付けを削除するには、ホームリージョンの Security Hub CSPM 委任管理者アカウントから StartConfigurationPolicyDisassociation API を呼び出します。
5. `ConfigurationPolicyIdentifier` フィールドには、関連付けを更新する設定ポリシーの ARN または ID を指定します。

6. `Target` フィールドには、関連付けるまたは関連付けを解除するアカウント、OU、またはルート ID を指定します。このアクションは、指定した OU またはアカウントに対する以前のポリシー関連付けを上書きします。

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

設定ポリシーを更新する API リクエストの例:

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

```
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

AWS CLI

設定ポリシーを更新するには

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

> **Note**
>
> `update-configuration-policy` コマンドを実行すると、Security Hub CSPM は `EnabledStandardIdentifiers`、、`EnabledSecurityControlIdentifiers`、`DisabledSe`
> よび `SecurityControlCustomParameters`フィールドの完全なリスト置換を実行しま

す。このコマンドを実行するたびに、有効にする標準の全リストと、有効または無効にしてパラメータをカスタマイズするコントロールの全リストを指定します。

設定ポリシーを更新するコマンドの例:

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

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

設定ポリシーの削除

設定ポリシーを作成すると、委任 AWS Security Hub CSPM 管理者はそのポリシーを削除できます。また、委任管理者はポリシーを保持したまま、特定のアカウントや組織単位 (OU) またはルートとの関連付けを解除することもできます。ポリシーの関連付けを解除する手順については、「ターゲットから設定の関連付けを解除する」を参照してください。

中央設定の利点とその仕組みについては、「Security Hub CSPM の中央設定について」を参照してください。

このセクションでは、設定ポリシーを削除する方法について説明します。

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

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

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

任意の方法を選択し、その手順に従って設定ポリシーを削除します。

Console

設定ポリシーを削除するには

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

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

API

設定ポリシーを削除するには

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

削除する設定ポリシーの Amazon リソースネーム (ARN) または ID を指定します。`ConflictException` エラーを受け取った場合でも、設定ポリシーは組織内のアカウントま

たは OU に適用されます。このエラーを解決するには、削除する前に、設定ポリシーとこれらのアカウントまたは OU との関連付けを解除します。

設定ポリシーを削除する API リクエストの例:

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

AWS CLI

設定ポリシーを削除するには

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

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

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

ターゲットから設定の関連付けを解除する

委任 AWS Security Hub CSPM 管理者アカウントから、アカウント、OU、またはルートから設定ポリシーまたはセルフマネージド設定の関連付けを解除できます。関連付けを解除すると、ポリシーは将来の使用のために保持されますが、特定のアカウント、OU、またはルートからの既存の関連付けは削除されます。関連付けを解除できるのは、継承された設定ではなく、直接適用された設定のみです。継承された設定を変更するには、影響を受けるアカウントまたは OU に設定ポリシーまたはセルフマネージド型の動作を適用します。また、必要な変更を含む新しい設定ポリシーを、最も近い親に適用することもできます。

関連付けを解除しても設定ポリシーは削除されません。ポリシーはアカウントに保持されるため、組織内の他のターゲットと関連付けることができます。設定ポリシーの削除手順については、「設定ポ

リシーの削除」を参照してください。関連付けの解除が完了すると、影響を受けるターゲットは、設定ポリシーまたは最も近い親のセルフマネージド型の動作を継承します。継承が可能な設定がない場合、ターゲットは関連付け解除前の設定を保持しますが、セルフマネージド型になります。

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

Console

アカウントまたは OU と現在の設定との関連付けを解除するには

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

   ホームリージョンの委任 Security Hub CSPM 管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで、[設定]、[設定] の順に選択します。
3. [組織] タブで、現在の設定との関連付けを解除したいアカウント、OU、またはルートを選択します。[編集] を選択します。
4. 委任管理者がターゲットに直接ポリシーを適用できるようにするには、[構成を定義] ページの [管理] で、適用される [ポリシー] を選択します。ターゲットに最も近い親の設定を継承する場合は、[継承済み] を選択します。いずれの場合も、委任管理者がターゲットの設定をコントロールします。アカウントまたは OU に独自の設定を管理する場合は、[セルフマネージド] を選択します。
5. 変更を確認したら、[次へ] と [適用] を選択します。このアクションは、対象範囲内のアカウントまたは OU の既存の設定が現在の選択内容と矛盾する場合、それらの設定を上書きします。

API

アカウントまたは OU と現在の設定との関連付けを解除するには

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

3. `Target` の場合、この設定ポリシーとの関連付けを解除するアカウント、OU、またはルートを指定します。

設定ポリシーの関連付けを解除する API リクエストの例:

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

AWS CLI

アカウントまたは OU と現在の設定との関連付けを解除するには

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

設定ポリシーの関連付けを解除するコマンドの例:

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

コンテキストでの標準またはコントロールの設定

AWS Security Hub CSPM で中央設定を使用する場合、委任 Security Hub CSPM 管理者は、Security Hub CSPM、セキュリティ標準、およびセキュリティコントロールを組織に対して設定する方法を

指定する設定ポリシーを作成できます。委任管理者は、ポリシーを特定のアカウントおよび組織単位 (OU) に関連付けることができます。ポリシーは、ホームリージョンとリンクされたすべてのリージョンで有効になります。委任管理者は、必要に応じて設定ポリシーを更新できます。

Security Hub CSPM コンソールでは、委任管理者は設定ページから、または既存のワークフローとのコンテキストで、2 つの方法で設定ポリシーを更新できます。後者は、セキュリティの検出結果を表示すると、環境に最も関連性の高い標準とコントロールを検出し、同時に設定できるため、有益です。

コンテキスト内設定は、Security Hub CSPM コンソールでのみ使用できます。プログラムにより、委任管理者は Security Hub CSPM API の UpdateConfigurationPolicyオペレーションを呼び出して、組織内の特定の標準またはコントロールの設定方法を変更する必要があります。

コンテキストで Security Hub CSPM 標準またはコントロールを設定するには、次の手順に従います。

コンテキストで標準またはコントロールを設定するには (コンソール)

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

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

2. ナビゲーションペインで、次のいずれかのオプションを選択します。

   - 標準を設定するには、セキュリティ標準を選択し、特定の標準を選択します。
   - コントロールを設定するには、コントロールを選択し、特定のコントロールを選択します。

3. コンソールには、既存の Security Hub CSPM 設定ポリシーと、選択した標準またはコントロールのステータスが一覧表示されます。既存の各設定ポリシーで標準またはコントロールを有効または無効にするオプションを選択します。コントロールでは、コントロールパラメータをカスタマイズすることもできます。コンテキスト内設定中に新しいポリシーを作成することはできません。新しいポリシーを作成するには、[設定]ページに移動し、[ポリシー]タブを選択し、[ポリシーの作成] を選択する必要があります。

4. 変更を加えたら、[次へ] を選択します。

5. 変更内容を確認したら、[適用] を選択します。更新は、変更された設定ポリシーに関連付けられているすべてのアカウントと OUs に影響します。更新は、ホームリージョンとリンクされたすべてのリージョンでも有効になります。

Security Hub CSPM での中央設定の無効化

AWS Security Hub CSPM で中央設定を無効にすると、委任された管理者は、複数の組織単位 (OUs) および で Security Hub CSPM AWS アカウント、セキュリティ標準、セキュリティコントロールを設定できなくなります AWS リージョン。代わりに、各リージョンでその設定のほとんどをアカウントごとに設定する必要があります。

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

中央設定を無効化すると、次の変更が行われます。

- 委任管理者は、組織の設定ポリシーを作成できなくなります。
- 設定ポリシーが適用または継承されたアカウントは、現在の設定を保持しますが、セルフマネージド型になります。
- 組織はローカル設定に切り替わります。ローカル設定では、Security Hub CSPM 設定の大部分を組織アカウントとリージョンごとに個別に設定する必要があります。委任管理者は、Security Hub CSPM、デフォルトのセキュリティ標準、および新しい組織アカウントのデフォルトの標準の一部であるすべてのコントロールを自動的に有効にすることを選択できます。デフォルトの標準は、 AWS Foundational Security Best Practices (FSBP) と Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 です。これらの設定は現在のリージョンでのみ有効で、新しい組織アカウントにのみ影響します。委任管理者は、どの標準がデフォルトになるかを変更できません。ローカル設定では、設定ポリシーの使用や OU レベルでの設定はサポートされていません。

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

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

Security Hub CSPM console

中央設定を無効化するには (コンソール)

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

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

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

Security Hub CSPM API

中央設定 (API) を無効にするには

1. UpdateOrganizationConfiguration API を呼び出します。
2. `OrganizationConfiguration` オブジェクト内の `ConfigurationType` フィールドを `LOCAL` に設定します。既存の設定ポリシーまたはポリシーの関連付けがある場合、API はエラーを返します。設定ポリシーの関連付けを解除するには、`StartConfigurationPolicyDisassociation` API を呼び出します。設定ポリシーを削除するには、`DeleteConfigurationPolicy` API を呼び出します。
3. 新しい組織アカウントで Security Hub CSPM を自動的に有効にする場合は、`AutoEnable`フィールドを に設定します`true`。デフォルトでは、このフィールドの値は であり`false`、Security Hub CSPM は新しい組織アカウントでは自動的に有効になっていません。必要に応じて、新しい組織アカウントでデフォルトのセキュリティ基準を自動的に有効にする場合は、`AutoEnableStandards` フィールドを `DEFAULT` に設定します。これは、デ

フォルト値です。新しい組織アカウントでデフォルトのセキュリティ基準を自動的に有効化しない場合は、AutoEnableStandards フィールドを NONE に設定します。

API リクエストの例:

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

AWS CLI

中央設定を無効にするには (AWS CLI)

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

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

Security Hub CSPM での管理者アカウントとメンバーアカウントの管理

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

メンバーアカウントを管理者に関連付けるには、Security Hub CSPM を と統合 AWS Organizations するか、Security Hub CSPM でメンバーシップの招待を手動で送受信します。

を使用したアカウントの管理 AWS Organizations

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

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

委任管理者を指定したら、中央設定で Security Hub CSPM でアカウントを管理することをお勧めします。これは、Security Hub CSPM をカスタマイズし、組織に適切なセキュリティカバレッジを確保する最も効率的な方法です。

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

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

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

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

招待によるアカウントの手動での管理

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

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

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

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

Security Hub CSPM で複数のアカウントを管理するための推奨事項

次のセクションでは、 AWS Security Hub CSPM でメンバーアカウントを管理する際に注意すべき制限と推奨事項をまとめます。

メンバーアカウントの最大数

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

管理者とメンバーの関係の作成

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

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

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

手動の招待プロセスでは、メンバーシップの招待の承諾はオプションです。

によるメンバーシップ AWS Organizations

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

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

また、 AWS セキュリティ関連の問題を 1 つの画面で管理できるように、セキュリティおよびコンプライアンスサービス全体で同じ DA アカウントを選択することをお勧めします。

招待によるメンバーシップ

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

> **Note**
>
> メンバーアカウントを管理するには、Security Hub CSPM の招待 AWS Organizations の代わりに を使用することをお勧めします。

サービス間の管理者アカウントの調整

Security Hub CSPM は、Amazon GuardDuty、Amazon Inspector、Amazon Macie などのさまざまな AWS サービスの結果を集約します。Security Hub CSPM では、GuardDuty の検出結果からピボットして Amazon Detective で調査を開始することもできます。

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

例えば、GuardDuty 管理アカウント A のユーザーは、GuardDuty コンソールで GuardDuty メンバーアカウント B と C の結果を表示できます。アカウント A が Security Hub CSPM を有効にした場合、アカウント A のユーザーは、Security Hub CSPM のアカウント B とアカウント C の GuardDuty の検出結果を自動的には表示しません。これらのアカウントには、Security Hub CSPM 管理者とメンバーの関係も必要です。

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

を使用した複数のアカウントの Security Hub CSPM の管理 AWS Organizations

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

Security Hub CSPM を と統合するには AWS Organizations、 で組織を作成します AWS Organizations。Organizations 管理アカウントは、1 つのアカウントを組織の Security Hub CSPM 委任管理者として指定します。その後、委任管理者は、組織内の他のアカウントに対して Security Hub CSPM を有効にし、それらのアカウントを Security Hub CSPM メンバーアカウントとして追加して、メンバーアカウントに対して許可されたアクションを実行できます。Security Hub CSPM 委任管理者は、最大 10,000 のメンバーアカウントに対して Security Hub CSPM を有効におよび管理できます。

委任された管理者が設定できる範囲は、中央設定を使用するかどうかによって異なります。中央設定を有効にすると、各メンバーアカウントと で Security Hub CSPM を個別に設定する必要はありません AWS リージョン。委任管理者は、リージョン間で指定されたメンバーアカウントと組織単位 (OUs) に特定の Security Hub CSPM 設定を適用できます。

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

- 中央設定を使用する場合は、Security Hub CSPM 設定ポリシーを作成して、メンバーアカウントと OUs の Security Hub CSPM を一元的に設定します。設定ポリシーを使用して、Security Hub CSPM の有効化と無効化、標準の有効化と無効化、コントロールの有効化と無効化を行うことができます。
- 新しいアカウントが組織に加わると、Security Hub CSPM メンバーアカウントとして自動的に扱われます。中央設定を使用する場合、OU に関連付けられた設定ポリシーには、その OU に含まれる既存のアカウントと新しいアカウントが含まれます。
- 既存の組織アカウントを Security Hub CSPM メンバーアカウントとして扱います。中央設定を使用すると、この処理は自動的に行われます。
- 組織に属するメンバーアカウントの関連付けを解除します。中央設定を使用している場合は、メンバーアカウントをセルフマネージド型として指定してからでないと、そのアカウントの関連付けを解除できません。または、Security Hub CSPM を無効にする設定ポリシーを、特定の一元管理されたメンバーアカウントに関連付けることもできます。

中央設定にオプトインしない場合、組織はローカル設定と呼ばれるデフォルトの設定タイプを使用します。ローカル設定では、委任管理者は、メンバーアカウントで設定を強制する機能が制限されます。詳細については、「Security Hub CSPM のローカル設定について」を参照してください。

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

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

トピック

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

Security Hub CSPM と の統合 AWS Organizations

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

中央設定を使用する場合、委任管理者は、Security Hub CSPM サービス、標準、コントロールを組織アカウントで設定する方法を指定する Security Hub CSPM 設定ポリシーを作成することもできます。

組織の作成

組織は、単一のユニットとして管理 AWS アカウント できるように を統合するために作成するエンティティです。

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

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

委任 Security Hub CSPM 管理者を選択するための推奨事項

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

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

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

委任管理者を設定するために必要なアクセス許可の検証

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

必要なアクセス許可をすべて付与するには、次の Security Hub CSPM 管理ポリシーを組織管理アカウントの IAM プリンシパルにアタッチします。

- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess

委任管理者を指定する

委任 Security Hub CSPM 管理者アカウントを指定するには、Security Hub CSPM コンソール、Security Hub CSPM API、または を使用できます AWS CLI。Security Hub CSPM は、委任された管理者を現在の AWS リージョン のみに設定し、他のリージョンで アクションを繰り返す必要があります。中央設定の使用を開始すると、Security Hub CSPM はホームリージョンとリンクされたリージョンに同じ委任管理者を自動的に設定します。

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

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

次のいずれかの方法を使用して、委任 Security Hub CSPM 管理者を指定する必要があります。Organizations APIs で委任 Security Hub CSPM 管理者を指定しても、Security Hub CSPM には反映されません。

任意の方法を選択し、手順に従って委任 Security Hub CSPM 管理者アカウントを指定します。

Security Hub CSPM console

委任 Security Hub 管理者をオンボーディング中に削除するには

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

[設定] ページから 委任管理者の委任を解除するには

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

現在のアカウントを削除するには、[Delegated Administrator] (代理管理者) で、[Remove] (削除) を選択します。

4. Security Hub CSPM 管理者アカウントとして指定するアカウントのアカウント ID を入力します。

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

5. [委任] を選択します。

Security Hub CSPM API, AWS CLI

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

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

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

委任管理者の削除または変更

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

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

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

Security Hub CSPM コンソールを使用して 1 つのリージョンで委任された管理者を削除すると、すべてのリージョンで自動的に削除されます。

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

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

委任管理者の削除 (Organizations API、 AWS CLI)

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

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

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

Organizations API, AWS CLI

委任 Security Hub CSPM 管理者を削除するには

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

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

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

委任管理者の削除 (Security Hub CSPM コンソール)

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

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

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

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

Security Hub CSPM へようこそページから委任 Security Hub CSPM 管理者アカウントを削除するには

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

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

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

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

委任管理者の削除 (Security Hub CSPM API、 AWS CLI)

の Security Hub CSPM API または Security Hub CSPM オペレーションを使用して AWS CLI 、委任 Security Hub CSPM 管理者を削除できます。上記のいずれかの方法で委任された管理者を削除する

場合、API コールまたはコマンドが発行されたリージョンでのみ削除されます。Security Hub CSPM は他のリージョンを更新せず、委任管理者アカウントも削除しません AWS Organizations。

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

Security Hub CSPM API, AWS CLI

委任 Security Hub CSPM 管理者を削除するには

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

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

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

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

AWS Organizations 組織が AWS Security Hub CSPM と統合されると、Organizations 管理アカウントはその後統合を無効にすることができます。Organizations 管理アカウントのユーザーは、Security Hub CSPM の信頼されたアクセスを無効にすることでこれを行うことができます AWS Organizations。

Security Hub CSPM の信頼されたアクセスを無効にすると、以下が発生します。

- Security Hub CSPM は、信頼されたサービスとしてのステータスを失います AWS Organizations。
- Security Hub CSPM 委任管理者アカウントは、すべての Security Hub CSPM メンバーアカウントの Security Hub CSPM 設定、データ、リソースにアクセスできなくなります AWS リージョン。
- 中央設定を使用している場合、Security Hub CSPM は組織での使用を自動的に停止します。設定ポリシーとポリシーの関連付けは削除されます。アカウントでは、信頼されたアクセスを無効にする前の設定が保持されます。
- すべての Security Hub CSPM メンバーアカウントはスタンドアロンアカウントになり、現在の設定を保持します。1 つ以上のリージョンのメンバーアカウントで Security Hub CSPM が有効になっている場合、Security Hub CSPM はそれらのリージョンのアカウントで引き続き有効になり

ます。有効になっている標準とコントロールも変わりません。これらの設定は、アカウントやリージョンごとに個別に変更できます。ただし、そのアカウントはどのリージョンの委任管理者とも関連付けられなくなります。

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

信頼されたアクセスを無効にするには、 AWS Organizations コンソール、Organizations API、または を使用できます AWS CLI。Organizations 管理アカウントのユーザーのみが、Security Hub CSPM の信頼されたサービスアクセスを無効にできます。必要なアクセス許可に関する詳細は、AWS Organizations ユーザーガイドの信頼できるアクセスを無効にするために必要なアクセス許可を参照してください。

信頼されたアクセスを無効にする前に、組織の委任管理者と協力して、メンバーアカウントで Security Hub CSPM を無効にし、それらのアカウントの Security Hub CSPM リソースをクリーンアップすることをお勧めします。

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

Organizations console

Security Hub CSPM の信頼されたアクセスを無効にするには

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

Organizations API

Security Hub CSPM の信頼されたアクセスを無効にするには

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

AWS CLI

Security Hub CSPM の信頼されたアクセスを無効にするには

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

例:

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

新しい組織アカウントで Security Hub CSPM を自動的に有効にする

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

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

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

新しい組織アカウントを自動的に有効にする (中央設定)

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

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

設定ポリシーでは、OU で有効にするセキュリティ標準とコントロールを定義することもできます。有効な標準のコントロール結果を生成するには、OU のアカウントで必要なリソースを記録するように AWS Config を有効にして設定する必要があります。 AWS Config 記録の詳細については、「有効化と設定 AWS Config」を参照してください。

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

新しい組織アカウントを自動的に有効にする (ローカル設定)

ローカル設定を使用してデフォルト標準の自動有効化を有効にすると、Security Hub CSPM は新しい組織アカウントをメンバーとして追加し、現在のリージョンで Security Hub CSPM を有効にします。他のリージョンは影響を受けません。さらに、自動有効化を有効にしても、メンバーアカウントとして既に追加されていない限り、既存の組織アカウントで Security Hub CSPM は有効になりません。

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

デフォルトの標準 (および他の有効な標準) のコントロール結果を生成するには、組織内のアカウントが、必要なリソースを記録するように AWS Config 有効化および設定されている必要があります。AWS Config 記録の詳細については、「有効化と設定 AWS Config」を参照してください。

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

Security Hub CSPM console

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

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

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

Security Hub CSPM API

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

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

AWS CLI

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

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

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

新しい組織アカウントで Security Hub CSPM を手動で有効にする

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

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

別の組織内のメンバーアカウントがすでにある場合、アカウントで Security Hub CSPM を有効にすることはできません。

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

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

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

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

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

Security Hub CSPM console

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

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

委任された管理者アカウントの認証情報を使用してサインインします。

2. Security Hub の CSPM ナビゲーションペインの「設定」で、「設定」を選択します。
3. [アカウント] リストで、有効にする各組織アカウントを選択します。
4. [アクション]、[メンバーを追加] の順に選択します。

Security Hub CSPM API

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

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

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

AWS CLI

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

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

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

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

例

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

組織から Security Hub CSPM メンバーアカウントの関連付けを解除する

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

> **Note**
>
> 中央設定を使用する場合、関連付け解除の仕組みが異なります。1 つ以上の一元管理メンバーアカウントで Security Hub CSPM を無効にする設定ポリシーを作成できます。その後、これらのアカウントは引き続き組織の一部ですが、Security Hub CSPM の結果は生成されません。中央設定を使用しているが、手動で招待したメンバーアカウントも含まれている場合は、手動で招待した 1 つ以上のアカウントの関連付けを解除できます。

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

メンバーアカウントの関連付けを解除しても、アカウントは削除されません。その代わり、組織からメンバーアカウントが削除されます。関連付けが解除され AWS アカウント たメンバーアカウントは、Security Hub CSPM との統合によって管理されなくなったスタンドアロンアカウントになります AWS Organizations。

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

Security Hub CSPM console

組織とのメンバーアカウントの関連付けを解除するには

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

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

Security Hub CSPM API

組織とのメンバーアカウントの関連付けを解除するには

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

AWS CLI

組織とのメンバーアカウントの関連付けを解除するには

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

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

例

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

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

Security Hub CSPM での招待によるアカウントの管理

Security AWS Hub CSPM を と統合 AWS Organizations するか、メンバーシップの招待を手動で送受信することで、複数の Security Hub CSPM アカウントを 2 つの方法で一元管理できます。スタンドアロンアカウントを持っている場合、または と統合していない場合は、手動プロセスを使用する必要があります AWS Organizations。手動アカウント管理では、Security Hub CSPM 管理者はアカウントをメンバーに招待します。管理者とメンバーの関係は、候補となるメンバーが招待を承諾したときに確立されます。Security Hub CSPM 管理者アカウントは、招待ベースのメンバーアカウントを最大 1,000 個管理できます。

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

めします。詳細については、「を使用した複数のアカウントの Security Hub CSPM の管理 AWS Organizations」を参照してください。

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

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

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

Security Hub CSPM コンソールの設定ページで、招待によって追加されたアカウントが招待アカウントタブに表示されます。中央設定を使用しているが、組織外のアカウントを招待する場合は、このタブで招待ベースのアカウントの結果を表示できます。ただし、Security Hub CSPM 管理者は、設定ポリシーを使用してリージョン間で招待ベースのアカウントを設定することはできません。

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

トピック

- Security Hub CSPM でのメンバーアカウントの追加と招待
- Security Hub CSPM メンバーアカウントへの招待への応答
- Security Hub CSPM のメンバーアカウントの関連付けを解除する
- Security Hub CSPM でのメンバーアカウントの削除
- Security Hub CSPM 管理者アカウントからの関連付けの解除
- Security Hub CSPM でアカウントを管理するための Organizations への移行

Security Hub CSPM でのメンバーアカウントの追加と招待

> **Note**
>
> メンバーアカウントを管理するには、Security Hub CSPM の招待 AWS Organizations の代わりに を使用することをお勧めします。詳細については、「を使用した複数のアカウントの Security Hub CSPM の管理 AWS Organizations」を参照してください。

アカウントは、 AWS Security Hub CSPM メンバーアカウントへの招待を受け入れるアカウントの Security Hub CSPM 管理者になります。

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

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

メンバーアカウントの追加は、以下のステップで構成されています。

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

メンバーアカウントを組織に追加する

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

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

お好みの方法を選択し、手順に従ってメンバーアカウントを追加します。

Security Hub CSPM console

メンバーアカウントのリストにアカウントを追加するには

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

   管理者アカウントの認証情報を使用してサインインします。

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

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

     アカウントごとにこのプロセスを繰り返します。

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

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

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

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

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

     スプレッドシートプログラムでは、フィールドは別々の列に表示されます。基になる形式はコンマで区切られています。アカウント ID の書式設定は 10 進数以外の数値にする必要があります。たとえば、アカウント ID 444455556666 の場合、書式設定を

444455556666.0 とすることはできません。また、数値の書式設定によってアカウント ID の先頭のゼロが削除されないようにしてください。

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

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

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

Security Hub CSPM API

メンバーアカウントのリストにアカウントを追加するには

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

AWS CLI

メンバーアカウントのリストにアカウントを追加するには

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

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

例

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

メンバーアカウントの招待

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

Security Hub CSPM console

メンバー候補アカウントを招待するには

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

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

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

Security Hub CSPM API

メンバー候補アカウントを招待するには

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

AWS CLI

メンバー候補アカウントを招待するには

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

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

例

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

Security Hub CSPM メンバーアカウントへの招待への応答

> **Note**
>
> メンバーアカウントを管理するには、Security Hub CSPM の招待 AWS Organizations の代わりに を使用することをお勧めします。詳細については、「を使用した複数のアカウントの Security Hub CSPM の管理 AWS Organizations」を参照してください。

AWS Security Hub CSPM メンバーアカウントへの招待を承諾または拒否できます。

招待を受け入れると、アカウントは Security Hub CSPM メンバーアカウントになります。招待を送信したアカウントは、Security Hub CSPM 管理者アカウントになります。管理者アカウントユーザーは、Security Hub CSPM でメンバーアカウントの結果を表示できます。

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

メンバーアカウントへの招待は 1 つしか承諾できません。

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

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

招待の承諾

管理者アカウントから Security Hub CSPM メンバーアカウントへの招待を送信できます。その後、メンバーアカウントにサインインした後に招待を承諾できます。

お好みの方法を選択し、手順に従ってメンバーアカウントへの招待を承諾します。

Security Hub CSPM console

メンバーシップの招待を承諾するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで、[Settings] (設定) を選択し、[Accounts] (アカウント) を選択します。

3. [管理者アカウント] セクションで、[承諾] をオンにし、[招待を承諾] を選択します。

Security Hub CSPM API

メンバーシップの招待を承諾するには

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

AWS CLI

メンバーシップの招待を承諾するには

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

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

例

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

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

招待の拒否

Security Hub CSPM メンバーアカウントへの招待を拒否できます。Security Hub CSPM コンソールで招待を拒否すると、アカウントは管理者アカウントのメンバーアカウントのリストで Resigned としてマークされます。署名ステータスは、管理者アカウントを使用して Security Hub CSPM コンソールにサインインした場合にのみ表示されます。ただし、管理者アカウントにサインインして招待を削除するまで、招待はメンバーアカウントのコンソールで変更されません。

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

お好みの方法を選択し、手順に従ってメンバーアカウントへの招待を拒否します。

Security Hub CSPM console

メンバーシップへの招待を拒否するには

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

Security Hub CSPM API

メンバーシップへの招待を拒否するには

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

AWS CLI

メンバーシップへの招待を拒否するには

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

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

例

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

Security Hub CSPM のメンバーアカウントの関連付けを解除する

> **Note**
>
> メンバーアカウントを管理するには、Security Hub CSPM の招待 AWS Organizations の代わりに を使用することをお勧めします。詳細については、「を使用した複数のアカウントの Security Hub CSPM の管理 AWS Organizations」を参照してください。

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

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

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

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

Security Hub CSPM console

手動で招待したメンバーアカウントの関連付けを解除するには

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

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

Security Hub CSPM API

手動で招待したメンバーアカウントの関連付けを解除するには

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

AWS CLI

手動で招待したメンバーアカウントの関連付けを解除するには

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

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

例

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

Security Hub CSPM でのメンバーアカウントの削除

> **Note**
>
> メンバーアカウントを管理するには、Security Hub CSPM の招待 AWS Organizations の代わりに を使用することをお勧めします。詳細については、「を使用した複数のアカウントの Security Hub CSPM の管理 AWS Organizations」を参照してください。

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

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

組織に属するアカウントと、 との統合を使用して管理されているアカウントを削除することはできません AWS Organizations。

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

Security Hub CSPM console

手動で招待したメンバーアカウントを削除するには

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

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

Security Hub CSPM API

手動で招待したメンバーアカウントを削除するには

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

AWS CLI

手動で招待したメンバーアカウントを削除するには

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

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

例

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

Security Hub CSPM 管理者アカウントからの関連付けの解除

> **Note**
>
> メンバーアカウントを管理するには、Security Hub CSPM の招待 AWS Organizations の代わりに を使用することをお勧めします。詳細については、「を使用した複数のアカウントの Security Hub CSPM の管理 AWS Organizations」を参照してください。

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

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

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

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

Security Hub CSPM console

管理者アカウントとの関連付けを解除するには

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

Security Hub CSPM API

管理者アカウントとの関連付けを解除するには

`DisassociateFromAdministratorAccount` API を呼び出します。

AWS CLI

管理者アカウントとの関連付けを解除するには

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

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

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

Security Hub CSPM でアカウントを管理するための Organizations への移行

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

Security Hub CSPM と を統合することで AWS Organizations、招待を送信する必要がなくなり、Security Hub CSPM が組織内でどのように設定およびカスタマイズされるかをより詳細に制御できます。このため、Security Hub CSPM の招待の代わりに を使用して AWS Organizations メンバーアカウントを管理することをお勧めします。詳細については、「を使用した複数のアカウントの Security Hub CSPM の管理 AWS Organizations」を参照してください。

AWS Organizations 統合を使用する複合アプローチを使用できますが、組織外にアカウントを手動で招待することもできます。ただし、Organizations の統合のみを使用することをお勧めします。中央設定は、複数のアカウントとリージョンで Security Hub CSPM を管理するのに役立つ機能であり、Organizations と統合する場合にのみ使用できます。

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

Security Hub CSPM と の統合 AWS Organizations

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

次の手順を完了することで、これらのサービスを統合できます。

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

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

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

前のステップを完了することで、Security Hub CSPM の信頼されたアクセスを許可します AWS Organizations。これにより、委任管理者アカウントの現在の で Security Hub CSPM AWS リージョン も有効になります。

委任管理者は、主に組織のアカウントを Security Hub CSPM メンバーアカウントとして追加することで、Security Hub CSPM で組織を管理できます。管理者は、それらのアカウントの特定の Security Hub CSPM 設定、データ、リソースにアクセスすることもできます。

Organizations を使用してアカウント管理に移行する場合、招待ベースのアカウントは自動的に Security Hub CSPM メンバーになることはありません。新しい組織に追加するアカウントのみが Security Hub CSPM メンバーになることができます。

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

Security Hub CSPM で管理者アカウントとメンバーアカウントによって許可されるアクション

管理者アカウントとメンバーアカウントは、次の表に示す AWS Security Hub CSPM アクションにアクセスできます。テーブルの値の意味は次のとおりです。

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

表で説明したように、許可されるアクションは、 と統合するかどうか AWS Organizations 、および組織が使用する設定タイプによって異なります。中央設定とローカル設定の違いについては、「を使用したアカウントの管理 AWS Organizations」を参照してください。

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

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

次の表は、管理者アカウントとメンバーアカウントのデフォルトのアクセス許可を示しています。カスタム IAM ポリシーを使用して、Security Hub CSPM の機能と関数へのアクセスをさらに制限できます。ガイダンスと例については、ブログ記事「IAM ポリシーを AWS Security Hub CSPM のユーザーペルソナに調整する」を参照してください。

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

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

アクション	Security Hub CSPM 委任管理者アカウント	一元管理型メンバーアカウント	セルフマネージド型メンバーアカウント
Security Hub CSPM 設定ポリシーの作成と管理	セルフマネージド型アカウントおよび一元管理型アカウント用	–	–

アクション	Security Hub CSPM 委任管理者アカウント	一元管理型メンバーアカウント	セルフマネージド型メンバーアカウント
組織のアカウントを表示する	いずれか	–	–
メンバーアカウントの関連付けを解除する	いずれか	–	–
メンバーアカウントを削除する	組織以外のアカウントすべて	–	–
Security Hub CSPM を無効にする	現在のアカウントおよび一元管理型アカウント用	–	現在 (管理者アカウントから関連付けを解除する必要があります)
検出結果と検索履歴を表示する	いずれか	Current	Current
結果を更新する	いずれか	Current	Current
インサイトの結果を表示する	いずれか	Current	Current
コントロールの詳細を表示する	いずれか	Current	Current
統合コントロール検出結果のオン/オフを切り替える	いずれか	–	–
標準を有効または無効にする	現在のアカウントおよび一元管理型アカウント用	–	Current

アクション	Security Hub CSPM 委任管理者アカウント	一元管理型メンバーアカウント	セルフマネージド型メンバーアカウント
コントロールを有効または無効にする	現在のアカウントおよび一元管理型アカウント用	–	Current
統合を有効または無効にする	Current	Current	Current
クロスリージョン集約を設定する	いずれか	–	–
ホームリージョンとリンクされたリージョンを選択する	すべて (ホームリージョンを変更するには、中央設定をいったん停止して再起動する必要があります)	–	–
カスタムアクションを設定する	Current	Current	Current
自動化ルールを設定する	いずれか	–	–
カスタムインサイトを設定する	Current	Current	Current

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

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

アクション	Security Hub CSPM 委任管理者アカウント	メンバーアカウント
Security Hub CSPM 設定ポリシーの作成と管理	–	–
組織のアカウントを表示する	いずれか	–
メンバーアカウントの関連付けを解除する	いずれか	–
メンバーアカウントを削除する	–	–
Security Hub CSPM を無効にする	–	現在 (アカウントと委任された管理者との関連付けが解除されている場合)
検出結果と検索履歴を表示する	いずれか	Current
結果を更新する	いずれか	Current
インサイトの結果を表示する	いずれか	Current
コントロールの詳細を表示する	いずれか	Current
統合コントロール検出結果のオン/オフを切り替える	いずれか	–
標準を有効または無効にする	Current	Current
新しい組織アカウントで Security Hub CSPM とデフォルト標準を自動的に有効にする	現在のアカウントと新しい組織アカウント用	–

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

招待ベースのアカウントで許可されるアクション

招待ベースの方法を使用して、 と統合するのではなく、アカウントを手動で管理する場合、管理者アカウントとメンバーアカウントは、次のように Security Hub CSPM アクションにアクセスできます AWS Organizations。

アクション	Security Hub CSPM 管理者アカウント	メンバーアカウント
Security Hub CSPM 設定ポリシーの作成と管理	–	–
組織のアカウントを表示する	いずれか	–
メンバーアカウントの関連付けを解除する	いずれか	Current
メンバーアカウントを削除する	いずれか	–

アクション	Security Hub CSPM 管理者アカウント	メンバーアカウント
Security Hub CSPM を無効にする	現在 (有効なメンバーアカウントがない場合)	現在 (アカウントと管理者アカウントの関連付けが解除されている場合)
検出結果と検索履歴を表示する	いずれか	Current
結果を更新する	いずれか	Current
インサイトの結果を表示する	いずれか	Current
コントロールの詳細を表示する	いずれか	Current
統合コントロール検出結果のオン/オフを切り替える	いずれか	–
標準を有効または無効にする	Current	Current
新しい組織アカウントで Security Hub CSPM とデフォルト標準を自動的に有効にする	–	–
コントロールを有効または無効にする	Current	Current
統合を有効または無効にする	Current	Current
クロスリージョン集約を設定する	いずれか	–
カスタムアクションを設定する	Current	Current
自動化ルールを設定する	いずれか	–

アクション	Security Hub CSPM 管理者アカウント	メンバーアカウント
カスタムインサイトを設定する	Current	Current

Security Hub CSPM データに対するアカウントアクションの影響

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

Security Hub CSPM が無効

中央設定を使用する場合、委任管理者 (DA) は、特定のアカウントおよび組織単位 (OUs) で Security Hub CSPM を無効にする AWS Security Hub CSPM 設定ポリシーを作成できます。この場合、Security Hub CSPM は、ホームリージョンとリンクされたリージョンの指定されたアカウントと OUs で無効になります。中央設定を使用しない場合は、Security Hub CSPM を有効にしたアカウントとリージョンごとに個別に無効にする必要があります。DA アカウントで Security Hub CSPM が無効になっている場合、中央設定を使用することはできません。

管理者アカウントで Security Hub CSPM が無効になっている場合、管理者アカウントの結果は生成または更新されません。アーカイブされた既存の検出結果は 30 日後に削除されます。既存のアクティブな検出結果は 90 日後に削除されます。

他の との統合 AWS のサービス は削除されます。

有効になっているセキュリティ標準およびコントロールは無効になります。

カスタムアクション、インサイト、サードパーティー製品のサブスクリプションなど、他の Security Hub CSPM データおよび設定は 90 日間保持されます。

管理者アカウントからメンバーアカウントとの関連付けを解除する

メンバーアカウントが管理者アカウントとの関連付けを解除されると、管理者アカウントはそのメンバーアカウントの結果を表示するための許可を失います。ただし、Security Hub CSPM は両方のアカウントで引き続き有効になっています。

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

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

Security Hub CSPM 管理者アカウントのアカウントリストで、削除されたアカウントのステータスは関連付け解除です。

メンバーアカウントが組織から削除されている

メンバーアカウントが組織から削除されると、Security Hub CSPM 管理者アカウントは、メンバーアカウントの結果を表示するアクセス許可を失います。ただし、Security Hub CSPM は、削除前と同じ設定で両方のアカウントで引き続き有効になっています。

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

Security Hub CSPM 管理者アカウントのアカウントリストで、削除されたアカウントのステータスは Deleted です。

アカウントの停止

AWS アカウント が停止されると、アカウントは Security Hub CSPM で検出結果を表示するアクセス許可を失います。そのアカウントの結果は生成または更新されません。停止されたアカウントの管理者アカウントは、アカウントの既存の検出結果を表示できます。

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

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

90 日後、アカウントは削除または再アクティブ化されます。アカウントが再アクティブ化されると、Security Hub CSPM アクセス許可が復元されます。メンバーアカウントのステータスが

[Account Suspended] (アカウントの停止) の場合、管理者アカウントでそのアカウントを手動で有効にする必要があります。

アカウントの閉鎖

AWS アカウント が閉鎖されると、Security Hub CSPM は閉鎖に次のように応答します。

アカウントが Security Hub CSPM 管理者アカウントである場合、管理者アカウントとして削除され、すべてのメンバーアカウントが削除されます。アカウントがメンバーアカウントの場合、関連付けが解除され、Security Hub CSPM 管理者アカウントからメンバーとして削除されます。

Security Hub CSPM は、アーカイブされた既存の検出結果を 30 日間アカウントに保持します。コントロールの検出結果の場合、30 日の計算は検出結果の `UpdatedAt`フィールドの値に基づきます。別のタイプの検出結果の場合、計算は、検出結果の フィールド`UpdatedAt`または`ProcessedAt`フィールドのいずれか遅い日付の値に基づきます。この 30 日間の終了時に、Security Hub CSPM はアカウントから検出結果を完全に削除します。

Security Hub CSPM は、アカウント内の既存のアクティブな検出結果を 90 日間保持します。コントロールの検出結果の場合、90 日の計算は検出結果の `UpdatedAt`フィールドの値に基づきます。別のタイプの検出結果の場合、計算は、検出結果の フィールド`UpdatedAt`または`ProcessedAt`フィールドのいずれか遅い日付の値に基づきます。この 90 日間の終了時に、Security Hub CSPM はアカウントから検出結果を完全に削除します。

既存の検出結果を長期間保持するには、検出結果を S3 バケットにエクスポートできます。これを行うには、Amazon EventBridge ルールでカスタムアクションを使用します。詳細については、「EventBridge を使用した自動応答と修復」を参照してください。

> **Important**
>
> のお客様は AWS GovCloud (US) Regions、アカウントを閉鎖する前に、ポリシーデータやその他のアカウントリソースをバックアップして削除してください。アカウントを閉鎖した後は、リソースとデータにアクセスできなくなります。

詳細については、「 AWS アカウント管理 リファレンスガイド」の「 AWS アカウントを閉じる」を参照してください。

Security Hub CSPM でのクロスリージョン集約について

> **Note**
>
> 集約リージョンがホームリージョンと呼ばれるようになりました。一部の Security Hub CSPM API オペレーションでは、依然として古い用語の集約リージョンを使用します。

AWS Security Hub CSPM でクロスリージョン集約を使用すると、検出結果、検出結果の更新、インサイト、コントロールコンプライアンスステータス、セキュリティスコアを複数の から単一のホームリージョン AWS リージョン に集約できます。その後は、これらすべてのデータをホームリージョンで管理できます。

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

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

コントロールが、リンクされたリージョンでは有効になっていても、ホームリージョンでは無効になっている場合、そのコントロールのコンプライアンスステータスはホームリージョンで確認できます。ただし、ホームリージョンからそのコントロールを有効または無効にすることはできません。ただし、中央設定を使用している場合は例外です。中央設定を使用する場合、委任 Security Hub CSPM 管理者は、ホームリージョンおよびホームリージョンからリンクされたリージョンでコントロールを設定できます。

ホームリージョンを設定した場合、セキュリティスコアはすべてのリンクされたリージョンのコントロールステータスを考慮します。

。クロスリージョンのセキュリティスコアとコンプライアンスステータスを表示するには、Security Hub CSPM を使用する IAM ロールに次のアクセス許可を追加します。

- ListSecurityControlDefinitions
- BatchGetStandardsControlAssociations
- BatchUpdateStandardsControlAssociations

集計されるデータのタイプ

クロスリージョン集約が 1 つ以上のリンクされたリージョンで有効になっている場合、Security Hub CSPM はリンクされたリージョンからホームリージョンに次のデータをレプリケートします。これは、クロスリージョン集約が有効になっているすべてのアカウントで発生します。

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

前のリストの新しいデータに加えて、Security Hub CSPM はリンクされたリージョンとホームリージョン間でこのデータの更新をレプリケートします。リンクされたリージョンで発生した更新は、ホームリージョンにレプリケートされます。ホームリージョンで発生した更新は、元のリンクされたリージョンにレプリケートされます。ホームリージョンとリンクされたリージョンに相反する更新がある場合は、最も新しい更新が使用されます。

クロスリージョン集約では、Security Hub CSPM のコストは増加しません。Security Hub CSPM が新しいデータまたは更新をレプリケートする場合、料金は発生しません。

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

ホームリージョンのセキュリティスコアは、リンクされているすべてのリージョンで有効になっているコントロールと、合格の状態にあるコントロールの数を比較して計算されます。また、コントロールが 1 つ以上のリンクされたリージョンで有効になっている場合、そのコントロールは、ホームリージョンの [セキュリティ標準] の詳細ページに表示されます。標準の詳細ページの、コントロー

ルのコンプライアンスステータスには、リンクされたリージョンの結果が反映されています。1 つまたは複数のリンクされたリージョンでコントロールに関連付けられたセキュリティチェックが失敗した場合、そのコントロールのコンプライアンスステータスは、ホームリージョンの標準の詳細ページに [失敗] と表示されます。セキュリティチェックの数値には、リンクされているすべてのリージョンの結果が含まれます。

Security Hub CSPM は、アカウントで Security Hub CSPM が有効になっているリージョンからのデータのみを集約します。Security Hub CSPM は、クロスリージョン集約設定に基づいてアカウントに対して自動的に有効になるわけではありません。

リンクされたリージョンを選択せずに、クロスリージョン集約を有効にできます。この場合、データレプリケーションは発生しません。

管理者アカウントとメンバーアカウントの集計

クロスリージョン集約は、スタンドアロンのアカウント、メンバーカウントおよび管理者アカウントによって設定できます。管理者が設定した場合、管理アカウントでクロスリージョン集約を使用するには、管理者アカウントの存在が不可欠です。管理者アカウントが削除されたりメンバーアカウントとの関連付けが解除されたりすると、そのメンバーアカウントに対するクロスリージョン集約は停止されます。これは、管理者とメンバーの関係が始まる前にクロスリージョン集約を有効にしていた場合でも、同様です。

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

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

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

管理者アカウントは、メンバーアカウントを手動で招待したり、統合されている組織の委任管理者として機能することができます AWS Organizations。手動で招待されたメンバーアカウントの場合、ク

クロスリージョン集約を機能させるには、管理者がホームリージョンとリンクされたすべてのリージョンのアカウントを招待する必要があります。さらに、管理者がメンバーアカウントの結果を表示できるようにするには、メンバーアカウントで、ホームリージョンとすべてのリンクされたリージョンで Security Hub CSPM が有効になっている必要があります。他の目的でホームリージョンを使用しない場合は、そのリージョンで Security Hub CSPM 標準と統合を無効にして、課金を防ぐことができます。

クロスリージョン集約を使用する予定で、複数の管理者アカウントがある場合、次のベストプラクティスを推奨します。

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

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

中央設定がクロスリージョン集約に与える影響

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

委任管理者は、ホームリージョンからのみ組織の設定ポリシーを作成および管理できます。また、設定ポリシーは、ホームリージョンおよびすべてのリンクされたリージョンで有効になります。一部のリンクされたリージョンにのみ適用され、他のリージョンには適用されない設定ポリシーは作成できません。クロスリージョン集約については、「クロスリージョン集約」を参照してください。

中央設定を使用するには、ホームリージョンを指定する必要があります。必要に応じて、リンクされたリージョンとして 1 つ以上のリージョンを選択できます。リンクされたリージョンなしでホームリージョンを指定することもできます。

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

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

中央設定の詳細については、「Security Hub CSPM の中央設定について」を参照してください。

クロスリージョン集約の有効化

> **Note**
>
> 集約リージョンがホームリージョンと呼ばれるようになりました。一部の Security Hub CSPM API オペレーションでは、依然として古い用語の集約リージョンを使用します。

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

クロスリージョン集約を有効にするには、検出結果アグリゲータと呼ばれる Security Hub CSPM リソースを作成します。検出結果アグリゲーターリソースは、ホームリージョンとリンクされたリージョン (存在する場合) を指定します。

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

クロスリージョン集約を有効にする場合、必要に応じて 1 つ以上のリンクされたリージョンを指定します。Security Hub CSPM がサポートを開始し、オプトインしたときに、新しいリージョンを自動的にリンクするかどうかを選択することもできます。

Security Hub CSPM console

クロスリージョン集約を拡張するには

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

   デフォルトでは、ホームリージョンは [集約リージョンなし] に設定されています。
5. [集約リージョン] で、オプションを選択して、ホームリージョンを集約リージョンとして指定します。
6. 必要に応じて、[リンクされたリージョン] で、データの集約元となるリージョンを選択します。
7. Security Hub CSPM がサポートし、オプトインするときに、パーティション内の新しいリージョンからデータを自動的に集約するには、今後のリージョンをリンクを選択します。
8. [保存] を選択します。

Security Hub CSPM API

ホームリージョンとして使用するリージョンから、Security Hub CSPM API の `CreateFindingAggregator`オペレーションを使用します。を使用する場合は AWS CLI、create-finding-aggregator コマンドを実行します。

[`RegionLinkingMode`] で、以下のいずれかのオプションを選択します。

- `ALL_REGIONS` – Security Hub CSPM は、すべてのリージョンのデータを集約します。また、Security Hub CSPM は、サポートされている新しいリージョンからのデータを集約し、オプトインします。
- `ALL_REGIONS_EXCEPT_SPECIFIED` – Security Hub CSPM は、除外するリージョンを除くすべてのリージョンのデータを集約します。また、Security Hub CSPM は、サポートされている新しいリージョンからのデータを集約し、オプトインします。`Regions` を使用して、集約から除外するリージョンのリストを提供します。

- `SPECIFIED_REGIONS` – Security Hub CSPM は、選択したリージョンのリストからデータを集約します。Security Hub CSPM は、新しいリージョンからのデータを自動的に集約しません。`Regions` を使用して、集約するリージョンのリストを提供します。
- `NO_REGIONS` – リンクされたリージョンを選択しないため、Security Hub CSPM はデータを集約しません。

以下の例では、クロスリージョン集約が設定されています。ホームリージョンは米国東部 (バージニア北部) です。リンクされたリージョンは、米国西部 (北カリフォルニア)と米国西部 (オレゴン) です。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

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

クロスリージョン集約設定の確認

> **Note**
>
> 集約リージョンがホームリージョンと呼ばれるようになりました。一部の Security Hub CSPM API オペレーションでは、依然として古い用語の集約リージョンを使用します。

現在のクロスリージョン集約設定は、任意の から AWS Security Hub CSPM で表示できます AWS リージョン。設定には、ホームリージョン、リンクされたリージョン (存在する場合) 、Security Hub CSPM がサポートする新しいリージョンを自動的にリンクするかどうかが含まれます。

メンバーアカウントは、管理者アカウントが設定したクロスリージョン集約設定を閲覧できます。

任意の方法を選択し、ステップに従って現在のクロスリージョン集約の設定を表示します。

Security Hub CSPM console

クロスリージョン集約設定を表示するには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで、[設定]、[リージョン] タブの順に選択します。

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

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

- ホームリージョン
- Security Hub CSPM がサポートし、オプトインする新しいリージョンの検出結果、インサイト、コントロールステータス、セキュリティスコアを自動的に集計するかどうか
- リンクされたリージョンのリスト (選択されている場合)

Security Hub CSPM API

クロスリージョン集約設定を確認するには (Security Hub CSPM API)

Security Hub CSPM API の `GetFindingAggregator`オペレーションを使用します。を使用する場合は AWS CLI、get-finding-aggregator コマンドを実行します。

リクエストするときには、検出結果アグリゲーター ARN を指定します。検出結果アグリゲーター ARN を取得するには、 `ListFindingAggregators` オペレーションまたは list-finding-aggregators コマンドを使用します。

次の例は、指定された検出結果アグリゲーター ARN のクロスリージョン集約設定を示しています。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています

```
$aws securityhub get-finding-aggregator --finding-aggregator-
arn arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-
e89b-12d3-a456-426652340000
```

クロスリージョン集約設定の更新

> **Note**
>
> 集約リージョンがホームリージョンと呼ばれるようになりました。一部の Security Hub CSPM API オペレーションでは、依然として古い用語の集約リージョンを使用します。

リンクされたリージョンまたは現在のホームリージョンを変更することで、 AWS Security Hub CSPM で現在のクロスリージョン集約設定を更新できます。 AWS リージョン Security Hub CSPM がサポートされている新しい からデータを自動的に集計するかどうかを変更することもできます。

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

リンクされたリージョンからのデータの集約を停止しても、 AWS Security Hub CSPM は、ホームリージョンでアクセスできるそのリージョンから既存の集約データを削除しません。

このセクションの更新手順を使用して、ホームリージョンを変更することはできません。ホームリージョンを変更するには、以下を実行する必要があります:

1. クロスリージョン集約を停止します。手順については、「the section called “集約の停止”」を参照してください。
2. 新しいホームリージョンにするリージョンに変更します。
3. クロスリージョン集約を有効にします。手順については、「the section called “集約の有効化”」を参照してください。

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

Security Hub CSPM console

リンクされたリージョンを変更するには

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

   現在の集約リージョンにサインインします。
2. Security Hub の CSPM ナビゲーションメニューで、設定を選択し、リージョンを選択します。
3. [検出結果の集約] の場合は、[編集] を選択します。
4. [リンクされたリージョン] の場合はで、選択したリンクされたリージョンを更新します。
5. 必要に応じて、[Link future Regions] (将来のリージョンをリンクする) の選択を変更します。この設定は、Security Hub CSPM が新しいリージョンのサポートを追加してオプトインするときに、新しいリージョンを自動的にリンクするかどうかを決定します。
6. [保存] を選択します。

Security Hub CSPM API

UpdateFindingAggregator 操作を使用します。を使用する場合は AWS CLI、update-finding-aggregator コマンドを実行します。結果アグリゲーターを識別するには、結果アグリゲーター ARN を提供する必要があります。検出結果アグリゲーター ARN を取得するには、ListFindingAggregators オペレーションまたは list-finding-aggregators コマンドを使用します。

リンクモードが ALL_REGIONS_EXCEPT_SPECIFIED または SPECIFIED_REGIONS の場合、除外されるリージョンまたは含まれるリージョンのリストを変更できます。リージョンリンクモードを NO_REGIONS に変更する場合は、リージョンリストを指定しないでください。

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

以下の例では、クロスリージョン集約が、選択したリージョンに対して更新されています。コマンドは、現在のホームリージョンである米国東部 (バージニア北部) から実行されます。リンクされたリージョンは、米国西部 (北カリフォルニア)と米国西部 (オレゴン) です。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

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

クロスリージョン集約を停止する

> **Note**
> 集約リージョンがホームリージョンと呼ばれるようになりました。一部の Security Hub CSPM API オペレーションでは、依然として古い用語の集約リージョンを使用します。

AWS Security Hub CSPM でデータを集約しない場合は、検出結果アグリゲータを削除できます。または、既存のアグリゲータ AWS リージョン をリンクNO_REGIONSモードに更新することで、検出結果アグリゲータを保持できますが、ホームリージョンにリンクすることはできません。

ホームリージョンを変更するには、現在の検出結果アグリゲーターを削除し、新しい検出結果アグリゲータを作成する必要があります。

検出結果アグリゲータを削除すると、Security Hub CSPM はデータの集約を停止します。それによって、ホームリージョンから既存の集約データが削除されることはありません。

検出結果アグリゲーターの削除 (コンソール)

検出結果アグリゲーターは、現在のホームリージョンからのみ削除できます。

ホームリージョン以外のリージョンでは、Security Hub CSPM コンソールの検出結果集約パネルに、ホームリージョンの設定を編集する必要があるというメッセージが表示されます。このメッセージを選択して、ホームリージョンへと切り替えるリンクを表示します。

Security Hub CSPM console

クロスリージョン集約を停止するには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. 現在のホームリージョンにサインインしていることを確認します。
3. Security Hub CSPM ナビゲーションメニューで、設定を選択し、リージョンを選択します。
4. [Finding aggregation] (結果の集約) で、[Edit] (編集) を選択します。
5. [Aggregation Region] (集約リージョン) で、[No aggregation Region] (集約リージョンなし) を選択します。
6. [Save] (保存) を選択します。
7. 確認ダイアログの確認フィールドに、**`Confirm`** と入力します。
8. [Confirm] (確認) を選択します。

Security Hub CSPM API

Security Hub CSPM API の `DeleteFindingAggregator`オペレーションを使用します。を使用している場合は AWS CLI、 `delete-finding-aggregator` コマンドを実行します。

削除する検出結果アグリゲーターを識別するには、検出結果アグリゲーター ARN を指定します。検出結果アグリゲーター ARN を取得するには、 `ListFindingAggregators` オペレーションまたは `list-finding-aggregators` コマンドを使用します。

次の例では、検出結果アグリゲーターを削除します。コマンドは、現在のホームリージョンである米国東部 (バージニア北部) から実行されます。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$aws securityhub delete-finding-aggregator arn:aws:securityhub:us-
east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-a456-426652340000 --
region us-east-1
```

Security Hub CSPM のセキュリティ標準について

AWS Security Hub CSPM では、セキュリティ標準は規制フレームワーク、業界のベストプラクティス、または企業ポリシーに基づく一連の要件です。それぞれに適用されるセキュリティコントロールなど、Security Hub CSPM が現在サポートしている標準の詳細については、「」を参照してくださいSecurity Hub CSPM の標準リファレンス。

標準を有効にすると、Security Hub CSPM は、標準に適用されるすべてのコントロールを自動的に有効にします。次に、Security Hub CSPM はコントロールに対してセキュリティチェックを実行し、Security Hub CSPM の検出結果を生成します。必要に応じて、個々のコントロールを無効にし、後で再度有効にすることができます。標準を完全に無効にすることもできます。標準を無効にすると、Security Hub CSPM は、標準に適用されるコントロールに対するセキュリティチェックの実行を停止します。コントロールの結果は生成されなくなりました。

Security Hub CSPM は、検出結果に加えて、有効にした標準ごとにセキュリティスコアを生成します。スコアは、標準に適用されるコントロールのステータスに基づきます。集約リージョンを設定すると、標準のセキュリティスコアには、リンクされたすべてのリージョンのコントロールのステータスが反映されます。お客様が組織の Security Hub CSPM 管理者である場合、スコアには組織内のすべてのアカウントのコントロールのステータスが反映されます。詳細については、「セキュリティスコアの計算」を参照してください。

標準を確認および管理するには、Security Hub CSPM コンソールまたは Security Hub CSPM API を使用できます。コンソールのセキュリティ標準ページには、Security Hub CSPM が現在サポートしているすべてのセキュリティ標準が表示されます。これには、各標準の説明と標準の現在のステータスが含まれます。標準を有効にすると、このページを使用して標準の追加の詳細にアクセスすることもできます。たとえば、以下を確認できます。

- 標準の現在のセキュリティスコア。
- 標準に適用されるコントロールの集計統計。

- 標準に適用され、各コントロールのコンプライアンスステータスなど、現在有効になっているコントロールのリスト。
- 標準に適用されているが、現在無効になっているコントロールのリスト。

より詳細な分析のために、データをフィルタリングしてソートし、ドリルダウンして標準に適用される個々のコントロールの詳細を確認できます。

1 つのアカウントと に対して標準を個別に有効にできます AWS リージョン。ただし、マルチアカウントおよびマルチリージョン環境の時間を節約し、設定ドリフトを減らすには、中央設定を使用して標準を有効にして管理することをお勧めします。中央設定では、委任 Security Hub CSPM 管理者は、複数のアカウントとリージョンで標準を設定する方法を指定するポリシーを作成できます。

トピック

- Security Hub CSPM の標準リファレンス
- セキュリティ標準の有効化
- セキュリティ標準の詳細の確認
- 自動的に有効になっているセキュリティ標準をオフにする
- セキュリティ標準の無効化

Security Hub CSPM の標準リファレンス

AWS Security Hub CSPM では、セキュリティ標準は規制フレームワーク、業界のベストプラクティス、または企業ポリシーに基づく一連の要件です。Security Hub CSPM は、これらの要件をコントロールにマッピングし、コントロールに対してセキュリティチェックを実行して、標準の要件が満たされているかどうかを評価します。各標準には複数のコントロールが含まれています。

Security Hub CSPM は現在、次の標準をサポートしています。

- AWS 基本的なセキュリティのベストプラクティス – AWS および業界の専門家によって開発されたこの標準は、セクターや規模に関係なく、組織のセキュリティのベストプラクティスをまとめたものです。 AWS アカウント および リソースがセキュリティのベストプラクティスから逸脱した場合を検出する一連のコントロールを提供します。また、セキュリティ体制を改善および維持する方法に関する規範的なガイダンスも提供します。
- AWS リソースのタグ付け – Security Hub CSPM によって開発されたこの標準は、 AWS リソースにタグがあるかどうかを判断するのに役立ちます。タグは、 AWS リソースのメタデータとして機

能するキーと値のペアです。タグは、 AWS リソースの特定、分類、管理、検索に役立ちます。たとえば、タグを使用して、リソースを目的、所有者、または環境別に分類できます。

- CIS AWS Foundations Benchmark – Center for Internet Security (CIS) によって開発されたこの標準は、安全な設定ガイドラインを提供します AWS。基盤設定、テスト可能設定、アーキテクチャに依存しない設定に重点を置いて、 AWS のサービス および リソースのサブセットのセキュリティ設定ガイドラインとベストプラクティスのセットを指定します。ガイドラインには、明確で step-by-step実装と評価の手順が含まれています。
- NIST SP 800-53 Revision 5 – この標準は、情報システムと重要なリソースの機密性、完全性、可用性を保護するための米国国立標準技術研究所 (NIST) の要件に準拠しています。関連するフレームワークは、通常、米国の連邦機関、または米国の連邦機関や情報システムと連携する組織に適用されます。ただし、プライベート組織は要件をガイドフレームワークとして使用することもできます。
- NIST SP 800-171 リビジョン 2 – この標準は、米国連邦政府の一部ではないシステムや組織で管理された未分類情報 (CUI) の機密性を保護するための NIST セキュリティの推奨事項と要件に準拠しています。CUI は、政府の分類基準を満たしていないが、機密と見なされ、米国連邦政府または米国連邦政府に代わって他の団体によって作成または所有されている情報です。
- PCI DSS – この標準は、PCI Security Standards Council (SSC) によって定義された Payment Card Industry Data Security Standard (PCI DSS) コンプライアンスフレームワークに準拠しています。このフレームワークは、クレジットカードとデビットカードの情報を安全に処理するための一連のルールとガイドラインを提供します。フレームワークは通常、カード所有者データを保存、処理、または送信する組織に適用されます。
- サービスマネージド標準 – この標準は、 AWS Control TowerSecurity Hub CSPM が提供する AWS Control Tower 検出コントロールとともに が提供するプロアクティブコントロールを設定するのに役立ちます。 AWS Control Tower は、規範的なベストプラクティスに従って、 AWS マルチアカウント環境を簡単にセットアップして管理する方法を提供します。 AWS 環境のプロアクティブコントロールと検出コントロールの両方を有効にすることで、さまざまな開発段階でセキュリティ体制を強化できます。

Security Hub CSPM の標準とコントロールは、規制フレームワークや監査への準拠を保証するものではありません。代わりに、 および リソースの状態を評価およびモニタリングする方法 AWS アカウント を提供します。ビジネスニーズ、業界、またはユースケースに関連する各標準を有効にすることをお勧めします。

個々のコントロールは、複数の標準に適用できます。複数の標準を有効にする場合は、統合コントロールの検出結果も有効にすることをお勧めします。これを行うと、コントロールが複数の標準に適用されていても、Security Hub CSPM はコントロールごとに 1 つの検出結果を生成します。統合

コントロールの検出結果を有効にしない場合、Security Hub CSPM は、コントロールが適用される有効な標準ごとに個別の検出結果を生成します。例えば、2 つの標準を有効にし、その両方にコントロールが適用される場合、コントロールには 2 つの異なる検出結果が表示され、各標準に 1 つずつ表示されます。統合コントロールの検出結果を有効にすると、コントロールに対して 1 つの検出結果のみが表示されます。詳細については、「統合されたコントロールの検出結果」を参照してください。

標準による詳細なリファレンス

- AWS Security Hub CSPM の基本的なセキュリティのベストプラクティス標準
- AWS Security Hub CSPM のリソースタグ付け標準
- Security Hub CSPM の CIS AWS Foundations Benchmark
- Security Hub CSPM の NIST SP 800-53 リビジョン 5
- Security Hub CSPM の NIST SP 800-171 リビジョン 2
- Security Hub CSPM の PCI DSS
- Security Hub CSPM のサービスマネージド標準

AWS Security Hub CSPM の基本的なセキュリティのベストプラクティス標準

AWS および業界の専門家によって開発された AWS Foundational Security Best Practices (FSBP) 標準は、組織の部門や規模に関係なく、組織のセキュリティベストプラクティスをまとめたものです。AWS アカウント とリソースがセキュリティのベストプラクティスから逸脱した場合を検出する一連のコントロールを提供します。また、組織のセキュリティ体制を改善および維持する方法に関する規範的なガイダンスも提供します。

AWS Security Hub CSPM の AWS Foundational Security Best Practices 標準には、 AWS アカウント および ワークロードを継続的に評価し、セキュリティのベストプラクティスから逸脱する領域を特定するのに役立つコントロールが含まれています。コントロールには、複数の AWS のサービスからの、リソースに対するセキュリティのベストプラクティスが含まれます。各コントロールには、コントロールが適用されるセキュリティ機能を反映するカテゴリが割り当てられます。カテゴリのリストとその他の詳細については、「」を参照してくださいコントロールのカテゴリ。

標準に適用されるコントロール

次のリストは、基本的な AWS セキュリティのベストプラクティス標準 (v1.0.0) に適用される Security Hub AWS CSPM コントロールを指定します。コントロールの詳細を確認するには、コントロールを選択します。

[Account.1] のセキュリティ連絡先情報は に提供する必要があります AWS アカウント

[ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります

[ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります

[APIGateway.1] API Gateway REST および WebSocket API 実行ログ記録を有効にする必要があります

[APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります

[APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります

[APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります

[APIGateway.5] API Gateway REST API のキャッシュデータは、保管中に暗号化する必要があります

[APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります

[APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります

[AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります

[AppSync.2] AWS AppSync フィールドレベルのログ記録を有効にする必要があります

[AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください

[AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります

[Athena.4] Athena ワークグループではログ記録が有効になっている必要があります

[AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要がある

[AutoScaling.2] Amazon EC2 Auto Scaling グループは、複数のアベイラビリティーゾーンをカバーする必要があります

[AutoScaling.3] Auto Scaling グループ起動設定は、EC2 インスタンスを、インスタンスメタデータサービスバージョン 2 (IMDSv2) を必要とするように設定する必要があります

[Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません

[AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります

[AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります

[Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります

[CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります

[CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります

[CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります

[CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります

[CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります

[CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります

[CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります

[CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります

[CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください

[CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります

[CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります

[CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります

[CloudTrail.1] CloudTrail を有効にして、少なくとも 1 つのマルチリージョンの追跡で、読み取りと書き込みの管理イベントを含めた設定をする必要があります。

[CloudTrail.2] CloudTrail は保管時の暗号化を有効にする必要があります

[PCI.CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります

[CloudTrail.5] CloudTrail 追跡は Amazon CloudWatch Logs と統合する必要があります

[CodeBuild.1] CodeBuild Bitbucket ソースリポジトリの URL には機密認証情報を含めないでください

[CodeBuild.2] CodeBuild プロジェクト環境変数にクリアテキストの認証情報を含めることはできません

[CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります

[CodeBuild.4] CodeBuild AWS Configプロジェクト環境にはログ記録設定が必要です

[CodeBuild.7] CodeBuild レポートグループのエクスポートは保管時に暗号化する必要があります

[Cognito.2] Cognito ID プールは認証されていない ID を許可しないでください

[Config.1] を有効にし、サービスにリンクされたロールをリソース記録に使用 AWS Config する必要があります

[Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります

[DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります

[DataSync.1] DataSync タスクではログ記録が有効になっている必要があります

[DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります

[DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。

[DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。

[DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。

[DMS.9] DMS エンドポイントは SSL を使用する必要があります。

[DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります

[DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります

[DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります

[DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります

[DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です

[DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません

[DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります

[DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります

[DocumentDB.6] Amazon DocumentDB クラスターは転送中に暗号化する必要があります

[DynamoDB.1] DynamoDB テーブルは、需要に応じて容量をオートスケーリングする必要があります

[DynamoDB.2] DynamoDB テーブルでは、ポイントインタイムリカバリが有効になっている必要があります。

[DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります

[DynamoDB.6] DynamoDB テーブルで、削除保護が有効になっている必要があります

[DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります

[EC2.1] Amazon EBS スナップショットはパブリックに復元できないようにすることをお勧めします

[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします

[EC2.3] アタッチされた Amazon EBS ボリュームは、保管時に暗号化することをお勧めします

[EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります

[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします

[EC2.7] EBS のデフォルト暗号化を有効にすることをお勧めします

[EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします

[EC2.9] Amazon EC2 インスタンスは、パブリック IPv4 アドレスを未設定にすることをお勧めします

[EC2.10] Amazon EC2 サービス用に作成された VPC エンドポイントを使用するようにAmazon EC2 を設定することをお勧めします

[EC2.15] Amazon EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないことをお勧めします

[EC2.16] 未使用のネットワークアクセスコントロールリストを削除することをお勧めします

[EC2.17] Amazon EC2 インスタンスが複数の ENI を使用しないようにすることをお勧めします

[EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします

[EC2.19] セキュリティグループは、リスクの高いポートへの無制限アクセスを許可してはいけません

[EC2.20] AWS Site-to-Site VPN トンネルが稼働している必要があります

[EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります

[EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします

[EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします

[EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします

[EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります

[EC2.55] VPCs は ECR API のインターフェイスエンドポイントで設定する必要があります

[EC2.56] VPCsは Docker Registry のインターフェイスエンドポイントで設定する必要があります

[EC2.57] VPCsは Systems Manager のインターフェイスエンドポイントで設定する必要があります

[EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります

[EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります

[EC2.170] EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします

[EC2.171] EC2 VPN 接続では、ログ記録が有効になっている必要があります

[EC2.172] EC2 VPC ブロックパブリックアクセス設定はインターネットゲートウェイトラフィックをブロックする必要があります

[EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります

[EC2.180] EC2 ネットワークインターフェイスでは、送信元/送信先チェックを有効にする必要があります

[ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります

[ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります

[ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります

[ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。

[ECS.2] ECS サービスには、パブリック IP アドレスを自動で割り当てないでください

[ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください

[ECS.4] ECS コンテナは、非特権として実行する必要があります

[ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。

[ECS.8] シークレットは、コンテナ環境の変数として渡さないでください

[ECS.9] ECS タスク定義にはログ設定が必要です。

[ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。

[ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります

[ECS.16] ECS タスクセットはパブリック IP アドレスを自動的に割り当てないでください。

[EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS

[EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります

[EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります

[EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります

[EFS.6] EFS マウントターゲットは、起動時にパブリック IP アドレスを割り当てるサブネットに関連付けるべきではありません

[EFS .7] EFS ファイルシステムでは、自動バックアップが有効になっている必要があります

[EFS .8] EFS ファイルシステムは保管中に暗号化する必要があります

[EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります

[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。

[EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります

[EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります

[ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります

[ElastiCache.2] ElastiCache クラスターでは、マイナーバージョンの自動アップグレードを有効にする必要があります

[ElastiCache.3] ElastiCache (Redis OSS) レプリケーショングループでは、自動フェイルオーバーを有効にする必要があります

[ElastiCache.4] ElastiCache レプリケーショングループは保管中に暗号化する必要があります

[ElastiCache.5] ElastiCache レプリケーショングループは転送時に暗号化する必要があります

[ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります

[ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください

[ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。

[ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります

[ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります

[ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります

[ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager

[ELB.3] Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります

[ELB.4] Application Load Balancer は、無効な http ヘッダーを削除するように設定する必要があります

[ELB.5] アプリケーションおよび Classic Load Balancer のログ記録を有効にする必要があります

[ELB.6] アプリケーション、ゲートウェイ、および Network Load Balancer で削除保護を有効にする必要があります

[ELB.7] Classic Load Balancers は、Connection Draining を有効にする必要があります

[ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な uration AWS Configを持つ事前定義されたセキュリティポリシーを使用する必要があります

[ELB.9] Classic Load Balancer では、クロスゾーンロードバランシングが有効になっている必要があります

[ELB.10] Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります

[ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります

[ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります

[ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります

[ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります

[ELB.18] Application and Network Load Balancer リスナーは、安全なプロトコルを使用して転送中のデータを暗号化する必要があります

[EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります

[EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります

[EMR.3] Amazon EMR セキュリティ設定は保管時に暗号化する必要があります

[EMR.4] Amazon EMR セキュリティ設定は転送中に暗号化する必要があります

[ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります

[ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります

[ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります

[ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります

[ES.5] Elasticsearch ドメインで監査ログ記録が有効になっている必要があります

[ES.6] Elasticsearch ドメインには少なくとも 3 つのデータノードが必要です

[ES.7] Elasticsearch ドメインは、少なくとも 3 つの専用マスターノードを設定する必要があります。

[ES.8] Elasticsearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります

[EventBridge.3] Amazon EventBridge カスタムイベントバスにリソースポリシーがアタッチされている必要があります

[FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります

[FSx.2] FSx for Lustre ファイルシステムでは、タグをバックアップにコピーするように設定する必要があります

[FSx.3] FSx for OpenZFS ファイルシステムは、マルチ AZ 配置用に設定する必要があります

[FSx.4] FSx for NetApp ONTAP ファイルシステムは、マルチ AZ 配置用に設定する必要があります

[FSx.5] FSx for Windows File Server ファイルシステムは、マルチ AZ 配置用に設定する必要があります

[Glue.3] AWS Glue 機械学習変換は保管時に暗号化する必要があります

[Glue.4] AWS Glue Spark ジョブは、サポートされているバージョンの AWS Glue で実行する必要があります

[GuardDuty.1] GuardDuty を有効にする必要があります

[GuardDuty.5] GuardDuty EKS 監査ログモニタリングを有効にする必要があります

[GuardDuty.6] GuardDuty Lambda Protection を有効にする必要があります

[GuardDuty.7] GuardDuty EKS ランタイムモニタリングを有効にする必要があります

[GuardDuty.8] GuardDuty Malware Protection for EC2 を有効にする必要があります

[GuardDuty.9] GuardDuty RDS Protection を有効にする必要があります

[GuardDuty.10] GuardDuty S3 Protection を有効にする必要があります

[GuardDuty.11] GuardDuty Runtime Monitoring を有効にする必要があります

[GuardDuty.12] GuardDuty ECS Runtime Monitoring を有効にする必要があります

[GuardDuty.13] GuardDuty EC2 Runtime Monitoring を有効にする必要があります

[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください

[IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください

[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります

[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません

[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります

[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります

[IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です

[IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります

[IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません

[Inspector.1] Amazon Inspector EC2 スキャンを有効にする必要があります

[Inspector.2] Amazon Inspector ECR スキャンを有効にする必要があります

[Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります

[Inspector.4] Amazon Inspector Lambda 標準スキャンを有効にする必要があります

[Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります

[Kinesis.3] Kinesis ストリームには適切なデータ保持期間が必要です

[KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください

[KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください

[KMS.3] AWS KMS keys を意図せずに削除しないでください

[KMS.5] KMS キーはパブリックにアクセスしないでください

[Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります

[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります

[Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります

[Macie.1] Amazon Macie を有効にする必要があります

[Macie.2] Macie 機密データ自動検出を有効にする必要があります

[MQ.2] ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります

[MQ.3] Amazon MQ ブローカーでは、自動マイナーバージョンアップグレードが有効になっている必要があります

[MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります

[MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります

[MSK.4] MSK クラスターではパブリックアクセスを無効にする必要があります

[MSK.5] MSK コネクタではログ記録が有効になっている必要があります

[MSK.6] MSK クラスターは認証されていないアクセスを無効にする必要があります

[Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります

[Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります

[Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください

[Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります

[Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります

[Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります

[Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります

[Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります

[NetworkFirewall.2] Network Firewall ログ記録を有効にする必要があります

[Network Firewall.3] Network Firewall ポリシーには、1 つ以上のルールグループが関連付けられている必要があります

[NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、完全なパケットに対してドロップまたは転送される必要があります。

[NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、断片化されたパケットに対してドロップまたは転送される必要があります。

[NetworkFirewall.6] ステートレス Network Firewall のルールグループを空にしないでください

[NetworkFirewall.9] Network Firewall は削除保護を有効にする必要があります

[NetworkFirewall.10] Network Firewall ファイアウォールでは、サブネット変更保護を有効にする必要があります

[Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります

[Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります

[Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります

[Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります

[Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります

[Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です

[Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります

[Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります

[Opensearch.10] OpenSearch ドメインには、最新のソフトウェアアップデートがインストールされている必要があります

[PCA.1] AWS Private CA ルート認証機関を無効にする必要があります

[Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります

[RDS.1] RDS スナップショットはプライベートである必要があります

[RDS.2] RDS DB インスタンスは、PubliclyAccessible 設定によって判断される、パブリックアクセスを禁止する必要があります

[RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。

[RDS.4] RDS クラスタースナップショットとデータベーススナップショットは保管中に暗号化する必要があります

[RDS.5] RDS DB インスタンスは、複数のアベイラビリティーゾーンで設定する必要があります

[RDS.6] RDS DB インスタンスの拡張モニタリングを設定する必要があります

[RDS.7] RDS クラスターでは、削除保護が有効になっている必要があります

[RDS.8] RDS DB インスタンスで、削除保護が有効になっている必要があります

[RDS.9] RDS DB インスタンスは CloudWatch Logs にログを発行する必要があります

[RDS.10] IAM 認証は RDS インスタンス用に設定する必要があります

[RDS.11] RDS インスタンスでは、自動バックアップが有効になっている必要があります

[RDS.12] IAM 認証は RDS クラスター用に設定する必要があります

[RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります

[RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります

[RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります

[RDS.16] Aurora DB クラスターは、タグを DB スナップショットにコピーするように設定する必要があります

[RDS.17] RDS DB インスタンスは、タグをスナップショットにコピーするように設定する必要があります

[RDS.19] 重大なクラスターイベントについて、既存の RDS イベント通知サブスクリプションを設定する必要があります

[RDS.20] 重大なデータベースインスタンスイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります

[RDS.21] 重大なデータベースパラメータグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります

[RDS.22] 重大なデータベースセキュリティグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります

[RDS.23] RDS インスタンスはデータベースエンジンのデフォルトポートを使用しないようにする必要があります

[RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります

[RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります

[RDS.27] RDS DB クラスターは保管中に暗号化する必要があります

[RDS.34] Aurora MySQL DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります

[RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります

[RDS.36] RDS for PostgreSQL DB は CloudWatch Logs にログを発行する必要があります

[RDS.37] Aurora PostgreSQL DB クラスターでは、ログを CloudWatch Logs に発行する必要があります

[RDS.40] RDS for SQL Server DB インスタンスは CloudWatch Logs にログを発行する必要があります

[RDS.41] RDS for SQL Server DB インスタンスは転送中に暗号化する必要があります

[RDS.42] RDS for MariaDB DB インスタンスは CloudWatch Logs にログを発行する必要があります

[RDS.44] RDS for MariaDB DB インスタンスは転送中に暗号化する必要があります

[RDS.45] Aurora MySQL DB クラスターでは、監査ログ記録を有効にする必要があります

[PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります

[Redshift.2] Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります

[Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります

[Redshift.4] Amazon Redshift クラスターでは、監査ログ記録が有効になっている必要があります

[Redshift.6] Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります

[Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります

[Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください

[Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください

[Redshift.10] Redshift クラスターは保存時に暗号化する必要があります

[Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの入力を許可する必要があります

[Redshift.18] Redshift クラスターでは、マルチ AZ 配置を有効にする必要があります

[RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります

[RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です

[RedshiftServerless.3] Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります

[RedshiftServerless.5] Redshift Serverless 名前空間では、デフォルトの管理者ユーザー名を使用しないでください

[RedshiftServerless.6] Redshift Serverless 名前空間は CloudWatch Logs にログをエクスポートする必要があります

[RedshiftServerless.7] Redshift Serverless 名前空間はデフォルトのデータベース名を使用しないでください

[S3.1] S3 汎用バケットではブロックパブリックアクセスの設定が有効になっている必要があります。

[S3.2] S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります

[S3.3] S3 汎用バケットではパブリック書き込みアクセスをブロックする必要があります。

[S3.5] S3 汎用バケットではリクエストに SSL を使用する必要があります。

[S3.6] S3 汎用バケットポリシーは、他の へのアクセスを制限する必要があります AWS アカウント

[S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります

[S3.9] S3 汎用バケットは、サーバーアクセスログ記録を有効にする必要があります

[S3.12] ACL は、S3 汎用バケットへのユーザーアクセスの管理に使用しないでください。

[S3.13] S3 汎用バケットにはライフサイクル設定が必要です

[S3.19] S3 アクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります

[S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります

[S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です

[SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります

[SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります

[SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません

[SageMaker.4] SageMaker エンドポイントの本番稼働バリアントの初期インスタンス数は 1 より大きい必要があります

[SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります

[SageMaker.8] SageMaker ノートブックインスタンスは、サポートされているプラットフォームで実行する必要があります

[SecretsManager.1] Secrets Manager のシークレットは、自動ローテーションを有効にする必要があります

[SecretsManager.2] 自動ローテーションを設定した Secrets Manager のシークレットは正常にローテーションする必要があります

[SecretsManager.3] 未使用の Secrets Manager のシークレットを削除します

[SecretsManager.4] Secrets Manager のシークレットは、指定された日数以内にローテーションする必要があります

[ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります

[SNS.4] SNS トピックアクセスポリシーはパブリックアクセスを許可しないでください

[SQS.1] Amazon SQS キューは保管中に暗号化する必要があります

[SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください

[SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager

[SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります

[SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります

[SSM.4] SSM ドキュメントはパブリックにしないでください

[SSM.6] SSM Automation では CloudWatch ログ記録が有効になっている必要があります

[SSM.7] SSM ドキュメントでは、パブリック共有ブロック設定を有効にする必要があります

[StepFunctions.1] Step Functions ステートマシンではログ記録がオンになっている必要があります

[Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください

[Transfer.3] Transfer Family コネクタではログ記録が有効になっている必要があります

[WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります

[WAF.2] AWS WAF Classic リージョンルールには少なくとも 1 つの条件が必要です

[WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です

[WAF.4] AWS WAF Classic Regional Web ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

[WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です

[WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です

[WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

[WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

[WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります

[WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります

[WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

AWS Security Hub CSPM のリソースタグ付け標準

AWS Security Hub CSPM によって開発された AWS リソースタグ付け標準は、 AWS リソースにタグがないかどうかを判断するのに役立ちます。タグは、 AWS リソースを整理するためのメタデータとして機能するキーと値のペアです。ほとんどの AWS リソースでは、リソースの作成時または作成後にリソースにタグを追加するオプションがあります。リソースの例としては、Amazon CloudFront ディストリビューション、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、 のシークレットなどがあります AWS Secrets Manager。タグは、 AWS リソースの管理、識別、整理、検索、フィルタリングに役立ちます。

各 タグは 2 つの部分で構成されます:

- タグキー - 、`CostCenterEnvironment`、 など`Project`。タグキーでは、大文字と小文字が区別されます。
- タグ値 - 例: `111122223333`または `Production`。タグキーと同様に、タグ値では大文字と小文字が区別されます。

タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。 AWS リソースへのタグの追加については、「リソースのタグ付けとタグエディタユーザーガイド AWS」を参照してください。

Security Hub CSPM の AWS リソースタグ付け標準に適用されるコントロールごとに、オプションでサポートされているパラメータを使用して、コントロールがチェックするタグキーを指定できます。タグキーを指定しない場合、コントロールは少なくとも 1 つのタグキーの存在のみをチェックし、リソースにタグキーがない場合に失敗します。

AWS リソースタグ付け標準を有効にする前に、まず でリソース記録を有効にして設定することが重要です AWS Config。リソース記録を設定するときは、標準に適用されるコントロールによってチェックされるすべてのタイプの AWS リソースに対しても有効にしてください。それ以外の場合、Security Hub CSPM は適切なリソースを評価し、標準に適用されるコントロールの正確な検出結果を生成できない可能性があります。記録するリソースのタイプのリストなどの詳細については、「」を参照してくださいコントロールの検出結果に必要な AWS Config リソース。

> **Note**
>
> AWS リソースタグ付け標準は、カナダ西部 (カルガリー) 、中国、および AWS GovCloud (US) リージョンでは利用できません。

AWS リソースタグ付け標準を有効にした後、標準に適用されるコントロールの検出結果の受信を開始します。Security Hub CSPM が、他の有効な標準に適用されるコントロールと同じ AWS Config サービスにリンクされたルールを使用するコントロールの検出結果を生成するまでに最大 18 時間かかる場合があることに注意してください。詳細については、「セキュリティチェックの実行スケジュール」を参照してください。

AWS リソースタグ付け標準には、次の Amazon リソースネーム (ARN) があります: `arn:aws:securityhub:region::standards/aws-resource-tagging-standard/v/1.0.0`。Security Hub CSPM API の GetEnabledStandards オペレーションを使用して、有効な標準の ARN を検索することもできます。

標準に適用されるコントロール

次のリストは、 AWS リソースタグ付け標準 (v1.0.0) に適用される AWS Security Hub CSPM コントロールを指定します。コントロールの詳細を確認するには、コントロールを選択します。

- [ACM.3] ACM 証明書にはタグを付ける必要があります

- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります
- [AppConfig.1] AWS AppConfig アプリケーションにはタグを付ける必要があります
- [AppConfig.2] AWS AppConfig 設定プロファイルにはタグを付ける必要があります
- [AppConfig.3] AWS AppConfig 環境にはタグを付ける必要があります
- [AppConfig.4] AWS AppConfig 拡張機能の関連付けにはタグを付ける必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.4] AWS AppSync GraphQL APIsにはタグを付ける必要があります
- [Athena.2] Athena データカタログにはタグを付ける必要があります
- [Athena.3] Athena ワークグループにはタグを付ける必要があります
- [AutoScaling.10] EC2 Auto Scaling グループにタグを付ける必要があります
- [Backup.2] AWS Backup 復旧ポイントにはタグを付ける必要があります
- [Backup.3] AWS Backup ボールトにはタグを付ける必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [Backup.5] AWS Backup バックアッププランにはタグを付ける必要があります
- 〔バッチ.1] バッチジョブキューにはタグを付ける必要があります
- [Batch.2] バッチスケジューリングポリシーにはタグを付ける必要があります
- [Batch.3] バッチコンピューティング環境にはタグを付ける必要があります
- [Batch.4] マネージドバッチコンピューティング環境のコンピューティングリソースプロパティにはタグを付ける必要があります
- [CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudTrail.9] CloudTrail 証跡にはタグを付ける必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります

- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [DataSync.2] DataSync タスクにはタグを付ける必要があります
- [Detective.1] 検出動作グラフにはタグを付ける必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにはタグを付ける必要があります
- [DynamoDB.5] DynamoDB テーブルにはタグを付ける必要があります
- [EC2.33] EC2 Transit Gateway アタッチメントにはタグを付ける必要があります
- [EC2.34] EC2 Transit Gateway ルートテーブルにはタグを付ける必要があります
- [EC2.35] EC2 ネットワークインターフェイスにはタグを付ける必要があります
- [EC2.36] EC2 カスタマーゲートウェイにはタグを付ける必要があります
- [EC2.37] EC2 Elastic IP アドレスにはタグを付ける必要があります
- [EC2.38] EC2 インスタンスにはタグを付ける必要があります
- [EC2.39] EC2 インターネットゲートウェイにはタグを付ける必要があります
- [EC2.40] EC2 NAT ゲートウェイにはタグを付ける必要があります
- [EC2.41] EC2 ネットワーク ACL にはタグを付ける必要があります
- [EC2.42] EC2 ルートテーブルにはタグを付ける必要があります
- [EC2.43] EC2 セキュリティグループにはタグを付ける必要があります
- [EC2.44] EC2 サブネットにはタグを付ける必要があります
- [EC2.45] EC2 ボリュームにはタグを付ける必要があります
- [EC2.46] Amazon VPC にはタグを付ける必要があります
- [EC2.47] Amazon VPC エンドポイントサービスはタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります
- [EC2.49] Amazon VPC ピアリング接続にはタグを付ける必要があります
- [EC2.50] EC2 VPN ゲートウェイにはタグを付ける必要があります
- [EC2.52] EC2 Transit Gateway にはタグを付ける必要があります
- [EC2.174] EC2 DHCP オプションセットにはタグを付ける必要があります
- [EC2.175] EC2 起動テンプレートにはタグを付ける必要があります

- [EC2.176] EC2 プレフィックスリストにはタグを付ける必要があります
- [EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります
- [EC2.178] EC2 トラフィックミラーフィルターにはタグを付ける必要があります
- [EC2.179] EC2 トラフィックミラーターゲットにはタグを付ける必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.13] ECS サービスにはタグを付ける必要があります
- [ECS.14] ECS クラスターにはタグを付ける必要があります
- [ECS.15] ECS タスク定義にはタグを付ける必要があります
- [EFS .5] EFS アクセスポイントにはタグを付ける必要があります
- [EKS.6] EKS クラスターにはタグを付ける必要があります
- [EKS.7] EKS ID プロバイダーの設定にはタグを付ける必要があります
- [ES.9] Elasticsearch ドメインにはタグを付ける必要があります
- [EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.1] AWS Glue ジョブにはタグを付ける必要があります
- [GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- [GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- [GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [IAM.23] IAM Access Analyzer アナライザーにはタグを付ける必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーにはタグを付ける必要があります
- [IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります

- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [Kinesis.2] Kinesis ストリームにはタグを付ける必要があります
- [Lambda.6] Lambda 関数にはタグを付ける必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります
- [NetworkFirewall.7] Network Firewall ファイアウォールにはタグを付ける必要があります
- [NetworkFirewall.8] Network Firewall ファイアウォールポリシーにはタグを付ける必要があります
- [Opensearch.9] OpenSearch ドメインはにはタグを付ける必要があります
- [PCA.2] AWS プライベート CA 認証機関にはタグを付ける必要があります
- [RDS.28] RDS DB クラスターにはタグを付ける必要があります

- [RDS.29] RDS DB クラスタースナップショットにはタグを付ける必要があります
- [RDS.30] RDS DB インスタンスにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RDS.32] RDS DB スナップショットにはタグを付ける必要があります
- [RDS.33] RDS DB サブネットグループにはタグを付ける必要があります
- [Redshift.11] Redshift クラスターにはタグを付ける必要があります
- [Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります
- [Redshift.13] Redshift クラスタースナップショットにはタグを付ける必要があります
- [Redshift.14] Redshift クラスターサブネットグループにはタグを付ける必要があります
- [Redshift.17] Redshift クラスターパラメータグループにはタグを付ける必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [SageMaker.6] SageMaker アプリのイメージ設定にはタグを付ける必要があります
- [SageMaker.7] SageMaker イメージにはタグを付ける必要があります
- [SecretsManager.5] Secrets Manager のシークレットにはタグを付ける必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- [SNS.3] SNS トピックにはタグを付ける必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SSM.5] SSM ドキュメントにはタグを付ける必要があります
- [StepFunctions.2] Step Functions アクティビティにはタグを付ける必要があります
- [Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります
- [Transfer.4] Transfer Family 契約にはタグを付ける必要があります
- [Transfer.5] Transfer Family 証明書にはタグを付ける必要があります
- [Transfer.6] Transfer Family コネクタにはタグを付ける必要があります
- [Transfer.7] Transfer Family プロファイルにはタグを付ける必要があります

Security Hub CSPM の CIS AWS Foundations Benchmark

Center for Internet Security (CIS) AWS Foundations Benchmark は、一連のセキュリティ設定のベストプラクティスとして機能します AWS。業界で認められているこれらのベストプラクティスは、明

確かつステップバイステップの実装および評価手順を提供します。オペレーティングシステムからクラウドサービスやネットワークデバイスに至るまで、このベンチマークのコントロールは、組織が使用する特定のシステムの保護に役立ちます。

AWS Security Hub CSPM は、CIS AWS Foundations Benchmark バージョン 3.0.0、1.4.0、および 1.2.0 をサポートしています。このページには、各バージョンがサポートするセキュリティコントロールが一覧表示されます。また、バージョンの比較も提供します。

CIS AWS Foundations Benchmark バージョン 3.0.0

Security Hub CSPM は、CIS AWS Foundations Benchmark のバージョン 3.0.0 (v3.0.0) をサポートしています。Security Hub CSPM は CIS セキュリティソフトウェア認定の要件を満たしており、次の CIS ベンチマークに対して CIS セキュリティソフトウェア認定を受けています。

- CIS Benchmark for CIS AWS Foundations Benchmark、v3.0.0、レベル 1
- CIS Benchmark for CIS AWS Foundations Benchmark、v3.0.0、レベル 2

CIS AWS Foundations Benchmark バージョン 3.0.0 に適用されるコントロール

[Account.1] のセキュリティ連絡先情報は に提供する必要があります AWS アカウント

[CloudTrail.1] CloudTrail を有効にして、少なくとも 1 つのマルチリージョンの追跡で、読み取りと書き込みの管理イベントを含めた設定をする必要があります。

[CloudTrail.2] CloudTrail は保管時の暗号化を有効にする必要があります

[PCI.CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります

[CloudTrail.7] CloudTrail S3 バケットで、S3 バケットアクセスログ記録が有効であることを確認します

[Config.1] を有効にし、サービスにリンクされたロールをリソース記録に使用 AWS Config する必要があります

[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします

[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします

[EC2.7] EBS のデフォルト暗号化を有効にすることをお勧めします

[EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします

[EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります

[EC2.53] EC2 セキュリティグループが 0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可することがないようにする必要があります

[EC2.54] EC2 セキュリティグループは ::/0 からリモートサーバー管理ポートへの入力を許可しない必要があります

[EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS

[IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください

[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります

[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません

[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります

[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります

[IAM.9] ルートユーザーに対して MFA を有効にする必要があります

[IAM.15] IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認します

[IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています

[IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します

[IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります

[IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります

[IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください

[IAM.28] IAM Access Analyzer 外部アクセスアナライザーを有効にする必要があります

[KMS.4] AWS KMS キーローテーションを有効にする必要があります

[RDS.2] RDS DB インスタンスは、PubliclyAccessible 設定によって判断される、パブリックアクセスを禁止する必要があります

[RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。

[RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります

[S3.1] S3 汎用バケットではブロックパブリックアクセスの設定が有効になっている必要があります。

[S3.5] S3 汎用バケットではリクエストに SSL を使用する必要があります。

[S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります

[S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります

[S3.22] S3 汎用バケットはオブジェクトレベルの書き込みイベントをログに記録する必要があります

[S3.23] S3 汎用バケットはオブジェクトレベルの読み取りイベントをログに記録する必要があります

CIS AWS Foundations Benchmark バージョン 1.4.0

Security Hub CSPM は、CIS AWS Foundations Benchmark のバージョン 1.4.0 (v1.4.0) をサポートしています。

CIS AWS Foundations Benchmark バージョン 1.4.0 に適用されるコントロール

[CloudTrail.1] CloudTrail を有効にして、少なくとも 1 つのマルチリージョンの追跡で、読み取りと書き込みの管理イベントを含めた設定をする必要があります。

[CloudTrail.2] CloudTrail は保管時の暗号化を有効にする必要があります

[PCI.CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります

[CloudTrail.5] CloudTrail 追跡は Amazon CloudWatch Logs と統合する必要があります

[CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットが一般公開されていないことを確認します

[CloudTrail.7] CloudTrail S3 バケットで、S3 バケットアクセスログ記録が有効であることを確認します

[CloudWatch.1] 「ルート」ユーザーの使用に対するログメトリクスフィルターとアラームが存在する必要があります

[CloudWatch.4] IAM ポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します

[CloudWatch.5] CloudTrail 設定変更のログメトリクスフィルターとアラームが存在することを確認する

[CloudWatch.6] AWS Management Console 認証失敗のログメトリクスフィルターとアラームが存在することを確認する

[CloudWatch.7] カスタマーマネージドキーの無効化またはスケジュールされた削除に対するログメトリクスフィルターとアラームが存在することを確認します

[CloudWatch.8] S3 バケットポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します

[CloudWatch.9] AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する

[CloudWatch.10] セキュリティグループの変更に対するログメトリクスフィルターとアラームが存在することを確認します

[CloudWatch.11] ネットワークアクセスコントロールリスト (NACL) への変更に対するログメトリクスフィルターとアラームが存在することを確認します

[CloudWatch.12] ネットワークゲートウェイへの変更に対するログメトリクスフィルターとアラームが存在することを確認します

[CloudWatch.13] ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認します

[CloudWatch.14] VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認します

[Config.1] を有効にし、サービスにリンクされたロールをリソース記録に使用 AWS Config する必要があります

[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします

[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします

[EC2.7] EBS のデフォルト暗号化を有効にすることをお勧めします

[EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります

[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください

[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります

[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません

[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります

[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります

[IAM.9] ルートユーザーに対して MFA を有効にする必要があります

[IAM.15] IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認します

[IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています

[IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します

[IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります

[KMS.4] AWS KMS キーローテーションを有効にする必要があります

[RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。

[S3.1] S3 汎用バケットではブロックパブリックアクセスの設定が有効になっている必要があります。

[S3.5] S3 汎用バケットではリクエストに SSL を使用する必要があります。

[S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります

[S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります

CIS AWS Foundations Benchmark バージョン 1.2.0

Security Hub CSPM は、CIS AWS Foundations Benchmark のバージョン 1.2.0 (v1.2.0) をサポートしています。Security Hub CSPM は CIS セキュリティソフトウェア認定の要件を満たしており、次の CIS ベンチマークに対して CIS セキュリティソフトウェア認定を受けています。

- CIS Benchmark for CIS AWS Foundations Benchmark、v1.2.0、レベル 1
- CIS Benchmark for CIS AWS Foundations Benchmark、v1.2.0、レベル 2

CIS AWS Foundations Benchmark バージョン 1.2.0 に適用されるコントロール

[CloudTrail.1] CloudTrail を有効にして、少なくとも 1 つのマルチリージョンの追跡で、読み取りと書き込みの管理イベントを含めた設定をする必要があります。

[CloudTrail.2] CloudTrail は保管時の暗号化を有効にする必要があります

[PCI.CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります

[CloudTrail.5] CloudTrail 追跡は Amazon CloudWatch Logs と統合する必要があります

[CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットが一般公開されていないことを確認します

[CloudTrail.7] CloudTrail S3 バケットで、S3 バケットアクセスログ記録が有効であることを確認します

[CloudWatch.1] 「ルート」ユーザーの使用に対するログメトリクスフィルターとアラームが存在する必要があります

[CloudWatch.2] 不正な API 呼び出しに対してログメトリクスフィルターとアラームが存在することを確認します

[CloudWatch.3] MFA を使用しないマネジメントコンソールサインインに対してログメトリクスフィルターとアラームが存在することを確認します

[CloudWatch.4] IAM ポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します

[CloudWatch.5] CloudTrail 設定変更のログメトリクスフィルターとアラームが存在することを確認する

[CloudWatch.6] AWS Management Console 認証失敗のログメトリクスフィルターとアラームが存在することを確認する

[CloudWatch.7] カスタマーマネージドキーの無効化またはスケジュールされた削除に対するログメトリクスフィルターとアラームが存在することを確認します

[CloudWatch.8] S3 バケットポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します

[CloudWatch.9] AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する

[CloudWatch.10] セキュリティグループの変更に対するログメトリクスフィルターとアラームが存在することを確認します

[CloudWatch.11] ネットワークアクセスコントロールリスト (NACL) への変更に対するログメトリクスフィルターとアラームが存在することを確認します

[CloudWatch.12] ネットワークゲートウェイへの変更に対するログメトリクスフィルターとアラームが存在することを確認します

[CloudWatch.13] ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認します

[CloudWatch.14] VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認します

[Config.1] を有効にし、サービスにリンクされたロールをリソース記録に使用 AWS Config する必要があります

[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします

[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします

[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります

[EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります

[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください

[IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください

[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります

[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません

[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります

[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります

[IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります

[IAM.9] ルートユーザーに対して MFA を有効にする必要があります

[IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します

[IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します

[IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します

[IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します

[IAM.15] IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認します

[IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています

[IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します

[IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します

[KMS.4] AWS KMS キーローテーションを有効にする必要があります

CIS AWS Foundations Benchmark のバージョン比較

このセクションでは、Center for Internet Security (CIS) AWS Foundations Benchmark – v3.0.0、v1.4.0、および v1.2.0 の特定のバージョンの違いをまとめています。 AWS Security Hub CSPM は、CIS AWS Foundations Benchmark の各バージョンをサポートしています。ただし、v3.0.0 を使用して、セキュリティのベストプラクティスを最新の状態に保つことをお勧めします。複数のバージョンの標準を同時に有効にできます。標準を有効にする方法については、「」を

参照してくださいセキュリティ標準の有効化。v3.0.0 にアップグレードする場合は、古いバージョンを無効にする前に有効にします。これにより、セキュリティチェックのギャップを防ぐことができます。Security Hub CSPM と の統合を使用して AWS Organizations いて、複数のアカウントで v3.0.0 をバッチ有効化する場合は、中央設定を使用することをお勧めします。

各バージョンの CIS 要件に対するコントロールのマッピング

CIS AWS Foundations Benchmark がサポートする各バージョンのコントロールを理解します。

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
[Account.1] のセキュリティ連絡先情報は に提供する必要があります AWS アカウント	1.2	1.2	1.18
[CloudTrail.1] CloudTrail を有効にして、少なくとも 1 つのマルチリージョンの追跡で、読み取りと書き込みの管理イベントを含めた設定をする必要があります。	3.1	3.1	2.1
[CloudTrail.2] CloudTrail は保管時の暗号化を有効にする必要があります	3.5	37	2.7
[PCI.CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります	3.2	3.2	2.2
[CloudTrail.5] CloudTrail 追跡は Amazon CloudWatch Logs と統合する必要があります	サポートされていません – CIS がこの要件を削除しました	3.4	2.4
[CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットが一般公開されていないことを確認します	サポートされていません – CIS がこの要件を削除しました	3.3	2.3

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
[CloudTrail.7] CloudTrail S3 バケットで、S3 バケットアクセスログ記録が有効であることを確認します	3.4	3.6	2.6
[CloudWatch.1] 「ルート」ユーザーの使用に対するログメトリクスフィルターとアラームが存在する必要があります	サポートされていません – 手動チェック	4.3	3.3
[CloudWatch.2] 不正な API 呼び出しに対してログメトリクスフィルターとアラームが存在することを確認します	サポートされていません – 手動チェック	サポートされていません – 手動チェック	3.1
[CloudWatch.3] MFA を使用しないマネジメントコンソールサインインに対してログメトリクスフィルターとアラームが存在することを確認します	サポートされていません – 手動チェック	サポートされていません – 手動チェック	3.2
[CloudWatch.4] IAM ポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します	サポートされていません – 手動チェック	4.4	3.4
[CloudWatch.5] CloudTrail 設定変更のログメトリクスフィルターとアラームが存在することを確認する	サポートされていません – 手動チェック	4.5	3.5
[CloudWatch.6] AWS Management Console 認証失敗のログメトリクスフィルターとアラームが存在することを確認する	サポートされていません – 手動チェック	4.6	3.6

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
[CloudWatch.7] カスタマーマネージドキーの無効化またはスケジュールされた削除に対するログメトリクスフィルターとアラームが存在することを確認します	サポートされていません – 手動チェック	4.7	37
[CloudWatch.8] S3 バケットポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します	サポートされていません – 手動チェック	4.8	3.8
[CloudWatch.9] AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する	サポートされていません – 手動チェック	4.9	3.9
[CloudWatch.10] セキュリティグループの変更に対するログメトリクスフィルターとアラームが存在することを確認します	サポートされていません – 手動チェック	4.10	3.10
[CloudWatch.11] ネットワークアクセスコントロールリスト (NACL) への変更に対するログメトリクスフィルターとアラームが存在することを確認します	サポートされていません – 手動チェック	4.11	3.11
[CloudWatch.12] ネットワークゲートウェイへの変更に対するログメトリクスフィルターとアラームが存在することを確認します	サポートされていません – 手動チェック	4.12	3.12
[CloudWatch.13] ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認します	サポートされていません – 手動チェック	4.13	3.13

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
[CloudWatch.14] VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認します	サポートされていません – 手動チェック	4.14	3.14
[Config.1] を有効にし、サービスにリンクされたロールをリソース記録に使用 AWS Config する必要があります	3.3	3.5	2.5
[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします	5.4	5.3	4.3
[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします	37	3.9	2.9
[EC2.7] EBS のデフォルト暗号化を有効にすることをお勧めします	2.2.1	2.2.1	サポートされていません
[EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします	5.6	サポートされません	サポートされません
[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります	サポートされません – 要件 5.2 および 5.3 に置き換えられました	サポートされません – 要件 5.2 および 5.3 に置き換えられました	4.1

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
[EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります	サポートされません – 要件 5.2 および 5.3 に置き換えられました	サポートされません – 要件 5.2 および 5.3 に置き換えられました	4.2
[EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります	5.1	5.1	サポートされていません
[EC2.53] EC2 セキュリティグループが 0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可することがないようにする必要があります	5.2	サポートされません	サポートされません
[EC2.54] EC2 セキュリティグループは ::/0 からリモートサーバー管理ポートへの入力を許可しない必要があります	5.3	サポートされません	サポートされません
[EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS	2.4.1	サポートされません	サポートされません
[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください	サポートされません	1.16	1.22
[IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください	1.15	サポートされていません	1.16

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります	1.14	1.14	1.4
[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません	1.4	1.4	1.12
[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります	1.10	1.10	1.2
[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります	1.6	1.6	1.14
[IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります	サポートされていません – 代わりに「[IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります」を参照してください。	サポートされていません – 代わりに「[IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります」を参照してください。	1.3
[IAM.9] ルートユーザーに対して MFA を有効にする必要があります	1.5	1.5	1.13
[IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します	サポートされていません – CIS がこの要件を削除しました	サポートされていません – CIS がこの要件を削除しました	1.5

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
[IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します	サポートされていません – CIS がこの要件を削除しました	サポートされていません – CIS がこの要件を削除しました	1.6
[IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します	サポートされていません – CIS がこの要件を削除しました	サポートされていません – CIS がこの要件を削除しました	1.7
[IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します	サポートされていません – CIS がこの要件を削除しました	サポートされていません – CIS がこの要件を削除しました	1.8
[IAM.15] IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認します	1.8	1.8	1.9
[IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています	1.9	1.9	1.10
[IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します	サポートされていません – CIS がこの要件を削除しました	サポートされていません – CIS がこの要件を削除しました	1.11
[IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します	1.17	1.17	1.2

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
[IAM.20] ルートユーザーの使用を避けます	サポートされていません – CIS がこの要件を削除しました	サポートされていません – CIS がこの要件を削除しました	1.1
[IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります	1.12	1.12	サポートされていません – CIS は、この要件を以降のバージョンで追加しました
[IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります	1.19	サポートされていません – CIS は、この要件を以降のバージョンで追加しました	サポートされていません – CIS は、この要件を以降のバージョンで追加しました
[IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください	1.22	サポートされていません – CIS は、この要件を以降のバージョンで追加しました	サポートされていません – CIS は、この要件を以降のバージョンで追加しました
[IAM.28] IAM Access Analyzer 外部アクセスアナライザーを有効にする必要があります	1.20	サポートされていません – CIS は、この要件を以降のバージョンで追加しました	サポートされていません – CIS は、この要件を以降のバージョンで追加しました
[KMS.4] AWS KMS キーローテーションを有効にする必要があります	3.6	3.8	2.8

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
[Macie.1] Amazon Macie を有効にする必要があります	サポートされていません – 手動チェック	サポートされていません – 手動チェック	サポートされていません – 手動チェック
[RDS.2] RDS DB インスタンスは、PubliclyAccessible 設定によって判断される、パブリックアクセスを禁止する必要があります	2.3.3	サポートされていません – CIS は、この要件を以降のバージョンで追加しました	サポートされていません – CIS は、この要件を以降のバージョンで追加しました
[RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。	2.3.1	2.3.1	サポートされていません – CIS は、この要件を以降のバージョンで追加しました
[RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります	2.3.2	サポートされていません – CIS は、この要件を以降のバージョンで追加しました	サポートされていません – CIS は、この要件を以降のバージョンで追加しました
[S3.1] S3 汎用バケットではブロックパブリックアクセスの設定が有効になっている必要があります。	2.1.4	2.1.5	サポートされていません – CIS は、この要件を以降のバージョンで追加しました

コントロール ID とタイトル	CIS v3.0.0 の要件	CIS v1.4.0 の要件	CIS v1.2.0 の要件
[S3.5] S3 汎用バケットではリクエストに SSL を使用する必要があります。	2.1.1	2.1.2	サポートされていません – CIS は、この要件を以降のバージョンで追加しました
[S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります	2.1.4	2.1.5	サポートされていません – CIS は、この要件を以降のバージョンで追加しました
[S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります	2.1.2	2.1.3	サポートされていません – CIS は、この要件を以降のバージョンで追加しました

CIS AWS Foundations Benchmarks の ARNs

CIS AWS Foundations Benchmark の 1 つ以上のバージョンを有効にすると、 AWS Security Finding 形式 (ASFF) で結果の受信を開始します。ASFF では、各バージョンは次の Amazon リソースネーム (ARN) を使用します。

CIS AWS Foundations Benchmark v3.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/3.0.0
```

CIS AWS Foundations Benchmark v1.4.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/
v/1.4.0
```

CIS AWS Foundations Benchmark v1.2.0

```
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

Security Hub CSPM API の GetEnabledStandardsオペレーションを使用して、有効な標準の ARN を検索できます。

上記の値は `StandardsArn` 用です。ただし、 は、リージョンBatchEnableStandardsで を呼び出して標準をサブスクライブするときに Security Hub CSPM が作成する標準サブスクリプションリソース`StandardsSubscriptionArn`を指します。

> **Note**
>
> CIS AWS Foundations Benchmark のバージョンを有効にすると、Security Hub CSPM が他の有効な標準で有効なコントロールと同じ AWS Config サービスにリンクされたルールを使用するコントロールの検出結果を生成するまでに最大 18 時間かかることがあります。コントロール結果の生成スケジュールの詳細については、「セキュリティチェックの実行スケジュール」を参照してください。

[統合されたコントロールの検出結果] を有効にすると、検出結果フィールドが異なります。これらの違いについては、「」を参照してくださいASFF フィールドと値への統合の影響。サンプルコントロールの検出結果については、「コントロールの検出結果のサンプル」を参照してください。

Security Hub CSPM でサポートされていない CIS 要件

前の表で説明したように、Security Hub CSPM は CIS AWS Foundations Benchmark のすべてのバージョンですべての CIS 要件をサポートしているわけではありません。サポートされていない要件の多くは、 AWS リソースの状態を手動で確認することによってのみ評価できます。

Security Hub CSPM の NIST SP 800-53 リビジョン 5

NIST Special Publication 800-53 Revision 5 (NIST SP 800-53 Rev. 5) は、米国商務省の一部である米国国立標準技術研究所 (NIST) によって開発されたサイバーセキュリティとコンプライアンスのフレームワークです。このコンプライアンスフレームワークは、情報システムと重要なリソースの機密性、完全性、可用性を保護するためのセキュリティ要件とプライバシー要件のカタログを提供します。米国連邦政府機関と請負業者は、システムや組織を保護するために、これらの要件に従う必要があります。プライベート組織は、サイバーセキュリティリスクを軽減するための指針となるフレーム

ワークとして、要件を自主的に使用することもできます。フレームワークとその要件の詳細については、NIST Computer Security Resource Center の「NIST SP 800-53 Rev. 5」を参照してください。

AWS Security Hub CSPM は、NIST SP 800-53 Revision 5 要件のサブセットをサポートするセキュリティコントロールを提供します。コントロールは、特定の AWS のサービス および リソースの自動セキュリティチェックを実行します。これらのコントロールを有効にして管理するには、Security Hub CSPM で NIST SP 800-53 Revision 5 フレームワークを標準として有効にします。コントロールは、手動チェックを必要とする NIST SP 800-53 Revision 5 の要件をサポートしていないことに注意してください。

他のフレームワークとは異なり、NIST SP 800-53 Revision 5 フレームワークは、その要件の評価方法に関する規範ではありません。代わりに、フレームワークはガイドラインを提供します。Security Hub CSPM では、NIST SP 800-53 Revision 5 標準とコントロールは、これらのガイドラインに対するサービスの理解を表しています。

トピック

- 標準に適用されるコントロールのリソース記録の設定
- 標準に適用されるコントロールの決定

標準に適用されるコントロールのリソース記録の設定

検出結果の範囲と精度を最適化するには、 AWS Security Hub CSPM で NIST SP 800-53 Revision 5 標準を有効にする AWS Config 前に、 でリソース記録を有効にして設定することが重要です。リソース記録を設定するときは、標準に適用されるコントロールによってチェックされるすべてのタイプの AWS リソースでも有効にしてください。これは主に、変更によってトリガーされるスケジュールタイプを持つコントロール用です。ただし、定期的なスケジュールタイプの一部のコントロールでは、リソースの記録も必要です。リソース記録が正しく有効または設定されていない場合、Security Hub CSPM は適切なリソースを評価し、標準に適用されるコントロールの正確な検出結果を生成できない可能性があります。

Security Hub CSPM が でリソース記録を使用する方法については AWS Config、「」を参照してくださいSecurity Hub CSPM AWS Config の有効化と設定。でのリソース記録の設定については AWS Config、「 AWS Config デベロッパーガイド」の「設定レコーダーの使用」を参照してください。

次の表は、Security Hub CSPM の NIST SP 800-53 Revision 5 標準に適用されるコントロールに記録するリソースのタイプを示しています。

AWS のサービス	リソースタイプ
Amazon API Gateway	`AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint` , `AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationTask`
Amazon DynamoDB	`AWS::DynamoDB::Table`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::EIP` , `AWS::EC2::Instance` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::TransitGateway` , `AWS::EC2::VPNConnection` , `AWS::EC2::Volume`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` , `AWS::AutoScaling::LaunchConfiguration`

AWS のサービス	リソースタイプ
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon エラスティックKubernetesサービス (Amazon EKS)	`AWS::EKS::Cluster`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
エラスティックロードバランシング	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
Amazon ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
Amazon EventBridge	`AWS::Events::Endpoint` , `AWS::Events::EventBus`
AWS Glue	`AWS::Glue::Job`
AWS Identity and Access Management (IAM)	`AWS::IAM::Group` , `AWS::IAM::Policy` , `AWS::IAM::Role` , `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`

AWS のサービス	リソースタイプ
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster`
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
Amazon OpenSearch Service	`AWS::OpenSearch::Domain`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster` , `AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSnapshot` , `AWS::RDS::EventSubscription`
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterSubnetGroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint` , `AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket`
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`

AWS のサービス	リソースタイプ
Amazon SageMaker AI	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Transfer Family	`AWS::Transfer::Connector`
AWS WAF	`AWS::WAF::Rule` , `AWS::WAF::RuleGroup` , `AWS::WAF::WebACL` , `AWS::WAFRegional::Rule` , `AWS::WAFRegional::RuleGroup` , `AWS::WAFRegional::WebACL` , `AWS::WAFv2::RuleGroup` , `AWS::WAFv2::WebACL`

標準に適用されるコントロールの決定

次のリストは、NIST SP 800-53 Revision 5 の要件をサポートするコントロールを指定し、 AWS Security Hub CSPM の NIST SP 800-53 Revision 5 標準に適用されます。コントロールがサポートする特定の要件の詳細については、コントロールを選択します。次に、コントロールの詳細の関連要件フィールドを参照してください。このフィールドは、コントロールがサポートする各 NIST 要件を指定します。フィールドで特定の NIST 要件が指定されていない場合、コントロールは要件をサポートしていません。

- [Account.1] のセキュリティ連絡先情報は に提供する必要があります AWS アカウント
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [APIGateway.1] API Gateway REST および WebSocket API 実行ログ記録を有効にする必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります
- [APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります
- [APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります

- [APIGateway.5] API Gateway REST API のキャッシュデータは、保管中に暗号化する必要があります
- [APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- [AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- [AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要がある
- [AutoScaling.2] Amazon EC2 Auto Scaling グループは、複数のアベイラビリティーゾーンをカバーする必要があります
- [AutoScaling.3] Auto Scaling グループ起動設定は、EC2 インスタンスを、インスタンスメタデータサービスバージョン 2 (IMDSv2) を必要とするように設定する必要があります
- [Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません
- [AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります
- [AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください

- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudTrail.1] CloudTrail を有効にして、少なくとも 1 つのマルチリージョンの追跡で、読み取りと書き込みの管理イベントを含めた設定をする必要があります。
- [CloudTrail.2] CloudTrail は保管時の暗号化を有効にする必要があります
- [PCI.CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります
- [CloudTrail.5] CloudTrail 追跡は Amazon CloudWatch Logs と統合する必要があります
- [CloudTrail.10] CloudTrail Lake イベントデータストアはカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [CloudWatch.15] CloudWatch アラームには、指定されたアクションが設定されている必要があります
- [CloudWatch.16] CloudWatch ロググループは指定した期間保持する必要があります
- [CloudWatch.17] CloudWatch アラームアクションをアクティブにする必要があります
- [CodeBuild.1] CodeBuild Bitbucket ソースリポジトリの URL には機密認証情報を含めないでください
- [CodeBuild.2] CodeBuild プロジェクト環境変数にクリアテキストの認証情報を含めることはできません
- [CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- [CodeBuild.4] CodeBuild AWS Configプロジェクト環境にはログ記録設定が必要です
- [Config.1] を有効にし、サービスにリンクされたロールをリソース記録に使用 AWS Config する必要があります
- [DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。

- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります
- [DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.1] DynamoDB テーブルは、需要に応じて容量をオートスケーリングする必要があります
- [DynamoDB.2] DynamoDB テーブルでは、ポイントインタイムリカバリが有効になっている必要があります。
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.6] DynamoDB テーブルで、削除保護が有効になっている必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.1] Amazon EBS スナップショットはパブリックに復元できないようにすることをお勧めします
- [EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします
- [EC2.3] アタッチされた Amazon EBS ボリュームは、保管時に暗号化することをお勧めします
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします
- [EC2.7] EBS のデフォルト暗号化を有効にすることをお勧めします
- [EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.9] Amazon EC2 インスタンスは、パブリック IPv4 アドレスを未設定にすることをお勧めします

- [EC2.10] Amazon EC2 サービス用に作成された VPC エンドポイントを使用するようにAmazon EC2 を設定することをお勧めします
- [EC2.12] 未使用の Amazon EC2 EIP を削除することをお勧めします
- [EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります
- [EC2.15] Amazon EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないことをお勧めします
- [EC2.16] 未使用のネットワークアクセスコントロールリストを削除することをお勧めします
- [EC2.17] Amazon EC2 インスタンスが複数の ENI を使用しないようにすることをお勧めします
- [EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします
- [EC2.19] セキュリティグループは、リスクの高いポートへの無制限アクセスを許可してはいけません
- [EC2.20] AWS Site-to-Site VPN トンネルが稼働している必要があります
- [EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.55] VPCs は ECR API のインターフェイスエンドポイントで設定する必要があります
- [EC2.56] VPCsは Docker Registry のインターフェイスエンドポイントで設定する必要があります
- [EC2.57] VPCsは Systems Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります

- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECR.5] ECR リポジトリはカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。
- [ECS.2] ECS サービスには、パブリック IP アドレスを自動で割り当てないでください
- [ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください
- [ECS.4] ECS コンテナは、非特権として実行する必要があります
- [ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。
- [ECS.8] シークレットは、コンテナ環境の変数として渡さないでください
- [ECS.9] ECS タスク定義にはログ設定が必要です。
- [ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。
- [ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります
- [ECS.17] ECS タスク定義はホストネットワークモードを使用しないでください
- [EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります
- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EFS.6] EFS マウントターゲットは、起動時にパブリック IP アドレスを割り当てるサブネットに関連付けるべきではありません
- [EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります

- [EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります
- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElastiCache.2] ElastiCache クラスターでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [ElastiCache.3] ElastiCache (Redis OSS) レプリケーショングループでは、自動フェイルオーバーを有効にする必要があります
- [ElastiCache.4] ElastiCache レプリケーショングループは保管中に暗号化する必要があります
- [ElastiCache.5] ElastiCache レプリケーショングループは転送時に暗号化する必要があります
- [ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります
- [ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください
- [ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。
- [ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります
- [ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.3] Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります
- [ELB.4] Application Load Balancer は、無効な http ヘッダーを削除するように設定する必要があります
- [ELB.5] アプリケーションおよび Classic Load Balancer のログ記録を有効にする必要があります
- [ELB.6] アプリケーション、ゲートウェイ、および Network Load Balancer で削除保護を有効にする必要があります
- [ELB.7] Classic Load Balancers は、Connection Draining を有効にする必要があります
- [ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な uration AWS Configを持つ事前定義されたセキュリティポリシーを使用する必要があります
- [ELB.9] Classic Load Balancer では、クロスゾーンロードバランシングが有効になっている必要があります

- [ELB.10] Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります
- [ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- [ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります
- [EMR.3] Amazon EMR セキュリティ設定は保管時に暗号化する必要があります
- [EMR.4] Amazon EMR セキュリティ設定は転送中に暗号化する必要があります
- [ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります
- [ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります
- [ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります
- [ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります
- [ES.5] Elasticsearch ドメインで監査ログ記録が有効になっている必要があります
- [ES.6] Elasticsearch ドメインには少なくとも 3 つのデータノードが必要です
- [ES.7] Elasticsearch ドメインは、少なくとも 3 つの専用マスターノードを設定する必要があります。
- [ES.8] Elasticsearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [EventBridge.3] Amazon EventBridge カスタムイベントバスにリソースポリシーがアタッチされている必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります

- [FSx.2] FSx for Lustre ファイルシステムでは、タグをバックアップにコピーするように設定する必要があります
- [Glue.4] AWS Glue Spark ジョブは、サポートされているバージョンの AWS Glue で実行する必要があります
- [GuardDuty.1] GuardDuty を有効にする必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [KMS.3] AWS KMS keys を意図せずに削除しないでください
- [KMS.4] AWS KMS キーローテーションを有効にする必要があります
- [Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります
- [Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります
- [Lambda.3] Lambda 関数は VPC 内に存在する必要があります
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Lambda.7] Lambda 関数では AWS X-Ray アクティブなトレースを有効にする必要があります
- [Macie.1] Amazon Macie を有効にする必要があります

- [Macie.2] Macie 機密データ自動検出を有効にする必要があります
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります
- [MQ.3] Amazon MQ ブローカーでは、自動マイナーバージョンアップグレードが有効になっている必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.1] Network Firewall ファイアウォールを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.2] Network Firewall ログ記録を有効にする必要があります
- [Network Firewall.3] Network Firewall ポリシーには、1 つ以上のルールグループが関連付けられている必要があります
- [NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、完全なパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、断片化されたパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.6] ステートレス Network Firewall のルールグループを空にしないでください

- [NetworkFirewall.9] Network Firewall は削除保護を有効にする必要があります
- [NetworkFirewall.10] Network Firewall ファイアウォールでは、サブネット変更保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.10] OpenSearch ドメインには、最新のソフトウェアアップデートがインストールされている必要があります
- [Opensearch.11] OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です
- [PCA.1] AWS Private CA ルート認証機関を無効にする必要があります
- [RDS.1] RDS スナップショットはプライベートである必要があります
- [RDS.2] RDS DB インスタンスは、PubliclyAccessible 設定によって判断される、パブリックアクセスを禁止する必要があります
- [RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。
- [RDS.4] RDS クラスタースナップショットとデータベーススナップショットは保管中に暗号化する必要があります
- [RDS.5] RDS DB インスタンスは、複数のアベイラビリティーゾーンで設定する必要があります
- [RDS.6] RDS DB インスタンスの拡張モニタリングを設定する必要があります
- [RDS.7] RDS クラスターでは、削除保護が有効になっている必要があります
- [RDS.8] RDS DB インスタンスで、削除保護が有効になっている必要があります
- [RDS.9] RDS DB インスタンスは CloudWatch Logs にログを発行する必要があります
- [RDS.10] IAM 認証は RDS インスタンス用に設定する必要があります
- [RDS.11] RDS インスタンスでは、自動バックアップが有効になっている必要があります
- [RDS.12] IAM 認証は RDS クラスター用に設定する必要があります

- [RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります
- [RDS.16] Aurora DB クラスターは、タグを DB スナップショットにコピーするように設定する必要があります
- [RDS.17] RDS DB インスタンスは、タグをスナップショットにコピーするように設定する必要があります
- [RDS.19] 重大なクラスターイベントについて、既存の RDS イベント通知サブスクリプションを設定する必要があります
- [RDS.20] 重大なデータベースインスタンスイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります
- [RDS.21] 重大なデータベースパラメータグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります
- [RDS.22] 重大なデータベースセキュリティグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります
- [RDS.23] RDS インスタンスはデータベースエンジンのデフォルトポートを使用しないようにする必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [RDS.34] Aurora MySQL DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.40] RDS for SQL Server DB インスタンスは CloudWatch Logs にログを発行する必要があります
- [RDS.42] RDS for MariaDB DB インスタンスは CloudWatch Logs にログを発行する必要があります
- [RDS.45] Aurora MySQL DB クラスターでは、監査ログ記録を有効にする必要があります
- [PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります

- [Redshift.2] Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります
- [Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります
- [Redshift.4] Amazon Redshift クラスターでは、監査ログ記録が有効になっている必要があります
- [Redshift.6] Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります
- [Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります
- [Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください
- [Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [RedshiftServerless.4] Redshift Serverless 名前空間はカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [RedshiftServerless.7] Redshift Serverless 名前空間はデフォルトのデータベース名を使用しないでください
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.1] S3 汎用バケットではブロックパブリックアクセスの設定が有効になっている必要があります。
- [S3.2] S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります
- [S3.3] S3 汎用バケットではパブリック書き込みアクセスをブロックする必要があります。
- [S3.5] S3 汎用バケットではリクエストに SSL を使用する必要があります。
- [S3.6] S3 汎用バケットポリシーは、他の へのアクセスを制限する必要があります AWS アカウント
- [S3.7] S3 汎用バケットでクロスリージョンレプリケーションを使用する必要があります
- [S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります
- [S3.9] S3 汎用バケットは、サーバーアクセスログ記録を有効にする必要があります
- [S3.10] バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です
- [S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります
- [S3.12] ACL は、S3 汎用バケットへのユーザーアクセスの管理に使用しないでください。
- [S3.13] S3 汎用バケットにはライフサイクル設定が必要です
- [S3.14] S3 汎用バケットではバージョニングが有効になっている必要があります
- [S3.15] S3 汎用バケットでは Object Lock が有効になっている必要があります

- [S3.17] S3 汎用バケットは保管時に で暗号化する必要があります AWS KMS keys
- [S3.19] S3 アクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります
- [SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります
- [SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- [SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません
- [SageMaker.4] SageMaker エンドポイントの本番稼働バリアントの初期インスタンス数は 1 より大きい必要があります
- [SecretsManager.1] Secrets Manager のシークレットは、自動ローテーションを有効にする必要があります
- [SecretsManager.2] 自動ローテーションを設定した Secrets Manager のシークレットは正常にローテーションする必要があります
- [SecretsManager.3] 未使用の Secrets Manager のシークレットを削除します
- [SecretsManager.4] Secrets Manager のシークレットは、指定された日数以内にローテーションする必要があります
- [ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SNS.1] SNS トピックは、保管時に を使用して暗号化する必要があります AWS KMS
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [SSM.4] SSM ドキュメントはパブリックにしないでください
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [Transfer.3] Transfer Family コネクタではログ記録が有効になっている必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.2] AWS WAF Classic リージョンルールには少なくとも 1 つの条件が必要です
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です

- [WAF.4] AWS WAF Classic Regional Web ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります
- [WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります

Security Hub CSPM の NIST SP 800-171 リビジョン 2

NIST Special Publication 800-171 Revision 2 (NIST SP 800-171 Rev. 2) は、米国商務省の一部である米国国立標準技術研究所 (NIST) によって開発されたサイバーセキュリティとコンプライアンスのフレームワークです。このコンプライアンスフレームワークは、米国連邦政府の一部ではないシステムや組織で、管理対象未分類情報の機密性を保護するための推奨セキュリティ要件を提供します。CUI とも呼ばれる管理された未分類情報は、政府の分類基準を満たしていないが保護する必要がある機密情報です。 これは機密情報と見なされ、米国連邦政府または米国連邦政府に代わって他の団体によって作成または所有される情報です。

NIST SP 800-171 Rev. 2 は、以下の場合に CUI の機密性を保護するための推奨セキュリティ要件を提供します。

- 情報は、連邦以外のシステムや組織にあります。
- 非連邦組織が連邦機関に代わって情報を収集または維持していない、または機関に代わってシステムを使用または運用していない。
- CUI Registry にリストされている CUI カテゴリの認可法、規制、または政府全体のポリシーに規定された CUI の機密性を保護するための具体的な保護要件はありません。

この要件は、CUI を処理、保存、送信する、またはコンポーネントのセキュリティ保護を提供する非フェデラルシステムおよび組織のすべてのコンポーネントに適用されます。詳細については、NIST Computer Security Resource Center の「NIST SP 800-171 Rev. 2」を参照してください。

AWS Security Hub CSPM は、NIST SP 800-171 Revision 2 要件のサブセットをサポートするセキュリティコントロールを提供します。コントロールは、特定の AWS のサービス および リソースの自

動セキュリティチェックを実行します。これらのコントロールを有効にして管理するには、Security Hub CSPM で NIST SP 800-171 Revision 2 フレームワークを標準として有効にします。コントロールは、手動チェックを必要とする NIST SP 800-171 Revision 2 の要件をサポートしていないことに注意してください。

トピック

- 標準に適用されるコントロールのリソース記録の設定
- 標準に適用されるコントロールの決定

標準に適用されるコントロールのリソース記録の設定

検出結果の範囲と精度を最適化するには、 AWS Security Hub CSPM で NIST SP 800-171 Revision 2 標準を有効にする AWS Config 前に、 でリソース記録を有効にして設定することが重要です。リソース記録を設定するときは、標準に適用されるコントロールによってチェックされるすべてのタイプの AWS リソースに対しても有効にしてください。それ以外の場合、Security Hub CSPM は適切なリソースを評価し、標準に適用されるコントロールの正確な検出結果を生成できない可能性があります。

Security Hub CSPM が でリソース記録を使用する方法については AWS Config、「」を参照してくださいSecurity Hub CSPM AWS Config の有効化と設定。でのリソース記録の設定については AWS Config、「 AWS Config デベロッパーガイド」の「設定レコーダーの使用」を参照してください。

次の表は、Security Hub CSPM の NIST SP 800-171 Revision 2 標準に適用されるコントロールに記録するリソースのタイプを示しています。

AWS のサービス	リソースタイプ
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`
Amazon API Gateway	`AWS::ApiGateway::Stage`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::NetworkAcl` , `AWS::EC2:`

AWS のサービス	リソースタイプ
	`:SecurityGroup` , `AWS::EC2::VPC` , `AWS::EC2::VPNConnection`
エラスティックロードバランシング	`AWS::ElasticLoadBalancing::LoadBalancer`
AWS Identity and Access Management(IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
AWS Systems Manager(SSM)	`AWS::SSM::PatchCompliance`
AWS WAF	`AWS::WAFv2::RuleGroup`

標準に適用されるコントロールの決定

次のリストは、NIST SP 800-171 Revision 2 の要件をサポートするコントロールを指定し、 AWS Security Hub CSPM の NIST SP 800-171 Revision 2 標準に適用されます。コントロールがサポートする特定の要件の詳細については、コントロールを選択します。次に、コントロールの詳細の関連要件フィールドを参照してください。このフィールドは、コントロールがサポートする各 NIST 要件を指定します。フィールドで特定の NIST 要件が指定されていない場合、コントロールは要件をサポートしていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります

- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudTrail.2] CloudTrail は保管時の暗号化を有効にする必要があります
- [CloudTrail.3] 少なくとも 1 つの CloudTrail 証跡を有効にする必要があります
- [PCI.CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります
- [CloudWatch.1] 「ルート」ユーザーの使用に対するログメトリクスフィルターとアラームが存在する必要があります
- [CloudWatch.2] 不正な API 呼び出しに対してログメトリクスフィルターとアラームが存在することを確認します
- [CloudWatch.4] IAM ポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します
- [CloudWatch.5] CloudTrail 設定変更のログメトリクスフィルターとアラームが存在することを確認する
- [CloudWatch.6] AWS Management Console 認証失敗のログメトリクスフィルターとアラームが存在することを確認する
- [CloudWatch.7] カスタマーマネージドキーの無効化またはスケジュールされた削除に対するログメトリクスフィルターとアラームが存在することを確認します
- [CloudWatch.8] S3 バケットポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します
- [CloudWatch.9] AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する
- [CloudWatch.10] セキュリティグループの変更に対するログメトリクスフィルターとアラームが存在することを確認します
- [CloudWatch.11] ネットワークアクセスコントロールリスト (NACL) への変更に対するログメトリクスフィルターとアラームが存在することを確認します
- [CloudWatch.12] ネットワークゲートウェイへの変更に対するログメトリクスフィルターとアラームが存在することを確認します
- [CloudWatch.13] ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認します
- [CloudWatch.14] VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認します

- [CloudWatch.15] CloudWatch アラームには、指定されたアクションが設定されている必要があります
- [EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします
- [EC2.10] Amazon EC2 サービス用に作成された VPC エンドポイントを使用するようにAmazon EC2 を設定することをお勧めします
- [EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります
- [EC2.16] 未使用のネットワークアクセスコントロールリストを削除することをお勧めします
- [EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします
- [EC2.19] セキュリティグループは、リスクの高いポートへの無制限アクセスを許可してはいけません
- [EC2.20] AWS Site-to-Site VPN トンネルが稼働している必要があります
- [EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.3] Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります
- [ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な uration AWS Configを持つ事前定義されたセキュリティポリシーを使用する必要があります
- [GuardDuty.1] GuardDuty を有効にする必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.10] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します

- [IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します
- [IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します
- [IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します
- [IAM.15] IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認します
- [IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています
- [IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [NetworkFirewall.2] Network Firewall ログ記録を有効にする必要があります
- [Network Firewall.3] Network Firewall ポリシーには、1 つ以上のルールグループが関連付けられている必要があります
- [NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、断片化されたパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.6] ステートレス Network Firewall のルールグループを空にしないでください
- [S3.5] S3 汎用バケットではリクエストに SSL を使用する必要があります。
- [S3.6] S3 汎用バケットポリシーは、他の へのアクセスを制限する必要があります AWS アカウント
- [S3.9] S3 汎用バケットは、サーバーアクセスログ記録を有効にする必要があります
- [S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります
- [S3.14] S3 汎用バケットではバージョニングが有効になっている必要があります
- [S3.17] S3 汎用バケットは保管時に で暗号化する必要があります AWS KMS keys
- [SNS.1] SNS トピックは、保管時に を使用して暗号化する必要があります AWS KMS
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
- [WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります

Security Hub CSPM の PCI DSS

Payment Card Industry Data Security Standard (PCI DSS) は、クレジットカードとデビットカードの情報を安全に処理するための一連のルールとガイドラインを提供するサードパーティーのコンプライアンスフレームワークです。PCI Security Standards Council (SSC) は、このフレームワークを作成および更新します。

AWS Security Hub CSPM は、このサードパーティーフレームワークへの準拠を維持するのに役立つ PCI DSS 標準を提供します。この標準を使用して、カード所有者データを処理する AWS リソースのセキュリティの脆弱性を検出できます。カード所有者データまたは機密認証データを保存、処理、または送信するリソース AWS アカウント がある でこの標準を有効にすることをお勧めします。PCI SSC による評価では、この標準を検証しました。

Security Hub CSPM は、PCI DSS v3.2.1 と PCI DSS v4.0.1 の両方をサポートしています。v4.0.1 を使用して、セキュリティのベストプラクティスを最新の状態に保つことをお勧めします。標準の両方のバージョンを同時に有効にできます。標準を有効にする方法については、「」を参照してください[セキュリティ標準の有効化](#)。現在 v3.2.1 を使用しているが v4.0.1 のみを使用する場合は、古いバージョンを無効にする前に新しいバージョンを有効にします。これにより、セキュリティチェックのギャップを防ぐことができます。Security Hub CSPM と の統合を使用して AWS Organizations いて、複数のアカウントで v4.0.1 をバッチ有効化する場合は、[中央設定](#)を使用して有効にすることをお勧めします。

以下のセクションでは、PCI DSS v3.2.1 および PCI DSS v4.0.1 に適用されるコントロールを指定します。

PCI DSS v3.2.1 に適用されるコントロール

次のリストは、PCI DSS v3.2.1 に適用される Security Hub CSPM コントロールを指定します。コントロールの詳細を確認するには、コントロールを選択します。

[[AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要がある](#)

[[CloudTrail.2] CloudTrail は保管時の暗号化を有効にする必要があります](#)

[[CloudTrail.3] 少なくとも 1 つの CloudTrail 証跡を有効にする必要があります](#)

[[PCI.CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります](#)

[[CloudTrail.5] CloudTrail 追跡は Amazon CloudWatch Logs と統合する必要があります](#)

[CloudWatch.1] 「ルート」ユーザーの使用に対するログメトリクスフィルターとアラームが存在する必要があります

[CodeBuild.1] CodeBuild Bitbucket ソースリポジトリの URL には機密認証情報を含めないでください

[CodeBuild.2] CodeBuild プロジェクト環境変数にクリアテキストの認証情報を含めることはできません

[Config.1] を有効にし、サービスにリンクされたロールをリソース記録に使用 AWS Config する必要があります

[DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります

[EC2.1] Amazon EBS スナップショットはパブリックに復元できないようにすることをお勧めします

[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします

[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします

[EC2.12] 未使用の Amazon EC2 EIP を削除することをお勧めします

[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります

[ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります

[ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります

[ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります

[GuardDuty.1] GuardDuty を有効にする必要があります

[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください

[IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください

[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません

[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります

[IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります

[IAM.9] ルートユーザーに対して MFA を有効にする必要があります

[IAM.10] IAM ユーザーのパスワードポリシーには強力な設定が必要です

[IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります

[KMS.4] AWS KMS キーローテーションを有効にする必要があります

[Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります

[Lambda.3] Lambda 関数は VPC 内に存在する必要があります

[Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります

[Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります

[RDS.1] RDS スナップショットはプライベートである必要があります

[RDS.2] RDS DB インスタンスは、PubliclyAccessible 設定によって判断される、パブリックアクセスを禁止する必要があります

[PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります

[S3.1] S3 汎用バケットではブロックパブリックアクセスの設定が有効になっている必要があります。

[S3.2] S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります

[S3.3] S3 汎用バケットではパブリック書き込みアクセスをブロックする必要があります。

[S3.5] S3 汎用バケットではリクエストに SSL を使用する必要があります。

[S3.7] S3 汎用バケットでクロスリージョンレプリケーションを使用する必要があります

[SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります

[SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager

[SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります

[SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります

PCI DSS v4.0.1 に適用されるコントロール

次のリストは、PCI DSS v4.0.1 に適用される Security Hub CSPM コントロールを指定します。コントロールの詳細を確認するには、コントロールを選択します。

[ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります

[ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります

[APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります

[AppSync.2] AWS AppSync フィールドレベルのログ記録を有効にする必要があります

[AutoScaling.3] Auto Scaling グループ起動設定は、EC2 インスタンスを、インスタンスメタデータサービスバージョン 2 (IMDSv2) を必要とするように設定する必要があります

[Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません

[CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります

[CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください

[CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります

[CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります

[CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります

[CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります

[CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります

[CloudTrail.2] CloudTrail は保管時の暗号化を有効にする必要があります

[CloudTrail.3] 少なくとも 1 つの CloudTrail 証跡を有効にする必要があります

[PCI.CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります

[CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットが一般公開されていないことを確認します

[CloudTrail.7] CloudTrail S3 バケットで、S3 バケットアクセスログ記録が有効であることを確認します

[CodeBuild.1] CodeBuild Bitbucket ソースリポジトリの URL には機密認証情報を含めないでください

[CodeBuild.2] CodeBuild プロジェクト環境変数にクリアテキストの認証情報を含めることはできません

[CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります

[DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります

[DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります

[DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります

[DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります

[DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。

[DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。

[DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。

[DMS.9] DMS エンドポイントは SSL を使用する必要があります。

[DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です

[DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません

[DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります

[DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります

[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります

[EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります

[EC2.15] Amazon EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないことをお勧めします

[EC2.16] 未使用のネットワークアクセスコントロールリストを削除することをお勧めします

[EC2.170] EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします

[EC2.171] EC2 VPN 接続では、ログ記録が有効になっている必要があります

[EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります

[EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします

[EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります

[EC2.53] EC2 セキュリティグループが 0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可することがないようにする必要があります

[EC2.54] EC2 セキュリティグループは ::/0 からリモートサーバー管理ポートへの入力を許可しない必要があります

[EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします

[ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります

[ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。

[ECS.16] ECS タスクセットはパブリック IP アドレスを自動的に割り当てないでください。

[ECS.2] ECS サービスには、パブリック IP アドレスを自動で割り当てないでください

[ECS.8] シークレットは、コンテナ環境の変数として渡さないでください

[EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります

[EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります

[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。

[EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります

[EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります

[ElastiCache.2] ElastiCache クラスターでは、マイナーバージョンの自動アップグレードを有効にする必要があります

[ElastiCache.5] ElastiCache レプリケーショングループは転送時に暗号化する必要があります

[ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります

[ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります

[ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります

[ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります

[ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります

[ELB.3] Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります

[ELB.4] Application Load Balancer は、無効な http ヘッダーを削除するように設定する必要があります

[ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な uration AWS Configを持つ事前定義されたセキュリティポリシーを使用する必要があります

[EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります

[EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります

[ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります

[ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります

[ES.5] Elasticsearch ドメインで監査ログ記録が有効になっている必要があります

[ES.8] Elasticsearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります

[EventBridge.3] Amazon EventBridge カスタムイベントバスにリソースポリシーがアタッチされている必要があります

[GuardDuty.1] GuardDuty を有効にする必要があります

[GuardDuty.10] GuardDuty S3 Protection を有効にする必要があります

[GuardDuty.6] GuardDuty Lambda Protection を有効にする必要があります

[GuardDuty.7] GuardDuty EKS ランタイムモニタリングを有効にする必要があります

[GuardDuty.9] GuardDuty RDS Protection を有効にする必要があります

[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります

[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります

[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります

[IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です

[IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります

[IAM.9] ルートユーザーに対して MFA を有効にする必要があります

[IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します

[IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します

[IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します

[IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています

[IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します

[IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します

[IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります

[Inspector.1] Amazon Inspector EC2 スキャンを有効にする必要があります

[Inspector.2] Amazon Inspector ECR スキャンを有効にする必要があります

[Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります

[Inspector.4] Amazon Inspector Lambda 標準スキャンを有効にする必要があります

[KMS.4] AWS KMS キーローテーションを有効にする必要があります

[Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります

[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります

[MQ.2] ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります

[MQ.3] Amazon MQ ブローカーでは、自動マイナーバージョンアップグレードが有効になっている必要があります

[MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります

[MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります

[Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります

[Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください

[Opensearch.10] OpenSearch ドメインには、最新のソフトウェアアップデートがインストールされている必要があります

[Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります

[RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります

[RDS.2] RDS DB インスタンスは、PubliclyAccessible 設定によって判断される、パブリックアクセスを禁止する必要があります

[RDS.20] 重大なデータベースインスタンスイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります

[RDS.21] 重大なデータベースパラメータグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります

[RDS.22] 重大なデータベースセキュリティグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります

[RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります

[RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります

[RDS.34] Aurora MySQL DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります

[RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります

[RDS.36] RDS for PostgreSQL DB は CloudWatch Logs にログを発行する必要があります

[RDS.37] Aurora PostgreSQL DB クラスターでは、ログを CloudWatch Logs に発行する必要があります

[RDS.9] RDS DB インスタンスは CloudWatch Logs にログを発行する必要があります

[PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります

[Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの入力を許可する必要があります

[Redshift.2] Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります

[Redshift.4] Amazon Redshift クラスターでは、監査ログ記録が有効になっている必要があります

[Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります

[S3.1] S3 汎用バケットではブロックパブリックアクセスの設定が有効になっている必要があります。

[S3.15] S3 汎用バケットでは Object Lock が有効になっている必要があります

[S3.17] S3 汎用バケットは保管時に で暗号化する必要があります AWS KMS keys

[S3.19] S3 アクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります

[S3.22] S3 汎用バケットはオブジェクトレベルの書き込みイベントをログに記録する必要があります

[S3.23] S3 汎用バケットはオブジェクトレベルの読み取りイベントをログに記録する必要があります

[S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります

[S3.5] S3 汎用バケットではリクエストに SSL を使用する必要があります。

[S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります

[S3.9] S3 汎用バケットは、サーバーアクセスログ記録を有効にする必要があります

[SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります

[SecretsManager.1] Secrets Manager のシークレットは、自動ローテーションを有効にする必要があります

[SecretsManager.2] 自動ローテーションを設定した Secrets Manager のシークレットは正常にローテーションする必要があります

[SecretsManager.4] Secrets Manager のシークレットは、指定された日数以内にローテーションする必要があります

[SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります

[SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります

[StepFunctions.1] Step Functions ステートマシンではログ記録がオンになっている必要があります

[Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください

[WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります

[WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります

Security Hub CSPM のサービスマネージド標準

サービスマネージド標準は、別の が AWS のサービス 管理するセキュリティ標準ですが、Security Hub CSPM で表示できます。たとえば、サービスマネージドスタンダード： AWS Control Tower は、 が AWS Control Tower 管理するサービスマネージドスタンダードです。サービスマネージド標準は、 AWS Security Hub CSPM が以下の方法で管理するセキュリティ標準とは異なります。

- 標準の作成と削除 — 管理サービスのコンソールまたは API、または AWS CLIを使用して、サービスマネージドスタンダードを作成および削除します。これらの方法のいずれかで管理サービスで標準を作成するまで、標準は Security Hub CSPM コンソールに表示されず、Security Hub CSPM API または からアクセスできません AWS CLI。
- コントロールの自動有効化なし – サービスマネージド標準を作成する場合、Security Hub CSPM と管理サービスは、標準に適用されるコントロールを自動的に有効にしません。さらに、Security Hub CSPM が標準の新しいコントロールをリリースすると、それらは自動的に有効になっていません。これは、Security Hub CSPM が管理する標準からの逸脱です。Security Hub CSPM でコントロールを設定する通常の方法の詳細については、「」を参照してくださいSecurity Hub CSPM のセキュリティコントロールについて。
- コントロールの有効化と無効化 — ドリフトを防ぐために、管理サービスでコントロールを有効または無効にすることをお勧めします。
- コントロールの可用性 – 管理サービスは、サービスマネージドスタンダードの一部として使用できるコントロールを選択します。使用可能なコントロールには、既存の Security Hub CSPM コントロールのすべてまたはサブセットが含まれます。

管理サービスによってサービスマネージド標準が作成され、コントロールが利用可能になったら、Security Hub CSPM コンソール、Security Hub CSPM API、または でコントロールの検出結果、コントロールステータス、標準セキュリティスコアにアクセスできます AWS CLI。この情報の一部または全部は、管理サービスで使用することもできます。

以下のリストからサービスマネージドスタンダードを選択すると、その詳細が表示されます。

サービスマネージドスタンダード

- サービスマネージドスタンダード： AWS Control Tower

サービスマネージドスタンダード： AWS Control Tower

このセクションでは、サービスマネージドスタンダードについて説明します AWS Control Tower。

サービスマネージドスタンダードとは AWS Control Tower

この標準は、 AWS Security Hub CSPM および のユーザー向けに設計されています AWS Control Tower。これにより、 AWS Control Tower サービスの Security Hub CSPM の検出コントロール AWS Control Tower とともに のプロアクティブコントロールを設定できます。

プロアクティブコントロールは、ポリシー違反や設定ミスにつながる可能性のあるアクションにフラグを付けるため、 がコンプライアンス AWS アカウント を維持するのに役立ちます。検出コントロールは、 AWS アカウント内のリソースのコンプライアンス違反 (設定ミスなど) を検出します。AWS 環境のプロアクティブコントロールと検出コントロールを有効にすることで、開発のさまざまな段階でセキュリティ体制を強化できます。

> **Tip**
>
> サービスマネージド標準は、 AWS Security Hub CSPM が管理する標準とは異なります。例えば、サービスマネージドスタンダードの作成および削除は、管理サービスで行う必要があります。詳細については、「Security Hub CSPM のサービスマネージド標準」を参照してください。

Security Hub CSPM コンソールと API では、Service-Managed Standard: AWS Control Tower と他の Security Hub CSPM 標準を表示できます。

標準の作成

この標準は、 で標準を作成する場合にのみ使用できます AWS Control Tower。 AWS Control Tower は、次のいずれかの方法を使用して該当するコントロールを最初に有効にするときに標準を作成します。

- AWS Control Tower コンソール
- AWS Control Tower API (`EnableControl` API を呼び出す)

- AWS CLI (`enable-control` コマンドを実行します)

Security Hub CSPM コントロールは、 AWS Control Tower コンソールで SH.***ControlID*** (SH.CodeBuild.1 など) として識別されます。

標準を作成するときに、Security Hub CSPM をまだ有効にしていない場合、 は Security Hub CSPM AWS Control Tower も有効にします。

を設定していない場合 AWS Control Tower、Security Hub CSPM コンソール、Security Hub CSPM API、または でこの標準を表示またはアクセスすることはできません AWS CLI。をセットアップした場合でも AWS Control Tower、前述の方法のいずれか AWS Control Tower を使用して で標準を作成しないと、Security Hub CSPM でこの標準を表示またはアクセスできません。

この標準は、 を含む AWS リージョンAWS Control Tower が利用可能な でのみ使用できます AWS GovCloud (US)。

標準のコントロールの有効化と無効化

AWS Control Tower コンソールで標準を作成したら、両方のサービスで標準とその使用可能なコントロールを表示できます。

最初に標準を作成すると、これに自動的に有効化されたコントロールはありません。さらに、Security Hub CSPM が新しいコントロールを追加すると、サービスマネージドスタンダード: に対して自動的に有効になるわけではありません AWS Control Tower。次のいずれかの方法 AWS Control Tower を使用して、 で標準のコントロールを有効または無効にする必要があります。

- AWS Control Tower コンソール
- AWS Control Tower API (`EnableControl`および `DisableControl` APIsを呼び出す)
- AWS CLI (コマンド`enable-control`と `disable-control` コマンドを実行します)

でコントロールの有効化ステータスを変更すると AWS Control Tower、その変更は Security Hub CSPM にも反映されます。

ただし、Security Hub CSPM で有効になっているコントロールを無効にすると、コントロールドリフト AWS Control Tower が発生します。のコントロールステータスは として AWS Control Tower 表示されます`Drifted`。このドリフトを解決するには、 AWS Control Tower コンソールで OU の再登録を選択するか、前述の方法のいずれか AWS Control Tower を使用して でコントロールを無効化および再有効化します。

で有効化アクションと無効化アクションを完了すると、コントロールドリフトを回避 AWS Control Tower できます。

でコントロールを有効または無効にすると AWS Control Tower、アクションはアカウントとリージョンに適用されます。Security Hub CSPM でコントロールを有効または無効にすると (この標準では推奨されません) 、アクションは現在のアカウントとリージョンにのみ適用されます。

> **Note**
>
> 中央設定は、サービスマネージドスタンダードの管理には使用できません AWS Control Tower。中央設定を使用する場合は、 AWS Control Tower サービスのみを使用して、一元管理されたアカウントのこの標準のコントロールを有効または無効にできます。

有効化ステータスとコントロールステータスの表示

次のいずれかの方法を使用して、コントロールの有効化ステータスを表示できます。

- Security Hub CSPM コンソール、Security Hub CSPM API、または AWS CLI
- AWS Control Tower コンソール
- AWS Control Tower 有効なコントロールのリストを表示する API (`ListEnabledControls` API を呼び出す)
- AWS CLI 有効になっているコントロールのリストを表示するには (`list-enabled-controls` コマンドを実行)

で無効にしたコントロール AWS Control Tower は、Security Hub CSPM `Disabled`でそのコントロールを明示的に有効にしない限り、Security Hub CSPM で有効化ステータスが になります。

Security Hub CSPM は、コントロールの検出結果のワークフローステータスとコンプライアンスステータスに基づいてコントロールステータスを計算します。有効化ステータスとコントロールステータスの詳細については、「Security Hub CSPM でのコントロールの詳細の確認」 を参照してください。

コントロールのステータスに基づいて、Security Hub CSPM はサービスマネージドスタンダードのセキュリティスコアを計算します AWS Control Tower。このスコアは Security Hub CSPM でのみ使用できます。さらに、コントロールの検出結果は Security Hub CSPM でのみ表示できます。標準のセキュリティスコアとコントロールの検出結果は では使用できません AWS Control Tower。

> **Note**
>
> サービスマネージドスタンダード: のコントロールを有効にすると AWS Control Tower、Security Hub CSPM が既存の AWS Config サービスにリンクされたルールを使用するコントロールの検出結果を生成するまでに最大 18 時間かかる場合があります。Security Hub CSPM で他の標準とコントロールを有効にしている場合は、既存のサービスにリンクされたルールがある場合があります。詳細については、「セキュリティチェックの実行スケジュール」を参照してください。

標準を削除する

次のいずれかの方法を使用して、該当するすべてのコントロールを無効にする AWS Control Tower ことで、 でこの標準を削除できます。

- AWS Control Tower コンソール
- AWS Control Tower API (`DisableControl` API を呼び出す)
- AWS CLI (`disable-control` コマンドを実行します)

すべてのコントロールを無効にすることにより、 AWS Control Tower のすべてのマネージドアカウントと管理対象リージョンの標準が削除されます。で標準を削除すると AWS Control Tower 、Security Hub CSPM コンソールの標準ページから削除され、Security Hub CSPM API または を使用してアクセスできなくなります AWS CLI。

> **Note**
>
> Security Hub CSPM で標準からすべてのコントロールを無効にしても、標準は無効または削除されません。

Security Hub CSPM サービスを無効にすると、Service-Managed Standard: AWS Control Tower および有効にしたその他の標準が削除されます。

サービスマネージドスタンダードの検出結果フィールド形式： AWS Control Tower

Service-Managed Standard: を作成し、そのコントロールを有効にする AWS Control Tower と、Security Hub CSPM でコントロールの検出結果を受信し始めます。Security Hub CSPM は、 で

コントロールの検出結果をレポートしますAWS Security Finding 形式 (ASFF)。これらは、この標準の Amazon リソースネーム (ARN) および `GeneratorId` の ASFF 値です。

- 標準 ARN — *`arn:aws:us-east-1`*`:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0`
- GeneratorId – `service-managed-aws-control-tower/v/1.0.0/`*`CodeBuild.1`*

サービスマネージドスタンダード: の検出結果の例については AWS Control Tower、「」を参照してくださいコントロールの検出結果のサンプル。

サービスマネージドスタンダードに適用されるコントロール： AWS Control Tower

サービスマネージドスタンダード: AWS Foundational Security Best Practices (FSBP) 標準の一部であるコントロールのサブセット AWS Control Tower をサポートします。コントロールを選択して、失敗した検出結果の修正ステップなど、そのコントロールに関する情報を表示します。

次のリストは、サービスマネージドスタンダードで使用可能なコントロールを示しています AWS Control Tower。コントロールに対するリージョンの制限は、FSBP 標準のコロラリーコントロールに対するリージョンの制限と一致します。このリストには、標準に依存しないセキュリティコントロール ID が表示されます。 AWS Control Tower コンソールでは、コントロール IDsは SH.***`ControlID`*** (SH.CodeBuild.1 など) の形式になります。Security Hub CSPM で、アカウントで統合コントロールの検出結果がオフになっている場合、 `ProductFields.ControlId`フィールドは標準ベースのコントロール ID を使用します。標準ベースのコントロール ID は、CT.***`ControlId`*** (CT.CodeBuild.1 など) としてフォーマットされます。

- [Account.1] のセキュリティ連絡先情報は に提供する必要があります AWS アカウント
- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [APIGateway.1] API Gateway REST および WebSocket API 実行ログ記録を有効にする必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります
- [APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります

- [APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります
- [APIGateway.5] API Gateway REST API のキャッシュデータは、保管中に暗号化する必要があります
- [APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- [AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- [AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要がある
- [AutoScaling.2] Amazon EC2 Auto Scaling グループは、複数のアベイラビリティーゾーンをカバーする必要があります
- [AutoScaling.3] Auto Scaling グループ起動設定は、EC2 インスタンスを、インスタンスメタデータサービスバージョン 2 (IMDSv2) を必要とするように設定する必要があります
- [Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません
- [AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります
- [AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります
- [CloudTrail.1] CloudTrail を有効にして、少なくとも 1 つのマルチリージョンの追跡で、読み取りと書き込みの管理イベントを含めた設定をする必要があります。
- [CloudTrail.2] CloudTrail は保管時の暗号化を有効にする必要があります
- [PCI.CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります
- [CloudTrail.5] CloudTrail 追跡は Amazon CloudWatch Logs と統合する必要があります
- [CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットが一般公開されていないことを確認します
- [CodeBuild.1] CodeBuild Bitbucket ソースリポジトリの URL には機密認証情報を含めないでください
- [CodeBuild.2] CodeBuild プロジェクト環境変数にクリアテキストの認証情報を含めることはできません
- [CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- [CodeBuild.4] CodeBuild AWS Configプロジェクト環境にはログ記録設定が必要です

- [DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DynamoDB.1] DynamoDB テーブルは、需要に応じて容量をオートスケーリングする必要があります
- [DynamoDB.2] DynamoDB テーブルでは、ポイントインタイムリカバリが有効になっている必要があります。
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [EC2.1] Amazon EBS スナップショットはパブリックに復元できないようにすることをお勧めします
- [EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします
- [EC2.3] アタッチされた Amazon EBS ボリュームは、保管時に暗号化することをお勧めします
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします
- [EC2.7] EBS のデフォルト暗号化を有効にすることをお勧めします
- [EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.9] Amazon EC2 インスタンスは、パブリック IPv4 アドレスを未設定にすることをお勧めします
- [EC2.10] Amazon EC2 サービス用に作成された VPC エンドポイントを使用するようにAmazon EC2 を設定することをお勧めします
- [EC2.15] Amazon EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないことをお勧めします
- [EC2.16] 未使用のネットワークアクセスコントロールリストを削除することをお勧めします
- [EC2.17] Amazon EC2 インスタンスが複数の ENI を使用しないようにすることをお勧めします
- [EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします

- [EC2.19] セキュリティグループは、リスクの高いポートへの無制限アクセスを許可してはいけません
- [EC2.20] AWS Site-to-Site VPN トンネルが稼働している必要があります
- [EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。
- [ECS.2] ECS サービスには、パブリック IP アドレスを自動で割り当てないでください
- [ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください
- [ECS.4] ECS コンテナは、非特権として実行する必要があります
- [ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。
- [ECS.8] シークレットは、コンテナ環境の変数として渡さないでください
- [ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。
- [ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります
- [EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります
- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります

- [EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [ElastiCache.3] ElastiCache (Redis OSS) レプリケーショングループでは、自動フェイルオーバーを有効にする必要があります
- [ElastiCache.4] ElastiCache レプリケーショングループは保管中に暗号化する必要があります
- [ElastiCache.5] ElastiCache レプリケーショングループは転送時に暗号化する必要があります
- [ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります
- [ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。
- [ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります
- [ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.3] Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります
- [ELB.4] Application Load Balancer は、無効な http ヘッダーを削除するように設定する必要があります
- [ELB.5] アプリケーションおよび Classic Load Balancer のログ記録を有効にする必要があります
- [ELB.6] アプリケーション、ゲートウェイ、および Network Load Balancer で削除保護を有効にする必要があります
- [ELB.7] Classic Load Balancers は、Connection Draining を有効にする必要があります
- [ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な uration AWS Configを持つ事前定義されたセキュリティポリシーを使用する必要があります
- [ELB.9] Classic Load Balancer では、クロスゾーンロードバランシングが有効になっている必要があります
- [ELB.10] Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります

- [ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります
- [ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります
- [ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります
- [ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります
- [ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります
- [ES.5] Elasticsearch ドメインで監査ログ記録が有効になっている必要があります
- [ES.6] Elasticsearch ドメインには少なくとも 3 つのデータノードが必要です
- [ES.7] Elasticsearch ドメインは、少なくとも 3 つの専用マスターノードを設定する必要があります。
- [ES.8] Elasticsearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [EventBridge.3] Amazon EventBridge カスタムイベントバスにリソースポリシーがアタッチされている必要があります
- [GuardDuty.1] GuardDuty を有効にする必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります

- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [KMS.3] AWS KMS keys を意図せずに削除しないでください
- [KMS.4] AWS KMS キーローテーションを有効にする必要があります
- [Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります
- [Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります
- [Lambda.3] Lambda 関数は VPC 内に存在する必要があります
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Network Firewall.3] Network Firewall ポリシーには、1 つ以上のルールグループが関連付けられている必要があります
- [NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、完全なパケットに対してドロップまたは転送される必要があります。

- [NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、断片化されたパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.6] ステートレス Network Firewall のルールグループを空にしないでください
- [Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [RDS.1] RDS スナップショットはプライベートである必要があります
- [RDS.2] RDS DB インスタンスは、PubliclyAccessible 設定によって判断される、パブリックアクセスを禁止する必要があります
- [RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。
- [RDS.4] RDS クラスタースナップショットとデータベーススナップショットは保管中に暗号化する必要があります
- [RDS.5] RDS DB インスタンスは、複数のアベイラビリティーゾーンで設定する必要があります
- [RDS.6] RDS DB インスタンスの拡張モニタリングを設定する必要があります
- [RDS.8] RDS DB インスタンスで、削除保護が有効になっている必要があります
- [RDS.9] RDS DB インスタンスは CloudWatch Logs にログを発行する必要があります
- [RDS.10] IAM 認証は RDS インスタンス用に設定する必要があります
- [RDS.11] RDS インスタンスでは、自動バックアップが有効になっている必要があります
- [RDS.12] IAM 認証は RDS クラスター用に設定する必要があります
- [RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります

- [RDS.17] RDS DB インスタンスは、タグをスナップショットにコピーするように設定する必要があります
- [RDS.18] RDS インスタンスは VPC 内にデプロイする必要があります
- [RDS.19] 重大なクラスターイベントについて、既存の RDS イベント通知サブスクリプションを設定する必要があります
- [RDS.20] 重大なデータベースインスタンスイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります
- [RDS.21] 重大なデータベースパラメータグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります
- [RDS.22] 重大なデータベースセキュリティグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります
- [RDS.23] RDS インスタンスはデータベースエンジンのデフォルトポートを使用しないようにする必要があります
- [RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります
- [Redshift.2] Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります
- [Redshift.4] Amazon Redshift クラスターでは、監査ログ記録が有効になっている必要があります
- [Redshift.6] Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります
- [Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります
- [Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください
- [Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [S3.1] S3 汎用バケットではブロックパブリックアクセスの設定が有効になっている必要があります。
- [S3.2] S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります
- [S3.3] S3 汎用バケットではパブリック書き込みアクセスをブロックする必要があります。
- [S3.5] S3 汎用バケットではリクエストに SSL を使用する必要があります。

- [S3.6] S3 汎用バケットポリシーは、他の へのアクセスを制限する必要があります AWS アカウント
- [S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります
- [S3.9] S3 汎用バケットは、サーバーアクセスログ記録を有効にする必要があります
- [S3.12] ACL は、S3 汎用バケットへのユーザーアクセスの管理に使用しないでください。
- [S3.13] S3 汎用バケットにはライフサイクル設定が必要です
- [S3.17] S3 汎用バケットは保管時に で暗号化する必要があります AWS KMS keys
- [SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります
- [SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- [SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません
- [SecretsManager.1] Secrets Manager のシークレットは、自動ローテーションを有効にする必要があります
- [SecretsManager.2] 自動ローテーションを設定した Secrets Manager のシークレットは正常にローテーションする必要があります
- [SecretsManager.3] 未使用の Secrets Manager のシークレットを削除します
- [SecretsManager.4] Secrets Manager のシークレットは、指定された日数以内にローテーションする必要があります
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [SSM.4] SSM ドキュメントはパブリックにしないでください
- [WAF.2] AWS WAF Classic リージョンルールには少なくとも 1 つの条件が必要です
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です
- [WAF.4] AWS WAF Classic Regional Web ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

この標準の詳細については、「 AWS Control Tower ユーザーガイド」の「Security Hub CSPM コントロール」を参照してください。

セキュリティ標準の有効化

AWS Security Hub CSPM でセキュリティ標準を有効にすると、Security Hub CSPM は標準に適用されるすべてのコントロールを自動的に作成して有効にします。Security Hub CSPM は、セキュリティチェックの実行とコントロールの検出結果の生成も開始します。

検出結果の範囲と精度を最適化するには、標準を有効にする AWS Config 前に、 でリソース記録を有効にして設定します。リソース記録を設定するときは、標準に適用されるコントロールによってチェックされるすべてのタイプのリソースに対しても有効にしてください。それ以外の場合、Security Hub CSPM は適切なリソースを評価し、標準に適用されるコントロールの正確な検出結果を生成できない可能性があります。詳細については、「Security Hub CSPM AWS Config の有効化と設定」を参照してください。

標準を有効にしたら、標準に適用される個々のコントロールを無効にしたり、後で再度有効にしたりできます。標準のコントロールを無効にすると、Security Hub CSPM はコントロールの検出結果の生成を停止します。さらに、Security Hub CSPM は、標準のセキュリティスコアを計算するときにコントロールを無視します。セキュリティスコアは、標準に適用され、有効になっており、評価データがあるコントロールの総数に対する、評価に合格したコントロールの割合です。

標準を有効にすると、Security Hub CSPM は、通常、Security Hub CSPM コンソールの 概要またはセキュリティ標準ページに初めてアクセスしてから 30 分以内に、標準の予備セキュリティスコアを生成します。セキュリティスコアは、コンソールでそれらのページにアクセスしたときに有効になっている標準に対してのみ生成されます。さらに、 AWS Config スコアを表示するには、 でリソース記録を設定する必要があります。中国リージョンおよび では AWS GovCloud (US) Regions、Security Hub CSPM が標準の予備セキュリティスコアを生成するまでに最大 24 時間かかる場合があります。Security Hub CSPM が予備スコアを生成した後、24 時間ごとにスコアを更新します。セキュリティスコアが最後に更新された日時を確認するには、Security Hub CSPM がスコアに提供するタイムスタンプを参照できます。詳細については、「セキュリティスコアの計算」を参照してください。

標準を有効にする方法は、中央設定を使用して複数のアカウントと の Security Hub CSPM を管理するかどうかによって異なります AWS リージョン。マルチアカウント、マルチリージョン環境で標準を有効にする場合、中央設定を使用することをお勧めします。Security Hub CSPM を と統合する場合は、中央設定を使用できます AWS Organizations。中央設定を使用しない場合は、各アカウントと各リージョンで各標準を個別に有効にする必要があります。

トピック

- 複数のアカウントで標準を有効にし、 AWS リージョン
- 1 つのアカウントで標準を有効にし、 AWS リージョン
- 標準のステータスの確認

複数のアカウントで標準を有効にし、 AWS リージョン

複数のアカウントおよび でセキュリティ標準を有効にして設定するには AWS リージョン、中央設定を使用します。中央設定を使用すると、委任 Security Hub CSPM 管理者は、1 つ以上の標準を有効にする Security Hub CSPM 設定ポリシーを作成できます。その後、管理者は設定ポリシーを個々のアカウント、組織単位 (OUs)、またはルートに関連付けることができます。設定ポリシーは、集約リージョンとも呼ばれるホームリージョンと、すべてのリンクされたリージョンに影響します。

設定ポリシーにはカスタマイズオプションがあります。たとえば、1 つの OU に対して AWS Foundational Security Best Practices (FSBP) 標準のみを有効にするように選択できます。別の OU では、FSBP 標準と Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 標準の両方を有効にすることができます。指定した特定の標準を有効にする設定ポリシーの作成については、「」を参照してください設定ポリシーの作成と関連付け。

中央設定を使用する場合、Security Hub CSPM は新規または既存のアカウントの標準を自動的に有効にしません。代わりに、Security Hub CSPM 管理者は、組織の Security Hub CSPM 設定ポリシーを作成するときに、異なるアカウントで有効にする標準を指定します。Security Hub CSPM には、FSBP 標準のみが有効になっている推奨設定ポリシーが用意されています。詳細については、「設定ポリシーのタイプ」を参照してください。

> **Note**
>
> Security Hub CSPM 管理者は、設定ポリシーを使用して、AWS Control Tower サービスマネージド標準以外の標準を有効にできます。この標準を有効にするには、管理者が AWS Control Tower を直接使用する必要があります。また、 を使用して AWS Control Tower 、一元管理されたアカウントのこの標準の個々のコントロールを有効または無効にする必要があります。

一部のアカウントで自分のアカウントの標準を有効にして設定する場合、Security Hub CSPM 管理者はそれらのアカウントをセルフマネージドアカウントとして指定できます。セルフマネージドアカウントは、各リージョンで個別に標準を有効にして設定する必要があります。

1 つのアカウントで標準を有効にし、 AWS リージョン

中央設定を使用しない場合、またはセルフマネージドアカウントがある場合は、設定ポリシーを使用して、複数のアカウントまたは でセキュリティ標準を一元的に有効にすることはできません AWS リージョン。ただし、1 つのアカウントとリージョンで標準を有効にできます。これを行うには、Security Hub CSPM コンソールまたは Security Hub CSPM API を使用します。

Security Hub CSPM console

Security Hub CSPM コンソールを使用して、1 つのアカウントとリージョンで標準を有効にするには、次の手順に従います。

1 つのアカウントおよびリージョンで標準を有効にするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、標準を有効にするリージョンを選択します。
3. ナビゲーションペインで、[セキュリティ標準] を選択します。セキュリティ標準ページには、Security Hub CSPM が現在サポートしているすべての標準が一覧表示されます。標準を既に有効にしている場合、標準の セクションには、現在のセキュリティスコアと標準の追加の詳細が含まれます。
4. 有効にする標準のセクションで、標準を有効にするを選択します。

追加のリージョンで標準を有効にするには、追加のリージョンごとに前述のステップを繰り返します。

Security Hub CSPM API

単一のアカウントとリージョンで標準をプログラムで有効にするには、 BatchEnableStandardsオペレーションを使用します。または、 AWS Command Line Interface （ AWS CLI) を使用している場合は、 batch-enable-standards コマンドを実行します。

リクエストで、 `StandardsArn`パラメータを使用して、有効にする標準の Amazon リソースネーム (ARN) を指定します。また、リクエストが適用されるリージョンも指定します。たとえば、次のコマンドは AWS Foundational Security Best Practices (FSBP) 標準を有効にします。

```
$ aws securityhub batch-enable-standards \
```

```
--standards-subscription-requests '{"StandardsArn":"arn:aws:securityhub:us-
east-1::standards/aws-foundational-security-best-practices/v/1.0.0"}' \
--region us-east-1
```

arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0 は米国東部 (バージニア北部) リージョンの FSBP 標準の ARN であり、*us-east-1* はそれを有効にするリージョンです。

標準の ARN を取得するには、 DescribeStandardsオペレーションを使用するか、 を使用している場合は describe-standards コマンド AWS CLIを実行します。

まず、アカウントで現在有効になっている標準のリストを確認するには、GetEnabledStandardsオペレーションを使用できます。を使用している場合は AWS CLI、get-enabled-standards コマンドを実行して、このリストを取得できます。

標準を有効にすると、Security Hub CSPM は、アカウントと指定されたリージョンで標準を有効にするタスクの実行を開始します。これには、標準に適用されるすべてのコントロールの作成が含まれます。これらのタスクのステータスをモニタリングするには、アカウントとリージョンの標準のステータスを確認できます。

標準のステータスの確認

アカウントのセキュリティ標準を有効にすると、Security Hub CSPM はアカウントの標準に適用されるすべてのコントロールの作成を開始します。Security Hub CSPM は、標準の予備セキュリティスコアの生成など、アカウントの標準を有効にするための追加のタスクも実行します。Security Hub CSPM がこれらのタスクを実行する間、標準のステータスはアカウントPending用です。その後、標準のステータスは追加の状態を通過し、これをモニタリングして確認できます。

> **Note**
>
> 標準の個々のコントロールを変更しても、標準の全体的なステータスには影響しません。たとえば、以前に無効にしたコントロールを有効にしても、変更は標準のステータスには影響しません。同様に、有効なコントロールのパラメータ値を変更しても、標準のステータスには影響しません。

Security Hub CSPM コンソールを使用して標準のステータスを確認するには、ナビゲーションペインでセキュリティ標準を選択します。セキュリティ標準ページには、Security Hub CSPM が現在サポートしているすべての標準が一覧表示されます。Security Hub CSPM が標準を有効にするタスク

を現在実行している場合、標準の セクションは、Security Hub CSPM がまだ標準のセキュリティスコアを生成していることを示しています。標準が有効になっている場合、標準のセクションには現在のスコアが含まれます。結果の表示を選択して、標準に適用される個々のコントロールのステータスなど、追加の詳細を確認します。詳細については、「セキュリティチェックの実行スケジュール」を参照してください。

Security Hub CSPM API を使用して標準のステータスをプログラムで確認するには、GetEnabledStandardsオペレーションを使用します。リクエストでは、オプションで`StandardsSubscriptionArns`パラメータを使用して、ステータスを確認する標準の Amazon リソースネーム (ARN) を指定します。 AWS Command Line Interface （ AWS CLI) を使用している場合は、get-enabled-standards コマンドを実行して、標準のステータスを確認できます。チェックする標準の ARN を指定するには、 `standards-subscription-arns`パラメータを使用します。指定する ARN を確認するには、 DescribeStandardsオペレーションを使用するか、 で describe-standards コマンド AWS CLIを実行します。

リクエストが成功すると、Security Hub CSPM は`StandardsSubscription`オブジェクトの配列で応答します。標準サブスクリプションは、アカウントで標準が有効になっている場合に Security Hub CSPM がアカウントで作成する AWS リソースです。各`StandardsSubscription`オブジェクトは、アカウントに対して現在有効または無効になっている標準に関する詳細を提供します。各オブジェクト内で、 `StandardsStatus`フィールドはアカウントの標準の現在のステータスを指定します。

標準 (`StandardsStatus`) のステータスは、次のいずれかになります。

PENDING

Security Hub CSPM は現在、アカウントの標準を有効にするタスクを実行しています。これには、標準に適用されるコントロールの作成と、標準の予備セキュリティスコアの生成が含まれます。Security Hub CSPM がすべてのタスクを完了するまでに数分かかる場合があります。標準は、アカウントで既に有効になっており、Security Hub CSPM が現在標準に新しいコントロールを追加している場合にも、このステータスになることがあります。

標準にこのステータスがある場合、標準に適用される個々のコントロールの詳細を取得できない場合があります。さらに、標準の個々のコントロールを設定または無効にできない場合があります。たとえば、 UpdateStandardsControlオペレーションを使用してコントロールを無効にしようとすると、エラーが発生します。

標準に対して個々のコントロールを設定または管理できるかどうかを確認するには、`StandardsControlsUpdatable`フィールドの値を参照してください。このフィールドの値が

の場合`READY_FOR_UPDATES`、標準の個々のコントロールの管理を開始できます。それ以外の場合は、Security Hub CSPM が追加の処理タスクを完了して標準を有効にするまで待ちます。

READY

標準は現在、アカウントに対して有効になっています。Security Hub CSPM は、セキュリティチェックを実行し、標準に適用され、現在有効になっているすべてのコントロールの検出結果を生成できます。Security Hub CSPM は、標準のセキュリティスコアを計算することもできます。

標準にこのステータスがある場合は、標準に適用される個々のコントロールの詳細を取得できます。さらに、コントロールを設定、無効化、または再有効化できます。標準を無効にすることもできます。

INCOMPLETE

Security Hub CSPM は、アカウントに対して標準を完全に有効にできませんでした。Security Hub CSPM は、セキュリティチェックを実行して、標準に適用され、現在有効になっているすべてのコントロールの検出結果を生成することはできません。さらに、Security Hub CSPM は標準のセキュリティスコアを計算できません。

標準が完全に有効になっていない理由を確認するには、 `StandardsStatusReason`配列の情報を参照してください。この配列は、Security Hub CSPM が標準を有効にできない問題を指定します。内部エラーが発生した場合は、アカウントの標準を再度有効にしてみてください。その他のタイプの問題については、AWS Config 設定を確認してください。チェックしたくない個々のコントロールを無効にしたり、標準を完全に無効にしたりすることもできます。

DELETING

Security Hub CSPM は現在、アカウントの標準を無効にするリクエストを処理しています。これには、標準に適用されるコントロールの無効化、および関連するセキュリティスコアの削除が含まれます。Security Hub CSPM がリクエストの処理を完了するまでに数分かかる場合があります。

標準にこのステータスがある場合、標準を再度有効にしたり、アカウントに対して再度無効にしたりすることはできません。Security Hub CSPM は、まず現在のリクエストの処理を完了する必要があります。さらに、標準に適用される個々のコントロールの詳細を取得したり、コントロールを管理したりすることはできません。

FAILED

Security Hub CSPM は、アカウントの標準を無効にできませんでした。Security Hub CSPM が標準を無効にしようとしたときに 1 つ以上のエラーが発生しました。さらに、Security Hub CSPM は標準のセキュリティスコアを計算できません。

標準が完全に無効になっていない理由を確認するには、 `StandardsStatusReason`配列の情報を参照してください。この配列は、Security Hub CSPM が標準を無効にできない問題を指定します。

標準にこのステータスがある場合、標準に適用される個々のコントロールの詳細を取得したり、コントロールを管理したりすることはできません。ただし、アカウントの標準を再度有効にすることはできます。Security Hub CSPM が標準を無効にできない問題に対処する場合は、標準を再度無効にすることもできます。

標準のステータスが の場合`READY`、Security Hub CSPM はセキュリティチェックを実行し、標準に適用され、現在有効になっているすべてのコントロールの検出結果を生成します。他のステータスの場合、Security Hub CSPM はチェックを実行し、すべての有効なコントロールではなく一部のコントロールの検出結果を生成することがあります。コントロール結果の生成または更新には最大 24 時間かかる場合があります。詳細については、「セキュリティチェックの実行スケジュール」を参照してください。

セキュリティ標準の詳細の確認

AWS Security Hub CSPM でセキュリティ標準を有効にしたら、 コンソールを使用して標準の詳細を確認できます。 コンソールの標準の詳細ページには、以下の情報が含まれます。

- 標準の現在のセキュリティスコア。
- 標準に適用されるコントロールの表。
- 標準に適用されるコントロールの集計統計。
- 標準に適用されるコントロールのステータスの視覚的な概要。
- 有効化され、標準に適用されるコントロールのセキュリティチェックの視覚的な概要。と統合すると AWS Organizations、少なくとも 1 つの組織アカウントで有効になっているコントロールは有効と見なされます。

これらの詳細を確認するには、コンソールのナビゲーションペインでセキュリティ標準を選択します。次に、標準の セクションで、結果の表示を選択します。より詳細な分析のために、データをフィルタリングしてソートし、ドリルダウンして標準に適用される個々のコントロールの詳細を確認できます。

トピック

- 標準セキュリティスコアについて

- 標準のコントロールの確認

標準セキュリティスコアについて

AWS Security Hub CSPM コンソールで、標準の詳細ページに標準のセキュリティスコアが表示されます。スコアは、標準に適用され、有効になっており、評価データがあるコントロールの総数に対する、評価に合格したコントロールの割合です。スコアの下には、標準で有効になっているコントロールのセキュリティチェックをまとめたグラフがあります。これには、合格したセキュリティチェックと失敗したセキュリティチェックの数が含まれます。管理者アカウントの場合、標準のスコアと図は、管理者アカウントとメンバーアカウントの両方を合わせて集計されます。特定の重要度を持つコントロールの失敗したセキュリティチェックを確認するには、重要度を選択します。

標準を有効にすると、Security Hub CSPM は、通常、概要ページまたは Security Hub CSPM コンソールのセキュリティ標準ページに初めてアクセスしてから 30 分以内に、標準の予備セキュリティスコアを生成します。スコアは、それらのページにアクセスしたときに有効になっている標準に対してのみ生成されます。さらに、スコアが表示されるように AWS Config リソース記録を設定する必要があります。中国リージョンおよび では AWS GovCloud (US) Regions、Security Hub CSPM が予備スコアを生成するまでに最大 24 時間かかる場合があります。Security Hub CSPM が標準の予備スコアを生成した後、24 時間ごとにスコアを更新します。詳細については、「セキュリティスコアの計算」を参照してください。

セキュリティ標準の詳細ページのすべてのデータは、集約リージョンを設定 AWS リージョン しない限り、現在の に固有です。集約リージョンを設定すると、セキュリティスコアがリージョン間で適用され、リンクされたすべてのリージョンの結果が含まれます。さらに、コントロールのコンプライアンスステータスには、リンクされたリージョンの検出結果が反映され、セキュリティチェックの数にはリンクされたリージョンの検出結果が含まれます。

標準のコントロールの確認

AWS Security Hub CSPM コンソールを使用して、有効にした標準の詳細を確認すると、標準に適用されるセキュリティコントロールの表を確認できます。各コントロールについて、テーブルには次の情報が含まれます。

- コントロール ID とタイトル。
- コントロールのステータス。詳細については、「コンプライアンスステータスとコントロールステータスの評価」を参照してください。
- コントロールに割り当てられた重要度。

- 失敗したチェックの数とチェックの合計数。該当する場合、Failed checks フィールドは、ステータスが Unknown の検出結果の数も指定します。
- コントロールがカスタムパラメータをサポートしているかどうか。詳細については、「Security Hub CSPM のコントロールパラメータについて」を参照してください。

Security Hub CSPM は、24 時間ごとにコントロールステータスとセキュリティチェックの数を更新します。ページ上部のタイムスタンプは、Security Hub CSPM がこのデータを最後に更新した日時を示します。

管理者アカウントの場合、コントロールステータスとセキュリティチェックの数は、管理者アカウントとすべてのメンバーアカウント全体で集計されます。有効なコントロールの数には、管理者アカウントまたは少なくとも 1 つのメンバーアカウントの標準で有効になっているコントロールが含まれます。無効になっているコントロールの数には、管理者アカウントとすべてのメンバーアカウントの標準で無効になっているコントロールが含まれます。

標準に適用されるコントロールのテーブルをフィルタリングできます。テーブルの横にあるフィルターオプションを使用して、標準の有効または無効のコントロールのみを表示するように選択できます。有効なコントロールのみを表示する場合は、コントロールステータスでテーブルをさらにフィルタリングできます。その後、特定のコントロールステータスを持つコントロールに集中できます。Filter by オプションに加えて、フィルターコントロールボックスにフィルター条件を入力できます。例えば、コントロール ID またはタイトルでフィルタリングできます。

任意のアクセス方法を選択します。次に、ステップに従って、有効にした標準に適用されるコントロールを確認します。

Security Hub CSPM console

有効な標準のコントロールを確認するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで、[セキュリティ基準] を選択します。
3. 標準の セクションで、結果の表示 を選択します。

ページの下部にある表には、標準に適用されるすべてのコントロールが一覧表示されます。テーブルをフィルタリングおよびソートできます。テーブルの現在のページを CSV ファイルとしてダウンロードすることもできます。これを行うには、テーブルの上にダウンロードを選択しま

す。テーブルをフィルタリングすると、ダウンロードされたファイルには、現在のフィルター設定に一致するコントロールのみが含まれます。

Security Hub CSPM API

有効な標準のコントロールを確認するには

1. Security Hub CSPM API の ListSecurityControlDefinitionsオペレーションを使用します。を使用している場合は AWS CLI、list-security-control-definitions コマンドを実行します。

   コントロールを確認する標準の Amazon リソースネーム (ARN) を指定します。標準ARNs を取得するには、DescribeStandards オペレーションを使用するか、describe-standards コマンドを実行します。標準の ARN を指定しない場合、Security Hub CSPM はすべてのセキュリティコントロール IDsを返します。
2. Security Hub CSPM API の ListStandardsControlAssociationsオペレーションを使用するか、list-standards-control-associations コマンドを実行します。このオペレーションは、コントロールが有効になっている標準を示します。

   セキュリティコントロール ID または ARN を指定してコントロールを特定します。ページ分割パラメータはオプションです。

次の例では、Config.1 コントロールが有効になっている標準を示します。

```
$ aws securityhub list-standards-control-associations --region us-east-1 --security-control-id Config.1
```

自動的に有効になっているセキュリティ標準をオフにする

組織が中央設定を使用しない場合は、ローカル設定と呼ばれる設定タイプを使用します。ローカル設定では、 AWS Security Hub CSPM は、アカウントが組織に参加するときに、新しいメンバーアカウントのデフォルトのセキュリティ標準を自動的に有効にできます。これらのデフォルト標準に適用されるすべてのコントロールも自動的に有効になります。

現在、デフォルトのセキュリティ標準は AWS 、 Foundational Security Best Practices 標準と Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 標準です。これらの標準の詳細については、「」を参照してくださいSecurity Hub CSPM の標準リファレンス。

新しいメンバーアカウントのセキュリティ標準を手動で有効にする場合は、デフォルトの標準の自動有効化をオフにできます。これは、 と統合 AWS Organizations してローカル設定を使用する場合に

のみ実行できます。中央設定を使用する場合は、代わりにデフォルトの標準を有効にし、ポリシーをルートに関連付ける設定ポリシーを作成できます。その後、すべての組織アカウントと OUs は、別のポリシーに関連付けられているか、セルフマネージド型でない限り、この設定ポリシーを継承します。と統合しない場合 AWS Organizations、Security Hub CSPM 以降を最初に有効にするときに、デフォルトの標準を無効にすることができます。この方法の詳細は、「セキュリティ標準の無効化」を参照してください。

新しいメンバーアカウントのデフォルト標準の自動有効化を無効にするには、Security Hub CSPM コンソールまたは Security Hub CSPM API を使用できます。

Security Hub CSPM console

Security Hub CSPM コンソールを使用してデフォルト標準の自動有効化を無効にするには、次の手順に従います。

デフォルト標準の自動有効化を無効にするには

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

   管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインの [設定] で [設定] を選択します。
3. [概要] セクションで [編集] を選択します。
4. 新しいアカウント設定で、デフォルトのセキュリティ標準を有効にするチェックボックスをオフにします。
5. [確認] を選択してください。

Security Hub CSPM API

デフォルトの標準の自動有効化をプログラムで無効にするには、Security Hub CSPM 管理者アカウントから、Security Hub CSPM API の UpdateOrganizationConfigurationオペレーションを使用します。リクエストで、 `AutoEnableStandards`パラメータ`NONE`に を指定します。

を使用している場合は AWS CLI、 update-organization-configuration コマンドを実行して、デフォルトの標準の自動有効化をオフにします。`auto-enable-standards` パラメータでは、`NONE` を指定します。たとえば、次のコマンドは、新しいメンバーアカウントに対して Security Hub CSPM を自動的に有効にし、アカウントのデフォルト標準の自動有効化をオフにします。

```
$ aws securityhub update-organization-configuration --auto-enable --auto-enable-
standards NONE
```

セキュリティ標準の無効化

AWS Security Hub CSPM でセキュリティ標準を無効にすると、以下が発生します。

- 標準に適用されるすべてのコントロールは、現在有効になっている別の標準に関連付けられている場合を除き、無効になります。
- 無効化されたコントロールのセキュリティチェックは実行されなくなり、無効化されたコントロールに対して追加の検出結果は生成されません。
- 無効になっているコントロールの既存の検出結果は、約 3～5 日後に自動的にアーカイブされます。
- AWS Config 無効化されたコントロール用に Security Hub CSPM が作成した ルールは削除されます。

通常、適切な AWS Config ルールの削除は、標準を無効にしてから数分以内に行われます。ただし、時間がかかる場合があります。最初のリクエストでルールの削除に失敗した場合、Security Hub CSPM は 12 時間ごとに再試行します。ただし、Security Hub CSPM を無効にした場合、または他の標準が有効になっていない場合、Security Hub CSPM は再試行できません。つまり、ルールを削除することはできません。これが発生し、ルールを削除する必要がある場合は、 にお問い合わせください AWS サポート。

トピック

- 複数のアカウントで標準を無効にする AWS リージョン
- 1 つのアカウントで標準を無効にする AWS リージョン

複数のアカウントで標準を無効にする AWS リージョン

複数のアカウントおよび でセキュリティ標準を無効にするには AWS リージョン、中央設定を使用します。中央設定では、委任 Security Hub CSPM 管理者は、1 つ以上の標準を無効にする Security Hub CSPM 設定ポリシーを作成できます。その後、管理者は設定ポリシーを個々のアカウント、組織単位 (OUs)、またはルートに関連付けることができます。設定ポリシーは、集約リージョンとも呼ばれるホームリージョンと、すべてのリンクされたリージョンに影響します。

設定ポリシーにはカスタマイズオプションがあります。たとえば、1 つの OU で Payment Card Industry Data Security Standard (PCI DSS) を無効にすることを選択できます。別の OU では、PCI DSS と米国国立標準技術研究所 (NIST) SP 800-53 Rev. 5 標準の両方を無効にすることができます。指定した個々の標準を有効または無効にする設定ポリシーの作成については、「」を参照してください設定ポリシーの作成と関連付け。

> **Note**
>
> Security Hub CSPM 管理者は、設定ポリシーを使用して、AWS Control Tower サービスマネージド標準以外の標準を無効にすることができます。この標準を無効にするには、管理者が AWS Control Tower を直接使用する必要があります。また、 を使用して AWS Control Tower 、一元管理されたアカウントのこの標準の個々のコントロールを無効または有効にする必要があります。

一部のアカウントで自分のアカウントの標準を設定または無効にする場合、Security Hub CSPM 管理者はそれらのアカウントをセルフマネージドアカウントとして指定できます。セルフマネージドアカウントは、リージョンごとに個別に標準を無効にする必要があります。

1 つのアカウントで標準を無効にする AWS リージョン

中央設定を使用しない場合、またはセルフマネージドアカウントがある場合は、設定ポリシーを使用して、複数のアカウントまたは のセキュリティ標準を一元的に無効にすることはできません AWS リージョン。ただし、1 つのアカウントとリージョンで標準を無効にすることができます。これを行うには、Security Hub CSPM コンソールまたは Security Hub CSPM API を使用します。

Security Hub CSPM console

Security Hub CSPM コンソールを使用して、1 つのアカウントとリージョンで標準を無効にするには、次の手順に従います。

1 つのアカウントおよびリージョンで標準を無効にするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ページの右上隅にある AWS リージョン セレクターを使用して、標準を無効にするリージョンを選択します。
3. ナビゲーションペインで、[セキュリティ標準] を選択します。
4. 無効にする標準のセクションで、標準を無効にするを選択します。

追加のリージョンで標準を無効にするには、追加のリージョンごとに前述のステップを繰り返します。

Security Hub CSPM API

単一のアカウントとリージョンで標準をプログラムで無効にするには、BatchDisableStandardsオペレーションを使用します。または、 AWS Command Line Interface（AWS CLI) を使用している場合は、 batch-disable-standards コマンドを実行します。

リクエストで、 `StandardsSubscriptionArns`パラメータを使用して、無効にする標準の Amazon リソースネーム (ARN) を指定します。を使用している場合は AWS CLI、 `standards-subscription-arns`パラメータを使用して ARN を指定します。また、リクエストが適用されるリージョンも指定します。たとえば、次のコマンドは、アカウント (*123456789012*) AWS の Foundational Security Best Practices (FSBP) 標準を無効にします。

```
$ aws securityhub batch-disable-standards \
--standards-subscription-arns "arn:aws:securityhub:us-
east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0" \
--region us-east-1
```

ここで*#arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0* は米国東部 (バージニア北部) リージョンのアカウントの FSBP 標準の ARN であり、*us-east-1* は無効にするリージョンです。

標準の ARN を取得するには、 GetEnabledStandardsオペレーションを使用できます。このオペレーションは、アカウントで現在有効になっている標準に関する情報を取得します。を使用している場合は AWS CLI、get-enabled-standards コマンドを実行してこの情報を取得できます。

標準を無効にすると、Security Hub CSPM は、アカウントと指定されたリージョンで標準を無効にするタスクの実行を開始します。これには、標準に適用されるすべてのコントロールの無効化が含まれます。これらのタスクのステータスをモニタリングするには、アカウントとリージョンの標準のステータスを確認できます。

Security Hub CSPM のセキュリティコントロールについて

AWS Security Hub CSPM では、セキュリティコントロールはコントロールとも呼ばれ、組織が情報の機密性、完全性、可用性を保護するのに役立つセキュリティ標準内の保護手段です。Security Hub CSPM では、コントロールは特定の AWS リソースに関連しています。

1 つ以上の標準でコントロールを有効にすると、Security Hub CSPM はセキュリティチェックの実行を開始します。セキュリティチェックの結果、Security Hub CSPM の検出結果が得られます。コントロールを無効にすると、Security Hub CSPM はそのコントロールに対するセキュリティチェックの実行を停止し、検出結果は生成されなくなります。

1 つのアカウントと のコントロールを個別に有効または無効にできます AWS リージョン。マルチアカウント環境で時間を節約し、設定ドリフトを減らすには、中央設定を使用してコントロールを有効または無効にすることをお勧めします。中央設定では、委任 Security Hub CSPM 管理者は、複数のアカウントとリージョンでコントロールを設定する方法を指定するポリシーを作成できます。コントロールの有効化と無効化の詳細については、「Security Hub CSPM でのコントロールの有効化」を参照してください。

統合コントロールビュー

Security Hub CSPM コンソールのコントロールページには、現在の で利用可能なすべてのコントロールが表示されます AWS リージョン（セキュリティ標準ページにアクセスして有効な標準を選択すると、標準コンテキストでコントロールを表示できます）。Security Hub CSPM は、標準全体で一貫したセキュリティコントロール ID、タイトル、説明をコントロールに割り当てます。コントロール IDsには、関連する番号 AWS のサービス と一意の番号 (CodeBuild.3).

以下の情報は、Security Hub CSPM コンソールの「コントロール」ページで確認できます。 https://console.aws.amazon.com/securityhub/

- データを含む有効なコントロールの総数に対する合格したコントロールの割合に基づく、総合的なセキュリティスコア
- サポートされているすべての Security Hub CSPM コントロールのコントロールステータスの内訳
- セキュリティチェックの合格と不合格の合計数。
- 重要度の異なるコントロールの失敗したセキュリティチェックの数と、それらの失敗したチェックの詳細を表示するリンク。
- Security Hub CSPM コントロールのリスト。コントロールの特定のサブセットを表示するフィルターがあります。

[コントロール] ページでコントロールを選択して詳細を確認し、コントロールが生成した検出結果に対してアクションを実行することができます。このページでは、現在の AWS アカウント および で セキュリティコントロールを有効または無効にすることもできます AWS リージョン。[コントロール] ページからの有効化および無効化アクションは、すべての標準に適用されます。詳細については、「Security Hub CSPM でのコントロールの有効化」を参照してください。

管理者アカウントの場合、[コントロール] ページには、メンバーアカウント全体のコントロールのステータスが反映されます。コントロールチェックが少なくとも 1 つのメンバーアカウントで失敗した場合、コントロールステータスは [失敗] です。集約リージョンを設定している場合、[コントロール] ページには、リンクされているすべてのリージョンのコントロールステータスが反映されます。少なくとも 1 つのリンクされたリージョンでコントロールチェックが失敗した場合、コントロールステータスは [失敗] です。

統合コントロールビューでは、ワークフローに影響を与える可能性のある AWS Security Finding Format (ASFF) のコントロール検出結果フィールドが変更されます。詳細については、「統合コントロールビュー — ASFF の変更」を参照してください。

コントロールのセキュリティスコアの概要

[コントロール] ページには、0 ~ 100% のセキュリティスコアの概要が表示されます。セキュリティスコアの概要は、標準全体のデータを含む有効なコントロールの総数に対する合格したコントロールの割合に基づき計算されます。

> **Note**
>
> コントロールの全体的なセキュリティスコアを表示するには、Security Hub CSPM へのアクセスに使用する **`BatchGetControlEvaluations`** IAM ロールに を呼び出すアクセス許可を追加する必要があります。この権限は、特定の標準のセキュリティスコアを表示する場合には必要ありません。

Security Hub CSPM を有効にすると、Security Hub CSPM は、Security Hub CSPM コンソールの 概要ページまたはセキュリティ標準ページに初めてアクセスしてから 30 分以内に最初のセキュリティスコアを計算します。中国リージョンおよび AWS GovCloud (US) Regionsでは、最初のセキュリティスコアが作成されるまで、最大 24 時間かかる場合があります。

セキュリティスコア全体に加えて、Security Hub CSPM は、概要ページまたはセキュリティ標準ページに初めてアクセスしてから 30 分以内に、有効な標準ごとに標準セキュリティスコアを計算します。現在有効になっている標準のリストを表示するには、`GetEnabledStandards` API オペレーションを使用します。

AWS Config スコアを表示するには、リソース記録で を有効にする必要があります。Security Hub CSPM がセキュリティスコアを計算する方法については、「」を参照してくださいセキュリティスコアの計算。

初めてスコアを生成した後、Security Hub CSPM はセキュリティスコアを 24 時間ごとに更新します。Security Hub CSPM には、セキュリティスコアが最後に更新された日時を示すタイムスタンプが表示されます。

集約リージョンを設定している場合、全体のセキュリティスコアには、リンクされたリージョン全体の検出結果が反映されます。

Security Hub CSPM のコントロールリファレンス

このコントロールリファレンスは、利用可能な AWS Security Hub CSPM コントロールの表と、各コントロールに関する詳細情報へのリンクを提供します。表では、コントロールはコントロール ID でアルファベット順にリストされています。Security Hub CSPM によってアクティブに使用されているコントロールのみがここに含まれています。廃止されたコントロールはテーブルから除外されます。

このテーブルには、各コントロールの以下の情報が表示されます。

- セキュリティコントロール ID – この ID は標準に適用され、コントロールに関連する AWS のサービス とリソースを示します。Security Hub CSPM コンソールには、統合コントロールの検出結果がアカウントで有効か無効かにかかわらず、セキュリティコントロール IDs が表示されます。ただし、Security Hub CSPM の検出結果は、アカウントで統合コントロールIDs を参照します。アカウントで [統合されたコントロールの検出結果] が無効になっている場合、一部のコントロール ID はコントロールの検出結果に含まれる標準によって異なります。標準固有のコントロール ID をセキュリティコントロール ID にマッピングする方法については、「統合がコントロール ID とタイトルに与える影響」を参照してください。

  セキュリティコントロールの自動化を設定するときは、タイトルや説明ではなく、コントロール ID に基づいてフィルタリングすることをお勧めします。Security Hub CSPM はコントロールのタイトルや説明を更新することがありますが、コントロール IDsは変わりません。

  コントロール ID は数字が飛ばされることがあります。これらは将来のコントロール用のプレースホルダーです。

- セキュリティコントロールタイトル — このタイトルはあらゆる標準に適用されます。Security Hub CSPM コンソールには、統合コントロールの検出結果がアカウントで有効か無効かに関係なく、セキュリティコントロールのタイトルが表示されます。ただし、Security Hub CSPM の検出結果は、アカウントで統合コントロールの検出結果がオンになっている場合にのみ、セキュリティコントロールのタイトルを参照します。アカウントで [統合されたコントロールの検出結果] が無効になっている場合、一部のコントロールタイトルはコントロールの検出結果に含まれる標準に

よって異なります。標準固有のコントロール ID をセキュリティコントロール ID にマッピングする方法については、「統合がコントロール ID とタイトルに与える影響」を参照してください。

- 適用される標準 — コントロールが適用される標準を示します。コントロールを選択して、サードパーティーのコンプライアンスフレームワークから特定の要件を確認します。
- 重要度 — コントロールの重要度は、セキュリティの観点からその重要性を示します。Security Hub CSPM がコントロールの重要度を決定する方法については、「」を参照してくださいコントロールの検出結果の重要度レベル。
- カスタムパラメータをサポート — コントロールが 1 つ以上のパラメータのカスタム値をサポートしているかどうかを示します。コントロールを選択して、パラメータの詳細を確認します。詳細については、「Security Hub CSPM のコントロールパラメータについて」を参照してください。
- スケジュールタイプ — コントロールがいつ評価されるかを示します。詳細については、「セキュリティチェックの実行スケジュール」を参照してください。

コントロールを選択して、追加の詳細を確認します。コントロールは、セキュリティコントロール ID によってアルファベット順に一覧表示されます。

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Account.1	のセキュリティ連絡先情報は、 に提供する必要があります。AWS アカウント	CIS AWS Foundations Benchmark v3.0.0、 AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Account.2	AWS アカウント は AWS Organizations 組織の一部である必要があります	NIST SP 800-53 Rev. 5	高	いいえ	定期的
ACM.1	インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1	中	はい	変更によるトリガーと定期的なトリガー
ACM.2	ACM が管理する RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります	AWS Foundational Security Best Practices v1.0.0、PCI DSS v4.0.1	高	いいえ	変更によってトリガーされる
ACM.3	ACM 証明書にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
Amplify.1	Amplify アプリにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Amplify.2	Amplify ブランチにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
APIGateway.1	API Gateway REST および WebSocket API 実行ログ記録を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	はい	変更によってトリガーされる
APIGateway.2	API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	中	いいえ	変更によってトリガーされる
APIGateway.3	API Gateway REST API ステージでは、AWS X-Ray トレースを有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
APIGateway.4	API Gateway は、WAF ウェブ ACL に関連付けられている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
APIGateway.5	API Gateway REST API のキャッシュデータは、保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
APIGateway.8	API Gateway ルートには認可タイプを指定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✓ はい	定期的
APIGateway.9	API Gateway V2 ステージにアクセスログ記録を設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
AppConfig.1	AWS AppConfig アプリケーションにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
AppConfig.2	AWS AppConfig 設定プロファイルにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
AppConfig.3	AWS AppConfig 環境にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
AppConfig.4	AWS AppConfig 拡張機能の関連付けにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
AppFlow.1	Amazon AppFlow フローにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
AppRunner.1	App Runner サービスにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
AppRunner.2	App Runner VPC コネクタにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
AppSync.1	AWS AppSync API キャッシュは保管時に暗号化する必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	変更によってトリガーされる
AppSync.2	AWS AppSync ではフィールドレベルのログ記録が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、PCI DSS v4.0.1	中	はい	変更によってトリガーされる
AppSync.4	AWS AppSync GraphQL APIsタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
AppSync.5	AWS AppSync GraphQL APIsは API キーで認証しないでください	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	高	いいえ	変更によってトリガーされる
AppSync.6	AWS AppSync API キャッシュは転送中に暗号化する必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Athena.2	Athena データカタログにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
Athena.3	Athena ワークグループにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
Athena.4	Athena ワークグループではログ記録が有効になっている必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	変更によってトリガーされる
AutoScaling.1	ロードバランサーに関連付けられた Auto Scaling グループは、ELB のヘルスチェックを使用する必要があります	AWS 基本的なセキュリティのベストプラクティス、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	低	いいえ	変更によってトリガーされる
AutoScaling.2	Amazon EC2 Auto Scaling グループは、複数のアベイラビリティーゾーンをカバーする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
AutoScaling.3	Auto Scaling グループの起動設定は、EC2 インスタンスを、インスタンスメタデータサービスバージョン 2 (IMDSv2) を必要とするように設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	高	✗ いいえ	変更によってトリガーされる
Autoscaling.5	Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	高	✗ いいえ	変更によってトリガーされる
AutoScaling.6	Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
AutoScaling.9	EC2 Auto Scaling グループは EC2 起動テンプレートを使用する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
AutoScaling.10	EC2 Auto Scaling グループにタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
Backup.1	AWS Backup リカバリポイントは保管時に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
Backup.2	AWS Backup 復旧ポイントにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
Backup.3	AWS Backup ボールトにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
Backup.4	AWS Backup レポートプランにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Backup.5	AWS Backup バックアッププランにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
バッチ.1	バッチジョブキューにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
バッチ.2	バッチスケジューリングポリシーにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
バッチ.3	バッチコンピューティング環境にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
バッチ.4	マネージドバッチコンピューティング環境のコンピューティングリソースプロパティにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
CloudFormation.2	CloudFormation スタックにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudFront.1	CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	高	✗ いいえ	変更によってトリガーされる
CloudFront.3	CloudFront ディストリビューションでは、転送中に暗号化が必要となります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	✗ いいえ	変更によってトリガーされる
CloudFront.4	CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	低	✗ いいえ	変更によってトリガーされる
CloudFront.5	CloudFront ディストリビューションでは、ログ記録を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	✗ いいえ	変更によってトリガーされる
CloudFront.6	CloudFront ディストリビューションでは、WAF を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudFront.7	CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	中	いいえ	変更によってトリガーされる
CloudFront.8	CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	低	いいえ	変更によってトリガーされる
CloudFront.9	CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	いいえ	変更によってトリガーされる
CloudFront.10	CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudFront.12	CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります。	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	高	いいえ	定期的
CloudFront.13	CloudFront ディストリビューションはオリジンアクセスコントロールを使用する必要があります	AWS 基本的なセキュリティのベストプラクティス v1.0.0	中	いいえ	変更によってトリガーされる
CloudFront.14	CloudFront ディストリビューションにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
CloudFront.15	CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります	AWS 基本的なセキュリティのベストプラクティス v1.0.0	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudTrail.1	CloudTrail を有効にして、少なくとも 1 つのマルチリージョンの追跡で、読み取りと書き込みの管理イベントを含めた設定をする必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	高	✗ いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudTrail.2	CloudTrail は保管時の暗号化を有効にする必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0 AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v3.2.1、PCI DSS v4.0.1、Service-Managed Standard: AWS Control Tower	中	いいえ	定期的
CloudTrail.3	少なくとも 1 つの CloudTrail 証跡を有効にする必要があります	NIST SP 800-171 Rev. 2、PCI DSS v4.0.1、PCI DSS v3.2.1	高	いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudTrail.4	CloudTrail ログファイルの検証を有効にする必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1、PCI DSS v3.2.1、Service-Managed Standard: AWS Control Tower	低	いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudTrail.5	CloudTrail 証跡は、Amazon CloudWatch Logs と統合する必要があります	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0、AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	低	✗ いいえ	定期的
CloudTrail.6	CloudTrail ログの保存に使用されるS3 バケットが一般公開されていないことを確認します	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0、PCI DSS v4.0.1	重大	✗ いいえ	変更によるトリガーと定期的なトリガー

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudTrail.7	S3 バケットアクセスログ記録が CloudTrail S3 バケットで有効になっていることを確認します	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v3.0.0、PCI DSS v4.0.1	低	✗ いいえ	定期的
CloudTrail.9	CloudTrail 証跡にはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
CloudTrail.10	CloudTrail Lake イベントデータストアはカスタマーマネージドで暗号化する必要があります AWS KMS keys	NIST SP 800-53 Rev. 5	中	✓ はい	定期的
CloudWatch.1	「ルート」ユーザーの使用に対するログメトリックフィルターとアラームが存在する必要があります	CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2、PCI DSS v3.2.1	低	✗ いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudWatch.2	不正な API コールに対するログメトリクスフィルターとアラームが存在することを確認する	CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2	低	いいえ	定期的
CloudWatch.3	MFA を使用しないマネジメントコンソールサインインに対してログメトリクスフィルターとアラームが存在することを確認します	CIS AWS Foundations Benchmark v1.2.0	低	いいえ	定期的
CloudWatch.4	MFA なしの IAM ポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認します。	CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2	低	いいえ	定期的
CloudWatch.5	CloudTrail の設定の変更に対するログメトリクスフィルターとアラームが存在することを確認します。	CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2	低	いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudWatch.6	AWS Management Console 認証失敗のログメトリクスフィルターとアラームが存在することを確認する	CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2	低	いいえ	定期的
CloudWatch.7	カスタマー作成の CMK の無効化またはスケジュールされた削除に対してログメトリクスフィルターとアラームが存在することを確認します	CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2	低	いいえ	定期的
CloudWatch.8	S3 バケットの変更に対してログメトリクスフィルターとアラームが存在することを確認します	CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2	低	いいえ	定期的
CloudWatch.9	AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する	CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2	低	いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudWatch.10	セキュリティグループの変更に対するメトリクスフィルターとアラームが存在することを確認します	CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2	低	✗ いいえ	定期的
CloudWatch.11	ネットワークアクセスコントロールリスト (NACL) への変更に対するログメトリクスとアラームが存在することを確認します	CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2	低	✗ いいえ	定期的
CloudWatch.12	ネットワークゲートウェイへの変更に対するログメトリクスとアラームが存在することを確認します	CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2	低	✗ いいえ	定期的
CloudWatch.13	ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認します	CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2	低	✗ いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CloudWatch.14	VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認します	CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2	低	✗ いいえ	定期的
CloudWatch.15	CloudWatch アラームには、指定されたアクションが設定されている必要があります	NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	高い	✓ はい	変更によってトリガーされる
CloudWatch.16	CloudWatch ロググループは指定された期間保持する必要があります	NIST SP 800-53 Rev. 5	中	✓ はい	定期的
CloudWatch.17	CloudWatch アラームアクションを有効にする必要があります	NIST SP 800-53 Rev. 5	高	✗ いいえ	変更によってトリガーされる
CodeArtifact.1	CodeArtifact リポジトリにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CodeBuild.1	CodeBuild Bitbucket のソースリポジトリの URL には機密認証情報を含めないでください	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	重大	いいえ	変更によってトリガーされる
CodeBuild.2	CodeBuild プロジェクト環境変数に、クリアテキストの認証情報を含めるべきでない	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	重大	いいえ	変更によってトリガーされる
CodeBuild.3	CodeBuild S3 ログは暗号化する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower、	低	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
CodeBuild.4	CodeBuild プロジェクト環境にはログ記録の設定が必要です	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
CodeBuild.7	CodeBuild レポートグループのエクスポートは保管時に暗号化する必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	変更によってトリガーされる
CodeGuruProfiler.1	CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
CodeGuruReviewer.1	CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
Cognito.1	Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります	AWS 基本的なセキュリティのベストプラクティス	中	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Cognito.2	Cognito ID プールは認証されていない ID を許可しないでください	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	変更によってトリガーされる
Config.1	AWS Config を有効にし、サービスにリンクされたロールをリソース記録に使用する必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1	重大	はい	定期的
Connect.1	Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
Connect.2	Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
DataFirehose.1	Firehose 配信ストリームは保管時に暗号化する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	いいえ	定期的
DataSync.1	DataSync タスクではログ記録が有効になっている必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	変更によってトリガーされる
DataSync.2	DataSync タスクにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
Detective.1	検出動作グラフにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
DMS.1	Database Migration Service のレプリケーションインスタンスは、パブリックではない必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	重大	いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
DMS.2	DMS 証明書にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
DMS.3	DMS イベントサブスクリプションにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
DMS.4	DMS レプリケーションインスタンスにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
DMS.5	DMS レプリケーションサブネットグループにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
DMS.6	DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
DMS.7	ターゲットデータベースの DMS レプリケーションタスクでは、ログ記録が有効になっている必要があります。	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	✗ いいえ	変更によってトリガーされる
DMS.8	ソースデータベースの DMS レプリケーションタスクでは、ログ記録が有効になっている必要があります。	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	✗ いいえ	変更によってトリガーされる
DMS.9	DMS エンドポイントは SSL を使用する必要があります。	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	✗ いいえ	変更によってトリガーされる
DMS.10	Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	✗ いいえ	変更によってトリガーされる
DMS.11	MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
DMS.12	Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	✗ いいえ	変更によってトリガーされる
DocumentDB.1	Amazon DocumentDB クラスターは、保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	中	✗ いいえ	変更によってトリガーされる
DocumentDB.2	Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✓ はい	変更によってトリガーされる
DocumentDB.3	Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	重大	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
DocumentDB.4	Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	いいえ	変更によってトリガーされる
DocumentDB.5	Amazon DocumentDB では、削除保護が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
DocumentDB.6	Amazon DocumentDB クラスターは転送中に暗号化する必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	定期的
DynamoDB.1	DynamoDB テーブルは、需要に応じて容量をオートスケーリングする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	はい	定期的
DynamoDB.2	DynamoDB テーブルでは、ポイントインタイムリカバリが有効になっている必要があります。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
DynamoDB 3	DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	いいえ	定期的
DynamoDB 4	DynamoDB テーブルはバックアッププランに含まれている必要があります	NIST SP 800-53 Rev. 5	中	はい	定期的
DynamoDB 5	DynamoDB テーブルにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
DynamoDB 6	DynamoDB テーブルで、削除保護が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
DynamoDB 7	DynamoDB Accelerator クラスターは、転送中に暗号化する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.1	EBS スナップショットをパブリックに復元可能であってはなりません	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	✗ いいえ	定期的
EC2.2	VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにする必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices v1.0.0、Service-Managed Standard: AWS Control Tower、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	高	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.3	アタッチされた EBS ボリュームは、保管時に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
EC2.4	停止した EC2 インスタンスは、指定した期間後に削除する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	はい	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.6	すべての VPC で VPC フローログ記録を有効にする必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices v1.0.0、Service-Managed Standard: AWS Control Tower、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	中	✗ いいえ	定期的
EC2.7	EBS のデフォルト暗号化を有効にする必要があります	CIS AWS Foundations Benchmark v3.0.0、 AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	中	✗ いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.8	EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用する必要があります	CIS AWS Foundations Benchmark v3.0.0、 AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	高	✗ いいえ	変更によってトリガーされる
EC2.9	EC2 インスタンスは、パブリック IPv4 アドレスを未設定にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	高	✗ いいえ	変更によってトリガーされる
EC2.10	Amazon EC2 サービス用に作成された VPC エンドポイントを使用するように Amazon EC2 を設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	中	✗ いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.12	未使用の EC2 EIP を削除する必要があります	PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	低	いいえ	変更によってトリガーされる
EC2.13	セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります	CIS AWS Foundations Benchmark v1.2.0、PCI DSS v3.2.1、PCI DSS v4.0.1、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	高	いいえ	変更によるトリガーと定期的なトリガー
EC2.14	セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります	CIS AWS Foundations Benchmark v1.2.0、PCI DSS v4.0.1	高	いいえ	変更によるトリガーと定期的なトリガー
EC2.15	EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないでください	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower、	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.16	未使用のネットワークアクセスコントロールリストを削除する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower、	低	いいえ	変更によってトリガーされる
EC2.17	EC2 インスタンスは複数の ENI を使用しないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	いいえ	変更によってトリガーされる
EC2.18	セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可する必要があります。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	高い	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.19	セキュリティグループは、リスクの高いポートへの無制限アクセスを許可しないでください	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	重大	✗ いいえ	変更によるトリガーと定期的なトリガー
EC2.20	AWS Site-to-Site VPN トンネルが稼働している必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.21	ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、AWS Foundational Security Best Practices、Service-Managed Standard: AWS Control Tower、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1	中	✗ いいえ	変更によってトリガーされる
EC2.22	未使用の EC2 セキュリティグループを削除する必要があります	サービスマネージドスタンダード： AWS Control Tower	中	✗ いいえ	定期的
EC2.23	EC2 Transit Gateway は VPC アタッチメントリクエストを自動的に受け付けないようにする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	高	✗ いいえ	変更によってトリガーされる
EC2.24	EC2 準仮想化インスタンスタイプは使用しないでください	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.25	EC2 起動テンプレートはパブリック IP をネットワークインターフェイスに割り当ててはなりません	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	高	✗ いいえ	変更によってトリガーされる
EC2.28	EBS ボリュームはバックアッププランに入っている必要があります	NIST SP 800-53 Rev. 5	低	✓ はい	定期的
EC2.33	EC2 Transit Gateway アタッチメントにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
EC2.34	EC2 Transit Gateway ルートテーブルにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
EC2.35	EC2 ネットワークインターフェイスにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.36	EC2 カスタマーゲートウェイにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
EC2.37	EC2 Elastic IP アドレスにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
EC2.38	EC2 インスタンスにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
EC2.39	EC2 インターネットゲートウェイにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
EC2.40	EC2 NAT ゲートウェイにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
EC2.41	EC2 ネットワーク ACL にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.42	EC2 ルートテーブルにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
EC2.43	EC2 セキュリティグループにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
EC2.44	EC2 サブネットにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
EC2.45	EC2 ボリュームにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
EC2.46	Amazon VPC にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
EC2.47	Amazon VPC エンドポイントサービスはタグ付けする必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.48	Amazon VPC フローログにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
EC2.49	Amazon VPC ピアリング接続にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
EC2.50	EC2 VPN ゲートウェイにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
EC2.51	EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1	低	いいえ	変更によってトリガーされる
EC2.52	EC2 Transit Gateway にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.53	EC2 セキュリティグループは、0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可しないようにする必要があります。	CIS AWS Foundations Benchmark v3.0.0、PCI DSS v4.0.1	高	いいえ	定期的
EC2.54	EC2 セキュリティグループは、::/0 からリモートサーバー管理ポートへの入力を許可していないようにする必要があります。	CIS AWS Foundations Benchmark v3.0.0、PCI DSS v4.0.1	高	いいえ	定期的
EC2.55	VPCsは ECR API のインターフェイスエンドポイントで設定する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	はい	定期的
EC2.56	VPCsは Docker Registry のインターフェイスエンドポイントで設定する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	はい	定期的
EC2.57	VPCsは Systems Manager のインターフェイスエンドポイントで設定する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	はい	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.58	VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	はい	定期的
EC2.60	VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	はい	定期的
EC2.170	EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用する必要があります	AWS Foundational Security Best Practices、PCI DSS v4.0.1	低	いいえ	変更によってトリガーされる
EC2.171	EC2 VPN 接続ではログ記録が有効になっている必要があります	AWS Foundational Security Best Practices、PCI DSS v4.0.1	中	いいえ	変更によってトリガーされる
EC2.172	EC2 VPC ブロックパブリックアクセス設定はインターネットゲートウェイトラフィックをブロックする必要があります	AWS 基本的なセキュリティのベストプラクティス	中	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.173	起動パラメータを含む EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります	AWS 基本的なセキュリティのベストプラクティス	中	✗ いいえ	変更によってトリガーされる
EC2.174	EC2 DHCP オプションセットにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
EC2.175	EC2 起動テンプレートにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
EC2.176	EC2 プレフィックスリストにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
EC2.177	EC2 トラフィックミラーセッションにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
EC2.178	EC2 トラフィックミラーフィルターにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EC2.179	EC2 トラフィックミラーターゲットにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
EC2.180	EC2 ネットワークインターフェイスでは、送信元/送信先チェックを有効にする必要があります	AWS 基本的なセキュリティのベストプラクティス v1.0.0	中	いいえ	変更によってトリガーされる
ECR.1	ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	高	いいえ	定期的
ECR.2	ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ECR.3	ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
ECR.4	ECR パブリックリポジトリにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
ECR.5	ECR リポジトリはカスタマーマネージドで暗号化する必要があります AWS KMS keys	NIST SP 800-53 Rev. 5	中	✓ はい	変更によってトリガーされる
ECS.1	Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	高	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ECS.2	Amazon ECS サービスには、パブリック IP アドレスを自動で割り当てないでください	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	高	いいえ	変更によってトリガーされる
ECS.3	ECS タスク定義では、ホストのプロセス名前空間を共有しないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	高	いいえ	変更によってトリガーされる
ECS.4	ECS コンテナは、非特権として実行する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	高	いいえ	変更によってトリガーされる
ECS.5	ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	高	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ECS.8	シークレットは、コンテナ環境の変数として渡さないでください	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	高	✗ いいえ	変更によってトリガーされる
ECS.9	ECS タスク定義には ログ設定が必要です。	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	高	✗ いいえ	変更によってトリガーされる
ECS.10	ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✗ いいえ	変更によってトリガーされる
ECS.12	ECS クラスターはコンテナインサイトを使用する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ECS.13	ECS サービスにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
ECS.14	ECS クラスターにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
ECS.15	ECS タスク定義にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
ECS.16	ECS タスクは、パブリック IP アドレスを自動的に割り当てないでください	AWS Foundational Security Best Practices、PCI DSS v4.0.1	高	いいえ	変更によってトリガーされる
ECS.17	ECS タスク定義ではホストネットワークモードを使用しないでください	NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EFS.1	Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります。 AWS KMS	CIS AWS Foundations Benchmark v3.0.0、 AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	定期的
EFS.2	Amazon EFS ボリュームは、バックアッププランに含める必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	定期的
EFS.3	EFS アクセスポイントは、ルートディレクトリを適用する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EFS.4	EFS アクセスポイントは、ユーザー ID を適用する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	いいえ	変更によってトリガーされる
EFS.5	EFS アクセスポイントにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
EFS.6	EFS マウントターゲットは、起動時にパブリック IP アドレスを割り当てるサブネットに関連付けるべきではありません	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	定期的
EFS.7	EFS ファイルシステムでは、自動バックアップが有効になっている必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	変更によってトリガーされる
EFS.8	EFS ファイルシステムは保管時に暗号化する必要があります	AWS 基本的なセキュリティのベストプラクティス	中	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EKS.1	EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	高	✗ いいえ	定期的
EKS.2	EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	高	✗ いいえ	変更によってトリガーされる
EKS.3	EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	✗ いいえ	定期的
EKS.6	EKS クラスターにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
EKS.7	EKS ID プロバイダー設定にはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EKS.8	EKS クラスターでは、監査ログ記録が有効になっている必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	いいえ	変更によってトリガーされる
ElastiCache.1	ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	高い	はい	定期的
ElastiCache.2	ElastiCache クラスターでは、マイナーバージョンの自動アップグレードを有効にする必要があります。	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	高	いいえ	定期的
ElastiCache.3	ElastiCache レプリケーショングループでは自動フェイルオーバーを有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	いいえ	定期的
ElastiCache.4	ElastiCache レプリケーショングループは保管時に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ElastiCache.5	ElastiCache レプリケーショングループは、転送中に暗号化されている必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	✗ いいえ	定期的
ElastiCache.6	以前の Redis バージョンの ElastiCache (Redis OSS) レプリケーショングループでは、Redis OSS AUTH を有効にする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	✗ いいえ	定期的
ElastiCache.7	ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	高	✗ いいえ	定期的
ElasticBeanstalk.1	Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ElasticBeanstalk.2	Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	高い	はい	変更によってトリガーされる
ElasticBeanstalk.3	Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります	AWS Foundational Security Best Practices、PCI DSS v4.0.1	高い	はい	変更によってトリガーされる
ELB.1	Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	中	いいえ	定期的
ELB.2	SSL/HTTPS リスナーを使用する Classic Load Balancer は、AWS Certificate Manager によって提供される証明書を使用する必要があります。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ELB.3	Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✗ いいえ	変更によってトリガーされる
ELB.4	Application Load Balancer は、http ヘッダーを削除するように設定する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✗ いいえ	変更によってトリガーされる
ELB.5	アプリケーションおよび Classic Load Balancer のログ記録を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ELB.6	アプリケーション、ゲートウェイ、Network Load Balancer で削除保護を有効にする必要があります	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
ELB.7	Classic Load Balancer は、Connection Draining を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
ELB.8	SSL リスナーを使用する Classic Load Balancer は、強力な設定を持つ事前定義されたセキュリティポリシーを使用する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ELB.9	Classic Load Balancer では、クロスゾーンロードバランシングが有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
ELB.10	Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	はい	変更によってトリガーされる
ELB.12	Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	いいえ	変更によってトリガーされる
ELB.13	Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ELB.14	Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✗ いいえ	変更によってトリガーされる
ELB.16	Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります	NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
ELB.17	リスナーを使用する Application Load Balancer と Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります。	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ELB.18	Application Load Balancer リスナーと Network Load Balancer リスナーは、転送中のデータを暗号化するために安全なプロトコルを使用する必要があります	AWS 基本的なセキュリティのベストプラクティス v1.0.0	中	✗ いいえ	変更によってトリガーされる
EMR.1	Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	高	✗ いいえ	定期的
EMR.2	Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	重大	✗ いいえ	定期的
EMR.3	Amazon EMR セキュリティ設定は保管時に暗号化する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
EMR.4	Amazon EMR セキュリティ設定は転送中に暗号化する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
ES.1	Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	中	いいえ	定期的
ES.2	Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります	AWS Foundational Security Best Practices、PCI DSS v3.2.1、PCI DSS v4.0.1、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード： AWS Control Tower	重大	いいえ	定期的
ES.3	Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower、	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ES.4	CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
ES.5	Elasticsearch ドメインで監査ログ記録が有効になっている必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード： AWS Control Tower	中	いいえ	変更によってトリガーされる
ES.6	Elasticsearch ドメインには少なくとも 3 つのデータノードが必要です	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
ES.7	Elasticsearch ドメインは、少なくとも 3 つの専用マスターノードを設定する必要があります。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ES.8	Elasticsearch ドメインへの接続は TLS セキュリティポリシーを使用して暗号化する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✗ いいえ	変更によってトリガーされる
ES.9	Elasticsearch ドメインには タグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
EventBridge.2	EventBridge イベントバスにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
EventBridge.3	Amazon EventBridge カスタムイベントバスにリソースポリシーがアタッチされている必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	低	✗ いいえ	変更によってトリガーされる
EventBridge.4	EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります	NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
FraudDetector.1	Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
FraudDetector.2	Amazon Fraud Detector ラベルにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
FraudDetector.3	Amazon Fraud Detector の結果にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
FraudDetector.4	Amazon Fraud Detector 変数にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
FSx.1	FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	低	いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
FSx.2	FSx for Lustre ファイルシステムでは、タグをバックアップにコピーするように設定する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	低	✗ いいえ	定期的
FSx.3	FSx for OpenZFS ファイルシステムは、マルチ AZ 配置用に設定する必要があります	AWS 基本的なセキュリティのベストプラクティス	中	✗ いいえ	定期的
FSx.4	FSx for NetApp ONTAP ファイルシステムは、マルチ AZ 配置用に設定する必要があります	AWS 基本的なセキュリティのベストプラクティス	中	✓ はい	定期的
FSx.5	FSx for Windows File Server ファイルシステムは、マルチ AZ 配置用に設定する必要があります	AWS 基本的なセキュリティのベストプラクティス	中	✗ いいえ	定期的
Glue.1	AWS Glue ジョブにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Glue.3	AWS Glue 機械学習変換は保管時に暗号化する必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	変更によってトリガーされる
Glue.4	AWS Glue Spark ジョブは、サポートされているバージョンので実行する必要があります。 AWS Glue	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
GlobalAccelerator.1	Global Accelerator アクセラレーターにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
GuardDuty.1	GuardDuty を有効にする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v3.2.1、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	高	いいえ	定期的
GuardDuty.2	GuardDuty フィルターにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
GuardDuty.3	GuardDuty IPSet タグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
GuardDuty.4	GuardDuty ディテクターにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
GuardDuty.5	GuardDuty EKS 監査ログモニタリングを有効にする必要があります	AWS 基本的なセキュリティのベストプラクティス	高	いいえ	定期的
GuardDuty.6	GuardDuty Lambda Protection を有効にする必要があります	AWS Foundational Security Best Practices、PCI DSS v4.0.1	高	いいえ	定期的
GuardDuty.7	GuardDuty EKS ランタイムモニタリングを有効にする必要があります	AWS Foundational Security Best Practices、PCI DSS v4.0.1	中	いいえ	定期的
GuardDuty.8	EC2 の GuardDuty Malware Protection を有効にする必要があります	AWS 基本的なセキュリティのベストプラクティス	高	いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
GuardDuty.9	GuardDuty RDS Protection を有効にする必要があります	AWS Foundational Security Best Practices、PCI DSS v4.0.1	高	いいえ	定期的
GuardDuty.10	GuardDuty S3 Protection を有効にする必要があります	AWS Foundational Security Best Practices、PCI DSS v4.0.1	高	いいえ	定期的
GuardDuty.11	GuardDuty Runtime Monitoring を有効にする必要があります	AWS 基本的なセキュリティのベストプラクティス	高	いいえ	定期的
GuardDuty.12	GuardDuty ECS Runtime Monitoring を有効にする必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	定期的
GuardDuty.13	GuardDuty EC2 Runtime Monitoring を有効にする必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.1	IAM ポリシーでは、完全な「*」管理権限を許可してはなりません	CIS AWS Foundations Benchmark v1.2.0、 AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	高	✗ いいえ	変更によってトリガーされる
IAM.2	IAM ユーザーには IAM ポリシーをアタッチしてはなりません	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	低	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.3	IAM ユーザーのアクセスキーは 90 日以内ごとに更新する必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✗ いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.4	IAM ルートユーザーのアクセスキーが存在してはいけません	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	✗ いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.5	MFA は、コンソールパスワードを持つすべての IAM ユーザーに対して有効にする必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✗ いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.6	ルートユーザーに対してハードウェア MFA を有効にする必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	重大	✗ いいえ	定期的
IAM.7	IAM ユーザーのパスワードポリシーには強力な設定が必要です	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✓ はい	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.8	未使用の IAM ユーザー認証情報は削除する必要があります	CIS AWS Foundations Benchmark v1.2.0、 AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v3.2.1、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✗ いいえ	定期的
IAM.9	ルートユーザーに対して MFA を有効にする必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1	重大	✗ いいえ	定期的
IAM.10	IAM ユーザーのパスワードポリシーには強力な設定が必要です	NIST SP 800-171 Rev. 2、PCI DSS v3.2.1	中	✗ いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.11	IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認する	CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1	中	✗ いいえ	定期的
IAM.12	IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認する	CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1	中	✗ いいえ	定期的
IAM.13	IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認する	CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2	中	✗ いいえ	定期的
IAM.14	IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認する	CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1	中	✗ いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.15	IAM パスワードポリシーにおいて、14 文字以上のパスワードが要求されるようにする	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2	中	いいえ	定期的
IAM.16	IAM パスワードポリシーはパスワードの再使用を禁止しています	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1	低	いいえ	定期的
IAM.17	IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認する	CIS AWS Foundations Benchmark v1.2.0、PCI DSS v4.0.1	低	いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.18	AWS サポート でインシデントを管理するためのサポートロールが作成されていることを確認する	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1	低	✗ いいえ	定期的
IAM.19	すべての IAM ユーザーに対して MFA を有効にする必要があります	NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v3.2.1、PCI DSS v4.0.1	中	✗ いいえ	定期的
IAM.21	作成する IAM カスタマー管理ポリシーにはサービスのワイルドカードアクションを許可しないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	低	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.22	45 日間未使用の IAM ユーザー認証情報は削除する必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-171 Rev. 2	中	いいえ	定期的
IAM.23	IAM Access Analyzer アナライザーにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IAM.24	IAM ロールにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IAM.25	IAM ユーザーはタグ付けする必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IAM.26	IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります	CIS AWS Foundations Benchmark v3.0.0	中	いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IAM.27	IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください	CIS AWS Foundations Benchmark v3.0.0	中	✗ いいえ	変更によってトリガーされる
IAM.28	IAM Access Analyzer の外部アクセスアナライザーを有効にする必要があります	CIS AWS Foundations Benchmark v3.0.0	高	✗ いいえ	定期的
Inspector.1	Amazon Inspector EC2 スキャンを有効にする必要があります	AWS Foundational Security Best Practices、PCI DSS v4.0.1	高	✗ いいえ	定期的
Inspector.2	Amazon Inspector ECR スキャンを有効にする必要があります	AWS Foundational Security Best Practices、PCI DSS v4.0.1	高	✗ いいえ	定期的
Inspector.3	Amazon Inspector Lambda コードスキャンを有効にする必要があります	AWS Foundational Security Best Practices、PCI DSS v4.0.1	高	✗ いいえ	定期的
Inspector.4	Amazon Inspector Lambda 標準スキャンを有効する必要があります	AWS Foundational Security Best Practices、PCI DSS v4.0.1	高	✗ いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IoT.1	AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IoT.2	AWS IoT Core 緩和アクションにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IoT.3	AWS IoT Core ディメンションにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IoT.4	AWS IoT Core オーソライザーにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IoT.5	AWS IoT Core ロールエイリアスにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IoT.6	AWS IoT Core ポリシーにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IoTEvents.1	AWS IoT Events 入力にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IoTEvents.2	AWS IoT Events ディテクターモデルにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IoTEvents.3	AWS IoT Events アラームモデルにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IoTSiteWise.1	AWS IoT SiteWise アセットモデルにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IoTSiteWise.2	AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IoTSiteWise.3	AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IoTSiteWise.4	AWS IoT SiteWise ポータルにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IoTSiteWise.5	AWS IoT SiteWise プロジェクトにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IoTTwinMaker.1	AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IoTTwinMaker.2	AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IoTTwinMaker.3	AWS IoT TwinMaker シーンにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IoTTwinMaker.4	AWS IoT TwinMaker エンティティにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
IoTWireless.1	AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IoTWireless.2	AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IoTWireless.3	AWS IoT Wireless FUOTA タスクにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IVS.1	IVS 再生キーペアにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IVS.2	IVS 記録設定にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
IVS.3	IVS チャネルにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Keyspaces.1	Amazon Keyspaces キースペースにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
Kinesis.1	Kinesis Streams は、保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
Kinesis.2	Kinesis ストリームにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
Kinesis.3	Kinesis ストリームには適切なデータ保持期間が必要です	AWS 基本的なセキュリティのベストプラクティス	中	はい	変更によってトリガーされる
KMS.1	IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
KMS.2	IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用ないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
KMS.3	AWS KMS keys 意図せずに削除しないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	重大	✗ いいえ	変更によってトリガーされる
KMS.4	AWS KMS key ローテーションを有効にする必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1	中	✗ いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
KMS.5	KMS キーはパブリックにアクセスできません	AWS 基本的なセキュリティのベストプラクティス	重大	✗ いいえ	変更によってトリガーされる
Lambda.1	Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	重大	✗ いいえ	変更によってトリガーされる
Lambda.2	Lambda 関数はサポートされているランタイムを使用する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✗ いいえ	変更によってトリガーされる
Lambda.3	Lambda 関数は VPC 内に存在する必要があります	PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	低	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Lambda.5	VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	はい	変更によってトリガーされる
Lambda.6	Lambda 関数にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
Lambda.7	Lambda 関数では AWS X-Ray アクティブトレースが有効になっている必要があります	NIST SP 800-53 Rev. 5	低	いいえ	変更によってトリガーされる
Macie.1	Amazon Macie を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	いいえ	定期的
Macie.2	Macie 自動機密データ検出を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	高	いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
MSK.1	MSK クラスターはブローカーノード間の転送時に暗号化される必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	いいえ	変更によってトリガーされる
MSK.2	MSK クラスターでは、拡張モニタリングを設定する必要があります	NIST SP 800-53 Rev. 5	低	いいえ	変更によってトリガーされる
MSK.3	MSK Connect コネクタは転送中に暗号化する必要があります	AWS Foundational Security Best Practices、PCI DSS v4.0.1	中	いいえ	変更によってトリガーされる
MSK.4	MSK クラスターではパブリックアクセスを無効にする必要があります	AWS 基本的なセキュリティのベストプラクティス	重大	いいえ	変更によってトリガーされる
MSK.5	MSK コネクタではログ記録が有効になっている必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	変更によってトリガーされる
MSK.6	MSK クラスターは認証されていないアクセスを無効にする必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
MQ.2	ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	いいえ	変更によってトリガーされる
MQ.3	Amazon MQ ブローカーでは自動マイナーバージョンアップグレードが有効になっている必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	低	いいえ	変更によってトリガーされる
MQ.4	Amazon MQ ブローカーにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
MQ.5	ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります	NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	低	いいえ	変更によってトリガーされる
MQ.6	RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。	NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	低	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Neptune.1	Neptune DB クラスターは、保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	中	✗ いいえ	変更によってトリガーされる
Neptune.2	Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✗ いいえ	変更によってトリガーされる
Neptune.3	Neptune DB クラスタースナップショットはパブリックにしないでください	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	重大	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Neptune.4	Neptune DB クラスターでは、削除保護が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	低	いいえ	変更によってトリガーされる
Neptune.5	Neptune DB クラスターでは、自動バックアップが有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	中	はい	変更によってトリガーされる
Neptune.6	Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	中	いいえ	変更によってトリガーされる
Neptune.7	Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Neptune.8	Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	低	✗ いいえ	変更によってトリガーされる
Neptune.9	Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります	NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
NetworkFirewall.1	Network Firewall ファイアウォールを複数のアベイラビリティーゾーンにデプロイする必要があります	NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
NetworkFirewall.2	Network Firewall ログ記録を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	中	✗ いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
NetworkFirewall.3	Network Firewall ポリシーには、1 つ以上のルールグループが関連付けられている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	中	いいえ	変更によってトリガーされる
NetworkFirewall.4	Network Firewall ポリシーのデフォルトのステートレスアクションは、完全なパケットに対してドロップまたは転送される必要があります。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
NetworkFirewall.5	Network Firewall ポリシーのデフォルトのステートレスアクションは、断片化されたパケットに対してドロップまたは転送される必要があります。	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
NetworkFirewall.6	ステートレスネットワークファイアウォールのルールグループを空にしないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	中	いいえ	変更によってトリガーされる
NetworkFirewall.7	Network Firewall ファイアウォールにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
NetworkFirewall.8	Network Firewall ファイアウォールポリシーにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
NetworkFirewall.9	Network Firewall は削除保護を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
NetworkFirewall.10	Network Firewall ファイアウォールでは、サブネット変更保護を有効にする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Opensearch.1	OpenSearch ドメインは保管中の暗号化を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
Opensearch.2	OpenSearch ドメインがパブリックにアクセスできないようにする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	✗ いいえ	変更によってトリガーされる
Opensearch.3	OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Opensearch.4	CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
Opensearch.5	OpenSearch ドメインでは、監査ログ記録を有効にする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✗ いいえ	変更によってトリガーされる
Opensearch.6	OpenSearch ドメインには少なくとも 3 つのデータノードが必要です	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
Opensearch.7	OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	高	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Opensearch.8	OpenSearch ドメインへの接続は 最新の TLS セキュリティポリシーを使用して暗号化する必要があります	AWS 基本的なセキュリティのベストプラクティス、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
Opensearch.9	OpenSearch ドメインにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
Opensearch.10	OpenSearch ドメインには、最新のソフトウェアアップデートがインストールされている必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	低	いいえ	変更によってトリガーされる
Opensearch.11	OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です	NIST SP 800-53 Rev. 5	低	いいえ	定期的
PCA.1	AWS Private CA ルート認証機関を無効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	低	いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
PCA.2	AWS プライベート CA 認証機関にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
RDS.1	RDS スナップショットはプライベートである必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	いいえ	変更によってトリガーされる
RDS.2	RDS DB インスタンスは、PubliclyAccessible 設定によって判断される、パブリックアクセスを禁止する必要があります	CIS AWS Foundations Benchmark v3.0.0、 AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1	重大	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.3	RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
RDS.4	RDS クラスタースナップショットとデータベーススナップショットは保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
RDS.5	RDS DB インスタンスは、複数のアベイラビリティーゾーンで設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.6	RDS DB インスタンスの拡張モニタリングを設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	はい	変更によってトリガーされる
RDS.7	RDS クラスターでは、削除保護が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	低	いいえ	変更によってトリガーされる
RDS.8	RDS DB インスタンスで、削除保護が有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	いいえ	変更によってトリガーされる
RDS.9	RDS DB インスタンスは CloudWatch Logs にログを発行する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.10	IAM 認証は RDS インスタンス用に設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
RDS.11	Amazon RDS インスタンスでは、自動バックアップが有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	はい	変更によってトリガーされる
RDS.12	IAM 認証は RDS クラスター用に設定する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
RDS.13	RDS 自動マイナーバージョンアップグレードを有効にする必要があります	CIS AWS Foundations Benchmark v3.0.0、 AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	高	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.14	Amazon Aurora クラスターはバックトラッキングを有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	はい	変更によってトリガーされる
RDS.15	RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
RDS.16	Aurora DB クラスターは、タグを DB スナップショットにコピーするように設定する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	低	いいえ	変更によってトリガーされる
RDS.17	RDS DB インスタンスは、タグをスナップショットにコピーするように設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	いいえ	変更によってトリガーされる
RDS.18	RDS インスタンスは VPC 内にデプロイする必要があります	サービスマネージドスタンダード： AWS Control Tower	高	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.19	重大なクラスターイベントについて、既存の RDS イベント通知サブスクリプションを設定する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	✗ いいえ	変更によってトリガーされる
RDS.20	重大なデータベースインスタンスイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	低	✗ いいえ	変更によってトリガーされる
RDS.21	重大なデータベースパラメータグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	低	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.22	重大なデータベースセキュリティグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	低	✗ いいえ	変更によってトリガーされる
RDS.23	RDS インスタンスはデータベースエンジンのデフォルトポートを使用しないようにする必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	✗ いいえ	変更によってトリガーされる
RDS.24	RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	✗ いいえ	変更によってトリガーされる
RDS.25	RDS データベースインスタンスはカスタム管理者ユーザー名を使用する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.26	RDS DB インスタンスはバックアッププランで保護する必要があります	NIST SP 800-53 Rev. 5	中	はい	定期的
RDS.27	RDS DB クラスターは保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード：AWS Control Tower	中	いいえ	変更によってトリガーされる
RDS.28	RDS DB クラスターにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
RDS.29	RDS DB クラスタースナップショットにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
RDS.30	RDS DB インスタンスにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
RDS.31	RDS DB セキュリティグループにタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.32	RDS DB スナップショットにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
RDS.33	RDS DB サブネットグループはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
RDS.34	Aurora MySQL DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	いいえ	変更によってトリガーされる
RDS.35	RDS DB クラスターではマイナーバージョンの自動アップグレードを有効にしておく必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	いいえ	変更によってトリガーされる
RDS.36	RDS for PostgreSQL DB インスタンスは CloudWatch Logs にログを発行する必要があります	AWS Foundational Security Best Practices、PCI DSS v4.0.1	中	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.37	Aurora PostgreSQL DB クラスターでは、ログを CloudWatch Logs に発行する必要があります	AWS Foundational Security Best Practices、PCI DSS v4.0.1	中	✗ いいえ	変更によってトリガーされる
RDS.38	RDS for PostgreSQL DB インスタンスは転送中に暗号化する必要があります	AWS 基本的なセキュリティのベストプラクティス	中	✗ いいえ	定期的
RDS.39	RDS for MySQL DB インスタンスは転送中に暗号化する必要があります	AWS 基本的なセキュリティのベストプラクティス	中	✗ いいえ	定期的
RDS.40	RDS for SQL Server DB インスタンスは CloudWatch Logs にログを発行する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	✓ はい	変更によってトリガーされる
RDS.41	RDS for SQL Server DB インスタンスは転送中に暗号化する必要があります	AWS 基本的なセキュリティのベストプラクティス	中	✗ いいえ	定期的
RDS.42	RDS for MariaDB DB インスタンスは CloudWatch Logs にログを発行する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	✓ はい	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RDS.44	RDS for MariaDB DB インスタンスは転送中に暗号化する必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	定期的
RDS.45	Aurora MySQL DB クラスターでは、監査ログ記録を有効にする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	いいえ	定期的
Redshift.1	Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	重大	いいえ	変更によってトリガーされる
Redshift.2	Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Redshift.3	Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	はい	変更によってトリガーされる
Redshift.4	Amazon Redshift クラスターでは、監査ログ記録が有効になっている必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	いいえ	変更によってトリガーされる
Redshift.6	Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
Redshift.7	Redshift クラスターは拡張 VPC ルーティングを使用する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Redshift.8	Amazon Redshift クラスターでデフォルトの管理者ユーザー名を使用しないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
Redshift.9	Redshift クラスターでは、デフォルトのデータベース名を使用しないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
Redshift.10	Redshift クラスターは保存時に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
Redshift.11	Redshift クラスターにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Redshift.12	Redshift イベントサブスクリプション通知にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
Redshift.13	Redshift クラスタースナップショットにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
Redshift.14	Redshift クラスターサブネットグループはタグ付けする必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
Redshift.15	Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの入力を許可する必要があります	AWS Foundational Security Best Practices、PCI DSS v4.0.1	高	いいえ	定期的
Redshift.16	Redshift クラスターサブネットグループには、複数のアベイラビリティーゾーンからのサブネットが必要です	NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Redshift.17	Redshift クラスターパラメータグループにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
Redshift.18	Redshift クラスターでは、マルチ AZ 配置を有効にする必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	変更によってトリガーされる
RedshiftServerless.1	Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります	AWS 基本的なセキュリティのベストプラクティス	高	いいえ	定期的
RedshiftServerless.2	SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	定期的
RedshiftServerless.3	Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります	AWS 基本的なセキュリティのベストプラクティス	高	いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
RedshiftServerless.4	Redshift Serverless 名前空間はカスタマーマネージドで暗号化する必要があります AWS KMS keys	NIST SP 800-53 Rev. 5	中	はい	定期的
RedshiftServerless.5	Redshift Serverless 名前空間では、デフォルトの管理者ユーザー名を使用しないでください	AWS 基本的なセキュリティのベストプラクティス	中	はい	定期的
RedshiftServerless.6	Redshift Serverless 名前空間は CloudWatch Logs にログをエクスポートする必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	定期的
RedshiftServerless.7	Redshift Serverless 名前空間はデフォルトのデータベース名を使用しないでください	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	いいえ	定期的
Route53.1	Route 53 ヘルスチェックにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Route53.2	Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	✗ いいえ	変更によってトリガーされる
S3.1	S3 汎用バケットではブロックパブリックアクセスの設定が有効になっている必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✗ いいえ	定期的
S3.2	S3 汎用バケットではパブリック読み取りアクセスをブロックする必要があります	AWS 基本的なセキュリティのベストプラクティス、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	✗ いいえ	変更によるトリガーと定期的なトリガー

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
S3.3	S3 汎用バケットではパブリック書き込みアクセスをブロックする必要があります。	AWS 基本的なセキュリティのベストプラクティス、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	重大	✗ いいえ	変更によるトリガーと定期的なトリガー
S3.5	S3 汎用バケットではリクエストに SSL を使用する必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v3.2.1、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
S3.6	S3 汎用バケットポリシーは、他の へのアクセスを制限する必要があります AWS アカウント	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	高	✗ いいえ	変更によってトリガーされる
S3.7	S3 汎用バケットではクロスリージョンレプリケーションを使用する必要があります	PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	低	✗ いいえ	変更によってトリガーされる
S3.8	S3 汎用バケットではパブリックアクセスをブロックする必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	高	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
S3.9	S3 汎用バケットでは、サーバーアクセスログ記録が有効になっている必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	いいえ	変更によってトリガーされる
S3.10	バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です	NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
S3.11	S3 汎用バケットでは、イベント通知を有効にする必要があります	NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	中	はい	変更によってトリガーされる
S3.12	ACL は、S3 汎用バケットへのユーザーアクセスの管理に使用しません	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
S3.13	S3 汎用バケットにはライフサイクル設定が必要です	AWS Foundational Security Best Practices、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	低	はい	変更によってトリガーされる
S3.14	S3 汎用バケットではバージョニングが有効になっている必要があります	NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	低	いいえ	変更によってトリガーされる
S3.15	S3 汎用バケットでは Object Lock が有効になっている必要があります	NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	はい	変更によってトリガーされる
S3.17	S3 汎用バケットは保管時に で暗号化する必要があります AWS KMS keys	NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	いいえ	変更によってトリガーされる
S3.19	S3 アクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	重大	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
S3.20	S3 汎用バケットでは MFA 削除が有効になっている必要があります	CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	低	いいえ	変更によってトリガーされる
S3.22	S3 汎用バケットはオブジェクトレベルの書き込みイベントをログに記録する必要があります	CIS AWS Foundations Benchmark v3.0.0、PCI DSS v4.0.1	中	いいえ	定期的
S3.23	S3 汎用バケットはオブジェクトレベルの読み取りイベントをログに記録する必要があります	CIS AWS Foundations Benchmark v3.0.0、PCI DSS v4.0.1	中	いいえ	定期的
S3.24	S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります	AWS Foundational Security Best Practices、PCI DSS v4.0.1	高	いいえ	変更によってトリガーされる
S3.25	S3 ディレクトリバケットにはライフサイクル設定が必要です	AWS 基本的なセキュリティのベストプラクティス	低	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
SageMaker.1	Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	高	✗ いいえ	定期的
SageMaker.2	SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	高	✗ いいえ	変更によってトリガーされる
SageMaker.3	ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	高	✗ いいえ	変更によってトリガーされる
SageMaker.4	SageMaker エンドポイントの本番稼働バリアントの初期インスタンス数は 1 より大きい必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	✗ いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
SageMaker.5	SageMaker モデルでは、ネットワーク分離を有効にする必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	変更によってトリガーされる
SageMaker.6	SageMaker アプリのイメージ設定にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
SageMaker.7	SageMaker イメージにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
SageMaker.8	SageMaker ノートブックインスタンスは、サポートされているプラットフォームで実行する必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	定期的
SecretsManager.1	Secrets Manager のシークレットは、自動ローテーションを有効にする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
SecretsManager.2	自動ローテーションを設定した Secrets Manager のシークレットは正常にローテーションする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✗ いいえ	変更によってトリガーされる
SecretsManager.3	未使用の Secrets Manager のシークレットを削除します	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、サービスマネージドスタンダード： AWS Control Tower	中	✓ はい	定期的
SecretsManager.4	Secrets Manager のシークレットは、指定された日数以内にローテーションする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	中	✓ はい	定期的
SecretsManager.5	Secrets Manager シークレットにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
ServiceCatalog.1	Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	高	✗ いいえ	定期的
SES.1	SES 連絡先リストにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
SES.2	SES 設定セットにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
SNS.1	SNS トピックは、保管時に を使用して暗号化する必要があります AWS KMS	NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	中	✗ いいえ	変更によってトリガーされる
SNS.3	SNS トピックにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
SNS.4	SNS トピックアクセスポリシーでパブリックアクセスを許可しないでください	AWS 基本的なセキュリティのベストプラクティス	高	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
SQS.1	Amazon SQS キューは保管中に暗号化する必要があります	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる
SQS.2	SQS キューにはタグを付ける必要があります	AWS リソースタグ付け標準	低	✓ はい	変更によってトリガーされる
SQS.3	SQS キューアクセスポリシーはパブリックアクセスを許可しないでください	AWS 基本的なセキュリティのベストプラクティス	高	✗ いいえ	変更によってトリガーされる
SSM.1	EC2 インスタンスはによって管理する必要があります AWS Systems Manager	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	中	✗ いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
SSM.2	Systems Manager によって管理される EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v3.2.1、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	高	✗ いいえ	変更によってトリガーされる
SSM.3	Systems Manager によって管理される EC2 インスタンスの関連付けコンプライアンスステータスは、COMPLIANT である必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1、サービスマネージドスタンダード： AWS Control Tower	低	✗ いいえ	変更によってトリガーされる
SSM.4	SSM ドキュメントはパブリックにしないでください	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	重大	✗ いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
SSM.5	SSM ドキュメントにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
SSM.6	SSM Automation では CloudWatch ログ記録が有効になっている必要があります	AWS 基本的なセキュリティのベストプラクティス v1.0.0	中	いいえ	定期的
SSM.7	SSM ドキュメントでは、パブリック共有ブロック設定が有効になっている必要があります	AWS 基本的なセキュリティのベストプラクティス v1.0.0	重大	いいえ	定期的
StepFunctions.1	Step Functions ステートマシンでは、ログ記録がオンになっている必要があります	AWS Foundational Security Best Practices v1.0.0、PCI DSS v4.0.1	中	はい	変更によってトリガーされる
StepFunctions.2	Step Functions アクティビティにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
Transfer.1	Transfer Family ワークフローにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
Transfer.2	Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	いいえ	定期的
Transfer.3	Transfer Family コネクタでは、ログ記録が有効になっている必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
Transfer.4	Transfer Family 契約にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
Transfer.5	Transfer Family 証明書にはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
Transfer.6	Transfer Family コネクタにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる
転送.7	Transfer Family プロファイルにはタグを付ける必要があります	AWS リソースタグ付け標準	低	はい	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
WAF.1	AWS WAF Classic グローバルウェブ ACL ログ記録を有効にする必要があります	AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	中	いいえ	定期的
WAF.2	AWS WAF Classic リージョンルールには少なくとも 1 つの条件が必要です	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
WAF.3	AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
WAF.4	AWS WAF Classic リージョンウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
WAF.6	AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
WAF.7	AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
WAF.8	AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
WAF.10	AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です	AWS Foundational Security Best Practices v1.0.0、サービスマネージドスタンダード： AWS Control Tower、NIST SP 800-53 Rev. 5	中	いいえ	変更によってトリガーされる
WAF.11	AWS WAF ウェブ ACL ログ記録を有効にする必要があります	NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	低	いいえ	定期的

セキュリティコントロール ID	セキュリティコントロールのタイトル	適用される標準	緊急度	カスタムパラメータをサポート	スケジュールタイプ
WAF.12	AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります	AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	中	いいえ	変更によってトリガーされる
WorkSpaces.1	WorkSpaces ユーザーボリュームは保管時に暗号化する必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	変更によってトリガーされる
WorkSpaces.2	WorkSpaces ルートボリュームは保管時に暗号化する必要があります	AWS 基本的なセキュリティのベストプラクティス	中	いいえ	変更によってトリガーされる

Security Hub CSPM コントロールの変更ログ

次の変更ログは、既存の AWS Security Hub CSPM セキュリティコントロールの重要な変更を追跡します。これにより、コントロールの全体的なステータスとその検出結果のコンプライアンスステータスが変更される可能性があります。Security Hub CSPM がコントロールステータスを評価する方法については、「」を参照してください[コンプライアンスステータスとコントロールステータスの評価](#)。このログへの入力後、コントロールが利用可能なすべての AWS リージョン に影響するまで、変更に数日かかる場合があります。

このログは、2023 年 4 月以降に発生した変更を追跡します。コントロールを選択して、そのコントロールに関する追加の詳細を確認します。タイトルの変更は、コントロールの 90 日間の詳細な説明に記載されています。

変更日	コントロール ID とタイトル	変更点の説明
2025 年 8 月 13 日	[SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります	Security Hub CSPM は、このコントロールのタイトルと説明を変更しました。新しいタイトルと説明は、コントロールが Amazon SageMaker AI ホストモデルの `EnableNetworkIsolation` パラメータの設定をチェックしていることをより正確に反映しています。以前は、このコントロールのタイトルは でしたSageMaker models should block inbound traffic。
2025 年 8 月 13 日	[EFS.6] EFS マウントターゲットは、起動時にパブリック IP アドレスを割り当てるサブネットに関連付けるべきではありません	Security Hub CSPM は、このコントロールのタイトルと説明を変更しました。新しいタイトルと説明は、コントロールが実行するチェックの範囲と性質をより正確に反映します。以前は、このコントロールのタイトルは でしたEFS mount targets should not

変更日	コントロール ID とタイトル	変更点の説明
		be associated with a public subnet。
2025 年 7 月 24 日	[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。	このコントロールは、Amazon EKS クラスターがサポートされている Kubernetes バージョンで実行されているかどうかをチェックします。Security Hub CSPM は、このコントロールのパラメータ値をから `1.30`に変更しました`1.31`。Amazon EKS での Kubernetes バージョン 1.30 の標準サポートは、2025 年 7 月 23 日に終了しました。

変更日	コントロール ID とタイトル	変更点の説明
2025 年 7 月 23 日	[EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります	Security Hub CSPM がこのコントロールのタイトルを変更しました。新しいタイトルは、コントロールが起動パラメータを指定する Amazon EC2 スポットフリートリクエストのみをチェックすることをより正確に反映しています。以前は、このコントロールのタイトルは でしたEC2 Spot Fleet requests should enable encryption for attached EBS volumes。
2025 年 6 月 30 日	[IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します	Security Hub CSPM は、PCI DSS v4.0.1 標準からこのコントロールを削除しました。PCI DSS v4.0.1 では、パスワードに記号を使用することを明示的に要求していません。

変更日	コントロール ID とタイトル	変更点の説明
2025 年 6 月 30 日	[IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します	Security Hub CSPM は、このコントロールを NIST SP 800-171 Revision 2 標準から削除しました。NIST SP 800-171 リビジョン 2 では、パスワードの有効期限を 90 日以内に明示的に設定する必要はありません。
2025 年 6 月 30 日	[RDS.16] Aurora DB クラスターは、タグを DB スナップショットにコピーするように設定する必要があります	Security Hub CSPM がこのコントロールのタイトルを変更しました。新しいタイトルは、コントロールが Amazon Aurora DB クラスターのみをチェックすることをより正確に反映しています。以前は、このコントロールのタイトルは でしたRDS DB clusters should be configured to copy tags to snapshots。

変更日	コントロール ID とタイトル	変更点の説明
2025 年 6 月 30 日	[SageMaker.8] SageMaker ノートブックインスタンスは、サポートされているプラットフォームで実行する必要があります	このコントロールは、ノートブックインスタンスに指定されたプラットフォーム識別子に基づいて、Amazon SageMaker AI ノートブックインスタンスがサポートされているプラットフォームで実行されるように設定されているかどうかを確認します。Security Hub CSPM は、このコントロールのパラメータ値`notebook-al2-v2` として `notebook-al2-v1`および をサポートしなくなりました。これらのプラットフォームで実行されるノートブックインスタンスは、2025 年 6 月 30 日にサポートが終了しました。

変更日	コントロール ID とタイトル	変更点の説明
2025 年 5 月 30 日	[IAM.10] IAM ユーザーのパスワードポリシーには強力な設定が必要です	Security Hub CSPM は、PCI DSS v4.0.1 標準からこのコントロールを削除しました。このコントロールは、IAM ユーザーのアカウントパスワードポリシーが、パスワードの最小長 7 文字を含む最小要件を満たしているかどうかをチェックします。PCI DSS v4.0.1 では、パスワードを 8 文字以上にする必要があります。このコントロールは、異なるパスワード要件を持つ PCI DSS v3.2.1 標準に引き続き適用されます。 PCI DSS v4.0.1 の要件に照らしてアカウントのパスワードポリシーを評価するには、IAM.7 コントロールを使用できます。このコントロールでは、8 文字以上のパスワードが必要です。また、パスワードの長さやその他のパラメータのカスタム値もサポートしていま

変更日	コントロール ID とタイトル	変更点の説明
		す。IAM.7 コントロールは、Security Hub CSPM の PCI DSS v4.0.1 標準の一部です。
2025 年 5 月 8 日	[RDS.46] RDS DB インスタンスは、インターネットゲートウェイへのルートを持つパブリックサブネットにデプロイしないでください	Security Hub CSPM は、すべて RDS.46 コントロールのリリースをロールバックしました AWS リージョン。以前は、このコントロールは AWS Foundational Security Best Practices (FSBP) 標準をサポートしていました。

変更日	コントロール ID とタイトル	変更点の説明
2025 年 4 月 7 日	[ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります	このコントロールは、Application Load Balancer の HTTPS リスナーまたは Network Load Balancer の TLS リスナーが、推奨されるセキュリティポリシーを使用して転送中のデータを暗号化するように設定されているかどうかを確認します。Security Hub CSPM は、このコントロールで `ELBSecurityPolicy-TLS13-1-2-Res-2021-06` との 2 つの追加のパラメータ値をサポートするようになりましたELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 。

変更日	コントロール ID とタイトル	変更点の説明
2025 年 3 月 27 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	このコントロールは、関数のランタイム設定が、 AWS Lambda 各言語でサポートされているランタイムの期待値と一致するかどうかをチェックします。Security Hub CSPM は、このコントロールのパラメータ値`ruby3.4`としてをサポートするようになりました。このランタイムのサポート AWS Lambda が追加されました。

変更日	コントロール ID とタイトル	変更点の説明
2025 年 3 月 26 日	[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。	このコントロールは、Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、サポートされている Kubernetes バージョンで実行されるかどうかをチェックします。`oldestVersionSupported` パラメータの場合、Security Hub CSPM は値を から `1.29`に変更しました`1.30`。サポートされている最も古い Kubernetes バージョンは になりました`1.30`。

変更日	コントロール ID とタイトル	変更点の説明
2025 年 3 月 10 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	このコントロールは、関数のランタイム設定が、 AWS Lambda 各言語でサポートされているランタイムの期待値と一致するかどうかをチェックします。Security Hub CSPM は、このコントロールのパラメータ値`python3.8` として `dotnet6`および をサポートしなくなりました。 は、これらのランタイムをサポートし AWS Lambda なくなりました。

変更日	コントロール ID とタイトル	変更点の説明
2025 年 3 月 7 日	[RDS.18] RDS インスタンスは VPC 内にデプロイする必要があります	Security Hub CSPM は、NIST SP 800-53 Rev. 5 要件の AWS Foundational Security Best Practices 標準および自動チェックからこのコントロールを削除しました。Amazon EC2-Classic ネットワークが廃止されたため、Amazon Relational Database Service (Amazon RDS) インスタンスを VPC の外部にデプロイできなくなります。コントロールは引き続き AWS Control Tower サービスマネージド標準の一部です。
2025年1月10日	[Glue.2] AWS Glue ジョブではログ記録を有効にする必要があります	Security Hub CSPM はこのコントロールを廃止し、すべての標準から削除しました。
2024 年 12 月 20 日	EC2.61 から EC2.169	Security Hub CSPM は、EC2.169 コントロールを通じて EC2.61 のリリースをロールバックしました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 12 月 12 日	[RDS.23] RDS インスタンスはデータベースエンジンのデフォルトポートを使用しないようにする必要があります	RDS.23 は、Amazon Relational Database Service (Amazon RDS) クラスターまたはインスタンスがデータベースエンジンのデフォルトポート以外のポートを使用しているかどうかを確認します。コントロールを更新し、基盤となる AWS Config ルールがクラスターの一部である RDS インスタンス`NOT_APPLICABLE` に対して の結果を返すようにしました。
2024 年 12 月 2 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub CSPM がパラメータ`nodejs22.x` として をサポートするようになりました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 11 月 26 日	[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。	このコントロールは、Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、サポートされている Kubernetes バージョンで実行されるかどうかをチェックします。サポートされている最も古いバージョンは になりました`1.29`。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 11 月 20 日	[Config.1] を有効にし、サービスにリンクされたロールをリソース記録に使用 AWS Config する必要があります	Config.1 AWS Config は、 が有効になっているかどうかをチェックし、サービスにリンクされたロールを使用し、有効なコントロールのリソースを記録します。Security Hub CSPM は、このコントロールの重要度を から `MEDIUM`に引き上げました`CRITICAL`。Security Hub CSPM は、Config.1 の検出に失敗した新しいステータスコードとステータス理由も追加しました。これらの変更は、Security Hub CSPM コントロールのオペレーションに対する Config.1 の重要性を反映しています。 AWS Config または リソースの記録が無効になっている場合、不正確なコントロール結果を受け取る可能性があります。 Config.1 `PASSED`の結果を受け取るに

変更日	コントロール ID とタイトル	変更点の説明
		は、有効な Security Hub CSPM コントロールに対応するリソースのリソース記録をオンにし、組織で必要のないコントロールを無効にします。Security Hub CSPM AWS Config の を設定する手順については、「」を参照してくださいSecurity Hub CSPM AWS Config の有効化と設定。Security Hub CSPM コントロールとその対応するリソースのリストについては、「」を参照してくださいコントロールの検出結果に必要な AWS Config リソース。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 11 月 12 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub CSPM がパラメータ`python3.13` として をサポートするようになりました。
2024 年 10 月 11 日	ElastiCache コントロール	ElastiCache.3、ElastiCache.4、ElastiCache.5、および ElastiCache.7 のコントロールのタイトルを変更しました。コントロールは ElastiCache for Valkey にも適用されるため、タイトルは Redis OSS で言及されなくなりました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 9 月 27 日	[ELB.4] Application Load Balancer は、無効な http ヘッダーを削除するように設定する必要があります	タイトルを「Application Load Balancer は、httpヘッダーを削除するように設定する必要があります」から「Application Load Balancer は無効な http ヘッダーを削除するように設定する必要があります」に変更しました。
2024 年 8 月 19 日	DMS.12 および ElastiCache コントロールのタイトルの変更	DMS.12 および ElastiCache.1 から ElastiCache.7 までのコントロールのタイトルを変更しました。Amazon ElastiCache (Redis OSS) サービスの名前変更を反映するように、これらのタイトルを変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 8 月 15 日	[Config.1] を有効にし、サービスにリンクされたロールをリソース記録に使用 AWS Config する必要があります	Config.1 AWS Config は、 が有効になっているかどうかをチェックし、サービスにリンクされたロールを使用し、有効なコントロールのリソースを記録します。Security Hub CSPM に、 という名前のカスタムコントロールパラメータが追加されましたincludeConfigServiceLinkedRoleCheck 。このパラメータを false に設定することで、AWS Config がサービスにリンクされたロールを使用するかどうかの確認をオプトアウトできます。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 7 月 31 日	[IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります	コントロールのタイトルを「AWS IoT Core セキュリティプロファイルにタグ付けする必要があります」から「AWS IoT Device Defender セキュリティプロファイルにタグ付けする必要があります」に変更しました。
2024 年 7 月 29 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub CSPM がパラメータ`nodejs16.x` として をサポートしなくなりました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 7 月 29 日	[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。	このコントロールは、Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、サポートされている Kubernetes バージョンで実行されるかどうかをチェックします。サポートされている最も古いバージョンは 1.28 です。
2024 年 6 月 25 日	[Config.1] を有効にし、サービスにリンクされたロールをリソース記録に使用 AWS Config する必要があります	このコントロールは、 AWS Config が有効になっているかどうかをチェックし、サービスにリンクされたロールを使用し、有効なコントロールのリソースを記録します。Security Hub CSPM は、コントロールが評価する内容を反映するようにコントロールタイトルを更新しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 6 月 14 日	[RDS.34] Aurora MySQL DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります	このコントロールは、Amazon Aurora MySQL DB クラスターが監査ログを Amazon CloudWatch Logs に発行するように設定されているかどうかをチェックします。Security Hub CSPM は、Aurora Serverless v1 DB クラスターの検出結果を生成しないようにコントロールを更新しました。
2024 年 6 月 11 日	[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。	このコントロールは、Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、サポートされている Kubernetes バージョンで実行されるかどうかをチェックします。サポートされている最も古いバージョンは `1.27` です。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 6 月 10 日	[Config.1] を有効にし、サービスにリンクされたロールをリソース記録に使用 AWS Config する必要があります	このコントロール AWS Config は、 が有効で、 AWS Config リソース記録が有効になっているかどうかを確認します。以前は、コントロールは、すべてのリソースに対して記録を設定した場合のみ PASSED 検出結果を生成していました。Security Hub CSPM は、有効なコントロールに必要なリソースの記録が有効になっているときにPASSED検出結果を生成するようにコントロールを更新しました。コントロールも更新され、 AWS Config サービスにリンクされたロールが使用されているかどうかが確認されました。これにより、必要なリソースを記録するためのアクセス許可が提供されます。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 5 月 8 日	[S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります	このコントロールは、Amazon S3 の汎用バージョンバケットで多要素認証 (MFA) 削除が有効になっているかどうかをチェックします。以前は、コントロールはライフサイクル設定を持つバケットの `FAILED` 検出結果を生成していました。ただし、ライフサイクル設定を持つバケットでは、バージョニングによる MFA 削除を有効にすることはできません。Security Hub CSPM は、ライフサイクル設定を持つバケットの検出結果を生成しないようにコントロールを更新しました。コントロールの説明は、現在の動作を反映して更新されました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 5 月 2 日	[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。	Security Hub CSPM は、Amazon EKS クラスターが実行できる最も古いサポートされているバージョンの Kubernetes を更新し、合格した検出結果を生成しました。現在サポートされている最も古いバージョンは Kubernetes 1.26 です。
2024 年 4 月 30 日	[CloudTrail.3] 少なくとも 1 つの CloudTrail 証跡を有効にする必要があります	コントロールのタイトルを「CloudTrail を有効にする必要があります」から「少なくとも 1 つの CloudTrail 証跡を有効にする必要があります」に変更しました。このコントロールは現在、 AWS アカウント で少なくとも 1 つの CloudTrail 証跡が有効になっている場合にPASSED検出結果を生成します。現在の動作を正確に反映するように、タイトルと説明が変更されました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 29 日	[AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要がある	コントロールのタイトルを「Classic Load Balancer に関連付けられた Auto Scaling グループはロードバランサーのヘルスチェックを使用する必要があります」から「ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要があります」に変更しました。このコントロールは現在、アプリケーション、ゲートウェイ、ネットワーク、Classic Load Balancer を評価します。現在の動作を正確に反映するように、タイトルと説明が変更されました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 19 日	[CloudTrail.1] CloudTrail を有効にして、少なくとも 1 つのマルチリージョンの追跡で、読み取りと書き込みの管理イベントを含めた設定をする必要があります。	コントロール AWS CloudTrail は、 が有効で、読み取りおよび書き込み管理イベントを含む少なくとも 1 つのマルチリージョン証跡で設定されているかどうかを確認します。以前は、アカウントで CloudTrail が有効で、少なくとも 1 つのマルチリージョン証跡が設定されていると、証跡がキャプチャされた読み取りおよび書き込み管理イベントがない場合でも、コントロールは誤って PASSED 検出結果を生成していました。コントロールは、CloudTrail が有効で、読み取りおよび書き込み管理イベントをキャプチャする少なくとも 1 つのマルチリージョン証跡で設定されている場合にのみ、PASSED 検出結果を生成するようになりました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 10 日	[Athena.1] Athena ワークグループは、保管中に暗号化する必要があります	Security Hub CSPM はこのコントロールを廃止し、すべての標準から削除しました。Athena ワークグループは、Amazon Simple Storage Service (Amazon S3) バケットにログを送信します。Amazon S3 では、新規および既存の S3 バケットで S3 マネージドキー (SS3-S3) によるデフォルトの暗号化を提供するようになりました。
2024 年 4 月 10 日	[AutoScaling.4] Auto Scaling グループの起動設定では、メタデータ応答ホップ制限が 1 を超えることはできません	Security Hub CSPM はこのコントロールを廃止し、すべての標準から削除しました。Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのメタデータ応答ホップ制限はワークロードによって異なります。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 10 日	[CloudFormation.1] CloudFormation スタックは、Simple Notification Service (SNS) と統合させる必要があります	Security Hub CSPM はこのコントロールを廃止し、すべての標準から削除しました。 AWS CloudFormation スタックを Amazon SNS トピックと統合することは、もはやセキュリティのベストプラクティスではありません。重要な CloudFormation スタックを SNS トピックと統合することは便利ですが、すべてのスタックに必要というわけではありません。
2024 年 4 月 10 日	[CodeBuild.5] CodeBuild プロジェクト環境では特権モードを有効にしないでください	Security Hub CSPM はこのコントロールを廃止し、すべての標準から削除しました。CodeBuild プロジェクトで特権モードを有効にしても、顧客環境に追加のリスクは課されません。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 10 日	[IAM.20] ルートユーザーの使用を避けます	Security Hub CSPM はこのコントロールを廃止し、すべての標準から削除しました。このコントロールの目的は、別のコントロール [CloudWatch.1] 「ルート」ユーザーの使用に対するログメトリクスフィルターとアラームが存在する必要があります でカバーされています。
2024 年 4 月 10 日	[SNS.2] トピックに送信される通知メッセージでは、配信ステータスのログ記録を有効にする必要があります	Security Hub CSPM はこのコントロールを廃止し、すべての標準から削除しました。SNS トピックの配信ステータスのログ記録は、もはやセキュリティのベストプラクティスではありません。重要な SNS トピックの配信ステータスのログ記録は便利ですが、すべてのトピックに必要というわけではありません。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 10 日	[S3.10] バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です	Security Hub CSPM は、このコントロールを AWS Foundational Security Best Practices および Service-Managed Standard: から削除しました AWS Control Tower。このコントロールの目的は、[S3.13] S3 汎用バケットにはライフサイクル設定が必要です と [S3.14] S3 汎用バケットではバージョニングが有効になっている必要があります の 2 つの他のコントロールでカバーされています。このコントロールは依然として NIST SP 800-53 Rev. 5 の一部です。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 10 日	[S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります	Security Hub CSPM は、このコントロールを AWS Foundational Security Best Practices および Service-Managed Standard: から削除しました AWS Control Tower。S3 バケットのイベント通知が役立つ場合もありますが、これは一般的なセキュリティのベストプラクティスではありません。このコントロールは依然として NIST SP 800-53 Rev. 5 の一部です。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 10 日	[SNS.1] SNS トピックは、保管時に を使用して暗号化する必要があります AWS KMS	Security Hub CSPM は、このコントロールを AWS Foundational Security Best Practices および Service-Managed Standard: から削除しました AWS Control Tower。デフォルトでは、SNS はディスク暗号化を使用して保管中のトピックを暗号化します。詳細については、「データの暗号化」を参照してください。AWS KMS を使用してトピックを暗号化することは、セキュリティのベストプラクティスとしては推奨されなくなりました。このコントロールは依然として NIST SP 800-53 Rev. 5 の一部です。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 4 月 8 日	[ELB.6] アプリケーション、ゲートウェイ、および Network Load Balancer で削除保護を有効にする必要があります	コントロールのタイトルを「Application Load Balancer の削除保護を有効化する必要があります」から「アプリケーション、ゲートウェイ、および Network Load Balancer で削除保護が有効になっている必要があります」に変更しました。このコントロールは現在、アプリケーション、ゲートウェイ、Network Load Balancer を評価します。現在の動作を正確に反映するように、タイトルと説明が変更されました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 22 日	[Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります	コントロールのタイトルを「OpenSearch ドメインへの接続は TLS 1.2 を使用して暗号化する必要があります」から「OpenSearch ドメインへの接続は最新の TLS セキュリティポリシー を使用して暗号化する必要があります」に変更しました。以前は、コントロールは OpenSearch ドメインへの接続で TLS 1.2 が使用されたかどうかのみを確認していました。コントロールは、OpenSearch ドメインが最新の TLS セキュリティポリシーを使用して暗号化されている場合に PASSED 検出結果を生成するようになりました。コントロールのタイトルと説明は、現在の動作を反映して更新されました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 22 日	[ES.8] Elasticsearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります	コントロールのタイトルを「Elasticsearch ドメインへの接続は TLS 1.2 を使用して暗号化する必要があります」から「Elasticsearch ドメインへの接続は最新の TLS セキュリティポリシー を使用して暗号化する必要があります」に変更しました。以前は、コントロールは Elasticsearch ドメインへの接続で TLS 1.2 が使用されたかどうかのみを確認していました。コントロールは、Elasticsearch ドメインが最新の TLS セキュリティポリシーを使用して暗号化されている場合に PASSED 検出結果を生成するようになりました。コントロールのタイトルと説明は、現在の動作を反映して更新されました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 12 日	[S3.1] S3 汎用バケットではブロックパブリックアクセスの設定が有効になっている必要があります。	タイトルを「S3 パブリックアクセスブロック設定を有効にする必要があります」から「S3 汎用バケットではパブリックアクセスブロック設定を有効にする必要があります」に変更しました。Security Hub CSPM はタイトルを新しい S3 バケットタイプを考慮して変更しました。
2024 年 3 月 12 日	[S3.2] S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります	タイトルを「S3 バケットはパブリック読み取りアクセスを禁止する必要があります」から「S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります」に変更しました。Security Hub CSPM はタイトルを新しい S3 バケットタイプを考慮して変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 12 日	[S3.3] S3 汎用バケットではパブリック書き込みアクセスをブロックする必要があります。	タイトルを「S3 バケットではパブリック書き込みアクセスを禁止する必要があります」から「S3 汎用バケットではパブリック書き込みアクセスをブロックする必要があります」に変更しました。Security Hub CSPM はタイトルを新しい S3 バケットタイプを考慮して変更しました。
2024 年 3 月 12 日	[S3.5] S3 汎用バケットではリクエストに SSL を使用する必要があります。	タイトルを「S3 バケットでは Secure Socket Layer を使用するリクエストが必要です」から「S3 汎用バケットでは SSL を使用するリクエストが必要です」に変更しました。Security Hub CSPM はタイトルを新しい S3 バケットタイプを考慮して変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 12 日	[S3.6] S3 汎用バケットポリシーは、他の への アクセスを制限する必要があります AWS アカウント	タイトルを「バケットポリシーで他の AWS アカウント に付与される S3 アクセス許可を制限する必要があります」から「S3 汎用バケットポリシーは他の AWS アカウントへのアクセスを制限する必要があります」に変更しました。Security Hub CSPM はタイトルを新しい S3 バケットタイプを考慮して変更しました。
2024 年 3 月 12 日	[S3.7] S3 汎用バケットでクロスリージョンレプリケーションを使用する必要があります	タイトルを「S3 バケットではクロスリージョンレプリケーションが有効になっている必要があります」から「S3 汎用バケットではクロスリージョンレプリケーションを使用する必要があります」に変更しました。Security Hub CSPM はタイトルを新しい S3 バケットタイプを考慮して変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 12 日	[S3.7] S3 汎用バケットでクロスリージョンレプリケーションを使用する必要があります	タイトルを「S3 バケットではクロスリージョンレプリケーションが有効になっている必要があります」から「S3 汎用バケットではクロスリージョンレプリケーションを使用する必要があります」に変更しました。Security Hub CSPM はタイトルを新しい S3 バケットタイプを考慮して変更しました。
2024 年 3 月 12 日	[S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります	タイトルを「S3 パブリックアクセスブロック設定はバケットレベルで有効にする必要があります」から「S3 汎用バケットはパブリックアクセスをブロックする必要があります」に変更しました。Security Hub CSPM はタイトルを新しい S3 バケットタイプを考慮して変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 12 日	[S3.9] S3 汎用バケットは、サーバーアクセスログ記録を有効にする必要があります	タイトルを「S3 バケットサーバーのアクセスログ記録を有効にする必要があります」から「S3 汎用バケット のサーバーアクセスログ記録を有効にする必要があります」に変更しました。Security Hub CSPM はタイトルを新しい S3 バケットタイプを考慮して変更しました。
2024 年 3 月 12 日	[S3.10] バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です	タイトルを「バージョニングが有効になっている S3 バケットはライフサイクルポリシーを設定する必要があります」から「バージョニングが有効になっている S3 汎用バケットはライフサイクルポリシーを設定する必要があります」に変更しました。Security Hub CSPM はタイトルを新しい S3 バケットタイプを考慮して変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 12 日	[S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります	タイトルを「S3 バケットではイベント通知が有効になっている必要があります」から「S3 汎用バケットではイベント通知が有効になっている必要があります」に変更しました。Security Hub CSPM はタイトルを新しい S3 バケットタイプを考慮して変更しました。
2024 年 3 月 12 日	[S3.12] ACL は、S3 汎用バケットへのユーザーアクセスの管理に使用しないでください。	タイトルを「S3 アクセスコントロールリスト (ACLs) はバケットへのユーザーアクセスを管理するのに使用しないでください」から「ACLs へのユーザーアクセスは S3 汎用バケット へのユーザーアクセスを管理するために使用しないでください」に変更しました。Security Hub CSPM はタイトルを新しい S3 バケットタイプを考慮して変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 12 日	[S3.13] S3 汎用バケットにはライフサイクル設定が必要です	タイトルを「S3 バケットはライフサイクルポリシーをから設定する必要があります」から「S3 汎用バケットはライフサイクル設定する必要があります」に変更しました。Security Hub CSPM はタイトルを新しい S3 バケットタイプを考慮して変更しました。
2024 年 3 月 12 日	[S3.14] S3 汎用バケットではバージョニングが有効になっている必要があります	タイトルを「S3 バケットはバージョニングを使用する必要があります」から「S3 汎用バケットでバージョニングが有効になっている必要があります」に変更しました。Security Hub CSPM はタイトルを新しい S3 バケットタイプを考慮して変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 12 日	[S3.15] S3 汎用バケットでは Object Lock が有効になっている必要があります	タイトルを「S3 バケットは Object Lock を使用するように設定する必要があります」から「S3 汎用バケットでは Object Lock が有効になっている必要があります」に変更しました。Security Hub CSPM はタイトルを新しい S3 バケットタイプを考慮して変更しました。
2024 年 3 月 12 日	[S3.17] S3 汎用バケットは保管時に で暗号化する必要があります AWS KMS keys	タイトルを「S3 バケットを保管時に AWS KMS keysで暗号化する必要があります」から「S3 汎用バケットを保管時に AWS KMS keysで暗号化する必要があります」に変更しました。Security Hub CSPM はタイトルを新しい S3 バケットタイプを考慮して変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 3 月 7 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub CSPM がパラメータ`ruby3.3`として `nodejs20.x` およびをサポートするようになりました。
2024 年 2 月 22 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub CSPM がパラメータ`dotnet8`として をサポートするようになりました。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 2 月 5 日	[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。	Security Hub CSPM は、Amazon EKS クラスターが実行できる最も古いサポートされているバージョンの Kubernetes を更新し、合格した検出結果を生成しました。現在サポートされている最も古いバージョンは Kubernetes `1.25` です。

変更日	コントロール ID とタイトル	変更点の説明
2024 年 1 月 10 日	[CodeBuild.1] CodeBuild Bitbucket ソースリポジトリの URL には機密認証情報を含めないでください	タイトルを「CodeBuild GitHub または Bitbucket のソースリポジトリの URL は OAuth を使用する必要があります」から「CodeBuild Bitbucket ソースリポジトリ URL に機密認証情報 を含めないでください」に変更しました。Security Hub CSPM は、他の接続方法も安全であるため、OAuth に関する言及を削除しました。Security Hub CSPM はGitHub ソースリポジトリ URL に個人用アクセストークンまたはユーザー名とパスワードを持つことができなくなるため、GitHub に関する言及を削除しました。 URLs

変更日	コントロール ID とタイトル	変更点の説明
2024 年 1 月 8 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub CSPM は、廃止されたランタイムであるため、`go1.x`および をパラメータ`java8`としてサポートしなくなりました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 12 月 29 日	[RDS.8] RDS DB インスタンスで、削除保護が有効になっている必要があります	RDS.8 は、サポートされているデータベースエンジンのいずれかを使用する Amazon RDS DB インスタンスで削除保護が有効になっているかどうかをチェックします。Security Hub CSPM は`custom-oracle-ee` 、データベースエンジン`oracle-se2-cdb` として 、`oracle-ee-cdb`、および をサポートするようになりました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 12 月 22 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub CSPM がパラメータ`python3.12` として `java21`および を サポートするようになりました。Security Hub CSPM がパラメータ`ruby2.7`として をサポートしなくなりました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 12 月 15 日	[CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります	CloudFront.1 は、Amazon CloudFront ディストリビューションにデフォルトルートオブジェクトが設定されているかどうかを確認します。Security Hub CSPM は、デフォルトのルートオブジェクトの追加がユーザーのアプリケーションと特定の要件に依存する推奨事項であるため、このコントロールの重要度を CRITICAL から HIGH に下げました。
2023 年 12 月 5 日	[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります	コントロールタイトルが「セキュリティグループでは 0.0.0.0/0 からポート 22 へのイングレスは許可しない必要があります」から「セキュリティグループでは 0.0.0.0/0 または ::/0 からポート 22 へのイングレスは許可しない必要があります」に変更されました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 12 月 5 日	[EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります	コントロールタイトルが「セキュリティグループでは 0.0.0.0/0 からポート 3389 へのイングレスは許可されないことを確認します」から「セキュリティグループでは 0.0.0.0/0 または ::/0 からポート 3389 へのイングレスは許可しない必要があります」に変更されました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 12 月 5 日	[RDS.9] RDS DB インスタンスは CloudWatch Logs にログを発行する必要があります	コントロールタイトルが「データベースのログ記録を有効にする必要があります」から「RDS DB インスタンスは CloudWatch Logs にログを発行する必要があります」に変更されました。Security Hub CSPM は、このコントロールがログが Amazon CloudWatch Logs に発行されているかどうかのみをチェックし、RDS ログが有効になっているかどうかをチェックしないことを特定しました。RDS DB インスタンスが CloudWatch Logs にログを発行するように設定されている場合、このコントロールは PASSED 検出結果を生成します。コントロールタイトルは、現在の動作を反映して更新されました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 12 月 5 日	[EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります	このコントロールは、Amazon EKS クラスターで監査ログ記録が有効になっているかどうかをチェックします。Security Hub CSPM がこのコントロールを評価するために使用する AWS Config ルールが から `eks-cluster-logging-enabled` に変更されました`eks-cluster-log-enabled` 。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 11 月 17 日	[EC2.19] セキュリティグループは、リスクの高いポートへの無制限アクセスを許可してはいけません	EC2.19 は、指定した高リスクと見なされるポートにセキュリティグループの無制限の受信トラフィックがアクセス可能かどうかをチェックします。Security Hub CSPM は、マネージドプレフィックスリストがセキュリティグループルールのソースとして提供されたときに、マネージドプレフィックスリストを考慮するようにこのコントロールを更新しました。コントロールは、プレフィックスリストに文字列「0.0.0.0/0」または「::/0」が含まれている場合、FAILED 検出結果を生成します。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 11 月 16 日	[CloudWatch.15] CloudWatch アラームには、指定されたアクションが設定されている必要があります	コントロールタイトルが「CloudWatch アラームには ALARM 状態用に設定されたアクションが必要です」から、「CloudWatch アラームには、指定されたアクションが設定されている必要があります」に変更されました。
2023 年 11 月 16 日	[CloudWatch.16] CloudWatch ロググループは指定した期間保持する必要があります	コントロールタイトルが「CloudWatch ロググループは少なくとも 1 年間保持する必要があります」から「CloudWatch ロググループは指定された期間保持する必要があります」に変更されました。
2023 年 11 月 16 日	[Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります	コントロールタイトルが「VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります」から「VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります」に変更されました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 11 月 16 日	[AppSync.2] AWS AppSync フィールドレベルのログ記録を有効にする必要があります	コントロールタイトルが「AWS AppSync は、リクエストレベルとフィールドレベルのログ記録をオンにする必要があります」から「AWS AppSync はフィールドレベルのログ記録を有効にする必要があります」に変更されました。
2023 年 11 月 16 日	[EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります	コントロールタイトルが「Amazon Elastic MapReduce クラスターマスターノードは、パブリック IP アドレスを未設定にする必要があります」から「Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります」に変更されました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 11 月 16 日	[Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります	コントロールタイトルが「OpenSearch ドメインは VPC 内に含まれている必要があります」から「OpenSearch ドメインがパブリックにアクセスできないようにする必要があります」に変更されました。
2023 年 11 月 16 日	[ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります	コントロールタイトルが「Elasticsearch ドメインは VPC 内に含まれている必要があります」から「Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります」に変更されました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 10 月 31 日	[ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります	ES.4 は Elasticsearch ドメインが、Amazon CloudWatch Logs にエラーログを送信するように設定されているかどうかを確認します。このコントロールは以前、CloudWatch Logs に送信するように設定されているログを含む Elasticsearch ドメインの PASSED 検出結果を生成していました。Security Hub CSPM は、CloudWatch Logs にエラーログを送信するように設定された Elasticsearch ドメインのみPASSEDの結果を生成するようにコントロールを更新しました。コントロールも更新され、エラーログをサポートしない Elasticsearch バージョンを評価から除外するようになりました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 10 月 16 日	[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります	EC2.13 は、セキュリティグループがポート 22 への無制限のイングレスアクセスを許可しているかどうかをチェックします。Security Hub CSPM は、マネージドプレフィックスリストがセキュリティグループルールのソースとして提供されたときに、マネージドプレフィックスリストを考慮するようにこのコントロールを更新しました。コントロールは、プレフィックスリストに文字列「0.0.0.0/0」または「::/0」が含まれている場合、FAILED 検出結果を生成します。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 10 月 16 日	[EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります	EC2.14 は、セキュリティグループがポート 3389 への無制限のイングレスアクセスを許可しているかどうかをチェックします。Security Hub CSPM は、マネージドプレフィックスリストがセキュリティグループルールのソースとして提供されたときに、マネージドプレフィックスリストを考慮するようにこのコントロールを更新しました。コントロールは、プレフィックスリストに文字列「0.0.0.0/0」または「::/0」が含まれている場合、FAILED 検出結果を生成します。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 10 月 16 日	[EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします	EC2.18 は、使用中のセキュリティグループが、無制限の受信トラフィックを許可しているかどうかをチェックします。Security Hub CSPM は、マネージドプレフィックスリストがセキュリティグループルールのソースとして提供されたときに、マネージドプレフィックスリストを考慮するようにこのコントロールを更新しました。コントロールは、プレフィックスリストに文字列「0.0.0.0/0」または「::/0」が含まれている場合、FAILED 検出結果を生成します。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 10 月 16 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub CSPM がパラメータ`python3.11` として をサポートするようになりました。
2023 年 10 月 4 日	[S3.7] S3 汎用バケットでクロスリージョンレプリケーションを使用する必要があります	Security Hub CSPM は、S3 バケットで同じリージョンレプリケーションではなくクロスリージョンレプリケーションが有効になっているように`CROSS-REGION` 、の値`ReplicationType` を持つ パラメータを追加しました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 9 月 27 日	[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。	Security Hub CSPM は、Amazon EKS クラスターが実行できる最も古いサポートされているバージョンの Kubernetes を更新し、合格した検出結果を生成しました。現在サポートされている最も古いバージョンは Kubernetes `1.24` です。
2023 年 9 月 20 日	[CloudFront.2] CloudFront ディストリビューションでは、オリジンアクセスアイデンティティを有効にする必要があります	Security Hub CSPM はこのコントロールを廃止し、すべての標準から削除しました。代わりに、「[CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります」を参照してください。オリジンのアクセスコントロールは、現在のセキュリティのベストプラクティスです。このコントロールは 90 日後にドキュメントから削除されます。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 9 月 20 日	[EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします	Security Hub CSPM は AWS 、 Foundational Security Best Practices (FSBP) と National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 からこのコントロールを削除しました。これはまだサービスマネージドスタンダードの一部です AWS Control Tower。この コントロールでは、セキュリティグループが EC2 インスタンス、または Elastic Network Interface にアタッチされている場合に、合格の検出結果を生成します。ただし、特定のユースケースでは、セキュリティグループがアタッチされていなくてもセキュリティ上のリスクはありません。他の EC2 コントロール (EC2.2、EC2.13、EC2.14、EC2.18、EC2.19 など) を使用すると、

変更日	コントロール ID とタイトル	変更点の説明
		セキュリティグループをモニタリングできます。
2023 年 9 月 20 日	[EC2.29] EC2 インスタンスは VPC で起動することをお勧めします	Security Hub CSPM はこのコントロールを廃止し、すべての標準から削除しました。Amazon EC2 では、EC2-Classic インスタンスが VPC に移行されました。このコントロールは 90 日後にドキュメントから削除されます。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 9 月 20 日	[S3.4] S3 バケットでは、サーバー側の暗号化を有効にする必要があります	Security Hub CSPM はこのコントロールを廃止し、すべての標準から削除しました。Amazon S3 では、新規および既存の S3 バケットで S3 マネージドキー (SS3-S3) によるデフォルトの暗号化を提供するようになりました。SS3-S3 または SS3-KMS のサーバー側の暗号化を使用して暗号化された既存のバケットの場合、暗号化設定は変更されません。このコントロールは 90 日後にドキュメントから削除されます。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 9 月 14 日	[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします	コントロールタイトルを「VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックとアウトバウンドトラフィックを許可しないようにする必要があります」から「VPC のデフォルトのセキュリティグループ (複数可) では、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにする必要があります」に変更しました。
2023 年 9 月 14 日	[IAM.9] ルートユーザーに対して MFA を有効にする必要があります	コントロールタイトルを「ルートユーザーに対して仮想 MFA を有効にする必要があります」から「ルートユーザーに対して MFA を有効にする必要があります」に変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 9 月 14 日	[RDS.19] 重大なクラスターイベントについて、既存の RDS イベント通知サブスクリプションを設定する必要があります	コントロールタイトルを「重大なクラスターイベントについて、RDS イベント通知のサブスクリプションを設定する必要があります」から「重大なクラスターイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります」に変更しました。
2023 年 9 月 14 日	[RDS.20] 重大なデータベースインスタンスイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります	コントロールタイトルを「重大なデータベースインスタンスイベントに対して RDS イベント通知サブスクリプションを設定する必要があります」から「重大なデータベースインスタンスイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります」に変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 9 月 14 日	[WAF.2] AWS WAF Classic リージョンルールには少なくとも 1 つの条件が必要です	コントロールタイトルを「WAF リージョンルールには、1 つ以上の条件が必要です」から「AWS WAF Classic リージョンルールには、1 つ以上の条件が必要です」に変更しました。
2023 年 9 月 14 日	[WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です	コントロールタイトルを「WAF リージョンルールグループには、1 つ以上の条件が必要です」から「AWS WAF Classic リージョンルールグループには、1 つ以上の条件が必要です」に変更しました。
2023 年 9 月 14 日	[WAF.4] AWS WAF Classic Regional Web ACLs には、少なくとも 1 つのルールまたはルールグループが必要です	コントロールタイトルを「WAF リージョンウェブ ACL には、1 つ以上のルールまたはルールグループが必要です」から「AWS WAF Classic リージョンウェブ ACL には、1 つ以上のルールまたはルールグループが必要です」に変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 9 月 14 日	[WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です	コントロールタイトルを「WAF グローバルルールには、1 つ以上の条件が必要です」から「AWS WAF Classic グローバルルールには、1 つ以上の条件が必要です」に変更しました。
2023 年 9 月 14 日	[WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です	コントロールタイトルを「WAF グローバルルールグループには、1 つ以上の条件が必要です」から「AWS WAF Classic グローバルルールグループには、1 つ以上の条件が必要です」に変更しました。
2023 年 9 月 14 日	[WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です	コントロールタイトルを「WAF グローバルウェブ ACL には、1 つ以上のルールまたはルールグループが必要です」から「AWS WAF Classic グローバルウェブ ACL には、1 つ以上のルールまたはルールグループが必要です」に変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 9 月 14 日	[WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です	コントロールタイトルを「WAFv2 ウェブ ACL には、1 つ以上のルールまたはルールグループが必要です」から「AWS WAF ウェブ ACL には、1 つ以上のルールまたはルールグループが必要です」に変更しました。
2023 年 9 月 14 日	[WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります	コントロールタイトルを「AWS WAF v2 ウェブ ACL ログ記録を有効にする必要があります」から「AWS WAF ウェブ ACL ログ記録を有効にする必要があります」に変更しました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 7 月 20 日	[S3.4] S3 バケットでは、サーバー側の暗号化を有効にする必要があります	S3.4 は、Amazon S3 バケットでサーバー側の暗号化が有効になっているか、または S3 バケットポリシーでサーバー側の暗号化なしの `PutObject` リクエストを明示的に拒否しているかどうかをチェックします。Security Hub CSPM は、KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS) を含むようにこのコントロールを更新しました。S3 バケットが SSE-S3、SSE-KMS、または DSSE-KMS で暗号化されている場合、このコントロールは合格の検出結果を生成します。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 7 月 17 日	[S3.17] S3 汎用バケットは保管時に で暗号化する必要があります AWS KMS keys	S3.17 は Amazon S3 バケットが AWS KMS keyで暗号化されているかどうかをチェックします。Security Hub CSPM は、KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS) を含むようにこのコントロールを更新しました。S3 バケットが SSE-KMS または DSSE-KMS で暗号化されている場合、このコントロールは合格の検出結果を生成します。
2023 年 6 月 9 日	[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。	EKS.2 は、Amazon EKS クラスターがサポートされている Kubernetes バージョンで実行されているかどうかをチェックします。サポートされている最も古いバージョンは現在のところ、1.23 です。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 6 月 9 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub CSPM がパラメータ`ruby3.2`として をサポートするようになりました。
2023 年 6 月 5 日	[APIGateway.5] API Gateway REST API のキャッシュデータは、保管中に暗号化する必要があります	APIGateway.5. は、Amazon API Gateway REST API ステージのすべてのメソッドが保存時に暗号化されているかどうかをチェックします。Security Hub CSPM は、そのメソッドでキャッシュが有効になっている場合にのみ、特定のメソッドの暗号化を評価するようにコントロールを更新しました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 5 月 18 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub CSPM がパラメータ`java17`として をサポートするようになりました。
2023 年 5 月 18 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub CSPM は、 をパラメータ`nodejs12.x` としてサポートしなくなりました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 4 月 23 日	[ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。	ECS.10 は、Amazon ECS Fargate サービスが最新の Fargate プラットフォームバージョンで実行されているかどうかをチェックします。お客様は ECS を通じて直接、または CodeDeploy を使用して Amazon ECS をデプロイできます。Security Hub CSPM は、CodeDeploy を使用して ECS Fargate サービスをデプロイするときに、合格の検出結果を生成するようにこのコントロールを更新しました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 4 月 20 日	[S3.6] S3 汎用バケットポリシーは、他の へのアクセスを制限する必要があります AWS アカウント	S3.6 は、Amazon Simple Storage Service (Amazon S3) バケットポリシーによって、他の のプリンシパルが S3 バケット内のリソースに対して AWS アカウント 拒否されたアクションを実行できないかどうかを確認します。Security Hub CSPM は、バケットポリシーの条件を考慮してコントロールを更新しました。
2023 年 4 月 18 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub CSPM がパラメータ`python3.10` として をサポートするようになりました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 4 月 18 日	[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります	Lambda.2 は、ランタイムの AWS Lambda 関数設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかを確認します。Security Hub CSPM がパラメータ`dotnetcore3.1` として をサポートしなくなりました。

変更日	コントロール ID とタイトル	変更点の説明
2023 年 4 月 17 日	[RDS.11] RDS インスタンスでは、自動バックアップが有効になっている必要があります	RDS.11 は、Amazon RDS インスタンスで自動バックアップが有効になっているかどうか、およびバックアップ保持期間が 7 日以上であるかどうかをチェックします。Security Hub CSPM は、すべてのエンジンがリードレプリカの自動バックアップをサポートしているわけではないため、このコントロールを更新してリードレプリカを評価から除外しました。また、RDS には、リードレプリカの作成時にバックアップ保持期間を指定するオプションはありません。リードレプリカは、デフォルトでバックアップ保持期間 `0` で作成されます。

の Security Hub コントロール AWS アカウント

これらの Security Hub コントロールは AWS アカウントを評価します。

これらのコントロールは、一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Account.1] のセキュリティ連絡先情報は に提供する必要があります AWS アカウント

関連する要件: NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 識別 > リソース設定

重要度: 中

リソースタイプ : `AWS::::Account`

AWS Config ルール : `security-account-information-provided`

スケジュールタイプ: 定期的

パラメータ : なし

このコントロールは、Amazon Web Services (AWS) アカウントにセキュリティの連絡先情報があるかどうかを確認します。アカウントにセキュリティの連絡先情報が提供されていない場合、コントロールは失敗します。

代替のセキュリティ連絡先を使用すると AWS 、利用できなくなった場合に、アカウントに関する問題について他のユーザーに連絡できます。通知は サポート、 または他の AWS のサービス チームから、 AWS アカウント の使用に関連するセキュリティ関連のトピックについて行うことができます。

修正

代替連絡先をセキュリティ連絡先として に追加するには AWS アカウント、「 AWS アカウント管理リファレンスガイド」の「 の代替連絡先の更新 AWS アカウント」を参照してください。

[Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります

カテゴリ: 保護 > セキュアなアクセス管理 > アクセスコントロール

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

重要度: 高

リソースタイプ : `AWS::::Account`

AWS Config ルール : `account-part-of-organizations`

スケジュールタイプ: 定期的

パラメータ : なし

このコントロール AWS アカウント は、 が によって管理される組織の一部であるかどうかをチェックします AWS Organizations。アカウントが組織の一部ではない場合、コントロールは失敗します。

Organizations は、ワークロードのスケーリングに合わせて環境を一元管理するのに役立ちます AWS。特定のセキュリティ要件があるワークロードの分離や、HIPAA または PCI といったフレームワークへの準拠のため、 AWS アカウント を複数使用できます。組織を作成することで、複数のアカウントを 1 つのユニットとして管理し AWS のサービス、それらのアクセス、リソース、リージョンを一元管理できます。

修正

新しい組織を作成して自動的に追加するには、 AWS アカウント 「 AWS Organizations ユーザーガイド」の「組織の作成」を参照してください。既存の組織にアカウントを追加するには、「 ユーザーガイド」の「組織への AWS アカウント の招待」を参照してください。 AWS Organizations

の Security Hub コントロール AWS Amplify

これらの Security Hub コントロールは、 AWS Amplify サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Amplify.1] Amplify アプリにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Amplify::App`

AWS Config ルール : amplify-app-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグ	StringList (最大 6 項目)	AWS 要件を満たす 1 ~	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	キーでは、大文字と小文字が区別されます。		6 個のタグキー。	

このコントロールは、 AWS Amplify アプリケーションに `requiredKeyTags`パラメータで指定されたタグキーがあるかどうかをチェックします。アプリケーションにタグキーがない場合、または `requiredKeyTags`パラメータで指定されたすべてのキーがない場合、コントロールは失敗します。`requiredKeyTags` パラメータの値を指定しない場合、コントロールはタグキーの存在のみをチェックし、アプリにタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、 `aws:` プレフィックスが付いています。

タグは、 AWS リソースに作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの識別、整理、検索、フィルタリングに役立ちます。また、アクションと通知のリソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセスコントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 Tagging AWS Resources and Tag Editor User Guide」を参照してください。

> **Note**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

AWS Amplify アプリにタグを追加する方法については、「 ホスティングユーザーガイド」の「リソースタグ付けのサポート」を参照してください。 AWS Amplify

[Amplify.2] Amplify ブランチにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Amplify::Branch`

AWS Config ルール : amplify-branch-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS Amplify ブランチに `requiredKeyTags`パラメータで指定されたタグキーがあるかどうかをチェックします。ブランチにタグキーがない場合、または `requiredKeyTags`パラメータで指定されたすべてのキーがない場合、コントロールは失敗します。`requiredKeyTags` パラメータの値を指定しない場合、コントロールはタグキーの存在のみをチェックし、ブランチにタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、 `aws:` プレフィックスが付いています。

タグは、 AWS リソースに作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの識別、整理、検索、フィルタリングに役立ちます。また、アクションと通知のリソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセスコントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 Tagging AWS Resources and Tag Editor User Guide」を参照してください。

> **Note**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

AWS Amplify ブランチにタグを追加する方法については、「 ホスティングユーザーガイド」の「リソースタグ付けのサポート」を参照してください。 AWS Amplify

Amazon API Gateway の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon API Gateway サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[APIGateway.1] API Gateway REST および WebSocket API 実行ログ記録を有効にする必要があります

関連する要件: NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::ApiGateway::Stage`、`AWS::ApiGatewayV2::Stage`

AWS Config ルール : api-gw-execution-logging-enabled

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`loggingLevel`	ログ記録レベル	列挙型	`ERROR`, `INFO`	`No default value`

このコントロールは、Amazon API Gateway REST または WebSocket API のすべてのステージでログ記録が有効になっているかどうかをチェックします。API のすべてのステージで、`loggingLevel` が `ERROR` でも `INFO` でもない場合、コントロールは失敗します。特定のログタ

イプを有効にする必要があることを示すカスタムパラメータ値を指定しない限り、ログ記録レベルが `ERROR` または `INFO` であれば、Security Hub は成功の検出結果を生成します。

API Gateway REST または WebSocket API ステージでは、関連するログを有効にする必要があります。API Gateway REST および WebSocket API 実行ログ記録は、API Gateway REST および WebSocket API ステージに対して行われたリクエストの詳細な記録を提供します。ステージには、API 統合バックエンドレスポンス、Lambda オーソライザーレスポンス、統合 AWS エンドポイント`requestId`の が含まれます。

修正

REST および WebSocket API オペレーションのログ記録を有効にするには、「API Gateway 開発者ガイド」の「API Gateway コンソールを使用した CloudWatch による API のログの設定」を参照してください。

[APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります

関連する要件： NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8800NIST.800-53.r5 SC-8r SI-7 3.13.155

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::ApiGateway::Stage`

AWS Config ルール : api-gw-ssl-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon API Gateway REST API ステージに SSL 証明書が設定されているかどうかをチェックします。バックエンドシステムは、これらの証明書を使用して、API Gateway からの受信リクエストであることを認証します。

API Gateway からのリクエストをバックエンドシステムが認証できるようにするには、API Gateway REST API ステージを SSL 証明書を設定する必要があります。

修正

API Gateway REST API SSL 証明書を生成し設定する方法の詳細については、「API Gateway 開発者ガイド」の「バックエンド認証用 SSL 証明書の生成と設定」を参照してください。

[APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります

関連する要件: NIST.800-53.r5 CA-7

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ : `AWS::ApiGateway::Stage`

AWS Config ルール : api-gw-xray-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon API Gateway REST API ステージで AWS X-Ray アクティブトレースが有効になっているかどうかを確認します。

X-Ray アクティブトレースを使用すると、基盤となるインフラストラクチャのパフォーマンスの変化に対してより迅速に対応できます。パフォーマンスの変化により、API が利用できなくなる可能性があります。X-Ray アクティブトレースは、API Gateway REST API オペレーションと接続サービスを介して流れるユーザーリクエストのリアルタイムメトリクスを提供します。

修正

API Gateway REST API オペレーションの X-Ray アクティブトレースを有効にする方法の詳細については、[AWS X-Ray 開発者ガイド]の[AWS X-Rayの Amazon API Gateway アクティブトレースサポート]を参照してください。

[APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります

関連する要件: NIST.800-53.r5 AC-4(21)

カテゴリ: 保護 > 保護サービス

重要度: 中

リソースタイプ : `AWS::ApiGateway::Stage`

AWS Config ルール : api-gw-associated-with-waf

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、API Gateway ステージが AWS WAF ウェブアクセスコントロールリスト (ACL) を使用しているかどうかをチェックします。 AWS WAF ウェブ ACL が REST API Gateway ステージにアタッチされていない場合、このコントロールは失敗します。

AWS WAF は、ウェブアプリケーションと APIsから保護するのに役立つウェブアプリケーションファイアウォールです。これにより、ユーザーが定義するカスタマイズ可能なウェブセキュリティルールと条件に基づいて、ウェブリクエストを許可、ブロック、またはカウントする一連のルールである ACL を設定することができます。悪意のある攻撃から保護するために、API Gateway ステージが AWS WAF ウェブ ACL に関連付けられていることを確認します。

修正

API Gateway コンソールを使用して AWS WAF リージョンウェブ ACL を既存の API Gateway API ステージに関連付ける方法については、「 API Gateway デベロッパーガイド」の「 を使用して AWS WAF API を保護する APIs」を参照してください。

[APIGateway.5] API Gateway REST API のキャッシュデータは、保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::ApiGateway::Stage`

AWS Config ルール: `api-gw-cache-encrypted` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ: なし

このコントロールは、キャッシュが有効になっている API Gateway REST API ステージ内のすべてのメソッドが暗号化されているかどうかをチェックします。API Gateway REST API ステージ内のメソッドのキャッシュ機能が設定されており、そのキャッシュが暗号化されていない場合、コントロールは失敗します。Security Hub は、特定のメソッドのキャッシュが有効になっている場合にのみ、そのメソッドの暗号化を評価します。

保管中のデータを暗号化することで、ディスクに保存されているデータが認証されていないユーザーがアクセスするリスクが軽減されます AWS。これにより、権限のないユーザーによるデータへのアクセスを制限するために、別の一連のアクセスコントロールが追加されます。例えば、データを読み取る前にデータを復号化するには、API の許可が必要です。

API Gateway REST API キャッシュは、セキュリティを強化するために、保管中に暗号化する必要があります。

修正

ステージの API キャッシュを設定するには、「API Gateway デベロッパーガイド」の「Amazon API Gateway のキャッシュを有効にする」を参照してください。[キャッシュ設定] で、[キャッシュデータを暗号化する] を選択します。

[APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります

関連する要件: NIST.800-53.r5 AC-3、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::ApiGatewayV2::Route`

AWS Config ルール : api-gwv2-authorization-type-configured

スケジュールタイプ : 定期的

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`authorizationType`	API ルートの認可タイプ	列挙型	`AWS_IAM`, `CUSTOM`, `JWT`	デフォルト値なし

このコントロールは、Amazon API Gateway ルートに認可タイプが設定されているかどうかを確認します。API Gateway ルートで認可タイプが指定されていない場合、コントロールは失敗します。`authorizationType` パラメータで指定された認可タイプをルートが使用する場合にのみコントロールを成功させたい場合は、必要に応じてカスタムパラメータ値を指定できます。

API Gateway は API へのアクセスを制御し管理する複数のメカニズムをサポートしています。認可タイプを指定することで、API へのアクセスを許可されたユーザーまたはプロセスのみに制限できます。

修正

HTTP API の認可タイプを設定するには、「API Gateway デベロッパーガイド」の「API Gateway での HTTP API へのアクセスの制御と管理」を参照してください。WebSocket API の認可タイプを設定するには、「API Gateway デベロッパーガイド」の「API Gateway での WebSocket API へのアクセスの制御と管理」を参照してください。

[APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります

関連する要件： NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)、PCI v4.0.1/10.4.2

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::ApiGatewayV2::Stage`

AWS Config ルール : api-gwv2-access-logs-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon API Gateway V2 ステージのアクセスログが設定されているかどうかをチェックします。アクセスログ設定が定義されていない場合、このコントロールは失敗します。

API Gateway アクセスログは、誰が API にアクセスしたかや、発信者が API にアクセスした方法に関する詳細情報を提供します。これらのログは、セキュリティ監査やアクセス監査、証拠調査などのアプリケーションに役立ちます。トラフィックパターンの分析や問題のトラブルシューティングを行うには、これらのアクセスログを有効にします。

その他のベストプラクティスについては、「API Gateway デベロッパーガイド」の「REST API のモニタリング」を参照してください。

修正

アクセスログ記録を設定するには、「API Gateway デベロッパーガイド」の「API Gateway コンソールを使用した CloudWatch による API のログの設定」を参照してください。

の Security Hub コントロール AWS AppConfig

これらの Security Hub コントロールは、 AWS AppConfig サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[AppConfig.1] AWS AppConfig アプリケーションにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::AppConfig::Application`

AWS Config ルール : `appconfig-application-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されている カスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS AppConfig アプリケーションにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。アプリケーションにタグキー

がない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredKeyTags。パラメータ が指定されていない場合、コントロールrequiredKeyTagsはタグキーの存在のみをチェックし、アプリケーションにキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS AppConfig アプリケーションにタグを追加するには、 AWS AppConfig API リファレンスTagResourceの「」を参照してください。

[AppConfig.2] AWS AppConfig 設定プロファイルにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::AppConfig::ConfigurationProfile`

AWS Config ルール : `appconfig-configuration-profile-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
requiredKeyTags	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS AppConfig 設定プロファイルにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredKeyTags。設定プロファイルにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredKeyTags。パラメータ が指定されていない場合、コントロールrequiredKeyTagsはタグキーの存在のみをチェックし、設定プロファイルにキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS AppConfig 設定プロファイルにタグを追加するには、 AWS AppConfig API リファレンスTagResourceの「」を参照してください。

[AppConfig.3] AWS AppConfig 環境にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::AppConfig::Environment`

AWS Config ルール : `appconfig-environment-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS AppConfig 環境にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。環境にタグキーがない場合、またはパラメータで指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータが指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、環境にキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセ

ス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS AppConfig 環境にタグを追加するには、 AWS AppConfig API リファレンスTagResourceの「」を参照してください。

[AppConfig.4] AWS AppConfig 拡張機能の関連付けにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::AppConfig::ExtensionAssociation`

AWS Config ルール : `appconfig-extension-association-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタ	StringList (最大 6 項目)	AWS 要件を満たす 1 ~	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	グキーのリスト。タグキーでは、大文字と小文字が区別されます。		6 個のタグキー。	

このコントロールは、 AWS AppConfig 拡張機能の関連付けに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredKeyTags。拡張機能の関連付けにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredKeyTags。パラメータ が指定されていない場合、コントロールrequiredKeyTagsはタグキーの存在のみをチェックし、拡張の関連付けにキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS AppConfig 拡張機能の関連付けにタグを追加するには、 AWS AppConfig API リファレンスTagResourceの「」を参照してください。

Amazon AppFlow の Security Hub コントロール

これらの Security Hub コントロールは、Amazon AppFlow サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::AppFlow::Flow`

AWS Config ルール : `appflow-flow-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon AppFlow フローにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。フローにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、フローにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの

識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

Amazon AppFlow フローにタグを追加するには、「Amazon AppFlow ユーザーガイド」の「Amazon AppFlow でのフローの作成」を参照してください。 AppFlow

の Security Hub コントロール AWS App Runner

これらの AWS Security Hub コントロールは、 AWS App Runner サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[AppRunner.1] App Runner サービスにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::AppRunner::Service`

AWS Config ルール : apprunner-service-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS App Runner サービスにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。App Runner サービスにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、App Runner サービスにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS App Runner サービスへのタグの追加については、 AWS App Runner API リファレンスTagResourceの「」を参照してください。

[AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::AppRunner::VpcConnector`

AWS Config ルール : apprunner-vpc-connector-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS App Runner VPC コネクタにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredKeyTags。VPC コネクタにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredKeyTags。パラメータ が指定されていない場合、コントロールrequiredKeyTagsはタグキーの存在のみをチェックし、VPC コネクタにキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあ

るリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS App Runner VPC コネクタにタグを追加する方法については、 AWS App Runner API リファレンスTagResourceの「」を参照してください。

の Security Hub コントロール AWS AppSync

これらの Security Hub コントロールは、 AWS AppSync サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::AppSync::GraphQLApi`

AWS Config ルール : appsync-cache-ct-encryption-at-rest

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS AppSync API キャッシュが保管時に暗号化されているかどうかを確認します。API キャッシュが保管時に暗号化されていない場合、コントロールは失敗します。

保管中のデータとは、永続的な不揮発性ストレージに任意の期間保管されているデータを指します。保管中のデータを暗号化すると、その機密性が保護され、権限のないユーザーがアクセスするリスクが低減されます。

修正

AWS AppSync API のキャッシュを有効にした後で暗号化設定を変更することはできません。代わりに、キャッシュを削除し、暗号化を有効にして再作成する必要があります。詳細については、「AWS AppSync デベロッパーガイド」の「キャッシュ暗号化」を参照してください。

[AppSync.2] AWS AppSync フィールドレベルのログ記録を有効にする必要があります

関連する要件： PCI DSS v4.0.1/10.4.2

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::AppSync::GraphQLApi`

AWS Config ルール : `appsync-logging-enabled`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値	
`fieldLoggingLevel`	フィールドのログ記録レベル	列挙型	`ERROR`, `ALL`, `INFO`, `DEBUG`	`No default value`	

このコントロールは、 AWS AppSync API でフィールドレベルのログ記録が有効になっているかどうかを確認します。フィールドリゾルバーのログレベルが [なし] に設定されている場合、コントロールは失敗します。特定のログタイプを有効にする必要があることを示すカスタムパラメータ値を指定

しない限り、フィールドリゾルバーのログレベルが ERROR または ALL であれば、Security Hub は成功の検出結果を生成します。

ログおよびメトリクスを使用して、GraphQL クエリを特定、トラブルシューティング、最適化できます。 AWS AppSync GraphQL のログ記録を有効にすると、API リクエストとレスポンスに関する詳細情報を取得し、問題を特定して対応し、規制要件に準拠できます。

修正

のログ記録を有効にするには AWS AppSync、 AWS AppSync デベロッパーガイドの「セットアップと設定」を参照してください。

[AppSync.4] AWS AppSync GraphQL APIsにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::AppSync::GraphQLApi`

AWS Config ルール: `tagged-appsync-graphqlapi` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS AppSync GraphQL API にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。GraphQL API にタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在の

みをチェックし、GraphQL API にキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS AppSync GraphQL API にタグを追加するには、 AWS AppSync API リファレンスTagResourceの「」を参照してください。

[AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理 > パスワードレス認証

重要度: 高

リソースタイプ : `AWS::AppSync::GraphQLApi`

AWS Config ルール : `appsync-authorization-check`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `AllowedAuthorizationTypes: AWS_LAMBDA, AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS` (カスタマイズ不可)

このコントロールは、アプリケーションが API キーを使用して AWS AppSync GraphQL API とやり取りするかどうかをチェックします。 AWS AppSync GraphQL API が API キーで認証されている場合、コントロールは失敗します。

API キーは、認証されていない GraphQL エンドポイントを作成するときに AWS AppSync サービスによって生成されるアプリケーション内のハードコードされた値です。この API キーが侵害されると、エンドポイントは意図しないアクセスに対して脆弱になります。一般にアクセス可能なアプリケーションやウェブサイトをサポートしている場合を除き、API キーを認証に使用することはお勧めしません。

修正

AWS AppSync GraphQL API の認可オプションを設定するには、「 AWS AppSync デベロッパーガイド」の「認可と認証」を参照してください。

[AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::AppSync::ApiCache`

AWS Config ルール : appsync-cache-ct-encryption-in-transit

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS AppSync API キャッシュが転送中に暗号化されているかどうかを確認します。API キャッシュが転送中に暗号化されていない場合、コントロールは失敗します。

転送中のデータとは、クラスター内のノード間やクラスターとアプリケーション間など、ある場所から別の場所に移動するデータを指します。データはインターネット内またはプライベートネットワーク内を移動する場合があります。転送中のデータを暗号化することで、権限のないユーザーがネットワークトラフィックを盗聴するリスクが軽減されます。

修正

AWS AppSync API のキャッシュを有効にした後で暗号化設定を変更することはできません。代わりに、キャッシュを削除し、暗号化を有効にして再作成する必要があります。詳細については、「AWS AppSync デベロッパーガイド」の「キャッシュ暗号化」を参照してください。

Amazon Athena の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon Athena サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Athena.1] Athena ワークグループは、保管中に暗号化する必要があります

> **Important**
>
> Security Hub は、2024 年 4 月にこのコントロールを廃止しました。詳細については、「Security Hub CSPM コントロールの変更ログ」を参照してください。

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

重要度: 中

リソースタイプ : `AWS::Athena::WorkGroup`

AWS Config ルール : athena-workgroup-encrypted-at-rest

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Athena ワークグループが保管中に暗号化されているかどうかをチェックします。Athena ワークグループが保管中に暗号化されていない場合、コントロールは失敗します。

Athena では、チーム、アプリケーション、またはさまざまなワークロードのクエリを実行するためのワークグループを作成できます。各ワークグループには、すべてのクエリで暗号化を有効にする設

定があります。Amazon Simple Storage Service (Amazon S3) マネージドキーによるサーバー側の暗号化、 AWS Key Management Service （ AWS KMS) キーによるサーバー側の暗号化、またはカスタマーマネージド KMS キーによるクライアント側の暗号化を使用するオプションがあります。保管中のデータとは、永続的な不揮発性ストレージに任意の期間保管されているデータを指します。暗号化は、このようなデータの機密性を保護し、権限のないユーザーがデータにアクセスするリスクを低減するのに役立ちます。

修正

Athena ワークグループの保管中の暗号化を有効にするには、「Amazon Athena ユーザーガイド」の「ワークグループの編集」を参照してください。[クエリ結果の設定] セクションで [クエリ結果の暗号化] をクリックします。

[Athena.2] Athena データカタログにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Athena::DataCatalog`

AWS Config ルール: `tagged-athena-datacatalog` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されている カスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、Amazon Athena データカタログにパラメータ `requiredTagKeys` で定義された特定のキーを含むタグがあるかどうかをチェックします。データカタログにタグキーがない場合、

またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、データカタログにキーがタグ付けされていない場合に失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Athena データカタログにタグを追加するには、「Amazon Athena ユーザーガイド」の「Athena リソースのタグ付け」を参照してください。

[Athena.3] Athena ワークグループにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Athena::WorkGroup`

AWS Config ルール: `tagged-athena-workgroup` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、Amazon Athena ワークグループにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。ワークグループにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ワークグループにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Athena ワークグループにタグを追加するには、「Amazon Athena ユーザーガイド」の「個々のワークグループでのタグの追加と削除」を参照してください。

[Athena.4] Athena ワークグループではログ記録が有効になっている必要があります

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::Athena::WorkGroup`

AWS Config ルール : athena-workgroup-logging-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon Athena ワークグループでログ記録が有効になっているかどうかを確認します。ワークグループでログ記録が有効になっていない場合、コントロールは失敗します。

監査ログは、システムアクティビティを追跡およびモニタリングします。これらは、セキュリティ違反の検出、インシデントの調査、規制の遵守に役立つイベントの記録を提供します。監査ログは、組織の全体的な説明責任と透明性も強化します。

修正

Athena ワークグループのログ記録を有効にする方法については、「Amazon Athena ユーザーガイド」の「Athena で CloudWatch クエリメトリクスを有効にする」を参照してください。 Amazon Athena

の Security Hub コントロール AWS Backup

これらの Security Hub コントロールは、 AWS Backup サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります

関連する要件: NIST.800-53.r5 CP-9(8)、NIST.800-53.r5 SI-12

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::Backup::RecoveryPoint`

AWS Config ルール : `backup-recovery-point-encrypted`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、保管時に AWS Backup 復旧ポイントが暗号化されているかどうかを確認します。復旧ポイントが保管時に暗号化されていない場合、コントロールは失敗します。

AWS Backup 復旧ポイントとは、バックアッププロセスの一部として作成されるデータの特定のコピーまたはスナップショットを指します。データがバックアップされた特定の瞬間を表し、元のデータが失われたり、破損したり、アクセス不能になったりした場合の復元ポイントとして機能します。バックアップ復旧ポイントを暗号化すると、不正アクセスに対する保護をさらに強化することができます。暗号化は、バックアップデータの機密性、完全性、およびセキュリティを保護するためのベストプラクティスです。

修正

AWS Backup 復旧ポイントを暗号化するには、 AWS Backup デベロッパーガイドの「 でのバックアップの暗号化 AWS Backup」を参照してください。

[Backup.2] AWS Backup 復旧ポイントにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Backup::RecoveryPoint`

AWS Configルール: `tagged-backup-recoverypoint` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS Backup 復旧ポイントにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。リカバリポイントにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、復旧ポイントにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS Backup 復旧ポイントにタグを追加するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアッププラン] を選択します。
3. リストからバックアッププランを選択します。
4. [バックアッププランタグ] セクションで、[タグを管理] を選択します。
5. タグのキーと値を入力します。追加のキーと値のペアについては [新しいタグの追加] を選択します。
6. タグの追加を完了したら、[Save (保存)] を選択します。

[Backup.3] AWS Backup ボールトにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Backup::BackupVault`

AWS Configルール: `tagged-backup-backupvault` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されている カスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS Backup ボールトにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。リカバリポイントにタグキーがない場合、ま

たはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、復旧ポイントにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS Backup ボールトにタグを追加するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアップボールト] を選択します。
3. リストからバックアップボールトを選択します。
4. [バックアップボールトタグ] セクションで、[タグを管理] を選択します。
5. タグのキーと値を入力します。追加のキーと値のペアについては [新しいタグの追加] を選択します。
6. タグの追加を完了したら、[Save (保存)] を選択します。

[Backup.4] AWS Backup レポートプランにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Backup::ReportPlan`

AWS Configルール: `tagged-backup-reportplan` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS Backup レポートプランにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。レポートプランにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、レポートプランにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これ

らの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS Backup レポートプランにタグを追加するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアップボールト] を選択します。
3. リストからバックアップボールトを選択します。
4. [バックアップボールトタグ] セクションで、[タグを管理] を選択します。
5. [新しいタグを追加] をクリックします。タグのキーと値を入力します。追加のキーと値のペアについても繰り返します。
6. タグの追加を完了したら、[Save (保存)] を選択します。

[Backup.5] AWS Backup バックアッププランにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Backup::BackupPlan`

AWS Configルール: `tagged-backup-backupplan` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS Backup バックアッププランにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。バックアッププランにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、バックアッププランにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS Backup バックアッププランにタグを追加するには

1. https://console.aws.amazon.com/backup で AWS Backup コンソールを開きます。
2. ナビゲーションペインで、[バックアップボールト] を選択します。
3. リストからバックアップボールトを選択します。
4. [バックアップボールトタグ] セクションで、[タグを管理] を選択します。
5. [新しいタグを追加] をクリックします。タグのキーと値を入力します。追加のキーと値のペアについても繰り返します。
6. タグの追加を完了したら、[Save (保存)] を選択します。

の Security Hub コントロール AWS Batch

これらの Security Hub コントロールは、 AWS Batch サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

〔バッチ.1] バッチジョブキューにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Batch::JobQueue`

AWS Config ルール : batch-job-queue-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタ	StringList (最大 6 項目)	AWS 要件を満たす 1 ~	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	グキーのリスト。タグキーでは、大文字と小文字が区別されます。		6 個のタグキー。	

このコントロールは、 AWS Batch ジョブキューにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredKeyTags。ジョブキューにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredKeyTags。パラメータ が指定されていない場合、コントロールrequiredKeyTagsはタグキーの存在のみをチェックし、ジョブキューにキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

バッチジョブキューにタグを追加するには、AWS Batch 「 ユーザーガイド」の「リソースのタグ付け」を参照してください。

[Batch.2] バッチスケジューリングポリシーにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Batch::SchedulingPolicy`

AWS Config ルール : batch-scheduling-policy-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS Batch スケジューリングポリシーにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。スケジューリングポリシーにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、スケジューリングポリシーにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これ

らの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

バッチスケジューリングポリシーにタグを追加するには、AWS Batch 「 ユーザーガイド」の「リソースのタグ付け」を参照してください。

[Batch.3] バッチコンピューティング環境にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Batch::ComputeEnvironment`

AWS Config ルール : batch-compute-environment-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS Batch コンピューティング環境にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredKeyTags。コンピューティング環境にタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredKeyTags。パラメータ が指定されていない場合、コントロールrequiredKeyTagsはタグキーの存在のみをチェックし、コンピューティング環境にキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

バッチコンピューティング環境にタグを追加するには、AWS Batch 「 ユーザーガイド」の「リソースのタグ付け」を参照してください。

[Batch.4] マネージドバッチコンピューティング環境のコンピューティングリソースプロパティにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : AWS::Batch::ComputeEnvironment

AWS Config ルール : batch-managed-compute-env-compute-resources-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、マネージド AWS Batch コンピューティング環境のコンピューティングリソースプロパティに、 `requiredKeyTags`パラメータで指定されたタグキーがあるかどうかをチェックします。コンピューティングリソースプロパティにタグキーがない場合、または`requiredKeyTags`パラメータで指定されたすべてのキーがない場合、コントロールは失敗します。`requiredKeyTags` パラメータに値を指定しない場合、コントロールはタグキーの存在のみをチェックし、コンピューティングリソースプロパティにタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、`aws:`プレフィックスが付いています。このコントロールは、アンマネージド型のコンピューティング環境や、 AWS Fargate リソースを使用するマネージド環境を評価しません。

タグは、 AWS リソースを作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの特定、整理、検索、フィルタリングに役立ちます。また、アクションと通知のリソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセスコントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 Tagging AWS Resources and Tag Editor User Guide」を参照してください。

> **Note**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

マネージドコンピューティング環境で AWS Batch コンピューティングリソースにタグを追加する方法については、AWS Batch 「 ユーザーガイド」の「リソースにタグを付ける」を参照してください。

の Security Hub コントロール AWS Certificate Manager

これらの AWS Security Hub コントロールは、 AWS Certificate Manager (ACM) サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります

関連する要件： NIST.800-53.r5 SC-28(3)、NIST.800-53.r5 SC-7(16)、NIST.800-171.r2 3.13.15、PCI DSS v4.0.1/4.2.1

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::ACM::Certificate`

AWS Config ルール : acm-certificate-expiration-check

スケジュールタイプ: 変更がトリガーされ、定期的に行われる場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
daysToExpiration	ACM 証明書を更新する必要がある日数	整数	14 ~ 365	30

このコントロールは、 AWS Certificate Manager (ACM) 証明書が指定された期間内に更新されるかどうかをチェックします。インポートした証明書と ACM によって提供された証明書の両方をチェックします。指定された期間内に証明書が更新されない場合、コントロールは失敗します。更新期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 30 日を使用します。

ACM は DNS 検証を使用する証明書を自動的に更新できます。E メール検証を使用する証明書の場合、ドメイン検証 E メールに応答する必要があります。ACM は、ユーザーがインポートした証明書を自動的に更新しません。インポートした証明書を手動で更新する必要があります。

修正

ACM は、Amazon 発行の SSL/TLS 証明書のマネージド更新が可能です。つまり、ACM は証明書を自動的に更新するか (DNS 検証を使用している場合)、有効期限が近づくと E メール通知を送信します。これらのサービスは、パブリック ACM 証明書とプライベート ACM 証明書の両方に対して提供されます。

E メールで検証されたドメイン

証明書の有効期限まで 45 日間の時点で、ACM はドメイン所有者にドメイン名ごとに E メールを送信します。ドメインを検証して更新を完了するには、E メール通知に応答する必要があります。

詳細については、「AWS Certificate Manager ユーザーガイド」の「E メールで検証されたドメインの更新」を参照してください。

DNS によって検証されたドメイン

ACM は DNS 検証を使用する証明書を自動的に更新します。有効期限の 60 日前に、ACM は証明書が更新できることを確認します。

ドメイン名を検証できない場合、ACM は手動検証が必要である旨の通知を送信します。これらの通知は、有効期限の 45 日、30 日、7 日、1 日前に送信されます。

詳細については、「AWS Certificate Manager ユーザーガイド」の「DNS によって検証されたドメインの更新」を参照してください。

[ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります

関連する要件： PCI DSS v4.0.1/4.2.1

カテゴリ: 識別 > インベントリ > インベントリサービス

重要度: 高

リソースタイプ : `AWS::ACM::Certificate`

AWS Config ルール : acm-certificate-rsa-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 によって管理される RSA 証明書が少なくとも 2,048 ビットのキー長 AWS Certificate Manager を使用しているかどうかを確認します。キーの長さが 2,048 ビットより小さい場合、コントロールは失敗します。

暗号化の強度はキーサイズと直接相関します。コンピューティング能力が安くなり、サーバーがより高度になるため、 AWS リソースを保護するために、キーの長さを 2,048 ビット以上にすることをお勧めします。

修正

ACM が発行する RSA 証明書における最小のキーの長さは、既に 2,048 ビットです。ACM で新しい RSA 証明書を発行する手順については、「AWS Certificate Manager ユーザーガイド」の「証明書の発行と管理」を参照してください。

ACM では短いキーの長さで証明書をインポートできますが、この制御を行うには少なくとも 2,048 ビットのキーを使用する必要があります。証明書をインポートした後で、キーの長さを変更することはできません。代わりに、キーの長さが 2,048 ビット未満の証明書を削除する必要があります。ACM への証明書のインポートに関する詳細については、「AWS Certificate Manager ユーザーガイド」の「証明書をインポートするための前提条件」を参照してください。

[ACM.3] ACM 証明書にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::ACM::Certificate`

AWS Config ルール: `tagged-acm-certificate` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS Certificate Manager (ACM) 証明書にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。証明書にタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、証明書にキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

ACM 証明書にタグを追加するには、AWS Certificate Manager 「 ユーザーガイド」の AWS Certificate Manager 「証明書のタグ付け」を参照してください。

の Security Hub コントロール AWS CloudFormation

これらの Security Hub コントロールは、 AWS CloudFormation サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[CloudFormation.1] CloudFormation スタックは、Simple Notification Service (SNS) と統合させる必要があります

> **Important**
>
> Security Hub は、2024 年 4 月にこのコントロールを廃止しました。詳細については、「Security Hub CSPM コントロールの変更ログ」を参照してください。

関連する要件: NIST.800-53.r5 SI-4(12)、NIST.800-53.r5 SI-4(5)

カテゴリ: 検出 > 検出サービス > アプリケーションモニタリング

重要度: 低

リソースタイプ : `AWS::CloudFormation::Stack`

AWS Config ルール : `cloudformation-stack-notification-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon Simple Notification Service の通知が AWS CloudFormation スタックに統合されているかどうかをチェックします。CloudFormation スタックに関連付けられた SNS 通知がない場合、そのコントロールは失敗します。

SNS 通知を、CloudFormation スタックを使って設定すると、スタックで発生したイベントや変更を、ステークホルダーにすぐに通知することができます。

修正

CloudFormation スタックと SNS トピックを統合するには、「AWS CloudFormation ユーザーガイド」の「スタックの直接更新」を参照してください。

[CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::CloudFormation::Stack`

AWS Config ルール: `tagged-cloudformation-stack` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS CloudFormation スタックにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。スタックにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存

在のみをチェックし、スタックにキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

CloudFormation スタックにタグを追加するには、「AWS CloudFormation API リファレンス」の「CreateStack」を参照してください。

Amazon CloudFront の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon CloudFront サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります

関連する要件： NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、PCI DSS v4.0.1/2.2.6

カテゴリ: 保護 > セキュアなアクセス管理 > パブリックアクセスが不可能なリソース

重要度: 高

リソースタイプ : `AWS::CloudFront::Distribution`

AWS Config ルール : cloudfront-default-root-object-configured

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon CloudFront ディストリビューションがデフォルトのルートオブジェクトである特定のオブジェクトを返すように設定されているかどうかをチェックします。CloudFront ディストリビューションにデフォルトのルートオブジェクトが設定されていない場合、コントロールは失敗します。

ユーザーは、ディストリビューション内のオブジェクトではなく、ディストリビューションのルート URL を要求することがあります。この場合、デフォルトのルートオブジェクトを指定することで、ウェブディストリビューションのコンテンツの漏洩を防止できます。

修正

CloudFront ディストリビューションのデフォルトルートオブジェクトを設定するには、「Amazon CloudFront デベロッパーガイド」の「デフォルトのルートオブジェクトの指定」を参照してください。

[CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります

関連する要件： NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8800NIST.800-53.r5 SC-8.r SI-75

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::CloudFront::Distribution`

AWS Config ルール : cloudfront-viewer-policy-https

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon CloudFront ディストリビューションで視聴者が HTTPS を直接使用する必要性、またはリダイレクトを使用するかどうかをチェックします。`ViewerProtocolPolicy` が `defaultCacheBehavior` または `cacheBehaviors` の `allow-all` に設定されている場合、コントロールは失敗します。

HTTPS (TLS) を使用すると、潜在的な攻撃者が中間者攻撃または同様の攻撃を使用してネットワークトラフィックを盗聴または操作することを防止できます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。転送中のデータの暗号化は、パフォーマンスに影響する可能性があります。TLS のパフォーマンスプロファイルと TLS の影響を把握するには、この機能を使用してアプリケーションをテストする必要があります。

修正

転送中の CloudFront ディストリビューションを暗号化するには、「Amazon CloudFront デベロッパーガイド」の「ビューワーと CloudFront 間の通信で HTTPS を必須にする」を参照してください。

[CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 低

リソースタイプ : `AWS::CloudFront::Distribution`

AWS Config ルール : cloudfront-origin-failover-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon CloudFront ディストリビューションが 2 つ以上のオリジンを使用するオリジングループで構成されているかどうかをチェックします。

CloudFront オリジンのフェイルオーバーにより、可用性を向上できます。オリジンフェイルオーバーは、プライマリオリジンが使用できない場合、または特定の HTTP レスポンスステータスコードを返した場合に、自動的にセカンダリーオリジンにトラフィックをリダイレクトします。

修正

CloudFront ディストリビューションのオリジンフェイルオーバーを設定するには、「Amazon CloudFront デベロッパーガイド」の「オリジングループの作成」を参照してください。

[CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります

関連する要件： NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53AU-6.r5 CA-7、NIST.800-53.r5 SC-7(7) SI-3 SI-4 SI-710.4.2

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::CloudFront::Distribution`

AWS Config ルール : cloudfront-accesslogs-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、CloudFront ディストリビューションでサーバーアクセスのログ記録が有効になっているかどうかをチェックします。ディストリビューションでアクセスのログ記録が有効でない場合、コントロールは失敗します。このコントロールは、ディストリビューションに対して標準ログ記録 (レガシー) が有効になっているかどうかのみを評価します。

CloudFront アクセスログは、CloudFront が受信するすべてのユーザーリクエストに関する詳細情報を提供します。各ログには、リクエストが受信された日時、リクエストを行ったビューワーの IP アドレス、リクエストソース、ビューワーからのリクエストポート番号などの情報が含まれます。これらのログは、セキュリティ監査やアクセス監査、証拠調査などのアプリケーションに役立ちます。アクセスログの分析の詳細については、Amazon CloudFront ログのクエリ」を参照してください。Amazon Athena

修正

CloudFront ディストリビューションの標準ログ記録 (レガシー) を設定するには、Amazon CloudFront デベロッパーガイド」の「標準ログ記録 (レガシー) の設定」を参照してください。

[CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります

関連する要件： NIST.800-53.r5 AC-4(21)、PCI DSS v4.0.1/6.4.2

カテゴリ: 保護 > 保護サービス

重要度: 中

リソースタイプ : `AWS::CloudFront::Distribution`

AWS Config ルール : cloudfront-associated-with-waf

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、CloudFront ディストリビューションが AWS WAF Classic または AWS WAF ウェブ ACLs に関連付けられているかどうかをチェックします。ディストリビューションがウェブ ACL に関連付けられていない場合、コントロールは失敗します。

AWS WAF は、ウェブアプリケーションと APIsから保護するのに役立つウェブアプリケーションファイアウォールです。これで、ウェブアクセスコントロールリスト (ウェブ ACL) と呼ばれる一連のルールを設定することができます。このルールは、ユーザーが定義するカスタマイズ可能なウェブセキュリティルールと条件に基づいて、ウェブリクエストを許可、ブロック、またはカウントします。CloudFront ディストリビューションが AWS WAF ウェブ ACL に関連付けられていることを確認し、悪意のある攻撃から保護します。

修正

AWS WAF ウェブ ACL を CloudFront ディストリビューションに関連付けるには、Amazon CloudFront デベロッパーガイド」の「 AWS WAF を使用してコンテンツへのアクセスを制御する」を参照してください。

[CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります

関連する要件： NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8800NIST.800-53.r5 SC-8.r SI-7 3.13.155

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::CloudFront::Distribution`

AWS Config ルール : cloudfront-custom-ssl-certificate

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、CloudFront ディストリビューションで、CloudFront が提供するデフォルトの SSL/TLS 証明書を使用しているかどうかをチェックします。CloudFront ディストリビューションで、カスタム SSL/TLS 証明書が使用されている場合に、このコントロールは成功します。CloudFront ディストリビューションで、デフォルト SSL/TLS 証明書が使用されている場合に、このコントロールは失敗します。

カスタム SSL/TLS を使用すると、ユーザーは代替ドメイン名を使用してコンテンツにアクセスできます。カスタム証明書は AWS Certificate Manager (推奨)、または IAM で保存できます。

修正

カスタム SSL/TLS 証明書を使用して CloudFront ディストリビューション用の代替ドメイン名を追加する場合、「Amazon CloudFront デベロッパーガイド」の「代替ドメイン名の追加」を参照してください。

[CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 低

リソースタイプ : `AWS::CloudFront::Distribution`

AWS Config ルール : cloudfront-sni-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon CloudFront ディストリビューションでカスタム SSL/TLS 証明書が使用されていて、SNI を使用して HTTPS リクエストを処理するように設定されているかチェックしま

す。カスタム SSL/TLS 証明書が関連付けられているものの、SSL/TLS サポートメソッドが専用 IP アドレスである場合、このコントロールは失敗します。

Server Name Indication (SNI) は、2010 年以降にリリースされたブラウザとクライアントでサポートされている TLS プロトコルを拡張したものです。SNI を使用して HTTPS リクエストに対応するように CloudFront を設定した場合、CloudFront は代替ドメイン名を各エッジロケーションの IP アドレスと関連付けます。ビューワーがコンテンツに対して HTTPS リクエストを送信すると、DNS は、正しいエッジロケーションの IP アドレスにリクエストをルーティングします。ドメイン名の IP アドレスが SSL/TLS ハンドシェイクネゴシエーション中に決定されます。IP アドレスはディストリビューション専用にはなりません。

修正

SNI を使用して HTTPS リクエストを処理するように CloudFront ディストリビューションを設定するには、「CloudFront デベロッパーガイド」の「SNI を使用した HTTPS リクエストの処理 (ほとんどのクライアントで動作)」を参照してください。カスタム SSL 証明書の詳細については、「CloudFront で SSL/TLS 証明書を使用するための要件」を参照してください。

[CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります

関連する要件： NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8800NIST.800-53.r5 SC-8r SI-75

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::CloudFront::Distribution`

AWS Config ルール : cloudfront-traffic-to-origin-encrypted

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon CloudFront ディストリビューションがカスタムオリジンへのトラフィックを暗号化しているかチェックします。このコントロールは、オリジンプロトコルポリシー

が「http-only」を許可されている CloudFront ディストリビューションでは失敗します。ディストリビューションのオリジンプロトコルポリシーが「match-viewer」で、ビューワープロトコルポリシーが「allow-all」である場合にも、このコントロールは失敗します。

HTTPS (TLS) は、ネットワークトラフィックの傍受や操作を防止するために使用できます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。

修正

CloudFront 接続の暗号化を要求するようにオリジンプロトコルポリシーを更新するには、「Amazon CloudFront デベロッパーガイド」の「CloudFront とカスタムオリジン間の通信で HTTPS を必須にする」を参照してください。

[CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください

関連する要件： NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6) 3.13.15

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::CloudFront::Distribution`

AWS Config ルール : cloudfront-no-deprecated-ssl-protocols

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon CloudFront ディストリビューションが、CloudFront エッジロケーションとカスタムオリジン間の HTTPS 通信に、非推奨の SSL プロトコルを使用しているかどうかをチェックします。CloudFront ディストリビューションに、`OriginSslProtocols` が `SSLv3` を含む `CustomOriginConfig` が使用されていると、このコントロールは失敗します。

2015 年、Internet Engineering Task Force (IETF) は、SSL 3.0 はプロトコルの安全性が不十分であることから廃止すべきであると、正式に発表しました。カスタムオリジンへの HTTPS 通信には、TLSv1.2 以降を使用することが推奨されます。

修正

CloudFront ディストリビューションのオリジン SSL プロトコルを更新する方法については、「Amazon CloudFront デベロッパーガイド」の「CloudFront とカスタムオリジン間の通信で HTTPS を必須にする」を参照してください。

[CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります

関連する要件： NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、PCI DSS v4.0.1/2.2.6

カテゴリ: 識別 > リソース設定

重要度: 高

リソースタイプ : `AWS::CloudFront::Distribution`

AWS Config ルール : cloudfront-s3-origin-non-existent-bucket

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon CloudFront ディストリビューションが存在しない Amazon S3 オリジンをポイントしていないかどうかを確認します。存在しないバケットをポイントするようにオリジンが設定されている場合、CloudFront ディストリビューション用のコントロールは失敗します。このコントロールは、静的ウェブサイトホスティングのない S3 バケットが S3 オリジンである CloudFront ディストリビューションのみに適用されます。

アカウントの CloudFront ディストリビューションが、存在しないバケットをポイントする設定になっている場合、悪意のある第三者が参照先のバケットを作成し、ディストリビューションを通して独自のコンテンツを供給してくる恐れがあります。ルーティング動作に関係なくすべてのオリジンをチェックして、ディストリビューションが適切なオリジンをポイントしていることを確認することをお勧めします。

修正

CloudFront ディストリビューションを変更して新しいオリジンをポイントさせるには、「Amazon CloudFront デベロッパーガイド」の「ディストリビューションの更新」を参照してください。

[CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります

カテゴリ: 保護 > セキュアなアクセス管理 > パブリックアクセスが不可能なリソース

重要度: 中

リソースタイプ : `AWS::CloudFront::Distribution`

AWS Config ルール : cloudfront-s3-origin-access-control-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon S3 オリジンを使用する Amazon CloudFront ディストリビューションにオリジンアクセスコントロール (OAC) が設定されているかどうかをチェックします。OAC が CloudFront ディストリビューション用に設定されていない場合、コントロールは失敗します。

S3 バケットを CloudFront ディストリビューションのオリジンとして使用する場合、OAC を有効にできます。これにより、指定した CloudFront ディストリビューションを介してのみバケット内のコンテンツにアクセスでき、バケットや他のディストリビューションからの直接アクセスは禁止されます。CloudFront はオリジンアクセスアイデンティティ (OAI) をサポートしていますが、OAC には追加機能があり、OAI を使用するディストリビューションは OAC に移行できます。OAI は S3 オリジンにアクセスするための安全な方法を提供しますが、きめ細かなポリシー設定や、 AWS 署名バージョン 4 (SigV4) AWS リージョン を必要とする で POST メソッドを使用する HTTP/HTTPS リクエストのサポートがないなどの制限があります。OAI は による暗号化もサポートしていません AWS Key Management Service。OAC は、IAM サービスプリンシパルを使用して S3 オリジンで認証するという AWS ベストプラクティスに基づいています。

修正

S3 オリジンの CloudFront ディストリビューション用に OAC を設定するには、「Amazon CloudFront デベロッパーガイド」の「Amazon S3 オリジンへのアクセス制限」を参照してください。

[CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::CloudFront::Distribution`

AWS Config rule:`tagged-cloudfront-distribution` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon CloudFront ディストリビューションにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。ディストリビューションにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ディストリビューションにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) と AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS

Billing。タグ付けのベストプラクティスの詳細については、の「AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

CloudFront ディストリビューションにタグを追加するには、「Amazon CloudFront デベロッパーガイド」の「Amazon CloudFront ディストリビューションのタグ付け」を参照してください。

[CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::CloudFront::Distribution`

AWS Config ルール : cloudfront-ssl-policy-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ： `securityPolicies`: `TLSv1.2_2021` (カスタマイズ不可)

このコントロールは、Amazon CloudFront ディストリビューションが推奨 TLS セキュリティポリシーを使用するように設定されているかどうかをチェックします。CloudFront ディストリビューションが推奨 TLS セキュリティポリシーを使用するように設定されていない場合、コントロールは失敗します。

ビューワーが HTTPS を使用してコンテンツにアクセスするように Amazon CloudFront ディストリビューションを設定する場合は、セキュリティポリシーを選択し、使用する最小 SSL/TLS プロトコルバージョンを指定する必要があります。これにより、CloudFront がビューワーとの通信に使用するプロトコルバージョンと、CloudFront が通信の暗号化に使用する暗号が決まります。CloudFront が提供する最新のセキュリティポリシーを使用することをお勧めします。これにより、CloudFront は最新の暗号スイートを使用して、ビューワーと CloudFront ディストリビューション間の転送中のデータを暗号化できます。

> **Note**
>
> このコントロールは、カスタム SSL 証明書を使用するように設定され、レガシークライアントをサポートするように設定されていない CloudFront ディストリビューションに対してのみ結果を生成します。

修正

CloudFront ディストリビューションのセキュリティポリシーの設定については、Amazon CloudFront デベロッパーガイド」の「ディストリビューションの更新」を参照してください。ディストリビューションのセキュリティポリシーを設定するときは、最新のセキュリティポリシーを選択します。

の Security Hub コントロール AWS CloudTrail

これらの AWS Security Hub コントロールは、 AWS CloudTrail サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[CloudTrail.1] CloudTrail を有効にして、少なくとも 1 つのマルチリージョンの追跡で、読み取りと書き込みの管理イベントを含めた設定をする必要があります。

関連する要件： CIS AWS Foundations Benchmark v1.2.0/2.1、 CIS AWS Foundations Benchmark v1.4.0/3.1、 CIS AWS Foundations Benchmark v3.0.0/3.1、 NIST.800-53.r5 AC-2(4)、 NIST.800-53.r5 AC-4(26)、 NIST.800-53.r5 AC-6(9)、 NIST.800-53.r5 AU-10、 NIST.800-53.r5 AU-12、 NIST.800-53.r5 AU-2、 NIST.800-53.r5 AU-3、 NIST.800-53.r5 AU-6(3)、 NIST.800-53.r5 AU-6(4)、 NIST.800-53.r5 AU-14(1)、 NIST.800-53.r5 CA-7、 NIST.800-53.r5 SC-7(9)、 NIST.800-53.r5 SI-3(8)、 NIST.800-53.r5 SI-4(20)、 NIST.800-53.r5 SI-7(8)、 NIST.800-53.r5 SA-8(22)

カテゴリ: 識別 > ログ記録

重要度: 高

リソースタイプ : `AWS::::Account`

AWS Config ルール : multi-region-cloudtrail-enabled

スケジュールタイプ : 定期的

パラメータ :

- `readWriteType`: `ALL` (カスタマイズ不可)

  `includeManagementEvents`: `true` (カスタマイズ不可)

このコントロールは、読み取りおよび書き込み管理イベントをキャプチャするマルチリージョン AWS CloudTrail 証跡が少なくとも 1 つあるかどうかを確認します。CloudTrail が無効になっているか、読み取りおよび書き込み管理イベントをキャプチャする CloudTrail 証跡が少なくとも 1 つ存在しない場合、コントロールは失敗します。

AWS CloudTrail は、アカウントの AWS API コールを記録し、ログファイルを配信します。記録された情報には、以下の情報が含まれます。

- API 発信者の ID
- API コールの時刻
- API 発信者の送信元 IP アドレス
- パラメータのリクエスト
- によって返されるレスポンス要素 AWS のサービス

CloudTrail は、、 AWS SDKs AWS Management Console、コマンドラインツールからの AWS API コールなど、アカウントの API コールの履歴を提供します。履歴には、 AWS のサービス などの上位レベルの API コールも含まれます AWS CloudFormation。

CloudTrail によって生成された AWS API コール履歴により、セキュリティ分析、リソース変更の追跡、コンプライアンス監査が可能になります。マルチリージョン追跡には、次の利点もあります。

- マルチリージョン追跡により、使用していないリージョンで発生する予期しないアクティビティを検出できます。
- マルチリージョン追跡では、グローバルサービスイベントのログ記録がデフォルトで追跡に対して確実に有効になっています。グローバルサービスイベントのログ記録は、 AWS グローバルサービスによって生成されたイベントを記録します。
- マルチリージョン追跡では、すべての読み取りオペレーションと書き込みオペレーションの管理イベントによって、CloudTrail がすべての AWS アカウントアカウントのリソースに対する管理オペレーションを確実に記録します。

デフォルトでは、 を使用して作成された CloudTrail 証跡はマルチリージョン証跡 AWS Management Console です。

修正

CloudTrail で新しいマルチリージョンの追跡を作成するには、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。以下の値を使用します。

フィールド	値
追加設定、ログファイル検証	有効
ログイベント、管理イベント、API アクティビティを選択	[読み取り] と [書き込み] 除外にするチェックボックスはオフにしてください。

既存の追跡を更新するには、「AWS CloudTrail ユーザーガイド」の「証跡の更新」を参照してください。[管理イベント] の [API アクティビティ] で、[読み取り] と [書き込み] を選択します。

[CloudTrail.2] CloudTrail は保管時の暗号化を有効にする必要があります

関連する要件： CIS AWS Foundations Benchmark v1.2.0/2.7、CIS AWS Foundations Benchmark v1.4.0/3.7、CIS AWS Foundations Benchmark v3.0.0/3.5、NIST.800-53.r5 AU-9、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-710.3.2

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::CloudTrail::Trail`

AWS Config ルール : cloud-trail-encryption-enabled

スケジュールタイプ : 定期的

パラメータ: なし

このコントロールは、CloudTrail がサーバー側の暗号化 (SSE) AWS KMS key 暗号化を使用するよう設定されているかどうかをチェックします。`KmsKeyId` が定義されていない場合、コントロールは失敗します。

機密性の高い CloudTrail ログファイルのセキュリティを強化するには、CloudTrail ログファイルに AWS KMS keys (SSE-KMS) を使用したサーバー側の暗号化を使用して保管時の暗号化を行う必要が

あります。デフォルトでは、CloudTrail によってバケットに配信されるログファイルは、「Amazon S3 マネージド暗号化キーによる Amazon サーバー側の暗号化 (SSE-S3)」によって暗号化されることに注意してください。

修正

CloudTrail ログファイルの SSE-KMS 暗号化を有効にするには、「AWS CloudTrail ユーザーガイド」の「KMS キーを使用するように証跡を更新する」を参照してください。

[CloudTrail.3] 少なくとも 1 つの CloudTrail 証跡を有効にする必要があります

関連する要件： NIST.800-171.r2 3.3.1、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7、PCI DSS v3.2.1/10.1、PCI DSS v3.2.1/10.2.1、PCI DSS v3.2.1/10.2.2、PCI DSS v3.2.1/10.2.3、PCI DSS v3.2.1/10.2.4、PCI v3.2.1/10.2.5、10.2.6PCI DSS v3.2.1/、10.3.1PCI v310.2.7.2.1/10.3.210.3.310.3.410.3.510.3.610.2.1

カテゴリ: 識別 > ログ記録

重要度: 高

リソースタイプ : `AWS::::Account`

AWS Config ルール : cloudtrail-enabled

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、 で AWS CloudTrail 証跡が有効になっているかどうかを確認します AWS アカウント。アカウントに少なくとも 1 つの CloudTrail 追跡が有効になっていない場合、コントロールは失敗します。

ただし、一部の AWS サービスでは、すべての APIsとイベントのログ記録が有効になっていません。CloudTrail 以外の監査追跡を追加で実装し、「CloudTrail のサポートされているサービスと統合」内の各サービスのドキュメントを確認してください。

修正

CloudTrail の使用を開始し、証跡を作成するには、AWS CloudTrail 「 ユーザーガイド」の「入門 AWS CloudTrail チュートリアル」を参照してください。

[PCI.CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります

関連する要件： CIS AWS Foundations Benchmark v1.2.0/2.2、CIS AWS Foundations Benchmark v1.4.0/3.2、CIS AWS Foundations Benchmark v3.0.0/3.2、NIST.800-53.r5 AU-9、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-7(1)、NIST.800-53.r5 SI-7(3)、NIST.800-53.r5 SI-7(7)10.5.2、NIST.800-171.r2 3.3.3.8、PCI DSS v3.2.1/10.5.5、PCI DSS v3.2.10.3.21

カテゴリ: データ保護 > データの整合性

重要度: 低

リソースタイプ : `AWS::CloudTrail::Trail`

AWS Config ルール : cloud-trail-log-file-validation-enabled

スケジュールタイプ : 定期的

パラメータ: なし

このコントロールは、CloudTrail 追跡でログファイルの整合性の検証が有効になっているかどうかをチェックします。

CloudTrail ログファイルの検証では、CloudTrail が Amazon S3 に書き込む各ログのハッシュを含むデジタル署名されたダイジェストファイルを作成します。これらのダイジェストファイルを使用して、CloudTrail がログを配信した後でログファイルが変更、削除、または変更されなかったかどうかを判断できます。

Security Hub では、すべての追跡でファイルの検証を有効にすることを推奨します。ログファイルの検証により、CloudTrail ログの追加の整合性チェックが提供されます。

修正

CloudTrail ログファイルの検証を有効にするには、「AWS CloudTrail ユーザーガイド」の「CloudTrail のログファイルの整合性検証を有効にする」を参照してください。

[CloudTrail.5] CloudTrail 追跡は Amazon CloudWatch Logs と統合する必要があります

関連する要件： PCI DSS v3.2.1/10.5.3、 CIS AWS Foundations Benchmark v1.2.0/2.4、 CIS AWS Foundations Benchmark v1.4.0/3.4、 NIST.800-53.r5 AC-2(4)、 NIST.800-53.r5 AC-4(26)、 NIST.800-53.r5 AC-6(9)、 NIST.800-53.r5 AU-10、 NIST.800-53.r5 AU-12、 NIST.800-53.r5 AU-2、 NIST.800-53.r5 AU-3、 NIST.800-53.r5 AU-6(1)、 NIST.800-53.r5 AU-6(3)、 NIST.800-53.r5

AU-6(4)、 NIST.800-53.r5 AU-6(5)、 NIST.800-53.r5 AU-7(1)、 NIST.800-53.r5 CA-7、 NIST.800-53.r5 SC-7(9)、 NIST.800-53.r5 SI-20、 NIST.800-53.r5 SI-3(8)、 NIST.800-53.r5 SI-4(20)、 NIST.800-53.r5 SI-4(5)、 NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 低

リソースタイプ : `AWS::CloudTrail::Trail`

AWS Config ルール : cloud-trail-cloud-watch-logs-enabled

スケジュールタイプ : 定期的

パラメータ: なし

このコントロールは、CloudWatch Logs にログを送信するように CloudTrail 追跡が設定されているかどうかをチェックします。追跡の `CloudWatchLogsLogGroupArn` プロパティが空の場合、コントロールは失敗します。

CloudTrail は、特定のアカウントで行われた AWS API コールを記録します。記録された情報には、以下が含まれます。

- API 発信者のアイデンティティ
- API コールの時刻
- API 発信者の送信元 IP アドレス
- リクエストパラメータ
- によって返されるレスポンス要素 AWS のサービス

CloudTrail はログファイルの保存と配信に Amazon S3 を使用します。長期分析のために、指定した S3 バケットの CloudTrail ログをキャプチャできます。リアルタイム分析を実行するには、CloudWatch Logs にログを送信するように CloudTrail を設定できます。

アカウント内のすべてのリージョンで有効になっている追跡では、CloudTrail はそれらすべてのリージョンからログファイルを CloudWatch Logs ロググループに送信します。

Security Hub では、CloudTrail ログを CloudWatch Logs に送信することを推奨します。この推奨事項は、アカウントアクティビティが確実にキャプチャおよびモニタリングされ、適切なアラームが出されることを確認する目的であることにご注意ください CloudWatch Logs を使用して、 でこれを

セットアップできます AWS のサービス。この推奨事項は、別のソリューションの使用を除外するものではありません。

CloudTrail ログを CloudWatch Logs に送信すると、ユーザー、API、リソース、および IP アドレスに基づいてリアルタイムおよび過去のアクティビティを簡単にログに記録できます。この方法を使用して、異常または機密性の高いアカウントアクティビティに対してアラームと通知を確立できます。

修正

CloudTrail を CloudWatch Logs と統合するには、「AWS CloudTrail ユーザーガイド」の「CloudWatch Logs へのイベントの送信」を参照してください。

[CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットが一般公開されていないことを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/2.3、CIS AWS Foundations Benchmark v1.4.0/3.3、PCI DSS v4.0.1/1.4.4

カテゴリ: 識別 > ログ記録

重要度: 非常事態

リソースタイプ : `AWS::S3::Bucket`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ: 定期的および変更がトリガーされた場合

パラメータ : なし

CloudTrail は、アカウント内で実行された API コールをすべて記録します。これらのログファイルは S3 バケットに保存されます。CIS では、CloudTrail が記録する S3 バケットに S3 バケットポリシーまたはアクセスコントロールリスト (ACL) を適用して、CloudTrail ログへのパブリックアクセスを禁止することを推奨しています。CloudTrail ログコンテンツへのパブリックアクセスを許可すると、攻撃者が感染したアカウントの使用または設定における弱点を特定する手助けとなる可能性があります。

このチェックを実行するために、Security Hub は最初にカスタムロジックを使用して、CloudTrail ログが保存されている S3 バケットを探します。次に、 AWS Config マネージドルールを使用して、バケットがパブリックにアクセス可能であることを確認します。

ログを単一の集中管理 S3 バケットに集約する場合、Security Hub は、集中管理された S3 バケットがあるアカウントとリージョンに対してのみチェックを実行します。他のアカウントとリージョンでは、コントロールステータスは [No data] (データなし) となります。

バケットがパブリックアクセス可能な場合、チェックにより結果 (失敗) が生成されます。

修正

CloudTrail S3 バケットへのパブリックアクセスをブロックするには、「Amazon Simple Storage Service ユーザーガイド」の「S3 バケットへのパブリックアクセスブロック設定の構成」を参照してください。4 つの Amazon S3 パブリックアクセスブロック設定をすべて選択します。

[CloudTrail.7] CloudTrail S3 バケットで、S3 バケットアクセスログ記録が有効であることを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/2.6、CIS AWS Foundations Benchmark v1.4.0/3.6、CIS AWS Foundations Benchmark v3.0.0/3.4、PCI DSS v4.0.1/10.2.1

カテゴリ: 識別 > ログ記録

重要度: 低

リソースタイプ : `AWS::S3::Bucket`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ : 定期的

パラメータ : なし

S3 バケットアクセスログ記録により、S3 バケットに対して行われたリクエストごとのアクセスレコードを含むログが生成されます。アクセスログレコードには、リクエストのタイプ、リクエストに指定されたリソース、リクエストが処理された日時など、リクエストの詳細が記録されます。

CIS では、CloudTrail S3 バケットでバケットアクセスログ記録を有効にすることを推奨しています。

ターゲット S3 バケットで S3 バケットのログ記録を有効にすることで、ターゲットバケット内のオブジェクトに影響を与える可能性のあるすべてのイベントをキャプチャできます。ログを別のバケットに配置するように設定すると、ログ情報にアクセスできるようになり、セキュリティおよびインシデント対応のワークフローで役立ちます。

このチェックを実行するために、Security Hub はまずカスタムロジックを使用して CloudTrail ログが保存されているバケットを検索し、次に AWS Config マネージドルールを使用してログ記録が有効になっているかどうかを確認します。

CloudTrail が複数の から 1 つの送信先 Amazon S3 バケット AWS アカウント にログファイルを配信する場合、Security Hub はこのコントロールが配置されているリージョンの送信先バケットに対してのみこのコントロールを評価します。これにより、結果が効率化されます。ただし、宛先バケットにログを配信するすべてのアカウントで CloudTrail を有効にする必要があります。宛先バケットを保持しているアカウントを除くすべてのアカウントの制御ステータスは「データなし」です。

修正

CloudTrail S3 バケットのサーバーアクセスのログ記録を有効にするには、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 サーバーアクセスログの有効化」を参照してください。

[CloudTrail.9] CloudTrail 証跡にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::CloudTrail::Trail`

AWS Config ルール: `tagged-cloudtrail-trail` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、 AWS CloudTrail 証跡にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。証跡にタグキーがない場合、またはパラメータ requiredTagKeys で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ requiredTagKeys が指定されていない場合、コントロールはタグキーの存在のみをチェックし、証跡にキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

CloudTrail 証跡にタグを追加するには、「AWS CloudTrail API リファレンス」の「AddTags」を参照してください。

[CloudTrail.10] CloudTrail Lake イベントデータストアはカスタマーマネージドで暗号化する必要があります AWS KMS keys

関連する要件： NIST.800-53.r5 AU-9、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-12(2)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::CloudTrail::EventDataStore`

AWS Config ルール : event-data-store-cmk-encryption-enabled

スケジュールタイプ : 定期的

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`kmsKeyArns`	評価 AWS KMS keys に含めるの Amazon リソースネーム (ARNs) のリスト。イベントデータストアがリスト内の KMS キーで暗号化されていない場合、コントロールは`FAILED`結果を生成します。	StringList (最大 3 項目)	既存の KMS キーの ARNs。例: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` 。	デフォルト値なし

このコントロールは、 AWS CloudTrail Lake イベントデータストアが保管時にカスタマーマネージドで暗号化されているかどうかを確認します AWS KMS key。イベントデータストアがカスタマーマネージド KMS キーで暗号化されていない場合、コントロールは失敗します。オプションで、評価に含めるコントロールの KMS キーのリストを指定できます。

デフォルトでは、 AWS CloudTrail Lake は AES-256 アルゴリズムを使用して Amazon S3 マネージドキー (SSE-S3) でイベントデータストアを暗号化します。追加の制御のために、代わりにカスタマーマネージド AWS KMS key (SSE-KMS) を使用してイベントデータストアを暗号化するように CloudTrail Lake を設定できます。カスタマーマネージド KMS キーは、 AWS KMS key で作成、所有、管理する です AWS アカウント。このタイプの KMS キーを完全に制御できます。これには、キーポリシーの定義と保守、許可の管理、暗号化マテリアルのローテーション、タグの割り当て、エ

イリアスの作成、キーの有効化と無効化が含まれます。CloudTrail データの暗号化オペレーションでカスタマーマネージド KMS キーを使用し、CloudTrail ログで使用状況を監査できます。

修正

指定した を使用して AWS CloudTrail Lake イベントデータストアを暗号化する方法については、AWS CloudTrail 「 ユーザーガイド」の AWS KMS key 「イベントデータストアを更新する」を参照してください。イベントデータストアを KMS キーに関連付けた後に、その KMS キーを削除または変更することはできません。

Amazon CloudWatch の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon CloudWatch サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[CloudWatch.1] 「ルート」ユーザーの使用に対するログメトリクスフィルターとアラームが存在する必要があります

関連する要件： CIS AWS Foundations Benchmark v1.2.0/1.1、CIS AWS Foundations Benchmark v1.2.0/3.3、CIS AWS Foundations Benchmark v1.4.0/1.7、CIS AWS Foundations Benchmark v1.4.0/4.3、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7、PCI DSS v3.2.1/7.2.1

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ : 定期的

パラメータ : なし

ルートユーザーは、 AWS アカウントのすべてのリソースとサービスに完全かつ無制限にアクセスできます。日常的なタスクにはルートユーザーを使用しないことが強く推奨されます。ルートユーザーの使用を最小限に抑え、アクセス管理の最小特権の原則を採用することで、偶発的な変更や高特権認証情報の意図しない開示のリスクが軽減されます。

ベストプラクティスは、アカウントおよびサービスの管理タスクを実行するときに必要となる場合のみ、ルートユーザー認証情報を使用することです。 AWS Identity and Access Management (IAM) ポリシーをグループとロールに直接適用しますが、ユーザーには適用しません。日常的に使用する管理者を設定する方法のチュートリアルについては、「IAM ユーザーガイド」の「最初の IAM 管理者のユーザーおよびグループの作成」を参照してください。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 1.7 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 追跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
> チェックの結果、以下の場合は結果 `FAILED` となります。
>
> - 追跡が設定されていません。
> - 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。
>
> チェックの結果、以下の場合はコントロール状況が `NO_DATA` になります。
>
> - マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
> - マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。
>
> 組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任管理者アカウントによってのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは `NO_DATA` になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者の

アカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、`ListSubscriptionsByTopic` を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての AWS リージョンに適用される CloudTrail 追跡を作成します。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 追跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon CloudWatch Logs ユーザーガイド」の「ロググループのメトリクスフィルターの作成」を参照してください。以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}`
メトリクス名前空間	**`LogMetrics`**
メトリクス値	**`1`**

フィールド	値
デフォルト値	**0**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon CloudWatch ユーザーガイド」の「ロググループメトリクスフィルターに基づいて CloudWatch アラームを作成する」を参照してください。 Amazon CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が以下の条件の場合 ...	以上
条件は...	**1**

[CloudWatch.2] 不正な API 呼び出しに対してログメトリクスフィルターとアラームが存在することを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.1、NIST.800-171.r2 3.13.1、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ : 定期的

パラメータ : なし

CloudTrail ログを CloudWatch Logs に転送し、対応するメトリクスフィルターとアラームを設定することにより、API コールのリアルタイムモニタリングを実行できます。

CIS では、不正な API コールのメトリクスフィルターとアラームを作成することをお勧めします。不正な API コールをモニタリングすることでアプリケーションエラーを明らかにし、悪意のあるアクティビティを検出するのにかかる時間を短縮できる可能性があります。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.2 のコントロール 3.1 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 追跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
> チェックの結果、以下の場合は結果 `FAILED` となります。
>
> - 追跡が設定されていません。
> - 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。
>
> チェックの結果、以下の場合はコントロール状況が `NO_DATA` になります。
>
> - マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
> - マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。
>
> 組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任管理者アカウントによってのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは `NO_DATA` になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、`ListSubscriptionsByTopic` を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての AWS リージョンに適用される CloudTrail 追跡を作成します。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 追跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon CloudWatch Logs ユーザーガイド」の「ロググループのメトリクスフィルターの作成」を参照してください。以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.errorCode="*UnauthorizedOperation") \|\| ($.errorCode="AccessDenied*")}`
メトリクス名前空間	**`LogMetrics`**
メトリクス値	**`1`**
デフォルト値	**`0`**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon CloudWatch ユーザーガイド」の「ロググループメトリクスフィルターに基づいて CloudWatch アラームを作成する」を参照してください。 Amazon CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が以下の条件の場合 ...	以上
条件は...	**1**

[CloudWatch.3] MFA を使用しないマネジメントコンソールサインインに対してログメトリクスフィルターとアラームが存在することを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.2

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ : 定期的

パラメータ : なし

CloudTrail ログを CloudWatch Logs に転送し、対応するメトリクスフィルターとアラームを設定することにより、API コールのリアルタイムモニタリングを実行できます。

CIS では、MFA で保護されていないコンソールログインに対するメトリクスフィルターとアラームを作成することを推奨しています。単一要素のコンソールログインをモニタリングすることにより、MFA によって保護されていないアカウントへの可視性が向上します。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.2 のコントロール 3.2 に規定された正確な監査ステップを実行しま

す。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 追跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
> チェックの結果、以下の場合は結果 `FAILED` となります。
>
> - 追跡が設定されていません。
> - 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。
>
> チェックの結果、以下の場合はコントロール状況が `NO_DATA` になります。
>
> - マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
> - マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。
>
> 組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任管理者アカウントによってのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは `NO_DATA` になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。
>
> アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、`ListSubscriptionsByTopic` を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての AWS リージョンに適用される CloudTrail 追跡を作成します。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 追跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon CloudWatch Logs ユーザーガイド」の「ロググループのメトリクスフィルターの作成」を参照してください。以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") && ($.userIdentity.type = "IAMUser") && ($.responseElements.ConsoleLogin = "Success") }`
メトリクス名前空間	**`LogMetrics`**
メトリクス値	**`1`**
デフォルト値	**`0`**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon CloudWatch ユーザーガイド」の「ロググループメトリクスフィルターに基づいて CloudWatch アラームを作成する」を参照してください。 Amazon CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が以下の条件の場合 ...	以上
条件は...	**1**

[CloudWatch.4] IAM ポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.4、CIS AWS Foundations Benchmark v1.4.0/4.4、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、CloudTrail ログを CloudWatch Logs に転送し、対応するメトリクスフィルターとアラームを設定することにより、API コールのリアルタイムモニタリングを実行するかどうかを確認します。

CIS では、IAM ポリシーに加えられた変更に対するメトリクスフィルターとアラームを作成することを推奨しています。これらの変更をモニタリングすることで、認証と認可の管理が損なわれないようにできます。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 追跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡であ

る可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
チェックの結果、以下の場合は結果 FAILED となります。

- 追跡が設定されていません。
- 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。

チェックの結果、以下の場合はコントロール状況が NO_DATA になります。

- マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

  組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任管理者アカウントによってのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは NO_DATA になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、ListSubscriptionsByTopic を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 WARNING を生成します。

修正

> **Note**
>
> これらの修復手順で推奨されるフィルターパターンは、CIS ガイダンスのフィルターパターンとは異なります。推奨フィルターは IAM API 呼び出しからのイベントのみを対象としています。

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての AWS リージョンに適用される CloudTrail 追跡を作成します。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 追跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon CloudWatch Logs ユーザーガイド」の「ロググループのメトリクスフィルターの作成」を参照してください。以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventSource=iam.amazonaws.com) && (($.eventName=DeleteGroupPolicy) || ($.eventName=DeleteRolePolicy) \|\| ($.eventName=DeleteUserPolicy) || ($.eventName=PutGroupPolicy) \|\| ($.eventName=PutRolePolicy) || ($.eventName=PutUserPolicy) \|\| ($.eventName=CreatePolicy) || ($.eventName=Delet`

フィールド	値
	`ePolicy) || ($.eventName=CreatePolicyVersion) \|\| ($.eventName=DeletePolicyVersion) || ($.eventName=AttachRolePolicy) \|\| ($.eventName=DetachRolePolicy) || ($.eventName=AttachUserPolicy) \|\| ($.eventName=DetachUserPolicy) || ($.eventName=AttachGroupPolicy) \|\| ($.eventName=DetachGroupPolicy))}`
メトリクス名前空間	**LogMetrics**
メトリクス値	**1**
デフォルト値	**0**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon CloudWatch ユーザーガイド」の「ロググループメトリクスフィルターに基づいて CloudWatch アラームを作成する」を参照してください。 Amazon CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が以下の条件の場合...	以上
条件は...	**1**

[CloudWatch.5] CloudTrail 設定変更のログメトリクスフィルターとアラームが存在することを確認する

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.5、CIS AWS Foundations Benchmark v1.4.0/4.5、NIST.800-171.r2 3.3.8、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ : 定期的

パラメータ : なし

CloudTrail ログを CloudWatch Logs に転送し、対応するメトリクスフィルターとアラームを設定することにより、API コールのリアルタイムモニタリングを実行できます。

CIS では、CloudTrail 構成設定の変更に対するメトリクスフィルターとアラームを作成することを推奨しています。これらの変更をモニタリングすることで、アカウント内のアクティビティを継続的に可視化できます。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 4.5 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 追跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
>
> チェックの結果、以下の場合は結果 `FAILED` となります。
>
> - 追跡が設定されていません。
> - 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。
>
> チェックの結果、以下の場合はコントロール状況が `NO_DATA` になります。

- マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

  組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任管理者アカウントによってのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは `NO_DATA` になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、`ListSubscriptionsByTopic` を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての AWS リージョンに適用される CloudTrail 追跡を作成します。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 追跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。

3. メトリクスのフィルターを作成します。手順については、「Amazon CloudWatch Logs ユーザーガイド」の「ロググループのメトリクスフィルターの作成」を参照してください。以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventName=CreateTrail) \|\| ($.eventName=UpdateTrail) || ($.eventName=DeleteTrail) \|\| ($.eventName=StartLogging) || ($.eventName=StopLogging)}`
メトリクス名前空間	**`LogMetrics`**
メトリクス値	**`1`**
デフォルト値	**`0`**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon CloudWatch ユーザーガイド」の「ロググループメトリクスフィルターに基づいて CloudWatch アラームを作成する」を参照してください。 Amazon CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
`your-metric-name` が以下の条件の場合 ...	以上
条件は...	**`1`**

[CloudWatch.6] AWS Management Console 認証失敗のログメトリクスフィルターとアラームが存在することを確認する

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.6、CIS AWS Foundations Benchmark v1.4.0/4.6、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ : 定期的

パラメータ : なし

CloudTrail ログを CloudWatch Logs に転送し、対応するメトリクスフィルターとアラームを設定することにより、API コールのリアルタイムモニタリングを実行できます。

CIS では、コンソール認証の試行の失敗に対するメトリクスフィルターとアラームを作成することを推奨しています。コンソールログインの失敗をモニタリングすることにより、認証情報へのブルートフォース攻撃の試行の検出にかかるリードタイムを短縮できる可能性があり、ソース IP などの、他のイベント相関で使用できるインジケータが得られる可能性もあります。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 4.6 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 追跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
>
> チェックの結果、以下の場合は結果 `FAILED` となります。
>
> - 追跡が設定されていません。
> - 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。
>
> チェックの結果、以下の場合はコントロール状況が `NO_DATA` になります。

- マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

  組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任管理者アカウントによってのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは `NO_DATA` になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、`ListSubscriptionsByTopic` を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての AWS リージョンに適用される CloudTrail 追跡を作成します。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 追跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。

3. メトリクスのフィルターを作成します。手順については、「Amazon CloudWatch Logs ユーザーガイド」の「ロググループのメトリクスフィルターの作成」を参照してください。以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventName=ConsoleLogin) && ($.errorMessage="Failed authentication")}`
メトリクス名前空間	**`LogMetrics`**
メトリクス値	**`1`**
デフォルト値	**`0`**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon CloudWatch ユーザーガイド」の「ロググループメトリクスフィルターに基づいて CloudWatch アラームを作成する」を参照してください。 Amazon CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
`your-metric-name` が以下の条件の場合 ...	以上
条件は...	**`1`**

[CloudWatch.7] カスタマーマネージドキーの無効化またはスケジュールされた削除に対するログメトリクスフィルターとアラームが存在することを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.7、CIS AWS Foundations Benchmark v1.4.0/4.7、NIST.800-171.r2 3.13.10、NIST.800-171.r2 3.13.16、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ:
`AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ : 定期的

パラメータ : なし

CloudTrail ログを CloudWatch Logs に転送し、対応するメトリクスフィルターとアラームを設定することにより、API コールのリアルタイムモニタリングを実行できます。

CIS では、状態が無効またはスケジュールされた削除に変更されたカスタマーマネージドキーに対するメトリクスフィルターとアラームを作成することを推奨しています。無効になっているか、または削除されたキーで暗号化されたデータには、アクセスできなくなります。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 4.7 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。`ExcludeManagementEventSources` が `kms.amazonaws.com` を含む場合も、コントロールは失敗します。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 追跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
> チェックの結果、以下の場合は結果 `FAILED` となります。
>
> - 追跡が設定されていません。
> - 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。
>
> チェックの結果、以下の場合はコントロール状況が `NO_DATA` になります。
>
> - マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。

- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

  組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任管理者アカウントによってのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは `NO_DATA` になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、`ListSubscriptionsByTopic` を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての AWS リージョンに適用される CloudTrail 追跡を作成します。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 追跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon CloudWatch Logs ユーザーガイド」の「ロググループのメトリクスフィルターの作成」を参照してください。以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventSource=kms.amazonaws.com) && (($.eventName=DisableKey) || ($.eventName=ScheduleKeyDeletion))}`
メトリクス名前空間	**LogMetrics**
メトリクス値	**1**
デフォルト値	**0**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon CloudWatch ユーザーガイド」の「ロググループメトリクスフィルターに基づいて CloudWatch アラームを作成する」を参照してください。 Amazon CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が以下の条件の場合...	以上
条件は...	**1**

[CloudWatch.8] S3 バケットポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.8、CIS AWS Foundations Benchmark v1.4.0/4.8、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ : 定期的

パラメータ : なし

CloudTrail ログを CloudWatch Logs に転送し、対応するメトリクスフィルターとアラームを設定することにより、API コールのリアルタイムモニタリングを実行できます。

CIS では、S3 バケットポリシーの変更に対するメトリクスフィルターとアラームを作成することを推奨しています。これらの変更をモニタリングすることで、機密性の高い S3 バケットの過剰な権限のあるポリシーを検出して修正するまでの時間を短縮できます。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 4.8 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 追跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
> チェックの結果、以下の場合は結果 `FAILED` となります。
>
> - 追跡が設定されていません。
> - 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。
>
> チェックの結果、以下の場合はコントロール状況が `NO_DATA` になります。
>
> - マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
> - マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。
>
> 組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管

理アカウントまたは CloudTrail 委任管理者アカウントによってのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは NO_DATA になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、ListSubscriptionsByTopic を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 WARNING を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての AWS リージョンに適用される CloudTrail 追跡を作成します。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 追跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon CloudWatch Logs ユーザーガイド」の「ロググループのメトリクスフィルターの作成」を参照してください。以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	{($.eventSource=s3.amazonaws.com) && (($.eventName=PutBucketAcl) || ($.eventName=PutBucketPolicy) \|\| ($.eventN

フィールド	値
	`ame=PutBucketCors) || ($.eventName=PutBucketLifecycle) \|\| ($.eventName=PutBucketReplication) || ($.eventName=DeleteBucketPolicy) \|\| ($.eventName=DeleteBucketCors) || ($.eventName=DeleteBucketLifecycle) \|\| ($.eventName=DeleteBucketReplication))}`
メトリクス名前空間	**`LogMetrics`**
メトリクス値	**`1`**
デフォルト値	**`0`**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon CloudWatch ユーザーガイド」の「ロググループメトリクスフィルターに基づいて CloudWatch アラームを作成する」を参照してください。 Amazon CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
`your-metric-name` が以下の条件の場合...	以上
条件は...	**`1`**

[CloudWatch.9] AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.9、CIS AWS Foundations Benchmark v1.4.0/4.9、NIST.800-171.r2 3.3.8、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ : 定期的

パラメータ : なし

CloudTrail ログを CloudWatch Logs に転送し、対応するメトリクスフィルターとアラームを設定することにより、API コールのリアルタイムモニタリングを実行できます。

CIS では、 AWS Config 構成設定の変更に対するメトリクスフィルターとアラームを作成することを推奨しています。これらの変更をモニタリングすることで、アカウント内の設定項目を継続的に可視化できます。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 4.9 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 追跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
> チェックの結果、以下の場合は結果 `FAILED` となります。
>
> - 追跡が設定されていません。
> - 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。
>
> チェックの結果、以下の場合はコントロール状況が `NO_DATA` になります。
>
> - マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。

- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

  組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任管理者アカウントによってのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは `NO_DATA` になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、`ListSubscriptionsByTopic` を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての AWS リージョンに適用される CloudTrail 追跡を作成します。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 追跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon CloudWatch Logs ユーザーガイド」の「ロググループのメトリクスフィルターの作成」を参照してください。以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventSource=config.amazonaws.com) && (($.eventName=StopConfigurationRecorder) || ($.eventName=DeleteDeliveryChannel) \|\| ($.eventName=PutDeliveryChannel) || ($.eventName=PutConfigurationRecorder))}`
メトリクス名前空間	**`LogMetrics`**
メトリクス値	**`1`**
デフォルト値	**`0`**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon CloudWatch ユーザーガイド」の「ロググループメトリクスフィルターに基づいて CloudWatch アラームを作成する」を参照してください。 Amazon CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
`your-metric-name` が以下の条件の場合...	以上
条件は...	**`1`**

[CloudWatch.10] セキュリティグループの変更に対するログメトリクスフィルターとアラームが存在することを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.10、CIS AWS Foundations Benchmark v1.4.0/4.10、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ : 定期的

パラメータ : なし

CloudTrail ログを CloudWatch Logs に転送し、対応するメトリクスフィルターとアラームを設定することにより、API コールのリアルタイムモニタリングを実行できます。セキュリティグループは、VPC の入力トラフィックと出力トラフィックを制御するステートフルパケットフィルターです。

CIS では、セキュリティグループの変更に対するメトリクスフィルターとアラームを作成することを推奨しています。これらの変更をモニタリングすることにより、リソースやサービスが意図せずに公開されないようにできます。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 4.10 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 追跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
>
> チェックの結果、以下の場合は結果 `FAILED` となります。
>
> - 追跡が設定されていません。
> - 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。
>
> チェックの結果、以下の場合はコントロール状況が `NO_DATA` になります。

- マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

  組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任管理者アカウントによってのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは `NO_DATA` になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、`ListSubscriptionsByTopic` を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての AWS リージョンに適用される CloudTrail 追跡を作成します。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 追跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。

3. メトリクスのフィルターを作成します。手順については、「Amazon CloudWatch Logs ユーザーガイド」の「ロググループのメトリクスフィルターの作成」を参照してください。以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventName=AuthorizeSecurityGroupIngress) \|\| ($.eventName=AuthorizeSecurityGroupEgress) || ($.eventName=RevokeSecurityGroupIngress) \|\| ($.eventName=RevokeSecurityGroupEgress) || ($.eventName=CreateSecurityGroup) \|\| ($.eventName=DeleteSecurityGroup)}`
メトリクス名前空間	**LogMetrics**
メトリクス値	**1**
デフォルト値	**0**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon CloudWatch ユーザーガイド」の「ロググループメトリクスフィルターに基づいて CloudWatch アラームを作成する」を参照してください。 Amazon CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が以下の条件の場合 ...	以上
条件は...	**1**

[CloudWatch.11] ネットワークアクセスコントロールリスト (NACL) への変更に対するログメトリクスフィルターとアラームが存在することを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.11、CIS AWS Foundations Benchmark v1.4.0/4.11、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ : 定期的

パラメータ : なし

CloudTrail ログを CloudWatch Logs に転送し、対応するメトリクスフィルターとアラームを設定することにより、API コールのリアルタイムモニタリングを実行できます。NACL は、VPC 内のサブネットの入力トラフィックと出力トラフィックを制御するためのステートレスパケットフィルターとして使用されます。

CIS では、NACL の変更に対するメトリクスフィルターとアラームを作成することを推奨しています。これらの変更をモニタリングすることで、 AWS リソースとサービスが意図せずに公開されないようにすることができます。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 4.11 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 追跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。

チェックの結果、以下の場合は結果 FAILED となります。

- 追跡が設定されていません。
- 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。

チェックの結果、以下の場合はコントロール状況が NO_DATA になります。

- マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

  組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任管理者アカウントによってのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは NO_DATA になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、ListSubscriptionsByTopic を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 WARNING を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。

2. すべての AWS リージョンに適用される CloudTrail 追跡を作成します。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 追跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。

3. メトリクスのフィルターを作成します。手順については、「Amazon CloudWatch Logs ユーザーガイド」の「ロググループのメトリクスフィルターの作成」を参照してください。以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventName=CreateNetworkAcl) \|\| ($.eventName=CreateNetworkAclEntry) || ($.eventName=DeleteNetworkAcl) \|\| ($.eventName=DeleteNetworkAclEntry) || ($.eventName=ReplaceNetworkAclEntry) \|\| ($.eventName=ReplaceNetworkAclAssociation)}`
メトリクス名前空間	**`LogMetrics`**
メトリクス値	**`1`**
デフォルト値	**`0`**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon CloudWatch ユーザーガイド」の「ロググループメトリクスフィルターに基づいて CloudWatch アラームを作成する」を参照してください。 Amazon CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
`your-metric-name` が以下の条件の場合 ...	以上

フィールド	値
条件は...	**1**

[CloudWatch.12] ネットワークゲートウェイへの変更に対するログメトリクスフィルターとアラームが存在することを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.12、CIS AWS Foundations Benchmark v1.4.0/4.12、NIST.800-171.r2 3.3.1、NIST.800-171.r2 3.13.1

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ : 定期的

パラメータ : なし

CloudTrail ログを CloudWatch Logs に転送し、対応するメトリクスフィルターとアラームを設定することにより、API コールのリアルタイムモニタリングを実行できます。ネットワークゲートウェイは、VPC の外部にある送信先との間でトラフィックを送受信する必要があります。

CIS では、ネットワークゲートウェイの変更に対するメトリクスフィルターとアラームを作成することを推奨しています。これらの変更をモニタリングすることにより、すべての入力トラフィックと出力トラフィックが制御されたパスを通じて VPC 境界を通過するようになります。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.2 のコントロール 4.12 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 追跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡であ

る可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
チェックの結果、以下の場合は結果 FAILED となります。

- 追跡が設定されていません。
- 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。

チェックの結果、以下の場合はコントロール状況が NO_DATA になります。

- マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

  組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任管理者アカウントによってのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは NO_DATA になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、ListSubscriptionsByTopic を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 WARNING を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS ア

ラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。

2. すべての AWS リージョンに適用される CloudTrail 追跡を作成します。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 追跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。

3. メトリクスのフィルターを作成します。手順については、「Amazon CloudWatch Logs ユーザーガイド」の「ロググループのメトリクスフィルターの作成」を参照してください。以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventName=CreateCustomerGateway) \|\| ($.eventName=DeleteCustomerGateway) || ($.eventName=AttachInternetGateway) \|\| ($.eventName=CreateInternetGateway) || ($.eventName=DeleteInternetGateway) \|\| ($.eventName=DetachInternetGateway)}`
メトリクス名前空間	**`LogMetrics`**
メトリクス値	**`1`**
デフォルト値	**`0`**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon CloudWatch ユーザーガイド」の「ロググループメトリクスフィルターに基づいて CloudWatch アラームを作成する」を参照してください。 Amazon CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的

フィールド	値
your-metric-name が以下の条件の場合 ...	以上
条件は...	**1**

[CloudWatch.13] ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.13、CIS AWS Foundations Benchmark v1.4.0/4.13、NIST.800-171.r2 3.3.1、NIST.800-171.r2 3.13.1、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、CloudTrail ログを CloudWatch Logs に転送し、対応するメトリクスフィルターとアラームを設定することにより、API コールのリアルタイムモニタリングを実行するかどうかを確認します。ルーティングテーブルは、サブネット間およびネットワークゲートウェイへのネットワークトラフィックをルーティングします。

CIS では、ルートテーブルの変更に対するメトリクスフィルターとアラームを作成することを推奨しています。これらの変更をモニタリングすることで、すべての VPC トラフィックが確実に想定どおりのパスを通過するようにできます。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 追跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡であ

る可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
チェックの結果、以下の場合は結果 FAILED となります。

- 追跡が設定されていません。
- 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。

チェックの結果、以下の場合はコントロール状況が NO_DATA になります。

- マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

  組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任管理者アカウントによってのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは NO_DATA になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、ListSubscriptionsByTopic を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 WARNING を生成します。

修正

> **Note**
>
> これらの修復手順で推奨されるフィルターパターンは、CIS ガイダンスのフィルターパターンとは異なります。推奨フィルターは Amazon Elastic Compute Cloud (EC2) 呼び出しからのイベントのみを対象としています。

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての AWS リージョンに適用される CloudTrail 追跡を作成します。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 追跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon CloudWatch Logs ユーザーガイド」の「ロググループのメトリクスフィルターの作成」を参照してください。以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventSource=ec2.amazonaws.com) && (($.eventName=CreateRoute) || ($.eventName=CreateRouteTable) \|\| ($.eventName=ReplaceRoute) || ($.eventName=ReplaceRouteTableAssociation) \|\| ($.eventName=DeleteRouteTable) || ($.eventName=DeleteRoute) \|\| ($.eventName=DisassociateRouteTable))}`

フィールド	値
メトリクス名前空間	**LogMetrics**
メトリクス値	**1**
デフォルト値	**0**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon CloudWatch ユーザーガイド」の「ロググループメトリクスフィルターに基づいて CloudWatch アラームを作成する」を参照してください。 Amazon CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
your-metric-name が以下の条件の場合 ...	以上
条件は...	**1**

[CloudWatch.14] VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/3.14、CIS AWS Foundations Benchmark v1.4.0/4.14、NIST.800-171.r2 3.3.1、NIST.800-171.r2 3.13.1、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ: `AWS::Logs::MetricFilter`、`AWS::CloudWatch::Alarm`、`AWS::CloudTrail::Trail`、`AWS::SNS`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ : 定期的

パラメータ : なし

CloudTrail ログを CloudWatch Logs に転送し、対応するメトリクスフィルターとアラームを設定することにより、API コールのリアルタイムモニタリングを実行できます。1 つのアカウントに複数の VPC を含めることができるのに加えて、2 つの VPC 間にピア接続を作成し、ネットワークトラフィックを VPC 間でルーティングすることができます。

CIS では、VPC の変更に対するメトリクスフィルターとアラームを作成することを推奨しています。これらの変更をモニタリングすることで、認証と認可の管理が損なわれないようにできます。

このチェックを実行するために、Security Hub はカスタムロジックを使用して、CIS AWS Foundations Benchmark v1.4.0 のコントロール 4.14 に規定された正確な監査ステップを実行します。CIS によって規定された正確なメトリクスフィルターが使用されていない場合、このコントロールは失敗します。追加のフィールドまたは用語をメトリクスフィルターに追加することはできません。

> **Note**
>
> Security Hub がこのコントロールのチェックを実行すると、現在のアカウントが使用する CloudTrail 追跡が検索されます。これらの追跡は、別のアカウントに属する組織の追跡である可能性があります。マルチリージョンの追跡は、別のリージョンに基づいている可能性もあります。
> チェックの結果、以下の場合は結果 `FAILED` となります。
>
> - 追跡が設定されていません。
> - 現在のリージョンにあり、現在のアカウントが所有している利用可能な追跡が、コントロール要件を満たしていません。
>
> チェックの結果、以下の場合はコントロール状況が `NO_DATA` になります。
>
> - マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
> - マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。
>
> 組織内の多数のアカウントからのイベントを記録するには、組織の証跡をお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任管理者アカウントによってのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは `NO_DATA` になります。メンバーアカウントでは、Security Hub はメンバー所有のリ

ソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

アラームの場合、現在のアカウントは、参照されている Amazon SNS トピックを所有しているか、`ListSubscriptionsByTopic` を呼び出すことで Amazon SNS トピックにアクセスできる必要があります。それ以外の場合は、Security Hub はコントロールに対して結果 `WARNING` を生成します。

修正

このコントロールに合格するには、以下の手順に従って Amazon SNS トピック、 AWS CloudTrail 追跡、メトリクスフィルター、メトリクスフィルターのアラームを作成します。

1. Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照してください。すべての CIS アラームを受信するトピックを作成し、そのトピックへのサブスクリプションを少なくとも 1 つ作成します。
2. すべての AWS リージョンに適用される CloudTrail 追跡を作成します。手順については、「AWS CloudTrail ユーザーガイド」の「証跡の作成」を参照してください。

   CloudTrail 追跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。次の手順で、そのロググループに対してメトリクスフィルターを作成します。
3. メトリクスのフィルターを作成します。手順については、「Amazon CloudWatch Logs ユーザーガイド」の「ロググループのメトリクスフィルターの作成」を参照してください。以下の値を使用します。

フィールド	値
定義パターン、フィルターパターン	`{($.eventName=CreateVpc) \|\| ($.eventName=DeleteVpc) || ($.eventName=ModifyVpcAttribute) \|\| ($.eventName=AcceptVpcPeeringConnection) || ($.eventName=CreateVpcPeeringConnection) \|\| ($.eventN`

フィールド	値
	`ame=DeleteVpcPeeringConnection) || ($.eventName=RejectVpcPeeringConnection) \|\| ($.eventName=AttachClassicLinkVpc) || ($.eventName=DetachClassicLinkVpc) \|\| ($.eventName=DisableVpcClassicLink) || ($.eventName=EnableVpcClassicLink)}`
メトリクス名前空間	**`LogMetrics`**
メトリクス値	**`1`**
デフォルト値	**`0`**

4. フィルターに基づいてアラームを作成します。手順については、「Amazon CloudWatch ユーザーガイド」の「ロググループメトリクスフィルターに基づいて CloudWatch アラームを作成する」を参照してください。 Amazon CloudWatch 以下の値を使用します。

フィールド	値
条件、しきい値タイプ	静的
`your-metric-name` が以下の条件の場合...	以上
条件は...	**`1`**

[CloudWatch.15] CloudWatch アラームには、指定されたアクションが設定されている必要があります

関連する要件： NIST.800-53.r5 AU-6(1)、NIST.800-53.r5 AU-6(5)、NIST.800-53.r5 CA-7、NIST.800-53.r5 IR-4(1)、NIST.800-53.r5 IR-4(5)、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-20、NIST.800-53.r5 SI-4(12)、NIST.800-1SI-471.r2 3.4、NIST7.800-1

カテゴリ: 検出 > 検出サービス

重要度: 高

リソースタイプ : `AWS::CloudWatch::Alarm`

AWS Config ルール： `cloudwatch-alarm-action-check`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`alarmActionRequired`	パラメータが `true` に設定されていて、アラームの状態が `ALARM` に変わるとアラームがアクションを起こす場合に、コントロールが `PASSED` 検出結果を生成します。	ブール値	カスタマイズ不可	`true`
`insufficientDataActionRequired`	パラメータが `true` に設定されていて、アラームの状態が `INSUFFICIENT_DATA` に変わるとアラームがアクションを起こす場合に、コントロールが `PASSED` 検出結果を生成します。	ブール値	`true` 、、または `false`	`false`
`okActionRequired`	パラメータが `true` に設定されていて、アラームの状態が `OK` に変わるとアラームがアクションを起こす場合に、コントロールが `PASSED` 検出結果を生成します。	ブール値	`true` 、、または `false`	`false`

このコントロールは、Amazon CloudWatch アラームに `ALARM` 状態に応じて設定されたアクションが 1 つ以上あるかどうかを確認します。`ALARM` 状態に対して設定されたアクションがア

ラームにない場合、コントロールは失敗します。必要に応じて、カスタムパラメータ値を含めて、INSUFFICIENT_DATA 状態または OK 状態のアラームアクションを要求することもできます。

> **Note**
>
> Security Hub は、CloudWatch メトリクスアラームに基づいてこのコントロールを評価します。メトリクスアラームは、指定されたアクションが設定された複合アラームの一部である場合があります。コントロールは、次の場合に FAILED 検出結果を生成します。
>
> - 指定されたアクションは、メトリクスアラーム用に設定されていません。
> - メトリクスアラームは、指定されたアクションが設定された複合アラームの一部です。

このコントロールは CloudWatch アラームでアラームアクションが設定されているかどうかに重点を置いていますが、CloudWatch.17 は CloudWatch アラームアクションのアクティベーションステータスに重点を置いています。

モニタリング対象のメトリクスが定義されたしきい値を超えると自動的に警告する CloudWatch アラームアクションを使用することをお勧めします。アラームをモニタリングすることで、異常なアクティビティを特定し、アラームが特定の状態になったときのセキュリティや運用上の問題に迅速に対応できます。アラームアクションの最も一般的なタイプは、Amazon Simple Notification Service (Amazon SNS) トピックにメッセージを送信して、1 人または複数のユーザーに通知することです。

修正

CloudWatch アラームでサポートされているアクションの詳細については、「Amazon CloudWatch ユーザーガイド」の「アラームアクション」を参照してください。

[CloudWatch.16] CloudWatch ロググループは指定した期間保持する必要があります

カテゴリ: 識別 > ログ記録

関連する要件: NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-11、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-12

重要度: 中

リソースタイプ : `AWS::Logs::LogGroup`

AWS Config ルール： `cw-loggroup-retention-period-check`

スケジュールタイプ : 定期的

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値	
`minRetentionTime`	CloudWatch ロググループの最小保持期間 (日数)	列挙型	`365, 400, 545, 731, 1827, 3653`	`365`	

このコントロールは、Amazon CloudWatch ロググループの保持期間が少なくとも指定された日数以上あるかどうかをチェックします。保持期間が指定された日数未満の場合、コントロールは失敗します。保持期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 365 日を使用します。

CloudWatch Logs は、すべてのシステム、アプリケーション、および からのログを 1 つの高度にスケーラブルなサービス AWS のサービス に一元化します。CloudWatch Logs を使用して、Amazon Elastic Compute Cloud (EC2) インスタンス、Amazon Route 53、およびその他のソースからログファイルをモニタリング AWS CloudTrail、保存、およびアクセスできます。ログを少なくとも 1 年間保存することで、ログ保持標準への準拠に役立ちます。

修正

ログ保持の設定については、「Amazon CloudWatch ユーザーガイド」の「CloudWatch Logs でログデータ保管期間を変更する」を参照してください。

[CloudWatch.17] CloudWatch アラームアクションをアクティブにする必要があります

カテゴリ: 検出 > 検出サービス

関連する要件: NIST.800-53.r5 AU-6(1)、NIST.800-53.r5 AU-6(5)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-4(12)

重要度: 高

リソースタイプ : `AWS::CloudWatch::Alarm`

AWS Config ルール： `cloudwatch-alarm-action-enabled-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、CloudWatch アラームアクションがアクティブになっているかどうかをチェックします (`ActionEnabled` を true に設定する必要があります)。CloudWatch アラームのアラームアクションが非アクティブ化されていると、コントロールは失敗します。

> **Note**
>
> Security Hub は、CloudWatch メトリクスアラームに基づいてこのコントロールを評価します。メトリクスアラームは、アラームアクションがアクティブ化された複合アラームの一部である場合があります。コントロールは、次の場合に `FAILED` 検出結果を生成します。
>
> - 指定されたアクションは、メトリクスアラーム用に設定されていません。
> - メトリクスアラームは、アラームアクションがアクティブ化された複合アラームの一部です。

このコントロールは CloudWatch アラームアクションのアクティベーションステータスに重点を置いていますが、CloudWatch.15 は CloudWatch アラームで `ALARM` アクションが設定されているかどうかに重点を置いています。

アラームアクションは、モニタリング対象のメトリクスが定義されたしきい値を超えると自動的に警告します。アラームアクションが非アクティブ化されている場合、アラームの状態が変わってもアクションは実行されず、モニタリング対象メトリクスの変更に関する警告は表示されません。セキュリティや運用上の問題に迅速に対応できるように、CloudWatch アラームアクションをアクティブにすることをお勧めします。

修正

CloudWatch アラームアクションを有効にアクティブにするには (コンソール)

1. CloudWatch コンソールの https://console.aws.amazon.com/cloudwatch/ を開いてください。
2. ナビゲーションペインの [アラーム] で、[すべてのアラーム] を選択します。
3. アクションをアクティブにするアラームを選択します。
4. [アクション] で、[アラームアクション — 新規] を選択し、[有効化] を選択します。

CloudWatch アラームアクションのアクティブ化の詳細については、[Amazon CloudWatch ユーザーガイド]の[アラームアクション]を参照してください。

CodeArtifact の Security Hub コントロール

これらの Security Hub コントロールは、 AWS CodeArtifact サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::CodeArtifact::Repository`

AWS Config ルール: `tagged-codeartifact-repository` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS CodeArtifact リポジトリにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。リポジトリにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、リポジトリにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

CodeArtifact リポジトリにタグを追加するには、「AWS CodeArtifact ユーザーガイド」の「CodeArtifact のリポジトリにタグを付ける」を参照してください。

CodeBuild の Security Hub コントロール

これらの Security Hub コントロールは、 AWS CodeBuild サービスとリソースを評価します。

これらのコントロールは、一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[CodeBuild.1] CodeBuild Bitbucket ソースリポジトリの URL には機密認証情報を含めないでください

関連する要件： NIST.800-53.r5 SA-3、PCI DSS v3.2.1/8.2.1、PCI DSS v4.0.1/8.3.2

カテゴリ: 保護 > セキュアな開発

重要度: 非常事態

リソースタイプ : `AWS::CodeBuild::Project`

AWS Config ルール : `codebuild-project-source-repo-url-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS CodeBuild プロジェクトの Bitbucket ソースリポジトリ URL に個人用アクセストークンが含まれているか、ユーザー名とパスワードが含まれているかをチェックします。コントロールは、Bitbucket のソースレポジトリの URL に、個人用のアクセストークンまたはユーザー名とパスワードが含まれているかどうかをチェックします。

> **Note**
>
> このコントロールは、CodeBuild ビルドプロジェクトのプライマリソースとセカンダリソースの両方を評価します。プロジェクトソースの詳細については、「AWS CodeBuild ユーザーガイド」の「複数の入力ソースと出力アーティファクトのサンプル」を参照してください。

サインイン認証情報は、クリアテキストで保存または送信したり、ソースリポジトリ URL に表示しないでください。個人用アクセストークンやサインイン認証情報の代わりに、CodeBuild のソースプロバイダーにアクセスし、Bitbucket リポジトリの場所へのパスのみを含むようにソースリポジトリ URL を変更する必要があります。個人用アクセストークンまたはサインイン認証情報を使用すると、意図しないデータ漏えいや不正アクセスに認証情報が公開される可能性があります。

修正

CodeBuild プロジェクトを更新することで OAuth を使用できます。

基本認証/(GitHub) 個人用のアクセストークンを CodeBuild プロジェクトソースから削除するには

1. CodeBuild コンソール (https://console.aws.amazon.com/codebuild/) を開きます。
2. 個人用のアクセストークンまたはユーザー名とパスワードを含むビルドプロジェクトを選択します。
3. [Edit] (編集) から、[Source] (ソース) を選択します。
4. [Disconnect from GitHub / Bitbucket] (GitHub/Bitbucket から切断) を選択します。
5. [Connect using OAuth] (OAuth を使用して接続する) を選択し、[Connect to GitHub / Bitbucket] (GitHub/Bitbucket に接続する) を選択します。
6. プロンプトが表示されたら、[authorize as appropriate] (必要に応じて認可)を選択します。

7. 必要に応じて、[Repository URL] (リポジトリ URL) と [additional configuration] (追加の設定) を再設定します。
8. [Update source] (ソースの更新) を選択します。

詳細については、「AWS CodeBuild ユーザーガイド」の「CodeBuild ユースケースベースのサンプル」を参照してください。

[CodeBuild.2] CodeBuild プロジェクト環境変数にクリアテキストの認証情報を含めることはできません

関連する要件： NIST.800-53.r5 IA-5(7)、NIST.800-53.r5 SA-3、PCI DSS v3.2.1/8.2.1、PCI DSS v4.0.1/8.3.2

カテゴリ: 保護 > セキュアな開発

重要度: 非常事態

リソースタイプ : `AWS::CodeBuild::Project`

AWS Config ルール : `codebuild-project-envvar-awscred-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、プロジェクトに環境変数 `AWS_ACCESS_KEY_ID` と `AWS_SECRET_ACCESS_KEY` が含まれているかどうかをチェックします。

認証情報 `AWS_ACCESS_KEY_ID` および `AWS_SECRET_ACCESS_KEY` はクリアテキストで保存しないでください。これは、意図しないデータ漏えいや不正アクセスに認証情報が公開される可能性があるためです。

修正

CodeBuild プロジェクトから環境変数を削除するには、「AWS CodeBuild ユーザーガイド」の「AWS CodeBuildでのビルドプロジェクトの設定の変更」を参照してください。[環境変数] に何も選択されていないことを確認します。

機密値を持つ環境変数を Parameter Store AWS Systems Manager または に保存し AWS Secrets Manager 、ビルド仕様から取得できます。手順については、「AWS CodeBuild ユーザーガイド」の「環境」セクションで、「重要」ラベルの付いたボックスを参照してください。

[CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります

関連する要件： NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)、PCI DSS v4.0.1/10.3.2

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 低

リソースタイプ : `AWS::CodeBuild::Project`

AWS Config ルール : `codebuild-project-s3-logs-encrypted`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS CodeBuild プロジェクトの Amazon S3 ログが暗号化されているかどうかを確認します。CodeBuild プロジェクトの S3 ログの暗号化が無効になっていると、コントロールは失敗します。

保管中のデータの暗号化は、データ周辺にアクセス管理のレイヤーを追加するために推奨されるベストプラクティスです。保管中のログを暗号化すると、 によって認証されていないユーザーがディスクに保存されているデータにアクセスするリスクが軽減 AWS されます。権限のないユーザーがデータにアクセスできる能力を制限するための一連のアクセスコントロールが追加されます。

修正

CodeBuild プロジェクトの S3 ログの暗号化設定を変更するには、「AWS CodeBuild ユーザーガイド」の「AWS CodeBuildでのビルドプロジェクトの設定の変更」を参照してください。

[CodeBuild.4] CodeBuild AWS Configプロジェクト環境にはログ記録設定が必要です

関連する要件: NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 AU-9(7)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::CodeBuild::Project`

AWS Config ルール : `codebuild-project-logging-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、CodeBuild プロジェクト環境で S3 または CloudWatch ログが有効になっているログオプションが、少なくとも 1 つあるかどうかをチェックします。CodeBuild プロジェクト環境で少なくとも 1 つのログオプションが有効になっていない場合は、このコントロールは失敗します。

セキュリティの観点から、ログ記録はセキュリティインシデントが発生した場合に、将来的に証拠の取り組みを可能にするために重要な機能です。CodeBuild プロジェクトの異常を脅威検出と関連付けることで、これらの脅威検出の精度に対する信頼性を高めることができます。

修正

CodeBuild プロジェクトログの設定方法の詳細については、「CodeBuild ユーザーガイド」の「ビルドプロジェクトの作成 (コンソール)」を参照してください。

[CodeBuild.5] CodeBuild プロジェクト環境では特権モードを有効にしないでください

> **Important**
>
> Security Hub は、2024 年 4 月にこのコントロールを廃止しました。詳細については、「Security Hub CSPM コントロールの変更ログ」を参照してください。

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(10)、NIST.800-53.r5 AC-6(2)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 高

リソースタイプ : `AWS::CodeBuild::Project`

AWS Config ルール : `codebuild-project-environment-privileged-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS CodeBuild プロジェクト環境で特権モードが有効か無効かをチェックします。コントロールは、CodeBuild プロジェクト環境で特権モードが有効な場合は失敗します。

デフォルトでは、Docker コンテナはどのデバイスにもアクセスを許可できません。権限モードは、ビルドプロジェクトの Docker コンテナにすべてのデバイスへのアクセスを許可します。Docker コンテナ内で Docker デーモンの実行を許可するには、`privilegedMode` に `true` の値を設定します。Docker デーモンは、Docker API リクエストをリッスンし、イメージ、コンテナ、ネットワーク、ボリュームなどの Docker オブジェクトを管理します。このパラメータは、ビルドプロジェクトを使用して Docker イメージをビルドする場合にのみ、true に設定する必要があります。それ以外の場合、Docker API およびコンテナの基盤となるハードウェアへの意図しないアクセスを防ぐため、この設定を無効にする必要があります。`privilegedMode` を `false` に設定すると、重要なリソースを改ざんや削除から保護するのに役立ちます。

修正

CodeBuild プロジェクト環境設定を設定するには、「CodeBuild ユーザーガイド」の「ビルドプロジェクトの作成 (コンソール)」を参照してください。[環境] セクションでは、[特権付与] 設定を選択しないでください。

[CodeBuild.7] CodeBuild レポートグループのエクスポートは保管時に暗号化する必要があります

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::CodeBuild::ReportGroup`

AWS Config ルール : `codebuild-report-group-encrypted-at-rest`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon Simple Storage Service (Amazon S3) バケットにエクスポートされた AWS CodeBuild レポートグループのテスト結果が保管中に暗号化されているかどうかを確認します。レポートグループのエクスポートが保管時に暗号化されていない場合、コントロールは失敗します。

保管中のデータとは、永続的な不揮発性ストレージに任意の期間保管されているデータを指します。保管中のデータを暗号化すると、その機密性が保護され、権限のないユーザーがアクセスするリスクが低減されます。

修正

S3 へのレポートグループのエクスポートを暗号化するには、「AWS CodeBuild ユーザーガイド」の「レポートグループの更新」を参照してください。

Amazon CodeGuru Profiler の Security Hub コントロール

これらの Security Hub コントロールは、Amazon CodeGuru Profiler サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::CodeGuruProfiler::ProfilingGroup`

AWS Config ルール : `codeguruprofiler-profiling-group-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon CodeGuru Profiler プロファイリンググループにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。プロファイリンググループにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、

コントロールは失敗しますrequiredKeyTags。パラメータ が指定されていない場合、コントロールrequiredKeyTagsはタグキーの存在のみをチェックし、プロファイリンググループにキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

CodeGuru Profiler プロファイリンググループにタグを追加するには、「Amazon CodeGuru Profiler ユーザーガイド」の「プロファイリンググループのタグ付け」を参照してください。 CodeGuru

Amazon CodeGuru Reviewer の Security Hub コントロール

これらの Security Hub コントロールは、Amazon CodeGuru Reviewer サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::CodeGuruReviewer::RepositoryAssociation`

AWS Config ルール : `codegururevieweer-repository-association-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon CodeGuru Reviewer リポジトリの関連付けに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。リポジトリの関連付けにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、リポジトリの関連付けにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

CodeGuru Reviewer リポジトリの関連付けにタグを追加するには、「Amazon CodeGuru Reviewer ユーザーガイド」の「リポジトリの関連付けのタグ付け」を参照してください。

Amazon Cognito の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon Cognito サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::Cognito::UserPool`

AWS Config ルール : cognito-user-pool-advanced-security-enabled

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`SecurityMode`	コントロールがチェックする脅威保護の適用モード。	String	`AUDIT`, `ENFORCED`	`ENFORCED`

このコントロールは、Amazon Cognito ユーザープールで脅威保護が有効になっているかどうかをチェックし、エンフォースメントモードを標準認証の完全な 関数に設定します。ユーザープールで脅威保護が無効になっている場合、または標準認証の強制モードがフル関数に設定されていない場合、コントロールは失敗します。カスタムパラメータ値を指定しない限り、Security Hub はエンフォースメントモード`ENFORCED`のデフォルト値を標準認証の完全な関数に設定します。

Amazon Cognito ユーザープールを作成したら、脅威保護をアクティブ化し、さまざまなリスクに応じて実行されるアクションをカスタマイズできます。または、監査モードを使用して、セキュリティ緩和策を適用せずに、検出されたリスクに関するメトリクスを収集することもできます。監査モードでは、脅威保護はメトリクスを Amazon CloudWatch に発行します。Amazon Cognito が最初のイベントを生成した後、メトリクスを表示できます。

修正

Amazon Cognito ユーザープールの脅威保護のアクティブ化については、Amazon Cognito デベロッパーガイド」の「脅威保護を使用した高度なセキュリティ」を参照してください。

[Cognito.2] Cognito ID プールは認証されていない ID を許可しないでください

カテゴリ: 保護 > セキュアなアクセス管理 > パスワードレス認証

重要度: 中

リソースタイプ : `AWS::Cognito::IdentityPool`

AWS Config ルール : cognito-identity-pool-unauth-access-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon Cognito ID プールが認証されていない ID を許可するように設定されているかどうかをチェックします。ID プールのゲストアクセスがアクティブ化されている場合 (`AllowUnauthenticatedIdentities`パラメータが に設定されている場合`true`) 、コントロールは失敗します。

Amazon Cognito ID プールで認証されていない ID が許可されている場合、ID プールは ID プロバイダー (ゲスト) を介して認証されていないユーザーに一時的な AWS 認証情報を提供します。これにより、 AWS リソースへの匿名アクセスが許可されるため、セキュリティリスクが発生します。ゲストアクセスを非アクティブ化すると、適切に認証されたユーザーのみが AWS リソースにアクセスできるため、不正アクセスや潜在的なセキュリティ違反のリスクが軽減されます。ベストプラクティスとして、ID プールでは、サポートされている ID プロバイダーによる認証が必要です。認証されてい

ないアクセスが必要な場合は、認証されていない ID のアクセス許可を慎重に制限し、その使用状況を定期的に確認およびモニタリングすることが重要です。

修正

Amazon Cognito ID プールのゲストアクセスを無効にする方法については、Amazon Cognito デベロッパーガイド」の「ゲストアクセスをアクティブ化または非アクティブ化する」を参照してください。

の Security Hub コントロール AWS Config

これらの Security Hub コントロールは、 AWS Config サービスとリソースを評価します。

これらのコントロールは、一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Config.1] を有効にし、サービスにリンクされたロールをリソース記録に使用 AWS Config する必要があります

関連する要件： CIS AWS Foundations Benchmark v1.2.0/2.5、CIS AWS Foundations Benchmark v1.4.0/3.5、CIS AWS Foundations Benchmark v3.0.0/3.3、NIST.800-53.r5 CM-3、NIST.800-53.r5 CM-6(1)、NIST.800-53.r5 CM-8、NIST.800-53.r5 CM-8(2)、PCI DSS v3.2.1/10.5.2、PCI DSS v3.2.1/11.5

カテゴリ: 識別 > インベントリ

重要度: 非常事態

リソースタイプ : `AWS::::Account`

AWS Config ルール： なし (カスタム Security Hub ルール)

スケジュールタイプ : 定期的

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`includeConfigServi`	パラメータが に設定されている場合、コントロールはがサービスにリンクされた	ブール値	`true` 、、または `false`	`true`

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`ceLinkedRoleCheck`	ロール AWS Config を使用するかどうかを評価しませんfalse。			

このコントロール AWS Config は、現在の のアカウントで が有効になっているかどうかをチェックし AWS リージョン、現在のリージョンで有効になっているコントロールに対応するすべてのリソースを記録し、サービスにリンクされた AWS Config ロールを使用します。サービスにリンクされたロールの名前は、AWSServiceRoleForConfig です。サービスにリンクされたロールを使用せず、`includeConfigServiceLinkedRoleCheck`パラメータを に設定しない場合`false`、他のロールには AWS Config がリソースを正確に記録するために必要なアクセス許可がないため、コントロールは失敗します。

この AWS Config サービスは、アカウントでサポートされている AWS リソースの設定管理を実行し、ログファイルをユーザーに配信します。記録された情報には、設定項目 (AWS リソース) 、設定項目間の関係、リソース内の設定変更が含まれます。グローバルリソースは、どのリージョンでも利用できるリソースです。

コントロールは次のように評価されます。

- 現在のリージョンが集約リージョンとして設定されている場合、コントロールは AWS Identity and Access Management (IAM) グローバルリソースが記録されている場合にのみ`PASSED`結果を生成します (それらを必要とするコントロールを有効にしている場合) 。
- 現在のリージョンがリンクされたリージョンとして設定されている場合、コントロールは IAM グローバルリソースが記録されているかどうかを評価しません。
- 現在のリージョンがアグリゲータにない場合、またはクロスリージョン集約がアカウントで設定されていない場合、コントロールは IAM グローバルリソースが記録されている (それらを必要とするコントロールを有効にしている場合) 場合にのみ `PASSED` 検出結果を生成します。

コントロールの結果は、 AWS Configでリソースの状態の変化を毎日記録するか、継続的に記録するかにかかわらず、影響を受けません。ただし、新しいコントロールの自動有効化を設定している場合、または新しいコントロールを自動的に有効にする中央設定ポリシーがある場合、新しいコントロールがリリースされると、このコントロールの結果が変わる可能性があります。このような場合、

すべてのリソースを記録しない場合は、PASSED 検出結果を受け取るために新しいコントロールに関連付けられているリソースの記録を設定する必要があります。

Security Hub セキュリティチェックは、すべてのリージョン AWS Config で を有効にし、それを必要とするコントロールのリソース記録を設定する場合にのみ、意図したとおりに機能します。

> **Note**
>
> Config.1 では AWS Config 、Security Hub を使用するすべてのリージョンで が有効になっている必要があります。
> Security Hub はリージョナルサービスであるため、このコントロールに対して実行されるチェックでは、アカウントの現在のリージョンのみが評価されます。
> グローバルリソースに対するセキュリティチェックをリージョンで許可するには、そのリージョン内の IAM グローバルリソースを記録する必要があります。IAM グローバルリソースが記録されていないリージョンには、IAM グローバルリソースをチェックするコントロールのデフォルトの PASSED 検出結果が送信されます。IAM グローバルリソースは 間で同じであるため AWS リージョン、IAM グローバルリソースはホームリージョンのみに記録することをお勧めします (クロスリージョン集約がアカウントで有効になっている場合) 。IAM リソースはグローバルリソース記録が有効になっているリージョンでのみ記録されます。
> AWS Config がサポートする IAM グローバルに記録されたリソースタイプは、IAM ユーザー、グループ、ロール、カスタマー管理ポリシーです。グローバルリソースの記録がオフになっているリージョンでは、これらのリソースタイプをチェックする Security Hub コントロールを無効にすることをお勧めします。詳細については、「Security Hub CSPM で無効にする推奨コントロール」を参照してください。

修正

ホームリージョンとアグリゲータの一部ではないリージョンでは、IAM グローバルリソースを必要とするコントロールを有効にしている場合は、IAM グローバルリソースを含め、現在のリージョンで有効になっているコントロールに必要なすべてのリソースを記録します。

リンクされたリージョンでは、現在のリージョンで有効になっているコントロールに対応するすべてのリソースを記録する限り、任意の記録 AWS Config モードを使用できます。リンクされたリージョンで、IAM グローバルリソースの記録を必要とするコントロールを有効にしている場合、FAILED検出結果を受け取ることはできません (他のリソースの記録で十分です) 。

検出結果の `Compliance` オブジェクトの `StatusReasons`フィールドは、このコントロールの検出結果に失敗した理由を特定するのに役立ちます。詳細については、「コントロールの検出結果のコンプライアンスの詳細」を参照してください。

コントロールごとに記録する必要があるリソースのリストについては、「コントロールの検出結果に必要な AWS Config リソース」を参照してください。リソース記録の有効化 AWS Config と設定に関する一般的な情報については、「」を参照してくださいSecurity Hub CSPM AWS Config の有効化と設定。

Amazon Connect の Security Hub コントロール

これらの Security Hub コントロールは、Amazon Connect サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::CustomerProfiles::ObjectType`

AWS Config ルール : `customerprofiles-object-type-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon Connect Customer Profiles オブジェクトタイプにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredKeyTags。オブジェクトタイプにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredKeyTags。パラメータが指定されていない場合、コントロールrequiredKeyTagsはタグキーの存在のみをチェックし、オブジェクトタイプにキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

Customer Profiles オブジェクトタイプにタグを追加するには、Amazon Connect 管理者ガイド」の「Amazon Connect のリソースにタグを追加する」を参照してください。 Amazon Connect

[Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::Connect::Instance`

AWS Config ルール： connect-instance-logging-enabled

スケジュールタイプ : 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon Connect インスタンスがフローログを生成して Amazon CloudWatch ロググループに保存するように構成されているかどうかをチェックします。Amazon Connect インスタンスが CloudWatch ロググループにフローログを生成して保存するように設定されていない場合、コントロールは失敗します。

Amazon Connect フローログは、Amazon Connect フローのイベントに関するリアルタイムの詳細を提供します。フローは、Amazon Connect コンタクトセンターでのカスタマーエクスペリエンスを最初から最後まで定義します。デフォルトでは、新しい Amazon Connect インスタンスを作成すると、インスタンスのフローログを保存するために Amazon CloudWatch ロググループが自動的に作成されます。フローログは、フローの分析、エラーの検索、運用メトリクスのモニタリングに役立ちます。フローで発生する可能性のある特定のイベントのアラートを設定することもできます。

修正

Amazon Connect インスタンスのフローログを有効にする方法については、Amazon Connect 管理者ガイド」のAmazon CloudWatch ロググループの Amazon Connect フローログを有効にする」を参照してください。 Amazon Connect

Amazon Data Firehose の Security Hub コントロール

これらの Security Hub コントロールは、Amazon Data Firehose サービスとリソースを評価します。

これらのコントロールは、一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります

関連する要件: NIST.800-53.r5 AC-3、NIST.800-53.r5 AU-3、NIST.800-53.r5 SC-12、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::KinesisFirehose::DeliveryStream`

AWS Config ルール : `kinesis-firehose-delivery-stream-encrypted`

スケジュールタイプ: 定期的

パラメータ : なし

このコントロールは、Amazon Data Firehose 配信ストリームが保管中にサーバー側の暗号化を使用して暗号化されているかどうかをチェックします。Firehose 配信ストリームが、保管中にサーバー側の暗号化を使用して暗号化されていない場合、このコントロールは失敗します。

サーバー側の暗号化は、Amazon Data Firehose 配信ストリームの機能であり、 AWS Key Management Service () で作成されたキーを使用して、保管中のデータを自動的に暗号化しますAWS KMS。データは、Data Firehose ストリームストレージレイヤーに書き込まれる前に暗号化され、ストレージから取得された後で復号されます。これにより、厳格な規制要件に準拠し、データのセキュリティを強化することが可能になります。

修正

Firehose 配信ストリームでサーバー側の暗号化を有効にするには、「Amazon Data Firehose デベロッパーガイド」の「Amazon Data Firehose でのデータ保護」を参照してください。

の Security Hub コントロール AWS DataSync

これらの Security Hub コントロールは、 AWS DataSync サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[DataSync.1] DataSync タスクではログ記録が有効になっている必要があります

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::DataSync::Task`

AWS Config ルール : datasync-task-logging-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS DataSync タスクでログ記録が有効になっているかどうかを確認します。タスクでログ記録が有効になっていない場合、コントロールは失敗します。

監査ログは、システムアクティビティを追跡およびモニタリングします。これらは、セキュリティ違反の検出、インシデントの調査、規制の遵守に役立つイベントの記録を提供します。監査ログは、組織の全体的な説明責任と透明性も強化します。

修正

AWS DataSync タスクのログ記録の設定については、「 AWS DataSync ユーザーガイド」のAmazon CloudWatch Logs によるデータ転送のモニタリング」を参照してください。

[DataSync.2] DataSync タスクにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::DataSync::Task`

AWS Config ルール : datasync-task-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS DataSync タスクに `requiredKeyTags`パラメータで指定されたタグキーがあるかどうかをチェックします。タスクにタグキーがない場合、または `requiredKeyTags`パラメータで指定されたすべてのキーがない場合、コントロールは失敗します。`requiredKeyTags` パラメータの値を指定しない場合、コントロールはタグキーの存在のみを

チェックし、タスクにタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、`aws:`プレフィックスが付いています。

タグは、 AWS リソースを作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの特定、整理、検索、フィルタリングに役立ちます。また、アクションと通知のリソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセスコントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 Tagging AWS Resources and Tag Editor User Guide」を参照してください。

> **Note**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

AWS DataSync タスクにタグを追加する方法については、AWS DataSync 「 ユーザーガイド」の AWS DataSync 「タスクのタグ付け」を参照してください。

Amazon Detective の Security Hub コントロール

この AWS Security Hub コントロールは、Amazon Detective サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Detective.1] 検出動作グラフにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Detective::Graph`

AWS Config ルール: `tagged-detective-graph` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、Amazon Detective 動作グラフにパラメータ `requiredTagKeys` で定義された特定のキーを含むタグがあるかどうかをチェックします。動作グラフにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、動作グラフにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、のAWS 「リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Detective 動作グラフにタグを追加するには、「Amazon Detective 管理ガイド」の「動作グラフにタグを追加する」を参照してください。

の Security Hub コントロール AWS DMS

これらの Security Hub コントロールは、 AWS Database Migration Service （ AWS DMS) サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります

関連する要件： NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)NIST.800-53.r5 SC-7NIST.800-53.r5 SC-75 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-73

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 非常事態

リソースタイプ : `AWS::DMS::ReplicationInstance`

AWS Config ルール : `dms-replication-not-public`

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、 AWS DMS レプリケーションインスタンスがパブリックかどうかをチェックします。これを行うために、`PubliclyAccessible` フィールドの値を調査します。

プライベートレプリケーションインスタンスには、レプリケーションネットワーク外からアクセスできないプライベート IP アドレスがあります。ソースデータベースとターゲットデータベースが同じネットワーク内にある場合、レプリケーションインスタンスにはプライベート IP アドレスが必要です。ネットワークは、VPN、 AWS Direct Connect、または VPC ピアリングを使用してレプリケーションインスタンスの VPC にも接続する必要があります。パブリックおよびプライベートレプリ

ケーションインスタンスの詳細については、「AWS Database Migration Service ユーザーガイド」の「パブリックおよびプライベートレプリケーションインスタンス」を参照してください。

また、 AWS DMS インスタンス設定へのアクセスが承認されたユーザーのみに制限されていることを確認する必要があります。これを行うには、ユーザーの IAM アクセス許可を制限して、 AWS DMS 設定とリソースを変更します。

修正

DMS レプリケーションインスタンスのパブリックアクセス設定は、作成後に変更できません。パブリックアクセス設定を変更するには、現在のインスタンスを削除してから再作成します。[パブリックアクセス可能] オプションは選択しないでください。

[DMS.2] DMS 証明書にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::DMS::Certificate`

AWS Config ルール: `tagged-dms-certificate` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、 AWS DMS 証明書にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。証明書にタグキーがない場合、またはパラメータ

`requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、証明書にキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

DMS 証明書にタグを追加するには、「AWS Database Migration Service ユーザーガイド」の「AWS Database Migration Serviceのリソースのタグ付け」を参照してください。

[DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::DMS::EventSubscription`

AWS Config ルール: `tagged-dms-eventsubscription` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、 AWS DMS イベントサブスクリプションにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。イベントサブスクリプションにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、イベントサブスクリプションにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

DMS イベントサブスクリプションにタグを追加するには、「AWS Database Migration Service ユーザーガイド」の「AWS Database Migration Serviceのリソースのタグ付け」を参照してください。

[DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::DMS::ReplicationInstance`

AWS Config ルール: `tagged-dms-replicationinstance` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、レ AWS DMS プリケーションインスタンスにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。レプリケーションインスタンスにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、レプリケーションインスタンスにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセ

ス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

DMS レプリケーションインスタンスにタグを追加するには、「AWS Database Migration Service ユーザーガイド」の「AWS Database Migration Serviceのリソースのタグ付け」を参照してください。

[DMS.5] DMS レプリケーションサブネットグループにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::DMS::ReplicationSubnetGroup`

AWS Config ルール: `tagged-dms-replicationsubnetgroup` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタ	StringList (最大 6 項目)	AWS 要件を満たす 1 ~	`No default value`

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	グキーのリスト。タグキーでは、大文字と小文字が区別されます。		6 個のタグキー。	

このコントロールは、 AWS DMS レプリケーションサブネットグループにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。レプリケーションサブネットグループにタグキーがない場合、またはパラメータ requiredTagKeys で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ requiredTagKeys が指定されていない場合、コントロールはタグキーの存在のみをチェックし、レプリケーションサブネットグループにキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

DMS レプリケーションサブネットグループにタグを追加するには、「AWS Database Migration Service ユーザーガイド」の「AWS Database Migration Serviceのリソースのタグ付け」を参照してください。

[DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。

関連する要件： NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、PCI DSS v4.0.1/6.3.3

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 中

リソースタイプ : `AWS::DMS::ReplicationInstance`

AWS Config ルール : `dms-auto-minor-version-upgrade-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS DMS レプリケーションインスタンスで自動マイナーバージョンアップグレードが有効になっているかどうかを確認します。このコントロールは、DMS レプリケーションインスタンスのマイナーバージョンの自動アップグレードが有効になっているかどうかを確認します。

DMS は、サポートされている各レプリケーションエンジンに自動的にマイナーバージョンアップグレードを行うため、レプリケーションインスタンスを最新の状態に保つことができます。マイナーバージョンには、ソフトウェアの新機能、バグ修正、セキュリティパッチ、およびパフォーマンスの向上を含む可能性があります。DMS レプリケーションインスタンスでマイナーバージョン自動アップグレードを有効にすると、マイナーアップグレードはメンテナンス期間中に自動的に適用され、[変更を今すぐ適用] オプションが選択されている場合はすぐに適用されます。

修正

DMS レプリケーションインスタンスのマイナーバージョン自動アップグレードを有効にするには、「AWS Database Migration Service ユーザーガイド」の「レプリケーションインスタンスの変更」を参照してください。

[DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。

関連する要件： NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.8AU-600-53.r5 CA-7、NIST.800-53.r5 SC-7(9) SI-3 SI-4 SI-710.4.2

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::DMS::ReplicationTask`

AWS Config ルール : `dms-replication-task-targetdb-logging`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、DMS レプリケーションタスク `TARGET_APPLY` および `TARGET_LOAD` の `LOGGER_SEVERITY_DEFAULT` の最小重要度レベルでログ記録が有効になっているかどうかを確認します。これらのタスクでロギングが有効になっていない場合や、最小重大度レベルが `LOGGER_SEVERITY_DEFAULT` よりも低い場合、コントロールは失敗します。

DMS は、移行プロセス中に Amazon CloudWatch を使用して情報をログ記録します。ロギングタスク設定を使用して、ログ記録するコンポーネントアクティビティとログに記録する情報量を指定できます。次のタスクにはロギングを指定する必要があります。

- `TARGET_APPLY` - データおよびデータ定義言語 (DDL) ステートメントがターゲットデータベースに適用されます。
- `TARGET_LOAD` — データはターゲットデータベースにロードされます。

ロギングは、モニタリング、トラブルシューティング、監査、パフォーマンス分析、エラー検出、リカバリのほか、履歴分析やレポート作成を可能にするため、DMS のレプリケーションタスクにおいて重要な役割を果たします。これにより、データの整合性と規制要件の遵守を維持しながら、データベース間のデータレプリケーションを正常に行うことができます。これらのコンポーネントでは、トラブルシューティング時に `DEFAULT` 以外のログレベルが必要になることは、ほぼありません。サポートにより特に変更の要求がない限り、これらのコンポーネントには `DEFAULT` と同じログレベルを維持するようにしてください。`DEFAULT` の最低限のロギングレベルでは、情報メッセージ、

警告、エラーメッセージが確実にログに書き込まれます。このコントロールは、前述のレプリケーションタスクのログレベルが、LOGGER_SEVERITY_DEFAULT、LOGGER_SEVERITY_DEBUG または LOGGER_SEVERITY_DETAILED_DEBUG のいずれかのログレベルであるかどうかを確認します。

修正

ターゲットデータベースの DMS レプリケーションタスクのログ記録を有効にするには、AWS Database Migration Service 「 ユーザーガイド」の AWS DMS 「タスクログの表示と管理」を参照してください。

[DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。

関連する要件： NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.8AU-600-53.r5 CA-7、NIST.800-53.r5 SC-7(9) SI-3 SI-4 SI-710.4.2

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::DMS::ReplicationTask`

AWS Config ルール : `dms-replication-task-sourcedb-logging`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、DMS レプリケーションタスク SOURCE_CAPTURE および SOURCE_UNLOAD の LOGGER_SEVERITY_DEFAULT の最小重要度レベルでログ記録が有効になっているかどうかを確認します。これらのタスクでロギングが有効になっていない場合や、最小重大度レベルが LOGGER_SEVERITY_DEFAULT よりも低い場合、コントロールは失敗します。

DMS は、移行プロセス中に Amazon CloudWatch を使用して情報をログ記録します。ロギングタスク設定を使用して、ログ記録するコンポーネントアクティビティとログに記録する情報量を指定できます。次のタスクにはロギングを指定する必要があります。

- SOURCE_CAPTURE— 進行中のレプリケーションまたは変更データキャプチャ (CDC) データがソースデータベースまたはサービスからキャプチャされ、SORTER サービスコンポーネントに渡されます。

- SOURCE_UNLOAD— 全ロード中に、データがソースデータベースまたはサービスからアンロードされます。

ロギングは、モニタリング、トラブルシューティング、監査、パフォーマンス分析、エラー検出、リカバリのほか、履歴分析やレポート作成を可能にするため、DMS のレプリケーションタスクにおいて重要な役割を果たします。これにより、データの整合性と規制要件の遵守を維持しながら、データベース間のデータレプリケーションを正常に行うことができます。これらのコンポーネントでは、トラブルシューティング時に DEFAULT 以外のログレベルが必要になることは、ほぼありません。サポートにより特に変更の要求がない限り、これらのコンポーネントには DEFAULT と同じログレベルを維持するようにしてください。DEFAULT の最低限のロギングレベルでは、情報メッセージ、警告、エラーメッセージが確実にログに書き込まれます。このコントロールは、前述のレプリケーションタスクのログレベルが、LOGGER_SEVERITY_DEFAULT、LOGGER_SEVERITY_DEBUG または LOGGER_SEVERITY_DETAILED_DEBUG のいずれかのログレベルであるかどうかを確認します。

修正

ソースデータベースの DMS レプリケーションタスクのログ記録を有効にするには、AWS Database Migration Service 「 ユーザーガイド」の AWS DMS 「タスクログの表示と管理」を参照してください。

[DMS.9] DMS エンドポイントは SSL を使用する必要があります。

関連する要件： NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、PCI DSS v4.0.1/4.2.1

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : AWS::DMS::Endpoint

AWS Config ルール : dms-endpoint-ssl-configured

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS DMS エンドポイントが SSL 接続を使用しているかどうかをチェックします。エンドポイントが SSL を使用していない場合、コントロールは失敗します。

SSL/TLS 接続は、DMS レプリケーションインスタンスとデータベースの間の接続を暗号化することによって、セキュリティレイヤーを 1 つ提供します。証明書を使用すると、想定されるデータベースへの接続が確立されていることを検証することによって、追加のセキュリティレイヤーが提供されます。これを行うには、プロビジョニングしたすべての DB インスタンスに自動インストールされたサーバー証明書を確認します。DMS エンドポイントで SSL 接続を有効にすることで、移行中のデータの機密性を保護できます。

修正

SSL 接続を新規または既存の DMS エンドポイントに追加するには、「AWS Database Migration Service ユーザーガイド」の「AWS Database Migration Serviceでの SSL の使用」を参照してください。

[DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります

関連する要件： NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-17、NIST.800-53.r5 IA-2、NIST.800-53.r5 IA-5、PCI DSS v4.0.1/7.3.1

カテゴリ: 保護 > セキュアなアクセス管理 > パスワードレス認証

重要度: 中

リソースタイプ : `AWS::DMS::Endpoint`

AWS Config ルール : `dms-neptune-iam-authorization-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon Neptune データベースの AWS DMS エンドポイントが IAM 認可で設定されているかどうかを確認します。DMS エンドポイントで IAM 認証が有効になっていない場合、コントロールは失敗します。

AWS Identity and Access Management (IAM) は、 全体できめ細かなアクセスコントロールを提供します AWS。IAM では、誰がどのサービスとリソースにアクセスできるか、またどの条件下でアクセスできるかを指定できます。IAM ポリシーを使用すると、ワークフォースとシステムへのアクセス許可を管理し、最小特権のアクセス許可を確保できます。Neptune データベースの AWS DMS エンドポイントで IAM 認可を有効にすると、 `ServiceAccessRoleARN`パラメータで指定されたサービスロールを使用して、IAM ユーザーに認可権限を付与できます。

修正

Neptune データベースの DMS エンドポイントで IAM 認証を有効にするには、「AWS Database Migration Service ユーザーガイド」の「Amazon Neptune を AWS Database Migration Serviceのターゲットとして使用する」を参照してください。

[DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります

関連する要件： NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-6、NIST.800-53.r5 IA-2、NIST.800-53.r5 IA-5、PCI DSS v4.0.1/7.3.1

カテゴリ: 保護 > セキュアなアクセス管理 > パスワードレス認証

重要度: 中

リソースタイプ : `AWS::DMS::Endpoint`

AWS Config ルール : `dms-mongo-db-authentication-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、MongoDB の AWS DMS エンドポイントが認証メカニズムで設定されているかどうかを確認します。エンドポイントに認証タイプが設定されていない場合、コントロールは失敗します。

AWS Database Migration Service は、MongoDB の 2 つの認証方法をサポートします。MongoDB バージョン 2.x の場合は MongoDB-CR、MongoDB バージョン 3.x 以降の場合は SCRAM-SHA-1 です。これらの認証方法は、ユーザーがパスワードを使用してデータベースにアクセスする場合に MongoDB パスワードを認証および暗号化するために使用されます。 AWS DMS エンドポイントでの認証により、承認されたユーザーのみがデータベース間で移行されるデータにアクセスして変更できるようになります。適切な認証がないと、移行プロセス中に権限のないユーザーが機密データにアクセスできる可能性があります。これにより、データ侵害、データ損失、またはその他のセキュリティインシデントが発生する可能性があります。

修正

MongoDB の DMS エンドポイントで認証メカニズムを有効にするには、「AWS Database Migration Service ユーザーガイド」の「MongoDB を AWS DMSのソースとして使用する」を参照してください。

[DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります

関連する要件： NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-13、PCI DSS v4.0.1/4.2.1

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::DMS::Endpoint`

AWS Config ルール : `dms-redis-tls-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Redis OSS の AWS DMS エンドポイントが TLS 接続で設定されているかどうかを確認します。エンドポイントで TLS が有効になっていない場合、コントロールは失敗します。

TLS は、データがインターネット経由でアプリケーションまたはデータベース間で送信されるときに、エンドツーエンドのセキュリティを提供します。DMS エンドポイントに SSL 暗号化を設定すると、移行プロセス中にソースデータベースとターゲットデータベース間の暗号化された通信が可能になります。これにより、悪意のある攻撃者による機密データの盗聴や傍受を防ぐことができます。SSL 暗号化を使用しないと、機密データにアクセスされ、データ侵害、データ損失、またはその他のセキュリティインシデントが発生する可能性があります。

修正

Redis の DMS エンドポイントで TLS 接続を有効にするには、「AWS Database Migration Service ユーザーガイド」の「AWS Database Migration Serviceのターゲットとして Redis を使用する」を参照してください。

Amazon DocumentDB の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon DocumentDB (MongoDB 互換) サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : docdb-cluster-encrypted

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon DocumentDB クラスターが保管中に暗号化されているかどうかをチェックします。Amazon DocumentDB クラスターが保管中に暗号化されていない場合、コントロールは失敗します。

保管中のデータとは、永続的な不揮発性ストレージに任意の期間保管されているデータを指します。暗号化は、このようなデータの機密性を保護し、権限のないユーザーがデータにアクセスするリスクを低減するのに役立ちます。Amazon DocumentDB クラスター内のデータは、セキュリティを強化するために、保管中に暗号化する必要があります。Amazon DocumentDB は、256 ビット高度暗号化標準 (AES-256) を使用し、 AWS Key Management Service (AWS KMS) に保存されている暗号化キーを使用してデータを暗号化します。

修正

Amazon DocumentDB クラスターを作成するときに、保管中の暗号化を有効にできます。クラスターを作成した後で暗号化設定を変更することはできません。詳細については、「Amazon DocumentDB デベロッパーガイド」の「Enabling encryption at rest for an Amazon DocumentDB cluster」を参照してください。

[DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です

関連する要件： NIST.800-53.r5 SI-12、PCI DSS v4.0.1/3.2.1

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : docdb-cluster-backup-retention-check

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値	
`minimumBackupRetentionPeriod`	最小バックアップ保持期間 (日数)	整数	7 ~ 35	7	

このコントロールは、Amazon DocumentDB クラスターのバックアップ保持期間が指定された時間枠以上であるかどうかをチェックします。バックアップ保持期間が指定された時間枠未満の場合、コントロールは失敗します。バックアップ保持期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 7 日を使用します。

バックアップは、セキュリティインシデントからの迅速な復元と、システムの耐障害性の強化に役立ちます。Amazon DocumentDB クラスターのバックアップを自動化すると、システムを特定の時点に復元し、ダウンタイムとデータ損失を最小限に抑えることができます。Amazon DocumentDB では、クラスターのデフォルトのバックアップ保持期間は 1 日です。このコントロールを成功させるには、この値を 7 日から 35 日までの値に増やす必要があります。

修正

Amazon DocumentDB クラスターのバックアップ保持期間を変更するには、「Amazon DocumentDB デベロッパーガイド」の「Amazon DocumentDB クラスターの変更」を参照してください。[バックアップ] で、バックアップ保持期間を選択します。

[DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません

関連する要件： NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7NIST.800-53.r5 SC-7.r5 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7r

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 非常事態

リソースタイプ : `AWS::RDS::DBClusterSnapshot`

AWS Config ルール : docdb-cluster-snapshot-public-prohibited

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon DocumentDB の手動クラスタースナップショットがパブリックかどうかをチェックします。手動クラスタースナップショットがパブリックの場合、コントロールは失敗します。

Amazon DocumentDB 手動クラスタースナップショットは、意図しない限りパブリックにしないでください。暗号化されていない手動スナップショットをパブリックとして共有すると、すべての AWS アカウントでこのスナップショットを使用できるようになります。パブリックスナップショットは、意図しないデータ漏えいにつながる可能性があります。

> **Note**
>
> このコントロールは手動クラスタースナップショットを評価します。Amazon DocumentDB 自動クラスタースナップショットを共有することはできません。ただし、自動スナップショットをコピーして手動スナップショットを作成し、そのコピーを共有できます。

修正

Amazon DocumentDB 手動クラスタースナップショットへのパブリックアクセスを削除するには、「Amazon DocumentDB デベロッパーガイド」の「スナップショットの共有」を参照してください。プログラムでは、Amazon DocumentDB のオペレーション `modify-db-snapshot-attribute` を使用できます。`attribute-name` を `restore` として、`values-to-remove` を `all` として設定します。

[DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります

関連する要件： NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53AU-6.r5 CA-7、NIST.800-53.r5 SC-7(7) SI-3 SI-4 SI-710.3.3

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : docdb-cluster-audit-logging-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon DocumentDB クラスターが監査ログを Amazon CloudWatch Logs に発行しているかどうかを確認します。クラスターが監査ログを CloudWatch Logs に発行していない場合、コントロールは失敗します。

Amazon DocumentDB (MongoDB 互換) を使用すると、クラスター内で実行されたイベントを監査できます。ログに記録されるイベントの例としては、認証の成功と失敗、データベース内のコレクションの削除、インデックスの作成などがあります。デフォルトでは、監査が Amazon DocumentDB 上で無効化されているため、この機能を有効化する必要があります。

修正

Amazon DocumentDB 監査ログを CloudWatch Logs に公開するには、「Amazon DocumentDB デベロッパーガイド」の「監査の有効化」を参照してください。

[DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

カテゴリ: 保護 > データ保護 > データ削除保護

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : docdb-cluster-deletion-protection-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon DocumentDB クラスターで削除保護が有効になっているかどうかを確認します。クラスターで削除保護が有効になっていない場合、コントロールは失敗します。

クラスターの削除保護を有効にすることで、偶発的なデータベース削除や権限のないユーザーによる削除に対して保護の強化を提供します。削除保護が有効の間、Amazon DocumentDB クラスター

は削除できません。削除リクエストを成功させるには、まず削除保護を無効にする必要があります。Amazon DocumentDB コンソールを使用してクラスターを作成する場合は、デフォルトで削除保護が有効になっています。

修正

既存の Amazon DocumentDB クラスターの削除保護を有効にするには、「Amazon DocumentDB デベロッパーガイド」の「Amazon DocumentDB クラスターの変更」を参照してください。[クラスターの変更] セクションで、[削除保護の有効化]を選択します。

[DocumentDB.6] Amazon DocumentDB クラスターは転送中に暗号化する必要があります

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : docdb-cluster-encrypted-in-transit

スケジュールタイプ: 定期的

パラメータ： `excludeTlsParameters`: `disabled`、 `enabled` (カスタマイズ不可)

このコントロールは、Amazon DocumentDB クラスターがクラスターへの接続に TLS を必要とするかどうかをチェックします。クラスターに関連付けられたクラスターパラメータグループが同期していない場合、または TLS クラスターパラメータが `disabled`または に設定されている場合、コントロールは失敗します`enabled`。

TLS を使用して、アプリケーションと Amazon DocumentDB クラスター間の接続を暗号化できます。TLS を使用すると、アプリケーションと Amazon DocumentDB クラスター間でデータが転送されている間、データが傍受されないように保護できます。Amazon DocumentDB クラスターの転送中の暗号化は、クラスターに関連付けられているクラスターパラメータグループの TLS パラメータを使用して管理されます。転送中の暗号化が有効になっている場合、クラスターに接続するには TLS を使用したセキュアな接続が必要です。、`tls1.2+`、 `tls1.3+`の TLS パラメータを使用することをお勧めします`fips-140-3`。

修正

Amazon DocumentDB クラスターの TLS 設定を変更する方法については、Amazon DocumentDB デベロッパーガイド」の「転送中のデータの暗号化」を参照してください。

DynamoDB の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon DynamoDB サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[DynamoDB.1] DynamoDB テーブルは、需要に応じて容量をオートスケーリングする必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-2(2)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::DynamoDB::Table`

AWS Config ルール : `dynamodb-autoscaling-enabled`

スケジュールタイプ : 定期的

パラメータ :

パラメータ	説明	[Type] (タイプ)	有効なカスタム値	Security Hub のデフォルト値
`minProvisionedReadCapacity`	DynamoDB 自動スケーリング用にプロビジョニングされた読み込みキャパシティユニットの最小数	整数	`1 ~ 40000`	デフォルト値なし
`targetReadUtilization`	読み込みキャパシティのターゲット使用率 (%)	整数	`20 ~ 90`	デフォルト値なし
`minProvisionedWriteCapacity`	DynamoDB 自動スケーリング用にプロビジョニングされた書き込みキャパシティユニットの最小数	整数	`1 ~ 40000`	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	有効なカスタム値	Security Hub のデフォルト値
`targetWriteUtilization`	書き込みキャパシティのターゲット使用率 (%)	整数	`20 ~ 90`	デフォルト値なし

このコントロールは、Amazon DynamoDB テーブルが必要に応じて読み取りおよび書き込み容量をスケーリングできるかどうかをチェックします。テーブルで自動スケーリングが設定されたオンデマンドキャパシティモードまたはプロビジョンモードを使用しない場合、コントロールは失敗します。デフォルトでは、このコントロールは、特定のレベルの読み込みまたは書き込みキャパシティに関係なく、これらのモードのいずれかを設定するだけで済みます。必要に応じて、特定のレベルの読み込みおよび書き込みキャパシティ、またはターゲット使用率を必要とするカスタムパラメータ値を指定できます。

需要に応じて容量をスケーリングすると、スロットリング例外を回避し、アプリケーションの可用性を維持するのに役立ちます。オンデマンドキャパシティモードを使用する DynamoDB テーブルは、DynamoDB スループットのデフォルトテーブルクォータによってのみ制限されます。これらのクォータを引き上げるには、 にサポートチケットを提出できます サポート。自動スケーリングを使うプロビジョニングモードを使用する DynamoDB テーブルでは、トラフィックパターンに応じてプロビジョンドスループットキャパシティ性能を動的に調整します。DynamoDB リクエストスロットリングの詳細については、「Amazon DynamoDB 開発者ガイド」の「リクエストのスロットリングとバーストキャパシティ」を参照してください。

修正

キャパシティモードで既存テーブルの DynamoDB 自動スケーリングを有効にするには、「Amazon DynamoDB デベロッパーガイド」の「既存のテーブルでの DynamoDB Auto Scaling の有効化」を参照してください。

[DynamoDB.2] DynamoDB テーブルでは、ポイントインタイムリカバリが有効になっている必要があります。

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

重要度: 中

リソースタイプ : `AWS::DynamoDB::Table`

AWS Config ルール : `dynamodb-pitr-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon DynamoDB テーブルに対してポイントインタイムリカバリ (PITR) が有効になっているかどうかをチェックします。

バックアップは、セキュリティインシデントからより迅速に復元するために役立ちます。また、システムの耐障害性を強化します。DynamoDB のポイントインタイムリカバリでは、DynamoDB テーブルのバックアップがオートメーションされます。偶発的な削除や書き込み操作から回復する時間が短縮されます。PITR を有効にした DynamoDB テーブルは、過去 35 日間の任意の時点に復元できます。

修正

DynamoDB テーブルを特定の時点に復元するには、「Amazon DynamoDB 開発者ガイド」の「DynamoDB テーブルをある時点に復元する」を参照してください。

[DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::DAX::Cluster`

AWS Config ルール : `dax-encryption-enabled`

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon DynamoDB Accelerator (DAX) クラスターが保管時に暗号化されているかどうかをチェックします。DAX クラスターが保管中に暗号化されていない場合、コントロールは失敗します。

保管中のデータを暗号化すると、ディスクに保存されているデータが認証されていないユーザーがアクセスするリスクが軽減されます AWS。暗号化により、権限のないユーザーがデータにアクセスする能力を制限するために、別の一連のアクセスコントロールが追加されます。例えば、データを読み取る前にデータを復号化するには、API の許可が必要です。

修正

クラスターが作成された後は、保管中の暗号化を有効または無効にすることはできません。保管中の暗号化を有効にするにはクラスターを再作成する必要があります。保管中の暗号化が有効な DAX クラスターを作成する方法の詳細については、「Amazon DynamoDB 開発者ガイド」の「AWS Management Consoleを使用して保管中の暗号化を有効にする」を参照してください。

[DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

重要度: 中

リソースタイプ : `AWS::DynamoDB::Table`

AWS Config ルール： `dynamodb-resources-protected-by-backup-plan`

スケジュールタイプ : 定期的

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`backupVaultLockCheck`	パラメータが に設定`true`され、リソースが AWS Backup ボールトロックを使用する場	ブール値	`true` 、、または `false`	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	合、コントロールはPASSED検出結果を生成します。			

このコントロールは、ACTIVE 状態の Amazon DynamoDB テーブルがバックアッププランの対象になっているかどうかを評価します。DynamoDB テーブルがバックアッププランの対象になっていない場合、コントロールは失敗します。backupVaultLockCheck パラメータを に設定するとtrue、DynamoDB テーブルが AWS Backup ロックされたボールトにバックアップされている場合にのみコントロールが渡されます。

AWS Backup は、 全体のデータのバックアップを一元化および自動化するのに役立つフルマネージドバックアップサービスです AWS のサービス。を使用すると AWS Backup、データのバックアップ頻度やバックアップの保持期間など、バックアップ要件を定義するバックアッププランを作成できます。バックアッププランに DynamoDB テーブルを含めると、意図しない損失や削除からデータを保護できます。

修正

AWS Backup バックアッププランに DynamoDB テーブルを追加するには、「 AWS Backup デベロッパーガイド」の「バックアッププランへのリソースの割り当て」を参照してください。

[DynamoDB.5] DynamoDB テーブルにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : AWS::DynamoDB::Table

AWS Config ルール: tagged-dynamodb-table (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、Amazon DynamoDB テーブルにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。テーブルにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、テーブルにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

DynamoDB テーブルにタグを追加するには、「Amazon DynamoDB デベロッパーガイド」の「DynamoDB でのリソースのタグ付け」を参照してください。

[DynamoDB.6] DynamoDB テーブルで、削除保護が有効になっている必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

カテゴリ: 保護 > データ保護 > データ削除保護

重要度: 中

リソースタイプ : `AWS::DynamoDB::Table`

AWS Config ルール： `dynamodb-table-deletion-protection-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon DynamoDB テーブルで削除保護が有効になっているかどうかをチェックします。DynamoDB テーブルで削除保護が有効になっていない場合、コントロールは失敗します。

削除保護プロパティを使用すると、DynamoDB テーブルを誤って削除しないように保護できます。テーブルに対してこのプロパティを有効にすると、管理者が通常のテーブル管理オペレーションを行うときにテーブルが誤って削除されるのを防ぐことができます。これにより、通常業務が中断されるのを防ぐことができます。

修正

DynamoDB テーブルの削除保護を有効にするには、「Amazon DynamoDB 開発者ガイド」の「削除保護の使用」を参照してください。

[DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります

関連する要件： NIST.800-53.r5 AC-17、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、PCI DSS v4.0.1/4.2.1

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::DAX::Cluster`

AWS Config ルール : `dax-tls-endpoint-encryption`

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon DynamoDB Accelerator (DAX) クラスターが転送中に暗号化され、エンドポイント暗号化タイプが TLS に設定されているかどうかを確認します。DAX クラスターが転送中に暗号化されていない場合、コントロールは失敗します。

HTTPS (TLS) を使用すると、潜在的な攻撃者が中間者攻撃または同様の攻撃を使用してネットワークトラフィックを盗聴または操作することを防止できます。DAX クラスターへのアクセスには、TLS 経由の暗号化された接続のみを許可する必要があります。ただし、転送中のデータの暗号化は、パフォーマンスに影響する可能性があります。TLS のパフォーマンスプロファイルと TLS の影響を把握するには、暗号化を有効にしてアプリケーションをテストする必要があります。

修正

DAX クラスターを作成した後で TLS 暗号化設定を変更することはできません。既存の DAX クラスターを暗号化するには、転送中の暗号化を有効にした新しいクラスターを作成し、アプリケーションのトラフィックをそのクラスターに移行してから、古いクラスターを削除します。詳細については、「Amazon DynamoDB ディベロッパーガイド」の「削除保護の使用」を参照してください。

Amazon EC2 の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon Elastic Compute Cloud (Amazon EC2) サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[EC2.1] Amazon EBS スナップショットはパブリックに復元できないようにすることをお勧めします

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 非常事態

リソースタイプ : `AWS::::Account`

AWS Config ルール : `ebs-snapshot-public-restorable-check`

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon Elastic Block Store スナップショットがパブリックではないかどうかをチェックします。Amazon EBS スナップショットを誰でも復元できる場合、コントロールは失敗します。

EBS スナップショットは、特定の時点の EBS ボリュームのデータを Amazon S3 にバックアップするために使用されます。スナップショットを使用して、EBS ボリュームを以前の状態に復元できます。スナップショットのパブリックへの共有は滅多に認められていません。一般的に、スナップショットを公開する決定は、誤って行われたか、影響を完全に理解せずに行われています。このチェックは、そのような共有がすべて完全に計画され、意図的であったことを確認するのに役立ちます。

修正

パブリック EBS スナップショットをプライベートにするには、「Amazon EC2 ユーザーガイド」の「スナップショットの共有」を参照してください。[アクション、権限の変更] で、[非公開] を選択します。

[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします

関連する要件： PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/2.1、CIS AWS Foundations Benchmark v1.2.0/4.3、CIS AWS Foundations Benchmark v1.4.0/5.3、CIS AWS Foundations Benchmark v3.0.0/5.4、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(1 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-76

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ : `AWS::EC2::SecurityGroup`

AWS Config ルール : `vpc-default-security-group-closed`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、VPC のデフォルトのセキュリティグループがインバウンドとアウトバウンドのいずれかのトラフィックを許可しているかをチェックします。セキュリティグループがインバウンドまたはアウトバウンドのトラフィックを許可している場合、このコントロールは失敗します。

デフォルトのセキュリティグループのルールでは、同じセキュリティグループに割り当てられているネットワークインターフェイス (および関連するインスタンス) からのすべてのアウトバウンドトラフィックとインバウンドトラフィックを許可します。デフォルトのセキュリティグループを使用しないことをお勧めします。デフォルトのセキュリティグループは削除できないため、デフォルトのセキュリティグループルール設定を変更して、インバウンドトラフィックとアウトバウンドトラフィックを制限する必要があります。これにより、デフォルトのセキュリティグループが EC2 インスタンスなどのリソースに対して誤って設定されている場合に、意図しないトラフィックが防止されます。

修正

この問題を解決するには、まず新しい最小特権のセキュリティグループを作成することから始めます。手順については、「Amazon VPC ユーザーガイド」の「セキュリティグループの作成」を参照してください。次に、新しいセキュリティグループを EC2 インスタンスに割り当てます。手順については、「Amazon EC2 ユーザーガイド」の「インスタンスのセキュリティグループの変更」を参照してください。

新しいセキュリティグループをリソースに割り当てた後、デフォルトのセキュリティグループからすべてのインバウンドルールとアウトバウンドルールを削除します。手順については、「Amazon VPC ユーザーガイド」の「セキュリティグループの設定」を参照してください。

[EC2.3] アタッチされた Amazon EBS ボリュームは、保管時に暗号化することをお勧めします

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::EC2::Volume`

AWS Config ルール : `encrypted-volumes`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、添付済みの EBS ボリュームが暗号化されているかどうかをチェックします。このチェックに合格するには、EBS ボリュームが使用中であり、暗号化されている必要があります。EBS ボリュームが添付済みでない場合、このチェックは対象外です。

EBS ボリュームの機密データのセキュリティを強化するには、保管中の EBS 暗号化を有効にする必要があります。Amazon EBS 暗号化は、EBS リソースに対して、独自のキー管理インフラストラクチャの構築、保守、および保護を必要としない、簡単な暗号化ソリューションを提供します。暗号化されたボリュームとスナップショットを作成する際に、KMS キー を使用します。

Amazon EBS 暗号化の詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EBS 暗号化」を参照してください。

修正

暗号化されていない既存のボリュームまたはスナップショットを暗号化する直接的な方法はありません。新しいボリュームまたはスナップショットは、作成時にのみ暗号化できます。

暗号化をデフォルトで有効にした場合、Amazon EBS は Amazon EBS 暗号化のデフォルトキーを使用して、作成された新しいボリュームまたはスナップショットを暗号化します。デフォルトで暗号化を有効にしていない場合でも、個々のボリュームまたはスナップショットを作成するときに暗号化を有効にすることができます。どちらの場合も、Amazon EBS 暗号化のデフォルトキーを上書きし、対称カスタマーマネージドキーを選択できます。

詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EBS ボリュームの作成」および「Amazon EBS スナップショットのコピー」を参照してください。

[EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 識別 > インベントリ

重要度: 中

リソースタイプ : `AWS::EC2::Instance`

AWS Config ルール : `ec2-stopped-instance`

スケジュールタイプ : 定期的

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
AllowedDays	失敗の検出結果が生成される前に、EC2 インスタンスが停止状態になっても許容される日数。	整数	1 ~ 365	30

このコントロールは、許可されている日数よりも長く停止している Amazon EC2 インスタンスがあるかどうかをチェックします。EC2 インスタンスが最大許容期間よりも長く停止すると、コントロールは失敗します。最大許容期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 30 日を使用します。

EC2 インスタンスが長期間実行されていないと、インスタンスがアクティブに保守 (分析、パッチ適用、更新) されていないため、セキュリティリスクが発生します。後で起動すると、適切なメンテナンスを行わないと、 AWS 環境で予期しない問題が発生する可能性があります。EC2 インスタンスを非アクティブ状態で長期間安全に維持するには、メンテナンスのために定期的に起動し、メンテナンス後に停止します。これは自動化されたプロセスであるべきです。

修正

非アクティブな EC2 インスタンスを終了するには、「Amazon EC2 ユーザーガイド」の「インスタンスの終了」を参照してください。

[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします

関連する要件： CIS AWS Foundations Benchmark v1.2.0/2.9、CIS AWS Foundations Benchmark v1.4.0/3.9、CIS AWS Foundations Benchmark v3.0.0/3.7、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.8000-53 SI-7 3.1.2010.3.310.3.410.3.510.3.6.

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::EC2::VPC`

AWS Config ルール : `vpc-flow-logs-enabled`

スケジュールタイプ : 定期的

パラメータ :

- `trafficType`: `REJECT` (カスタマイズ不可)

このコントロールは、Amazon VPC フローログが見つかり、VPC に対して有効になっているかどうかをチェックします。トラフィックタイプは `Reject` に設定されています。アカウント内の VPC に対して VPC フローログが有効になっていない場合、コントロールは失敗します。

> **Note**
>
> このコントロールは、 AWS アカウントの Amazon Security Lake を介して Amazon VPC フローログが有効になっているかどうかをチェックしません。

VPC フローログ機能を使用して、VPC のネットワークインターフェイスとの間で行き来する IP アドレストラフィックに関する情報をキャプチャします。フローログを作成すると、そのデータを CloudWatch Logs で表示し、取得できます。コストを削減するために、フローログを Amazon S3 に送信することもできます。

Security Hub では、VPC のパケット拒否のフローログ記録を有効にすることを推奨します。フローログは、VPC を通過するネットワークトラフィックを可視化し、セキュリティワークフロー中の異常なトラフィックを検出したりインサイトを提供できます。

デフォルトでは、レコードには送信元、送信先、プロトコルなど、IP アドレスフローのさまざまなコンポーネントの値が含まれています。ログフィールドの詳細と説明については、「Amazon VPC ユーザーガイド」の「VPC フローログ」を参照してください。

修正

VPC フローログを作成するには、「Amazon VPC ユーザーガイド」の「VPC フローログを作成する」を参照してください。Amazon VPC コンソールを開いたら、[お客様の VPC] を選択します。[フィルター] で、[拒否] または [すべて] を選択します。

[EC2.7] EBS のデフォルト暗号化を有効にすることをお勧めします

関連する要件： CIS AWS Foundations Benchmark v1.4.0/2.2.1、CIS AWS Foundations Benchmark v3.0.0/2.2.1、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::::Account`

AWS Config ルール : `ec2-ebs-encryption-by-default`

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon Elastic Block Store (Amazon EBS) ボリュームでアカウントレベルの暗号化がデフォルトで有効になっているかどうかをチェックします。EBS ボリュームでアカウントレベルの暗号化が有効になっていない場合、コントロールは失敗します。

アカウントで暗号化が有効になっている場合、Amazon EBS ボリュームとスナップショットのコピーは保管中に暗号化されます。これにより、データの保護レイヤーが追加されます。詳細については、「Amazon EC2 ユーザーガイド」の「デフォルトで暗号化」を参照してください。

修正

Amazon EBS ボリュームのデフォルト暗号化の設定については、「Amazon EC2 ユーザーガイド」の「デフォルトでの暗号化」を参照してください。

[EC2.8] EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします

関連する要件： CIS AWS Foundations Benchmark v3.0.0/5.6、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6、PCI DSS v4.0.1/2.2.6

カテゴリ: 保護 > ネットワークセキュリティ

重要度: 高

リソースタイプ : `AWS::EC2::Instance`

AWS Config ルール : `ec2-imdsv2-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、EC2 インスタンスメタデータバージョンが、インスタンスメタデータサービスバージョン 2 (IMDSv2) で設定されているかどうかをチェックします。IMDSv2 で `HttpTokens` が必須に設定されている場合、コントロールは成功します。`HttpTokens` が `optional` に設定されている場合、コントロールは失敗します。

インスタンスメタデータは、実行中のインスタンスを設定または管理するために使用します。IMDS は、一時的で頻繁にローテーションされる認証情報へのアクセスを提供します。これらの認証情報を使用すると、機密認証情報を手動でまたはプログラムでインスタンスにハードコーディングや、配信する必要がなくなります。IMDS は、すべての EC2 インスタンスにローカルに添付されます。これは、特別な「リンクローカル」IP アドレス 169.254.169.254 で実行されます。この IP アドレスは、インスタンスで実行されるソフトウェアによってのみアクセスできます。

IMDS のバージョン 2 では、次の種類の脆弱性に対する新しい保護が追加されています。これらの脆弱性は IMDS へのアクセスに利用される可能性があります。

- ウェブサイトアプリケーションのファイアウォールを開く
- リバースプロキシを開く
- サーバー側リクエスト偽造 (SSRF) の脆弱性
- レイヤー 3 ファイアウォールおよびネットワークアドレス変換 (NAT) を開く

Security Hub では、EC2 インスタンスを IMDSv2 で設定することを推奨します。

修正

EC2 インスタンスを IMDSv2 で設定するには、「Amazon EC2 ユーザーガイド」の「IMDSv2 を必要とする場合の推奨方法」を参照してください。

[EC2.9] Amazon EC2 インスタンスは、パブリック IPv4 アドレスを未設定にすることをお勧めします

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5

SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 高

リソースタイプ : `AWS::EC2::Instance`

AWS Config ルール : `ec2-instance-no-public-ip`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、EC2 インスタンスにパブリック IP アドレスがあるかどうかをチェックします。EC2 インスタンスの設定項目に `publicIp` フィールドが存在する場合、コントロールは失敗します。このコントロールは、IPv4 アドレスにのみ適用されます。

パブリック IPv4 アドレスは、インターネットから到達可能な IP アドレスです。パブリック IP アドレスを使用してインスタンスを起動すると、EC2 インスタンスはインターネットから到達可能です。プライベート IPv4 アドレスは、インターネットから到達できない IP アドレスです。プライベート IPv4 アドレスは、同じ VPC 内の EC2 インスタンス間または接続されたプライベートネットワークの通信に使用できます。

IPv6 アドレスはグローバルに一意であるため、インターネットから到達できます。ただし、デフォルトではすべてのサブネットで IPv6 アドレス指定属性が false に設定されています。VPC での IPv6 の詳細については、「Amazon VPC ユーザーガイド」の「VPC での IP アドレス指定」を参照してください。

パブリック IP アドレスで EC2 インスタンスを維持する正当なユースケースがある場合は、このコントロールの結果を抑制できます。フロントエンドアーキテクチャオプションの詳細については、AWS 「アーキテクチャブログ」または「This Is My Architecture series AWS video series」を参照してください。

修正

デフォルト以外の VPC を使用し、デフォルトでインスタンスがパブリック IP アドレスに割り当てられないようにします。

デフォルトの VPC で EC2 インスタンスを起動すると、パブリック IP アドレスが割り当てられます。EC2 インスタンスをデフォルト以外の VPC で起動すると、サブネット設定によって、パブリッ

ク IP アドレスを受信するかどうかが決まります。サブネットには、サブネット内の新しい EC2 インスタンスがパブリック IPv4 アドレスプールからパブリック IP アドレスを受け取るかどうかを判断する属性があります。

自動で割り当てられたパブリック IP アドレスを EC2 インスタンスから関連付け解除することができます。詳細については、「Amazon EC2 ユーザーガイド」の「パブリック IPv4 アドレスと外部 DNS ホスト名」を参照してください。

[EC2.10] Amazon EC2 サービス用に作成された VPC エンドポイントを使用するようにAmazon EC2 を設定することをお勧めします

関連する要件： NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7NIST.800-53.r5 SC-7-53.r5 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7r

カテゴリ: 保護 > セキュアなネットワーク設定 > API プライベートアクセス

重要度: 中

リソースタイプ : `AWS::EC2::VPC`

AWS Config ルール : `service-vpc-endpoint-enabled`

スケジュールタイプ : 定期的

パラメータ :

- `serviceName`: `ec2` (カスタマイズ不可)

このコントロールは、Amazon EC2 のサービスエンドポイントが各 VPC に対して作成しているかどうかをチェックします。VPC に Amazon EC2 サービス用に作成した VPC エンドポイントがない場合、コントロールは失敗します。

このコントロールは、単一のアカウントのリソースを評価します。アカウント外のリソースは記述できません。 AWS Config と Security Hub はクロスアカウントチェックを実行しないため、アカウント間で共有されている VPCs `FAILED`の検出結果が表示されます。Security Hub では、これらの `FAILED` 結果を抑制することを推奨します。

VPC のセキュリティ体制を強化するために、インターフェイス VPC エンドポイントを使用するように Amazon EC2 を設定できます。インターフェイスエンドポイントは AWS PrivateLink、Amazon

EC2 API オペレーションにプライベートにアクセスできるテクノロジーである を利用しています。これは、VPC と Amazon EC2 間のすべてのネットワークトラフィックを Amazon ネットワークに限定します。エンドポイントは同じリージョンでのみサポートされるため、別のリージョンの VPC とサービス間にエンドポイントを作成することはできません。これにより、他のリージョンへの意図しない Amazon EC2 API コールを防ぐことができます。

Amazon EC2 の VPC エンドポイントの作成の詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 とインターフェイス VPC エンドポイント」を参照してください。

修正

Amazon VPC コンソールから Amazon EC2 へのインターフェイスエンドポイントを作成するには、「AWS PrivateLink ガイド」の「VPC エンドポイントを作成する」を参照してください。[サービス名] で [com.amazonaws.***region***.ec2] を選択します。

また、エンドポイントポリシーを作成し、VPC エンドポイントにアタッチして Amazon EC2 API へのアクセスを制御することもできます。VPC エンドポイントポリシーを作成する手順については、「Amazon EC2 ユーザーガイド」の「エンドポイントポリシーの作成」を参照してください。

[EC2.12] 未使用の Amazon EC2 EIP を削除することをお勧めします

関連する要件: PCI DSS v3.2.1/2.4、NIST.800-53.r5 CM-8(1)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 低

リソースタイプ : `AWS::EC2::EIP`

AWS Config ルール : `eip-attached`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、VPC に割り当てられた Elastic IP (EIP) アドレスが、 EC2 インスタンスまたは使用中の Elastic Network Interface (ENI) にアタッチされているかどうかを確認します。

検出に失敗した場合は、未使用の EC2 EIP がある可能性があります。

これにより、カード所有者データ環境 (CDE) 内の EIP のアセットインベントリを正確な状態に維持できます。

修正

未使用の EIP をリリースするには、「Amazon EC2 ユーザーガイド」の「Elastic IP アドレスを解放する」を参照してください。

[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります

関連する要件： CIS AWS Foundations Benchmark v1.2.0/4.1、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CM-7、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7NIST.800-53.r5 SC-7(5)、NIST.800-17r2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ : `AWS::EC2::SecurityGroup`

AWS Config ルール : `restricted-ssh`

スケジュールタイプ: 変更がトリガーされ、定期的に行われる場合

パラメータ : なし

このコントロールは、Amazon EC2 セキュリティグループが 0.0.0.0/0 または ::/0 からポート 22 への入力を許可しているかどうかをチェックします。セキュリティグループが 0.0.0.0/0 または ::/0 からポート 22 への入力を許可している場合、コントロールは失敗します。

セキュリティグループは、 AWS リソースへの入力および出力ネットワークトラフィックのステートフルフィルタリングを提供します。セキュリティグループはポート 22 への無制限の入力を許可しません。SSH などのリモートコンソールサービスへの自由な接続を制限することにより、サーバーがリスクにさらされることを軽減できます。

修正

ポート 22 への進入を禁止するには、VPC に関連付けられている各セキュリティグループにそのようなアクセスを許可するルールを削除します。手順については、「Amazon EC2 ユーザーガイド」の「セキュリティグループのルールの更新」を参照してください。Amazon EC2 コンソールでセキュリティグループを選択したら、[アクション、インバウンドルールの編集] を選択します。ポート 22 へのアクセスを許可するルールを削除します。

[EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります

関連する要件： CIS AWS Foundations Benchmark v1.2.0/4.2、PCI DSS v4.0.1/1.3.1

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ : `AWS::EC2::SecurityGroup`

AWS Config ルール： `restricted-common-ports` (作成されたルールは `restricted-rdp`)

スケジュールタイプ: 変更がトリガーされ、定期的に行われる場合

パラメータ : なし

このコントロールは、Amazon EC2 セキュリティグループが 0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しているかどうかをチェックします。セキュリティグループが 0.0.0.0/0 または ::/0 からポート 3389 への入力を許可している場合、コントロールは失敗します。

セキュリティグループは、 AWS リソースへの入力および出力ネットワークトラフィックのステートフルフィルタリングを提供します。セキュリティグループはポート 3389 への無制限の入力を許可しません。RDP などのリモートコンソールサービスへの自由な接続を制限することにより、サーバーがリスクにさらされることを軽減できます。

修正

ポート 3389 への進入を禁止するには、VPC に関連付けられている各セキュリティグループにそのようなアクセスを許可するルールを削除します。手順については、「Amazon VPC ユーザーガイド」の「セキュリティグループのルールの更新」を参照してください。Amazon VPC コンソールでセキュリティグループを選択したら、[アクション、インバウンドルールの編集] を選択します。ポート 3389 へのアクセスを許可するルールを削除します。

[EC2.15] Amazon EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないことをお勧めします

関連する要件： NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7NIST.800-53.r5 SC-7.r5 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7r

カテゴリ: 保護 > ネットワークセキュリティ

重要度: 中

リソースタイプ : `AWS::EC2::Subnet`

AWS Config ルール : `subnet-auto-assign-public-ip-disabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon Virtual Private Cloud (Amazon VPC) サブネット内のパブリック IP の割り当ての `MapPublicIpOnLaunch` が `FALSE` に設定されているかチェックします。フラグが `FALSE` に設定されている場合、コントロールは成功します。

すべてのサブネットには、サブネット内に作成されたネットワークインターフェイスが自動的にパブリック IPv4 アドレスを受信するかどうかを判断する属性があります。この属性が有効になっているサブネットで起動されるインスタンスには、プライマリアネットワークインターフェイスに割り当てられるパブリック IP アドレスが割り当てられます。

修正

パブリック IP アドレスを割り当てないようにサブネットを設定するには、「Amazon VPC ユーザーガイド」の「サブネットのパブリック IPv4 アドレス指定属性の変更」を参照してください。[パブリック IPv4 アドレスの自動割り当てを有効にする] チェックボックスをオフにします。

[EC2.16] 未使用のネットワークアクセスコントロールリストを削除することをお勧めします

関連する要件： NIST.800-53.r5 CM-8(1)、NIST.800-171.r2 3.4.7、PCI DSS v4.0.1/1.2.7

カテゴリ: 保護 > ネットワークセキュリティ

重要度: 低

リソースタイプ : `AWS::EC2::NetworkAcl`

AWS Config ルール : `vpc-network-acl-unused-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、仮想プライベートクラウド (VPC) に未使用のネットワークアクセスコントロールリスト (ネットワーク ACL) があるかどうかをチェックします。ネットワーク ACL がサブネッ

トに関連付けられていない場合、コントロールは失敗します。コントロールは、未使用のデフォルトネットワーク ACL の検出結果を生成しません。

コントロールは、リソース `AWS::EC2::NetworkAcl` の項目設定をチェックして、ネットワーク ACL の関係を判断します。

ネットワーク ACL の VPC のみの関係の場合、コントロールは失敗します。

他の関係がリスト済みの場合、コントロールは成功します。

修正

未使用のネットワーク ACL を削除する方法については、「Amazon VPC ユーザーガイド」の「ネットワーク ACL の削除」を参照してください。デフォルトのネットワーク ACL またはサブネットに関連付けられた ACL は削除できません。

[EC2.17] Amazon EC2 インスタンスが複数の ENI を使用しないようにすることをお勧めします

関連する要件: NIST.800-53.r5 AC-4(21)

カテゴリ: 保護 > ネットワークセキュリティ

重要度: 低

リソースタイプ : `AWS::EC2::Instance`

AWS Config ルール : `ec2-instance-multiple-eni-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、EC2 インスタンスが複数の Elastic Network Interface (ENI) または Elastic Fabric Adapter (EFA) を使用しているかどうかをチェックします。このコントロールは、単一のネットワークアダプタが使用されている場合に成功します。コントロールには、許可された ENI を識別するためのオプションのパラメータリストが含まれています。Amazon EKS クラスターに属する EC2 インスタンスが複数の ENI を使用している場合も、このコントロールは失敗します。EC2 インスタンスに Amazon EKS クラスターの一部として複数の ENI が必要な場合は、これらのコントロールの検出結果を抑制できます。

複数の ENI の使用は、デュアルホームインスタンス (複数のサブネットを持つインスタンス) を引き起こす可能性があります。これにより、ネットワークセキュリティの複雑性が増し、意図しないネットワークパスとアクセスが導入する可能性があります。

修正

EC2 インスタンスからネットワークインターフェイスをデタッチするには、「Amazon EC2 ユーザーガイド」の「インスタンスからネットワークインターフェイスをデタッチする」を参照してください。

[EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします

関連する要件： NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(5)、NIST.800-171.r2 3.1.20、NIST.800-171.r2

カテゴリ: 保護 > セキュアなネットワーク設定 > セキュリティグループの設定

重要度: 高

リソースタイプ : `AWS::EC2::SecurityGroup`

AWS Config ルール : `vpc-sg-open-only-to-authorized-ports`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`authorizedTcpPorts`	許可されている TCP ポートのリスト	IntegerList (最小 1 項目、最大 32 項目)	`1 ~ 65535`	`[80,443]`
`authorizedUdpPorts`	許可されている UDP ポートのリスト	IntegerList (最小 1 項目、最大 32 項目)	`1 ~ 65535`	デフォルト値なし

このコントロールは、Amazon EC2 セキュリティグループが、許可されていないポートからの無制限の着信トラフィックを許可しているかどうかをチェックします。コントロールのステータスは次のように決定されます。

- `authorizedTcpPorts` のデフォルト値を使用する場合、セキュリティグループがポート 80 およびポート 443 以外のポートからの無制限の着信トラフィックを許可すると、コントロールは失敗します。
- `authorizedTcpPorts` または `authorizedUdpPorts` にカスタム値を指定した場合、セキュリティグループがリストにないポートからの無制限の着信トラフィックを許可すると、コントロールは失敗します。

セキュリティグループは、 AWSへの入力および出力ネットワークトラフィックのステートフルフィルタリングを提供します。セキュリティグループのルールは、最小特権アクセスのプリンシパルに従う必要があります。無制限アクセス (/0 サフィックスを持つ IP アドレス) を使用すると、ハッキング、サービス拒否攻撃、データ損失などの悪意のあるアクティビティの機会が増えます。ポートが特別に許可されていない限り、ポートは無制限アクセスを拒否する必要があります。

修正

セキュリティグループを変更するには、「Amazon VPC ユーザーガイド」の「セキュリティグループの操作」を参照してください。

[EC2.19] セキュリティグループは、リスクの高いポートへの無制限アクセスを許可してはいけません

関連する要件： NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-7、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-73(2) NIST.800-53.r5 SC-7 3.1.20

カテゴリ: 保護 > 制限付きネットワークアクセス

重要度: 非常事態

リソースタイプ : `AWS::EC2::SecurityGroup`

AWS Config ルール： `restricted-common-ports` (作成されたルールは `vpc-sg-restricted-common-ports`)

スケジュールタイプ: 変更がトリガーされ、定期的に行われる場合

パラメータ: `"blockedPorts": "20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,560` (カスタマイズ不可)

このコントロールは、指定した高リスクと見なされるポートに Amazon EC2 セキュリティグループの無制限の受信トラフィックがアクセス可能かどうかをチェックします。セキュリティグループ内のルールがこれらのポートへの「0.0.0.0/0」または「::/0」からの入力トラフィックを許可している場合、このコントロールは失敗します。

セキュリティグループは、 AWS リソースへの入力および出力ネットワークトラフィックのステートフルフィルタリングを提供します。無制限のアクセス (0.0.0.0/0) では、ハッキング、サービス拒否攻撃、データ損失などの悪意のあるアクティビティの機会が増えます。どのセキュリティグループでも、以下のポートへの無制限の入力アクセスを許可してはいけません。

- 20、21 (FTP)
- 22 (SSH)
- 23 (Telnet)
- 25 (SMTP)
- 110 (POP3)
- 135 (RPC)
- 143 (IMAP)
- 445 (CIFS)
- 1433、1434 (MSSQL)
- 3000 (Go、Node.js、および Ruby のウェブ開発フレームワーク)
- 3306 (mySQL)
- 3389 (RDP)
- 4333 (ahsp)
- 5000 (Python ウェブ開発フレームワーク)
- 5432 (postgresql)
- 5500 (fcp-addr-srvr1)
- 5601 (OpenSearch Dashboards)
- 8080 (proxy)
- 8088 (レガシー HTTP ポート)

- 8888 (代替 HTTP ポート)
- 9200 または 9300 (OpenSearch)

修正

セキュリティグループからルールを削除するには、「Amazon EC2 ユーザーガイド」の「セキュリティグループからのルールの削除」を参照してください。

[EC2.20] AWS Site-to-Site VPN トンネルが稼働している必要があります

関連する要件： NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)、NIST.800-171.r2 3.1.13、NIST.800-171.r2 3.1.20

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ: `AWS::EC2::VPNConnection`

AWS Config ルール : `vpc-vpn-2-tunnels-up`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

VPN トンネルは、カスタマーネットワークから AWS Site-to-Site VPN 接続 AWS との間でデータを渡すことができる暗号化されたリンクです。各 VPN 接続には、高可用性のために同時に使用できる 2 つの VPN トンネルが含まれています。 AWS VPC とリモートネットワーク間の安全で可用性の高い接続を確認するには、両方の VPN トンネルが VPN 接続用に稼働していることを確認することが重要です。

このコントロールは、 AWS Site-to-Site VPN によって提供される両方の VPN トンネルが UP ステータスであることを確認します。一方または両方のトンネルのステータスが DOWN の場合、コントロールは失敗します。

修正

VPN トンネルオプションを変更するには、Site-to-Site VPN ユーザーガイド」の「Modifying Site-to-Site VPN tunnel options」を参照してください。 AWS Site-to-Site

[EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります

関連する要件： CIS AWS Foundations Benchmark v1.4.0/5.1、CIS AWS Foundations Benchmark v3.0.0/5.1、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-7、NIST.800-53.r5 SC-7NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(5)、NIST.800-17r2 3.1.20

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ: `AWS::EC2::NetworkAcl`

AWS Config ルール : `nacl-no-unrestricted-ssh-rdp`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、ネットワークアクセスコントロールリスト (ネットワーク ACL) が、 SSH/RDP 入力トラフィックのデフォルト TCP ポートへのアクセスを無制限に許可しているかどうかをチェックします。ネットワーク ACL インバウンドエントリが TCP ポート 22 または 3389 に対して「0.0.0.0/0」または「::/0」の送信元 CIDR ブロックを許可する場合、コントロールは失敗します。コントロールは、デフォルトのネットワーク ACL の検出結果を生成しません。

ポート 22 (SSH) やポート 3389 (RDP) などのリモートサーバー管理ポートへのアクセスは、VPC 内のリソースへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスできないようにする必要があります。

修正

ネットワーク ACL トラフィックルールを編集するには、「Amazon VPC ユーザーガイド」の「ネットワーク ACL を操作する」を参照してください。

[EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします

カテゴリ: 識別 > インベントリ

重要度: 中

リソースタイプ: `AWS::EC2::NetworkInterface`、`AWS::EC2::SecurityGroup`

AWS Config ルール : `ec2-security-group-attached-to-eni-periodic`

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、セキュリティグループが Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは Elastic Network Interface に添付済みであるかどうかをチェックします。セキュリティグループが Amazon EC2 インスタンスまたは Elastic Network Interface に関連付けられていない場合、コントロールは失敗します。

> **Important**
>
> 2023 年 9 月 20 日、Security Hub は AWS Foundational Security Best Practices および NIST SP 800-53 Revision 5 標準からこのコントロールを削除しました。このコントロールは、引き続き AWS Control Tower サービスマネージド標準の一部です。このコントロールは、セキュリティグループが EC2 インスタンスまたは Elastic Network Interface にアタッチされている場合に、合格の検出結果を生成します。ただし、特定のユースケースでは、セキュリティグループがアタッチされていなくてもセキュリティ上のリスクはありません。他の EC2 コントロール (EC2.2、EC2.13、EC2.14、EC2.18、EC2.19 など) を使用すると、セキュリティグループをモニタリングできます。

修正

セキュリティグループを作成、割り当て、削除するには、「Amazon EC2 ユーザーガイド」の「EC2 インスタンスのセキュリティグループ」を参照してください。 Amazon EC2

[EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします

関連する要件: NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ: `AWS::EC2::TransitGateway`

AWS Config ルール : `ec2-transit-gateway-auto-vpc-attach-disabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、EC2 中継ゲートウェイが共有 VPC アタッチメントを自動的に受け入れているかどうかをチェックします。中継ゲートウェイが共有 VPC アタッチメントリクエストを自動的に受け入れていると、このコントロールは失敗します。

`AutoAcceptSharedAttachments` をオンにすると、中継ゲートウェイは、リクエストまたはアタッチメントの発信元であるアカウントを確認せずに、クロスアカウント VPC アタッチメントリクエストを自動的に受け入れるように設定されます。認可および認証のベストプラクティスに従うため、この機能はオフにして、認可された VPC アタッチメントリクエストのみを受け入れることが推奨されます。

修正

中継ゲートウェイを変更するには、「Amazon VPC デベロッパーガイド」の「中継ゲートウェイの変更」を参照してください。

[EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします

関連する要件: NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 中

リソースタイプ: `AWS::EC2::Instance`

AWS Config ルール : `ec2-paravirtual-instance-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、EC2 インスタンスの仮想化タイプが準仮想化かどうかをチェックします。EC2 インスタンスの `virtualizationType` が `paravirtual` に設定されている場合、このコントロールは失敗します。

Linux Amazon マシンイメージ (AMI)では、2 つの仮想化タイプ、準仮想化 (PV) とハードウェア仮想化 (HVM) のうち、いずれかを使用します。PV AMI と HVM AMI の主な違いは、起動の方法と、パ

フォーマンス向上のための特別なハードウェア拡張機能 (CPU、ネットワーク、ストレージ) を利用できるかどうかという点です。

従来、PV のゲストは HVM のゲストよりも多くの場合にパフォーマンスが向上しました。ただし、HVM 仮想化の機能強化や HVM AMI で PV ドライバが利用可能になったことにより、このようなパフォーマンスの向上はなくなりました。詳細については、「Amazon EC2 ユーザーガイド」の「Linux AMI 仮想化タイプ」を参照してください。

修正

EC2 インスタンスを新しいインスタンスタイプに更新するには、「Amazon EC2 ユーザーガイド」の「インスタンスタイプを変更する」を参照してください。

[EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします

関連する要件： NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7NIST.800-53.r5 SC-7.r5 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7r

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 高

リソースタイプ: `AWS::EC2::LaunchTemplate`

AWS Config ルール : `ec2-launch-template-public-ip-disabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon EC2 起動テンプレートが起動の際にネットワークインターフェイスにパブリック IP アドレスを割り当てる設定になっていないかをチェックします。EC2 起動テンプレートがネットワークインターフェイスにパブリック IP アドレスを割り当てる設定になっている場合、またはパブリック IP アドレスを持つネットワークインターフェイスが 1 つ以上ある場合、コントロールは失敗します。

パブリック IP アドレスは、インターネットから到達可能な IP アドレスです。パブリック IP アドレスを使用してネットワークインターフェイスを設定すると、それらのネットワークインターフェイス

に関連付けられたリソースは、インターネットからアクセスできる可能性があります。EC2 リソースへのパブリックアクセスを可能にすべきではありません。ワークロードへの意図しないアクセスが可能になるおそれがあるためです。

修正

EC2 起動テンプレートを更新するには、「Amazon EC2 Auto Scaling ユーザーガイド」の「デフォルトのネットワークインターフェイス設定を変更する」を参照してください。

[EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

重要度: 低

リソースタイプ : `AWS::EC2::Volume`

AWS Config ルール： `ebs-resources-protected-by-backup-plan`

スケジュールタイプ : 定期的

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`backupVaultLockCheck`	パラメータが `true` に設定されていて、リソースが AWS Backup Vault Lock を使用している場合、コントロールは `PASSED` 検出結果を生成します。	ブール値	`true` 、、または `false`	デフォルト値なし

このコントロールは、`in-use` 状態の Amazon EBS ボリュームがバックアッププランの対象になっているかどうかを評価します。EBS ボリュームがバックアッププランの対象でない場合、コント

ロールは失敗します。`backupVaultLockCheck` パラメータを に設定すると`true`、EBS ボリュームが AWS Backup ロックされたボールトにバックアップされている場合にのみコントロールが成功します。

バックアップは、セキュリティインシデントからより迅速に復元するために役立ちます。また、システムの耐障害性を強化します。バックアッププランに Amazon EBS ボリュームを含めると、意図しない損失や削除からデータを保護できます。

修正

Amazon EBS ボリュームを AWS Backup バックアッププランに追加するには、「 AWS Backup デベロッパーガイド」の「バックアッププランへのリソースの割り当て」を参照してください。

[EC2.33] EC2 Transit Gateway アタッチメントにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::TransitGatewayAttachment`

AWS Config ルール: `tagged-ec2-transitgatewayattachment` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 Transit Gateway アタッチメントに、パラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。Transit

Gateway アタッチメントにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、トランジットゲートウェイアタッチメントにキーがタグ付けされていない場合に失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

EC2 Transit Gateway アタッチメントにタグを追加するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。

[EC2.34] EC2 Transit Gateway ルートテーブルにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::TransitGatewayRouteTable`

AWS Config ルール: `tagged-ec2-transitgatewayroutetable` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 トランジットゲートウェイルートテーブルに、パラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。トランジットゲートウェイルートテーブルにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、トランジットゲートウェイルートテーブルにキーがタグ付けされていない場合に失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。

タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

EC2 トランジットゲートウェイルートテーブルにタグを追加するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。

[EC2.35] EC2 ネットワークインターフェイスにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::NetworkInterface`

AWS Config ルール: `tagged-ec2-networkinterface` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 ネットワークインターフェイスにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。ネットワークインターフェイスにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ネットワークインターフェイス

にキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

EC2 ネットワークインターフェイスにタグを追加するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。

[EC2.36] EC2 カスタマーゲートウェイにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::CustomerGateway`

AWS Config ルール: `tagged-ec2-customergateway` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 カスタマーゲートウェイにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。カスタマーゲートウェイにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、カスタマーゲートウェイにキーがタグ付けされていない場合に失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

EC2 カスタマーゲートウェイにタグを追加するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。

[EC2.37] EC2 Elastic IP アドレスにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::EIP`

AWS Config ルール: `tagged-ec2-eip` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 Elastic IP アドレスに、パラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。Elastic IP アドレスにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、Elastic IP アドレスにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス

許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

EC2 Elastic IP アドレスにタグを追加するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。

[EC2.38] EC2 インスタンスにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::Instance`

AWS Config ルール: `tagged-ec2-instance` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタ	StringList (最大 6 項目)	AWS 要件を満たす 1 ~	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	グキーのリスト。タグキーでは、大文字と小文字が区別されます。		6 個のタグキー。	

このコントロールは、Amazon EC2 インスタンスにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。インスタンスにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、インスタンスにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

EC2 インスタンスにタグを追加するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。

[EC2.39] EC2 インターネットゲートウェイにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::InternetGateway`

AWS Config ルール: `tagged-ec2-internetgateway` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 インターネットゲートウェイにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。インターネットゲートウェイにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、インターネットゲートウェイにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これ

らの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

EC2 インターネットゲートウェイにタグを追加するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。

[EC2.40] EC2 NAT ゲートウェイにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::NatGateway`

AWS Config ルール: `tagged-ec2-natgateway` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 ネットワークアドレス変換 (NAT) ゲートウェイに、パラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。NAT ゲートウェイにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、NAT ゲートウェイにキーがタグ付けされていない場合に失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

EC2 NAT ゲートウェイにタグを追加するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。

[EC2.41] EC2 ネットワーク ACL にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::NetworkAcl`

AWS Config ルール: `tagged-ec2-networkacl` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 ネットワークアクセスコントロールリスト (ネットワーク ACL) に、`requiredTagKeys` パラメータで定義された特定のキーを持つタグがあるかどうかをチェックします。ネットワーク ACL にタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ネットワーク ACL にキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。

タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

EC2 ネットワーク ACL にタグを追加するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。

[EC2.42] EC2 ルートテーブルにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::RouteTable`

AWS Config ルール: `tagged-ec2-routetable` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 ルートテーブルに、パラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。ルートテーブルにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ルートテーブルにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

EC2 ルートテーブルにタグを追加するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。

[EC2.43] EC2 セキュリティグループにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::SecurityGroup`

AWS Config ルール: `tagged-ec2-securitygroup` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 セキュリティグループにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。セキュリティグループにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、セキュリティグループがキーでタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

EC2 セキュリティグループにタグを追加するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付ける」を参照してください。

[EC2.44] EC2 サブネットにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::Subnet`

AWS Config ルール: `tagged-ec2-subnet` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 サブネットにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。サブネットにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、サブネットにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス

許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

EC2 サブネットにタグを追加するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。

[EC2.45] EC2 ボリュームにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::Volume`

AWS Config ルール: `tagged-ec2-volume` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタ	StringList (最大 6 項目)	AWS 要件を満たす 1 ~	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	グキーのリスト。タグキーでは、大文字と小文字が区別されます。		6 個のタグキー。	

このコントロールは、Amazon EC2 ボリュームにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。ボリュームにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ボリュームにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

EC2 ボリュームにタグを追加するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。

[EC2.46] Amazon VPC にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::VPC`

AWS Config ルール: `tagged-ec2-vpc` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon Virtual Private Cloud (Amazon VPC) に、 パラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。Amazon VPC にタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、Amazon VPC にキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これ

らの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

VPC にタグを追加するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。

[EC2.47] Amazon VPC エンドポイントサービスはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::VPCEndpointService`

AWS Config ルール: `tagged-ec2-vpcendpointservice` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon VPC エンドポイントサービスにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。エンドポイントサービスにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、エンドポイントサービスにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

Amazon VPC エンドポイントサービスにタグを追加するには、「AWS PrivateLink ガイド」の「エンドポイントサービスの設定」セクションの「タグの管理」を参照してください。

[EC2.48] Amazon VPC フローログにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::FlowLog`

AWS Config ルール: `tagged-ec2-flowlog` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon VPC フローログにパラメータ `requiredTagKeys` で定義された特定のキーを含むタグがあるかどうかをチェックします。フローログにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、フローログにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。

タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

Amazon VPC フローログにタグを追加するには、「Amazon VPC ユーザーガイド」の「フローログのタグ付け」を参照してください。

[EC2.49] Amazon VPC ピアリング接続にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::VPCPeeringConnection`

AWS Config ルール: `tagged-ec2-vpcpeeringconnection` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon VPC ピアリング接続に、パラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。ピアリング接続にタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ピアリング接続にどのキーもタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

Amazon VPC ピアリング接続にタグを追加するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。

[EC2.50] EC2 VPN ゲートウェイにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::VPNGateway`

AWS Config ルール: `tagged-ec2-vpngateway` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 VPN ゲートウェイにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。VPN ゲートウェイにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、VPN ゲートウェイにキーがタグ付けされていない場合に失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

EC2 VPN ゲートウェイにタグを追加するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。

[EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります

関連する要件： NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6AU-6(3)、NIST.800-53.r5 AU-9 CA-7 NIST.800-53.r5 SC-7 SI-3 SI-4 SI-4 SI-7 3.1.12 3.1.2010.2.1

カテゴリ: 識別 > ログ記録

重要度: 低

リソースタイプ : `AWS::EC2::ClientVpnEndpoint`

AWS Config ルール： `ec2-client-vpn-connection-log-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS Client VPN エンドポイントでクライアント接続のログ記録が有効になっているかどうかを確認します。エンドポイントでクライアント接続ログ記録が有効になっていない場合、コントロールは失敗します。

Client VPN エンドポイントにより、リモートクライアントは AWSの仮想プライベートクラウド (VPC) 内のリソースに安全に接続できます。接続ログにより、VPN エンドポイントでのユーザーアクティビティを追跡し、可視化することができます。接続ログを有効にすると、ロググループ内のログストリームの名前を指定できます。ログストリームを指定しない場合、クライアント VPN サービスによって自動的に作成されます。

修正

接続ログ記録を有効にするには、「AWS Client VPN 管理者ガイド」の「既存のクライアント VPN エンドポイントの接続ログを有効にする」を参照してください。

[EC2.52] EC2 Transit Gateway にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::TransitGateway`

AWS Config ルール: `tagged-ec2-transitgateway` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、Amazon EC2 トランジットゲートウェイにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。トランジットゲートウェイにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、トランジットゲートウェイにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これ

らの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

EC2 トランジットゲートウェイにタグを追加するには、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付ける」を参照してください。

[EC2.53] EC2 セキュリティグループが 0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可することがないようにする必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/5.2、PCI DSS v4.0.1/1.3.1

カテゴリ: 保護 > セキュアなネットワーク設定 > セキュリティグループの設定

重要度: 高

リソースタイプ : `AWS::EC2::SecurityGroup`

AWS Config ルール : `vpc-sg-port-restriction-check`

スケジュールタイプ : 定期的

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`ipType`	IP バージョン	String	カスタマイズ不可	`IPv4`

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`restrictPorts`	入力トラフィックを拒否するポートのリスト	IntegerList	カスタマイズ不可	`22,3389`

このコントロールは、Amazon EC2 セキュリティグループが 0.0.0.0/0 からリモートサーバー管理ポート (ポート 22 と 3389) への入力を許可しているかどうかをチェックします。セキュリティグループが 0.0.0.0/0 からポート 22 または 3389 への入力を許可している場合、コントロールは失敗します。

セキュリティグループは、 AWS リソースへの入力および出力ネットワークトラフィックのステートフルフィルタリングを提供します。TDP (6)、UDP (17)、または ALL (-1) プロトコルのいずれかを使用して、SSH からポート 22、RDP からポート 3389 などのリモートサーバー管理ポートへの無制限の入力アクセスをセキュリティグループで許可しないことをお勧めします。これらのポートへのパブリックアクセスを許可すると、リソースのアタックサーフェスが増加し、リソースが侵害されるリスクが高まります。

修正

指定されたポートへの入力トラフィックを禁止するように EC2 セキュリティグループルールを更新するには、「Amazon EC2 ユーザーガイド」の「セキュリティグループルールの更新」を参照してください。Amazon EC2 コンソールでセキュリティグループを選択したら、[アクション、インバウンドルールの編集] を選択します。ポート 22 または 3389 へのアクセスを許可するルールを削除します。

[EC2.54] EC2 セキュリティグループは ::/0 からリモートサーバー管理ポートへの入力を許可しない必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/5.3、PCI DSS v4.0.1/1.3.1

カテゴリ: 保護 > セキュアなネットワーク設定 > セキュリティグループの設定

重要度: 高

リソースタイプ : `AWS::EC2::SecurityGroup`

AWS Config ルール : `vpc-sg-port-restriction-check`

スケジュールタイプ : 定期的

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`ipType`	IP バージョン	String	カスタマイズ不可	`IPv6`
`restrictPorts`	入力トラフィックを拒否するポートのリスト	IntegerList	カスタマイズ不可	`22,3389`

このコントロールは、Amazon EC2 セキュリティグループが ::/0 からリモートサーバー管理ポート (ポート 22 および 3389) への入力を許可するかどうかをチェックします。セキュリティグループが ::/0 からポート 22 または 3389 への入力を許可している場合、コントロールは失敗します。

セキュリティグループは、 AWS リソースへの入力および出力ネットワークトラフィックのステートフルフィルタリングを提供します。TDP (6)、UDP (17)、または ALL (-1) プロトコルのいずれかを使用して、SSH からポート 22、RDP からポート 3389 などのリモートサーバー管理ポートへの無制限の入力アクセスをセキュリティグループで許可しないことをお勧めします。これらのポートへのパブリックアクセスを許可すると、リソースのアタックサーフェスが増加し、リソースが侵害されるリスクが高まります。

修正

指定されたポートへの入力トラフィックを禁止するように EC2 セキュリティグループルールを更新するには、「Amazon EC2 ユーザーガイド」の「セキュリティグループルールの更新」を参照してください。Amazon EC2 コンソールでセキュリティグループを選択したら、[アクション、インバウンドルールの編集] を選択します。ポート 22 または 3389 へのアクセスを許可するルールを削除します。

[EC2.55] VPCs は ECR API のインターフェイスエンドポイントで設定する必要があります

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)

カテゴリ: 保護 > セキュアなアクセス管理 > アクセスコントロール

重要度: 中

リソースタイプ: `AWS::EC2::VPC`、`AWS::EC2::VPCEndpoint`

AWS Config ルール : vpc-endpoint-enabled

スケジュールタイプ : 定期的

パラメータ :

[Parameter] (パラメータ)	必須	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`serviceNames`	必須	コントロールが評価するサービスの名前	String	カスタマイズ不可	`ecr.api`
`vpcIds`	オプションです。	VPC エンドポイントの Amazon VPC ID のカンマ区切りリスト。指定した場合、`serviceName` パラメータで指定されたサービスにこれらの VPC エンドポイントのいずれかがない場	StringList	1 つ以上の VPC IDs	デフォルト値なし

[Parameter] (パラメータ)	必須	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
		合、コントロールは失敗します。			

このコントロールは、管理する仮想プライベートクラウド (VPC) に Amazon ECR API のインターフェイス VPC エンドポイントがあるかどうかをチェックします。VPC に ECR API 用のインターフェイス VPC エンドポイントがない場合、コントロールは失敗します。このコントロールは、1 つのアカウントのリソースを評価します。

AWS PrivateLink を使用すると、お客様はネットワーク内のすべてのネットワークトラフィックを維持しながら、高可用性でスケーラブルな方法で AWS でホストされているサービスにアクセスできます AWS 。サービスユーザーは、パブリック IPs を使用せずに、インターネットを通過するトラフィックを必要とせずに、VPC またはオンプレミスから PrivateLink を搭載したサービスにプライベートにアクセスできます。

修正

VPC エンドポイントを設定するには、「 AWS PrivateLink ガイド」の「インターフェイス VPC エンドポイント AWS のサービス を使用して にアクセスする」を参照してください。

[EC2.56] VPCsは Docker Registry のインターフェイスエンドポイントで設定する必要があります

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)

カテゴリ: 保護 > セキュアなアクセス管理 > アクセスコントロール

重要度: 中

リソースタイプ: `AWS::EC2::VPC`、`AWS::EC2::VPCEndpoint`

AWS Config ルール : vpc-endpoint-enabled

スケジュールタイプ : 定期的

パラメータ：

[Parameter] (パラメータ)	必須	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`serviceNames`	必須	コントロールが評価するサービスの名前	String	カスタマイズ不可	`ecr.dkr`
`vpcIds`	オプションです。	VPC エンドポイントの Amazon VPC ID のカンマ区切りリスト。指定した場合、`serviceName` パラメータで指定されたサービスにこれらの VPC エンドポイントのいずれかがない場合、コントロールは失敗します。	StringList	1 つ以上の VPC IDs	デフォルト値なし

このコントロールは、管理する仮想プライベートクラウド (VPC) に Docker Registry のインターフェイス VPC エンドポイントがあるかどうかをチェックします。VPC に Docker Registry のインター

フェイス VPC エンドポイントがない場合、コントロールは失敗します。このコントロールは、1 つのアカウントのリソースを評価します。

AWS PrivateLink を使用すると、お客様はネットワーク内のすべてのネットワークトラフィックを維持しながら、高可用性でスケーラブルな方法で AWS でホストされているサービスにアクセスできます AWS 。サービスユーザーは、パブリック IPs を使用せずに、インターネットを通過するトラフィックを必要とせずに、VPC またはオンプレミスから PrivateLink を搭載したサービスにプライベートにアクセスできます。

修正

VPC エンドポイントを設定するには、「 AWS PrivateLink ガイド」の「インターフェイス VPC エンドポイント AWS のサービス を使用して にアクセスする」を参照してください。

[EC2.57] VPCsは Systems Manager のインターフェイスエンドポイントで設定する必要があります

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)

カテゴリ: 保護 > セキュアなアクセス管理 > アクセスコントロール

重要度: 中

リソースタイプ: `AWS::EC2::VPC`、`AWS::EC2::VPCEndpoint`

AWS Config ルール : vpc-endpoint-enabled

スケジュールタイプ : 定期的

パラメータ :

[Parameter] (パラメータ)	必須	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`serviceNames`	必須	コントロールが評価す	String	カスタマイズ不可	`ssm`

[Parameter] (パラメータ)	必須	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
		るサービスの名前			
`vpcIds`	オプションです。	VPC エンドポイントの Amazon VPC ID のカンマ区切りリスト。指定した場合、`serviceName` パラメータで指定されたサービスにこれらの VPC エンドポイントのいずれかがない場合、コントロールは失敗します。	StringList	1 つ以上の VPC IDs	デフォルト値なし

このコントロールは、管理する仮想プライベートクラウド (VPC) にインターフェイス VPC エンドポイントがあるかどうかをチェックします AWS Systems Manager。VPC に Systems Manager のインターフェイス VPC エンドポイントがない場合、コントロールは失敗します。このコントロールは、1 つのアカウントのリソースを評価します。

AWS PrivateLink を使用すると、お客様はネットワーク内のすべてのネットワークトラフィックを維持しながら、高可用性でスケーラブルな方法で AWS でホストされているサービスにアクセスできます AWS 。サービスユーザーは、パブリック IPs を使用せずに、インターネットを通過するトラ

フィックを必要とせずに、VPC またはオンプレミスから PrivateLink を搭載したサービスにプライベートにアクセスできます。

修正

VPC エンドポイントを設定するには、「 AWS PrivateLink ガイド」の「インターフェイス VPC エンドポイント AWS のサービス を使用して にアクセスする」を参照してください。

[EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)

カテゴリ: 保護 > セキュアなアクセス管理 > アクセスコントロール

重要度: 中

リソースタイプ: `AWS::EC2::VPC`、`AWS::EC2::VPCEndpoint`

AWS Config ルール : vpc-endpoint-enabled

スケジュールタイプ : 定期的

パラメータ :

[Parameter] (パラメータ)	必須	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`serviceNames`	必須	コントロールが評価するサービスの名前	String	カスタマイズ不可	`ssm-contacts`
`vpcIds`	オプションです。	VPC エンドポイントの Amazon VPC ID のカンマ区	StringList	1 つ以上の VPC IDs	デフォルト値なし

[Parameter] (パラメータ)	必須	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
		切りリスト。指定した場合、`serviceName` パラメータで指定されたサービスにこれらの VPC エンドポイントのいずれかがない場合、コントロールは失敗します。			

このコントロールは、管理する仮想プライベートクラウド (VPC) に AWS Systems Manager Incident Manager Contacts のインターフェイス VPC エンドポイントがあるかどうかをチェックします。VPC に Systems Manager Incident Manager Contacts のインターフェイス VPC エンドポイントがない場合、コントロールは失敗します。このコントロールは、1 つのアカウントのリソースを評価します。

AWS PrivateLink を使用すると、お客様はネットワーク内のすべてのネットワークトラフィックを維持しながら、高可用性でスケーラブルな方法で AWS でホストされているサービスにアクセスできます AWS 。サービスユーザーは、パブリック IPs を使用せずに、インターネットを通過するトラフィックを必要とせずに、VPC またはオンプレミスから PrivateLink を搭載したサービスにプライベートにアクセスできます。

修正

VPC エンドポイントを設定するには、「 AWS PrivateLink ガイド」の「インターフェイス VPC エンドポイント AWS のサービス を使用して にアクセスする」を参照してください。

[EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)

カテゴリ: 保護 > セキュアなアクセス管理 > アクセスコントロール

重要度: 中

リソースタイプ: `AWS::EC2::VPC`、`AWS::EC2::VPCEndpoint`

AWS Config ルール : vpc-endpoint-enabled

スケジュールタイプ : 定期的

パラメータ :

[Parameter] (パラメータ)	必須	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`serviceNames`	必須	コントロールが評価するサービスの名前	String	カスタマイズ不可	`ssm-incidents`
`vpcIds`	オプションです。	VPC エンドポイントの Amazon VPC ID のカンマ区切りリスト。指定した場合、`serviceName` パラメータで	StringList	1 つ以上の VPC IDs	デフォルト値なし

[Parameter] (パラメータ)	必須	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
		指定されたサービスにこれらの VPC エンドポイントのいずれかがない場合、コントロールは失敗します。			

このコントロールは、管理する仮想プライベートクラウド (VPC) に AWS Systems Manager Incident Manager のインターフェイス VPC エンドポイントがあるかどうかをチェックします。VPC に Systems Manager Incident Manager のインターフェイス VPC エンドポイントがない場合、コントロールは失敗します。このコントロールは、1 つのアカウントのリソースを評価します。

AWS PrivateLink を使用すると、お客様はネットワーク内のすべてのネットワークトラフィックを維持しながら、高可用性でスケーラブルな方法で AWS でホストされているサービスにアクセスできます AWS 。サービスユーザーは、パブリック IPs を使用せずに、インターネットを通過するトラフィックを必要とせずに、VPC またはオンプレミスから PrivateLink を利用したサービスにプライベートにアクセスできます。

修正

VPC エンドポイントを設定するには、「 AWS PrivateLink ガイド」の「インターフェイス VPC エンドポイント AWS のサービス を使用して にアクセスする」を参照してください。

[EC2.170] EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします

関連する要件： PCI DSS v4.0.1/2.2.6

カテゴリ: 保護 > ネットワークセキュリティ

重要度: 低

リソースタイプ : `AWS::EC2::LaunchTemplate`

AWS Config ルール : ec2-launch-template-imdsv2-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon EC2 起動テンプレートが、インスタンスメタデータサービスバージョン 2 (IMDSv2) で設定されているかどうかをチェックします。`HttpTokens` が `optional` に設定されている場合、コントロールは失敗します。

サポートされているソフトウェアバージョンでリソースを実行すると、最適なパフォーマンス、セキュリティ、最新機能へのアクセスが保証されます。定期的な更新は脆弱性から保護するため、安定した効率的なユーザーエクスペリエンスを確保できます。

修正

EC2 起動テンプレートで IMDSv2 を要求するには、「Amazon EC2 ユーザーガイド」の「インスタンスメタデータサービスオプションの設定」を参照してください。

[EC2.171] EC2 VPN 接続では、ログ記録が有効になっている必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/5.3、PCI DSS v4.0.1/10.4.2

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::EC2::VPNConnection`

AWS Config ルール : ec2-vpn-connection-logging-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS Site-to-Site VPN 接続で両方のトンネルに対して Amazon CloudWatch Logs が有効になっているかどうかを確認します。Site-to-Site VPN 接続で両方のトンネルで CloudWatch Logs が有効になっていない場合、コントロールは失敗します。

AWS Site-to-Site VPN ログを使用すると、Site-to-Site VPN デプロイをより詳細に把握できます。この機能を使用すると、IP セキュリティ (IPsec)トンネル確立、インターネットキー交換 (IKE) ネゴシ

エーション、およびデッドピア検出 (DPD) プロトコルメッセージの詳細を示す Site-to-Site VPN 接続ログにアクセスできます。Site-to-Site VPN ログは CloudWatch Logs に発行できます。この機能により、単一の一貫した方法で、すべての Site-to-Site VPN 接続の詳細なログにアクセスして分析できます。

修正

EC2 VPN 接続でトンネルログ記録を有効にするには、「AWS Site-to-Site VPN ユーザーガイド」の「AWS Site-to-Site VPN ログ」を参照してください。

[EC2.172] EC2 VPC ブロックパブリックアクセス設定はインターネットゲートウェイトラフィックをブロックする必要があります

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 中

リソースタイプ : `AWS::EC2::VPCBlockPublicAccessOptions`

AWS Config ルール: `ec2-vpc-bpa-internet-gateway-blocked` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`vpcBpaInternetGatewayBlockMode`	VPC BPA オプションモードの文字列値。	列挙型	`block-bidirectional` , `block-ingress`	デフォルト値なし

このコントロールは、Amazon EC2 VPC Block Public Access (BPA) 設定が、 内のすべての Amazon VPCs のインターネットゲートウェイトラフィックをブロックするように設定されているかどうかを確認します AWS アカウント。VPC BPA 設定がインターネットゲートウェイトラフィックをブロックするように設定されていない場合、コントロールは失

敗します。コントロールを渡すには、VPC BPA を `block-bidirectional`または に設定`InternetGatewayBlockMode`する必要がありますblock-ingress。パラメータが指定されている場合、コントロール`vpcBpaInternetGatewayBlockMode`は の VPC BPA 値が パラメータ`InternetGatewayBlockMode`と一致する場合にのみ渡されます。

でアカウントの VPC BPA 設定 AWS リージョン を構成すると、そのリージョンで所有している VPCs とサブネットのリソースが、インターネットゲートウェイと Egress-Only インターネットゲートウェイを介してインターネットに到達したり、インターネットから到達したりすることをブロックできます。特定の VPCs とサブネットがインターネットに到達可能またはインターネットから到達可能にする必要がある場合は、VPC BPA の除外を設定することでそれらを除外できます。除外の作成と削除の手順については、「Amazon VPC ユーザーガイド」の「除外の作成と削除」を参照してください。

修正

アカウントレベルで双方向 BPA を有効にするには、「Amazon VPC ユーザーガイド」の「アカウントの BPA 双方向モードを有効にする」を参照してください。イングレスのみの BPA を有効にするには、「VPC BPA モードをイングレスのみに変更する」を参照してください。組織レベルで VPC BPA を有効にするには、「組織レベルで VPC BPA を有効にする」を参照してください。

[EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::EC2::SpotFleet`

AWS Config ルール : ec2-spot-fleet-request-ct-encryption-at-rest

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、起動パラメータを指定する Amazon EC2 スポットフリートリクエストがEC2 インスタンスにアタッチされたすべての Amazon Elastic Block Store (Amazon EBS) ボリュームの暗号化を有効にするように設定されているかどうかを確認します。スポットフリートリクエストが起動パラメータを指定し、リクエストで指定された 1 つ以上の EBS ボリュームの暗号化を有効にしない場合、コントロールは失敗します。

セキュリティを強化するために、Amazon EBS ボリュームの暗号化を有効にする必要があります。その後、Amazon EC2 インスタンスをホストするサーバーで暗号化オペレーションが実行され、インスタンスとそのアタッチされた EBS ストレージ間で保管中のデータと転送中のデータの両方のセキュリティが確保されます。Amazon EBS 暗号化は、EC2 インスタンスに関連付けられた EBS リソース用の簡単な暗号化ソリューションです。EBS 暗号化を使用すると、独自のキー管理インフラストラクチャを構築、保守、保護する必要はありません。EBS 暗号化は、暗号化されたボリュームを作成する AWS KMS keys ときに を使用します。

> **メモ**
>
> このコントロールは、起動テンプレートを使用する Amazon EC2 スポットフリートリクエストの結果を生成しません。また、 `encrypted`パラメータの値を明示的に指定しないスポットフリートリクエストの検出結果は生成されません。
> 2025 年 7 月 23 日、Security Hub はこのコントロールのタイトルを変更しました。以前は、このコントロールのタイトルは でしたEC2 Spot Fleet requests should enable encryption for attached EBS volumes。新しいタイトルは、コントロールが起動パラメータを指定するスポットフリートリクエストのみをチェックすることをより正確に反映しています。

修正

暗号化されていない既存の Amazon EBS ボリュームを直接暗号化する方法はありません。新しいボリュームは、作成時にのみ暗号化できます。

ただし、デフォルトで暗号化を有効にすると、Amazon EBS は EBS 暗号化のデフォルトキーを使用して新しいボリュームを暗号化します。デフォルトでは暗号化を有効にしない場合、個々のボリュームを作成するときに暗号化を有効にできます。どちらの場合も、EBS 暗号化のデフォルトキーを上書きし、カスタマー管理の を選択できます AWS KMS key。EBS 暗号化の詳細については、「Amazon EBS ユーザーガイド」の「Amazon EBS 暗号化」を参照してください。

Amazon EC2 スポットフリートリクエストの作成については、「Amazon Elastic Compute Cloud ユーザーガイド」の「スポットフリートの作成」を参照してください。

[EC2.174] EC2 DHCP オプションセットにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::DHCPOptions`

AWS Config ルール : ec2-dhcp-options-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 DHCP オプションセットに `requiredKeyTags`パラメータで指定されたタグキーがあるかどうかをチェックします。オプションセットにタグキーがない場合、または `requiredKeyTags`パラメータで指定されたすべてのキーがない場合、コントロールは失敗します。`requiredKeyTags` パラメータの値を指定しない場合、コントロールはタグキーの存在のみをチェックし、オプションセットにタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、 `aws:` プレフィックスが付いています。

タグは、 AWS リソースを作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの識別、整理、検索、フィルタリングに役立ちます。また、アクションと通知のリソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセスコントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 AWS リソースのタグ付け」および「タグエディタユーザーガイド」を参照してください。

> **Note**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

Amazon EC2 DHCP オプションセットにタグを追加する方法については、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。 Amazon EC2

[EC2.175] EC2 起動テンプレートにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::LaunchTemplate`

AWS Config ルール : ec2-launch-template-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 起動テンプレートに `requiredKeyTags`パラメータで指定されたタグキーがあるかどうかをチェックします。起動テンプレートにタグキーがない場合、または `requiredKeyTags`パラメータで指定されたすべてのキーがない場合、コントロールは失敗します。`requiredKeyTags` パラメータの値を指定しない場合、コントロールはタグキーの存在のみをチェックし、起動テンプレートにタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、 `aws:` プレフィックスが付いています。

タグは、 AWS リソースを作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの識別、整理、検索、フィルタリングに役立ちます。また、アクションと通知のリソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセス

コントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 AWS リソースのタグ付け」および「タグエディタユーザーガイド」を参照してください。

> **Note**
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

Amazon EC2 起動テンプレートにタグを追加する方法については、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。 Amazon EC2

[EC2.176] EC2 プレフィックスリストにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::PrefixList`

AWS Config ルール : ec2-prefix-list-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 プレフィックスリストに `requiredKeyTags`パラメータで指定されたタグキーがあるかどうかをチェックします。プレフィックスリストにタグキーがない場合、または `requiredKeyTags`パラメータで指定されたすべてのキーがない場合、コントロールは失敗します。`requiredKeyTags` パラメータの値を指定しない場合、コントロールはタグキーの存在のみをチェックし、プレフィックスリストにタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、 `aws:` プレフィックスが付いています。

タグは、 AWS リソースを作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの識別、整理、検索、フィルタリングに役立ちます。また、アクションと通知のリソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセスコントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 AWS リソースのタグ付け」と「タグエディタユーザーガイド」を参照してください。

> **Note**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

Amazon EC2 プレフィックスリストにタグを追加する方法については、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。 Amazon EC2

[EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::TrafficMirrorSession`

AWS Config ルール : ec2-traffic-mirror-session-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
requiredKeyTags	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 トラフィックミラーセッションに requiredKeyTagsパラメータで指定されたタグキーがあるかどうかをチェックします。セッションにタグキーがない場合、または requiredKeyTagsパラメータで指定されたすべてのキーがない場合、コントロールは失敗します。requiredKeyTags パラメータに値を指定しない場合、コントロールはタグキーの存在のみをチェックし、セッションにタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、 aws: プレフィックスが付いています。

タグは、 AWS リソースを作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの識別、整理、検索、フィルタリングに役立ちます。また、アクションと通知のリソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセスコントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 AWS リソースのタグ付け」および「タグエディタユーザーガイド」を参照してください。

> **Note**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

Amazon EC2 トラフィックミラーセッションにタグを追加する方法については、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。 Amazon EC2

[EC2.178] EC2 トラフィックミラーフィルターにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::TrafficMirrorFilter`

AWS Config ルール : ec2-traffic-mirror-filter-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 トラフィックミラーフィルターに `requiredKeyTags`パラメータで指定されたタグキーがあるかどうかをチェックします。フィルターにタグキーがない場合、または `requiredKeyTags`パラメータで指定されたすべてのキーがない場合、コントロールは失敗します。`requiredKeyTags` パラメータに値を指定しない場合、コントロールはタグキーの存在のみをチェックし、フィルターにタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、 `aws:` プレフィックスが付いています。

タグは、 AWS リソースを作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの識別、整理、検索、フィルタリングに役立ちます。また、アクションと通知のリソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセスコントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 AWS リソースのタグ付け」および「タグエディタユーザーガイド」を参照してください。

> **Note**
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

Amazon EC2 トラフィックミラーフィルターにタグを追加する方法については、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。 Amazon EC2

[EC2.179] EC2 トラフィックミラーターゲットにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EC2::TrafficMirrorTarget`

AWS Config ルール : ec2-traffic-mirror-target-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されている カスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 トラフィックミラーターゲットに `requiredKeyTags`パラメータで指定されたタグキーがあるかどうかをチェックします。ターゲットにタグキーがない場合、また

は requiredKeyTagsパラメータで指定されたすべてのキーがない場合、コントロールは失敗します。requiredKeyTags パラメータの値を指定しない場合、コントロールはタグキーの存在のみをチェックし、ターゲットにタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、 aws: プレフィックスが付いています。

タグは、 AWS リソースを作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの識別、整理、検索、フィルタリングに役立ちます。また、アクションと通知のリソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセスコントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 AWS リソースのタグ付け」および「タグエディタユーザーガイド」を参照してください。

> **Note**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

Amazon EC2 トラフィックミラーターゲットにタグを追加する方法については、Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースにタグを付ける」を参照してください。 Amazon EC2

[EC2.180] EC2 ネットワークインターフェイスでは、送信元/送信先チェックを有効にする必要があります

カテゴリ: 保護 > ネットワークセキュリティ

重要度: 中

リソースタイプ : AWS::EC2::NetworkInterface

AWS Config ルール : ec2-enis-source-destination-check-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、ユーザーが管理する Amazon EC2 Elastic Network Interface (ENI) で送信元/送信先チェックが有効になっているかどうかを確認します。ユーザー管理の ENI で送信元/送信先チェックが無効になっている場合、コントロールは失敗します。このコントロールは、、`aws_codestar_connections_managed`、`branch`、、`lambda`、および `efa` `interface`のタイプの ENIs のみをチェックします`quicksight`。

Amazon EC2 インスタンスとアタッチされた ENIs の送信元/送信先チェックは、EC2 インスタンス全体で一貫して有効にして設定する必要があります。各 ENI には、送信元/送信先チェック用の独自の設定があります。送信元/送信先チェックが有効になっている場合、Amazon EC2 は送信元/送信先アドレスの検証を適用し、インスタンスが受信するトラフィックの送信元または送信先であることを確認します。これにより、リソースが意図しないトラフィックを処理しないようにし、IP アドレスのスプーフィングを防止することで、ネットワークセキュリティをさらに強化できます。

> **Note**
>
> EC2 インスタンスを NAT インスタンスとして使用していて、その ENI の送信元/送信先チェックを無効にしている場合は、代わりに NAT ゲートウェイを使用できます。

修正

Amazon EC2 ENI の送信元/送信先チェックを有効にする方法については、Amazon EC2 ユーザーガイド」の「ネットワークインターフェイス属性の変更」を参照してください。

Auto Scaling の Security Hub コントロール

これらの Security Hub コントロールは、Amazon EC2 Auto Scaling サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要がある

関連する要件: PCI DSS v3.2.1/2.2、NIST.800-53.r5 CA-7、NIST.800-53.r5 CP-2(2)、NIST.800-53.r5 SI-2

カテゴリ: 識別 > インベントリ

重要度: 低

リソースタイプ : `AWS::AutoScaling::AutoScalingGroup`

AWS Config ルール : `autoscaling-group-elb-healthcheck-required`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、ロードバランサーに関連付けられた Amazon EC2 Auto Scaling グループで、Elastic Load Balancing (ELB) のヘルスチェックが使用されているかどうかをチェックします。Auto Scaling グループが ELB ヘルスチェックを使用しない場合、コントロールは失敗します。

ELB ヘルスチェックにより、ロードバランサーによって提供される追加のテストに基づいて、Auto Scaling グループはインスタンスのヘルスを確実に判断できるようになります。Elastic Load Balancing ヘルスチェックを使用すると、EC2 Auto Scaling グループを使用するアプリケーションの可用性もサポートできます。

修正

Elastic Load Balancing ヘルスチェックを追加するには、「Amazon EC2 Auto Scaling ユーザーガイド」の「Elastic Load Balancing のヘルスチェックを追加する」を参照してください。

[AutoScaling.2] Amazon EC2 Auto Scaling グループは、複数のアベイラビリティーゾーンをカバーする必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-2(2)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::AutoScaling::AutoScalingGroup`

AWS Config ルール : `autoscaling-multiple-az`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値	
`minAvailabilityZones`	アベイラビリティーゾーンの最小数	列挙型	`2, 3, 4, 5, 6`	`2`	

このコントロールは、Amazon EC2 Auto Scaling グループが少なくとも指定された数のアベイラビリティーゾーン (AZ) にまたがっているかどうかをチェックします。Auto Scaling グループが少なくとも指定された数の AZ にまたがっていない場合、コントロールは失敗します。AZ の最小数に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 2 つの AZ を使用します。

複数の AZ にまたがらない Auto Scaling グループは、設定された単一の AZ が使用できなくなった場合、埋め合わせとなる別の AZ ではインスタンスを起動できません。ただし、バッチジョブや AZ 内の転送コストを最小限に抑える必要がある場合など、一部のユースケースでは、単一のアベイラビリティーゾーンを持つ Auto Scaling グループが推奨されることがあります。このような場合は、このコントロールを無効にしたり、検出結果を抑制したりすることができます。

修正

既存の Auto Scaling グループに AZ を追加するには、「Amazon EC2 Auto Scaling ユーザーガイド」の「アベイラビリティーゾーンを追加および削除する」を参照してください。

[AutoScaling.3] Auto Scaling グループ起動設定は、EC2 インスタンスを、インスタンスメタデータサービスバージョン 2 (IMDSv2) を必要とするように設定する必要があります

関連する要件： NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、PCI DSS v4.0.1/2.2.6

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ : `AWS::AutoScaling::LaunchConfiguration`

AWS Config ルール : `autoscaling-launchconfig-requires-imdsv2`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon EC2 Auto Scaling グループが起動するすべてのインスタンスで IMDSv2 が有効になっているかどうかをチェックします。インスタンスメタデータサービス (IMDS) バージョンが起動設定に含まれていない場合、または IMDSv1 または IMDSv2 を許可する設定である `token optional` として設定されている場合、コントロールは失敗します。

IMDS は、インスタンスに関するデータで、実行中のインスタンスを設定または管理するために使用します。

IMDS のバージョン 2 では、EC2 インスタンスの保護を強化するために、IMDSv1 では利用できなかった新しい保護が追加されています。

修正

Auto Scaling グループは、一度に 1 つの起動設定に関連付けられます。起動設定は、作成後に変更することはできません。Auto Scaling グループの起動設定を変更するには、新しい起動設定のベースとして、既存の起動設定を IMDSv2 を有効にした上で使用します。詳細については、「Amazon EC2 ユーザーガイド」の「新規インスタンスのインスタンスメタデータオプションの設定」を参照してください。

[AutoScaling.4] Auto Scaling グループの起動設定では、メタデータ応答ホップ制限が 1 を超えることはできません

> **Important**
>
> Security Hub は、2024 年 4 月にこのコントロールを廃止しました。詳細については、「Security Hub CSPM コントロールの変更ログ」を参照してください。

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ : `AWS::AutoScaling::LaunchConfiguration`

AWS Config ルール : `autoscaling-launch-config-hop-limit`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

これにより、メタデータトークンが移動できる、ネットワークホップの数をチェックします。メタデータの応答ホップ制限が 1 を越えるとコントロールは失敗します。

Instance Metadata Service (IMDS) は、Amazon EC2 インスタンスに関するメタデータ情報を提供するものであり、アプリケーションの設定に役立ちます。メタデータサービスの HTTP PUT 応答を EC2 インスタンスのみに制限することで、IMDS を不正使用から保護します。

IP パケットの Time To Live (TTL) フィールドは、ホップごとに 1 ずつ削減されます。この削減により、パケットを EC2 外に移動させないようにすることができます。IMDSv2 は、オープンルーター、レイヤー 3 ファイアウォール、VPN、トンネル、または NAT デバイスとして誤って構成された可能性のある EC2 インスタンスを保護し、権限のないユーザーがメタデータを取得できないようにします。IMDSv2 では、デフォルトのメタデータ応答ホップ制限が 1 に設定されているため、シークレットトークンを含む PUT 応答は、インスタンスの外に移動することができません。ただし、この値が 1 より大きい場合、トークンは EC2 インスタンスから移動することができます。

修正

既存の起動設定のメタデータ応答ホップ制限を変更する方法については、「Amazon EC2 ユーザーガイド」の「既存インスタンスのインスタンスメタデータオプションの変更」を参照してください。

[Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません

関連する要件： NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)NIST.800-53.r5 SC-7NIST.800-53.r5 SC-75 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-73

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 高

リソースタイプ : `AWS::AutoScaling::LaunchConfiguration`

AWS Config ルール : `autoscaling-launch-config-public-ip-disabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Auto Scaling グループに関連付けられた起動設定が、グループのインスタンスにパブリック IP アドレスを割り当てるかどうかをチェックします。関連付けられた起動設定が、パブリック IP アドレスを割り当てている場合に、このコントロールは失敗します。

Auto Scaling グループの起動設定の Amazon EC2 インスタンスには、限定されたエッジケースを除き、パブリック IP アドレスを関連付けないでください。Amazon EC2 インスタンスは、インターネットに直接公開されるのではなく、ロードバランサーを介した場合のみアクセスできるようにする必要があります。

修正

Auto Scaling グループは、一度に 1 つの起動設定に関連付けられます。起動設定は、作成後に変更することはできません。Auto Scaling グループの起動設定を変更するには、新しい起動設定のベースとして既存の起動設定を使用します。次に、Auto Scaling グループを新しい起動設定を使用するように更新します。手順については、「Amazon EC2 Auto Scaling ユーザーガイド」の「Auto Scaling グループの起動設定を変更する」を参照してください。新しい起動設定を作成する際、[追加設定] にある [高度な詳細] の [IP アドレスタイプ] で、[どのインスタンスにもパブリック IP アドレスを割り当てない] を選択します。

起動設定を変更すると、Auto Scaling は、新しいインスタンスを新しい設定オプションで起動します。既存のインスタンスは影響を受けません。既存のインスタンスを更新するには、インスタンスの更新を行うか、終了ポリシーに基づいて自動スケーリングで古いインスタンスを新しいインスタンスに徐々に置き換えるようにすることをお勧めします。Auto Scaling インスタンスの更新についての詳細は、「Amazon EC2 Auto Scaling ユーザーガイド」の「Auto Scaling インスタンスの更新」を参照してください。

[AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-2(2)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::AutoScaling::AutoScalingGroup`

AWS Config ルール : `autoscaling-multiple-instance-types`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon EC2 Auto Scaling グループが複数のインスタンスタイプを使用しているかどうかをチェックします。Auto Scaling グループで 1 つのインスタンスタイプしか定義されていない場合、そのコントロールは失敗します。

複数のアベイラビリティーゾーンで実行されている複数のインスタンスタイプ間でアプリケーションをデプロイすることで、可用性を向上させることができます。Security Hub では、選択したアベイラビリティーゾーンに十分なインスタンス容量がない場合に Auto Scaling グループが別のインスタンスタイプを起動できるよう、複数のインスタンスタイプを使用することが推奨されます。

修正

複数のインスタンスタイプで Auto Scaling グループを作成するには、「Amazon EC2 Auto Scaling ユーザーガイド」の「複数のインスタンスタイプと購入オプションを使用する Auto Scaling グループ」を参照してください。

[AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 識別 > リソース設定

重要度: 中

リソースタイプ : `AWS::AutoScaling::AutoScalingGroup`

AWS Config ルール : `autoscaling-launch-template`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon EC2 Auto Scaling グループが、EC2 起動テンプレートから作成されたものかどうかを確認します。Amazon EC2 Auto Scaling グループが起動テンプレートを使用して作成されていない場合、または混合インスタンスポリシーで起動テンプレートが指定されていない場合、このコントロールは失敗します。

EC2 Auto Scaling グループは、EC2 起動テンプレートまたは起動設定のいずれかから作成できます。ただし、起動テンプレートを使用して Auto Scaling グループを作成することで、最新の機能や改善点に確実にアクセスできます。

修正

EC2 起動テンプレートを使用して Auto Scaling グループを作成するには、「Amazon EC2 Auto Scalingユーザーガイド」の「起動テンプレートを使用して Auto Scaling グループを作成する」を参照してください。起動設定を起動テンプレートに置き換える方法については、「Amazon EC2 ユーザーガイド」の「起動設定を起動テンプレートに置き換える」を参照してください。

[AutoScaling.10] EC2 Auto Scaling グループにタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::AutoScaling::AutoScalingGroup`

AWS Config ルール: `tagged-autoscaling-autoscalinggroup` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EC2 Auto Scaling グループにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。Auto Scaling グループにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタ

グキーの存在のみをチェックし、Auto Scaling グループがキーでタグ付けされていない場合に失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、のAWS 「リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Auto Scaling グループにタグを追加するには、「Amazon EC2 Auto Scaling ユーザーガイド」の「Auto Scaling グループとインスタンスにタグを付ける」を参照してください。

Amazon ECR の Security Hub コントロール

これらの Security Hub コントロールは、Amazon Elastic Container Registry (Amazon ECR) サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります

関連する要件： NIST.800-53.r5 RA-5、PCI DSS v4.0.1/6.2.3、PCI DSS v4.0.1/6.2.4

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 高

リソースタイプ : `AWS::ECR::Repository`

AWS Config ルール : ecr-private-image-scanning-enabled

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、プライベート Amazon ECR リポジトリでイメージスキャニングが設定されているかどうかをチェックします。プライベート ECR リポジトリがプッシュ時スキャンまたは連続スキャン用に設定されていない場合、コントロールは失敗します。

ECR イメージスキャニングは、コンテナイメージ内のソフトウェアの脆弱性を特定するのに役立ちます。ECR リポジトリでイメージスキャンを設定すると、保存されているイメージの整合性と安全性を検証するレイヤーが追加されます。

修正

ECR リポジトリのイメージスキャニングを設定する方法については、「Amazon Elastic Container Registry User Guide」(Amazon Elastic Container Registry ユーザーガイド) の「Image scanning」(イメージスキャニング) を参照してください。

[ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-8(1)

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 中

リソースタイプ : `AWS::ECR::Repository`

AWS Config ルール : ecr-private-tag-immutability-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、プライベート ECR リポジトリでタグのイミュータビリティが有効になっているかどうかをチェックします。プライベート ECR リポジトリでタグのイミュータビリティが無効になっていると、このコントロールは失敗します。このルールは、タグのイミュータビリティが有効で、かつ値が `IMMUTABLE` に設定されていると成功します。

Amazon ECR のタグのイミュータビリティにより、ユーザーは、イメージの説明タグを信頼性の高いメカニズムとして使用し、イメージを追跡して一意に識別することができます。イミュータブルなタグは静的です。つまり、各タグは一意のイメージを参照します。静的タグを使用すると、常に同じイメージがデプロイされるので、信頼性とスケーラビリティが向上します。設定すると、タグのイミュータビリティにより、タグが上書きされなくなり、アタックサーフェスが減少します。

修正

イミュータブル (変更不可能) なタグが設定されたリポジトリを作成する場合、または既存のリポジトリのイメージタグのイミュータビリティ (変更不可能性) を更新するには、Amazon Elastic Container Registry ユーザーガイドの「イメージタグの変更可能性」を参照してください。

[ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 識別 > リソース設定

重要度: 中

リソースタイプ : `AWS::ECR::Repository`

AWS Config ルール : ecr-private-lifecycle-policy-configured

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon ECR リポジトリに少なくとも 1 つのライフサイクルポリシーが設定されているかどうかをチェックします。ECR リポジトリにライフサイクルポリシーが設定されていない場合、このコントロールは失敗します。

Amazon ECR ライフサイクルポリシーを使用すると、リポジトリ内のイメージのライフサイクル管理を有効にすることができます。ライフサイクルポリシーを設定することで、未使用イメージのク

リーンアップと、年数またはカウントに基づいたイメージの有効期限を自動化することができます。これらのタスクを自動化することで、リポジトリで古いイメージを意図せずに使用することを回避できます。

修正

ライフサイクルポリシーを設定するには、「Amazon Elastic Container Registry ユーザーガイド」の「ライフサイクルポリシーのプレビューを作成する」を参照してください。

[ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::ECR::PublicRepository`

AWS Config ルール: `tagged-ecr-publicrepository` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon ECR パブリックリポジトリにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。パブリックリポジトリにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、パブリックリポジトリにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

ECR パブリックリポジトリにタグを追加するには、「Amazon Elastic Container Registry ユーザーガイド」の「Amazon ECR パブリックリポジトリのタグ付け」を参照してください。

[ECR.5] ECR リポジトリはカスタマーマネージドで暗号化する必要があります AWS KMS keys

関連する要件: NIST.800-53.r5 SC-12(2)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 SI-7(6)、NIST.800-53.r5 AU-9

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::ECR::Repository`

AWS Config ルール : ecr-repository-cmk-encryption-enabled

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`kmsKeyArns`	評価 AWS KMS keys に含める の Amazon リソースネーム (ARNs) のリスト。ECR リポジトリがリスト内の KMS キーで暗号化されていない場合、コントロールは`FAILED`検出結果を生成します。	StringList (最大 10 項目)	既存の KMS キーの ARNs。例: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`	デフォルト値なし

このコントロールは、Amazon ECR リポジトリがカスタマー管理の保管時に暗号化されているかどうかを確認します AWS KMS key。ECR リポジトリがカスタマーマネージド KMS キーで暗号化されていない場合、コントロールは失敗します。オプションで、評価に含めるコントロールの KMS キーのリストを指定できます。

デフォルトでは、Amazon ECR は AES-256 アルゴリズムを使用して Amazon S3 マネージドキー (SSE-S3) でリポジトリデータを暗号化します。追加の制御のために、代わりに AWS KMS key (SSE-KMS または DSSE-KMS) を使用してデータを暗号化するように Amazon ECR を設定できます。KMS キーは、Amazon ECR AWS マネージドキー が作成および管理し、エイリアス を持つ `aws/ecr`、または で作成および管理しているカスタマーマネージドキーです AWS アカウント。カスタマーマネージド KMS キーを使用すると、キーを完全に制御できます。これには、キーポリシーの定義と保守、許可の管理、暗号化マテリアルのローテーション、タグの割り当て、エイリアスの作成、キーの有効化と無効化が含まれます。

> **Note**
>
> AWS KMS は、KMS キーへのクロスアカウントアクセスをサポートしています。ECR リポジトリが別のアカウントが所有する KMS キーで暗号化されている場合、このコントロール

はリポジトリを評価するときにクロスアカウントチェックを実行しません。コントロールは、リポジトリの暗号化オペレーションを実行するときに Amazon ECR がキーにアクセスして使用できるかどうかを評価しません。

修正

既存の ECR リポジトリの暗号化設定を変更することはできません。ただし、後で作成する ECR リポジトリには異なる暗号化設定を指定できます。Amazon ECR は、個々のリポジトリに対して異なる暗号化設定の使用をサポートしています。

ECR リポジトリの暗号化オプションの詳細については、「Amazon ECR ユーザーガイド」の「保管時の暗号化」を参照してください。カスタマー管理の詳細については AWS KMS keys、「 AWS Key Management Service デベロッパーガイドAWS KMS keys」の「」を参照してください。

Amazon ECS の Security Hub コントロール

これらの Security Hub コントロールは、Amazon Elastic Container Service (Amazon ECS) サービスとリソースを評価します。コントロールはすべてで使用できるとは限りません AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 高

リソースタイプ : `AWS::ECS::TaskDefinition`

AWS Config ルール : ecs-task-definition-user-for-host-mode-check

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `SkipInactiveTaskDefinitions`: `true` (カスタマイズ不可)

このコントロールは、ホストネットワークモードを使用するアクティブな Amazon ECS タスク定義に `privileged` または `user` コンテナの定義もあるかどうかをチェックします。ホストネット

ワークモードとコンテナ定義が `privileged=false`、空で、`user=root`、または空のタスク定義では、制御に失敗します。

このコントロールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

この制御の目的は、ホストネットワークモードを使用するタスクを実行するときに、アクセスが意図的に定義されるようにすることです。タスク定義に昇格されたアクセス権限がある場合は、その構成を選択したことによるものです。このコントロールは、タスク定義でホストネットワークが有効になっていても、お客様が昇格されたアクセス権限を選択していない場合に、予期しない権限の昇格の有無をチェックします。

修正

タスク定義を更新する方法については、「Amazon Elastic Container Service 開発者ガイド」の「タスク定義の更新」を参照してください。

タスク定義を更新しても、以前のタスク定義から起動された実行中のタスクは更新されません。実行中のタスクを更新するには、新しいタスク定義を使用してタスクを再デプロイする必要があります。

[ECS.2] ECS サービスには、パブリック IP アドレスを自動で割り当てないでください

関連する要件： NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-75

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 高

リソースタイプ : `AWS::ECS::Service`

AWS Config ルール: `ecs-service-assign-public-ip-disabled` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon ECS サービスがパブリック IP アドレスの自動割り当てが設定されているかどうかをチェックします。`AssignPublicIP` が `ENABLED` の場合、このコントロールは失敗します。`AssignPublicIP` が `DISABLED` の場合、このコントロールは成功です。

パブリック IP アドレスは、インターネットから到達可能な IP アドレスです。パブリック IP アドレスを使用して Amazon ECS インスタンスを起動すると、Amazon ECS インスタンスにインターネットから到達することができます。Amazon ECS サービスは、コンテナアプリケーションサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスができないようにする必要があります。

修正

まず、`awsvpc` ネットワークモードを使用し、`requiresCompatibilities` の FARGATE を指定するクラスターのタスク定義を作成する必要があります。次に、[コンピューティング設定]で、[起動タイプ] と [FARGATE] を選択します。最後に、[ネットワーキング] フィールドで [パブリック IP] をオフにして、サービスの自動パブリック IP 割り当てを無効にします。

[ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 識別 > リソース設定

重要度: 高

リソースタイプ : `AWS::ECS::TaskDefinition`

AWS Config ルール : ecs-task-definition-pid-mode-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon ECS のタスク定義が、ホストのプロセス名前空間をそのコンテナと共有するように設定されているかどうかをチェックします。タスク定義が、ホストのプロセス名前空間を、そこで実行されているコンテナと共有している場合、このコントロールは失敗します。このコントロールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

プロセス ID (PID) 名前空間は、プロセス間を分離します。これにより、システムプロセスが可視化されることを防ぎ、PID 1 を含む PID の再利用が可能になります。ホストの PID 名前空間がコンテナと共有されている場合、コンテナは、ホストシステム上のすべてのプロセスを参照できるようになります。これにより、ホストとコンテナ間をプロセスレベルで分離するメリットが減ります。このような状況は、ホストそれ自体で行われているプロセスへの、不正アクセス (プロセスの操作や終了など) につながる可能性があります。ユーザーは、ホストのプロセス名前空間を、そこで実行されているコンテナと共有すべきではありません。

修正

タスク定義上で `pidMode` を設定する方法については、「Amazon Elastic Container Service デベロッパーガイド」の「タスク定義パラメータ」を参照してください。

[ECS.4] ECS コンテナは、非特権として実行する必要があります

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理 > ルートユーザーのアクセス制限

重要度: 高

リソースタイプ : `AWS::ECS::TaskDefinition`

AWS Config ルール : ecs-containers-nonprivileged

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon ECS のタスク定義の、コンテナ定義の `privileged` パラメータが `true` に設定されているかどうかをチェックします。このパラメータの値が `true` である場合、このコントロールは失敗します。このコントロールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

昇格された特権を、ECS タスク定義から削除することが推奨されます。この特権パラメータが `true` の場合、このコンテナには、ホストコンテナインスタンスに対する昇格された特権が付与されます (ルートユーザーと同様)。

修正

タスク定義上で `privileged` を設定する方法については、「Amazon Elastic Container Service デベロッパーガイド」の「詳細コンテナ定義パラメータ」を参照してください。

[ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 高

リソースタイプ : `AWS::ECS::TaskDefinition`

AWS Config ルール : ecs-containers-readonly-access

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon ECS コンテナがルートファイルシステムへの読み取り専用アクセス権を持っているかどうかをチェックします。`readonlyRootFilesystem` パラメータが に設定されている場合`false`、またはタスク定義内のコンテナ定義に パラメータが存在しない場合、コントロールは失敗します。このコントロールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

Amazon ECS タスク定義`true`で `readonlyRootFilesystem`パラメータが に設定されている場合、ECS コンテナにはルートファイルシステムへの読み取り専用アクセス権が付与されます。これにより、ファイルシステムフォルダとディレクトリの読み取り/書き込み権限を持つ明示的なボリュームマウントがないと、コンテナインスタンスのルートファイルシステムを改ざんしたり書き込んだりできないため、セキュリティ攻撃ベクトルが減少します。このオプションを有効にすると、最小特権の原則にも準拠します。

修正

Amazon ECS コンテナにルートファイルシステムへの読み取り専用アクセスを許可するには、コンテナのタスク定義に `readonlyRootFilesystem`パラメータを追加し、 パラメータの値を に設定します`true`。タスク定義パラメータとそのパラメータをタスク定義に追加する方法については、「Amazon Elastic Container Service デベロッパーガイド」の「Amazon ECS タスク定義」および「タスク定義の更新」を参照してください。

[ECS.8] シークレットは、コンテナ環境の変数として渡さないでください

関連する要件： NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、PCI DSS v4.0.1/8.6.2

カテゴリ: 保護 > セキュアな開発 > 認証情報がハードコーディングされていない

重要度: 高

リソースタイプ : `AWS::ECS::TaskDefinition`

AWS Config ルール : ecs-no-environment-secrets

スケジュールタイプ: 変更がトリガーされた場合

パラメータ： `secretKeys: AWS_ACCESS_KEY_ID、AWS_SECRET_ACCESS_KEY、ECS_ENGINE_AUTH_DATA` (カスタマイズ不可)

このコントロールは、コンテナ定義の `environment` パラメータにある、任意の変数のキー値に、`AWS_ACCESS_KEY_ID`、`AWS_SECRET_ACCESS_KEY`、`ECS_ENGINE_AUTH_DATA` のいずれかが含まれているかどうかをチェックします。任意のコンテナ定義内の単一の環境変数が、`AWS_ACCESS_KEY_ID`、`AWS_SECRET_ACCESS_KEY`、`ECS_ENGINE_AUTH_DATA` のいずれかである場合、このコントロールは失敗します。このコントロールは、Amazon S3 など、他のロケーションから渡される環境変数は対象としません。このコントロールは、Amazon ECS タスク定義の最新のアクティブなリビジョンのみを評価します。

AWS Systems Manager Parameter Store は、組織のセキュリティ体制の改善に役立ちます。シークレットと認証情報は、コンテナインスタンスに直接渡したり、コードにハードコーディングしたりするのではなく、Parameter Store を使用して保存することが推奨されます。

修正

SSM を使用してパラメータを作成する方法については、「AWS Systems Manager ユーザーガイド」の「Systems Manager パラメータを作成する」を参照してください。シークレットを指定するタスク定義の作成に関する詳細は、「Amazon Elastic Container Service デベロッパーガイド」の「Secrets Manager を使用した機密データの指定」を参照してください。

[ECS.9] ECS タスク定義にはログ設定が必要です。

関連する要件: NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 高

リソースタイプ : `AWS::ECS::TaskDefinition`

AWS Config rule: ecs-task-definition-log-configuration

スケジュールタイプ : 変更がトリガーされた場合

パラメータ : なし

このコントロールは、最新のアクティブな Amazon ECS タスク定義にロギング設定が指定されているかどうかを確認します。タスク定義に `logConfiguration` プロパティが定義されていない場合、または少なくとも 1 つのコンテナ定義で `logDriver` の値が null の場合、コントロールは失敗します。

ログ記録は Amazon ECS の信頼性、可用性、パフォーマンスの維持に有益です。タスク定義からデータを収集すると可視性が得られ、プロセスのデバッグやエラーの根本原因の特定に役立ちます。ECS タスク定義で定義する必要のないロギングソリューション (サードパーティのロギングソリューションなど) を使用している場合は、ログを無効にできますが、無効にする前に、ログが適切に取得、保存されていることを確認してください。

修正

Amazon ECS タスク定義のログ設定を定義するには、「Amazon Elastic Container Service デベロッパーガイド」の「タスク定義でログ設定を指定する」を参照してください。

[ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。

関連する要件： NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、PCI DSS v4.0.1/6.3.3

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 中

リソースタイプ : `AWS::ECS::Service`

AWS Config ルール : ecs-fargate-latest-platform-version

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `latestLinuxVersion: 1.4.0` (カスタマイズ不可)
- `latestWindowsVersion: 1.0.0` (カスタマイズ不可)

このコントロールは、Amazon ECS Fargate サービスが最新バージョンの Fargate プラットフォームで実行されているかどうかをチェックします。プラットフォームが最新バージョンでない場合、このコントロールは失敗します。

AWS Fargate プラットフォームバージョンは、Fargate タスクインフラストラクチャの特定のランタイム環境を指します。これは、カーネルランタイムバージョンとコンテナランタイムバージョンの組み合わせです。新しいプラットフォームのバージョンは、ランタイム環境の進化に伴ってリリースされます。例えば、新しいバージョンは、カーネルやオペレーティングシステムの更新、新機能、バグ修正、セキュリティ更新があったときなどにリリースされます。セキュリティの更新やパッチは、 Fargate のタスクに自動的にデプロイされます。プラットフォームバージョンに影響するセキュリティ問題が見つかった場合、 はプラットフォームバージョンを AWS パッチします。

修正

プラットフォームバージョンを含む既存サービスの更新方法については、「Amazon Elastic Container Service デベロッパーガイド」の「サービスの更新」を参照してください。

[ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります

関連する要件: NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::ECS::Cluster`

AWS Config ルール : ecs-container-insights-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、ECS クラスターが Container Insights を使用しているかどうかをチェックします。クラスターで Container Insights がセットアップされていない場合、このコントロールは失敗します。

モニタリングは、Amazon ECS クラスターの信頼性、可用性、パフォーマンスを維持する上で欠かせない要素です。CloudWatch Container Insights を使用して、コンテナ化されたアプリケーションとマイクロサービスのメトリクスとログを収集、集計、要約します。CloudWatch は、CPU やメモリ、ディスク、ネットワークなど、多数のリソースのメトリクスを自動的に収集します。Container Insights では、問題の迅速な特定と解決に役立つ、コンテナの再起動失敗などの診断情報も提供されます。また、Container Insights が収集するメトリクスには CloudWatch アラームを設定できます。

修正

Container Insights の使用方法については、「Amazon CloudWatch ユーザーガイド」の「サービスの更新」を参照してください。

[ECS.13] ECS サービスにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::ECS::Service`

AWS Config ルール: `tagged-ecs-service` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon ECS サービスにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。サービスにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、サービスがキーでタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス

許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

ECS サービスにタグを追加するには、「Amazon Elastic Container Service デベロッパーガイド」の「Amazon ECS リソースにタグを付ける」を参照してください。

[ECS.14] ECS クラスターにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::ECS::Cluster`

AWS Config ルール: `tagged-ecs-cluster` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタ	StringList (最大 6 項目)	AWS 要件を満たす 1 ~	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	グキーのリスト。タグキーでは、大文字と小文字が区別されます。		6 個のタグキー。	

このコントロールは、Amazon ECS クラスターにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。クラスターにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、クラスターにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

ECS クラスターにタグを追加するには、「Amazon Elastic Container Service デベロッパーガイド」の「Amazon ECS リソースにタグを付ける」を参照してください。

[ECS.15] ECS タスク定義にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::ECS::TaskDefinition`

AWS Config ルール: `tagged-ecs-taskdefinition` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon ECS タスク定義に、パラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。タスク定義にタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、タスク定義にキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するよう

に設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

ECS タスク定義にタグを追加するには、「Amazon Elastic Container Service デベロッパーガイド」の「Amazon ECS リソースのタグ付け」を参照してください。

[ECS.16] ECS タスクセットはパブリック IP アドレスを自動的に割り当てないでください。

関連する要件： PCI DSS v4.0.1/1.4.4

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 高

リソースタイプ : `AWS::ECS::TaskSet`

AWS Config ルール: `ecs-taskset-assign-public-ip-disabled` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon ECS タスクセットがパブリック IP アドレスの自動割り当てが設定されているかどうかをチェックします。`AssignPublicIP` が `ENABLED` に設定されている場合、コントロールは失敗します。

パブリック IP アドレスは、インターネットから到達可能です。タスクセットをパブリック IP アドレスで設定すると、タスクセットに関連付けられたリソースにインターネットからアクセスできます。ECS タスクセットは、コンテナアプリケーションサーバーへの意図しないアクセスを許可する可能性があるため、パブリックにアクセスができないようにする必要があります。

修正

パブリック IP アドレスを使用しないように ECS タスクセットを更新するには、「Amazon Elastic Container Service デベロッパーガイド」の「コンソールを使用した Amazon ECS タスク定義の更新」を参照してください。

[ECS.17] ECS タスク定義はホストネットワークモードを使用しないでください

関連する要件： NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ : `AWS::ECS::TaskDefinition`

AWS Config ルール : ecs-task-definition-network-mode-not-host

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon ECS タスク定義の最新のアクティブなリビジョンが`host`ネットワークモードを使用しているかどうかをチェックします。ECS タスク定義の最新のアクティブなリビジョンが`host`ネットワークモードを使用している場合、コントロールは失敗します。

`host` ネットワークモードを使用する場合、Amazon ECS コンテナのネットワークは、コンテナを実行している基盤となるホストに直接関連付けられます。したがって、このモードでは、コンテナはホスト上のプライベートループバックネットワークサービスに接続し、ホストを偽装できます。その他の大きな欠点は、`host`ネットワークモードを使用する場合にコンテナポートを再マッピングする方法がなく、各ホストでタスクを 1 回だけインスタンス化できないことです。

修正

Amazon EC2 インスタンスでホストされる Amazon ECS タスクのネットワークモードとオプションについては、「Amazon Elastic Container Service デベロッパーガイド」のEC2 起動タイプの Amazon ECS タスクネットワークオプション」を参照してください。 タスク定義の新しいリビジョンを作成し、別のネットワークモードを指定する方法については、そのガイドの「Amazon ECS タスク定義の更新」を参照してください。

Amazon ECS タスク定義が によって作成された場合は AWS Batch、「ジョブのネットワークモード」を参照して、 AWS Batchジョブ AWS Batch タイプのネットワークモードと一般的な使用方法を確認し、安全なオプションを選択します。

Amazon EFS の Security Hub コントロール

これらの Security Hub コントロールは、Amazon Elastic File System (Amazon EFS) サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS

関連する要件： CIS AWS Foundations Benchmark v3.0.0/2.4.1、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::EFS::FileSystem`

AWS Config ルール : efs-encrypted-check

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon Elastic File System が を使用してファイルデータを暗号化するように設定されているかどうかを確認します AWS KMS。次の場合、チェックは失敗します。

- `DescribeFileSystems` レスポンスで `Encrypted` は、`false` に設定されている。
- `DescribeFileSystems` レスポンスの `KmsKeyId` キーが `efs-encrypted-check` の `KmsKeyId` パラメータと一致しない。

このコントロールでは、`efs-encrypted-check` の `KmsKeyId` パラメータを使用しないことに注意してください。`Encrypted` の値のみをチェックします。

Amazon EFS で機密データのセキュリティを強化するには、暗号化されたファイルシステムを作成する必要があります。Amazon EFS は保管時のファイルシステムの暗号化をサポートしま

す。Amazon EFS ファイルシステムを作成する場合、保管中のデータの暗号化を有効にすることができます。Amazon EFS 暗号化の詳細については、「Amazon Elastic File System ユーザーガイド」の「Amazon EFS でのデータ暗号化」を参照してください。

修正

新しい Amazon EFS ファイルシステムを暗号化する方法の詳細については、「Amazon Elastic File System ユーザーガイド」の「保管中のデータの暗号化」を参照してください。

[EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > バックアップ

重要度: 中

リソースタイプ : `AWS::EFS::FileSystem`

AWS Config ルール : efs-in-backup-plan

スケジュールタイプ : 定期的

パラメータ: なし

このコントロールは、Amazon Elastic File System (Amazon EFS) ファイルシステムが AWS Backup のバックアッププランに追加されているかどうかをチェックします。Amazon EFS ファイルシステムがバックアッププランに含まれていない場合、コントロールは失敗します。

バックアッププランに EFS ファイルシステムを組み込むと、データの削除やデータの損失からデータを保護できます。

修正

既存の Amazon EFS ファイルシステムの自動バックアップを有効にするには、AWS Backup デベロッパーガイドの「開始方法 4: Amazon EFS 自動バックアップの作成」を参照してください。

[EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります

関連する要件: NIST.800-53.r5 AC-6(10)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::EFS::AccessPoint`

AWS Config ルール : efs-access-point-enforce-root-directory

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon EFS アクセスポイントが、ルートディレクトリを適用するように設定されているかどうかをチェックします。`Path` の値が `/` (ファイルシステムのデフォルトのルートディレクトリ) に設定されていると、このコントロールは失敗します。

ルートディレクトリを適用すると、アクセスポイントを使用する NFS クライアントは、ファイルシステムのルートディレクトリではなく、アクセスポイントに設定されているルートディレクトリを使用します。アクセスポイントのルートディレクトリを適用すると、アクセスポイントのユーザーを、指定されたサブディレクトリのファイルにのみアクセスさせ、データアクセスを制限することができます。

修正

EFS アクセスポイントのルートディレクトリを適用する方法については、Amazon Elastic File System ユーザーガイドの「アクセスポイントでルートディレクトリを適用する」を参照してください。

[EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります

関連する要件： NIST.800-53.r5 AC-6(2)、PCI DSS v4.0.1/7.3.1

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::EFS::AccessPoint`

AWS Config ルール : efs-access-point-enforce-user-identity

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon EFS アクセスポイントが、ユーザーアイデンティティを適用するように設定されているかどうかをチェックします。EFS アクセスポイントの作成中に POSIX ユーザー ID が定義されていない場合、このコントロールは失敗します。

Amazon EFS アクセスポイントは、EFS ファイルシステムへのアプリケーション固有のエントリポイントです。これにより、共有データセットへのアプリケーションアクセスが管理しやすくなります。アクセスポイントを使用すると、アクセスポイントを介したすべてのファイルシステム要求に対してユーザーアイデンティティ (ユーザーの POSIX グループなど) を適用できます。また、ファイルシステムに対して別のルートディレクトリを適用し、このディレクトリまたはそのサブディレクトリ内のデータに対してのみ、クライアントにアクセスを許可することもできます。

修正

Amazon EFS アクセスポイントのユーザーアイデンティティを適用する方法については、Amazon Elastic File System ユーザーガイドの「アクセスポイントを使用したユーザ ID の適用」を参照してください。

[EFS .5] EFS アクセスポイントにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EFS::AccessPoint`

AWS Configルール: `tagged-efs-accesspoint` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EFS アクセスポイントにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。アクセスポイントにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、アクセスポイントにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。IAM エンティティ (ユーザーまたはロール) と AWS リソースにタグをアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EFS アクセスポイントにタグを追加するには、「Amazon Elastic File System ユーザーガイド」の「Amazon EFS リソースのタグ付け」を参照してください。

[EFS.6] EFS マウントターゲットは、起動時にパブリック IP アドレスを割り当てるサブネットに関連付けるべきではありません

カテゴリ： 保護 > ネットワークセキュリティ > パブリックにアクセスできないリソース

重要度: 中

リソースタイプ : `AWS::EFS::FileSystem`

AWS Config ルール : efs-mount-target-public-accessible

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon EFS マウントターゲットが、起動時にパブリック IP アドレスを割り当てるサブネットに関連付けられているかどうかをチェックします。マウントターゲットが起動時にパブリック IP アドレスを割り当てるサブネットに関連付けられている場合、コントロールは失敗します。

すべてのサブネットには、サブネット内に作成されたネットワークインターフェイスが自動的にパブリック IPv4 アドレスを受信するかどうかを判断する属性があります。この属性が有効になっているサブネットで起動される Amazon EFS マウントターゲットには、プライマリネットワークインターフェイスにパブリック IP アドレスが割り当てられます。

> **Note**
>
> 2025 年 8 月 13 日、Security Hub はこのコントロールのタイトルと説明を変更しました。新しいタイトルと説明は、コントロールが実行するチェックの範囲と性質をより正確に反映します。以前は、このコントロールのタイトルは でしたEFS mount targets should not be associated with a public subnet。

修正

既存のマウントターゲットを別のサブネットに関連付けるには、起動時にパブリック IP アドレスを割り当てないサブネットに新しいマウントターゲットを作成し、古いマウントターゲットを削除する必要があります。マウントターゲットの管理については、「Amazon Elastic File System ユーザーガイド」の「マウントターゲットとセキュリティグループの作成と管理」を参照してください。

[EFS .7] EFS ファイルシステムでは、自動バックアップが有効になっている必要があります

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

重要度: 中

リソースタイプ : `AWS::EFS::FileSystem`

AWS Config ルール : efs-automatic-backups-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon EFS ファイルシステムに自動バックアップが有効になっているかどうかを確認します。EFS ファイルシステムに自動バックアップが有効になっていない場合、このコントロールは失敗します。

データバックアップは、システム、設定、またはアプリケーションデータのコピーであり、元のデータとは別に保存されます。定期的なバックアップを有効にすると、システム障害、サイバー攻撃、偶発的な削除などの予期しないイベントから貴重なデータを保護することができます。堅牢なバックアップ戦略を持つことで、データ損失の可能性に直面しても、より迅速な復旧、事業継続性、安心感が得られます。

修正

AWS Backup EFS ファイルシステムで を使用する方法については、「Amazon Elastic File System ユーザーガイド」のEFS ファイルシステムのバックアップ」を参照してください。 Amazon Elastic File System

[EFS .8] EFS ファイルシステムは保管中に暗号化する必要があります

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::EFS::FileSystem`

AWS Config ルール : efs-filesystem-ct-encrypted

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon EFS ファイルシステムが AWS Key Management Service () でデータを暗号化しているかどうかをチェックしますAWS KMS。ファイルシステムが暗号化されていない場合、コントロールは失敗します。

保管中のデータとは、永続的な不揮発性ストレージに任意の期間保管されているデータを指します。保管中のデータを暗号化すると、その機密性が保護され、権限のないユーザーがアクセスするリスクが低減されます。

修正

新しい EFS ファイルシステムの保管中の暗号化を有効にするには、「Amazon Elastic File System ユーザーガイド」の「保管中のデータの暗号化」を参照してください。

Amazon EKS の Security Hub コントロール

これらの Security Hub コントロールは、Amazon Elastic Kubernetes Service (Amazon EKS) サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります

関連する要件： NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7NIST.800-53.r5 SC-7.r5 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7r

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 高

リソースタイプ : `AWS::EKS::Cluster`

AWS Config ルール : eks-endpoint-no-public-access

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon EKS クラスターエンドポイントがパブリックにアクセス可能かどうかをチェックします。EKS クラスターにパブリックにアクセス可能なエンドポイントがある場合、コントロールは失敗します。

新しいクラスターを作成すると、Amazon EKS によって、マネージド型 Kubernetes API サーバー用にエンドポイントが作成されます。このエンドポイントは、ユーザーがクラスターとの通信に使用します。デフォルトでは、この API サーバーエンドポイントはインターネットで公開されています。API サーバーへのアクセスは、 AWS Identity and Access Management (IAM) とネイティブ Kubernetes ロールベースアクセスコントロール (RBAC) の組み合わせを使用して保護されます。エンドポイントへのパブリックアクセスを削除することで、意図しない公開やクラスターへのアクセスを防ぐことができます。

修正

既存の EKS クラスターのエンドポイントアクセスを変更するには、「Amazon EKS ユーザーガイド」の「クラスターエンドポイントのアクセスの変更」を参照してください。新しい EKS クラスターの作成時に、エンドポイントアクセスを設定できます。新しい Amazon EKS クラスターを作成

する手順については、「Amazon EKS ユーザーガイド」の「Amazon EKS クラスターの作成」を参照してください。

[EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。

関連する要件： NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、PCI DSS v4.0.1/12.3.4

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 高

リソースタイプ : `AWS::EKS::Cluster`

AWS Config ルール : eks-cluster-supported-version

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `oldestVersionSupported`: `1.31` (カスタマイズ不可)

このコントロールは、Amazon Elastic Kubernetes Service (Amazon EKS) クラスターが、サポートされている Kubernetes バージョンで実行されるかどうかをチェックします。EKS クラスターがサポートされていないバージョンで実行される場合、このコントロールは失敗します。

アプリケーションが Kubernetes の特定のバージョンを必要としない場合は、EKS がクラスター用にサポートしている、Kubernetes の使用可能な最新バージョンを使用することが推奨されます。詳細については、「Amazon EKS ユーザーガイド」の「Amazon EKS Kubernetes リリースカレンダー」および「Amazon EKS の Kubernetes バージョンライフサイクルを理解する」を参照してください。

修正

EKS クラスターを更新するには、「Amazon EKS ユーザーガイド」の「既存のクラスターを新しい Kubernetes バージョンに更新する」を参照してください。

[EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります

関連する要件： NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-12、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、PCI DSS v4.0.1/8.3.2

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::EKS::Cluster`

AWS Config ルール : eks-cluster-secrets-encrypted

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon EKS クラスターが暗号化された Kubernetes シークレットを使用しているかどうかを確認します。クラスターの Kubernetes シークレットが暗号化されていない場合、コントロールは失敗します。

シークレットを暗号化するときは、 AWS Key Management Service （ AWS KMS) キーを使用して、クラスターの etcd に保存されている Kubernetes シークレットのエンベロープ暗号化を提供できます。この暗号化は、EKS クラスターの一部として etcd に保存されているすべてのデータ (シークレットを含む) に対してデフォルトで有効になっている EBS ボリューム暗号化に加えて行われます。EKS クラスターにシークレット暗号化を使用すると、定義して管理する KMS キーを使用して Kubernetes シークレットを暗号化することで、Kubernetes アプリケーションの防御を詳細にデプロイできます。

修正

EKS クラスターでシークレット暗号化を有効にするには、「Amazon EKS ユーザーガイド」の「既存のクラスターでシークレット暗号化を有効にする」を参照してください。

[EKS.6] EKS クラスターにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EKS::Cluster`

AWS Config ルール: `tagged-eks-cluster` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EKS クラスターにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。クラスターにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、クラスターにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、のAWS 「リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EKS クラスターにタグを追加するには、「Amazon EKS ユーザーガイド」の「Amazon EKS リソースのタグ付け」を参照してください。

[EKS.7] EKS ID プロバイダーの設定にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::EKS::IdentityProviderConfig`

AWS Config ルール: `tagged-eks-identityproviderconfig` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EKS ID プロバイダー設定に、パラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。設定にタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、設定にキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあ

るリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EKS ID プロバイダー設定にタグを追加するには、「Amazon EKS ユーザーガイド」の「Amazon EKS リソースのタグ付け」を参照してください。

[EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります

関連する要件： NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6AU-6(3)、NIST.800-53.r5 AU-9 CA-7 NIST.800-53.r5 SC-7 SI-3 SI-4 SI-4 SI-710.2.1

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::EKS::Cluster`

AWS Config ルール : eks-cluster-log-enabled

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `logTypes: audit` (カスタマイズ不可)

このコントロールは、Amazon EKS クラスターで監査ログ記録が有効になっているかどうかをチェックします。クラスターで監査ログ記録が有効になっていない場合、コントロールは失敗します。

> **Note**
>
> このコントロールは、 AWS アカウントの Amazon Security Lake を介して Amazon EKS 監査ログ記録が有効になっているかどうかをチェックしません。

EKS コントロールプレーンのログ記録により、アカウント内で EKS コントロールプレーンから Amazon CloudWatch Logs に対し、監査および診断ログを直接送れるようになります。必要なログタイプを選択することで、CloudWatch 内で各 EKS クラスターのためのグループに対し、ログストリームの形態でログを送信できます。ログ記録により、EKS クラスターのアクセスとパフォーマンスを可視化できます。EKS クラスターの EKS コントロールプレーンログを CloudWatch Logs に送信することで、監査と診断を目的とした操作を一元的な場所に記録できます。

修正

EKS クラスターの監査ログを有効にするには、「Amazon EKS ユーザーガイド」の「コントロールプレーンログの有効化と無効化」を参照してください。

ElastiCache の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon ElastiCache サービスとリソースを評価します。

これらのコントロールは、一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

重要度: 高

リソースタイプ: `AWS::ElastiCache::CacheCluster`、`AWS:ElastiCache:ReplicationGroup`

AWS Config ルール : elasticache-redis-cluster-automatic-backup-check

スケジュールタイプ : 定期的

パラメータ:

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`snapshotRetentionPeriod`	最小スナップショット保持期間 (日数)	整数	1 ~ 35	1

このコントロールは、Amazon ElastiCache (Redis OSS) クラスターに自動バックアップがスケジュールされているかどうかを評価します。Redis クラスターの `SnapshotRetentionLimit` が指定された期間未満の場合、コントロールは失敗します。スナップショット保持期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 1 日を使用します。

Amazon ElastiCache (Redis OSS) クラスターでは、データをバックアップできます。バックアップを使用して、クラスターを復元したり、新しいクラスターをシードしたりできます。バックアップは、クラスター内の全データとクラスターのメタデータで構成されます。すべてのバックアップは、耐久性のあるストレージを提供する Amazon Simple Storage Service (Amazon S3) に書き込まれます。新しい Redis クラスターを作成し、バックアップのデータを挿入することでデータを復元できます。バックアップは、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、および ElastiCache API を使用して管理できます。

修正

ElastiCache (Redis OSS) クラスターで自動バックアップをスケジュールするには、「Amazon ElastiCache ユーザーガイド」の「自動バックアップのスケジュール」を参照してください。

[ElastiCache.2] ElastiCache クラスターでは、マイナーバージョンの自動アップグレードを有効にする必要があります

関連する要件： NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5) PCI DSS v4.0.1/6.3.3

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 高

リソースタイプ : `AWS::ElastiCache::CacheCluster`

AWS Config ルール : `elasticache-auto-minor-version-upgrade-check`

スケジュールタイプ: 定期的

パラメータ : なし

このコントロールは、Amazon ElastiCache がキャッシュクラスターにマイナーバージョンアップグレードを自動的に適用するかどうかを評価します。キャッシュクラスターにマイナーバージョンアップグレードが自動的に適用されていない場合、コントロールは失敗します。

> **Note**
>
> このコントロールは、ElastiCache Memcached クラスターには適用されません。

自動マイナーバージョンアップグレードは、Amazon ElastiCache で有効にして、新しいマイナーキャッシュエンジンバージョンが利用可能になったときにキャッシュクラスターを自動的にアップグレードできる機能です。これらのアップグレードには、セキュリティパッチとバグ修正を含む場合があります。パッチのインストールを最新の状態に保つことは、システムを保護する上で重要なステップです。

修正

既存の ElastiCache キャッシュクラスターにマイナーバージョンアップグレードを自動的に適用するには、「Amazon ElastiCache ユーザーガイド」の「ElastiCache のバージョン管理」を参照してください。 Amazon ElastiCache

[ElastiCache.3] ElastiCache (Redis OSS) レプリケーショングループでは、自動フェイルオーバーを有効にする必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::ElastiCache::ReplicationGroup`

AWS Config ルール : `elasticache-repl-grp-auto-failover-enabled`

スケジュールタイプ: 定期的

パラメータ : なし

このコントロールは、ElastiCache レプリケーショングループで自動フェイルオーバーが有効になっているかどうかを確認します。レプリケーショングループに対して自動フェイルオーバーが有効になっていない場合、コントロールは失敗します。

レプリケーショングループで自動フェイルオーバーを有効にすると、プライマリノードのロールは、いずれかのリードレプリカに自動的にフェイルオーバーされます。このフェイルオーバーとレプリカの昇格により、昇格の完了後すぐに新しいプライマリへの書き込みを再開できるため、障害発生時も全体のダウンタイムを短縮できます。

修正

既存の ElastiCache レプリケーショングループの自動フェイルオーバーを有効にするには、「Amazon ElastiCache ユーザーガイド」の「ElastiCache クラスターの変更」を参照してください。 Amazon ElastiCache ElastiCache コンソールを使用する場合は、[自動フェイルオーバー] を有効に設定します。

[ElastiCache.4] ElastiCache レプリケーショングループは保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::ElastiCache::ReplicationGroup`

AWS Config ルール : `elasticache-repl-grp-encrypted-at-rest`

スケジュールタイプ: 定期的

パラメータ : なし

このコントロールは、ElastiCache レプリケーショングループが保管中に暗号化されているかどうかをチェックします。レプリケーショングループが保管時に暗号化されていない場合、コントロールは失敗します。

保管中のデータを暗号化すると、認証されていないユーザーがディスクに保存しているデータにアクセスするリスクが低減されます。ElastiCache (Redis OSS) レプリケーショングループは、セキュリティを強化するために、保管中に暗号化する必要があります。

修正

ElastiCache レプリケーショングループの保管時の暗号化を設定するには、Amazon ElastiCache ユーザーガイド」の「保管時の暗号化の有効化」を参照してください。

[ElastiCache.5] ElastiCache レプリケーショングループは転送時に暗号化する必要があります

関連する要件： NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8-53.rNIST.800-53.r5 SC-8 SI-75

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::ElastiCache::ReplicationGroup`

AWS Config ルール : `elasticache-repl-grp-encrypted-in-transit`

スケジュールタイプ: 定期的

パラメータ : なし

このコントロールは、ElastiCache レプリケーショングループが転送中に暗号化されているかどうかをチェックします。レプリケーショングループが転送中に暗号化されていない場合、コントロールは失敗します。

転送中のデータを暗号化することで、権限のないユーザーがネットワークトラフィックを盗聴するリスクが軽減されます。ElastiCache レプリケーショングループで転送中の暗号化を有効にすると、ク

ラスター内のノード間やクラスターとアプリケーション間など、ある場所から別の場所に移動するたびにデータが暗号化されます。

修正

ElastiCache レプリケーショングループで転送時の暗号化を設定するには、Amazon ElastiCache ユーザーガイド」の「転送時の暗号化の有効化」を参照してください。

[ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります

関連する要件： NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6、PCI DSS v4.0.1/8.3.1

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::ElastiCache::ReplicationGroup`

AWS Config ルール : `elasticache-repl-grp-redis-auth-enabled`

スケジュールタイプ: 定期的

パラメータ : なし

このコントロールは、ElastiCache (Redis OSS) レプリケーショングループの Redis OSS AUTH が有効になっているかどうかを確認します。Redis OSS バージョンが 6.0 より前で `AuthToken` が使用されていない場合、ElastiCache for Redis レプリケーショングループのコントロールは失敗します。

Redis 認証トークンまたはパスワードを使用すると、Redis はクライアントにコマンドの実行を許可する前にパスワードを要求するため、データのセキュリティが向上します。Redis 6.0 以降のバージョンでは、ロールベースのアクセス制御 (RBAC) の使用をお勧めします。RBAC は 6.0 より前のバージョンの Redis ではサポートされていないため、このコントロールは RBAC 機能を使用できないバージョンのみを評価します。

修正

ElastiCache (Redis OSS) レプリケーショングループで Redis AUTH を使用するには、「Amazon ElastiCache ユーザーガイド」の「既存の ElastiCache (Redis OSS) クラスターでの AUTH トークンの変更」を参照してください。

[ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください

関連する要件: NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(5)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ : `AWS::ElastiCache::CacheCluster`

AWS Config ルール : `elasticache-subnet-group-check`

スケジュールタイプ: 定期的

パラメータ : なし

このコントロールは、ElastiCache クラスターにカスタムサブネットグループが設定されているかどうかを確認します。ElastiCache クラスターの `CacheSubnetGroupName` の値が `default` である場合、コントロールは失敗します。

ElastiCache クラスターを起動すると、デフォルトのサブネットグループがまだ存在しない場合は作成されます。デフォルトグループは、デフォルトの仮想プライベートクラウド (VPC) のサブネットを使用します。クラスターが存在するサブネットや、クラスターがサブネットから継承するネットワークの制限機能がより強力な、カスタムサブネットグループを使用することをお勧めします。

修正

ElastiCache クラスターの新しいサブネットグループを作成するには、「Amazon ElastiCache ユーザーガイド」の「サブネットグループの作成」を参照してください。

Elastic Beanstalk の Security Hub コントロール

これらの AWS Security Hub コントロールは、 AWS Elastic Beanstalk サービスとリソースを評価します。

これらのコントロールは、一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。

関連する要件: NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2

カテゴリ: 検出 > 検出サービス > アプリケーションモニタリング

重要度: 低

リソースタイプ : `AWS::ElasticBeanstalk::Environment`

AWS Config ルール : `beanstalk-enhanced-health-reporting-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、 AWS Elastic Beanstalk 環境で拡張ヘルスレポートが有効になっているかどうかをチェックします。

Elastic Beanstalk 拡張ヘルスレポートにより、基盤となるインフラストラクチャの健全性の変化に対するより迅速な対応が可能になります。これらの変更は、アプリケーションの可用性を低下させる可能性があります。

Elastic Beanstalk 拡張ヘルスレポートは、特定された問題の重要度を測定し、調査すべき可能性のある原因を特定するためのステータス記述子を提供します。サポートされている Amazon マシンイメージ (AMI) に含まれる Elastic Beanstalk ヘルスエージェントは、環境 EC2 インスタンスのログとメトリクスを評価します。

詳細については、「AWS Elastic Beanstalk 開発者ガイド」の「拡張ヘルスレポートおよびモニタリング」を参照してください。

修正

拡張ヘルスレポートを有効にする手順については、「AWS Elastic Beanstalk 開発者ガイド」の「Elastic Beanstalk コンソールを使用した拡張ヘルスレポートの有効化」を参照してください。

[ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります

関連する要件： NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、PCI DSS v4.0.1/6.3.3

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 高

リソースタイプ : `AWS::ElasticBeanstalk::Environment`

AWS Config ルール : `elastic-beanstalk-managed-updates-enabled`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`UpdateLevel`	バージョン更新レベル	列挙型	`minor`, `patch`	デフォルト値なし

このコントロールは、Elastic Beanstalk 環境でマネージドプラットフォームの更新が有効になっているかどうかをチェックします。マネージドプラットフォームの更新が有効になっていない場合、コントロールは失敗します。デフォルトでは、何らかのプラットフォーム更新が有効になっていればコントロールは成功します。必要に応じて、特定の更新レベルを要求するカスタムパラメータ値を指定できます。

マネージドプラットフォームの更新を有効にすると、環境で使用可能な最新のプラットフォームの修正、更新、および機能がインストールされます。パッチのインストールを最新の状態に保つことは、システムを保護する上で重要なステップです。

修正

マネージドプラットフォームの更新を有効にするには、「AWS Elastic Beanstalk 開発者ガイド」の「マネージドプラットフォームの更新でマネージドプラットフォームの更新を設定するには」を参照してください。

[ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります

関連する要件： PCI DSS v4.0.1/10.4.2

カテゴリ: 識別 > ログ記録

重要度: 高

リソースタイプ : `AWS::ElasticBeanstalk::Environment`

AWS Config ルール : `elastic-beanstalk-logs-to-cloudwatch`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`RetentionInDays`	有効期限が切れるまでログイベントを保持する日数	列挙型	`1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365 , 400, 545, 731, 1827, 3653`	デフォルト値なし

このコントロールは、Elastic Beanstalk 環境が CloudWatch Logs にログを送信するように設定されているかどうかをチェックします。Elastic Beanstalk 環境が CloudWatch Logs にログを送信するように設定されていない場合、コントロールは失敗します。有効期限が切れる前の指定された日数だけログが保持される場合にのみコントロールを成功させたい場合は、必要に応じて `RetentionInDays` パラメータにカスタム値を指定できます。

CloudWatch は、アプリケーションやインフラストラクチャリソースのさまざまなメトリクスを収集して監視するのに役立ちます。CloudWatch を使用して、特定のメトリックスに基づいてアラームアクションを設定することもできます。Elastic Beanstalk 環境への可視性を高めるために、Elastic Beanstalk を CloudWatch と統合することをおすすめします。Elastic Beanstalk のログには、eb-activity.log、その環境の nginx または Apache プロキシサーバーからのアクセスログ、および環境に固有のログが含まれます。

修正

Elastic Beanstalk を CloudWatch Logs と統合するには、「AWS Elastic Beanstalk デベロッパーガイド」の「CloudWatch Logs へのインスタンスログのストリーミング」を参照してください。

Elastic Load Balancing の Security Hub コントロール

これらの AWS Security Hub コントロールは、Elastic Load Balancing サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります

関連する要件: PCI DSS v3.2.1/2.3、PCI DSS v3.2.1/4.1、NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)

カテゴリ: 検出 > 検出サービス

重要度: 中

リソースタイプ : `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config ルール : alb-http-to-https-redirection-check

スケジュールタイプ : 定期的

パラメータ: なし

このコントロールは、HTTP から HTTPS へのリダイレクトが Application Load Balancer のすべての HTTP リスナーで設定されているかどうかを確認します。HTTP から HTTPS へのリダイレクトが設定されていない Application Load Balancer の HTTP リスナーがある場合、コントロールは失敗します。

Application Load Balancer の使用を開始する前に、1 つ以上のリスナーを追加する必要があります。リスナーとは、設定したプロトコルとポートを使用して接続リクエストをチェックするプロセスです。リスナーは、HTTP プロトコルと HTTPS プロトコルの両方をサポートします。HTTPS リスナーを使用して、暗号化と復号化の作業をロードバランサーにオフロードできます。転送中の暗号化を強制するには、Application Load Balancer でリダイレクトアクションを使用して、クライアントの HTTP リクエストをポート 443 の HTTPS リクエストにリダイレクトする必要があります。

詳細については、「Application Load Balancer ユーザーガイド」の「Application Load Balancer のリスナー」を参照してください。

修正

HTTP リクエストを HTTPS にリダイレクトするには、Application Load Balancer のリスナールールを追加するか、既存のルールを編集する必要があります。

新しいルールを追加する手順については、「Application Load Balancer ユーザーガイド」の「ルールの追加」を参照してください。[プロトコル: ポート] で [HTTP] を選択し、**80** と入力します。[アクションの追加、リダイレクト先] で [HTTPS] を選択し、**443** と入力します。

既存のルールを編集する手順については、「Application Load Balancer ユーザーガイド」の「ルールの編集」を参照してください。[プロトコル: ポート] で [HTTP] を選択し、**80** と入力します。[アクションの追加、リダイレクト先] で [HTTPS] を選択し、**443** と入力します。

[ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager

関連する要件： NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(5)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8800NIST.800-53.r5 SC-8.r SI-75

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config ルール : elb-acm-certificate-required

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

Classic Load Balancer が AWS Certificate Manager (ACM) によって提供される HTTPS/SSL 証明書を使用しているかどうかをチェックします。HTTPS/SSL リスナーで構成された Classic Load Balancer が ACM によって提供される証明書を使用しない場合、コントロールは失敗します。

証明書の作成には、ACM または SSL や TLS プロトコルをサポートする OpenSSL などのツールを使用できます。Security Hub では、ACM を使用して、ロードバランサーの証明書を作成またはインポートすることを推奨します。

ACM は Classic Load Balancer と統合して、ロードバランサーに証明書をデプロイできます。また、これらの証明書は自動的に更新する必要があります。

修正

ACM SSL/TLS 証明書を Classic Load Balancer に関連付ける方法については、 AWS ナレッジセンターの記事「ACM SSL/TLS 証明書を Classic、Application、または Network Load Balancer に関連付けるにはどうすればよいですか？」を参照してください。

[ELB.3] Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります

関連する要件： NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8800-53.NIST.800-53.r5 SC-8r SI-7 3.13.155

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config ルール : elb-tls-https-listeners-only

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Classic Load Balancer リスナーがフロントエンド (クライアントからロードバランサー) 接続に HTTPS または TLS プロトコルを使用するよう設定されているかどうかをチェックします。このコントロールは、Classic Load Balancer にリスナーが有効な場合に適用されます。Classic Load Balancer にリスナーが設定されていない場合、コントロールは結果を報告しません。

Classic Load Balancer のリスナーがフロントエンド接続に TLS または HTTPS が設定されている場合、コントロールは成功します。

リスナーがフロントエンド接続に TLS または HTTPS が設定されていない場合、コントロールは失敗します。

ロードバランサーの使用を開始する前に、1 つまたは複数のリスナーを追加する必要があります。リスナーとは、設定したプロトコルとポートを使用して接続リクエストをチェックするプロセスです。リスナーは、HTTP プロトコルと HTTPS/TLS プロトコルの両方をサポートします。ロードバランサーが転送中に暗号化と復号化を行うため、常に HTTPS または TLS リスナーを使用する必要があります。

修正

この問題を修正するには、TLS または HTTPS プロトコルを使用するようにリスナーを更新します。

すべての非準拠リスナーを TLS/HTTPS リスナーに変更するには

1. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
2. ナビゲーションペインの [Load Balancing] で、[Load Balancers] を選択します。
3. Classic Load Balancer を選択します。
4. [Listeners] タブで、[Edit] を選択します。
5. すべてのリスナーについて、[Load Balancer Protocol] (ロードバランサーのプロトコル) が HTTPS または SSL に設定されていない場合は、設定を HTTPS または SSL に変更します。
6. 変更されたすべてのリスナーに対して、[証明書] タブで [デフォルトの変更] を選択します。
7. [ACM 証明書と IAM 証明書]の場合は、証明書を選択します。
8. [デフォルトとして保存] を選択します。
9. すべてのリスナーを更新したら、[Save] (保存) を選択します。

[ELB.4] Application Load Balancer は、無効な http ヘッダーを削除するように設定する必要があります

関連する要件： NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8(2)、PCI DSS v4.0.1/6.2.4

カテゴリ: 保護 > ネットワークセキュリティ

重要度: 中

リソースタイプ : `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config ルール : alb-http-drop-invalid-header-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 Application Load Balancer が無効な HTTP ヘッダーを削除するように設定されているかどうかを評価します。`routing.http.drop_invalid_header_fields.enabled` の値が `false` に設定されている場合、コントロールは失敗します。

デフォルトでは、Application Load Balancer は、無効な HTTP ヘッダー値を削除するように設定されていません。これらのヘッダー値を削除すると、HTTP desync 攻撃を防ぐことができます。

> **Note**
>
> アカウントで ELB.12 が有効になっている場合は、このコントロールを無効にすることをお勧めします。詳細については、「[ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります」を参照してください。

修正

この問題を修正するには、無効なヘッダーフィールドを削除するようにロードバランサーを設定します。

ロードバランサーで無効なヘッダーフィールドを削除するように設定するには

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. ナビゲーションペインで、[Load Balancers] (ロードバランサー) を選択します。
3. Application Load Balancer を選択します。
4. [Actions] (アクション) で、[Edit attributes] (属性の編集) を選択します。
5. [Drop Invalid Header Fields] (無効なヘッダーフィールドを削除) で、[Enable] (有効) を選択します。
6. [Save] (保存) を選択します。

[ELB.5] アプリケーションおよび Classic Load Balancer のログ記録を有効にする必要があります

関連する要件: NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ: `AWS::ElasticLoadBalancing::LoadBalancer`、`AWS::ElasticLoadBalancingV2::LoadBalance`

AWS Config ルール : elb-logging-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

Application Load Balancer と Classic Load Balancer でログ記録が有効になっているかどうかをチェックします。`access_logs.s3.enabled` が `false` の場合、コントロールは失敗します。

Elastic Load Balancing は、ロードバランサーに送信されるリクエストに関する詳細情報をキャプチャしたアクセスログを提供します。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。これらのアクセスログを使用して、トラフィックパターンの分析や、問題のトラブルシューティングを行うことができます。

詳細については、「Classic Load Balancer ユーザーガイド」の「Classic Load Balancerのアクセスログ」を参照してください。

修正

アクセスログを有効にするには、「Application Load Balancer ユーザーガイド」の「ステップ 3: アクセスログの設定」を参照してください。

[ELB.6] アプリケーション、ゲートウェイ、および Network Load Balancer で削除保護を有効にする必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config ルール : elb-deletion-protection-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、アプリケーション、ゲートウェイ、または Network Load Balancer で削除保護が有効になっているかどうかをチェックします。削除保護が無効になっている場合、コントロールは失敗します。

削除保護を有効にして、アプリケーション、ゲートウェイ、または Network Load Balancer を削除されないよう保護します。

修正

ロードバランサーが誤って削除されるのを防ぐために、削除保護を有効にできます。デフォルトでは、ロードバランサーで削除保護が無効になっています。

ロードバランサーの削除保護を有効にした場合、ロードバランサーを削除する前に無効にする必要があります。

Application Load Balancer の削除保護については、「Application Load Balancer ユーザーガイド」の「削除保護」を参照してください。Gateway Load Balancer の削除保護については、「Gateway Load Balancer ユーザーガイド」の「削除保護」を参照してください。Network Load Balancer の削除保護については、「Network Load Balancer ユーザーガイド」の「削除保護」を参照してください。

[ELB.7] Classic Load Balancers は、Connection Draining を有効にする必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: リカバリ > 耐障害性

重要度: 中

リソースタイプ : `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config ルール: `elb-connection-draining-enabled` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Classic Load Balancers で Connection Draining が有効になっているかどうかをチェックします。

Classic Load Balancers で Connection Draining を有効にすることで、ロードバランサーは、登録解除中のインスタンスまたは異常の発生したインスタンスへのリクエストの送信を確実に停止します。既存の接続を開いたままにします。これは、Auto Scaling グループのインスタンスで、接続が突然切断されないようにするために特に役立ちます。

修正

Classic Load Balancers で Connection Draining を有効にするには、Classic Load Balancer のユーザーガイドの「Classic Load Balancer の Connection Draining の設定」を参照してください。

[ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な uration AWS Configを持つ事前定義されたセキュリティポリシーを使用する必要があります

関連する要件： NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8800NIST.800-53.r5 SC-8r SI-7 3.13.155

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config ルール : elb-predefined-security-policy-ssl-check

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `predefinedPolicyName`: `ELBSecurityPolicy-TLS-1-2-2017-01` (カスタマイズ不可)

このコントロールは、Classic Load Balancer の HTTPS/SSL リスナーが事前定義されたポリシー `ELBSecurityPolicy-TLS-1-2-2017-01` を使用しているかどうかをチェックします。Classic Load Balancer の HTTPS/SSL リスナーが `ELBSecurityPolicy-TLS-1-2-2017-01` を使用しない場合、コントロールは失敗します。

セキュリティポリシーは、SSL プロトコル、暗号、およびサーバーの優先順位オプションを組み合わせたものです。事前定義されたポリシーは、クライアントとロードバランサー間の SSL ネゴシエーションでサポートする暗号、プロトコル、および優先順位をコントロールします。

`ELBSecurityPolicy-TLS-1-2-2017-01` を使用すると、SSL および TLS の特定のバージョンを無効にする必要があるコンプライアンスとセキュリティ標準に準拠することに役立ちます。詳細については、「Classic Load Balancer ユーザーガイド」の「Classic Load Balancer の事前定義された SSL セキュリティポリシー」を参照してください。

修正

Classic Load Balancer で定義済みのセキュリティポリシー `ELBSecurityPolicy-TLS-1-2-2017-01` を使用する方法については、「Classic Load Balancer ユーザーガイド」の「セキュリティ設定の構成」を参照してください。

[ELB.9] Classic Load Balancer では、クロスゾーンロードバランシングが有効になっている必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config ルール : elb-cross-zone-load-balancing-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、クロスゾーンロードバランシングが Classic Load Balancer (CLB) に対して有効になっているかどうかをチェックします。クロスゾーンロードバランシングが CLB に対して有効になっていない場合、コントロールは失敗します。

ロードバランサノードは、アベイラビリティーゾーン内の登録済みターゲット全体にのみトラフィックを分散します。クロスゾーンロードバランシングが無効の場合、各ロードバランサーノードは、そのアベイラビリティーゾーンの登録済みターゲットにのみトラフィックを分散します。登録済みターゲット数がアベイラビリティーゾーン間で同じでない場合、トラフィックは均等に分散されず、あるゾーンのインスタンスは、別のゾーンのインスタンスと比較して過剰に使用される可能性があります。クロスゾーンロードバランシングを有効にすると、Classic Load Balancer の各ロードバランサーノードは、有効なすべてのアベイラビリティーゾーンに登録済みのインスタンスにリクエストを

均等に分散します。詳細については、「Elastic Load Balancing ユーザーガイド」の「クロスゾーンロードバランシング」を参照してください。

修正

Classic Load Balancer でクロスゾーンロードバランシングを有効にするには、「Classic Load Balancer ユーザーガイド」の「クロスゾーンロードバランシングを有効にする」を参照してください。

[ELB.10] Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config ルール : clb-multiple-az

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`minAvailabilityZones`	アベイラビリティーゾーンの最小数	列挙型	`2, 3, 4, 5, 6`	2

このコントロールは、Classic Load Balancer が少なくとも指定された数のアベイラビリティーゾーン (AZ) にまたがるように設定されているかどうかをチェックします。Classic Load Balancer が少なくとも指定された数の AZ にまたがっていない場合、コントロールは失敗します。AZ の最小数に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 2 つの AZ を使用します。

Classic Load Balancer は、単一のアベイラビリティーゾーンまたは複数のアベイラビリティーゾーンにある Amazon EC2 インスタンスに受信リクエストを配信するように設定できます。複数のアベイラビリティーゾーンにまたがらない Classic Load Balancer は、単独で構成されたアベイラビリティーゾーンが使用できなくなった場合、別のアベイラビリティーゾーンのターゲットにトラフィックをリダイレクトすることはできません。

修正

Classic Load Balancer にアベイラビリティーゾーンを追加するには、「Classic Load Balancer のユーザーガイド」の「Classic Load Balancer でのサブネットの追加もしくは削除」を参照してください。

[ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります

関連する要件： NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、PCI DSS v4.0.1/6.2.4

カテゴリ: 保護 > データ保護 > データの整合性

重要度: 中

リソースタイプ : `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config ルール : alb-desync-mode-check

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `desyncMode`: `defensive`, `strictest` (カスタマイズ不可)

このコントロールは、Application Load Balancer が防御モードまたは最も厳密な非同期緩和モードに設定されているかどうかをチェックします。Application Load Balancer が防御モードまたは最も厳密な非同期緩和モードに設定されていない場合、このコントロールは失敗します。

HTTP 非同期の問題はリクエストスマグリングにつながり、アプリケーションがリクエストキューやキャッシュポイズニングに対して脆弱になる可能性があります。そしてこうした脆弱性は、認証情報スタッフィングや不正なコマンドの実行につながります。防御モードまたは最も厳密な非同期緩和モードで構成された Application Load Balancer は、HTTP 非同期に起因するセキュリティ上の問題からアプリケーションを保護します。

修正

Application Load Balancer の非同期緩和モードの更新方法については、「Application Load Balancer ユーザーガイド」の「Desync mitigation mode」(非同期緩和モード) を参照してください。

[ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config ルール : elbv2-multiple-az

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`minAvailabilityZones`	アベイラビリティーゾーンの最小数	列挙型	`2, 3, 4, 5, 6`	`2`

このコントロールは、Elastic Load Balancer V2 (アプリケーション、ネットワーク、または Gateway Load Balancer) に少なくとも指定された数のアベイラビリティーゾーン (AZ) のインスタンスが登録されているかどうかをチェックします。Elastic Load Balancer V2 で、少なくとも指定された数の AZ にインスタンスが登録されていない場合、コントロールは失敗します。AZ の最小数に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 2 つの AZ を使用します。

Elastic Load Balancing は、受信したトラフィックを複数のアベイラビリティーゾーンの複数のターゲット (EC2 インスタンス、コンテナ、IP アドレスなど) に自動的に分散させます。Elastic Load Balancing は、受信トラフィックの時間的な変化に応じて、ロードバランサーをスケーリングしま

す。サービスの可用性を確保するため、2 つ以上のアベイラビリティーゾーンを設定することが推奨されます。それにより、Elastic Load Balancer はアベイラビリティーゾーンを使用できなくなったときに、別のアベイラビリティーゾーンにトラフィックを転送することができます。複数のアベイラビリティーゾーンを設定しておくと、アプリケーションの単一障害点を回避できます。

修正

アベイラビリティーゾーンを Application Load Balancer に追加する方法については、「Application Load Balancer ユーザーガイド」の「Application Load Balancer のアベイラビリティーゾーン」参照してください。アベイラビリティーゾーンを Network Load Balancer に追加する方法については、「Network Load Balancer ユーザーガイド」の「Network Load Balancer」を参照してください。アベイラビリティーゾーンを Gateway Load Balancer に追加する方法については、「Gateway Load Balancer ユーザーガイド」の「Create a Gateway Load Balancer」(Gateway Load Balancer の作成) を参照してください。

[ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります

関連する要件： NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、PCI DSS v4.0.1/6.2.4

カテゴリ: 保護 > データ保護 > データの整合性

重要度: 中

リソースタイプ : `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config ルール : clb-desync-mode-check

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `desyncMode`: `defensive, strictest` (カスタマイズ不可)

このコントロールは、Classic Load Balancer が防御モードまたは最も厳密な非同期緩和モードで設定されているかどうかをチェックします。Classic Load Balancer が防御モードまたは最も厳密な非同期緩和モードに設定されていない場合、このコントロールは失敗します。

HTTP 非同期の問題はリクエストスマグリングにつながり、アプリケーションがリクエストキューやキャッシュポイズニングに対して脆弱になる可能性があります。そしてこうした脆弱性は、認証情報の乗っ取りや不正なコマンドの実行につながります。防御モードまたは最も厳密な非同期緩和モード

で構成された Classic Load Balancer は、HTTP 非同期に起因するセキュリティ上の問題からアプリケーションを保護します。

修正

Classic Load Balancer の非同期緩和モードの更新方法については、「Classic Load Balancer ユーザーガイド」の「非同期緩和モードの変更」を参照してください。

[ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります

関連する要件: NIST.800-53.r5 AC-4(21)

カテゴリ: 保護 > 保護サービス

重要度: 中

リソースタイプ : `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config ルール : alb-waf-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Application Load Balancer が AWS WAF Classic または AWS WAF ウェブアクセスコントロールリスト (ウェブ ACL) に関連付けられているかどうかをチェックします。 AWS WAF 設定の `Enabled`フィールドが に設定されている場合、コントロールは失敗します`false`。

AWS WAF は、ウェブアプリケーションと APIsから保護するのに役立つウェブアプリケーションファイアウォールです。を使用すると AWS WAF、ウェブ ACL を設定できます。これは、定義したカスタマイズ可能なウェブセキュリティルールと条件に基づいてウェブリクエストを許可、ブロック、またはカウントする一連のルールです。Application Load Balancer を AWS WAF ウェブ ACL に関連付けて、悪意のある攻撃から保護することをお勧めします。

修正

Application Load Balancer をウェブ ACL に関連付けるには、「 デベロッパーガイド」の「ウェブ ACL と AWS リソースの関連付けまたは関連付け解除」を参照してください。 AWS WAF

[ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります

関連する要件: NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5

SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::ElasticLoadBalancingV2::Listener`

AWS Config ルール : elbv2-predefined-security-policy-ssl-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ： `sslPolicies`: `ELBSecurityPolicy-TLS13-1-2-2021-06`, `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04`, `ELBSecurityPolicy-TLS13-1-3-2021-06`, `ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04`, `ELBSecurityPolicy-TLS13-1-2-Res-2021-06`, `ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04` (カスタマイズ不可)

このコントロールは、Application Load Balancer の HTTPS リスナーまたは Network Load Balancer の TLS リスナーが、推奨されるセキュリティポリシーを使用して転送中のデータを暗号化するように設定されているかどうかを確認します。ロードバランサーの HTTPS または TLS リスナーが推奨セキュリティポリシーを使用するように設定されていない場合、コントロールは失敗します。

Elastic Load Balancing は、セキュリティポリシーと呼ばれる SSL ネゴシエーション設定を使用して、クライアントとロードバランサー間の接続をネゴシエートします。セキュリティポリシーは、プロトコルと暗号の組み合わせを指定します。プロトコルは、クライアントとサーバー間の安全な接続を確立します。暗号とは、暗号化キーを使用してコード化されたメッセージを作成する暗号化アルゴリズムです。接続ネゴシエーションのプロセスで、クライアントとロードバランサーでは、それぞれサポートされる暗号とプロトコルのリストが優先される順に表示されます。ロードバランサーに推奨されるセキュリティポリシーを使用すると、コンプライアンスとセキュリティの基準を満たすのに役立ちます。

修正

推奨されるセキュリティポリシーとリスナーの更新方法については、Elastic Load Balancing ユーザーガイド」の次のセクションを参照してください。Application Load Balancer のセキュリティポリシー、Network Load Balancer のセキュリティポリシー、Application Load Balancer の HTTPS リスナーの更新、Network Load Balancer のリスナーの更新。

[ELB.18] Application and Network Load Balancer リスナーは、安全なプロトコルを使用して転送中のデータを暗号化する必要があります

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::ElasticLoadBalancingV2::Listener`

AWS Config ルール : elbv2-listener-encryption-in-transit

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Application Load Balancer または Network Load Balancer のリスナーが、転送中のデータの暗号化に安全なプロトコルを使用するように設定されているかどうかを確認します。Application Load Balancer リスナーが HTTPS プロトコルを使用するように設定されていない場合、または Network Load Balancer リスナーが TLS プロトコルを使用するように設定されていない場合、コントロールは失敗します。

クライアントとロードバランサーの間で送信されるデータを暗号化するには、Elastic Load Balancer リスナーを、業界標準のセキュリティプロトコルである Application Load Balancer の場合は HTTPS、Network Load Balancer の場合は TLS を使用するように設定する必要があります。それ以外の場合、クライアントとロードバランサーの間で送信されるデータは、傍受、改ざん、不正アクセスに対して脆弱になります。リスナーによる HTTPS または TLS の使用は、セキュリティのベストプラクティスに沿ったものであり、送信中のデータの機密性と整合性を確保するのに役立ちます。これは、機密情報を処理するアプリケーションや、転送中のデータの暗号化を必要とするセキュリティ標準に準拠する必要があるアプリケーションにとって特に重要です。

修正

リスナーのセキュリティプロトコルの設定の詳細については、Elastic Load Balancing ユーザーガイド」の次のセクションを参照してください。Application Load Balancer の HTTPS リスナーを作成する」および「Network Load Balancer のリスナーを作成する」。

Elasticsearch の Security Hub

これらの AWS Security Hub コントロールは、Elasticsearch サービスとリソースを評価します。

これらのコントロールは、一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります

関連する要件: PCI DSS v3.2.1/3.4、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::Elasticsearch::Domain`

AWS Config ルール : `elasticsearch-encrypted-at-rest`

スケジュールタイプ : 定期的

パラメータ: なし

このコントロールは、Elasticsearch ドメインで保管中の暗号化設定が有効になっているかどうかをチェックします。保管中の暗号化が有効になっていない場合、チェックは失敗します。

OpenSearch 内の機密データのセキュリティを強化するには、保管中に暗号化されるように OpenSearch を設定する必要があります。Elasticsearch ドメインは、保管中のデータの暗号化を提供します。この機能では、 AWS KMS を使用して暗号化キーを保存および管理します。暗号化の実行には、256 ビットキーを使用した Advanced Encryption Standard アルゴリズム (AES-256) を使用します。

保管中の OpenSearch での暗号化の詳細については、「Amazon OpenSearch Service 開発者ガイド」の「Amazon OpenSearch Service の保管中のデータの暗号化」を参照してください。

`t.small` や `t.medium` などの特定のインスタンスタイプでは、保管中のデータの暗号化がサポートされていません。詳細については、「Amazon OpenSearch Service 開発者ガイド」の「サポートされるインスタンスタイプ」を参照してください。

修正

新規および既存の Elasticsearch ドメインの保管時の暗号化を有効にするには、「Amazon OpenSearch Service 開発者ガイド」の「保管中のデータの暗号化の有効化」を参照してください。

[ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります

関連する要件： PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.6、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3

(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

カテゴリ: 保護 > セキュアなネットワーク設定 > VPC 内のリソース

重要度: 非常事態

リソースタイプ : `AWS::Elasticsearch::Domain`

AWS Config ルール : `elasticsearch-in-vpc-only`

スケジュールタイプ : 定期的

パラメータ: なし

このコントロールは、Elasticsearch ドメインが VPC 内にあるかどうかをチェックします。このコントロールは、パブリックアクセスの可能性を判断するための VPC サブネットルーティング設定を評価しません。Elasticsearch ドメインがパブリックサブネットに添付済みでないことを確認する必要があります。「Amazon OpenSearch Service 開発者ガイド」の「リソースベースのポリシー」を参照してください。また、推奨されるベストプラクティスに従って VPC が確実に設定されていることを確認する必要があります。「Amazon VPC ユーザーガイド」の「VPC のセキュリティのベストプラクティス」を参照してください。

VPC 内にデプロイされた Elasticsearch ドメインは、パブリックインターネットを経由することなく、プライベート AWS ネットワーク経由で VPC リソースと通信できます。この設定では、転送中のデータへのアクセスを制限することにより、セキュリティ体制が向上します。VPC は、ネットワーク ACL やセキュリティグループを含む Elasticsearch ドメインへのアクセスを保護するための多数のネットワークコントロールを提供します。Security Hub では、これらのコントロールを有効に利用するために、パブリック Elasticsearch ドメインを VPC に移行することを推奨します。

修正

パブリックエンドポイントを使用してドメインを作成する場合、後で VPC 内にドメインを配置することはできません。代わりに、新規のドメインを作成して、データを移行する必要があります。逆の場合も同様です。VPC 内にドメインを作成する場合、パブリックエンドポイントを持つことはできません。代わりに、別のドメインを作成するか、このコントロールを無効にする必要があります。

「Amazon OpenSearch Service 開発者ガイド」の「VPC 内で Amazon OpenSearch Service ドメインを起動する」を参照してください。

[ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります

関連する要件： NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、PCI DSS v4.0.1/4.2.1

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::Elasticsearch::Domain`

AWS Config ルール : `elasticsearch-node-to-node-encryption-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは Elasticsearch ドメインでノード間の暗号化が有効になっているかどうかをチェックします。Elasticsearch ドメインでノード間の暗号化が有効になっていない場合、このコントロールは失敗します。Elasticsearch バージョンがノード間の暗号化チェックをサポートしていない場合、コントロールは失敗した検出結果も生成します。

HTTPS (TLS) を使用すると、潜在的な攻撃者が中間者攻撃または同様の攻撃を使用してネットワークトラフィックを盗聴または操作することを防止できます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。Elasticsearch ドメインのノード間の暗号化を有効にすると、クラスター内の通信が転送中に確実に暗号化されます。

この設定には、パフォーマンス上のペナルティが発生する可能性があります。このオプションを有効にする前に、パフォーマンスのトレードオフを認識してテストする必要があります。

修正

新規および既存のドメインでノード間の暗号化を有効にする方法については、「Amazon OpenSearch Service デベロッパーガイド」の「ノード間の暗号化を有効にする」を参照してください。

[ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります

関連する要件: NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5

AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 - ログ記録

重要度: 中

リソースタイプ : `AWS::Elasticsearch::Domain`

AWS Config ルール : `elasticsearch-logs-to-cloudwatch`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `logtype = 'error'` (カスタマイズ不可)

このコントロールは、Elasticsearch ドメインが CloudWatch Logs にエラーログを送信するように設定されているかどうかをチェックします。

Elasticsearch ドメインのエラーログを有効にし、これらのログは保持と応答のために CloudWatch Logs に送信する必要があります。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

修正

ログ発行を有効にする方法については、「Amazon OpenSearch Service 開発者ガイド」の「ログ発行を有効にする (コンソール)」を参照してください。

[ES.5] Elasticsearch ドメインで監査ログ記録が有効になっている必要があります

関連する要件： NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53AU-6.r5 CA-7、NIST.800-53.r5 SC-7(7) SI-3 SI-4 SI-710.4.2

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::Elasticsearch::Domain`

AWS Config ルール: `elasticsearch-audit-logging-enabled` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `cloudWatchLogsLogGroupArnList` (カスタマイズ不可)。Security Hub は、このパラメータを設定しません。監査ログ用に設定する必要がある CloudWatch Logs ロググループのカンマ区切りリスト。

  Elasticsearch ドメインの CloudWatch Logs ロググループがこのパラメータリストで指定されていない場合、このルールは `NON_COMPLIANT` です。

このコントロールは、Elasticsearch ドメインで監査ログ記録が有効になっているかどうかをチェックします。Elasticsearch ドメインで監査ログ記録が有効になっていない場合、このコントロールは失敗します。

監査ログは高度なカスタマイズが可能です。これにより、認証の成功と失敗、OpenSearch へのリクエスト、インデックス変更、受信検索クエリなど、Elasticsearch クラスターでのユーザーアクティビティを追跡できます。

修正

監査ログを有効にする詳細な手順については、「Amazon OpenSearch Service 開発者ガイド」の「監査ログの有効化」を参照してください。

[ES.6] Elasticsearch ドメインには少なくとも 3 つのデータノードが必要です

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::Elasticsearch::Domain`

AWS Config ルール: `elasticsearch-data-node-fault-tolerance` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Elasticsearch ドメインに少なくとも 3 つのデータノードが設定されていること、また `zoneAwarenessEnabled` が `true` かどうかをチェックします。

Elasticsearch ドメインでは、高可用性と耐障害性のために少なくとも 3 つのデータノードが必要です。少なくとも 3 つのデータノードを持つ Elasticsearch ドメインをデプロイすると、ノードに障害が発生した場合のクラスター操作が確保されます。

修正

Elasticsearch ドメインのデータノードの数を変更するには

1. https://console.aws.amazon.com/aos/ で Amazon OpenSearch Service コンソールを開きます。
2. [ドメイン] で、編集するドメインの名前を選択します。
3. [Edit domain] (ドメインの編集) を選択します。
4. [Data nodes] (データノード) で、[Number of nodes] (ノード数) に 3 以上の数値を設定します。

   3 つのアベイラビリティーゾーンのデプロイは、3 の倍数に設定してアベイラビリティーゾーン間で均等に配信されるようにします。
5. [Submit] (送信) を選択します。

[ES.7] Elasticsearch ドメインは、少なくとも 3 つの専用マスターノードを設定する必要があります。

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::Elasticsearch::Domain`

AWS Configルール: `elasticsearch-primary-node-fault-tolerance` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Elasticsearch ドメインが、少なくとも 3 つの専用プライマリノードで構成されているかどうかをチェックします。ドメインが専用プライマリノードを使用しない場合、このコン

トロールは失敗します。Elasticsearch ドメインに 5 つの専用プライマリノードがある場合、このコントロールは成功します。ただし、3 つ以上のプライマリノードの使用は、可用性リスクを低減するために不要な場合があり、使用により追加コストが発生します。

Elasticsearch ドメインでは、高可用性と耐障害性のために、少なくとも 3 つの専用プライマリノードが必要です。専用プライマリノードのリソースは、データノードのブルー/グリーンのデプロイ中に管理が必要なノードが追加されるため、負荷がかかることがあります。少なくとも 3 つの専用プライマリノードを持つ Elasticsearch ドメインをデプロイすると、ノードに障害が発生した場合に十分なプライマリノードのリソース容量とクラスター操作が確保されます。

修正

OpenSearch ドメイン内の専用プライマリノード数を変更するには

1. https://console.aws.amazon.com/aos/ で Amazon OpenSearch Service コンソールを開きます。
2. [ドメイン] で、編集するドメインの名前を選択します。
3. [Edit domain] (ドメインの編集) を選択します。
4. [Dedicated master nodes] (専用マスターノード) で、[Instance type] (インスタンスタイプ) に目的のインスタンスタイプを設定します。
5. [Number of master nodes] (マスターノードの数) を 3 以上に設定します。
6. [Submit] (送信) を選択します。

[ES.8] Elasticsearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります

関連する要件： NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8800NIST.800-53.r5 SC-8r SI-75

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::Elasticsearch::Domain`

AWS Config ルール: `elasticsearch-https-required` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Elasticsearch ドメインエンドポイントが最新の TLS セキュリティポリシーを使用するように設定されているかどうかを確認します。Elasticsearch ドメインエンドポイントが最新のサポートされているポリシーを使用するように設定されていない場合、または HTTP が有効になっていない場合、コントロールは失敗します。現在サポートされている最新の TLS セキュリティポリシーは `Policy-Min-TLS-1-2-PFS-2023-10` です。

HTTPS (TLS) を使用すると、潜在的な攻撃者が中間者攻撃または同様の攻撃を使用してネットワークトラフィックを盗聴または操作することを防止できます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。転送中のデータの暗号化は、パフォーマンスに影響する可能性があります。TLS のパフォーマンスプロファイルと TLS の影響を把握するには、この機能を使用してアプリケーションをテストする必要があります。TLS 1.2 は、以前の TLS バージョンに比べて、いくつかのセキュリティ機能の強化を提供します。

修正

TLS 暗号化を有効にするには、UpdateDomainConfig API オペレーションを使用して、DomainEndpointOptions を設定します。これにより、`TLSSecurityPolicy` が設定されます。

[ES.9] Elasticsearch ドメインにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Elasticsearch::Domain`

AWS Config ルール: `tagged-elasticsearch-domain` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタ	StringList (最大 6 項目)	AWS 要件を満たす 1 ~	`No default value`

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	グキーのリスト。タグキーでは、大文字と小文字が区別されます。		6 個のタグキー。	

このコントロールは、Elasticsearch ドメインにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。ドメインにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ドメインにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。IAM エンティティ (ユーザーまたはロール) と AWS リソースにタグをアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Elasticsearch ドメインにタグを追加するには、「Amazon OpenSearch Service デベロッパーガイド」の「タグの使用」を参照してください。

Amazon EMR の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon EMR (以前は Amazon Elastic MapReduce と呼ばれていました) サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります

関連する要件： PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.6、PCI DSS v4.0.1/1.4.4、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21) NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ : `AWS::EMR::Cluster`

AWS Config ルール： emr-master-no-public-ip

スケジュールタイプ : 定期的

パラメータ: なし

このコントロールは、Amazon EMR クラスターのマスターノードにパブリック IP アドレスが設定されているかどうかをチェックします。マスターノードインスタンスのいずれかにパブリック IP アドレスが関連付けられている場合、コントロールは失敗します。

パブリック IP アドレスは、インスタンスの `NetworkInterfaces` 設定の `PublicIp` フィールドで指定されます。このコントロールは、`RUNNING` または `WAITING` 状態にある Amazon EMR クラスターのみをチェックします。

修正

起動中に、デフォルトサブネットまたはデフォルト以外のサブネット内のインスタンスがパブリック IPv4 アドレスを割り当てられるかどうかをコントロールできます。デフォルトでは、デフォルトサブネットのこの属性は `true` に設定されています。Amazon EC2 起動インスタンスウィザード

によって作成された場合を除き、デフォルト以外のサブネットで IPv4 パブリックアドレス属性は `false` に設定されています。その場合、属性は `true` に設定されます。

起動後に、インスタンスからパブリック IPv4 アドレスの割り当てを手動で解除することはできません。

失敗した検出結果を修正するには、IPv4 パブリックアドレス属性が `false` に設定されているプライベートサブネットを使用して、VPC で新しいクラスターを起動する必要があります。手順については、「Amazon EMR 管理ガイド」の「VPC でクラスターを起動する」を参照してください。

[EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります

関連する要件： PCI DSS v4.0.1/1.4.4、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

カテゴリ: 保護 > セキュアなアクセス管理 > パブリックアクセスが不可能なリソース

重要度: 非常事態

リソースタイプ : `AWS::::Account`

AWS Config ルール： emr-block-public-access

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、アカウントに Amazon EMR ブロックパブリックアクセスが設定されているかどうかをチェックします。ブロックパブリックアクセス設定が有効になっていない場合、またはポート 22 以外のポートが許可されている場合、コントロールは失敗します。

Amazon EMR のブロックパブリックアクセスは、クラスターのセキュリティ設定でポートのパブリック IP アドレスからのインバウンドトラフィックが許可されている場合に、ユーザーがパブリックサブネットでクラスターを起動するのを防止します。 AWS アカウント のユーザーがクラスターを起動すると、Amazon EMR はクラスターのセキュリティグループのポートルールをチェックし、インバウンドトラフィックルールと比較します。セキュリティグループに、パブリック IP アドレス IPv4 0.0.0.0/0 または IPv6 ::/0 に対してポートを開くインバウンドルールがあり、それらのポートが

アカウントで適切に指定されていない場合、Amazon EMR はユーザーにクラスターの作成を許可しません。

> **Note**
> ブロックパブリックアクセスはデフォルトで有効になっています。アカウントの保護を強化するには、これを有効のままにしておくことが推奨されます。

修正

Amazon EMR のブロックパブリックアクセスを設定するには、「Amazon EMR 管理ガイド」の「Amazon EMR のパブリックアクセスブロックの使用」を参照してください。

[EMR.3] Amazon EMR セキュリティ設定は保管時に暗号化する必要があります

関連する要件： NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CP-9(8)、NIST.800-53.r5 SI-12

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::EMR::SecurityConfiguration`

AWS Config ルール : emr-security-configuration-encryption-rest

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon EMR セキュリティ設定で保管時の暗号化が有効になっているかどうかを確認します。セキュリティ設定が保管時の暗号化を有効にしていない場合、コントロールは失敗します。

保管中のデータとは、永続的な不揮発性ストレージに任意の期間保管されているデータを指します。保管中のデータを暗号化すると、その機密性が保護され、権限のないユーザーがアクセスするリスクが低減されます。

修正

Amazon EMR セキュリティ設定で保管時の暗号化を有効にするには、「Amazon EMR 管理ガイド」の「データ暗号化の設定」を参照してください。

[EMR.4] Amazon EMR セキュリティ設定は転送中に暗号化する必要があります

関連する要件： NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::EMR::SecurityConfiguration`

AWS Config ルール : emr-security-configuration-encryption-transit

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon EMR セキュリティ設定で転送中の暗号化が有効になっているかどうかをチェックします。セキュリティ設定が転送中の暗号化を有効にしていない場合、コントロールは失敗します。

転送中のデータとは、クラスター内のノード間やクラスターとアプリケーション間など、ある場所から別の場所に移動するデータを指します。データはインターネット内またはプライベートネットワーク内を移動する場合があります。転送中のデータを暗号化することで、権限のないユーザーがネットワークトラフィックを盗聴するリスクが軽減されます。

修正

Amazon EMR セキュリティ設定で転送中の暗号化を有効にするには、「Amazon EMR 管理ガイド」の「データ暗号化の設定」を参照してください。

EventBridge の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon EventBridge サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Events::EventBus`

AWS Config ルール : `tagged-events-eventbus` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon EventBridge イベントバスにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。イベントバスにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、イベントバスにキーがタグ付けされていない場合に失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、のAWS 「リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

EventBridge イベントバスにタグを追加するには、「Amazon EventBridge ユーザーガイド」の「Amazon EventBridge タグ」を参照してください。

[EventBridge.3] Amazon EventBridge カスタムイベントバスにリソースポリシーがアタッチされている必要があります

関連する要件： NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(3)、PCI DSS v4.0.1/10.3.1

カテゴリ: 保護 > セキュアなアクセス管理 > パブリックアクセスが不可能なリソース

重要度: 低

リソースタイプ : `AWS::Events::EventBus`

AWS Config ルール : custom-eventbus-policy-attached

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは Amazon EventBridge カスタムイベントバスにリソースベースのポリシーがアタッチされているかどうかを確認します。カスタムイベントバスにリソースベースのポリシーがない場合、このコントロールは失敗します。

デフォルトでは、EventBridge カスタムイベントバスには、リソースベースのポリシーはアタッチされていません。これにより、アカウント内のプリンシパルはイベントバスにアクセスできます。リソースベースのポリシーをイベントバスにアタッチすることで、イベントバスへのアクセスを特定のアカウントに制限したり、別のアカウントのエンティティへのアクセスを意図的に許可したりできます。

修正

リソースベースのポリシーを EventBridge カスタムイベントバスにアタッチするには、「Amazon EventBridge ユーザーガイド」の「Amazon EventBridge のリソースベースのポリシーの使用」を参照してください。

[EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::Events::Endpoint`

AWS Config ルール : `global-endpoint-event-replication-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは Amazon EventBridge グローバルエンドポイントでイベントレプリケーションが有効になっているかどうかを確認します。グローバルエンドポイントでイベントレプリケーションが有効になっていない場合、コントロールは失敗します。

グローバルエンドポイントによりアプリケーションをリージョンフォールトトレラントにできます。開始するには、エンドポイントに Amazon Route 53 ヘルスチェックを割り当てます。フェイルオーバーが開始されると、ヘルスチェックは「異常」状態を報告します。フェイルオーバーの開始から数分以内に、すべてのカスタムイベントがセカンダリリージョンのイベントバスにルーティングされ、そのイベントバスによって処理されます。グローバルエンドポイントを使用する場合、イベントレプリケーションを有効にできます。イベントレプリケーションは、マネージドルールを使用して、すべてのカスタムイベントをプライマリリージョンとセカンダリリージョンのイベントバスに送信します。グローバルエンドポイントを設定する場合は、イベントレプリケーションを有効にすることをお勧めします。イベントレプリケーションは、グローバルエンドポイントが正しく設定されていることを確認するのに役立ちます。フェイルオーバーイベントから自動的にリカバリするには、イベントレプリケーションが必要です。イベントレプリケーションを有効にしていない場合は、イベントがプライマリリージョンにルーティングされる前に、Route 53 ヘルスチェックを手動で「正常」にリセットする必要があります。

> **Note**
>
> カスタムイベントバスを使用している場合、フェイルオーバーが正常に機能するためには、各リージョンに同じ名前と同じアカウントを持つカスタムイベントバスが必要です。イベントレプリケーションを有効にすると、月額のコストが増加する可能性があります。料金の詳細については、Amazon EventBridge の料金を参照してください。

修正

EventBridge グローバルエンドポイントのイベントレプリケーションを有効にするには、「Amazon EventBridge ユーザーガイド」の「グローバルエンドポイントの作成」を参照してください。イベントレプリケーションの場合は、[イベントレプリケーションが有効] を選択します。

Amazon Fraud Detector の Security Hub コントロール

これらの Security Hub コントロールは、Amazon Fraud Detector サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::FraudDetector::EntityType`

AWS Config ルール : `frauddetector-entity-type-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタ	StringList (最大 6 項目)	AWS 要件を満たす 1 ~	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	グキーのリスト。タグキーでは、大文字と小文字が区別されます。		6 個のタグキー。	

このコントロールは、Amazon Fraud Detector エンティティタイプにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。エンティティタイプにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、エンティティタイプにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

Amazon Fraud Detector エンティティタイプにタグを追加するには (コンソール)

1. https://console.aws.amazon.com/frauddetector で Amazon Fraud Detector コンソールを開きます。
2. ナビゲーションペインで、エンティティを選択します。
3. リストからエンティティタイプを選択します。
4. エンティティタイプのタグセクションで、タグの管理を選択します。
5. [新しいタグを追加] をクリックします。タグのキーと値を入力します。追加のキーと値のペアについても繰り返します。
6. タグの追加を完了したら、[Save (保存)] を選択します。

[FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::FraudDetector::Label`

AWS Config ルール : `frauddetector-label-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon Fraud Detector ラベルにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredKeyTags。ラベルにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredKeyTags。パラメータ が指定されていない場合、コントロールrequiredKeyTagsはタグキーの存在のみをチェックし、ラベルにキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

Amazon Fraud Detector ラベルにタグを追加するには (コンソール)

1. https://console.aws.amazon.com/frauddetector で Amazon Fraud Detector コンソールを開きます。
2. ナビゲーションペインで、ラベル を選択します。
3. リストからラベルを選択します。
4. ラベルタグ セクションで、タグの管理 を選択します。
5. [新しいタグを追加] をクリックします。タグのキーと値を入力します。追加のキーと値のペアについても繰り返します。

6. タグの追加を完了したら、[Save (保存)] を選択します。

[FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::FraudDetector::Outcome`

AWS Config ルール : `frauddetector-outcome-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon Fraud Detector の結果にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。結果にタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、結果がキーでタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグ

は、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

Amazon Fraud Detector の結果にタグを追加するには (コンソール)

1. https://console.aws.amazon.com/frauddetector で Amazon Fraud Detector コンソールを開きます。
2. ナビゲーションペインで、結果を選択します。
3. リストから結果を選択します。
4. 結果タグセクションで、タグの管理を選択します。
5. [新しいタグを追加] をクリックします。タグのキーと値を入力します。追加のキーと値のペアについても繰り返します。
6. タグの追加を完了したら、[Save (保存)] を選択します。

[FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::FraudDetector::Variable`

AWS Config ルール : `frauddetector-variable-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon Fraud Detector 変数にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。変数にタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、変数にキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

Amazon Fraud Detector 変数にタグを追加するには (コンソール)

1. https://console.aws.amazon.com/frauddetector で Amazon Fraud Detector コンソールを開きます。
2. ナビゲーションペインで、変数を選択します。
3. リストから変数を選択します。
4. 変数タグセクションで、タグの管理を選択します。
5. [新しいタグを追加] をクリックします。タグのキーと値を入力します。追加のキーと値のペアについても繰り返します。
6. タグの追加を完了したら、[Save (保存)] を選択します。

Amazon FSx の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon FSx サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::FSx::FileSystem`

AWS Config ルール : fsx-openzfs-copy-tags-enabled

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon FSx for OpenZFS ファイルシステムがバックアップとボリュームにタグをコピーするように設定されているかどうかを確認します。OpenZFS ファイルシステムがタグをバックアップとボリュームにコピーするように設定されていない場合、コントロールは失敗します。

IT アセットの身分証明書とインベントリはガバナンスとセキュリティの重要な側面です。タグは、目的、所有者、環境など、さまざまな方法で AWS リソースを分類するのに役立ちます。割り当てたタグに基づいて特定のリソースをすばやく識別できるため、これは同じ型のリソースが多い場合に役立ちます。

修正

タグをバックアップとボリュームにコピーするように FSx for OpenZFS ファイルシステムを設定する方法については、「Amazon FSx for OpenZFS ユーザーガイド」の「ファイルシステムの更新」を参照してください。

[FSx.2] FSx for Lustre ファイルシステムでは、タグをバックアップにコピーするように設定する必要があります

関連する要件: NIST.800-53.r5 CP-9、NIST.800-53.r5 CM-8

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::FSx::FileSystem`

AWS Config ルール : fsx-lustre-copy-tags-to-backups

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon FSx for Lustre ファイルシステムがタグをバックアップとボリュームにコピーするように設定されているかどうかをチェックします。Lustre ファイルシステムがタグをバックアップとボリュームにコピーするように設定されていない場合、コントロールは失敗します。

IT アセットの身分証明書とインベントリはガバナンスとセキュリティの重要な側面です。タグは、目的、所有者、環境など、さまざまな方法で AWS リソースを分類するのに役立ちます。割り当てたタグに基づいて特定のリソースをすばやく識別できるため、これは同じ型のリソースが多い場合に役立ちます。

修正

タグをバックアップにコピーするように FSx for Lustre ファイルシステムを設定する方法については、「Amazon FSx for Lustre ユーザーガイド」の「同じ 内でバックアップをコピー AWS アカウントする」を参照してください。

[FSx.3] FSx for OpenZFS ファイルシステムは、マルチ AZ 配置用に設定する必要があります

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::FSx::FileSystem`

AWS Config ルール : fsx-openzfs-deployment-type-check

スケジュールタイプ: 定期的

パラメータ: `deploymentTypes: MULTI_AZ_1` (カスタマイズ不可)

このコントロールは、Amazon FSx for OpenZFS ファイルシステムが複数のアベイラビリティーゾーン (マルチ AZ) デプロイタイプを使用するように設定されているかどうかを確認します。ファイルシステムがマルチ AZ デプロイタイプを使用するように設定されていない場合、コントロールは失敗します。

Amazon FSx for OpenZFS は、マルチ AZ (HA)、シングル AZ (HA)、シングル AZ (非 HA) のいくつかのデプロイタイプをサポートしています。デプロイタイプは、さまざまなレベルの可用性と耐久性を提供します。マルチ AZ (HA) ファイルシステムは、2 つのアベイラビリティーゾーン (AZs) にまたがる高可用性 (HA) ペアのファイルサーバーで構成されます。マルチ AZ (HA) デプロイタイプは、高可用性と耐久性モデルを提供するため、ほとんどの本番ワークロードで使用することをお勧めします。

修正

ファイルシステムの作成時にマルチ AZ デプロイタイプを使用するように Amazon FSx for OpenZFS ファイルシステムを設定できます。既存の FSx for OpenZFS ファイルシステムのデプロイタイプを変更することはできません。

FSx for OpenZFS ファイルシステムのデプロイタイプとオプションの詳細については、「Amazon FSx for OpenZFS ユーザーガイド」の「Amazon FSx for OpenZFS の可用性と耐久性」および「ファイルシステムリソースの管理」を参照してください。 FSx OpenZFS

[FSx.4] FSx for NetApp ONTAP ファイルシステムは、マルチ AZ 配置用に設定する必要があります

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::FSx::FileSystem`

AWS Config ルール : fsx-ontap-deployment-type-check

スケジュールタイプ : 定期的

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`deploymentTypes`	評価に含めるデプロイタイプのリスト。ファイルシステムがリストで指定されたデプロイタイプを使用するように設定されていない場合、コントロールはFAILED結果を生成します。	列挙型	`MULTI_AZ_1` , `MULTI_AZ_2`	`MULTI_AZ_1` , `MULTI_AZ_2`

このコントロールは、Amazon FSx for NetApp ONTAP ファイルシステムが複数のアベイラビリティーゾーン (マルチ AZ) デプロイタイプを使用するように設定されているかどうかを確認します。ファイルシステムがマルチ AZ デプロイタイプを使用するように設定されていない場合、コントロールは失敗します。オプションで、評価に含めるデプロイタイプのリストを指定できます。

Amazon FSx for NetApp ONTAP は、ファイルシステム用に、シングル AZ 1、シングル AZ 2、マルチ AZ 1、マルチ AZ 2 のいくつかのデプロイタイプをサポートしています。デプロイタイプは、さまざまなレベルの可用性と耐久性を提供します。マルチ AZ デプロイタイプが提供する高可用性と耐久性モデルのため、ほとんどの本番ワークロードにはマルチ AZ デプロイタイプを使用することをお勧めします。マルチ AZ ファイルシステムは、シングル AZ ファイルシステムの可用性と耐久性の機能をすべてサポートしています。さらに、アベイラビリティーゾーン (AZ) が利用できない場合でも、データに継続的な可用性を提供するように設計されています。

修正

既存の Amazon FSx for NetApp ONTAP ファイルシステムのデプロイタイプを変更することはできません。ただし、データをバックアップし、マルチ AZ デプロイタイプを使用する新しいファイルシステムに復元できます。

FSx for ONTAP ファイルシステムのデプロイタイプとオプションの詳細については、FSx for ONTAP ユーザーガイド」の「可用性、耐久性、デプロイオプション」および「ファイルシステムの管理」を参照してください。

[FSx.5] FSx for Windows File Server ファイルシステムは、マルチ AZ 配置用に設定する必要があります

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::FSx::FileSystem`

AWS Config ルール : fsx-windows-deployment-type-check

スケジュールタイプ: 定期的

パラメータ: `deploymentTypes: MULTI_AZ_1` (カスタマイズ不可)

このコントロールは、Amazon FSx for Windows File Server ファイルシステムが複数のアベイラビリティーゾーン (マルチ AZ) デプロイタイプを使用するように設定されているかどうかを確認します。ファイルシステムがマルチ AZ デプロイタイプを使用するように設定されていない場合、コントロールは失敗します。

Amazon FSx for Windows File Server は、ファイルシステム用にシングル AZ とマルチ AZ の 2 つのデプロイタイプをサポートしています。デプロイタイプは、さまざまなレベルの可用性と耐久性を提供します。シングル AZ ファイルシステムは、単一の Windows ファイルサーバーインスタンスと、単一のアベイラビリティーゾーン (AZ) 内の一連のストレージボリュームで構成されます。マルチ AZ ファイルシステムは、2 つのアベイラビリティーゾーンにまたがる Windows ファイルサーバーの高可用性クラスターで構成されています。高可用性と耐久性モデルが提供されるため、ほとんどの本番ワークロードにはマルチ AZ デプロイタイプを使用することをお勧めします。

修正

ファイルシステムの作成時にマルチ AZ デプロイタイプを使用するように Amazon FSx for Windows File Server ファイルシステムを設定できます。既存の FSx for Windows File Server ファイルシステムのデプロイタイプを変更することはできません。

FSx for Windows File Server ファイルシステムのデプロイタイプとオプションの詳細については、Amazon FSx for Windows File Server ユーザーガイドの「可用性と耐久性: シングル AZ およびマルチ AZ ファイルシステム」および「Amazon FSx for Windows File Server の開始方法」を参照してください。 FSx FSx

Global Accelerator の Security Hub コントロール

これらの AWS Security Hub コントロールは、 AWS Global Accelerator サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::GlobalAccelerator::Accelerator`

AWS Config ルール: `tagged-globalaccelerator-accelerator` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、アクセラレーターにパラメータ AWS Global Accelerator で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。アクセラレータにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、アクセラレータにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、のAWS 「リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Global Accelerator グローバルアクセラレーターにタグを追加するには、「AWS Global Accelerator デベロッパーガイド」の「AWS Global Acceleratorのタグ付け」を参照してください。

の Security Hub コントロール AWS Glue

これらの AWS Security Hub コントロールは、 AWS Glue サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Glue.1] AWS Glue ジョブにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Glue::Job`

AWS Config ルール: `tagged-glue-job` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1～6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS Glue ジョブにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。ジョブにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ジョブにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS Glue ジョブにタグを追加するには、「 AWS Glue ユーザーガイド」の「 AWS のタグ AWS Glue」を参照してください。

[Glue.3] AWS Glue 機械学習変換は保管時に暗号化する必要があります

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::Glue::MLTransform`

AWS Config ルール : glue-ml-transform-encrypted-at-rest

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS Glue 機械学習変換が保管時に暗号化されているかどうかを確認します。機械学習変換が保管中に暗号化されていない場合、コントロールは失敗します。

保管中のデータとは、永続的な不揮発性ストレージに任意の期間保管されているデータを指します。保管中のデータを暗号化すると、その機密性が保護され、権限のないユーザーがアクセスするリスクが低減されます。

修正

AWS Glue 機械学習変換の暗号化を設定するには、「 AWS Glue ユーザーガイド」の「機械学習変換の使用」を参照してください。

[Glue.4] AWS Glue Spark ジョブは、サポートされているバージョンの で実行する必要があります AWS Glue

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 中

リソースタイプ : `AWS::Glue::Job`

AWS Config ルール : glue-spark-job-supported-version

スケジュールタイプ: 変更がトリガーされた場合

パラメータ： `minimumSupportedGlueVersion`: `3.0` (カスタマイズ不可)

このコントロールは、 AWS Glue for Spark ジョブがサポートされているバージョンの で実行されるように設定されているかどうかを確認します AWS Glue。Spark ジョブが、サポートされている最小バージョンより AWS Glue 前のバージョンの で実行されるように設定されている場合、コントロールは失敗します。

> **Note**
>
> このコントロールは、 AWS Glue バージョン (`GlueVersion`) プロパティが存在しないか、ジョブの設定項目 (CI) が null の場合にも、 AWS Glue for Spark ジョブ`FAILED`の検出結果を生成します。このような場合、検出結果には という注釈が含まれます`GlueVersion is null or missing in glueetl job configuration`。このタイプの`FAILED`検出結果に対処するには、ジョブの設定に `GlueVersion`プロパティを追加します。サポートされているバージョンとランタイム環境のリストについては、AWS Glue 「 ユーザーガイド」の[AWS Glue 「バージョン」](#)を参照してください。

の最新バージョンで AWS Glue Spark ジョブを実行すると、パフォーマンス、セキュリティ、および の最新機能へのアクセスを最適化 AWS Glue できます AWS Glue。また、セキュリティの脆弱性に対する保護にも役立ちます。たとえば、新しいバージョンをリリースして、セキュリティ更新プログラムの提供、問題に対処、新機能の導入を行うことができます。

修正

Spark ジョブをサポートされている バージョンに移行する方法については AWS Glue、AWS Glue 「 ユーザーガイド」の[「Spark ジョブ AWS Glue の移行」](#)を参照してください。

Amazon GuardDuty の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon GuardDuty サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「[リージョン別のコントロールの可用性](#)」を参照してください。

[GuardDuty.1] GuardDuty を有効にする必要があります

関連する要件： NIST.800-53.r5 AC-2(12)、 NIST.800-53.r5 AU-6(1)、 NIST.800-53.r5 AU-6(5)、 NIST.800-53.r5 CA-7、 NIST.800-53.r5 CM-8(3)、 NIST.800-53.r5 RA-3(4)、 NIST.800-53.r5 SA-11(1)、 NIST.800-53.r5 SA-11(6)、 NIST.800-53.r5 SA-15(2)、 NIST.800-53.r5 SA-15(8)、

NIST.800-53.r5 SA-8(19)、 NIST.800-53.r5 SA-8(21)、 NIST.800-53.r5 SA-8(25)、 NIST.800-53.r5 SC-5、 NIST.800-53.r5 SC-5(1)、 NIST.800-53.r5 SC-5(3)、 NIST.800-53.r5 SI-20、 NIST.800-53.r5 SI-3(8)、 NIST.800-53.r5 SI-4、 NIST.800-53.r5 SI-4(1)、 NIST.800-53.r5 SI-4(13)、 NIST.800-53.r5 SI-4(2)、 NIST.800-53.r5 SI-4(22)、 NIST.800-53.r5 SI-4(25)、 NIST.800-53.r5 SI-4(4)、 NIST.800-53.r5 SI-4(5)、 NIST.800-171.r2 3.4.2、 NIST.800-171.r2 3.14.6、 NIST.800-171.r2 3.14.7、 PCI DSS v3.2.1/11.4、 PCI DSS v4.0.1/11.5.1

カテゴリ: 検出 > 検出サービス

重要度: 高

リソースタイプ : `AWS::::Account`

AWS Config ルール : guardduty-enabled-centralized

スケジュールタイプ : 定期的

パラメータ: なし

このコントロールは、GuardDuty アカウントおよびリージョンで Amazon GuardDuty が有効になっているかどうかをチェックします。

サポートされているすべての AWS リージョンで GuardDuty を有効にすることを強くお勧めします。このように設定することで、ユーザーが能動的に使用していないリージョンでも、許可されていないアクティビティや異常なアクティビティに関する結果を GuardDuty で生成できます。これにより GuardDuty で、IAM などのグローバルな AWS のサービス の CloudTrail イベントもモニタリングできます。

修正

GuardDuty を有効にするには、「Amazon GuardDuty ユーザーガイド」の「GuardDuty の開始方法」を参照してください。

[GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::GuardDuty::Filter`

AWS Config ルール: `tagged-guardduty-filter` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、Amazon GuardDuty フィルターにパラメータ `requiredTagKeys` で定義された特定のキーを含むタグがあるかどうかをチェックします。フィルターにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、フィルターにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、のAWS 「リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

GuardDuty フィルターにタグを追加するには、「Amazon GuardDutyリファレンス」の「TagResource」を参照してください。

[GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::GuardDuty::IPSet`

AWS Config ルール: `tagged-guardduty-ipset` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、Amazon GuardDuty IPSet にパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。IPSet にタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、IPSet にキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス

許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、のAWS 「リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

GuardDuty IPSet にタグを追加するには、「Amazon GuardDutyリファレンス」の「TagResource」を参照してください。

[GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::GuardDuty::Detector`

AWS Config ルール: `tagged-guardduty-detector` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタ	StringList (最大 6 項目)	AWS 要件を満たす 1 ~	`No default value`

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	グキーのリスト。タグキーでは、大文字と小文字が区別されます。		6 個のタグキー。	

このコントロールは、Amazon GuardDuty ディテクターにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。ディテクターにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ディテクターがキーでタグ付けされていない場合に失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

GuardDuty ディテクターにタグを追加するには、「Amazon GuardDutyリファレンス」の「TagResource」を参照してください。

[GuardDuty.5] GuardDuty EKS 監査ログモニタリングを有効にする必要があります

カテゴリ: 検出 > 検出サービス

重要度: 高

リソースタイプ : `AWS::GuardDuty::Detector`

AWS Config ルール : guardduty-eks-protection-audit-enabled

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、GuardDuty EKS 監査ログモニタリングが有効になっているかを確認します。スタンドアロンアカウントの場合、アカウントで GuardDuty EKS 監査ログモニタリングが無効になっていると、コントロールは失敗します。マルチアカウント環境では、委任 GuardDuty 管理者アカウントとすべてのメンバーアカウントで EKS 監査ログモニタリングが有効になっていない場合、コントロールは失敗します。

マルチアカウント環境では、コントロールは委任 GuardDuty 管理者アカウントでのみ結果を生成します。組織内のメンバーアカウントの EKS 監査ログのモニタリング機能を有効または無効にできるのは、委任管理者アカウントのみです。GuardDuty メンバーアカウントからは、この設定を変更できません。このコントロールは、委任 GuardDuty 管理者に GuardDuty EKS 監査ログモニタリングが有効になっていない停止されたメンバーアカウントがある場合に `FAILED` 検出結果を生成します。`PASSED` 検出結果を受け取るには、委任管理者が GuardDuty でこれらの停止されたアカウントの関連付けを解除する必要があります。

GuardDuty EKS 監査ログのモニタリングは、Amazon Elastic Kubernetes Service (Amazon EKS) クラスターの疑わしいアクティビティの可能性を検出するのに役立ちます。EKS 監査ログのモニタリングは、ユーザー、Kubernetes API を使用するアプリケーション、およびコントロールプレーンからの時系列アクティビティをキャプチャします。

修正

GuardDuty EKS 監査ログモニタリングを有効にするには、「Amazon GuardDuty ユーザーガイド」の「EKS 監査ログモニタリング」を参照してください。

[GuardDuty.6] GuardDuty Lambda Protection を有効にする必要があります

関連する要件： PCI DSS v4.0.1/11.5.1

カテゴリ: 検出 > 検出サービス

重要度: 高

リソースタイプ : `AWS::GuardDuty::Detector`

AWS Config ルール : guardduty-lambda-protection-enabled

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、GuardDuty Lambda Protection が有効になっているかどうかをチェックします。スタンドアロンアカウントの場合、アカウントで GuardDuty Lambda Protection が無効になっていると、コントロールは失敗します。マルチアカウント環境では、委任 GuardDuty 管理者アカウントとすべてのメンバーアカウントで Lambda Protection が有効になっていない場合、コントロールは失敗します。

マルチアカウント環境では、コントロールは委任 GuardDuty 管理者アカウントでのみ結果を生成します。委任管理者は、組織内の既存のメンバーアカウントに対して Lambda Protection 機能を有効または無効にできます。GuardDuty メンバーアカウントからは、この設定を変更できません。このコントロールは、委任 GuardDuty 管理者に GuardDuty Lambda Protection が有効になっていない停止メンバーアカウントがある場合に `FAILED` 検出結果を生成します。`PASSED` 検出結果を受け取るには、委任管理者が GuardDuty でこれらの停止されたアカウントの関連付けを解除する必要があります。

GuardDuty Lambda Protection は、 AWS Lambda 関数が呼び出されたときに潜在的なセキュリティ脅威を特定するのに役立ちます。Lambda Protection を有効にすると、GuardDuty は AWS アカウントの Lambda 関数に関連付けられた Lambda ネットワークアクティビティログのモニタリングを開始します。Lambda 関数が呼び出され GuardDuty が Lambda 関数に潜在的に悪意のあるコードが存在することを示す疑わしいネットワークトラフィックを特定した場合、GuardDuty は検出結果を生成します。

修正

GuardDuty Lambda Protection を有効にするには、「Amazon GuardDutyユーザーガイド」の「Lambda Protection の設定」を参照してください。

[GuardDuty.7] GuardDuty EKS ランタイムモニタリングを有効にする必要があります

関連する要件： PCI DSS v4.0.1/11.5.1

カテゴリ: 検出 > 検出サービス

重要度: 中

リソースタイプ : `AWS::GuardDuty::Detector`

AWS Config ルール : guardduty-eks-protection-runtime-enabled

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、自動エージェント管理による GuardDuty EKS ランタイムモニタリングが有効になっているかを確認します。スタンドアロンアカウントの場合、アカウントで自動エージェント管理による GuardDuty EKS ランタイムモニタリングが無効になっていると、コントロールは失敗します。マルチアカウント環境では、委任 GuardDuty 管理者アカウントとすべてのメンバーアカウントに自動エージェント管理が有効になっている EKS Runtime Monitoring がない場合、コントロールは失敗します。

マルチアカウント環境では、コントロールは委任 GuardDuty 管理者アカウントでのみ結果を生成します。委任管理者のみが、組織内のメンバーアカウントのエージェント管理を自動化して EKS ランタイムモニタリング機能を有効または無効にできます。GuardDuty メンバーアカウントからは、この設定を変更できません。このコントロールは、委任 GuardDuty 管理者に GuardDuty EKS ランタイムモニタリングが有効になっていない停止メンバーアカウントがある場合に `FAILED` 検出結果を生成します。`PASSED` 検出結果を受け取るには、委任管理者が GuardDuty でこれらの停止されたアカウントの関連付けを解除する必要があります。

Amazon GuardDuty の EKS Protection は、脅威検出の範囲を提供し、 AWS 環境内の Amazon EKS クラスターを保護するのに役立ちます。EKS Runtime Monitoring は、オペレーティングシステムレベルのイベントを使用して、EKS クラスター内の EKS ノードとコンテナにおける潜在的な脅威を検出するのに役立ちます。

修正

自動エージェント管理で EKS ランタイムモニタリングを有効にするには、「Amazon GuardDuty ユーザーガイド」の「GuardDuty ランタイムモニタリングの有効化」を参照してください。

[GuardDuty.8] GuardDuty Malware Protection for EC2 を有効にする必要があります

カテゴリ: 検出 > 検出サービス

重要度: 高

リソースタイプ : `AWS::GuardDuty::Detector`

AWS Config ルール : guardduty-malware-protection-enabled

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、GuardDuty Malware Protection が有効になっているかどうかをチェックします。スタンドアロンアカウントの場合、アカウントで GuardDuty Malware Protection が無効になっていると、コントロールは失敗します。マルチアカウント環境では、委任 GuardDuty 管理者アカウントとすべてのメンバーアカウントで Malware Protection が有効になっていない場合、コントロールは失敗します。

マルチアカウント環境では、コントロールは委任 GuardDuty 管理者アカウントでのみ結果を生成します。委任管理者のみが、組織内のメンバーアカウントに対して Malware Protection 機能を有効または無効にできます。GuardDuty メンバーアカウントからは、この設定を変更できません。このコントロールは、委任された GuardDuty 管理者に GuardDuty Malware Protection が有効になっていない停止メンバーアカウントがある場合に `FAILED` 検出結果を生成します。`PASSED` 検出結果を受け取るには、委任管理者が GuardDuty でこれらの停止されたアカウントの関連付けを解除する必要があります。

GuardDuty Malware Protection for EC2 は、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスおよびコンテナワークロードにアタッチされた Amazon Elastic Block Store (Amazon EBS) ボリュームをスキャンすることで、マルウェアの潜在的な存在を検出することに役立ちます。Malware Protection は、スキャン時に特定の EC2 インスタンスおよびコンテナワークロードを含めるか除外するかを決定できるスキャンオプションを提供します。EC2 インスタンスまたはコンテナワークロードにアタッチされた EBS ボリュームのスナップショットを GuardDuty アカウントに保持するオプションも提供します。スナップショットは、マルウェアが検出されて Malware Protection の検出結果が生成された場合にのみ保持されます。

修正

EC2 で GuardDuty Malware Protection を有効にするには、「Amazon GuardDuty ユーザーガイド」の「GuardDuty で開始されたマルウェアスキャンの設定」を参照してください。

[GuardDuty.9] GuardDuty RDS Protection を有効にする必要があります

関連する要件： PCI DSS v4.0.1/11.5.1

カテゴリ: 検出 > 検出サービス

重要度: 高

リソースタイプ : `AWS::GuardDuty::Detector`

AWS Config ルール : guardduty-rds-protection-enabled

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、GuardDuty RDS Protection が有効になっているかを確認します。スタンドアロンアカウントの場合、アカウントで GuardDuty RDS Protection が無効になっていると、コントロールは失敗します。マルチアカウント環境では、委任 GuardDuty 管理者アカウントとすべてのメンバーアカウントで RDS Protection が有効になっていない場合、コントロールは失敗します。

マルチアカウント環境では、コントロールは委任 GuardDuty 管理者アカウントでのみ結果を生成します。委任管理者のみが、組織内のメンバーアカウントに対して RDS Protection 機能を有効または無効にできます。GuardDuty メンバーアカウントからは、この設定を変更できません。このコントロールは、委任された GuardDuty 管理者に GuardDuty RDS Protection が有効になっていない停止メンバーアカウントがある場合に`FAILED` 検出結果を生成します。`PASSED` 検出結果を受け取るには、委任管理者が GuardDuty でこれらの停止されたアカウントの関連付けを解除する必要があります。

GuardDuty の RDS Protection は、RDS ログインアクティビティを分析してプロファイリングし、Amazon Aurora データベース (Aurora MySQL 互換エディションおよび Aurora PostgreSQL 互換エディション) への潜在的なアクセス脅威がないかどうかを調べます。この機能により、潜在的に疑わしいログイン動作を特定できます。RDS Protection は追加のインフラストラクチャが不要で、データベースインスタンスのパフォーマンスに影響を与えないように設計されています。RDS Protection がデータベースへの脅威を示す潜在的に疑わしいログイン試行または異常なログイン試行を検出すると、GuardDuty は侵害の可能性があるデータベースに関する詳細な新しい検出結果を生成します。

修正

GuardDuty RDS Protection を有効にするには、「Amazon GuardDuty ユーザーガイド」の「GuardDuty RDS Protection」を参照してください。

[GuardDuty.10] GuardDuty S3 Protection を有効にする必要があります

関連する要件： PCI DSS v4.0.1/11.5.1

カテゴリ: 検出 > 検出サービス

重要度: 高

リソースタイプ : `AWS::GuardDuty::Detector`

AWS Config ルール : guardduty-s3-protection-enabled

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、GuardDuty S3 Protection が有効になっているかどうかをチェックします。スタンドアロンアカウントの場合、アカウントで GuardDuty S3 Protection が無効になっていると、コントロールは失敗します。マルチアカウント環境では、委任 GuardDuty 管理者アカウントとすべてのメンバーアカウントで S3 Protection が有効になっていない場合、コントロールは失敗します。

マルチアカウント環境では、コントロールは委任 GuardDuty 管理者アカウントでのみ結果を生成します。委任管理者のみが、組織内のメンバーアカウントに対して S3 Protection 機能を有効または無効にできます。GuardDuty メンバーアカウントからは、この設定を変更できません。このコントロールは、委任された GuardDuty 管理者に GuardDuty S3 Protection が有効になっていない停止メンバーアカウントがある場合に `FAILED` 検出結果を生成します。`PASSED` 検出結果を受け取るには、委任管理者が GuardDuty でこれらの停止されたアカウントの関連付けを解除する必要があります。

S3 Protectionにより、GuardDuty は、オブジェクトレベルの API オペレーションをモニタリングし、Amazon Simple Storage Service (Amazon S3) バケット内のデータに関する潜在的なセキュリティリスクを特定できるようになります。GuardDuty は、 AWS CloudTrail 管理イベントと CloudTrail S3 データイベントを分析して、S3 リソースに対する脅威をモニタリングします。

修正

GuardDuty S3 Protection を有効にするには、「Amazon GuardDuty ユーザーガイド」の「Amazon S3 protection in Amazon GuardDuty」を参照してください。

[GuardDuty.11] GuardDuty Runtime Monitoring を有効にする必要があります

カテゴリ: 検出 > 検出サービス

重要度: 高

リソースタイプ : `AWS::GuardDuty::Detector`

AWS Config ルール : guardduty-runtime-monitoring-enabled

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon GuardDuty で Runtime Monitoring が有効になっているかどうかをチェックします。スタンドアロンアカウントの場合、アカウントで GuardDuty Runtime Monitoring が無効になっていると、コントロールは失敗します。マルチアカウント環境では、委任 GuardDuty 管理者アカウントとすべてのメンバーアカウントで GuardDuty Runtime Monitoring が無効になっていると、コントロールは失敗します。

マルチアカウント環境では、委任 GuardDuty 管理者のみが組織内のアカウントの GuardDuty Runtime Monitoring を有効または無効にできます。さらに、GuardDuty 管理者のみが、GuardDuty が組織内のアカウントの AWS ワークロードとリソースのランタイムモニタリングに使用するセキュリティエージェントを設定および管理できます。GuardDuty メンバーアカウントは、自分のアカウントの Runtime Monitoring を有効、設定、または無効にすることはできません。

GuardDuty Runtime Monitoring は、オペレーティングシステムレベル、ネットワーク、ファイルイベントを監視および分析して、環境内の特定の AWS ワークロードで潜在的な脅威を検出するのに役立ちます。ファイルアクセス、プロセス実行、コマンドライン引数、ネットワーク接続などのランタイム動作を可視化する GuardDuty セキュリティエージェントを使用します。Amazon EKS クラスターや Amazon EC2 インスタンスなど、潜在的な脅威をモニタリングするリソースのタイプごとにセキュリティエージェントを有効にして管理できます。

修正

GuardDuty Runtime Monitoring の設定と有効化の詳細については、Amazon GuardDuty ユーザーガイドの「GuardDuty Runtime Monitoring Amazon GuardDuty と GuardDuty Runtime Monitoring の有効化 GuardDuty」を参照してください。

[GuardDuty.12] GuardDuty ECS Runtime Monitoring を有効にする必要があります

カテゴリ: 検出 > 検出サービス

重要度: 中

リソースタイプ : `AWS::GuardDuty::Detector`

AWS Config ルール : guardduty-ecs-protection-runtime-enabled

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon GuardDuty 自動セキュリティエージェントが Amazon ECS クラスターのランタイムモニタリングが有効になっているかどうかを確認します AWS Fargate。スタンドアロンアカウントの場合、アカウントでセキュリティエージェントが無効になっていると、コントロールは失敗します。マルチアカウント環境では、委任 GuardDuty 管理者アカウントとすべてのメンバーアカウントでセキュリティエージェントが無効になっていると、コントロールは失敗します。

マルチアカウント環境では、このコントロールは委任 GuardDuty 管理者アカウントでのみ結果を生成します。これは、委任 GuardDuty 管理者のみが、組織内のアカウントの ECS-Fargate リソースの Runtime Monitoring を有効または無効にできるためです。GuardDuty メンバーアカウントは、自分のアカウントに対してこれを行うことはできません。さらに、GuardDuty がメンバーアカウントで停止され、ECS-Fargate リソースのランタイムモニタリングがメンバーアカウントで無効になっている場合、このコントロールは`FAILED`検出結果を生成します。`PASSED` 検出結果を受け取るには、GuardDuty 管理者は、GuardDuty を使用して、停止されたメンバーアカウントと管理者アカウントの関連付けを解除する必要があります。

GuardDuty Runtime Monitoring は、オペレーティングシステムレベル、ネットワーク、ファイルイベントを監視および分析して、環境内の特定の AWS ワークロードで潜在的な脅威を検出するのに役立ちます。ファイルアクセス、プロセス実行、コマンドライン引数、ネットワーク接続などのランタイム動作を可視化する GuardDuty セキュリティエージェントを使用します。潜在的な脅威をモニタリングするリソースのタイプごとに、セキュリティエージェントを有効にして管理できます。これには、 上の Amazon ECS クラスターが含まれます AWS Fargate。

修正

ECS-Fargate リソースの GuardDuty Runtime Monitoring のセキュリティエージェントを有効にして管理するには、GuardDuty を直接使用する必要があります。ECS-Fargate リソースに対して手動で有効化または管理することはできません。セキュリティエージェントの有効化と管理の詳細については、「Amazon GuardDuty ユーザーガイド」の AWS Fargate 「(Amazon ECS のみ) サポートの前提条件」とAWS Fargate 「(Amazon ECS のみ) の自動セキュリティエージェントの管理」を参照してください。 Amazon GuardDuty

[GuardDuty.13] GuardDuty EC2 Runtime Monitoring を有効にする必要があります

カテゴリ: 検出 > 検出サービス

重要度: 中

リソースタイプ : `AWS::GuardDuty::Detector`

AWS Config ルール : guardduty-ec2-protection-runtime-enabled

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon GuardDuty 自動セキュリティエージェントが Amazon EC2 インスタンスのランタイムモニタリングが有効になっているかどうかを確認します。スタンドアロンアカウントの場合、アカウントでセキュリティエージェントが無効になっていると、コントロールは失敗します。マルチアカウント環境では、委任 GuardDuty 管理者アカウントとすべてのメンバーアカウントでセキュリティエージェントが無効になっていると、コントロールは失敗します。

マルチアカウント環境では、このコントロールは委任 GuardDuty 管理者アカウントでのみ結果を生成します。これは、委任 GuardDuty 管理者のみが、組織内のアカウントの Amazon EC2 インスタンスのランタイムモニタリングを有効または無効にできるためです。GuardDuty メンバーアカウントは、自分のアカウントに対してこれを行うことはできません。さらに、メンバーアカウントで GuardDuty が中断され、メンバーアカウントで EC2 インスタンスのランタイムモニタリングが無効になっている場合、このコントロールは`FAILED`検出結果を生成します。`PASSED` 検出結果を受け取るには、GuardDuty 管理者は、GuardDuty を使用して、停止されたメンバーアカウントと管理者アカウントの関連付けを解除する必要があります。

GuardDuty Runtime Monitoring は、オペレーティングシステムレベル、ネットワーク、ファイルイベントを監視および分析して、環境内の特定の AWS ワークロードで潜在的な脅威を検出するのに役立ちます。ファイルアクセス、プロセス実行、コマンドライン引数、ネットワーク接続などのランタイム動作を可視化する GuardDuty セキュリティエージェントを使用します。潜在的な脅威をモニタリングするリソースのタイプごとに、セキュリティエージェントを有効にして管理できます。これには Amazon EC2 インスタンスが含まれます。

修正

EC2 インスタンスの GuardDuty Runtime Monitoring の自動セキュリティエージェントの設定と管理の詳細については、Amazon EC2 インスタンスのサポートの前提条件」とAmazon EC2 インスタンスの自動セキュリティエージェントの有効化」を参照してください。 Amazon GuardDuty

の Security Hub コントロール AWS Identity and Access Management

これらの AWS Security Hub コントロールは、 AWS Identity and Access Management (IAM) サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください

関連する要件： CIS AWS Foundations Benchmark v1.2.0/1.22、CIS AWS Foundations Benchmark v1.4.0/1.16、NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6NIST.800-53.r5 AC-6(10)、NIST.800-53.r5 AC-6(2) NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 高

リソースタイプ : `AWS::IAM::Policy`

AWS Config ルール : `iam-policy-no-statements-with-admin-access`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `excludePermissionBoundaryPolicy: true` (カスタマイズ不可)

このコントロールは、IAM ポリシー (カスタマー管理ポリシーとも呼ばれます) のデフォルトバージョンに、`"Action": "*"` が `"Resource": "*"` に対して規定された `"Effect": "Allow"` ステートメントを持つ管理者アクセス権があるかどうかをチェックします。このようなステートメントを含む IAM ポリシーがある場合、コントロールは失敗します。

コントロールは、作成したカスタマーマネージドポリシーのみをチェックします。インラインポリシーと AWS 管理ポリシーはチェックされません。

IAM ポリシーは、ユーザー、グループ、またはロールに付与される権限のセットを定義します。標準のセキュリティアドバイスに従って、 AWS は最小権限を付与することをお勧めします。これは、タスクの実行に必要なアクセス許可のみを付与することを意味します。ユーザーが必要とする最小限の許可セットではなく、完全な管理者権限を提供すると、リソースが不要なアクションにさらされる可能性があります。

完全な管理者権限を許可するのではなく、ユーザーが何をする必要があるのかを決定し、ユーザーが、それらのタスクのみを実行できるポリシーを作成します。最小限の許可セットから開始し、必要に応じて追加許可を付与する方がより安全です。あまりにも寛大な許可から始めて、後でそれらを強化しようとしないでください。

`"Effect": "Allow"` および `"Action": "*"` が `"Resource": "*"` に対して規定されたステートメントを持つ IAM ポリシーは削除する必要があります。

> **Note**
>
> AWS Config は、Security Hub を使用するすべてのリージョンで有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。グローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

IAM ポリシーを変更して、完全な「*」管理者権限を許可しないようにする方法については、「IAM ユーザーガイド」の「IAM ポリシーの編集」を参照してください。

[IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.15、CIS AWS Foundations Benchmark v1.2.0/1.16、NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(3)、NIST.800-171.r2

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 低

リソースタイプ : `AWS::IAM::User`

AWS Config ルール : `iam-user-no-policies-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、IAM ユーザーにポリシーが添付済みかどうかをチェックします。IAM ユーザーにポリシーが添付されている場合、コントロールは失敗します。代わりに、IAM ユーザーは、IAM グループまたはロールから許可を継承するか、ロールを引き受ける必要があります。

デフォルトでは、IAM ユーザー、グループ、ロールは AWS リソースにアクセスできません。IAM ポリシーで、ユーザー、グループ、またはロールに権限を付与します。IAM ポリシーはグループとロールには直接適用しますが、ユーザーには直接適用しないことを推奨します。グループレベルまた

はロールレベルで権限を割り当てると、ユーザー数が増えるにつれてアクセス管理の複雑さが軽減されます。アクセス管理の複雑さを軽減することで、プリンシパルが誤って過剰な権限を受け取ったり保持する機会を減らすことができます。

> **Note**
>
> AWS Config は、Security Hub を使用するすべてのリージョンで有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。グローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

この問題を解決するには、IAM グループを作成し、ポリシーをこのグループにアタッチします。続いて、ユーザーをこのグループに追加します。ポリシーは、グループ内の各ユーザーに適用されます。ユーザーに直接添付されているポリシーを削除するには、IAM ユーザーガイドの「IAM ID のアクセス許可の追加および削除」を参照してください。

[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.14、CIS AWS Foundations Benchmark v1.4.0/1.14、CIS AWS Foundations Benchmark v1.2.0/1.4、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-2(3)、NIST.800-53.r5 AC-3(15)、PCI DSS v4.0.1/8.3.9、PCI DSS v4.0.1/8.6.3

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::IAM::User`

AWS Config ルール : `access-keys-rotated`

スケジュールタイプ : 定期的

パラメータ :

- `maxAccessKeyAge`: `90` (カスタマイズ不可)

このコントロールは、アクティブなアクセスキーが 90 日以内にローテーションされているかどうかをチェックします。

アカウントのすべてのアクセスキーを生成したり削除したりしないことを強く推奨します。代わりに、1 つ以上の IAM ロールを作成するか、フェデレーションを使用することをお勧めします AWS IAM Identity Center。これらの方法を使用して、ユーザーに AWS Management Console および へのアクセスを許可できます AWS CLI。

各アプローチにはそれぞれのユースケースがあります。フェデレーションは、既存の中央ディレクトリを保有する企業や、現在の制限 IAM ユーザーよりも多くを必要とする予定の企業にとって一般的に適しています。 AWS 環境外で実行されるアプリケーションには、 AWS リソースへのプログラムによるアクセスのためのアクセスキーが必要です。

ただし、プログラムによるアクセスを必要とするリソースが内部で実行されている場合 AWS、ベストプラクティスは IAM ロールを使用することです。ロールを使用すると、アクセスキー ID とシークレットアクセスキーを設定にハードコーディングすることなく、リソースへのアクセスを許可できます。

アクセスキーとアカウントの保護の詳細については、のAWS 「アクセスキーを管理するためのベストプラクティス」を参照してくださいAWS 全般のリファレンス。また、ブログ記事「プログラムによるアクセスの使用 AWS アカウント 中に を保護するためのガイドライン」も参照してください。

アクセスキーが既に存在する場合、Security Hub では 90 日ごとにアクセスキーをローテーションすることを推奨します。アクセスキーをローテーションすることにより、侵害されたアカウントや終了したアカウントに関連付けられているアクセスキーが使用される可能性が低くなります。また、紛失した、クラックされた、盗まれた古いキーでデータにアクセスできないようにします。アクセスキーをローテーションしたら、必ずアプリケーションを更新してください。

アクセスキーは、アクセスキー ID とシークレットアクセスキーで構成されます。これは AWSへのプログラムによるリクエストの署名に使用されます。ユーザーは、、Tools for Windows PowerShell AWS CLI、 AWS SDKs、または個々の API オペレーションを使用した直接 HTTP 呼び出し AWS からプログラムで を呼び出すために、独自のアクセスキーが必要です AWS のサービス。

組織が AWS IAM Identity Center (IAM Identity Center) を使用している場合、ユーザーは Active Directory、組み込みの IAM Identity Center ディレクトリ、または IAM Identity Center に接続された別の ID プロバイダー (IdP) にサインインできます。その後、アクセスキーを必要とせずに AWS CLI コマンドを実行したり AWS API オペレーションを呼び出すことができる IAM ロールにマッピングできます。詳細については、「 AWS Command Line Interface ユーザーガイド」の「 を使用する AWS CLI ように AWS IAM Identity Centerを設定する」を参照してください。

> **Note**
>
> AWS Config は、Security Hub を使用するすべてのリージョンで有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。グローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

90 日以上経過したアクセスキーをローテーションするには、「IAM ユーザーガイド」の「アクセスキーのローテーション」を参照してください。[アクセスキーの有効期間] が 90 日を超えるすべてのユーザーに対する指示に従ってください。

[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.4、CIS AWS Foundations Benchmark v1.4.0/1.4、CIS AWS Foundations Benchmark v1.2.0/1.12、PCI DSS v3.2.1/2.2、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)NIST.800-53.r5 AC-6NIST.800-53.r5 AC-610)、 NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 非常事態

リソースタイプ : `AWS::::Account`

AWS Config ルール : `iam-root-access-key-check`

スケジュールタイプ : 定期的

パラメータ: なし

このコントロールは、ルートユーザーアクセスキーが存在するかどうかをチェックします。

ルートユーザーは、 の最も特権のあるユーザーです AWS アカウント。 AWS アクセスキーは、特定のアカウントへのプログラムによるアクセスを提供します。

Security Hub では、ルートユーザーに関連付けられたすべてのアクセスキーの削除を推奨します。これにより、お使いのアカウントの侵害に使用できるベクトルが制限されます。また、最小特権のロールベースのアカウントの作成と使用が促進されます。

修正

ルートユーザーアクセスキーを削除するには、「IAM ユーザーガイドの「ルートユーザーのアクセスキーの削除」を参照してください。 AWS アカウント の からルートユーザーアクセスキーを削除するには AWS GovCloud (US)、AWS GovCloud (US) 「 ユーザーガイド」の AWS GovCloud (US) 「アカウントルートユーザーアクセスキーの削除」を参照してください。

[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.10、CIS AWS Foundations Benchmark v1.4.0/1.10、CIS AWS Foundations Benchmark v1.2.0/1.2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 IA-2(1)、NIST.800-53.r5 IA-2(2)、NIST.800-53.r5 IA-2(6)、NIST.800-53.r5 IA-2(8)、PCI DSS v4.0.1/8.4.2

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::IAM::User`

AWS Config ルール : `mfa-enabled-for-iam-console-access`

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、コンソールパスワードを使用するすべての IAM ユーザーに対して AWS 多要素認証 (MFA) が有効になっているかどうかをチェックします。

多要素認証 (MFA) は、ユーザー名とパスワードに更なる保護手段を追加します。MFA を有効にすると、ユーザーが AWS ウェブサイトにサインインすると、ユーザー名とパスワードの入力を求められます。さらに、 AWS MFA デバイスから認証コードの入力を求められます。

コンソールパスワードを使用するすべてのアカウントにおいて、MFA を有効にすることを推奨します。MFA は、コンソールアクセスのセキュリティを強化するために設計されています。認証プリンシパルは、時間的制約のあるキーを発行するデバイスを所有し、認証情報に関する知識がある必要があります。

> **Note**
>
> AWS Config は、Security Hub を使用するすべてのリージョンで有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。

グローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

IAM ユーザーを MFA に追加するには、IAM ユーザーガイドの「AWSでの多要素認証 (MFA) の使用」を参照してください。

対象となるお客様には、MFA セキュリティキーを無料で提供しています。資格があるかどうかを確認し、無料のキーを注文します。

[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.6、CIS AWS Foundations Benchmark v1.4.0/1.6、CIS AWS Foundations Benchmark v1.2.0/1.14、PCI DSS v3.2.1/8.3.1、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 IA-2(1)、NIST.800-53.r5 IA-2(2)、NIST.80IA-20-53.r5 IA-2(8)、PCI v4。

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 非常事態

リソースタイプ : `AWS::::Account`

AWS Config ルール : `root-account-hardware-mfa-enabled`

スケジュールタイプ : 定期的

パラメータ : なし

このコントロール AWS アカウント は、 がハードウェア多要素認証 (MFA) デバイスを使用してルートユーザー認証情報でサインインできるかどうかを確認します。ハードウェア MFA が有効になっていない場合、または仮想 MFA デバイスがルートユーザー認証情報でサインインすることを許可されている場合、コントロールは失敗します。

仮想 MFA はハードウェア MFA デバイスと同じレベルのセキュリティを提供しない可能性があります。仮想 MFA デバイスは、ハードウェア購入の承認またはハードウェアの到着を待つ間のみ使用することをお勧めします。詳細については、IAM ユーザーガイドの「仮想 MFA デバイスの割り当て (コンソール)」を参照してください。

> **Note**
>
> Security Hub は、 内のルートユーザー認証情報 (ログインプロファイル) の存在に基づいてこのコントロールを評価します AWS アカウント。コントロールは、次の場合に PASSED 検出結果を生成します。
>
> - ルートユーザー認証情報がアカウントに存在し、ルートユーザーに対してハードウェア MFA が有効になっています。
> - ルートユーザーの認証情報はアカウントに存在しません。
>
> ルートユーザーの認証情報がアカウントに存在し、ルートユーザーに対してハードウェア MFA が有効になっていない場合、コントロールはFAILED検出結果を生成します。

修正

ルートユーザーのハードウェア MFA を有効にする方法については、IAM ユーザーガイドの「 の多要素認証 AWS アカウントのルートユーザー」を参照してください。

対象となるお客様には、MFA セキュリティキーを無料で提供しています。資格があるかどうかを確認するには、MFA セキュリティキープログラムのFAQsを参照してください。

[IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です

関連する要件： NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-2(3)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 IA-5(1)、NIST.800-171.r2 3.5.2、NIST.800-171.r2 3.5.7、NIST.800-171.r2 3.5.8、PCI DSS v4.0.1/8.3.7、PCI DSS v4.0.1/8.3.9、PCI v4.08.3.10

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::::Account`

AWS Config ルール : `iam-password-policy`

スケジュールタイプ : 定期的

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
RequireUppercaseCharacters	パスワードには少なくとも 1 つの大文字が必要です	ブール値	true 、、または false	true
RequireLowercaseCharacters	パスワードには少なくとも 1 つの小文字が必要です	ブール値	true 、、または false	true
RequireSymbols	パスワードには少なくとも 1 つの記号が必要です	ブール値	true 、、または false	true
RequireNumbers	パスワードには少なくとも 1 つの数字が必要です	ブール値	true 、、または false	true
MinimumPasswordLength	パスワードに含まれる文字の最小数	整数	8 ~ 128	8
PasswordReusePrevention	古いパスワードを再使用できるようになるまでのパスワードローテーション回数	整数	12 ~ 24	デフォルト値なし
MaxPasswordAge	パスワードが有効期限切れになるまでの日数	整数	1 ~ 90	デフォルト値なし

このコントロールは、IAM ユーザーのアカウントパスワードポリシーが強力な設定を使用しているかどうかをチェックします。パスワードポリシーが強力な設定を使用していない場合、コントロールは失敗します。カスタムパラメータ値を指定しない限り、Security Hub は前の表に記載されているデフォルト値を使用します。PasswordReusePrevention パラメータおよび MaxPasswordAge パラメータにはデフォルト値がないため、これらのパラメータを除外した場合、Security Hub はこのコントロールを評価する際にパスワードローテーションの回数とパスワードの有効期間を無視します。

にアクセスするには AWS Management Console、IAM ユーザーにパスワードが必要です。ベストプラクティスとして、Security Hub では IAM ユーザーを作成する代わりに、フェデレーションの使

用を強く推奨します。フェデレーションでは、ユーザーは既存の企業認証情報を使用して、 AWS Management Consoleにログインできます。 AWS IAM Identity Center (IAM Identity Center) を使用してユーザーを作成またはフェデレーションし、アカウントに IAM ロールを引き受けます。

アイデンティティプロバイダーとフェデレーションの詳細については、「IAM ユーザーガイド」の「アイデンティティプロバイダーとフェデレーション」を参照してください。IAM Identity Center の詳細については、AWS IAM Identity Center ユーザーガイドを参照してください。

IAM ユーザーを使用する必要がある場合は、Security Hub では、強力なユーザーパスワードの作成を強制することを推奨します。でパスワードポリシーを設定 AWS アカウント して、パスワードの複雑さの要件と必須のローテーション期間を指定できます。パスワードポリシーを作成または変更する場合、パスワードポリシーの設定の多くは、ユーザーが次回パスワードを変更するときに適用されます。ただし、一部の設定は即座に適用されます。

修正

パスワードポリシーの更新については、「IAM ユーザーガイド」の「IAM ユーザーのアカウントパスワードポリシーの設定」を参照してください。

[IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります

関連する要件： CIS AWS Foundations Benchmark v1.2.0/1.3、NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-2(3)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6、NIST.800-171.r2 3.1.2、PCI DSS v3.2.1/8.1.4、PCI DSS v4.0.1/8.2.

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::IAM::User`

AWS Config ルール : `iam-user-unused-credentials-check`

スケジュールタイプ : 定期的

パラメータ :

- `maxCredentialUsageAge`: `90` (カスタマイズ不可)

このコントロールは、IAM ユーザーが 90 日間使用されていないパスワードまたはアクティブなアクセスキーを持っているかどうかをチェックします。

IAM ユーザーは、パスワードやアクセスキーなど、さまざまなタイプの認証情報を使用して AWS リソースにアクセスできます。

Security Hub では、90 日以上使用されていないすべての認証情報を削除または非アクティブ化することを推奨します。不要な認証情報を無効化または削除することにより、侵害または放棄されたアカウントに関連付けられている認証情報が使用される可能性が少なくなります。

> **Note**
>
> AWS Config は、Security Hub を使用するすべてのリージョンで有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。グローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

IAM コンソールでユーザー情報を表示すると、[アクセスキーの有効期間]、[パスワードの有効期間]、[最終アクティビティ] の列が表示されます。これらの列の値のいずれかが 90 日より大きい場合は、それらのユーザーの認証情報を非アクティブにします。

認証情報レポートを使用してユーザーアカウントをモニタリングし、90 日以上アクティビティのないアカウントを特定することもできます。IAM コンソールから認証情報レポートを `.csv` 形式でダウンロードできます。

非アクティブなアカウント、または未使用の認証情報を特定したら、それらを非アクティブ化します。手順については、「IAM ユーザーガイド」の「IAM ユーザーパスワードの作成、変更、削除 (コンソール)」を参照してください。

[IAM.9] ルートユーザーに対して MFA を有効にする必要があります

関連する要件： PCI DSS v3.2.1/8.3.1、PCI DSS v4.0.1/8.4.2、CIS AWS Foundations Benchmark v3.0.0/1.5、CIS AWS Foundations Benchmark v1.4.0/1.5、CIS AWS Foundations Benchmark v1.2.0/1.13、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 IA-2(1)、NIST.800-53.r5 IA-2(IA-22)、NIST.800-5 IA-2

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 非常事態

リソースタイプ : `AWS::::Account`

AWS Config ルール : `root-account-mfa-enabled`

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、 の IAM ルートユーザーが にサインイン AWS アカウント するために多要素認証 (MFA) が有効になっているかどうかを確認します AWS Management Console。アカウントのルートユーザーに対して MFA が有効になっていない場合、コントロールは失敗します。

の IAM ルートユーザーは AWS アカウント 、アカウント内のすべてのサービスとリソースに完全にアクセスできます。MFA が有効になっている場合、 にサインインするには、ユーザーは AWS MFA デバイスからユーザー名、パスワード、および認証コードを入力する必要があります AWS Management Console。MFA はユーザー名とパスワードの上に保護レイヤーを追加します。

このコントロールは、次の場合に`PASSED`検出結果を生成します。

- ルートユーザーの認証情報がアカウントに存在し、ルートユーザーに対して MFA が有効になっています。
- ルートユーザーの認証情報はアカウントに存在しません。

ルートユーザーの認証情報がアカウントに存在し、ルートユーザーに対して MFA が有効になっていない場合、コントロールは`FAILED`検出結果を生成します。

修正

のルートユーザーの MFA を有効にする方法については AWS アカウント、AWS Identity and Access Management 「 ユーザーガイド」の「 の多要素認証 AWS アカウントのルートユーザー」を参照してください。

[IAM.10] IAM ユーザーのパスワードポリシーには強力な設定が必要です

関連する要件： NIST.800-171.r2 3.5.2、NIST.800-171.r2 3.5.7、NIST.800-171.r2 3.5.8、PCI DSS v3.2.1/8.1.4、PCI DSS v3.2.1/8.2.3、PCI DSS v3.2.1/8.2.4、PCI DSS v3.2.1/8.2.5

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::::Account`

AWS Config ルール : `iam-password-policy`

スケジュールタイプ : 定期的

パラメータ: なし

このコントロールは、IAM ユーザーのアカウントパスワードポリシーが次の最低限の PCI DSS 設定を使用しているかどうかをチェックします。

- `RequireUppercaseCharacters` - パスワードには少なくとも 1 つの大文字が必要。(デフォルト = `true`)
- `RequireLowercaseCharacters` - パスワードには少なくとも 1 つの小文字が必要。(デフォルト = `true`)
- `RequireNumbers` - パスワードには少なくとも 1 つの数字が必要。(デフォルト = `true`)
- `MinimumPasswordLength` - パスワードの最小文字数。(デフォルト = 7 以上)
- `PasswordReusePrevention` - パスワードの再利用を許可するまでのパスワードの数。(デフォルト = 4)
- `MaxPasswordAge` – パスワードの有効期限が切れるまでの日数。(デフォルト = 90)

> **Note**
>
> 2025 年 5 月 30 日、Security Hub は PCI DSS v4.0.1 標準からこのコントロールを削除しました。PCI DSS v4.0.1 では、8 文字以上のパスワードが必要です。このコントロールは、異なるパスワード要件を持つ PCI DSS v3.2.1 標準に引き続き適用されます。
> PCI DSS v4.0.1 の要件に照らしてアカウントのパスワードポリシーを評価するには、IAM.7 コントロールを使用できます。このコントロールでは、8 文字以上のパスワードが必要です。また、パスワードの長さやその他のパラメータのカスタム値もサポートしています。IAM.7 コントロールは、Security Hub の PCI DSS v4.0.1 標準の一部です。

修正

推奨される設定を使用するようにパスワードポリシーを更新するには、「IAM ユーザーガイドの「IAM ユーザー用のアカウントパスワードポリシーの設定」を参照してください。

[IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/1.5、NIST.800-171.r2 3.5.7、PCI DSS v4.0.1/8.3.6、PCI DSS v4.0.1/8.6.3

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::::Account`

AWS Config ルール : `iam-password-policy`

スケジュールタイプ : 定期的

パラメータ : なし

パスワードポリシーは、パスワードの複雑さの要件をある程度強制します。IAM パスワードポリシーを使用して、パスワードで異なる文字セットを使用するようにします。

CIS では、パスワードポリシーで少なくとも 1 文字の大文字を要求することを推奨しています。パスワードの複雑さに関するポリシーを設定すると、ブルートフォースのログイン試行に対するアカウントの耐障害性が高まります。

修正

パスワードポリシーの変更については、「IAM ユーザーガイド」の「IAM ユーザーのアカウントパスワードポリシーの設定」を参照してください。[パスワードの強度] で、[ラテンアルファベット (A–Z) の少なくとも 1 つの大文字が必要] を選択します。

[IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/1.6、NIST.800-171.r2 3.5.7、PCI DSS v4.0.1/8.3.6、PCI DSS v4.0.1/8.6.3

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::::Account`

AWS Config ルール : `iam-password-policy`

スケジュールタイプ : 定期的

パラメータ : なし

パスワードポリシーは、パスワードの複雑さの要件をある程度強制します。IAM パスワードポリシーを使用して、パスワードで異なる文字セットを使用するようにします。CIS では、パスワードポリシーで少なくとも 1 文字の小文字を要求することを推奨しています。パスワードの複雑さに関するポリシーを設定すると、ブルートフォースのログイン試行に対するアカウントの耐障害性が高まります。

修正

パスワードポリシーの変更については、「IAM ユーザーガイド」の「IAM ユーザーのアカウントパスワードポリシーの設定」を参照してください。[パスワードの強度] で、[ラテンアルファベット (A–Z) の少なくとも 1 つの小文字が必要] を選択します。

[IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/1.7、NIST.800-171.r2 3.5.7

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::::Account`

AWS Config ルール : `iam-password-policy`

スケジュールタイプ : 定期的

パラメータ : なし

パスワードポリシーは、パスワードの複雑さの要件をある程度強制します。IAM パスワードポリシーを使用して、パスワードで異なる文字セットを使用するようにします。

CIS では、パスワードポリシーで少なくとも 1 文字の記号を要求することを推奨しています。パスワードの複雑さに関するポリシーを設定すると、ブルートフォースのログイン試行に対するアカウントの耐障害性が高まります。

修正

パスワードポリシーの変更については、「IAM ユーザーガイド」の「IAM ユーザーのアカウントパスワードポリシーの設定」を参照してください。[パスワードの強度] で、[少なくとも 1 つの英数字以外の文字が必要] を選択します。

[IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/1.8、NIST.800-171.r2 3.5.7、PCI DSS v4.0.1/8.3.6、PCI DSS v4.0.1/8.6.3

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::::Account`

AWS Config ルール : `iam-password-policy`

スケジュールタイプ : 定期的

パラメータ : なし

パスワードポリシーは、パスワードの複雑さの要件をある程度強制します。IAM パスワードポリシーを使用して、パスワードで異なる文字セットを使用するようにします。

CIS では、パスワードポリシーで少なくとも 1 文字の数字を要求することを推奨しています。パスワードの複雑さに関するポリシーを設定すると、ブルートフォースのログイン試行に対するアカウントの耐障害性が高まります。

修正

パスワードポリシーの変更については、「IAM ユーザーガイド」の「IAM ユーザーのアカウントパスワードポリシーの設定」を参照してください。[パスワードの強度] で、[少なくとも 1 つの数字が必要] を選択します。

[IAM.15] IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認します

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.8、CIS AWS Foundations Benchmark v1.4.0/1.8、CIS AWS Foundations Benchmark v1.2.0/1.9、NIST.800-171.r2 3.5.7

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::::Account`

AWS Config ルール : `iam-password-policy`

スケジュールタイプ : 定期的

パラメータ : なし

パスワードポリシーは、パスワードの複雑さの要件をある程度強制します。IAM パスワードポリシーを使用して、パスワードが指定された長さ以上になるようにします。

CIS では、パスワードポリシーで 14 文字以上の長さを要求することを推奨しています。パスワードの複雑さに関するポリシーを設定すると、ブルートフォースのログイン試行に対するアカウントの耐障害性が高まります。

修正

パスワードポリシーの変更については、「IAM ユーザーガイド」の「IAM ユーザーのアカウントパスワードポリシーの設定」を参照してください。[パスワードの最小文字数] で、**14** またはそれ以上の数字を入力します。

[IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.9、CIS AWS Foundations Benchmark v1.4.0/1.9、CIS AWS Foundations Benchmark v1.2.0/1.10、NIST.800-171.r2 3.5.8、PCI DSS v4.0.1/8.3.7

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 低

リソースタイプ : `AWS::::Account`

AWS Config ルール : `iam-password-policy`

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、記憶するパスワードの数が 24 に設定されているかどうかをチェックします。値が 24 でない場合、コントロールは失敗します。

IAM パスワードポリシーにより、同じユーザーによる特定のパスワードの再使用を防ぐことができます。

CIS では、パスワードポリシーでパスワードの再使用を禁止することを推奨しています。パスワードの再使用を禁止すると、ブルートフォースのログイン試行に対するアカウントの耐障害性が高まります。

修正

パスワードポリシーの変更については、「IAM ユーザーガイド」の「IAM ユーザーのアカウントパスワードポリシーの設定」を参照してください。[パスワードの再利用を禁止] で、**24** と入力します。

[IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します

関連する要件： CIS AWS Foundations Benchmark v1.2.0/1.11、PCI DSS v4.0.1/8.3.9、PCI DSS v4.0.1/8.3.10.1

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 低

リソースタイプ : `AWS::::Account`

AWS Config ルール : `iam-password-policy`

スケジュールタイプ : 定期的

パラメータ : なし

IAM パスワードポリシーでは、指定された日数後にパスワードをローテーションするか、または有効期限切れにすることを要求できます。

CIS では、パスワードポリシーでパスワードを 90 日以内に有効期限切れにすることを推奨しています。パスワードの有効期間を短くすると、ブルートフォースのログイン試行に対するアカウントの耐障害性が高まります。定期的なパスワード変更の要求は、以下のシナリオでも役立ちます。

- パスワードはユーザーが知らない間に、盗まれたり漏洩したりする可能性があります。これは、システムの侵害、ソフトウェアの脆弱性、または内部の脅威によって起こりえます。
- 特定の企業や政府のウェブフィルターまたはプロキシサーバーは、暗号化されている場合でもトラフィックを傍受し記録できます。
- 多くの人々が仕事、E メール、個人用など多くのシステムで同じパスワードを使用しています。
- 侵害されたエンドユーザーのワークステーションに、キーストロークロガーが設置されている可能性があります。

修正

パスワードポリシーの変更については、「IAM ユーザーガイド」の「IAM ユーザーのアカウントパスワードポリシーの設定」を参照してください。[パスワードの有効期間をオンにする] で、**90** またはそれより小さい数字を入力します。

[IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.17、CIS AWS Foundations Benchmark v1.4.0/1.17、CIS AWS Foundations Benchmark v1.2.0/1.20、NIST.800-171.r2 3.1.2、PCI DSS v4.0.1/12.10.3

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 低

リソースタイプ : `AWS::::Account`

AWS Config ルール : `iam-policy-in-use`

スケジュールタイプ : 定期的

パラメータ :

- `policyARN`: `arn:`*`partition`*`:iam::aws:policy/AWSSupportAccess` (カスタマイズ不可)
- `policyUsageType`: ANY (カスタマイズ不可)

AWS は、インシデントの通知と対応、テクニカルサポート、カスタマーサービスに使用できるサポートセンターを提供します。

IAM ロールを作成して、認可済みのユーザーが AWS サポートでインシデントを管理できるようにします。アクセスコントロールの最小権限を実装することで、IAM ロールには、インシデントを管理するためにサポートセンターへのアクセスを許可する適切な IAM ポリシーが必要です サポート。

> **Note**
>
> AWS Config は、Security Hub を使用するすべてのリージョンで有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。グローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記

録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

この問題を修正するには、認可済みのユーザーに サポート インシデントの管理を許可するロールを作成します。

サポート アクセスに使用するロールを作成するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. IAM ナビゲーションペインで [Roles] (ロール) を選択し、続いて [Create role] (ロールの作成) を選択します。
3. [Role type] (ロールタイプ) で、[Another AWS アカウント] を選択します。
4. アカウント ID には、リソースへのアクセスを許可する AWS アカウント の AWS アカウント ID を入力します。

   このロールを引き受けるユーザーまたはグループが同じアカウントに属している場合は、ローカルアカウント番号を入力します。

   > **Note**
   > 指定したアカウントの管理者は、そのアカウントのすべての ユーザーに、このロールを引き受けるアクセス許可を付与できます。そのためには、管理者から `sts:AssumeRole` アクションの許可を付与するユーザーまたはグループにポリシーを添付します。そのポリシーで、リソースはロール ARN である必要があります。

5. [Next: Permissions] (次へ: 許可) を選択します。
6. マネージドポリシー `AWSSupportAccess` を検索します。
7. `AWSSupportAccess` マネージドポリシーのチェックボックスを選択します。
8. [Next: Tags] (次へ: タグ) を選択します。
9. (オプション) ロールにメタデータを追加するには、キーバリューのペアとしてタグをアタッチします。

   IAM でのタグの使用の詳細については、「IAM ユーザーガイド」の「Tagging IAM users and roles」 (IAM ユーザーとロールのタグ付け) を参照してください。

10. [Next: Review] (次へ: レビュー) を選択します。
11. [Role name] (ロール名) に、ロールの名前を入力します。

    ロール名は 内で一意である必要があります AWS アカウント。大文字と小文字は区別されません。
12. (オプション) [Role description] (ロールの説明) に、新しいロールの説明を入力します。
13. ロールを確認し、[Create role] (ロールの作成) を選択します。

[IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります

関連する要件： NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 IA-2(1)、NIST.800-53.r5 IA-2(2)、NIST.800-53.r5 IA-2(6)、NIST.800-53.r5 IA-2(8)、NIST.800-171.r2 3.3.8、NIST.800-171.r2 3.5.3、NIST.800-171.r2 3.5.5.4、NIST.8000-1.r2 IA-

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::IAM::User`

AWS Config ルール : `iam-user-mfa-enabled`

スケジュールタイプ : 定期的

パラメータ: なし

このコントロールは、IAM ユーザーが多要素認証 (MFA) を有効にしているかどうかを確認します。

> **Note**
>
> AWS Config は、Security Hub を使用するすべてのリージョンで有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。グローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

IAM ユーザーに MFA を追加するには、「IAM ユーザーガイド」の「AWSユーザーの MFA デバイスの有効化」を参照してください。

[IAM.20] ルートユーザーの使用を避けます

> **Important**
>
> Security Hub は、2024 年 4 月にこのコントロールを廃止しました。詳細については、「Security Hub CSPM コントロールの変更ログ」を参照してください。

関連する要件： CIS AWS Foundations Benchmark v1.2.0/1.1

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 低

リソースタイプ : `AWS::IAM::User`

AWS Config ルール: `use-of-root-account-test` (カスタム Security Hub ルール)

スケジュールタイプ : 定期的

パラメータ : なし

このコントロール AWS アカウント は、 にルートユーザーの使用に制限があるかどうかをチェックします。このコントロールは、以下のリソースを評価します。

- Amazon Simple Notification Service (Amazon SNS)のトピック
- AWS CloudTrail 証跡
- CloudTrail トレイルに関連するメトリックスフィルター
- フィルターに基づく Amazon CloudWatch アラーム

チェックの結果、以下の記述の 1 つ以上が真であれば `FAILED` と判定されます:

- アカウントには CloudTrail トレイルは存在しません。
- CloudTrail を有効にして、少なくとも 1 つのマルチリージョンの追跡で、読み取りと書き込みの管理イベントを含めた設定をする必要があります
- CloudTrail トレイルは有効になっていますが、CloudWatch Logs ロググループには関連付けられていません。
- Center for Internet Security (CIS) が規定する正確なメトリックフィルターが使用されていません。規定のメトリックフィルターは `'{$.userIdentity.type="Root" &&`

`$.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}'` です。

- メトリックスフィルターに基づく CloudWatch アラームがアカウントに存在しません。
- 関連する SNS トピックに通知を送信するように設定された CloudWatch アラームは、アラーム条件に基づいてトリガーされません。
- SNS トピックが、SNS トピックにメッセージを送信するための制約に準拠していません。
- SNS トピックに 1 人以上のサブスクライバーが存在しません。

チェックの結果、以下の条件の 1 つ以上に当てはまれば、`NO_DATA` コントロールステータスになります:

- マルチリージョンの追跡が別のリージョンに基づいています。Security Hub は、追跡が基づいているリージョンでのみ結果を生成できます。
- マルチリージョンの追跡が別のアカウントに属しています。Security Hub は、追跡を所有するアカウントの結果のみを生成できます。

チェックの結果、以下の条件の 1 つ以上に当てはまれば、`WARNING` コントロールステータスになります:

- 現在のアカウントは、CloudWatch アラームで参照されている SNS トピックを所有していません。
- `ListSubscriptionsByTopic` SNS API を呼び出しても、現在のアカウントは SNS トピックにアクセスできません。

> **Note**
>
> 組織内の多数のアカウントからのイベントを記録するには、組織の証跡を使用することをお勧めします。組織の証跡は、デフォルトではマルチリージョンの証跡であり、 AWS Organizations 管理アカウントまたは CloudTrail 委任管理者アカウントによってのみ管理できます。組織の証跡を使用すると、組織のメンバーアカウントで評価されたコントロールの管理ステータスは NO_DATA になります。メンバーアカウントでは、Security Hub はメンバー所有のリソースの検出結果のみを生成します。組織の証跡に関する検出結果は、リソース所有者のアカウントで生成されます。クロスリージョン集約を使用すると、Security Hub の委任された管理者アカウントでこれらの検出結果を確認できます。

ベストプラクティスは、アカウントおよびサービスの管理タスクを実行するときに必要となる場合のみ、ルートユーザー認証情報を使用することです。IAM ポリシーは直接ユーザーに適用するのではなく、グループとロールに適用します。日常的に使用する管理者を設定する方法については、「IAM ユーザーガイド」の「最初の IAM 管理者のユーザーおよびグループの作成」を参照してください。

修正

この問題を修正するためのステップには、Amazon SNS トピック、CloudTrail 追跡、メトリクスフィルター、およびメトリクスフィルターのアラームの設定が含まれます。

Amazon SNS トピックを作成するには

1. Amazon SNS コンソール (https://console.aws.amazon.com/sns/v3/home) を開きます。
2. すべての CIS アラームを受信する Amazon SNS トピックを作成します。

   トピックに少なくとも 1 人の受信者を作成します。詳細については、「Amazon Simple Notification Service 開発者ガイド」の「Amazon SNS の開始方法」を参照してください。

次に、すべてのリージョンに適用されるアクティブな CloudTrail を設定します。これを行うには、the section called “[CloudTrail.1] CloudTrail を有効にして、少なくとも 1 つのマルチリージョンの追跡で、読み取りと書き込みの管理イベントを含めた設定をする必要があります。” の修正ステップに従います。

CloudTrail 追跡に関連付ける CloudWatch Logs ロググループの名前を書き留めます。そのロググループに対してメトリクスフィルターを作成します。

最後に、メトリクスフィルターとアラームを作成します。

メトリクスフィルターとアラームを作成するには

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. ナビゲーションペインで、[Log groups] (ロググループ) を選択します。
3. 作成した CloudTrail 追跡に関連付けられている CloudWatch Logs ロググループのチェックボックスを選択します。
4. [Actions] (アクション) から、[Create Metric Filter] (メトリクスフィルターの作成) を選択します。
5. [Define pattern] (パターンを定義) で、以下の操作を行います。

a. 次のパターンをコピーして、[Filter Pattern] (フィルターパターン) フィールドに貼り付けます。

```
{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS &&
 $.eventType !="AwsServiceEvent"}
```

b. [Next] (次へ) を選択します。

6. [Assign Metric] (メトリクスの割り当て) で、以下の操作を行います。

   a. [Filter name] (フィルター名) に、メトリクスフィルターの名前を入力します。

   b. [Metric namespace] (メトリクス名前空間) に **`LogMetrics`** と入力します。

      すべての CIS ログメトリクスフィルターに同じ名前空間を使用した場合、すべての CIS Benchmark メトリクスがグループ化されます。

   c. [Metric Name] (メトリクス名) に、メトリクスの名前を入力します。メトリクスの名前を忘れないでください。アラームの作成時にメトリクスを選択する必要があります。

   d. [Metric value] (メトリクス値) に **1** と入力します。

   e. [Next] (次へ) を選択します。

7. [Review and create] (確認して作成) で、新しいメトリクスフィルター用に入力した情報を確認します。その後、[Create metric filter] (メトリクスフィルターの作成) を選択します。

8. ナビゲーションペインで [Log groups] (ロググループ)を選択し、[Metric filters] (メトリクスフィルター) で作成したフィルターを選択します。

9. フィルターのチェックボックスをオンにします。[アラームの作成] を選択します。

10. [Specify metric and conditions] (メトリクスと条件の指定) で、以下の操作を行います。

    a. [Conditions] (条件) の [Threshold] (しきい値) で、[Static] (静的) を選択します。

    b. [Define the alarm condition] (アラーム条件を定義) で、[Greater/Equal] (より大きい/等しい) を選択します。

    c. [Define the threshold value] (しきい値の定義) で、**1** を入力します。

    d. [Next] (次へ) を選択します。

11. [Configure actions] (アクションの設定) で、次の作業を行います。

    a. [Alarm state trigger] (アラーム状態トリガー) で、[In alarm] (アラーム状態) を選択します。

    b. [Select an SNS topic] (SNS トピックの選択) で、[Select an existing SNS topic] (既存の SNS トピックの選択) を選択します。

c. [Send a notification to] (通知の送信先) で、前の手順で作成した SNS トピックの名前を入力します。

d. [Next] (次へ) を選択します。

12. [Add name and description] (名前と説明を追加) に、アラームの [Name] (名前)と [Description] (説明)を **`CIS-1.1-RootAccountUsage`** のように入力します。続いて、[Next] (次へ) を選択します。
13. [Preview and create] (プレビューと作成) で、アラームの設定を確認します。次に [Create alarm] (アラームの作成) を選択します。

[IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません

関連する要件： NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(10)、NIST.800-53.r5 AC-6NIST.800-53.r5 AC-6(3)、NIST.800-171.r2

カテゴリ: 検出 > セキュアなアクセス管理

重要度: 低

リソースタイプ : `AWS::IAM::Policy`

AWS Config ルール : `iam-policy-no-statements-with-full-access`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `excludePermissionBoundaryPolicy`: `True` (カスタマイズ不可)

このコントロールは、作成した IAM アイデンティティベースのポリシーに、ワイルドカード (*) を使用して、任意のサービスに対してすべてのアクションに許可を付与する許可ステートメントがあるかどうかをチェックします。ポリシーステートメントに、`"Effect": "Allow"` と `"Action": "Service:*"` が含まれている場合、コントロールは失敗します。

例えば、ポリシーに次のような記述があると、結果は失敗となります。

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
```

```
  "Effect": "Allow",
  "Action": "ec2:*",
  "Resource": "*"
}
```

`"Effect": "Allow"` と `"NotAction": "service:*"` を使用する場合も、コントロールは失敗します。この場合、 `NotAction`要素は、 で指定されたアクションを除き AWS のサービス、 のすべてのアクションへのアクセスを提供します`NotAction`。

このコントロールは、カスタマー管理 IAM ポリシーにのみ適用されます。 AWSによって管理される IAM ポリシーには適用されません。

アクセス許可を割り当てるときは AWS のサービス、IAM ポリシーで許可された IAM アクションの範囲を設定することが重要です。IAM アクションは、必要なアクションのみに制限する必要があります。これは、最小特権の許可のプロビジョンに役立ちます。ポリシーが許可を必要としない IAM プリンシパルに添付済みの場合、過度に許可されたポリシーは特権エスカレーションにつながる可能性があります。

場合によっては、`DescribeFlowLogs` や `DescribeAvailabilityZones` のような類似のプレフィックスを持つ IAM アクションを許可する必要があります。これらの承認済みのケースでは、共通プレフィクスにサフィックス付きワイルドカードを追加することができます。例えば、`ec2:Describe*`。

プレフィクスが付いた IAM アクションとサフィックス付きワイルドカードを使用する場合、このコントロールは成功します。例えば、ポリシー内の次のステートメントでは、結果が成功になります。

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:Describe*",
  "Resource": "*"
}
```

この方法で関連する IAM アクションをグループ化することで、IAM ポリシーのサイズ制限を超えないようにすることもできます。

> **Note**
>
> AWS Config は、Security Hub を使用するすべてのリージョンで有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。

グローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

この問題を修正するには、IAM ポリシーを更新して、完全な「*」管理者権限を許可しないようにします。IAM ポリシーを編集する方法の詳細は、「IAM ユーザーガイド」の「IAM ポリシーの編集」を参照してください。

[IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.12、CIS AWS Foundations Benchmark v1.4.0/1.12、NIST.800-171.r2 3.1.2

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::IAM::User`

AWS Config ルール: `iam-user-unused-credentials-check`

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、IAM ユーザーが 45 日以上使用されていないパスワードまたはアクティブなアクセスキーを持っていないかどうかをチェックします。これを行うには、 AWS Config ルールの `maxCredentialUsageAge`パラメータが 45 以上であるかどうかをチェックします。

ユーザーは、パスワードやアクセスキーなど、さまざまなタイプの認証情報を使用して AWS リソースにアクセスできます。

CIS では、45 日以上使用されていないすべての認証情報を削除または非アクティブ化することが推奨されています。不要な認証情報を無効化または削除することにより、侵害または放棄されたアカウントに関連付けられている認証情報が使用される可能性が少なくなります。

このコントロールの AWS Config ルールは、4 時間ごとにのみ更新される `GetCredentialReport`および `GenerateCredentialReport` API オペレーションを使用しま

す。IAM ユーザーへの変更がこのコントロールから確認できるようになるまでに、最大 4 時間かかる場合があります。

> **Note**
>
> AWS Config Security Hub を使用するすべてのリージョンで を有効にする必要があります。ただし、グローバルリソースの記録は 1 つのリージョンで有効にすることができます。グローバルリソースを 1 つのリージョンにのみ記録する場合は、グローバルリソースを記録するリージョン以外のすべてのリージョンでこのコントロールを無効にすることができます。

修正

IAM コンソールでユーザー情報を表示すると、[アクセスキーの有効期間]、[パスワードの有効期間]、[最終アクティビティ] の列が表示されます。これらの列の値のいずれかが 45 日より大きい場合は、それらのユーザーの認証情報を非アクティブにします。

認証情報レポートを使用してユーザーアカウントをモニタリングし、45 日以上アクティビティのないアカウントを特定することもできます。IAM コンソールから認証情報レポートを `.csv` 形式でダウンロードできます。

非アクティブなアカウント、または未使用の認証情報を特定したら、それらを非アクティブ化します。手順については、「IAM ユーザーガイド」の「IAM ユーザーパスワードの作成、変更、削除 (コンソール)」を参照してください。

[IAM.23] IAM Access Analyzer アナライザーにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::AccessAnalyzer::Analyzer`

AWS Config rule: `tagged-accessanalyzer-analyzer` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、 AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) によって管理されるアナライザーに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。アナライザーにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、アナライザーにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

アナライザーにタグを追加するには、「AWS IAM Access Analyzer API リファレンス」の「TagResource」を参照してください。

[IAM.24] IAM ロールにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IAM::Role`

AWS Config rule: `tagged-iam-role` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、 AWS Identity and Access Management (IAM) ロールにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。ロールにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ロールにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス

許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

IAM ロールにタグを追加するには、「IAM ユーザーガイド」の「IAM リソースのタグ付け」を参照してください。

[IAM.25] IAM ユーザーにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IAM::User`

AWS Config rule: `tagged-iam-user` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタ	StringList (最大 6 項目)	AWS 要件を満たす 1 ~	`No default value`

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	グキーのリスト。タグキーでは、大文字と小文字が区別されます。		6 個のタグキー。	

このコントロールは、 AWS Identity and Access Management (IAM) ユーザーにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。ユーザーにタグキーがない場合、またはパラメータ requiredTagKeys で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ requiredTagKeys が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ユーザーがキーでタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、のAWS 「リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

IAM ユーザーにタグを追加するには、「IAM ユーザーガイド」の「IAM リソースのタグ付け」を参照してください。

[IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.19

カテゴリ： 識別 > コンプライアンス

重要度: 中

リソースタイプ : `AWS::IAM::ServerCertificate`

AWS Config ルール: `iam-server-certificate-expiration-check`

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、IAM で管理されているアクティブな SSL/TLS サーバー証明書の有効期限が切れているかどうかを確認します。期限切れの SSL/TLS サーバー証明書が削除されない場合、コントロールは失敗します。

でウェブサイトまたはアプリケーションへの HTTPS 接続を有効にするには AWS、SSL/TLS サーバー証明書が必要です。IAM または AWS Certificate Manager (ACM) を使用して、サーバー証明書を保存およびデプロイできます。ACM でサポートされていない で HTTPS 接続をサポートする必要がある場合にのみ、IAM AWS リージョン を証明書マネージャーとして使用します。IAM はプライベートキーを安全に暗号化し、暗号化されたバージョンを IAM SSL 証明書ストレージに保存します。IAM はすべてのリージョンでのサーバー証明書のデプロイをサポートしていますが、 で使用するには外部プロバイダーから証明書を取得する必要があります AWS。ACM 証明書を IAM にアップロードすることはできません。また、IAM コンソールから証明書を管理することはできません。期限切れの SSL/TLS 証明書を削除すると、基盤となるアプリケーションやウェブサイトの信頼性を損うような、無効な証明書が誤ってリソースにデプロイされるといったリスクがなくなります。

修正

IAM からサーバー証明書を削除するには、「IAM ユーザーガイド」の「IAM でのサーバー証明書の管理」を参照してください。

[IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.22

カテゴリ: 保護 > セキュアなアクセス管理 > セキュアな IAM ポリシー

重要度: 中

リソースタイプ: `AWS::IAM::Role`、`AWS::IAM::User`、`AWS::IAM::Group`

AWS Config ルール: [iam-policy-blacklisted-check]

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- "policyArns": "arn:aws:iam::aws:policy/AWSCloudShellFullAccess,arn:aws-cn:iam::aws:policy/AWSCloudShellFullAccess, arn:aws-us-gov:iam::aws:policy/AWSCloudShellFullAccess"

このコントロールは、IAM アイデンティティ (ユーザー、ロール、またはグループ) に AWS 管理ポリシーが`AWSCloudShellFullAccess`アタッチされているかどうかを確認します。IAM ID に `AWSCloudShellFullAccess` ポリシーがアタッチされている場合、コントロールは失敗します。

AWS CloudShell は、 CLI コマンドを実行するのに便利な方法を提供します AWS のサービス。AWS マネージドポリシー`AWSCloudShellFullAccess`は CloudShell へのフルアクセスを提供します。これにより、ユーザーのローカルシステムと CloudShell 環境間のファイルのアップロードおよびダウンロード機能が可能になります。CloudShell 環境内では、ユーザーは sudo アクセス許可を持ち、インターネットにアクセスできます。その結果、このマネージドポリシーを IAM ID にアタッチすることで、ファイル転送ソフトウェアをインストールし、データを CloudShell から外部のインターネットサーバーに移動できます。最小特権の原則に従い、IAM ID に狭いアクセス許可をアタッチすることをお勧めします。

修正

IAM ID から `AWSCloudShellFullAccess` ポリシーをデタッチするには、「IAM ユーザーガイド」の「IAM ID アクセス許可の追加と削除」を参照してください。

[IAM.28] IAM Access Analyzer 外部アクセスアナライザーを有効にする必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/1.20

カテゴリ: 検出 > 検出サービス > 特権使用状況モニタリング monitoring

重要度: 高

リソースタイプ : `AWS::AccessAnalyzer::Analyzer`

AWS Config ルール: `iam-external-access-analyzer-enabled`

スケジュールタイプ : 定期的

パラメータ : なし

このコントロール AWS アカウント は、 で IAM Access Analyzer 外部アクセスアナライザーが有効になっているかどうかを確認します。現在選択されている AWS リージョンで外部アクセスアナライザーが有効になっていない場合、コントロールは失敗します。

IAM Access Analyzer 外部アクセスアナライザーは、外部エンティティと共有されている Amazon Simple Storage Service (Amazon S3) バケットや IAM ロールなどのリソースを識別するのに役立ちます。これは、リソースやデータへの意図しないアクセスを回避するのに役立ちます。IAM Access Analyzer はリージョン別であり、各リージョンで有効にする必要があります。外部プリンシパルと共有されているリソースを識別するために、アクセスアナライザーはロジックベースの推論を使用して AWS 環境内のリソースベースのポリシーを分析します。外部アクセスアナライザーを作成すると、組織全体または個々のアカウントに対してアナライザーを作成して有効にできます。

> **Note**
>
> アカウントが の組織の一部である場合 AWS Organizations、このコントロールでは、組織を信頼ゾーンとして指定し、現在のリージョンの組織に対して有効になっている外部アクセスアナライザーは考慮されません。組織がこのタイプの設定を使用している場合は、 リージョンの組織内の個々のメンバーアカウントに対してこのコントロールを無効にすることを検討してください。

修正

特定のリージョンで外部アクセスアナライザーを有効にする方法については、IAM ユーザーガイドの「IAM Access Analyzer の開始方法」を参照してください。アナライザーは、リソースへのアクセスをモニタリングするリージョンごとに有効にする必要があります。

Amazon Inspector の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon Inspector サービスとリソースを評価します。

これらのコントロールは、一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Inspector.1] Amazon Inspector EC2 スキャンを有効にする必要があります

関連する要件： PCI DSS v4.0.1/11.3.1

カテゴリ: 検出 > 検出サービス

重要度: 高

リソースタイプ : `AWS::::Account`

AWS Config ルール : `inspector-ec2-scan-enabled`

スケジュールタイプ: 定期的

パラメータ : なし

このコントロールは、Amazon Inspector EC2 スキャンが有効になっているかを確認します。スタンドアロンアカウントの場合、アカウントで Amazon Inspector EC2 スキャンが無効になっていると、コントロールは失敗します。マルチアカウント環境では、委任 Amazon Inspector 管理者アカウントとすべてのメンバーアカウントで EC2 スキャンが有効になっていない場合、コントロールは失敗します。

マルチアカウント環境では、コントロールは委任 Amazon Inspector 管理者アカウントでのみ検出結果を生成します。委任管理者のみが、組織内のメンバーアカウントの EC2 スキャン機能を有効または無効にできます。Amazon Inspector メンバーアカウントからは、この設定を変更できません。このコントロールは、委任管理者に Amazon Inspector EC2 スキャンが有効になっていない停止メンバーアカウントがある場合に `FAILED` 検出結果を生成します。`PASSED` 検出結果を受け取るには、委任管理者は Amazon Inspector でこれらの停止されたアカウントの関連付けを解除する必要があります。

Amazon Inspector EC2 スキャンは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスからメタデータを抽出し、このメタデータをセキュリティアドバイザリから収集されたルールと比較して、検出結果を生成します。Amazon Inspector はインスタンスをスキャンして、パッケージの脆弱性とネットワークの到達性の問題がないか調べます。SSM エージェントなしでスキャンできるオペレーティングシステムなど、サポートされているオペレーティングシステムの詳細については、「サポートされているオペレーティングシステム: Amazon EC2 スキャン」を参照してください。

修正

Amazon Inspector EC2 スキャンを有効にするには、「Amazon Inspector ユーザーガイド」の「スキャンのアクティブ化」を参照してください。

[Inspector.2] Amazon Inspector ECR スキャンを有効にする必要があります

関連する要件： PCI DSS v4.0.1/11.3.1

カテゴリ: 検出 > 検出サービス

重要度: 高

リソースタイプ : `AWS::::Account`

AWS Config ルール : `inspector-ecr-scan-enabled`

スケジュールタイプ: 定期的

パラメータ : なし

このコントロールは、Amazon Inspector ECR スキャンが有効になっているかを確認します。スタンドアロンアカウントの場合、アカウントで Amazon Inspector ECR スキャンが無効になっていると、コントロールは失敗します。マルチアカウント環境では、委任 Amazon Inspector 管理者アカウントとすべてのメンバーアカウントで ECR スキャンが有効になっていない場合、コントロールは失敗します。

マルチアカウント環境では、コントロールは委任 Amazon Inspector 管理者アカウントでのみ検出結果を生成します。委任管理者のみが、組織内のメンバーアカウントの ECR スキャン機能を有効または無効にできます。Amazon Inspector メンバーアカウントからは、この設定を変更できません。このコントロールは、委任管理者に Amazon Inspector ECR スキャンが有効になっていない停止メンバーアカウントがある場合に `FAILED` 検出結果を生成します。`PASSED` 検出結果を受け取るには、委任管理者は Amazon Inspector でこれらの停止されたアカウントの関連付けを解除する必要があります。

Amazon Inspector は、Amazon Elastic Container Registry (Amazon ECR) に保存されているコンテナイメージをスキャンしてソフトウェアの脆弱性がないかを調べ、パッケージ 脆弱性の検出結果を生成します。Amazon ECR の Amazon Inspector スキャンをアクティブ化すると、Amazon Inspector をプライベートレジストリの優先スキャンサービスとして設定します。これにより、Amazon ECR が無料で提供する基本的なスキャンが、Amazon Inspector を通じて提供および請求される拡張スキャンに置き換わります。拡張スキャンでは、オペレーティングシステムパッケージとプログラミング言語パッケージの両方をレジストリレベルで脆弱性スキャンできるという利点があります。拡張スキャンを使用して検出された検出結果は、Amazon ECR コンソールで、イメージのレイヤーごとにイメージレベルで確認できます。さらに、 や AWS Security Hub Amazon EventBridge など、基本的なスキャンの検出結果には利用できない他のサービスで、これらの検出結果を確認して操作できます。

修正

Amazon Inspector ECR スキャンを有効にするには、「Amazon Inspector ユーザーガイド」の「スキャンのアクティブ化」を参照してください。

[Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります

関連する要件： PCI DSS v4.0.1/6.2.4、PCI DSS v4.0.1/6.3.1

カテゴリ: 検出 > 検出サービス

重要度: 高

リソースタイプ : `AWS::::Account`

AWS Config ルール : `inspector-lambda-code-scan-enabled`

スケジュールタイプ: 定期的

パラメータ : なし

このコントロールは、Amazon Inspector Lambda コードスキャンが有効になっているかを確認します。スタンドアロンアカウントの場合、アカウントで Amazon Inspector Lambda コードスキャンが無効になっていると、コントロールは失敗します。マルチアカウント環境では、委任 Amazon Inspector 管理者アカウントとすべてのメンバーアカウントで Lambda コードスキャンが有効になっていない場合、コントロールは失敗します。

マルチアカウント環境では、コントロールは委任 Amazon Inspector 管理者アカウントでのみ検出結果を生成します。委任管理者のみが、組織内のメンバーアカウントの Lambda コードスキャン機能を有効または無効にできます。Amazon Inspector メンバーアカウントからは、この設定を変更できません。このコントロールは、委任管理者に Amazon Inspector Lambda コードスキャンが有効になっていない停止メンバーアカウントがある場合に `FAILED` 検出結果を生成します。`PASSED` 検出結果を受け取るには、委任管理者は Amazon Inspector でこれらの停止されたアカウントの関連付けを解除する必要があります。

Amazon Inspector Lambda コードスキャンは、 AWS セキュリティのベストプラクティスに基づいて、 AWS Lambda 関数内のカスタムアプリケーションコードをスキャンして、コードの脆弱性がないか調べます。Lambda コードスキャンでは、コード内のインジェクションの欠陥、データ漏洩、脆弱な暗号化、または暗号化の欠落を検出できます。この機能は、特定の AWS リージョン でのみ使用できます。Lambda コードスキャンを Lambda 標準スキャンと同時にアクティブ化できます ([Inspector.4] Amazon Inspector Lambda 標準スキャンを有効にする必要があります を参照)。

修正

Amazon Inspector Lambda コードスキャンを有効にするには、「Amazon Inspector ユーザーガイド」の「スキャンのアクティブ化」を参照してください。

[Inspector.4] Amazon Inspector Lambda 標準スキャンを有効にする必要があります

関連する要件： PCI DSS v4.0.1/6.2.4、PCI DSS v4.0.1/6.3.1

カテゴリ: 検出 > 検出サービス

重要度: 高

リソースタイプ : `AWS::::Account`

AWS Config ルール : `inspector-lambda-standard-scan-enabled`

スケジュールタイプ: 定期的

パラメータ : なし

このコントロールは、Amazon Inspector Lambda 標準スキャンが有効になっているかを確認します。スタンドアロンアカウントの場合、アカウントで Amazon Inspector Lambda 標準スキャンが無効になっていると、コントロールは失敗します。マルチアカウント環境では、委任 Amazon Inspector 管理者アカウントとすべてのメンバーアカウントで Lambda 標準スキャンが有効になっていない場合、コントロールは失敗します。

マルチアカウント環境では、コントロールは委任 Amazon Inspector 管理者アカウントでのみ検出結果を生成します。委任管理者のみが、組織内のメンバーアカウントの Lambda 標準スキャン機能を有効または無効にできます。Amazon Inspector メンバーアカウントからは、この設定を変更できません。このコントロールは、委任管理者に Amazon Inspector Lambda 標準スキャンが有効になっていない停止メンバーアカウントがある場合に `FAILED` 検出結果を生成します。`PASSED` 検出結果を受け取るには、委任管理者は Amazon Inspector でこれらの停止されたアカウントの関連付けを解除する必要があります。

Amazon Inspector Lambda 標準スキャンは、 AWS Lambda 関数コードとレイヤーに追加するアプリケーションパッケージの依存関係内のソフトウェアの脆弱性を特定します。Amazon Inspector が Lambda 関数のアプリケーションパッケージの依存関係に脆弱性を検出すると、Amazon Inspector は詳細な `Package Vulnerability` タイプの検出結果を生成します。Lambda コードスキャンを Lambda 標準スキャンと同時にアクティブ化できます ([Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります を参照)。

修正

Amazon Inspector Lambda 標準スキャンを有効にするには、「Amazon Inspector ユーザーガイド」の「スキャンのアクティブ化」を参照してください。

の Security Hub コントロール AWS IoT

これらの AWS Security Hub コントロールは、 AWS IoT サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoT::SecurityProfile`

AWS Config ルール: `tagged-iot-securityprofile` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、 AWS IoT Device Defender セキュリティプロファイルにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。セキュリティプロファイルにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキー

がない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、セキュリティプロファイルにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS IoT Device Defender セキュリティプロファイルにタグを追加するには、「 AWS IoT デベロッパーガイド」の「 AWS IoT リソースのタグ付け」を参照してください。

[IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoT::MitigationAction`

AWS Config ルール: `tagged-iot-mitigationaction` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、 AWS IoT Core 緩和アクションにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。緩和アクションにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、緩和アクションにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS IoT Core 緩和アクションにタグを追加するには、「 AWS IoT デベロッパーガイド」の「 AWS IoT リソースのタグ付け」を参照してください。

[IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoT::Dimension`

AWS Config ルール: `tagged-iot-dimension` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、 AWS IoT Core ディメンションにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。ディメンションにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ディメンションにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス

許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS IoT Core ディメンションにタグを追加するには、「 AWS IoT デベロッパーガイド」の AWS IoT 「リソースのタグ付け」を参照してください。

[IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoT::Authorizer`

AWS Config ルール: `tagged-iot-authorizer` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタ	StringList (最大 6 項目)	AWS 要件を満たす 1 ~	`No default value`

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	グキーのリスト。タグキーでは、大文字と小文字が区別されます。		6 個のタグキー。	

このコントロールは、 AWS IoT Core オーソライザーにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。オーソライザーにタグキーがない場合、またはパラメータ requiredTagKeys で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ requiredTagKeys が指定されていない場合、コントロールはタグキーの存在のみをチェックし、オーソライザーがキーでタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS IoT Core オーソライザーにタグを追加するには、「 AWS IoT デベロッパーガイド」の「 AWS IoT リソースのタグ付け」を参照してください。

[IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoT::RoleAlias`

AWS Config ルール: `tagged-iot-rolealias` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、 AWS IoT Core ロールエイリアスにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。ロールエイリアスにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ロールエイリアスがキーでタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これ

らの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS IoT Core ロールエイリアスにタグを追加するには、「 AWS IoT デベロッパーガイド」の「 AWS IoT リソースのタグ付け」を参照してください。

[IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoT::Policy`

AWS Config ルール: `tagged-iot-policy` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、 AWS IoT Core ポリシーにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredTagKeys。ポリシーにタグキーがない場合、またはパラメータ requiredTagKeys で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ requiredTagKeys が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ポリシーにキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

AWS IoT Core ポリシーにタグを追加するには、「 デベロッパーガイド」の「 AWS IoT リソースのタグ付け」を参照してください。 AWS IoT

AWS IoT Events の Security Hub コントロール

これらの AWS Security Hub コントロールは、 AWS IoT Events サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoTEvents::Input`

AWS Config ルール : `iotevents-input-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS IoT Events 入力にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。入力にタグキーがない場合、またはパラメータで指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータが指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、入力にキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これ

らの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS IoT Events 入力にタグを追加するには、「 AWS IoT Events デベロッパーガイド」の「 AWS IoT Events リソースのタグ付け」を参照してください。

[IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoTEvents::DetectorModel`

AWS Config ルール : `iotevents-detector-model-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS IoT Events ディテクターモデルにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredKeyTags。ディテクターモデルにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredKeyTags。パラメータ が指定されていない場合、コントロールrequiredKeyTagsはタグキーの存在のみをチェックし、ディテクターモデルにキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS IoT Events ディテクターモデルにタグを追加するには、「 AWS IoT Events デベロッパーガイド」の AWS IoT Events 「リソースのタグ付け」を参照してください。

[IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoTEvents::AlarmModel`

AWS Config ルール : `iotevents-alarm-model-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS IoT Events アラームモデルにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。アラームモデルにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、アラームモデルにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS

Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS IoT Events アラームモデルにタグを追加するには、「 AWS IoT Events デベロッパーガイド」の AWS IoT Events 「リソースのタグ付け」を参照してください。

AWS IoT SiteWise の Security Hub コントロール

これらの AWS Security Hub コントロールは、 AWS IoT SiteWise サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoTSiteWise::AssetModel`

AWS Config ルール : `iotsitewise-asset-model-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS IoT SiteWise アセットモデルにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredKeyTags。アセットモデルにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredKeyTags。パラメータ が指定されていない場合、コントロールrequiredKeyTagsはタグキーの存在のみをチェックし、アセットモデルにキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS IoT SiteWise アセットモデルにタグを追加するには、AWS IoT SiteWise 「 ユーザーガイド」のAWS IoT SiteWise 「リソースのタグ付け」を参照してください。

[IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoTSiteWise::Dashboard`

AWS Config ルール : `iotsitewise-dashboard-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS IoT SiteWise ダッシュボードにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。ダッシュボードにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、ダッシュボードにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS

Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS IoT SiteWise ダッシュボードにタグを追加するには、AWS IoT SiteWise 「 ユーザーガイド」のAWS IoT SiteWise 「リソースのタグ付け」を参照してください。

[IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoTSiteWise::Gateway`

AWS Config ルール : `iotsitewise-gateway-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS IoT SiteWise ゲートウェイにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。ゲートウェイにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、ゲートウェイにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS IoT SiteWise ゲートウェイにタグを追加するには、AWS IoT SiteWise 「 ユーザーガイド」のAWS IoT SiteWise 「リソースのタグ付け」を参照してください。

[IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoTSiteWise::Portal`

AWS Config ルール : `iotsitewise-portal-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS IoT SiteWise ポータルにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。ポータルにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、ポータルにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS IoT SiteWise ポータルにタグを追加するには、AWS IoT SiteWise 「 ユーザーガイド」のAWS IoT SiteWise 「リソースのタグ付け」を参照してください。

[IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoTSiteWise::Project`

AWS Config ルール : `iotsitewise-project-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS IoT SiteWise プロジェクトにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。プロジェクトにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、プロジェクトにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任

のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS IoT SiteWise プロジェクトにタグを追加するには、AWS IoT SiteWise 「 ユーザーガイド」のAWS IoT SiteWise 「リソースのタグ付け」を参照してください。

AWS IoT TwinMaker の Security Hub コントロール

これらの AWS Security Hub コントロールは、 AWS IoT TwinMaker サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoTTwinMaker::SyncJob`

AWS Config ルール : `iottwinmaker-sync-job-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS IoT TwinMaker 同期ジョブにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。同期ジョブにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、同期ジョブにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS IoT TwinMaker 同期ジョブにタグを追加するには、AWS IoT TwinMaker 「 ユーザーガイドTagResource」の「」を参照してください。

[IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoTTwinMaker::Workspace`

AWS Config ルール : `iottwinmaker-workspace-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS IoT TwinMaker ワークスペースにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。ワークスペースにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、ワークスペースにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス

許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS IoT TwinMaker ワークスペースにタグを追加するには、AWS IoT TwinMaker 「 ユーザーガイドTagResource」の「」を参照してください。

[IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoTTwinMaker::Scene`

AWS Config ルール : `iottwinmaker-scene-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタ	StringList (最大 6 項目)	AWS 要件を満たす 1 ~	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	グキーのリスト。タグキーでは、大文字と小文字が区別されます。		6 個のタグキー。	

このコントロールは、 AWS IoT TwinMaker シーンにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredKeyTags。シーンにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredKeyTags。パラメータ が指定されていない場合、コントロールrequiredKeyTagsはタグキーの存在のみをチェックし、シーンにキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS IoT TwinMaker シーンにタグを追加するには、AWS IoT TwinMaker 「 ユーザーガイドTagResource」の「」を参照してください。

[IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoTTwinMaker::Entity`

AWS Config ルール : `iottwinmaker-entity-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS IoT TwinMaker エンティティにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。エンティティにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、エンティティにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これ

らの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS IoT TwinMaker エンティティにタグを追加するには、AWS IoT TwinMaker 「 ユーザーガイドTagResource」の「」を参照してください。

AWS IoT Wireless の Security Hub コントロール

これらの AWS Security Hub コントロールは、 AWS IoT Wireless サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoTWireless::MulticastGroup`

AWS Config ルール : `iotwireless-multicast-group-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS IoT Wireless マルチキャストグループにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。マルチキャストグループにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、マルチキャストグループにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS IoT Wireless マルチキャストグループにタグを追加するには、「 AWS IoT Wireless デベロッパーガイド」の AWS IoT Wireless 「リソースのタグ付け」を参照してください。

[IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoTWireless::ServiceProfile`

AWS Config ルール : `iotwireless-service-profile-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS IoT Wireless サービスプロファイルにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。サービスプロファイルにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、サービスプロファイルにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス

許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS IoT Wireless サービスプロファイルにタグを追加するには、「 AWS IoT Wireless デベロッパーガイド」の AWS IoT Wireless 「リソースのタグ付け」を参照してください。

[IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IoTWireless::FuotaTask`

AWS Config ルール : `iotwireless-fuota-task-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーで	StringList (最大 6 項目)	AWS 要件を満たす 1 ~	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	は、大文字と小文字が区別されます。		6 個のタグキー。	

このコントロールは、 AWS IoT Wireless ファームウェアのover-the-air更新 (FUOTA) タスクに、パラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。FUOTA タスクにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、FUOTA タスクにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS IoT Wireless FUOTA タスクにタグを追加するには、「 AWS IoT Wireless デベロッパーガイド」の「 AWS IoT Wireless リソースのタグ付け」を参照してください。

Amazon IVS の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon Interactive Video Service (IVS) サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[IVS.1] IVS 再生キーペアにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IVS::PlaybackKeyPair`

AWS Config ルール : `ivs-playback-key-pair-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon IVS 再生キーペアにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。再生キーペアにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、再生キーペアにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

IVS 再生キーペアにタグを追加するには、「Amazon IVS Real-Time Streaming API リファレンスTagResource」の「」を参照してください。

[IVS.2] IVS 記録設定にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IVS::RecordingConfiguration`

AWS Config ルール : `ivs-recording configuration-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon IVS 記録設定にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。記録設定にタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、記録設定にキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

IVS 記録設定にタグを追加するには、「Amazon IVS Real-Time Streaming API リファレンスTagResource」の「」を参照してください。

[IVS.3] IVS チャネルにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::IVS::Channel`

AWS Config ルール : `ivs-channel-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon IVS チャネルにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックしますrequiredKeyTags。チャネルにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗しますrequiredKeyTags。パラメータ が指定されていない場合、コントロールrequiredKeyTagsはタグキーの存在のみをチェックし、チャネルにキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあ

るリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

IVS チャネルにタグを追加するには、「Amazon IVS Real-Time Streaming API リファレンスTagResource」の「」を参照してください。

Amazon Keyspaces の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon Keyspaces サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Cassandra::Keyspace`

AWS Config ルール : `cassandra-keyspace-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon Keyspaces キースペースにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。キースペースにタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`はタグキーの存在のみをチェックし、キースペースにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

Amazon Keyspaces キースペースにタグを追加するには、「Amazon Keyspaces デベロッパーガイド」の「キースペースにタグを追加する」を参照してください。

Kinesis の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon Kinesis サービスとリソースを評価します。

これらのコントロールは、一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::Kinesis::Stream`

AWS Config ルール : kinesis-stream-encrypted

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon Kinesis Streams が保管中にサーバー側の暗号化を使用して暗号化されているかどうかをチェックします。Amazon Kinesis Streams が、保管中にサーバー側の暗号化を使用して暗号化されていない場合、このコントロールは失敗します。

サーバー側の暗号化は、 AWS KMS keyを使用してデータを保管中になる前に自動的に暗号化する、Amazon Kinesis Data Streams の機能です。データは、Kinesis ストリームストレージレイヤーに書き込まれる前に暗号化され、ストレージから取得された後で復号されます。これにより、Amazon Kinesis Data Streams サービス内に保管中のデータは暗号化されます。

修正

Kinesis Streams でサーバー側の暗号化を有効にする方法については、「Amazon Kinesis Data Streams デベロッパーガイド」の「サーバー側の暗号化を使用する」を参照してください。

[Kinesis.2] Kinesis ストリームにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Kinesis::Stream`

AWS Configルール: `tagged-kinesis-stream` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon Kinesis データストリームにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。データストリームにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、データストリームにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するよう

に設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Kinesis データストリームにタグを追加するには、「Amazon Kinesis デベロッパーガイド」の「Amazon Kinesis Data Streams でのストリームのタグ付け」を参照してください。

[Kinesis.3] Kinesis ストリームには適切なデータ保持期間が必要です

重要度: 中

リソースタイプ : `AWS::Kinesis::Stream`

AWS Configルール : kinesis-stream-backup-retention-check

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`minimumBackupRetentionPeriod`	データが保持される最小時間数。	String	24 ~ 8760	168

このコントロールは、Amazon Kinesis データストリームのデータ保持期間が指定された時間枠以上であるかどうかをチェックします。データ保持期間が指定された時間枠未満の場合、コントロール

は失敗します。データ保持期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 168 時間を使用します。

Kinesis Data Streams では、データストリームは、データレコードの順序付けられたシーケンスで、リアルタイムで書き込みと読み取りができることが前提となっています。データレコードはシャードに一時的に保存されます。レコードが追加されてからアクセスできなくなるまでの期間は、保持期間と呼ばれます。Kinesis Data Streams は、保持期間が短縮されると、新しい保持期間よりも古いレコードをほぼ即座にアクセス不能にします。たとえば、保持期間を 24 時間から 48 時間に変更すると、23 時間 55 分前にストリームに追加されたレコードは、さらに 24 時間後まで使用できます。

修正

Kinesis Data Streams のバックアップ保持期間を変更するには、「Amazon Kinesis Data Streams デベロッパーガイド」の「データ保持期間の変更」を参照してください。

の Security Hub コントロール AWS KMS

これらの AWS Security Hub コントロールは、 AWS Key Management Service （ AWS KMS) サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください

関連する要件: NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(3)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::IAM::Policy`

AWS Config ルール : iam-customer-policy-blocked-kms-actions

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt` (カスタマイズ不可)

- `excludePermissionBoundaryPolicy`: `True` (カスタマイズ不可)

IAM カスタマー管理ポリシーのデフォルトバージョンで、プリンシパルがすべてのリソースで復 AWS KMS 号アクションを使用できるかどうかをチェックします。ポリシーがすべての KMS キーに対して `kms:Decrypt` または `kms:ReEncryptFrom` のアクションを許可するのに十分にオープンな場合、このコントロールは失敗します。

コントロールはリソース要素の KMS キーのみをチェックし、ポリシーの Condition 要素の条件は考慮しません。このコントロールは、添付済みのカスタマーマネージドポリシーと添付されていないカスタマーマネージドポリシーの両方を評価します。インラインポリシーや AWS 管理ポリシーはチェックされません。

を使用すると AWS KMS、KMS キーを使用できるユーザーを制御し、暗号化されたデータにアクセスできます。IAM ポリシーは、アイデンティティ (ユーザー、グループ、またはロール) がどのリソースに対してどのアクションを実行できるかを定義します。セキュリティのベストプラクティスに従って、 は最小権限を許可することを AWS 推奨しています。つまり、ID に付与するのは `kms:Decrypt` または `kms:ReEncryptFrom` 許可と、タスクの実行に必要なキーのみにする必要があります。そうでない場合、ユーザーはデータに適さないキーを使用する可能性があります。

すべてのキーに対する許可を付与する代わりに、ユーザーが暗号化されたデータにアクセスするために必要な最小限のキーのセットを決定します。次に、ユーザーがそれらのキーのみを使用できるようにするポリシーを設計します。例えば、すべての KMS キーに `kms:Decrypt` 許可を付与しないでください。代わりに、アカウントの特定のリージョン内のキーのみに `kms:Decrypt` を許可します。最小特権のプリンシパルを採用することで、意図しないデータ開示のリスクを減らすことができます。

修正

IAM カスタマー管理ポリシーを変更するには、「IAM ユーザーガイド」の「カスタマー管理ポリシーの編集」を参照してください。`Resource` フィールドのポリシーを編集する際、復号化アクションを許可する特定の 1 つまたは複数キーの Amazon リソースネーム (ARN) を指定します。

[KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください

関連する要件: NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(3)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ:

- `AWS::IAM::Group`
- `AWS::IAM::Role`
- `AWS::IAM::User`

AWS Config ルール : iam-inline-policy-blocked-kms-actions

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt` (カスタマイズ不可)

このコントロールは、IAM ID (ロール、ユーザー、またはグループ) に埋め込まれたインラインポリシーが、すべての AWS KMS KMS キーで復号化アクションと再暗号化アクションを許可しているかどうかをチェックします。ポリシーがすべての KMS キーに対して `kms:Decrypt` または `kms:ReEncryptFrom` のアクションを許可するのに十分にオープンな場合、このコントロールは失敗します。

コントロールはリソース要素の KMS キーのみをチェックし、ポリシーの Condition 要素の条件は考慮しません。

を使用すると AWS KMS、KMS キーを使用できるユーザーを制御し、暗号化されたデータにアクセスできます。IAM ポリシーは、アイデンティティ (ユーザー、グループ、またはロール) がどのリソースに対してどのアクションを実行できるかを定義します。セキュリティのベストプラクティスに従って、 は最小権限を許可することを AWS 推奨しています。つまり、ID には必要な許可のみを、タスクの実行に必要なキーにのみ付与する必要があります。そうでない場合、ユーザーはデータに適さないキーを使用する可能性があります。

すべてのキーに対する許可を付与する代わりに、ユーザーが暗号化されたデータにアクセスするために必要なキーの最小セットを決定します。次に、ユーザーがそれらのキーのみを使用できるようにするポリシーを設計します。例えば、すべての KMS キーに `kms:Decrypt` 許可を付与しないでください。代わりに、アカウントの特定リージョンでの特定のキーにのみ許可を付与してください。最小特権のプリンシパルを採用することで、意図しないデータ開示のリスクを減らすことができます。

修正

IAM インラインポリシーを変更するには、「IAM ユーザーガイド」の「インラインポリシーの編集」を参照してください。`Resource` フィールドのポリシーを編集する際、復号化アクションを許可する特定の 1 つまたは複数キーの Amazon リソースネーム (ARN) を指定します。

[KMS.3] AWS KMS keys を意図せずに削除しないでください

関連する要件: NIST.800-53.r5 SC-12、NIST.800-53.r5 SC-12(2)

カテゴリ: 保護 > データ保護 > データ削除保護

重要度: 非常事態

リソースタイプ : `AWS::KMS::Key`

AWS Config ルール: `kms-cmk-not-scheduled-for-deletion-2` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ : なし

このコントロールは、KMS キーの削除がスケジュール済みかどうかをチェックします。KMS キーの削除がスケジュール済みの場合、コントロールは失敗します。

KMS キーは、一度削除すると復元できません。KMS キーで暗号化されたデータも、KMS キーが削除された場合は永久に回復できません。削除予定の KMS キーで、意味のあるデータが暗号化されている場合、意図的に暗号化消去を実行しない限り、データの復号化または新しい KMS キーでデータの再暗号化を検討してください。

KMS キーの削除がスケジュール済みで、誤ってスケジュールされた場合、削除の取り消し時間を確保するために、強制的に待ち時間が適用されます。デフォルトの待機期間は 30 日間ですが、KMS キーの削除がスケジュールされている場合は 7 日以内に短縮できます。待機期間中、スケジュール済みの削除はキャンセルすることができ、KMS キーは削除されません。

KMS キーの削除の詳細については、「AWS Key Management Service 開発者ガイド」の「KMS キーの削除」を参照してください。

修正

スケジュール済み KMS キーの削除をキャンセルには、「AWS Key Management Service デベロッパーガイド」の「キー削除のスケジュールとキャンセル (コンソール)」内にある「キーの削除をキャンセルするには」を参照してください。

[KMS.4] AWS KMS キーローテーションを有効にする必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/3.6、CIS AWS Foundations Benchmark v1.4.0/3.8、CIS AWS Foundations Benchmark v1.2.0/2.8、NIST.800-53.r5 SC-12、NIST.800-53.r5 SC-12(2)、NIST.800-53.r5 SC-28(3)、PCI DSS v3.2.1/3.6.4、PCI DSS v4.0.1/3.7.4

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::KMS::Key`

AWS Config ルール : cmk-backing-key-rotation-enabled

スケジュールタイプ : 定期的

パラメータ : なし

AWS KMS では、 に保存されているキーマテリアルであり、KMS キーのキー ID AWS KMS に関連付けられているバッキングキーをローテーションできます。バッキングキーは、暗号化や復号化などの暗号化オペレーションを実行するために使用されます。現在、キーの自動ローテーションでは以前のすべてのバッキングキーが保持されるため、暗号化したデータは透過的に復号化できます。

CIS では、KMS キーのローテーションを有効にすることを推奨しています。新しいキーで暗号化されたデータは、漏洩した可能性がある以前のキーではアクセスできないため、暗号化キーをローテーションすることで、漏洩したキーにより起こる可能性のある被害を減らすことができます。

修正

KMS キーローテーションを有効にするには、「AWS Key Management Service デベロッパーガイド」の「自動キーローテーションを有効または無効にする方法」を参照してください。

[KMS.5] KMS キーはパブリックにアクセスしないでください

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 非常事態

リソースタイプ : `AWS::KMS::Key`

AWS Config ルール : kms-key-policy-no-public-access

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロール AWS KMS key は、 がパブリックにアクセス可能かどうかをチェックします。KMS キーがパブリックにアクセス可能な場合、コントロールは失敗します。

最小特権アクセスの実装は、セキュリティリスクおよびエラーの影響や悪意ある行動を減らす上での基礎となります。のキーポリシーで外部アカウントからのアクセス AWS KMS key が許可されている場合、サードパーティーは キーを使用してデータを暗号化および復号化できる場合があります。これにより、 キーを使用する から内部または外部の脅威 AWS のサービス がデータを流出する可能性があります。

> **Note**
>
> このコントロールは、設定で が KMS キーの設定項目 (CI) にキーポリシー AWS Config を記録 AWS KMS key できない場合も、 `FAILED`の結果を返します。 AWS Config が KMS キーの CI にキーポリシーを入力するには、AWS Config ロールに GetKeyPolicy API コールを使用してキーポリシーを読み取るためのアクセス権が必要です。このタイプの`FAILED`検出結果を解決するには、 AWS Config ロールが KMS キーのキーポリシーに読み取りアクセスできないようにするポリシーを確認します。たとえば、以下を確認します。
>
> - KMS キーのキーポリシー。
> - アカウント AWS Organizations に適用される のサービスコントロールポリシー (SCPs) とリソースコントロールポリシー (RCPs)。
> - AWS Config サービスにリンクされた AWS Config ロールを使用していない場合のロールのアクセス許可。
>
> さらに、このコントロールは、ワイルドカード文字または変数を使用するポリシー条件を評価しません。`PASSED` 結果を生成するには、キーポリシーの条件は固定値のみを使用する必要があります。固定値は、ワイルドカード文字やポリシー変数を含まない値です。ポリシー変数の詳細については、「 AWS Identity and Access Management ユーザーガイド」の「変数とタグ」を参照してください。

修正

のキーポリシーの更新については AWS KMS key、「 AWS Key Management Service デベロッパーガイド」の「 のキーポリシー AWS KMS」を参照してください。

の Security Hub コントロール AWS Lambda

これらの AWS Security Hub コントロールは、 AWS Lambda サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります

関連する要件： NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)NIST.800-53.r5 SC-7.r5 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7r

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 非常事態

リソースタイプ : `AWS::Lambda::Function`

AWS Config ルール : lambda-function-public-access-prohibited

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Lambda 関数リソースベースポリシーがアカウントの外部からのパブリックアクセスを禁止しているかどうかをチェックします。パブリックアクセスが許可されている場合、コントロールは失敗します。Lambda 関数が Amazon S3 から呼び出され、ポリシーが `AWS:SourceAccount` などパブリックアクセスを制限する条件が含まれていない場合も、コントロールは失敗します。より細かくアクセスするには、バケットポリシーで他の S3 条件を `AWS:SourceAccount` と併用することをおすすめします。

> **Note**
>
> このコントロールは、ワイルドカード文字または変数を使用するポリシー条件を評価しません。`PASSED` 結果を生成するには、Lambda 関数のポリシーの条件は固定値のみを使用す

る必要があります。固定値は、ワイルドカード文字やポリシー変数を含まない値です。ポリシー変数の詳細については、「 AWS Identity and Access Management ユーザーガイド」の「変数とタグ」を参照してください。

Lambda 関数は、関数コードへの意図しないアクセスを許可する可能性があるため、パブリックからアクセスできない必要があります。

修正

この問題を修正するには、関数のリソースベースのポリシーを更新して許可を削除するか、`AWS:SourceAccount` 条件を追加します。リソースベースのポリシーは、Lambda API またはからのみ更新できます AWS CLI。

まず、Lambda コンソールでリソースベースのポリシーを確認します。`"*"` や `{ "AWS": "*" }` など、ポリシーをパブリックにする `Principal` フィールド値を持つポリシーステートメントを特定します。

ポリシーはコンソールから編集できません。関数から許可を削除するには、 AWS CLIから remove-permission コマンドを作動します。

```
$ aws lambda remove-permission --function-name <function-name> --statement-
id <statement-id>
```

`<function-name>` を Lambda 関数の名前で置き換え、*`<statement-id>`* を削除するステートメントのステートメント ID (`Sid`) に置き換えます。

[Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります

関連する要件： NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、PCI DSS v4.0.1/12.3.4

カテゴリ: 保護 > セキュアな開発

重要度: 中

リソースタイプ : `AWS::Lambda::Function`

AWS Config ルール : lambda-function-settings-check

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `runtime`: `dotnet8, java21, java17, java11, java8.al2, nodejs22.x, nodejs20.x, nodejs18.x, python3.13, python3.12, python3.11, python3.10, python3.9, ruby3.4, ruby3.3, ruby3.2` (カスタマイズ不可)

このコントロールは、 AWS Lambda 関数のランタイム設定が、各言語でサポートされているランタイムに設定された想定値と一致するかどうかをチェックします。Lambda 関数がサポートされているランタイムを使用しない場合、「パラメータ」セクションに記載されているように、コントロールは失敗します。Security Hub は、パッケージタイプが `Image` の関数を無視します。

Lambda ランタイムは、メンテナンスとセキュリティの更新の対象となる OS、プログラミング言語、およびソフトウェアライブラリの組み合わせを中心に構築されています。ランタイムコンポーネントがセキュリティアップデートでサポート対象外となった場合、Lambda はこのランタイムを非推奨にします。非推奨のランタイムを使用する関数を作成することはできませんが、この関数は呼び出しイベントのプロセスに使用できます。Lambda 関数が最新であり、非推奨のランタイム環境の使用は避けることをお勧めします。サポートされているランタイム識別子のリストについては、「AWS Lambda デベロッパーガイド」の「Lambda ランタイム」を参照してください。

修正

サポートされているランタイムおよび非推奨スケジュールの詳細については、「AWS Lambda デベロッパーガイド」の「ランタイムの非推奨化に関するポリシー」を参照してください。ランタイムを最新バージョンに移行するときは、言語の発行元からの構文とガイダンスに従ってください。ランタイムバージョンの非互換性というまれな状況で、ワークロードに影響が及ぶリスクを軽減するために、ランタイム更新を適用することをお勧めします。

[Lambda.3] Lambda 関数は VPC 内に存在する必要があります

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 低

リソースタイプ : `AWS::Lambda::Function`

AWS Config ルール: lambda-inside-vpc

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Lambda 関数が 仮想プライベートクラウド (VPC) にデプロイされているかどうかをチェックします。Lambda 関数が VPC にデプロイされていない場合、コントロールは失敗します。Security Hub は、パブリック到達可能性を判断するための VPC サブネットルーティング設定は評価しません。Lambda@Edge リソースに関する失敗の結果が表示される場合があります。

VPC にリソースをデプロイすると、ネットワーク設定のセキュリティとコントロールが強化されます。このようなデプロイでは、複数のアベイラビリティーゾーンにわたってスケーラビリティと高い耐障害性も提供されます。VPC デプロイをカスタマイズして、さまざまなアプリケーション要件を満たすことができます。

修正

VPC のプライベートサブネットに接続する既存の機能を設定するには、「AWS Lambda デベロッパーガイド」の「VPC アクセスの設定」を参照してください。可用性を高めるためにプライベートサブネットを少なくとも 2 つ選択し、機能の接続要件を満たすセキュリティグループを少なくとも 1 つ選択することをお勧めします。

[Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::Lambda::Function`

AWS Config ルール : lambda-vpc-multi-az-check

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`availabilityZones`	アベイラビリティーゾーンの最小数	列挙型	`2, 3, 4, 5, 6`	2

このコントロールは、仮想プライベートクラウド (VPC) に接続する AWS Lambda 関数が、少なくとも指定された数のアベイラビリティーゾーン (AZs) で動作しているかどうかをチェックします。少なくとも指定された数の AZ で関数が動作していない場合、コントロールは失敗します。AZ の最小数に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 2 つの AZ を使用します。

複数の AZs にリソースをデプロイすることは、アーキテクチャ内で高可用性を確保するための AWS ベストプラクティスです。可用性は、機密性、完全性、可用性から成り立つセキュリティモデルの 3 要素における中心的な柱です。VPC に接続するすべての Lambda 関数には、1 つのゾーンで障害が発生しても運用が完全に中断されないように、マルチ AZ 配置がある必要があります。

修正

お客様のアカウントで VPC に接続するように関数を設定する場合は、複数のアベイラビリティーゾーン (AZ) でサブネットを指定することで、高可用性を確保します。手順については、「AWS Lambda デベロッパーガイド」の「VPC アクセスの設定」を参照してください。

Lambda は、複数のアベイラビリティーゾーン (AZ) で他の関数を自動的に実行し、1 つのゾーンでサービスの中断が発生した場合にも、関数をイベントの処理に使用できることを保証します。

[Lambda.6] Lambda 関数にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Lambda::Function`

AWS Config ルール: `tagged-lambda-function` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、 AWS Lambda 関数にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。関数にタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、関数にキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くの がアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「AWS 全般のリファレンス」の「AWS リソースのタグ付け」を参照してください。

修正

Lambda 関数にタグを追加するには、「AWS Lambda デベロッパーガイド」の「Lambda 関数でのタグの使用」を参照してください。

[Lambda.7] Lambda 関数では AWS X-Ray アクティブなトレースを有効にする必要があります

関連する要件: NIST.800-53.r5 CA-7

カテゴリ: 識別 > ログ記録

重要度: 低

リソースタイプ : `AWS::Lambda::Function`

AWS Config ルール : lambda-function-xray-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロール AWS X-Ray は、 関数で を使用したアクティブトレースが有効になっている AWS Lambda かどうかを確認します。Lambda 関数で X-Ray を使用したアクティブトレースが無効になっている場合、コントロールは失敗します。

AWS X-Ray は AWS Lambda 関数のトレースとモニタリング機能を提供し、Lambda 関数のデバッグと運用にかかる時間と労力を節約できます。Lambda 関数のレイテンシーを分割することで、エラーを診断し、パフォーマンスのボトルネック、スローダウン、タイムアウトを特定するのに役立ちます。また、データのプライバシーとコンプライアンスの要件にも役立ちます。Lambda 関数のアクティブトレースを有効にすると、X-Ray は Lambda 関数内のデータフローと処理の全体像を提供し、潜在的なセキュリティ脆弱性や非準拠のデータ処理プラクティスを特定するのに役立ちます。この可視性は、データの整合性、機密性、関連規制への準拠を維持するのに役立ちます。

> **Note**
>
> AWS X-Ray 現在、トレースは、Amazon Managed Streaming for Apache Kafka (Amazon MSK)、セルフマネージド Apache Kafka、ActiveMQ および RabbitMQ を使用する Amazon MQ、または Amazon DocumentDB イベントソースマッピングを使用する Lambda 関数ではサポートされていません。

修正

AWS Lambda 関数のアクティブトレースを有効にする方法については、 AWS Lambda デベロッパーガイドの「 を使用して Lambda 関数の呼び出しを視覚化する AWS X-Ray」を参照してください。

Macie の Security Hub コントロール

これらの AWS Security Hub コントロールは Amazon Macie サービスを評価します。

これらのコントロールは、一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Macie.1] Amazon Macie を有効にする必要があります

関連する要件: NIST.800-53.r5 CA-7、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 RA-5、NIST.800-53.r5 SA-8(19)、NIST.800-53.r5 SI-4

カテゴリ: 検出 > 検出サービス

重要度: 中

リソースタイプ : `AWS::::Account`

AWS Config ルール : `macie-status-check`

スケジュールタイプ: 定期的

このコントロールは、アカウントで Amazon Macie が有効になっているかどうかをチェックします。アカウントに対して Macie が有効になっていない場合、コントロールは失敗します。

Amazon Macie は、機械学習とパターンマッチングを使用して機密データを検出し、データセキュリティリスクを可視化し、それらのリスクに対する自動保護を可能にします。Macie は、Amazon Simple Storage Service (Amazon S3) バケットのセキュリティとアクセスコントロールを自動的かつ継続的に評価し、検出結果を生成して、Amazon S3 データのセキュリティまたはプライバシーに関する潜在的な問題について通知します。また、Macie は、Amazon S3 に保存している個人を特定できる情報 (PII) などの機密データを詳細に把握できるよう、そのようなデータの検出とレポートを自動化します。詳細については、「Amazon Macie ユーザーガイド」を参照してください。

修正

Macie を有効にするには、「Amazon Macie ユーザーガイド」の「Macie を有効化する」を参照してください。

[Macie.2] Macie 機密データ自動検出を有効にする必要があります

関連する要件: NIST.800-53.r5 CA-7、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 RA-5、NIST.800-53.r5 SA-8(19)、NIST.800-53.r5 SI-4

カテゴリ: 検出 > 検出サービス

重要度: 高

リソースタイプ : `AWS::::Account`

AWS Config ルール : `macie-auto-sensitive-data-discovery-check`

スケジュールタイプ: 定期的

このコントロールは、Amazon Macie 管理者アカウントに対して機密データ自動検出が有効になっているかどうかを確認します。Macie 管理者アカウントに対して機密データ自動検出が有効になっていない場合、コントロールは失敗します。このコントロールは管理者アカウントにのみ適用されます。

Macie は、Amazon Simple Storage Service (Amazon S3) バケット内の個人を特定できる情報 (PII) などの機密データの検出と報告を自動化します。機密データ自動検出により、Macie はバケットインベントリを継続的に評価し、サンプリング技術を使用してバケットから代表的な S3 オブジェクトを識別して選択します。その後、Macie は選択したオブジェクトを分析し、機密データがないか検査します。分析が進むにつれて、Macie は S3 データについて提供する統計、インベントリデータ、およびその他の情報を更新します。Macie は検出結果を生成して、検出した機密データを報告します。

修正

S3 バケット内のオブジェクトを分析するための自動機密データ検出ジョブを作成して設定するには、「Amazon Macie ユーザーガイド」の「アカウントの自動機密データ検出の設定」を参照してください。

Amazon MSK の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon Managed Streaming for Apache Kafka (Amazon MSK) サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります

関連する要件： NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、PCI DSS v4.0.1/4.2.1

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::MSK::Cluster`

AWS Config ルール : msk-in-cluster-node-require-tls

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは Amazon MSK クラスターが、クラスターのブローカーノードで HTTPS (TLS) で転送中のデータを暗号化しているかどうかを確認します。クラスターブローカーノード接続でプレーンテキスト通信が有効になっていると、コントロールは失敗します。

HTTPS ではデータの移動に TLS を使用する追加のセキュリティレイヤーが提供されており、これをすると、潜在的な攻撃者が中間者攻撃または同様の攻撃を使用してネットワークトラフィックを盗聴または操作することを防止できます。デフォルトでは、Amazon MSK は転送中のデータを TLS で暗号化します。ただし、このデフォルトはクラスターの作成時に上書きできます。ブローカーノード接続には、HTTPS (TLS) 経由の暗号化接続を使用することをお勧めします。

修正

Amazon MSK クラスターの暗号化設定の更新については、「Amazon Managed Streaming for Apache Kafka デベロッパーガイド」の「クラスターのセキュリティ設定の更新」を参照してください。

[MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります

関連する要件: NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ : `AWS::MSK::Cluster`

AWS Config ルール : msk-enhanced-monitoring-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon MSK クラスターに、少なくとも PER_TOPIC_PER_BROKER のモニタリングレベルで指定された拡張モニタリングが設定されているかどうかをチェックします。クラスターのモニタリングレベルが DEFAULT または PER_BROKER に設定されている場合、コントロールは失敗します。

PER_TOPIC_PER_BROKER モニタリングレベルでは、MSK クラスターのパフォーマンスをより詳細に把握できる他、CPU やメモリ使用量などのリソース使用率に関連するメトリクスも表示されます。これにより、個々のトピックおよびブローカーのパフォーマンスボトルネックやリソース使用パターンを特定できるようになります。この可視性により、Kafka ブローカーのパフォーマンスを最適化できます。

修正

MSK クラスターの拡張モニタリングを設定するには、以下の手順を実行します。

1. https://console.aws.amazon.com/msk/home?region=us-east-1#/home/ で Amazon MSK コンソールを開きます。
2. ナビゲーションペインで [Clusters] (クラスター) を選択してください。次に、クラスターを選択します。
3. [アクション] で [モニタリングを編集] を選択します。
4. [拡張トピックレベルモニタリング] のオプションを選択します。
5. [Save changes] (変更の保存) をクリックします。

モニタリングレベルの詳細については、「Amazon Managed Streaming for Apache Kafka デベロッパーガイド」のCloudWatch で標準ブローカーをモニタリングするための Amazon MSK メトリクス」を参照してください。

[MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります

関連する要件： PCI DSS v4.0.1/4.2.1

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::KafkaConnect::Connector`

AWS Config ルール: `msk-connect-connector-encrypted` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon MSK Connect コネクタが転送中の暗号化されているかどうかを確認します。コネクタが転送中に暗号化されていない場合、このコントロールは失敗します。

転送中のデータとは、クラスター内のノード間やクラスターとアプリケーション間など、ある場所から別の場所に移動するデータを指します。データはインターネット内またはプライベートネットワーク内を移動する場合があります。転送中のデータを暗号化することで、権限のないユーザーがネットワークトラフィックを盗聴するリスクが軽減されます。

修正

MSK Connect コネクタを作成するときに、転送中の暗号化を有効にすることができます。コネクタを作成した後で暗号化設定を変更することはできません。詳細については、「Amazon Managed Streaming for Apache Kafka デベロッパーガイド」の「コネクタの作成」を参照してください。

[MSK.4] MSK クラスターではパブリックアクセスを無効にする必要があります

カテゴリ: 保護 > セキュアなアクセス管理 > パブリックアクセスが不可能なリソース

重要度: 非常事態

リソースタイプ : `AWS::MSK::Cluster`

AWS Config ルール : msk-cluster-public-access-disabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon MSK クラスターでパブリックアクセスが無効になっているかどうかをチェックします。MSK クラスターでパブリックアクセスが有効になっている場合、コントロールは失敗します。

デフォルトでは、クライアントはクラスターと同じ VPC にある場合にのみ Amazon MSK クラスターにアクセスできます。Kafka クライアントと MSK クラスター間のすべての通信はデフォルトでプライベートであり、ストリーミングデータはインターネットを経由しません。ただし、MSK クラ

スターがパブリックアクセスを許可するように設定されている場合、インターネット上の誰でも、クラスター内で実行されている Apache Kafka ブローカーへの接続を確立できます。これにより、不正アクセス、データ侵害、脆弱性の悪用などの問題が発生する可能性があります。認証と認可の手段を要求してクラスターへのアクセスを制限すると、機密情報を保護し、リソースの整合性を維持できます。

修正

Amazon MSK クラスターへのパブリックアクセスの管理については、「Amazon Managed Streaming for Apache Kafka デベロッパーガイド」の「MSK プロビジョンドクラスターへのパブリックアクセスを有効にする」を参照してください。

[MSK.5] MSK コネクタではログ記録が有効になっている必要があります

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::KafkaConnect::Connector`

AWS Config ルール : msk-connect-connector-logging-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon MSK コネクタのログ記録が有効になっているかどうかを確認します。MSK コネクタのログ記録が無効になっていると、コントロールは失敗します。

Amazon MSK コネクタは、データソースから Apache Kafka クラスターにストリーミングデータを継続的にコピーするか、クラスターからデータシンクにデータを継続的にコピーすることで、外部システムと Amazon サービスを Apache Kafka と統合します。MSK Connect は、コネクタのデバッグに役立つログイベントを書き込むことができます。コネクタを作成するときに、Amazon CloudWatch Logs、Amazon S3、Amazon Data Firehose のログ送信先を 0 つ以上指定できます。

> **Note**
>
> プラグインで機密設定値をシークレットとして定義していない場合、機密設定値がコネクタログに表示される可能性があります。Kafka Connect は、未定義の設定値を他のプレーンテキスト値と同じように扱います。

修正

既存の Amazon MSK コネクタのログ記録を有効にするには、適切なログ記録設定でコネクタを再作成する必要があります。設定オプションの詳細については、「Amazon Managed Streaming for Apache Kafka デベロッパーガイド」の「MSK Connect のログ記録」を参照してください。

[MSK.6] MSK クラスターは認証されていないアクセスを無効にする必要があります

カテゴリ: 保護 > セキュアなアクセス管理 > パスワードレス認証

重要度: 中

リソースタイプ : `AWS::MSK::Cluster`

AWS Config ルール : msk-unrestricted-access-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon MSK クラスターで認証されていないアクセスが有効になっているかどうかを確認します。MSK クラスターで認証されていないアクセスが有効になっている場合、コントロールは失敗します。

Amazon MSK は、クラスターへのアクセスを制御するためのクライアント認証および認可メカニズムをサポートしています。これらのメカニズムは、クラスターに接続するクライアントのアイデンティティを検証し、クライアントが実行できるアクションを決定します。MSK クラスターは、認証されていないアクセスを許可するように設定できます。これにより、ネットワーク接続を持つすべてのクライアントは、認証情報を指定せずに Kafka トピックを発行およびサブスクライブできます。認証を必要とせずに MSK クラスターを実行することは、最小特権の原則に違反し、クラスターが不正アクセスにさらされる可能性があります。これにより、すべてのクライアントが Kafka トピックのデータにアクセス、変更、または削除でき、データ侵害、不正なデータ変更、またはサービスの中断につながる可能性があります。適切なアクセスコントロールを確保し、セキュリティコンプライアンスを維持するために、IAM 認証、SASL/SCRAM、相互 TLS などの認証メカニズムを有効にすることをお勧めします。

修正

Amazon MSK クラスターの認証設定を変更する方法については、Amazon Managed Streaming for Apache Kafka デベロッパーガイドの以下のセクションを参照してください。Amazon MSK クラスターのセキュリティ設定の更新と、Apache Kafka APIs の認証と認可。

Amazon MQ の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon MQ サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[MQ.2] ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります

関連する要件： NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-12、NIST.800-53.r5 SI-4、PCI DSS v4.0.1/10.3.3

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::AmazonMQ::Broker`

AWS Config ルール : `mq-cloudwatch-audit-log-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon MQ ActiveMQ ブローカーが監査ログを Amazon CloudWatch Logs にストリーミングするかどうかをチェックします。ブローカーが監査ログを CloudWatch Logs にストリーミングしていない場合、コントロールは失敗します。

ActiveMQ ブローカーログを CloudWatch Logs に発行することで、セキュリティ関連情報の可視性を高める CloudWatch アラームとメトリクスを作成できます。

修正

ActiveMQ ブローカーログを CloudWatch Logs にストリーミングするには、「Amazon MQ デベロッパーガイド」の「Amazon MQ for ActiveMQ ログの設定」を参照してください。

[MQ.3] Amazon MQ ブローカーでは、自動マイナーバージョンアップグレードが有効になっている必要があります

関連する要件： NIST.800-53.r5 CM-3、NIST.800-53.r5 SI-2、PCI DSS v4.0.1/6.3.3

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 低

リソースタイプ : `AWS::AmazonMQ::Broker`

AWS Config ルール : `mq-auto-minor-version-upgrade-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon MQ ブローカーの自動マイナーバージョンアップグレードが有効になっているかどうかを確認します。ブローカーの自動マイナーバージョンアップグレードが有効になっていない場合、コントロールは失敗します。

Amazon MQ が新しいブローカーエンジンバージョンをリリースしてサポートしているため、変更は既存のアプリケーションと下位互換性があり、既存の機能を非推奨にすることはありません。自動ブローカーエンジンバージョン更新は、セキュリティリスクから保護し、バグを修正し、機能を改善します。

> **Note**
>
> 自動マイナーバージョンアップグレードに関連付けられたブローカーが最新のパッチにあり、サポートされない場合は、アップグレードのために手動アクションを実行する必要があります。

修正

MQ ブローカーの自動マイナーバージョンアップグレードを有効にするには、「Amazon MQ デベロッパーガイド」の「マイナーエンジンバージョンの自動アップグレード」を参照してください。

[MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::AmazonMQ::Broker`

AWS Config ルール: `tagged-amazonmq-broker` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、Amazon MQ ブローカーにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。ブローカーにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ブローカーがキーでタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、のAWS 「リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Amazon MQ ブローカーにタグを追加するには、「Amazon MQ デベロッパーガイド」の「リソースのタグ付け」を参照してください。

[MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 低

リソースタイプ : `AWS::AmazonMQ::Broker`

AWS Config ルール : `mq-active-deployment-mode`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon MQ ActiveMQ ブローカーのデプロイモードがアクティブ/スタンバイに設定されているかどうかを確認します。単一インスタンスブローカー (デフォルトで有効) がデプロイモードに設定されている場合、コントロールは失敗します。

アクティブ/スタンバイデプロイにより、 AWS リージョン内の Amazon MQ ActiveMQ ブローカーの可用性が高くなります。アクティブ/スタンバイのデプロイモードには、2 つの異なるアベイラビリティーゾーンの 2 つのブローカーインスタンスが冗長ペアとして設定されています。これらのブローカーはアプリケーションと同期して通信するため、障害発生時のダウンタイムやデータ損失を減らすことができます。

修正

アクティブ/スタンバイデプロイモードで新しい ActiveMQ ブローカーを作成するには、「Amazon MQ デベロッパーガイド」の「ActiveMQ ブローカーの作成と設定」を参照してください。[デプロイモード] で、[アクティブ/スタンバイブローカー] を選択します。既存のブローカーのデプロイモードは変更できません。代わりに、新しいブローカーを作成し、古いブローカーから設定をコピーする必要があります。

[MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 低

リソースタイプ : `AWS::AmazonMQ::Broker`

AWS Config ルール : `mq-rabbit-deployment-mode`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon MQ RabbitMQ ブローカーのデプロイモードがクラスターデプロイに設定されているかどうかを確認します。単一インスタンスブローカー (デフォルトで有効) がデプロイモードに設定されている場合、コントロールは失敗します。

クラスターデプロイにより、 AWS リージョン内の Amazon MQ RabbitMQ ブローカーの可用性が高くなります。クラスターデプロイは、3 つの RabbitMQ ブローカーノードを論理的にグループ化したもので、それぞれに独自の Amazon Elastic Block Store (Amazon EBS) ボリュームと 1 つの共有状態があります。クラスターデプロイは、データがクラスター内の全ノードに確実に複製され、障害発生時のダウンタイムとデータ損失が減少するようにします。

修正

クラスターデプロイモードで新しい RabbitMQ ブローカーを作成するには、「Amazon MQ デベロッパーガイド」の「RabbitMQ ブローカーの作成と接続」を参照してください。[デプロイモード] で、[クラスターデプロイ] を選択します。既存のブローカーのデプロイモードは変更できません。代わりに、新しいブローカーを作成し、古いブローカーから設定をコピーする必要があります。

Neptune の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon Neptune サービスとリソースを評価します。

これらのコントロールは、一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : `neptune-cluster-encrypted`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Neptune DB クラスターが保管中に暗号化されているかどうかをチェックします。Neptune DB クラスターが保管中に暗号化されていない場合、コントロールは失敗します。

保管中のデータとは、永続的な不揮発性ストレージに任意の期間保管されているデータを指します。暗号化は、このようなデータの機密性を保護し、権限のないユーザーがデータにアクセスするリスクを低減するのに役立ちます。Neptune DB クラスターを暗号化することで、データとメタデータを不正アクセスから保護します。また、本番稼働用ファイルシステムにおける保管中のデータの暗号化に関するコンプライアンス要件も満たします。

修正

Neptune DB クラスターを作成するときに、保管中の暗号化を有効にできます。クラスターを作成した後で暗号化設定を変更することはできません。詳細については、「Neptune ユーザーガイド」の「Encrypting Neptune resources at rest」を参照してください。

[Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります

関連する要件： NIST.800-53.r5 AC-2(4)、 NIST.800-53.r5 AC-4(26)、 NIST.800-53.r5 AC-6(9)、 NIST.800-53.r5 AU-10、 NIST.800-53.r5 AU-12、 NIST.800-53.r5 AU-2、 NIST.800-53.r5 AU-3、 NIST.800-53.r5 AU-6(1)、 NIST.800-53.r5 AU-6(3)、 NIST.800-53.r5 AU-6(4)、 NIST.800-53.r5 AU-6(5)、 NIST.800-53.r5 AU-7(1)、 NIST.800-53.r5 AU-9(7)、 NIST.800-53.r5 CA-7、 NIST.800-53.r5 SC-7(9)、 NIST.800-53.r5 SI-20、 NIST.800-53.r5 SI-3(8)、 NIST.800-53.r5 SI-4 (20)、 NIST.800-53.r5 SI-4 (5)、 NIST.800-53.r5 SI-7(8)、 PCI DSS v4.0.1/10.3.3

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : `neptune-cluster-cloudwatch-log-export-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Neptune DB クラスターが監査ログを Amazon CloudWatch Logs に発行しているかどうかをチェックします。Neptune DB クラスターが監査ログを CloudWatch Logs に発行しない場合、コントロールは失敗します。`EnableCloudWatchLogsExport` は `Audit` に設定する必要があります。

Amazon Neptune と Amazon CloudWatch が統合され、パフォーマンスメトリクスを収集して分析できるようになりました。Neptune はメトリクスを自動的に CloudWatch に送信し、CloudWatch アラームもサポートしています。監査ログは高度なカスタマイズが可能です。データベースを監査すると、データに対する各操作をモニタリングし、どのデータベースクラスターがどのようにアクセスされたかに関する情報などを監査証跡に記録できます。Neptune DB クラスターのモニタリングに役立てるため、これらのログを CloudWatch に送信することをお勧めします。

修正

Neptune の監査ログを CloudWatch Logs に発行するには、「Neptune ユーザーガイド」の「Publishing Neptune logs to Amazon CloudWatch Logs」を参照してください。[Log exports] セクションで、[Audit] を選択します。

[Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください

関連する要件： NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-75

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 非常事態

リソースタイプ : `AWS::RDS::DBClusterSnapshot`

AWS Config ルール : `neptune-cluster-snapshot-public-prohibited`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Neptune の手動 DB クラスタースナップショットがパブリックかどうかをチェックします。Neptune の手動 DB クラスタースナップショットがパブリックの場合、コントロールは失敗します。

Neptune DB クラスターの手動スナップショットは、意図しない限りパブリックにしないでください。暗号化されていない手動スナップショットをパブリックとして共有すると、すべての AWS アカウントでこのスナップショットを使用できるようになります。パブリックスナップショットは、意図しないデータ漏えいにつながる可能性があります。

修正

Neptune の手動 DB クラスタースナップショットからパブリックアクセスを削除するには、「Neptune ユーザーガイド」の「Sharing a DB cluster snapshot」を参照してください。

[Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

カテゴリ: 保護 > データ保護 > データ削除保護

重要度: 低

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : `neptune-cluster-deletion-protection-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Neptune DB クラスターの削除保護が有効になっているかどうかをチェックします。Neptune DB クラスターで削除保護が有効になっていない場合、コントロールは失敗します。

クラスターの削除保護を有効にすることで、偶発的なデータベース削除や権限のないユーザーによる削除に対して保護の強化を提供します。削除保護が有効の間、Neptune DB クラスターは削除できません。削除リクエストを成功させるには、まず削除保護を無効にする必要があります。

修正

既存の Neptune DB クラスターの削除保護を有効にするには、「Amazon Aurora ユーザーガイド」の「コンソール、CLI、API を使用した DB クラスターの変更」を参照してください。

[Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります

関連する要件: NIST.800-53.r5 SI-12

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : `neptune-cluster-backup-retention-check`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値	
`minimumBackupRetentionPeriod`	最小バックアップ保持期間 (日数)	整数	7 ~ 35	7	

このコントロールは、Neptune DB クラスターで自動バックアップが有効になっているかどうか、およびバックアップ保持期間が指定された時間枠以上であるかどうかをチェックします。Neptune DB クラスターのバックアップが有効になっていない場合や、保持期間が指定された時間枠未満の場合、コントロールは失敗します。バックアップ保持期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 7 日を使用します。

バックアップは、セキュリティインシデントからの迅速な復元と、システムの耐障害性の強化に役立ちます。Neptune DB クラスターのバックアップを自動化すると、システムを特定の時点に復元し、ダウンタイムとデータ損失を最小限に抑えることができます。

修正

Neptune DB クラスターの自動バックアップを有効にしてバックアップ保持期間を設定するには、「Amazon RDS ユーザーガイド」の「自動バックアップの有効化」を参照してください。[バックアップ保持期間] で 7 以上の値を選択します。

[Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-7(18)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::RDS::DBClusterSnapshot`

AWS Config ルール : `neptune-cluster-snapshot-encrypted`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Neptune DB クラスタースナップショットが保管中に暗号化されているかどうかをチェックします。Neptune DB クラスターが保管中に暗号化されていない場合、コントロールは失敗します。

保管中のデータとは、永続的な不揮発性ストレージに任意の期間保管されているデータを指します。暗号化は、このようなデータの機密性を保護し、権限のないユーザーがデータにアクセスするリスクを低減するのに役立ちます。Neptune DB クラスタースナップショット内のデータは、セキュリティを強化するために、保管中に暗号化する必要があります。

修正

既存の Neptune DB クラスタースナップショットは暗号化できません。代わりに、スナップショットを新しい DB クラスターに復元し、このクラスターで暗号化を有効にする必要があります。これで、

暗号化されたクラスターから、暗号化されたスナップショットを作成できます。手順については、「Neptune ユーザーガイド」の「Restoring from a DB cluster snapshot」と「Creating a DB cluster snapshot in Neptune」を参照してください。

[Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理 > パスワードレス認証

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : `neptune-cluster-iam-database-authentication`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Neptune DB クラスターで IAM データベース認証が有効になっているかどうかをチェックします。Neptune DB クラスターで IAM データベース認証が有効になっていない場合、コントロールは失敗します。

Amazon Neptune データベースクラスターの IAM データベース認証では、認証は IAM を使用して外部で管理されるため、ユーザー認証情報をデータベース設定内に保存する必要がなくなります。IAM データベース認証が有効になっている場合、各リクエストは AWS 署名バージョン 4 を使用して署名する必要があります。

修正

デフォルトでは、Neptune DB クラスターの作成時、IAM データベース認証は無効になっています。有効にするには、「Neptune ユーザーガイド」の「Enabling IAM database authentication in Neptune」を参照してください。

[Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : `neptune-cluster-copy-tags-to-snapshot-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、スナップショットの作成時に、すべてのタグをスナップショットにコピーするように Neptune DB クラスターが設定されているかどうかをチェックします。Neptune DB クラスターがタグをスナップショットにコピーするように設定されていない場合、コントロールは失敗します。

IT アセットの身分証明書とインベントリはガバナンスとセキュリティの重要な側面です。スナップショットは、親 Amazon RDS データベースクラスターと同じ方法でタグ付けする必要があります。タグをコピーすると、DB スナップショットと親データベースクラスターのメタデータが確実に一致し、また、DB スナップショットと親 DB インスタンスのアクセスポリシーが確実に一致するようになります。

修正

Neptune DB クラスターのスナップショットにタグをコピーするには、「Neptune ユーザーガイド」の「Copying tags in Neptune」を参照してください。

[Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : `neptune-cluster-multi-az-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon Neptune DB クラスターで、複数のアベイラビリティーゾーン (AZ) にリードレプリカインスタンスがあるかどうかをチェックします。クラスターが 1 つの AZ にのみデプロイされている場合、コントロールは失敗します。

AZ が使用できなくなった場合や、定期的なメンテナンスイベントでは、リードレプリカがプライマリインスタンスのフェイルオーバーターゲットとして機能します。つまり、プライマリインスタンスが失敗した場合、Neptune はリードレプリカをプライマリインスタンスに昇格します。対照的に、DB クラスターにリードレプリカインスタンスが含まれていない場合、プライマリインスタンスが再作成されるまで障害が発生しても、DB クラスターは使用できないままになります。プライマリインスタンスの再作成は、リードレプリカの昇格よりもかなり時間がかかります。高可用性を確保するために、プライマリインスタンスと同じ DB インスタンスクラスを持ち、プライマリインスタンスとは異なる AZ に配置する 1 つ以上のリードレプリカインスタンスを作成することをお勧めします。

修正

Neptune DB クラスターを複数の AZ にデプロイするには、「Neptune ユーザーガイド」の「Neptune DB クラスター内のリードレプリカ DB インスタンス」を参照してください。

の Security Hub コントロール AWS Network Firewall

これらの AWS Security Hub コントロールは、 AWS Network Firewall サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[NetworkFirewall.1] Network Firewall ファイアウォールを複数のアベイラビリティーゾーンにデプロイする必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::NetworkFirewall::Firewall`

AWS Config ルール : netfw-multi-az-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 で管理されるファイアウォール AWS Network Firewall が複数のアベイラビリティーゾーン (AZs) にデプロイされているかどうかを評価します。ファイアウォールが 1 つの AZ にのみデプロイされている場合、コントロールは失敗します。

AWS グローバルインフラストラクチャには複数の が含まれています AWS リージョン。AZ は、低レイテンシー、高スループット、高冗長性のネットワークで接続されている、各リージョン内の物理的に独立し隔離されたロケーションです。Network Firewall ファイアウォールを複数の AZ にデプロイすることで、AZ 間でトラフィックを分散およびシフトできるため、可用性の高いソリューションを設計できるようになります。

修正

Network Firewall ファイアウォールを複数の AZ にデプロイする

1. Amazon VPC コンソールの https://console.aws.amazon.com/vpc/ を開いてください。
2. ナビゲーションペインで、ネットワークファイアウォールの下にあるファイアウォールを選択します。
3. [ファイアウォール] ページで、編集するファイアウォールを選択します。
4. ファイアウォールの詳細ページで、[ファイアウォールの詳細] タブを選択します。
5. [関連付けられたポリシーと VPC] セクションで、[編集] を選択します。
6. 新しい AZ を追加するには、[新しいサブネットを追加] を選択します。使用する AZ とサブネットを選択します。少なくとも 2 つの AZ を選択するようにします。
7. [保存] を選択します。

[NetworkFirewall.2] Network Firewall ログ記録を有効にする必要があります

関連する要件： NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6AU-6(3)、NIST.800-53.r5 AU-9 CA-7 NIST.800-53.r5 SC-7 SI-3 SI-4 SI-4 SI-7 3.1.20

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::NetworkFirewall::LoggingConfiguration`

AWS Config ルール : netfw-logging-enabled

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、 AWS Network Firewall ファイアウォールでログ記録が有効になっているかどうかをチェックします。少なくとも 1 つのログタイプでログ記録が有効になっていない場合、またはログ記録先が存在しない場合、コントロールは失敗します。

ログ記録はファイアウォールの信頼性、可用性、パフォーマンスの維持に有益です。Network Firewall でログを記録すると、ステートフルエンジンがパケットフローを受信した時間、パケットフローに関する詳細情報、パケットフローに対して実行されたステートフルルールアクションなど、ネットワークトラフィックに関する詳細情報が得られます。

修正

ファイアウォールのログ記録を有効にするには、「AWS Network Firewall 開発者ガイド」の「Updating a firewall's logging configuration」を参照してください。

[Network Firewall.3] Network Firewall ポリシーには、1 つ以上のルールグループが関連付けられている必要があります

関連する要件： NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-171.r2 3.1.3、NIST.800-171.r2 3.13.1

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ : `AWS::NetworkFirewall::FirewallPolicy`

AWS Config ルール : netfw-policy-rule-group-associated

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Network Firewall ポリシーに、ステートフルなルールグループかステートレスなルールグループのいずれかが関連付けられているかどうかをチェックします。ステートレスまたはステートフルなルールグループが割り当てられていない場合、このコントロールは失敗します。

ファイアウォールポリシーは、ファイアウォールが Amazon Virtual Private Cloud (Amazon VPC) のトラフィックをモニタリングおよび処理する方法を定義します。ステートレスおよびステートフルのルールグループの設定は、パケットとトラフィックフローのフィルタリングに役立ち、デフォルトのトラフィック処理を定義します。

修正

Network Firewall ポリシーにルールグループを追加する方法については、「AWS Network Firewall デベロッパーガイド」の「Updating a firewall policy」(ファイアウォールポリシーの更新) を参照してください。ルールグループの作成および管理方法については、「AWS Network Firewallのルールグループ」を参照してください。

[NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、完全なパケットに対してドロップまたは転送される必要があります。

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ : `AWS::NetworkFirewall::FirewallPolicy`

AWS Config ルール : netfw-policy-default-action-full-packets

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `statelessDefaultActions: aws:drop,aws:forward_to_sfe` (カスタマイズ不可)

このコントロールは、Network Firewall ポリシーの完全なパケットに対するデフォルトのステートレスアクションが、ドロップまたは転送かどうかをチェックします。`Drop` または `Forward` が選択されている場合、コントロールはパスします。`Pass` が選択されている場合、このコントロールは失敗します。

ファイアウォールポリシーは、ファイアウォールが Amazon VPC のトラフィックをモニタリングおよび処理する方法を定義します。ステートレスおよびステートフルのルールグループを設定し、パケットとトラフィックフローをフィルタリングします。`Pass` をデフォルトに設定すると、意図しないトラフィックが許可される可能性があります。

修正

ファイアウォール ポリシーを変更する方法については、「AWS Network Firewall デベロッパーガイド」の「ファイアウォールポリシーの更新」 を参照してください。[ステートレスデフォルトアクション] で、[編集] を選択します。続いて、[アクション] として、[ドロップ] または [ステートフルルールグループに転送] を選択します。

[NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、断片化されたパケットに対してドロップまたは転送される必要があります。

関連する要件： NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-171.r2 3.1.3、NIST.800-171.r2 3.1.14、NIST.800-171.r2 3.13.1、NIST.800-171.r2 3.13.6

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ : `AWS::NetworkFirewall::FirewallPolicy`

AWS Config ルール : netfw-policy-default-action-fragment-packets

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe` (カスタマイズ不可)

このコントロールは、Network Firewall ポリシーの断片化されたパケットに対するデフォルトのステートレスアクションが、ドロップまたは転送かどうかをチェックします。`Drop` または `Forward` が選択されている場合、コントロールはパスします。`Pass` が選択されている場合、このコントロールは失敗します。

ファイアウォールポリシーは、ファイアウォールが Amazon VPC のトラフィックをモニタリングおよび処理する方法を定義します。ステートレスおよびステートフルのルールグループを設定し、パケットとトラフィックフローをフィルタリングします。`Pass` をデフォルトに設定すると、意図しないトラフィックが許可される可能性があります。

修正

ファイアウォール ポリシーを変更する方法については、「AWS Network Firewall デベロッパーガイド」の「ファイアウォールポリシーの更新」 を参照してください。[ステートレスデフォルトアク

ション] で、[編集] を選択します。続いて、[アクション] として、[ドロップ] または [ステートフルルールグループに転送] を選択します。

[NetworkFirewall.6] ステートレス Network Firewall のルールグループを空にしないでください

関連する要件： NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(5)、NIST.800-171.r2 3.1.3、NIST.800-171.r2 3.13.1.14、NIST.800-171.r2 3.6

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ : `AWS::NetworkFirewall::RuleGroup`

AWS Config ルール : netfw-stateless-rule-group-not-empty

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 のステートレスルールグループにルール AWS Network Firewall が含まれているかどうかを確認します。ルールグループにルールが含まれない場合、コントロールは失敗します。

ルールグループには、ファイアウォールが VPC 内のトラフィックを処理する方法を定義するルールが含まれています。ファイアウォールポリシーに空のステートレスルールグループが存在する場合、ルールグループがトラフィックを処理するという印象を与える可能性があります。ただし、ステートレスルールグループが空の場合、トラフィックは処理されません。

修正

ネットワークファイアウォールのルールグループにルールを追加するには、「AWS Network Firewall デベロッパーガイド」の「ステートフルルールグループの更新」を参照してください。ファイアウォールの詳細ページの [ステートレスルールグループ] で、[編集] を選択してルールを追加します。

[NetworkFirewall.7] Network Firewall ファイアウォールにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::NetworkFirewall::Firewall`

AWS Config ルール: `tagged-networkfirewall-firewall` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、 AWS Network Firewall ファイアウォールにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。ファイアウォールにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ファイアウォールにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS

Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Network Firewall ファイアウォールにタグを追加するには、「 AWS Network Firewall デベロッパーガイド」の AWS Network Firewall 「リソースのタグ付け」を参照してください。

[NetworkFirewall.8] Network Firewall ファイアウォールポリシーにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::NetworkFirewall::FirewallPolicy`

AWS Config ルール: `tagged-networkfirewall-firewallpolicy` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、 AWS Network Firewall ファイアウォールポリシーにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。ファイアウォールポリシーにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コ

ントロールはタグキーの存在のみをチェックし、ファイアウォールポリシーにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、のAWS 「リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Network Firewall ポリシーにタグを追加するには、「 AWS Network Firewall デベロッパーガイド」の AWS Network Firewall 「リソースのタグ付け」を参照してください。

[NetworkFirewall.9] Network Firewall は削除保護を有効にする必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

カテゴリ: 保護 > ネットワークセキュリティ

重要度: 中

リソースタイプ : `AWS::NetworkFirewall::Firewall`

AWS Config ルール : netfw-deletion-protection-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS Network Firewall ファイアウォールで削除保護が有効になっているかどうかを確認します。ファイアウォールで削除保護が有効になっていないと、コントロールは失敗します。

AWS Network Firewall は、仮想プライベートクラウド (VPCs。削除防止設定は、ファイアウォールが誤って削除されないように保護するものです。

修正

既存の Network Firewall ファイアウォールで削除保護を有効にするには、「AWS Network Firewall デベロッパーガイド」の「ファイアウォールの更新」を参照してください。[変更保護] で [有効化] を選択します。UpdateFirewallDeleteProtection API を呼び出し、`DeleteProtection` フィールドを `true` に設定することで削除保護を有効にすることもできます。

[NetworkFirewall.10] Network Firewall ファイアウォールでは、サブネット変更保護を有効にする必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

カテゴリ: 保護 > ネットワークセキュリティ

重要度: 中

リソースタイプ : `AWS::NetworkFirewall::Firewall`

AWS Config ルール : netfw-subnet-change-protection-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、ファイアウォールでサブネット変更保護が有効になっている AWS Network Firewall かどうかをチェックします。ファイアウォールでサブネット変更保護が有効になっていない場合、コントロールは失敗します。

AWS Network Firewall は、仮想プライベートクラウド (VPCs。Network Firewall ファイアウォールのサブネット変更保護を有効にすると、ファイアウォールのサブネットの関連付けが誤って変更されないようにファイアウォールを保護できます。

修正

既存の Network Firewall ファイアウォールのサブネット変更保護を有効にする方法については、AWS Network Firewall デベロッパーガイドの「ファイアウォールの更新」を参照してください。

Amazon OpenSearch Service の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon OpenSearch Service (OpenSearch Service) サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::OpenSearch::Domain`

AWS Config ルール : `opensearch-encrypted-at-rest`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、OpenSearch ドメインで保管中の暗号化設定が有効になっているかどうかをチェックします。保管中の暗号化が有効になっていない場合、チェックは失敗します。

機密データのセキュリティを強化するには、保管中に暗号化するように OpenSearch Service ドメインを設定する必要があります。保管中のデータの暗号化を設定すると、 は暗号化キー AWS KMS を保存および管理します。暗号化を実行するために、 は 256 ビットキー (AES-256) で Advanced Encryption Standard アルゴリズム AWS KMS を使用します。

保管中の OpenSearch での暗号化の詳細については、Amazon OpenSearch Service デベロッパーガイド」の「Amazon OpenSearch Service の保管中のデータの暗号化」を参照してください。

修正

新規および既存の OpenSearch ドメインの保管時の暗号化を有効にするには、「Amazon OpenSearch Service 開発者ガイド」の「保管中のデータの暗号化の有効化」を参照してください。

[Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > VPC 内のリソース

重要度: 非常事態

リソースタイプ : `AWS::OpenSearch::Domain`

AWS Config ルール : `opensearch-in-vpc-only`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、OpenSearch ドメインが VPC 内にあるかどうかをチェックします。このコントロールは、パブリックアクセスの可能性を判断するための VPC サブネットルーティング設定を評価しません。

OpenSearch ドメインがパブリックサブネットに添付済みではないことを確認する必要があります。「Amazon OpenSearch Service 開発者ガイド」の「リソースベースのポリシー」を参照してください。また、推奨されるベストプラクティスに従って VPC が確実に設定されていることを確認する必要があります。「Amazon VPC ユーザーガイド」の「VPC のセキュリティのベストプラクティス」を参照してください。

VPC 内にデプロイされた OpenSearch ドメインは、パブリックインターネットを経由することなく、プライベート AWS ネットワーク経由で VPC リソースと通信できます。この設定では、転送中のデータへのアクセスを制限することにより、セキュリティ体制が向上します。VPC は、ネットワーク ACL やセキュリティグループを含む、OpenSearch ドメインへのアクセスを安全にするため、多数のネットワークコントロールを提供します。Security Hub では、これらのコントロールを有効に利用するために、パブリック OpenSearch ドメインを VPC に移行することを推奨します。

修正

パブリックエンドポイントを使用してドメインを作成する場合、後で VPC 内にドメインを配置することはできません。代わりに、新規のドメインを作成して、データを移行する必要があります。逆の

場合も同様です。VPC 内にドメインを作成する場合、パブリックエンドポイントを持つことはできません。代わりに、別のドメインを作成するか、このコントロールを無効にする必要があります。

手順については、「Amazon OpenSearch Service デベロッパーガイド」の「VPC 内で Amazon OpenSearch Service ドメインを起動する」を参照してください。

[Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります

関連する要件: NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::OpenSearch::Domain`

AWS Config ルール : `opensearch-node-to-node-encryption-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、OpenSearch ドメインでノード間の暗号化が有効になっているかどうかをチェックします。ドメインでノード間の暗号化が無効になっている場合、このコントロールは失敗します。

HTTPS (TLS) を使用すると、潜在的な攻撃者が中間者攻撃または同様の攻撃を使用してネットワークトラフィックを盗聴または操作することを防止できます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。OpenSearch ドメインでノード間の暗号化を有効にすると、クラスター内通信は転送中に確実に暗号化されます。

この設定には、パフォーマンス上のペナルティが発生する可能性があります。このオプションを有効にする前に、パフォーマンスのトレードオフを認識してテストする必要があります。

修正

OpenSearch ドメインでノード間の暗号化を有効にするには、「Amazon OpenSearch Service デベロッパーガイド」の「ノード間の暗号化を有効にする」を参照してください。

[Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります

関連する要件: NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::OpenSearch::Domain`

AWS Config ルール : `opensearch-logs-to-cloudwatch`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `logtype = 'error'` (カスタマイズ不可)

このコントロールは、OpenSearch ドメインが CloudWatch Logs にエラーログを送信するように設定されているかどうかをチェックします。CloudWatch へのエラーログ記録がドメインに対して有効になっていない場合、このコントロールは失敗します。

OpenSearch ドメインのエラーログを有効にし、それらのログを CloudWatch Logs に送信して保持と応答を行う必要があります。ドメインのエラーログは、セキュリティとアクセス監査や、可用性の問題の診断に役立ちます。

修正

ログ発行を有効にするには、「Amazon OpenSearch Service デベロッパーガイド」の「ログ発行を有効にする (コンソール)」を参照してください。

[Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります

関連する要件： NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53AU-6.r5 CA-7、NIST.800-53.r5 SC-7(7) SI-3 SI-4 SI-710.2.1

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::OpenSearch::Domain`

AWS Config ルール : `opensearch-audit-logging-enabled`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `cloudWatchLogsLogGroupArnList` (カスタマイズ不可) – Security Hub は、このパラメータを設定しません。監査ログ用に設定する必要がある CloudWatch Logs ロググループのカンマ区切りリスト。

このコントロールは、OpenSearch ドメインで監査ログ記録が有効になっているかどうかをチェックします。OpenSearch ドメインで監査ログ記録が有効になっていない場合、このコントロールは失敗します。

監査ログは高度なカスタマイズが可能です。これらを使用することで、認証の成功と失敗、OpenSearch へのリクエスト、インデックスの変更、受信検索クエリなど、OpenSearch クラスターでのユーザーアクティビティを追跡できます。

修正

監査ログを有効にする手順については、「Amazon OpenSearch Service デベロッパーガイド」の「監査ログの有効化」を参照してください。

[Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::OpenSearch::Domain`

AWS Config ルール : `opensearch-data-node-fault-tolerance`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは OpenSearch ドメインが少なくとも 3 つのデータノードが設定されているか、また `zoneAwarenessEnabled` が `true` かどうかをチェックします。OpenSearch ドメインでは、`instanceCount` が 3 より小さいか `zoneAwarenessEnabled` が `false` の場合、このコントロールは失敗します。

クラスターレベルの高可用性と耐障害性を実現するには、OpenSearch ドメインに少なくとも 3 つのデータノードが必要です。少なくとも 3 つのデータノードを持つ OpenSearch ドメインをデプロイすると、ノードに障害が発生した場合のクラスター操作が確実になります。

修正

OpenSearch ドメインのデータノード数を変更するには

1. AWS コンソールにサインインし、https://console.aws.amazon.com/aos/ で Amazon OpenSearch Service コンソールを開きます。
2. [My domains] (ドメイン) で、編集するドメインの名前を選択し、[Edit] (編集) を選択します。
3. [Data nodes] (データノード) で、[Number of nodes] (ノード数) を 3 以上の数値に設定します。3 つのアベイラビリティーゾーンに展開する場合は、アベイラビリティーゾーン間で均等に分配されるように 3 の倍数に設定します。
4. [Submit] を選択してください。

[Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理 > 機密性の高い API オペレーションアクションを制限する

重要度: 高

リソースタイプ : `AWS::OpenSearch::Domain`

AWS Config ルール : `opensearch-access-control-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

OpenSearch ドメインが、きめ細かなアクセスコントロールを有効にしているかどうかをチェックします。きめ細かなアクセスコントロールが有効でない場合、このコントロールは失敗します。OpenSearch パラメータ `update-domain-config` を有効にするには、きめ細かなアクセスコントロールに `advanced-security-options` が必要となります。

きめ細かなアクセスコントロールは、Amazon OpenSearch Service のデータへのアクセスをコントロールする追加の方法を提供します。

修正

きめ細かなアクセスコントロールを有効にする方法については、「Amazon OpenSearch Service デベロッパーガイド」の「Amazon OpenSearch Service のきめ細かなアクセスコントロール」を参照してください。

[Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります

関連する要件: NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::OpenSearch::Domain`

AWS Config ルール : `opensearch-https-required`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `tlsPolicies: Policy-Min-TLS-1-2-PFS-2023-10` (カスタマイズ不可)

このコントロールは、Amazon OpenSearch Service ドメインエンドポイントが最新の TLS セキュリティポリシーを使用するように設定されているかどうかを確認します。OpenSearch ドメインエン

ドポイントが最新のサポートされているポリシーを使用するように設定されていない場合、または HTTPS が有効になっていない場合、コントロールは失敗します。

HTTPS (TLS) を使用すると、潜在的な攻撃者が中間者攻撃または同様の攻撃を使用してネットワークトラフィックを盗聴または操作することを防止できます。HTTPS (TLS) 経由の暗号化された接続のみを許可する必要があります。転送中のデータの暗号化は、パフォーマンスに影響する可能性があります。TLS のパフォーマンスプロファイルと TLS の影響を把握するには、この機能を使用してアプリケーションをテストする必要があります。TLS 1.2 は、以前の TLS バージョンに比べて、いくつかのセキュリティ機能の強化を提供します。

修正

TLS 暗号化を有効にするには、UpdateDomainConfig API オペレーションを使用してください。「DomainEndpointOptions」フィールドを設定して、`TLSSecurityPolicy` の値を指定します。詳細については、「Amazon OpenSearch Service デベロッパーガイド」の「ノード間の暗号化」を参照してください。

[Opensearch.9] OpenSearch ドメインはにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::OpenSearch::Domain`

AWS Config ルール: `tagged-opensearch-domain` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、Amazon OpenSearch Service ドメインにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。ドメインにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ドメインにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

OpenSearch Service ドメインにタグを追加するには、「Amazon OpenSearch Service デベロッパーガイド」の「タグの使用」を参照してください。

[Opensearch.10] OpenSearch ドメインには、最新のソフトウェアアップデートがインストールされている必要があります

関連する要件： NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、PCI DSS v4.0.1/6.3.3

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 低

リソースタイプ : `AWS::OpenSearch::Domain`

AWS Config ルール : `opensearch-update-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon OpenSearch Service ドメインに最新のソフトウェアアップデートがインストールされているかどうかをチェックします。ソフトウェアアップデートが利用可能で、ドメインにインストールされていない場合、コントロールは失敗します。

OpenSearch Service のソフトウェアアップデートは、環境で使用可能な最新のプラットフォーム修正、更新、および機能を提供します。パッチのインストールを最新の状態に保つことは、ドメインのセキュリティと可用性を維持するのに役立ちます。必要なアップデートに関するアクションを実行しない場合、サービスソフトウェアは (通常 2 週間後に) 自動的に更新されます。サービスの中断を最小限に抑えるため、ドメインへのトラフィックが少ない時間帯にアップデートをスケジュールすることをお勧めします。

修正

OpenSearch ドメインのソフトウェアアップデートをインストールするには、「Amazon OpenSearch Service 開発者ガイド」の「更新を開始する」を参照してください。

[Opensearch.11] OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-2、NIST.800-53.r5 SC-5、NIST.800-53.r5 SC-36、NIST.800-53.r5 SI-13

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 低

リソースタイプ : `AWS::OpenSearch::Domain`

AWS Config ルール : `opensearch-primary-node-fault-tolerance`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは Amazon OpenSearch Service ドメインが少なくとも 3 つの専用プライマリノードで設定されているかどうかをチェックします。ドメインの専用プライマリノードが 3 つ未満の場合、コントロールは失敗します。

OpenSearch Service では、クラスターの安定性を向上するために専用プライマリノードを使用します。専用プライマリノードはクラスター管理タスクを実行しますが、データは保持せず、データのアップロードリクエストにも応答しません。スタンバイ付きマルチ AZ を使用することを推奨します。これにより、本番稼働用の各 OpenSearch Service ドメインに 3 つの専用プライマリノードが追加されます。

修正

OpenSearch ドメインのプライマリノードの数を変更するには、「Amazon OpenSearch Service デベロッパーガイド」の「Amazon OpenSearch Service ドメインの作成と管理」を参照してください。

の Security Hub コントロール AWS Private CA

これらの AWS Security Hub コントロールは、 AWS Private Certificate Authority （ AWS Private CA) サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[PCA.1] AWS Private CA ルート認証機関を無効にする必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 低

リソースタイプ : `AWS::ACMPCA::CertificateAuthority`

AWS Config ルール : `acm-pca-root-ca-disabled`

スケジュールタイプ : 定期的

パラメータ : なし

このコントロール AWS Private CA は、 に無効なルート認証機関 (CA) があるかどうかをチェックします。ルート CA が有効になっている場合、コントロールは失敗します。

を使用すると AWS Private CA、ルート CA と下位 CA を含む CAs階層を作成できます。特に本番環境では、日常的なタスクでのルート CA の使用を最小限に抑える必要があります。ルート CA は、中間 CA 認定を交付するためにのみ使用する必要があります。これにより、中間 CA がエンドエンティティ証明書を発行する毎日のタスクを実行しながら、ルート CA を害のない方法で保存することができます。

修正

ルート CA を無効にするには、「AWS Private Certificate Authority ユーザーガイド」の「CA ステータスの更新」を参照してください。

[PCA.2] AWS プライベート CA 認証機関にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::ACMPCA::CertificateAuthority`

AWS Config ルール : `acmpca-certificate-authority-tagged`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS プライベート CA 認証機関にパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredKeyTags`。認証機関にタグキーがない場合、またはパラメータ で指定されたすべてのキーがない場合、コントロールは失敗します`requiredKeyTags`。パラメータ が指定されていない場合、コントロール`requiredKeyTags`は

タグキーの存在のみをチェックし、認証局にキーがタグ付けされていない場合は失敗します。自動的に適用され、aws: で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「ベストプラクティスと戦略」を参照してください。 AWS

修正

AWS プライベート CA 権限にタグを追加するには、AWS Private Certificate Authority 「 ユーザーガイド」の「プライベート CA のタグを追加する」を参照してください。

Amazon RDS の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon Relational Database Service (Amazon RDS) サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[RDS.1] RDS スナップショットはプライベートである必要があります

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5

SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 非常事態

リソースタイプ: `AWS::RDS::DBClusterSnapshot`、`AWS::RDS::DBSnapshot`

AWS Config ルール : `rds-snapshots-public-prohibited`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon RDS スナップショットがパブリックかどうかをチェックします。RDS スナップショットがパブリックである場合、このコントロールは失敗します。このコントロールは、RDS インスタンス、Aurora DB インスタンス、Neptune DB インスタンス、Amazon DocumentDB クラスターを評価します。

RDS スナップショットは、特定の時点で RDS インスタンスのデータをバックアップするために使用されます。これらは、RDS インスタンスを以前の状態に復元するために使用できます。

RDS スナップショットは、意図しない限りパブリックにしないでください。暗号化されていない手動スナップショットをパブリックとして共有すると、このスナップショットをすべての AWS アカウントが使用できるようになります。これにより、RDS インスタンスの意図しないデータ漏えいが発生する可能性があります。

パブリックアクセスを許可するように設定を変更した場合、 AWS Config ルールは最大 12 時間変更を検出できない場合があります。 AWS Config ルールが変更を検出するまで、設定がルールに違反していてもチェックは成功します。

DB スナップショットの共有の詳細については、「Amazon RDS ユーザーガイド」の「DB スナップショットの共有」を参照してください。

修正

RDS スナップショットからパブリックアクセスを削除するには、「Amazon RDS ユーザーガイド」の「スナップショットの共有」を参照してください。[DB スナップショットの可視性] で、[プライベート] を選択します。

[RDS.2] RDS DB インスタンスは、PubliclyAccessible 設定によって判断される、パブリックアクセスを禁止する必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/2.3.3、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7NIST.800-53.r5 SC-7(5)、PCI DSS v3.2.1/1.2.1、PCI v3.2.1。

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 非常事態

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール : `rds-instance-public-access-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、インスタンス設定項目内の `PubliclyAccessible` フィールドを評価して、Amazon RDS インスタンスがパブリックにアクセスできるかどうかをチェックします。

Neptune DB インスタンスと Amazon DocumentDB クラスターには、`PubliclyAccessible` フラグがないため、評価できません。ただし、このコントロールでは、これらのリソースに関する結果を生成できます。これらの結果を抑制できます。

RDS インスタンス設定 の `PubliclyAccessible` 値は、DB インスタンスがパブリックにアクセスできるかどうかを示します。DB インスタンスが `PubliclyAccessible` で設定されている場合、パブリックに解決可能な DNS 名を持つインターネット向けインスタンスであり、パブリック IP アドレスに解決されます。DB インスタンスがパブリックにアクセスできない場合、それはプライベート IP アドレスに解決される DNS 名を持つ内部インスタンスとなります。

RDS インスタンスのパブリックアクセスを可能にする意図がない限り、RDS インスタンスを `PubliclyAccessible` 値に設定しないでください。この設定を行った場合、データベースインスタンスへの不要なトラフィックが許可される可能性があります。

修正

RDS DB インスタンスからパブリックアクセスを削除するには、「Amazon RDS ユーザーガイド」の「Amazon RDS DB インスタンスを変更する」を参照してください。[パブリックアクセス] で [いいえ] を選択します。

[RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。

関連する要件： CIS AWS Foundations Benchmark v3.0.0/2.3.1、CIS AWS Foundations Benchmark v1.4.0/2.3.1、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール : `rds-storage-encrypted`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon RDS DB インスタンスに対してストレージの暗号化が有効になっているかどうかをチェックします。

このコントロールは、RDS DB インスタンスを対象としています。ただし、Aurora DB インスタンス、Neptune DB インスタンス、および Amazon DocumentDB クラスターの結果を生成することもできます。これらの結果が役に立たない場合は、それらを抑制できます。

RDS DB インスタンスの機密データのセキュリティを強化するには、RDS DB インスタンスを保管中に暗号化するように設定する必要があります。保管中の Amazon RDS DB インスタンスとスナップショットを暗号化するには、RDS DB インスタンスの暗号化オプションを有効にします。保管中に暗号化されるデータには、DB インスタンス、自動バックアップ、リードレプリカ、スナップショットの基本的なストレージが含まれます。

RDS の暗号化された DB インスタンスでは、RDS DB インスタンスをホストしているサーバーでデータを暗号化するために、オープン標準の AES-256 暗号化アルゴリズムを使用します。データが暗号化されると、Amazon RDS はパフォーマンスの影響を最小限に抑えながら、データへのアクセスと復号化の認証を透過的に処理します。暗号化を使用するために、データベースのクライアントアプリケーションを変更する必要はありません。

Amazon RDS 暗号化は、現在すべてのデータベースエンジンおよびストレージタイプに使用できます。Amazon RDS 暗号化は、ほとんどの DB インスタンスクラスで使用できます。Amazon RDS 暗

号化をサポートしていない DB インスタンスクラスの詳細については、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースの暗号化」を参照してください。

修正

Amazon RDS での DB インスタンスの暗号化の詳細については、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースの暗号化」を参照してください。

[RDS.4] RDS クラスタースナップショットとデータベーススナップショットは保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::RDS::DBClusterSnapshot`、 `AWS::RDS::DBSnapshot`

AWS Config ルール : `rds-snapshot-encrypted`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、RDS DB スナップショットが暗号化されているかどうかをチェックします。RDS DB スナップショットが暗号化されていない場合、コントロールは失敗します。

このコントロールは、RDS DB インスタンスを対象としています。ただし、Aurora DB インスタンス、Neptune DB インスタンス、および Amazon DocumentDB クラスターのスナップショットに関する結果を生成することもできます。これらの結果が役に立たない場合は、それらを抑制できます。

保管中のデータを暗号化すると、認証されていないユーザーがディスクに保存しているデータにアクセスするリスクが低減されます。RDS スナップショット内のデータは、セキュリティを強化するために、保管中に暗号化する必要があります。

修正

RDS スナップショットを暗号化するには、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースの暗号化」を参照してください。RDS DB インスタンスを暗号化するとき、暗号化された

データにはインスタンスの基盤となるストレージ、自動バックアップ、リードレプリカ、スナップショットが含まれます。

RDS DB インスタンスを暗号化できるのは作成時のみであり、DB インスタンスの作成後には暗号化できません。ただし、暗号化されていないスナップショットのコピーは暗号化できるので、暗号化されていない DB インスタンスに効果的に暗号化を追加できます。つまり、DB インスタンスのスナップショットを作成し、そのスナップショットの暗号化済みコピーを作成します。この暗号化されたスナップショットから DB インスタンスを復元することで、元の DB インスタンスの暗号化されたコピーを作成できます。

[RDS.5] RDS DB インスタンスは、複数のアベイラビリティーゾーンで設定する必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール : `rds-multi-az-support`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、RDS DB インスタンスの高可用性が有効になっているかどうかをチェックします。RDS DB インスタンスが複数のアベイラビリティーゾーン (AZ) で設定されていない場合、コントロールは失敗します。このコントロールは、マルチ AZ DB クラスターデプロイの一部である RDS DB インスタンスには適用されません。

AZ を使用して Amazon RDS DB インスタンスを設定すると、保存されたデータの可用性を確保できます。マルチ AZ 配置では、AZ の可用性に問題が発生した場合や、RDS の定期メンテナンス中に自動フェイルオーバーを実行できます。

修正

DB インスタンスを複数の AZ にデプロイするには、「Amazon RDS ユーザーガイド」の「DB インスタンスをマルチ AZ DB インスタンスのデプロイに変更する」を参照してください。

[RDS.6] RDS DB インスタンスの拡張モニタリングを設定する必要があります

関連する要件: NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール : `rds-enhanced-monitoring-enabled`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値	
`monitoringInterval`	モニタリングメトリクスの収集間隔の秒数	列挙型	`1, 5, 10, 15, 30, 60`	デフォルト値なし	

このコントロールは、Amazon Relational Database Service (Amazon RDS) DB インスタンスに対して拡張モニタリングが有効になっているかどうかをチェックします。インスタンスで拡張モニタリングが有効になっていない場合、コントロールは失敗します。`monitoringInterval` パラメータにカスタム値を指定したときは、指定された間隔でインスタンスの拡張モニタリングメトリクスが収集された場合にのみコントロールが成功します。

Amazon RDS では、拡張モニタリングによって、基盤となるインフラストラクチャのパフォーマンスの変化に対してより迅速にレスポンスできます。これらのパフォーマンスの変化により、データの可用性が低下する可能性があります。拡張モニタリングが有効になっている場合、RDS DB インスタンスが実行される OS のリアルタイムメトリクスを提供します。エージェントがインスタンスにインストールされています。エージェントは、ハイパーバイザーレイヤーから得られるよりも正確にメトリクスを取得できます。

拡張モニタリングのメトリクスは、DB インスタンス上のさまざまなプロセスやスレッドがどのように CPU を使用しているかを表示するときに便利です。詳細については、「Amazon RDS ユーザーガイド」の「拡張モニタリング」を参照してください。

修正

DB インスタンスで拡張モニタリングを有効にする手順の詳細については、「Amazon RDS ユーザーガイド」の「拡張モニタリングの設定と有効化」を参照してください。

[RDS.7] RDS クラスターでは、削除保護が有効になっている必要があります

関連する要件: NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

カテゴリ: 保護 > データ保護 > データ削除保護

重要度: 低

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : `rds-cluster-deletion-protection-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、RDS DB クラスターで削除保護が有効になっているかどうかをチェックします。RDS DB クラスターで削除保護が有効になっていない場合、コントロールは失敗します。

このコントロールは、RDS DB インスタンスを対象としています。ただし、Aurora DB インスタンス、Neptune DB インスタンス、および Amazon DocumentDB クラスターの結果を生成することもできます。これらの結果が役に立たない場合は、それらを抑制できます。

クラスターの削除保護を有効にすることで、偶発的なデータベース削除や不正なエンティティによる削除に対して保護の強化を提供します。

削除保護が有効になっている場合、RDS クラスターは削除できません。削除リクエストが成功するには、削除保護を無効にする必要があります。

修正

RDS DB クラスターの削除保護を有効にするには、「Amazon RDS ユーザーガイド」の「コンソール、CLI、API を使用した DB クラスターの変更」を参照してください。[削除保護] で [削除保護の有効化] を選択します。

[RDS.8] RDS DB インスタンスで、削除保護が有効になっている必要があります

関連する要件: NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: 保護 > データ保護 > データ削除保護

重要度: 低

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール : `rds-instance-deletion-protection-enabled`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `databaseEngines`: `mariadb,mysql,custom-oracle-ee,oracle-ee-cdb,oracle-se2-cdb,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web` (カスタマイズ不可)

このコントロールは、リストされたデータベースエンジンのいずれかを使用する RDS DB インスタンスで削除保護が有効になっているかどうかをチェックします。RDS DB インスタンスで削除保護が有効になっていない場合、コントロールは失敗します。

インスタンス削除保護を有効にすると、偶発的なデータベース削除や不正なエンティティによる削除に対する保護の強化を提供します。

削除保護が有効になっている間は、RDS DB インスタンスを削除できません。削除リクエストが成功するには、削除保護を無効にする必要があります。

修正

RDS DB インスタンスの削除保護を有効にするには、「Amazon RDS ユーザーガイド」の「Amazon RDS DB インスタンスを変更する」を参照してください。[削除保護] で [削除保護の有効化] を選択します。

[RDS.9] RDS DB インスタンスは CloudWatch Logs にログを発行する必要があります

関連する要件： NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53AU-6.r5 CA-7、NIST.800-53.r5 SC-73 NIST.800-53.r5 SC-7 SI-3 SI-4 SI-710.2.1

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール : `rds-logging-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon RDS DB インスタンスが以下のログを Amazon CloudWatch Logs に発行するように設定されているかどうかをチェックします。インスタンスが以下のログを CloudWatch Logs に発行するように設定されていない場合、コントロールは失敗します。

- Oracle: アラート、監査、トレース、リスナー
- PostgreSQL: Postgresql、アップグレード
- MySQL: 監査、エラー、一般、SlowQuery
- MariaDB: 監査、エラー、一般、SlowQuery
- SQL Server: エラー、エージェント
- Aurora: 監査、エラー、一般、SlowQuery
- Aurora-MySQL: 監査、エラー、一般、SlowQuery
- Aurora-PostgreSQL: Postgresql

RDS データベースでは、関連するログを有効にする必要があります。データベースログ記録は、RDS に対して行われたリクエストの詳細な記録を提供します。データベースログは、セキュリティとアクセス監査に役立ち、可用性の問題を診断するのに役立ちます。

修正

RDS データベースログを CloudWatch Logs に発行する方法については、「Amazon RDS ユーザーガイド」のCloudWatch Logs に発行するログの指定」を参照してください。

[RDS.10] IAM 認証は RDS インスタンス用に設定する必要があります

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理 > パスワードレス認証

重要度: 中

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール : `rds-instance-iam-authentication-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、RDS DB インスタンスで IAM データベース認証が有効になっているかどうかをチェックします。RDS DB インスタンスに IAM 認証が設定されていない場合、コントロールは失敗します。このコントロールは、`mysql`、`postgres`、`aurora`、`aurora-mysql`、`aurora-postgresql` および `mariadb` のエンジンタイプの RDS インスタンスのみを評価します。また、RDS インスタンスが結果を生成するには、`available`、`backing-up`、`storage-optimization`、`storage-full` のいずれかの状態になっている必要があります。

IAM データベース認証では、パスワードではなく、認証トークンを使用したデータベースインスタンスへの認証が可能です。データベースに出入りするネットワークトラフィックは、SSL を使用して暗号化されます。詳細については、「Amazon Aurora ユーザーガイド」の「IAM データベース認証」を参照してください。

修正

RDS DB インスタンスで IAM データベース認証を有効にするには、「Amazon RDS ユーザーガイド」の「IAM データベース認証の有効化と無効化」を参照してください。

[RDS.11] RDS インスタンスでは、自動バックアップが有効になっている必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

重要度: 中

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール : `db-instance-backup-enabled`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`backupRetentionMinimum`	最小バックアップ保持期間 (日数)	整数	`7 ~ 35`	`7`
`checkReadReplicas`	リードレプリカに対して RDS DB インスタンスでバックアップが有効になっているかどうかを確認します	ブール値	カスタマイズ不可	`false`

このコントロールは、Amazon Relational Database Service インスタンスで自動バックアップが有効に設定されていて、バックアップ保持期間が指定された時間枠以上であるかどうかをチェックします。リードレプリカは評価から除外されます。インスタンスのバックアップが有効になっていない場合や、保持期間が指定された時間枠未満の場合、コントロールは失敗します。バックアップ保持期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 7 日を使用します。

バックアップは、セキュリティインシデントからより迅速に復元し、システムの耐障害性を強化するのに役立ちます。Amazon RDS により、毎日のフルインスタンスボリュームスナップショットを設定することができます。Amazon RDS の自動バックアップの詳細については、「Amazon RDS ユーザーガイド」の「バックアップの使用」を参照してください。

修正

RDS DB インスタンスの自動バックアップを有効化するには、「Amazon RDS ユーザーガイド」の「自動バックアップの有効化」を参照してください。

[RDS.12] IAM 認証は RDS クラスター用に設定する必要があります

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理 > パスワードレス認証

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : `rds-cluster-iam-authentication-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon RDS DB クラスターで IAM データベース認証が有効になっているかどうかをチェックします。

IAM データベース認証では、データベースインスタンスへパスワードなしの認証が許可されています。認証には、認証トークンが使用されます。データベースに出入りするネットワークトラフィックは、SSL を使用して暗号化されます。詳細については、「Amazon Aurora ユーザーガイド」の「IAM データベース認証」を参照してください。

修正

DB クラスターで IAM 認証を有効にするには、「Amazon Aurora ユーザーガイド」の「IAM データベース認証の有効化と無効化」を参照してください。

[RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/2.3.2、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、PCI DSS v4.0.1/6.3.3

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 高

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール : `rds-automatic-minor-version-upgrade-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、RDS データベースインスタンスでマイナーバージョン自動アップグレードが有効になっているかどうかをチェックします。

自動マイナーバージョンアップグレードは、データベースを最新のデータベースエンジンバージョンに定期的に更新します。ただし、アップグレードに最新のデータベースエンジンのバージョンが含まれているとは限りません。特定の時間に特定のバージョンでデータベースを維持する必要がある場合は、必要なスケジュールに従って必要なデータベースのバージョンに手動でアップグレードすることをお勧めします。重大なセキュリティ問題が発生した場合、またはバージョンがend-of-supportに達すると、自動マイナーバージョンアップグレードオプションを有効にしていない場合でも、Amazon RDS はマイナーバージョンアップグレードを適用することがあります。詳細については、特定のデータベースエンジンの Amazon RDS アップグレードドキュメントを参照してください。

- RDS for MariaDB の自動マイナーバージョンアップグレード
- RDS for MySQL の自動マイナーバージョンアップグレード
- RDS for PostgreSQL の自動マイナーバージョンアップグレード
- Amazon RDS バージョンの Db2
- Oracle マイナーバージョンアップグレード
- Microsoft SQL Server DB エンジンのアップグレード

修正

既存の DB インスタンスの自動マイナーバージョンアップグレードを有効にするには、「Amazon RDS ユーザーガイド」の「Amazon RDS DB インスタンスを変更する」を参照してください。[マイナーバージョン自動アップグレード] で [はい] を選択します。

[RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : `aurora-mysql-backtracking-enabled`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`BacktrackWindowInHours`	Aurora MySQL クラスターをバックトラックする時間数	倍精度	`0.1~72`	デフォルト値なし

このコントロールは、Amazon Aurora クラスターでバックトラックが有効になっているかどうかをチェックします。クラスターでバックトラックが有効になっていない場合、コントロールは失敗します。`BacktrackWindowInHours` パラメータにカスタム値を指定したときは、指定された時間、クラスターがバックトラックされた場合にのみコントロールが成功します。

バックアップは、セキュリティインシデントからより迅速に復元するために役立ちます。また、システムの耐障害性を強化します。Aurora バックトラッキングによって、データベースを特定の時点に復元する時間が短縮されます。復元を実行する場合にデータベースの復元は必要ありません。

修正

Aurora バックトラックを有効にするには、「Amazon Aurora ユーザーガイド」の「バックトラックの設定」を参照してください。

既存のクラスターではバックトラッキングを有効にできないことに注意してください。代わりに、バックトラッキングが有効になっているクローンを作成できます。Aurora でのバックトラック制限の詳細については、「バックトラックの概要」の制限事項の一覧を参照してください。

[RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : `rds-cluster-multi-az-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、RDS DB クラスターで高可用性が有効になっているかどうかをチェックします。RDS DB クラスターが複数のアベイラビリティーゾーン (AZ) にデプロイされていない場合、コントロールは失敗します。

RDS DB クラスターは、保存されたデータの可用性を確保するために、複数の AZ に対して設定する必要があります。複数の AZ にデプロイすると、AZ の可用性に問題が発生した場合や、RDS の定期メンテナンスイベント中に自動フェイルオーバーを実行できます。

修正

DB クラスターを複数の AZ にデプロイするには、「Amazon RDS ユーザーガイド」の「DB インスタンスをマルチ AZ DB インスタンスのデプロイに変更する」を参照してください。

Aurora グローバルデータベースでは、修正の手順が異なります。Aurora グローバルデータベースに複数のアベイラビリティーゾーンを設定するには、DB クラスターを選択します。次に、[アクション] と [リーダーの追加] を選択し、複数の AZ を指定します。詳細については、「Amazon Aurora ユーザーガイド」の「Aurora レプリカを DB クラスターに追加する」を参照してください。

[RDS.16] Aurora DB クラスターは、タグを DB スナップショットにコピーするように設定する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 識別 > インベントリ

重要度: 低

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール: `rds-cluster-copy-tags-to-snapshots-enabled` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ : なし

このコントロールは、スナップショットの作成時に、Amazon Aurora DB クラスターが DB クラスターのスナップショットにタグを自動的にコピーするように設定されているかどうかを確認します。スナップショットの作成時にクラスターのスナップショットにタグを自動的にコピーするように Aurora DB クラスターが設定されていない場合、コントロールは失敗します。

IT アセットの身分証明書とインベントリはガバナンスとセキュリティの重要な側面です。セキュリティ体制を評価し、潜在的な弱点に対処できるように、すべての Amazon Aurora DB クラスターを可視化する必要があります。Aurora DB スナップショットには、親 DB クラスターと同じタグが必要です。Amazon Aurora では、クラスターのすべてのタグをクラスターのスナップショットに自動的にコピーするように DB クラスターを設定できます。この設定を有効にすると、DB スナップショットは親 DB クラスターと同じタグを継承します。

> **Note**
>
> 2025 年 6 月 30 日、Security Hub はこのコントロールのタイトルを変更しました。以前は、このコントロールのタイトルは でしたRDS DB clusters should be configured to copy tags to snapshots。新しいタイトルは、コントロールが Amazon Aurora DB クラスターのみをチェックしていることをより正確に反映しています。

修正

タグを DB スナップショットに自動的にコピーするように Amazon Aurora DB クラスターを設定する方法については、「Amazon Aurora ユーザーガイド」の「Amazon Aurora DB クラスターの変更」を参照してください。

[RDS.17] RDS DB インスタンスは、タグをスナップショットにコピーするように設定する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

カテゴリ: 識別 > インベントリ

重要度: 低

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール: `rds-instance-copy-tags-to-snapshots-enabled` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ: なし

このコントロールは、スナップショットの作成時に、すべてのタグをスナップショットにコピーするように RDS DB インスタンスが構成されているかどうかをチェックします。

IT アセットの身分証明書とインベントリはガバナンスとセキュリティの重要な側面です。すべての RDS DB インスタンスを可視化することで、それらのセキュリティ体制を評価し、潜在的な弱点に対してアクションを起こせるようにする必要があります。スナップショットは、親 RDS データベースインスタンスと同じ方法でタグ付けする必要があります。この設定を有効にすると、スナップショットが親データベースインスタンスのタグを継承します。

修正

RDS DB インスタンスのスナップショットにタグを自動的にコピーするには、「Amazon RDS ユーザーガイド」の「Amazon RDS DB インスタンスを変更する」を参照してください。[タグをスナップショットへコピー] を選択します。

[RDS.18] RDS インスタンスは VPC 内にデプロイする必要があります

カテゴリ: 保護 > セキュアなネットワーク設定 > VPC 内のリソース

重要度: 高

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール: `rds-deployed-in-vpc` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon RDS インスタンスが EC2-VPC にデプロイされているかどうかをチェックします。

VPC は、RDS リソースへのアクセスを保護するための多数のネットワークコントロールを提供します。これらのコントロールには、VPC エンドポイント、ネットワーク ACL、セキュリティグループが含まれます。これらのコントロールを利用するには、EC2-VPC 上に RDS インスタンスを作成することが推奨されます。

修正

RDS インスタンスを VPC に移動する方法については、「Amazon RDS ユーザーガイド」の「DB インスタンスの VPC を更新する」を参照してください。

[RDS.19] 重大なクラスターイベントについて、既存の RDS イベント通知サブスクリプションを設定する必要があります

関連する要件: NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2

カテゴリ: 検出 > 検出サービス > アプリケーションモニタリング

重要度: 低

リソースタイプ : `AWS::RDS::EventSubscription`

AWS Config ルール: `rds-cluster-event-notifications-configured` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ : なし

このコントロールは、データベースクラスターの既存の Amazon RDS イベントサブスクリプションに、次のソースタイプ、イベントカテゴリのキーと値のペアに対して有効な通知があるかどうかをチェックします。

```
DBCluster: ["maintenance","failure"]
```

アカウントに既存のイベントサブスクリプションがない場合、コントロールはパスします。

RDS イベント通知は Amazon SNS を使用して、RDS リソースの可用性または設定の変更を通知します。これらの通知により、迅速な対応が実現します。RDS イベント通知の詳細については、「Amazon RDS ユーザーガイド」の「Amazon RDS イベント通知の使用」を参照してください。

修正

RDS クラスターイベント通知にサブスクライブするには、「アマゾン RDS ユーザーガイド」の「Amazon RDS イベント通知にサブスクライブする」を参照してください。以下の値を使用します。

フィールド	値
ソースタイプ	クラスター
含めるクラスター	すべてのクラスター
含めるイベントカテゴリ	[Specific event categories] (特定のイベントカテゴリ) または [All event categories] (すべてのイベントカテゴリ) を選択します

[RDS.20] 重大なデータベースインスタンスイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります

関連する要件： NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2、PCI DSS v4.0.1/11.5.2

カテゴリ: 検出 > 検出サービス > アプリケーションモニタリング

重要度: 低

リソースタイプ : `AWS::RDS::EventSubscription`

AWS Config ルール: `rds-instance-event-notifications-configured` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ : なし

このコントロールは、データベースインスタンスの既存の Amazon RDS イベントサブスクリプションに、次のソースタイプ、イベントカテゴリのキーと値のペアに対して有効な通知があるかどうかをチェックします。

```
DBInstance: ["maintenance","configuration change","failure"]
```

アカウントに既存のイベントサブスクリプションがない場合、コントロールはパスします。

RDS イベント通知は Amazon SNS を使用して、RDS リソースの可用性または設定の変更をユーザーに知らせます。これらの通知により、迅速な対応が実現します。RDS イベント通知の詳細については、「Amazon RDS ユーザーガイド」の「Amazon RDS イベント通知の使用」を参照してください。

修正

RDS インスタンスイベント通知にサブスクライブするには、「Amazon RDS ユーザーガイド」の「Amazon RDS イベント通知にサブスクライブする」を参照してください。以下の値を使用します。

フィールド	値
ソースタイプ	インスタンス
含めるインスタンス	すべてのインスタンス

フィールド	値
含めるイベントカテゴリ	[Specific event categories] (特定のイベントカテゴリ) または [All event categories] (すべてのイベントカテゴリ) を選択します

[RDS.21] 重大なデータベースパラメータグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります

関連する要件： NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2、PCI DSS v4.0.1/11.5.2

カテゴリ: 検出 > 検出サービス > アプリケーションモニタリング

重要度: 低

リソースタイプ : `AWS::RDS::EventSubscription`

AWS Config ルール: `rds-pg-event-notifications-configured` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ: なし

このコントロールは、次のソースタイプ、イベントカテゴリのキーバリューペアに対して通知が有効になっている Amazon RDS イベントサブスクリプションが存在するかどうかをチェックします。アカウントに既存のイベントサブスクリプションがない場合、コントロールはパスします。

```
DBParameterGroup: ["configuration change"]
```

RDS イベント通知は Amazon SNS を使用して、RDS リソースの可用性または設定の変更をユーザーに知らせます。これらの通知により、迅速な対応が実現します。RDS イベント通知の詳細については、「Amazon RDS ユーザーガイド」の「Amazon RDS イベント通知の使用」を参照してください。

修正

RDS データベースパラメータグループイベント通知にサブスクライブするには、「Amazon RDS ユーザーガイド」の「Amazon RDS イベント通知にサブスクライブする」を参照してください。以下の値を使用します。

フィールド	値
ソースタイプ	パラメータグループ
含めるパラメータグループ	すべてのパラメータグループ
含めるイベントカテゴリ	[Specific event categories] (特定のイベントカテゴリ) または [All event categories] (すべてのイベントカテゴリ) を選択します

[RDS.22] 重大なデータベースセキュリティグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります

関連する要件： NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2、PCI DSS v4.0.1/11.5.2

カテゴリ: 検出 > 検出サービス > アプリケーションモニタリング

重要度: 低

リソースタイプ : `AWS::RDS::EventSubscription`

AWS Config ルール: `rds-sg-event-notifications-configured` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ: なし

このコントロールは、次のソースタイプ、イベントカテゴリのキーバリューペアに対して通知が有効になっている Amazon RDS イベントサブスクリプションが存在するかどうかをチェックします。アカウントに既存のイベントサブスクリプションがない場合、コントロールはパスします。

```
DBSecurityGroup: ["configuration change","failure"]
```

RDS イベント通知は Amazon SNS を使用して、RDS リソースの可用性または設定の変更をユーザーに知らせます。これらの通知により、迅速なレスポンスが可能になります。RDS イベント通知の詳細については、「Amazon RDS ユーザーガイド」の「Amazon RDS イベント通知の使用」を参照してください。

修正

RDS インスタンスイベント通知にサブスクライブするには、「Amazon RDS ユーザーガイド」の「Amazon RDS イベント通知にサブスクライブする」を参照してください。以下の値を使用します。

フィールド	値
ソースタイプ	セキュリティグループ
含めるセキュリティグループ	すべてのセキュリティグループ
含めるイベントカテゴリ	[Specific event categories] (特定のイベントカテゴリ) または [All event categories] (すべてのイベントカテゴリ) を選択します

[RDS.23] RDS インスタンスはデータベースエンジンのデフォルトポートを使用しないようにする必要があります

関連する要件: NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(5)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 低

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール: `rds-no-default-ports` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ : なし

このコントロールは、RDS クラスターまたはインスタンスがデータベースエンジンのデフォルトポート以外のポートを使用しているかどうかをチェックします。RDS クラスターまたはインスタンスがデフォルトポートを使用する場合、このコントロールは失敗します。このコントロールは、クラスターの一部である RDS インスタンスには適用されません。

既知のポートを使用して RDS クラスターまたはインスタンスをデプロイすると、攻撃者はクラスターまたはインスタンスに関する情報を推測できる可能性があります。攻撃者は、この情報を他の情報と組み合わせ、RDS クラスターまたはインスタンスに接続したり、ユーザーのアプリケーションに関する追加情報を取得できます。

ポートを変更する場合は、古いポートへの接続に使用された既存の接続文字列も更新する必要があります。また、ユーザーは DB インスタンスのセキュリティグループをチェックして、新しいポートでの接続を許可するイングレスルールが確実に含まれていることを確認する必要があります。

修正

既存の RDS DB インスタンスのデフォルトポートを変更するには、「Amazon RDS ユーザーガイド」の「Amazon RDS DB インスタンスを変更する」を参照してください。既存の RDS DB クラスターのデフォルトポートを変更するには、「Amazon Aurora ユーザーガイド」の「コンソール、CLI、API を使用した DB クラスターの変更」を参照してください。データベースポートについて、ポート値をデフォルト以外の値に変更します。

[RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります

関連する要件： NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、PCI DSS v4.0.1/2.2.2

カテゴリ: 識別 > リソース設定

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : `rds-cluster-default-admin-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon RDS データベースクラスターが管理者ユーザーネームをデフォルト値から変更したかどうかをチェックします。このコントロールは、Neptune (Neptune DB) または docdb (DocumentDB) タイプのエンジンには適用されません。管理者ユーザーネームがデフォルト値に設定されている場合、このルールは失敗します。

Amazon RDS データベースを作成するときは、デフォルトの管理者ユーザーネームを一意の値に変更する必要があります。デフォルトのユーザーネームはパブリックナレッジであり、RDS データ

ベースの作成時に変更する必要があります。デフォルトのユーザーネームを変更すると、意図しないアクセスのリスクが軽減されます。

修正

Amazon RDS データベースクラスターに関連付けられている管理者ユーザーネームを変更するには、新しい RDS データベースクラスターを作成し、データベースの作成時に、デフォルトの管理者ユーザーネームを変更します。

[RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります

関連する要件： NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、PCI DSS v4.0.1/2.2.2

カテゴリ: 識別 > リソース設定

重要度: 中

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール : `rds-instance-default-admin-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールでは、Amazon Relational Database Service (Amazon RDS) のデータベースインスタンスの管理者ユーザーネームがデフォルト値から変更されたかどうかをチェックします。管理者ユーザーネームがデフォルト値に設定されている場合、このコントロールは失敗します。このコントロールは、neptune (Neptune DB) または docdb (DocumentDB) タイプのエンジン、およびクラスターの一部である RDS インスタンスには適用されません。

Amazon RDS データベースのデフォルトの管理ユーザーネームは、パブリックナレッジです。Amazon RDS データベースを作成するときは、意図しないアクセスのリスクを減らすために、デフォルトの管理ユーザーネームを一意の値に変更する必要があります。

修正

RDS データベースインスタンスに関連付けられている管理ユーザーネームを変更するには、始めに新しい RDS データベースインスタンスを作成します。データベースの作成時に、デフォルトの管理ユーザーネームを変更します。

[RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

重要度: 中

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール： `rds-resources-protected-by-backup-plan`

スケジュールタイプ : 定期的

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`backupVaultLockCheck`	パラメータが true に設定され、リソースが AWS Backup ボールトロックを使用する場合、コントロールはPASSED結果を生成します。	ブール値	`true` 、、または `false`	デフォルト値なし

このコントロールは、Amazon RDS DB インスタンスがバックアッププランの対象かどうかを評価します。RDS DB インスタンスがバックアッププランの対象となっていない場合、このコントロールは失敗します。`backupVaultLockCheck` パラメータを に設定すると`true`、インスタンスが AWS Backup ロックされたボールトにバックアップされている場合にのみコントロールが成功します。

AWS Backup は、データのバックアップを一元化および自動化するフルマネージドバックアップサービスです AWS のサービス。を使用すると AWS Backup、バックアッププランと呼ばれるバックアップポリシーを作成できます。これらのプランを使用して、データのバックアップ頻度やバックアップを保持する期間など、バックアップ要件を定義できます。バックアッププランに RDS DB インスタンスを含めると、意図しない損失や削除からデータを保護できます。

修正

RDS DB インスタンスを AWS Backup バックアッププランに追加するには、「 AWS Backup デベロッパーガイド」の「バックアッププランへのリソースの割り当て」を参照してください。

[RDS.27] RDS DB クラスターは保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール： `rds-cluster-encrypted-at-rest`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、RDS DB クラスターが保管中に暗号化されているかどうかをチェックします。RDS DB クラスターが保管中に暗号化されていない場合、コントロールは失敗します。

保管中のデータとは、永続的な不揮発性ストレージに任意の期間保管されているデータを指します。暗号化は、このようなデータの機密性を保護し、権限のないユーザーがデータにアクセスするリスクを低減するのに役立ちます。RDS DB クラスターを暗号化することで、データとメタデータを不正アクセスから保護します。また、本番稼働用ファイルシステムにおける保管中のデータの暗号化に関するコンプライアンス要件も満たします。

修正

RDS DB クラスターを作成するときに、保管中の暗号化を有効にできます。クラスターを作成した後で暗号化設定を変更することはできません。詳細については、「Amazon Aurora ユーザーガイド」の「Amazon Aurora DB クラスターの暗号化」を参照してください。

[RDS.28] RDS DB クラスターにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config rule:`tagged-rds-dbcluster` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon RDS DB クラスターにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。DB クラスターにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、DB クラスターにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

RDS DB クラスターにタグを追加するには、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースのタグ付け」を参照してください。

[RDS.29] RDS DB クラスタースナップショットにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::RDS::DBClusterSnapshot`

AWS Config rule:`tagged-rds-dbclustersnapshot` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon RDS DB クラスタースナップショットに、パラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。DB クラ

スタースナップショットにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、DB クラスタースナップショットにキーがタグ付けされていない場合に失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

RDS DB クラスタースナップショットにタグを追加するには、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースのタグ付け」を参照してください。

[RDS.30] RDS DB インスタンスにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config rule:`tagged-rds-dbinstance` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon RDS DB インスタンスにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。DB インスタンスにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、DB インスタンスにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

RDS DB インスタンスにタグを追加するには、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースのタグ付け」を参照してください。

[RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::RDS::DBSecurityGroup`

AWS Config rule:`tagged-rds-dbsecuritygroup` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon RDS DB セキュリティグループに、パラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。DB セキュリティグループにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、DB セキュリティグループがキーでタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス

許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、のAWS 「リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

RDS DB セキュリティグループにタグを追加するには、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースのタグ付け」を参照してください。

[RDS.32] RDS DB スナップショットにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::RDS::DBSnapshot`

AWS Config rule:`tagged-rds-dbsnapshot` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタ	StringList (最大 6 項目)	AWS 要件を満たす 1 ~	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	グキーのリスト。タグキーでは、大文字と小文字が区別されます。		6 個のタグキー。	

このコントロールは、Amazon RDS DB スナップショットにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。DB スナップショットにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、DB スナップショットにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

RDS スナップショットにタグを追加するには、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースのタグ付け」を参照してください。

[RDS.33] RDS DB サブネットグループにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::RDS::DBSubnetGroup`

AWS Config rule:`tagged-rds-dbsubnetgroups` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon RDS DB サブネットグループに、パラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。DB サブネットグループにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、DB サブネットグループがキーでタグ付けされていない場合に失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これ

らの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

RDS DB サブネットグループにタグを追加するには、「Amazon RDS ユーザーガイド」の「Amazon RDS リソースのタグ付け」を参照してください。

[RDS.34] Aurora MySQL DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります

関連する要件： NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53AU-6.r5 CA-7、NIST.800-53.r5 SC-7(7) SI-3 SI-4 SI-710.2.1

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール： `rds-aurora-mysql-audit-logging-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon Aurora MySQL DB クラスターが監査ログを Amazon CloudWatch Logs に発行するように設定されているかどうかをチェックします。クラスターが監査ログを CloudWatch Logs に発行するように設定されていない場合、コントロールは失敗します。コントロールは Aurora Serverless v1 DB クラスターの検出結果を生成しません。

監査ログには、ログイン試行、データ変更、スキーマ変更、セキュリティとコンプライアンスの目的で監査の対象となる可能性のあるその他のイベントなど、データベースアクティビティのレコードが記録されます。Aurora MySQL DB クラスターを Amazon CloudWatch Logs のロググループに発行するように設定すると、ログデータのリアルタイム分析を実行できます。CloudWatch Logs は、耐久性の高いストレージにログを保持します。また、CloudWatch でのアラームの作成やメトリクスの表示が可能です。

> **Note**
>
> CloudWatch Logs に監査ログを発行する別の方法は、高度な監査を有効にし、クラスターレベルの DB パラメータ `server_audit_logs_upload` を 1 に設定することです。`server_audit_logs_upload parameter` のデフォルト値は `0` です。ただし、このコントロールを渡すには、代わりに以下の修正手順を使用することをおすすめします。

修正

Aurora MySQL DB のクラスターの監査ログを CloudWatch Logs に発行するには、「Amazon Aurora ユーザーガイド」の「Amazon CloudWatch Logs への Amazon Aurora MySQL ログの発行」を参照してください。

[RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります

関連する要件： NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、PCI DSS v4.0.1/6.3.3

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール： `rds-cluster-auto-minor-version-upgrade-enable`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon RDS マルチ AZ DB クラスターの自動マイナーバージョンアップグレードが有効になっているかどうかを確認します。マルチ AZ DB クラスターで自動マイナーバージョンアップグレードが有効になっていない場合、コントロールは失敗します。

RDS では、マルチ AZ DB クラスターを最新の状態に保つことができるように、マイナーバージョンの自動アップグレードを実行します。マイナーバージョンには、ソフトウェアの新機能、バグ修正、セキュリティパッチ、およびパフォーマンスの向上を含む可能性があります。RDS データベースクラスターでマイナーバージョンの自動アップグレードを有効にすると、新しいバージョンが利用可能になった時点で、クラスターとクラスター内のインスタンスがマイナーバージョンへ自動更新を受け取ります。更新はメンテナンスの時間帯に自動で適用されます。

修正

マルチ AZ DB クラスターでマイナーバージョンの自動アップグレードを有効にするには、「Amazon RDS ユーザーガイド」の「マルチ AZ DB クラスターの変更」を参照してください。

[RDS.36] RDS for PostgreSQL DB は CloudWatch Logs にログを発行する必要があります

関連する要件： PCI DSS v4.0.1/10.4.2

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール : rds-postgresql-logs-to-cloudwatch

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`logTypes`	CloudWatch Logs に発行するログタイプのカンマ区切りリスト	StringList	カスタマイズ不可	`postgresql`

このコントロールは、Amazon RDS for PostgreSQL DB インスタンスがログを Amazon CloudWatch Logs に発行するように設定されているかどうかをチェックします。PostgreSQL DB インスタンスが、 `logTypes` パラメータに記載されているログタイプを CloudWatch Logs に発行するように設定されていない場合、コントロールは失敗します。

データベースログ記録は、RDS インスタンスに対して行われたリクエストの詳細な記録を提供します。PostgreSQL は、管理者に役立つ情報を含むイベントログを生成します。これらのログを CloudWatch Logs に発行すると、ログ管理が一元化され、ログデータのリアルタイム分析の実行に役立ちます。CloudWatch Logs は、耐久性の高いストレージにログを保持します。また、CloudWatch でのアラームの作成やメトリクスの表示が可能です。

修正

PostgreSQL DB インスタンスログを CloudWatch Logs に発行するには、「Amazon RDS ユーザーガイド」の「Amazon CloudWatch Logs への PostgreSQL ログの発行」を参照してください。

[RDS.37] Aurora PostgreSQL DB クラスターでは、ログを CloudWatch Logs に発行する必要があります

関連する要件： PCI DSS v4.0.1/10.4.2

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : rds-aurora-postgresql-logs-to-cloudwatch

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon Aurora PostgreSQL DB クラスターがログを Amazon CloudWatch Logs に発行するように設定されているかどうかをチェックします。Aurora PostgreSQL DB クラスターが PostgreSQL ログを CloudWatch Logs に発行するように設定されていない場合、コントロールは失敗します。

データベースログ記録は、RDS クラスターに対して行われたリクエストの詳細な記録を提供します。Aurora PostgreSQL は、管理者に役立つ情報を含むイベントログを生成します。これらのログを CloudWatch Logs に発行すると、ログ管理が一元化され、ログデータのリアルタイム分析の実行に役立ちます。CloudWatch Logs は、耐久性の高いストレージにログを保持します。また、CloudWatch でのアラームの作成やメトリクスの表示が可能です。

修正

Aurora PostgreSQL DB クラスターの監査ログを CloudWatch Logs に発行するには、「Amazon Aurora ユーザーガイド」の「Amazon CloudWatch Logs への Amazon Aurora PostgreSQL ログの発行」を参照してください。

[RDS.38] RDS for PostgreSQL DB インスタンスは転送中に暗号化する必要があります

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール : rds-postgres-instance-encrypted-in-transit

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、 Amazon RDS for PostgreSQL データベース (DB) インスタンスへの接続が転送中に暗号化されているかどうかを確認します。インスタンスに関連付けられた`rds.force_ssl`パラメータグループの パラメータが `0` (オフ) に設定されている場合、コントロールは失敗します。このコントロールは、DB クラスターの一部である RDS DB インスタンスを評価しません。

転送中のデータとは、クラスター内のノード間やクラスターとアプリケーション間など、ある場所から別の場所に移動するデータを指します。データはインターネット内またはプライベートネットワーク内を移動する場合があります。転送中のデータを暗号化することで、権限のないユーザーがネットワークトラフィックを盗聴するリスクが軽減されます。

修正

RDS for PostgreSQL DB インスタンスへのすべての接続に SSL の使用を要求するには、「Amazon RDS ユーザーガイド」のPostgreSQL DB インスタンスでの SSL の使用」を参照してください。

[RDS.39] RDS for MySQL DB インスタンスは転送中に暗号化する必要があります

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール : rds-mysql-instance-encrypted-in-transit

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、 Amazon RDS for MySQL データベース (DB) インスタンスへの接続が転送中に暗号化されているかどうかを確認します。インスタンスに関連付けられたrds.require_secure_transportパラメータグループの パラメータが 0 (オフ) に設定されている場合、コントロールは失敗します。このコントロールは、DB クラスターの一部である RDS DB インスタンスを評価しません。

転送中のデータとは、クラスター内のノード間やクラスターとアプリケーション間など、ある場所から別の場所に移動するデータを指します。データはインターネット内またはプライベートネットワーク内を移動する場合があります。転送中のデータを暗号化することで、権限のないユーザーがネットワークトラフィックを盗聴するリスクが軽減されます。

修正

RDS for MySQL DB インスタンスへのすべての接続に SSL の使用を要求するには、「Amazon RDS ユーザーガイド」の「Amazon RDS での MySQL DB インスタンスの SSL/TLS サポート」を参照してください。

[RDS.40] RDS for SQL Server DB インスタンスは CloudWatch Logs にログを発行する必要があります

関連する要件: NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : AWS::RDS::DBInstance

AWS Config ルール : rds-sql-server-logs-to-cloudwatch

スケジュールタイプ : 変更がトリガーされた場合

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`logTypes`	RDS for SQL Server DB インスタンスが CloudWatch Logs に発行するように設定する必要があるログのタイプのリスト。DB インスタンスがリストで指定されたタイプのログを発行するように設定されていない場合、このコントロールは失敗します。	EnumList (最大 2 項目)	`agent`, `error`	`agent`, `error`

このコントロールは、Amazon RDS for Microsoft SQL Server DB インスタンスが Amazon CloudWatch Logs にログを発行するように設定されているかどうかを確認します。RDS for SQL Server DB インスタンスが CloudWatch Logs にログを発行するように設定されていない場合、コントロールは失敗します。オプションで、DB インスタンスが発行するように設定する必要があるログのタイプを指定できます。

データベースログ記録は、Amazon RDS DB インスタンスに対して行われたリクエストの詳細なレコードを提供します。CloudWatch Logs にログを発行すると、ログ管理が一元化され、ログデータのリアルタイム分析の実行に役立ちます。CloudWatch Logs は、耐久性の高いストレージにログを保持します。さらに、これを使用して、エラーログに記録される頻繁な再起動など、発生する可能性のある特定のエラーのアラームを作成できます。同様に、SQL エージェントジョブに関連する SQL Server エージェントログに記録されるエラーまたは警告のアラームを作成できます。

修正

RDS for SQL Server DB インスタンスの CloudWatch Logs へのログの発行については、「Amazon Relational Database Service ユーザーガイド」の「Amazon RDS for Microsoft SQL Server データベースログファイル」を参照してください。 Amazon Relational Database Service

[RDS.41] RDS for SQL Server DB インスタンスは転送中に暗号化する必要があります

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール : rds-sqlserver-encrypted-in-transit

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon RDS for Microsoft SQL Server DB インスタンスへの接続が転送中に暗号化されているかどうかを確認します。DB インスタンスに関連付けられた`rds.force_ssl`パラメータグループの パラメータが に設定されている場合、コントロールは失敗します`0 (off)`。

転送中のデータとは、DB クラスター内のノード間、DB クラスターとクライアントアプリケーション間など、ある場所から別の場所に移動するデータを指します。データはインターネット内またはプライベートネットワーク内を移動できます。転送中のデータを暗号化すると、不正なユーザーがネットワークトラフィックを盗聴するリスクが軽減されます。

修正

Microsoft SQL Server を実行している Amazon RDS DB インスタンスへの接続で SSL/TLS を有効にする方法については、Amazon Relational Database Service ユーザーガイド」の「Microsoft SQL Server DB インスタンスでの SSL の使用」を参照してください。

[RDS.42] RDS for MariaDB DB インスタンスは CloudWatch Logs にログを発行する必要があります

関連する要件： NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 AU-10、NIST.800-53AU-12.r5 CA-7、NIST.800-53.r5 SC-73(7) NIST.800-53.r5 SC-7 SI-3 SI-4 SI-7

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール : mariadb-publish-logs-to-cloudwatch-logs

スケジュールタイプ : 定期的

パラメータ：

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`logTypes`	MariaDB DB インスタンスが CloudWatch Logs に発行するように設定する必要があるログのタイプのリスト。DB インスタンスがリストで指定されたログタイプを発行するように設定されていない場合、コントロールは`FAILED`結果を生成します。	EnumList (最大 4 項目)	`audit`, `error`, `general`, `slowquery`	`audit`, `error`

このコントロールは、Amazon RDS for MariaDB DB インスタンスが特定のタイプのログを Amazon CloudWatch Logs に発行するように設定されているかどうかを確認します。MariaDB DB インスタンスが CloudWatch Logs にログを発行するように設定されていない場合、コントロールは失敗します。オプションで、MariaDB DB インスタンスが発行するように設定する必要があるログのタイプを指定できます。

データベースログ記録は、Amazon RDS for MariaDB DB インスタンスに対して行われたリクエストの詳細なレコードを提供します。Amazon CloudWatch Logs にログを発行すると、ログ管理が一元化され、ログデータのリアルタイム分析の実行に役立ちます。さらに、CloudWatch Logs はログを耐久性のあるストレージに保持し、セキュリティ、アクセス、可用性のレビューと監査をサポートできます。CloudWatch Logs を使用すると、アラームを作成してメトリクスを確認することもできます。

修正

Amazon CloudWatch Logs にログを発行するように Amazon RDS for MariaDB DB インスタンスを設定する方法については、「Amazon Amazon Relational Database Serviceユーザーガイド」の「Amazon CloudWatch Logs への MariaDB ログの発行」を参照してください。

[RDS.44] RDS for MariaDB DB インスタンスは転送中に暗号化する必要があります

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::RDS::DBInstance`

AWS Config ルール : rds-mariadb-instance-encrypted-in-transit

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon RDS for MariaDB DB インスタンスへの接続が転送中に暗号化されているかどうかをチェックします。DB インスタンスに関連付けられた DB パラメータグループが同期していない場合、または`require_secure_transport`パラメータグループの パラメータが に設定されていない場合、コントロールは失敗します`ON`。

> **Note**
>
> このコントロールは、バージョン 10.5 より前の MariaDB バージョンを使用する Amazon RDS DB インスタンスを評価しません。`require_secure_transport` パラメータは、MariaDB バージョン 10.5 以降でのみサポートされています。

転送中のデータとは、DB クラスター内のノード間、DB クラスターとクライアントアプリケーション間など、ある場所から別の場所に移動するデータを指します。データはインターネット内またはプライベートネットワーク内を移動できます。転送中のデータを暗号化すると、不正なユーザーがネットワークトラフィックを盗聴するリスクが軽減されます。

修正

Amazon RDS for MariaDB DB インスタンスへの接続で SSL/TLS を有効にする方法については、Amazon Relational Database Service ユーザーガイド」の「Requiring SSL/TLS for all connections to a MariaDB DB instance」を参照してください。

[RDS.45] Aurora MySQL DB クラスターでは、監査ログ記録を有効にする必要があります

関連する要件： NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 AU-10、NIST.800-53.AU-12r5 CA-7、NIST.800-53.r5 SC-73 SI-3 SI-4 SI-7

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::RDS::DBCluster`

AWS Config ルール : aurora-mysql-cluster-audit-logging

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon Aurora MySQL DB クラスターで監査ログ記録が有効になっているかどうかを確認します。DB クラスターに関連付けられた DB パラメータグループが同期していない場合、 `server_audit_logging` パラメータが に設定されていない場合、または `server_audit_events`パラメータが空の値に設定されている場合1、コントロールは失敗します。

データベースログは、セキュリティとアクセスの監査を支援し、可用性の問題の診断に役立ちます。監査ログには、ログイン試行、データ変更、スキーマ変更、セキュリティとコンプライアンスの目的で監査の対象となる可能性のあるその他のイベントなど、データベースアクティビティのレコードが記録されます。

修正

Amazon Aurora MySQL DB クラスターのログ記録を有効にする方法については、「Amazon Aurora ユーザーガイド」のAmazon CloudWatch Logs への Amazon Aurora MySQL ログの発行」を参照してください。

Amazon Redshift の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon Redshift サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります

関連する要件： NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7NIST.800-53.r5 SC-7NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7r

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 非常事態

リソースタイプ : `AWS::Redshift::Cluster`

AWS Config ルール : redshift-cluster-public-access-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon Redshift クラスターがパブリックにアクセス可能かどうかをチェックします。このコントロールは、クラスター設定項目の `PubliclyAccessible` フィールドを評価します。

Amazon Redshift クラスター設定の `PubliclyAccessible` 属性は、クラスターがパブリックにアクセス可能かどうかを示します。クラスターが `PubliclyAccessible` を `true` に設定して構成されている場合、パブリックに解決可能な DNS 名を持つインターネット向けインスタンスであり、パブリック IP アドレスに解決されます。

クラスターがパブリックにアクセスできない場合、プライベート IP アドレスに解決される DNS 名を持つ内部インスタンスです。クラスターをパブリックにアクセスさせる意図がない限り、クラスターは `PubliclyAccessible` を `true` に設定しないでください。

修正

Amazon Redshift クラスターを更新してパブリックアクセスを無効にするには、「Amazon Redshift 管理ガイド」の「クラスターの変更」を参照してください。[Publicly Accessible] を [No] に設定します。

[Redshift.2] Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります

関連する要件： NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、PCI DSS v4.0.1/4.2.1

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ： `AWS::Redshift::Cluster` `AWS::Redshift::ClusterParameterGroup`

AWS Config ルール : redshift-require-tls-ssl

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon Redshift クラスターへの接続において、転送中に暗号化を使用する必要があるかどうかをチェックします。Amazon Redshift クラスターパラメータ `require_SSL` が `True` に設定されていない場合、チェックは失敗します。

TLS を使用すると、潜在的な攻撃者が中間者攻撃または同様の攻撃を使用してネットワークトラフィックを盗聴または操作することを防止できます。TLS 経由の暗号化された接続のみを許可する必要があります。転送中のデータの暗号化は、パフォーマンスに影響する可能性があります。TLS のパフォーマンスプロファイルと TLS の影響を把握するには、この機能を使用してアプリケーションをテストする必要があります。

修正

Amazon Redshift パラメータグループを更新して暗号化を要求するには、「Amazon Redshift 管理ガイド」の「パラメータグループの変更」を参照してください。`require_ssl`を True に設定します。

[Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-13(5)

カテゴリ: リカバリ > 耐障害性 > バックアップの有効化

重要度: 中

リソースタイプ : `AWS::Redshift::Cluster`

AWS Config ルール : redshift-backup-enabled

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値	
`MinRetentionPeriod`	最小スナップショット保持期間 (日数)	整数	7 ~ 35	7	

このコントロールは、Amazon Redshift クラスターで自動スナップショットが有効になっているかどうか、および保持期間が指定された時間枠以上であるかどうかをチェックします。クラスターの自動スナップショットが有効になっていない場合や、保持期間が指定された時間枠未満の場合、コントロールは失敗します。スナップショット保持期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 7 日を使用します。

バックアップは、セキュリティインシデントからより迅速に復元するために役立ちます。これにより、システムの耐障害性が強化されます。Amazon Redshift は、デフォルトで定期的にスナップショットを作成します。このコントロールは、自動スナップショットが有効で、少なくとも 7 日間保持されているかどうかをチェックします。Amazon Redshift の自動スナップショットの詳細については、「Amazon Redshift 管理ガイド」の「自動スナップショット」を参照してください。

修正

Amazon Redshift クラスターのスナップショット保持期間を更新するには、「Amazon Redshift 管理ガイド」の「クラスターの変更」を参照してください。[Backup] (バックアップ) の場合、[Snapshot retention] (スナップショットの保持) を 7 以上の値に設定します。

[Redshift.4] Amazon Redshift クラスターでは、監査ログ記録が有効になっている必要があります

関連する要件： NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53AU-6.r5 CA-7、NIST.800-53.r5 SC-7(7) SI-3 SI-4 SI-710.2.1

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::Redshift::Cluster`

AWS Config ルール: `redshift-cluster-audit-logging-enabled` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `loggingEnabled = true` (カスタマイズ不可)

このコントロールは、Amazon Redshift クラスターで監査ログ記録が有効になっているかどうかをチェックします。

Amazon Redshift 監査ログ記録は、ユーザーのクラスター内の接続とユーザーアクティビティに関する追加情報を提供します。このデータは、Amazon S3 内で保存および保護することができ、セキュリティ監査や調査に役立ちます。詳細については、「Amazon Redshift 管理ガイド」の「データベース監査ログ記録」を参照してください。

修正

Amazon Redshift クラスターの監査ログを設定するには、「Amazon Redshift 管理ガイド」の「コンソールを使用して監査を設定する」を参照してください。

[Redshift.6] Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)

カテゴリ: 特定 > 脆弱性、パッチ、バージョン管理

重要度: 中

リソースタイプ : `AWS::Redshift::Cluster`

AWS Config ルール : redshift-cluster-maintenancesettings-check

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `allowVersionUpgrade = true` (カスタマイズ不可)

このコントロールは、Amazon Redshift クラスターで自動メジャーバージョンアップグレードが有効になっているかどうかをチェックします。

自動メジャーバージョンアップグレードを有効にすることで、メンテナンスウィンドウ中に Amazon Redshift クラスターの最新のメジャーバージョンの更新がインストールされます。これらのアップデートには、セキュリティパッチやバグ修正が含まれる場合があります。パッチのインストールを最新の状態に保つことは、システムを保護する上で重要なステップです。

修正

からこの問題を修正するには AWS CLI、Amazon Redshift `modify-cluster` コマンドを使用して `--allow-version-upgrade` 属性を設定します。 *`clustername`*は Amazon Redshift クラスターの名前です。

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

[Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります

関連する要件: NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > API プライベートアクセス

重要度: 中

リソースタイプ : `AWS::Redshift::Cluster`

AWS Config ルール : redshift-enhanced-vpc-routing-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ: なし

このコントロールは、Amazon Redshift クラスターで `EnhancedVpcRouting` が有効かどうかをチェックします。

拡張 VPC ルーティングは、クラスターとデータリポジトリ間のすべての `COPY` および `UNLOAD` トラフィックが VPC を経由するよう強制します。その後、セキュリティグループやネットワークアクセ

スコントロールリストなどの VPC 機能を使用して、ネットワークトラフィックを保護することができます。VPC フローログを使用して、ネットワークトラフィックをモニタリングすることもできます。

修正

詳細な修正手順については、「Amazon Redshift 管理ガイド」の「拡張された VPC ルーティングの有効化」を参照してください。

[Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 識別 > リソース設定

重要度: 中

リソースタイプ : `AWS::Redshift::Cluster`

AWS Config ルール : redshift-default-admin-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon Redshift クラスターが、管理者ユーザーネームをデフォルト値から変更したかどうかをチェックします。Redshift クラスターの管理者ユーザーネームが `awsuser` に設定されている場合、このコントロールは失敗します。

Amazon RDS クラスターを作成するときは、デフォルトの管理者ユーザーネームを一意の値に変更する必要があります。デフォルトのユーザーネームはパブリックナレッジであり、設定時に変更する必要があります。デフォルトのユーザーネームを変更すると、意図しないアクセスのリスクが軽減されます。

修正

Amazon Redshift クラスターの管理者ユーザーネームは、作成後に変更することはできません。デフォルト以外のユーザー名で新しいクラスターを作成するには、「Amazon Redshift 入門ガイド」の「ステップ 1: サンプル Amazon Redshift クラスターを作成する」を参照してください。

[Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 識別 > リソース設定

重要度: 中

リソースタイプ : `AWS::Redshift::Cluster`

AWS Config ルール : redshift-default-db-name-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon Redshift クラスターが、データベース名をデフォルト値から変更したかどうかをチェックします。Redshift クラスターのデータベース名が dev に設定されている場合、このコントロールは失敗します。

Redshift クラスターを作成するときは、デフォルトのデータベース名を一意の値に変更する必要があります。デフォルトの名前は一般に知られているため、設定時に変更する必要があります。よく知られた名前は、IAM ポリシー条件などで使用されると偶発的なアクセスにつながる可能性があります。

修正

Amazon Redshift クラスターのデータベース名は、作成後に変更することはできません。新規クラスターの作成方法については、「Amazon Redshift の入門ガイド」の「Amazon Redshift の開始方法」を参照してください。

[Redshift.10] Redshift クラスターは保存時に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::Redshift::Cluster`

AWS Config ルール : redshift-cluster-kms-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon Redshift クラスターが保管時に暗号化されているかどうかをチェックします。Redshift クラスターが保存時に暗号化されていない場合、または暗号化キーがルールパラメータで指定されたキーと異なる場合、コントロールは失敗します。

Amazon Redshift では、クラスターに対してデータベースの暗号化を有効にして、保管中のデータを保護できます。クラスターに対して暗号化を有効にすると、クラスターとそのスナップショットのデータブロックとシステムメタデータが暗号化されます。保管中のデータの暗号化は、データにアクセス管理のレイヤーを追加できるため、推奨されるベストプラクティスです。保管中の Redshift クラスターを暗号化すると、認証されていないユーザーがディスクに保存しているデータにアクセスするリスクが低減されます。

修正

KMS 暗号化を使用するように Redshift クラスターを変更するには、Amazon Redshift 管理ガイドの「クラスターの暗号化の変更」を参照してください。

[Redshift.11] Redshift クラスターにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Redshift::Cluster`

AWS Config ルール: `tagged-redshift-cluster` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタ	StringList (最大 6 項目)	AWS 要件を満たす 1 ~	`No default value`

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	グキーのリスト。タグキーでは、大文字と小文字が区別されます。		6 個のタグキー。	

このコントロールは、Amazon Redshift クラスターにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。クラスターにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、クラスターにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Redshift クラスターにタグを追加するには、「Amazon Redshift 管理ガイド」の「Amazon Redshift でのリソースのタグ付け」を参照してください。

[Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Redshift::EventSubscription`

AWS Config ルール: `tagged-redshift-eventsubscription` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、Amazon Redshift クラスタースナップショットに、パラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。クラスタースナップショットにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、クラスタースナップショットにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プ

リンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Redshift イベント通知サブスクリプションにタグを追加するには、「Amazon Redshift 管理ガイド」の「Amazon Redshift でのリソースのタグ付け」を参照してください。

[Redshift.13] Redshift クラスタースナップショットにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Redshift::ClusterSnapshot`

AWS Config ルール: `tagged-redshift-clustersnapshot` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーで	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	は、大文字と小文字が区別されます。			

このコントロールは、Amazon Redshift クラスタースナップショットに、パラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。クラスタースナップショットにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、クラスタースナップショットにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Redshift クラスタースナップショットにタグを追加するには、「Amazon Redshift 管理ガイド」の「Amazon Redshift でのリソースのタグ付け」を参照してください。

[Redshift.14] Redshift クラスターサブネットグループにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Redshift::ClusterSubnetGroup`

AWS Config ルール: `tagged-redshift-clustersubnetgroup` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、Amazon Redshift クラスターサブネットグループに、パラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。クラスターサブネットグループにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、クラスターサブネットグループがキーでタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これ

らの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Redshift クラスターサブネットグループにタグを追加するには、「Amazon Redshift 管理ガイド」の「Amazon Redshift でのリソースのタグ付け」を参照してください。

[Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの入力を許可する必要があります

関連する要件： PCI DSS v4.0.1/1.3.1

カテゴリ: 保護 > セキュアなネットワーク設定 > セキュリティグループの設定

重要度: 高

リソースタイプ : `AWS::Redshift::Cluster`

AWS Config ルール : redshift-unrestricted-port-access

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon Redshift クラスターに関連付けられたセキュリティグループに、インターネット (0.0.0.0/0 または ::/0) からのクラスターポートへのアクセスを許可する入力ルールがあるかどうかをチェックします。セキュリティグループの入力ルールがインターネットからのクラスターポートへのアクセスを許可すると、コントロールは失敗します。

Redshift クラスターポート (/0 サフィックスを持つ IP アドレス) への無制限のインバウンドアクセスを許可すると、不正アクセスやセキュリティインシデントが発生する可能性があります。セキュリ

ティグループを作成し、インバウンドルールを設定するときは、最小特権アクセスのプリンシパルを適用することをお勧めします。

修正

Redshift クラスターポートの入力を制限されたオリジンに制限するには、「Amazon VPC ユーザーガイド」の「セキュリティグループルールの操作」を参照してください。ポート範囲が Redshift クラスターポートと一致し、IP ポート範囲が 0.0.0.0/0 であるルールを更新します。

[Redshift.16] Redshift クラスターサブネットグループには、複数のアベイラビリティーゾーンからのサブネットが必要です

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::Redshift::ClusterSubnetGroup`

AWS Config ルール : redshift-cluster-subnet-group-multi-az

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon Redshift クラスターサブネットグループに複数のアベイラビリティーゾーン (AZ) からのサブネットがあるかどうかをチェックします。クラスターサブネットグループに少なくとも 2 つの異なる AZs。

複数の AZs、障害イベントが発生した場合でも Redshift データウェアハウスが動作し続けることができます。

修正

Redshift クラスターサブネットグループを複数の AZs、「Amazon Redshift 管理ガイド」の「クラスターサブネットグループの変更」を参照してください。

[Redshift.17] Redshift クラスターパラメータグループにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Redshift::ClusterParameterGroup`

AWS Config ルール : redshift-cluster-parameter-group-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon Redshift クラスターパラメータグループに `requiredKeyTags`パラメータで指定されたタグキーがあるかどうかをチェックします。パラメータグループにタグキーがない場合、または `requiredKeyTags` パラメータで指定されたすべてのキーがない場合、コントロールは失敗します。`requiredKeyTags` パラメータに値を指定しない場合、コントロールはタグキーの存在のみをチェックし、パラメータグループにタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、 `aws:` プレフィックスが付いています。

タグは、 AWS リソースを作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの識別、整理、検索、フィルタリングに役立ちます。また、アクションと通知のリソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセスコントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 AWS リソースのタグ付け」および「タグエディタユーザーガイド」を参照してください。

> **Note**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

Amazon Redshift クラスターパラメータグループにタグを追加する方法については、「Amazon Redshift 管理ガイド」の「Amazon Redshift のリソースのタグ付け」を参照してください。

[Redshift.18] Redshift クラスターでは、マルチ AZ 配置を有効にする必要があります

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::Redshift::Cluster`

AWS Config ルール : redshift-cluster-multi-az-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon Redshift クラスターで複数のアベイラビリティーゾーン (マルチ AZ) デプロイが有効になっているかどうかを確認します。Amazon Redshift クラスターでマルチ AZ 配置が有効になっていない場合、コントロールは失敗します。

Amazon Redshift は、プロビジョニングされたクラスターに対して複数のアベイラビリティーゾーン (マルチ AZ) デプロイをサポートしています。クラスターでマルチ AZ 配置が有効になっている場合、Amazon Redshift データウェアハウスは、アベイラビリティーゾーン (AZ) で予期しないイベントが発生した場合でも、障害シナリオで動作し続けることができます。マルチ AZ 配置は、コンピューティングリソースを複数の AZ にデプロイし、これらのコンピューティングリソースには 1 つのエンドポイントからアクセスできます。AZ 全体に障害が発生した場合、別の AZ の残りのコンピューティングリソースを使用してワークロードの処理を継続できます。既存のシングル AZ データウェアハウスをマルチ AZ データウェアハウスに変換できます。その後、追加のコンピューティングリソースが 2 番目の AZ にプロビジョニングされます。

修正

Amazon Redshift クラスターのマルチ AZ 配置の設定については、「Amazon Redshift 管理ガイド」の「シングル AZ データウェアハウスをマルチ AZ データウェアハウスに変換する」を参照してください。

Amazon Redshift Serverless の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon Redshift Serverless サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります

カテゴリ: 保護 > セキュアなネットワーク設定 > VPC 内のリソース

重要度: 高

リソースタイプ : `AWS::RedshiftServerless::Workgroup`

AWS Config ルール : redshift-serverless-workgroup-routes-within-vpc

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon Redshift Serverless ワークグループで拡張 VPC ルーティングが有効になっているかどうかを確認します。ワークグループで拡張 VPC ルーティングが無効になっている場合、コントロールは失敗します。

Amazon Redshift Serverless ワークグループで拡張 VPC ルーティングが無効になっている場合、Amazon Redshift は AWS ネットワーク内の他のサービスへのトラフィックを含め、インターネット経由でトラフィックをルーティングします。ワークグループの拡張 VPC ルーティングを有効にすると、Amazon Redshift は Amazon VPC サービスに基づいて仮想プライベートクラウド (VPC) を介してクラスターとデータリポジトリ間のすべての `COPY`および `UNLOAD`トラフィックを強制します。拡張 VPC ルーティングを使用すると、標準の VPC 機能を使用して、Amazon Redshift クラスターと他のリソース間のデータフローを制御できます。これには、VPC セキュリティグループとエンドポイントポリシー、ネットワークアクセスコントロールリスト (ACLs)、ドメインネームシステム (DNS) サーバーなどの機能が含まれます。VPC フローログを使用して、 `COPY`および `UNLOAD`トラフィックをモニタリングすることもできます。

修正

拡張 VPC ルーティングとワークグループで有効にする方法の詳細については、「Amazon Redshift 管理ガイド」の「Redshift 拡張 VPC ルーティングによるネットワークトラフィックの制御」を参照してください。

[RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::RedshiftServerless::Workgroup`

AWS Config ルール : redshift-serverless-workgroup-encrypted-in-transit

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、転送中のデータを暗号化するために Amazon Redshift Serverless ワークグループへの接続が必要かどうかを確認します。ワークグループ`require_ssl`の設定パラメータが に設定されている場合、コントロールは失敗します`false`。

Amazon Redshift Serverless ワークグループは、RPUs、セキュリティグループなどのコンピューティングリソースをグループ化するコンピューティングリソースのコレクションです。ワークグループのプロパティには、ネットワーク設定とセキュリティ設定が含まれます。これらの設定は、転送中のデータを暗号化するために SSL を使用するためにワークグループへの接続が必要かどうかを指定します。

修正

Amazon Redshift Serverless ワークグループの設定を更新して SSL 接続を要求する方法については、「Amazon Redshift 管理ガイド」の「Amazon Redshift Serverless への接続」を参照してください。

[RedshiftServerless.3] Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 高

リソースタイプ : `AWS::RedshiftServerless::Workgroup`

AWS Config ルール : redshift-serverless-workgroup-no-public-access

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon Redshift Serverless ワークグループのパブリックアクセスが無効になっているかどうかをチェックします。Redshift Serverless ワークグループの `publiclyAccessible`プロパティを評価します。ワークグループのパブリックアクセス (`true`) が有効になっている場合、コントロールは失敗します。

Amazon Redshift Serverless ワークグループのパブリックアクセス (`publiclyAccessible`) 設定は、ワークグループにパブリックネットワークからアクセスできるかどうかを指定します。ワークグループのパブリックアクセスが有効になっている場合 (`true`) 、Amazon Redshift はワークグループを VPC の外部からパブリックにアクセスできるようにする Elastic IP アドレスを作成します。ワークグループにパブリックアクセスを許可しない場合は、そのワークグループのパブリックアクセスを無効にします。

修正

Amazon Redshift Serverless ワークグループのパブリックアクセス設定を変更する方法については、「Amazon Redshift 管理ガイド」の「ワークグループのプロパティの表示」を参照してください。

[RedshiftServerless.4] Redshift Serverless 名前空間はカスタマーマネージドで暗号化する必要があります AWS KMS keys

関連する要件： NIST.800-53.r5 AU-9、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-12(2)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::RedshiftServerless::Namespace`

AWS Config ルール : redshift-serverless-namespace-cmk-encryption

スケジュールタイプ : 定期的

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
kmsKeyArns	評価 AWS KMS keys に含める の Amazon リソースネーム (ARNs) のリスト。Redshift Serverless 名前空間がリスト内の KMS キーで暗号化されていない場合、コントロールはFAILED検出結果を生成します。	StringList (最大 3 項目)	既存の KMS キーの ARNs。例: arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab 。	デフォルト値なし

このコントロールは、Amazon Redshift Serverless 名前空間がカスタマーマネージドで保管中に暗号化されているかどうかを確認します AWS KMS key。Redshift Serverless 名前空間がカスタマーマネージド KMS キーで暗号化されていない場合、コントロールは失敗します。オプションで、評価に含めるコントロールの KMS キーのリストを指定できます。

Amazon Redshift Serverless では、名前空間はデータベースオブジェクトの論理コンテナを定義します。このコントロールは、名前空間の暗号化設定が、名前空間内のデータの暗号化のために AWS KMS key、マネージド KMS キーではなくカスタマー AWS マネージド を指定するかどうかを定期的にチェックします。カスタマーマネージド KMS キーを使用すると、キーを完全に制御できます。これには、キーポリシーの定義と保守、許可の管理、暗号化マテリアルのローテーション、タグの割り当て、エイリアスの作成、キーの有効化と無効化が含まれます。

修正

Amazon Redshift Serverless 名前空間の暗号化設定の更新とカスタマー管理の指定については AWS KMS key、「Amazon Redshift 管理ガイド」の「名前空間 AWS KMS key の の変更」を参照してください。

[RedshiftServerless.5] Redshift Serverless 名前空間では、デフォルトの管理者ユーザー名を使用しないでください

カテゴリ: 識別 > リソース設定

重要度: 中

リソースタイプ : `AWS::RedshiftServerless::Namespace`

AWS Config ルール : redshift-serverless-default-admin-check

スケジュールタイプ : 定期的

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`validAdminUserNames`	Redshift Serverless 名前空間で使用する管理者ユーザー名のリスト。名前空間がリストにない管理者ユーザー名を使用している場合、コントロールは`FAILED`結果を生成します。リストでデフォルト値 を指定することはできません`admin`。	StringList (最大 6 項目)	Redshift Serverless 名前空間の有効な管理者ユーザー名は 1 ~ 6 個です。	デフォルト値なし

このコントロールは、Amazon Redshift Serverless 名前空間の管理者ユーザー名がデフォルトの管理者ユーザー名 であるかどうかをチェックします`admin`。Redshift Serverless 名前空間の管理者ユーザー名が の場合、コントロールは失敗します`admin`。必要に応じて、コントロールの管理者ユーザー名のリストを指定して、評価に含めることができます。

Amazon Redshift Serverless 名前空間を作成するときは、名前空間のカスタム管理者ユーザー名を指定する必要があります。デフォルトの管理者ユーザー名はパブリックナレッジです。カスタム管理者ユーザー名を指定することで、たとえば、名前空間に対するブルートフォース攻撃のリスクや有効性を軽減できます。

修正

Amazon Redshift Serverless コンソールまたは API を使用して、Amazon Redshift Serverless 名前空間の管理者ユーザー名を変更できます。コンソールを使用して変更するには、名前空間設定を選択し、アクションメニューで管理者認証情報の編集を選択します。プログラムで変更するには、UpdateNamespace オペレーションを使用するか、 を使用している場合は update-namespace コマンド AWS CLIを実行します。管理者ユーザー名を変更する場合は、管理者パスワードも同時に変更する必要があります。

[RedshiftServerless.6] Redshift Serverless 名前空間は CloudWatch Logs にログをエクスポートする必要があります

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::RedshiftServerless::Namespace`

AWS Config ルール : redshift-serverless-publish-logs-to-cloudwatch

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon Redshift Serverless 名前空間が接続ログとユーザーログを Amazon CloudWatch Logs にエクスポートするように設定されているかどうかを確認します。Redshift Serverless 名前空間がログを CloudWatch Logs にエクスポートするように設定されていない場合、コントロールは失敗します。

接続ログ (`connectionlog`) とユーザーログ (`userlog`) のデータを Amazon CloudWatch Logs のロググループにエクスポートするように Amazon Redshift Serverless を設定すると、ログレコードを収集して耐久性のあるストレージに保存し、セキュリティ、アクセス、可用性のレビューと監査をサポートできます。CloudWatch Logs を使用すると、ログデータのリアルタイム分析を実行し、CloudWatch を使用してアラームを作成し、メトリクスを確認することもできます。

修正

Amazon Redshift Serverless 名前空間のログデータを Amazon CloudWatch Logs にエクスポートするには、名前空間の監査ログ記録設定でエクスポートする各ログを選択する必要があります。これらの設定の更新については、「Amazon Redshift 管理ガイド」の「セキュリティと暗号化の編集」を参照してください。

[RedshiftServerless.7] Redshift Serverless 名前空間はデフォルトのデータベース名を使用しないでください

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 識別 > リソース設定

重要度: 中

リソースタイプ : `AWS::RedshiftServerless::Namespace`

AWS Config ルール : redshift-serverless-default-db-name-check

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon Redshift Serverless 名前空間がデフォルトのデータベース名 を使用しているかどうかをチェックします`dev`。Redshift Serverless 名前空間でデフォルトのデータベース名 が使用されている場合、コントロールは失敗します`dev`。

Amazon Redshift Serverless 名前空間を作成するときは、データベース名に一意のカスタム値を指定し、デフォルトのデータベース名 は使用しないでください`dev`。デフォルトのデータベース名はパブリックナレッジです。別のデータベース名を指定することで、権限のないユーザーが誤って名前空間内のデータにアクセスするなどのリスクを軽減できます。

修正

名前空間の作成後に Amazon Redshift Serverless 名前空間のデータベース名を変更することはできません。ただし、名前空間の作成時に Redshift Serverless 名前空間のカスタムデータベース名を指定できます。名前空間の作成の詳細については、「Amazon Redshift 管理ガイド」の「ワークグループと名前空間」を参照してください。

Route 53 の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon Route 53 サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Route53::HealthCheck`

AWS Config ルール : `tagged-route53-healthcheck` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon Route 53 ヘルスチェックにパラメータ `requiredTagKeys` で定義された特定のキーを含むタグがあるかどうかをチェックします。ヘルスチェックにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ヘルスチェックにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルであり、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Route 53 ヘルスチェックにタグを追加するには、「Amazon Route 53 デベロッパーガイド」の「ヘルスチェックの命名とタグ付け」を参照してください。

[Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります

関連する要件： NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53AU-6.r5 CA-7、NIST.800-53.r5 SC-7(9) SI-3 SI-4 SI-710.4.2

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::Route53::HostedZone`

AWS Config ルール : `route53-query-logging-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

Amazon Route 53 パブリックホストゾーンで DNS クエリログ記録が有効になっているかどうかを確認します。このコントロールは Amazon Route 53 パブリックホストゾーンで DNS クエリログ記録が有効になっているかどうかを確認します。

Route 53 ホストゾーンの DNS クエリを記録することで、DNS のセキュリティとコンプライアンスの要件に対応し、可視性を高めます。ログには、クエリされたドメインまたはサブドメイン、クエリの日時、DNS レコードタイプ (A や AAAA など)、DNS 応答コード (`NoError` または `ServFail`) などの情報が含まれます。DNS クエリのロギングが有効になると、Route 53 はログファイルを Amazon CloudWatch Logs に発行します。

修正

Route 53 パブリックホストゾーンの DNS クエリをログ記録するには、「Amazon Route 53 デベロッパーガイド」の「DNS クエリのログ記録の設定」を参照してください。

Amazon S3 の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon Simple Storage Service (Amazon S3) サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[S3.1] S3 汎用バケットではブロックパブリックアクセスの設定が有効になっている必要があります。

関連する要件： CIS AWS Foundations Benchmark v3.0.0/2.1.4、 CIS AWS Foundations Benchmark v1.4.0/2.1.5、 NIST.800-53.r5 AC-21、 NIST.800-53.r5 AC-3、 NIST.800-53.r5 AC-3(7)、 NIST.800-53.r5 AC-4、 NIST.800-53.r5 AC-4(21)、 NIST.800-53.r5 AC-6、 NIST.800-53.r5 SC-7、 NIST.800-53.r5 SC-7(11)、 NIST.800-53.r5 SC-7(16)、 NIST.800-53.r5 SC-7(20)、 NIST.800-53.r5 SC-7(21)、 NIST.800-53.r5 SC-7(3)、 NIST.800-53.r5 SC-7(4)、 NIST.800-53.r5 SC-7(9)、 PCI DSS v3.2.1/1.2.1、 PCI DSS v3.2.1/1.3.1、 PCI DSS v3.2.1/1.3.2、 PCI DSS v3.2.1/1.3.4、 PCI DSS v3.2.1/1.3.6、 PCI DSS v4.0.1/1.4.4

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ : `AWS::::Account`

AWS Config ルール : s3-account-level-public-access-blocks-periodic

スケジュールタイプ : 定期的

パラメータ :

- `ignorePublicAcls`: `true` (カスタマイズ不可)
- `blockPublicPolicy`: `true` (カスタマイズ不可)
- `blockPublicAcls`: `true` (カスタマイズ不可)
- `restrictPublicBuckets`: `true` (カスタマイズ不可)

このコントロールは、前の Amazon S3 パブリックアクセス設定が S3 汎用バケットのアカウントレベルで設定されているかどうかをチェックします: 1 つ以上のブロックパブリックアクセス設定が `false` に設定されている場合、このコントロールは失敗します。

いずれかの設定が `false` に設定されているか、またはいずれかが設定されていない場合、コントロールは失敗します。

Amazon S3 パブリックアクセスブロックは、オブジェクトがパブリックアクセスを持たないように、 全体 AWS アカウント または個々の S3 バケットレベルでコントロールを提供するように設計されています。パブリックアクセスは、アクセスコントロールリスト (ACL)、バケットポリシー、またはその両方からバケットおよびオブジェクトに付与されます。

S3 バケットをパブリックにアクセスできるように意図する場合を除き、アカウントレベルの Amazon S3 ブロックパブリックアクセス機能を設定する必要があります。

詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 ブロックパブリックアクセスの使用」を参照してください。

修正

の Amazon S3 パブリックアクセスブロックを有効にするには AWS アカウント、「Amazon Simple Storage Service ユーザーガイド」の「アカウントのパブリックアクセスブロック設定の構成」を参照してください。

[S3.2] S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.6、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5

AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 非常事態

リソースタイプ : `AWS::S3::Bucket`

AWS Config ルール : s3-bucket-public-read-prohibited

スケジュールタイプ: 定期的および変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon S3 汎用バケットがパブリック読み取りアクセスを許可するかどうかをチェックします。これにより、ブロックパブリックアクセス設定、バケットポリシー、およびバケットアクセスコントロールリスト (ACL) を評価します。バケットが公開読み取りアクセスを許可している場合、このコントロールは失敗します。

> **Note**
>
> S3 バケットにバケットポリシーがある場合、このコントロールはワイルドカード文字または変数を使用するポリシー条件を評価しません。PASSED 結果を生成するには、バケットポリシーの条件は固定値のみを使用する必要があります。固定値は、ワイルドカード文字やポリシー変数を含まない値です。ポリシー変数の詳細については、「 AWS Identity and Access Management ユーザーガイド」の「変数とタグ」を参照してください。

ユースケースによっては、インターネット上のすべてのユーザーが S3 バケットからの読み取りが必要な場合があります。しかし、そのような状況は稀です。データの整合性とセキュリティを確保するために、S3 バケットをパブリックに読み取り可能にしないでください。

修正

Amazon S3 バケットで公開読み取りアクセスをブロックするには、「Amazon Simple Storage Service ユーザーガイド」の「S3 バケットのブロックパブリックアクセス設定の構成」を参照してください。

[S3.3] S3 汎用バケットではパブリック書き込みアクセスをブロックする必要があります。

関連する要件: PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 非常事態

リソースタイプ : `AWS::S3::Bucket`

AWS Config ルール : s3-bucket-public-write-prohibited

スケジュールタイプ: 定期的および変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon S3 汎用バケットがパブリック書き込みアクセスを許可するかどうかをチェックします。これにより、ブロックパブリックアクセス設定、バケットポリシー、およびバケットアクセスコントロールリスト (ACL) を評価します。バケットが公開書き込みアクセスを許可している場合、このコントロールは失敗します。

> **Note**
>
> S3 バケットにバケットポリシーがある場合、このコントロールはワイルドカード文字または変数を使用するポリシー条件を評価しません。PASSED 結果を生成するには、バケットポリシーの条件は固定値のみを使用する必要があります。固定値は、ワイルドカード文字やポリシー変数を含まない値です。ポリシー変数の詳細については、「 AWS Identity and Access Management ユーザーガイド」の「変数とタグ」を参照してください。

ユースケースによっては、インターネット上の全員が S3 バケットに書き込むことができる必要があります。しかし、そのような状況は稀です。データの整合性とセキュリティを確保するため、S3 バケットはパブリックに書き込み可能にしないでください。

修正

Amazon S3 バケットで公開書き込みアクセスをブロックするには、「Amazon Simple Storage Service ユーザーガイド」の「S3 バケットのブロックパブリックアクセス設定の構成」を参照してください。

[S3.5] S3 汎用バケットではリクエストに SSL を使用する必要があります。

関連する要件： CIS AWS Foundations Benchmark v3.0.0/2.1.1、CIS AWS Foundations Benchmark v1.4.0/2.1.2、NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23SC-23(3)、NIST.800-53.r5 SC-7(4)NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 NIST.800-53.r5 SC-8 SI-7 3.13.15

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::S3::Bucket`

AWS Config ルール : s3-bucket-ssl-requests-only

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon S3 汎用バケットに SSL を使用するためのリクエストを要求するポリシーがあるかどうかをチェックします。バケットポリシーが SSL を使用するリクエストを必要としない場合、コントロールは失敗します。

S3 バケットには、条件キー `aws:SecureTransport` によって示される S3 リソースポリシーで HTTPS 経由のデータ送信のみを受け入れるために、すべてのリクエスト (`Action: S3:*`) を要求するポリシーを備える必要があります。

修正

Amazon S3 バケットポリシーを更新して非セキュアなトランスポートを拒否するには、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 コンソールを使用したバケットポリシーの追加」を参照してください。

以下のポリシーに、同様のポリシーステートメントを追加します。`amzn-s3-demo-bucket` を変更するバケットの名前で置き換えます。

JSON

```
{
    "Id": "ExamplePolicy",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "Bool": {
                     "aws:SecureTransport": "false"
                }
            },
           "Principal": "*"
        }
    ]
}
```

詳細については、 AWS 公式ナレッジセンターの「ルール AWS Config sS3-bucket-ssl-requests-only に準拠するためにどの S3 バケットポリシーを使用すればよいですか？」を参照してください。

[S3.6] S3 汎用バケットポリシーは、他の へのアクセスを制限する必要があります AWS アカウント

関連する要件： NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-171.r2 3.13.4

カテゴリ: 保護 > セキュアなアクセス管理 > 機密性の高いAPIオペレーションアクションを制限する

重要度: 高

リソースタイプ : `AWS::S3::Bucket`

AWS Configルール : s3-bucket-blacklisted-actions-prohibited

スケジュールタイプ: 変更がトリガーされた場合

パラメータ :

- `blacklistedactionpatterns`: `s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl` (カスタマイズ不可)

このコントロールは、Amazon S3 汎用バケットポリシーが別の AWS アカウント からのプリンシパルが、S3 バケット内のリソースに対して拒否されたアクションの実行を防止するかどうかをチェックします。バケットポリシーで、別の AWS アカウントのプリンシパルに対して前のいずれかのアクションが許可されている場合、このコントロールは失敗します。

最小特権アクセスの実装は、セキュリティリスクおよびエラーの影響や悪意ある行動を減らす上での基礎となります。もしS3 バケットポリシーで外部アカウントからのアクセスを許可している場合、内部脅威または攻撃者によるデータの漏えいにつながる可能性があります。

`blacklistedactionpatterns` パラメータを使用すると、S3 バケットのルールを正常に評価できます。パラメータは、外部アカウントに対して `blacklistedactionpatterns` リストに含まれていないアクションパターンのアクセス許可を付与します。

修正

Amazon S3 バケットポリシーを更新してアクセス許可を削除するには、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 コンソールを使用したバケットポリシーの追加」を参照してください。

[バケットポリシーを編集] ページのポリシー編集テキストボックスで、以下のいずれかのアクションを実行します。

- 拒否されたアクションへのアクセス許可を別の AWS アカウント に付与するステートメントを削除する。
- 許可済みの拒否されたアクションをステートメントから削除する。

[S3.7] S3 汎用バケットでクロスリージョンレプリケーションを使用する必要があります

関連する要件: PCI DSS v3.2.1/2.2、NIST.800-53.r5 AU-9(2)、NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-36(2)、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 低

リソースタイプ : `AWS::S3::Bucket`

AWS Config ルール: s3-bucket-cross-region-replication-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは Amazon S3 バケット 汎用バケットでクロスリージョンレプリケーションが有効かどうかをチェックします。バケットでクロスリージョンレプリケーションが有効になっていない場合、このコントロールは失敗します。

レプリケーションとは、同じまたは異なるバケット間でオブジェクトを自動的に非同期コピーすることです AWS リージョン。レプリケーションは、新しく作成されたオブジェクトと、レプリケート元バケットからレプリケート先バケットへのオブジェクトの更新をコピーします。 AWS ベストプラクティスでは、同じ AWS アカウント が所有するレプリケート元バケットとレプリケート先バケットのレプリケーションを推奨しています。可用性に加えて、他のシステム強化構成も考慮する必要があります。

このコントロールは、リージョン間のレプリケーションが有効になっていない場合、レプリケーション先バケット `FAILED` の検出結果を生成します。送信先バケットでクロスリージョンレプリケーションを有効にする必要がない正当な理由がある場合は、このバケットの検出結果を抑制できます。

修正

Amazon S3 バケットのレプリケーションを有効にするには、「Amazon Simple Storage Service ユーザーガイド」の「同じアカウントが所有するレプリケート元バケットとレプリケート先バケットのレプリケーションの設定」を参照してください。[ソースバケット] で、[バケット内のすべてのオブジェクトに適用] を選択します。

[S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/2.1.4、CIS AWS Foundations Benchmark v1.4.0/2.1.5、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7NIST.800-53.r5 SC-7(1)、NIST.800-53.r5 SC-73(1) NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7

カテゴリ: 保護 > セキュアなアクセス管理 > アクセスコントロール

重要度: 高

リソースタイプ : `AWS::S3::Bucket`

AWS Config ルール : s3-bucket-level-public-access-prohibited

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

- `excludedPublicBuckets` (カスタマイズ不可) - 既知の許可されているパブリック S3 バケット名のカンマ区切りリスト

このコントロールは、Amazon S3 汎用バケットがバケットレベルでパブリックアクセスをブロックするかどうかをチェックします。次の設定のいずれかが `false` に設定されている場合、コントロールは失敗します。

- `ignorePublicAcls`
- `blockPublicPolicy`
- `blockPublicAcls`
- `restrictPublicBuckets`

S3 バケットレベルのブロックパブリックアクセスは、オブジェクトがパブリックアクセスできないようにコントロールを提供します。パブリックアクセスは、アクセスコントロールリスト (ACL)、バケットポリシー、またはその両方からバケットおよびオブジェクトに付与されます。

S3 バケットをパブリックにアクセスできるように意図する場合を除き、バケットレベルの Amazon S3 ブロックパブリックアクセス機能を設定する必要があります。

修正

バケットレベルでパブリックアクセスを削除する方法については、「Amazon S3 ユーザーガイド」の「Amazon S3 ストレージへのパブリックアクセスのブロック」を参照してください。

[S3.9] S3 汎用バケットは、サーバーアクセスログ記録を有効にする必要があります

関連する要件： NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53AU-6.r5 CA-7、NIST.800-53.r5 SC-7(7) SI-3 SI-4 SI-710.2.1

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::S3::Bucket`

AWS Config ルール : s3-bucket-logging-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon S3 汎用バケットでサーバーアクセスログ記録が有効になっているかどうかをチェックします。サーバーアクセスのログ記録が有効になっていない場合、コントロールは失敗します。ログ記録を有効にすると、Amazon S3 は、ソースバケットのアクセスログを選択されたターゲットバケットに配信します。ターゲットバケットはソースバケット AWS リージョン と同じ にある必要があり、デフォルトの保持期間を設定してはいけません。ターゲットのログ記録バケットは、サーバーアクセスのログ記録を有効にする必要がないため、このバケットの結果は非表示にします。

サーバーアクセスのログ記録には、バケットに対するリクエストの詳細を提供します。サーバーアクセスログは、セキュリティとアクセス監査に役立ちます。詳細については、「Amazon S3 のセキュリティベストプラクティス: Amazon S3 サーバーアクセスログを有効にします」を参照してください。

修正

Amazon S3 のサーバーアクセスのログ記録を有効にするには、「Amazon S3 ユーザーガイド」の「Amazon S3 サーバーアクセスログの有効化」を参照してください。

[S3.10] バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::S3::Bucket`

AWS Config ルール : s3-version-lifecycle-policy-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon S3 汎用バージョニングバケットにライフサイクル設定があるかどうかをチェックします。バケットにライフサイクル設定がない場合、コントロールは失敗します。

オブジェクトの存続期間中に Amazon S3 で実行するアクションの定義に役立てるため、S3 バケットにライフサイクル設定を作成することを推奨します。

修正

Amazon S3 バケットでのライフサイクルの設定の詳細については、「バケットのライフサイクル設定の指定」と「ストレージのライフサイクルの管理」を参照してください。

[S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります

関連する要件： NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-4(4)、NIST.800-171.r2 3.3.8

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::S3::Bucket`

AWS Config ルール : s3-event-notifications-enabled

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`eventTypes`	推奨される S3 イベントタイプのリスト	EnumList (最大 28 項目)	`s3:IntelligentTiering`, `s3:LifecycleExpiration:*`, `s3:LifecycleExpiration:Dele`	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
			te, s3:LifecycleExpiration:DeleteMarkerCreated, s3:LifecycleTransition, s3:ObjectAcl:Put, s3:ObjectCreated:*, s3:ObjectCreated:CompleteMultipartUpload, s3:ObjectCreated:Copy, s3:ObjectCreated:Post, s3:ObjectCreated:Put, s3:ObjectRemoved:*, s3:Object	

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
			Removed:Delete, s3:ObjectRemoved:DeleteMarkerCreated, s3:ObjectRestore:*, s3:ObjectRestore:Completed, s3:ObjectRestore:Delete, s3:ObjectRestore:Post, s3:ObjectTagging:*, s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject,	

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
			s3:Replication:*, s3:Replication:OperationFailedReplication, s3:Replication:OperationMissedThreshold, s3:Replication:OperationNotTracked, s3:Replication:OperationReplicatedAfterThreshold, s3:TestEvent	

このコントロールは、S3 イベント通知が Amazon S3 汎用バケットで有効になっているかどうかをチェックします。バケットで S3 イベント通知が有効になっていない場合、コントロールは失敗します。`eventTypes` パラメータにカスタム値を指定したときは、指定されたタイプのイベントに対してイベント通知が有効になっている場合にのみコントロールが成功します。

S3 イベント通知を有効にすると、S3 バケットに影響する特定のイベントが発生したときに、アラートを受信します。例えば、オブジェクトの作成、オブジェクトの削除、オブジェクトの復元を通知を

受けることができます。これらの通知により、不正なデータアクセスにつながる可能性のある偶発的または意図的な変更を関連チームに警告することができます。

修正

S3 バケットおよびオブジェクトの変更を、検出する方法の詳細については、「Amazon S3 ユーザーガイド」の「Amazon S3 イベント通知」を参照してください。

[S3.12] ACL は、S3 汎用バケットへのユーザーアクセスの管理に使用しないでください。

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

カテゴリ: 保護 > セキュアなアクセス管理 > アクセスコントロール

重要度: 中

リソースタイプ : `AWS::S3::Bucket`

AWS Config ルール : s3-bucket-acl-prohibited

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon S3 汎用バケットがアクセスコントロールリスト (ACL) を持つユーザーアクセス許可を提供するかどうかをチェックします。バケットでのユーザーアクセスを管理するために ACL が設定されている場合、コントロールは失敗します。

ACL は、IAM よりも前のレガシーアクセスコントロールメカニズムです。ACLs の代わりに、S3 バケットポリシーまたは AWS Identity and Access Management (IAM) ポリシーを使用して S3 バケットへのアクセスを管理することをお勧めします。

修正

このコントロールに合格するには、S3 バケットの ACL を無効にする必要があります。手順については、「Amazon Simple Storage Service ユーザーガイド」の「オブジェクトの所有権の制御とバケットの ACL の無効化」を参照してください。

S3 バケットポリシーを作成するには、「Amazon S3 コンソールを使用したバケットポリシーの追加」を参照してください。S3 バケットに IAM ユーザーポリシーを作成するには、「ユーザーポリシーを使用したバケットへのアクセスの制御」を参照してください。

[S3.13] S3 汎用バケットにはライフサイクル設定が必要です

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

カテゴリ: 保護 > データ保護

重要度: 低

リソースタイプ : `AWS::S3::Bucket`

AWS Config ルール : s3-lifecycle-policy-check

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`targetTransitionDays`	オブジェクトが、その作成後、指定されたストレージクラスに移行するまでの日数	整数	`1~36500`	デフォルト値なし
`targetExpirationDays`	オブジェクトが作成されてから削除されるまでの日数	整数	`1~36500`	デフォルト値なし
`targetTransitionStorageClass`	送信先 S3 ストレージクラスのタイプ	列挙型	`STANDARD_IA, INTELLIGENT_TIERING, ONEZONE_IA, GLACIER, GLACIER_IR,`	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
			`DEEP_ARCHIVE`	

このコントロールは、Amazon S3 汎用バケットにライフサイクル設定があるかどうかをチェックします。バケットにライフサイクル設定がない場合、コントロールは失敗します。前述の 1 つ以上のパラメータにカスタム値を指定したときは、指定されたストレージクラス、削除時間、または移行時間がポリシーに含まれている場合にのみコントロールが成功します。

S3 バケットでライフサイクル設定を作成すると、オブジェクトの存続期間中に Amazon S3 が実行するアクションが定義されます。例えば、オブジェクトを別のストレージクラスに移行させる、アーカイブする、あるいは指定した期間後に削除する、といったことが可能です。

修正

Amazon S3 バケットでライフサイクルポリシーを設定する方法の詳細については、「Amazon S3 ユーザーガイド」の「バケットのライフサイクル設定の指定」および「ストレージのライフサイクルの管理」を参照してください。

[S3.14] S3 汎用バケットではバージョニングが有効になっている必要があります

カテゴリ: 保護 > データ保護 > データ削除保護

関連する要件： NIST.800-53.r5 AU-9(2)、NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)、NIST.800-171.r2 3.8

重要度: 低

リソースタイプ : `AWS::S3::Bucket`

AWS Config ルール : s3-bucket-versioning-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon S3 汎用バケットでバージョニングが有効になっているかどうかを確認します。バケットのバージョニングが停止されている場合、コントロールは失敗します。

バージョニングにより、同じ S3 バケット内でオブジェクトの複数のバリアントを保持します。バージョニングを使用して、S3 バケットに保存されたオブジェクトの旧バージョンを保存、取得、復元することができます。バージョニングによって、意図しないユーザーアクションとアプリケーション障害から復旧できます。

> **Tip**
> バージョニングによるバケット内オブジェクト数の増加に合わせて、ルールに基づき、バージョニングされたオブジェクトを自動的にアーカイブまたは削除するようにライフサイクル設定をセットアップできます。詳細については、「バージョニングされたオブジェクトの Amazon S3 ライフサイクル管理」を参照してください。

修正

S3 バケットでバージョニングを使用するには、「Amazon S3 ユーザーガイド」の「バケットでのバージョニングの有効化」を参照してください。

[S3.15] S3 汎用バケットでは Object Lock が有効になっている必要があります

カテゴリ: 保護 > データ保護 > データ削除保護

関連する要件： NIST.800-53.r5 CP-6(2)、PCI DSS v4.0.1/10.5.1

重要度: 中

リソースタイプ : `AWS::S3::Bucket`

AWS Config ルール : s3-bucket-default-lock-enabled

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`mode`	S3 Object Lock の保持モード	列挙型	`GOVERNANCE` ,	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
			`COMPLIANCE`	

このコントロールは、Amazon S3 汎用バケットで Object Lock が有効になっているかどうかを確認します。バケットで Object Lock が有効になっていない場合、コントロールは失敗します。`mode` パラメータにカスタム値を指定したときは、S3 Object Lock が指定された保持モードを使用する場合にのみコントロールが成功します。

S3 Object Lock では、Write Once Read Many (WORM) モデルを使用してオブジェクトを保存できます。Object Lock により、S3 バケットのオブジェクトが削除または上書きされることを、一定期間または無期限に防止できます。S3 Object Lock を使用して、WORM ストレージを必要とする規制要件を満たしたり、オブジェクトの変更や削除に対する保護レイヤーを追加したりできます。

修正

新規および既存の S3 バケットの Object Lock を設定するには、「Amazon S3 ユーザーガイド」の「オブジェクトロックの設定」を参照してください。

[S3.17] S3 汎用バケットは保管時に で暗号化する必要があります AWS KMS keys

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

関連する要件： NIST.800-53.r5 SC-12(2)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 SI-7(6)、NIST.800-53.r5 AU-9、NIST.800-171.r2 3.8.9、NIST.80 3.13.11 3.13.160

重要度: 中

リソースタイプ : `AWS::S3::Bucket`

AWS Config ルール : s3-default-encryption-kms

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon S3 汎用バケットが AWS KMS key (SSE-KMS または DSSE-KMS) で暗号化されているかどうかをチェックします。バケットがデフォルトの暗号化 (SSE-S3) で暗号化されている場合、コントロールは失敗します。

サーバー側の暗号化 (SSE)とは、データを受信するアプリケーションまたはサービスによって、送信先でデータを暗号化することです。特に指定しない限り、デフォルトでは、S3 バケットはサーバー側の暗号化に Amazon S3 マネージドキー (SSE-S3) を使用します。ただし、コントロールを強化するために、代わりに AWS KMS keys (SSE-KMS または DSSE-KMS) でサーバー側の暗号化を使用するようにバケットを設定することもできます。Amazon S3 は、 AWS データセンターのディスクに書き込むときにオブジェクトレベルでデータを暗号化し、アクセス時に復号します。

修正

SSE-KMS を使用して S3 バケットを暗号化するには、Amazon S3 ユーザーガイド」の AWS KMS「 (SSE-KMS) を使用したサーバー側の暗号化の指定」を参照してください。DSSE-KMS を使用して S3 バケットを暗号化するには、Amazon S3 ユーザーガイド」の AWS KMS keys 「(DSSE-KMS) を使用した二層式サーバー側の暗号化の指定」を参照してください。

[S3.19] S3 アクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります

関連する要件： NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7NIST.800-53.r5 SC-70-53.r5 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7r

カテゴリ: 保護 > セキュアなアクセス管理 > パブリックアクセスが不可能なリソース

重要度: 非常事態

リソースタイプ : `AWS::S3::AccessPoint`

AWS Config ルール : s3-access-point-public-access-blocks

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon S3 アクセスポイントでブロックパブリックアクセス設定が有効になっているかどうかをチェックします。アクセスポイントのブロックパブリックアクセス設定が有効になっていない場合、コントロールは失敗します。

Amazon S3 パブリックアクセスブロック機能は、アカウント、バケット、アクセスポイントの 3 つのレベルで S3 リソースへのアクセスを管理するのに役立ちます。各レベルの設定は個別に構成できるため、データに対して異なるレベルのパブリックアクセス制限を設定できます。アクセスポイントの設定で、より高いレベル (アカウントレベルまたはアクセスポイントに割り当てられたバケット) のより制限的な設定を個別にオーバーライドすることはできません。むしろ、アクセスポイントレベルの設定は付加的です。つまり、他のレベルの設定を補完し、連携して機能します。S3 アクセスポイントをパブリックにアクセス可能にする予定がない限り、ブロックパブリックアクセス設定を有効にする必要があります。

修正

Amazon S3 は、現在、アクセスポイントの作成後におけるアクセスポイントのブロックパブリックアクセス設定の変更をサポートしていません。デフォルトでは、新しいアクセスポイントを作成すると、すべてのブロックパブリックアクセス設定が有効になります。これらの設定を特に無効にする必要がある場合を除いて、すべての設定を有効にしておくことをお勧めします。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「アクセスポイントへのパブリックアクセスの管理」を参照してください。

[S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/2.1.2、CIS AWS Foundations Benchmark v1.4.0/2.1.3、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

カテゴリ: 保護 > データ保護 > データ削除保護

重要度: 低

リソースタイプ : `AWS::S3::Bucket`

AWS Config ルール : s3-bucket-mfa-delete-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon S3 汎用バケットで多要素認証 (MFA) 削除が有効になっているかどうかを確認します。バケットに対して MFA 削除が有効になっていない場合、コントロールは失敗します。コントロールは、ライフサイクル設定を持つバケットの検出結果を生成しません。

S3 汎用バケットのバージョニングを有効にする場合は、オプションでバケットの MFA 削除を設定することで、別のセキュリティレイヤーを追加できます。これを行う場合、バケット所有者は、バ

ケット内のオブジェクトのバージョンを削除するか、バケットのバージョニング状態を変更するリクエストに 2 つの形式の認証を含める必要があります。MFA 削除は、バケット所有者のセキュリティ認証情報が侵害された場合などに、セキュリティを強化します。MFA 削除は、削除アクションを開始したユーザーに MFA コードを使用して MFA デバイスの物理的な所有を証明するように要求することで、バケットの偶発的な削除を防ぐのにも役立ちます。これにより、削除アクションに摩擦とセキュリティのレイヤーが追加されます。

> **Note**
>
> このコントロールは、S3 汎用バケットで MFA 削除が有効になっている場合にのみ検出PASSED結果を生成します。バケットの MFA 削除を有効にするには、バケットのバージョニングも有効にする必要があります。バケットバージョニングは、S3 オブジェクトの複数のバリエーションを同じバケットに保存する方法です。さらに、ルートユーザーとしてログインしているバケット所有者のみが MFA 削除を有効にし、バケットに対して削除アクションを実行できます。ライフサイクル設定を持つバケットで MFA 削除を使用することはできません。

修正

S3 バケットのバージョニングの有効化と MFA 削除の設定については、「Amazon Simple Storage Service ユーザーガイド」の「MFA 削除の設定」を参照してください。

[S3.22] S3 汎用バケットはオブジェクトレベルの書き込みイベントをログに記録する必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/3.8、PCI DSS v4.0.1/10.2.1

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::::Account`

AWS Config ルール : cloudtrail-all-write-s3-data-event-check

スケジュールタイプ : 定期的

パラメータ : なし

このコントロール AWS アカウント は、 に Amazon S3 バケットのすべての書き込みデータイベントを記録する AWS CloudTrail マルチリージョン証跡が少なくとも 1 つあるかどうかをチェックしま

す。 Amazon S3 S3 バケットの書き込みデータイベントをログに記録するマルチリージョン証跡がアカウントに存在しない場合、コントロールは失敗します。

`GetObject`、`DeleteObject`、`PutObject` などの S3 オブジェクトレベルのオペレーションは、データイベントと呼ばれます。デフォルトでは、CloudTrail はデータイベントを記録しませんが、S3 バケットのデータイベントを記録するように証跡を設定できます。書き込みデータイベントのオブジェクトレベルのログ記録を有効にすると、S3 バケット内の個々のオブジェクト (ファイル) アクセスをログ記録できます。オブジェクトレベルのログ記録を有効にすると、Amazon CloudWatch Events を使用して、データコンプライアンス要件を満たし、包括的なセキュリティ分析を実行し、 のユーザー動作の特定のパターンをモニタリングし AWS アカウント、S3 バケット内のオブジェクトレベルの API アクティビティに対してアクションを実行できます。このコントロールは、すべての S3 バケットの書き込み専用またはすべてのタイプのデータイベントを記録するマルチリージョン証跡を設定すると、`PASSED` 検出結果を生成します。

修正

S3 バケットのオブジェクトレベルのログ記録を有効にするには、「Amazon Simple Storage Service ユーザーガイド」の「S3 バケットとオブジェクトの CloudTrail イベントログ記録の有効化」を参照してください。

[S3.23] S3 汎用バケットはオブジェクトレベルの読み取りイベントをログに記録する必要があります

関連する要件： CIS AWS Foundations Benchmark v3.0.0/3.9、PCI DSS v4.0.1/10.2.1

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::::Account`

AWS Config ルール : cloudtrail-all-read-s3-data-event-check

スケジュールタイプ : 定期的

パラメータ : なし

このコントロール AWS アカウント は、 に Amazon S3 バケットのすべての読み取りデータイベントを記録する AWS CloudTrail マルチリージョン証跡が少なくとも 1 つあるかどうかをチェックします。 Amazon S3 S3 バケットの読み取りデータイベントをログに記録するマルチリージョン証跡がアカウントにない場合、コントロールは失敗します。

`GetObject`、`DeleteObject`、`PutObject` などの S3 オブジェクトレベルのオペレーションは、データイベントと呼ばれます。デフォルトでは、CloudTrail はデータイベントを記録しませんが、S3 バケットのデータイベントを記録するように証跡を設定できます。読み取りデータイベントのオブジェクトレベルのログ記録を有効にすると、S3 バケット内の個々のオブジェクト (ファイル) アクセスをログ記録できます。オブジェクトレベルのログ記録を有効にすると、Amazon CloudWatch Events を使用して、データコンプライアンス要件を満たし、包括的なセキュリティ分析を実行し、 のユーザー動作の特定のパターンをモニタリングし AWS アカウント、S3 バケット内のオブジェクトレベルの API アクティビティに対してアクションを実行できます。このコントロールは、すべての S3 バケットの読み取り専用またはすべてのタイプのデータイベントを記録するマルチリージョン証跡を設定すると、`PASSED` 検出結果を生成します。

修正

S3 バケットのオブジェクトレベルのログ記録を有効にするには、「Amazon Simple Storage Service ユーザーガイド」の「S3 バケットとオブジェクトの CloudTrail イベントログ記録の有効化」を参照してください。

[S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります

関連する要件： PCI DSS v4.0.1/1.4.4

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 高

リソースタイプ : `AWS::S3::MultiRegionAccessPoint`

AWS Config ルール: `s3-mrap-public-access-blocked` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon S3 マルチリージョンアクセスポイントでブロックパブリックアクセス設定が有効になっているかどうかをチェックします。マルチリージョンアクセスポイントでブロックパブリックアクセス設定が有効になっていない場合、コントロールは失敗します。

パブリックにアクセス可能なリソースは、不正アクセス、データ侵害、または脆弱性の悪用につながる可能性があります。認証および認可手段によるアクセスの制限は、機密情報を保護し、リソースの整合性を維持するのに役立ちます。

修正

デフォルトでは、S3 マルチリージョンアクセスポイントに対してすべてのブロックパブリックアクセス設定が有効になります。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 マルチリージョンアクセスポイントによるパブリックアクセスのブロック」を参照してください。マルチリージョンアクセスポイントを作成した後にブロックパブリックアクセス設定を変更することはできません。

[S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です

カテゴリ： 保護 > データ保護

重要度: 低

リソースタイプ : `AWS::S3Express::DirectoryBucket`

AWS Config ルール : s3express-dir-bucket-lifecycle-rules-check

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`targetExpirationDays`	オブジェクトの作成後、オブジェクトの有効期限が切れる日数。	整数	`1 ~ 2147483647`	デフォルト値なし

このコントロールは、S3 ディレクトリバケットにライフサイクルルールが設定されているかどうかを確認します。ディレクトリバケットにライフサイクルルールが設定されていない場合、またはバケットのライフサイクルルールでオプションで指定したパラメータ値と一致しない有効期限設定が指定されている場合、コントロールは失敗します。

Amazon S3 では、ライフサイクル設定は、バケット内のオブジェクトのグループに適用する Amazon S3 のアクションを定義する一連のルールです。S3 ディレクトリバケットの場合、経過時間 (日数) に基づいてオブジェクトの有効期限を指定するライフサイクルルールを作成できます。不完全なマルチパートアップロードを削除するライフサイクルルールを作成することもできます。汎用バケットなどの他のタイプの S3 バケットとは異なり、ディレクトリバケットは、ストレージクラス間

でオブジェクトを移行するなど、ライフサイクルルールの他のタイプのアクションをサポートしていません。

修正

S3 ディレクトリバケットのライフサイクル設定を定義するには、バケットのライフサイクルルールを作成します。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「ディレクトリバケットのライフサイクル設定の作成と管理」を参照してください。

SageMaker AI の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon SageMaker AI サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります

関連する要件： NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7NIST.800-53.r5 SC-7.r5 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7r

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 高

リソースタイプ : `AWS::SageMaker::NotebookInstance`

AWS Config ルール : sagemaker-notebook-no-direct-internet-access

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、SageMaker AI ノートブックインスタンスで直接インターネットアクセスが無効になっているかどうかをチェックします。ノートブックインスタンスで `DirectInternetAccess` フィールドが有効になっている場合、コントロールは失敗します。

VPC なしで SageMaker AI インスタンスを設定すると、デフォルトでインスタンスで直接インターネットアクセスが有効になります。VPC ありでインスタンスを設定し、デフォルト設定を [無効化 - VPC 経由でインターネットにアクセスする] に変更する必要があります。ノートブックからモデルをトレーニングまたはホストするには、インターネットアクセスが必要です。インターネットアクセ

スを有効にするには、VPC にインターフェイスエンドポイント (AWS PrivateLink) または NAT ゲートウェイ、およびアウトバウンド接続を許可するセキュリティグループが必要です。ノートブックインスタンスを VPC 内のリソースに接続する方法の詳細については、Amazon SageMaker AI デベロッパーガイド」の「VPC 内のリソースにノートブックインスタンスを接続する」を参照してください。また、SageMaker AI 設定へのアクセスが承認されたユーザーのみに制限されていることを確認する必要があります。SageMaker AI の設定とリソースの変更をユーザーに許可する IAM アクセス許可を制限します。

修正

ノートブックインスタンスを作成した後は、インターネットアクセスの設定を変更することはできません。代わりに、インターネットアクセスがブロックされているインスタンスを停止して削除し、再作成できます。直接インターネットアクセスを許可するノートブックインスタンスを削除するには、Amazon SageMaker AI デベロッパーガイド」の「ノートブックインスタンスを使用してモデルを構築する: クリーンアップ」を参照してください。インターネットアクセスを拒否するノートブックインスタンスを再作成するには、「ノートブックインスタンスを作成する」を参照してください。[ネットワーク] の [直接インターネットアクセス] で、[無効化 - VPC 経由でインターネットにアクセスする] を選択します。

[SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > VPC 内のリソース

重要度: 高

リソースタイプ : `AWS::SageMaker::NotebookInstance`

AWS Config ルール : sagemaker-notebook-instance-inside-vpc

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon SageMaker AI ノートブックインスタンスがカスタム Virtual Private Cloud (VPC) 内で起動されているかどうかを確認します。SageMaker AI ノートブックインスタンス

がカスタム VPC 内で起動されない場合、または SageMaker AI サービス VPC で起動された場合、このコントロールは失敗します。

サブネットは、ある範囲の IP アドレスが示す VPC 内の領域です。インフラストラクチャの安全なネットワーク保護を確保するために、リソースは可能な限りカスタム VPC 内に保管することをお勧めします。Amazon VPC は、 専用の仮想ネットワークです AWS アカウント。Amazon VPC を使用すると、SageMaker AI Studio インスタンスとノートブックインスタンスのネットワークアクセスとインターネット接続を制御できます。

修正

ノートブックインスタンスを作成した後は、VPC の設定を変更することはできません。代わりに、インスタンスを停止して削除し、再作成できます。手順については、Amazon SageMaker AI デベロッパーガイド」の「ノートブックインスタンスを使用してモデルを構築する: クリーンアップ」を参照してください。

[SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(10)、NIST.800-53.r5 AC-6(2)

カテゴリ: 保護 > セキュアなアクセス管理 > ルートユーザーのアクセス制限

重要度: 高

リソースタイプ : `AWS::SageMaker::NotebookInstance`

AWS Config ルール : sagemaker-notebook-instance-root-access-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon SageMaker AI ノートブックインスタンスのルートアクセスが有効になっているかどうかを確認します。SageMaker AI ノートブックインスタンスのルートアクセスが有効になっている場合、コントロールは失敗します。

最小特権のプリンシパルに従い、意図せずに権限を過剰にプロビジョニングしないために、ルートアクセスをインスタンスリソースに制限することが、推奨されるセキュリティ上のベストプラクティスです。

修正

SageMaker AI ノートブックインスタンスへのルートアクセスを制限するには、「Amazon SageMaker AI デベロッパーガイド」の「SageMaker AI ノートブックインスタンスへのルートアクセスを制御する」を参照してください。 Amazon SageMaker

[SageMaker.4] SageMaker エンドポイントの本番稼働バリアントの初期インスタンス数は 1 より大きい必要があります

関連する要件: NIST.800-53.r5 CP-10、NIST.800-53.r5 SC-5、NIST.800-53.r5 SC-36、NIST.800-53.r5 SA-13

カテゴリ: リカバリ > 耐障害性 > 高可用性

重要度: 中

リソースタイプ : `AWS::SageMaker::EndpointConfig`

AWS Config ルール : sagemaker-endpoint-config-prod-instance-count

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、Amazon SageMaker AI エンドポイントの本番稼働用バリアントの初期インスタンス数が 1 より大きいかどうかをチェックします。エンドポイントの本番稼働用バリアントの初期インスタンスが 1 つしかない場合、コントロールは失敗します。

インスタンス数が 1 を超える本番稼働用バリアントは、SageMaker AI によって管理されるマルチ AZ インスタンスの冗長性を許可します。複数のアベイラビリティーゾーンにリソースをデプロイすることは、アーキテクチャ内で高可用性を提供するための AWS ベストプラクティスです。高可用性は、セキュリティインシデントからの復旧に役立ちます。

> **Note**
>
> このコントロールは、インスタンスベースのエンドポイント設定にのみ適用されます。

修正

エンドポイント設定のパラメータの詳細については、Amazon SageMaker AI デベロッパーガイド」の「エンドポイント設定の作成」を参照してください。

[SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 中

リソースタイプ : `AWS::SageMaker::Model`

AWS Config ルール : sagemaker-model-isolation-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon SageMaker AI ホストモデルでネットワーク分離が有効になっているかどうかを確認します。ホストされたモデルの `EnableNetworkIsolation`パラメータが に設定されている場合、コントロールは失敗します`False`。

SageMaker AI トレーニングとデプロイされた推論コンテナは、デフォルトでインターネットに対応しています。SageMaker AI でトレーニングコンテナまたは推論コンテナへの外部ネットワークアクセスを提供したくない場合は、ネットワーク分離を有効にできます。ネットワーク分離を有効にすると、他の との呼び出しを含め、モデルコンテナとの間でインバウンドまたはアウトバウンドのネットワーク呼び出しを行うことはできません AWS のサービス。さらに、コンテナランタイム環境で使用できる AWS 認証情報はありません。ネットワーク分離を有効にすると、インターネットから SageMaker AI リソースへの意図しないアクセスを防ぐことができます。

> **Note**
>
> 2025 年 8 月 13 日、Security Hub はこのコントロールのタイトルと説明を変更しました。新しいタイトルと説明は、コントロールが Amazon SageMaker AI ホストモデルの `EnableNetworkIsolation`パラメータの設定をチェックしていることをより正確に反映しています。以前は、このコントロールのタイトルは でしたSageMaker models should block inbound traffic。

修正

SageMaker AI モデルのネットワーク分離の詳細については、Amazon SageMaker AI デベロッパーガイド」の「トレーニングコンテナと推論コンテナをインターネットフリーモードで実行する」を参

照してください。モデルを作成するときに、 `EnableNetworkIsolation`パラメータの値を に設定することで、ネットワーク分離を有効にできます`True`。

[SageMaker.6] SageMaker アプリのイメージ設定にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::SageMaker::AppImageConfig`

AWS Config ルール : sagemaker-app-image-config-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon SageMaker AI アプリイメージ設定 (`AppImageConfig`) に `requiredKeyTags`パラメータで指定されたタグキーがあるかどうかをチェックします。アプリケーションイメージ設定にタグキーがない場合、または `requiredKeyTags`パラメータで指定されたすべてのキーがない場合、コントロールは失敗します。`requiredKeyTags` パラメータの値を指定しない場合、コントロールはタグキーの存在のみをチェックし、アプリケーションイメージ設定にタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、 `aws:` プレフィックスが付いています。

タグは、 AWS リソースを作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの識別、整理、検索、フィルタリングに役立ちます。また、アクションと通知の

リソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセスコントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 Tagging AWS Resources and Tag Editor User Guide」を参照してください。

> **Note**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

Amazon SageMaker AI アプリイメージ設定 (`AppImageConfig`) にタグを追加するには、SageMaker AI API の AddTags オペレーションを使用するか、 を使用している場合は add-tags コマンド AWS CLIを実行します。

[SageMaker.7] SageMaker イメージにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::SageMaker::Image`

AWS Config ルール : sagemaker-image-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグ	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
	キーでは、大文字と小文字が区別されます。			

このコントロールは、Amazon SageMaker AI イメージに `requiredKeyTags`パラメータで指定されたタグキーがあるかどうかをチェックします。イメージにタグキーがない場合、または`requiredKeyTags`パラメータで指定されたすべてのキーがない場合、コントロールは失敗します。`requiredKeyTags` パラメータに値を指定しない場合、コントロールはタグキーの存在のみをチェックし、イメージにタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、 `aws:` プレフィックスが付いています。

タグは、 AWS リソースを作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの識別、整理、検索、フィルタリングに役立ちます。また、アクションと通知のリソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセスコントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 AWS リソースのタグ付け」および「タグエディタユーザーガイド」を参照してください。

> **Note**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

Amazon SageMaker AI イメージにタグを追加するには、SageMaker AI API の AddTags オペレーションを使用するか、 を使用している場合は add-tags コマンド AWS CLIを実行します。

[SageMaker.8] SageMaker ノートブックインスタンスは、サポートされているプラットフォームで実行する必要があります

カテゴリ: 検出 > 脆弱性、パッチ、バージョン管理

重要度: 中

リソースタイプ : `AWS::SageMaker::NotebookInstance`

AWS Config ルール : sagemaker-notebook-instance-platform-version

スケジュールタイプ : 定期的

パラメータ :

- `supportedPlatformIdentifierVersions`: `notebook-al2-v3` (カスタマイズ不可)

このコントロールは、ノートブックインスタンスに指定されたプラットフォーム識別子に基づいて、Amazon SageMaker AI ノートブックインスタンスがサポートされているプラットフォームで実行されるように設定されているかどうかを確認します。サポートされなくなったプラットフォームでノートブックインスタンスを実行するように設定されている場合、コントロールは失敗します。

Amazon SageMaker AI ノートブックインスタンスのプラットフォームがサポートされなくなった場合、セキュリティパッチ、バグ修正、またはその他のタイプの更新を受信しない可能性があります。ノートブックインスタンスは引き続き機能する可能性がありますが、SageMaker AI セキュリティ更新プログラムや重大なバグ修正は行われません。サポートされていないプラットフォームの使用に関連するリスクを引き受けます。詳細については、Amazon SageMaker AI デベロッパーガイド」のJupyterLab バージョニング」を参照してください。

修正

Amazon SageMaker AI が現在サポートしているプラットフォームとその移行方法については、「Amazon Amazon SageMaker Linux 2 ノートブックインスタンス」を参照してください。

Secrets Manager の Security Hub コントロール

これらの AWS Security Hub コントロールは、 AWS Secrets Manager サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[SecretsManager.1] Secrets Manager のシークレットは、自動ローテーションを有効にする必要があります

関連する要件： NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、PCI DSS v4.0.1/8.6.3、PCI DSS v4.0.1/8.3.9

カテゴリ: 保護 > セキュアな開発

重要度: 中

リソースタイプ : `AWS::SecretsManager::Secret`

AWS Config ルール : `secretsmanager-rotation-enabled-check`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`maximumAllowedRotationFrequency`	シークレットローテーション頻度の許容最大日数	整数	1 ~ 365	デフォルト値なし

このコントロール AWS Secrets Manager は、 に保存されているシークレットが自動ローテーションで設定されているかどうかを確認します。シークレットが自動ローテーションで構成されていない場合、コントロールは失敗します。`maximumAllowedRotationFrequency` パラメータにカスタム値を指定したときは、指定された時間帯内にシークレットが自動的にローテーションされた場合にのみコントロールが成功します。

Secrets Manager は、組織のセキュリティ体制を向上するのに役立ちます。シークレットとは、データベース認証情報、パスワード、サードパーティーの API キーなどが含まれます。Secrets Manager を使用することで、シークレットを一元的に保存、シークレットの自動暗号化、シークレットへのアクセスコントロール、シークレットを安全かつ自動的にローテーションすることができます。

Secrets Manager はシークレットをローテーションできます。ローテーションを使用して、長期のシークレットを短期のシークレッに置き換えることができます。シークレットをローテーションすることで、権限のないユーザーが侵害されたシークレットを使用できる期間を制限することができます。このため、シークレットは頻繁にローテーションする必要があります。ローテーションの詳細については、「 AWS Secrets Manager ユーザーガイド」の「シーAWS Secrets Manager クレットのローテーション」を参照してください。

修正

Secrets Manager シークレットの自動ローテーションを有効にするには、「 AWS Secrets Manager ユーザーガイド」の「コンソールを使用してシーク AWS Secrets Manager レットの自動ローテーションを設定する」を参照してください。ローテーションする AWS Lambda 関数を選択して設定する必要があります。

[SecretsManager.2] 自動ローテーションを設定した Secrets Manager のシークレットは正常にローテーションする必要があります

関連する要件： NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、PCI DSS v4.0.1/8.6.3、PCI DSS v4.0.1/8.3.9

カテゴリ: 保護 > セキュアな開発

重要度: 中

リソースタイプ : `AWS::SecretsManager::Secret`

AWS Config ルール : `secretsmanager-scheduled-rotation-success-check`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、ローテーションスケジュールに基づいて AWS Secrets Manager シークレットが正常にローテーションされたかどうかをチェックします。`RotationOccurringAsScheduled` が `false` の場合、コントロールは失敗します。コントロールは、ローテーションがオンになっているシークレットのみを評価します。

Secrets Manager は、組織のセキュリティ体制を向上するのに役立ちます。シークレットとは、データベース認証情報、パスワード、サードパーティーの API キーなどが含まれます。Secrets Manager を使用することで、シークレットを一元的に保存、シークレットの自動暗号化、シークレットへのアクセスコントロール、シークレットを安全かつ自動的にローテーションすることができます。

Secrets Manager はシークレットをローテーションできます。ローテーションを使用して、長期のシークレットを短期のシークレッに置き換えることができます。シークレットをローテーションすることで、権限のないユーザーが侵害されたシークレットを使用できる期間を制限することができます。このため、シークレットは頻繁にローテーションする必要があります。

シークレットが自動的にローテーションされるように設定することに加えて、これらのシークレットがローテーションスケジュールに基づいて正常にローテーションするように設定する必要があります。

ローテーションの詳細については、「AWS Secrets Manager ユーザーガイド」の「AWS Secrets Manager シークレットのローテーション」を参照してください。

修正

自動ローテーションが失敗した場合、Secrets Manager の設定でエラーが発生している可能性があります。Secrets Manager でシークレットをローテーションさせるには、シークレットを所有するデータベースまたはサービスとの対話方法を定義する Lambda 関数を使用する必要があります。

シークレットのローテーションに関連する一般的なエラーの診断と修正については、AWS Secrets Manager 「 ユーザーガイド」の「シークレットの AWS Secrets Manager ローテーションのトラブルシューティング」を参照してください。

[SecretsManager.3] 未使用の Secrets Manager のシークレットを削除します

関連する要件: NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::SecretsManager::Secret`

AWS Config ルール : `secretsmanager-secret-unused`

スケジュールタイプ : 定期的

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`unusedForDays`	シークレットを未使用のままにできる最大日数	整数	`1 ~ 365`	`90`

このコントロールは、シー AWS Secrets Manager クレットが指定された期間内にアクセスされたかどうかを確認します。指定された時間枠を過ぎてもシークレットが使用されない場合、コントロールは失敗します。アクセス期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 90 日を使用します。

未使用のシークレットを削除することは、シークレットをローテーションするのと同様に重要です。未使用のシークレットは、これらのシークレットにアクセスする必要のない以前のユーザーによって悪用される可能性があります。また、より多くのユーザーがシークレットへのアクセスすると、誰かが誤って処理して権限のないエンティティに漏洩する可能性があるため、不正使用のリスクが高まります。未使用のシークレットを削除することで、必要としないユーザーからのシークレットへのアクセスを取り消すことができます。また、Secrets Manager の使用コスト削減にも役立ちます。したがって、未使用のシークレットを定期的に削除することが不可欠です。

修正

非アクティブな Secrets Manager シークレットを削除するには、AWS Secrets Manager 「ユーザーガイド」の「AWS Secrets Manager シークレットの削除」を参照してください。

[SecretsManager.4] Secrets Manager のシークレットは、指定された日数以内にローテーションする必要があります

関連する要件： NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、PCI DSS v4.0.1/8.6.3、PCI DSS v4.0.1/8.3.9

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 中

リソースタイプ : `AWS::SecretsManager::Secret`

AWS Config ルール : `secretsmanager-secret-periodic-rotation`

スケジュールタイプ : 定期的

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`maxDaysSinceRotation`	シークレットを未変更のままにできる最大日数	整数	`1 ~ 180`	`90`

このコントロールは、シー AWS Secrets Manager クレットが指定された期間内に少なくとも 1 回ローテーションされているかどうかを確認します。シークレットを少なくともこの頻度でローテー

ションしないと、コントロールは失敗します。ローテーション期間に対してカスタムパラメータ値を指定しない限り、Security Hub はデフォルト値の 90 日を使用します。

シークレットをローテーションすることで、 AWS アカウントでユーザーのシークレットが不正に使用されるリスクを減らすのに役立ちます。例えば、データベース認証情報、パスワード、サードパーティーの API キーおよび任意のテキストなどがあります。シークレットを長期間変更しない場合、シークレットが侵害される可能性が高くなります。

より多くのユーザーがシークレットへのアクセスすると、誰かが操作を誤り、権限のないエンティティに漏洩する可能性があります。シークレットは、ログとキャッシュデータを介して漏洩する可能性があります。これらはデバッグ目的で共有でき、デバッグ完了後に変更または取り消されることはありません。これらすべての理由から、シークレットは頻繁にローテーションする必要があります。

AWS Secrets Managerでシークレットの自動ローテーションを設定できます。自動ローテーションにより、長期のシークレットを短期のシークレットに置き換えることが可能となり、侵害されるリスクを大幅に減少させるのに役立ちます。Secrets Manager のシークレットの自動ローテーションを設定することをお勧めします。詳細については、「AWS Secrets Manager ユーザーガイド」の「AWS Secrets Manager シークレットのローテーション」を参照してください。

修正

Secrets Manager シークレットの自動ローテーションを有効にするには、「 AWS Secrets Manager ユーザーガイド」の「コンソールを使用してシーク AWS Secrets Manager レットの自動ローテーションを設定する」を参照してください。ローテーションする AWS Lambda 関数を選択して設定する必要があります。

[SecretsManager.5] Secrets Manager のシークレットにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::SecretsManager::Secret`

AWS Config ルール: `tagged-secretsmanager-secret` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、 AWS Secrets Manager シークレットにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。シークレットにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、シークレットにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Secrets Manager シークレットにタグを追加するには、AWS Secrets Manager 「 ユーザーガイド」の「タグシー AWS Secrets Manager クレット」を参照してください。

の Security Hub コントロール AWS Service Catalog

この AWS Security Hub コントロールは、 AWS Service Catalog サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります

関連する要件: NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-6、NIST.800-53.r5 CM-8、NIST.800-53.r5 SC-7

カテゴリ: 保護 > セキュアなアクセス管理

重要度: 高

リソースタイプ : `AWS::ServiceCatalog::Portfolio`

AWS Config ルール : service-catalog-shared-within-organization

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 と AWS Organizations の統合が有効になっているときに、 が組織内のポートフォリオ AWS Service Catalog を共有するかどうかをチェックします。ポートフォリオが組織内で共有されていない場合、コントロールは失敗します。

Organizations 内でのみポートフォリオを共有すると、ポートフォリオが間違った AWS アカウントと共有されないようになります。Service Catalog ポートフォリオを組織内のアカウントと共有するには、`ACCOUNT` の代わりに `ORGANIZATION_MEMBER_ACCOUNT` を使用することをお勧めします。これにより、組織全体のアカウントに付与されたアクセスを制御できるため、管理が簡素化されます。Service Catalog ポートフォリオを外部アカウントと共有する必要がある場合は、このコントロールの検出結果を自動的に抑制するか、無効にすることができます。

修正

とのポートフォリオ共有を有効にするには AWS Organizations、 AWS Service Catalog 管理者ガイドの「 との共有 AWS Organizations」を参照してください。

Amazon SES の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon Simple Email Service (Amazon SES) サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[SES.1] SES 連絡先リストにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::SES::ContactList`

AWS Configルール: `tagged-ses-contactlist` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon SES 連絡先リストにパラメータ `requiredTagKeys` で定義された特定のキーを含むタグがあるかどうかをチェックします。連絡先リストにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、連絡先リストにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Amazon SES 連絡先リストにタグを追加するには、「Amazon SES API v2 リファレンス」の「TagResource」を参照してください。

[SES.2] SES 設定セットにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::SES::ConfigurationSet`

AWS Configルール: `tagged-ses-configurationset` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、Amazon SES 設定セットにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。設定セットにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、設定セットにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Amazon SES 設定セットにタグを追加するには、「Amazon SES API v2 リファレンス」の「TagResource」を参照してください。

Amazon SNS の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon Simple Notification Service (Amazon SNS) サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[SNS.1] SNS トピックは、保管時に を使用して暗号化する必要があります AWS KMS

関連する要件： NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)、NIST.800-171.r2 3.13.11、NIST.800-171.r2 3.13.16

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::SNS::Topic`

AWS Config ルール : `sns-encrypted-kms`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon SNS トピックが AWS Key Management Service (AWS KMS) に管理されているキーを使用して保管中に暗号化されているかどうかをチェックします。SNS トピックがサーバー側の暗号化 (SSE) に KMS キーを使用しない場合、コントロールは失敗します。デフォルトでは、SNS はディスク暗号化を使用してメッセージとファイルを保存します。このコントロールに合格するには、代わりに暗号化に KMS キーを使用する必要があります。これにより、セキュリティレイヤーが追加され、アクセスコントロールの柔軟性が向上します。

保管中のデータを暗号化することで、ディスクに保存されているデータが認証されていないユーザーがアクセスするリスクが軽減されます AWS。データを読み取る前にデータを復号化するには、API の許可が必要です。セキュリティを強化するために、SNS トピックを KMS キーで暗号化することをお勧めします。

修正

SNS トピックで SSE を有効にするには、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS トピックのサーバー側の暗号化 (SSE) を有効にする」を参照してください。SSE を使用する前に、トピックの暗号化とメッセージの暗号化と復号を許可する AWS KMS key ポリシーも設定する必要があります。詳細については、Amazon Simple Notification Service デベロッパーガイドのAWS KMS 「アクセス許可の設定」を参照してください。

[SNS.2] トピックに送信される通知メッセージでは、配信ステータスのログ記録を有効にする必要があります

> **Important**
>
> Security Hub は、2024 年 4 月にこのコントロールを廃止しました。詳細については、「Security Hub CSPM コントロールの変更ログ」を参照してください。

関連する要件: NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::SNS::Topic`

AWS Config ルール : `sns-topic-message-delivery-notification-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、エンドポイントの Amazon SNS トピックに送信される通知メッセージの配信ステータスで、ログ記録が有効になっているかどうかをチェックします。メッセージの配信ステータス通知が有効になっていない場合、このコントロールは失敗します。

ログ記録は、サービスの信頼性、可用性、パフォーマンスを維持するための重要な要素です。メッセージの配信ステータスをログ記録することで、以下のようなオペレーション上のインサイトを得ることができます。

- メッセージが Amazon SNS エンドポイントに配信されたかどうかを知ることができます。
- Amazon SNS エンドポイントから Amazon SNS に送信された応答を識別します。

- メッセージの滞留時間 (メッセージの発行から Amazon SNS エンドポイントに渡されるまでの時間) を決定する。

修正

トピックの配信ステータスロギングを設定する方法については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS メッセージ配信ステータス」を参照してください。

[SNS.3] SNS トピックにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::SNS::Topic`

AWS Config ルール: `tagged-sns-topic` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、Amazon SNS トピックにパラメータ `requiredTagKeys` で定義された特定のキーを含むタグがあるかどうかをチェックします。トピックにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、トピックにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

SNS トピックにタグを追加するには、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS トピックタグの設定」を参照してください。

[SNS.4] SNS トピックアクセスポリシーはパブリックアクセスを許可しないでください

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 高

リソースタイプ : `AWS::SNS::Topic`

AWS Config ルール : sns-topic-no-public-access

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon SNS トピックアクセスポリシーがパブリックアクセスを許可するかどうかを確認します。SNS トピックアクセスポリシーでパブリックアクセスが許可されている場合、このコントロールは失敗します。

特定のトピックで Amazon SNS アクセスポリシーを使用して、そのトピックを操作できるユーザー (メッセージを発行できるユーザーやサブスクライブできるユーザーなど) を制限します。SNS ポリシーは AWS アカウント、他のユーザー、または独自の 内のユーザーにアクセス権を付与できます AWS アカウント。トピックポリシーの `Principal` フィールドにワイルドカード (*) を指定し、トピックポリシーを制限する条件がないと、攻撃者によるデータの流出、サービス拒否、またはサービスへの望ましくないメッセージの挿入につながる可能性があります。

> **Note**
>
> このコントロールは、ワイルドカード文字または変数を使用するポリシー条件を評価しません。`PASSED` 検出結果を生成するには、トピックの Amazon SNS アクセスポリシーの条件は固定値のみを使用する必要があります。固定値は、ワイルドカード文字やポリシー変数を含まない値です。ポリシー変数の詳細については、「 AWS Identity and Access Management ユーザーガイド」の「変数とタグ」を参照してください。

修正

SNS トピックのアクセスポリシーを更新するには、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNSでのアクセス管理の概要」を参照してください。

Amazon SQS の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon Simple Queue Service (Amazon SQS) サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[SQS.1] Amazon SQS キューは保管中に暗号化する必要があります

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::SQS::Queue`

AWS Config ルール: `sqs-queue-encrypted` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon SQS キューが保管中に暗号化されるかどうかをチェックします。キューが SQS マネージドキー (SSE-SQS) または AWS Key Management Service () キー (SSE-KMS AWS KMS) で暗号化されていない場合、コントロールは失敗します。

保管中のデータを暗号化すると、認証されていないユーザーがディスクに保存されているデータにアクセスするリスクが低減されます。サーバー側の暗号化 (SSE) は、SQS マネージド暗号化キー (SSE-SQS) または AWS KMS キー (SSE-KMS) を使用して、SQS キュー内のメッセージの内容を保護します。

修正

SQS キューの SSE を設定するには、「Amazon Simple Queue Service デベロッパーガイド」の「キューのサーバー側の暗号化 (SSE) の設定 (コンソール)」を参照してください。

[SQS.2] SQS キューにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::SQS::Queue`

AWS Config ルール: `tagged-sqs-queue` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、Amazon SQS キューにパラメータ `requiredTagKeys` で定義された特定のキーを持つタグがあるかどうかをチェックします。キューにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、キューにキーがタグ付けされていない場合に失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Amazon SQS コンソールを使用して既存のキューにタグを追加するには、「Amazon Simple Queue Service デベロッパーガイド」のAmazon SQSキュー (コンソール) のコスト配分タグの設定」を参照してください。

[SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください

カテゴリ: 保護 > セキュアなアクセス管理 > パブリックアクセスが不可能なリソース

重要度: 高

リソースタイプ : `AWS::SQS::Queue`

AWS Config ルール : sqs-queue-no-public-access

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon SQS アクセスポリシーが SQS キューへのパブリックアクセスを許可するかどうかをチェックします。SQS アクセスポリシーがキューへのパブリックアクセスを許可すると、コントロールは失敗します。

Amazon SQS アクセスポリシーでは、SQS キューへのパブリックアクセスを許可できます。これにより、匿名ユーザーまたは認証された IAM ID AWS がキューにアクセスできるようになります。SQS アクセスポリシーは、通常、ポリシーの `Principal`要素でワイルドカード文字 (*) を指定し、適切な条件を使用してキューへのアクセスを制限するのではなく、またはその両方を指定することで、このアクセスを提供します。SQS アクセスポリシーでパブリックアクセスが許可されている場合、サードパーティーはキューからのメッセージの受信、キューへのメッセージの送信、キューのアクセスポリシーの変更などのタスクを実行できます。これにより、データ流出、サービス拒否、脅威アクターによるキューへのメッセージの挿入などのイベントが発生する可能性があります。

> **Note**
>
> このコントロールは、ワイルドカード文字または変数を使用するポリシー条件を評価しません。`PASSED` 結果を生成するには、キューの Amazon SQS アクセスポリシーの条件は固定値のみを使用する必要があります。固定値は、ワイルドカード文字やポリシー変数を含まない値です。ポリシー変数の詳細については、「 AWS Identity and Access Management ユーザーガイド」の「変数とタグ」を参照してください。

修正

SQS キューの SQS アクセスポリシーの設定については、Amazon Simple Queue Service デベロッパーガイドのAmazon SQS アクセスポリシー言語を使用したカスタムポリシーの使用」を参照してください。

Step Functions の Security Hub コントロール

これらの AWS Security Hub コントロールは、 AWS Step Functions サービスとリソースを評価します。

これらのコントロールは、一部で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[StepFunctions.1] Step Functions ステートマシンではログ記録がオンになっている必要があります

関連する要件： PCI DSS v4.0.1/10.4.2

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::StepFunctions::StateMachine`

AWS Config ルール : `step-functions-state-machine-logging-enabled`

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`logLevel`	最小ログ記録レベル	列挙型	`ALL`, `ERROR`, `FATAL`	デフォルト値なし

このコントロールは、 AWS Step Functions ステートマシンでログ記録が有効になっているかどうかをチェックします。ステートマシンでログ記録が有効になっていない場合、コントロールは失敗します。`logLevel` パラメータにカスタム値を指定したときは、ステートマシンで指定されたログ記録レベルがオンになっている場合にのみコントロールが成功します。

モニタリングは、Step Functions の信頼性、可用性、パフォーマンスを維持するのに役立ちます。マルチポイント障害をより簡単にデバッグできるように、 AWS のサービス 使用する からモニタリングデータを収集する必要があります。Step Functions のステートマシンにログ記録の設定を定義しておくと、Amazon CloudWatch Logs で実行履歴と結果を追跡できます。オプションで、エラーまたは致命的なイベントのみを追跡できます。

修正

Step Functions ステートマシンのログ記録を有効にするには、「AWS Step Functions デベロッパーガイド」の「ログ記録の設定」を参照してください。

[StepFunctions.2] Step Functions アクティビティにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::StepFunctions::Activity`

AWS Config ルール : `tagged-stepfunctions-activity` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS Step Functions アクティビティにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。アクティビティにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、アクティビティにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するよう

に設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS Billing。タグ付けのベストプラクティスの詳細については、『』の「 AWS リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Step Functions アクティビティにタグを追加するには、「AWS Step Functions デベロッパーガイド」の「Step Functions のタグ付け」を参照してください。

Systems Manager の Security Hub コントロール

これらの AWS Security Hub コントロールは、 AWS Systems Manager (SSM) サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager

関連する要件: PCI DSS v3.2.1/2.4、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-8、NIST.800-53.r5 CM-8(1)、NIST.800-53.r5 CM-8(2)、NIST.800-53.r5 CM-8(3)、NIST.800-53.r5 SA-15(2)、NIST.800-53.r5 SA-15(8)、NIST.800-53.r5 SA-3、NIST.800-53.r5 SI-2(3)

カテゴリ: 識別 > インベントリ

重要度: 中

評価されたリソース: `AWS::EC2::Instance`

必要な AWS Config 記録リソース： `AWS::EC2::Instance`、`AWS::SSM::ManagedInstanceInventory`

AWS Config ルール : ec2-instance-managed-by-systems-manager

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、アカウントで停止および実行中の EC2 インスタンスが によって管理されているかどうかを確認します AWS Systems Manager。Systems Manager は、 AWS インフラストラクチャを表示および制御するために AWS のサービス 使用できる です。

セキュリティとコンプライアンスを維持するために、Systems Manager は停止中および実行中のマネージドインスタンスをスキャンします。マネージドインスタンスとは、Systems Manager で使用するために設定されたマシンです。Systems Manager が検出したポリシー違反について報告または是正処置を講じます。Systems Manager は、マネージドインスタンスの設定と維持管理にも役立ちます。

詳細については、「AWS Systems Manager ユーザーガイド」を参照してください。

修正

Systems Manager を使用して EC2 インスタンスを管理するには、「AWS Systems Manager ユーザーガイド」の「Amazon EC2 ホスト管理」を参照してください。[設定オプション] セクションでは、デフォルトの選択肢をそのまま使用することも、希望の設定に合わせて必要に応じて変更することもできます。

[SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります

関連する要件： NIST.800-53.r5 CM-8(3)、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(3)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、NIST.800-171.r2 3.7.1、PCI DSS v3.2.1/6.2、PCI DSS v4.0.1/2.2.1、PCI DSS v4.0.1/6.3.3.3

カテゴリ: 検出 > 検出サービス

重要度: 高

リソースタイプ : `AWS::SSM::PatchCompliance`

AWS Config ルール : ec2-managedinstance-patch-compliance-status-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、インスタンスへのパッチインストール後、Systems Manager パッチコンプライアンスのコンプライアンスステータスが、`COMPLIANT` と `NON_COMPLIANT` のどちらであるかをチェックします。コンプライアンスステータスが `NON_COMPLIANT` の場合、コントロールは失敗し

ます。このコントロールは、Systems Manager Patch Manager によって管理されているインスタンスのみをチェックします。

組織の要求に応じて EC2 インスタンスにパッチを適用すると、 AWS アカウントのアタックサーフェスが低減されます。

修正

Systems Manager では、パッチポリシーを使用して、マネージドインスタンスのパッチ適用を設定することを推奨しています。次の手順で説明するように、Systems Manager のドキュメントを使用してインスタンスにパッチを適用することもできます。

非準拠のパッチを修正するには

1. https://console.aws.amazon.com/systems-manager/ で AWS Systems Manager コンソールを開きます。
2. [ノード管理] で、[コマンドを実行する] を選択し、[コマンドを実行する] を選択します。
3. AWS-RunPatchBaseline のオプションを選択します。
4. [Operation] (オペレーション) を [Install] (インストール) に変更します。
5. [インスタンスを手動で選択する] を選択し、非準拠のインスタンスを選択します。
6. [Run] (実行) を選択します。
7. コマンドの完了後に、パッチを適用したインスタンスの新しいコンプライアンスステータスをモニタリングするには、ナビゲーションペインで [コンプライアンス] を選択します。

[SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります

関連する要件： NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-8、NIST.800-53.r5 CM-8(1)、NIST.800-53.r5 CM-8(3)、NIST.800-53.r5 SI-2(3)、PCI DSS v3.2.1/2.4、PCI DSS v4.0.1/2.2.1、PCI DSS v4.0.1/6.3.3

カテゴリ: 検出 > 検出サービス

重要度: 低

リソースタイプ : `AWS::SSM::AssociationCompliance`

AWS Config ルール : ec2-managedinstance-association-compliance-status-check

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS Systems Manager 関連付けコンプライアンスのステータスが であるかCOMPLIANT、インスタンスで関連付けが実行されNON_COMPLIANTた後であるかをチェックします。関連付けのコンプライアンスステータスが NON_COMPLIANT の場合、コントロールは失敗します。

State Manager の関連付けは、マネージドインスタンスに割り当てられる設定です。この設定では、インスタンスで維持する状態を定義します。例えば、関連付けでは、アンチウイルスソフトウェアをインスタンス上にインストールして実行する必要があること、または特定のポートを閉じる必要があることを指定できます。

State Manager の関連付けを 1 つまたは複数作成することで、コンプライアンスステータス情報をすぐに表示できるようになります。コンプライアンスステータスは、 コンソールで、または AWS CLI コマンドまたは対応する Systems Manager API アクションに応答して表示できます。関連付けでは、設定コンプライアンスはコンプライアンスステータスを表示します (Compliant または Non-compliant)。また、関連付けに割り当てられた Critical または Medium などの重要度レベルを表示します。

State Manager 関連付けのコンプライアンスの詳細については、「AWS Systems Manager ユーザーガイド」の「State Manager 関連付けのコンプライアンスについて」を参照してください。

修正

失敗した関連付けは、ターゲットや Systems Manager ドキュメント名など、さまざまなものに関連している可能性があります。この問題を修正するには、まず関連付けの履歴を表示し、関連付けを特定して調査する必要があります。関連付けの履歴を表示するには、「AWS Systems Manager ユーザーガイド」の「関連付けの履歴の表示」を参照してください。

調査後、関連付けを編集して特定された問題を修正できます。関連付けを編集して、新しい名前やスケジュール、重要度レベル、ターゲットを指定できます。関連付けを編集すると、 は新しいバージョン AWS Systems Manager を作成します。関連付けの編集については、「AWS Systems Manager ユーザーガイド」の「関連付けの編集と新しいバージョンの作成」を参照してください。

[SSM.4] SSM ドキュメントはパブリックにしないでください

関連する要件: NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5

SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

カテゴリ: 保護 > セキュアなネットワーク設定 > パブリックアクセス不可のリソース

重要度: 非常事態

リソースタイプ : `AWS::SSM::Document`

AWS Config ルール : ssm-document-not-public

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、アカウントが所有する AWS Systems Manager ドキュメントがパブリックかどうかをチェックします。所有者`Self`として を持つ Systems Manager ドキュメントがパブリックである場合、コントロールは失敗します。

パブリックの Systems Manager ドキュメントは、ドキュメントへの意図しないアクセスを許可する場合があります。パブリック Systems Manager ドキュメントは、アカウント、リソース、および内部プロセスに関する貴重な情報を公開する可能性があります。

ユースケースでパブリック共有が必要でない限り、 を所有者`Self`とする Systems Manager ドキュメントのパブリック共有をブロックすることをお勧めします。

修正

Systems Manager ドキュメントの共有の設定については、AWS Systems Manager 「 ユーザーガイド」の「SSM ドキュメントの共有」を参照してください。

[SSM.5] SSM ドキュメントにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::SSM::Document`

AWS Config ルール : ssm-document-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS Systems Manager ドキュメントに `requiredKeyTags`パラメータで指定されたタグキーがあるかどうかをチェックします。ドキュメントにタグキーがない場合、または `requiredKeyTags`パラメータで指定されたすべてのキーがない場合、コントロールは失敗します。`requiredKeyTags` パラメータの値を指定しない場合、コントロールはタグキーの存在のみをチェックし、ドキュメントにタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、 `aws:` プレフィックスが付いています。このコントロールは、Amazon が所有する Systems Manager ドキュメントを評価しません。

タグは、 AWS リソースを作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの識別、整理、検索、フィルタリングに役立ちます。また、アクションと通知のリソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセスコントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 AWS リソースのタグ付け」および「タグエディタユーザーガイド」を参照してください。

> **Note**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

AWS Systems Manager ドキュメントにタグを追加するには、 AWS Systems Manager API の AddTagsToResource オペレーションを使用するか、 を使用している場合は AWS CLI addadd-tags-to-resource コマンドを実行します。 AWS Systems Manager コンソールを使用することもできます。

[SSM.6] SSM Automation では CloudWatch ログ記録が有効になっている必要があります

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::::Account`

AWS Config ルール : ssm-automation-logging-enabled

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールはAmazon CloudWatch ログ記録が AWS Systems Manager (SSM) Automation で有効になっているかどうかをチェックします。CloudWatch ログ記録が SSM Automation で有効になっていない場合、コントロールは失敗します。

SSM Automation は、事前定義されたランブックまたはカスタムランブックを使用して、リソースを大規模 AWS にデプロイ、設定、管理するための自動ソリューションを構築するのに役立つ AWS Systems Manager ツールです。組織の運用要件またはセキュリティ要件を満たすには、実行するスクリプトの記録を提供する必要がある場合があります。ランブックの`aws:executeScript`アクションからの出力を、指定した Amazon CloudWatch Logs ロググループに送信するように SSM Automation を設定できます。CloudWatch Logs を使用すると、さまざまな AWS のサービスからのログファイルについて、モニタリング、保存、アクセスが行えます。

修正

SSM Automation で CloudWatch ログ記録を有効にする方法については、AWS Systems Manager「 ユーザーガイド」のCloudWatch Logs を使用したオートメーションアクション出力のログ記録」を参照してください。

[SSM.7] SSM ドキュメントでは、パブリック共有ブロック設定を有効にする必要があります

カテゴリ: 保護 > セキュアなアクセス管理 > パブリックアクセスが不可能なリソース

重要度: 非常事態

リソースタイプ : `AWS::::Account`

AWS Config ルール : ssm-automation-block-public-sharing

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、ドキュメントに対してパブリック共有ブロック設定が有効になっている AWS Systems Manager かどうかをチェックします。Systems Manager ドキュメントでブロックパブリック共有設定が無効になっていると、コントロールは失敗します。

AWS Systems Manager (SSM) ドキュメントのブロックパブリック共有設定は、アカウントレベルの設定です。この設定を有効にすると、SSM ドキュメントへの不要なアクセスを防ぐことができます。この設定を有効にしても、現在パブリックと共有している SSM ドキュメントには影響しません。ユースケースで SSM ドキュメントをパブリックと共有する必要がある場合を除き、パブリック共有ブロック設定を有効にすることをお勧めします。設定は、それぞれ異なる場合があります AWS リージョン。

修正

(SSM) ドキュメントのブロックパブリック共有設定 AWS Systems Manager を有効にする方法については、AWS Systems Manager 「 ユーザーガイド」の「SSM ドキュメントのブロックパブリック共有」を参照してください。

の Security Hub コントロール AWS Transfer Family

これらの AWS Security Hub コントロールは、 AWS Transfer Family サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Transfer::Workflow`

AWS Config ルール: `tagged-transfer-workflow` (カスタム Security Hub ルール)

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredTagKeys`	評価されたリソースに含める必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	`No default value`

このコントロールは、 AWS Transfer Family ワークフローにパラメータ で定義された特定のキーを持つタグがあるかどうかをチェックします`requiredTagKeys`。ワークフローにタグキーがない場合、またはパラメータ `requiredTagKeys` で指定されたすべてのキーがない場合、コントロールは失敗します。パラメータ `requiredTagKeys` が指定されていない場合、コントロールはタグキーの存在のみをチェックし、ワークフローにキーがタグ付けされていない場合は失敗します。自動的に適用され、`aws:` で始まるシステムタグは無視されます。

タグは、 AWS リソースに割り当てるラベルで、キーとオプションの値で構成されます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。タグは、リソースの識別、整理、検索、フィルタリングに役立ちます。タグ付けは、アクションと通知の説明責任のあるリソース所有者を追跡するのに役立ちます。タグ付けを使用する場合、タグに基づいてアクセス許可を定義する認証戦略として属性ベースのアクセスコントロール (ABAC) を実装できます。タグは、IAM エンティティ (ユーザーまたはロール) および AWS リソースにアタッチできます。IAM プリンシパルに対して、単一の ABAC ポリシー、または個別のポリシーセットを作成できます。これらの ABAC ポリシーを、プリンシパルのタグがリソースタグと一致するときに操作を許可するように設計することができます。詳細については、IAM ユーザーガイドの「ABAC とは AWS」を参照してください。

> **Note**
>
> タグには、個人を特定できる情報 (PII) や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグには AWS のサービス、 を含む多くのユーザーがアクセスできます AWS

Billing。タグ付けのベストプラクティスの詳細については、のAWS 「リソースのタグ付け」を参照してくださいAWS 全般のリファレンス。

修正

Transfer Family ワークフローにタグを追加するには (コンソール)

1. AWS Transfer Family コンソールを開きます。
2. ナビゲーションペインで、[Workflows] (ワークフロー) をクリックします。次に、タグ付けするワークフローを選択します。
3. タグの管理を選択し、タグを追加します。

[Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください

関連する要件： NIST.800-53.r5 CM-7、NIST.800-53.r5 IA-5、NIST.800-53.r5 SC-8、PCI DSS v4.0.1/4.2.1

カテゴリ: 保護 > データ保護 > 転送中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::Transfer::Server`

AWS Config ルール : transfer-family-server-no-ftp

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、 AWS Transfer Family サーバーがエンドポイント接続に FTP 以外のプロトコルを使用しているかどうかをチェックします。サーバーがクライアントに FTP プロトコルを使用してサーバーのエンドポイントに接続すると、コントロールは失敗します。

FTP (File Transfer Protocol) は、暗号化されていないチャネルを介してエンドポイント接続を確立し、これらのチャネル経由で送信されたデータは傍受されやすくなります。SFTP (SSH File Transfer Protocol)、FTPS (File Transfer Protocol Secure)、または AS2 (適用可能性ステートメント 2) を使用すると、転送中のデータを暗号化することでセキュリティを強化できます。また、潜在的な攻撃者が中間者攻撃や類似の攻撃を使用してネットワークトラフィックを盗聴または操作するのを防ぐのに役立ちます。

修正

Transfer Family サーバーのプロトコルを変更するには、「AWS Transfer Family ユーザーガイド」の「ファイル転送プロトコルの編集」を参照してください。

[Transfer.3] Transfer Family コネクタではログ記録が有効になっている必要があります

関連する要件: NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 AU-9(7)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-4(20)、NIST.800-53.r5 SI-7(8)

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::Transfer::Connector`

AWS Config ルール : transfer-connector-logging-enabled

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS Transfer Family コネクタで Amazon CloudWatch ログ記録が有効になっているかどうかを確認します。コネクタで CloudWatch ログ記録が有効になっていない場合、コントロールは失敗します。

Amazon CloudWatch は、 AWS リソースを含む AWS Transfer Family リソースを可視化するモニタリングおよびオブザーバビリティサービスです。Transfer Family の場合、CloudWatch はワークフローの進行状況と結果の統合監査とログ記録を提供します。これには、Transfer Family がワークフロー用に定義するいくつかのメトリクスが含まれます。Transfer Family を設定して、コネクタイベントを CloudWatch に自動的にログ記録できます。これを行うには、コネクタのログ記録ロールを指定します。ログ記録ロールには、IAM ロールと、ロールのアクセス許可を定義するリソースベースの IAM ポリシーを作成します。

修正

Transfer Family コネクタの CloudWatch ログ記録を有効にする方法については、AWS Transfer Family 「 ユーザーガイド」のAWS Transfer Family 「サーバーの Amazon CloudWatch ログ記録」を参照してください。

[Transfer.4] Transfer Family 契約にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Transfer::Agreement`

AWS Config ルール : transfer-agreement-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS Transfer Family 契約に `requiredKeyTags`パラメータで指定されたタグキーがあるかどうかをチェックします。契約にタグキーがない場合、または `requiredKeyTags`パラメータで指定されたすべてのキーがない場合、コントロールは失敗します。`requiredKeyTags` パラメータの値を指定しない場合、コントロールはタグキーの存在のみをチェックし、契約にタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、`aws:`プレフィックスが付いています。

タグは、 AWS リソースを作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの特定、整理、検索、フィルタリングに役立ちます。また、アクションと通知のリソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセスコントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 AWS リソースのタグ付けとタグエディタのユーザーガイド」を参照してください。

> **Note**
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

AWS Transfer Family 契約へのタグの追加の詳細については、「 リソースのタグ付けとタグエディタユーザーガイド」の「リソースのタグ付け方法 AWS 」を参照してください。

[Transfer.5] Transfer Family 証明書にはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Transfer::Certificate`

AWS Config ルール : transfer-certificate-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されている カスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS Transfer Family 証明書に `requiredKeyTags`パラメータで指定されたタグキーがあるかどうかをチェックします。証明書にタグキーがない場合、または

requiredKeyTagsパラメータで指定されたすべてのキーがない場合、コントロールは失敗します。requiredKeyTags パラメータに値を指定しない場合、コントロールはタグキーの存在のみをチェックし、証明書にタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、aws:プレフィックスが付いています。

タグは、 AWS リソースを作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの特定、整理、検索、フィルタリングに役立ちます。また、アクションと通知のリソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセスコントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 AWS リソースのタグ付けとタグエディタのユーザーガイド」を参照してください。

> **Note**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

AWS Transfer Family 証明書にタグを追加する方法については、「 リソースのタグ付けとタグエディタユーザーガイド」の「リソースのタグ付け方法 AWS 」を参照してください。

[Transfer.6] Transfer Family コネクタにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Transfer::Connector`

AWS Config ルール : transfer-connector-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
requiredKeyTags	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS Transfer Family コネクタに requiredKeyTagsパラメータで指定されたタグキーがあるかどうかをチェックします。コネクタにタグキーがない場合、または requiredKeyTagsパラメータで指定されたすべてのキーがない場合、コントロールは失敗します。requiredKeyTags パラメータに値を指定しない場合、コントロールはタグキーの存在のみをチェックし、コネクタにタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、aws:プレフィックスが付いています。

タグは、 AWS リソースを作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの特定、整理、検索、フィルタリングに役立ちます。また、アクションと通知のリソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセスコントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を使用して属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 AWS リソースのタグ付け」および「タグエディタユーザーガイド」を参照してください。

> **Note**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

AWS Transfer Family コネクタへのタグの追加については、「リソースのタグ付けとタグエディタユーザーガイド」の「リソースのタグ付け方法 AWS 」を参照してください。

[Transfer.7] Transfer Family プロファイルにはタグを付ける必要があります

カテゴリ: 識別 > インベントリ > タグ付け

重要度: 低

リソースタイプ : `AWS::Transfer::Profile`

AWS Config ルール : transfer-profile-tagged

スケジュールタイプ : 変更がトリガーされた場合

パラメータ :

パラメータ	説明	[Type] (タイプ)	許可されているカスタム値	Security Hub のデフォルト値
`requiredKeyTags`	評価されたリソースに割り当てる必要があるシステム以外のタグキーのリスト。タグキーでは、大文字と小文字が区別されます。	StringList (最大 6 項目)	AWS 要件を満たす 1 ~ 6 個のタグキー。	デフォルト値なし

このコントロールは、 AWS Transfer Family プロファイルに `requiredKeyTags`パラメータで指定されたタグキーがあるかどうかをチェックします。プロファイルにタグキーがない場合、または `requiredKeyTags`パラメータで指定されたすべてのキーがない場合、コントロールは失敗します。`requiredKeyTags` パラメータの値を指定しない場合、コントロールはタグキーの存在のみをチェックし、プロファイルにタグキーがない場合に失敗します。コントロールはシステムタグを無視します。システムタグは自動的に適用され、`aws:`プレフィックスが付いています。コントロールは、ローカルプロファイルとパートナープロファイルを評価します。

タグは、 AWS リソースを作成して割り当てるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグを使用し、リソースを目的、所有者、環境などの基準別に分類できます。リソースの特定、整理、検索、フィルタリングに役立ちます。また、アクションと通知のリソース所有者を追跡するのに役立ちます。タグを使用して、認可戦略として属性ベースのアクセスコントロール (ABAC) を実装することもできます。ABAC 戦略の詳細については、IAM ユーザーガイドの「ABAC 認可を持つ属性に基づいてアクセス許可を定義する」を参照してください。タグの詳細については、「 Tagging AWS Resources and Tag Editor User Guide」を参照してください。

> **Note**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。タグには多くの からアクセスできます AWS のサービス。これらは、プライベートデータや機密データに使用することを目的としたものではありません。

修正

AWS Transfer Family プロファイルにタグを追加する方法については、「リソースのタグ付けとタグエディタユーザーガイド」の「リソースのタグ付け方法 AWS 」を参照してください。

の Security Hub コントロール AWS WAF

これらの AWS Security Hub コントロールは、 AWS WAF サービスとリソースを評価します。コントロールは一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります

関連する要件： NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)、PCI v4.0.1/10.4.2

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::WAF::WebACL`

AWS Config ルール : `waf-classic-logging-enabled`

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、 AWS WAF グローバルウェブ ACL でログ記録が有効になっているかどうかをチェックします。ウェブ ACL のログ記録が有効でない場合、このコントロールは失敗します。

ログ記録は、 の信頼性、可用性、パフォーマンスを AWS WAF グローバルに維持する上で重要な部分です。これは、多くの組織でビジネスおよびコンプライアンス要件であり、アプリケーションの動

作をトラブルシューティングできます。また、 AWS WAFに添付済みのウェブ ACL によって分析されるトラフィックに関する詳細情報も提供します。

修正

AWS WAF ウェブ ACL のログ記録を有効にするには、「 AWS WAF デベロッパーガイド」の「ウェブ ACL トラフィック情報のログ記録」を参照してください。

[WAF.2] AWS WAF Classic リージョンルールには少なくとも 1 つの条件が必要です

関連する要件: NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ : `AWS::WAFRegional::Rule`

AWS Config ルール : `waf-regional-rule-not-empty`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS WAF リージョンルールに少なくとも 1 つの条件があるかどうかをチェックします。ルールに条件が 1 つもない場合、このコントロールは失敗します。

WAF リージョンルールには、複数の条件を含めることが可能です。このルールの条件によってトラフィックの検査が許可され、定義されたアクション (許可、ブロック、カウント) が実行されます。条件が 1 つもないと、トラフィックは検査なしで通過します。条件がないにもかかわらず、許可、ブロック、カウントを示す名前またはタグが付いている WAF リージョンルールは、上記いずれかのアクションが行われているという誤解を生む可能性があります。

修正

空のルールに条件を追加する方法については、には、「AWS WAF デベロッパーガイド」の「ルールの条件の追加と削除」を参照してください。

[WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です

関連する要件: NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ : `AWS::WAFRegional::RuleGroup`

AWS Config ルール : `waf-regional-rulegroup-not-empty`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS WAF リージョンルールグループに少なくとも 1 つのルールがあるかどうかをチェックします。ルールグループにルールが 1 つもない場合、このコントロールは失敗します。

WAF リージョンルールグループには、複数のルールを含めることができます。このルールの条件によってトラフィックの検査が許可され、定義されたアクション (許可、ブロック、カウント) が実行されます。ルールが 1 つもないと、トラフィックは検査なしで通過します。ルールはないにもかかわらず、許可、ブロック、カウントを示す名前またはタグが付いている WAF リージョンルールグループは、上記いずれかのアクションが行われているという誤解を生む可能性があります。

修正

空のルールグループにルールとルール条件を追加するには、「 AWS WAF デベロッパーガイド」のAWS WAF 「 Classic ルールグループへのルールの追加と削除」および「ルールの条件の追加と削除」を参照してください。

[WAF.4] AWS WAF Classic Regional Web ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ : `AWS::WAFRegional::WebACL`

AWS Config ルール : `waf-regional-webacl-not-empty`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS WAF Classic Regional ウェブ ACL に WAF ルールまたは WAF ルールグループが含まれているかどうかをチェックします。ウェブ ACL に WAF ルールまたはルールグループが含まれていない場合、このコントロールは失敗します。

WAF リージョンウェブ ACL には、ウェブリクエストを検査および制御する、ルールおよびルールグループのコレクションを含めることができます。ウェブ ACL が空の場合、ウェブトラフィックは、デフォルトのアクションに応じて WAF による検出または処理なしに通過できます。

修正

空の AWS WAF Classic Regional Web ACL にルールまたはルールグループを追加するには、「AWS WAF デベロッパーガイド」の「ウェブ ACL の編集」を参照してください。

[WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ : `AWS::WAF::Rule`

AWS Config ルール : `waf-global-rule-not-empty`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS WAF グローバルルールに条件が含まれているかどうかをチェックします。ルールに条件が 1 つもない場合、このコントロールは失敗します。

WAF グローバルルールには、複数の条件を含めることが可能です。ルールの条件によってトラフィックの検査が可能になり、定義されたアクション (許可、ブロック、カウント) を実行できます。条件が 1 つもないと、トラフィックは検査なしで通過します。条件はないにもかかわらず、許可、ブロック、カウントを示す名前またはタグが付いている WAF グローバルルールは、上記いずれかのアクションが行われているという誤解を生む可能性があります。

修正

ルールの作成方法および条件の追加方法については、「AWS WAF デベロッパーガイド」の「ルールの作成と条件の追加」を参照してください。

[WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ : `AWS::WAF::RuleGroup`

AWS Config ルール : `waf-global-rulegroup-not-empty`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS WAF グローバルルールグループに少なくとも 1 つのルールがあるかどうかをチェックします。ルールグループにルールが 1 つもない場合、このコントロールは失敗します。

WAF グローバルルールグループには、複数のルールを含めることができます。このルールの条件によってトラフィックの検査が許可され、定義されたアクション (許可、ブロック、カウント) が実行されます。ルールが 1 つもないと、トラフィックは検査なしで通過します。ルールはないにもかかわらず、許可、ブロック、カウントを示す名前またはタグが付いている WAF グローバルルールグループは、上記いずれかのアクションが行われているという誤解を生む可能性があります。

修正

ルールグループにルールを追加する手順については、 AWS WAF デベロッパーガイドの AWS WAF Classic ルールグループの作成を参照してください。

[WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

関連する要件: NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ : `AWS::WAF::WebACL`

AWS Config ルール : `waf-global-webacl-not-empty`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS WAF グローバルウェブ ACL に少なくとも 1 つの WAF ルールまたは WAF ルールグループが含まれているかどうかをチェックします。ウェブ ACL に WAF ルールまたはルールグループが含まれていない場合、このコントロールは失敗します。

WAF グローバルウェブ ACL には、ウェブリクエストを検査および制御するルールおよびルールグループのコレクションを含めることができます。ウェブ ACL が空の場合、ウェブトラフィックは、デフォルトのアクションに応じて WAF による検出または処理なしに通過できます。

修正

空の AWS WAF グローバルウェブ ACL にルールまたはルールグループを追加するには、「 AWS WAF デベロッパーガイド」の「ウェブ ACL の編集」を参照してください。[Filter] (フィルター) で [Global (CloudFront)] (グローバル (CloudFront)) を選択します。

[WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

関連する要件: NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

カテゴリ: 保護 > セキュアなネットワーク設定

重要度: 中

リソースタイプ : `AWS::WAFv2::WebACL`

AWS Config ルール : `wafv2-webacl-not-empty`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS WAF V2 ウェブアクセスコントロールリスト (ウェブ ACL) に少なくとも 1 つのルールまたはルールグループが含まれているかどうかをチェックします。ウェブ ACL にルールまたはルールグループが含まれていない場合、このコントロールは失敗します。

ウェブ ACL を使用すると、保護されたリソースが応答するすべての HTTP(S) ウェブリクエストをきめ細かく制御できます。ウェブ ACL には、ウェブリクエストを検査および制御するルールおよびルールグループのコレクションを含める必要があります。ウェブ ACL が空の場合、デフォルトのアクション AWS WAF に応じて、ウェブトラフィックは検出されず、 によって処理されずに通過できます。

修正

ルールまたはルールグループを空の WAFV2 ウェブ ACL に追加するには、「AWS WAF デベロッパーガイド」の「ウェブ ACL の編集」を参照してください。

[WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります

関連する要件： NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-7(9)、NIST.800-53.SI-710.4.2r

カテゴリ: 識別 > ログ記録

重要度: 低

リソースタイプ : `AWS::WAFv2::WebACL`

AWS Config ルール： `wafv2-logging-enabled`

スケジュールタイプ : 定期的

パラメータ : なし

このコントロールは、 AWS WAF V2 ウェブアクセスコントロールリスト (ウェブ ACL) のログ記録が有効になっているかどうかをチェックします。ウェブ ACL のログ記録が無効の場合、このコントロールは失敗します。

> **Note**
>
> このコントロールは、Amazon Security Lake を介してアカウントに対して AWS WAF ウェブ ACL ログ記録が有効になっているかどうかをチェックしません。

ログ記録は、 の信頼性、可用性、パフォーマンスを維持します AWS WAF。また、多くの組織において、ログ記録はビジネスおよびコンプライアンス要件となっています。ウェブ ACL で分析されたトラフィックをログに記録することで、アプリケーションの挙動のトラブルシューティングができます。

修正

AWS WAF ウェブ ACL のログ記録を有効にするには、「 AWS WAF デベロッパーガイド」の「ウェブ ACL のログ記録の管理」を参照してください。

[WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります

関連する要件： NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-7(9)、NIST.8000-53 SI-7.

カテゴリ: 識別 > ログ記録

重要度: 中

リソースタイプ : `AWS::WAFv2::RuleGroup`

AWS Config ルール： `wafv2-rulegroup-logging-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、 AWS WAF ルールまたはルールグループで Amazon CloudWatch メトリクスが有効になっているかどうかを確認します。ルールまたはルールグループで CloudWatch メトリクスが有効になっていない場合、コントロールは失敗します。

AWS WAF ルールとルールグループで CloudWatch メトリクスを設定すると、トラフィックフローを可視化できます。どの ACL ルールがトリガーされ、どのリクエストが受け入れられブロックされたかを確認できます。この可視性は、関連リソースでの悪意のあるアクティビティを特定するのに役立ちます。

修正

AWS WAF ルールグループで CloudWatch メトリクスを有効にするには、UpdateRuleGroup API を呼び出します。 AWS WAF ルールで CloudWatch メトリクスを有効にするには、UpdateWebACL API を呼び出します。`CloudWatchMetricsEnabled` フィールドは `true` に設定されます。 AWS WAF コンソールを使用してルールまたはルールグループを作成すると、CloudWatch メトリクスが自動的に有効になります。

WorkSpaces の Security Hub コントロール

これらの AWS Security Hub コントロールは、Amazon WorkSpaces サービスとリソースを評価します。

これらのコントロールは、一部の で使用できない場合があります AWS リージョン。詳細については、「リージョン別のコントロールの可用性」を参照してください。

[WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::WorkSpaces::Workspace`

AWS Config ルール : `workspaces-user-volume-encryption-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon WorkSpaces WorkSpace のユーザーボリュームが保管中に暗号化されているかどうかを確認します。WorkSpace ユーザーボリュームが保管中に暗号化されていない場合、コントロールは失敗します。

保管中のデータとは、永続的な不揮発性ストレージに任意の期間保管されているデータを指します。保管中のデータを暗号化すると、その機密性が保護され、権限のないユーザーがアクセスするリスクが低減されます。

修正

WorkSpaces ユーザーボリュームを暗号化するには、「Amazon WorkSpaces 管理ガイド」の「WorkSpace の暗号化」を参照してください。

[WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

カテゴリ: 保護 > データ保護 > 保管中のデータの暗号化

重要度: 中

リソースタイプ : `AWS::WorkSpaces::Workspace`

AWS Config ルール : `workspaces-root-volume-encryption-enabled`

スケジュールタイプ: 変更がトリガーされた場合

パラメータ : なし

このコントロールは、Amazon WorkSpaces WorkSpace のルートボリュームが保管中に暗号化されているかどうかを確認します。WorkSpace ルートボリュームが保管中に暗号化されていない場合、コントロールは失敗します。

保管中のデータとは、永続的な不揮発性ストレージに任意の期間保管されているデータを指します。保管中のデータを暗号化すると、その機密性が保護され、権限のないユーザーがアクセスするリスクが低減されます。

修正

WorkSpaces ルートボリュームを暗号化するには、「Amazon WorkSpaces 管理ガイド」の「WorkSpace の暗号化」を参照してください。

Security Hub CSPM でコントロールを設定するために必要なアクセス許可

セキュリティコントロールに関する情報を表示し、標準でセキュリティコントロールを有効または無効にするには、 AWS Security Hub CSPM にアクセスするために使用する AWS Identity and Access Management (IAM) ロールに、Security Hub CSPM API の次のオペレーションを呼び出すためのアクセス許可が必要です。

必要なアクセス許可を取得するには、Security Hub CSPM 管理ポリシーを使用できます。または、カスタム IAM ポリシーを更新してこれらのアクションの権限を含めることもできます。

- BatchGetSecurityControls – 現在のアカウントと のセキュリティコントロールのバッチに関する情報を返します AWS リージョン。
- ListSecurityControlDefinitions — 指定された標準に適用されるセキュリティコントロールについての情報を返します。
- ListStandardsControlAssociations — アカウントで有効になっている各標準で、セキュリティコントロールが現在有効か無効かを識別します。
- BatchGetStandardsControlAssociations — セキュリティコントロールのバッチについて、指定された標準の各コントロールが有効か無効かを識別します。
- BatchUpdateStandardsControlAssociations — コントロールを含む標準のセキュリティコントロールを有効化するか、標準のコントロールを無効化するために使用します。これは、既存の `UpdateStandardsControl` オペレーションのバッチ代替です。
- BatchUpdateStandardsControlAssociations — コントロールを含む標準のセキュリティコントロールのバッチを有効化するか、無効化するために使用します。これは、既存の `UpdateStandardsControl` オペレーションのバッチ代替です。

- UpdateStandardsControl — コントロールを含む標準の単一のセキュリティコントロールを有効化するか、無効化するために使用します。
- DescribeStandardsControl – 指定されたセキュリティコントロールに関する詳細を返します。

前述の API に加えて、IAM ロールに `BatchGetControlEvaluations` を呼び出す権限を追加する必要があります。このアクセス許可は、Security Hub CSPM コンソールでコントロールの有効化とコンプライアンスのステータス、コントロールの検出結果数、およびコントロールの全体的なセキュリティスコアを表示するために必要です。コンソールのみが を呼び出すため`BatchGetControlEvaluations`、このアクセス許可は公開されている Security Hub CSPM APIs または AWS CLI コマンドに直接対応していません。

Security Hub CSPM でのコントロールの有効化

AWS Security Hub CSPM では、コントロールは、組織が情報の機密性、完全性、可用性を保護するのに役立つセキュリティ標準内の保護手段です。各 Security Hub CSPM コントロールは、特定の AWS リソースに関連しています。コントロールを有効にすると、Security Hub CSPM はコントロールのセキュリティチェックの実行を開始し、その結果を生成します。Security Hub CSPM は、セキュリティスコアを計算する際に、有効なすべてのコントロールも考慮します。

適用されるすべてのセキュリティ標準でコントロールを有効にすることができます。または、異なる標準で有効化ステータスを異なる方法で設定できます。有効なすべての標準でコントロールの有効化ステータスを一致させる前者のオプションを使用することをお勧めします。コントロールを適用するすべての標準にわたってコントロールを有効にする手順については、「すべての標準にわたってコントロールを有効にする」を参照してください。特定の標準でコントロールを有効にする手順については、「特定の標準のコントロールを有効にする」を参照してください。

クロスリージョン集約を有効にして集約リージョンにサインインすると、Security Hub CSPM コンソールには、少なくとも 1 つのリンクされたリージョンで使用できるコントロールが表示されます。リンクされたリージョンでコントロールを使用できるが、集約リージョンでは使用できない場合は、集約リージョンからそのコントロールを有効または無効にすることはできません。

Security Hub CSPM コンソール、Security Hub CSPM API、または を使用して、各リージョンでコントロールを有効または無効にできます AWS CLI。

コントロールを有効または無効にする手順は、中央設定を使用するかどうかによって異なります。このトピックでは、その違いについて説明します。Security Hub CSPM と を統合するユーザーは、中央設定を使用できます AWS Organizations。マルチアカウント、マルチリージョン環境でコントロールを有効または無効にするプロセスを簡略化するために、中央設定を使用することをお勧めします。

中央設定を使用する場合は、設定ポリシーを使用して、複数のアカウントとリージョンのコントロールを有効にすることができます。中央設定を使用しない場合は、各リージョンとアカウントで個別にコントロールを有効にする必要があります。

すべての標準にわたってコントロールを有効にする

コントロールが適用されるすべての標準で AWS Security Hub CSPM コントロールを有効にすることをお勧めします。統合コントロールの検出結果を有効にすると、コントロールが複数の標準に属する場合でも、コントロールチェックごとに 1 つの検出結果を受け取ります。

マルチアカウント、マルチリージョン環境でのクロススタンダード有効化

複数の AWS アカウント と でセキュリティコントロールを有効にするには AWS リージョン、委任 Security Hub CSPM 管理者アカウントにサインインし、中央設定を使用する必要があります。

中央設定では、委任管理者は、有効な標準全体で指定されたコントロールを有効にする Security Hub CSPM 設定ポリシーを作成できます。そして、設定ポリシーを特定のアカウントや組織単位 (OU)、またはルートに関連付けることができます。設定ポリシーは、ホームリージョン (集約リージョンとも呼ばれる) およびリンクされているすべてのリージョンで有効になります。

設定ポリシーではカスタマイズが可能です。例えば、ある OU ではすべてのコントロールを有効にし、別の OU では Amazon Elastic Compute Cloud (EC2) コントロールのみを有効にすることができます。詳細度のレベルは、組織のセキュリティカバレッジについて目指す目標によって異なります。標準全体で指定されたコントロールを有効にする設定ポリシーの作成手順については、「設定ポリシーの作成と関連付け」を参照してください。

> **Note**
>
> 委任管理者は、サービスマネージドスタンダードを除くすべての標準でコントロールを管理する設定ポリシーを作成できます AWS Control Tower。この標準のコントロールは、 AWS Control Tower サービスで設定する必要があります。

委任管理者ではなく一部のアカウントに独自のコントロールを設定させたい場合は、委任管理者がそれらのアカウントをセルフマネージドとして指定できます。セルフマネージドアカウントは、リージョンごとにコントロールを個別に設定する必要があります。

単一アカウントとリージョンでのクロススタンダード有効化

中央設定を使用していない場合、またはセルフマネージドアカウントの場合、設定ポリシーを使用して複数のアカウントおよびリージョンでコントロールを一元的に有効にすることはできません。ただ

し、次の手順を使用して、1 つのアカウントおよびリージョンでコントロールを有効にすることができます。

Security Hub CSPM console

1 つのアカウントおよびリージョンの標準全体でコントロールを有効にするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで [コントロール] を選択します。
3. [無効] タブを選択します。
4. コントロールの横にあるオプションを選択します。
5. [コントロールの有効化] を選択します (このオプションは、既に有効になっているコントロールには表示されません)。
6. コントロールを有効にするリージョンごとに、これらの手順を繰り返します。

Security Hub CSPM API

1 つのアカウントおよびリージョンの標準全体でコントロールを有効にするには

1. ListStandardsControlAssociations API を呼び出します。セキュリティコントロール ID を指定します。

   リクエストの例:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. BatchUpdateStandardsControlAssociations API を呼び出します。コントロールが有効になっていない標準の Amazon リソースネーム (ARN) を指定します。標準 ARN を取得するには、`DescribeStandards` を実行します。
3. `AssociationStatus` パラメータを `ENABLED` と等しい値に設定します。既に有効化されているコントロールに対してこれらの手順を実行すると、API は HTTP ステータスコード 200 の応答を返します。

   リクエストの例:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]
}
```

4. コントロールを有効にするリージョンごとに、これらの手順を繰り返します。

AWS CLI

1 つのアカウントおよびリージョンの標準全体でコントロールを有効にするには

1. list-standards-control-associations コマンドを実行します。セキュリティコントロール ID を指定します。

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. batch-update-standards-control-associations コマンドを実行します。コントロールが有効になっていない標準の Amazon リソースネーム (ARN) を指定します。標準 ARN を取得するには、`describe-standards` コマンドを実行します。
3. `AssociationStatus` パラメータを ENABLED と等しい値に設定します。既に有効化されているコントロールに対してこれらの手順を実行すると、コマンドは HTTP ステータスコード 200 の応答を返します。

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0", "AssociationStatus": "ENABLED"}]'
```

4. コントロールを有効にするリージョンごとに、これらの手順を繰り返します。

特定の標準のコントロールを有効にする

AWS Security Hub CSPM で標準を有効にすると、その標準に適用されるすべてのコントロールが自動的に有効になります (この例外はサービスマネージド標準です) 。その後、標準内の特定のコントロールを無効化または再有効化できます。ただし、有効なすべての標準でコントロールの有効化ステータスを一致させることをお勧めします。すべての標準にわたってコントロールを有効にする手順については、「すべての標準にわたってコントロールを有効にする」を参照してください。

標準の詳細ページには、その標準に適用されるコントロールの一覧と、その標準で現在有効化されているコントロールと無効化されているコントロールに関する情報が含まれます。

また、標準の詳細ページで、特定の標準のコントロールを有効にすることもできます。各 AWS アカウント と で、特定の標準でコントロールを個別に有効にする必要があります AWS リージョン。特定の標準でコントロールを有効にした場合、現在のアカウントとリージョンにのみ影響します。

標準のコントロールを有効にするには、まず、そのコントロールが適用される標準を少なくとも 1 つ有効にする必要があります。標準を有効にする手順については、「セキュリティ標準の有効化」を参照してください。1 つ以上の標準でコントロールを有効にすると、Security Hub CSPM はそのコントロールの検出結果の生成を開始します。Security Hub CSPM は、全体的なセキュリティスコアと標準セキュリティスコアの計算にコントロールステータスを含めます。コントロールを複数の標準で有効にしている場合でも、コントロール検出結果を統合して有効にすると、標準全体のセキュリティチェックごとに 1 つの検出結果を受け取ることができます。詳細については、統合コントロールの検出結果を参照してください。

標準でコントロールを有効にするには、そのコントロールが現在のリージョンで使用可能である必要があります。詳細については、「リージョン別のコントロールの可用性」を参照してください。

特定の標準で Security Hub CSPM コントロールを有効にするには、次の手順に従います。以下の手順の代わりに、`UpdateStandardsControl` API アクションを使用して特定の標準のコントロールを有効にすることもできます。すべての標準でコントロールを有効にする手順については、「単一アカウントとリージョンでのクロススタンダード有効化」を参照してください。

Security Hub CSPM console

特定の標準のコントロールを有効にするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで、[セキュリティ基準] を選択します。
3. 該当する標準の [結果を表示する] を選択します。

4. コントロールを選択します。
5. [コントロールの有効化] を選択します (このオプションは、既に有効になっているコントロールには表示されません)。[有効化] を選択して確定します。

Security Hub CSPM API

特定の標準のコントロールを有効にするには

1. ListSecurityControlDefinitions を実行して標準 ARN を提供すると、特定の標準で利用できるコントロールのリストが表示されます。標準 ARN を取得するには、DescribeStandards を実行します。この API は、標準固有のコントロール ID ではなく、標準に依存しないセキュリティコントロール ID を返します。

   リクエストの例:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. ListStandardsControlAssociations を実行し、特定のコントロール ID を提供すると、各標準のコントロールの現在の有効化ステータスが返されます。

   リクエストの例:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. BatchUpdateStandardsControlAssociations を実行します。コントロールを有効にする標準の ARN を指定します。
4. `AssociationStatus` パラメータを `ENABLED` と等しい値に設定します。

   リクエストの例:

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "ENABLED"}]
   }
   ```

AWS CLI

特定の標準のコントロールを有効にするには

1. list-security-control-definitions コマンドを実行して標準 ARN を提供すると、特定の標準で利用できるコントロールのリストが表示されます。標準 ARN を取得するには、describe-standards を実行します。このコマンドは、標準固有のコントロール ID ではなく、標準に依存しないセキュリティコントロール ID を返します。

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. list-standards-control-associations コマンドを実行し、特定のコントロール ID を提供すると、各標準のコントロールの現在の有効化ステータスが返されます。

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. batch-update-standards-control-associations コマンドを実行します。コントロールを有効にする標準の ARN を指定します。
4. AssociationStatus パラメータを ENABLED と等しい値に設定します。

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]'
```

有効な標準で新しいコントロールを自動的に有効化する

AWS Security Hub CSPM は定期的に新しいコントロールをリリースし、1 つ以上の標準に追加します。有効化した標準で新しいコントロールを自動的に有効化するかどうかは、ユーザーが選択できます。

Security Hub CSPM 中央設定を使用して、新しいセキュリティコントロールを自動的に有効にすることをお勧めします。標準全体で無効にするコントロールのリストが含まれた設定ポリシーを作成できます。新しくリリースされたものも含め、他のすべてのコントロールはデフォルトで有効になっています。また、標準全体で有効にするコントロールのリストが含まれたポリシーを作成することもで

きます。新しくリリースされたものも含め、他のすべてのコントロールはデフォルトで無効になっています。詳細については、「Security Hub CSPM の中央設定について」を参照してください。

Security Hub CSPM は、有効にしていない標準に新しいコントロールが追加された場合、新しいコントロールを有効にしません。

以下の手順は、中央設定を使用しない場合にのみ適用されます。

お好みのアクセス方法を選択し、次の手順に従って、有効な標準の新しいコントロールを自動的に有効化します。

> **Note**
>
> 次の手順を使用して新しいコントロールを自動的に有効にすると、コンソールでコントロールを操作し、リリース直後にプログラムで操作できます。ただし、自動有効化されたコントロールの一時的なデフォルトステータスは無効です。Security Hub CSPM がコントロールリリースを処理し、アカウントでコントロールを有効として指定するまでに、最大数日かかることがあります。処理期間中は、コントロールを手動で有効または無効にできます。自動コントロールの有効化が有効になっているかどうかにかかわらず、Security Hub CSPM はその指定を維持します。

Security Hub CSPM console

新しいコントロールを自動的に有効化するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで、[Settings] (設定)、[General] (一般) タブの順に選択します。
3. [コントロール] で [編集] を選択します。
4. [有効になっている標準で新しいコントロールを自動的に有効にする] をオンにします。
5. [保存] を選択します。

Security Hub CSPM API

新しいコントロールを自動的に有効化するには

1. `UpdateSecurityHubConfiguration` を実行します。

2. 有効な標準で新しいコントロールを自動的に有効にするには、`AutoEnableControls` を `true` に設定します。新しいコントロールを自動的に有効化しない場合は、`AutoEnableControls` を false に設定します。

AWS CLI

新しいコントロールを自動的に有効化するには

1. `update-security-hub-configuration` コマンドを実行します。
2. 有効な標準で新しいコントロールを自動的に有効にするには、`--auto-enable-controls` を指定します。新しいコントロールを自動的に有効化しない場合は、`--no-auto-enable-controls` を指定します。

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

コマンドの例

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

新しいコントロールを自動的に有効化しない場合は、手動で有効化する必要があります。手順については、「Security Hub CSPM でのコントロールの有効化」を参照してください。

Security Hub CSPM でのコントロールの無効化

検出結果のノイズを減らすには、環境に関連しないコントロールを無効にすると便利です。 AWS Security Hub CSPM では、すべてのセキュリティ標準または特定の標準に対してのみコントロールを無効にすることができます。

すべての標準でコントロールを無効にすると、以下が発生します。

- コントロールのセキュリティチェックは実行されなくなります。
- コントロールに対して追加の検出結果は生成されません。
- コントロールの既存の検出結果は更新されなくなりました。
- コントロールの既存の検出結果は、通常はベストエフォートベースで 3~5 日以内に自動的にアーカイブされます。

- Security Hub CSPM は、コントロール用に作成した関連 AWS Config ルールをすべて削除します。

特定の標準のみのコントロールを無効にすると、Security Hub CSPM はそれらの標準のみのコントロールのセキュリティチェックの実行を停止します。これにより、これらの各標準のセキュリティスコアの計算からコントロールも削除されます。コントロールが他の標準で有効になっている場合、Security Hub CSPM は必要に応じて関連する AWS Config ルールを保持し、他の標準に対するコントロールのセキュリティチェックを引き続き実行します。Security Hub CSPM には、他の各標準のセキュリティスコアを計算する際のコントロールも含まれています。これは、セキュリティスコアの概要に影響します。

標準を無効にすると、標準に適用されるすべてのコントロールがその標準に対して自動的に無効になります。ただし、コントロールは他の標準で引き続き有効になる場合があります。標準を無効にすると、Security Hub CSPM は標準に対して無効にされたコントロールを追跡しません。したがって、後で同じ標準を再度有効にすると、その標準に適用されるすべてのコントロールが自動的に有効になります。標準の無効化の詳細については、「セキュリティ標準の無効化」を参照してください。

コントロールを無効にすることは永続的なアクションではありません。コントロールを無効にし、そのコントロールを含む標準を有効にするとします。その後、コントロールはその標準で有効になります。Security Hub CSPM で標準を有効にすると、標準に適用されるすべてのコントロールが自動的に有効になります。標準を有効にする方法については、「」を参照してください標準を有効にする。

トピック

- すべての標準にわたってコントロールを無効にする
- 特定の標準のコントロールを無効にする
- Security Hub CSPM で無効にする推奨コントロール

すべての標準にわたってコントロールを無効にする

組織全体の整合性を維持するために、標準全体で AWS Security Hub CSPM コントロールを無効にすることをお勧めします。特定の標準でのみコントロールを無効にすると、他の標準で有効になっている場合、コントロールの結果が引き続き表示されます。

複数のアカウントとリージョンでのクロススタンダード無効化

複数の AWS アカウント と でセキュリティコントロールを無効にするには AWS リージョン、中央設定を使用する必要があります。

中央設定を使用する場合、委任管理者は、有効な標準全体で指定されたコントロールを無効にする Security Hub CSPM 設定ポリシーを作成できます。そして、設定ポリシーを特定のアカウント、OU、またはルートに関連付けることができます。設定ポリシーは、ホームリージョン (集約リージョンとも呼ばれる) およびリンクされているすべてのリージョンで有効になります。

設定ポリシーではカスタマイズが可能です。たとえば、1 つの OU ですべての AWS CloudTrail コントロールを無効にすることを選択し、別の OU ですべての IAM コントロールを無効にすることを選択できます。詳細度のレベルは、組織のセキュリティカバレッジについて目指す目標によって異なります。標準全体で指定されたコントロールを無効にする設定ポリシーの作成手順については、「設定ポリシーの作成と関連付け」を参照してください。

> **Note**
>
> 委任管理者は、サービスマネージドスタンダードを除くすべての標準でコントロールを管理する設定ポリシーを作成できます AWS Control Tower。この標準のコントロールは、 AWS Control Tower サービスで設定する必要があります。

委任管理者ではなく一部のアカウントに独自のコントロールを設定させたい場合は、委任管理者がそれらのアカウントをセルフマネージドとして指定できます。セルフマネージドアカウントは、リージョンごとにコントロールを個別に設定する必要があります。

単一のアカウントとリージョンでのクロススタンダード無効化

中央設定を使用していない場合、またはセルフマネージドアカウントの場合、設定ポリシーを使用して複数のアカウントおよびリージョンでコントロールを一元的に無効にすることはできません。ただし、1 つのアカウントとリージョンでコントロールを無効にすることができます。

Security Hub CSPM console

1 つのアカウントおよびリージョンの標準全体でコントロールを無効にするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで [コントロール] を選択します。
3. コントロールの横にあるオプションを選択します。
4. コントロールを無効にするを選択します。このオプションは、既に無効になっているコントロールには表示されません。

5. コントロールを無効にする理由を選択し、[無効化] を選択して確定します。
6. コントロールを無効にするリージョンごとに、これらの手順を繰り返します。

Security Hub CSPM API

1 つのアカウントおよびリージョンの標準全体でコントロールを無効にするには

1. ListStandardsControlAssociations API を呼び出します。セキュリティコントロール ID を指定します。

   リクエストの例:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. BatchUpdateStandardsControlAssociations API を呼び出します。コントロールが有効になっている標準の ARN を指定します。標準 ARN を取得するには、`DescribeStandards` を実行します。
3. `AssociationStatus` パラメータを `DISABLED` と等しい値に設定します。既に無効化されているコントロールに対してこれらの手順を実行すると、API は HTTP ステータスコード 200 の応答を返します。

   リクエストの例:

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-
   benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not
    applicable to environment"}, {"SecurityControlId": "IAM.1", "StandardsArn":
    "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/
   v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
    environment"}}]
   }
   ```

4. コントロールを無効にするリージョンごとに、これらの手順を繰り返します。

AWS CLI

1 つのアカウントおよびリージョンの標準全体でコントロールを無効にするには

1. list-standards-control-associations コマンドを実行します。セキュリティコントロール ID を指定します。

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. batch-update-standards-control-associations コマンドを実行します。コントロールが有効になっている標準の ARN を指定します。標準 ARN を取得するには、`describe-standards` コマンドを実行します。
3. `AssociationStatus` パラメータを `DISABLED` と等しい値に設定します。既に無効化されているコントロールに対してこれらの手順を実行すると、コマンドは HTTP ステータスコード 200 の応答を返します。

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable
 to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":
 "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/v/1.4.0",
 "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}]'
```

4. コントロールを無効にするリージョンごとに、これらの手順を繰り返します。

特定の標準のコントロールを無効にする

コントロールは、すべての標準ではなく、特定のセキュリティ標準でのみ無効にできます。コントロールが他の有効な標準に適用される場合、 AWS Security Hub CSPM は引き続きコントロールのセキュリティチェックを実行し、引き続きコントロールの検出結果を受け取ります。

コントロールが適用されるすべての有効な標準にわたって、コントロールの有効化ステータスを一致させることをお勧めします。適用されるすべての標準でコントロールを無効にする方法については、「」を参照してくださいすべての標準にわたってコントロールを無効にする。

また、標準の詳細ページで、特定の標準のコントロールを無効にすることもできます。各 AWS アカウント および で、特定の標準のコントロールを個別に無効にする必要があります AWS リージョン。特定の標準でコントロールを無効にすると、現在のアカウントとリージョンのみに影響します。

任意の方法を選択し、以下の手順に従って 1 つ以上の特定の標準でコントロールを無効にします。

Security Hub CSPM console

特定の標準のコントロールを無効にするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで、[セキュリティ基準] を選択します。該当する標準の [結果を表示する] を選択します。
3. コントロールを選択します。
4. コントロールを無効にする を選択します。このオプションは、既に無効になっているコントロールには表示されません。
5. コントロールを無効にする理由を入力し、[無効化] を選択して確定します。

Security Hub CSPM API

特定の標準のコントロールを無効にするには

1. `ListSecurityControlDefinitions` を実行して標準 ARN を提供すると、特定の標準で利用できるコントロールのリストが表示されます。標準 ARN を取得するには、`DescribeStandards` を実行します。この API は、標準固有のコントロール ID ではなく、標準に依存しないセキュリティコントロール ID を返します。

   リクエストの例:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. `ListStandardsControlAssociations` を実行し、特定のコントロール ID を提供すると、各標準のコントロールの現在の有効化ステータスが返されます。

   リクエストの例:

```
{
    "SecurityControlId": "IAM.1"
}
```

3. BatchUpdateStandardsControlAssociations を実行します。コントロールを無効にする標準の ARN を指定します。
4. AssociationStatus パラメータを DISABLED と等しい値に設定します。既に無効化されているコントロールに対してこれらの手順を実行すると、API は HTTP ステータスコード 200 の応答を返します。

   リクエストの例:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED",  "UpdatedReason": "Not applicable to
 environment"}]
}
```

AWS CLI

特定の標準のコントロールを無効にするには

1. list-security-control-definitions コマンドを実行して標準 ARN を提供すると、特定の標準で利用できるコントロールのリストが表示されます。標準 ARN を取得するには、describe-standards を実行します。このコマンドは、標準固有のコントロール ID ではなく、標準に依存しないセキュリティコントロール ID を返します。

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. list-standards-control-associations コマンドを実行し、特定のコントロール ID を提供すると、各標準のコントロールの現在の有効化ステータスが返されます。

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. batch-update-standards-control-associations コマンドを実行します。コントロールを無効にする標準の ARN を指定します。
4. AssociationStatus パラメータを DISABLED と等しい値に設定します。既に有効化されているコントロールに対してこれらの手順を実行すると、コマンドは HTTP ステータスコード 200 の応答を返します。

```
aws securityhub  --region us-east-1 batch-update-standards-control-
associations --standards-control-association-updates '[{"SecurityControlId":
 "CloudTrail.1", "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "AssociationStatus": "DISABLED",
 "UpdatedReason": "Not applicable to environment"}]'
```

Security Hub CSPM で無効にする推奨コントロール

検出結果のノイズと使用コストを削減するために、一部の AWS Security Hub CSPM コントロールを無効にすることをお勧めします。

グローバルリソースを使用するコントロール

一部の はグローバルリソース AWS のサービス をサポートしています。つまり、任意の からリソースにアクセスできます AWS リージョン。のコストを節約するために AWS Config、1 つのリージョンを除くすべてのリージョンでグローバルリソースの記録を無効にすることができます。ただし、これを行った後も、Security Hub CSPM はコントロールが有効になっているすべてのリージョンでセキュリティチェックを実行し、リージョンごとのアカウントあたりのチェック数に基づいて課金されます。したがって、検出結果のノイズを減らし、Security Hub CSPM のコストを節約するには、グローバルリソースを記録するリージョンを除くすべてのリージョンで、グローバルリソースを含むコントロールを無効にする必要もあります。

コントロールにグローバルリソースが含まれるが、1 つのリージョンでのみ利用可能な場合、そのリージョンでコントロールを無効にすると、基盤となるリソースの検出結果を取得できなくなります。この場合、コントロールを有効にしておくことをお勧めします。クロスリージョン集約を使用する場合、コントロールが利用可能なリージョンは、集約リージョンまたはリンクされたリージョンのいずれかである必要があります。以下のコントロールにはグローバルリソースが含まれますが、1 つのリージョンでのみ使用できます。

- すべての CloudFront コントロール – 米国東部 (バージニア北部) リージョンでのみ使用可能
- GlobalAccelerator.1 – 米国西部 (オレゴン) リージョンでのみ使用可能

- Route53.2 – 米国東部 (バージニア北部) リージョンでのみ使用可能
- WAF.1、WAF.6、WAF.7、WAF.8 – 米国東部 (バージニア北部) リージョンでのみ利用可能

> **Note**
>
> 中央設定を使用する場合、Security Hub CSPM は、ホームリージョンを除くすべてのリージョンでグローバルリソースを含むコントロールを自動的に無効にします。設定ポリシーを通じて有効を選択したその他のコントロールは、利用可能なすべてのリージョンで有効になります。これらのコントロールの検出結果を 1 つのリージョンのみに制限するには、 AWS Config レコーダー設定を更新し、ホームリージョンを除くすべてのリージョンでグローバルリソース記録をオフにします。
> グローバルリソースを含む有効なコントロールがホームリージョンでサポートされていない場合、Security Hub CSPM は、コントロールがサポートされているリンクされた 1 つのリージョンでコントロールを有効にしようとします。中央設定では、ホームリージョンまたはリンクされたリージョンで利用できないコントロールのカバレッジがありません。
> 中央設定の詳細については、「Security Hub CSPM の中央設定について」を参照してください。

定期的なスケジュールタイプのコントロールの場合、請求を防ぐために Security Hub CSPM で無効にする必要があります。 AWS Config パラメータを に設定`false`して も`includeGlobalResourceTypes`、定期的な Security Hub CSPM コントロールには影響しません。

次の Security Hub CSPM コントロールは、グローバルリソースを使用します。

- [Account.1] のセキュリティ連絡先情報は に提供する必要があります AWS アカウント
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります

- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.10] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します
- [IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します
- [IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します

- [IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します
- [IAM.15] IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認します
- [IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています
- [IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します
- [IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

CloudTrail ログ記録コントロール

このコントロールは、 AWS Key Management Service （ AWS KMS) を使用して AWS CloudTrail 証跡ログを暗号化します。これらの証跡を一元的なログ記録アカウントに記録する場合は、一元的なログ記録が行われるアカウントとリージョンでのみこのコントロールを有効にする必要があります。

> **Note**
>
> 中央設定を使用した場合、コントロールの有効化ステータスは、ホームリージョンおよびリンクされたリージョンで統一されます。一部のリージョンでコントロールを無効にして、他のリージョンで有効にすることはできません。この場合は、以下のコントロールの検出結果を抑制し、検出結果のノイズを減らします。

- [CloudTrail.2] CloudTrail は保管時の暗号化を有効にする必要があります

CloudWatch アラームコントロール

Amazon CloudWatch アラームの代わりに異常検出に Amazon Amazon GuardDuty を使用する場合は、CloudWatch アラームに焦点を当てた以下のコントロールを無効にできます。

- [CloudWatch.1] 「ルート」ユーザーの使用に対するログメトリクスフィルターとアラームが存在する必要があります
- [CloudWatch.2] 不正な API 呼び出しに対してログメトリクスフィルターとアラームが存在することを確認します
- [CloudWatch.3] MFA を使用しないマネジメントコンソールサインインに対してログメトリクスフィルターとアラームが存在することを確認します
- [CloudWatch.4] IAM ポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します
- [CloudWatch.5] CloudTrail 設定変更のログメトリクスフィルターとアラームが存在することを確認する
- [CloudWatch.6] AWS Management Console 認証失敗のログメトリクスフィルターとアラームが存在することを確認する
- [CloudWatch.7] カスタマーマネージドキーの無効化またはスケジュールされた削除に対するログメトリクスフィルターとアラームが存在することを確認します
- [CloudWatch.8] S3 バケットポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します
- [CloudWatch.9] AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する
- [CloudWatch.10] セキュリティグループの変更に対するログメトリクスフィルターとアラームが存在することを確認します

- [CloudWatch.11] ネットワークアクセスコントロールリスト (NACL) への変更に対するログメトリクスフィルターとアラームが存在することを確認します
- [CloudWatch.12] ネットワークゲートウェイへの変更に対するログメトリクスフィルターとアラームが存在することを確認します
- [CloudWatch.13] ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認します
- [CloudWatch.14] VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認します

Security Hub CSPM のセキュリティチェックとスコアについて

有効にするコントロールごとに、 AWS Security Hub CSPM はセキュリティチェックを実行します。セキュリティチェックは、特定の AWS リソースがコントロールに含まれるルールに準拠しているかどうかを示す結果を生成します。

一部のチェックは定期的なスケジュールで実行されます。その他のチェックは、リソースの状態が変更された場合にのみ実行されます。詳細については、「セキュリティチェックの実行スケジュール」を参照してください。

多くのセキュリティチェックでは、 AWS Config マネージドルールまたはカスタムルールを使用してコンプライアンス要件を確立します。これらのチェックを実行するには、必要なリソースのリソース記録を設定 AWS Config して有効にする必要があります。設定の詳細については AWS Config、「」を参照してくださいSecurity Hub CSPM AWS Config の有効化と設定。標準ごとに記録する必要がある AWS Config リソースのリストについては、「」を参照してくださいコントロールの検出結果に必要な AWS Config リソース。その他のコントロールは、Security Hub CSPM によって管理され、前提条件を必要としないカスタム Lambda 関数を使用します。

Security Hub CSPM がセキュリティチェックを実行すると、検出結果が生成され、コンプライアンスステータスが割り当てられます。コンプライアンスステータスの詳細については、「Security Hub CSPM の検出結果のコンプライアンスステータスの評価」を参照してください。

Security Hub CSPM は、コントロール検出結果のコンプライアンスステータスを使用して、全体的なコントロールステータスを決定します。コントロールステータスに基づいて、Security Hub CSPM は、有効なすべてのコントロールと特定の標準のセキュリティスコアも計算します。詳細については、「the section called “コンプライアンスステータスとコントロールステータス”」および「the section called “セキュリティスコアの計算”」を参照してください。

統合コントロールの検出結果を有効にすると、コントロールが複数の標準に関連付けられている場合でも、Security Hub CSPM は 1 つの検出結果を生成します。詳細については、「統合されたコントロールの検出結果」を参照してください。

トピック

- コントロールの検出結果に必要な AWS Config リソース
- セキュリティチェックの実行スケジュール
- コントロールの結果を生成および更新する
- コンプライアンスステータスとコントロールステータスの評価
- セキュリティスコアの計算

コントロールの検出結果に必要な AWS Config リソース

AWS Security Hub CSPM では、一部のコントロールは、 AWS リソースの設定変更を検出するサービスにリンクされた AWS Config ルールを使用します。Security Hub CSPM がこれらのコントロールの正確な検出結果を生成するには、リソース記録を有効に AWS Config してオンにする必要があります AWS Config。Security Hub CSPM が AWS Config ルールを使用する方法と、 を有効にして設定する方法については AWS Config、「」を参照してくださいSecurity Hub CSPM AWS Config の有効化と設定。リソースの記録の詳細については、「 AWS Config デベロッパーガイド」の「設定レコーダーの使用」を参照してください。

正確なコントロール結果を受け取るには、変更がトリガーされたスケジュールタイプで有効なコントロールの AWS Config リソース記録を有効にする必要があります。定期的なスケジュールタイプの一部のコントロールでは、リソースの記録も必要です。このページには、これらの Security Hub CSPM コントロールに必要なリソースが一覧表示されます。

Security Hub CSPM コントロールは、マネージド AWS Config ルールまたはカスタム Security Hub CSPM ルールに依存します。リソースを記録するアクセス許可が AWS Config に付与されない AWS Identity and Access Management (IAM) ポリシーや AWS Organizations 管理ポリシーがないことを確認します。Security Hub CSPM コントロールは、リソース設定を直接評価し、 AWS Organizations ポリシーを考慮しません。

> **Note**
>
> コントロールが利用できない AWS リージョン では、対応するリソースは では使用できません AWS Config。これらの制限のリストについては、「」を参照してくださいSecurity Hub CSPM コントロールのリージョン制限。

トピック

- すべての Security Hub CSPM コントロールに必要なリソース
- Foundational Security Best Practices AWS 標準に必要なリソース
- CIS AWS Foundations Benchmark に必要なリソース
- NIST SP 800-53 リビジョン 5 標準に必要なリソース
- NIST SP 800-171 リビジョン 2 標準に必要なリソース
- PCI DSS v3.2.1 に必要なリソース
- リソースタグ付け標準に必要な AWS リソース
- AWS Control Tower サービスマネージド標準に必要なリソース

すべての Security Hub CSPM コントロールに必要なリソース

Security Hub CSPM が有効化され、 AWS Config ルールを使用する変更トリガーコントロールの検出結果を生成するには、次のタイプのリソースを に記録する必要があります AWS Config。この表は、特定のタイプのリソースを評価するコントロールも示しています。1 つのコントロールが複数のタイプのリソースを評価する場合があります。

AWS のサービス	リソースタイプ	関連するコントロール
AWS Amplify	`AWS::Amplify::App`	Amplify.1
	`AWS::Amplify::Branch`	Amplify.2
Amazon API Gateway	`AWS::ApiGateway::Stage`	APIGateway.1 APIGateway.2 APIGateway.3 APIGateway.4 APIGateway.5

AWS のサービス	リソースタイプ	関連するコントロール
	`AWS::ApiGatewayV2::Stage`	APIGateway.1 APIGateway.9
AWS AppConfig	`AWS::AppConfig::Application`	AppConfig.1
	`AWS::AppConfig::ConfigurationProfile`	AppConfig.2
	`AWS::AppConfig::Environment`	AppConfig.3
	`AWS::AppConfig::ExtensionAssociation`	AppConfig.4
Amazon AppFlow	`AWS::AppFlow::Flow`	AppFlow.1
AWS App Runner	`AWS::AppRunner::Service`	AppRunner.1
	`AWS::AppRunner::VpcConnector`	AppRunner.2
AWS AppSync	`AWS::AppSync::GraphQLApi`	AppSync.2 AppSync.4 AppSync.5

AWS のサービス	リソースタイプ	関連するコントロール
	`AWS::AppSync::ApiCache`	AppSync.1 AppSync.6
AWS Backup	`AWS::Backup::BackupPlan`	Backup.5
	`AWS::Backup::BackupVault`	Backup.3
	`AWS::Backup::RecoveryPoint`	Backup.1 Backup.2
	`AWS::Backup::ReportPlan`	Backup.4
AWS Batch	`AWS::Batch::ComputeEnvironment`	バッチ.3 バッチ.4
	`AWS::Batch::JobQueue`	バッチ.1
	`AWS::Batch::SchedulingPolicy`	バッチ.2
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`	ACM.1 ACM.2 ACM.3
Amazon Athena	`AWS::Athena::DataCatalog`	Athena.2

AWS のサービス	リソースタイプ	関連するコントロール
	`AWS::Athena::WorkGroup`	Athena.3 Athena.4
AWS CloudFormation	`AWS::CloudFormation::Stack`	CloudFormation.2
Amazon CloudFront	`AWS::CloudFront::Distribution`	CloudFront.1 CloudFront.3 CloudFront.4 CloudFront.5 CloudFront.6 CloudFront.7 CloudFront.8 CloudFront.9 CloudFront.10 CloudFront.13 CloudFront.14 CloudFront.15
AWS CloudTrail	`AWS::CloudTrail::Trail`	CloudTrail.9
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	CloudWatch.15 CloudWatch.17

AWS のサービス	リソースタイプ	関連するコントロール
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	CodeArtifact.1
AWS CodeBuild	`AWS::CodeBuild::Project`	CodeBuild.1 CodeBuild.2 CodeBuild.3 CodeBuild.4
	`AWS::CodeBuild::ReportGroup`	CodeBuild.7
Amazon CodeGuru Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`	CodeGuruProfiler.1
Amazon CodeGuru Reviewer	`AWS::CodeGuruReviewer::RepositoryAssociation`	CodeGuruReviewer.1
Amazon Cognito	`AWS::Cognito::IdentityPool`	Cognito.2
	`AWS::Cognito::UserPool`	Cognito.1

AWS のサービス	リソースタイプ	関連するコントロール
Amazon Connect	`AWS::CustomerProfiles::ObjectType`	Connect.1
	`AWS::Connect::Instance`	Connect.2
AWS DataSync	`AWS::DataSync::Task`	DataSync.1 DataSync.2
Amazon Detective	`AWS::Detective::Graph`	Detective.1
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate`	DMS.2
	`AWS::DMS::Endpoint`	DMS.9 DMS.10 DMS.11 DMS.12
	`AWS::DMS::EventSubscription`	DMS.3
	`AWS::DMS::ReplicationInstance`	DMS.4 DMS.6
	`AWS::DMS::ReplicationSubnetGroup`	DMS.5

AWS のサービス	リソースタイプ	関連するコントロール
	`AWS::DMS::ReplicationTask`	DMS.7 DMS.8
Amazon DynamoDB	`AWS::DynamoDB::Table`	DynamoDB.1 DynamoDB.2 DynamoDB.5 DynamoDB.6
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`	EC2.51
	`AWS::EC2::CustomerGateway`	EC2.36
	`AWS::EC2::DHCPOptions`	EC2.174
	`AWS::EC2::EIP`	EC2.12 EC2.37
	`AWS::EC2::FlowLog`	EC2.48

AWS のサービス	リソースタイプ	関連するコントロール
	AWS::EC2::Instance	EC2.4 EC2.8 EC2.9 EC2.17 EC2.24 EC2.38 EMR.1 SSM.1
	AWS::EC2::InternetGateway	EC2.39
	AWS::EC2::LaunchTemplate	EC2.25 EC2.170 EC2.175
	AWS::EC2::NatGateway	EC2.40
	AWS::EC2::NetworkAcl	EC2.16 EC2.21 EC2.41
	AWS::EC2::NetworkInterface	EC2.22 EC2.35 EC2.180

AWS のサービス	リソースタイプ	関連するコントロール
	AWS::EC2::PrefixList	EC2.176
	AWS::EC2::RouteTable	EC2.42
	AWS::EC2::SecurityGroup	EC2.2 EC2.13 EC2.14 EC2.18 EC2.19 EC2.43
	AWS::EC2::SpotFleet	EC2.173
	AWS::EC2::Subnet	EC2.15 EC2.44 ElastiCache.7
	AWS::EC2::TrafficMirrorFilter	EC2.178
	AWS::EC2::TrafficMirrorSession	EC2.177
	AWS::EC2::TrafficMirrorTarget	EC2.179

AWS のサービス	リソースタイプ	関連するコントロール
	AWS::EC2::TransitGateway	EC2.23 EC2.52
	AWS::EC2::TransitGatewayAttachment	EC2.33
	AWS::EC2::TransitGatewayRouteTable	EC2.34
	AWS::EC2::Volume	EC2.3 EC2.45
	AWS::EC2::VPC	EC2.6 EC2.46
	AWS::EC2::VPCBlockPublicAccessOptions	EC2.172
	AWS::EC2::VPCEndpointService	EC2.47
	AWS::EC2::VPCPeeringConnection	EC2.49

AWS のサービス	リソースタイプ	関連するコントロール
	`AWS::EC2::VPNConnection`	EC2.20 EC2.171
	`AWS::EC2::VPNGateway`	EC2.50
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	AutoScaling.1 AutoScaling.2 AutoScaling.6 AutoScaling.9 AutoScaling.10
	`AWS::AutoScaling::LaunchConfiguration`	AutoScaling.3 Autoscaling.5
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`	SSM.3
	`AWS::SSM::ManagedInstanceInventory`	SSM.1
	`AWS::SSM::PatchCompliance`	SSM.2
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`	ECR.4

AWS のサービス	リソースタイプ	関連するコントロール
	`AWS::ECR::Repository`	ECR.2 ECR.3 ECR.5
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`	ECS.12 ECS.14
	`AWS::ECS::Service`	ECS.2 ECS.10 ECS.13
	`AWS::ECS::TaskDefinition`	ECS.1 ECS.3 ECS.4 ECS.5 ECS.8 ECS.9 ECS.15 ECS.17
	`AWS::ECS::TaskSet`	ECS.16
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`	EFS.3 EFS.4 EFS.5

AWS のサービス	リソースタイプ	関連するコントロール
	`AWS::EFS::FileSystem`	EFS.7 EFS.8
Amazon エラスティックKubernetesサービス (Amazon EKS)	`AWS::EKS::Cluster`	EKS.2 EKS.6 EKS.8
	`AWS::EKS::IdentityProviderConfig`	EKS.7
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`	ElasticBeanstalk.1 ElasticBeanstalk.2 ElasticBeanstalk.3
エラスティックロードバランシング	`AWS::ElasticLoadBalancing::LoadBalancer`	ELB.2 ELB.3 ELB.5 ELB.7 ELB.8 ELB.9 ELB.10 ELB.14
	`AWS::ElasticLoadBalancingV2::Listener`	ELB.17 ELB.18

AWS のサービス	リソースタイプ	関連するコントロール
	`AWS::ElasticLoadBalancingV2::LoadBalancer`	ELB.1 ELB.4 ELB.5 ELB.6 ELB.12 ELB.13 ELB.16
ElasticSearch	`AWS::Elasticsearch::Domain`	ES.3 ES.4 ES.5 ES.6 ES.7 ES.8 ES.9
Amazon EMR	`AWS::EMR::SecurityConfiguration`	EMR.3 EMR.4
Amazon EventBridge	`AWS::Events::EventBus`	EventBridge.2 EventBridge.3
	`AWS::Events::Endpoint`	EventBridge.4

AWS のサービス	リソースタイプ	関連するコントロール
Amazon Fraud Detector	`AWS::FraudDetector::EntityType`	FraudDetector.1
	`AWS::FraudDetector::Label`	FraudDetector.2
	`AWS::FraudDetector::Outcome`	FraudDetector.3
	`AWS::FraudDetector::Variable`	FraudDetector.4
AWS Global Accelerator	`AWS::GlobalAccelerator::Accelerator`	GlobalAccelerator.1
AWS Glue	`AWS::Glue::Job`	Glue.1 Glue.4
	`AWS::Glue::MLTransform`	Glue.3
Amazon GuardDuty	`AWS::GuardDuty::Detector`	GuardDuty.4
	`AWS::GuardDuty::Filter`	GuardDuty.2
	`AWS::GuardDuty::IPSet`	GuardDuty.3

AWS のサービス	リソースタイプ	関連するコントロール
AWS Identity and Access Management (IAM)	`AWS::IAM::Group`	IAM.27 KMS.2
	`AWS::IAM::Policy`	IAM.1 IAM.21 KMS.1
	`AWS::IAM::Role`	IAM.24 IAM.27 KMS.2
	`AWS::IAM::User`	IAM.2 IAM.3 IAM.5 IAM.8 IAM.19 IAM.22 IAM.25 IAM.27 KMS.2
AWS Identity and Access Management Access Analyzer	`AWS::AccessAnalyzer::Analyzer`	IAM.23

AWS のサービス	リソースタイプ	関連するコントロール
Amazon Interactive Video Service (Amazon IVS)	`AWS::IVS::PlaybackKeyPair`	IVS.1
	`AWS::IVS::RecordingConfiguration`	IVS.2
	`AWS::IVS::Channel`	IVS.3
AWS IoT	`AWS::IoT::Authorizer`	IoT.4
	`AWS::IoT::Dimension`	IoT.3
	`AWS::IoT::MitigationAction`	IoT.2
	`AWS::IoT::Policy`	IoT.6
	`AWS::IoT::RoleAlias`	IoT.5
	`AWS::IoT::SecurityProfile`	IoT.1
AWS IoT イベント	`AWS::IoTEvents::AlarmModel`	IoTEvents.3

AWS のサービス	リソースタイプ	関連するコントロール
	`AWS::IoTEvents::DetectorModel`	IoTEvents.2
	`AWS::IoTEvents::Input`	IoTEvents.1
AWS IoT SiteWise	`AWS::IoTSiteWise::AssetModel`	IoTSiteWise.1
	`AWS::IoTSiteWise::Dashboard`	IoTSiteWise.2
	`AWS::IoTSiteWise::Gateway`	IoTSiteWise.3
	`AWS::IoTSiteWise::Portal`	IoTSiteWise.4
	`AWS::IoTSiteWise::Project`	IoTSiteWise.5
AWS IoT TwinMaker	`AWS::IoTTwinMaker::Entity`	IoTTwinMaker.4
	`AWS::IoTTwinMaker::Scene`	IoTTwinMaker.3

AWS のサービス	リソースタイプ	関連するコントロール
	`AWS::IoTTwinMaker::SyncJob`	IoTTwinMaker.1
	`AWS::IoTTwinMaker::Workspace`	IoTTwinMaker.2
AWS IoT Wireless	`AWS::IoTWireless::MulticastGroup`	IoTWireless.1
	`AWS::IoTWireless::ServiceProfile`	IoTWireless.2
	`AWS::IoTWireless::FuotaTask`	IoTWireless.3
Amazon Keyspaces (Apache Cassandra 向け)	`AWS::Cassandra::Keyspace`	Keyspaces.1
Amazon Kinesis	`AWS::Kinesis::Stream`	Kinesis.1 Kinesis.2 Kinesis.3
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias`	S3.17
	`AWS::KMS::Key`	KMS.3 KMS.5 S3.17

AWS のサービス	リソースタイプ	関連するコントロール
AWS Lambda	`AWS::Lambda::Function`	Lambda.1 Lambda.2 Lambda.3 Lambda.5 Lambda.6 Lambda.7
Amazon MSK	`AWS::MSK::Cluster`	MSK.1 MSK.2 MSK.4 MSK.6
	`AWS::KafkaConnect::Connector`	MSK.3 MSK.5
Amazon MQ	`AWS::AmazonMQ::Broker`	MQ.2 MQ.3 MQ.4 MQ.5 MQ.6

AWS のサービス	リソースタイプ	関連するコントロール
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	NetworkFirewall.1 NetworkFirewall.7 NetworkFirewall.9 NetworkFirewall.10
	`AWS::NetworkFirewall::FirewallPolicy`	NetworkFirewall.3 NetworkFirewall.4 NetworkFirewall.5 NetworkFirewall.8
	`AWS::NetworkFirewall::RuleGroup`	NetworkFirewall.6

AWS のサービス	リソースタイプ	関連するコントロール
Amazon OpenSearch Service	`AWS::OpenSearch::Domain`	Opensearch.1 Opensearch.2 Opensearch.3 Opensearch.4 Opensearch.5 Opensearch.6 Opensearch.7 Opensearch.8 Opensearch.9 Opensearch.10 Opensearch.11
AWS Private CA	`AWS::ACMPCA::CertificateAuthority`	PCA.2

AWS のサービス	リソースタイプ	関連するコントロール
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`	DocumentDB.1 DocumentDB.2 DocumentDB.4 DocumentDB.5 Neptune.1 Neptune.2 Neptune.4 Neptune.5 Neptune.7 Neptune.8 Neptune.9 RDS.7 RDS.12 RDS.14 RDS.15 RDS.16 RDS.24 RDS.27 RDS.28 RDS.34 RDS.35

AWS のサービス	リソースタイプ	関連するコントロール
		RDS.37
	`AWS::RDS::DBClusterSnapshot`	DocumentDB.3 Neptune.3 Neptune.6 RDS.1 RDS.4 RDS.29

AWS のサービス	リソースタイプ	関連するコントロール
	`AWS::RDS::DBInstance`	RDS.2 RDS.3 RDS.5 RDS.6 RDS.8 RDS.9 RDS.10 RDS.11 RDS.13 RDS.17 RDS.18 RDS.23 RDS.25 RDS.30 RDS.36 RDS.40
	`AWS::RDS::DBSecurityGroup`	RDS.31

AWS のサービス	リソースタイプ	関連するコントロール
	`AWS::RDS::DBSnapshot`	RDS.1 RDS.4 RDS.32
	`AWS::RDS::DBSubnetGroup`	RDS.33
	`AWS::RDS::EventSubscription`	RDS.19 RDS.20 RDS.21 RDS.22
Amazon Redshift	`AWS::Redshift::Cluster`	Redshift.1 Redshift.2 Redshift.3 Redshift.4 Redshift.6 Redshift.7 Redshift.8 Redshift.9 Redshift.10 Redshift.11 Redshift.18

AWS のサービス	リソースタイプ	関連するコントロール
	`AWS::Redshift::ClusterParameterGroup`	Redshift.2 Redshift.17
	`AWS::Redshift::ClusterSnapshot`	Redshift.13
	`AWS::Redshift::ClusterSubnetGroup`	Redshift.14 Redshift.16
	`AWS::Redshift::EventSubscription`	Redshift.12
Amazon Route 53	`AWS::Route53::HostedZone`	Route53.2
	`AWS::Route53::HealthCheck`	Route53.1
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint`	S3.19
	`AWS::S3::AccountPublicAccessBlock`	S3.2 S3.3

AWS のサービス	リソースタイプ	関連するコントロール
	`AWS::S3::Bucket`	CloudTrail.6 CloudTrail.7 S3.2 S3.3 S3.5 S3.6 S3.7 S3.8 S3.9 S3.10 S3.11 S3.12 S3.13 S3.14 S3.15 S3.17 S3.20
	`AWS::S3::MultiRegionAccessPoint`	S3.24

AWS のサービス	リソースタイプ	関連するコントロール
	`AWS::S3Express::DirectoryBucket`	S3.25
Amazon SageMaker AI	`AWS::SageMaker::AppImageConfig`	SageMaker.6
	`AWS::SageMaker::Image`	SageMaker.7
	`AWS::SageMaker::Model`	SageMaker.5
	`AWS::SageMaker::NotebookInstance`	SageMaker.2 SageMaker.3
AWS Secrets Manager	`AWS::SecretsManager::Secret`	SecretsManager.1 SecretsManager.2 SecretsManager.5
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`	ServiceCatalog.1
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet`	SES.2
	`AWS::SES::ContactList`	SES.1

AWS のサービス	リソースタイプ	関連するコントロール
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`	SNS.1 SNS.3 SNS.4
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`	SQS.1 SQS.2 SQS.3
AWS Step Functions	`AWS::StepFunctions::StateMachine`	StepFunctions.1
	`AWS::StepFunctions::Activity`	StepFunctions.2
AWS Systems Manager (SSM)	`AWS::SSM::Document`	SSM.5
AWS Transfer Family	`AWS::Transfer::Agreement`	Transfer.4
	`AWS::Transfer::Certificate`	Transfer.5
	`AWS::Transfer::Connector`	Transfer.3 Transfer.6
	`AWS::Transfer::Profile`	Transfer.7

AWS のサービス	リソースタイプ	関連するコントロール
	`AWS::Transfer::Workflow`	Transfer.1
AWS WAF	`AWS::WAF::Rule`	WAF.6
	`AWS::WAF::RuleGroup`	WAF.7
	`AWS::WAF::WebACL`	WAF.1 WAF.8
	`AWS::WAFRegional::Rule`	WAF.2
	`AWS::WAFRegional::RuleGroup`	WAF.3
	`AWS::WAFRegional::WebACL`	WAF.4
	`AWS::WAFv2::RuleGroup`	WAF.12
	`AWS::WAFv2::WebACL`	WAF.10 WAF.11
Amazon WorkSpaces	`AWS::WorkSpaces::WorkSpace`	WorkSpaces.1 WorkSpaces.2

Foundational Security Best Practices AWS 標準に必要なリソース

Security Hub CSPM が AWS Foundational Security Best Practices 標準 (v.1.0.0) に適用され、有効になっている変更トリガーコントロールの検出結果を正確にレポートし、 AWS Config ルールを使用するには、次のタイプのリソースを に記録する必要があります AWS Config。この標準の詳細については、「」を参照してください[AWS Security Hub CSPM の基本的なセキュリティのベストプラクティス標準](#)。

AWS のサービス	リソースタイプ
Amazon API Gateway	`AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::ApiCache` , `AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CodeBuild	`AWS::CodeBuild::Project` , `AWS::CodeBuild::ReportGroup`
Amazon Cognito	`AWS::Cognito::IdentityPool` , `AWS::Cognito::UserPool`
Amazon Connect	`AWS::Connect::Instance`
AWS DataSync	`AWS::DataSync::Task`
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint` , `AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationTask`
Amazon DynamoDB	`AWS::DynamoDB::Table`

AWS のサービス	リソースタイプ
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::Instance` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::SecurityGroup` , `AWS::EC2::SpotFleet` , `AWS::EC2::Subnet` , `AWS::EC2::TransitGateway` , `AWS::EC2::VPCBlockPublicAccessOptions` , `AWS::EC2::VPNConnection` , `AWS::EC2::Volume`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` , `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition` , `AWS::ECS::TaskSet`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint` , `AWS::EFS::FileSystem`
Amazon エラスティックKubernetesサービス (Amazon EKS)	`AWS::EKS::Cluster`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`

AWS のサービス	リソースタイプ
エラスティックロードバランシング	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
AWS Glue	`AWS::Glue::Job` , `AWS::Glue::MLTransform`
AWS Identity and Access Management (IAM)	`AWS::IAM::Group` , `AWS::IAM::Policy` , `AWS::IAM::Role` , `AWS::IAM::User`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`
AWS Lambda	`AWS::Lambda::Function`
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster` , `AWS::KafkaConnect::Connector`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
Amazon OpenSearch Service	`AWS::OpenSearch::Domain`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster` , `AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBProxy` , `AWS::RDS::DBSnapshot` , `AWS::RDS::EventSubscription`

AWS のサービス	リソースタイプ
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterSubnetGroup`
Amazon Redshift Serverless	`AWS::RedshiftServerless::Workgroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint` , `AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket` , `AWS::S3::MultiRegionAccessPoint` , `AWS::S3Express::DirectoryBucket`
Amazon SageMaker AI	`AWS::SageMaker::Model` , `AWS::SageMaker::NotebookInstance`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Step Functions	`AWS::StepFunctions::StateMachine`
AWS Transfer Family	`AWS::Transfer::Connector`
AWS WAF	`AWS::WAF::Rule` , `AWS::WAF::RuleGroup` , `AWS::WAF::WebACL` , `AWS::WAFRegional::Rule` , `AWS::WAFRegional::RuleGroup` , `AWS::WAFRegional::WebACL` , `AWS::WAFv2::RuleGroup` , `AWS::WAFv2::WebACL`
Amazon WorkSpaces	`AWS::WorkSpaces::WorkSpace`

CIS AWS Foundations Benchmark に必要なリソース

Center for Internet Security (CIS) AWS Foundations Benchmark に適用される有効なコントロールのセキュリティチェックを実行するには、Security Hub CSPM はチェックに規定された正確な監査ステップを実行するか、特定の AWS Config マネージドルールを使用します。Security Hub CSPM のこの標準の詳細については、「」を参照してください[Security Hub CSPM の CIS AWS Foundations Benchmark](#)。

CIS v3.0.0 に必要なリソース

Security Hub CSPM が AWS Config ルールを使用する有効な CIS v3.0.0 変更トリガーコントロールの検出結果を正確にレポートするには、 に次のタイプのリソースを記録する必要があります AWS Config。

AWS のサービス	リソースタイプ
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::Instance` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Group` , `AWS::IAM::User` , `AWS::IAM::Role`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

CIS v1.4.0 に必要な リソース

Security Hub CSPM が AWS Config ルールを使用する有効な CIS v1.4.0 変更トリガーコントロールの検出結果を正確にレポートするには、 に次のタイプのリソースを記録する必要があります AWS Config。

AWS のサービス	リソースタイプ
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup`

AWS のサービス	リソースタイプ
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

CIS v1.2.0 に必要な リソース

Security Hub CSPM が AWS Config ルールを使用する有効な CIS v1.2.0 変更トリガーコントロールの検出結果を正確にレポートするには、 に次のタイプのリソースを記録する必要があります AWS Config。

AWS のサービス	リソースタイプ
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::SecurityGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`

NIST SP 800-53 リビジョン 5 標準に必要なリソース

Security Hub CSPM が NIST SP 800-53 Revision 5 標準に適用され、有効になっており、 AWS Config ルールを使用する変更トリガーコントロールの検出結果を正確にレポートするには、次のタイプのリソースを に記録する必要があります AWS Config。この標準の詳細については、「」を参照してください[Security Hub CSPM の NIST SP 800-53 リビジョン 5](#)。

AWS のサービス	リソースタイプ
Amazon API Gateway	`AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`

AWS のサービス	リソースタイプ
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint` , `AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationTask`
Amazon DynamoDB	`AWS::DynamoDB::Table`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::EIP` , `AWS::EC2::Instance` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::TransitGateway` , `AWS::EC2::VPNConnection` , `AWS::EC2::Volume`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` , `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`

AWS のサービス	リソースタイプ
Amazon エラスティックKubernetesサービス (Amazon EKS)	`AWS::EKS::Cluster`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
エラスティックロードバランシング	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
Amazon ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
Amazon EventBridge	`AWS::Events::Endpoint` , `AWS::Events::EventBus`
AWS Glue	`AWS::Glue::Job`
AWS Identity and Access Management (IAM)	`AWS::IAM::Group` , `AWS::IAM::Policy` , `AWS::IAM::Role` , `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster`
Amazon MQ	`AWS::AmazonMQ::Broker`

AWS のサービス	リソースタイプ
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
Amazon OpenSearch Service	`AWS::OpenSearch::Domain`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster` , `AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSnapshot` , `AWS::RDS::EventSubscription`
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterSubnetGroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint` , `AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket`
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`
Amazon SageMaker AI	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Transfer Family	`AWS::Transfer::Connector`

AWS のサービス	リソースタイプ
AWS WAF	`AWS::WAF::Rule` , `AWS::WAF::RuleGroup` , `AWS::WAF::WebACL` , `AWS::WAFRegional::Rule` , `AWS::WAFRegional::RuleGroup` , `AWS::WAFRegional::WebACL` , `AWS::WAFv2::RuleGroup` , `AWS::WAFv2::WebACL`

NIST SP 800-171 リビジョン 2 標準に必要なリソース

Security Hub CSPM が NIST SP 800-171 Revision 2 標準に適用され、有効になっており、 AWS Config ルールを使用する変更トリガーコントロールの検出結果を正確にレポートするには、次のタイプのリソースを に記録する必要があります AWS Config。この標準の詳細については、「」を参照してください[Security Hub CSPM の NIST SP 800-171 リビジョン 2](#)。

AWS のサービス	リソースタイプ
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`
Amazon API Gateway	`AWS::ApiGateway::Stage`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC` , `AWS::EC2::VPNConnection`
エラスティックロードバランシング	`AWS::ElasticLoadBalancing::LoadBalancer`
AWS Identity and Access Management(IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`

AWS のサービス	リソースタイプ
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
AWS Systems Manager(SSM)	`AWS::SSM::PatchCompliance`
AWS WAF	`AWS::WAFv2::RuleGroup`

PCI DSS v3.2.1 に必要なリソース

Security Hub CSPM が Payment Card Industry Data Security Standard (PCI DSS) の v3.2.1 に適用され、有効になっており、 ルールを使用する AWS Config コントロールの検出結果を正確にレポートするには、次のタイプのリソースを に記録する必要があります AWS Config。この標準の詳細については、「」を参照してください[Security Hub CSPM の PCI DSS](#)。

AWS のサービス	リソースタイプ
AWS CodeBuild	`AWS::CodeBuild::Project`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::EIP` , `AWS::EC2::Instance` , `AWS::EC2::SecurityGroup`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`
AWS Lambda	`AWS::Lambda::Function`
Amazon OpenSearch Service	`AWS::OpenSearch::Domain`

AWS のサービス	リソースタイプ
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSnapshot`
Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket`
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`

リソースタグ付け標準に必要な AWS リソース

AWS リソースタグ付け標準に適用されるすべてのコントロールは、変更がトリガーされ、 AWS Config ルールを使用します。Security Hub CSPM がこれらのコントロールの検出結果を正確にレポートするには、次のタイプのリソースを記録する必要があります AWS Config。この標準の詳細については、「」を参照してください[AWS Security Hub CSPM のリソースタグ付け標準](#)。

AWS のサービス	リソースタイプ
AWS Amplify	`AWS::Amplify::App` , `AWS::Amplify::Branch`
Amazon AppFlow	`AWS::AppFlow::Flow`
AWS App Runner	`AWS::AppRunner::Service` , `AWS::AppRunner::VpcConnector`
AWS AppConfig	`AWS::AppConfig::Application` , `AWS::AppConfig::ConfigurationProfile` , `AWS::AppConfig::Environment` , `AWS::AppConfig::ExtensionAssociation`

AWS のサービス	リソースタイプ
AWS AppSync	`AWS::AppSync::GraphQLApi`
Amazon Athena	`AWS::Athena::DataCatalog` , `AWS::Athena::WorkGroup`
AWS Backup	`AWS::Backup::BackupPlan` , `AWS::Backup::BackupVault` , `AWS::Backup::RecoveryPlan` , `AWS::Backup::ReportPlan`
AWS Batch	`AWS::Batch::ComputeEnvironment` , `AWS::Batch::JobQueue` , `AWS::Batch::SchedulingPolicy`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CloudTrail	`AWS::CloudTrail::Trail`
AWS CodeArtifact	`AWS::CodeArtifact::Repository`
Amazon CodeGuru	`AWS::CodeGuruProfiler::ProfilingGroup` , `AWS::CodeGuruReviewer::RepositoryAssociation`
Amazon Connect	`AWS::CustomerProfiles::ObjectType`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate` , `AWS::DMS::EventSubscription`
	
	`AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationSubnetGroup`

AWS DataSync	`AWS::DataSync::Task`

AWS のサービス	リソースタイプ
Amazon Detective	`AWS::Detective::Graph`
Amazon DynamoDB	`AWS::DynamoDB::Trail`
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::CustomerGateway` , `AWS::EC2::DHCPOptions` , `AWS::EC2::EIP` , `AWS::EC2::FlowLog` , `AWS::EC2::Instance` , `AWS::EC2::InternetGateway` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NatGateway` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::PrefixList` , `AWS::EC2::RouteTable` , `AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::TrafficMirrorFilter` , `AWS::EC2::TrafficMirrorSession` , `AWS::EC2::TrafficMirrorTarget` , `AWS::EC2::TransitGateway` , `AWS::EC2::TransitGatewayAttachment` , `AWS::EC2::TransitGatewayRouteTable` , `AWS::EC2::Volume` , `AWS::EC2::VPC` , `AWS::EC2::VPCEndpointService` , `AWS::EC2::VPCPeeringConnection` , `AWS::EC2::VPNGateway`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`

AWS のサービス	リソースタイプ
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon エラスティックKubernetesサービス (Amazon EKS)	`AWS::EKS::Cluster` , `AWS::EKS::IdentityProviderConfig`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EventBridge	`AWS::Events::EventBus`
Amazon Fraud Detector	`AWS::FraudDetector::EntityType` , `AWS::FraudDetector::Label` `AWS::FraudDetector::Outcome` , `AWS::FraudDetector::Variable`
AWS Global Accelerator	`AWS::GlobalAccelerator::Accelerator`
AWS Glue	`AWS::Glue::Job`
Amazon GuardDuty	`AWS::GuardDuty::Detector` , `AWS::GuardDuty::Filter` , `AWS::GuardDuty::IPSet`
AWS Identity and Access Management (IAM)	`AWS::IAM::Role` , `AWS::IAM::User`
AWS Identity and Access Management Access Analyzer (IAM Access Analyzer)	`AWS::AccessAnalyzer::Analyzer`

AWS のサービス	リソースタイプ
AWS IoT	`AWS::IoT::Authorizer` , `AWS::IoT::Dimension` , `AWS::IoT::MitigationAction` , `AWS::IoT::Policy` , `AWS::IoT::RoleAlias` , `AWS::IoT::SecurityProfile`
AWS IoT イベント	`AWS::IoTEvents::AlarmModel` , `AWS::IoTEvents::DetectorModel` , `AWS::IoTEvents::Input`
AWS IoT SiteWise	`AWS::IoTSiteWise::Dashboard` , `AWS::IoTSiteWise::Gateway` , `AWS::IoTSiteWise::Portal` , `AWS::IoTSiteWise::Project`
AWS IoT TwinMaker	`AWS::IoTTwinMaker::Entity` , `AWS::IoTTwinMaker::Scene` , `AWS::IoTTwinMaker::SyncJob` , `AWS::IoTTwinMaker::Workspace`
AWS IoT ワイヤレス	`AWS::IoTWireless::FuotaTask` , `AWS::IoTWireless::MulticastGroup` , `AWS::IoTWireless::ServiceProfile`
Amazon Interactive Video Service (Amazon IVS)	`AWS::IVS::Channel` , `AWS::IVS::PlaybackKeyPair` , `AWS::IVS::RecordingConfiguration`
Amazon Keyspaces (Apache Cassandra 向け)	`AWS::Cassandra::Keyspace`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MQ	`AWS::AmazonMQ::Broker`

AWS のサービス	リソースタイプ
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy`
Amazon OpenSearch Service	`AWS::OpenSearch::Domain`
AWS Private Certificate Authority	`AWS::ACMPCA::CertificateAuthority`
Amazon Relational Database Service	`AWS::RDS::DBCluster` , `AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSecurityGroup` , `AWS::RDS::DBSnapshot` , `AWS::RDS::DBSubnetGroup`
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterParameterGroup` , `AWS::Redshift::ClusterSnapshot` , `AWS::Redshift::ClusterSubnetGroup` , `AWS::Redshift::EventSubscription`
Amazon Route 53	`AWS::Route53::HealthCheck`
Amazon SageMaker AI	`AWS::SageMaker::AppImageConfig` , `AWS::SageMaker::Image`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet` , `AWS::SES::ContactList`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`

AWS のサービス	リソースタイプ
AWS Step Functions	`AWS::StepFunctions::Activity`
AWS Systems Manager (SSM)	`AWS::SSM::Document`
AWS Transfer Family	`AWS::Transfer::Agreement` , `AWS::Transfer::Certificate` , `AWS::Transfer::Connector` , `AWS::Transfer::Profile` , `AWS::Transfer::Workflow`

AWS Control Tower サービスマネージド標準に必要なリソース

Security Hub CSPM が、 AWS Control Tower サービスマネージド標準に適用され、有効になっており、 AWS Config ルールを使用する変更トリガーコントロールの検出結果を正確にレポートするには、次のタイプのリソースを に記録する必要があります AWS Config。この標準の詳細については、「」を参照してください[サービスマネージドスタンダード： AWS Control Tower](#)。

AWS のサービス	リソースタイプ
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CodeBuild	`AWS::CodeBuild::Project`
Amazon DynamoDB	`AWS::DynamoDB::Table`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::Instance`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`

AWS のサービス	リソースタイプ

	`AWS::EC2::VPNConnection`
	
	`AWS::EC2::Volume`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
	
	`AWS::AutoScaling::LaunchConfiguration`

Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	
	`AWS::ECS::Service`
	
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`

エラスティックロードバランシング	`AWS::ElasticLoadBalancing::LoadBalancer`
	
	`AWS::ElasticLoadBalancingV2::LoadBalancer`

ElasticSearch	`AWS::Elasticsearch::Domain`

AWS のサービス	リソースタイプ

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` `AWS::NetworkFirewall::RuleGroup`
Amazon OpenSearch Service	`AWS::OpenSearch::Domain`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccountPublicAccessBlock` `AWS::S3::Bucket`

AWS のサービス	リソースタイプ
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
AWS Secrets Manager	`AWS::SecretsManager::Secret`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

AWS WAF	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::WebACL`

セキュリティチェックの実行スケジュール

セキュリティ標準を有効にすると、 AWS Security Hub CSPM は 2 時間以内にすべてのチェックの実行を開始します。ほとんどのチェックは 25 分以内に実行開始されます。Security Hub CSPM は、コントロールの基盤となるルールを評価してチェックを実行します。コントロールのチェックの最初の実行が完了するまで、ステータスは [No data] (データなし) です。

新しい標準を有効にすると、Security Hub CSPM が、他の有効な標準で有効になっているコントロールと同じ基盤となる AWS Config サービスにリンクされたルールを使用するコントロールの検出結果を生成するまでに、最大 24 時間かかる場合があります。例えば、 AWS Foundational Security Best Practices (FSBP) 標準で Lambda.1 コントロールを有効にすると、Security Hub CSPM はサービスにリンクされたルールを作成し、通常は数分以内に結果を生成します。その後、Payment Card Industry Data Security Standard (PCI DSS) で Lambda.1 コントロールを有効にすると、Security Hub CSPM が同じサービスにリンクされたルールを使用するため、コントロールの結果を生成するまでに最大 24 時間かかる場合があります。

最初のチェックの後、各コントロールのスケジュールは、定期的に実行されるか、変更によってトリガーされます。マネージド AWS Config ルールに基づくコントロールの場合、コントロールの説明には、 AWS Config デベロッパーガイドのルールの説明へのリンクが含まれます。この説明では、ルールの変更がトリガーされるか、定期的に行われるかを指定します。

定期的なセキュリティチェック

定期的なセキュリティチェックは、最後の実行から 12 時間または 24 時間以内に自動的に実行されます。Security Hub CSPM は周期性を決定し、変更することはできません。定期的なコントロールは、チェック実行時の評価を反映したものになります。

定期的な統制結果のワークフローステータスを更新し、次のチェックで検出結果のコンプライアンスステータスが同じままであっても、ワークフローステータスは変更された状態のままです。たとえば、KMS.4 コントロールの検出に失敗し (AWS KMS key ローテーションを有効にする必要があります) 、検出結果を修復すると、Security Hub CSPM はワークフローステータスNEWを から に変更しますRESOLVED。次の定期チェックの前に KMS キーローテーションを無効にすると、検出結果のワークフローステータスは RESOLVED のままになります。

Security Hub CSPM カスタム Lambda 関数を使用するチェックは定期的に行われます。

変更によってトリガーされるセキュリティチェック

変更によってトリガーされるセキュリティチェックは、関連するリソースの状態が変更されたときに実行されます。リソースの状態の変化を継続的に記録 AWS Config するか、毎日記録するかを選択します。毎日の記録を選択した場合、 はリソース状態に変更があった場合、24 時間ごとにリソース設定データを AWS Config 配信します。変化がなければ、データは配信されません。これにより、Security Hub CSPM の検出結果の生成が 24 時間完了するまで遅延する可能性があります。選択した記録期間に関係なく、Security Hub CSPM は 18 時間ごとに をチェックし、 からのリソースの更新が見逃 AWS Config されていないことを確認します。

一般的に、Security Hub CSPM は可能な限り変更によってトリガーされるルールを使用します。リソースが変更によってトリガーされるルールを使用するには、 AWS Config 設定項目をサポートしている必要があります。

コントロールの結果を生成および更新する

AWS Security Hub CSPM は、セキュリティコントロールに対してチェックを実行すると、コントロールの検出結果を生成および更新します。コントロールの検出結果は AWS Security Finding 形式 (ASFF) を使用します。

Security Hub CSPM は通常、コントロールのセキュリティチェックごとに課金されます。ただし、複数のコントロールが同じ AWS Config ルールを使用する場合、Security Hub CSPM はルールに対するチェックごとに 1 回のみ課金します。たとえば、この AWS Config `iam-password-policy`ルールは CIS AWS Foundations Benchmark 標準と AWS Foundational Security Best Practices 標準の複数のコントロールで使用されます。Security Hub CSPM がそのルールに対してチェックを実行するたびに、関連するコントロールごとに個別のコントロール結果を生成しますが、チェックに対して課金されるのは 1 回のみです。

コントロール検出結果のサイズが最大 240 KB を超える場合、Security Hub CSPM は検出結果から`Resource.Details`オブジェクトを削除します。リソースによって AWS Config バックアップされるコントロールについては、 AWS Config コンソールを使用してリソースの詳細を確認できます。

トピック

- 統合されたコントロールの検出結果
- コントロールの検出結果の生成、更新、アーカイブ
- コントロールの検出結果の自動化と抑制
- コントロールの検出結果のコンプライアンスの詳細
- コントロールの検出結果の ProductFields の詳細
- コントロールの検出結果の重要度レベル

統合されたコントロールの検出結果

アカウントで統合コントロールの検出結果が有効になっている場合、Security Hub CSPM は、コントロールが複数の有効な標準に適用されていても、コントロールのセキュリティチェックごとに 1 つの検出結果または検出結果の更新を生成します。適用されるコントロールと標準のリストについては、「」を参照してくださいSecurity Hub CSPM のコントロールリファレンス。検出結果のノイズを減らすために、統合コントロールの検出結果を有効にすることをお勧めします。

2023 年 2 月 23 日より AWS アカウント 前に で Security Hub CSPM を有効にした場合は、このセクションの後半の手順に従って、統合コントロールの検出結果を有効にできます。2023 年 2 月 23 日以降に Security Hub CSPM を有効にすると、アカウントに対して統合コントロールの検出結果が自動的に有効になります。

手動の招待プロセスを通じて Security Hub CSPM と または招待されたメンバーアカウントとの統合 AWS Organizationsを使用する場合、統合コントロールの検出結果は、管理者アカウントに対して有効になっている場合にのみ、メンバーアカウントに対して有効になります。管理者アカウントでこの機能が無効になっている場合、メンバーアカウントでは無効になっています。この挙動は、新規およ

び既存のメンバーアカウントに適用されます。さらに、管理者が中央設定を使用して複数のアカウントの Security Hub CSPM を管理している場合、中央設定ポリシーを使用してアカウントの統合コントロール結果を有効または無効にすることはできません。

アカウントの統合コントロール検出結果を無効にすると、Security Hub CSPM は、コントロールを含む有効な標準ごとに個別のコントロール検出結果を生成または更新します。たとえば、コントロールを共有する 4 つの標準を有効にすると、コントロールのセキュリティチェック後に 4 つの個別の検出結果を受け取ります。[統合されたコントロールの検出結果] を有効にすると、検出結果が 1 つのみになります。

統合コントロールの検出結果を有効にすると、Security Hub CSPM は新しい標準に依存しない検出結果を作成し、元の標準ベースの検出結果をアーカイブします。一部のコントロール検出結果のフィールドと値は変更され、既存のワークフローに影響する可能性があります。これらの変更の詳細については、「」を参照してください統合されたコントロールの検出結果 — ASFF の変更。統合されたコントロールの検出結果を有効にすると、統合されたサードパーティー製品が Security Hub CSPM から受け取る検出結果にも影響する可能性があります。v2.0.0 AWS での自動化されたセキュリティ対応ソリューションを使用する場合は、統合統制結果をサポートしていることに注意してください。

[統合されたコントロールの検出結果] を有効または無効にするには、管理者アカウントまたはスタンドアロンアカウントにサインインする必要があります。

> **Note**
>
> 統合コントロールの検出結果を有効にすると、Security Hub CSPM が新しい統合検出結果を生成し、既存の標準ベースの検出結果をアーカイブするまでに最大 24 時間かかることがあります。同様に、統合コントロールの検出結果を無効にした後、Security Hub CSPM が新しい標準ベースの検出結果を生成し、既存の統合検出結果をアーカイブするまでに最大 24 時間かかることがあります。この間、アカウントに標準に依存しない検出結果と標準ベースの検出結果が混在することがあります。

Security Hub CSPM console

統合コントロールの検出結果を有効または無効にするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで [Settings] の [General] を選択します。

3. コントロール セクションで、編集 を選択します。
4. 統合コントロールの検出結果スイッチを使用して、統合コントロールの検出結果を有効または無効にします。
5. [保存] を選択します。

Security Hub CSPM API

プログラムで統合コントロールの検出結果を有効または無効にするには、Security Hub CSPM API の UpdateSecurityHubConfigurationオペレーションを使用します。または、 を使用している場合は AWS CLI、 update-security-hub-configuration コマンドを実行します。

`control-finding-generator` パラメータで、 を指定`SECURITY_CONTROL`して統合コントロールの検出結果を有効にします。統合コントロールの検出結果を無効にするには、 を指定します`STANDARD_CONTROL`。

たとえば、次の AWS CLI コマンドは、統合コントロールの検出結果を有効にします。

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-
finding-generator SECURITY_CONTROL
```

次の AWS CLI コマンドは、統合コントロールの検出結果を無効にします。

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-
finding-generator STANDARD_CONTROL
```

コントロールの検出結果の生成、更新、アーカイブ

Security Hub CSPM は、スケジュールに従ってセキュリティチェックを実行します。Security Hub CSPM がコントロールのセキュリティチェックを初めて実行すると、コントロールがチェックする AWS リソースごとに新しい検出結果が生成されます。Security Hub CSPM がその後コントロールのセキュリティチェックを実行するたびに、既存の検出結果を更新してチェックの結果を報告します。つまり、個々の検出結果から提供されたデータを使用して、特定のコントロールに対する特定のリソースのコンプライアンス変更を追跡できます。

たとえば、リソースのコンプライアンスステータスが特定のコントロール`PASSED`で から `FAILED` に変わった場合、Security Hub CSPM は新しい検出結果を生成しません。代わりに、Security Hub CSPM はコントロールとリソースの既存の検出結果を更新します。検出結果では、Security Hub

CSPM はコンプライアンスステータス (`Compliance.Status`) フィールドの値を に変更しますPASSED。Security Hub CSPM は、チェックの結果を反映するために追加のフィールドの値も更新します。例えば、Security Hub CSPM が最後にチェックを実行し、検出結果を更新した日時を示す重要度ラベル、ワークフローステータス、タイムスタンプなどです。

コンプライアンスステータスの変更を報告すると、Security Hub CSPM はコントロール検出結果の次のいずれかのフィールドを更新することがあります。

- `Compliance.Status` – 指定されたコントロールのリソースの新しいコンプライアンスステータス。
- `FindingProviderFields.Severity.Label` – 、、 などLOWMEDIUM、検出結果の重要度の新しい定性的表現HIGH。
- `FindingProviderFields.Severity.Original` – 準拠リソース0など、検出結果の重要度の新しい定量的表現。
- `FirstObservedAt` – リソースのコンプライアンスステータスが最後に変更されたとき。
- `LastObservedAt` – Security Hub CSPM が最後に、指定されたコントロールとリソースのセキュリティチェックを実行したとき。
- `ProcessedAt` – Security Hub CSPM が最近検出結果の処理を開始したとき。
- `ProductFields.PreviousComplianceStatus` – 指定されたコントロールのリソースの以前のコンプライアンスステータス (`Compliance.Status`) 。
- `UpdatedAt` – Security Hub CSPM が最後に検出結果を更新したとき。
- `Workflow.Status` – 指定されたコントロールのリソースの新しいコンプライアンスステータスに基づく、検出結果の調査のステータス。

Security Hub CSPM がフィールドを更新するかどうかは、主に該当するコントロールとリソースの最新のセキュリティチェックの結果によって異なります。たとえば、特定のコントロールFAILEDのリソースのコンプライアンスステータスが から PASSEDに変わった場合、Security Hub CSPM は検出結果のワークフローステータスを に変更しますNEW。個々の検出結果の更新を追跡するには、検出結果の履歴を参照できます。検出結果の個々のフィールドの詳細については、AWS 「Security Finding Format (ASFF)」を参照してください。

場合によっては、Security Hub CSPM は、既存の検出結果を更新する代わりに、コントロールによって後続のチェック用の新しい検出結果を生成します。これは、コントロールをバックアップする AWS Config ルールに問題がある場合に発生する可能性があります。この場合、Security Hub CSPM は既存の検出結果をアーカイブし、チェックごとに新しい検出結果を生成します。新しい検出結果で

は、コンプライアンスステータスは NOT_AVAILABLEで、レコードステータスは ですARCHIVED。AWS Config ルールの問題に対処すると、Security Hub CSPM は新しい検出結果を生成し、個々のリソースのコンプライアンスステータスに対するその後の変更を追跡するために更新を開始します。

Security Hub CSPM は、コントロールの検出結果の生成と更新に加えて、特定の基準を満たすコントロールの検出結果を自動的にアーカイブします。Security Hub CSPM は、コントロールが無効になっている場合、指定されたリソースが削除された場合、または指定されたリソースが存在しなくなった場合に、検出結果をアーカイブします。関連付けられたサービスが使用されなくなったため、リソースが存在しない可能性があります。具体的には、Security Hub CSPM は、検出結果が次のいずれかの基準を満たす場合に、コントロール検出結果を自動的にアーカイブします。

- 検出結果は 3~5 日間更新されていません。この時間枠に基づくアーカイブはベストエフォートベースであり、保証されていないことに注意してください。
- 指定されたリソースのコンプライアンスステータスNOT_APPLICABLEに対して返される関連する AWS Config 評価。

検出結果がアーカイブされているかどうかを判断するには、検出結果のレコード状態 (RecordState) フィールドを参照できます。結果がアーカイブされている場合、このフィールドの値は ですARCHIVED。

Security Hub CSPM は、アーカイブされたコントロールの検出結果を 30 日間保存します。30 日後、検出結果は期限切れになり、Security Hub CSPM によって完全に削除されます。アーカイブされたコントロールの検出結果の有効期限が切れているかどうかを判断するために、Security Hub CSPM は検出結果の UpdatedAtフィールドの値に基づいてその計算を行います。

アーカイブされたコントロールの検出結果を 30 日以上保存するには、検出結果を S3 バケットにエクスポートできます。これを行うには、Amazon EventBridge ルールでカスタムアクションを使用します。詳細については、「EventBridge を使用した自動応答と修復」を参照してください。

> **Note**
>
> 2025 年 7 月 3 日以前は、コントロールのリソースのコンプライアンスステータスが変更されると、Security Hub CSPM はコントロールの検出結果を生成および更新しました。以前は、Security Hub CSPM は新しいコントロール検出結果を作成し、リソースの既存の検出結果をアーカイブしていました。したがって、(30 日後に) 検出結果の有効期限が切れるまで、特定のコントロールとリソースに対して複数のアーカイブされた検出結果が存在する可能性があります。

コントロールの検出結果の自動化と抑制

Security Hub CSPM オートメーションルールを使用して、特定のコントロール検出結果を更新または抑制できます。検出結果を抑制すると、引き続きその検出結果にアクセスできます。ただし、抑制は、検出結果に対処するためのアクションは必要ないと考えていることを示します。

検出結果を抑制することで、検出結果のノイズを減らすことができます。たとえば、テストアカウントで生成されたコントロールの検出結果を抑制できます。または、特定のリソースに関連する検出結果を抑制することもできます。結果の自動更新または抑制の詳細については、「」を参照してくださいSecurity Hub CSPM のオートメーションルールについて。

自動化ルールは、特定のコントロール結果を更新または抑制する場合に適しています。ただし、コントロールが組織やユースケースに関連しない場合は、コントロールを無効にすることをお勧めします。コントロールを無効にすると、Security Hub CSPM はコントロールのセキュリティチェックを実行せず、課金されません。

コントロールの検出結果のコンプライアンスの詳細

コントロールのセキュリティチェックによって生成された検出結果では、 AWS Security Finding 形式 (ASFF) の Compliance オブジェクトとフィールドは、コントロールがチェックした個々のリソースのコンプライアンスの詳細を提供します。これには、次の情報が含まれます。

- `AssociatedStandards` – コントロールが有効になっている有効な標準。
- `RelatedRequirements` – 有効なすべての標準におけるコントロールの関連要件。これらの要件は、Payment Card Industry Data Security Standard (PCI DSS) や NIST SP 800-171 Revision 2 標準など、コントロール用のサードパーティーのセキュリティフレームワークから派生しています。
- `SecurityControlId` – Security Hub CSPM がサポートする標準全体のコントロールの識別子。
- `Status` – Security Hub CSPM がコントロールに対して実行した最新のチェックの結果。以前のチェックの結果は、検出結果の履歴に保持されます。
- `StatusReasons` – `Status`フィールドで指定された値の理由を示す配列。理由ごとに、理由コードと説明が含まれます。

次の表に、結果に含まれる可能性のある理由コードと説明を示します`StatusReasons`。修復手順は、指定された理由コードで結果を生成したコントロールによって異なります。コントロールの修復ガイダンスを確認するには、「」を参照してくださいSecurity Hub CSPM のコントロールリファレンス。

理由コード	コンプライアンス状況	説明
CLOUDTRAIL_METRIC_FILTER_NOT_VALID	FAILED	マルチリージョンの CloudTrail 追跡に有効なメトリクスフィルターが設定されていません。
CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT	FAILED	マルチリージョンの CloudTrail 追跡用のメトリクスフィルターがありません。
CLOUDTRAIL_MULTI_REGION_NOT_PRESENT	FAILED	アカウントに、必要な設定のマルチリージョンの CloudTrail 追跡が存在しません。
CLOUDTRAIL_REGION_INVAILD	WARNING	マルチリージョンの CloudTrail 追跡が現在のリージョンに存在しません。
CLOUDWATCH_ALARM_ACTIONS_NOT_VALID	FAILED	有効なアラームアクションが存在しません。
CLOUDWATCH_ALARMS_NOT_PRESENT	FAILED	CloudWatch アラームがアカウントに存在しません。
CONFIG_ACCESS_DENIED	NOT_AVAILABLE AWS Config ステータスは ですConfigError	AWS Config アクセスが拒否されました。 AWS Config が有効で、十分なアクセス許可が付与されていることを確認します。
CONFIG_EVALUATIONS_EMPTY	PASSED	AWS Config は、 ルールに基づいてリソースを評価しました。 ルールがスコープ内の AWS リソースに適用されなかったか、指定されたリソースが削除されたか、評価結果が削除されました。

理由コード	コンプライアンス状況	説明
CONFIG_RECORDER_CUSTOM_ROLE	FAILED (Config.1 の場合)	AWS Config レコーダーはサービス AWS Config にリンクされたロールの代わりにカスタム IAM ロールを使用し、Config.1 のincludeConfigServiceLinkedRoleCheck カスタムパラメータは に設定されませんfalse。
CONFIG_RECORDER_DISABLED	FAILED (Config.1 の場合)	AWS Config 設定レコーダーをオンにすると、 は有効になっていません。
CONFIG_RECORDER_MISSING_REQUIRED_RESOURCE_TYPES	FAILED (Config.1 の場合)	AWS Config は、有効な Security Hub CSPM コントロールに対応するすべてのリソースタイプを記録しているわけではありません。次のリソースの記録を有効にします: ########## 。

理由コード	コンプライアンス状況	説明
CONFIG_RETURNS_NOT_APPLICABLE	NOT_AVAILABLE	コンプライアンスステータスは、が該当なしのステータスを AWS Config 返したNOT_AVAILABLE ためです。 AWS Config はステータスの理由を提供しません。ステータスが Not Applicable である理由は、以下のように考えられます。 • リソースが AWS Config ルールのスコープから削除されました。 • AWS Config ルールが削除されました。 • リソースが削除された。 • AWS Config ルールロジックは、該当なしステータスを生成できます。

理由コード	コンプライアンス状況	説明
CONFIG_RULE_EVALUATION_ERROR	NOT_AVAILABLE AWS Config ステータスは ですConfigError	この理由コードは、いくつかの異なる種類の評価エラーに使用されます。 説明には、具体的な理由の情報が含まれます。 エラーの種類は、次のいずれかになります。 • 許可が不足しているため、評価を実行できない。説明には、欠落している特定の許可が含まれます。 • パラメータの値が欠落しているか、無効。説明には、パラメータとパラメータ値の要件が含まれます。 • S3 バケットからの読み取り中のエラー。説明では、バケットが識別され、特定のエラーが表示されます。 • AWS サブスクリプションがありません。 • 評価の一般的なタイムアウト。 • 停止中のアカウント。
CONFIG_RULE_NOT_FOUND	NOT_AVAILABLE AWS Config ステータスは ですConfigError	AWS Config ルールは作成中です。

理由コード	コンプライアンス状況	説明
INTERNAL_SERVICE_ERROR	NOT_AVAILABLE	不明なエラーが発生しました。
LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE	FAILED	Security Hub CSPM は、カスタム Lambda ランタイムに対してチェックを実行できません。
S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION	WARNING	このルールに関連付けられている S3 バケットが別のリージョンまたはアカウントにあるため、検出結果は WARNING状態です。 このルールは、クロスリージョンまたはクロスアカウントのチェックをサポートしていません。 このリージョンまたはアカウントでは、このコントロールを無効にすることをお勧めします。リソースがあるリージョンまたはアカウントでのみ実行します。
SNS_SUBSCRIPTION_NOT_PRESENT	FAILED	CloudWatch Logs メトリクスフィルターに有効な Amazon SNS サブスクリプションが含まれていません。

理由コード	コンプライアンス状況	説明
SNS_TOPIC_CROSS_ACCOUNT	WARNING	結果が WARNING 状態です。 このルールに関連付けられた SNS トピックは、別のアカウントによって所有されています。現在のアカウントでは、サブスクリプション情報を取得できません。 SNS トピックを所有するアカウントは、SNS トピックへの sns:ListSubscriptionsByTopic 許可を現在のアカウントに付与する必要があります。
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	このルールに関連付けられた SNS トピックが別のリージョンまたはアカウントにあるため、結果が WARNING 状態です。 このルールは、クロスリージョンまたはクロスアカウントのチェックをサポートしていません。 このリージョンまたはアカウントでは、このコントロールを無効にすることをお勧めします。リソースがあるリージョンまたはアカウントでのみ実行します。
SNS_TOPIC_INVALID	FAILED	このルールに関連付けられている SNS トピックが無効です。
THROTTLING_ERROR	NOT_AVAILABLE	関連する API オペレーションが許可されたレートを超えました。

コントロールの検出結果の ProductFields の詳細

コントロールのセキュリティチェックによって生成された検出結果では、 AWS Security Finding Format (ASFF) の ProductFields 属性に次のフィールドを含めることができます。

`ArchivalReasons:0/Description`

Security Hub CSPM が検出結果をアーカイブした理由について説明します。

例えば、コントロールまたは標準を無効にするか、統合コントロールの検出結果を有効または無効にすると、Security Hub CSPM は既存の検出結果をアーカイブします。

`ArchivalReasons:0/ReasonCode`

Security Hub CSPM が検出結果をアーカイブした理由を指定します。

例えば、コントロールまたは標準を無効にするか、統合コントロールの検出結果を有効または無効にすると、Security Hub CSPM は既存の検出結果をアーカイブします。

`PreviousComplianceStatus`

検出結果の最新の更新時点での、指定されたコントロールのリソースの以前のコンプライアンスステータス (`Compliance.Status`) 。リソースのコンプライアンスステータスが最新の更新中に変更されなかった場合、この値は検出結果の `Compliance.Status`フィールドの値と同じです。可能な値の一覧については、コンプライアンスステータスとコントロールステータスの評価を参照してください。

`StandardsGuideArn` または `StandardsArn`

コントロールに関連付けられた標準の ARN。

CIS AWS Foundations Benchmark 標準の場合、 フィールドは ですStandardsGuideArn。PCI DSS および AWS Foundational Security Best Practices 標準の場合、 フィールドは ですStandardsArn。

[統合されたコントロールの検出結果] を有効にすると、これらのフィールドは `Compliance.AssociatedStandards` に合わせて削除されます。

`StandardsGuideSubscriptionArn` または `StandardsSubscriptionArn`

標準へのアカウントのサブスクリプションの ARN。

CIS AWS Foundations Benchmark 標準の場合、 フィールドは ですStandardsGuideSubscriptionArn。PCI DSS および AWS Foundational Security Best Practices 標準の場合、 フィールドは ですStandardsSubscriptionArn。

[統合されたコントロールの検出結果] を有効にすると、これらのフィールドは削除されます。

`RuleId`、または `ControlId`

コントロールの識別子。

CIS AWS Foundations Benchmark 標準の場合、 フィールドは ですRuleId。他の標準の場合、このフィールドは `ControlId` です。

[統合されたコントロールの検出結果] を有効にすると、これらのフィールドは `Compliance.SecurityControlId` に合わせて削除されます。

`RecommendationUrl`

コントロールの修正情報の URL。[統合されたコントロールの検出結果] を有効にすると、このフィールドは `Remediation.Recommendation.Url` に合わせて削除されます。

`RelatedAWSResources:0/name`

結果に関連付けられたリソースの名前。

`RelatedAWSResource:0/type`

コントロールに関連付けられたリソースのタイプ。

`StandardsControlArn`

コントロールの ARN。[統合されたコントロールの検出結果] を有効にすると、このフィールドは削除されます。

`aws/securityhub/ProductName`

コントロールの検出結果の場合、製品名は ですSecurity Hub。

`aws/securityhub/CompanyName`

コントロールの検出結果の場合、会社名は ですAWS。

`aws/securityhub/annotation`

コントロールによって検出された問題の説明。

`aws/securityhub/FindingId`

検出結果の識別子。

[統合されたコントロールの検出結果] を有効にした場合、このフィールドは標準を参照しません。

コントロールの検出結果の重要度レベル

Security Hub CSPM コントロールに割り当てられた重要度は、コントロールの重要性を示します。コントロールの重要度により、コントロールの結果に割り当てられる重要度ラベルが決まります。

重要度の基準

コントロールの重要度は、以下の基準の評価に基づいて決定されます:

- 脅威アクターがコントロールに関連する設定の弱点を利用する際の難易度 この難易度は、弱点を利用して脅威シナリオを実行するために必要な洗練度または複雑さの度合いによって決まります。
- 弱点が AWS アカウント または リソースの侵害につながる可能性はどの程度ありますか？ AWS アカウント または リソースの侵害は、データまたは AWS インフラストラクチャの機密性、完全性、可用性が何らかの形で損なわれることを意味します。侵害の可能性は、脅威シナリオが AWS のサービス または リソースの中断または違反につながる可能性を示します。

例えば、次の設定の弱点について検討します。

- ユーザーアクセスキーが 90 日ごとにローテーションされません。
- IAM ルートユーザーキーが存在します。

どちらの弱点も、攻撃者が悪用する際の難易度は同程度です。両方の弱点とも、攻撃者は認証情報の盗難やその他の方法を使用してユーザーキーを取得します。その後、このユーザーキーを使用して、許可されない方法でリソースにアクセスします。

ただし、脅威アクターによって取得されたアクセスキーがルートユーザーのものである場合、よりアクセス性が高いため、侵害の可能性はより高くなります。この結果、ルートユーザーキーの弱点は、重要度が高くなります。

重要度では、基になるリソースの重大度は考慮されていません。重大度は、結果に関連付けられているリソースの重要性の程度として定義されます。たとえば、ミッションクリティカルなアプリケーションに関連付けられているリソースは、非本番テストに関連付けられているリソースよりも重要です。リソース重要度情報をキャプチャするには、 AWS Security Finding 形式 (ASFF) の `Criticality`フィールドを使用します。

次の表に、悪用行為の難易度と、セキュリティラベルが侵害される可能性を示します。

	侵害の可能性が非常に高い	侵害の可能性が高い	侵害の可能性が低い	侵害の可能性が非常に低い
悪用行為が非常に簡単	重大	重大	高	中
悪用行為がやや簡単	重大	高	中	中
悪用行為がやや難しい	高	中	中	低
悪用行為が非常に難しい	中	中	低	低

重要度の定義

重要度ラベルは次のように定義されています。

重大 - この問題は、さらに悪化しないように直ちに修復する必要があります。

例えば、公開された S3 バケットは重大な重要度の結果と考えられます。非常に多くの脅威アクターによって、公開された S3 バケットがスキャンされるため、公開された S3 バケット内のデータは、他者によって発見およびアクセスされる可能性があります。

一般に、パブリックにアクセス可能なリソースは、セキュリティ上の重大な問題と見なされます。重大な結果への対応は、緊急性が最も高くなります。また、リソースの重大度も考慮する必要があります。

高 - この問題は短期的な優先事項として対処する必要があります。

例えば、デフォルトの VPC セキュリティグループがインバウンドおよびアウトバウンドトラフィックに対して開かれている場合、重要度が高いと考えられます。脅威アクターがこの方法を使用して VPC を侵害することは、やや簡単であるためです。また、脅威アクターが VPC 内に侵入すると、リソースを中断または流出させる可能性があります。

Security Hub CSPM では、重要度の高い検出結果を短期的な優先度として扱うことをお勧めします。すぐに修復手順を実行する必要があります。また、リソースの重大度も考慮する必要があります。

中 - この問題は、中期的な優先事項として対処する必要があります。

例えば、転送中のデータの暗号化が欠如している場合、重要度が中程度の結果と考えられます。高度な中間者攻撃では、この弱点を悪用することになります。つまり、やや難しい攻撃手法です。脅威シナリオが成功すると、一部のデータが侵害される可能性があります。

Security Hub CSPM では、できるだけ早く関連するリソースを調査することをお勧めします。また、リソースの重大度も考慮する必要があります。

低 - この問題には、独自のアクションは必要ありません。

例えば、フォレンジック情報の収集に失敗した場合、重要度が低いと考えられます。この管理は将来の侵害を防ぐのに役立ちますが、フォレンジックが実行されない限り、侵害に直接つながりません。

重要度の低い結果については、すぐにアクションを実行する必要はありませんが、他の問題と相関関係がある場合は、コンテキストを入手できます。

情報 - 設定の弱点は見つかりませんでした。

つまり、ステータスは `PASSED`、`WARNING`、または `NOT AVAILABLE` です。

推奨されるアクションはありません。通知目的の結果は、顧客が準拠状態であることを実証するのに役立ちます。

コンプライアンスステータスとコントロールステータスの評価

AWS Security Finding 形式の `Compliance.Status`フィールドは、コントロール検出結果の結果を記述します。 AWS Security Hub CSPM は、コントロール検出結果のコンプライアンスステータスを使用して、全体的なコントロールステータスを決定します。コントロールのステータスは、Security Hub CSPM コンソールのコントロールの詳細ページに表示されます。

Security Hub CSPM の検出結果のコンプライアンスステータスの評価

各検出結果のコンプライアンスステータスには、以下のいずれかの値が割り当てられます。

- `PASSED` – コントロールが検出結果のセキュリティチェックに合格したことを示します。これにより、Security Hub CSPM が自動的に `Workflow.Status`に設定されます`RESOLVED`。
- `FAILED` – コントロールが検出結果のセキュリティチェックに合格しなかったことを示します。
- `WARNING` – Security Hub CSPM がリソースが `PASSED`または `FAILED`状態にあるかどうかを判断できないことを示します。たとえば、対応するAWS Config リソースタイプに対してリソース記録が有効になっていません。

- NOT_AVAILABLE – サーバーが失敗した、リソースが削除された、または AWS Config 評価の結果が であったため、チェックを完了できないことを示しますNOT_APPLICABLE。 AWS Config 評価結果が の場合NOT_APPLICABLE、Security Hub CSPM は自動的に結果をアーカイブします。

検出結果のコンプライアンスステータスが から FAILED、、WARNINGまたは PASSEDに変わりNOT_AVAILABLE、 が NOTIFIEDまたは Workflow.Statusの場合RESOLVED、Security Hub CSPM は自動的に Workflow.Statusに変わりますNEW。

コントロールに対応するリソースがない場合、Security Hub CSPM はアカウントレベルでPASSED結果を生成します。コントロールに対応するリソースがあるが、そのリソースを削除すると、Security Hub CSPM はNOT_AVAILABLE検出結果を作成し、すぐにアーカイブします。18 時間後、コントロールに対応するリソースがなくなったため、PASSED検出結果を受け取ります。

コンプライアンスステータスからコントロールステータスを取得する

Security Hub CSPM は、コントロールの検出結果のコンプライアンスステータスから全体的なコントロールステータスを取得します。コントロールステータスを決定する場合、Security Hub CSPM は RecordStateが である検出結果ARCHIVEDと が Workflow.Status である検出結果を無視しますSUPPRESSED。

コントロールステータスには、次のいずれかの値が割り当てられます。

- 合格 - すべての検出結果において PASSED がコンプライアンスステータス であることを示します。
- 失敗 - 少なくとも 1 つの検出結果において FAILED がコンプライアンスステータスであることを示します。
- 不明 - 少なくとも 1 つの検出結果のコンプライアンスステータスが WARNING または NOT_AVAILABLE であることを示します。コンプライアンスステータスが FAILED の検出結果はありません。
- データなし - コントロールの結果がないことを示します。例えば、新しく有効になったコントロールは、Security Hub CSPM がその検出結果の生成を開始するまで、このステータスになります。コントロールのすべての検出結果が SUPPRESSEDであるか、現在の で使用できない場合も、このステータスになります AWS リージョン。
- [無効] - 現在のアカウントとリージョンでコントロールが無効になっていることを示します。現在のアカウントとリージョンでは、現在このコントロールに対してセキュリティチェックは実行されていません。ただし、無効になっているコントロールの検出結果には、無効になった後、最大 24 時間コンプライアンスステータスの値が含まれる場合があります。

管理者アカウントの場合、コントロールステータスには管理者アカウントとメンバーアカウントのコントロールステータスが反映されます。具体的には、コントロールの全体的なステータスは、管理者アカウントまたはメンバーアカウントにコントロールに 1 つ以上の失敗した検出結果がある場合、[失敗]として表示されます。集約リージョンを設定している場合、集約リージョンのコントロールステータスには、集約リージョンとリンクされたリージョンのコントロールステータスが反映されます。具体的には、コントロールの全体的なステータスは、集約リージョンおよびリンクされたリージョンでコントロールに 1 つ以上の失敗した検出結果がある場合、[失敗] と表示されます。

Security Hub CSPM は通常、Security Hub CSPM コンソールの 概要ページまたはセキュリティ標準ページに初めてアクセスしてから 30 分以内に初期コントロールステータスを生成します。コントロールステータスを表示するには、AWS Config リソースレコードを設定する必要があります。コントロールステータスが初めて生成されると、Security Hub CSPM は、過去 24 時間の結果に基づいて 24 時間ごとにコントロールステータスを更新します。コントロールの詳細ページのタイムスタンプは、コントロールステータスが最後に更新された日時を示します。

> **Note**
>
> コントロールを初めて有効にすると、中国リージョンと でコントロールステータスが生成されるまでに最大 24 時間かかることがあります AWS GovCloud (US) Region。

セキュリティスコアの計算

AWS Security Hub CSPM コンソールで、概要ページとコントロールページに、有効なすべての標準にわたるセキュリティスコアの概要が表示されます。セキュリティ標準ページでは、Security Hub CSPM は、有効な標準ごとに 0 ~ 100% のセキュリティスコアも表示します。

Security Hub CSPM を初めて有効にすると、Security Hub CSPM は、コンソールの 概要またはセキュリティ標準ページに初めてアクセスしてから 30 分以内に、概要セキュリティスコアと標準セキュリティスコアを計算します。スコアは、コンソールでそれらのページにアクセスしたときに有効になっている標準に対してのみ生成されます。さらに、 AWS Config スコアが表示されるようにリソース記録を設定する必要があります。セキュリティスコアの概要は、標準のセキュリティスコアの平均値です。現在有効になっている標準のリストを確認するには、Security Hub CSPM API の GetEnabledStandards オペレーションを使用できます。

初めてスコアを生成した後、Security Hub CSPM はセキュリティスコアを 24 時間ごとに更新します。Security Hub CSPM には、セキュリティスコアが最後に更新された日時を示すタイムスタンプが表示されます。中国リージョンと で初めてセキュリティスコアが生成されるまでに最大 24 時間かかる場合があります AWS GovCloud (US) Regions。

統合コントロールの検出結果を有効にすると、セキュリティスコアが更新されるまでに最大 24 時間かかることがあります。さらに、新しい集約リージョンの有効化や、リンクされたリージョンの更新を行うと、既存のセキュリティスコアがリセットされます。Security Hub CSPM が、更新されたリージョンのデータを含む新しいセキュリティスコアを生成するまでに最大 24 時間かかる場合があります。

セキュリティスコアの計算方法

セキュリティスコアは、有効になっているコントロールのうち、合格の状態にあるコントロールの割合を示します。スコアは、小数点以下を最も近い整数に四捨五入したパーセンテージで表示されます。

Security Hub CSPM は、有効なすべての標準全体の概要セキュリティスコアを計算します。Security Hub CSPM は、有効な標準ごとにセキュリティスコアも計算します。スコアの計算に使用可能なコントロールには、[合格]、[失敗]、および [不明] のステータスが付いたコントロールが含まれます。ステータスが [データなし] のコントロールはスコア計算から除外されます。

Security Hub CSPM は、コントロールステータスを計算するときにアーカイブされた検出結果と抑制された検出結果を無視します。これはセキュリティスコアに影響する可能性があります。例えば、あるコントロールで失敗した検出結果をすべて抑制すると、そのステータスは「合格」になり、セキュリティスコアが向上する可能性があります。コントロールステータスの詳細については、コンプライアンスステータスとコントロールステータスの評価 を参照してください。

スコアリングの例:

規格	合格コントロール	失敗コントロール	未知のコントロール	標準スコア
AWS 基本的なセキュリティのベストプラクティス v1.0.0	168	22	0	88%
CIS AWS Foundations Benchmark v1.4.0	8	29	0	22%
CIS AWS Foundations	6	35	0	15%

規格	合格コントロール	失敗コントロール	未知のコントロール	標準スコア
Benchmark v1.2.0				
NIST 特別刊行物 800-53 リビジョン 5	159	56	0	74%
PCI DSS v3.2.1	28	17	0	62%

セキュリティスコアの概要を計算する場合、Security Hub CSPM は各コントロールを標準間で 1 回だけカウントします。例えば、有効な 3 つの標準に適用されるコントロールを有効にした場合、スコアの対象となるのは有効な 1 つのコントロールとしてのみカウントされます。

この例では、有効な標準全体で有効なコントロールの総数は 528 ですが、Security Hub CSPM はスコアリングの目的で各一意のコントロールを 1 回だけカウントします。有効になっている固有のコントロール数は 528 よりもおそらく少ないはずです。有効になっている固有のコントロール数が 515 で、通過した固有のコントロール数が 357 であると仮定すると、概要スコアは 69% になります。このスコアは、通過した固有のコントロール数を、有効なコントロールの総数 で割って計算されます。

現在のリージョンのアカウントで 1 つの標準のみを有効にした場合でも、標準セキュリティスコアとは異なる概要スコアがある場合があります。これは、管理者アカウントにサインインしていて、メンバーアカウントで追加の標準または異なる標準が有効になっている場合に発生する可能性があります。これは、集約リージョンからスコアを表示していて、リンクされたリージョンで追加の標準または異なる標準が有効になっている場合にも発生する可能性があります。

管理者アカウントのセキュリティスコア

管理者アカウントにログインしている場合、概要セキュリティスコアと標準スコアは、管理者アカウントおよびメンバーアカウントのすべてのコントロールステータスを考慮したものになります。

1 つのメンバーアカウントでコントロールのステータスが [失敗] の場合、管理者アカウントのステータスは [失敗] となり、管理者アカウントのスコアに影響を与えます。

管理者アカウントにログインしていて、集約リージョンを考慮したものになっている場合、セキュリティスコアは、すべてのメンバーアカウントおよびリンクされているすべてのリージョンを考慮したものになります。

集約リージョンを設定している場合のセキュリティスコア

集計を設定している場合 AWS リージョン、セキュリティスコアの概要と標準スコアは、すべてののコントロールステータスを考慮します。
リンクされたリージョン。

制御のステータスが 1 つのリンクされたリージョンでも [失敗] の場合、そのステータスは集約リージョンで [失敗] となり、集約リージョンスコアに影響を与えます。

管理者アカウントにログインしていて、集約リージョンを考慮したものになっている場合、セキュリティスコアは、すべてのメンバーアカウントおよびリンクされているすべてのリージョンを考慮したものになります。

Security Hub CSPM のコントロールカテゴリ

各コントロールにはカテゴリが割り当てられます。コントロールのカテゴリは、コントロールが適用されるセキュリティ機能を反映します。

カテゴリ値には、カテゴリ、カテゴリ内のサブカテゴリ、およびオプションでサブカテゴリ内の分類子が含まれます。例:

- 識別 > インベントリ
- 保護 > データ保護 > 転送中のデータの暗号化

ここでは、使用可能なカテゴリ、サブカテゴリ、および分類子の説明を示します。

識別

システム、アセット、データ、機能に対するサイバーセキュリティのリスクを管理するための組織の理解を深めます。

インベントリ

サービスは正しいリソースタグ付け戦略を実装していますか? タグ付け戦略にはリソース所有者が含まれていますか?

どのようなリソースをサービスで使用していますか? これらは、このサービスの承認されたリソースですか?

承認されたインベントリを可視化していますか? 例えば、Amazon EC2 Systems Manager やサービスカタログなどのサービスを使用しますか?

ログ記録

サービスに関連するすべてのログ記録を安全に有効化していますか? ログファイルの例は次のとおりです。

- Amazon VPC フローログ
- Elastic Load Balancing のアクセスログ
- Amazon CloudFront ログ
- Amazon CloudWatch Logs
- Amazon Relational Database Service のログ記録
- Amazon OpenSearch Service スローインデックスログ
- X-Ray トレース
- AWS Directory Service ログ
- AWS Config 項目
- スナップショット

保護

重要なインフラストラクチャサービスを確実に提供し、安全なコーディング手法を確保するための適切な保護策を開発および実施します。

安全なアクセス管理

サービスは、IAM ポリシーまたはリソースポリシーで最小特権プラクティスを使用していますか?

パスワードとシークレットは十分に複雑なものですか? 適切にローテーションしていますか?

サービスで多要素認証 (MFA) を使用しますか?

このサービスはルートユーザーを回避しますか?

リソースベースのポリシーはパブリックアクセスを許可しますか?

セキュアなネットワーク設定

サービスは、パブリックおよび安全でないリモートネットワークアクセスを回避しますか?

サービスは VPC を適切に使用しますか? 例えば、ジョブは VPC で実行する必要がありますか?

サービスは、機密性の高いリソースを適切にセグメント化および分離しますか?

データ保護

保管中のデータの暗号化 - サービスは保管中のデータを暗号化しますか?

転送中のデータの暗号化 - サービスで転送中のデータを暗号化していますか?

データの整合性 - サービスでデータの整合性を検証していますか?

データの削除保護 - サービスはデータの誤削除を防止しますか?

データの管理/使用状況 - 機密データの場所を証跡するために Amazon Macie などのサービスを使用していますか?

API の保護

サービスは、サービス API オペレーション AWS PrivateLink を保護するために を使用していますか ?

保護サービス

適切な保護サービスが提供されていますか? 保護サービスは正しい範囲をカバーしていますか?

保護サービスは、サービスに対する攻撃や侵害を回避するのに役立ちます。の保護サービスの例としては AWS AWS Control Tower、、 AWS WAF AWS Shield Advanced、Vanta、Secrets Manager、IAM Access Analyzer、 などがあります AWS Resource Access Manager。

安全な開発

安全なコーディングプラクティスを使用していますか?

Open Web Application Security Project (OWASP) Top 10 などの脆弱性を回避していますか?

検出

サイバーセキュリティイベントの発生を特定するための適切なアクティビティを開発および実施します。

検出サービス

正しい検出サービスは提供されていますか?

保護サービスは正しい範囲をカバーしていますか?

AWS 検出サービスの例としては、Amazon GuardDuty、 AWS Security Hub CSPM、Amazon Inspector、Amazon Detective、Amazon CloudWatch アラーム AWS IoT Device Defender、 などがあります AWS Trusted Advisor。

応答

検出されたサイバーセキュリティイベントに関するアクションを実行するための適切なアクティビティを開発および実施します。

レスポンスアクション

セキュリティイベントに迅速に対応していますか?

重要または重要度が高い結果が実際にありますか?

フォレンジック

サービスのフォレンジックデータを安全に取得できますか? 例えば、True ポジティブの結果に関連する Amazon EBS スナップショットを取得していますか?

フォレンジックアカウントを設定していますか?

復旧

耐障害性に関する計画を保持し、サイバーセキュリティイベントで損なわれた機能やサービスを復元するための適切なアクティビティを開発および実施します。

耐障害性

サービスの設定は、スムーズなフェイルオーバー、伸縮自在なスケーリング、高可用性をサポートしていますか?

バックアップを確立していますか?

Security Hub CSPM でのコントロールの詳細の確認

Security Hub CSPM コンソールのコントロールページまたは標準の詳細ページでコントロールを選択すると、コントロールの詳細のページが表示されます。

コントロールの詳細ページの上部には、コントロールのステータスが表示されます。コントロールステータスは、コントロールの検出結果のコンプライアンスステータスに基づき、コントロールのパフォーマンスを要約します。Security Hub CSPM は通常、Security Hub CSPM コンソールの 概要ページまたはセキュリティ標準ページに初めてアクセスしてから 30 分以内に初期コントロールステータスを生成します。ステータスは、これらのページにアクセスしたときに有効になっているコントロールでのみ使用できます。

コントロールの詳細ページには、過去 24 時間のコントロール結果のコンプライアンスステータスの内訳も表示されます。コントロールステータスとコンプライアンスステータスの詳細については、「コンプライアンスステータスとコントロールステータスの評価」 を参照してください。

AWS Config リソースの記録は、コントロールステータスが表示されるように設定する必要があります。コントロールステータスが初めて生成されると、Security Hub CSPM は過去 24 時間の調査結果に基づいて 24 時間ごとにコントロールステータスを更新します。

管理者アカウントには、管理者アカウントとメンバーアカウントを横断して集約されたコントロールステータスが表示されます。集約リージョンを設定すると、コントロールステータスには、リンクされたすべてのリージョンの検出結果が含まれます。コントロールステータスの詳細については、the section called “コンプライアンスステータスとコントロールステータス” を参照してください。

[コントロールの詳細] ページから、コントロールを無効または有効にすることもできます。

> **Note**
> 有効にしてから、最初のコントロールステータスのコントロールが中国リージョンと AWS GovCloud (US) Regionsで生成されるまで、最大で 24 時間かかります。

[標準と要件] タブには、コントロールが有効化できる標準と、さまざまなコンプライアンスフレームワークからのコントロールに関連する要件が一覧表示されます。

チェックタブには、過去 24 時間のコントロールのアクティブな検出結果が一覧表示されます。コントロールの検出結果は、Security Hub CSPM がコントロールのセキュリティチェックを実行するときに生成および更新されます。このタブのリストには、アーカイブされた結果は含まれません。

各検出結果について、リストからコンプライアンスステータスや関連リソースなどの検出結果の詳細にアクセスできます。各結果のワークフローステータスを設定し、結果をカスタムアクションに送信することもできます。詳細については、「コントロールの検出結果の確認と管理」を参照してください。

コントロールの詳細の表示

任意のアクセス方法を選択し、以下の手順に従ってコントロールの詳細を確認します。詳細は現在のアカウントとリージョンに適用されます。また、以下の内容を含みます。

- コントロールのタイトルと説明。
- 失敗したコントロールの検出結果の修正ガイダンスへのリンク。
- コントロールの重要度。
- コントロールのステータス。

コンソールでは、コントロールの最近の検出結果のリストを確認することもできます。プログラムでこれを行うには、Security Hub CSPM API の GetFindingsオペレーションを使用できます。

Security Hub CSPM console

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで [コントロール] を選択します。
3. コントロールを選択します。

Security Hub CSPM API

1. `ListSecurityControlDefinitions` を実行し、1 つ以上の標準 ARN を提供して、その標準におけるコントロール ID のリストを取得します。標準 ARN を取得するには、`DescribeStandards` を実行します。標準 ARN を指定しない場合、この API はすべての Security Hub CSPM コントロール IDsを返します。この API は、これらの機能リリース以前に存在していた標準ベースのコントロール ID ではなく、標準に依存しないセキュリティコントロール ID を返します。

   リクエストの例:

   ```
   {
   ```

```
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
}
```

2. を実行してBatchGetSecurityControls、現在の AWS アカウント および の 1 つ以上のコントロールに関する詳細を取得します AWS リージョン。

   リクエストの例:

```
{
    "SecurityControlIds": ["Config.1", "IAM.1"]
}
```

AWS CLI

1. list-security-control-definitions コマンドを実行し、1 つ以上の標準 ARN を提供してコントロール ID のリストを取得します。標準 ARN を取得するには、describe-standards コマンドを実行します。標準 ARN を指定しない場合、このコマンドはすべての Security Hub CSPM コントロール IDsを返します。このコマンドは、これらの機能リリース以前に存在していた標準ベースのコントロール ID ではなく、標準に依存しないセキュリティコントロール ID を返します。

```
aws securityhub --region us-east-1 list-security-control-definitions --standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0"
```

2. batch-get-security-controls コマンドを実行し、 AWS アカウント および AWS リージョンにおける 1 つ以上のコントロールの詳細を取得します。

```
aws securityhub --region us-east-1 batch-get-security-controls --security-control-ids '["Config.1", "IAM.1"]'
```

Security Hub CSPM でのコントロールのフィルタリングとソート

AWS Security Hub CSPM コンソールで、コントロールページを使用して、現在の で利用可能なコントロールのテーブルを確認できます AWS リージョン。例外は集約リージョンです。集約リージョン

を設定し、そのリージョンにサインインした場合、コンソールには集約リージョンまたは 1 つ以上のリンクされたリージョンで使用できるコントロールが表示されます。

コントロールの特定のサブセットに焦点を当てるために、コントロールのテーブルをソートおよびフィルタリングできます。テーブルの横にあるフィルターオプションを使用すると、これらの特定のサブセットにすばやく集中できます。

- すべての有効なコントロール。少なくとも 1 つの有効な標準で有効になっているコントロールです。
- すべての無効なコントロール。すべての標準で無効になっているコントロールです。
- Failed など、特定のコントロールステータスを持つすべての有効なコントロール。データなしオプションには、現在検出結果がないコントロールのみが表示されます。コントロールステータスの詳細については、「」を参照してください[コンプライアンスステータスとコントロールステータスの評価](#)。

Filter by オプションに加えて、テーブルの上にある Filter controls ボックスにフィルター条件を入力して、テーブルをフィルタリングできます。例えば、コントロール ID または重要度でフィルタリングできます。

デフォルトでは、失敗ステータスのコントロールが最初に重要度順に一覧表示されます。ソート順序を変更するには、別の列見出しを選択します。

> **Tip**
>
> コントロールの検出結果に基づいて自動化されたワークフローがある場合は、`SecurityControlId` または `SecurityControlArn` ASFF フィールドを `Title`または `Description`フィールドではなくフィルターとして使用することをお勧めします。後者のフィールドは変更されることがありますが、コントロール ID と ARN は静的識別子です。

Security Hub CSPM 管理者アカウントにサインインしている場合、有効なコントロールには、少なくとも 1 つのメンバーアカウントで有効になっているコントロールが含まれます。集約リージョンを設定した場合、有効なコントロールには、少なくとも 1 つのリンクされたリージョンで有効になっているコントロールが含まれます。

有効なコントロールの横にあるオプションを選択すると、パネルが表示され、コントロールが現在有効になっている標準が表示されます。また、コントロールが現在無効になっている標準も確認でき

ます。このパネルから、すべての標準でコントロールを無効にすることができます。詳細については、「Security Hub CSPM でのコントロールの無効化」を参照してください。管理者アカウントの場合、パネルの情報はすべてのメンバーアカウントの設定を反映します。

プログラムでコントロールのリストを取得するには、Security Hub CSPM API の ListSecurityControlDefinitionsオペレーションを使用できます。個々のコントロールの詳細を取得するには、 BatchGetSecurityControlsオペレーションを使用します。

Security Hub CSPM のコントロールパラメータについて

AWS Security Hub CSPM の一部のコントロールは、コントロールの評価方法に影響するパラメータを使用します。通常、このようなコントロールは、Security Hub CSPM が定義するデフォルトのパラメータ値に対して評価されます。ただし、これらのコントロールのサブセットについては、パラメータ値を変更することができます。コントロールパラメータ値を変更すると、Security Hub CSPM は指定した値に対してコントロールの評価を開始します。コントロールの基盤となるリソースがカスタム値を満たす場合、Security Hub CSPM は`PASSED`検出結果を生成します。リソースがカスタム値を満たさない場合、Security Hub CSPM は`FAILED`検出結果を生成します。

コントロールパラメータをカスタマイズすることで、ビジネス要件とセキュリティの期待に合わせて、Security Hub CSPM が推奨およびモニタリングするセキュリティのベストプラクティスを絞り込むことができます。コントロールの検出結果を抑制する代わりに、1 つ以上のパラメータをカスタマイズして、セキュリティニーズに合った検出結果を取得することができます。

コントロールパラメータの変更とカスタム値の設定のサンプルユースケースを以下に示します。

- [CloudWatch.16] – CloudWatch ロググループは指定した期間保持する必要があります

  保持期間を指定できます。
- [IAM.7] – IAM ユーザーのパスワードポリシーには強力な設定が必要です

  パスワード強度に関するパラメータを指定できます。
- [EC2.18] – セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可する必要があります

  無制限の着信トラフィックを許可するように承認するポートを指定できます。
- [Lambda.5] – VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります

  成功の検出結果を生成するアベイラビリティーゾーンの最小数を指定できます。

このセクションでは、コントロールパラメータを変更するときに考慮すべき事項について説明します。

コントロールパラメータ値の変更による影響

パラメータ値を変更する場合は、新しい値に基づいてコントロールを評価する新しいセキュリティチェックもトリガーします。次に、Security Hub CSPM は、新しい値に基づいて新しいコントロール結果を生成します。コントロールの検出結果の定期的な更新中、Security Hub CSPM は新しいパラメータ値も使用します。コントロールのパラメータ値を変更しても、コントロールを含む標準を有効にしていない場合、Security Hub CSPM は新しい値を使用してセキュリティチェックを行いません。新しいパラメータ値に基づいてコントロールを評価するには、Security Hub CSPM に関連する標準を少なくとも 1 つ有効にする必要があります。

コントロールは、1 つまたは複数のカスタマイズ可能なパラメータを持つことができます。それぞれのコントロールパラメータで使用可能なデータ型には以下が含まれます。

- ブール値
- 倍精度
- 列挙型
- EnumList
- 整数
- IntegerList
- String
- StringList

カスタムパラメータ値は、有効になっている標準全体に適用されます。現在のリージョンでサポートされていないコントロールのパラメータはカスタマイズできません。個々のコントロールに関するリージョンの制限のリストについては、「Security Hub CSPM コントロールのリージョン制限」を参照してください。

一部のコントロールは、許容パラメータ値も指定された範囲に収まらないと有効になりません。このような場合、Security Hub CSPM は許容範囲を提供します。

Security Hub CSPM はデフォルトのパラメータ値を選択し、場合によっては更新することがあります。コントロールパラメータをカスタマイズしても、その値は、変更しない限りパラメータに指定した値のままです。つまり、 パラメータのカスタム値が Security Hub CSPM で定義されている現在のデフォルト値と一致していても、 パラメータはデフォルトの Security Hub CSPM 値への更新の追跡

を停止します。コントロール「[ACM.1] – インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります」の例を以下に示します。

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 30
            }
        }
    }
}
```

前の例では、`daysToExpiration` パラメータのカスタム値は `30` です。このパラメータの現在のデフォルト値も `30` です。Security Hub CSPM がデフォルト値を に変更した場合14、この例の パラメータはその変更を追跡しません。`30` の値は保持されます。

パラメータのデフォルトの Security Hub CSPM 値の更新を追跡する場合は、 `DEFAULT`の代わりに `ValueType`フィールドを に設定します`CUSTOM`。詳細については、「1 つのアカウントおよびリージョンでデフォルトのコントロールパラメータ値に戻す」を参照してください。

カスタムパラメータをサポートするコントロール

カスタムパラメータをサポートするセキュリティコントロールのリストについては、Security Hub CSPM コンソールの「コントロール」ページまたは「」を参照してくださいSecurity Hub CSPM のコントロールリファレンス。このリストをプログラムで取得するには、ListSecurityControlDefinitions 操作を使用します。レスポンスで、`CustomizableProperties` オブジェクトによって、どのコントロールがカスタマイズ可能なパラメータをサポートしているかが示されます。

現在のコントロールパラメータ値の確認

変更する前に、コントロールパラメータの現在の値を知っておくと便利です。

アカウント内の個々のコントロールパラメータの現在の値を確認できます。中央設定を使用する場合、委任 AWS Security Hub CSPM 管理者は、設定ポリシーで指定されたパラメータ値を確認することもできます。

希望する方法を選択し、手順に従って現在のコントロールパラメータ値を確認します。

Security Hub CSPM console

現在のコントロールパラメータ値を確認するには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで [コントロール] を選択します。コントロールを選択します。
3. [パラメータ] タブを選択します。このタブに、コントロールの現在のパラメータ値が表示されます。

Security Hub CSPM API

現在のコントロールパラメータ値を確認するには (API)

BatchGetSecurityControls API を呼び出し、1 つ以上のセキュリティコントロール ID または ARN を指定します。レスポンス内の `Parameters` オブジェクトに、指定されたコントロールの現在のパラメータ値が表示されます。

たとえば、次の AWS CLI コマンドは、、`APIGatway.1`、`CloudWatch.15`および の現在のパラメータ値を示しています`IAM.7`。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

希望する方法を選択し、中央設定ポリシーの現在のパラメータ値を表示します。

Security Hub CSPM console

設定ポリシーの現在のコントロールパラメータ値を確認するには (コンソール)

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

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

3. [ポリシー] タブで、設定ポリシーを選択し、[詳細を表示] を選択します。すると、現在のパラメータ値を含むポリシーの詳細が表示されます。

Security Hub CSPM API

設定ポリシーの現在のコントロールパラメータ値を確認するには (API)

1. ホームリージョンの委任管理者アカウントから GetConfigurationPolicy API を呼び出します。
2. 詳細を確認したい設定ポリシーの ARN または ID を指定します。レスポンスに、現在のパラメータ値が含まれています。

たとえば、次の AWS CLI コマンドは、指定された設定ポリシーの現在のコントロールパラメータ値を取得します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

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

コントロールの検出結果には、コントロールパラメータの現在の値も含まれます。AWS Security Finding 形式 (ASFF) では、これらの値は `Compliance` オブジェクトの `Parameters` フィールドに表示されます。Security Hub CSPM コンソールで検出結果を確認するには、ナビゲーションペインで検出結果を選択します。プログラムで検出結果を確認するには、Security Hub CSPM API の GetFindingsオペレーションを使用します。

コントロールパラメータ値のカスタマイズ

コントロールパラメータをカスタマイズする手順は、 AWS Security Hub CSPM で中央設定を使用するかどうかによって異なります。中央設定は、委任 Security Hub CSPM 管理者が AWS リージョン、、アカウント、組織単位 (OUs。

組織が中央設定を使用している場合、委任管理者は、カスタムコントロールパラメータを含む設定ポリシーを作成できます。これらのポリシーは、一元管理されるメンバーアカウントや OU に関連付けることができ、自分のホームリージョンおよびリンクされているすべてのリージョンで有効にな

ります。委任管理者は 1 つ以上のアカウントをセルフマネージドとして指定することもできます。これにより、アカウント所有者は各リージョンで独自のパラメータを個別に設定できるようになります。組織で中央設定を使用していない場合は、アカウントおよびリージョンごとにコントロールパラメータを個別にカスタマイズする必要があります。

組織のさまざまな部分でコントロールパラメータ値を整合させることができるため、中央設定を使用することをお勧めします。例えば、すべてのテストアカウントが特定のパラメータ値を使用し、すべての本番稼働用アカウントが異なる値を使用する場合があります。

複数のアカウントおよびリージョンのコントロールパラメータをカスタマイズする

中央設定を使用する組織の委任 Security Hub CSPM 管理者である場合は、任意の方法を選択し、手順に従って複数のアカウントとリージョンでコントロールパラメータをカスタマイズします。

Security Hub CSPM console

複数のアカウントおよびリージョンのコントロールパラメータ値をカスタマイズするには (コンソール)

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

   ホームリージョンにサインインしていることを確認します。
2. ナビゲーションペインで、[設定]、[設定] の順に選択します。
3. [Policies] タブを選択します。
4. カスタムパラメータを含む新しい設定ポリシーを作成するには、[ポリシーの作成] を選択します。既存の設定ポリシーでカスタムパラメータを指定するには、ポリシーを選択し、[編集] を選択します。

   カスタムコントロールパラメータ値を使用して新しい設定ポリシーを作成するには

   1. [カスタムポリシー] セクションで、有効にするセキュリティ標準およびコントロールを選択します。
   2. [コントロールパラメータをカスタマイズする] を選択します。
   3. コントロールを選択し、1 つ以上のパラメータにカスタム値を指定します。
   4. その他のコントロールのパラメータをカスタマイズするには、[その他のコントロールをカスタマイズする] を選択します。
   5. [アカウント] セクションで、ポリシーを適用するアカウントまたは OU を選択します。

6. [次へ] を選択します。
7. [ポリシーを作成して適用] を選択します。ホームリージョンおよびリンクされているすべてのリージョンで、このアクションにより、この設定ポリシーに関連付けられているアカウントおよび OU の既存の構成設定がオーバーライドされます。アカウントと OU は、直接適用するか親から継承することによって、設定ポリシーに関連付けることができます。

既存の設定ポリシーでコントロールパラメータ値をカスタマイズするには

1. [コントロール] セクションの [カスタムポリシー] で、必要な新しいカスタムパラメータ値を指定します。
2. このポリシーでコントロールパラメータをカスタマイズするのが初めての場合は、[コントロールパラメータをカスタマイズする] を選択し、カスタマイズするコントロールを選択します。その他のコントロールのパラメータをカスタマイズするには、[その他のコントロールをカスタマイズする] を選択します。
3. [アカウント] セクションで、ポリシーを適用するアカウントまたは OU を確認します。
4. [次へ] を選択します。
5. 変更内容を見直し、それらが正しいことを確認します。完了したら、[ポリシーを保存して適用] を選択します。ホームリージョンおよびリンクされているすべてのリージョンで、このアクションにより、この設定ポリシーに関連付けられているアカウントおよび OU の既存の構成設定がオーバーライドされます。アカウントと OU は、直接適用するか親から継承することによって、設定ポリシーに関連付けることができます。

Security Hub CSPM API

複数のアカウントおよびリージョン (API) のコントロールパラメータ値をカスタマイズするには

カスタムコントロールパラメータ値を使用して新しい設定ポリシーを作成するには

1. ホームリージョンの委任管理者アカウントから CreateConfigurationPolicy API を呼び出します。
2. `SecurityControlCustomParameters` オブジェクトには、カスタマイズする各コントロールの識別子を指定します。
3. `Parameters` オブジェクトには、カスタマイズする各パラメータの名前を指定します。カスタマイズする各パラメータで、`ValueType` に `CUSTOM` を指定します。`Value` には、パラメータのデータ型とカスタム値を指定します。`ValueType` が `CUSTOM` の場合、`Value` フィールドを空にすることはできません。コントロールがサポートす

るパラメータをリクエストで省略した場合、そのパラメータは現在の値を保持します。GetSecurityControlDefinition API を呼び出すことで、コントロールでサポートされているパラメータ、データ型、有効な値を確認できます。

既存の設定ポリシーでコントロールパラメータ値をカスタマイズするには

1. ホームリージョンの委任管理者アカウントから UpdateConfigurationPolicy API を呼び出します。
2. `Identifier` フィールドには、更新する設定ポリシーの Amazon リソースネーム (ARN) または ID を指定します。
3. `SecurityControlCustomParameters` オブジェクトには、カスタマイズする各コントロールの識別子を指定します。
4. `Parameters` オブジェクトには、カスタマイズする各パラメータの名前を指定します。カスタマイズする各パラメータで、`ValueType` に `CUSTOM` を指定します。`Value` には、パラメータのデータ型とカスタム値を指定します。コントロールがサポートするパラメータをリクエストで省略した場合、そのパラメータは現在の値を保持します。GetSecurityControlDefinition API を呼び出すことで、コントロールでサポートされているパラメータ、データ型、有効な値を確認できます。

たとえば、次の AWS CLI コマンドは、 の `daysToExpiration`パラメータのカスタム値を使用して新しい設定ポリシーを作成します`ACM.1`。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

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

1 つのアカウントおよびリージョンでコントロールパラメータをカスタマイズする

中央設定を使用していない場合、またはセルフマネージドアカウントがある場合は、一度に 1 つのリージョンでのみアカウントのコントロールパラメータをカスタマイズできます。

希望する方法を選択し、手順に従ってコントロールパラメータをカスタマイズします。変更は、現在のリージョンのアカウントにのみ適用されます。別のリージョンでコントロールパラメータをカスタマイズするには、パラメータをカスタマイズする別のアカウントおよびリージョンごとに以下の手順を繰り返します。同じコントロールでも、リージョンごとに異なるパラメータ値を使用できます。

Security Hub CSPM console

1 つのアカウントおよびリージョン (コンソール) でコントロールパラメータ値をカスタマイズするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで [コントロール] を選択します。テーブルで、カスタムパラメータをサポートしていて、パラメータを変更したいコントロールを選択します。[カスタムパラメータ] 列に、どのコントロールがカスタムパラメータをサポートしているかが示されます。
3. コントロールの詳細ページで、[パラメータ] タブを選択し、[編集] を選択します。
4. 必要なパラメータ値を指定します。
5. 必要に応じて、[変更の理由] セクションで、パラメータをカスタマイズする理由を選択します。
6. [保存] を選択します。

Security Hub CSPM API

1 つのアカウントおよびリージョン (API) でコントロールパラメータ値をカスタマイズするには

1. UpdateSecurityControl API を呼び出します。
2. `SecurityControlId` には、カスタマイズするコントロールの ID を指定します。
3. `Parameters` オブジェクトには、カスタマイズする各パラメータの名前を指定します。カスタマイズする各パラメータで、`ValueType` に `CUSTOM` を指定します。`Value` には、パラメータのデータ型とカスタム値を指定します。コントロールがサポートするパラメータをリクエストで省略した場合、そのパラメータは現在の値を保持しま

す。GetSecurityControlDefinition API を呼び出すことで、コントロールでサポートされているパラメータ、データ型、有効な値を確認できます。

4. 必要に応じて、`LastUpdateReason` に、コントロールパラメータをカスタマイズする理由を入力します。

たとえば、次の AWS CLI コマンドは の `daysToExpiration`パラメータのカスタム値を定義しますACM.1。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer":
 15}}}' \
--last-update-reason "Internal compliance requirement"
```

デフォルトのコントロールパラメータ値に戻す

コントロールパラメータには、 AWS Security Hub CSPM が定義するデフォルト値を含めることができます。Security Hub CSPM は、進化するセキュリティのベストプラクティスを反映するために、パラメータのデフォルト値を更新することがあります。コントロールパラメータにカスタム値を指定していない場合、コントロールは、これらの更新を自動的に追跡し、新しいデフォルト値を使用します。

コントロールのデフォルトパラメータ値を使用するように戻すことができます。元に戻す手順は、Security Hub CSPM で中央設定を使用するかどうかによって異なります。中央設定は、委任 Security Hub CSPM 管理者が AWS リージョン、、アカウント、組織単位 (OUs。

> **Note**
>
> すべてのコントロールパラメータにデフォルトの Security Hub CSPM 値があるわけではありません。このような場合、 `ValueType`を に設定すると`DEFAULT`、Security Hub CSPM が使用する特定のデフォルト値はありません。むしろ、カスタム値がない場合、Security Hub CSPM は パラメータを無視します。

複数のアカウントおよびリージョンでデフォルトのパラメータに戻す

中央設定を使用すると、ホームリージョンとリンクされたリージョン内の複数の一元管理されるアカウントや OU のコントロールパラメータを元に戻すことができます。

希望する方法を選択し、手順に従って、中央設定を使用して複数のアカウントおよびリージョンでデフォルトのパラメータ値に戻します。

Security Hub CSPM console

複数のアカウントおよびリージョンでデフォルトのコントロールパラメータ値に戻すには (コンソール)

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

   ホームリージョンの委任 Security Hub CSPM 管理者アカウントの認証情報を使用してサインインします。
2. ナビゲーションペインで、[設定]、[設定] の順に選択します。
3. [Policies] タブを選択します。
4. ポリシーを選択し、[編集] を選択します。
5. [カスタムポリシー] の [コントロール] セクションに、カスタムパラメータを指定したコントロールのリストが表示されます。
6. 元に戻すパラメータ値が 1 つ以上あるコントロールを見つけます。そして、[削除] を選択してデフォルト値に戻します。
7. [アカウント] セクションで、ポリシーを適用するアカウントまたは OU を確認します。
8. [次へ] を選択します。
9. 変更内容を見直し、それらが正しいことを確認します。完了したら、[ポリシーを保存して適用] を選択します。ホームリージョンおよびリンクされているすべてのリージョンで、このアクションにより、この設定ポリシーに関連付けられているアカウントおよび OU の既存の構成設定がオーバーライドされます。アカウントと OU は、直接適用するか親から継承することによって、設定ポリシーに関連付けることができます。

Security Hub CSPM API

複数のアカウントおよびリージョンでデフォルトのコントロールパラメータ値に戻すには (API)

1. ホームリージョンの委任管理者アカウントから UpdateConfigurationPolicy API を呼び出します。
2. `Identifier` フィールドには、更新するポリシーの Amazon リソースネーム (ARN) または ID を指定します。
3. `SecurityControlCustomParameters` オブジェクトには、1 つ以上のパラメータを元に戻す各コントロールの識別子を指定します。
4. `Parameters` オブジェクトでは、元に戻すパラメータごとに、`ValueType` フィールドに `DEFAULT` を指定します。`ValueType` を `DEFAULT` に設定すると、`Value` フィールドに値を指定する必要がなくなります。リクエストに値が含まれている場合、Security Hub CSPM はそれを無視します。コントロールがサポートするパラメータをリクエストで省略した場合、そのパラメータは現在の値を保持します。

> **Warning**
>
> `SecurityControlCustomParameters` フィールドからコントロールオブジェクトを省略すると、Security Hub CSPM はコントロールのすべてのカスタムパラメータをデフォルト値に戻します。`SecurityControlCustomParameters` のリストが完全に空の場合は、すべてのコントロールのカスタムパラメータがデフォルト値に戻ります。

たとえば、次の AWS CLI コマンドは、 の`daysToExpiration`コントロールパラメータ`ACM.1`を、指定された設定ポリシーのデフォルト値に戻します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--name "TestConfigurationPolicy" \
--description "Updated configuration policy" \
--updated-reason "Revert ACM.1 parameter to default value"
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
```

```
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "DEFAULT"}}}]}}}'
```

1 つのアカウントおよびリージョンでデフォルトのコントロールパラメータ値に戻す

中央設定を使用していない場合、またはセルフマネージドアカウントがある場合は、一度に 1 つのリージョンでアカウントのデフォルトパラメータ値を使用するように戻すことができます。

希望する方法を選択し、手順に従って 1 つのリージョンでアカウントのデフォルトのパラメータ値に戻します。別のリージョンでデフォルトのパラメータ値に戻すには、それぞれのリージョンでこれらの手順を繰り返します。

> **Note**
>
> Security Hub CSPM を無効にすると、カスタムコントロールパラメータがリセットされます。今後 Security Hub CSPM を再度有効にすると、すべてのコントロールはデフォルトのパラメータ値を使用して開始します。

Security Hub CSPM console

1 つのアカウントおよびリージョンでデフォルトのコントロールパラメータ値に戻すには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで [コントロール] を選択します。デフォルトのパラメータ値に戻すコントロールを選択します。
3. `Parameters` タブで、コントロールパラメータの横にある [カスタマイズ済み] を選択します。そして、[カスタマイズを削除] を選択します。このパラメータは、デフォルトの Security Hub CSPM 値を使用し、デフォルト値への今後の更新を追跡するようになりました。
4. 元に戻すパラメータ値ごとに、上記のステップを繰り返します。

Security Hub CSPM API

1 つのアカウントおよびリージョンでデフォルトのコントロールパラメータ値に戻すには (API)

1. UpdateSecurityControl API を呼び出します。
2. `SecurityControlId` には、パラメータを元に戻すコントロールの ARN または ID を指定します。
3. `Parameters` オブジェクトでは、元に戻すパラメータごとに、`ValueType` フィールドに `DEFAULT` を指定します。`ValueType` を `DEFAULT` に設定すると、`Value` フィールドに値を指定する必要がなくなります。リクエストに値が含まれている場合、Security Hub CSPM はそれを無視します。
4. 必要に応じて、`LastUpdateReason` に、デフォルトのパラメータ値に戻す理由を入力します。

たとえば、次の AWS CLI コマンドは、 の`daysToExpiration`コントロールパラメータ`ACM.1`をデフォルト値に戻します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

コントロールパラメータの変更ステータスをチェックする

コントロールパラメータをカスタマイズしたり、デフォルト値に戻したりしようとすると、目的の変更が有効であったかどうかを検証できます。これにより、コントロールが期待どおりに機能し、意図したセキュリティ値を提供することを確認できます。パラメータの更新が失敗した場合、Security Hub CSPM はパラメータの現在の値を保持します。

パラメータの更新が成功したことを確認するには、Security Hub CSPM コンソールでコントロールの詳細を確認できます。コンソールで、[コントロール] をクリックします。次に、詳細を表示するコントロールを選択します。[パラメータ] タブに、パラメータ変更のステータスが表示されます。

プログラム上では、パラメータの更新リクエストが有効な場合、BatchGetSecurityControls 操作を受けて `UpdateStatus` フィールドの値が `UPDATING` になります。つまり、更新は有効でも、すべての検出結果には更新されたパラメータ値がまだ含まれていない可能性があります。の値がにUpdateState変わるとREADY、Security Hub CSPM は、コントロールのセキュリティチェックを実行するときに更新されたコントロールパラメータ値を使用します。検出結果には、更新されたパラメータ値が含まれます。

`UpdateSecurityControl` 操作は、無効なパラメータ値に対して `InvalidInputException` レスポンスを返します。このレスポンスにより、失敗の理由に関するさらなる詳細が提供されます。例えば、パラメータの有効範囲外の値を指定した可能性があります。あるいは、正しいデータ型を使用していない値を指定した可能性があります。有効な入力内容でリクエストを再送信します。

パラメータ値を更新しようとしたときに内部障害が発生した場合、 AWS Config 有効にすると Security Hub CSPM は自動的に再試行します。詳細については、「を有効にして設定する前に考慮すべき点 AWS Config」を参照してください。

Security Hub CSPM でのコントロールの検出結果の確認と管理

コントロールの詳細ページには、コントロールのアクティブな検出結果のリストが表示されます。このリストには、アーカイブされた結果は含まれていません。

コントロールの詳細ページでは、クロスリージョン集約をサポートしています。集約リージョンを設定している場合、コントロール詳細ページのコントロールステータスおよびセキュリティチェックのリストには、リンクされているすべての AWS リージョンのチェックが含まれます。

リストには、結果をフィルタリングおよびソートするためのツールが用意されており、急を要する結果から重点的に取り組むことができます。検出結果には、関連するサービスコンソールにおけるリソースの詳細へのリンクが含まれている場合があります。 AWS Config ルールに基づくコントロールの場合、ルールの詳細を表示できます。

AWS Security Hub CSPM API を使用して、検出結果と検出結果の詳細のリストを取得することもできます。

詳細については、「検出結果の詳細と履歴の確認」を参照してください。

コントロール検出結果の調査の現在のステータスを反映するには、ワークフローステータスを設定します。詳細については、「the section called “結果のワークフローステータスを設定する”」を参照してください。

選択した Security Hub CSPM の検出結果を Amazon EventBridge のカスタムアクションに送信することもできます。詳細については、「the section called “カスタムアクションに結果を送信する”」を参照してください。

トピック

- コントロール検出結果のフィルタリングとソート
- コントロールの検出結果のサンプル

コントロール検出結果のフィルタリングとソート

AWS Security Hub CSPM コンソールのコントロールページまたは標準の詳細ページからコントロールを選択すると、コントロールの詳細ページが表示されます。

コントロールの詳細ページには、コントロールのタイトルと説明、全体的なコントロールステータス、過去 24 時間のコントロールのセキュリティチェックの内訳が表示されます。

コントロールチェックリストの横にある [フィルター条件] オプションを使用して、特定のワークフローステータスまたはコンプライアンスステータス の検出結果にすばやく焦点を合わせます。

Filter by オプションに加えて、Add filter ボックスを使用して、 AWS アカウント ID やリソース ID などの他のフィールドでチェックリストをフィルタリングできます。

デフォルトでは、コンプライアンスステータスが [合格] の結果が最初に一覧表示されます。列ヘッダーで別のオプションを選択して、デフォルトのソートを変更できます。

コントロールの詳細ページから、[ダウンロード] を選んでコントロール検出結果の現在のページを.csv ファイルにダウンロードできます。

検出結果リストをフィルタリングする場合は、ダウンロードにはフィルターに一致するコントロールのみが含まれます。リストから特定の検出結果を選択する場合は、ダウンロードには選択した検出結果のみが含まれます。

検出結果フィルターの詳細については、Security Hub CSPM での検出結果のフィルタリング を参照してください。

コントロールの検出結果のサンプル

次のサンプルは、 AWS Security Finding 形式 (ASFF) の AWS Security Hub CSPM コントロールの検出結果の例を示しています。コントロールの検出結果の内容は、統合コントロールの検出結果を有効にしたかどうかによって異なります。

統合コントロールの検出結果を有効にすると、コントロールが複数の有効な標準に適用されていても、Security Hub CSPM はコントロールに対して 1 つの検出結果を生成します。この機能を有効にしない場合、Security Hub CSPM は、コントロールが適用される有効な標準ごとに個別のコントロール結果を生成します。例えば、2 つの標準を有効にし、その両方にコントロールが適用される場合、コントロールには 2 つの異なる検出結果が表示され、各標準に 1 つずつ表示されます。統合コントロールの検出結果を有効にすると、コントロールに対して 1 つの検出結果のみが表示されます。詳細については、「統合されたコントロールの検出結果」を参照してください。

このページのサンプルでは、両方のシナリオの例を示します。サンプルには、統合統制結果が無効になっている場合の個々の Security Hub CSPM 標準の統制結果と、統合統制結果が有効になっている場合の複数の Security Hub CSPM 標準の統制結果が含まれます。

コントロールの検出結果のサンプル

- AWS Foundational Security Best Practices 標準の調査結果の例
- CIS AWS Foundations Benchmark v3.0.0 のサンプル結果
- CIS AWS Foundations Benchmark v1.4.0 のサンプル結果
- CIS AWS Foundations Benchmark v1.2.0 のサンプル結果
- NIST SP 800-53 リビジョン 5 標準のサンプル結果
- NIST SP 800-171 リビジョン 2 標準のサンプル結果
- Payment Card Industry Data Security Standard v3.2.1 のサンプル結果
- AWS リソースタグ付け標準のサンプル結果
- AWS Control Tower サービスマネージド標準のサンプル検出結果
- 複数の標準の統合結果の例

> **Note**
>
> コントロールの検出結果は、中国リージョンと AWS GovCloud (US) リージョンのさまざまなフィールドと値を参照します。詳細については、「ASFF フィールドと値への統合の影響」を参照してください。

AWS Foundational Security Best Practices 標準の調査結果の例

次のサンプルは、 AWS Foundational Security Best Practices (FSBP) 標準に適用されるコントロールの検出結果の例を示しています。このサンプルでは、統合コントロールの検出結果は無効になっています。

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.076Z",
  "LastObservedAt": "2021-09-28T16:10:06.956Z",
  "CreatedAt": "2020-08-06T02:18:23.076Z",
  "UpdatedAt": "2021-09-28T16:10:00.093Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-
practices/v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0",
    "ControlId": "CloudTrail.2",
```

```
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/aws-foundation-best-practices/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
```

```
      "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
    ]
  }
}
```

CIS AWS Foundations Benchmark v3.0.0 のサンプル結果

次のサンプルは、CIS AWS Foundations Benchmark v3.0.0 に適用されるコントロールの検出結果の例を示しています。このサンプルでは、統合コントロールの検出結果は無効になっています。

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2024-04-18T07:46:18.193Z",
  "LastObservedAt": "2024-04-23T07:47:01.137Z",
  "CreatedAt": "2024-04-18T07:46:18.193Z",
  "UpdatedAt": "2024-04-23T07:46:46.165Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.2.1 EBS default encryption should be enabled",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
 the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
 at EBS volume creation is supported.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub CSPM controls documentation.",
```

```
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/3.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0",
    "ControlId": "2.2.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2843ed9e",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v3.0.0/2.2.1"
    ],
    "SecurityControlId": "EC2.7",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
```

```
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  },
  "ProcessedAt": "2024-04-23T07:47:07.088Z"
}
```

CIS AWS Foundations Benchmark v1.4.0 のサンプル結果

次のサンプルは、CIS AWS Foundations Benchmark v1.4.0 に適用されるコントロールの検出結果の例を示しています。このサンプルでは、統合コントロールの検出結果は無効になっています。

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/1.4.0/3.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2022-10-21T22:14:48.913Z",
  "LastObservedAt": "2022-12-22T22:24:56.980Z",
  "CreatedAt": "2022-10-21T22:14:48.913Z",
  "UpdatedAt": "2022-12-22T22:24:52.409Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
```

```
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS CloudTrail is a web service that records AWS API calls for an
 account and makes those logs available to users and resources in accordance with IAM
 policies. AWS Key Management Service (KMS) is a managed service that helps create
 and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail logs
 can be configured to leverage server side encryption (SSE) and AWS KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0",
    "ControlId": "3.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-855f82d1",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/1.4.0/3.7",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
```

```
      "Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  }
}
```

CIS AWS Foundations Benchmark v1.2.0 のサンプル結果

次のサンプルは、CIS AWS Foundations Benchmark v1.2.0 に適用されるコントロールの検出結果の例を示しています。このサンプルでは、統合コントロールの検出結果は無効になっています。

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
```

```
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/
rule/2.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2020-08-29T04:10:06.337Z",
  "LastObservedAt": "2021-09-28T16:10:05.350Z",
  "CreatedAt": "2020-08-29T04:10:06.337Z",
  "UpdatedAt": "2021-09-28T16:10:00.087Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS Key Management Service (KMS) is a managed service that helps
 create and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail
 logs can be configured to leverage server side encryption (SSE) and KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsGuideArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0",
    "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
    "RuleId": "2.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
```

```
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/cis-aws-
foundations-benchmark/v/1.2.0/2.7",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  }
}
```

NIST SP 800-53 リビジョン 5 標準のサンプル結果

次のサンプルは、NIST SP 800-53 Revision 5 標準に適用されるコントロールの検出結果の例を示しています。このサンプルでは、統合コントロールの検出結果は無効になっています。


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-53/v/5.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2023-02-17T14:22:46.726Z",
  "LastObservedAt": "2023-02-17T14:22:50.846Z",
  "CreatedAt": "2023-02-17T14:22:46.726Z",
  "UpdatedAt": "2023-02-17T14:22:46.726Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to fix this issue, consult the AWS Security Hub
 CSPM NIST 800-53 R5 documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-53/v/5.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-53/v/5.0.0",
    "ControlId": "CloudTrail.2",
```

```
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.9/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/
v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",

      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",

      "Partition": "aws",

      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
        "NIST.800-53.r5 AU-9",
        "NIST.800-53.r5 CA-9(1)",
        "NIST.800-53.r5 CM-3(6)",
        "NIST.800-53.r5 SC-13",
        "NIST.800-53.r5 SC-28",
        "NIST.800-53.r5 SC-28(1)",
        "NIST.800-53.r5 SC-7(10)",
        "NIST.800-53.r5 SI-7(6)"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-53/v/5.0.0"
      }
```

```
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2023-02-17T14:22:53.572Z"
}
```

NIST SP 800-171 リビジョン 2 標準のサンプル結果

次のサンプルは、NIST SP 800-171 Revision 2 標準に適用されるコントロールの検出結果の例を示しています。このサンプルでは、統合コントロールの検出結果は無効になっています。

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/v/2.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-171/v/2.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "AwsAccountName": "TestAcct",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2025-05-29T05:23:58.690Z",
  "LastObservedAt": "2025-05-30T05:50:11.898Z",
  "CreatedAt": "2025-05-29T05:24:24.772Z",
  "UpdatedAt": "2025-05-30T05:50:34.292Z",
  "Severity": {
```

```
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-171/v/2.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-171/v/2.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-0ab1c2d4",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/
nist-800-171/v/2.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-
BaselineCloudTrail",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/
v/2.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-
BaselineCloudTrail",
      "Partition": "aws",
      "Region": "us-east-1",
      "Type": "AwsCloudTrailTrail"
    }
```

```
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "RelatedRequirements": [
      "NIST.800-171.r2/3.3.8"
    ],
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-171/v/2.0.0"
      }
    ]
  },
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW",
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "Severity": {
      "Product": 40,
      "Label": "MEDIUM",
      "Normalized": 40,
      "Original": "MEDIUM"
    }
  },
  "ProcessedAt": "2025-05-30T05:50:40.297Z"
}
```

Payment Card Industry Data Security Standard v3.2.1 のサンプル結果

次のサンプルは、Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 に適用されるコントロールの検出結果の例を示しています。このサンプルでは、統合コントロールの検出結果は無効になっています。

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
```

```
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "pci-dss/v/3.2.1/PCI.CloudTrail.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.089Z",
  "LastObservedAt": "2021-09-28T16:10:06.942Z",
  "CreatedAt": "2020-08-06T02:18:23.089Z",
  "UpdatedAt": "2021-09-28T16:10:00.090Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest using AWS KMS
 CMKs",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption by checking if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/pci-dss/v/3.2.1",
    "ControlId": "PCI.CloudTrail.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/pci-dss/
v/3.2.1/PCI.CloudTrail.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
```

```
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "PCI DSS 3.4"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/pci-dss/v/3.2.1"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
    ]
  }
}
```

AWS リソースタグ付け標準のサンプル結果

次のサンプルは、 AWS リソースタグ付け標準に適用されるコントロールの検出結果の例を示しています。このサンプルでは、統合コントロールの検出結果は無効になっています。


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "security-control/EC2.44",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-02-19T21:00:32.206Z",
  "LastObservedAt": "2024-04-29T13:01:57.861Z",
  "CreatedAt": "2024-02-19T21:00:32.206Z",
  "UpdatedAt": "2024-04-29T13:01:41.242Z",
  "Severity": {
    "Label": "LOW",
    "Normalized": 1,
    "Original": "LOW"
  },
  "Title": "EC2 subnets should be tagged",
  "Description": "This control checks whether an Amazon EC2 subnet has tags with the
 specific keys defined in the parameter requiredTagKeys. The control fails if the
 subnet doesn't have any tag keys or if it doesn't have all the keys specified in
 the parameter requiredTagKeys. If the parameter requiredTagKeys isn't provided, the
 control only checks for the existence of a tag key and fails if the subnet isn't
 tagged with any key. System tags, which are automatically applied and begin with aws:,
 are ignored.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.44/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-tagged-ec2-subnet-6ceafede",
```

```
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "No tags are present.",
    "Resources:0/Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
    "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
securityhub/arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsEc2Subnet",
      "Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/subnet-1234567890abcdef0",
      "Partition": "aws",
      "Region": "eu-central-1",
      "Details": {
        "AwsEc2Subnet": {
          "AssignIpv6AddressOnCreation": false,
          "AvailabilityZone": "eu-central-1b",
          "AvailabilityZoneId": "euc1-az3",
          "AvailableIpAddressCount": 4091,
          "CidrBlock": "10.24.34.0/23",
          "DefaultForAz": true,
          "MapPublicIpOnLaunch": true,
          "OwnerId": "123456789012",
          "State": "available",
          "SubnetArn": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
          "SubnetId": "subnet-1234567890abcdef0",
          "VpcId": "vpc-021345abcdef6789"
        }
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.44",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/aws-resource-tagging-standard/v/1.0.0"
      }
    ],
    "SecurityControlParameters": [
```

```
      {
        "Name": "requiredTagKeys",
        "Value": [
          "peepoo"
        ]
      }
    ],
            },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "LOW",
      "Original": "LOW"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2024-04-29T13:02:03.259Z"
}
```

AWS Control Tower サービスマネージド標準のサンプル検出結果

次のサンプルは、 AWS Control Tower サービスマネージド標準に適用されるコントロールの検出結果の例を示しています。このサンプルでは、統合コントロールの検出結果は無効になっています。

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-
control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
```

```
  "FirstObservedAt": "2022-11-17T01:25:30.296Z",
  "LastObservedAt": "2022-11-17T01:25:45.805Z",
  "CreatedAt": "2022-11-17T01:25:30.296Z",
  "UpdatedAt": "2022-11-17T01:25:30.296Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CT.CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/service-managed-aws-control-tower/
v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0",
    "ControlId": "CT.CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/service-
managed-aws-control-tower/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-
aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
```

```
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}
```

複数の標準の統合結果の例

次のサンプルは、複数の有効な標準に適用されるコントロールの検出結果の例を示しています。このサンプルでは、統合コントロールの検出結果が有効になっています。

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "security-control/CloudTrail.2",
```

```
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-08-09T14:57:04.521Z",
  "LastObservedAt": "2025-05-30T03:30:17.407Z",
  "CreatedAt": "2024-08-09T14:57:04.521Z",
  "UpdatedAt": "2025-05-30T03:30:32.781Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-01a2b345",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-DO-
NOT-DELETE",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-DO-NOT-DELETE",
      "Partition": "aws",
      "Region": "us-east-1",
      "Details": {
        "AwsCloudTrailTrail": {
```

```
          "HasCustomEventSelectors": false,
          "IncludeGlobalServiceEvents": true,
          "LogFileValidationEnabled": true,
          "HomeRegion": "us-east-1",
          "IsMultiRegionTrail": true,
          "S3BucketName": "cloudtrail-awslogs-do-not-delete",
          "IsOrganizationTrail": false,
          "Name": "TestTrail-DO-NOT-DELETE"
        }
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.2.0/2.7",
      "CIS AWS Foundations Benchmark v1.4.0/3.7",
      "CIS AWS Foundations Benchmark v3.0.0/3.5",
      "NIST.800-171.r2/3.3.8",
      "PCI DSS v3.2.1/3.4",
      "PCI DSS v4.0.1/10.3.2"
    ],
    "AssociatedStandards": [
      { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
      { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
      { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
      { "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"},
      { "StandardsId": "standards/nist-800-171/v/2.0.0"},
      { "StandardsId": "standards/pci-dss/v/3.2.1"},
      { "StandardsId": "standards/pci-dss/v/4.0.1"}
    ]
  },
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW",
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "Severity": {
      "Normalized": 40,
```

```
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    }
  },
  "ProcessedAt": "2025-05-30T03:31:00.831Z"
}
```

Security Hub CSPM の統合について

AWS Security Hub CSPM は、サポートされている複数の AWS のサービス サードパーティーのセキュリティソリューションから AWS Partner Network セキュリティ検出結果を取り込むことができます。これらの統合により、 AWS 環境全体のセキュリティとコンプライアンスを包括的に把握できます。Security Hub CSPM は、統合ソリューションから検出結果を取り込み、 AWS Security Finding 形式 (ASFF) に変換します。

> **Important**
>
> サポートされる製品統合 AWS とサードパーティー製品統合の場合、Security Hub CSPM は、 で Security Hub CSPM を有効にした後にのみ生成された結果を受信して統合します AWS アカウント。このサービスは、Security Hub CSPM を有効にする前に生成されたセキュリティ検出結果を遡及的に受信して統合しません。

Security Hub CSPM コンソールの統合ページでは、利用可能な AWS およびサードパーティーの製品統合にアクセスできます。Security Hub CSPM API には、統合を管理するためのオペレーションもあります。

統合はすべてで使用できるとは限りません AWS リージョン。Security Hub CSPM コンソールで現在サインインしているリージョンで統合がサポートされていない場合、コンソールの統合ページには表示されません。中国リージョンで利用可能な統合のリストについては AWS GovCloud (US) Regions、「」を参照してください[リージョン別の統合の可用性](#)。

AWS のサービス および組み込みのサードパーティー統合に加えて、カスタムセキュリティ製品を Security Hub CSPM と統合できます。その後、Security Hub CSPM API を使用して、これらの製品の検出結果を Security Hub CSPM に送信できます。API を使用して、Security Hub CSPM がカスタムセキュリティ製品から受け取った既存の検出結果を更新することもできます。

トピック

- Security Hub CSPM 統合のリストの確認
- Security Hub CSPM 統合からの検出結果フローの有効化
- Security Hub CSPM 統合からの検出結果フローの無効化
- Security Hub CSPM 統合からの検出結果の表示
- AWS のサービス Security Hub CSPM との統合
- Security Hub CSPM とのサードパーティー製品統合
- Security Hub CSPM とカスタム製品の統合

Security Hub CSPM 統合のリストの確認

任意の方法を選択し、手順に従って AWS Security Hub CSPM の統合のリストまたは特定の統合の詳細を確認します。

Security Hub CSPM console

統合オプションと詳細を確認するには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. Security Hub の CSPM ナビゲーションペインで、統合を選択します。

統合ページで、他の との統合 AWS のサービス が最初にリストされ、次にサードパーティー製品との統合がリストされます。

統合ごとに、[統合] ページに以下の情報が表示されます。

- 会社名
- 製品名
- 統合の説明
- 統合が適用されるカテゴリ
- 統合を有効にする方法
- 統合の現在のステータス

以下のフィールドにテキストを入力してリストをフィルタリングできます。

- 会社名
- 製品名
- 統合の説明
- カテゴリ

Security Hub CSPM API

統合オプションと詳細を確認するには (API)

統合のリストを取得するには、 DescribeProducts オペレーションを使用します。を使用している場合は AWS CLI、 describe-products コマンドを実行します。

特定の製品統合の詳細を取得するには、 `ProductArn`パラメータを使用して統合の Amazon リソースネーム (ARN) を指定します。

たとえば、次の AWS CLI コマンドは、Security Hub CSPM と 3CORESec の統合に関する詳細を取得します。

```
$ aws securityhub describe-products --product-arn "arn:aws:securityhub:us-east-1::product/3coresec/3coresec"
```

Security Hub CSPM 統合からの検出結果フローの有効化

AWS Security Hub CSPM コンソールの統合ページで、各統合を有効にするために必要な手順を確認できます。

他の との統合のほとんどで AWS のサービス、統合を有効にするために必要なステップは、他のサービスを有効にすることです。統合情報には、他のサービスのホームページへのリンクが含まれています。他のサービスを有効にすると、Security Hub CSPM がサービスから結果を受信できるようにするリソースレベルのアクセス許可が自動的に作成され、適用されます。

サードパーティー製品統合の場合、 から統合を購入し AWS Marketplace、統合を設定する必要があります。統合情報には、これらのタスクを完了するためのリンクが含まれます。

複数のバージョンの製品が利用可能な場合は AWS Marketplace、サブスクライブするバージョンを選択し、「サブスクライブを続ける」を選択します。例えば、一部の製品は標準バージョンと AWS GovCloud (US) バージョンを提供しています。

製品の統合を有効にすると、リソースポリシーがその製品サブスクリプションに自動的に添付されます。このリソースポリシーは、Security Hub CSPM がその製品から検出結果を受信するために必要なアクセス許可を定義します。

統合を有効にするための事前ステップを完了したら、その統合からの検出結果の流れを無効にして再度有効にできます。[Integrations] (統合) ページで、結果を送信する統合の場合、[Status] (ステータス) 情報には、結果を現在受信しているかどうかが示されます。

Security Hub CSPM console

統合先からの結果のフローを有効にするには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. Security Hub CSPM ナビゲーションペインで、統合を選択します。
3. 検出結果を送信する統合の場合、ステータス情報は、Security Hub CSPM がその統合からの検出結果を現在受け入れているかどうかを示します。
4. [Accept findings (検出結果を受け入れる)] を選択します。

Security Hub CSPM API

EnableImportFindingsForProduct 操作を使用します。を使用している場合は AWS CLI、enable-import-findings-for-product コマンドを実行します。Security Hub を有効にして、統合先から結果を受信するには、製品 ARN が必要です。利用可能な統合先の ARN を取得するには、DescribeProducts オペレーションを使用します。を使用している場合は AWS CLI、 を実行しますdescribe-products。

たとえば、次の AWS CLI コマンドを使用すると、Security Hub CSPM は CrowdStrike Falcon 統合から検出結果を受信できます。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub enable-import-findings-for product --product-arn
 "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

Security Hub CSPM 統合からの検出結果フローの無効化

任意の方法を選択し、手順に従って AWS Security Hub CSPM 統合からの検出結果のフローを無効にします。

Security Hub CSPM console

統合先からの検出結果のフローを無効にするには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. Security Hub の CSPM ナビゲーションペインで、統合を選択します。
3. 結果を送信する統合の場合、ステータス情報は、Security Hub CSPM がその統合からの検出結果を現在受け入れているかどうかを示します。
4. [検出結果の受け入れを停止] を選択します。

Security Hub CSPM API

DisableImportFindingsForProduct 操作を使用します。を使用している場合は AWS CLI、 disable-import-findings-for-product コマンドを実行します。統合による検出結果のフローを無効にするには、有効になっている統合のサブスクリプションの ARN が必要です。サブスクリプションの ARN を取得するには、ListEnabledProductsForImport オペレーションを使用します。を使用している場合は AWS CLI、 を実行しますlist-enabled-products-for-import。

たとえば、次の AWS CLI コマンドは、CrowdStrike Falcon 統合から Security Hub CSPM への検出結果のフローを無効にします。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub disable-import-findings-for-product --product-subscription-arn
 "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/
crowdstrike-falcon"
```

Security Hub CSPM 統合からの検出結果の表示

AWS Security Hub CSPM 統合から結果の受け入れを開始すると、Security Hub CSPM コンソールの統合ページに、統合のステータスが結果の受け入れとして表示されます。統合の結果のリストを確認するには、「検出結果を表示」を選択します。

結果リストには、ワークフローステータスが `NEW` または `NOTIFIED` である、選択した統合先のアクティブな結果が表示されます。

クロスリージョン集約を有効にすると、集約リージョンでは、リストに、集約リージョンと、統合が有効にされているリンクされたリージョンの結果が含まれます。Security Hub では、クロスリージョン集約の設定に基づき統合が自動的に有効になることはありません。

他のリージョンでは、統合先の結果リストには、現在のリージョンの結果のみが含まれます。

クロスリージョン集約の設定方法については、the section called “リージョン間のデータの集約” を参照してください。

結果リストから、以下のアクションを実行できます。

- リストのフィルターとグループ化を変更する
- 個々の結果の詳細を表示する
- 結果のワークフローステータスを更新する
- カスタムアクションに結果を送信する

AWS のサービス Security Hub CSPM との統合

AWS Security Hub CSPM は、他のいくつかの との統合をサポートしています AWS のサービス。これらの統合は、 AWS 環境全体のセキュリティとコンプライアンスを包括的に把握するのに役立ちます。

以下に特に明記されていない限り、Security Hub CSPM および他のサービスを有効にすると、Security Hub CSPM に結果を送信する AWS のサービス 統合が自動的にアクティブ化されます。Security Hub CSPM の検出結果を受け取る統合では、アクティベーションに追加のステップが必要になる場合があります。詳細については、各統合に関する情報を確認してください。

一部の統合は、すべてで利用できるわけではありません AWS リージョン。Security Hub CSPM コンソールでは、統合が現在のリージョンでサポートされていない場合、統合は統合ページに表示されません。中国リージョンで利用可能な統合のリストについては AWS GovCloud (US) Regions、「」を参照してくださいリージョン別の統合の可用性。

Security Hub CSPM と AWS のサービス統合の概要

次の表は、Security Hub CSPM に検出結果を送信するサービス、または Security Hub CSPM から検出結果を受信する AWS サービスの概要を示しています。

統合 AWS サービス	[Direction] (方向)
AWS Config	結果の送信
AWS Firewall Manager	結果の送信
Amazon GuardDuty	結果の送信
AWS Health	結果の送信
AWS Identity and Access Management Access Analyzer	結果の送信
Amazon Inspector	結果の送信
AWS IoT Device Defender	結果の送信
Amazon Macie	結果の送信
Amazon Route 53 Resolver DNS ファイアウォール	結果の送信
AWS Systems Manager Patch Manager	結果の送信
AWS Audit Manager	結果の受信
Amazon Q Developer in chat applications	結果の受信
Amazon Detective	結果の受信
Amazon Security Lake	結果の受信
AWS Systems Manager Explorer および OpsCenter	結果の受信と更新
AWS Trusted Advisor	結果の受信

AWS Security Hub CSPM に検出結果を送信する サービス

以下は と AWS のサービス 統合され、Security Hub CSPM に結果を送信できます。Security Hub CSPM は、結果を AWS Security Finding 形式に変換します。

AWS Config（検出結果を送信します）

AWS Config は、 AWS リソースの設定を評価、監査、評価できるサービスです。 は AWS 、リソース設定 AWS Config を継続的にモニタリングおよび記録し、記録された設定を目的の設定と照らし合わせて評価を自動化できます。

との統合を使用すると AWS Config、 AWS Config マネージドルール評価とカスタムルール評価の結果を Security Hub CSPM の結果として確認できます。これらの検出結果は、他の Security Hub CSPM の検出結果と一緒に表示でき、セキュリティ体制の包括的な概要を提供します。

AWS Config は Amazon EventBridge を使用して、Security Hub CSPM に AWS Config ルール評価を送信します。Security Hub CSPM は、ルール評価を AWS Security Finding 形式に従う結果に変換します。次に、Security Hub CSPM は、Amazon リソースネーム (ARN)、リソースタグ、作成日など、影響を受けるリソースに関する詳細情報を取得することで、ベストエフォートベースで検出結果を強化します。

この統合に関する詳細は、以下のセクションを参照してください。

が Security Hub CSPM に検出結果 AWS Config を送信する方法

Security Hub CSPM のすべての検出結果は、ASFF の標準 JSON 形式を使用します。ASFF には、検出結果のオリジン、影響を受けるリソース、および検出結果の現在のステータスに関する詳細が含まれます。 AWS Config は、マネージドルールとカスタムルールの評価を EventBridge 経由で Security Hub CSPM に送信します。Security Hub CSPM は、ルール評価を ASFF に従う結果に変換し、ベストエフォートベースで結果を強化します。

が Security Hub CSPM AWS Config に送信する検出結果のタイプ

統合がアクティブ化されると、 はすべての AWS Config マネージドルールとカスタムルールの評価を Security Hub CSPM AWS Config に送信します。Security Hub CSPM が有効になった後に実行された評価のみが送信されます。例えば、 AWS Config ルール評価で 5 つの失敗したリソースが明らかになったとします。その後 Security Hub CSPM を有効にし、ルールが 6 番目に失敗したリソースを明らかにした場合、 AWS Config は 6 番目のリソース評価のみを Security Hub CSPM に送信します。

Security Hub CSPM コントロールでチェックを実行するために使用されるルールなど、サービスにリンクされた AWS Config ルールの評価は除外されます。

Security Hub CSPM に AWS Config 結果を送信する

統合がアクティブ化されると、Security Hub CSPM は検出結果の受信に必要なアクセス許可を自動的に割り当てます AWS Config。Security Hub CSPM はservice-to-serviceレベルのアクセス許可を使用します。 AWS Config EventBridge

結果が送信されるまでのレイテンシー

が新しい検出結果 AWS Config を作成すると、通常 5 分以内に Security Hub CSPM で検出結果を表示できます。

Security Hub CSPM が利用できない場合の再試行

AWS Config は、EventBridge を通じてベストエフォートベースで Security Hub CSPM に結果を送信します。イベントが Security Hub CSPM に正常に配信されない場合、EventBridge は最大 24 時間または 185 回のいずれか早い方まで配信を再試行します。

Security Hub CSPM での既存の AWS Config 検出結果の更新

AWS Config は、Security Hub CSPM に検出結果を送信すると、同じ検出結果の更新を Security Hub CSPM に送信して、検出結果アクティビティの追加の観察結果を反映することができます。更新は `ComplianceChangeNotification` イベントについてのみ送信されます。コンプライアンスの変更が発生しない場合、更新は Security Hub CSPM に送信されません。Security Hub CSPM は、最新の更新から 90 日後、または更新が発生しない場合は作成から 90 日後に検出結果を削除します。

Security Hub CSPM は、関連付けられたリソースを削除 AWS Config しても、 から送信された検出結果をアーカイブしません。

AWS Config 結果が存在するリージョン

AWS Config 検出結果はリージョンベースで発生します。 は検出結果が発生したのと同じリージョンの Security Hub CSPM に検出結果 AWS Config を送信します。

Security Hub CSPM で AWS Config の検出結果の表示

AWS Config 検出結果を表示するには、Security Hub CSPM ナビゲーションペインから検出結果を選択します。検出結果をフィルタリングして AWS Config 検出結果のみを表示するには、検索バーのドロップダウンで製品名を選択します。[Config] (設定) をクリックし、[Apply] (適用) を選択します。

Security Hub CSPM で AWS Config の検出結果名の解釈

Security Hub CSPM は、 AWS Config ルール評価を ルール評価に従う結果に変換しますAWS Security Finding 形式 (ASFF)。 AWS Config ルール評価では、ASFF とは異なるイベントパターンが使用されます。次の表は、 AWS Config Security Hub CSPM に表示されるルール評価フィールドと ASFF の対応するフィールドをマッピングしています。

Config ルール評価の検索タイプ	ASFF 結果タイプ	ハードコードされた値
detail.awsAccountId	AwsAccountId	
detail.newEvaluationResult.resultRecordedTime	CreatedAt	
detail.newEvaluationResult.resultRecordedTime	UpdatedAt	
	ProductArn	"arn:<partition>:securityhub:<region>::product/aws/config"
	ProductName	"Config"
	CompanyName	"AWS"
	リージョン	"eu-central-1"
configRuleArn	GeneratorId, ProductFields	
detail.ConfigRuleARN/finding/hash	ID	
detail.configRuleName	Title, ProductFields	
detail.configRuleName	説明	「この結果は、構成ルール `${detail.ConfigRuleName}` のリソースコンプライアンスの変更に対して作成されます。」

Config ルール評価の検索タイプ	ASFF 結果タイプ	ハードコードされた値
設定項目「ARN」または Security Hub CSPM コンピューティング ARN	Resources[i].id	
detail.resourceType	Resources[i].Type	"AwsS3Bucket"
	Resources[i].Partition	"aws"
	Resources[i].Region	"eu-central-1"
構成項目「構成」	Resources[i].Details	
	SchemaVersion	「2018-10-08」
	Severity.Label	以下の「重要度ラベルの解釈」を参照してください。
	Types	["Software and Configuration Checks"]
detail.newEvaluationResult.complianceType	Compliance.Status	「FAILED」、「NOT_AVAILABLE」、「PASSED」、または「WARNING」
	Workflow.Status	AWS Config 結果が Compliance.Status が「PASSED」で生成された場合、または Compliance.Status が「FAILED」から「PASSED」に変わった場合、「解決済み」。それ以外の場合、Workflow.Status は「NEW」になります。この値は BatchUpdateFindings API オペレーションを使用して変更できます。

重要度ラベルの解釈

AWS Config ルール評価のすべての結果の ASFF のデフォルトの重要度ラベルは MEDIUM です。結果の重要度ラベルは、BatchUpdateFindings API オペレーションで更新できます。

からの一般的な検出結果 AWS Config

Security Hub CSPM は、 AWS Config ルール評価を ASFF に従う検出結果に変換します。ASFF AWS Config の からの一般的な検出結果の例を次に示します。

> **Note**
>
> 説明が 1,024 文字を超える場合、1,024 文字に切り捨てられ、最後に「（切り捨て）」と表示されます。

```
{
 "SchemaVersion": "2018-10-08",
 "Id": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/45g070df80cb50b68fa6a43594kc6fda1e517932",
 "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/config",
 "ProductName": "Config",
 "CompanyName": "AWS",
 "Region": "eu-central-1",
 "GeneratorId": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-
mburzq",
 "AwsAccountId": "123456789012",
 "Types": [
  "Software and Configuration Checks"
 ],
 "CreatedAt": "2022-04-15T05:00:37.181Z",
 "UpdatedAt": "2022-04-19T21:20:15.056Z",
 "Severity": {
  "Label": "MEDIUM",
  "Normalized": 40
 },
 "Title": "s3-bucket-level-public-access-prohibited-config-integration-demo",
 "Description": "This finding is created for a resource compliance change for config
 rule: s3-bucket-level-public-access-prohibited-config-integration-demo",
 "ProductFields": {
  "aws/securityhub/ProductName": "Config",
  "aws/securityhub/CompanyName": "AWS",
```

```
  "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
config/arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/46f070df80cd50b68fa6a43594dc5fda1e517902",
  "aws/config/ConfigRuleArn": "arn:aws:config:eu-central-1:123456789012:config-rule/
config-rule-mburzq",
  "aws/config/ConfigRuleName": "s3-bucket-level-public-access-prohibited-config-
integration-demo",
  "aws/config/ConfigComplianceType": "NON_COMPLIANT"
 },
 "Resources": [{
  "Type": "AwsS3Bucket",
  "Id": "arn:aws:s3:::amzn-s3-demo-bucket",
  "Partition": "aws",
  "Region": "eu-central-1",
  "Details": {
   "AwsS3Bucket": {
    "OwnerId": "4edbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
    "CreatedAt": "2022-04-15T04:32:53.000Z"
   }
  }
 }],
 "Compliance": {
  "Status": "FAILED"
 },
 "WorkflowState": "NEW",
 "Workflow": {
  "Status": "NEW"
 },
 "RecordState": "ACTIVE",
 "FindingProviderFields": {
  "Severity": {
   "Label": "MEDIUM"
  },
  "Types": [
   "Software and Configuration Checks"
  ]
 }
}
```


統合の有効化と構成

Security Hub CSPM を有効にすると、この統合は自動的にアクティブ化されます。 AWS Config はすぐに Security Hub CSPM に結果の送信を開始します。

Security Hub CSPM への検出結果の発行の停止

Security Hub CSPM への検出結果の送信を停止するには、Security Hub CSPM コンソールまたは Security Hub CSPM API を使用できます。

検出結果のフローを停止する手順については、「Security Hub CSPM 統合からの検出結果フローの有効化」を参照してください。

AWS Firewall Manager（検出結果を送信します）

Firewall Manager は、リソースのウェブアプリケーションファイアウォール (WAF) ポリシーまたはウェブアクセスコントロールリスト (ウェブ ACL) ルールが準拠していない場合、結果を Security Hub CSPM に送信します。Firewall Manager は、 AWS Shield Advanced がリソースを保護していない場合、または攻撃が特定された場合にも検出結果を送信します。

Security Hub CSPM を有効にすると、この統合は自動的にアクティブ化されます。Firewall Manager は、すぐに Security Hub CSPM への検出結果の送信を開始します。

統合の詳細については、Security Hub CSPM コンソールの「統合」ページを参照してください。

Firewall Manager の詳細については、「AWS WAF 開発者ガイド」を参照してください。

Amazon GuardDuty (結果の送信)

GuardDuty は、生成したすべての検出結果タイプを Security Hub CSPM に送信します。一部の検出結果タイプには、前提条件、有効化要件、またはリージョンの制限があります。詳細については、「Amazon GuardDuty ユーザーガイド」の「GuardDuty の検出結果タイプ」を参照してください。
Amazon GuardDuty

GuardDuty の新しい検出結果は、5 分以内に Security Hub CSPM に送信されます。結果の更新は、GuardDuty 設定内の Amazon EventBridge の [Updated findings] (更新された調査結果) 設定に基づいて送信されます。

GuardDuty 設定ページを使用して GuardDuty サンプル検出結果を生成すると、Security Hub CSPM はサンプル検出結果を受け取り、検出結果タイプのプレフィックスを省略`[Sample]`します。たとえば、GuardDuty のサンプル検出結果タイプ`[SAMPLE] Recon:IAMUser/ResourcePermissions`は Security Hub CSPM `Recon:IAMUser/ResourcePermissions`の として表示されます。

Security Hub CSPM を有効にすると、この統合は自動的にアクティブ化されます。GuardDuty はすぐに Security Hub CSPM に結果を送信し始めます。

GuardDuty 統合の詳細については、「Amazon GuardDuty ユーザーガイド」のAWS 「Security Hub CSPM との統合」を参照してください。 Amazon GuardDuty

AWS Health（検出結果を送信します）

AWS Health は、リソースのパフォーマンスと AWS のサービス および の可用性を継続的に可視化します AWS アカウント。 AWS Health イベントを使用することで、サービスおよびリソースの変更が、 AWSで実行されるアプリケーションにどのような影響を及ぼすか確認することができます。

との統合 AWS Health では、 は使用されませんBatchImportFindings。代わりに、 service-to-serviceイベントメッセージング AWS Health を使用して、結果を Security Hub CSPM に送信します。

統合の詳細については、以下のセクションを参照してください。

が Security Hub CSPM に検出結果 AWS Health を送信する方法

Security Hub CSPM では、セキュリティの問題は検出結果として追跡されます。一部の検出結果は、他の AWS サービスまたはサードパーティーパートナーによって検出された問題から発生します。Security Hub CSPM には、セキュリティの問題を検出し、検出結果を生成するために使用される一連のルールもあります。

Security Hub CSPM には、これらのすべてのソースからの結果を管理するためのツールが用意されています。結果の一覧を表示およびフィルタリングして、結果の詳細を表示できます。「Security Hub CSPM での検出結果の詳細と履歴の確認」を参照してください。結果の調査状況を追跡することもできます。「Security Hub CSPM での検出結果のワークフローステータスの設定」を参照してください。

Security Hub CSPM のすべての検出結果は、 と呼ばれる標準の JSON 形式を使用しますAWS Security Finding 形式 (ASFF)。ASFF には、問題のソース、影響を受けるリソース、および結果の現在の状態に関する詳細が含まれます。

AWS Health は、Security Hub CSPM に結果を送信する AWS サービスの 1 つです。

が Security Hub CSPM AWS Health に送信する検出結果のタイプ

統合を有効にすると、 はリストされている 1 つ以上の仕様を満たす検出結果を Security Hub CSPM AWS Health に送信します。Security Hub CSPM は、 に検出結果を取り込みますAWS Security Finding 形式 (ASFF)。

- AWS のサービスの以下の値のいずれかを含む結果：
  - `RISK`

- ABUSE
- ACM
- CLOUDHSM
- CLOUDTRAIL
- CONFIG
- CONTROLTOWER
- DETECTIVE
- EVENTS
- GUARDDUTY
- IAM
- INSPECTOR
- KMS
- MACIE
- SES
- SECURITYHUB
- SHIELD
- SSO
- COGNITO
- IOTDEVICEDEFENDER
- NETWORKFIREWALL
- ROUTE53
- WAF
- FIREWALLMANAGER
- SECRETSMANAGER
- BACKUP
- AUDITMANAGER
- ARTIFACT
- CLOUDENDURE
- CODEGURU

- ORGANIZATIONS

- DIRECTORYSERVICE
- RESOURCEMANAGER
- CLOUDWATCH
- DRS
- INSPECTOR2
- RESILIENCEHUB
- certificate AWS Health typeCode フィールドに security、、abuseまたは という単語を含む結果
- AWS Health サービスが riskまたは である検出結果 abuse

Security Hub CSPM に AWS Health 結果を送信する

から検出結果を受け入れることを選択すると AWS Health、Security Hub CSPM は検出結果の受信に必要なアクセス許可を自動的に割り当てます AWS Health。Security Hub CSPM はservice-to-service レベルのアクセス許可を使用して、この統合を有効にし、ユーザーに代わって Amazon EventBridge AWS Health を介して から検出結果をインポートする安全かつ簡単な方法を提供します。Accept Findings を選択すると、Security Hub に結果を使用するアクセス許可が付与されます AWS Health。

結果が送信されるまでのレイテンシー

が新しい検出結果 AWS Health を作成すると、通常 5 分以内に Security Hub CSPM に送信されます。

Security Hub CSPM が利用できない場合の再試行

AWS Health はEventBridge を通じてベストエフォートベースで検出結果を Security Hub CSPM に送信します。イベントが Security Hub CSPM に正常に配信されない場合、EventBridge はイベントの送信を 24 時間再試行します。

Security Hub CSPM での既存の検出結果の更新

AWS Health は、Security Hub CSPM に検出結果を送信すると、同じ検出結果に更新を送信して、検出結果アクティビティの追加の観察結果を Security Hub CSPM にリフレクションできます。

結果が存在するリージョン

グローバルイベントの場合、 は、us-east-1 (AWS パーティション) 、cn-northwest-1 (中国パーティション) 、gov-us-west-1 (GovCloud パーティション) の Security Hub CSPM に結果 AWS Health を

送信します。 は、イベントが発生するのと同じリージョンの Security Hub CSPM にリージョン固有のイベント AWS Health を送信します。

Security Hub CSPM で AWS Health の検出結果の表示

Security Hub CSPM で検出 AWS Health 結果を表示するには、ナビゲーションパネルから検出結果を選択します。検出結果をフィルタリングして AWS Health 検出結果のみを表示するには、製品名フィールドからヘルスを選択します。

Security Hub CSPM で AWS Health の検出結果名の解釈

AWS Health は、 を使用して検出結果を Security Hub CSPM に送信しますAWS Security Finding 形式 (ASFF)。 AWS Health 検出では、Security Hub CSPM ASFF 形式とは異なるイベントパターンが使用されます。次の表は、Security Hub CSPM に表示される ASFF に対応するすべての AWS Health 検出結果フィールドの詳細を示しています。

Health 結果タイプ	ASFF 結果タイプ	ハードコードされた値
アカウント	AwsAccountId	
detail.StartTime	CreatedAt	
detail.eventDescription.latestDescription	説明	
detail.eventTypeCode	GeneratorId	
detail.eventArn (including account) + hash of detail.startTime	ID	
「arn: aws: securityhub:<region>:: product/aws/health」	ProductArn	
アカウントまたは resourceId	Resources[i].id	
	Resources[i].Type	「その他」
	SchemaVersion	「2018-10-08」

Health 結果タイプ	ASFF 結果タイプ	ハードコードされた値
	Severity.Label	以下の「重要度ラベルの解釈」を参照してください。
AWS Health 「-」 detail.eventTypeCode	タイトル	
-	Types	["Software and Configuration Checks"]
event.time	UpdatedAt	
Health コンソール上のイベントの URL	SourceUrl	

重要度ラベルの解釈

ASFF 結果の重要度ラベルは、次のロジックを使用して決定されます。

- 次の場合、重要度は [CRITICAL]:
  - AWS Health の結果の `service` フィールドの値が `Risk`
  - AWS Health の結果の `typeCode` フィールドの値が `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`
  - AWS Health の結果の `typeCode` フィールドの値が `AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK`
  - AWS Health の結果の `typeCode` フィールドの値が `AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES`

  次の場合、重要度は [HIGH]:
  - AWS Health の結果の `service` フィールドの値が `Abuse`
  - AWS Health 結果の `typeCode` フィールドの値に `SECURITY_NOTIFICATION` が含まれている
  - `typeCode` 結果の AWS Health フィールドの値に `ABUSE_DETECTION` が含まれている

  次の場合、重要度は [MEDIUM]:
  - 結果の `service` フィールドが次のいずれかである。`ACM`、`ARTIFACT`、`AUDITMANAGER`、`BACKUP`、`CLOUDENDURE`、`CLOUDHSM`、`CLOUDTRAIL`、`CLOU`

- AWS Health 結果の [typeCode] フィールドに値 `CERTIFICATE` が含まれている
- AWS Health 結果の [typeCode] フィールドに値 `END_OF_SUPPORT` が含まれている

からの一般的な検出結果 AWS Health

AWS Health は、 を使用して Security Hub CSPM に結果を送信します[AWS Security Finding 形式 (ASFF)](#)。以下は、 からの一般的な検出結果の例です AWS Health。

> **Note**
>
> 説明が 1,024 文字を超えると 1,024 文字まで切り捨てられ、末尾に (truncated) (切り捨て) と表示されます。

```
{
            "SchemaVersion": "2018-10-08",
            "Id": "arn:aws:health:us-east-1:123456789012:event/SES/
AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-
b533-78e29f49de96/101F7FBAEFC663977DA09CFF56A29236602834D2D361E6A8CA5140BFB3A69B30",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/health",
            "GeneratorId": "AWS_SES_CMF_PENDING_TO_SUCCESS",
            "AwsAccountId": "123456789012",
            "Types": [
                "Software and Configuration Checks"
            ],
            "CreatedAt": "2022-01-07T16:34:04.000Z",
            "UpdatedAt": "2022-01-07T19:17:43.000Z",
            "Severity": {
                "Label": "MEDIUM",
                "Normalized": 40
            },
            "Title": "AWS Health - AWS_SES_CMF_PENDING_TO_SUCCESS",
            "Description": "Congratulations! Amazon SES has successfully detected the
 MX record required to use 4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com as a custom MAIL FROM domain for verified identity cmf.pinpoint.sysmon-
iad.adzel.com in AWS Region US East (N. Virginia).\\n\\nYou can now use this MAIL
 FROM domain with cmf.pinpoint.sysmon-iad.adzel.com and any other verified identity
 that is configured to use it. For information about how to configure a verified
 identity to use a custom MAIL FROM domain, see http://docs.aws.amazon.com/ses/latest/
```

```
DeveloperGuide/mail-from-set.html .\\n\\nPlease note that this email only applies to
 AWS Region US East (N. Virginia).",
            "SourceUrl": "https://phd.aws.amazon.com/phd/home#/event-log?
eventID=arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
            "ProductFields": {
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
aws/health/arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
                "aws/securityhub/ProductName": "Health",
                "aws/securityhub/CompanyName": "AWS"
            },
            "Resources": [
                {
                    "Type": "Other",
                    "Id": "4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com"
                }
            ],
            "WorkflowState": "NEW",
            "Workflow": {
                "Status": "NEW"
            },
            "RecordState": "ACTIVE",
            "FindingProviderFields": {
                "Severity": {
                    "Label": "MEDIUM"
                },
                "Types": [
                    "Software and Configuration Checks"
                ]
            }
        }
    ]
}
```

統合の有効化と構成

Security Hub CSPM を有効にすると、この統合は自動的にアクティブ化されます。 は AWS Health すぐに Security Hub CSPM に結果を送信し始めます。

Security Hub CSPM への検出結果の発行の停止

Security Hub CSPM への検出結果の送信を停止するには、Security Hub CSPM コンソールまたは Security Hub CSPM API を使用できます。

検出結果のフローを停止する手順については、「Security Hub CSPM 統合からの検出結果フローの有効化」を参照してください。

AWS Identity and Access Management Access Analyzer（検出結果を送信します）

IAM Access Analyzer では、すべての検出結果が Security Hub CSPM に送信されます。

IAM Access Analyzer は、論理ベースの推論を使用して、アカウントでサポートされるリソースに適用されたリソースベースのポリシーを分析します。IAM Access Analyzer は、外部プリンシパルがアカウント内のリソースにアクセスすることを許可するポリシーステートメントを検出すると、検出結果を生成します。

IAM Access Analyzer では、組織に適用されるアナライザーの検出結果を確認できるのは管理者アカウントだけです。組織アナライザーの場合、`AwsAccountId` ASFF フィールドには管理者アカウント ID が反映されます。`ProductFields` 下の `ResourceOwnerAccount`フィールドには、検出結果が発見されたアカウントが表示されます。アカウントごとにアナライザーを個別に有効にすると、Security Hub CSPM は複数の検出結果を生成します。1 つは管理者アカウント ID を識別し、もう 1 つはリソースアカウント ID を識別します。

詳細については、IAM ユーザーガイドのAWS 「Security Hub CSPM との統合」を参照してください。

Amazon Inspector (結果の送信)

Amazon Inspector は、 AWS のワークロードにおける脆弱性を継続的にスキャンする脆弱性管理サービスです。Amazon Inspector は、Amazon Elastic Container Registry に存在する EC2 インスタンスとコンテナイメージを自動的に検出してスキャンします。このスキャンでは、ソフトウェアの脆弱性と意図しないネットワークへのエクスポージャーがないかチェックします。

Security Hub CSPM を有効にすると、この統合は自動的にアクティブ化されます。Amazon Inspector は、生成したすべての検出結果を Security Hub CSPM にすぐに送信し始めます。

統合の詳細については、Amazon Inspector ユーザーガイド」のAWS 「Security Hub CSPM との統合」を参照してください。

Security Hub CSPM は、Amazon Inspector Classic から検出結果を受信することもできます。Amazon Inspector Classic は、サポートされているすべてのルールパッケージの評価実行を通じて生成された結果を Security Hub CSPM に送信します。

統合の詳細については、Amazon Inspector Classic ユーザーガイド」のAWS 「Security Hub CSPM との統合」を参照してください。

Amazon Inspector と Amazon Inspector Classic の結果では、同じ製品の ARN が使用されます。Amazon Inspector の調査結果には、`ProductFields` に次のエントリがあります。

```
"aws/inspector/ProductVersion": "2",
```

> **Note**
>
> Amazon Inspector Code Security によって生成されたセキュリティ検出結果は、この統合では使用できません。ただし、これらの特定の検出結果には、Amazon Inspector コンソールおよび Amazon Inspector API からアクセスできます。

AWS IoT Device Defender（検出結果を送信します）

AWS IoT Device Defender は、IoT デバイスの設定を監査し、接続されたデバイスをモニタリングして異常な動作を検出し、セキュリティリスクを軽減するのに役立つセキュリティサービスです。

AWS IoT Device Defender と Security Hub CSPM の両方を有効にしたら、Security Hub CSPM コンソールの統合ページにアクセスし、監査、検出、またはその両方の結果を受け入れるを選択します。AWS IoT Device Defender 監査と検出は、すべての結果を Security Hub CSPM に送信し始めます。

AWS IoT Device Defender 監査は、特定の監査チェックタイプと監査タスクの一般情報を含むチェック概要を Security Hub CSPM に送信します。 AWS IoT Device Defender Detect は、機械学習 (ML)、統計、静的動作の違反検出結果を Security Hub CSPM に送信します。監査は、検出結果の更新も Security Hub CSPM に送信します。

この統合の詳細については、「 AWS IoT デベロッパーガイド」のAWS 「Security Hub CSPM との統合」を参照してください。

Amazon Macie (結果の送信)

Amazon Macie は、機械学習とパターンマッチングを使用して機密データを検出し、データセキュリティリスクを可視化し、それらのリスクに対する自動保護を可能にするデータセキュリティサービス

です。Macie の検出結果は、Amazon S3 データ資産に潜在的なポリシー違反または機密データが存在することを示している可能性があります。

Security Hub CSPM を有効にすると、Macie は Security Hub CSPM へのポリシー検出結果の送信を自動的に開始します。機密データの検出結果を Security Hub CSPM に送信するように統合を設定できます。

Security Hub CSPM では、ポリシーまたは機密データの検出結果タイプが ASFF と互換性のある値に変更されます。例えば、Macie `Policy:IAMUser/S3BucketPublic`の検出結果タイプは Security Hub CSPM `Effects/Data Exposure/Policy:IAMUser-S3BucketPublic`で として表示されます。

Macie は、生成されたサンプル検出結果を Security Hub CSPM にも送信します。結果のサンプルでは、影響を受けるリソースの名前は `macie-sample-finding-bucket` であり、`Sample` フィールドの値は `true` です。

詳細については、Amazon Macie Macie ユーザーガイド」の「Security Hub を使用した Macie の検出結果の評価」を参照してください。

Amazon Route 53 Resolver DNS ファイアウォール (検出結果を送信)

Amazon Route 53 Resolver DNS Firewall を使用すると、仮想プライベートクラウド (VPC) のアウトバウンド DNS トラフィックをフィルタリングおよび規制できます。これを行うには、DNS Firewall ルールグループにフィルタリングルールの再利用可能なコレクションを作成し、ルールグループを VPC に関連付けてから、DNS Firewall のログとメトリクスでアクティビティをモニタリングします。アクティビティに基づいて、DNS Firewall の動作を調整できます。DNS Firewall は Route 53 Resolver の機能です。

Route 53 Resolver DNS Firewall は、いくつかのタイプの検出結果を Security Hub CSPM に送信できます。

- が管理するドメインリスト AWS である AWS Managed Domain Lists に関連付けられたドメインについて、 でブロックまたはアラートが発生したクエリに関連する結果。
- 定義したカスタムドメインリストに関連付けられたドメインに対してブロックまたはアラートが発生したクエリに関連する結果。
- DNS Firewall Advanced によってブロックまたはアラートされたクエリに関連する検出結果。DNS Firewall Advanced は、ドメイン生成アルゴリズム (DGAs) や DNS トンネリングなどの高度な DNS 脅威に関連するクエリを検出できる Route 53 Resolver 機能です。

Security Hub CSPM と Route 53 Resolver DNS Firewall を有効にすると、DNS Firewall は AWS Managed Domain Lists と DNS Firewall Advanced の検出結果を Security Hub CSPM に自動的に送信し始めます。カスタムドメインリストの検出結果を Security Hub CSPM に送信するには、Security Hub CSPM で統合を手動で有効にします。

Security Hub CSPM では、Route 53 Resolver DNS Firewall のすべての検出結果のタイプは ですTTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation。

詳細については、「Amazon Route 53 デベロッパーガイド」の「Route 53 Resolver DNS Firewall から Security Hub への検出結果の送信」を参照してください。

AWS Systems Manager Patch Manager (結果を送信)

AWS Systems Manager Patch Manager は、お客様のフリート内のインスタンスがパッチコンプライアンス標準に準拠していない場合、結果を Security Hub CSPM に送信します。

Patch Manager は、セキュリティ関連のアップデートと他のタイプのアップデートの両方でマネージドインスタンスにパッチを適用するプロセスを自動化します。

Security Hub CSPM を有効にすると、この統合は自動的にアクティブ化されます。Systems Manager Patch Manager は、すぐに Security Hub CSPM に結果を送信し始めます。

Patch Manager の使用の詳細については、「AWS Systems Manager ユーザーガイド」の「AWS Systems Manager Patch Manager」を参照してください。

AWS Security Hub CSPM から検出結果を受け取る サービス

以下の AWS サービスは Security Hub CSPM と統合されており、Security Hub CSPM から検出結果を受け取ります。特に明記されている場合、統合されたサービスは結果を更新する場合もあります。この場合、統合サービスで行った更新の検出結果は Security Hub CSPM にも反映されます。

AWS Audit Manager （検出結果を受信 ）

AWS Audit Manager は Security Hub CSPM から検出結果を受け取ります。これらの結果は、Audit Manager ユーザーが監査の準備をするうえで役立ちます。

Audit Manager の詳細については、AWS Audit Manager ユーザーガイドを参照してください。AWS でサポートされている Security Hub CSPM チェック AWS Audit Managerには、Security Hub CSPM が検出結果を Audit Manager に送信するコントロールが一覧表示されます。

チャットアプリケーションの Amazon Q Developer (検出結果を受信)

チャットアプリケーションの Amazon Q Developer は、Slack チャネルと Amazon Chime チャットルームの AWS リソースをモニタリングして操作するのに役立つインタラクティブなエージェントです。

チャットアプリケーションの Amazon Q Developer は、Security Hub CSPM から検出結果を受け取ります。

Security Hub CSPM とチャットアプリケーションの統合における Amazon Q Developer の詳細については、「Amazon Q Developer in chat applications Administrator Guide」の「Security Hub CSPM integration overview」を参照してください。

Amazon Detective (結果の受信)

Detective は AWS リソースからログデータを自動的に収集し、機械学習、統計分析、グラフ理論を使用して、より迅速かつ効率的なセキュリティ調査を視覚化して実行できるようにします。

Security Hub CSPM と Detective の統合により、Security Hub CSPM の Amazon GuardDuty の検出結果から Detective にピボットできます。その後、Detective のツールと視覚化を使用して調査することができます。統合では、Security Hub CSPM または Detective で追加の設定は必要ありません。

他の から受け取った検出結果の場合 AWS のサービス、Security Hub CSPM コンソールの検出結果の詳細パネルには、Detective サブセクションの調査が含まれます。そのサブセクションには Detective へのリンクが含まれており、調査結果によって特定されたセキュリティ問題をさらに調査できます。Security Hub CSPM の検出結果に基づいて Detective で動作グラフを構築して、より効果的な調査を実行することもできます。詳細については、「Amazon Detective 管理ガイド」の「AWS セキュリティ結果」を参照してください。

クロスリージョン集約を有効にし、集約リージョンから方向を転換した場合、検出元のリージョンで Detective が開きます。

リンクが機能しない場合のトラブルシューティングのアドバイスについては、「ピボットのトラブルシューティング」を参照してください。

Amazon Security Lake (結果の受信)

Security Lake は、完全マネージド型のセキュリティデータレイクサービスです。Security Lake を使用すると、クラウド、オンプレミス、カスタムソースのセキュリティデータを、アカウントに保存されているデータレイクに自動的に一元化できます。サブスクライバーは、Security Lake のデータを調査や分析のユースケースに使用できます。

この統合をアクティブ化するには、両方のサービスを有効にし、Security Lake コンソール、Security Lake API、または で Security Hub CSPM をソースとして追加する必要があります AWS CLI。これらのステップを完了すると、Security Hub CSPM はすべての検出結果を Security Lake に送信し始めます。

Security Lake は、Security Hub CSPM の検出結果を自動的に正規化し、Open Cybersecurity Schema Framework (OCSF) と呼ばれる標準化されたオープンソーススキーマに変換します。Security Lake では、1 人以上のサブスクライバーを追加して Security Hub CSPM の検出結果を消費できます。

Security Hub CSPM をソースとして追加する手順やサブスクライバーを作成する手順など、この統合の詳細については、「Amazon Security Lake ユーザーガイド」のAWS 「Security Hub CSPM との統合」を参照してください。

AWS Systems Manager Explorer と OpsCenter (結果の受信と更新)

AWS Systems Manager Explorer と OpsCenter は Security Hub CSPM から検出結果を受け取り、それらの検出結果を Security Hub CSPM で更新します。

Explorer は、カスタマイズ可能なダッシュボードを提供し、ユーザーの運用の健全性と AWS 環境のパフォーマンスに関する主要なインサイトと分析を提供します。

OpsCenterでは、運用作業項目が一元的に表示され、調査と解決が可能です。

Explorer と OpsCenter の詳細については、「AWS Systems Manager ユーザーガイド」の「オペレーション管理」を参照してください。

AWS Trusted Advisor （ 検出結果を受信 ）

Trusted Advisor は、数十万人の AWS お客様にサービスを提供することから学んだベストプラクティスを活用しています。 はお客様の AWS 環境 Trusted Advisor を検査し、コスト削減、システムの可用性とパフォーマンスの向上、セキュリティギャップの解消に役立つ機会があれば、レコメンデーションを行います。

Trusted Advisor と Security Hub CSPM の両方を有効にすると、統合は自動的に更新されます。

Security Hub CSPM は、 AWS 基本的なセキュリティのベストプラクティスチェックの結果を に送信します Trusted Advisor。

Security Hub CSPM との統合の詳細については Trusted Advisor、AWS 「 サポートユーザーガイド」の「 での AWS Security Hub CSPM コントロールの表示 AWS Trusted Advisor」を参照してください。

Security Hub CSPM とのサードパーティー製品統合

AWS Security Hub CSPM は、複数のサードパーティーパートナー製品と統合されています。統合では、次の 1 つ以上のアクションを実行できます。

- 生成した検出結果を Security Hub CSPM に送信する
- Security Hub CSPM から検出結果を受信する
- Security Hub CSPM で検出結果を更新する

Security Hub CSPM に結果を送信する統合には、Amazon リソースネーム (ARN) があります。

統合はすべてで使用できるとは限りません AWS リージョン。Security Hub CSPM コンソールで現在サインインしているリージョンで統合がサポートされていない場合、コンソールの統合ページには表示されません。中国リージョンおよび で利用可能な統合のリストについては AWS GovCloud (US) Regions、「」を参照してくださいリージョン別の統合の可用性。

セキュリティソリューションがあり、Security Hub CSPM パートナーになることに関心がある場合は、`<securityhub-partners@amazon.com>` に E メールを送信してください。詳細については、「 パートナー統合ガイド」を参照してください。

Security Hub CSPM とのサードパーティー統合の概要

次の表は、Security Hub CSPM に検出結果を送信したり、Security Hub CSPM から検出結果を受信したりできるサードパーティー統合の概要を示しています。

Integration	[Direction] (方向)	ARN (該当する場合)
3CORESec – 3CORESec NTA	結果の送信	`arn:aws:securityhub: <REGION>::product/3coresec/3coresec`
Alert Logic – SIEMless Threat Management	結果の送信	`arn:aws:securityhub: <REGION>:733251395267:product/alertlogic/althreatmanagement`
Aqua Security – Aqua Cloud Native Security Platform	結果の送信	`arn:aws:securityhub: <REGION>::product`

Integration	[Direction] (方向)	ARN (該当する場合)
		/aquasecurity/aquasecurity
Aqua Security – Kube-bench	結果の送信	arn:aws:securityhub: <REGION>::product/aqua-security/kube-bench
Armor – Armor Anywhere	結果の送信	arn:aws:securityhub: <REGION>:679703615338:product/armordefense/armoranywhere
AttackIQ – AttackIQ	結果の送信	arn:aws:securityhub: <REGION>::product/attackiq/attackiq-platform
Barracuda Networks – Cloud Security Guardian	結果の送信	arn:aws:securityhub: <REGION>:151784055945:product/barracuda/cloudsecurityguardian
BigID – BigID Enterprise	結果の送信	arn:aws:securityhub: <REGION>::product/bigid/bigid-enterprise
Blue Hexagon – Blue Hexagon forAWS	結果の送信	arn:aws:securityhub: <REGION>::product/blue-hexagon/blue-hexagon-for-aws

Integration	[Direction] (方向)	ARN (該当する場合)
Check Point – CloudGuard IaaS	結果の送信	arn:aws:securityhub: <REGION>:758245563457:product/checkpoint/cloudguard-iaas
Check Point – CloudGuard Posture Management	結果の送信	arn:aws:securityhub: <REGION>:634729597623:product/checkpoint/dome9-arc
Claroty – xDome	結果の送信	arn:aws:securityhub: <REGION>::product/claroty/xdome
Cloud Storage Security – Antivirus for Amazon S3	結果の送信	arn:aws:securityhub: <REGION>::product/cloud-storage-security/antivirus-for-amazon-s3
Contrast Security	結果の送信	arn:aws:securityhub: <REGION>::product/contrast-security/security-assess
CrowdStrike – CrowdStrike Falcon	結果の送信	arn:aws:securityhub: <REGION>:517716713836:product/crowdstrike/crowdstrike-falcon
CyberArk – Privileged Threat Analytics	結果の送信	arn:aws:securityhub: <REGION>:749430749651:product/cyberark/cyberark-pta

Integration	[Direction] (方向)	ARN (該当する場合)
Data Theorem – Data Theorem	結果の送信	`arn:aws:securityhub: <REGION>::product/data-theorem/api-cloud-web-secure`
Drata	結果の送信	`arn:aws:securityhub: <REGION>::product/drata/drata-integration`
Forcepoint – Forcepoint CASB	結果の送信	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-casb`
Forcepoint – Forcepoint Cloud Security Gateway	結果の送信	`arn:aws:securityhub: <REGION>::product/forcepoint/forcepoint-cloud-security-gateway`
Forcepoint – Forcepoint DLP	結果の送信	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-dlp`
Forcepoint – Forcepoint NGFW	結果の送信	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Integration	[Direction] (方向)	ARN (該当する場合)
Fugue – Fugue	結果の送信	`arn:aws:securityhub: <REGION>::product/fugue/fugue`
Guardicore – Centra 4.0	結果の送信	`arn:aws:securityhub: <REGION>::product/guardicore/guardicore`
HackerOne – Vulnerability Intelligence	結果の送信	`arn:aws:securityhub: <REGION>::product/hackerone/vulnerability-intelligence`
JFrog – Xray	結果の送信	`arn:aws:securityhub: <REGION>::product/jfrog/jfrog-xray`
Juniper Networks – vSRX Next Generation Firewall	結果の送信	`arn:aws:securityhub: <REGION>::product/juniper-networks/vsrx-next-generation-firewall`
k9 Security – Access Analyzer	結果の送信	`arn:aws:securityhub: <REGION>::product/k9-security/access-analyzer`
Lacework – Lacework	結果の送信	`arn:aws:securityhub: <REGION>::product/lacework/lacework`

Integration	[Direction] (方向)	ARN (該当する場合)
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	結果の送信	`arn:aws:securityhub: <REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`
NETSCOUT – NETSCOUT Cyber Investigator	結果の送信	`arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator`
Orca Cloud Security Platform	結果の送信	`arn:aws:securityhub: <REGION>::product/orca-security/orca-security`
Palo Alto Networks – Prisma Cloud Compute	結果の送信	`arn:aws:securityhub: <REGION>:496947949261:product/twistlock/twistlock-enterprise`
Palo Alto Networks – Prisma Cloud Enterprise	結果の送信	`arn:aws:securityhub: <REGION>:188619942792:product/paloaltonetworks/redlock`
Plerion – Cloud Security Platform	結果の送信	`arn:aws:securityhub: <REGION>::product/plerion/cloud-security-platform`
Prowler – Prowler	結果の送信	`arn:aws:securityhub: <REGION>::product/prowler/prowler`

Integration	[Direction] (方向)	ARN (該当する場合)
Qualys – Vulnerability Management	結果の送信	`arn:aws:securityhub: <REGION>:805950163170:product/qualys/qualys-vm`
Rapid7 – InsightVM	結果の送信	`arn:aws:securityhub: <REGION>:336818582268:product/rapid7/insightvm`
SecureCloudDB – SecureCloudDB	結果の送信	`arn:aws:securityhub: <REGION>::product/securecloudb/secureclouddb`
SentinelOne – SentinelOne	結果の送信	`arn:aws:securityhub: <REGION>::product/sentinelone/endpoint-protection`
Snyk	結果の送信	`arn:aws:securityhub: <region>::product/snyk/snyk`
Sonrai Security – Sonrai Dig	結果の送信	`arn:aws:securityhub: <REGION>::product/sonrai-security/sonrai-dig`
Sophos – Server Protection	結果の送信	`arn:aws:securityhub: <REGION>:062897671886:product/sophos/sophos-server-protection`

Integration	[Direction] (方向)	ARN (該当する場合)
StackRox – StackRox Kubernetes Security	結果の送信	arn:aws:securityhub: <REGION>::product/stackrox/kubernetes-security
Sumo Logic – Machine Data Analytics	結果の送信	arn:aws:securityhub: <REGION>:956882708938:product/sumologicinc/sumologic-mda
Symantec – Cloud Workload Protection	結果の送信	arn:aws:securityhub: <REGION>:754237914691:product/symantec-corp/symantec-cwp
Tenable – Tenable.io	結果の送信	arn:aws:securityhub: <REGION>:422820575223:product/tenable/tenable-io
Trend Micro – Cloud One	結果の送信	arn:aws:securityhub: <REGION>::product/trend-micro/cloud-one
Vectra – Cognito Detect	結果の送信	arn:aws:securityhub: <REGION>:978576646331:product/vectra-ai/cognito-detect
Wiz	結果の送信	arn:aws:securityhub: <REGION>::product/wiz-security/wiz-security

Integration	[Direction] (方向)	ARN (該当する場合)
Atlassian - Jira Service Management	結果の受信と更新	該当しない
Atlassian - Jira Service Management Cloud	結果の受信と更新	該当しない
Atlassian – Opsgenie	結果の受信	該当しない
Dynatrace	結果の受信	該当しない
Fortinet – FortiCNP	結果の受信	該当しない
IBM – QRadar	結果の受信	該当しない
Logz.io Cloud SIEM	結果の受信	該当しない
MetricStream	結果の受信	該当しない
MicroFocus – MicroFocus Arcsight	結果の受信	該当しない
New Relic Vulnerability Management	結果の受信	該当しない
PagerDuty – PagerDuty	結果の受信	該当しない
Palo Alto Networks – Cortex XSOAR	結果の受信	該当しない
Palo Alto Networks – VM-Series	結果の受信	該当しない
Rackspace Technology – Cloud Native Security	結果の受信	該当しない
Rapid7 – InsightConnect	結果の受信	該当しない
RSA – RSA Archer	結果の受信	該当しない

Integration	[Direction] (方向)	ARN (該当する場合)
ServiceNow – ITSM	結果の受信と更新	該当しない
Slack – Slack	結果の受信	該当しない
Splunk – Splunk Enterprise	結果の受信	該当しない
Splunk – Splunk Phantom	結果の受信	該当しない
ThreatModeler	結果の受信	該当しない
Trellix – Trellix Helix	結果の受信	該当しない
Caveonix – Caveonix Cloud	結果の送受信	`arn:aws:securityhub: <REGION>::product/caveonix/caveonix-cloud`
Cloud Custodian – Cloud Custodian	結果の送受信	`arn:aws:securityhub: <REGION>::product/cloud-custodian/cloud-custodian`
DisruptOps, Inc. – DisruptOPS	結果の送受信	`arn:aws:securityhub: <REGION>::product/disruptops-inc/disruptops`
Kion	結果の送受信	`arn:aws:securityhub: <REGION>::product/cloudtamerio/cloudtamerio`
Turbot – Turbot	結果の送受信	`arn:aws:securityhub: <REGION>:453761072151:product/turbot/turbot`

Security Hub CSPM に結果を送信するサードパーティーの統合

次のサードパーティーパートナー製品統合は、Security Hub CSPM に結果を送信できます。Security Hub CSPM は、検出結果を AWS Security Finding 形式に変換します。

3CORESec – 3CORESec NTA

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/3coresec/3coresec`

3CORESec は、オンプレミスと AWS システムの両方にマネージド検出サービスを提供します。Security Hub CSPM との統合により、マルウェア、特権エスカレーション、水平移動、不適切なネットワークセグメンテーションなどの脅威を可視化できます。

製品リンク

パートナードキュメント

Alert Logic – SIEMless Threat Management

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

脆弱性とアセットの可視性、脅威の検出とインシデント管理、割り当てられた SOC アナリストオプションなど AWS WAF、適切なレベルのカバレッジを取得します。

製品リンク

パートナードキュメント

Aqua Security – Aqua Cloud Native Security Platform

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP) は、CI/CD パイプラインからランタイム運用環境まで、コンテナベースのアプリケーションおよびサーバーレスアプリケーションの完全なライフサイクルセキュリティを提供します。

製品リンク

パートナードキュメント

Aqua Security – Kube-bench

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-bench は、Center for Internet Security (CIS) Kubernetes Benchmark を環境に対して実行するオープンソースツールです。

製品リンク

パートナードキュメント

Armor – Armor Anywhere

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywhere は、 のマネージドセキュリティとコンプライアンスを提供します AWS。

製品リンク

パートナードキュメント

AttackIQ – AttackIQ

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platform は、MITRE ATT&CK Framework と連携して現実的な敵対的動作をエミュレートし、全体的なセキュリティ体制の検証と改善を支援します。

製品リンク

パートナードキュメント

Barracuda Networks – Cloud Security Guardian

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentry は、パブリッククラウドでアプリケーションを構築し、ワークロードをパブリッククラウドに移行するだけでなく、組織の安全性を維持するのに役立ちます。

AWS Marketplace リンク

製品リンク

BigID – BigID Enterprise

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

BigID Enterprise Privacy Management Platform は、企業がすべてのシステムで機密データ (PII) を管理および保護するのに役立ちます。

製品リンク

パートナードキュメント

Blue Hexagon – Blue Hexagon用 AWS

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagon は、リアルタイム脅威検出プラットフォームです。深層学習の原則を使用して、マルウェアやネットワークの異常を含む既知の脅威、および未知の脅威を検出します。

AWS Marketplace リンク

パートナードキュメント

Check Point – CloudGuard IaaS

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuard は、包括的な脅威防止セキュリティを に簡単に拡張 AWS し、クラウド内のアセットを保護します。

製品リンク

パートナードキュメント

Check Point – CloudGuard Posture Management

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

検証可能なクラウドネットワークセキュリティ、高度な IAM 保護、および包括的なコンプライアンスとガバナンスを提供する SaaS プラットフォームです。

製品リンク

パートナードキュメント

Claroty – xDome

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDome は、産業 (OT)、医療 (IoMT)、エンタープライズ (IoT) 環境内の拡張型モノのインターネット (XIoT) 全体で組織によるサイバーフィジカルシステムの保護を支援します。

製品リンク

パートナードキュメント

Cloud Storage Security – Antivirus for Amazon S3

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Security は、Amazon S3 オブジェクト向けのクラウドネイティブなマルウェア対策およびウイルス対策スキャンを提供します。

Antivirus for Amazon S3 は、Amazon S3 内のオブジェクトとファイルのマルウェアや脅威に対するスキャンを、リアルタイムおよびスケジュールされたタイミングで実行します。問題のあるファイルや感染したファイルに可視性を提供し、修復します。

製品リンク

パートナードキュメント

Contrast Security – Contrast Assess

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assess は、ウェブアプリケーション、APIs、マイクロサービスでリアルタイムの脆弱性検出を提供する IAST ツールです。 は Security Hub CSPM とContrast Assess統合されているため、すべてのワークロードを一元的に可視化して対応できます。

製品リンク

パートナードキュメント

CrowdStrike – CrowdStrike Falcon

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

CrowdStrike Falcon は、単一の軽量センサーで次世代のウイルス対策、エンドポイントの検出と対応、および 24 時間 365 日管理されるクラウド経由のハンティングを統合します。

AWS Marketplace リンク

パートナードキュメント

CyberArk – Privileged Threat Analytics

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat Analytics は、特権アカウントでのリスクの高いアクティビティや動作を収集、検出、アラートし、進行中の攻撃を阻止するよう対応します。

製品リンク

パートナードキュメント

Data Theorem – Data Theorem

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data Theorem は、ウェブアプリケーション、API、クラウドリソースを継続的にスキャンしてセキュリティ上の欠陥やデータプライバシーのギャップを特定し、AppSec データの侵害を防止します。

製品リンク

パートナードキュメント

Drata

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drata はコンプライアンス自動化プラットフォームです。SOC2 や ISO、GDPR など、さまざまなフレームワークのコンプライアンスの達成および維持に貢献します。Drata と Security Hub CSPM の統合により、セキュリティ検出結果を 1 つの場所に一元化できます。

AWS Marketplace リンク

パートナードキュメント

Forcepoint – Forcepoint CASB

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASB では、クラウドアプリケーションの使用を検出し、リスクを分析して、SaaS およびカスタムアプリケーションの適切なコントロールを実施できます。

製品リンク

パートナードキュメント

Forcepoint – Forcepoint Cloud Security Gateway

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Forcepoint Cloud Security Gateway は、ユーザーがどこにいるか、データがどこにあるかに関わらず、可視性、制御、脅威保護を提供する統合型クラウドセキュリティサービスです。

製品リンク

パートナードキュメント

Forcepoint – Forcepoint DLP

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLP は、人間が主体のリスクに対処し、ユーザーが作業するすべての場所とデータが存在するすべての場所を可視化して制御します。

製品リンク

パートナードキュメント

Forcepoint – Forcepoint NGFW

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFW では、ネットワークを管理し、脅威に対応するために必要なスケーラビリティ、保護、インサイトを使用して、 AWS 環境をエンタープライズネットワークに接続できます。

製品リンク

パートナードキュメント

Fugue – Fugue

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugue は、同一のポリシーを使用して、Infrastructure as Code とクラウドランタイム環境の継続的な検証を自動化する、エージェントレスかつスケーラブルなクラウドネイティブのプラットフォームです。

製品リンク

パートナードキュメント

Guardicore – Centra 4.0

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centra は、最新のデータセンターやクラウドにおけるワークロードのフローの可視化、マイクロセグメンテーション、および違反検出を行います。

製品リンク

パートナードキュメント

HackerOne – Vulnerability Intelligence

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

HackerOne プラットフォームは、世界中のハッカーのコミュニティと提携して、最も関連性の高いセキュリティ問題を発見します。Vulnerability Intelligence を使用することで、組織では自動スキャ

ンを上回る対策を講じることができます。HackerOne のホワイトハッカーによって検証され再現された脆弱性が共有されます。

AWS マーケットプレイスリンク

パートナードキュメント

JFrog – Xray

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xray は、セキュアなソフトウェアサプライチェーンを実行できるように、ライセンスコンプライアンスとセキュリティの脆弱性についてバイナリを継続的にスキャンするユニバーサルアプリケーションセキュリティソフトウェア構成分析 (SCA) ツールです。

AWS Marketplace リンク

パートナードキュメント

Juniper Networks – vSRX Next Generation Firewall

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks' vSRX Virtual Next Generation Firewall は、高度なセキュリティ、セキュアな SD-WAN、堅牢なネットワーク、組み込みオートメーションを備えた完全なクラウドベースの仮想ファイアウォールを提供します。

AWS Marketplace リンク

パートナードキュメント

製品リンク

k9 Security – Access Analyzer

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Security は、 AWS Identity and Access Management アカウントで重要なアクセス変更が発生したときに通知します。を使用するとk9 Security、ユーザーと IAM ロールが重要な AWS のサービスとデータにアクセスできることを理解できます。

k9 Security は継続的デリバリー用に構築されているため、 AWS CDK と Terraform の実用的なアクセス監査とシンプルなポリシー自動化を使用して IAM を運用できます。

製品リンク

パートナードキュメント

Lacework – Lacework

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/lacework/lacework`

Lacework は、クラウド向けのデータ駆動型セキュリティプラットフォームです。Lacework Cloud Security Platform は、クラウドセキュリティを大規模に自動化し、スピードと安全性を備えたイノベーションの実現を可能にします。

製品リンク

パートナードキュメント

McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

McAfee MVISION Cloud Native Application Protection Platform (CNAPP) は、お客様の AWS 環境にクラウドのセキュリティ体制管理 (CSPM) およびクラウドワークロード保護プラットフォーム (CWPP) を提供します。

製品リンク

パートナードキュメント

NETSCOUT – NETSCOUT Cyber Investigator

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

NETSCOUT Cyber Investigator は、企業全体のネットワーク脅威、リスク調査、フォレンジック分析プラットフォームで、サイバー脅威によるビジネスへの影響を軽減します。

製品リンク

パートナードキュメント

Orca Cloud Security Platform

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/orca-security/orca-security`

は、クラウド資産全体のリスクとコンプライアンスの問題Orca Cloud Security Platformを特定、優先順位付け、修復します。Orca's エージェントレスファーストの AI 駆動型プラットフォームは、脆弱性、設定ミス、側面移動、API リスク、機密データ、異常なイベントと動作、過度に寛容なアイデンティティを検出する包括的なカバレッジを提供します。

Orca は Security Hub CSPM と統合され、Security Hub CSPM に深層クラウドセキュリティテレメトリを導入します。 はOrca、そのSideScanningテクノロジーを使用して、クラウドインフラストラクチャ、ワークロード、アプリケーション、データ、APIs、アイデンティティなどのリスクに優先順位を付けます。

製品リンク

パートナードキュメント

Palo Alto Networks – Prisma Cloud Compute

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Compute は、VM、コンテナ、およびサーバーレスプラットフォームを保護する、クラウドネイティブのサイバーセキュリティプラットフォームです。

製品リンク

パートナードキュメント

Palo Alto Networks – Prisma Cloud Enterprise

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

クラウドセキュリティ分析、高度な脅威検出、コンプライアンスモニタリングにより、 AWS デプロイを保護します。

製品リンク

パートナードキュメント

Plerion – Cloud Security Platform

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerion は、脅威・リスク主導型の独自のアプローチを採用したクラウドセキュリティプラットフォームであり、ワークロード全体にわたって予防、検出、是正措置を提供します。Plerion と Security Hub CSPM の統合により、お客様はセキュリティの検出結果を 1 か所で一元化して対応できます。

AWS Marketplace リンク

パートナードキュメント

Prowler – Prowler

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowler は、セキュリティのベストプラクティス、強化、継続的モニタリングに関連する AWS チェックを実行するオープンソースのセキュリティツールです。

製品リンク

パートナードキュメント

Qualys – Vulnerability Management

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM) は脆弱性を継続的にスキャンして識別し、アセットを保護します。

製品リンク

パートナードキュメント

Rapid7 – InsightVM

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVM は、最新の環境の脆弱性管理を提供するため、脆弱性を効率的に検出、優先順位付け、修正できます。

製品リンク

パートナードキュメント

SecureCloudDB – SecureCloudDB

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/securecloudb/securecloudb`

SecureCloudDB は、内部および外部のセキュリティ体制とアクティビティを包括的に可視化するクラウドネイティブなデータベースセキュリティツールです。セキュリティ違反にフラグを立てて、悪用可能なデータベースの脆弱性に対する修復を提供します。

製品リンク

パートナードキュメント

SentinelOne – SentinelOne

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOne は、自律型の Extended Detection and Response (XDR) プラットフォームで、エンドポイント、コンテナ、クラウドワークロード、および IoT デバイスにわたって、AI を使用した防止、検知、対応、ハンティングなどを行います。

AWS Marketplace リンク

製品リンク

Snyk

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snyk には、 AWS で実行中のワークロードのセキュリティリスクについてアプリケーションコンポーネントをスキャンするセキュリティプラットフォームが用意されています。これらのリスクは、検出結果として Security Hub CSPM に送信され、デベロッパーとセキュリティチームが残りの AWS セキュリティ検出結果とともにそれらを視覚化して優先順位を付けるのに役立ちます。

AWS Marketplace リンク

パートナードキュメント

Sonrai Security – Sonrai Dig

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Dig は、クラウドの誤った構成とポリシー違反を監視および修正することで、セキュリティとコンプライアンス体制の改善を可能にします。

製品リンク

パートナードキュメント

Sophos – Server Protection

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protection は、包括的な多層防御テクノロジーを使用して、組織の中核となる重大なアプリケーションとデータを保護します。

製品リンク

StackRox – StackRox Kubernetes Security

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRox により、ビルド、デプロイ、実行など、コンテナのライフサイクル全体にわたってコンプライアンスとセキュリティポリシーを適用することで、エンタープライズにおけるコンテナと Kubernetes のデプロイを大規模に保護できます。

製品リンク

パートナードキュメント

Sumo Logic – Machine Data Analytics

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logic は、DevSecOps チームが AWS アプリケーションを構築、実行、および保護することができる、安全なマシンデータ分析プラットフォームです。

製品リンク

パートナードキュメント

Symantec – Cloud Workload Protection

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protection は、マルウェア対策、侵入防止、およびファイルの整合性モニタリングにより、Amazon EC2 インスタンスを完全に保護します。

製品リンク

パートナードキュメント

Tenable – Tenable.io

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

脆弱性を正確に特定し、調査し、優先順位を付けます。クラウドで管理されます。

製品リンク

パートナードキュメント

Trend Micro – Cloud One

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud One は、適切なセキュリティ情報を適切なタイミングで適切な場所のチームに提供します。この統合により、Security Hub CSPM にセキュリティ検出結果がリアルタイムで送信され、Security Hub CSPM の AWS リソースとTrend Micro Cloud Oneイベントの詳細の可視性が向上します。

AWS Marketplace リンク

パートナードキュメント

Vectra – Cognito Detect

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectra は、高度な AI を適用してサイバーセキュリティを変革し、隠れたサイバー攻撃者による盗難や損害を事前に検出して対応します。

AWS Marketplace リンク

パートナードキュメント

Wiz – Wiz Security

統合タイプ: 送信

製品 ARN: `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wiz は、設定、脆弱性、ネットワーク、IAM 設定、シークレットなどを継続的に分析し AWS アカウント、実際のリスクを表す重大な問題を検出します。Wiz を Security Hub CSPM と統合して、Wiz が Security Hub CSPM コンソールから検出した問題を視覚化して対応します。

AWS Marketplace リンク

パートナードキュメント

Security Hub CSPM から検出結果を受け取るサードパーティーの統合

次のサードパーティーパートナー製品統合は、Security Hub CSPM から結果を受け取ることができます。記載されている場合、製品は検出結果を更新することもあります。この場合、パートナー製品の結果に対して行った更新は、Security Hub CSPM にも反映されます。

Atlassian - Jira Service Management

統合タイプ: 受信と更新

AWS Service Management Connector の は、Security Hub CSPM から に検出結果Jiraを送信します Jira。 Jiraの問題は、検出結果に基づいて作成されます。Jira 問題が更新されると、対応する検出結果が Security Hub CSPM で更新されます。

統合では Jira サーバーと Jira データセンターのみがサポートされています。

統合の概要と仕組みについては、AWS 「Security Hub CSPM – Bidirectional integration with Atlassian Jira Service Management」の動画をご覧ください。

製品リンク

パートナードキュメント

Atlassian - Jira Service Management Cloud

統合タイプ: 受信と更新

Jira Service Management Cloud は、Jira Service Management のクラウドコンポーネントです。

AWS Service Management Connector の は、Security Hub CSPM から に検出結果Jiraを送信します Jira。検出結果は、Jira Service Management Cloud での問題の作成をトリガーします。でこれらの問題を更新するとJira Service Management Cloud、対応する検出結果は Security Hub CSPM でも更新されます。

製品リンク

パートナードキュメント

Atlassian – Opsgenie

統合タイプ: 受信

Opsgenie は、常時稼働のサービスを運用するための最新のインシデント管理ソリューションであり、開発および運用チームがサービス中断の計画を立て、インシデント中の管理を維持できるようにします。

Security Hub CSPM との統合により、ミッションクリティカルなセキュリティ関連のインシデントが適切なチームにルーティングされ、即時に解決されます。

製品リンク

パートナードキュメント

Dynatrace

統合タイプ: 受信

Security Hub CSPM とDynatraceの統合は、ツールと環境間でセキュリティ検出結果を統合、視覚化、自動化するのに役立ちます。セキュリティ検出結果にDynatraceランタイムコンテキストを追加すると、より賢明な優先順位付けが可能になり、アラートのノイズが軽減され、DevSecOps チームは本番環境やアプリケーションに影響を与える重要な問題を効率的に解決することに集中できます。

製品リンク

パートナードキュメント

Fortinet – FortiCNP

統合タイプ: 受信

FortiCNP は、セキュリティの結果を実用的なインサイトに集約し、リスクスコアに基づいてセキュリティの洞察に優先順位を付けてアラートの疲労を軽減し、修復を加速するクラウドネイティブ保護製品です。

AWS Marketplace リンク

パートナードキュメント

IBM – QRadar

統合タイプ: 受信

IBM QRadar SIEM は、迅速かつ正確に脅威を検出し、優先順位付けし、調査、および対応する機能をセキュリティチームに提供します。

製品リンク

パートナードキュメント

Logz.io Cloud SIEM

統合タイプ: 受信

Logz.io はログとイベントデータの高度な相関関係を提供し、セキュリティチームがセキュリティの脅威をリアルタイムで検出、分析、対応できるようにする Cloud SIEM のプロバイダです。

製品リンク

パートナードキュメント

MetricStream – CyberGRC

統合タイプ: 受信

MetricStream CyberGRC は、サイバーセキュリティリスクの管理、測定、軽減に役立ちます。Security Hub CSPM の検出結果を受け取ることで、 CyberGRCはこれらのリスクをより可視化できるため、サイバーセキュリティへの投資を優先し、IT ポリシーに準拠できます。

AWS Marketplace リンク

製品リンク

MicroFocus – MicroFocus Arcsight

統合タイプ: 受信

ArcSight はリアルタイムの効果的な脅威の検出と対応を加速し、レスポンスのオートメーションとオーケストレーションにより、イベントの相関と監視対象外の分析を統合します。

製品リンク

パートナードキュメント

New Relic Vulnerability Management

統合タイプ: 受信

New Relic Vulnerability Management は Security Hub CSPM からセキュリティ検出結果を受け取るため、スタック全体のコンテキストでパフォーマンステレメトリと並行してセキュリティを一元的に把握できます。

AWS Marketplace リンク

パートナードキュメント

PagerDuty – PagerDuty

統合タイプ: 受信

PagerDuty のデジタル運用管理プラットフォームを使用すると、あらゆるシグナルが自動的に適切なインサイトとアクションに変換されることで、顧客に影響を与える問題を事前に軽減できます。

AWS ユーザーは、PagerDuty一連の AWS 統合を使用して、 AWS およびハイブリッド環境を自信を持ってスケーリングできます。

Security Hub CSPM 集約および整理されたセキュリティアラートと組み合わせると、PagerDutyチームは脅威への対応プロセスを自動化し、潜在的な問題を防ぐためにカスタムアクションをすばやくセットアップできます。

クラウド移行プロジェクトを実施している PagerDuty ユーザーは、移行のライフサイクルを通して発生する問題の影響を軽減しながら、迅速に移行することができます。

製品リンク

パートナードキュメント

Palo Alto Networks – Cortex XSOAR

統合タイプ: 受信

Cortex XSOAR は、セキュリティ製品スタック全体と統合してインシデント対応とセキュリティ運用を迅速化する、Security Orchestration, Automation, and Response (SOAR) プラットフォームです。

製品リンク

パートナードキュメント

Palo Alto Networks – VM-Series

統合タイプ: 受信

Palo Alto VM-Series Security Hub CSPM との統合は、脅威インテリジェンスを収集し、悪意のある IP アドレスアクティビティをブロックする自動セキュリティポリシー更新としてVM-Series次世代ファイアウォールに送信します。

製品リンク

パートナードキュメント

Rackspace Technology – Cloud Native Security

統合タイプ: 受信

ネイティブ AWS セキュリティ製品に加えて、Rackspace Technology は Rackspace SOC による 24 時間 365 日のモニタリング、高度な分析、脅威の軽減によるマネージドセキュリティサービスを提供します。

製品リンク

Rapid7 – InsightConnect

統合タイプ: 受信

Rapid7 InsightConnect は、セキュリティ上のオーケストレーションとオートメーションのソリューションであり、コードをほとんどまたは一切使用せずに SOC 操作を最適化することが可能です。

製品リンク

パートナードキュメント

RSA – RSA Archer

統合タイプ: 受信

RSA Archer IT およびセキュリティリスク管理では、ビジネスにとって重要な資産を特定し、セキュリティポリシーと標準を確立して伝え、攻撃を検出して対応し、セキュリティ上の欠陥を特定して修正し、明確な IT リスク管理のベストプラクティスを確立できます。

製品リンク

パートナードキュメント

ServiceNow – ITSM

統合タイプ: 受信と更新

Security Hub CSPM とServiceNowの統合により、Security Hub CSPM からのセキュリティ検出結果を 内で表示できますServiceNow ITSM。Security Hub CSPM から検出結果を受け取ったときにインシデントまたは問題を自動的に作成ServiceNowするように を設定することもできます。

これらのインシデントと問題を更新すると、Security Hub CSPM の結果が更新されます。

統合の概要と仕組みについては、AWS Security Hub CSPM - Bidirectional integration with ServiceNow ITSMの動画をご覧ください。

製品リンク

パートナードキュメント

Slack – Slack

統合タイプ: 受信

Slack は、人、データ、およびアプリケーションを 1 か所に集約するビジネステクノロジースタックのレイヤーです。人々が効果的に協力し、重要な情報を見つけ、何十万もの重要なアプリケーションやサービスにアクセスして、最善の仕事ができるようにします。

製品リンク

パートナードキュメント

Splunk – Splunk Enterprise

統合タイプ: 受信

Splunk は、Security Hub CSPM の検出結果のコンシューマーとして Amazon CloudWatch Events を使用します。データを Splunk に送信すると、高度なセキュリティ分析と SIEM を実行できます。

製品リンク

パートナードキュメント

Splunk – Splunk Phantom

統合タイプ: 受信

AWS Security Hub CSPM のSplunk Phantomアプリケーションでは、検出結果は Phantom に送信され、追加の脅威インテリジェンス情報を含む自動コンテキストエンリッチメント、または自動応答アクションを実行します。

製品リンク

パートナードキュメント

ThreatModeler

統合タイプ: 受信

ThreatModeler は、エンタープライズソフトウェアとクラウド開発のライフサイクルを保護し、スケールする自動化された脅威モデリングソリューションです。

製品リンク

パートナードキュメント

Trellix – Trellix Helix

統合タイプ: 受信

Trellix Helix は、クラウドホスト型のセキュリティ運用プラットフォームであり、組織は、アラートから修正までのあらゆるインシデントを制御できるようになります。

製品リンク

パートナードキュメント

Security Hub CSPM に検出結果を送受信するサードパーティーの統合

次のサードパーティーパートナー製品統合は、Security Hub CSPM に検出結果を送受信できます。

Caveonix – Caveonix Cloud

統合タイプ: 送信と受信

製品 ARN: `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

Caveonix AI 搭載プラットフォームは、クラウドネイティブのサービスや VM、コンテナを対象に、ハイブリッドクラウドの可視性、評価、緩和を自動化します。 AWS Security Hub CSPM と統合され、 AWS データと高度な分析をCaveonixマージして、セキュリティアラートとコンプライアンスに関するインサイトを提供します。

AWS Marketplace リンク

パートナードキュメント

Cloud Custodian – Cloud Custodian

統合タイプ: 送信と受信

製品 ARN: `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodian により、ユーザーをクラウドで適切に管理できます。シンプルな YAML DSL を使用することでルールの定義が容易で、クラウドインフラストラクチャを適切に管理でき、セキュリティとコストの最適化の両方を実現することができます。

製品リンク

パートナードキュメント

DisruptOps, Inc. – DisruptOPS

統合タイプ: 送信と受信

製品 ARN: `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

DisruptOps の Security Operations Platform は、自動化されたガードレールを使用することにより、組織がクラウド内でベストプラクティスを維持するのに役立ちます。

製品リンク

パートナードキュメント

Kion

統合タイプ: 送信と受信

製品 ARN: `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion (旧 cloudtamer.io) は、 の完全なクラウドガバナンスソリューションです AWS。 は、ステークホルダーにクラウド運用の可視性Kionを提供し、クラウドユーザーがアカウントを管理し、予算とコストを制御し、継続的なコンプライアンスを確保するのに役立ちます。

製品リンク

パートナードキュメント

Turbot – Turbot

統合タイプ: 送信と受信

製品 ARN: `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbot は、クラウドインフラストラクチャの安全性、準拠性、スケーラブル性を保証し、そのコストを最適化します。

製品リンク

パートナードキュメント

Security Hub CSPM とカスタム製品の統合

統合された AWS サービスとサードパーティー製品によって生成された検出結果に加えて、 AWS Security Hub CSPM は他のカスタムセキュリティ製品によって生成された検出結果を消費できます。

これらの検出結果は、Security Hub CSPM API の BatchImportFindingsオペレーションを使用して Security Hub CSPM に送信できます。同じオペレーションを使用して、Security Hub CSPM に既に送信したカスタム製品の検出結果を更新できます。

カスタム統合を設定するときは、Security Hub CSPM パートナー統合ガイドに記載されているガイドラインとチェックリストを使用してください。

カスタム製品統合の要件と推奨事項

`BatchImportFindings` API オペレーションを正常に呼び出す前に、Security Hub CSPM を有効にする必要があります。

また、the section called “検出結果形式: ASFF” を使用して検出結果の詳細を指定する必要があります。カスタム製品統合に関する以下の要件と推奨事項を確認してください。

製品 ARN の設定

Security Hub CSPM を有効にすると、Security Hub CSPM のデフォルトの製品 Amazon リソースネーム (ARN) が現在のアカウントで生成されます。

この製品 ARN の形式は、`arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default` です。例えば、`arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default`。

`BatchImportFindings` API オペレーションを呼び出すときに、この製品 ARN を `ProductArn` 属性の値として使用します。

会社名と製品名の設定

`BatchImportFindings` を使用して、Security Hub CSPM に結果を送信するカスタム統合の優先会社名と製品名を設定できます。

指定された名前は、それぞれ個人名とデフォルト名と呼ばれる事前設定された会社名と製品名を置き換え、Security Hub CSPM コンソールと各結果の JSON に表示されます。「検出結果プロバイダーの BatchImportFindings」を参照してください。

結果 ID の設定

`Id` 属性を使用して、独自の結果の ID を提供、管理、および増分する必要があります。

それぞれの新しい検出結果には、一意の検出結果 ID が必要です。カスタム製品が同じ検出結果 ID で複数の検出結果を送信する場合、Security Hub CSPM は最初の検出結果のみを処理します。

アカウント ID の設定

`AwsAccountId` 属性を使用して、自分のアカウント ID を指定する必要があります。

作成日と更新日の設定

`CreatedAt` および `UpdatedAt` 属性に独自のタイムスタンプを渡す必要があります。

カスタム製品からの結果の更新

カスタム製品から新しい結果を送信するだけでなく、`BatchImportFindings` API オペレーションを使用して、カスタム製品から既存の結果を更新することもできます。

既存の結果を更新するには、既存の結果 ID を (`Id` 属性を介して) 使用します。リクエストで更新された適切な情報 (変更された `UpdatedAt` タイムスタンプを含む) を使用して、完全な結果を再送信します。

カスタム統合の例

次のカスタム製品の統合例をガイドとして使用して、独自のカスタムソリューションを作成できます。

Chef InSpec スキャンから Security Hub CSPM に検出結果を送信する

Chef InSpec コンプライアンススキャンを実行し、結果を Security Hub CSPM に送信する AWS CloudFormation テンプレートを作成できます。

詳細については、「 による継続的なコンプライアンスモニタリングChef InSpec」および AWS 「Security Hub CSPM」を参照してください。

によって検出されたコンテナの脆弱性Trivyを Security Hub CSPM に送信する

を使用してコンテナAquaSecurity Trivyの脆弱性をスキャンし、それらの脆弱性の検出結果を Security Hub CSPM に送信する AWS CloudFormation テンプレートを作成できます。

詳細については、「 を使用してコンテナ脆弱性スキャン用の CI/CD パイプラインを構築する方法Trivy」およびAWS 「Security Hub CSPM」を参照してください。

Security Hub CSPM での検出結果の作成と更新

AWS Security Hub CSPM では、検出結果はセキュリティチェックまたはセキュリティ関連の検出の観測可能なレコードです。検出結果は、次のいずれかのソースから取得できます。

- Security Hub CSPM のコントロールのセキュリティチェック。

- 別の との統合 AWS のサービス。
- サードパーティー製品との統合。
- カスタム統合。

Security Hub CSPM は、すべてのソースからの結果を AWS Security Finding Format (ASFF) と呼ばれる標準の構文と形式に正規化します。個々の ASFF フィールドの説明など、この形式の詳細については、「」を参照してくださいAWS Security Finding 形式 (ASFF)。クロスリージョン集約を有効にすると、Security Hub CSPM は、すべてのリンクされたリージョンから指定した集約リージョンに、新規および更新された検出結果を自動的に集約します。詳細については、「Security Hub CSPM でのクロスリージョン集約について」を参照してください。

検出結果を作成したら、次のように更新できます。

- 検出結果プロバイダーは、Security Hub CSPM API の BatchImportFindingsオペレーションを使用して、検出結果に関する一般的な情報を更新できます。結果プロバイダーは、自身が作成した結果のみを更新できます。
- お客様は、Security Hub CSPM コンソールまたは Security Hub CSPM API の BatchUpdateFindingsオペレーションを使用して、検出結果の調査のステータスを更新できます。`BatchUpdateFindings` オペレーションは、SIEM、チケット発行、インシデント管理、SOAR、またはその他のタイプのツールが顧客に代わって使用することもできます。

検出結果のノイズを減らし、個々の検出結果の追跡と分析を合理化するために、Security Hub CSPM は最近更新されていない検出結果を自動的に削除します。Security Hub CSPM がこれを行うタイミングは、検出結果がアクティブかアーカイブかによって異なります。

- アクティブな検出結果は、レコード状態 (`RecordState`) が である検出結果ですACTIVE。Security Hub CSPM はアクティブな検出結果を 90 日間保存します。アクティブな検出結果が 90 日間更新されていない場合、有効期限が切れ、Security Hub CSPM によって完全に削除されます。
- アーカイブされた検出結果は、レコード状態 (`RecordState`) が である検出結果ですARCHIVED。Security Hub CSPM は、アーカイブされた検出結果を 30 日間保存します。アーカイブされた検出結果が 30 日間更新されていない場合、有効期限が切れ、Security Hub CSPM によって完全に削除されます。

Security Hub CSPM がコントロールのセキュリティチェックから生成する検出結果であるコントロール検出結果の場合、Security Hub CSPM は検出結果の `UpdatedAt`フィールドの値に基づいて検

出結果の有効期限が切れたかどうかを判断します。アクティブな検出結果に対してこの値が 90 日以上前である場合、Security Hub CSPM は検出結果を完全に削除します。アーカイブされた検出結果に対してこの値が 30 日以上前である場合、Security Hub CSPM は検出結果を完全に削除します。

他のすべてのタイプの検出結果について、Security Hub CSPM は、検出結果の フィールド`ProcessedAt`と `UpdatedAt`フィールドの値に基づいて、検出結果の有効期限が切れたかどうかを判断します。Security Hub CSPM は、これらのフィールドの値を比較し、どちらが最新かを判断します。アクティブな検出結果の最新の値が 90 日以上前である場合、Security Hub CSPM は検出結果を完全に削除します。アーカイブされた検出結果の最新の値が 30 日以上前である場合、Security Hub CSPM は検出結果を完全に削除します。検出結果プロバイダーは、Security Hub CSPM API の BatchImportFindingsオペレーションを使用して、1 つ以上の検出結果の `UpdatedAt`フィールドの値を変更することができます。

結果を長期間保持するには、結果を S3 バケットにエクスポートできます。これを行うには、Amazon EventBridge ルールでカスタムアクションを使用します。詳細については、「EventBridge を使用した自動応答と修復」を参照してください。

トピック

- 検出結果プロバイダーの BatchImportFindings
- お客様の BatchUpdateFindings
- Security Hub CSPM での検出結果の詳細と履歴の確認
- Security Hub CSPM での検出結果のフィルタリング
- Security Hub CSPM での検出結果のグループ化
- Security Hub CSPM での検出結果のワークフローステータスの設定
- カスタム Security Hub CSPM アクションに結果を送信する
- AWS Security Finding 形式 (ASFF)

検出結果プロバイダーの BatchImportFindings

検出結果プロバイダーは、 BatchImportFindingsオペレーションを使用して AWS Security Hub CSPM で新しい検出結果を作成できます。また、このオペレーションを使用して、作成した検出結果を更新することもできます。検出結果プロバイダーは、作成しなかった検出結果を更新できません。

顧客、SIEMs、チケット発行、SOAR、およびその他のタイプのツールは、 BatchUpdateFindingsオペレーションを使用して、検出結果プロバイダーからの検出結果の調査に関連する更新を行う必要が

あります。詳細については、「the section called “お客様の BatchUpdateFindings”」を参照してください。

Security Hub CSPM は、検出結果を作成または更新するBatchImportFindingsリクエストを受信すると、Amazon EventBridge でSecurity Hub Findings - Importedイベントを自動的に生成します。そのイベントに対して自動アクションを実行できます。詳細については、「the section called “自動応答および自動修復”」を参照してください。

BatchImportFindings を使用するための前提条件

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

- 結果に関連付けられているアカウント。関連付けられたアカウントの識別子は、検出結果の AwsAccountId 属性の値に一致している必要があります。
- 公式の Security Hub CSPM パートナー統合として許可リストに登録されているアカウント。

Security Hub CSPM は、Security Hub CSPM が有効になっているアカウントの検出結果の更新のみを受け入れることができます。検出結果プロバイダーも有効にする必要があります。Security Hub CSPM が無効になっているか、検出結果プロバイダーの統合が有効になっていない場合、検出結果はInvalidAccessエラーでFailedFindingsリストに返されます。

結果を作成するか更新するかの決定

検出結果を作成または更新するかどうかを決定するために、Security Hub CSPM は IDフィールドをチェックします。の値が既存の検出結果と一致しIDない場合、Security Hub CSPM は新しい検出結果を作成します。

が既存の検出結果IDと一致する場合、Security Hub CSPM は更新の UpdatedAtフィールドをチェックし、次のように続行します。

- 更新UpdatedAt時に既存の検出結果UpdatedAtの より前に一致または発生した場合、Security Hub CSPM は更新リクエストを無視します。
- 更新UpdatedAt時に既存の検出結果UpdatedAtの の後に が発生した場合、Security Hub CSPM は既存の検出結果を更新します。

BatchImportFindings による検出結果の更新の制限

検出結果プロバイダーは BatchImportFindings を使用して既存の検出結果の次の属性を更新することはできません。

- `Note`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Security Hub CSPM は、これらの属性の`BatchImportFindings`リクエストで提供されたコンテンツを無視します。お客様、またはお客様に代わって行動するエンティティ (チケット発行ツールなど) は、 `BatchUpdateFindings` を使用してこれらの属性を更新できます。

FindingProviderFields での結果の更新

また、検出結果プロバイダーは、 `BatchImportFindings`を使用して AWS Security Finding Format (ASFF) の次の最上位属性を更新しないでください。

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

代わりに、検出結果プロバイダーは `FindingProviderFields` オブジェクトを使用して、これらの属性の値を提供する必要があります。

例

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

```
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

BatchImportFindings リクエストの場合、Security Hub CSPM は最上位属性と の値を[FindingProviderFields](#)次のように処理します。

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

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

Security Hub CSPM は、 の 属性の値を更新しますFindingProviderFields。

これは、属性が BatchUpdateFindings によってまだ更新されていない場合にのみ、値をトップレベル属性にレプリケートします。

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

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

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

Security Hub CSPM は、属性が によってまだ更新されていない場合にのみ、最上位属性を更新しますBatchUpdateFindings。

BatchImportFindings は、**FindingProviderFields** のトップレベル属性と対応する属性の両方の値を提供します。

例えば、BatchImportFindings は Confidence と FindingProviderFields.Confidence の両方を提供します。

新しい検出結果の場合、Security Hub CSPM は の 値FindingProviderFieldsを使用して、最上位属性と対応する属性の両方を に入力しますFindingProviderFields。指定されたトップレベルの属性値は使用しません。

既存の検出結果の場合、Security Hub CSPM は両方の値を使用します。ただし、トップレベルの属性値が更新されるのは、BatchUpdateFindings により属性がまだ更新されていない場合のみです。

お客様の BatchUpdateFindings

AWS Security Hub CSPM のお客様およびお客様に代わって行動するエンティティは、BatchUpdateFindings オペレーションを使用して、検出結果プロバイダーからの Security Hub CSPM の検出結果の処理に関連する情報を更新できます。お客様は、このオペレーションを直接使用できます。SIEM、チケット発行、インシデント管理、SOAR ツールも、顧客に代わってこのオペレーションを使用できます。

`BatchUpdateFindings` オペレーションを使用して新しい検出結果を作成することはできません。ただし、これを使用して、一度に最大 100 個の既存の検出結果を更新できます。`BatchUpdateFindings` リクエストでは、更新する検出結果、検出結果に対して更新する AWS Security Finding Format (ASFF) フィールド、およびフィールドの新しい値を指定します。次に、Security Hub CSPM はリクエストで指定されたとおりに検出結果を更新します。この処理には数分かかることもあります。`BatchUpdateFindings` オペレーションを使用して検出結果を更新しても、更新は検出結果の `UpdatedAt`フィールドの既存の値には影響しません。

Security Hub CSPM は、検出結果の更新`BatchUpdateFindings`リクエストを受信すると、Amazon EventBridge でSecurity Hub Findings – Importedイベントを自動的に生成します。オプションで、このイベントを使用して、指定された検出結果に対して自動アクションを実行できます。詳細については、「the section called “自動応答および自動修復”」を参照してください。

BatchUpdateFindings の使用可能なフィールド

Security Hub CSPM 管理者アカウントにサインインしている場合は、 `BatchUpdateFindings`を使用して、管理者アカウントまたはメンバーアカウントによって生成された検出結果を更新できます。メンバーアカウントは、`BatchUpdateFindings` を使用して、自分のアカウントのみの検出結果を更新できます。

お客様は `BatchUpdateFindings` を使用して、以下のフィールドとオブジェクトを更新できます。

- `Confidence`
- `Criticality`
- `Note`
- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`

- `VerificationState`
- `Workflow`

BatchUpdateFindings へのアクセスの設定

AWS Identity and Access Management (IAM) ポリシーを設定して、 `BatchUpdateFindings` を使用して検出結果フィールドとフィールド値を更新するアクセスを制限できます。

`BatchUpdateFindings` へのアクセスを制限するステートメントで、以下の値を使用します：

- `Action` は `securityhub:BatchUpdateFindings`
- `Effect` は `Deny`。
- `Condition` では、以下に基づいて `BatchUpdateFindings` リクエストを拒否できます。
  - 結果に特定のフィールドが含まれる。
  - 結果に特定のフィールド値が含まれる。

条件キー

これらは、`BatchUpdateFindings` へのアクセスを制限するための条件キーです。

ASFF フィールド

ASFF フィールドの条件キーは以下のとおりです：

```
securityhub:ASFFSyntaxPath/<fieldName>
```

`<fieldName>` を ASFF フィールドで置き換えます。`BatchUpdateFindings` へのアクセスを設定する場合は、1 つの親レベルのフィールドではなく、IAM ポリシーに 1 つ以上の特定の ASFF フィールドを含めます。例えば、`Workflow.Status` フィールドへのアクセスを制限するには、`Workflow` 親レベルフィールドの代わりに `securityhub:ASFFSyntaxPath/Workflow.Status` をポリシーに含める必要があります。

フィールドに対するすべての更新を禁止する

ユーザーが特定のフィールドを更新できないようにするには、以下のような条件を使用します。

```
"Condition": {
                "Null": {
```

```
                    "securityhub:ASFFSyntaxPath/<fieldName>": "false"
                }
}
```

例えば、以下のステートメントは、BatchUpdateFindings を使用して検出結果の Workflow.Status フィールドを更新できないことを示しています。

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
        "Null": {
            "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
        }
    }
}
```

特定のフィールド値の許可を禁止する

ユーザーがフィールドを特定の値に設定できないようにするには、以下のような条件を使用します:

```
"Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
                }
}
```

例えば、以下のステートメントは、BatchUpdateFindings を使用して Workflow.Status に SUPPRESSED を設定できないことを示しています。

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
}
```

許可されていない値のリストを提供することもできます。

```
 "Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
 "<fieldValue2>", "<fieldValuen>" ]
               }
}
```

例えば、以下のステートメントは、`BatchUpdateFindings` を使用して `Workflow.Status` を `RESOLVED` または `SUPPRESSED` に設定できないことを示しています。

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": [
            "RESOLVED",
            "NOTIFIED"
        ]
    }
}
```

Security Hub CSPM での検出結果の詳細と履歴の確認

AWS Security Hub CSPM では、検出結果はセキュリティチェックまたはセキュリティ関連の検出の観測可能なレコードです。Security Hub CSPM は、コントロールのセキュリティチェックを完了し、統合 AWS のサービス 製品またはサードパーティー製品から検出結果を取り込むときに検出結果を生成します。各検出結果には、変更の履歴や、重要度の評価や影響を受けるリソースに関する情報など、その他の詳細が含まれます。

Security Hub CSPM コンソールで、または Security Hub CSPM API または を使用してプログラムで、個々の検出結果の履歴やその他の詳細を確認できます AWS CLI。

分析を合理化するために、特定の検出結果を選択すると、Security Hub CSPM コンソールに検出結果パネルが表示されます。パネルには、検出結果の特定の詳細を確認するためのさまざまなメニューとタブが含まれています。

アクションメニュー

このメニューから、検出結果の完全な JSON を確認したり、メモを追加したりできます。検出結果にアタッチできるメモは一度に 1 つだけです。このメニューには、検出結果のワークフローステータスを設定したり、Amazon EventBridge のカスタムアクションに検出結果を送信したりするためのオプションもあります。

調査メニュー

このメニューから、Amazon Detective で検出結果を調査できます。Detective は、検出結果から IP アドレスや AWS ユーザーなどのエンティティを抽出し、そのアクティビティを視覚化します。エンティティアクティビティを出発点として使用して、検出結果の原因と影響を調べることができます。

[Overview (概要)] タブ

このタブには、検出結果の概要が表示されます。たとえば、検出結果がいつ作成され、最後に更新されたか、そのアカウントが存在するか、検出結果のソースを判断できます。コントロールの検出結果については、このタブには、関連する AWS Config ルールの名前と、Security Hub CSPM ドキュメントの修復ガイダンスへのリンクも表示されます。

概要タブのリソーススナップショットでは、検出結果に関連するリソースの概要を確認できます。一部のリソースでは、関連する AWS のサービス コンソールで影響を受けるリソースに直接リンクする Open resource オプションが含まれます。履歴スナップショットには、履歴が追跡されている最新の日付に検出結果に加えられた最大 2 つの変更が表示されます。たとえば、昨日 1 つの変更を行い、今日別の変更を行った場合、スナップショットには今日の変更が表示されます。以前のエントリを確認するには、履歴タブに切り替えます。

コンプライアンス行が展開され、詳細が表示されます。たとえば、コントロールにパラメータが含まれている場合、コントロールのセキュリティチェックを実行するときに Security Hub CSPM が現在使用しているパラメータ値を確認できます。

[リソース] タブ

このタブには、検出結果に関連するリソースの詳細が表示されます。リソースを所有するアカウントにサインインしている場合は、該当する AWS のサービス コンソールでリソースを確認できます。リソースの所有者でない場合、このタブには所有者の AWS アカウント ID が表示されます。

詳細行には、検出結果のリソース固有の詳細が表示されます。検出結果ResourceDetailsのセクションが JSON 形式で表示されます。

タグ行には、検出結果に関連するリソースに割り当てられたタグキーと値が表示されます。AWS Resource Groups タグ付け API の GetResources オペレーションでサポートされているリソースはタグ付けできます。Security Hub CSPM は、新規または更新された検出結果を処理するときにサービスにリンクされたロールを使用してこのオペレーションを呼び出し、 AWS Security Finding Format (ASFF) `Resource.Id`フィールドにリソースの ARN が入力されている場合はリソースタグを取得します。Security Hub CSPM は無効なリソース IDs。検出結果にリソースタグを含める方法の詳細については、「[タグ]」を参照してください。

履歴タブ

このタブは、検出結果の履歴を追跡します。検出結果履歴は、アクティブな検出結果とアーカイブされた検出結果に利用できます。これは、ASFF フィールドの変更、変更の発生日時、ユーザーなど、結果に加えられた変更の不変の証跡を提供します。タブの各ページには、最大 20 個の変更が表示されます。最新の変更が最初に表示されます。

アクティブな検出結果の場合、検出結果履歴は最大 90 日間使用できます。アーカイブされた検出結果の場合、検出結果履歴は最大 30 日間使用できます。検出結果履歴には、手動で行われた変更、または Security Hub CSPM オートメーションルールによって自動的に行われた変更が含まれます。`CreatedAt` フィールドや フィールドなど、最上位のタイムスタンプ`UpdatedAt`フィールドへの変更は含まれません。

Security Hub CSPM 管理者アカウントにサインインしている場合、検出結果は管理者アカウントとすべてのメンバーアカウントの履歴になります。

[脅威] タブ

このタブには、脅威のタイプやリソースがターゲットかアクターかなど、ASFF の Action、Malware、および ProcessDetails オブジェクトのデータが含まれます。これらの詳細は、通常、Amazon GuardDuty で発生した検出結果に適用されます。

[脆弱性] タブ

このタブには、検出結果に関連するエクスプロイトや利用可能な修正があるかどうかなど、ASFF の Vulnerability オブジェクトからのデータが表示されます。これらの詳細は、通常、Amazon Inspector で発生した検出結果に適用されます。

各タブの行には、コピーまたはフィルターオプションが含まれます。たとえば、ワークフローステータスが Notified の結果のパネルを開くと、ワークフローステータス行の横にあるフィルターオプションを選択できます。この値を持つすべての検出結果を表示するを選択すると、Security Hub CSPM は検出結果テーブルをフィルタリングし、同じワークフローステータスの検出結果のみを表示します。

検出結果の詳細と履歴の確認

任意の方法を選択し、手順に従って Security Hub CSPM で検出結果の詳細を確認します。

クロスリージョン集約を有効にし、集約リージョンにサインインすると、集約リージョンとリンクされたリージョンからの検出結果が含まれます。他のリージョンでは、検出結果はそのリージョンにのみ固有です。クロスリージョン集約の詳細については、「the section called “リージョン間のデータの集約”」を参照してください。

Security Hub CSPM console

検出結果の詳細と履歴の確認

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. 結果リストを表示するには、以下のいずれかを実行します。
   - ナビゲーションペインで 調査結果を選択します。必要に応じて検索フィルターを追加して、検出結果リストを絞り込みます。
   - ナビゲーションペインで、[Insights] を選択します。インサイトを選択します。次に、結果リストでインサイト結果を選択します。
   - ナビゲーションペインで、[統合] を選択します。統合の [検出結果を表示] を選択します。
   - ナビゲーションペインで [コントロール] を選択します。
3. 検出結果を選択します。検出結果パネルには、検出結果の詳細が表示されます。
4. 検出結果パネルで、次のいずれかを実行します。
   - 検出結果の特定の詳細を確認するには、タブを選択します。
   - 検出結果に対してアクションを実行するには、アクションメニューからオプションを選択します。
   - Amazon Detective で検出結果を調査するには、調査オプションを選択します。

> **Note**
>
> と統合 AWS Organizations し、メンバーアカウントにサインインしている場合、検出結果パネルにはアカウント名が含まれます。Organizations ではなく手動で招待されたメンバーアカウントの場合、検出結果パネルにはアカウント ID のみが含まれます。

Security Hub CSPM API

Security Hub CSPM API の GetFindingsオペレーションを使用するか、 を使用している場合は AWS CLIコマンドを実行しますget-findings。Filters パラメータに 1 つ以上の値を指定して、取得する結果を絞り込むことができます。

検出結果の量が多すぎる場合は、MaxResults パラメータを使用して結果を指定された数に制限し、NextToken パラメータを使用して検出結果をページ分割できます。SortCriteria パラメータを使用して、特定のフィールドで検出結果を並べ替えます。

たとえば、次の AWS CLI コマンドは、指定されたフィルター条件に一致する検出結果を取得し、 LastObservedAtフィールドで結果を降順でソートします。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub get-findings \
--filters '{"GeneratorId":[{"Value": "aws-
foundational","Comparison":"PREFIX"}],"WorkflowStatus": [{"Value":
 "NEW","Comparison":"EQUALS"}],"Confidence": [{"Gte": 85}]}' --sort-criteria
 '{"Field": "LastObservedAt","SortOrder": "desc"}' --page-size 5 --max-items 100
```

検出結果の履歴を確認するには、GetFindingHistory オペレーションを使用します。を使用している場合は AWS CLI、 get-finding-history コマンドを実行します。ProductArn および Id フィールドを使用して、履歴を取得する検出結果を特定します。これらのフィールドの詳細については、「AwsSecurityFindingIdentifier」を参照してください。各リクエストは、1 つの結果のみの履歴を取得できます。

たとえば、次の AWS CLI コマンドは、指定された結果の履歴を取得します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub get-finding-history \
--region us-west-2 \
--finding-identifier Id="a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2:123456789012:product/123456789012/default" \
--max-results 2 \
--start-time "2021-09-30T15:53:35.573Z" \
--end-time "2021-09-31T15:53:35.573Z"
```

PowerShell

`Get-SHUBFinding` コマンドレットを使用します。必要に応じて、 `Filter`パラメータを入力して、取得する結果を絞り込みます。

たとえば、次の コマンドレットは、指定されたフィルターに一致する検出結果を取得します。

```
Get-SHUBFinding -Filter @{AwsAccountId =
 [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =
 "XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =
 "EQUALS"; Value = 'FAILED'}}
```

> **Note**
>
> `CompanyName` または で結果をフィルタリングする場合`ProductName`、Security Hub CSPM は `ProductFields` ASFF オブジェクトの一部である値を使用します。Security Hub CSPM は、最上位の フィールド`CompanyName`と `ProductName`フィールドを使用しません。

Security Hub CSPM での検出結果のフィルタリング

AWS Security Hub CSPM は、セキュリティチェックから独自の検出結果を生成し、統合製品から検出結果を受け取ります。Security Hub CSPM コンソールの検出結果、統合、インサイトページに検出結果のリストを表示できます。フィルターを追加して、リストが組織またはユースケースに関連しているように検出結果リストを絞り込むことができます。

特定のセキュリティコントロールの検出結果をフィルタリングする方法については、「」を参照してくださいthe section called “コントロール検出結果のフィルタリングとソート”。このページの情報は、結果、インサイト、統合ページに適用されます。

検出結果リストのデフォルトフィルター

デフォルトでは、Security Hub CSPM コンソールの検出結果リストは、 AWS Security Finding 形式 (ASFF) の `RecordState`および `Workflow.Status`フィールドに基づいてフィルタリングされます。これは、特定のインサイトまたは統合のフィルターに追加されます。

レコードの状態は、その検出結果がアクティブかアーカイブされているかを示します。デフォルトでは、結果リストにはアクティブな結果のみが表示されます。検出結果プロバイダーは、検出結果が

アクティブでなくなった場合や重要でなくなった場合は、その検出結果をアーカイブできます。また、Security Hub CSPM は、関連付けられたリソースが削除されると、コントロールの検出結果を自動的にアーカイブします。

ワークフローステータスは、検出結果に対する調査のステータスを示します。デフォルトでは、結果リストには、ワークフローステータスが NEW または NOTIFIED の結果のみが表示されます。検出結果のワークフローステータスを更新することができます。

フィルターを追加する手順

検出結果リストは、最大 10 個の属性でフィルタリングできます。各属性に対して、最大 20 個のフィルター値を提供できます。

検出結果リストをフィルタリングする場合、Security Hub CSPM AND は一連のフィルターにロジックを適用します。結果は、指定されたすべてのフィルターに一致する場合にのみ一致します。たとえば、GuardDuty を製品名のフィルターとして追加し、リソースタイプのフィルターAwsS3Bucketとして追加すると、Security Hub CSPM はこれらの両方の基準に一致する検出結果を表示します。

Security Hub CSPM OR は、同じ属性と異なる値を使用するフィルターにロジックを適用します。たとえば、GuardDuty と Amazon Inspector の両方を製品名のフィルター値として追加すると、Security Hub CSPM は GuardDuty または Amazon Inspector によって生成された結果を表示します。

検出結果リストにフィルターを追加するには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. 検出結果リストを表示するには、ナビゲーションペインから次のいずれかのアクションを実行します。
   - 検出結果を選択します。
   - [Insights] を選択します。インサイトを選択します。次に、結果リストでインサイト結果を選択します。
   - [統合] を選択します。統合の [検出結果を表示] を選択します。
3. フィルターの追加ボックスで、フィルタリングする 1 つ以上のファイルを選択します。

   会社名または製品名でフィルタリングする場合、コンソールは AWS Security Finding Format (ASFF) の最上位の フィールドCompanyNameと ProductNameフィールドを使用します。API は、 の下にネストされた値を使用しますProductFields。

4. フィルターの一致タイプを選択します。

   文字列フィルターでは、次のオプションから選択できます。

   - is - フィルター値と完全に一致する値を検索します。
   - starts with - フィルター値で始まる値を検索します。
   - is not - フィルター値と一致しない値を検索します。
   - does not start with - フィルター値で始まらない値を検索します。

   リソースタグフィールドでは、特定のキーまたは値に基づいてフィルタリングできます。

   数値フィルターの場合、単一の数値 ([Simple] (シンプル)) を指定するか、数値の範囲 ([Range] (範囲)) を指定するかを選択できます。

   日時フィルターの場合、現在の日時からの時間の長さ ([Rolling window] (ローリングウィンドウ)) を指定するか、特定の日付範囲 ([Fixed range] (固定範囲)) を指定するかを選択できます。

   複数のフィルターを追加した場合、以下のように相互作用します。

   - is および starts with フィルターは OR で結合されます。フィルター値のいずれかが含まれている場合に、値が一致となります。例えば、[Severity label is CRITICAL] (重要度ラベルは重大) および [Severity label is HIGH] (重要度ラベルは高)と指定している場合、結果には重要度が重大な結果と重要度の高い結果の両方が含まれます。
   - is not および does not start with フィルターは AND で結合されます。値は、これらのフィルター値を一切含まなかった場合にのみ一致となります。例えば、[Severity label is not LOW] (重要度ラベルが低ではない) および [Severity label is not MEDIUM] (重要度ラベルは中ではない) と指定した場合、結果に重要度が低または中の結果は含まれません。

   フィールドに is フィルターを適用した場合、同じフィールドに is not または does not start with フィルターを使用することはできません。

5. フィルター値を指定します。文字列フィルターの場合、フィルター値では大文字と小文字が区別されます。

6. [Apply] (適用) を選択します。

   既存のフィルターでは、フィルター一致タイプまたは値を変更できます。フィルタリングされた検出結果リストで、フィルターを選択します。フィルターの編集ボックスで、新しい一致タイプまたは値を選択し、適用を選択します。

フィルターを削除するには、[x] アイコンを選択します。リストが自動的に更新され、変更が反映されます。

Security Hub CSPM での検出結果のグループ化

選択した属性の値に基づいて、 AWS Security Hub CSPM で結果をグループ化できます。

結果をグループ化すると、結果のリストが、一致する結果内の選択した属性の値のリストに置き換えられます。値ごとに、一致する検出結果の数がリストに表示されます。

例えば、検出結果を AWS アカウント ID でグループ化すると、アカウント識別子のリストと、各アカウントの一致する検出結果の数が表示されます。

Security Hub CSPM は、選択した属性に対して最大 100 個の値を表示できます。100 個を超える値がある場合、最初の 100 個のみが表示されます。

属性値を選択すると、Security Hub CSPM はその値に一致する検出結果のリストを表示します。

検出結果リスト内の検出結果をグループ化するには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. 検出結果リストを表示するには、ナビゲーションペインから次のいずれかのアクションを実行します。
   - 結果を選択します。
   - [Insights] を選択します。インサイトを選択します。次に、結果リストでインサイト結果を選択します。
   - [統合] を選択します。統合の [検出結果を表示] を選択します。
3. グループ化ドロップダウンで、グループ化に使用する属性を選択します。

   グループ化属性を削除するには、x アイコンを選択します。グループ化属性を削除すると、リストは属性値のリストから結果のリストに変わります。

Security Hub CSPM での検出結果のワークフローステータスの設定

ワークフローステータスは、検出結果に対する調査の進行状況を追跡します。ワークフローステータスは個々の検出結果に固有であり、新しい検出結果の生成には影響しません。たとえば、検出結果

のワークフローステータスを SUPPRESSEDまたは に変更してもRESOLVED、変更によって Security Hub CSPM が同じ問題に対して新しい検出結果を生成することが妨げられることはありません。

検出結果のワークフローステータスは、次のいずれかの値になります。

新規

レビューする前の結果の初期の状態です。

統合から取り込まれた AWS のサービスなどの検出結果は AWS Config、初期ステータスNEWとして を持ちます。

また、Security Hub CSPM は、次の場合にワークフローステータスを NOTIFIED または から RESOLVED にリセットNEWします。

- RecordState が ARCHIVED から ACTIVE に変更した場合。
- Compliance.Status が PASSED から FAILED 、WARNING、または NOT_AVAILABLE に変更した場合。

これらの変更は、追加の調査が必要であることを意味します。

通知済み

セキュリティ問題についてリソース所有者に通知したことを示しています。このステータスは、自分がリソース所有者ではなく、セキュリティ問題を解決するためにリソース所有者からの介入が必要な場合に使用できます。

次のいずれかが発生すると、ワークフローステータスは NOTIFIED から NEW に自動的に変更されます。

- RecordState が ARCHIVED から ACTIVE に変更した場合。
- Compliance.Status が PASSED から FAILED 、WARNING、または NOT_AVAILABLE に変更した場合。

非推奨

結果をレビューし、アクションが必要だとは判断しなかったことを示しています。

RecordState が ARCHIVED から ACTIVE に変更されても、SUPPRESSED 結果のワークフローステータスは変わりません。

解決済み

この結果はレビューおよび修正され、現在は解決済みと見なされていることを示しています。

以下のいずれかが発生しない限り、結果は RESOLVED を維持します。

- RecordState が ARCHIVED から ACTIVE に変更した場合。
- Compliance.Status が PASSED から FAILED 、WARNING、または NOT_AVAILABLE に変更した場合。

こういったケースでは、ワークフローステータスは自動的に NEW にリセットされます。

コントロールの検出結果の場合、 Compliance.Status が の場合PASSED、Security Hub CSPM は自動的にワークフローステータスを に設定しますRESOLVED。

結果のワークフローステータスを設定する

1 つ以上の検出結果のワークフローステータスを変更するには、Security Hub CSPM コンソールまたは Security Hub CSPM API を使用できます。検出結果のワークフローステータスを変更する場合、Security Hub CSPM がリクエストを処理して検出結果を更新するまでに数分かかる場合があることに注意してください。

> **Tip**
> 自動化ルールを使用して、検出結果のワークフローステータスを自動的に変更することもできます。自動化ルールでは、指定した基準に基づいて検出結果のワークフローステータスを自動的に更新するように Security Hub CSPM を設定します。詳細については、「Security Hub CSPM のオートメーションルールについて」を参照してください。

1 つ以上の検出結果のワークフローステータスを変更するには、任意の方法を選択し、ステップに従います。

Security Hub CSPM console

検出結果のワークフローステータスを変更するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで、次のいずれかを実行して検出結果のテーブルを表示します。
   - 検出結果を選択します。

- [Insights] を選択します。次に、インサイトを選択します。インサイト結果で、結果を選択します。
- [統合] を選択します。次に、統合の セクションで、「検出結果を表示」を選択します。
- セキュリティ標準を選択します。次に、標準の セクションで、結果の表示を選択します。コントロールの表で、コントロールを選択してコントロールの結果を表示します。

3. 検出結果テーブルで、ワークフローステータスを変更する各検出結果のチェックボックスをオンにします。
4. ページの上部で、ワークフローステータスを選択し、選択した結果の新しいワークフローステータスを選択します。
5. ワークフローステータスの設定ダイアログボックスに、ワークフローステータスを変更する理由の詳細を示すメモをオプションで入力します。次に、Set status を選択します。

Security Hub CSPM API

BatchUpdateFindings オペレーションを使用します。検出結果を生成した製品の検出結果 ID と ARN の両方を提供します。これらの詳細は、GetFindings オペレーションを使用して取得できます。

AWS CLI

batch-update-findings コマンドを実行します。検出結果を生成した製品の検出結果 ID と ARN の両方を提供します。これらの詳細を取得するには、get-findings コマンドを実行します。

```
batch-update-findings --finding-identifiers
 Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

例

```
aws securityhub batch-update-findings --finding-identifiers
 Id="arn:aws:securityhub:us-west-1:123456789012:subscription/
pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --
workflow Status="RESOLVED"
```

カスタム Security Hub CSPM アクションに結果を送信する

AWS Security Hub CSPM カスタムアクションを作成して、Amazon EventBridge で Security Hub CSPM を自動化できます。カスタムアクションの場合、イベントタイプは Security Hub Findings - Custom Action になります。カスタムアクションを設定したら、そのアクションに結果を送信できます。カスタムアクションの作成に関する情報と詳細な手順については、「the section called “自動応答および自動修復”」を参照してください。

カスタムアクション (コンソール) に結果を送信するには、以下を実行します。

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. 結果リストを表示するには、以下のいずれかを実行します。
   - Security Hub CSPM ナビゲーションペインで、検出結果を選択します。
   - Security Hub の CSPM ナビゲーションペインで、インサイトを選択します。インサイトを選択します。次に、検出結果リストで、インサイトの結果を選択します。
   - Security Hub の CSPM ナビゲーションペインで、統合を選択します。統合の [検出結果を表示] を選択します。
   - Security Hub の CSPM ナビゲーションペインで、セキュリティ標準を選択します。[結果を表示する] を選択して、コントロールのリストを表示します。次に、コントロール名を選択します。
3. 結果リストで、カスタムアクションに送信する各結果のチェックボックスを選択します。

   一度に最大 20 件の結果を送信できます。
4. [Actions] (アクション) から、カスタムアクションを選択します。

AWS Security Finding 形式 (ASFF)

AWS Security Hub CSPM は、統合された およびサードパーティー製品の結果を消費 AWS のサービス および集計します。Security Hub CSPM は、AWS Security Finding Format (ASFF) と呼ばれる標準の検出結果形式を使用してこれらの検出結果を処理します。これにより、時間のかかるデータ変換作業が不要になります。

このページでは、 AWS Security Finding 形式 (ASFF) の結果の JSON の完全な概要を示します。形式は JSON スキーマから派生します。リンクされたオブジェクトの名前を選択して、そのオブジェ

クトの検出結果の例を確認します。Security Hub CSPM の検出結果と、ここに示すリソースや例を比較すると、検出結果の解釈に役立ちます。

個々の ASFF 属性の詳細については、the section called “必須の ASFF 最上位属性”「」および「」を参照してくださいthe section called “オプションの最上位 ASFF 属性”。

```
"Findings": [
    {
     "Action": {
      "ActionType": "string",
      "AwsApiCallAction": {
       "AffectedResources": {
        "string": "string"
       },
       "Api": "string",
       "CallerType": "string",
       "DomainDetails": {
        "Domain": "string"
       },
       "FirstSeen": "string",
       "LastSeen": "string",
       "RemoteIpDetails": {
        "City": {
         "CityName": "string"
        },
        "Country": {
         "CountryCode": "string",
         "CountryName": "string"
        },
        "IpAddressV4": "string",
        "Geolocation": {
         "Lat": number,
         "Lon": number
        },
        "Organization": {
         "Asn": number,
         "AsnOrg": "string",
         "Isp": "string",
         "Org": "string"
        }
       },
       "ServiceName": "string"
      },
```

```
      "DnsRequestAction": {
       "Blocked": boolean,
       "Domain": "string",
       "Protocol": "string"
      },
      "NetworkConnectionAction": {
       "Blocked": boolean,
       "ConnectionDirection": "string",
       "LocalPortDetails": {
        "Port": number,
        "PortName": "string"
       },
       "Protocol": "string",
       "RemoteIpDetails": {
        "City": {
         "CityName": "string"
        },
        "Country": {
         "CountryCode": "string",
         "CountryName": "string"
        },
        "IpAddressV4": "string",
        "Geolocation": {
         "Lat": number,
         "Lon": number
        },
        "Organization": {
         "Asn": number,
         "AsnOrg": "string",
         "Isp": "string",
         "Org": "string"
        }
       },
       "RemotePortDetails": {
        "Port": number,
        "PortName": "string"
       }
      },
      "PortProbeAction": {
       "Blocked": boolean,
       "PortProbeDetails": [{
        "LocalIpDetails": {
         "IpAddressV4": "string"
        },
```

```
        "LocalPortDetails": {
         "Port": number,
         "PortName": "string"
        },
        "RemoteIpDetails": {
         "City": {
          "CityName": "string"
         },
         "Country": {
          "CountryCode": "string",
          "CountryName": "string"
         },
         "GeoLocation": {
          "Lat": number,
          "Lon": number
         },
         "IpAddressV4": "string",
         "Organization": {
          "Asn": number,
          "AsnOrg": "string",
          "Isp": "string",
          "Org": "string"
         }
        }
       }]
      }
     },
     "AwsAccountId": "string",
     "AwsAccountName": "string",
     "CompanyName": "string",
     "Compliance": {
      "AssociatedStandards": [{
       "StandardsId": "string"
      }],
      "RelatedRequirements": ["string"],
      "SecurityControlId": "string",
      "SecurityControlParameters": [
       {
        "Name": "string",
        "Value": ["string"]
       }
     ],
      "Status": "string",
      "StatusReasons": [
```

```
        {
         "Description": "string",
         "ReasonCode": "string"
        }
       ]
      },
      "Confidence": number,
      "CreatedAt": "string",
      "Criticality": number,
      "Description": "string",
      "Detection": {
       "Sequence": {
        "Uid": "string",
        "Actors": [{
         "Id": "string",
         "Session": {
          "Uid": "string",
          "MfAStatus": "string",
          "CreatedTime": "string",
          "Issuer": "string"
         },
         "User": {
          "CredentialUid": "string",
          "Name": "string",
          "Type": "string",
          "Uid": "string",
          "Account": {
           "Uid": "string",
           "Name": "string"
          }
         }
        }],
        "Endpoints": [{
         "Id": "string",
         "Ip": "string",
         "Domain": "string",
         "Port": number,
         "Location": {
          "City": "string",
          "Country": "string",
          "Lat": number,
          "Lon": number
         },
         "AutonomousSystem": {
```

```
          "Name": "string",
          "Number": number
        },
        "Connection": {
          "Direction": "string"
        }
      }],
      "Signals": [{
        "Id": "string",
        "Title": "string",
        "ActorIds": ["string"],
        "Count": number,
        "FirstSeenAt": number,
        "SignalIndicators": [
          {
            "Key": "string",
            "Title": "string",
            "Values": ["string"]
          },
          {
            "Key": "string",
            "Title": "string",
            "Values": ["string"]
          }
        ],
        "LastSeenAt": number,
        "Name": "string",
        "ResourceIds": ["string"],
        "Type": "string"
      }],
      "SequenceIndicators": [
        {
          "Key": "string",
          "Title": "string",
          "Values": ["string"]
        },
        {
          "Key": "string",
          "Title": "string",
          "Values": ["string"]
        }
      ]
    }
  },
```

```
      "FindingProviderFields": {
       "Confidence": number,
       "Criticality": number,
       "RelatedFindings": [{
        "ProductArn": "string",
        "Id": "string"
       }],
       "Severity": {
        "Label": "string",
        "Normalized": number,
        "Original": "string"
       },
       "Types": ["string"]
      },
      "FirstObservedAt": "string",
      "GeneratorId": "string",
      "Id": "string",
      "LastObservedAt": "string",
      "Malware": [{
       "Name": "string",
       "Path": "string",
       "State": "string",
       "Type": "string"
      }],
      "Network": {
       "DestinationDomain": "string",
       "DestinationIpV4": "string",
       "DestinationIpV6": "string",
       "DestinationPort": number,
       "Direction": "string",
       "OpenPortRange": {
        "Begin": integer,
        "End": integer
       },
       "Protocol": "string",
       "SourceDomain": "string",
       "SourceIpV4": "string",
       "SourceIpV6": "string",
       "SourceMac": "string",
       "SourcePort": number
      },
      "NetworkPath": [{
       "ComponentId": "string",
       "ComponentType": "string",
```

```
      "Egress": {
       "Destination": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       },
       "Protocol": "string",
       "Source": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       }
      },
      "Ingress": {
       "Destination": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       },
       "Protocol": "string",
       "Source": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       }
      }
     }],
     "Note": {
      "Text": "string",
      "UpdatedAt": "string",
      "UpdatedBy": "string"
     },
     "PatchSummary": {
      "FailedCount": number,
      "Id": "string",
      "InstalledCount": number,
```

```
      "InstalledOtherCount": number,
      "InstalledPendingReboot": number,
      "InstalledRejectedCount": number,
      "MissingCount": number,
      "Operation": "string",
      "OperationEndTime": "string",
      "OperationStartTime": "string",
      "RebootOption": "string"
    },
    "Process": {
      "LaunchedAt": "string",
      "Name": "string",
      "ParentPid": number,
      "Path": "string",
      "Pid": number,
      "TerminatedAt": "string"
    },
    "ProductArn": "string",
    "ProductFields": {
      "string": "string"
    },
    "ProductName": "string",
    "RecordState": "string",
    "Region": "string",
    "RelatedFindings": [{
      "Id": "string",
      "ProductArn": "string"
    }],
    "Remediation": {
      "Recommendation": {
        "Text": "string",
        "Url": "string"
      }
    },
    "Resources": [{
      "ApplicationArn": "string",
      "ApplicationName": "string",
      "DataClassification": {
        "DetailedResultsLocation": "string",
        "Result": {
          "AdditionalOccurrences": boolean,
          "CustomDataIdentifiers": {
            "Detections": [{
              "Arn": "string",
```

```
          "Count": integer,
          "Name": "string",
          "Occurrences": {
           "Cells": [{
            "CellReference": "string",
            "Column": integer,
            "ColumnName": "string",
            "Row": integer
           }],
           "LineRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "OffsetRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "Pages": [{
            "LineRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "OffsetRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          }
         }],
         "TotalCount": integer
        },
        "MimeType": "string",
        "SensitiveData": [{
         "Category": "string",
         "Detections": [{
```

```
          "Count": integer,
          "Occurrences": {
           "Cells": [{
            "CellReference": "string",
            "Column": integer,
            "ColumnName": "string",
            "Row": integer
           }],
           "LineRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "OffsetRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "Pages": [{
            "LineRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "OffsetRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          },
          "Type": "string"
         }],
         "TotalCount": integer
        }],
        "SizeClassified": integer,
        "Status": {
         "Code": "string",
         "Reason": "string"
```

```
          }
         }
        },
        "Details": {
         "AwsAmazonMQBroker": {
          "AutoMinorVersionUpgrade": boolean,
          "BrokerArn": "string",
          "BrokerId": "string",
          "BrokerName": "string",
          "Configuration": {
           "Id": "string",
           "Revision": integer
          },
          "DeploymentMode": "string",
          "EncryptionOptions": {
           "UseAwsOwnedKey": boolean
          },
          "EngineType": "string",
          "EngineVersion": "string",
          "HostInstanceType": "string",
          "Logs": {
           "Audit": boolean,
           "AuditLogGroup": "string",
           "General": boolean,
           "GeneralLogGroup": "string"
          },
          "MaintenanceWindowStartTime": {
           "DayOfWeek": "string",
           "TimeOfDay": "string",
           "TimeZone": "string"
          },
          "PubliclyAccessible": boolean,
          "SecurityGroups": [
           "string"
          ],
          "StorageType": "string",
          "SubnetIds": [
           "string",
           "string"
          ],
          "Users": [{
           "Username": "string"
          }]
         },
```

```
        "AwsApiGatewayRestApi": {
         "ApiKeySource": "string",
         "BinaryMediaTypes": [" string"],
         "CreatedDate": "string",
         "Description": "string",
         "EndpointConfiguration": {
          "Types": ["string"]
         },
         "Id": "string",
         "MinimumCompressionSize": number,
         "Name": "string",
         "Version": "string"
        },
        "AwsApiGatewayStage": {
         "AccessLogSettings": {
          "DestinationArn": "string",
          "Format": "string"
         },
         "CacheClusterEnabled": boolean,
         "CacheClusterSize": "string",
         "CacheClusterStatus": "string",
         "CanarySettings": {
          "DeploymentId": "string",
          "PercentTraffic": number,
          "StageVariableOverrides": [{
           "string": "string"
          }],
          "UseStageCache": boolean
         },
         "ClientCertificateId": "string",
         "CreatedDate": "string",
         "DeploymentId": "string",
         "Description": "string",
         "DocumentationVersion": "string",
         "LastUpdatedDate": "string",
         "MethodSettings": [{
          "CacheDataEncrypted": boolean,
          "CachingEnabled": boolean,
          "CacheTtlInSeconds": number,
          "DataTraceEnabled": boolean,
          "HttpMethod": "string",
          "LoggingLevel": "string",
          "MetricsEnabled": boolean,
          "RequireAuthorizationForCacheControl": boolean,
```

```
          "ResourcePath": "string",
          "ThrottlingBurstLimit": number,
          "ThrottlingRateLimit": number,
          "UnauthorizedCacheControlHeaderStrategy": "string"
        }],
        "StageName": "string",
        "TracingEnabled": boolean,
        "Variables": {
          "string": "string"
        },
        "WebAclArn": "string"
      },
      "AwsApiGatewayV2Api": {
        "ApiEndpoint": "string",
        "ApiId": "string",
        "ApiKeySelectionExpression": "string",
        "CorsConfiguration": {
          "AllowCredentials": boolean,
          "AllowHeaders": ["string"],
          "AllowMethods": ["string"],
          "AllowOrigins": ["string"],
          "ExposeHeaders": ["string"],
          "MaxAge": number
        },
        "CreatedDate": "string",
        "Description": "string",
        "Name": "string",
        "ProtocolType": "string",
        "RouteSelectionExpression": "string",
        "Version": "string"
      },
      "AwsApiGatewayV2Stage": {
        "AccessLogSettings": {
          "DestinationArn": "string",
          "Format": "string"
        },
        "ApiGatewayManaged": boolean,
        "AutoDeploy": boolean,
        "ClientCertificateId": "string",
        "CreatedDate": "string",
        "DefaultRouteSettings": {
          "DataTraceEnabled": boolean,
          "DetailedMetricsEnabled": boolean,
          "LoggingLevel": "string",
```

```
          "ThrottlingBurstLimit": number,
          "ThrottlingRateLimit": number
         },
         "DeploymentId": "string",
         "Description": "string",
         "LastDeploymentStatusMessage": "string",
         "LastUpdatedDate": "string",
         "RouteSettings": {
          "DetailedMetricsEnabled": boolean,
          "LoggingLevel": "string",
          "DataTraceEnabled": boolean,
          "ThrottlingBurstLimit": number,
          "ThrottlingRateLimit": number
         },
         "StageName": "string",
         "StageVariables": [{
          "string": "string"
         }]
        },
        "AwsAppSyncGraphQLApi": {
         "AwsAppSyncGraphQlApi": {
          "AdditionalAuthenticationProviders": [
          {
           "AuthenticationType": "string",
           "LambdaAuthorizerConfig": {
            "AuthorizerResultTtlInSeconds": integer,
            "AuthorizerUri": "string"
           }
          },
          {
           "AuthenticationType": "string"
          }
          ],
          "ApiId": "string",
          "Arn": "string",
          "AuthenticationType": "string",
          "Id": "string",
          "LogConfig": {
           "CloudWatchLogsRoleArn": "string",
           "ExcludeVerboseContent": boolean,
           "FieldLogLevel": "string"
          },
          "Name": "string",
          "XrayEnabled": boolean
```

```
        }
      },
      "AwsAthenaWorkGroup": {
       "Description": "string",
       "Name": "string",
       "WorkgroupConfiguration": {
        "ResultConfiguration": {
         "EncryptionConfiguration": {
          "EncryptionOption": "string",
          "KmsKey": "string"
         }
        }
       },
       "State": "string"
      },
      "AwsAutoScalingAutoScalingGroup": {
       "AvailabilityZones": [{
        "Value": "string"
       }],
       "CreatedTime": "string",
       "HealthCheckGracePeriod": integer,
       "HealthCheckType": "string",
       "LaunchConfigurationName": "string",
       "LoadBalancerNames": ["string"],
       "LaunchTemplate": {
                       "LaunchTemplateId": "string",
                       "LaunchTemplateName": "string",
                       "Version": "string"
                   },
       "MixedInstancesPolicy": {
        "InstancesDistribution": {
         "OnDemandAllocationStrategy": "string",
         "OnDemandBaseCapacity": number,
         "OnDemandPercentageAboveBaseCapacity": number,
         "SpotAllocationStrategy": "string",
         "SpotInstancePools": number,
         "SpotMaxPrice": "string"
        },
        "LaunchTemplate": {
         "LaunchTemplateSpecification": {
          "LaunchTemplateId": "string",
          "LaunchTemplateName": "string",
          "Version": "string"
         },
```

```
          "CapacityRebalance": boolean,
          "Overrides": [{
           "InstanceType": "string",
           "WeightedCapacity": "string"
          }]
         }
        }
       },
       "AwsAutoScalingLaunchConfiguration": {
        "AssociatePublicIpAddress": boolean,
        "BlockDeviceMappings": [{
         "DeviceName": "string",
         "Ebs": {
          "DeleteOnTermination": boolean,
          "Encrypted": boolean,
          "Iops": number,
          "SnapshotId": "string",
          "VolumeSize": number,
          "VolumeType": "string"
         },
         "NoDevice": boolean,
         "VirtualName": "string"
        }],
        "ClassicLinkVpcId": "string",
        "ClassicLinkVpcSecurityGroups": ["string"],
        "CreatedTime": "string",
        "EbsOptimized": boolean,
        "IamInstanceProfile": "string"
       },
       "ImageId": "string",
       "InstanceMonitoring": {
        "Enabled": boolean
       },
       "InstanceType": "string",
       "KernelId": "string",
       "KeyName": "string",
       "LaunchConfigurationName": "string",
       "MetadataOptions": {
        "HttpEndPoint": "string",
        "HttpPutReponseHopLimit": number,
        "HttpTokens": "string"
       },
       "PlacementTenancy": "string",
       "RamdiskId": "string",
```

```
        "SecurityGroups": ["string"],
        "SpotPrice": "string",
        "UserData": "string"
      },
      "AwsBackupBackupPlan": {
        "BackupPlan": {
          "AdvancedBackupSettings": [{
            "BackupOptions": {
              "WindowsVSS":"string"
            },
            "ResourceType":"string"
          }],
          "BackupPlanName": "string",
          "BackupPlanRule": [{
            "CompletionWindowMinutes": integer,
            "CopyActions": [{
              "DestinationBackupVaultArn": "string",
              "Lifecycle": {
                "DeleteAfterDays": integer,
                "MoveToColdStorageAfterDays": integer
              }
            }],
            "Lifecycle": {
              "DeleteAfterDays": integer
            },
            "RuleName": "string",
            "ScheduleExpression": "string",
            "StartWindowMinutes": integer,
            "TargetBackupVault": "string"
          }]
        },
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "VersionId": "string"
      },
      "AwsBackupBackupVault": {
        "AccessPolicy": {
          "Statement": [{
            "Action": ["string"],
            "Effect": "string",
            "Principal": {
              "AWS": "string"
            },
            "Resource": "string"
```

```
          }],
          "Version": "string"
        },
        "BackupVaultArn": "string",
        "BackupVaultName": "string",
        "EncryptionKeyArn": "string",
        "Notifications": {
          "BackupVaultEvents": ["string"],
          "SNSTopicArn": "string"
        }
      },
      "AwsBackupRecoveryPoint": {
        "BackupSizeInBytes": integer,
        "BackupVaultName": "string",
        "BackupVaultArn": "string",
        "CalculatedLifecycle": {
          "DeleteAt": "string",
          "MoveToColdStorageAt": "string"
        },
        "CompletionDate": "string",
        "CreatedBy": {
          "BackupPlanArn": "string",
          "BackupPlanId": "string",
          "BackupPlanVersion": "string",
          "BackupRuleId": "string"
        },
        "CreationDate": "string",
        "EncryptionKeyArn": "string",
        "IamRoleArn": "string",
        "IsEncrypted": boolean,
        "LastRestoreTime": "string",
        "Lifecycle": {
          "DeleteAfterDays": integer,
          "MoveToColdStorageAfterDays": integer
        },
        "RecoveryPointArn": "string",
        "ResourceArn": "string",
        "ResourceType": "string",
        "SourceBackupVaultArn": "string",
        "Status": "string",
        "StatusMessage": "string",
        "StorageClass": "string"
      },
      "AwsCertificateManagerCertificate": {
```

```
        "CertificateAuthorityArn": "string",
        "CreatedAt": "string",
        "DomainName": "string",
        "DomainValidationOptions": [{
         "DomainName": "string",
         "ResourceRecord": {
          "Name": "string",
          "Type": "string",
          "Value": "string"
         },
         "ValidationDomain": "string",
         "ValidationEmails": ["string"],
         "ValidationMethod": "string",
         "ValidationStatus": "string"
        }],
        "ExtendedKeyUsages": [{
         "Name": "string",
         "OId": "string"
        }],
        "FailureReason": "string",
        "ImportedAt": "string",
        "InUseBy": ["string"],
        "IssuedAt": "string",
        "Issuer": "string",
        "KeyAlgorithm": "string",
        "KeyUsages": [{
         "Name": "string"
        }],
        "NotAfter": "string",
        "NotBefore": "string",
        "Options": {
         "CertificateTransparencyLoggingPreference": "string"
        },
        "RenewalEligibility": "string",
        "RenewalSummary": {
         "DomainValidationOptions": [{
          "DomainName": "string",
          "ResourceRecord": {
           "Name": "string",
           "Type": "string",
           "Value": "string"
          },
          "ValidationDomain": "string",
          "ValidationEmails": ["string"],
```

```
          "ValidationMethod": "string",
          "ValidationStatus": "string"
         }],
         "RenewalStatus": "string",
         "RenewalStatusReason": "string",
         "UpdatedAt": "string"
        },
        "Serial": "string",
        "SignatureAlgorithm": "string",
        "Status": "string",
        "Subject": "string",
        "SubjectAlternativeNames": ["string"],
        "Type": "string"
       },
       "AwsCloudFormationStack": {
        "Capabilities": ["string"],
        "CreationTime": "string",
        "Description": "string",
        "DisableRollback": boolean,
        "DriftInformation": {
         "StackDriftStatus": "string"
        },
        "EnableTerminationProtection": boolean,
        "LastUpdatedTime": "string",
        "NotificationArns": ["string"],
        "Outputs": [{
         "Description": "string",
         "OutputKey": "string",
         "OutputValue": "string"
        }],
        "RoleArn": "string",
        "StackId": "string",
        "StackName": "string",
        "StackStatus": "string",
        "StackStatusReason": "string",
        "TimeoutInMinutes": number
       },
       "AwsCloudFrontDistribution": {
        "CacheBehaviors": {
         "Items": [{
          "ViewerProtocolPolicy": "string"
         }]
        },
        "DefaultCacheBehavior": {
```

```
          "ViewerProtocolPolicy": "string"
        },
        "DefaultRootObject": "string",
        "DomainName": "string",
        "Etag": "string",
        "LastModifiedTime": "string",
        "Logging": {
         "Bucket": "string",
         "Enabled": boolean,
         "IncludeCookies": boolean,
         "Prefix": "string"
        },
        "OriginGroups": {
         "Items": [{
          "FailoverCriteria": {
           "StatusCodes": {
            "Items": [number],
            "Quantity": number
           }
          }
         }]
        },
        "Origins": {
         "Items": [{
          "CustomOriginConfig": {
           "HttpPort": number,
           "HttpsPort": number,
           "OriginKeepaliveTimeout": number,
           "OriginProtocolPolicy": "string",
           "OriginReadTimeout": number,
           "OriginSslProtocols": {
            "Items": ["string"],
            "Quantity": number
           }
          },
          "DomainName": "string",
          "Id": "string",
          "OriginPath": "string",
          "S3OriginConfig": {
           "OriginAccessIdentity": "string"
          }
         }]
        },
        "Status": "string",
```

```
        "ViewerCertificate": {
         "AcmCertificateArn": "string",
         "Certificate": "string",
         "CertificateSource": "string",
         "CloudFrontDefaultCertificate": boolean,
         "IamCertificateId": "string",
         "MinimumProtocolVersion": "string",
         "SslSupportMethod": "string"
        },
        "WebAclId": "string"
       },
       "AwsCloudTrailTrail": {
        "CloudWatchLogsLogGroupArn": "string",
        "CloudWatchLogsRoleArn": "string",
        "HasCustomEventSelectors": boolean,
        "HomeRegion": "string",
        "IncludeGlobalServiceEvents": boolean,
        "IsMultiRegionTrail": boolean,
        "IsOrganizationTrail": boolean,
        "KmsKeyId": "string",
        "LogFileValidationEnabled": boolean,
        "Name": "string",
        "S3BucketName": "string",
        "S3KeyPrefix": "string",
        "SnsTopicArn": "string",
        "SnsTopicName": "string",
        "TrailArn": "string"
       },
       "AwsCloudWatchAlarm": {
        "ActionsEnabled": boolean,
        "AlarmActions": ["string"],
        "AlarmArn": "string",
        "AlarmConfigurationUpdatedTimestamp": "string",
        "AlarmDescription": "string",
        "AlarmName": "string",
        "ComparisonOperator": "string",
        "DatapointsToAlarm": number,
        "Dimensions": [{
         "Name": "string",
         "Value": "string"
        }],
        "EvaluateLowSampleCountPercentile": "string",
        "EvaluationPeriods": number,
        "ExtendedStatistic": "string",
```

```
        "InsufficientDataActions": ["string"],
        "MetricName": "string",
        "Namespace": "string",
        "OkActions": ["string"],
        "Period": number,
        "Statistic": "string",
        "Threshold": number,
        "ThresholdMetricId": "string",
        "TreatMissingData": "string",
        "Unit": "string"
      },
      "AwsCodeBuildProject": {
        "Artifacts": [{
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
        }],
        "SecondaryArtifacts": [{
                    "ArtifactIdentifier": "string",
                    "Type": "string",
                    "Location": "string",
                    "Name": "string",
                    "NamespaceType": "string",
                    "Packaging": "string",
                    "Path": "string",
                    "EncryptionDisabled": boolean,
                    "OverrideArtifactName": boolean
                }],
        "EncryptionKey": "string",
        "Certificate": "string",
        "Environment": {
          "Certificate": "string",
          "EnvironmentVariables": [{
            "Name": "string",
            "Type": "string",
            "Value": "string"
          }],
          "ImagePullCredentialsType": "string",
```

```
          "PrivilegedMode": boolean,
          "RegistryCredential": {
           "Credential": "string",
           "CredentialProvider": "string"
          },
          "Type": "string"
         },
         "LogsConfig": {
          "CloudWatchLogs": {
           "GroupName": "string",
           "Status": "string",
           "StreamName": "string"
          },
          "S3Logs": {
           "EncryptionDisabled": boolean,
           "Location": "string",
           "Status": "string"
          }
         },
         "Name": "string",
         "ServiceRole": "string",
         "Source": {
          "Type": "string",
          "Location": "string",
          "GitCloneDepth": integer
         },
         "VpcConfig": {
          "VpcId": "string",
          "Subnets": ["string"],
          "SecurityGroupIds": ["string"]
         }
        },
        "AwsDmsEndpoint": {
         "CertificateArn": "string",
         "DatabaseName": "string",
         "EndpointArn": "string",
         "EndpointIdentifier": "string",
         "EndpointType": "string",
         "EngineName": "string",
         "KmsKeyId": "string",
         "Port": integer,
         "ServerName": "string",
         "SslMode": "string",
         "Username": "string"
```

```
      },
      "AwsDmsReplicationInstance": {
       "AllocatedStorage": integer,
       "AutoMinorVersionUpgrade": boolean,
       "AvailabilityZone": "string",
       "EngineVersion": "string",
       "KmsKeyId": "string",
       "MultiAZ": boolean,
       "PreferredMaintenanceWindow": "string",
       "PubliclyAccessible": boolean,
       "ReplicationInstanceClass": "string",
       "ReplicationInstanceIdentifier": "string",
       "ReplicationSubnetGroup": {
           "ReplicationSubnetGroupIdentifier": "string"
       },
       "VpcSecurityGroups": [
           {
               "VpcSecurityGroupId": "string"
           }
       ]
      },
      "AwsDmsReplicationTask": {
       "CdcStartPosition": "string",
       "Id": "string",
       "MigrationType": "string",
       "ReplicationInstanceArn": "string",
       "ReplicationTaskIdentifier": "string",
       "ReplicationTaskSettings": {
        "string": "string"
       },
       "SourceEndpointArn": "string",
       "TableMappings": {
        "string": "string"
       },
       "TargetEndpointArn": "string"
      },
      "AwsDynamoDbTable": {
       "AttributeDefinitions": [{
        "AttributeName": "string",
        "AttributeType": "string"
       }],
       "BillingModeSummary": {
        "BillingMode": "string",
        "LastUpdateToPayPerRequestDateTime": "string"
```

```
        },
        "CreationDateTime": "string",
        "DeletionProtectionEnabled": boolean,
        "GlobalSecondaryIndexes": [{
         "Backfilling": boolean,
         "IndexArn": "string",
         "IndexName": "string",
         "IndexSizeBytes": number,
         "IndexStatus": "string",
         "ItemCount": number,
         "KeySchema": [{
          "AttributeName": "string",
          "KeyType": "string"
         }],
         "Projection": {
          "NonKeyAttributes": ["string"],
          "ProjectionType": "string"
         },
         "ProvisionedThroughput": {
          "LastDecreaseDateTime": "string",
          "LastIncreaseDateTime": "string",
          "NumberOfDecreasesToday": number,
          "ReadCapacityUnits": number,
          "WriteCapacityUnits": number
         }
        }],
        "GlobalTableVersion": "string",
        "ItemCount": number,
        "KeySchema": [{
         "AttributeName": "string",
         "KeyType": "string"
        }],
        "LatestStreamArn": "string",
        "LatestStreamLabel": "string",
        "LocalSecondaryIndexes": [{
         "IndexArn": "string",
         "IndexName": "string",
         "KeySchema": [{
          "AttributeName": "string",
          "KeyType": "string"
         }],
         "Projection": {
          "NonKeyAttributes": ["string"],
          "ProjectionType": "string"
```

```
          }
        }],
        "ProvisionedThroughput": {
         "LastDecreaseDateTime": "string",
         "LastIncreaseDateTime": "string",
         "NumberOfDecreasesToday": number,
         "ReadCapacityUnits": number,
         "WriteCapacityUnits": number
        },
        "Replicas": [{
         "GlobalSecondaryIndexes": [{
          "IndexName": "string",
          "ProvisionedThroughputOverride": {
           "ReadCapacityUnits": number
          }
         }],
         "KmsMasterKeyId": "string",
         "ProvisionedThroughputOverride": {
          "ReadCapacityUnits": number
         },
         "RegionName": "string",
         "ReplicaStatus": "string",
         "ReplicaStatusDescription": "string"
        }],
        "RestoreSummary": {
         "RestoreDateTime": "string",
         "RestoreInProgress": boolean,
         "SourceBackupArn": "string",
         "SourceTableArn": "string"
        },
        "SseDescription": {
         "InaccessibleEncryptionDateTime": "string",
         "KmsMasterKeyArn": "string",
         "SseType": "string",
         "Status": "string"
        },
        "StreamSpecification": {
         "StreamEnabled": boolean,
         "StreamViewType": "string"
        },
        "TableId": "string",
        "TableName": "string",
        "TableSizeBytes": number,
        "TableStatus": "string"
```

```
      },
      "AwsEc2ClientVpnEndpoint": {
       "AuthenticationOptions": [
        {
         "MutualAuthentication": {
          "ClientRootCertificateChainArn": "string"
         },
         "Type": "string"
        }
       ],
       "ClientCidrBlock": "string",
       "ClientConnectOptions": {
        "Enabled": boolean
       },
       "ClientLoginBannerOptions": {
        "Enabled": boolean
       },
       "ClientVpnEndpointId": "string",
       "ConnectionLogOptions": {
        "Enabled": boolean
       },
       "Description": "string",
       "DnsServer": ["string"],
       "ServerCertificateArn": "string",
       "SecurityGroupIdSet": [
        "string"
       ],
       "SelfServicePortalUrl": "string",
       "SessionTimeoutHours": "integer",
       "SplitTunnel": boolean,
       "TransportProtocol": "string",
       "VpcId": "string",
       "VpnPort": integer
      },
      "AwsEc2Eip": {
       "AllocationId": "string",
       "AssociationId": "string",
       "Domain": "string",
       "InstanceId": "string",
       "NetworkBorderGroup": "string",
       "NetworkInterfaceId": "string",
       "NetworkInterfaceOwnerId": "string",
       "PrivateIpAddress": "string",
       "PublicIp": "string",
```

```
        "PublicIpv4Pool": "string"
      },
      "AwsEc2Instance": {
        "IamInstanceProfileArn": "string",
        "ImageId": "string",
        "IpV4Addresses": ["string"],
        "IpV6Addresses": ["string"],
        "KeyName": "string",
        "LaunchedAt": "string",
        "MetadataOptions": {
          "HttpEndpoint": "string",
          "HttpProtocolIpv6": "string",
          "HttpPutResponseHopLimit": number,
          "HttpTokens": "string",
          "InstanceMetadataTags": "string"
        },
        "Monitoring": {
          "State": "string"
        },
        "NetworkInterfaces": [{
          "NetworkInterfaceId": "string"
        }],
        "SubnetId": "string",
        "Type": "string",
        "VirtualizationType": "string",
        "VpcId": "string"
      },
      "AwsEc2LaunchTemplate": {
        "DefaultVersionNumber": "string",
        "ElasticGpuSpecifications": ["string"],
        "ElasticInferenceAccelerators": ["string"],
        "Id": "string",
        "ImageId": "string",
        "LatestVersionNumber": "string",
        "LaunchTemplateData": {
          "BlockDeviceMappings": [{
            "DeviceName": "string",
            "Ebs": {
              "DeleteonTermination": boolean,
              "Encrypted": boolean,
              "SnapshotId": "string",
              "VolumeSize": number,
              "VolumeType": "string"
            }
```

```
        }],
        "MetadataOptions": {
         "HttpTokens": "string",
         "HttpPutResponseHopLimit" : number
        },
        "Monitoring": {
         "Enabled": boolean
        },
        "NetworkInterfaces": [{
         "AssociatePublicIpAddress" : boolean
        }]
       },
       "LaunchTemplateName": "string",
       "LicenseSpecifications": ["string"],
       "SecurityGroupIds": ["string"],
       "SecurityGroups": ["string"],
       "TagSpecifications": ["string"]
      },
      "AwsEc2NetworkAcl": {
       "Associations": [{
        "NetworkAclAssociationId": "string",
        "NetworkAclId": "string",
        "SubnetId": "string"
       }],
       "Entries": [{
        "CidrBlock": "string",
        "Egress": boolean,
        "IcmpTypeCode": {
         "Code": number,
         "Type": number
        },
        "Ipv6CidrBlock": "string",
        "PortRange": {
         "From": number,
         "To": number
        },
        "Protocol": "string",
        "RuleAction": "string",
        "RuleNumber": number
       }],
       "IsDefault": boolean,
       "NetworkAclId": "string",
       "OwnerId": "string",
       "VpcId": "string"
```

```
      },
      "AwsEc2NetworkInterface": {
       "Attachment": {
        "AttachmentId": "string",
        "AttachTime": "string",
        "DeleteOnTermination": boolean,
        "DeviceIndex": number,
        "InstanceId": "string",
        "InstanceOwnerId": "string",
        "Status": "string"
       },
       "Ipv6Addresses": [{
        "Ipv6Address": "string"
       }],
       "NetworkInterfaceId": "string",
       "PrivateIpAddresses": [{
        "PrivateDnsName": "string",
        "PrivateIpAddress": "string"
       }],
       "PublicDnsName": "string",
       "PublicIp": "string",
       "SecurityGroups": [{
        "GroupId": "string",
        "GroupName": "string"
       }],
       "SourceDestCheck": boolean
      },
      "AwsEc2RouteTable": {
       "AssociationSet": [{
        "AssociationState": {
         "State": "string"
        },
        "Main": boolean,
        "RouteTableAssociationId": "string",
        "RouteTableId": "string"
       }],
       "PropogatingVgwSet": [],
       "RouteTableId": "string",
       "RouteSet": [
        {
         "DestinationCidrBlock": "string",
         "GatewayId": "string",
         "Origin": "string",
         "State": "string"
```

```
        },
        {
         "DestinationCidrBlock": "string",
         "GatewayId": "string",
         "Origin": "string",
         "State": "string"
        }
       ],
       "VpcId": "string"
      },
      "AwsEc2SecurityGroup": {
       "GroupId": "string",
       "GroupName": "string",
       "IpPermissions": [{
        "FromPort": number,
        "IpProtocol": "string",
        "IpRanges": [{
         "CidrIp": "string"
        }],
        "Ipv6Ranges": [{
         "CidrIpv6": "string"
        }],
        "PrefixListIds": [{
         "PrefixListId": "string"
        }],
        "ToPort": number,
        "UserIdGroupPairs": [{
         "GroupId": "string",
         "GroupName": "string",
         "PeeringStatus": "string",
         "UserId": "string",
         "VpcId": "string",
         "VpcPeeringConnectionId": "string"
        }]
       }],
       "IpPermissionsEgress": [{
        "FromPort": number,
        "IpProtocol": "string",
        "IpRanges": [{
         "CidrIp": "string"
        }],
        "Ipv6Ranges": [{
         "CidrIpv6": "string"
        }],
```

```
        "PrefixListIds": [{
         "PrefixListId": "string"
        }],
        "ToPort": number,
        "UserIdGroupPairs": [{
         "GroupId": "string",
         "GroupName": "string",
         "PeeringStatus": "string",
         "UserId": "string",
         "VpcId": "string",
         "VpcPeeringConnectionId": "string"
        }]
       }],
       "OwnerId": "string",
       "VpcId": "string"
      },
      "AwsEc2Subnet": {
       "AssignIpv6AddressOnCreation": boolean,
       "AvailabilityZone": "string",
       "AvailabilityZoneId": "string",
       "AvailableIpAddressCount": number,
       "CidrBlock": "string",
       "DefaultForAz": boolean,
       "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "string",
        "Ipv6CidrBlock": "string",
        "CidrBlockState": "string"
       }],
       "MapPublicIpOnLaunch": boolean,
       "OwnerId": "string",
       "State": "string",
       "SubnetArn": "string",
       "SubnetId": "string",
       "VpcId": "string"
      },
      "AwsEc2TransitGateway": {
       "AmazonSideAsn": number,
       "AssociationDefaultRouteTableId": "string",
       "AutoAcceptSharedAttachments": "string",
       "DefaultRouteTableAssociation": "string",
       "DefaultRouteTablePropagation": "string",
       "Description": "string",
       "DnsSupport": "string",
       "Id": "string",
```

```
        "MulticastSupport": "string",
        "PropagationDefaultRouteTableId": "string",
        "TransitGatewayCidrBlocks": ["string"],
        "VpnEcmpSupport": "string"
      },
      "AwsEc2Volume": {
        "Attachments": [{
          "AttachTime": "string",
          "DeleteOnTermination": boolean,
          "InstanceId": "string",
          "Status": "string"
        }],
        "CreateTime": "string",
        "DeviceName": "string",
        "Encrypted": boolean,
        "KmsKeyId": "string",
        "Size": number,
        "SnapshotId": "string",
        "Status": "string",
        "VolumeId": "string",
        "VolumeScanStatus": "string",
        "VolumeType": "string"
      },
      "AwsEc2Vpc": {
        "CidrBlockAssociationSet": [{
          "AssociationId": "string",
          "CidrBlock": "string",
          "CidrBlockState": "string"
        }],
        "DhcpOptionsId": "string",
        "Ipv6CidrBlockAssociationSet": [{
          "AssociationId": "string",
          "CidrBlockState": "string",
          "Ipv6CidrBlock": "string"
        }],
        "State": "string"
      },
      "AwsEc2VpcEndpointService": {
        "AcceptanceRequired": boolean,
        "AvailabilityZones": ["string"],
        "BaseEndpointDnsNames": ["string"],
        "ManagesVpcEndpoints": boolean,
        "GatewayLoadBalancerArns": ["string"],
        "NetworkLoadBalancerArns": ["string"],
```

```
        "PrivateDnsName": "string",
        "ServiceId": "string",
        "ServiceName": "string",
        "ServiceState": "string",
        "ServiceType": [{
         "ServiceType": "string"
        }]
       },
       "AwsEc2VpcPeeringConnection": {
        "AccepterVpcInfo": {
         "CidrBlock": "string",
         "CidrBlockSet": [{
          "CidrBlock": "string"
         }],
         "Ipv6CidrBlockSet": [{
          "Ipv6CidrBlock": "string"
         }],
         "OwnerId": "string",
         "PeeringOptions": {
          "AllowDnsResolutionFromRemoteVpc": boolean,
          "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
          "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
         },
         "Region": "string",
         "VpcId": "string"
        },
        "ExpirationTime": "string",
        "RequesterVpcInfo": {
         "CidrBlock": "string",
         "CidrBlockSet": [{
          "CidrBlock": "string"
         }],
         "Ipv6CidrBlockSet": [{
          "Ipv6CidrBlock": "string"
         }],
         "OwnerId": "string",
         "PeeringOptions": {
          "AllowDnsResolutionFromRemoteVpc": boolean,
          "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
          "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
         },
         "Region": "string",
         "VpcId": "string"
        },
```

```
        "Status": {
         "Code": "string",
         "Message": "string"
        },
        "VpcPeeringConnectionId": "string"
       },
       "AwsEcrContainerImage": {
        "Architecture": "string",
        "ImageDigest": "string",
        "ImagePublishedAt": "string",
        "ImageTags": ["string"],
        "RegistryId": "string",
        "RepositoryName": "string"
       },
       "AwsEcrRepository": {
        "Arn": "string",
        "ImageScanningConfiguration": {
         "ScanOnPush": boolean
        },
        "ImageTagMutability": "string",
        "LifecyclePolicy": {
         "LifecyclePolicyText": "string",
         "RegistryId": "string"
        },
        "RepositoryName": "string",
        "RepositoryPolicyText": "string"
       },
       "AwsEcsCluster": {
        "ActiveServicesCount": number,
        "CapacityProviders": ["string"],
        "ClusterArn": "string",
        "ClusterName": "string",
        "ClusterSettings": [{
         "Name": "string",
         "Value": "string"
        }],
        "Configuration": {
         "ExecuteCommandConfiguration": {
          "KmsKeyId": "string",
          "LogConfiguration": {
           "CloudWatchEncryptionEnabled": boolean,
           "CloudWatchLogGroupName": "string",
           "S3BucketName": "string",
           "S3EncryptionEnabled": boolean,
```

```
          "S3KeyPrefix": "string"
         },
         "Logging": "string"
        }
       },
       "DefaultCapacityProviderStrategy": [{
        "Base": number,
        "CapacityProvider": "string",
        "Weight": number
       }],
       "RegisteredContainerInstancesCount": number,
       "RunningTasksCount": number,
       "Status": "string"
      },
      "AwsEcsContainer": {
       "Image": "string",
       "MountPoints": [{
        "ContainerPath": "string",
        "SourceVolume": "string"
       }],
       "Name": "string",
       "Privileged": boolean
      },
      "AwsEcsService": {
       "CapacityProviderStrategy": [{
        "Base": number,
        "CapacityProvider": "string",
        "Weight": number
       }],
       "Cluster": "string",
       "DeploymentConfiguration": {
        "DeploymentCircuitBreaker": {
         "Enable": boolean,
         "Rollback": boolean
        },
        "MaximumPercent": number,
        "MinimumHealthyPercent": number
       },
       "DeploymentController": {
        "Type": "string"
       },
       "DesiredCount": number,
       "EnableEcsManagedTags": boolean,
       "EnableExecuteCommand": boolean,
```

```
        "HealthCheckGracePeriodSeconds": number,
        "LaunchType": "string",
        "LoadBalancers": [{
         "ContainerName": "string",
         "ContainerPort": number,
         "LoadBalancerName": "string",
         "TargetGroupArn": "string"
        }],
        "Name": "string",
        "NetworkConfiguration": {
         "AwsVpcConfiguration": {
          "AssignPublicIp": "string",
          "SecurityGroups": ["string"],
          "Subnets": ["string"]
         }
        },
        "PlacementConstraints": [{
         "Expression": "string",
         "Type": "string"
        }],
        "PlacementStrategies": [{
         "Field": "string",
         "Type": "string"
        }],
        "PlatformVersion": "string",
        "PropagateTags": "string",
        "Role": "string",
        "SchedulingStrategy": "string",
        "ServiceArn": "string",
        "ServiceName": "string",
        "ServiceRegistries": [{
         "ContainerName": "string",
         "ContainerPort": number,
         "Port": number,
         "RegistryArn": "string"
        }],
        "TaskDefinition": "string"
       },
       "AwsEcsTask": {
        "CreatedAt": "string",
        "ClusterArn": "string",
        "Group": "string",
        "StartedAt": "string",
        "StartedBy": "string",
```

```
        "TaskDefinitionArn": "string",
        "Version": number,
        "Volumes": [{
         "Name": "string",
         "Host": {
          "SourcePath": "string"
         }
        }],
        "Containers": [{
         "Image": "string",
         "MountPoints": [{
          "ContainerPath": "string",
          "SourceVolume": "string"
         }],
         "Name": "string",
         "Privileged": boolean
        }]
       },
       "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [{
         "Command": ["string"],
         "Cpu": number,
         "DependsOn": [{
          "Condition": "string",
          "ContainerName": "string"
         }],
         "DisableNetworking": boolean,
         "DnsSearchDomains": ["string"],
         "DnsServers": ["string"],
         "DockerLabels": {
          "string": "string"
         },
         "DockerSecurityOptions": ["string"],
         "EntryPoint": ["string"],
         "Environment": [{
          "Name": "string",
          "Value": "string"
         }],
         "EnvironmentFiles": [{
          "Type": "string",
          "Value": "string"
         }],
         "Essential": boolean,
         "ExtraHosts": [{
```

```
          "Hostname": "string",
          "IpAddress": "string"
         }],
         "FirelensConfiguration": {
          "Options": {
           "string": "string"
          },
          "Type": "string"
         },
         "HealthCheck": {
          "Command": ["string"],
          "Interval": number,
          "Retries": number,
          "StartPeriod": number,
          "Timeout": number
         },
         "Hostname": "string",
         "Image": "string",
         "Interactive": boolean,
         "Links": ["string"],
         "LinuxParameters": {
          "Capabilities": {
           "Add": ["string"],
           "Drop": ["string"]
          },
          "Devices": [{
           "ContainerPath": "string",
           "HostPath": "string",
           "Permissions": ["string"]
          }],
          "InitProcessEnabled": boolean,
          "MaxSwap": number,
          "SharedMemorySize": number,
          "Swappiness": number,
          "Tmpfs": [{
           "ContainerPath": "string",
           "MountOptions": ["string"],
           "Size": number
          }]
         },
         "LogConfiguration": {
          "LogDriver": "string",
          "Options": {
           "string": "string"
```

```
          },
          "SecretOptions": [{
           "Name": "string",
           "ValueFrom": "string"
          }]
         },
         "Memory": number,
         "MemoryReservation": number,
         "MountPoints": [{
          "ContainerPath": "string",
          "ReadOnly": boolean,
          "SourceVolume": "string"
         }],
         "Name": "string",
         "PortMappings": [{
          "ContainerPort": number,
          "HostPort": number,
          "Protocol": "string"
         }],
         "Privileged": boolean,
         "PseudoTerminal": boolean,
         "ReadonlyRootFilesystem": boolean,
         "RepositoryCredentials": {
          "CredentialsParameter": "string"
         },
         "ResourceRequirements": [{
          "Type": "string",
          "Value": "string"
         }],
         "Secrets": [{
          "Name": "string",
          "ValueFrom": "string"
         }],
         "StartTimeout": number,
         "StopTimeout": number,
         "SystemControls": [{
          "Namespace": "string",
          "Value": "string"
         }],
         "Ulimits": [{
          "HardLimit": number,
          "Name": "string",
          "SoftLimit": number
         }],
```

```
          "User": "string",
          "VolumesFrom": [{
           "ReadOnly": boolean,
           "SourceContainer": "string"
          }],
          "WorkingDirectory": "string"
         }],
         "Cpu": "string",
         "ExecutionRoleArn": "string",
         "Family": "string",
         "InferenceAccelerators": [{
          "DeviceName": "string",
          "DeviceType": "string"
         }],
         "IpcMode": "string",
         "Memory": "string",
         "NetworkMode": "string",
         "PidMode": "string",
         "PlacementConstraints": [{
          "Expression": "string",
          "Type": "string"
         }],
         "ProxyConfiguration": {
          "ContainerName": "string",
          "ProxyConfigurationProperties": [{
           "Name": "string",
           "Value": "string"
          }],
          "Type": "string"
         },
         "RequiresCompatibilities": ["string"],
         "Status": "string",
         "TaskRoleArn": "string",
         "Volumes": [{
          "DockerVolumeConfiguration": {
           "Autoprovision": boolean,
           "Driver": "string",
           "DriverOpts": {
            "string": "string"
           },
           "Labels": {
            "string": "string"
           },
           "Scope": "string"
```

```
        },
        "EfsVolumeConfiguration": {
         "AuthorizationConfig": {
          "AccessPointId": "string",
          "Iam": "string"
         },
         "FilesystemId": "string",
         "RootDirectory": "string",
         "TransitEncryption": "string",
         "TransitEncryptionPort": number
        },
        "Host": {
         "SourcePath": "string"
        },
        "Name": "string"
       }]
      },
      "AwsEfsAccessPoint": {
       "AccessPointId": "string",
       "Arn": "string",
       "ClientToken": "string",
       "FileSystemId": "string",
       "PosixUser": {
        "Gid": "string",
        "SecondaryGids": ["string"],
        "Uid": "string"
       },
       "RootDirectory": {
        "CreationInfo": {
         "OwnerGid": "string",
         "OwnerUid": "string",
         "Permissions": "string"
        },
        "Path": "string"
       }
      },
      "AwsEksCluster": {
       "Arn": "string",
       "CertificateAuthorityData": "string",
       "ClusterStatus": "string",
       "Endpoint": "string",
       "Logging": {
        "ClusterLogging": [{
         "Enabled": boolean,
```

```
          "Types": ["string"]
         }]
        },
        "Name": "string",
        "ResourcesVpcConfig": {
         "EndpointPublicAccess": boolean,
         "SecurityGroupIds": ["string"],
         "SubnetIds": ["string"]
        },
        "RoleArn": "string",
        "Version": "string"
       },
       "AwsElasticBeanstalkEnvironment": {
        "ApplicationName": "string",
        "Cname": "string",
        "DateCreated": "string",
        "DateUpdated": "string",
        "Description": "string",
        "EndpointUrl": "string",
        "EnvironmentArn": "string",
        "EnvironmentId": "string",
        "EnvironmentLinks": [{
         "EnvironmentName": "string",
         "LinkName": "string"
        }],
        "EnvironmentName": "string",
        "OptionSettings": [{
         "Namespace": "string",
         "OptionName": "string",
         "ResourceName": "string",
         "Value": "string"
        }],
        "PlatformArn": "string",
        "SolutionStackName": "string",
        "Status": "string",
        "Tier": {
         "Name": "string",
         "Type": "string",
         "Version": "string"
        },
        "VersionLabel": "string"
       },
       "AwsElasticSearchDomain": {
        "AccessPolicies": "string",
```

```
        "DomainStatus": {
         "DomainId": "string",
         "DomainName": "string",
         "Endpoint": "string",
         "Endpoints": {
          "string": "string"
         }
        },
        "DomainEndpointOptions": {
         "EnforceHTTPS": boolean,
         "TLSSecurityPolicy": "string"
        },
        "ElasticsearchClusterConfig": {
         "DedicatedMasterCount": number,
         "DedicatedMasterEnabled": boolean,
         "DedicatedMasterType": "string",
         "InstanceCount": number,
         "InstanceType": "string",
         "ZoneAwarenessConfig": {
          "AvailabilityZoneCount": number
         },
         "ZoneAwarenessEnabled": boolean
        },
        "ElasticsearchVersion": "string",
        "EncryptionAtRestOptions": {
         "Enabled": boolean,
         "KmsKeyId": "string"
        },
        "LogPublishingOptions": {
         "AuditLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "IndexSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "SearchSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         }
        },
        "NodeToNodeEncryptionOptions": {
         "Enabled": boolean
```

```
        },
        "ServiceSoftwareOptions": {
         "AutomatedUpdateDate": "string",
         "Cancellable": boolean,
         "CurrentVersion": "string",
         "Description": "string",
         "NewVersion": "string",
         "UpdateAvailable": boolean,
         "UpdateStatus": "string"
        },
        "VPCOptions": {
         "AvailabilityZones": [
          "string"
         ],
         "SecurityGroupIds": [
          "string"
         ],
         "SubnetIds": [
          "string"
         ],
         "VPCId": "string"
        }
       },
       "AwsElbLoadBalancer": {
        "AvailabilityZones": ["string"],
        "BackendServerDescriptions": [{
         "InstancePort": number,
         "PolicyNames": ["string"]
        }],
        "CanonicalHostedZoneName": "string",
        "CanonicalHostedZoneNameID": "string",
        "CreatedTime": "string",
        "DnsName": "string",
        "HealthCheck": {
         "HealthyThreshold": number,
         "Interval": number,
         "Target": "string",
         "Timeout": number,
         "UnhealthyThreshold": number
        },
        "Instances": [{
         "InstanceId": "string"
        }],
        "ListenerDescriptions": [{
```

```
        "Listener": {
         "InstancePort": number,
         "InstanceProtocol": "string",
         "LoadBalancerPort": number,
         "Protocol": "string",
         "SslCertificateId": "string"
        },
        "PolicyNames": ["string"]
       }],
       "LoadBalancerAttributes": {
        "AccessLog": {
         "EmitInterval": number,
         "Enabled": boolean,
         "S3BucketName": "string",
         "S3BucketPrefix": "string"
        },
        "ConnectionDraining": {
         "Enabled": boolean,
         "Timeout": number
        },
        "ConnectionSettings": {
         "IdleTimeout": number
        },
        "CrossZoneLoadBalancing": {
         "Enabled": boolean
        },
        "AdditionalAttributes": [{
                        "Key": "string",
                        "Value": "string"
                    }]
       },
       "LoadBalancerName": "string",
       "Policies": {
        "AppCookieStickinessPolicies": [{
         "CookieName": "string",
         "PolicyName": "string"
        }],
        "LbCookieStickinessPolicies": [{
         "CookieExpirationPeriod": number,
         "PolicyName": "string"
        }],
        "OtherPolicies": ["string"]
       },
       "Scheme": "string",
```

```
        "SecurityGroups": ["string"],
        "SourceSecurityGroup": {
         "GroupName": "string",
         "OwnerAlias": "string"
        },
        "Subnets": ["string"],
        "VpcId": "string"
       },
       "AwsElbv2LoadBalancer": {
        "AvailabilityZones": {
         "SubnetId": "string",
         "ZoneName": "string"
        },
        "CanonicalHostedZoneId": "string",
        "CreatedTime": "string",
        "DNSName": "string",
        "IpAddressType": "string",
        "LoadBalancerAttributes": [{
         "Key": "string",
         "Value": "string"
        }],
        "Scheme": "string",
        "SecurityGroups": ["string"],
        "State": {
         "Code": "string",
         "Reason": "string"
        },
        "Type": "string",
        "VpcId": "string"
       },
       "AwsEventSchemasRegistry": {
        "Description": "string",
        "RegistryArn": "string",
        "RegistryName": "string"
       },
       "AwsEventsEndpoint": {
        "Arn": "string",
        "Description": "string",
        "EndpointId": "string",
        "EndpointUrl": "string",
        "EventBuses": [
            {
                "EventBusArn": "string"
            },
```

```
            {
                "EventBusArn": "string"
            }
        ],
        "Name": "string",
        "ReplicationConfig": {
            "State": "string"
        },
        "RoleArn": "string",
        "RoutingConfig": {
            "FailoverConfig": {
                "Primary": {
                    "HealthCheck": "string"
                },
                "Secondary": {
                    "Route": "string"
                }
            }
        },
        "State": "string"
      },
      "AwsEventsEventBus": {
        "Arn": "string",
        "Name": "string",
        "Policy": "string"
      },
      "AwsGuardDutyDetector": {
        "FindingPublishingFrequency": "string",
        "ServiceRole": "string",
        "Status": "string",
        "DataSources": {
          "CloudTrail": {
            "Status": "string"
          },
          "DnsLogs": {
            "Status": "string"
          },
          "FlowLogs": {
            "Status": "string"
          },
          "S3Logs": {
            "Status": "string"
          },
          "Kubernetes": {
```

```
          "AuditLogs": {
           "Status": "string"
          }
         },
         "MalwareProtection": {
          "ScanEc2InstanceWithFindings": {
           "EbsVolumes": {
            "Status": "string"
           }
          },
          "ServiceRole": "string"
         }
        }
       },
       "AwsIamAccessKey": {
        "AccessKeyId": "string",
        "AccountId": "string",
        "CreatedAt": "string",
        "PrincipalId": "string",
        "PrincipalName": "string",
        "PrincipalType": "string",
        "SessionContext": {
         "Attributes": {
          "CreationDate": "string",
          "MfaAuthenticated": boolean
         },
         "SessionIssuer": {
          "AccountId": "string",
          "Arn": "string",
          "PrincipalId": "string",
          "Type": "string",
          "UserName": "string"
         }
        },
        "Status": "string"
       },
       "AwsIamGroup": {
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "GroupId": "string",
        "GroupName": "string",
```

```
        "GroupPolicyList": [{
         "PolicyName": "string"
        }],
        "Path": "string"
       },
       "AwsIamPolicy": {
        "AttachmentCount": number,
        "CreateDate": "string",
        "DefaultVersionId": "string",
        "Description": "string",
        "IsAttachable": boolean,
        "Path": "string",
        "PermissionsBoundaryUsageCount": number,
        "PolicyId": "string",
        "PolicyName": "string",
        "PolicyVersionList": [{
         "CreateDate": "string",
         "IsDefaultVersion": boolean,
         "VersionId": "string"
        }],
        "UpdateDate": "string"
       },
       "AwsIamRole": {
        "AssumeRolePolicyDocument": "string",
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "InstanceProfileList": [{
         "Arn": "string",
         "CreateDate": "string",
         "InstanceProfileId": "string",
         "InstanceProfileName": "string",
         "Path": "string",
         "Roles": [{
          "Arn": "string",
          "AssumeRolePolicyDocument": "string",
          "CreateDate": "string",
          "Path": "string",
          "RoleId": "string",
          "RoleName": "string"
         }]
        }],
```

```
        "MaxSessionDuration": number,
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
        },
        "RoleId": "string",
        "RoleName": "string",
        "RolePolicyList": [{
         "PolicyName": "string"
        }]
       },
       "AwsIamUser": {
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "GroupList": ["string"],
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
        },
        "UserId": "string",
        "UserName": "string",
        "UserPolicyList": [{
         "PolicyName": "string"
        }]
       },
       "AwsKinesisStream": {
        "Arn": "string",
        "Name": "string",
        "RetentionPeriodHours": number,
        "ShardCount": number,
        "StreamEncryption": {
         "EncryptionType": "string",
         "KeyId": "string"
        }
       },
       "AwsKmsKey": {
        "AWSAccountId": "string",
        "CreationDate": "string",
        "Description": "string",
```

```
        "KeyId": "string",
        "KeyManager": "string",
        "KeyRotationStatus": boolean,
        "KeyState": "string",
        "Origin": "string"
       },
       "AwsLambdaFunction": {
        "Architectures": [
         "string"
        ],
        "Code": {
         "S3Bucket": "string",
         "S3Key": "string",
         "S3ObjectVersion": "string",
         "ZipFile": "string"
        },
        "CodeSha256": "string",
        "DeadLetterConfig": {
         "TargetArn": "string"
        },
        "Environment": {
         "Variables": {
          "Stage": "string"
         },
         "Error": {
          "ErrorCode": "string",
          "Message": "string"
         }
        },
        "FunctionName": "string",
        "Handler": "string",
        "KmsKeyArn": "string",
        "LastModified": "string",
        "Layers": {
         "Arn": "string",
         "CodeSize": number
        },
        "PackageType": "string",
        "RevisionId": "string",
        "Role": "string",
        "Runtime": "string",
        "Timeout": integer,
        "TracingConfig": {
         "Mode": "string"
```

```
        },
        "Version": "string",
        "VpcConfig": {
         "SecurityGroupIds": ["string"],
         "SubnetIds": ["string"]
        },
        "MasterArn": "string",
        "MemorySize": number
       },
       "AwsLambdaLayerVersion": {
        "CompatibleRuntimes": [
         "string"
        ],
        "CreatedDate": "string",
        "Version": number
       },
       "AwsMskCluster": {
        "ClusterInfo": {
         "ClientAuthentication": {
          "Sasl": {
           "Scram": {
            "Enabled": boolean
           },
           "Iam": {
            "Enabled": boolean
           }
          },
          "Tls": {
           "CertificateAuthorityArnList": [],
           "Enabled": boolean
          },
          "Unauthenticated": {
           "Enabled": boolean
          }
         },
         "ClusterName": "string",
         "CurrentVersion": "string",
         "EncryptionInfo": {
          "EncryptionAtRest": {
           "DataVolumeKMSKeyId": "string"
          },
          "EncryptionInTransit": {
           "ClientBroker": "string",
           "InCluster": boolean
```

```
          }
         },
         "EnhancedMonitoring": "string",
         "NumberOfBrokerNodes": integer
        }
       },
       "AwsNetworkFirewallFirewall": {
        "DeleteProtection": boolean,
        "Description": "string",
        "FirewallArn": "string",
        "FirewallId": "string",
        "FirewallName": "string",
        "FirewallPolicyArn": "string",
        "FirewallPolicyChangeProtection": boolean,
        "SubnetChangeProtection": boolean,
        "SubnetMappings": [{
         "SubnetId": "string"
        }],
        "VpcId": "string"
       },
       "AwsNetworkFirewallFirewallPolicy": {
        "Description": "string",
        "FirewallPolicy": {
         "StatefulRuleGroupReferences": [{
          "ResourceArn": "string"
         }],
         "StatelessCustomActions": [{
          "ActionDefinition": {
           "PublishMetricAction": {
            "Dimensions": [{
             "Value": "string"
            }]
           }
          },
          "ActionName": "string"
         }],
         "StatelessDefaultActions": ["string"],
         "StatelessFragmentDefaultActions": ["string"],
         "StatelessRuleGroupReferences": [{
          "Priority": number,
          "ResourceArn": "string"
         }]
        },
        "FirewallPolicyArn": "string",
```

```
        "FirewallPolicyId": "string",
        "FirewallPolicyName": "string"
      },
      "AwsNetworkFirewallRuleGroup": {
        "Capacity": number,
        "Description": "string",
        "RuleGroup": {
          "RulesSource": {
            "RulesSourceList": {
              "GeneratedRulesType": "string",
              "Targets": ["string"],
              "TargetTypes": ["string"]
            },
            "RulesString": "string",
            "StatefulRules": [{
              "Action": "string",
              "Header": {
                "Destination": "string",
                "DestinationPort": "string",
                "Direction": "string",
                "Protocol": "string",
                "Source": "string",
                "SourcePort": "string"
              },
              "RuleOptions": [{
                "Keyword": "string",
                "Settings": ["string"]
              }]
            }],
            "StatelessRulesAndCustomActions": {
              "CustomActions": [{
                "ActionDefinition": {
                  "PublishMetricAction": {
                    "Dimensions": [{
                      "Value": "string"
                    }]
                  }
                },
                "ActionName": "string"
              }],
              "StatelessRules": [{
                "Priority": number,
                "RuleDefinition": {
                  "Actions": ["string"],
```

```
            "MatchAttributes": {
             "DestinationPorts": [{
              "FromPort": number,
              "ToPort": number
             }],
             "Destinations": [{
              "AddressDefinition": "string"
             }],
             "Protocols": [number],
             "SourcePorts": [{
              "FromPort": number,
              "ToPort": number
             }],
             "Sources": [{
              "AddressDefinition": "string"
             }],
             "TcpFlags": [{
              "Flags": ["string"],
              "Masks": ["string"]
             }]
            }
           }
          }]
         }
        },
        "RuleVariables": {
         "IpSets": {
          "Definition": ["string"]
         },
         "PortSets": {
          "Definition": ["string"]
         }
        }
       },
       "RuleGroupArn": "string",
       "RuleGroupId": "string",
       "RuleGroupName": "string",
       "Type": "string"
      },
      "AwsOpenSearchServiceDomain": {
       "AccessPolicies": "string",
       "AdvancedSecurityOptions": {
        "Enabled": boolean,
        "InternalUserDatabaseEnabled": boolean,
```

```
          "MasterUserOptions": {
           "MasterUserArn": "string",
           "MasterUserName": "string",
           "MasterUserPassword": "string"
          }
         },
         "Arn": "string",
         "ClusterConfig": {
          "DedicatedMasterCount": number,
          "DedicatedMasterEnabled": boolean,
          "DedicatedMasterType": "string",
          "InstanceCount": number,
          "InstanceType": "string",
          "WarmCount": number,
          "WarmEnabled": boolean,
          "WarmType": "string",
          "ZoneAwarenessConfig": {
           "AvailabilityZoneCount": number
          },
          "ZoneAwarenessEnabled": boolean
         },
         "DomainEndpoint": "string",
         "DomainEndpointOptions": {
          "CustomEndpoint": "string",
          "CustomEndpointCertificateArn": "string",
          "CustomEndpointEnabled": boolean,
          "EnforceHTTPS": boolean,
          "TLSSecurityPolicy": "string"
         },
         "DomainEndpoints": {
          "string": "string"
         },
         "DomainName": "string",
         "EncryptionAtRestOptions": {
          "Enabled": boolean,
          "KmsKeyId": "string"
         },
         "EngineVersion": "string",
         "Id": "string",
         "LogPublishingOptions": {
          "AuditLogs": {
           "CloudWatchLogsLogGroupArn": "string",
           "Enabled": boolean
          },
```

```
        "IndexSlowLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        },
        "SearchSlowLogs": {
         "CloudWatchLogsLogGroupArn": "string",
         "Enabled": boolean
        }
       },
       "NodeToNodeEncryptionOptions": {
        "Enabled": boolean
       },
       "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "string",
        "Cancellable": boolean,
        "CurrentVersion": "string",
        "Description": "string",
        "NewVersion": "string",
        "OptionalDeployment": boolean,
        "UpdateAvailable": boolean,
        "UpdateStatus": "string"
       },
       "VpcOptions": {
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       }
      },
      "AwsRdsDbCluster": {
       "ActivityStreamStatus": "string",
       "AllocatedStorage": number,
       "AssociatedRoles": [{
        "RoleArn": "string",
        "Status": "string"
       }],
       "AutoMinorVersionUpgrade": boolean,
       "AvailabilityZones": ["string"],
       "BackupRetentionPeriod": integer,
       "ClusterCreateTime": "string",
       "CopyTagsToSnapshot": boolean,
       "CrossAccountClone": boolean,
       "CustomEndpoints": ["string"],
       "DatabaseName": "string",
       "DbClusterIdentifier": "string",
       "DbClusterMembers": [{
```

```
          "DbClusterParameterGroupStatus": "string",
          "DbInstanceIdentifier": "string",
          "IsClusterWriter": boolean,
          "PromotionTier": integer
        }],
        "DbClusterOptionGroupMemberships": [{
          "DbClusterOptionGroupName": "string",
          "Status": "string"
        }],
        "DbClusterParameterGroup": "string",
        "DbClusterResourceId": "string",
        "DbSubnetGroup": "string",
        "DeletionProtection": boolean,
        "DomainMemberships": [{
          "Domain": "string",
          "Fqdn": "string",
          "IamRoleName": "string",
          "Status": "string"
        }],
        "EnabledCloudwatchLogsExports": ["string"],
        "Endpoint": "string",
        "Engine": "string",
        "EngineMode": "string",
        "EngineVersion": "string",
        "HostedZoneId": "string",
        "HttpEndpointEnabled": boolean,
        "IamDatabaseAuthenticationEnabled": boolean,
        "KmsKeyId": "string",
        "MasterUsername": "string",
        "MultiAz": boolean,
        "Port": integer,
        "PreferredBackupWindow": "string",
        "PreferredMaintenanceWindow": "string",
        "ReaderEndpoint": "string",
        "ReadReplicaIdentifiers": ["string"],
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcSecurityGroups": [{
          "Status": "string",
          "VpcSecurityGroupId": "string"
        }]
      },
      "AwsRdsDbClusterSnapshot": {
        "AllocatedStorage": integer,
```

```
        "AvailabilityZones": ["string"],
        "ClusterCreateTime": "string",
        "DbClusterIdentifier": "string",
        "DbClusterSnapshotAttributes": [{
         "AttributeName": "string",
         "AttributeValues": ["string"]
        }],
        "DbClusterSnapshotIdentifier": "string",
        "Engine": "string",
        "EngineVersion": "string",
        "IamDatabaseAuthenticationEnabled": boolean,
        "KmsKeyId": "string",
        "LicenseModel": "string",
        "MasterUsername": "string",
        "PercentProgress": integer,
        "Port": integer,
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcId": "string"
       },
       "AwsRdsDbInstance": {
        "AllocatedStorage": number,
        "AssociatedRoles": [{
         "RoleArn": "string",
         "FeatureName": "string",
         "Status": "string"
        }],
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZone": "string",
        "BackupRetentionPeriod": number,
        "CACertificateIdentifier": "string",
        "CharacterSetName": "string",
        "CopyTagsToSnapshot": boolean,
        "DBClusterIdentifier": "string",
        "DBInstanceClass": "string",
        "DBInstanceIdentifier": "string",
        "DbInstancePort": number,
        "DbInstanceStatus": "string",
        "DbiResourceId": "string",
        "DBName": "string",
        "DbParameterGroups": [{
         "DbParameterGroupName": "string",
```

```
          "ParameterApplyStatus": "string"
        }],
        "DbSecurityGroups": ["string"],
        "DbSubnetGroup": {
         "DbSubnetGroupArn": "string",
         "DbSubnetGroupDescription": "string",
         "DbSubnetGroupName": "string",
         "SubnetGroupStatus": "string",
         "Subnets": [{
          "SubnetAvailabilityZone": {
           "Name": "string"
          },
          "SubnetIdentifier": "string",
          "SubnetStatus": "string"
         }],
         "VpcId": "string"
        },
        "DeletionProtection": boolean,
        "Endpoint": {
         "Address": "string",
         "Port": number,
         "HostedZoneId": "string"
        },
        "DomainMemberships": [{
         "Domain": "string",
         "Fqdn": "string",
         "IamRoleName": "string",
         "Status": "string"
        }],
        "EnabledCloudwatchLogsExports": ["string"],
        "Engine": "string",
        "EngineVersion": "string",
        "EnhancedMonitoringResourceArn": "string",
        "IAMDatabaseAuthenticationEnabled": boolean,
        "InstanceCreateTime": "string",
        "Iops": number,
        "KmsKeyId": "string",
        "LatestRestorableTime": "string",
        "LicenseModel": "string",
        "ListenerEndpoint": {
         "Address": "string",
         "HostedZoneId": "string",
         "Port": number
        },
```

```
        "MasterUsername": "admin",
        "MaxAllocatedStorage": number,
        "MonitoringInterval": number,
        "MonitoringRoleArn": "string",
        "MultiAz": boolean,
        "OptionGroupMemberships": [{
         "OptionGroupName": "string",
         "Status": "string"
        }],
        "PendingModifiedValues": {
         "AllocatedStorage": number,
         "BackupRetentionPeriod": number,
         "CaCertificateIdentifier": "string",
         "DbInstanceClass": "string",
         "DbInstanceIdentifier": "string",
         "DbSubnetGroupName": "string",
         "EngineVersion": "string",
         "Iops": number,
         "LicenseModel": "string",
         "MasterUserPassword": "string",
         "MultiAZ": boolean,
         "PendingCloudWatchLogsExports": {
          "LogTypesToDisable": ["string"],
          "LogTypesToEnable": ["string"]
         },
         "Port": number,
         "ProcessorFeatures": [{
          "Name": "string",
          "Value": "string"
         }],
         "StorageType": "string"
        },
        "PerformanceInsightsEnabled": boolean,
        "PerformanceInsightsKmsKeyId": "string",
        "PerformanceInsightsRetentionPeriod": number,
        "PreferredBackupWindow": "string",
        "PreferredMaintenanceWindow": "string",
        "ProcessorFeatures": [{
         "Name": "string",
         "Value": "string"
        }],
        "PromotionTier": number,
        "PubliclyAccessible": boolean,
        "ReadReplicaDBClusterIdentifiers": ["string"],
```

```
        "ReadReplicaDBInstanceIdentifiers": ["string"],
        "ReadReplicaSourceDBInstanceIdentifier": "string",
        "SecondaryAvailabilityZone": "string",
        "StatusInfos": [{
         "Message": "string",
         "Normal": boolean,
         "Status": "string",
         "StatusType": "string"
        }],
        "StorageEncrypted": boolean,
        "TdeCredentialArn": "string",
        "Timezone": "string",
        "VpcSecurityGroups": [{
         "VpcSecurityGroupId": "string",
         "Status": "string"
        }]
       },
       "AwsRdsDbSecurityGroup": {
        "DbSecurityGroupArn": "string",
        "DbSecurityGroupDescription": "string",
        "DbSecurityGroupName": "string",
        "Ec2SecurityGroups": [{
         "Ec2SecurityGroupuId": "string",
         "Ec2SecurityGroupName": "string",
         "Ec2SecurityGroupOwnerId": "string",
         "Status": "string"
        }],
        "IpRanges": [{
         "CidrIp": "string",
         "Status": "string"
        }],
        "OwnerId": "string",
        "VpcId": "string"
       },
       "AwsRdsDbSnapshot": {
        "AllocatedStorage": integer,
        "AvailabilityZone": "string",
        "DbInstanceIdentifier": "string",
        "DbiResourceId": "string",
        "DbSnapshotIdentifier": "string",
        "Encrypted": boolean,
        "Engine": "string",
        "EngineVersion": "string",
        "IamDatabaseAuthenticationEnabled": boolean,
```

```
        "InstanceCreateTime": "string",
        "Iops": number,
        "KmsKeyId": "string",
        "LicenseModel": "string",
        "MasterUsername": "string",
        "OptionGroupName": "string",
        "PercentProgress": integer,
        "Port": integer,
        "ProcessorFeatures": [],
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
        "SourceDbSnapshotIdentifier": "string",
        "SourceRegion": "string",
        "Status": "string",
        "StorageType": "string",
        "TdeCredentialArn": "string",
        "Timezone": "string",
        "VpcId": "string"
      },
      "AwsRdsEventSubscription": {
        "CustomerAwsId": "string",
        "CustSubscriptionId": "string",
        "Enabled": boolean,
        "EventCategoriesList": ["string"],
        "EventSubscriptionArn": "string",
        "SnsTopicArn": "string",
        "SourceIdsList": ["string"],
        "SourceType": "string",
        "Status": "string",
        "SubscriptionCreationTime": "string"
      },
      "AwsRedshiftCluster": {
        "AllowVersionUpgrade": boolean,
        "AutomatedSnapshotRetentionPeriod": number,
        "AvailabilityZone": "string",
        "ClusterAvailabilityStatus": "string",
        "ClusterCreateTime": "string",
        "ClusterIdentifier": "string",
        "ClusterNodes": [{
          "NodeRole": "string",
          "PrivateIPAddress": "string",
          "PublicIPAddress": "string"
        }],
        "ClusterParameterGroups": [{
```

```
          "ClusterParameterStatusList": [{
           "ParameterApplyErrorDescription": "string",
           "ParameterApplyStatus": "string",
           "ParameterName": "string"
          }],
          "ParameterApplyStatus": "string",
          "ParameterGroupName": "string"
         }],
         "ClusterPublicKey": "string",
         "ClusterRevisionNumber": "string",
         "ClusterSecurityGroups": [{
          "ClusterSecurityGroupName": "string",
          "Status": "string"
         }],
         "ClusterSnapshotCopyStatus": {
          "DestinationRegion": "string",
          "ManualSnapshotRetentionPeriod": number,
          "RetentionPeriod": number,
          "SnapshotCopyGrantName": "string"
         },
         "ClusterStatus": "string",
         "ClusterSubnetGroupName": "string",
         "ClusterVersion": "string",
         "DBName": "string",
         "DeferredMaintenanceWindows": [{
          "DeferMaintenanceEndTime": "string",
          "DeferMaintenanceIdentifier": "string",
          "DeferMaintenanceStartTime": "string"
         }],
         "ElasticIpStatus": {
          "ElasticIp": "string",
          "Status": "string"
         },
         "ElasticResizeNumberOfNodeOptions": "string",
         "Encrypted": boolean,
         "Endpoint": {
          "Address": "string",
          "Port": number
         },
         "EnhancedVpcRouting": boolean,
         "ExpectedNextSnapshotScheduleTime": "string",
         "ExpectedNextSnapshotScheduleTimeStatus": "string",
         "HsmStatus": {
          "HsmClientCertificateIdentifier": "string",
```

```
         "HsmConfigurationIdentifier": "string",
         "Status": "string"
        },
        "IamRoles": [{
         "ApplyStatus": "string",
         "IamRoleArn": "string"
        }],
        "KmsKeyId": "string",
        "LoggingStatus":{
                    "BucketName": "string",
                    "LastFailureMessage": "string",
                    "LastFailureTime": "string",
                    "LastSuccessfulDeliveryTime": "string",
                    "LoggingEnabled": boolean,
                    "S3KeyPrefix": "string"
                 },
        "MaintenanceTrackName": "string",
        "ManualSnapshotRetentionPeriod": number,
        "MasterUsername": "string",
        "NextMaintenanceWindowStartTime": "string",
        "NodeType": "string",
        "NumberOfNodes": number,
        "PendingActions": ["string"],
        "PendingModifiedValues": {
         "AutomatedSnapshotRetentionPeriod": number,
         "ClusterIdentifier": "string",
         "ClusterType": "string",
         "ClusterVersion": "string",
         "EncryptionType": "string",
         "EnhancedVpcRouting": boolean,
         "MaintenanceTrackName": "string",
         "MasterUserPassword": "string",
         "NodeType": "string",
         "NumberOfNodes": number,
         "PubliclyAccessible": "string"
        },
        "PreferredMaintenanceWindow": "string",
        "PubliclyAccessible": boolean,
        "ResizeInfo": {
         "AllowCancelResize": boolean,
         "ResizeType": "string"
        },
        "RestoreStatus": {
         "CurrentRestoreRateInMegaBytesPerSecond": number,
```

```
          "ElapsedTimeInSeconds": number,
          "EstimatedTimeToCompletionInSeconds": number,
          "ProgressInMegaBytes": number,
          "SnapshotSizeInMegaBytes": number,
          "Status": "string"
        },
        "SnapshotScheduleIdentifier": "string",
        "SnapshotScheduleState": "string",
        "VpcId": "string",
        "VpcSecurityGroups": [{
          "Status": "string",
          "VpcSecurityGroupId": "string"
        }]
      },
      "AwsRoute53HostedZone": {
        "HostedZone": {
          "Id": "string",
          "Name": "string",
          "Config": {
            "Comment": "string"
          }
        },
        "NameServers": ["string"],
        "QueryLoggingConfig": {
          "CloudWatchLogsLogGroupArn": {
            "CloudWatchLogsLogGroupArn": "string",
            "Id": "string",
            "HostedZoneId": "string"
          }
        },
        "Vpcs": [
          {
            "Id": "string",
            "Region": "string"
          }
        ]
      },
      "AwsS3AccessPoint": {
        "AccessPointArn": "string",
        "Alias": "string",
        "Bucket": "string",
        "BucketAccountId": "string",
        "Name": "string",
        "NetworkOrigin": "string",
```

```
        "PublicAccessBlockConfiguration": {
         "BlockPublicAcls": boolean,
         "BlockPublicPolicy": boolean,
         "IgnorePublicAcls": boolean,
         "RestrictPublicBuckets": boolean
        },
        "VpcConfiguration": {
         "VpcId": "string"
        }
       },
       "AwsS3AccountPublicAccessBlock": {
        "BlockPublicAcls": boolean,
        "BlockPublicPolicy": boolean,
        "IgnorePublicAcls": boolean,
        "RestrictPublicBuckets": boolean
       },
       "AwsS3Bucket": {
        "AccessControlList": "string",
        "BucketLifecycleConfiguration": {
         "Rules": [{
          "AbortIncompleteMultipartUpload": {
           "DaysAfterInitiation": number
          },
          "ExpirationDate": "string",
          "ExpirationInDays": number,
          "ExpiredObjectDeleteMarker": boolean,
          "Filter": {
           "Predicate": {
            "Operands": [{
              "Prefix": "string",
              "Type": "string"
             },
             {
              "Tag": {
               "Key": "string",
               "Value": "string"
              },
              "Type": "string"
             }
            ],
            "Type": "string"
           }
          },
          "Id": "string",
```

```
          "NoncurrentVersionExpirationInDays": number,
          "NoncurrentVersionTransitions": [{
           "Days": number,
           "StorageClass": "string"
          }],
          "Prefix": "string",
          "Status": "string",
          "Transitions": [{
           "Date": "string",
           "Days": number,
           "StorageClass": "string"
          }]
         }]
        },
        "BucketLoggingConfiguration": {
         "DestinationBucketName": "string",
         "LogFilePrefix": "string"
        },
        "BucketName": "string",
        "BucketNotificationConfiguration": {
         "Configurations": [{
          "Destination": "string",
          "Events": ["string"],
          "Filter": {
           "S3KeyFilter": {
            "FilterRules": [{
             "Name": "string",
             "Value": "string"
            }]
           }
          },
          "Type": "string"
         }]
        },
        "BucketVersioningConfiguration": {
         "IsMfaDeleteEnabled": boolean,
         "Status": "string"
        },
        "BucketWebsiteConfiguration": {
         "ErrorDocument": "string",
         "IndexDocumentSuffix": "string",
         "RedirectAllRequestsTo": {
          "HostName": "string",
          "Protocol": "string"
```

```
          },
          "RoutingRules": [{
           "Condition": {
            "HttpErrorCodeReturnedEquals": "string",
            "KeyPrefixEquals": "string"
           },
           "Redirect": {
            "HostName": "string",
            "HttpRedirectCode": "string",
            "Protocol": "string",
            "ReplaceKeyPrefixWith": "string",
            "ReplaceKeyWith": "string"
           }
          }]
         },
         "CreatedAt": "string",
         "ObjectLockConfiguration": {
          "ObjectLockEnabled": "string",
          "Rule": {
           "DefaultRetention": {
            "Days": integer,
            "Mode": "string",
            "Years": integer
           }
          }
         },
         "OwnerAccountId": "string",
         "OwnerId": "string",
         "OwnerName": "string",
         "PublicAccessBlockConfiguration": {
          "BlockPublicAcls": boolean,
          "BlockPublicPolicy": boolean,
          "IgnorePublicAcls": boolean,
          "RestrictPublicBuckets": boolean
         },
         "ServerSideEncryptionConfiguration": {
          "Rules": [{
           "ApplyServerSideEncryptionByDefault": {
            "KMSMasterKeyID": "string",
            "SSEAlgorithm": "string"
           }
          }]
         }
        },
```

```
      "AwsS3Object": {
       "ContentType": "string",
       "ETag": "string",
       "LastModified": "string",
       "ServerSideEncryption": "string",
       "SSEKMSKeyId": "string",
       "VersionId": "string"
      },
      "AwsSagemakerNotebookInstance": {
       "DirectInternetAccess": "string",
       "InstanceMetadataServiceConfiguration": {
        "MinimumInstanceMetadataServiceVersion": "string"
       },
       "InstanceType": "string",
       "LastModifiedTime": "string",
       "NetworkInterfaceId": "string",
       "NotebookInstanceArn": "string",
       "NotebookInstanceName": "string",
       "NotebookInstanceStatus": "string",
       "PlatformIdentifier": "string",
       "RoleArn": "string",
       "RootAccess": "string",
       "SecurityGroups": ["string"],
       "SubnetId": "string",
       "Url": "string",
       "VolumeSizeInGB": number
      },
      "AwsSecretsManagerSecret": {
       "Deleted": boolean,
       "Description": "string",
       "KmsKeyId": "string",
       "Name": "string",
       "RotationEnabled": boolean,
       "RotationLambdaArn": "string",
       "RotationOccurredWithinFrequency": boolean,
       "RotationRules": {
        "AutomaticallyAfterDays": integer
       }
      },
      "AwsSnsTopic": {
       "ApplicationSuccessFeedbackRoleArn": "string",
       "FirehoseFailureFeedbackRoleArn": "string",
       "FirehoseSuccessFeedbackRoleArn": "string",
       "HttpFailureFeedbackRoleArn": "string",
```

```
        "HttpSuccessFeedbackRoleArn": "string",
        "KmsMasterKeyId": "string",
        "Owner": "string",
        "SqsFailureFeedbackRoleArn": "string",
        "SqsSuccessFeedbackRoleArn": "string",
        "Subscription": {
         "Endpoint": "string",
         "Protocol": "string"
        },
        "TopicName": "string"
       },
       "AwsSqsQueue": {
        "DeadLetterTargetArn": "string",
        "KmsDataKeyReusePeriodSeconds": number,
        "KmsMasterKeyId": "string",
        "QueueName": "string"
       },
       "AwsSsmPatchCompliance": {
        "Patch": {
         "ComplianceSummary": {
          "ComplianceType": "string",
          "CompliantCriticalCount": integer,
          "CompliantHighCount": integer,
          "CompliantInformationalCount": integer,
          "CompliantLowCount": integer,
          "CompliantMediumCount": integer,
          "CompliantUnspecifiedCount": integer,
          "ExecutionType": "string",
          "NonCompliantCriticalCount": integer,
          "NonCompliantHighCount": integer,
          "NonCompliantInformationalCount": integer,
          "NonCompliantLowCount": integer,
          "NonCompliantMediumCount": integer,
          "NonCompliantUnspecifiedCount": integer,
          "OverallSeverity": "string",
          "PatchBaselineId": "string",
          "PatchGroup": "string",
          "Status": "string"
         }
        }
       },
       "AwsStepFunctionStateMachine": {
        "StateMachineArn": "string",
        "Name": "string",
```

```
        "Status": "string",
        "RoleArn": "string",
        "Type": "string",
        "LoggingConfiguration": {
         "Level": "string",
         "IncludeExecutionData": boolean
        },
        "TracingConfiguration": {
         "Enabled": boolean
        }
       },
       "AwsWafRateBasedRule": {
        "MatchPredicates": [{
         "DataId": "string",
         "Negated": boolean,
         "Type": "string"
        }],
        "MetricName": "string",
        "Name": "string",
        "RateKey": "string",
        "RateLimit": number,
        "RuleId": "string"
       },
       "AwsWafRegionalRateBasedRule": {
        "MatchPredicates": [{
         "DataId": "string",
         "Negated": boolean,
         "Type": "string"
        }],
        "MetricName": "string",
        "Name": "string",
        "RateKey": "string",
        "RateLimit": number,
        "RuleId": "string"
       },
       "AwsWafRegionalRule": {
        "MetricName": "string",
        "Name": "string",
        "RuleId": "string",
        "PredicateList": [{
            "DataId": "string",
            "Negated": boolean,
            "Type": "string"
        }]
```

```
      },
      "AwsWafRegionalRuleGroup": {
       "MetricName": "string",
       "Name": "string",
       "RuleGroupId": "string",
       "Rules": [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }]
      },
      "AwsWafRegionalWebAcl": {
       "DefaultAction": "string",
       "MetricName" : "string",
       "Name": "string",
       "RulesList" : [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string",
        "ExcludedRules": [{
         "ExclusionType": "string",
         "RuleId": "string"
        }],
        "OverrideAction": {
         "Type": "string"
        }
       }],
       "WebAclId": "string"
      },
      "AwsWafRule": {
       "MetricName": "string",
       "Name": "string",
       "PredicateList": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
       }],
       "RuleId": "string"
```

```
      },
      "AwsWafRuleGroup": {
       "MetricName": "string",
       "Name": "string",
       "RuleGroupId": "string",
       "Rules": [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }]
      },
      "AwsWafv2RuleGroup": {
       "Arn": "string",
       "Capacity": number,
       "Description": "string",
       "Id": "string",
       "Name": "string",
       "Rules": [{
        "Action": {
        "Allow": {
         "CustomRequestHandling": {
          "InsertHeaders": [
           {
           "Name": "string",
           "Value": "string"
           },
           {
           "Name": "string",
           "Value": "string"
           }
          ]
         }
        }
        },
        "Name": "string",
        "Priority": number,
        "VisibilityConfig": {
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string",
         "SampledRequestsEnabled": boolean
        }
```

```
        }],
        "VisibilityConfig": {
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string",
         "SampledRequestsEnabled": boolean
        }
       },
       "AwsWafWebAcl": {
        "DefaultAction": "string",
        "Name": "string",
        "Rules": [{
         "Action": {
          "Type": "string"
         },
         "ExcludedRules": [{
          "RuleId": "string"
         }],
         "OverrideAction": {
          "Type": "string"
         },
         "Priority": number,
         "RuleId": "string",
         "Type": "string"
        }],
        "WebAclId": "string"
       },
       "AwsWafv2WebAcl": {
        "Arn": "string",
        "Capacity": number,
        "CaptchaConfig": {
         "ImmunityTimeProperty": {
          "ImmunityTime": number
         }
        },
        "DefaultAction": {
         "Block": {}
        },
        "Description": "string",
        "ManagedbyFirewallManager": boolean,
        "Name": "string",
        "Rules": [{
         "Action": {
          "RuleAction": {
           "Block": {}
```

```
          }
         },
         "Name": "string",
         "Priority": number,
         "VisibilityConfig": {
          "SampledRequestsEnabled": boolean,
          "CloudWatchMetricsEnabled": boolean,
          "MetricName": "string"
         }
        }],
        "VisibilityConfig": {
         "SampledRequestsEnabled": boolean,
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string"
        }
       },
       "AwsXrayEncryptionConfig": {
        "KeyId": "string",
        "Status": "string",
        "Type": "string"
       },
       "CodeRepository": {
        "CodeSecurityIntegrationArn": "string",
        "ProjectName": "string",
        "ProviderType": "string"
       },
       "Container": {
        "ContainerRuntime": "string",
        "ImageId": "string",
        "ImageName": "string",
        "LaunchedAt": "string",
        "Name": "string",
        "Privileged": boolean,
        "VolumeMounts": [{
         "Name": "string",
         "MountPath": "string"
        }]
       },
       "Other": {
        "string": "string"
       },
       "Id": "string",
       "Partition": "string",
       "Region": "string",
```

```
      "ResourceRole": "string",
      "Tags": {
       "string": "string"
      },
      "Type": "string"
     }],
     "SchemaVersion": "string",
     "Severity": {
      "Label": "string",
      "Normalized": number,
      "Original": "string"
     },
     "Sample": boolean,
     "SourceUrl": "string",
     "Threats": [{
      "FilePaths": [{
       "FileName": "string",
       "FilePath": "string",
       "Hash": "string",
       "ResourceId": "string"
      }],
      "ItemCount": number,
      "Name": "string",
      "Severity": "string"
     }],
     "ThreatIntelIndicators": [{
      "Category": "string",
      "LastObservedAt": "string",
      "Source": "string",
      "SourceUrl": "string",
      "Type": "string",
      "Value": "string"
     }],
     "Title": "string",
     "Types": ["string"],
     "UpdatedAt": "string",
     "UserDefinedFields": {
      "string": "string"
     },
     "VerificationState": "string",
     "Vulnerabilities": [{
      "CodeVulnerabilities": [{
       "Cwes": [
        "string",
```

```
          "string"
         ],
         "FilePath": {
          "EndLine": integer,
          "FileName": "string",
          "FilePath": "string",
          "StartLine": integer
         },
         "SourceArn":"string"
        }],
        "Cvss": [{
         "Adjustments": [{
          "Metric": "string",
          "Reason": "string"
         }],
         "BaseScore": number,
         "BaseVector": "string",
         "Source": "string",
         "Version": "string"
        }],
        "EpssScore": number,
        "ExploitAvailable": "string",
        "FixAvailable": "string",
        "Id": "string",
        "LastKnownExploitAt": "string",
        "ReferenceUrls": ["string"],
        "RelatedVulnerabilities": ["string"],
        "Vendor": {
         "Name": "string",
         "Url": "string",
         "VendorCreatedAt": "string",
         "VendorSeverity": "string",
         "VendorUpdatedAt": "string"
        },
        "VulnerablePackages": [{
         "Architecture": "string",
         "Epoch": "string",
         "FilePath": "string",
         "FixedInVersion": "string",
         "Name": "string",
         "PackageManager": "string",
         "Release": "string",
         "Remediation": "string",
         "SourceLayerArn": "string",
```

```
        "SourceLayerHash": "string",
        "Version": "string"
       }]
      }],
      "Workflow": {
       "Status": "string"
      },
      "WorkflowState": "string"
     }
]
```

ASFF フィールドと値への統合の影響

AWS Security Hub CSPM は、コントロールに 2 種類の統合を提供します。

- 統合コントロールビュー – このタイプの統合では、各コントロールにはすべての標準で単一の識別子があります。さらに、Security Hub CSPM コンソールの「コントロール」ページには、すべての標準におけるすべてのコントロールが表示されます。
- 統合されたコントロールの検出結果 – このタイプの統合では、コントロールが複数の有効な標準に適用されていても、Security Hub CSPM はコントロールに対して 1 つの検出結果を生成します。これにより、検出結果のノイズを減らすことができます。

統合コントロールビューを有効または無効にすることはできません。2023 年 2 月 23 日以降に Security Hub CSPM を有効にすると、統合コントロールの検出結果はデフォルトで有効になります。それ以外の場合は、デフォルトで無効になっています。ただし、組織の場合、Security Hub CSPM メンバーアカウントで統合コントロールの検出結果は、管理者アカウントで有効になっている場合にのみ有効になります。統合コントロールの検出結果の詳細については、「」を参照してくださいコントロールの結果を生成および更新する。

どちらのタイプの統合も、 のコントロール結果のフィールドと値に影響しますAWS Security Finding 形式 (ASFF)。

トピック

- 統合コントロールビュー — ASFF の変更
- 統合されたコントロールの検出結果 — ASFF の変更
- 統合コントロールの検出結果を有効にする前後のジェネレータIDs
- 統合がコントロール ID とタイトルに与える影響
- 統合に向けたワークフローの更新

統合コントロールビュー — ASFF の変更

統合コントロールビュー機能では、ASFF のコントロール結果のフィールドと値に次の変更が導入されました。ワークフローがこれらの ASFF フィールドの値に依存していない場合、アクションは必要ありません。これらのフィールドの特定の値に依存するワークフローがある場合は、現在の値を使用するようにワークフローを更新します。

ASFF フィールド	統合コントロールビューのリリース前のサンプル値	統合コントロールビュー後のサンプル値と変更の説明
Compliance.SecurityControlId	該当なし (新しいフィールド)	EC2.2 標準全体で単一のコントロール ID を導入します。`ProductFields.RuleId` は、CIS v1.2.0 コントロールに引き続き標準ベースのコントロール ID を提供します。`ProductFields.ControlId` は、他の標準のコントロールについて、引き続き標準ベースのコントロール ID を提供します。
Compliance.AssociatedStandards	該当なし (新しいフィールド)	[{「StandardsId」:「standards/aws-foundational-security-best-practices/v/1.0.0」}] コントロールが有効になっている標準を示します。
ProductFields.ArchivalReasons:0/Description	該当なし (新しいフィールド)	「統合統制結果がオンまたはオフになっているため、結果はアーカイブ済み状態になっています。これにより、新しい結果が生成されるときに、

ASFF フィールド	統合コントロールビューのリリース前のサンプル値	統合コントロールビュー後のサンプル値と変更の説明
		以前の状態の結果がアーカイブされます。」 Security Hub CSPM が既存の検出結果をアーカイブした理由について説明します。
ProductFields.ArchivalReasons:0/ReasonCode	該当なし (新しいフィールド)	「統合統制結果更新」 Security Hub CSPM が既存の検出結果をアーカイブした理由を示します。
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation このフィールドは標準を参照しないようになりました。
Remediation.Recommendation.Text	「この問題を修正する方法については、 AWS Security Hub CSPM PCI DSS ドキュメントを参照してください。」	「この問題を修正する方法については、 AWS Security Hub CSPM コントロールのドキュメントを参照してください。」 このフィールドは標準を参照しないようになりました。
Remediation.Recommendation.Url	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation このフィールドは標準を参照しないようになりました。

統合されたコントロールの検出結果 — ASFF の変更

統合コントロールの検出結果を有効にすると、ASFF のコントロールの検出結果のフィールドと値に対する以下の変更の影響を受ける可能性があります。これらの変更は、統合コントロールビュー機能によって導入された変更に加えて行われます。ワークフローがこれらの ASFF フィールドの値に依存していない場合、アクションは必要ありません。これらのフィールドの特定の値に依存するワークフローがある場合は、現在の値を使用するようにワークフローを更新します。

> **Tip**
>
> v2.0.0 AWS での自動化されたセキュリティ対応ソリューションを使用する場合は、統合コントロールの検出結果をサポートしていることに注意してください。つまり、統合コントロールの検出結果を有効にすると、現在のワークフローを維持できます。

ASFF フィールド	統合コントロールの検出結果を有効にする前の値の例	統合コントロールの検出結果を有効にした後の値の例と変更の説明
GeneratorId	aws-foundational-security-best-practices/v/1.0.0/Config.1	security-control/Config.1 このフィールドは標準を参照しないようになりました。
タイトル	PCI.Config.1 AWS Config を有効にする必要があります	AWS Config を有効にする必要があります このフィールドでは、標準固有の情報は参照されなくなりました。
ID	arn:aws:securityhub:eu-central-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.IAM.5/finding/ab6d6a26-a156-48f0-9403-115983e5a956	arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/ab6d6a26-a156-48f0-9403-115983e5a956 このフィールドは標準を参照しないようになりました。

ASFF フィールド	統合コントロールの検出結果を有効にする前の値の例	統合コントロールの検出結果を有効にした後の値の例と変更の説明
ProductFields.ControlId	PCI.EC2.2	Removed。代わりに `Compliance.SecurityControlId` を参照してください。 このフィールドは削除され、標準にとらわれない単一のコントロール ID が優先されます。
ProductFields.RuleId	1.3	Removed。代わりに `Compliance.SecurityControlId` を参照してください。 このフィールドは削除され、標準にとらわれない単一のコントロール ID が優先されます。
説明	この PCI DSS コントロール AWS Config は、現在のアカウントとリージョンで が有効になっているかどうかをチェックします。	この AWS コントロール AWS Config は、現在のアカウントとリージョンで が有効になっているかどうかを確認します。 このフィールドは標準を参照しないようになりました。

緊急度	"Severity": {
	
	"Product": 90,
	
	"Label": "CRITICAL",
	
	"Normalized": 90,
	
	"Original": "CRITICAL"
	
	}
		"Severity": {
		
		"Label": "CRITICAL",
		
		"Normalized": 90,
		
		"Original": "CRITICAL"
		
		}
		
		Security Hub CSPM は、Product フィールドを使用して検出結果の重要度を記述しなくなりました。

ASFF フィールド	統合コントロールの検出結果を有効にする前の値の例	統合コントロールの検出結果を有効にした後の値の例と変更の説明
型	["Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"]	["Software and Configuration Checks/Industry and Regulatory Standards"] このフィールドは標準を参照しないようになりました。
Compliance.RelatedRequirements	["PCI DSS 10.5.2", "PCI DSS 11.5", 「CIS AWS Foundations 2.5」〕	["PCI DSS v3.2.1/10.5.2", "PCI DSS v3.2.1/11.5", 「CIS AWS Foundations Benchmark v1.2.0/2.5」〕 このフィールドには、有効なすべての標準の関連要件が表示されます。
CreatedAt	2022-05-05T08:18:13.138Z	2022-09-25T08:18:13.138Z 形式は変わりませんが、統合コントロールの検出結果を有効にすると値がリセットされます。
FirstObservedAt	2022-05-07T08:18:13.138Z	2022-09-28T08:18:13.138Z 形式は変わりませんが、統合コントロールの検出結果を有効にすると値がリセットされます。
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation	Removed。代わりに `Remediation.Recommendation.Url` を参照してください。
ProductFields.StandardsArn	arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0	Removed。代わりに `Compliance.AssociatedStandards` を参照してください。

ASFF フィールド	統合コントロールの検出結果を有効にする前の値の例	統合コントロールの検出結果を有効にした後の値の例と変更の説明
ProductFields.StandardsControlArn	arn:aws:securityhub:us-east-1:123456789012:control/aws-foundational-security-best-practices/v/1.0.0/Config.1	Removed。Security Hub CSPM は、標準間のセキュリティチェック用に 1 つの検出結果を生成します。
ProductFields.StandardsGuideArn	arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0	Removed。代わりに `Compliance.AssociatedStandards` を参照してください。
ProductFields.StandardsGuideSubscriptionArn	arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0	Removed。Security Hub CSPM は、標準間のセキュリティチェック用に 1 つの検出結果を生成します。
ProductFields.StandardsSubscriptionArn	arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0	Removed。Security Hub CSPM は、標準間のセキュリティチェック用に 1 つの検出結果を生成します。
ProductFields.aws/securityhub/FindingId	arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0/Config.1/finding/751c2173-7372-4e12-8656-a5210dfb1d67	arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/Config.1/finding/751c2173-7372-4e12-8656-a5210dfb1d67 このフィールドは標準を参照しないようになりました。

[統合されたコントロールの検出結果] を有効にした後における、顧客提供の ASFF フィールドの値

統合コントロールの検出結果を有効にすると、Security Hub CSPM は標準間で 1 つの検出結果を生成し、元の検出結果 (標準ごとに個別の検出結果) をアーカイブします。

Security Hub CSPM コンソールまたは BatchUpdateFindingsオペレーションを使用して元の検出結果に加えた更新は、新しい検出結果には保持されません。必要に応じて、アーカイブされた結果を参照することで、このデータを復元できます。アーカイブされた検出結果を確認するには、Security Hub CSPM コンソールの検出結果ページを使用し、レコード状態フィルターを ARCHIVED に設定します。または、Security Hub CSPM API の GetFindingsオペレーションを使用することもできます。

顧客提供の ASFF フィールド	統合コントロールの検出結果を有効にした後の変更の説明
信頼度	空の状態にリセットされます。
緊急性	空の状態にリセットされます。
メモ	空の状態にリセットされます。
RelatedFindings	空の状態にリセットされます。
緊急度	結果のデフォルトの重要度 (コントロールの重要度と同じ)。
型	標準に依存しない値にリセットされます。
UserDefinedFields	空の状態にリセットされます。
VerificationState	空の状態にリセットされます。
ワークフロー	新たに失敗した検出結果のデフォルト値は NEW になります。新たに成功した検出結果のデフォルト値は RESOLVED になります。

統合コントロールの検出結果を有効にする前後のジェネレータIDs

次の表に、統合コントロールの検出結果を有効にするときのコントロールのジェネレーター ID 値の変更を示します。これらの変更は、2023 年 2 月 15 日の時点で Security Hub CSPM がサポートしていたコントロールに適用されます。

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.1	security-control/CloudWatch.1
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.10	security-control/IAM.16
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.11	security-control/IAM.17
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.12	security-control/IAM.4
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.13	security-control/IAM.9
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.14	security-control/IAM.6
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.16	security-control/IAM.2
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.2	security-control/IAM.5
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.20	security-control/IAM.18
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.22	security-control/IAM.1
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.3	security-control/IAM.8
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.4	security-control/IAM.3

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.5	security-control/IAM.11
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.6	security-control/IAM.12
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.7	security-control/IAM.13
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.8	security-control/IAM.14
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.9	security-control/IAM.15
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.1	security-control/CloudTrail.1
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.2	security-control/CloudTrail.4
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.3	security-control/CloudTrail.6
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.4	security-control/CloudTrail.5
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.5	security-control/Config.1
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.6	security-control/CloudTrail.7
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.7	security-control/CloudTrail.2

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.8	security-control/KMS.4
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.9	security-control/EC2.6
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.1	security-control/CloudWatch.2
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.2	security-control/CloudWatch.3
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.3	security-control/CloudWatch.1
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.4	security-control/CloudWatch.4
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.5	security-control/CloudWatch.5
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.6	security-control/CloudWatch.6
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.7	security-control/CloudWatch.7
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.8	security-control/CloudWatch.8
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.9	security-control/CloudWatch.9
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.10	security-control/CloudWatch.10

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.11	security-control/CloudWatch.11
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.12	security-control/CloudWatch.12
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.13	security-control/CloudWatch.13
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.14	security-control/CloudWatch.14
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/4.1	security-control/EC2.13
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/4.2	security-control/EC2.14
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/4.3	security-control/EC2.2
cis-aws-foundations-benchmark/v/1.4.0/1.10	security-control/IAM.5
cis-aws-foundations-benchmark/v/1.4.0/1.14	security-control/IAM.3
cis-aws-foundations-benchmark/v/1.4.0/1.16	security-control/IAM.1
cis-aws-foundations-benchmark/v/1.4.0/1.17	security-control/IAM.18
cis-aws-foundations-benchmark/v/1.4.0/1.4	security-control/IAM.4
cis-aws-foundations-benchmark/v/1.4.0/1.5	security-control/IAM.9
cis-aws-foundations-benchmark/v/1.4.0/1.6	security-control/IAM.6
cis-aws-foundations-benchmark/v/1.4.0/1.7	security-control/CloudWatch.1
cis-aws-foundations-benchmark/v/1.4.0/1.8	security-control/IAM.15

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
cis-aws-foundations-benchmark/v/1.4.0/1.9	security-control/IAM.16
cis-aws-foundations-benchmark/v/1.4.0/2.1.2	security-control/S3.5
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.1	security-control/S3.1
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.2	security-control/S3.8
cis-aws-foundations-benchmark/v/1.4.0/2.2.1	security-control/EC2.7
cis-aws-foundations-benchmark/v/1.4.0/2.3.1	security-control/RDS.3
cis-aws-foundations-benchmark/v/1.4.0/3.1	security-control/CloudTrail.1
cis-aws-foundations-benchmark/v/1.4.0/3.2	security-control/CloudTrail.4
cis-aws-foundations-benchmark/v/1.4.0/3.4	security-control/CloudTrail.5
cis-aws-foundations-benchmark/v/1.4.0/3.5	security-control/Config.1
cis-aws-foundations-benchmark/v/1.4.0/3.6	security-control/S3.9
cis-aws-foundations-benchmark/v/1.4.0/3.7	security-control/CloudTrail.2
cis-aws-foundations-benchmark/v/1.4.0/3.8	security-control/KMS.4
cis-aws-foundations-benchmark/v/1.4.0/3.9	security-control/EC2.6
cis-aws-foundations-benchmark/v/1.4.0/4.3	security-control/CloudWatch.1
cis-aws-foundations-benchmark/v/1.4.0/4.4	security-control/CloudWatch.4
cis-aws-foundations-benchmark/v/1.4.0/4.5	security-control/CloudWatch.5
cis-aws-foundations-benchmark/v/1.4.0/4.6	security-control/CloudWatch.6
cis-aws-foundations-benchmark/v/1.4.0/4.7	security-control/CloudWatch.7
cis-aws-foundations-benchmark/v/1.4.0/4.8	security-control/CloudWatch.8

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
cis-aws-foundations-benchmark/v/1.4.0/4.9	security-control/CloudWatch.9
cis-aws-foundations-benchmark/v/1.4.0/4.10	security-control/CloudWatch.10
cis-aws-foundations-benchmark/v/1.4.0/4.11	security-control/CloudWatch.11
cis-aws-foundations-benchmark/v/1.4.0/4.12	security-control/CloudWatch.12
cis-aws-foundations-benchmark/v/1.4.0/4.13	security-control/CloudWatch.13
cis-aws-foundations-benchmark/v/1.4.0/4.14	security-control/CloudWatch.14
cis-aws-foundations-benchmark/v/1.4.0/5.1	security-control/EC2.21
cis-aws-foundations-benchmark/v/1.4.0/5.3	security-control/EC2.2
aws-foundational-security-best-practices/v/1.0.0/Account.1	security-control/Account.1
aws-foundational-security-best-practices/v/1.0.0/ACM.1	security-control/ACM.1
aws-foundational-security-best-practices/v/1.0.0/APIGateway.1	security-control/APIGateway.1
aws-foundational-security-best-practices/v/1.0.0/APIGateway.2	security-control/APIGateway.2
aws-foundational-security-best-practices/v/1.0.0/APIGateway.3	security-control/APIGateway.3
aws-foundational-security-best-practices/v/1.0.0/APIGateway.4	security-control/APIGateway.4
aws-foundational-security-best-practices/v/1.0.0/APIGateway.5	security-control/APIGateway.5

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/APIGateway.8	security-control/APIGateway.8
aws-foundational-security-best-practices/v/1.0.0/APIGateway.9	security-control/APIGateway.9
aws-foundational-security-best-practices/v/1.0.0/AutoScaling.1	security-control/AutoScaling.1
aws-foundational-security-best-practices/v/1.0.0/AutoScaling.2	security-control/AutoScaling.2
aws-foundational-security-best-practices/v/1.0.0/AutoScaling.3	security-control/AutoScaling.3
aws-foundational-security-best-practices/v/1.0.0/Autoscaling.5	security-control/Autoscaling.5
aws-foundational-security-best-practices/v/1.0.0/AutoScaling.6	security-control/AutoScaling.6
aws-foundational-security-best-practices/v/1.0.0/AutoScaling.9	security-control/AutoScaling.9
aws-foundational-security-best-practices/v/1.0.0/CloudFront.1	security-control/CloudFront.1
aws-foundational-security-best-practices/v/1.0.0/CloudFront.3	security-control/CloudFront.3
aws-foundational-security-best-practices/v/1.0.0/CloudFront.4	security-control/CloudFront.4
aws-foundational-security-best-practices/v/1.0.0/CloudFront.5	security-control/CloudFront.5

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/CloudFront.6	security-control/CloudFront.6
aws-foundational-security-best-practices/v/1.0.0/CloudFront.7	security-control/CloudFront.7
aws-foundational-security-best-practices/v/1.0.0/CloudFront.8	security-control/CloudFront.8
aws-foundational-security-best-practices/v/1.0.0/CloudFront.9	security-control/CloudFront.9
aws-foundational-security-best-practices/v/1.0.0/CloudFront.10	security-control/CloudFront.10
aws-foundational-security-best-practices/v/1.0.0/CloudFront.12	security-control/CloudFront.12
aws-foundational-security-best-practices/v/1.0.0/CloudTrail.1	security-control/CloudTrail.1
aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2	security-control/CloudTrail.2
aws-foundational-security-best-practices/v/1.0.0/CloudTrail.4	security-control/CloudTrail.4
aws-foundational-security-best-practices/v/1.0.0/CloudTrail.5	security-control/CloudTrail.5
aws-foundational-security-best-practices/v/1.0.0/CodeBuild.1	security-control/CodeBuild.1
aws-foundational-security-best-practices/v/1.0.0/CodeBuild.2	security-control/CodeBuild.2

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/CodeBuild.3	security-control/CodeBuild.3
aws-foundational-security-best-practices/v/1.0.0/CodeBuild.4	security-control/CodeBuild.4
aws-foundational-security-best-practices/v/1.0.0/Config.1	security-control/Config.1
aws-foundational-security-best-practices/v/1.0.0/DMS.1	security-control/DMS.1
aws-foundational-security-best-practices/v/1.0.0/DynamoDB.1	security-control/DynamoDB.1
aws-foundational-security-best-practices/v/1.0.0/DynamoDB.2	security-control/DynamoDB.2
aws-foundational-security-best-practices/v/1.0.0/DynamoDB.3	security-control/DynamoDB.3
aws-foundational-security-best-practices/v/1.0.0/EC2.1	security-control/EC2.1
aws-foundational-security-best-practices/v/1.0.0/EC2.3	security-control/EC2.3
aws-foundational-security-best-practices/v/1.0.0/EC2.4	security-control/EC2.4
aws-foundational-security-best-practices/v/1.0.0/EC2.6	security-control/EC2.6
aws-foundational-security-best-practices/v/1.0.0/EC2.7	security-control/EC2.7

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/EC2.8	security-control/EC2.8
aws-foundational-security-best-practices/v/1.0.0/EC2.9	security-control/EC2.9
aws-foundational-security-best-practices/v/1.0.0/EC2.10	security-control/EC2.10
aws-foundational-security-best-practices/v/1.0.0/EC2.15	security-control/EC2.15
aws-foundational-security-best-practices/v/1.0.0/EC2.16	security-control/EC2.16
aws-foundational-security-best-practices/v/1.0.0/EC2.17	security-control/EC2.17
aws-foundational-security-best-practices/v/1.0.0/EC2.18	security-control/EC2.18
aws-foundational-security-best-practices/v/1.0.0/EC2.19	security-control/EC2.19
aws-foundational-security-best-practices/v/1.0.0/EC2.2	security-control/EC2.2
aws-foundational-security-best-practices/v/1.0.0/EC2.20	security-control/EC2.20
aws-foundational-security-best-practices/v/1.0.0/EC2.21	security-control/EC2.21
aws-foundational-security-best-practices/v/1.0.0/EC2.23	security-control/EC2.23

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/EC2.24	security-control/EC2.24
aws-foundational-security-best-practices/v/1.0.0/EC2.25	security-control/EC2.25
aws-foundational-security-best-practices/v/1.0.0/ECR.1	security-control/ECR.1
aws-foundational-security-best-practices/v/1.0.0/ECR.2	security-control/ECR.2
aws-foundational-security-best-practices/v/1.0.0/ECR.3	security-control/ECR.3
aws-foundational-security-best-practices/v/1.0.0/ECS.1	security-control/ECS.1
aws-foundational-security-best-practices/v/1.0.0/ECS.10	security-control/ECS.10
aws-foundational-security-best-practices/v/1.0.0/ECS.12	security-control/ECS.12
aws-foundational-security-best-practices/v/1.0.0/ECS.2	security-control/ECS.2
aws-foundational-security-best-practices/v/1.0.0/ECS.3	security-control/ECS.3
aws-foundational-security-best-practices/v/1.0.0/ECS.4	security-control/ECS.4
aws-foundational-security-best-practices/v/1.0.0/ECS.5	security-control/ECS.5

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/ECS.8	security-control/ECS.8
aws-foundational-security-best-practices/v/1.0.0/EFS.1	security-control/EFS.1
aws-foundational-security-best-practices/v/1.0.0/EFS.2	security-control/EFS.2
aws-foundational-security-best-practices/v/1.0.0/EFS.3	security-control/EFS.3
aws-foundational-security-best-practices/v/1.0.0/EFS.4	security-control/EFS.4
aws-foundational-security-best-practices/v/1.0.0/EKS.2	security-control/EKS.2
aws-foundational-security-best-practices/v/1.0.0/ElasticBeanstalk.1	security-control/ElasticBeanstalk.1
aws-foundational-security-best-practices/v/1.0.0/ElasticBeanstalk.2	security-control/ElasticBeanstalk.2
aws-foundational-security-best-practices/v/1.0.0/ELBv2.1	security-control/ELB.1
aws-foundational-security-best-practices/v/1.0.0/ELB.2	security-control/ELB.2
aws-foundational-security-best-practices/v/1.0.0/ELB.3	security-control/ELB.3
aws-foundational-security-best-practices/v/1.0.0/ELB.4	security-control/ELB.4

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/ELB.5	security-control/ELB.5
aws-foundational-security-best-practices/v/1.0.0/ELB.6	security-control/ELB.6
aws-foundational-security-best-practices/v/1.0.0/ELB.7	security-control/ELB.7
aws-foundational-security-best-practices/v/1.0.0/ELB.8	security-control/ELB.8
aws-foundational-security-best-practices/v/1.0.0/ELB.9	security-control/ELB.9
aws-foundational-security-best-practices/v/1.0.0/ELB.10	security-control/ELB.10
aws-foundational-security-best-practices/v/1.0.0/ELB.11	security-control/ELB.11
aws-foundational-security-best-practices/v/1.0.0/ELB.12	security-control/ELB.12
aws-foundational-security-best-practices/v/1.0.0/ELB.13	security-control/ELB.13
aws-foundational-security-best-practices/v/1.0.0/ELB.14	security-control/ELB.14
aws-foundational-security-best-practices/v/1.0.0/EMR.1	security-control/EMR.1
aws-foundational-security-best-practices/v/1.0.0/ES.1	security-control/ES.1

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/ES.2	security-control/ES.2
aws-foundational-security-best-practices/v/1.0.0/ES.3	security-control/ES.3
aws-foundational-security-best-practices/v/1.0.0/ES.4	security-control/ES.4
aws-foundational-security-best-practices/v/1.0.0/ES.5	security-control/ES.5
aws-foundational-security-best-practices/v/1.0.0/ES.6	security-control/ES.6
aws-foundational-security-best-practices/v/1.0.0/ES.7	security-control/ES.7
aws-foundational-security-best-practices/v/1.0.0/ES.8	security-control/ES.8
aws-foundational-security-best-practices/v/1.0.0/GuardDuty.1	security-control/GuardDuty.1
aws-foundational-security-best-practices/v/1.0.0/IAM.1	security-control/IAM.1
aws-foundational-security-best-practices/v/1.0.0/IAM.2	security-control/IAM.2
aws-foundational-security-best-practices/v/1.0.0/IAM.21	security-control/IAM.21
aws-foundational-security-best-practices/v/1.0.0/IAM.3	security-control/IAM.3

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/IAM.4	security-control/IAM.4
aws-foundational-security-best-practices/v/1.0.0/IAM.5	security-control/IAM.5
aws-foundational-security-best-practices/v/1.0.0/IAM.6	security-control/IAM.6
aws-foundational-security-best-practices/v/1.0.0/IAM.7	security-control/IAM.7
aws-foundational-security-best-practices/v/1.0.0/IAM.8	security-control/IAM.8
aws-foundational-security-best-practices/v/1.0.0/Kinesis.1	security-control/Kinesis.1
aws-foundational-security-best-practices/v/1.0.0/KMS.1	security-control/KMS.1
aws-foundational-security-best-practices/v/1.0.0/KMS.2	security-control/KMS.2
aws-foundational-security-best-practices/v/1.0.0/KMS.3	security-control/KMS.3
aws-foundational-security-best-practices/v/1.0.0/Lambda.1	security-control/Lambda.1
aws-foundational-security-best-practices/v/1.0.0/Lambda.2	security-control/Lambda.2
aws-foundational-security-best-practices/v/1.0.0/Lambda.5	security-control/Lambda.5

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall.3	security-control/NetworkFirewall.3
aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall.4	security-control/NetworkFirewall.4
aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall.5	security-control/NetworkFirewall.5
aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall.6	security-control/NetworkFirewall.6
aws-foundational-security-best-practices/v/1.0.0/Opensearch.1	security-control/Opensearch.1
aws-foundational-security-best-practices/v/1.0.0/Opensearch.2	security-control/Opensearch.2
aws-foundational-security-best-practices/v/1.0.0/Opensearch.3	security-control/Opensearch.3
aws-foundational-security-best-practices/v/1.0.0/Opensearch.4	security-control/Opensearch.4
aws-foundational-security-best-practices/v/1.0.0/Opensearch.5	security-control/Opensearch.5
aws-foundational-security-best-practices/v/1.0.0/Opensearch.6	security-control/Opensearch.6
aws-foundational-security-best-practices/v/1.0.0/Opensearch.7	security-control/Opensearch.7
aws-foundational-security-best-practices/v/1.0.0/Opensearch.8	security-control/Opensearch.8

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/RDS.1	security-control/RDS.1
aws-foundational-security-best-practices/v/1.0.0/RDS.10	security-control/RDS.10
aws-foundational-security-best-practices/v/1.0.0/RDS.11	security-control/RDS.11
aws-foundational-security-best-practices/v/1.0.0/RDS.12	security-control/RDS.12
aws-foundational-security-best-practices/v/1.0.0/RDS.13	security-control/RDS.13
aws-foundational-security-best-practices/v/1.0.0/RDS.14	security-control/RDS.14
aws-foundational-security-best-practices/v/1.0.0/RDS.15	security-control/RDS.15
aws-foundational-security-best-practices/v/1.0.0/RDS.16	security-control/RDS.16
aws-foundational-security-best-practices/v/1.0.0/RDS.17	security-control/RDS.17
aws-foundational-security-best-practices/v/1.0.0/RDS.19	security-control/RDS.19
aws-foundational-security-best-practices/v/1.0.0/RDS.2	security-control/RDS.2
aws-foundational-security-best-practices/v/1.0.0/RDS.20	security-control/RDS.20

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/RDS.21	security-control/RDS.21
aws-foundational-security-best-practices/v/1.0.0/RDS.22	security-control/RDS.22
aws-foundational-security-best-practices/v/1.0.0/RDS.23	security-control/RDS.23
aws-foundational-security-best-practices/v/1.0.0/RDS.24	security-control/RDS.24
aws-foundational-security-best-practices/v/1.0.0/RDS.25	security-control/RDS.25
aws-foundational-security-best-practices/v/1.0.0/RDS.3	security-control/RDS.3
aws-foundational-security-best-practices/v/1.0.0/RDS.4	security-control/RDS.4
aws-foundational-security-best-practices/v/1.0.0/RDS.5	security-control/RDS.5
aws-foundational-security-best-practices/v/1.0.0/RDS.6	security-control/RDS.6
aws-foundational-security-best-practices/v/1.0.0/RDS.7	security-control/RDS.7
aws-foundational-security-best-practices/v/1.0.0/RDS.8	security-control/RDS.8
aws-foundational-security-best-practices/v/1.0.0/RDS.9	security-control/RDS.9

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/Redshift.1	security-control/Redshift.1
aws-foundational-security-best-practices/v/1.0.0/Redshift.2	security-control/Redshift.2
aws-foundational-security-best-practices/v/1.0.0/Redshift.3	security-control/Redshift.3
aws-foundational-security-best-practices/v/1.0.0/Redshift.4	security-control/Redshift.4
aws-foundational-security-best-practices/v/1.0.0/Redshift.6	security-control/Redshift.6
aws-foundational-security-best-practices/v/1.0.0/Redshift.7	security-control/Redshift.7
aws-foundational-security-best-practices/v/1.0.0/Redshift.8	security-control/Redshift.8
aws-foundational-security-best-practices/v/1.0.0/Redshift.9	security-control/Redshift.9
aws-foundational-security-best-practices/v/1.0.0/S3.1	security-control/S3.1
aws-foundational-security-best-practices/v/1.0.0/S3.12	security-control/S3.12
aws-foundational-security-best-practices/v/1.0.0/S3.13	security-control/S3.13
aws-foundational-security-best-practices/v/1.0.0/S3.2	security-control/S3.2

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/S3.3	security-control/S3.3
aws-foundational-security-best-practices/v/1.0.0/S3.5	security-control/S3.5
aws-foundational-security-best-practices/v/1.0.0/S3.6	security-control/S3.6
aws-foundational-security-best-practices/v/1.0.0/S3.8	security-control/S3.8
aws-foundational-security-best-practices/v/1.0.0/S3.9	security-control/S3.9
aws-foundational-security-best-practices/v/1.0.0/SageMaker.1	security-control/SageMaker.1
aws-foundational-security-best-practices/v/1.0.0/SageMaker.2	security-control/SageMaker.2
aws-foundational-security-best-practices/v/1.0.0/SageMaker.3	security-control/SageMaker.3
aws-foundational-security-best-practices/v/1.0.0/SecretsManager.1	security-control/SecretsManager.1
aws-foundational-security-best-practices/v/1.0.0/SecretsManager.2	security-control/SecretsManager.2
aws-foundational-security-best-practices/v/1.0.0/SecretsManager.3	security-control/SecretsManager.3
aws-foundational-security-best-practices/v/1.0.0/SecretsManager.4	security-control/SecretsManager.4

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/SQS.1	security-control/SQS.1
aws-foundational-security-best-practices/v/1.0.0/SSM.1	security-control/SSM.1
aws-foundational-security-best-practices/v/1.0.0/SSM.2	security-control/SSM.2
aws-foundational-security-best-practices/v/1.0.0/SSM.3	security-control/SSM.3
aws-foundational-security-best-practices/v/1.0.0/SSM.4	security-control/SSM.4
aws-foundational-security-best-practices/v/1.0.0/WAF.1	security-control/WAF.1
aws-foundational-security-best-practices/v/1.0.0/WAF.2	security-control/WAF.2
aws-foundational-security-best-practices/v/1.0.0/WAF.3	security-control/WAF.3
aws-foundational-security-best-practices/v/1.0.0/WAF.4	security-control/WAF.4
aws-foundational-security-best-practices/v/1.0.0/WAF.6	security-control/WAF.6
aws-foundational-security-best-practices/v/1.0.0/WAF.7	security-control/WAF.7
aws-foundational-security-best-practices/v/1.0.0/WAF.8	security-control/WAF.8

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
aws-foundational-security-best-practices/v/1.0.0/WAF.10	security-control/WAF.10
pci-dss/v/3.2.1/PCI.AutoScaling.1	security-control/AutoScaling.1
pci-dss/v/3.2.1/PCI.CloudTrail.1	security-control/CloudTrail.2
pci-dss/v/3.2.1/PCI.CloudTrail.2	security-control/CloudTrail.3
pci-dss/v/3.2.1/PCI.CloudTrail.3	security-control/CloudTrail.4
pci-dss/v/3.2.1/PCI.CloudTrail.4	security-control/CloudTrail.5
pci-dss/v/3.2.1/PCI.CodeBuild.1	security-control/CodeBuild.1
pci-dss/v/3.2.1/PCI.CodeBuild.2	security-control/CodeBuild.2
pci-dss/v/3.2.1/PCI.Config.1	security-control/Config.1
pci-dss/v/3.2.1/PCI.CW.1	security-control/CloudWatch.1
pci-dss/v/3.2.1/PCI.DMS.1	security-control/DMS.1
pci-dss/v/3.2.1/PCI.EC2.1	security-control/EC2.1
pci-dss/v/3.2.1/PCI.EC2.2	security-control/EC2.2
pci-dss/v/3.2.1/PCI.EC2.4	security-control/EC2.12
pci-dss/v/3.2.1/PCI.EC2.5	security-control/EC2.13
pci-dss/v/3.2.1/PCI.EC2.6	security-control/EC2.6
pci-dss/v/3.2.1/PCI.ELBv2.1	security-control/ELB.1
pci-dss/v/3.2.1/PCI.ES.1	security-control/ES.2
pci-dss/v/3.2.1/PCI.ES.2	security-control/ES.1

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
pci-dss/v/3.2.1/PCI.GuardDuty.1	security-control/GuardDuty.1
pci-dss/v/3.2.1/PCI.IAM.1	security-control/IAM.4
pci-dss/v/3.2.1/PCI.IAM.2	security-control/IAM.2
pci-dss/v/3.2.1/PCI.IAM.3	security-control/IAM.1
pci-dss/v/3.2.1/PCI.IAM.4	security-control/IAM.6
pci-dss/v/3.2.1/PCI.IAM.5	security-control/IAM.9
pci-dss/v/3.2.1/PCI.IAM.6	security-control/IAM.19
pci-dss/v/3.2.1/PCI.IAM.7	security-control/IAM.8
pci-dss/v/3.2.1/PCI.IAM.8	security-control/IAM.10
pci-dss/v/3.2.1/PCI.KMS.1	security-control/KMS.4
pci-dss/v/3.2.1/PCI.Lambda.1	security-control/Lambda.1
pci-dss/v/3.2.1/PCI.Lambda.2	security-control/Lambda.3
pci-dss/v/3.2.1/PCI.Opensearch.1	security-control/Opensearch.2
pci-dss/v/3.2.1/PCI.Opensearch.2	security-control/Opensearch.1
pci-dss/v/3.2.1/PCI.RDS.1	security-control/RDS.1
pci-dss/v/3.2.1/PCI.RDS.2	security-control/RDS.2
pci-dss/v/3.2.1/PCI.Redshift.1	security-control/Redshift.1
pci-dss/v/3.2.1/PCI.S3.1	security-control/S3.3
pci-dss/v/3.2.1/PCI.S3.2	security-control/S3.2
pci-dss/v/3.2.1/PCI.S3.3	security-control/S3.7

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
pci-dss/v/3.2.1/PCI.S3.5	security-control/S3.5
pci-dss/v/3.2.1/PCI.S3.6	security-control/S3.1
pci-dss/v/3.2.1/PCI.SageMaker.1	security-control/SageMaker.1
pci-dss/v/3.2.1/PCI.SSM.1	security-control/SSM.2
pci-dss/v/3.2.1/PCI.SSM.2	security-control/SSM.3
pci-dss/v/3.2.1/PCI.SSM.3	security-control/SSM.1
service-managed-aws-control-tower/v/1.0.0/ACM.1	security-control/ACM.1
service-managed-aws-control-tower/v/1.0.0/APIGateway.1	security-control/APIGateway.1
service-managed-aws-control-tower/v/1.0.0/APIGateway.2	security-control/APIGateway.2
service-managed-aws-control-tower/v/1.0.0/APIGateway.3	security-control/APIGateway.3
service-managed-aws-control-tower/v/1.0.0/APIGateway.4	security-control/APIGateway.4
service-managed-aws-control-tower/v/1.0.0/APIGateway.5	security-control/APIGateway.5
service-managed-aws-control-tower/v/1.0.0/AutoScaling.1	security-control/AutoScaling.1
service-managed-aws-control-tower/v/1.0.0/AutoScaling.2	security-control/AutoScaling.2

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/AutoScaling.3	security-control/AutoScaling.3
service-managed-aws-control-tower/v/1.0.0/AutoScaling.4	security-control/AutoScaling.4
service-managed-aws-control-tower/v/1.0.0/Autoscaling.5	security-control/Autoscaling.5
service-managed-aws-control-tower/v/1.0.0/AutoScaling.6	security-control/AutoScaling.6
service-managed-aws-control-tower/v/1.0.0/AutoScaling.9	security-control/AutoScaling.9
service-managed-aws-control-tower/v/1.0.0/CloudTrail.1	security-control/CloudTrail.1
service-managed-aws-control-tower/v/1.0.0/CloudTrail.2	security-control/CloudTrail.2
service-managed-aws-control-tower/v/1.0.0/CloudTrail.4	security-control/CloudTrail.4
service-managed-aws-control-tower/v/1.0.0/CloudTrail.5	security-control/CloudTrail.5
service-managed-aws-control-tower/v/1.0.0/CodeBuild.1	security-control/CodeBuild.1
service-managed-aws-control-tower/v/1.0.0/CodeBuild.2	security-control/CodeBuild.2
service-managed-aws-control-tower/v/1.0.0/CodeBuild.4	security-control/CodeBuild.4

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/CodeBuild.5	security-control/CodeBuild.5
service-managed-aws-control-tower/v/1.0.0/DMS.1	security-control/DMS.1
service-managed-aws-control-tower/v/1.0.0/DynamoDB.1	security-control/DynamoDB.1
service-managed-aws-control-tower/v/1.0.0/DynamoDB.2	security-control/DynamoDB.2
service-managed-aws-control-tower/v/1.0.0/EC2.1	security-control/EC2.1
service-managed-aws-control-tower/v/1.0.0/EC2.2	security-control/EC2.2
service-managed-aws-control-tower/v/1.0.0/EC2.3	security-control/EC2.3
service-managed-aws-control-tower/v/1.0.0/EC2.4	security-control/EC2.4
service-managed-aws-control-tower/v/1.0.0/EC2.6	security-control/EC2.6
service-managed-aws-control-tower/v/1.0.0/EC2.7	security-control/EC2.7
service-managed-aws-control-tower/v/1.0.0/EC2.8	security-control/EC2.8
service-managed-aws-control-tower/v/1.0.0/EC2.9	security-control/EC2.9

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/EC2.10	security-control/EC2.10
service-managed-aws-control-tower/v/1.0.0/EC2.15	security-control/EC2.15
service-managed-aws-control-tower/v/1.0.0/EC2.16	security-control/EC2.16
service-managed-aws-control-tower/v/1.0.0/EC2.17	security-control/EC2.17
service-managed-aws-control-tower/v/1.0.0/EC2.18	security-control/EC2.18
service-managed-aws-control-tower/v/1.0.0/EC2.19	security-control/EC2.19
service-managed-aws-control-tower/v/1.0.0/EC2.20	security-control/EC2.20
service-managed-aws-control-tower/v/1.0.0/EC2.21	security-control/EC2.21
service-managed-aws-control-tower/v/1.0.0/EC2.22	security-control/EC2.22
service-managed-aws-control-tower/v/1.0.0/ECR.1	security-control/ECR.1
service-managed-aws-control-tower/v/1.0.0/ECR.2	security-control/ECR.2
service-managed-aws-control-tower/v/1.0.0/ECR.3	security-control/ECR.3

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/ECS.1	security-control/ECS.1
service-managed-aws-control-tower/v/1.0.0/ECS.2	security-control/ECS.2
service-managed-aws-control-tower/v/1.0.0/ECS.3	security-control/ECS.3
service-managed-aws-control-tower/v/1.0.0/ECS.4	security-control/ECS.4
service-managed-aws-control-tower/v/1.0.0/ECS.5	security-control/ECS.5
service-managed-aws-control-tower/v/1.0.0/ECS.8	security-control/ECS.8
service-managed-aws-control-tower/v/1.0.0/ECS.10	security-control/ECS.10
service-managed-aws-control-tower/v/1.0.0/ECS.12	security-control/ECS.12
service-managed-aws-control-tower/v/1.0.0/EFS.1	security-control/EFS.1
service-managed-aws-control-tower/v/1.0.0/EFS.2	security-control/EFS.2
service-managed-aws-control-tower/v/1.0.0/EFS.3	security-control/EFS.3
service-managed-aws-control-tower/v/1.0.0/EFS.4	security-control/EFS.4

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/EKS.2	security-control/EKS.2
service-managed-aws-control-tower/v/1.0.0/ELB.2	security-control/ELB.2
service-managed-aws-control-tower/v/1.0.0/ELB.3	security-control/ELB.3
service-managed-aws-control-tower/v/1.0.0/ELB.4	security-control/ELB.4
service-managed-aws-control-tower/v/1.0.0/ELB.5	security-control/ELB.5
service-managed-aws-control-tower/v/1.0.0/ELB.6	security-control/ELB.6
service-managed-aws-control-tower/v/1.0.0/ELB.7	security-control/ELB.7
service-managed-aws-control-tower/v/1.0.0/ELB.8	security-control/ELB.8
service-managed-aws-control-tower/v/1.0.0/ELB.9	security-control/ELB.9
service-managed-aws-control-tower/v/1.0.0/ELB.10	security-control/ELB.10
service-managed-aws-control-tower/v/1.0.0/ELB.12	security-control/ELB.12
service-managed-aws-control-tower/v/1.0.0/ELB.13	security-control/ELB.13

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/ELB.14	security-control/ELB.14
service-managed-aws-control-tower/v/1.0.0/ELBv2.1	security-control/ELBv2.1
service-managed-aws-control-tower/v/1.0.0/EMR.1	security-control/EMR.1
service-managed-aws-control-tower/v/1.0.0/ES.1	security-control/ES.1
service-managed-aws-control-tower/v/1.0.0/ES.2	security-control/ES.2
service-managed-aws-control-tower/v/1.0.0/ES.3	security-control/ES.3
service-managed-aws-control-tower/v/1.0.0/ES.4	security-control/ES.4
service-managed-aws-control-tower/v/1.0.0/ES.5	security-control/ES.5
service-managed-aws-control-tower/v/1.0.0/ES.6	security-control/ES.6
service-managed-aws-control-tower/v/1.0.0/ES.7	security-control/ES.7
service-managed-aws-control-tower/v/1.0.0/ES.8	security-control/ES.8
service-managed-aws-control-tower/v/1.0.0/ElasticBeanstalk.1	security-control/ElasticBeanstalk.1

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/ElasticBeanstalk.2	security-control/ElasticBeanstalk.2
service-managed-aws-control-tower/v/1.0.0/GuardDuty.1	security-control/GuardDuty.1
service-managed-aws-control-tower/v/1.0.0/IAM.1	security-control/IAM.1
service-managed-aws-control-tower/v/1.0.0/IAM.2	security-control/IAM.2
service-managed-aws-control-tower/v/1.0.0/IAM.3	security-control/IAM.3
service-managed-aws-control-tower/v/1.0.0/IAM.4	security-control/IAM.4
service-managed-aws-control-tower/v/1.0.0/IAM.5	security-control/IAM.5
service-managed-aws-control-tower/v/1.0.0/IAM.6	security-control/IAM.6
service-managed-aws-control-tower/v/1.0.0/IAM.7	security-control/IAM.7
service-managed-aws-control-tower/v/1.0.0/IAM.8	security-control/IAM.8
service-managed-aws-control-tower/v/1.0.0/IAM.21	security-control/IAM.21
service-managed-aws-control-tower/v/1.0.0/Kinesis.1	security-control/Kinesis.1

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/KMS.1	security-control/KMS.1
service-managed-aws-control-tower/v/1.0.0/KMS.2	security-control/KMS.2
service-managed-aws-control-tower/v/1.0.0/KMS.3	security-control/KMS.3
service-managed-aws-control-tower/v/1.0.0/Lambda.1	security-control/Lambda.1
service-managed-aws-control-tower/v/1.0.0/Lambda.2	security-control/Lambda.2
service-managed-aws-control-tower/v/1.0.0/Lambda.5	security-control/Lambda.5
service-managed-aws-control-tower/v/1.0.0/NetworkFirewall.3	security-control/NetworkFirewall.3
service-managed-aws-control-tower/v/1.0.0/NetworkFirewall.4	security-control/NetworkFirewall.4
service-managed-aws-control-tower/v/1.0.0/NetworkFirewall.5	security-control/NetworkFirewall.5
service-managed-aws-control-tower/v/1.0.0/NetworkFirewall.6	security-control/NetworkFirewall.6
service-managed-aws-control-tower/v/1.0.0/Opensearch.1	security-control/Opensearch.1
service-managed-aws-control-tower/v/1.0.0/Opensearch.2	security-control/Opensearch.2

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/Opensearch.3	security-control/Opensearch.3
service-managed-aws-control-tower/v/1.0.0/Opensearch.4	security-control/Opensearch.4
service-managed-aws-control-tower/v/1.0.0/Opensearch.5	security-control/Opensearch.5
service-managed-aws-control-tower/v/1.0.0/Opensearch.6	security-control/Opensearch.6
service-managed-aws-control-tower/v/1.0.0/Opensearch.7	security-control/Opensearch.7
service-managed-aws-control-tower/v/1.0.0/Opensearch.8	security-control/Opensearch.8
service-managed-aws-control-tower/v/1.0.0/RDS.1	security-control/RDS.1
service-managed-aws-control-tower/v/1.0.0/RDS.2	security-control/RDS.2
service-managed-aws-control-tower/v/1.0.0/RDS.3	security-control/RDS.3
service-managed-aws-control-tower/v/1.0.0/RDS.4	security-control/RDS.4
service-managed-aws-control-tower/v/1.0.0/RDS.5	security-control/RDS.5
service-managed-aws-control-tower/v/1.0.0/RDS.6	security-control/RDS.6

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/RDS.8	security-control/RDS.8
service-managed-aws-control-tower/v/1.0.0/RDS.9	security-control/RDS.9
service-managed-aws-control-tower/v/1.0.0/RDS.10	security-control/RDS.10
service-managed-aws-control-tower/v/1.0.0/RDS.11	security-control/RDS.11
service-managed-aws-control-tower/v/1.0.0/RDS.13	security-control/RDS.13
service-managed-aws-control-tower/v/1.0.0/RDS.17	security-control/RDS.17
service-managed-aws-control-tower/v/1.0.0/RDS.18	security-control/RDS.18
service-managed-aws-control-tower/v/1.0.0/RDS.19	security-control/RDS.19
service-managed-aws-control-tower/v/1.0.0/RDS.20	security-control/RDS.20
service-managed-aws-control-tower/v/1.0.0/RDS.21	security-control/RDS.21
service-managed-aws-control-tower/v/1.0.0/RDS.22	security-control/RDS.22
service-managed-aws-control-tower/v/1.0.0/RDS.23	security-control/RDS.23

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/RDS.25	security-control/RDS.25
service-managed-aws-control-tower/v/1.0.0/Redshift.1	security-control/Redshift.1
service-managed-aws-control-tower/v/1.0.0/Redshift.2	security-control/Redshift.2
service-managed-aws-control-tower/v/1.0.0/Redshift.4	security-control/Redshift.4
service-managed-aws-control-tower/v/1.0.0/Redshift.6	security-control/Redshift.6
service-managed-aws-control-tower/v/1.0.0/Redshift.7	security-control/Redshift.7
service-managed-aws-control-tower/v/1.0.0/Redshift.8	security-control/Redshift.8
service-managed-aws-control-tower/v/1.0.0/Redshift.9	security-control/Redshift.9
service-managed-aws-control-tower/v/1.0.0/S3.1	security-control/S3.1
service-managed-aws-control-tower/v/1.0.0/S3.2	security-control/S3.2
service-managed-aws-control-tower/v/1.0.0/S3.3	security-control/S3.3
service-managed-aws-control-tower/v/1.0.0/S3.5	security-control/S3.5

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/S3.6	security-control/S3.6
service-managed-aws-control-tower/v/1.0.0/S3.8	security-control/S3.8
service-managed-aws-control-tower/v/1.0.0/S3.9	security-control/S3.9
service-managed-aws-control-tower/v/1.0.0/S3.12	security-control/S3.12
service-managed-aws-control-tower/v/1.0.0/S3.13	security-control/S3.13
service-managed-aws-control-tower/v/1.0.0/SageMaker.1	security-control/SageMaker.1
service-managed-aws-control-tower/v/1.0.0/SecretsManager.1	security-control/SecretsManager.1
service-managed-aws-control-tower/v/1.0.0/SecretsManager.2	security-control/SecretsManager.2
service-managed-aws-control-tower/v/1.0.0/SecretsManager.3	security-control/SecretsManager.3
service-managed-aws-control-tower/v/1.0.0/SecretsManager.4	security-control/SecretsManager.4
service-managed-aws-control-tower/v/1.0.0/SQS.1	security-control/SQS.1
service-managed-aws-control-tower/v/1.0.0/SSM.1	security-control/SSM.1

統合コントロールの検出結果を有効にする前の GeneratorID	統合コントロールの検出結果を有効にした後の GeneratorID
service-managed-aws-control-tower/v/1.0.0/SSM.2	security-control/SSM.2
service-managed-aws-control-tower/v/1.0.0/SSM.3	security-control/SSM.3
service-managed-aws-control-tower/v/1.0.0/SSM.4	security-control/SSM.4
service-managed-aws-control-tower/v/1.0.0/WAF.2	security-control/WAF.2
service-managed-aws-control-tower/v/1.0.0/WAF.3	security-control/WAF.3
service-managed-aws-control-tower/v/1.0.0/WAF.4	security-control/WAF.4

統合がコントロール ID とタイトルに与える影響

統合されたコントロールビューと統合されたコントロールの検出結果は、コントロール ID とタイトルを標準間で標準化します。セキュリティコントロール ID とセキュリティコントロールタイトルという用語は、これらの標準にとらわれない値を指します。

Security Hub CSPM コンソールには、アカウントで統合コントロールIDs とセキュリティコントロールタイトルが表示されます。ただし、Security Hub CSPM の検出結果には、アカウントで統合コントロールの検出結果が無効になっている場合、PCI DSS および CIS v1.2.0 の標準固有のコントロールタイトルが含まれています。さらに、Security Hub CSPM の検出結果には、標準固有のコントロール ID とセキュリティコントロール ID が含まれます。統合がコントロールの検出結果にどのように影響するかの例については、「」を参照してくださいコントロールの検出結果のサンプル。

AWS Control Tower サービスマネージド標準の一部であるコントロールの場合、統合コントロールの検出結果が有効になっていると、検出結果のコントロール ID とタイトルからプレフィックスがCT.削除されます。

Security Hub CSPM でセキュリティコントロールを無効にするには、セキュリティコントロールに対応するすべての標準コントロールを無効にする必要があります。次の表に、セキュリティコントロール ID とタイトルを標準固有のコントロール ID とタイトルにマッピングする方法について示します。 AWS Foundational Security Best Practices (FSBP) 標準に属するコントロールの IDs とタイトルは、既に標準に依存しません。コントロールと Center for Internet Security (CIS) v3.0.0 の要件のマッピングについては、「各バージョンの CIS 要件に対するコントロールのマッピング」を参照してください。このテーブルで独自のスクリプトを実行するには、.csv ファイルとしてダウンロードできます。

規格	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.2.0	1.1 ルートユーザーの使用を避ける	[CloudWatch.1] 「ルート」ユーザーの使用に対するログメトリクスフィルターとアラームが存在する必要があります
CIS v1.2.0	1.10 IAM パスワードポリシーでパスワードの再使用を防止していることを確認する	[IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています
CIS v1.2.0	1.11 IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認する	[IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します
CIS v1.2.0	1.12 ルートユーザーのアクセスキーが存在しないことを確認する	[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
CIS v1.2.0	1.13 MFA がルートユーザーで有効になっていることを確認する	[IAM.9] ルートユーザーに対して MFA を有効にする必要があります
CIS v1.2.0	1.14 ハードウェア MFA がルートユーザーで有効になっていることを確認する	[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
CIS v1.2.0	1.16 IAM ポリシーがグループまたはロールだけにアタッチされていることを確認する	[IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください

規格	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.2.0	1.2 コンソールパスワードを持つすべての IAM ユーザーに対して多要素認証 (MFA) が有効であることを確認する	[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
CIS v1.2.0	1.20 サポートでインシデントを管理するためのサポートロールが作成されていることを確認する	[IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
CIS v1.2.0	1.22 完全な「*:*」管理者権限を許可する IAM ポリシーが作成されていないことを確認する	[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
CIS v1.2.0	1.3 90 日間以上使用されていない認証情報は無効にします。	[IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
CIS v1.2.0	1.4 アクセスキーは 90 日ごとに更新します。	[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
CIS v1.2.0	1.5 IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認する	[IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します
CIS v1.2.0	1.6 IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認する	[IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します
CIS v1.2.0	1.7 IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認する	[IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します
CIS v1.2.0	1.8 IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認する	[IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します

規格	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.2.0	1.9 IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認する	[IAM.15] IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認します
CIS v1.2.0	2.1 CloudTrail がすべてのリージョンで有効であることを確認する	[CloudTrail.1] CloudTrail を有効にして、少なくとも 1 つのマルチリージョンの追跡で、読み取りと書き込みの管理イベントを含めた設定をする必要があります。
CIS v1.2.0	2.2 CloudTrail ログファイル検証が有効であることを確認する	[PCI.CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります
CIS v1.2.0	2.3 CloudTrail ログの保存に使用される S3 バケットが一般公開されていないことを確認する	[CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットが一般公開されていないことを確認します
CIS v1.2.0	2.4 CloudTrail 証跡が CloudWatch ログと統合されていることを確認する	[CloudTrail.5] CloudTrail 追跡は Amazon CloudWatch Logs と統合する必要があります
CIS v1.2.0	2.5 AWS Config が有効になっていることを確認する	[Config.1] を有効にし、サービスにリンクされたロールをリソース記録に使用 AWS Config する必要があります
CIS v1.2.0	2.6 CloudTrail S3 バケットで、S3 バケットアクセスログ記録が有効であることを確認する	[CloudTrail.7] CloudTrail S3 バケットで、S3 バケットアクセスログ記録が有効であることを確認します
CIS v1.2.0	2.7 CloudTrail ログは保管時に KMS CMK を使用して暗号化されていることを確認する	[CloudTrail.2] CloudTrail は保管時の暗号化を有効にする必要があります

規格	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.2.0	2.8 カスタマー作成の CMK のローテーションが有効になっていることを確認します	[KMS.4] AWS KMS キーローテーションを有効にする必要があります
CIS v1.2.0	2.9 すべての VPC で VPC フローログ記録が有効になっていることを確認します	[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします
CIS v1.2.0	3.1 不正な API 呼び出しに対してログメトリクスフィルターとアラームが存在することを確認します	[CloudWatch.2] 不正な API 呼び出しに対してログメトリクスフィルターとアラームが存在することを確認します
CIS v1.2.0	3.10 セキュリティグループの変更に対するメトリクスフィルターとアラームが存在することを確認します	[CloudWatch.10] セキュリティグループの変更に対するログメトリクスフィルターとアラームが存在することを確認します
CIS v1.2.0	3.11 ネットワークアクセスコントロールリスト (NACL) への変更に対するログメトリクスとアラームが存在することを確認します	[CloudWatch.11] ネットワークアクセスコントロールリスト (NACL) への変更に対するログメトリクスフィルターとアラームが存在することを確認します
CIS v1.2.0	3.12 ネットワークゲートウェイへの変更に対するログメトリクスとアラームが存在することを確認します	[CloudWatch.12] ネットワークゲートウェイへの変更に対するログメトリクスフィルターとアラームが存在することを確認します
CIS v1.2.0	3.13 ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認します	[CloudWatch.13] ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認します

規格	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.2.0	3.14 VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認します	[CloudWatch.14] VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認します
CIS v1.2.0	3.2 MFA を使用しないマネジメントコンソールサインインに対してログメトリックフィルターとアラームが存在することを確認する	[CloudWatch.3] MFA を使用しないマネジメントコンソールサインインに対してログメトリクスフィルターとアラームが存在することを確認します
CIS v1.2.0	3.3 ルートユーザーに使用するログメトリックフィルターとアラームが存在することを確認する	[CloudWatch.1] 「ルート」ユーザーの使用に対するログメトリクスフィルターとアラームが存在する必要があります
CIS v1.2.0	3.4 IAM ポリシーの変更に対するログメトリックフィルターとアラームが存在することを確認する	[CloudWatch.4] IAM ポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します
CIS v1.2.0	3.5 CloudTrail 設定の変更に対するログ メトリックフィルターとアラームが存在することを確認する	[CloudWatch.5] CloudTrail 設定変更のログメトリクスフィルターとアラームが存在することを確認する
CIS v1.2.0	3.6 AWS Management Console 認証の失敗に対してログメトリクスフィルターとアラームが存在することを確認する	[CloudWatch.6] AWS Management Console 認証失敗のログメトリクスフィルターとアラームが存在することを確認する
CIS v1.2.0	3.7 カスタマー作成の CMK の無効化またはスケジュールされた削除に対してログメトリクスフィルターとアラームが存在することを確認します	[CloudWatch.7] カスタマーマネージドキーの無効化またはスケジュールされた削除に対するログメトリクスフィルターとアラームが存在することを確認します

規格	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.2.0	3.8 S3 バケットの変更に対してログメトリクスフィルターとアラームが存在することを確認します	[CloudWatch.8] S3 バケットポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します
CIS v1.2.0	3.9 AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する	[CloudWatch.9] AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する
CIS v1.2.0	4.1 どのセキュリティグループでも 0.0.0.0/0 からポート 22 への入力を許可しないようにします	[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります
CIS v1.2.0	4.2 どのセキュリティグループでも 0.0.0.0/0 からポート 3389 への入力を許可しないようにします	[EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
CIS v1.2.0	4.3 すべての VPC のデフォルトセキュリティグループがすべてのトラフィックを制限するようにします。	[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします
CIS v1.4.0	1.10 コンソールパスワードを持つすべての IAM ユーザーに対して多要素認証 (MFA) が有効であることを確認する	[IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
CIS v1.4.0	1.14 アクセスキーは 90 日以内ごとに更新されているのを確認する	[IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります

規格	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.4.0	1.16 完全な「*:*」管理権限を許可する IAM ポリシーがアタッチされていないことを確認する	[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
CIS v1.4.0	1.17 サポートでインシデントを管理するためのサポートロールが作成されていることを確認する	[IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
CIS v1.4.0	1.4 ルートユーザーアカウントのアクセスキーが存在しないことを確認する	[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
CIS v1.4.0	1.5 ルートユーザーアカウントで MFA が有効であることを確認する	[IAM.9] ルートユーザーに対して MFA を有効にする必要があります
CIS v1.4.0	1.6 ルートユーザーアカウントでハードウェア MFA が有効であることを確認する	[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
CIS v1.4.0	1.7 管理および日常のタスクでのルートユーザーの使用を排除する	[CloudWatch.1] 「ルート」ユーザーの使用に対するログメトリクスフィルターとアラームが存在する必要があります
CIS v1.4.0	1.8 IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認する	[IAM.15] IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認します
CIS v1.4.0	1.9 IAM パスワードポリシーでパスワードの再使用を防止していることを確認する	[IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています
CIS v1.4.0	2.1.2 S3 バケットポリシーが HTTP リクエストを拒否するように設定されていることを確認する	[S3.5] S3 汎用バケットではリクエストに SSL を使用する必要があります。

規格	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.4.0	2.1.5.1 S3 ブロックパブリックアクセス設定を有効にする必要があります	[S3.1] S3 汎用バケットではブロックパブリックアクセスの設定が有効になっている必要があります。
CIS v1.4.0	2.1.5.2 S3 ブロックパブリックアクセス設定は、バケットレベルで有効にする必要があります	[S3.8] S3 汎用バケットはパブリックアクセスをブロックする必要があります
CIS v1.4.0	2.2.1 EBS ボリュームの暗号化が有効であることを確認する	[EC2.7] EBS のデフォルト暗号化を有効にすることをお勧めします
CIS v1.4.0	2.3.1 RDS インスタンスで暗号化が有効であることを確認する	[RDS.3] RDS DB インスタンスでは、保管時の暗号化が有効になっている必要があります。
CIS v1.4.0	3.1 CloudTrail がすべてのリージョンで有効であることを確認する	[CloudTrail.1] CloudTrail を有効にして、少なくとも 1 つのマルチリージョンの追跡で、読み取りと書き込みの管理イベントを含めた設定をする必要があります。
CIS v1.4.0	3.2 CloudTrail ログファイル検証が有効であることを確認する	[PCI.CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります
CIS v1.4.0	3.4 CloudTrail 証跡が CloudWatch ログと統合されていることを確認する	[CloudTrail.5] CloudTrail 追跡は Amazon CloudWatch Logs と統合する必要があります
CIS v1.4.0	3.5 すべてのリージョンで AWS Config が有効になっていることを確認する	[Config.1] を有効にし、サービスにリンクされたロールをリソース記録に使用 AWS Config する必要があります

規格	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.4.0	3.6 CloudTrail S3 バケットで、S3 バケットアクセスログ記録が有効であることを確認する	[CloudTrail.7] CloudTrail S3 バケットで、S3 バケットアクセスログ記録が有効であることを確認します
CIS v1.4.0	3.7 CloudTrail ログは保管時に KMS CMK を使用して暗号化されていることを確認する	[CloudTrail.2] CloudTrail は保管時の暗号化を有効にする必要があります
CIS v1.4.0	3.8 カスタマー作成の CMK のローテーションが有効になっていることを確認する	[KMS.4] AWS KMS キーローテーションを有効にする必要があります
CIS v1.4.0	3.9 すべての VPC で VPC フローログ記録が有効になっていることを確認する	[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします
CIS v1.4.0	4.4 IAM ポリシーの変更に対するログメトリックフィルターとアラームが存在することを確認する	[CloudWatch.4] IAM ポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します
CIS v1.4.0	4.5 CloudTrail 設定の変更に対するログメトリックフィルターとアラームが存在することを確認する	[CloudWatch.5] CloudTrail 設定変更のログメトリクスフィルターとアラームが存在することを確認する
CIS v1.4.0	4.6 AWS Management Console 認証の失敗に対してログメトリクスフィルターとアラームが存在することを確認する	[CloudWatch.6] AWS Management Console 認証失敗のログメトリクスフィルターとアラームが存在することを確認する
CIS v1.4.0	4.7 カスタマー作成の CMK の無効化またはスケジュールされた削除に対してログメトリックフィルターとアラームが存在することを確認する	[CloudWatch.7] カスタマーマネージドキーの無効化またはスケジュールされた削除に対するログメトリクスフィルターとアラームが存在することを確認します

規格	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.4.0	4.8 S3 バケットの変更に対してログメトリックフィルターとアラームが存在することを確認する	[CloudWatch.8] S3 バケットポリシーの変更に対するログメトリクスフィルターとアラームが存在することを確認します
CIS v1.4.0	4.9 AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する	[CloudWatch.9] AWS Config 設定変更のログメトリクスフィルターとアラームが存在することを確認する
CIS v1.4.0	4.10 セキュリティグループの変更に対するログメトリックフィルターとアラームが存在することを確認する	[CloudWatch.10] セキュリティグループの変更に対するログメトリクスフィルターとアラームが存在することを確認します
CIS v1.4.0	4.11 ネットワークアクセスコントロールリスト (NACL) への変更に対するログメトリックフィルターとアラームが存在することを確認する	[CloudWatch.11] ネットワークアクセスコントロールリスト (NACL) への変更に対するログメトリクスフィルターとアラームが存在することを確認します
CIS v1.4.0	4.12 ネットワークゲートウェイへの変更に対するログメトリックフィルターとアラームが存在することを確認する	[CloudWatch.12] ネットワークゲートウェイへの変更に対するログメトリクスフィルターとアラームが存在することを確認します
CIS v1.4.0	4.13 ルートテーブルの変更に対してログメトリックフィルターとアラームが存在することを確認する	[CloudWatch.13] ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認します
CIS v1.4.0	4.14 VPC の変更に対してログメトリックフィルターとアラームが存在することを確認する	[CloudWatch.14] VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認します

規格	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
CIS v1.4.0	5.1 ネットワーク ACL が 0.0.0.0/0 からリモートサーバー管理ポートへの侵入を許可していないことを確認する	[EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります
CIS v1.4.0	5.3 すべての VPC のデフォルトセキュリティグループがすべてのトラフィックを制限するようにします	[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします
PCI DSS v3.2.1	PCI.AutoScaling.1 ロードバランサーに関連付けられた Auto Scaling グループは、ロードバランサーのヘルスチェックを使用する必要があります	[AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要がある
PCI DSS v3.2.1	PCI.CloudTrail.1 CloudTrail ログは、AWS KMS CMKs を使用して保管時に暗号化する必要があります	[CloudTrail.2] CloudTrail は保管時の暗号化を有効にする必要があります
PCI DSS v3.2.1	PCI.CloudTrail.2 CloudTrail を有効にする必要があります	[CloudTrail.3] 少なくとも 1 つの CloudTrail 証跡を有効にする必要があります
PCI DSS v3.2.1	PCI.CloudTrail.3 CloudTrail ログファイルの検証を有効にする必要があります	[PCI.CloudTrail.4] CloudTrail ログファイルの検証を有効にする必要があります
PCI DSS v3.2.1	PCI.CloudTrail.4 CloudTrail 証跡は Amazon CloudWatch Logs と統合する必要があります	[CloudTrail.5] CloudTrail 追跡は Amazon CloudWatch Logs と統合する必要があります

規格	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
PCI DSS v3.2.1	PCI.CodeBuild.1 CodeBuild GitHub または Bitbucket のソースリポジトリの URL は、OAuth を使用する必要があります	[CodeBuild.1] CodeBuild Bitbucket ソースリポジトリの URL には機密認証情報を含めないでください
PCI DSS v3.2.1	PCI.CodeBuild.2 CodeBuild プロジェクト環境変数に、クリアテキストの認証情報を含めるべきではない	[CodeBuild.2] CodeBuild プロジェクト環境変数にクリアテキストの認証情報を含めることはできません
PCI DSS v3.2.1	PCI.Config.1 AWS Config を有効にする必要があります	[Config.1] を有効にし、サービスにリンクされたロールをリソース記録に使用 AWS Config する必要があります
PCI DSS v3.2.1	PCI.CW.1「ルート」ユーザーの使用に対するログメトリックフィルターとアラームが存在する必要があります	[CloudWatch.1] 「ルート」ユーザーの使用に対するログメトリクスフィルターとアラームが存在する必要があります
PCI DSS v3.2.1	PCI.DMS.1 Database Migration Service のレプリケーションインスタンスはパブリックではない必要があります	[DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります
PCI DSS v3.2.1	PCI.EC2.1 EBS スナップショットをパブリックに復元可能であってはなりません	[EC2.1] Amazon EBS スナップショットはパブリックに復元できないようにすることをお勧めします
PCI DSS v3.2.1	PCI.EC2.2 VPC のデフォルトのセキュリティグループで、インバウンドトラフィックとアウトバウンドトラフィックを禁止する必要があります	[EC2.2] VPC のデフォルトのセキュリティグループでは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないようにすることをお勧めします

規格	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
PCI DSS v3.2.1	PCI.EC2.4 未使用の EC2 EIP を削除する必要があります	[EC2.12] 未使用の Amazon EC2 EIP を削除することをお勧めします
PCI DSS v3.2.1	PCI.EC2.5 セキュリティグループは、0.0.0.0/0 からポート 22 への入力を許可しないようにする必要があります	[EC2.13] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 22 への入力を許可しないようにする必要があります
PCI DSS v3.2.1	PCI.EC2.6 VPC フローログ記録をすべての VPC で有効にする必要があります	[EC2.6] すべての VPC で VPC フローログ記録を有効にすることをお勧めします
PCI DSS v3.2.1	PCI.ELBV2.1 Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります	[ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります
PCI DSS v3.2.1	PCI.ES.1 Elasticsearch ドメインは VPC 内に存在する必要があります	[ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります
PCI DSS v3.2.1	PCI.ES.2 Elasticsearch ドメインで保管中の暗号化を有効にする必要があります	[ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります
PCI DSS v3.2.1	PCI.GuardDuty.1 GuardDuty を有効にする必要があります	[GuardDuty.1] GuardDuty を有効にする必要があります
PCI DSS v3.2.1	PCI.IAM.1 IAM ルートユーザーのアクセスキーが存在していてはなりません	[IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
PCI DSS v3.2.1	PCI.IAM.2 IAM ユーザーには IAM ポリシーをアタッチしてはなりません	[IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください

規格	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
PCI DSS v3.2.1	PCI.IAM.3 IAM ポリシーで、完全な「*」管理者権限を許可してはなりません	[IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
PCI DSS v3.2.1	PCI.IAM.4 ルートユーザーに対してハードウェア MFA を有効にする必要があります	[IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
PCI DSS v3.2.1	PCI.IAM.5 ルートユーザーに対して仮想 MFA を有効にする必要があります	[IAM.9] ルートユーザーに対して MFA を有効にする必要があります
PCI DSS v3.2.1	PCI.IAM.6 すべての IAM ユーザーに対して MFA を有効にする必要があります	[IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
PCI DSS v3.2.1	PCI.IAM.7 IAM ユーザー認証情報が事前定義された日数以内に使用されない場合、認証情報を無効にする必要があります	[IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
PCI DSS v3.2.1	PCI.IAM.8 IAM ユーザーのパスワードポリシーには強力な設定が必要です	[IAM.10] IAM ユーザーのパスワードポリシーには強力な設定が必要です
PCI DSS v3.2.1	PCI.KMS.1 カスタマーマスターキー (CMK) ローテーションを有効にする必要があります	[KMS.4] AWS KMS キーローテーションを有効にする必要があります
PCI DSS v3.2.1	PCI.Lambda.1 Lambda 関数は、パブリックアクセスを禁止する必要があります	[Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります
PCI DSS v3.2.1	PCI.Lambda.2 Lambda 関数は VPC 内に存在する必要があります	[Lambda.3] Lambda 関数は VPC 内に存在する必要があります

規格	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
PCI DSS v3.2.1	PCI.Opensearch.1 OpenSearch ドメインは VPC 内に含まれている必要があります	[Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
PCI DSS v3.2.1	PCI.Opensearch.2 EBS スナップショットをパブリックに復元可能であってはなりません	[Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります
PCI DSS v3.2.1	PCI.RDS.1 RDS スナップショットはプライベートである必要があります	[RDS.1] RDS スナップショットはプライベートである必要があります
PCI DSS v3.2.1	PCI.RDS.2 RDS DB インスタンスでパブリックアクセスを禁止する必要があります	[RDS.2] RDS DB インスタンスは、PubliclyAccessible 設定によって判断される、パブリックアクセスを禁止する必要があります
PCI DSS v3.2.1	PCI.Redshift.1 Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります	[PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります
PCI DSS v3.2.1	PCI.S3.1 S3 バケットはパブリック書き込みアクセスを禁止する必要があります	[S3.3] S3 汎用バケットではパブリック書き込みアクセスをブロックする必要があります。
PCI DSS v3.2.1	PCI.S3.2 S3 バケットではパブリック読み取りアクセスを禁止する必要があります	[S3.2] S3 汎用バケットはパブリック読み取りアクセスをブロックする必要があります
PCI DSS v3.2.1	PCI.S3.3 S3 バケットでクロスリージョンレプリケーションを有効にする必要があります	[S3.7] S3 汎用バケットでクロスリージョンレプリケーションを使用する必要があります
PCI DSS v3.2.1	PCI.S3.5 S3 バケットは Secure Socket Layer を使用するリクエストを要求する必要があります	[S3.5] S3 汎用バケットではリクエストに SSL を使用する必要があります。

規格	標準コントロール ID とタイトル	セキュリティコントロール ID とタイトル
PCI DSS v3.2.1	PCI.S3.6 S3 パブリックアクセスブロック設定を有効にする必要があります	[S3.1] S3 汎用バケットではブロックパブリックアクセスの設定が有効になっている必要があります。
PCI DSS v3.2.1	PCI.SageMaker.1 Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります	[SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります
PCI DSS v3.2.1	PCI.SSM.1 Systems Manager によって管理される EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります	[SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
PCI DSS v3.2.1	PCI.SSM.2 Systems Manager によって管理される EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります	[SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
PCI DSS v3.2.1	PCI.SSM.3 EC2 インスタンスは によって管理する必要があります AWS Systems Manager	[SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager

統合に向けたワークフローの更新

ワークフローがコントロールの検出結果のフィールドの特定形式に依存していない場合、アクションは必要ありません。

前の表で説明したように、ワークフローがコントロール結果の 1 つ以上のフィールドの特定形式に依存している場合は、ワークフローを更新する必要があります。たとえば、コントロール ID が CIS 2.7 と等しい場合に AWS Lambda 関数を呼び出すなど、特定のコントロール ID のア

クションをトリガーする Amazon EventBridge ルールを作成した場合は、そのコントロールの `Compliance.SecurityControlId`フィールドの値である CloudTrail.2, を使用するようにルールを更新します。

変更されたフィールドまたは値のいずれかを使用するカスタムインサイトを作成した場合は、それらのインサイトを更新して新しいフィールドまたは値を使用します。

必須の ASFF 最上位属性

Security Hub CSPM のすべての検出結果には、 AWS Security Finding 形式 (ASFF) の次の最上位属性が必要です。これらの属性の詳細については、AWS Security Hub API リファレンスのAwsSecurityFinding「」を参照してください。

AwsAccountId

検出結果が適用される AWS アカウント ID。

例

```
"AwsAccountId": "111111111111"
```

CreatedAt

検出結果によってキャプチャされた潜在的なセキュリティ問題またはイベントが作成された日時を示します。

例

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

説明

検出結果の説明。このフィールドには、固有ではない定型テキスト、または結果のインスタンスに固有の詳細を指定できます。

Security Hub CSPM が生成するコントロールの検出結果については、このフィールドにコントロールの説明が表示されます。

[統合されたコントロールの検出結果] を有効にした場合、このフィールドは標準を参照しません。

例

```
"Description": "This AWS control checks whether AWS Config is enabled in the current
 account and Region."
```

GeneratorId

検出結果を生成したソリューションに固有のコンポーネント (個別のロジック単位) の識別子。

Security Hub CSPM が生成するコントロールの検出結果については、統合コントロールの検出結果を有効にしても、このフィールドは標準を参照しません。

例

```
"GeneratorId": "security-control/Config.1"
```

ID

検出結果の製品に固有の識別子。Security Hub CSPM が生成するコントロールの検出結果については、このフィールドには検出結果の Amazon リソースネーム (ARN) が表示されます。

[統合されたコントロールの検出結果] を有効にした場合、このフィールドは標準を参照しません。

例

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/
ab6d6a26-a156-48f0-9403-115983e5a956"
```

ProductArn

製品が Security Hub CSPM に登録された後にサードパーティーの検出結果製品を一意に識別する、Security Hub CSPM によって生成された Amazon リソースネーム (ARN)。

このフィールドの形式は `arn:`*`partition`*`:securityhub:`*`region`*`:`*`account-id`*`:product/`*`company-id`*`/`*`product-id` です。

- Security Hub CSPM と統合 AWS のサービス されている `company-id`の場合、 は`aws`「」で、 は AWS パブリックサービス名`product-id`である必要があります。製品およびサービスはアカウントに関連付けられていないため AWS 、ARN の `account-id`セクションは空です。Security Hub CSPM とまだ統合されていない AWS のサービス は、サードパーティー製品と見なされます。
- パブリック製品の場合、`company-id` および `product-id` は登録時に指定された ID 値である必要があります。

- プライベート製品の場合、company-id はアカウント ID である必要があります。product-id は、予約語の "default"、または登録時に指定された ID である必要があります。

例

```
// Private ARN
    "ProductArn": "arn:aws:securityhub:us-east-1:111111111111:product/111111111111/
default"

// Public ARN
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty"
    "ProductArn": "arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-
pro"
```

リソース

オブジェクトのResources配列は、検出結果が参照するリソースを記述する一連の AWS リソースデータ型を提供します。必須のフィールドなど、Resourcesオブジェクトに含まれる可能性のあるフィールドの詳細については、AWS Security Hub API リファレンスResourceの「」を参照してください。特定の のResourcesオブジェクトの例については AWS のサービス、「」を参照してくださいResources ASFF オブジェクト。

例

```
"Resources": [
  {
    "ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0",
    "ApplicationName": "SampleApp",
    "DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
```

```
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
                        }
                    },
                    {
                        "Count": 59,
                        "Type": "EMAIL_ADDRESS",
                        "Occurrences": {
                            "Pages": [
                                {
                                    "PageNumber": 1,
                                    "OffsetRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                     },
                                    "LineRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                    }
                                }
                            ]
                        }
                    },
                    {
                        "Count": 2229,
                        "Type": "URL",
                        "Occurrences": {
                           "LineRanges": [
                               {
```

```
                                    "Start": 1,
                                    "End": 13
                                }
                            ]
                        }
                    },
                    {
                        "Count": 13826,
                        "Type": "NameDetection",
                        "Occurrences": {
                             "Records": [
                                 {
                                     "RecordIndex": 1,
                                     "JsonPath": "$.ssn.value"
                                 }
                             ]
                         }
                    },
                    {
                        "Count": 32,
                        "Type": "AddressDetection"
                    }
                ],
                "TotalCount": 32
            }
        ],
        "CustomDataIdentifiers": {
            "Detections": [
                 {
                     "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                     "Name": "1712be25e7c7f53c731fe464f1c869b8",
                     "Count": 2
                 }
            ],
            "TotalCount": 2
        }
    }
},
 "Type": "AwsEc2Instance",
 "Id": "arn:aws:ec2:us-west-2:123456789012:instance/i-abcdef01234567890",
 "Partition": "aws",
 "Region": "us-west-2",
 "ResourceRole": "Target",
 "Tags": {
```

```
  "billingCode": "Lotus-1-2-3",
  "needsPatching": true
 },
 "Details": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
  "ImageId": "ami-79fd7eee",
  "IpV4Addresses": ["1.1.1.1"],
  "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
  "KeyName": "testkey",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "MetadataOptions": {
   "HttpEndpoint": "enabled",
   "HttpProtocolIpv6": "enabled",
   "HttpPutResponseHopLimit": 1,
   "HttpTokens": "optional",
   "InstanceMetadataTags": "disabled"
  }
 },
  "NetworkInterfaces": [
  {
   "NetworkInterfaceId": "eni-e5aa89a3"
  }
  ],
  "SubnetId": "PublicSubnet",
  "Type": "i3.xlarge",
  "VirtualizationType": "hvm",
  "VpcId": "TestVPCIpv6"
 }

]
```

SchemaVersion

検出結果に使用されている形式のスキーマバージョン。このフィールドの値は、 AWSで識別される正式公開バージョンの 1 つである必要があります。現在のリリースでは、 AWS Security Finding 形式のスキーマバージョンは です`2018-10-08`。

例

```
"SchemaVersion": "2018-10-08"
```

緊急度

検出結果の重要性を定義します。このオブジェクトの詳細については、SeveritySecurity Hub CSPM API リファレンスの「」を参照してください。 AWS

Severity は検索結果の最上位オブジェクトであり、FindingProviderFields オブジェクトの下にネストされています。

検出結果の最上位Severityオブジェクトの値は、 BatchUpdateFindings API を使用してのみ更新する必要があります。

重要度情報を提供するには、BatchImportFindings API リクエストを行うときに結果プロバイダーが FindingProviderFields の下にある Severity オブジェクトを更新する必要があります。
新しい検出結果のBatchImportFindingsリクエストが のみを提供するLabelか、 のみを提供する場合Normalized、Security Hub CSPM は他のフィールドの値を自動的に入力します。
Product および Originalフィールドも入力される場合があります。

最上位Finding.Severityオブジェクトが存在するが、存在しない場合、Security Hub CSPM Finding.FindingProviderFieldsはFindingProviderFields.Severityオブジェクトを作成し、その全体をそのオブジェクトにコピーFinding.Severity objectします。これにより、最上位の Severity オブジェクトが上書きされても、プロバイダーが提供する元の詳細が FindingProviderFields.Severity 構造内に保持されます。

検出結果の重要度には、関連するアセットまたは基になるリソースの重要度は考慮されません。重要度は、検出結果に関連付けられたリソースの重要度のレベルとして定義されます。例えば、ミッションクリティカルなアプリケーションに関連付けられているリソースは、非本番稼働用テストに関連付けられたリソースより重大度が高くなります。リソースの重要度に関する情報をキャプチャするには、Criticality フィールドを使用します。

検出結果のネイティブ重要度スコアを ASFF の Severity.Label の値に変換する際には、以下のガイダンスを使用することを推奨します。

- INFORMATIONAL – このカテゴリには、PASSED、WARNING、NOT AVAILABLE チェック、または機密データの ID が含まれる場合があります。
- LOW — 将来の侵害につながる可能性のある結果。例えば、このカテゴリには、脆弱性、設定の弱点、公開されたパスワードなどが含まれる場合があります。
- MEDIUM – 現在進行中の侵害を示していても、攻撃者が目標を達成した兆候が見られない結果。例えば、このカテゴリには、マルウェアアクティビティ、ハッキングアクティビティ、異常な動作の検出などが含まれます。

- HIGH または CRITICAL – 実際のデータ損失、漏洩、サービス拒否など、攻撃者が目標を達成したことを示す結果。

例

```
"Severity": {
    "Label": "CRITICAL",
    "Normalized": 90,
    "Original": "CRITICAL"
}
```

タイトル

検出結果のタイトル。このフィールドには、固有ではない定型テキスト、または検出結果のインスタンスに固有の詳細を指定できます。

コントロール検出結果の場合、このフィールドにはコントロールのタイトルが表示されます。[統合されたコントロールの検出結果] を有効にした場合、このフィールドは標準を参照しません。

例

```
"Title": "AWS Config should be enabled"
```

型

namespace/*category*/*classifier* の形式の 1 つ以上の検出結果タイプで、検出結果を分類します。[統合されたコントロールの検出結果] を有効にした場合、このフィールドは標準を参照しません。

Types は BatchUpdateFindings API を使用してのみ更新する必要があります。

検出結果プロバイダーが Types に値を提供する場合は、FindingProviderFields にある Types 属性を使用する必要があります。

以下のリストでは、最上位の項目は名前空間、2 番目のレベルの項目はカテゴリ、3 番目のレベルの項目は分類子です。検出結果プロバイダーでは、定義済みの名前空間を使用して、検出結果の並べ替えおよびグループ化を行うことが推奨されます。定義済みのカテゴリおよび分類子を使用することが推奨される場合もありますが、必須ではありません。Software and Configuration Checks 名前空間でのみ、分類子が定義されています。

名前空間/カテゴリ/分類子の部分パスを定義することができます。例えば、以下の結果タイプはすべて有効です。

- TTP
- TTP/防衛回避
- TTP/防衛回避/CloudTrailStopped

次のリストの tactics、techniques、procedures (TTP) カテゴリは、MITRE ATT&CK MatrixTM に対応しています。Unusual Behaviors (異常動作) の名前空間は、一般的な異常動作 (統計的異常など) を反映しており、特定の TTP とは一致していません。ただし、Unusual Behaviors と TTP の両方の結果で結果を分類することは可能です。

名前空間、カテゴリ、分類子のリスト:

- ソフトウェアおよび設定チェック
  - 脆弱性
    - CVE
  - AWS セキュリティのベストプラクティス
    - ネットワーク到達可能性
    - ランタイム動作分析
  - 業界および規制の基準
    - AWS 基本的なセキュリティのベストプラクティス
    - CIS Host Hardening Benchmark
    - CIS AWS Foundations Benchmark
    - PCI-DSS
    - クラウドセキュリティアライアンス規制
    - ISO 90001 規制
    - ISO 27001 規制
    - ISO 27017 規制
    - ISO 27018 規制
    - SOC 1
    - SOC 2
    - HIPAA 規制 (米国)

    - NIST 800-53 規制 (米国)
    - NIST CSF 規制 (米国)
    - IRAP 規制 (オーストラリア)
    - K-ISMS 規制 (韓国)
    - MTCS 規制 (シンガポール)
    - FISC安全対策基準 (日本)
    - マイナンバー法 (日本)
    - ENS 規制 (スペイン)
    - Cyber Essentials Plus 規制 (英国)
    - G-Cloud 規制 (英国)
    - C5 規制 (ドイツ)
    - IT-Grundschutz 規制 (ドイツ)
    - GDPR 規制 (ヨーロッパ)
    - TISAX 規制 (ヨーロッパ)
  - パッチ管理
- TTP
  - 初回アクセス
  - 実行
  - 永続的
  - 権限昇格
  - 防衛回避
  - 認証情報アクセス
  - 発見
  - 横方向への移動
  - 収集
  - コマンドアンドコントロール
- 効果
  - データ流出
  - データ漏えい
  - データ破壊

  - サービス拒否
  - リソース消費
- 異常な動作
  - アプリケーション
  - ネットワークフロー
  - IP アドレス
  - ユーザー
  - VM
  - コンテナ
  - サーバーレス
  - プロセス
  - データベース
  - データ
- 機密データの識別
  - PII
  - パスワード
  - リーガル
  - 金融
  - セキュリティ
  - ビジネス

例

```
"Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
]
```

UpdatedAt

検出結果プロバイダーが最後に結果レコードを更新した日時を示します。

このタイムスタンプは、検出結果レコードが最後または最も最近に更新された時刻を反映しています。したがって、イベントまたは脆弱性が最後または最も最近に検出された日時を反映する `LastObservedAt` タイムスタンプとは異なる可能性があります。

検出結果レコードを更新する際には、このタイムスタンプを現在のタイムスタンプに更新する必要があります。検出結果レコードの作成時には、CreatedAt と UpdatedAt のタイムスタンプが同じである必要があります。検出結果レコードを更新した後は、このフィールドの値が、そのレコードに含まれる以前のすべての値よりも最近の値になる必要があります。

BatchUpdateFindings オペレーションを使用して を更新UpdatedAtすることはできません。更新するには、 BatchImportFindingsオペレーションを使用します。

例

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

オプションの最上位 ASFF 属性

AWS Security Hub CSPM の結果では、Security Finding 形式 (ASFF) の以下の最上位属性はオプションです。これらの属性の詳細については、Security AWS Hub API リファレンスのAwsSecurityFinding」を参照してください。

アクション

Action オブジェクトは、リソースに影響を与える、またはリソースに対して実行されたアクションに関する詳細を提供します。

例

```
"Action": {
    "ActionType": "PORT_PROBE",
    "PortProbeAction": {
        "PortProbeDetails": [
            {
                "LocalPortDetails": {
                    "Port": 80,
                    "PortName": "HTTP"
                  },
                "LocalIpDetails": {
                     "IpAddressV4": "192.0.2.0"
                 },
                "RemoteIpDetails": {
                    "Country": {
                        "CountryName": "Example Country"
                    },
```

```
                    "City": {
                        "CityName": "Example City"
                    },
                    "GeoLocation": {
                        "Lon": 0,
                        "Lat": 0
                    },
                    "Organization": {
                        "AsnOrg": "ExampleASO",
                        "Org": "ExampleOrg",
                        "Isp": "ExampleISP",
                        "Asn": 64496
                    }
                }
            }
        ],
        "Blocked": false
    }
}
```

AwsAccountName

検出結果が適用される AWS アカウント 名前。

例

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

結果を生成した製品の会社の名前。コントロールベースの検出結果の場合、会社は です AWS。

Security Hub CSPM は、検出結果ごとにこの属性を自動的に入力します。`BatchImportFindings` または `BatchUpdateFindings` を使用して更新することはできません。カスタム統合を使用している場合は例外です。「the section called “カスタム製品の統合”」を参照してください。

Security Hub CSPM コンソールを使用して会社名で結果をフィルタリングする場合は、この属性を使用します。Security Hub CSPM API を使用して会社名で結果をフィルタリングする場合は、 の `aws/securityhub/CompanyName` 属性を使用します`ProductFields`。Security Hub CSPM は、これらの 2 つの属性を同期しません。

例

```
"CompanyName": "AWS"
```

コンプライアンス

Compliance オブジェクトは通常、適用可能な標準やコントロールチェックのステータスなど、コントロールの検出結果に関する詳細を提供します。

例

```
"Compliance": {
    "AssociatedStandards": [
        {"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
        {"StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
        {"StandardsId": "standards/nist-800-53/v/5.0.0"}
    ],
    "RelatedRequirements": [
        "NIST.800-53.r5 AC-4",
        "NIST.800-53.r5 AC-4(21)",
        "NIST.800-53.r5 SC-7",
        "NIST.800-53.r5 SC-7(11)",
        "NIST.800-53.r5 SC-7(16)",
        "NIST.800-53.r5 SC-7(21)",
        "NIST.800-53.r5 SC-7(4)",
        "NIST.800-53.r5 SC-7(5)"
    ],
    "SecurityControlId": "EC2.18",
    "SecurityControlParameters":[
        {
            "Name": "authorizedTcpPorts",
            "Value": ["80", "443"]
        },
        {
            "Name": "authorizedUdpPorts",
            "Value": ["427"]
        }
    ],
    "Status": "NOT_AVAILABLE",
    "StatusReasons": [
        {
            "ReasonCode": "CONFIG_RETURNS_NOT_APPLICABLE",
            "Description": "This finding has a compliance status of NOT AVAILABLE
because AWS Config sent Security Hub CSPM a finding with a compliance state of Not
Applicable. The potential reasons for a Not Applicable finding from Config are that
```

```
 (1) a resource has been moved out of scope of the Config rule; (2) the Config rule has
 been deleted; (3) the resource has been deleted; or (4) the logic of the Config rule
 itself includes scenarios where Not Applicable is returned. The specific reason why
 Not Applicable is returned is not available in the Config rule evaluation."
        }
    ]
}
```

信頼度

特定することが想定されている挙動または問題を、結果が正確に特定できる可能性。

Confidence は、BatchUpdateFindings のみを使用して更新する必要があります。

結果プロバイダーが Confidence に値を提供する場合は、FindingProviderFields にある Confidence 属性を使用する必要があります。「the section called “FindingProviderFields での結果の更新”」を参照してください。

Confidence は、比率スケールを使用して 0 ~ 100 ベースで採点されます。0 は 0% の信頼度を意味し、100 は 100% の信頼度を意味します。例えば、ネットワークトラフィックの統計的偏差に基づくデータの不正引き出しは、実際の不正引き出しが確認されていないため、信頼性が低くなります。

例

```
"Confidence": 42
```

緊急性

結果に関連付けられているリソースに割り当てられている重要度です。

Criticality は、BatchUpdateFindings API オペレーションを呼び出すことによってのみ更新してください。このオブジェクトは BatchImportFindings で更新しないでください。

結果プロバイダーが Criticality に値を提供する場合は、FindingProviderFields にある Criticality 属性を使用する必要があります。「the section called “FindingProviderFields での結果の更新”」を参照してください。

Criticality は、比率スケールを使用して 0 ~ 100 ベースで採点され、完全な整数のみをサポートしています。スコア 0 は、基になるリソースに重要性がないことを示しており、スコア 100 は最も重要なリソース用に予約されています。

各リソースに対して、Criticality を割り当てる際に以下の点を考慮してください。

- 影響を受けたリソースに機密データ (PII が含まれる S3 バケットなど) が含まれていないか?
- 影響を受けたリソースにより、攻撃者はアクセスレベルを深めたり、能力を広げて悪意のあるアクティビティ (sysadmin アカウントへの侵害など) をさらに実行したりすることができるか?
- 当該のリソースは、ビジネスクリティカルなアセット (例えば、侵害された場合、収益に大きな影響を与える可能性がある主要なビジネスシステム) なのか ?

ガイドラインは次の通りです。

- ミッションクリティカルなシステムに電力を供給するリソースや、機密性の高いデータが含まれるリソースは、75 ~ 100 の範囲で採点することができます。
- 重要な (クリティカルではない) システムに電力を供給しているリソースや、やや重要なデータを含むリソースは、25 ~ 74 の範囲で採点することができます。
- 重要でないシステムに電力を供給しているリソースや、機密でないデータを含むリソースは、0 ~ 24 の範囲で採点する必要があります。

例

```
"Criticality": 99
```

検出

`Detection` オブジェクトは、Amazon GuardDuty 拡張脅威検出からの攻撃シーケンスの検出結果に関する詳細を提供します。GuardDuty は、複数のイベントが疑わしい可能性のあるアクティビティと一致すると、攻撃シーケンスの検出結果を生成します。 AWS Security Hub CSPM で GuardDuty 攻撃シーケンスの検出結果を受信するには、アカウントで GuardDuty が有効になっている必要があります。詳細については、Amazon GuardDutyユーザーガイド」の「Amazon GuardDuty 拡張脅威検出」を参照してください。 Amazon GuardDuty

例

```
"Detection": {
    "Sequence": {
     "Uid": "1111111111111-184ec3b9-cf8d-452d-9aad-f5bdb7afb010",
     "Actors": [{
      "Id": "USER:AROA987654321EXAMPLE:i-b188560f:1234567891",
      "Session": {
       "Uid": "1234567891",
       "MfAStatus": "DISABLED",
```

```
        "CreatedTime": "1716916944000",
        "Issuer": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      },
      "User": {
        "CredentialUid": "ASIAIOSFODNN7EXAMPLE",
        "Name": "ec2_instance_role_production",
        "Type": "AssumedRole",
        "Uid": "AROA987654321EXAMPLE:i-b188560f",
        "Account": {
          "Uid": "AccountId",
          "Name": "AccountName"
        }
      }
     }],
     "Endpoints": [{
      "Id": "EndpointId",
      "Ip": "203.0.113.1",
      "Domain": "example.com",
      "Port": 4040,
      "Location": {
        "City": "New York",
        "Country": "US",
        "Lat": 40.7123,
        "Lon": -74.0068
      },
      "AutonomousSystem": {
        "Name": "AnyCompany",
        "Number": 64496
      },
      "Connection": {
        "Direction": "INBOUND"
      }
     }],
     "Signals": [{
      "Id": "arn:aws:guardduty:us-east-1:123456789012:detector/
d0bfe135ab8b4dd8c3eaae7df9900073/finding/535a382b1bcc44d6b219517a29058fb7",
      "Title": "Someone ran a penetration test tool on your account.",
      "ActorIds": ["USER:AROA987654321EXAMPLE:i-b188560f:1234567891"],
      "Count": 19,
      "FirstSeenAt": 1716916943000,
      "SignalIndicators": [
        {
          "Key": "ATTACK_TACTIC",
          "Title": "Attack Tactic",
```

```
        "Values": [
         "Impact"
        ]
       },
       {
        "Key": "HIGH_RISK_API",
        "Title": "High Risk Api",
        "Values": [
         "s3:DeleteObject"
        ]
       },
       {
        "Key": "ATTACK_TECHNIQUE",
        "Title": "Attack Technique",
        "Values": [
         "Data Destruction"
        ]
       },
      ],
      "LastSeenAt": 1716916944000,
      "Name": "Test:IAMUser/KaliLinux",
      "ResourceIds": [
       "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      ],
      "Type": "FINDING"
     }],
     "SequenceIndicators": [
      {
       "Key": "ATTACK_TACTIC",
       "Title": "Attack Tactic",
       "Values": [
        "Discovery",
        "Exfiltration",
        "Impact"
       ]
      },
      {
       "Key": "HIGH_RISK_API",
       "Title": "High Risk Api",
       "Values": [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBuckets"
        "s3:ListObjects"
```

```
        ]
      },
      {
       "Key": "ATTACK_TECHNIQUE",
       "Title": "Attack Technique",
       "Values": [
        "Cloud Service Discovery",
        "Data Destruction"
       ]
      }
     ]
    }
}
```

FindingProviderFields

`FindingProviderFields` には次の属性が含まれます。

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

上記のフィールドは `FindingProviderFields` オブジェクトの下にネストされますが、最上位の ASFF フィールドと同じ名前のアナログがあります。検出結果プロバイダーによって新しい検出結果が Security Hub CSPM に送信されると、対応する最上位フィールドに基づいて`FindingProviderFields`空のオブジェクトが自動的に入力されます。

検出結果プロバイダーは、Security Hub CSPM API の オペレーション`FindingProviderFields`を使用して`BatchImportFindings`更新できます。検出結果プロバイダーは、このオブジェクトを `BatchUpdateFindings` で更新できません。

Security Hub CSPM が から `BatchImportFindings` `FindingProviderFields`および対応する最上位属性への更新を処理する方法の詳細については、「」を参照してくださいthe section called “FindingProviderFields での結果の更新”。

お客様は、`BatchUpdateFindings` オペレーションを使用して最上位フィールドを更新できます。お客様は `FindingProviderFields` を更新できません。

例

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

FirstObservedAt

検出結果によってキャプチャされた潜在的なセキュリティ上の問題またはイベントが最初に検出された日時を示します。

このタイムスタンプは、イベントまたは脆弱性が最初に検出された日時を指定します。したがって、この結果レコードが作成された日時を反映するCreatedAtタイムスタンプとは異なる場合があります。

Security Hub CSPM が生成および更新するコントロールの検出結果については、このタイムスタンプは、リソースのコンプライアンスステータスが最後に変更された日時を示すこともできます。他のタイプの検出結果では、このタイムスタンプは検出結果レコードの更新間で変更できませんが、より正確なタイムスタンプが決定された場合は更新できます。

例

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

検出結果によってキャプチャされた潜在的なセキュリティ問題またはイベントが、セキュリティ検出結果製品によって最後に検出された日時を示します。

このタイムスタンプは、イベントまたは脆弱性が最後に検出された日時を指定します。したがって、これはこの結果記録が最後に更新された日時または最近更新された日時が反映される UpdatedAt タイムスタンプとは異なる可能性があります。

このタイムスタンプを提供することもできますが、最初の観測時には必要ありません。最初の観察時にこのフィールドを入力する場合、タイムスタンプはFirstObservedAtタイムスタンプと同じである必要があります。結果が観測されるたびに、最後に検出されたタイムスタンプを反映するようにこのフィールドを更新する必要があります。

例

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

Malware

Malware オブジェクトは、検出結果に関連するマルウェアのリストを提供します。

例

```
"Malware": [
    {
        "Name": "Stringler",
        "Type": "COIN_MINER",
        "Path": "/usr/sbin/stringler",
        "State": "OBSERVED"
    }
]
```

Network (廃止)

Network オブジェクトは、結果に関するネットワーク関連情報を提供します。

このオブジェクトは廃止されました。このデータを提供するには、Resources 内のリソースにデータをマッピングするか、Action オブジェクトを使用できます。

例

```
"Network": {
    "Direction": "IN",
    "OpenPortRange": {
        "Begin": 443,
        "End": 443
```

```
    },
    "Protocol": "TCP",
    "SourceIpV4": "1.2.3.4",
    "SourceIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "SourcePort": "42",
    "SourceDomain": "example1.com",
    "SourceMac": "00:0d:83:b1:c0:8e",
    "DestinationIpV4": "2.3.4.5",
    "DestinationIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "DestinationPort": "80",
    "DestinationDomain": "example2.com"
}
```

NetworkPath

NetworkPath オブジェクトは、結果に関連するネットワークパスに関する情報を提供します。NetworkPath 内の各エントリは、パスのコンポーネントを表しています。

例

```
"NetworkPath" : [
    {
        "ComponentId": "abc-01a234bc56d8901ee",
        "ComponentType": "AWS::EC2::InternetGateway",
        "Egress": {
            "Destination": {
                "Address": [ "192.0.2.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": ["203.0.113.0/24"]
            }
        },
        "Ingress": {
            "Destination": {
                "Address": [ "198.51.100.0/24" ],
                "PortRanges": [
```

```
                    {
                        "Begin": 443,
                        "End": 443
                    }
                ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": [ "203.0.113.0/24" ]
            }
        }
    }
]
```

メモ

Note オブジェクトは、結果に追加できるユーザー定義のメモを指定します。

結果プロバイダーは、結果に対する最初のメモは提供できますが、それ以降にメモを追加することはできません。メモは BatchUpdateFindings を使用してのみ更新できます。

例

```
"Note": {
    "Text": "Don't forget to check under the mat.",
    "UpdatedBy": "jsmith",
    "UpdatedAt": "2018-08-31T00:15:09Z"
}
```

PatchSummary

PatchSummary オブジェクトは、選択したコンプライアンス標準に対するインスタンスのパッチコンプライアンス状態についての概要を提供します。

例

```
"PatchSummary" : {
    "FailedCount" : 0,
    "Id" : "pb-123456789098",
    "InstalledCount" : 100,
    "InstalledOtherCount" : 1023,
    "InstalledPendingReboot" : 0,
    "InstalledRejectedCount" : 0,
```

```
    "MissingCount" : 100,
    "Operation" : "Install",
    "OperationEndTime" : "2018-09-27T23:39:31Z",
    "OperationStartTime" : "2018-09-27T23:37:31Z",
    "RebootOption" : "RebootIfNeeded"
}
```

プロセス

`Process` オブジェクトは、結果に関するプロセス関連の詳細を提供します。

例:

```
"Process": {
    "LaunchedAt": "2018-09-27T22:37:31Z",
    "Name": "syslogd",
    "ParentPid": 56789,
    "Path": "/usr/sbin/syslogd",
    "Pid": 12345,
    "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

Security Hub CSPM が検出結果を受け取り、処理を開始した日時を示します。

これは、検出結果プロバイダーとセキュリティ問題`CreatedAt`および検出結果とのやり取りに関連する必須のタイムスタンプ`UpdatedAt`である および とは異なります。`ProcessedAt` タイムスタンプは、Security Hub CSPM が検出結果の処理を開始するタイミングを示します。処理が完了すると、検出結果はユーザーのアカウントに表示されます。

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

セキュリティ検出結果製品に、定義された AWS Security Finding 形式に含まれないソリューション固有の追加の詳細を含めることができるデータ型。

Security Hub CSPM コントロールによって生成された検出結果の場合、 にはコントロールに関する情報`ProductFields`が含まれます。「the section called “コントロールの結果を生成および更新する”」を参照してください。

このフィールドには冗長データを含めず、 AWS Security Finding 形式フィールドと競合するデータを含めないでください。

aws/「」プレフィックスは、 AWS 製品およびサービスの予約済み名前空間のみを表し、サードパーティー統合の結果とともに送信しないでください。

必須ではありませんが、製品はフィールド名を company-id/product-id/field-name のフォーマットにすることが推奨されます。ここにある、company-id と product-id は、結果の ProductArn にあるものと一致します。

参照するフィールドArchivalは、Security Hub CSPM が既存の検出結果をアーカイブするときに使用されます。例えば、コントロールまたは標準を無効にするとき、および統合コントロールの検出結果をオンまたはオフにするときに、Security Hub CSPM は既存の検出結果をアーカイブします。

このフィールドには、検出結果を生成したコントロールを含む標準に関する情報が含まれる場合もあります。

例

```
"ProductFields": {
    "API", "DeleteTrail",
    "ArchivalReasons:0/Description": "The finding is in an ARCHIVED state because
 consolidated control findings has been turned on or off. This causes findings in the
 previous state to be archived when new findings are being generated.",
    "ArchivalReasons:0/ReasonCode": "CONSOLIDATED_CONTROL_FINDINGS_UPDATE",
    "aws/inspector/AssessmentTargetName": "My prod env",
    "aws/inspector/AssessmentTemplateName": "My daily CVE assessment",
    "aws/inspector/RulesPackageName": "Common Vulnerabilities and Exposures",
    "generico/secure-pro/Action.Type", "AWS_API_CALL",
    "generico/secure-pro/Count": "6",
    "Service_Name": "cloudtrail.amazonaws.com"
}
```

ProductName

結果を生成した製品の名前を提供します。コントロールベースの検出結果の場合、製品名は Security Hub CSPM です。

Security Hub CSPM は、検出結果ごとにこの属性を自動的に入力します。BatchImportFindings または BatchUpdateFindings を使用して更新することはできません。カスタム統合を使用している場合は例外です。「the section called “カスタム製品の統合”」を参照してください。

Security Hub CSPM コンソールを使用して製品名で結果をフィルタリングする場合は、この属性を使用します。

Security Hub CSPM API を使用して製品名で検出結果をフィルタリングする場合は、 の `aws/securityhub/ProductName` 属性を使用します`ProductFields`。

Security Hub CSPM は、これらの 2 つの属性を同期しません。

RecordState

結果のレコード状態を提供します。

デフォルトでは、サービスによって最初に生成されたときの結果は `ACTIVE` と見なされます。

`ARCHIVED` 状態は、結果がビューで非表示になるべきであることを示します。アーカイブされた検出結果はすぐには削除されません。検索やレビュー、レポートを行うことができます。関連付けられたリソースが削除された場合、リソースが存在しない場合、またはコントロールが無効になっている場合、Security Hub CSPM はコントロールベースの検出結果を自動的にアーカイブします。

`RecordState` は検出結果プロバイダーを対象としており、 `BatchImportFindings`オペレーションを使用してのみ更新できます。`BatchUpdateFindings` オペレーションを使用して更新することはできません。

結果に対する調査状態を追跡する場合は、`RecordState` ではなく `Workflow` を使用してください。

レコードの状態が から `ARCHIVED`に変わり`ACTIVE`、検出結果のワークフローステータスが `NOTIFIED`または の場合`RESOLVED`、Security Hub CSPM は自動的にワークフローステータスを に変更します`NEW`。

例

```
"RecordState": "ACTIVE"
```

リージョン

結果の生成 AWS リージョン 元の を指定します。

Security Hub CSPM は、検出結果ごとにこの属性を自動的に入力します。`BatchImportFindings` または `BatchUpdateFindings` を使用して更新することはできません。

例

```
"Region": "us-west-2"
```

RelatedFindings

現在の検出結果に関連する検出結果のリストを提供します。

RelatedFindings は、BatchUpdateFindings API オペレーションでのみ更新してください。このオブジェクトは BatchImportFindings で更新しないでください。

BatchImportFindings リクエストの場合、検出結果プロバイダーは FindingProviderFields の RelatedFindings オブジェクトを使用する必要があります。

RelatedFindings 属性の説明を表示するには、RelatedFindingSecurity Hub CSPM API リファレンスの「」を参照してください。 AWS

例

```
"RelatedFindings": [
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000" },
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "AcmeNerfHerder-111111111111-x189dx7824" }
]
```

RiskAssessment

例

```
"RiskAssessment": {
    "Posture": {
        "FindingTotal": 4,
        "Indicators": [
            {
                "Type": "Reachability",
                "Findings": [
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/1234567890abcdef0",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    },
```

```
                    {
                        "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/
abcdef01234567890",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    }
                ]
            },
            {
                "Type": "Vulnerability",
                "Findings": [
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/021345abcdef6789",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    },
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/021345ghijkl6789",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    }
                ]
            }
        ]
    }
}
```

修正

Remediation オブジェクトは、検出結果に対処するために推奨される修復ステップに関する情報を提供します。

例

```
"Remediation": {
    "Recommendation": {
        "Text": "For instructions on how to fix this issue, see the AWS Security Hub
 CSPM documentation for EC2.2.",
```

```
        "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation"
    }
}
```

サンプル

検出結果がサンプルの検出結果かどうかを指定します。

```
"Sample": true
```

SourceUrl

`SourceUrl` オブジェクトは、検出製品内の現在の結果に関するページにリンクする URL を提供します。

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

`ThreatIntelIndicator` オブジェクトは、結果に関連する脅威インテリジェンスの詳細を提供します。

例

```
"ThreatIntelIndicators": [
  {
    "Category": "BACKDOOR",
    "LastObservedAt": "2018-09-27T23:37:31Z",
    "Source": "Threat Intel Weekly",
    "SourceUrl": "http://threatintelweekly.org/backdoors/8888",
    "Type": "IPV4_ADDRESS",
    "Value": "8.8.8.8",
  }
]
```

脅威

Threats オブジェクトは、検出結果によって検出された脅威の詳細を表示します。

例

```
"Threats": [{
```

```
    "FilePaths": [{
        "FileName": "b.txt",
        "FilePath": "/tmp/b.txt",
        "Hash": "sha256",
        "ResourceId": "arn:aws:ec2:us-west-2:123456789012:volume/vol-032f3bdd89aee112f"
    }],
    "ItemCount": 3,
    "Name": "Iot.linux.mirai.vwisi",
    "Severity": "HIGH"
}]
```

UserDefinedFields

検出結果に関連付けられている名前と値の文字列ペアのリストを提供します。検出結果に追加されるカスタムのユーザー定義フィールドです。これらのフィールドは、特定の設定で自動生成されることがあります。

検出結果プロバイダーでは、このフィールドを製品で生成されるデータに使用しないでください。代わりに、検出結果プロバイダーは標準の AWS Security Finding Format `ProductFields`フィールドにマッピングされないデータに フィールドを使用できます。

これらのフィールドは、`BatchUpdateFindings` を使用してのみ更新できます。

例

```
"UserDefinedFields": {
    "reviewedByCio": "true",
    "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

検出結果の正確性を提供します。結果プロバイダーは、このフィールドに値 `UNKNOWN` を設定できます。検出製品のシステムに意味のあるアナログが存在する場合、検出製品はこの値を提供する必要があります。このフィールドは一般的に、結果調査後のユーザーの決定またはアクションに従って入力されます。

検出結果プロバイダーはこの属性の初期値を提供できますが、それ以降は更新できません。この属性は、`BatchUpdateFindings` を使用してのみ更新できます。

```
"VerificationState": "Confirmed"
```

脆弱性

Vulnerabilities オブジェクトは、結果に関連付けられている脆弱性のリストを提供します。

例

```
"Vulnerabilities" : [
    {
        "CodeVulnerabilities": [{
            "Cwes": [
                "CWE-798",
                "CWE-799"
            ],
            "FilePath": {
                "EndLine": 421,
                "FileName": "package-lock.json",
                "FilePath": "package-lock.json",
                "StartLine": 420
            },
                "SourceArn":"arn:aws:lambda:us-east-1:123456789012:layer:AWS-AppConfig-
Extension:114"
        }],
        "Cvss": [
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N",
                "Version": "V3"
            },
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:L/AC:M/Au:N/C:C/I:N/A:N",
                "Version": "V2"
            }
        ],
        "EpssScore": 0.015,
        "ExploitAvailable": "YES",
        "FixAvailable": "YES",
        "Id": "CVE-2020-12345",
        "LastKnownExploitAt": "2020-01-16T00:01:35Z",
        "ReferenceUrls":[
           "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12418",
            "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17563"
        ],
        "RelatedVulnerabilities": ["CVE-2020-12345"],
```

```
        "Vendor": {
            "Name": "Alas",
            "Url":"https://alas.aws.amazon.com/ALAS-2020-1337.html",
            "VendorCreatedAt":"2020-01-16T00:01:43Z",
            "VendorSeverity":"Medium",
            "VendorUpdatedAt":"2020-01-16T00:01:43Z"
        },
        "VulnerablePackages": [
            {
                "Architecture": "x86_64",
                "Epoch": "1",
                "FilePath": "/tmp",
                "FixedInVersion": "0.14.0",
                "Name": "openssl",
                "PackageManager": "OS",
                "Release": "16.amzn2.0.3",
                "Remediation": "Update aws-crt to 0.14.0",
                "SourceLayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:id",
                "SourceLayerHash":
 "sha256:c1962c35b63a6ff6ce7df6e042ee82371a605ca9515569edec46ff14f926f001",
                "Version": "1.0.2k"
            }
        ]
    }
]
```

ワークフロー

`Workflow` オブジェクトは、検出結果の調査ステータスに関する情報を提供します。

このフィールドは、お客様が修復、オーケストレーション、チケット発行ツールで使用することを目的としています。検出結果プロバイダーを見つけるためのものではありません。

`Workflow` フィールドは `BatchUpdateFindings` でのみ更新できます。お客様は、コンソールから更新することもできます。「the section called “結果のワークフローステータスを設定する”」を参照してください。

例

```
"Workflow": {
    "Status": "NEW"
}
```

WorkflowState (廃止)

このオブジェクトは廃止され、`Workflow` オブジェクトの `Status` フィールドによって置き換えられています。

このフィールドは、検出結果のワークフローステータスを提供します。検出製品は、このフィールドに値 `NEW` を設定できます。検出製品のシステムに意味のあるアナログが存在する場合、検出製品はこの値を提供することができます。

例

```
"WorkflowState": "NEW"
```

Resources ASFF オブジェクト

AWS Security Finding Format (ASFF) では、 `Resources` オブジェクトは検出結果に関連するリソースに関する情報を提供します。最大 32 個のリソースからなるオブジェクト配列が含まれます。リソース名のフォーマット方法については、「AWS Security Finding 形式 (ASFF)」を参照してください。各リソースオブジェクトの例については、以下のリストからリソースを選択してください。

トピック

- ASFF のリソース属性
- ASFF の AwsAmazonMQ リソース
- ASFF の AwsApiGateway リソース
- ASFF の AwsAppSync リソース
- ASFF の AwsAthena リソース
- ASFF の AwsAutoScaling リソース
- ASFF の AwsBackup リソース
- ASFF の AwsCertificateManager リソース
- ASFF の AwsCloudFormation リソース
- ASFF の AwsCloudFront リソース
- ASFF の AwsCloudTrail リソース
- ASFF の AwsCloudWatch リソース
- ASFF の AwsCodeBuild リソース
- ASFF の AwsDms リソース
- ASFF の AwsDynamoDB リソース

- ASFF の AwsEc2 リソース
- ASFF の AwsEcr リソース
- ASFF の AwsEcs リソース
- ASFF の AwsEfs リソース
- ASFF の AwsEks リソース
- ASFF の AwsElasticBeanstalk リソース
- ASFF の AwsElasticSearch リソース
- ASFF の AwsElb リソース
- ASFF の AwsEventBridge リソース
- ASFF の AwsGuardDuty リソース
- ASFF の AwsIam リソース
- ASFF の AwsKinesis リソース
- ASFF の AwsKms リソース
- AwsLambda
- ASFF の AwsMsk リソース
- ASFF の AwsNetworkFirewall リソース
- ASFF の AwsOpenSearchService リソース
- ASFF の AwsRds リソース
- ASFF の AwsRedshift リソース
- ASFF の AwsRoute53 リソース
- ASFF の AwsS3 リソース
- ASFF の AwsSageMaker リソース
- ASFF の AwsSecretsManager リソース
- ASFF の AwsSns リソース
- ASFF の AwsSqs リソース
- ASFF の AwsSsm リソース
- ASFF の AwsStepFunctions リソース
- ASFF の AwsWaf リソース
- ASFF の AwsXray リソース
- CodeRepository ASFF の オブジェクト

- Container ASFF の オブジェクト
- Other ASFF の オブジェクト

ASFF のリソース属性

AWS Security Finding 形式 (ASFF) の `Resources` オブジェクトの説明と例を次に示します。これらのフィールドの詳細については、「リソース」を参照してください。

ApplicationArn

検出結果に関連するアプリケーションの Amazon リソースネーム (ARN) を識別します。

例

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0"
```

ApplicationName

検出結果に関連するアプリケーションの名前を識別します。

例

```
"ApplicationName": "SampleApp"
```

DataClassification

DataClassification フィールドは、リソースで検出された機密データに関する情報を提供します。

例

```
"DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
```

```
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
                        }
                    },
                    {
                        "Count": 59,
                        "Type": "EMAIL_ADDRESS",
                        "Occurrences": {
                            "Pages": [
                                {
                                    "PageNumber": 1,
                                    "OffsetRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                     },
                                    "LineRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                    }
                                }
                            ]
                        }
                    },
                    {
                        "Count": 2229,
                        "Type": "URL",
                        "Occurrences": {
```

```
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 13
                                }
                            ]
                        }
                    },
                    {
                        "Count": 13826,
                        "Type": "NameDetection",
                        "Occurrences": {
                             "Records": [
                                 {
                                     "RecordIndex": 1,
                                     "JsonPath": "$.ssn.value"
                                 }
                             ]
                         }
                    },
                    {
                        "Count": 32,
                        "Type": "AddressDetection"
                    }
                ],
                "TotalCount": 32
            }
        ],
        "CustomDataIdentifiers": {
            "Detections": [
                 {
                     "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                     "Name": "1712be25e7c7f53c731fe464f1c869b8",
                     "Count": 2,
                 }
            ],
            "TotalCount": 2
        }
    }
}
```

詳細

Details フィールドは、適切なオブジェクトを使用する単一のリソースに関する追加情報を提供します。各リソースは、Resources オブジェクト内の個別のリソースオブジェクトで指定する必要があります。

結果のサイズが最大の 240 KB を超えた場合、Details オブジェクトは結果から削除されます。AWS Config ルールを使用するコントロールの検出結果については、 AWS Config コンソールでリソースの詳細を表示できます。

Security Hub には、サポートされているリソースタイプに使用できる一連のリソースの詳細が用意されています。これらの詳細は、Type オブジェクトの値に対応しています。可能な場合、提供されたタイプを使用してください。

例えば、リソースが S3 バケットの場合、リソース Type を AwsS3Bucket に設定し、AwsS3Bucket オブジェクトにリソースの詳細を指定します。

Other オブジェクトでは、カスタムのフィールドや値を指定できます。Other オブジェクトは、次の場合に使用できます。

- リソースタイプ (リソース Type の値) に対応する詳細オブジェクトがない場合。リソースの詳細を指定するには、Other オブジェクトを使用します。
- リソースタイプのオブジェクトに、入力するすべてのフィールドが含まれていない場合。この場合は、リソースタイプの詳細オブジェクトを使用して、使用可能なフィールドに入力します。Other オブジェクトを使用して、タイプ固有のオブジェクトに含まれていないフィールドに入力してください。
- リソースタイプが提供されたタイプのいずれでもない場合。この場合、Resource.Type を Other に設定し、Other オブジェクトを使用して詳細を入力します。

例

```
"Details": {
  "AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IpV4Addresses": ["1.1.1.1"],
    "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
```

```
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    },
    "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
    ],
    "SubnetId": "PublicSubnet",
    "Type": "i3.xlarge",
    "VirtualizationType": "hvm",
    "VpcId": "TestVPCIpv6"
  },
  "AwsS3Bucket": {
    "OwnerId": "da4d66eac431652a4d44d490a00500bded52c97d235b7b4752f9f688566fe6de",
    "OwnerName": "acmes3bucketowner"
  },
  "Other": { "LightPen": "blinky", "SerialNo": "1234abcd"}
}
```

ID

指定されたリソースタイプの識別子。

Amazon AWS リソースネーム (ARNs) で識別されるリソースの場合、これは ARN です。

ARN がない AWS リソースの場合、これはリソースを AWS 作成したサービスによって定義された識別子です。 ARNs

AWS リソース以外の場合、これはリソースに関連付けられている一意の識別子です。

例

```
"Id": "arn:aws:s3:::amzn-s3-demo-bucket"
```

パーティション

リソースが置かれているパーティション。パーティションは のグループです AWS リージョン。各 AWS アカウント は 1 つのパーティションにスコープされます。

以下のパーティションがサポートされています。

- `aws` – AWS リージョン
- `aws-cn` - 中国リージョン
- `aws-us-gov` – AWS GovCloud (US) Region

例

```
"Partition": "aws"
```

リージョン

このリソース AWS リージョン が配置されている のコード。リージョンコードの一覧については、「リージョンエンドポイント」を参照してください。

例

```
"Region": "us-west-2"
```

ResourceRole

結果におけるリソースのロールを識別します。リソースは、結果アクティビティのターゲットか、アクティビティを実行するアクターのどちらかです。

例

```
"ResourceRole": "target"
```

[タグ]

このフィールドには、検出結果に関連するリソースのタグキーと値情報が表示されます。Tagging API の `GetResources`オペレーションでサポートされているリソースに AWS Resource Groups タグを付けることができます。Security Hub は、サービスにリンクされたロールを介してこのオペレーションを呼び出し、 AWS Security Finding Format (ASFF) `Resource.Id`フィールドにリソース ARN が入力されている場合に AWS リソースタグを取得します。無効なリソース ID は無視されます。

Security Hub が取り込む検出結果には、統合製品 AWS のサービス やサードパーティー製品の検出結果など、リソースタグを追加できます。

タグを追加すると、検出結果が処理された時点でリソースに関連付けられていたタグがわかります。タグが関連付けられているリソースにのみ、Tags 属性を含めることができます。リソースにタグが関連付けられていない場合は、結果に Tags 属性を含めないでください。

検出結果にリソースタグを含めることで、データエンリッチメントパイプラインを構築したり、セキュリティ検出結果のメタデータを手動で強化したりする必要がなくなります。タグを使用して、検出結果とインサイトを検索またはフィルタリングし、自動化ルールを作成することもできます。

タグに適用される制限の詳細については、「タグの命名制限と要件」を参照してください。

このフィールドには、 AWS リソースに存在するタグのみを指定できます。 AWS Security Finding 形式で定義されていないデータを提供するには、Other詳細サブフィールドを使用します。

例

```
"Tags": {
    "billingCode": "Lotus-1-2-3",
    "needsPatching": "true"
}
```

タイプ

詳細を提供しているリソースのタイプです。

可能な限り、提供されているリソースタイプの中の 1 つ (AwsEc2Instance または AwsS3Bucket など) を使用してください。

リソースタイプが提供されているリソースタイプと一致しない場合は、リソース Type を Other に設定し、Other 詳細サブフィールドを使用して詳細を入力します。

サポートされる値のリストについては、「Resources」を参照してください。

例

```
"Type": "AwsS3Bucket"
```

ASFF の AwsAmazonMQ リソース

以下は、 AwsAmazonMQリソースの AWS Security Finding Format (ASFF) 構文の例です。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsAmazonMQBroker

`AwsAmazonMQBroker` は、Amazon MQ で実行されるメッセージブローカー環境である Amazon MQ ブローカーに関する情報を提供します。

次の例は、`AwsAmazonMQBroker` オブジェクトの ASFF を示しています。`AwsAmazonMQBroker` 属性の詳細については、「AWS Security Hub API リファレンス」の「AwsAmazonMQBroker」を参照してください。

例

```
"AwsAmazonMQBroker": {
    "AutoMinorVersionUpgrade": true,
    "BrokerArn": "arn:aws:mq:us-east-1:123456789012:broker:TestBroker:b-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerId": "b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerName": "TestBroker",
    "Configuration": {
        "Id": "c-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "Revision": 1
    },
    "DeploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
    "EncryptionOptions": {
        "UseAwsOwnedKey": true
    },
    "EngineType": "ActiveMQ",
    "EngineVersion": "5.17.2",
    "HostInstanceType": "mq.t2.micro",
    "Logs": {
        "Audit": false,
        "AuditLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/
audit",
        "General": false,
        "GeneralLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111/general"
    },
    "MaintenanceWindowStartTime": {
        "DayOfWeek": "MONDAY",
        "TimeOfDay": "22:00",
        "TimeZone": "UTC"
    },
    "PubliclyAccessible": true,
    "SecurityGroups": [
```

```
        "sg-021345abcdef6789"
    ],
    "StorageType": "efs",
    "SubnetIds": [
        "subnet-1234567890abcdef0",
        "subnet-abcdef01234567890"
    ],
    "Users": [
        {
            "Username": "admin"
        }
    ]
}
```

ASFF の AwsApiGateway リソース

`AwsApiGateway` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsApiGatewayRestApi

`AwsApiGatewayRestApi` オブジェクトには、Amazon API Gateway のバージョン 1 の REST API に関する情報が含まれています。

以下は、 AWS Security Finding 形式 (ASFF) の `AwsApiGatewayRestApi` 検出の例です。`AwsApiGatewayRestApi` 属性の詳細については、AWS Security Hub APIリファレンスの「AwsApiGatewayRestApiDetails」を参照してください。

例

```
AwsApiGatewayRestApi: {
    "Id": "exampleapi",
    "Name": "Security Hub",
    "Description": "AWS Security Hub",
    "CreatedDate": "2018-11-18T10:20:05-08:00",
    "Version": "2018-10-26",
    "BinaryMediaTypes" : ["-'*~1*'"],
    "MinimumCompressionSize": 1024,
    "ApiKeySource": "AWS_ACCOUNT_ID",
    "EndpointConfiguration": {
        "Types": [
```

```
            "REGIONAL"
        ]
    }
}
```

AwsApiGatewayStage

`AwsApiGatewayStage` オブジェクトは、Amazon API Gateway ステージ バージョン 1 に関する情報を提供します。

以下は、 AWS Security Finding 形式 (ASFF) の `AwsApiGatewayStage` 検出の例です。`AwsApiGatewayStage` 属性の詳細については、AWS Security Hub API リファレンスの「AwsApiGatewayStageDetails」を参照してください。

例

```
"AwsApiGatewayStage": {
    "DeploymentId": "n7hlmf",
    "ClientCertificateId": "a1b2c3",
    "StageName": "Prod",
    "Description" : "Stage Description",
    "CacheClusterEnabled": false,
    "CacheClusterSize" : "1.6",
    "CacheClusterStatus": "NOT_AVAILABLE",
    "MethodSettings": [
        {
            "MetricsEnabled": true,
            "LoggingLevel": "INFO",
            "DataTraceEnabled": false,
            "ThrottlingBurstLimit": 100,
            "ThrottlingRateLimit": 5.0,
            "CachingEnabled": false,
            "CacheTtlInSeconds": 300,
            "CacheDataEncrypted": false,
            "RequireAuthorizationForCacheControl": true,
            "UnauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER",
            "HttpMethod": "POST",
            "ResourcePath": "/echo"
        }
    ],
    "Variables": {"test": "value"},
    "DocumentationVersion": "2.0",
    "AccessLogSettings": {
```

```
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "CanarySettings": {
        "PercentTraffic": 0.0,
        "DeploymentId": "ul73s8",
        "StageVariableOverrides" : [
            "String" : "String"
        ],
        "UseStageCache": false
    },
    "TracingEnabled": false,
    "CreatedDate": "2018-07-11T10:55:18-07:00",
    "LastUpdatedDate": "2020-08-26T11:51:04-07:00",
    "WebAclArn" : "arn:aws:waf-regional:us-west-2:111122223333:webacl/
cb606bd8-5b0b-4f0b-830a-dd304e48a822"
}
```

AwsApiGatewayV2Api

`AwsApiGatewayV2Api` オブジェクトには、Amazon API Gateway のバージョン 2 API に関する情報が含まれています。

以下は、 AWS Security Finding 形式 (ASFF) の `AwsApiGatewayV2Api` 検出の例です。`AwsApiGatewayV2Api` 属性の詳細については、AWS Security Hub API リファレンスの「AwsApiGatewayV2ApiDetails」を参照してください。

例

```
"AwsApiGatewayV2Api": {
    "ApiEndpoint": "https://example.us-west-2.amazonaws.com",
    "ApiId": "a1b2c3d4",
    "ApiKeySelectionExpression": "$request.header.x-api-key",
    "CreatedDate": "2020-03-28T00:32:37Z",
   "Description": "ApiGatewayV2 Api",
   "Version": "string",
    "Name": "my-api",
    "ProtocolType": "HTTP",
    "RouteSelectionExpression": "$request.method $request.path",
   "CorsConfiguration": {
        "AllowOrigins": [ "*" ],
        "AllowCredentials": true,
        "ExposeHeaders": [ "string" ],
        "MaxAge": 3000,
        "AllowMethods": [
          "GET",
          "PUT",
          "POST",
          "DELETE",
          "HEAD"
        ],
        "AllowHeaders": [ "*" ]
    }
}
```

AwsApiGatewayV2Stage

`AwsApiGatewayV2Stage` には、Amazon API Gateway のバージョン 2 ステージに関する情報が含まれています。

以下は、 AWS Security Finding 形式 (ASFF) の `AwsApiGatewayV2Stage` 検出の例です。`AwsApiGatewayV2Stage` 属性の詳細については、AWS Security Hub API リファレンスの「AwsApiGatewayV2StageDetails」を参照してください。

例

```
"AwsApiGatewayV2Stage": {
    "CreatedDate": "2020-04-08T00:36:05Z",
    "Description" : "ApiGatewayV2",
    "DefaultRouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
```

```
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "DeploymentId": "x1zwyv",
    "LastUpdatedDate": "2020-04-08T00:36:13Z",
    "RouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "StageName": "prod",
    "StageVariables": [
        "function": "my-prod-function"
    ],
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "AutoDeploy": false,
    "LastDeploymentStatusMessage": "Message",
    "ApiGatewayManaged": true,
}
```

ASFF の AwsAppSync リソース

AwsAppSync リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsAppSyncGraphQLApi

AwsAppSyncGraphQLApi は、アプリケーションの最上位コンストラクトである AWS AppSync GraphQL API に関する情報を提供します。

次の例は、AwsAppSyncGraphQLApi オブジェクトの ASFF を示しています。AwsAppSyncGraphQLApi 属性の詳細については、「AWS Security Hub API リファレンス」の「AwsAppSyncGraphQLApi」を参照してください。

例

```
"AwsAppSyncGraphQLApi": {
    "AdditionalAuthenticationProviders": [
    {
     "AuthenticationType": "AWS_LAMBDA",
     "LambdaAuthorizerConfig": {
      "AuthorizerResultTtlInSeconds": 300,
      "AuthorizerUri": "arn:aws:lambda:us-east-1:123456789012:function:mylambdafunc"
     }
    },
    {
     "AuthenticationType": "AWS_IAM"
    }
    ],
    "ApiId": "021345abcdef6789",
    "Arn": "arn:aws:appsync:eu-central-1:123456789012:apis/021345abcdef6789",
    "AuthenticationType": "API_KEY",
    "Id": "021345abcdef6789",
    "LogConfig": {
     "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/appsync-
graphqlapi-logs-eu-central-1",
     "ExcludeVerboseContent": true,
     "FieldLogLevel": "ALL"
    },
    "Name": "My AppSync App",
    "XrayEnabled": true,
}
```

ASFF の AwsAthena リソース

`AwsAthena` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsAthenaWorkGroup

`AwsAthenaWorkGroup` は、Amazon Athena ワークグループに関する情報を提供します。ワークグループは、ユーザー、チーム、アプリケーション、ワークロードを分離するのに役立ちます。また、データ処理の制限を設定したり、コストを追跡したりするのにも役立ちます。

次の例は、`AwsAthenaWorkGroup` オブジェクトの ASFF を示しています。`AwsAthenaWorkGroup` 属性の詳細については、AWS Security Hub API リファレンスの「AwsAthenaWorkGroup」を参照してください。

例

```
"AwsAthenaWorkGroup": {
    "Description": "My workgroup for prod workloads",
    "Name": "MyWorkgroup",
    "WorkgroupConfiguration" {
        "ResultConfiguration": {
            "EncryptionConfiguration": {
                "EncryptionOption": "SSE_KMS",
                "KmsKey": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
            }
        }
    },
        "State": "ENABLED"
}
```

ASFF の AwsAutoScaling リソース

`AwsAutoScaling` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsAutoScalingAutoScalingGroup

`AwsAutoScalingAutoScalingGroup` オブジェクトは、オートスケーリンググループの詳細を提供します。

以下は、 AWS Security Finding 形式 (ASFF) の `AwsAutoScalingAutoScalingGroup` 検出の例です。`AwsAutoScalingAutoScalingGroup` 属性の詳細については、AWS Security Hub API リファレンスの「AwsAutoScalingAutoScalingGroupDetails」を参照してください。

例

```
"AwsAutoScalingAutoScalingGroup": {
        "CreatedTime": "2017-10-17T14:47:11Z",
        "HealthCheckGracePeriod": 300,
        "HealthCheckType": "EC2",
        "LaunchConfigurationName": "mylaunchconf",
        "LoadBalancerNames": [],
        "LaunchTemplate": {
            "LaunchTemplateId": "string",
            "LaunchTemplateName": "string",
            "Version": "string"
        },
        "MixedInstancesPolicy": {
            "InstancesDistribution": {
                "OnDemandAllocationStrategy": "prioritized",
                "OnDemandBaseCapacity": number,
                "OnDemandPercentageAboveBaseCapacity": number,
                "SpotAllocationStrategy": "lowest-price",
                "SpotInstancePools": number,
                "SpotMaxPrice": "string"
            },
            "LaunchTemplate": {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "string",
                    "LaunchTemplateName": "string",
                    "Version": "string"
                 },
                "CapacityRebalance": true,
                "Overrides": [
                    {
                       "InstanceType": "string",
                       "WeightedCapacity": "string"
                    }
```

```
                ]
            }
        }
    }
}
```

AwsAutoScalingLaunchConfiguration

`AwsAutoScalingLaunchConfiguration` オブジェクトは、起動設定に関する詳細を提供します。

Security AWS Finding 形式 (ASFF) の検出`AwsAutoScalingLaunchConfiguration`結果の例を次に示します。

`AwsAutoScalingLaunchConfiguration` 属性の詳細については、AWS Security Hub API リファレンスの「AwsAutoScalingLaunchConfigurationDetails」を参照してください。

例

```
AwsAutoScalingLaunchConfiguration: {
    "LaunchConfigurationName": "newtest",
    "ImageId": "ami-058a3739b02263842",
    "KeyName": "55hundredinstance",
    "SecurityGroups": [ "sg-01fce87ad6e019725" ],
    "ClassicLinkVpcSecurityGroups": [],
    "UserData": "...Base64-Encoded user data..."
    "InstanceType": "a1.metal",
    "KernelId": "",
    "RamdiskId": "ari-a51cf9cc",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/sdh",
            "Ebs": {
                "VolumeSize": 30,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true,
                "SnapshotId": "snap-ffaa1e69",
                "VirtualName": "ephemeral1"
            }
        },
        {
            "DeviceName": "/dev/sdb",
```

```
            "NoDevice": true
        },
        {
            "DeviceName": "/dev/sda1",
            "Ebs": {
                "SnapshotId": "snap-02420cd3d2dea1bc0",
                "VolumeSize": 8,
                "VolumeType": "gp2",
                "DeleteOnTermination": true,
                "Encrypted": false
            }
        },
        {
            "DeviceName": "/dev/sdi",
            "Ebs": {
                "VolumeSize": 20,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true
            }
        },
        {
            "DeviceName": "/dev/sdc",
            "NoDevice": true
        }
    ],
    "InstanceMonitoring": {
        "Enabled": false
    },
    "CreatedTime": 1620842933453,
    "EbsOptimized": false,
    "AssociatePublicIpAddress": true,
    "SpotPrice": "0.045"
}
```

ASFF の AwsBackup リソース

`AwsBackup` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsBackupBackupPlan

AwsBackupBackupPlan オブジェクトは、 AWS Backup のバックアップ計画に関する情報を提供します。 AWS Backup バックアッププランは、 AWS リソースをバックアップするタイミングと方法を定義するポリシー式です。

次の例は、 AwsBackupBackupPlan オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsBackupBackupPlan 属性の詳細については、AWS Security Hub API リファレンスの「AwsBackupBackupPlan」を参照してください。

例

```
"AwsBackupBackupPlan": {
    "BackupPlan": {
     "AdvancedBackupSettings": [{
      "BackupOptions": {
       "WindowsVSS":"enabled"
      },
      "ResourceType":"EC2"
     }],
     "BackupPlanName": "test",
     "BackupPlanRule": [{
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "DailyBackups",
      "ScheduleExpression": "cron(0 5 ? * * *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
      },
      {
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
```

```
        "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
        "Lifecycle": {
         "DeleteAfterDays": 365,
         "MoveToColdStorageAfterDays": 30
        }
       }],
       "Lifecycle": {
        "DeleteAfterDays": 35
       },
       "RuleName": "Monthly",
       "ScheduleExpression": "cron(0 5 1 * ? *)",
       "StartWindowMinutes": 480,
       "TargetBackupVault": "Default"
      }]
     },
     "BackupPlanArn": "arn:aws:backup:us-east-1:858726136373:backup-
plan:b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
     "BackupPlanId": "b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
     "VersionId": "ZDVjNDIzMjItYTZiNS00NzczLTg4YzctNmExMWM2NjZhY2E1"
}
```

AwsBackupBackupVault

`AwsBackupBackupVault` オブジェクトは、 AWS Backup のバックアップボールトに関する情報を提供します。 AWS Backup バックアップボールトは、バックアップを保存および整理するコンテナです。

次の例は、 `AwsBackupBackupVault` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsBackupBackupVault` 属性の詳細については、AWS Security Hub API リファレンスの「AwsBackupBackupVault」を参照してください。

例

```
"AwsBackupBackupVault": {
    "AccessPolicy": {
     "Statement": [{
      "Action": [
       "backup:DeleteBackupVault",
       "backup:DeleteBackupVaultAccessPolicy",
       "backup:DeleteRecoveryPoint",
       "backup:StartCopyJob",
       "backup:StartRestoreJob",
```

```
        "backup:UpdateRecoveryPointLifecycle"
      ],
      "Effect": "Deny",
      "Principal": {
       "AWS": "*"
      },
      "Resource": "*"
     }],
     "Version": "2012-10-17"
    },
    "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:aws/efs/
automatic-backup-vault",
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "EncrytionKeyArn": "arn:aws:kms:us-east-1:444455556666:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "Notifications": {
     "BackupVaultEvents": ["BACKUP_JOB_STARTED", "BACKUP_JOB_COMPLETED",
 "COPY_JOB_STARTED"],
     "SNSTopicArn": "arn:aws:sns:us-west-2:111122223333:MyVaultTopic"
    }
}
```

AwsBackupRecoveryPoint

`AwsBackupRecoveryPoint` オブジェクトは、 AWS Backup のバックアップに関する情報 (復旧ポイント) を提供します。 AWS Backup 復旧ポイントは、指定した時刻のリソースの内容を表します。

次の例は、 `AwsBackupRecoveryPoint` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsBackupBackupVault` 属性の詳細については、AWS Security Hub API リファレンスの「AwsBackupRecoveryPoint」を参照してください。

例

```
"AwsBackupRecoveryPoint": {
    "BackupSizeInBytes": 0,
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "BackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/
automatic-backup-vault",
    "CalculatedLifecycle": {
     "DeleteAt": "2021-08-30T06:51:58.271Z",
     "MoveToColdStorageAt": "2020-08-10T06:51:58.271Z"
    },
```

```
    "CompletionDate": "2021-07-26T07:21:40.361Z",
    "CreatedBy": {
     "BackupPlanArn": "arn:aws:backup:us-east-1:111122223333:backup-plan:aws/
efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanId": "aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanVersion": "ZGM4YzY5YjktMWYxNC00ZTBmLWE5MjYtZmU5OWNiZmM5ZjIz",
     "BackupRuleId": "2a600c2-42ad-4196-808e-084923ebfd25"
    },
    "CreationDate": "2021-07-26T06:51:58.271Z",
    "EncryptionKeyArn": "arn:aws:kms:us-east-1:111122223333:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "IamRoleArn": "arn:aws:iam::111122223333:role/aws-service-role/
backup.amazonaws.com/AWSServiceRoleForBackup",
    "IsEncrypted": true,
    "LastRestoreTime": "2021-07-26T06:51:58.271Z",
    "Lifecycle": {
     "DeleteAfterDays": 35,
     "MoveToColdStorageAfterDays": 15
    },
    "RecoveryPointArn": "arn:aws:backup:us-east-1:111122223333:recovery-point:151a59e4-
f1d5-4587-a7fd-0774c6e91268",
    "ResourceArn": "arn:aws:elasticfilesystem:us-east-1:858726136373:file-system/
fs-15bd31a1",
    "ResourceType": "EFS",
    "SourceBackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/
efs/automatic-backup-vault",
    "Status": "COMPLETED",
    "StatusMessage": "Failure message",
    "StorageClass": "WARM"
}
```

ASFF の AwsCertificateManager リソース

以下は、 `AwsCertificateManager`リソースの AWS Security Finding Format (ASFF) 構文の例です。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsCertificateManagerCertificate

`AwsCertificateManagerCertificate` オブジェクトは、 AWS Certificate Manager (ACM) 証明書に関する詳細を提供します。

Security AWS Finding 形式 (ASFF) の検出`AwsCertificateManagerCertificate`結果の例を次に示します。`AwsCertificateManagerCertificate` 属性の詳細については、AWS Security Hub API リファレンスの「AwsCertificateManagerCertificateDetails」を参照してください。

例

```
"AwsCertificateManagerCertificate": {
    "CertificateAuthorityArn": "arn:aws:acm:us-west-2:444455556666:certificate-
authority/example",
    "CreatedAt": "2019-05-24T18:12:02.000Z",
    "DomainName": "example.amazondomains.com",
    "DomainValidationOptions": [
        {
            "DomainName": "example.amazondomains.com",
            "ResourceRecord": {
                "Name": "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                "Type": "CNAME",
                "Value": "_example.acm-validations.aws."
             },
             "ValidationDomain": "example.amazondomains.com",
             "ValidationEmails": [sample_email@sample.com],
             "ValidationMethod": "DNS",
             "ValidationStatus": "SUCCESS"
        }
    ],
    "ExtendedKeyUsages": [
        {
            "Name": "TLS_WEB_SERVER_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.1"
        },
        {
            "Name": "TLS_WEB_CLIENT_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.2"
        }
    ],
    "FailureReason": "",
    "ImportedAt": "2018-08-17T00:13:00.000Z",
    "InUseBy": ["arn:aws:amazondomains:us-west-2:444455556666:loadbalancer/example"],
    "IssuedAt": "2020-04-26T00:41:17.000Z",
    "Issuer": "Amazon",
    "KeyAlgorithm": "RSA-1024",
    "KeyUsages": [
        {
```

```
            "Name": "DIGITAL_SIGNATURE",
        },
        {
            "Name": "KEY_ENCIPHERMENT",
        }
    ],
    "NotAfter": "2021-05-26T12:00:00.000Z",
    "NotBefore": "2020-04-26T00:00:00.000Z",
    "Options": {
        "CertificateTransparencyLoggingPreference": "ENABLED",
    }
    "RenewalEligibility": "ELIGIBLE",
    "RenewalSummary": {
        "DomainValidationOptions": [
            {
                "DomainName": "example.amazondomains.com",
                "ResourceRecord": {
                    "Name":
 "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                    "Type": "CNAME",
                    "Value": "_example.acm-validations.aws.com",
                },
                "ValidationDomain": "example.amazondomains.com",
                "ValidationEmails": ["sample_email@sample.com"],
                "ValidationMethod": "DNS",
                "ValidationStatus": "SUCCESS"
            }
        ],
        "RenewalStatus": "SUCCESS",
        "RenewalStatusReason": "",
        "UpdatedAt": "2020-04-26T00:41:35.000Z",
    },
    "Serial": "02:ac:86:b6:07:2f:0a:61:0e:3a:ac:fd:d9:ab:17:1a",
    "SignatureAlgorithm": "SHA256WITHRSA",
    "Status": "ISSUED",
    "Subject": "CN=example.amazondomains.com",
    "SubjectAlternativeNames": ["example.amazondomains.com"],
    "Type": "AMAZON_ISSUED"
}
```

ASFF の AwsCloudFormation リソース

`AwsCloudFormation` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsCloudFormationStack

`AwsCloudFormationStack` オブジェクトは、 最上位のテンプレートでリソースとしてネストされている AWS CloudFormation スタックの詳細を表示します。

次の例は、 `AwsCloudFormationStack` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsCloudFormationStack` 属性の詳細については、AWS Security Hub API リファレンスの「AwsCloudFormationStackDetails」を参照してください。

例

```
"AwsCloudFormationStack": {
 "Capabilities": [
  "CAPABILITY_IAM",
  "CAPABILITY_NAMED_IAM"
 ],
 "CreationTime": "2022-02-18T15:31:53.161Z",
 "Description": "AWS CloudFormation Sample",
 "DisableRollback": true,
 "DriftInformation": {
  "StackDriftStatus": "DRIFTED"
 },
 "EnableTerminationProtection": false,
 "LastUpdatedTime": "2022-02-18T15:31:53.161Z",
 "NotificationArns": [
  "arn:aws:sns:us-east-1:978084797471:sample-sns-cfn"
 ],
 "Outputs": [{
  "Description": "URL for newly created LAMP stack",
  "OutputKey": "WebsiteUrl",
  "OutputValue": "http://ec2-44-193-18-241.compute-1.amazonaws.com"
 }],
 "RoleArn": "arn:aws:iam::012345678910:role/exampleRole",
 "StackId": "arn:aws:cloudformation:us-east-1:978084797471:stack/sample-stack/
e5d9f7e0-90cf-11ec-88c6-12ac1f91724b",
 "StackName": "sample-stack",
 "StackStatus": "CREATE_COMPLETE",
 "StackStatusReason": "Success",
 "TimeoutInMinutes": 1
}
```

ASFF の AwsCloudFront リソース

`AwsCloudFront` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsCloudFrontDistribution

`AwsCloudFrontDistribution` オブジェクトは、Amazon CloudFront ディストリビューション設定の詳細を表示します。

以下は、 AWS Security Finding 形式 (ASFF) の `AwsCloudFrontDistribution` 検出の例です。`AwsCloudFrontDistribution` 属性の詳細については、AWS Security Hub API リファレンスの「AwsCloudFrontDistributionDetails」を参照してください。

例

```
"AwsCloudFrontDistribution": {
    "CacheBehaviors": {
        "Items": [
            {
               "ViewerProtocolPolicy": "https-only"
            }
         ]
    },
    "DefaultCacheBehavior": {
         "ViewerProtocolPolicy": "https-only"
    },
    "DefaultRootObject": "index.html",
    "DomainName": "d2wkuj2w9l34gt.cloudfront.net",
    "Etag": "E37HOT42DHPVYH",
    "LastModifiedTime": "2015-08-31T21:11:29.093Z",
    "Logging": {
         "Bucket": "myawslogbucket.s3.amazonaws.com",
         "Enabled": false,
         "IncludeCookies": false,
         "Prefix": "myawslog/"
     },
     "OriginGroups": {
          "Items": [
              {
                 "FailoverCriteria": {
                     "StatusCodes": {
```

```
                        "Items": [
                            200,
                            301,
                            404
                        ]
                        "Quantity": 3
                    }
                }
            }
        ]
    },
    "Origins": {
        "Items": [
            {
                "CustomOriginConfig": {
                    "HttpPort": 80,
                    "HttpsPort": 443,
                    "OriginKeepaliveTimeout": 60,
                    "OriginProtocolPolicy": "match-viewer",
                    "OriginReadTimeout": 30,
                    "OriginSslProtocols": {
                      "Items": ["SSLv3", "TLSv1"],
                      "Quantity": 2
                    }
                }
            },
        ]
    },
                "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                "Id": "my-origin",
                "OriginPath": "/production",
                "S3OriginConfig": {
                    "OriginAccessIdentity": "origin-access-identity/cloudfront/
E2YFS67H6VB6E4"
                }
        ]
    },
    "Status": "Deployed",
    "ViewerCertificate": {
           "AcmCertificateArn": "arn:aws:acm::123456789012:AcmCertificateArn",
           "Certificate": "ASCAJRRE5XYF52TKRY5M4",
           "CertificateSource": "iam",
           "CloudFrontDefaultCertificate": true,
           "IamCertificateId": "ASCAJRRE5XYF52TKRY5M4",
```

```
            "MinimumProtocolVersion": "TLSv1.2_2021",
            "SslSupportMethod": "sni-only"
        },
        "WebAclId": "waf-1234567890"
}
```

ASFF の AwsCloudTrail リソース

`AwsCloudTrail` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsCloudTrailTrail

`AwsCloudTrailTrail` オブジェクトは、 AWS CloudTrail トレイルに関する詳細を表示します。

以下は、 AWS Security Finding 形式 (ASFF) の `AwsCloudTrailTrail` 検出の例です。`AwsCloudTrailTrail` 属性の詳細については、AWS Security Hub API リファレンスの「AwsCloudTrailTrailDetails」を参照してください。

例

```
"AwsCloudTrailTrail": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:CloudTrail/regression:*",
    "CloudWatchLogsRoleArn": "arn:aws:iam::866482105055:role/
CloudTrail_CloudWatchLogs",
    "HasCustomEventSelectors": true,
    "HomeRegion": "us-west-2",
    "IncludeGlobalServiceEvents": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "KmsKeyId": "kmsKeyId",
    "LogFileValidationEnabled": true,
    "Name": "regression-trail",
    "S3BucketName": "cloudtrail-bucket",
    "S3KeyPrefix": "s3KeyPrefix",
    "SnsTopicArn": "arn:aws:sns:us-east-2:123456789012:MyTopic",
    "SnsTopicName": "snsTopicName",
    "TrailArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail"
}
```

ASFF の AwsCloudWatch リソース

`AwsCloudWatch` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsCloudWatchAlarm

`AwsCloudWatchAlarm` オブジェクトは、アラームの状態が変化したときにメトリクスを監視するまたはアクションを実行する Amazon CloudWatch アラームの詳細を表示します。

次の例は、 `AwsCloudWatchAlarm` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsCloudWatchAlarm` 属性の詳細については、AWS Security Hub API リファレンスの「AwsCloudWatchAlarmDetails」を参照してください。

例

```
"AwsCloudWatchAlarm": {
 "ActionsEnabled": true,
 "AlarmActions": [
  "arn:aws:automate:region:ec2:stop",
  "arn:aws:automate:region:ec2:terminate"
 ],
 "AlarmArn": "arn:aws:cloudwatch:us-west-2:012345678910:alarm:sampleAlarm",
 "AlarmConfigurationUpdatedTimestamp": "2022-02-18T15:31:53.161Z",
 "AlarmDescription": "Alarm Example",
 "AlarmName": "Example",
 "ComparisonOperator": "GreaterThanOrEqualToThreshold",
 "DatapointsToAlarm": 1,
 "Dimensions": [{
  "Name": "InstanceId",
  "Value": "i-1234567890abcdef0"
 }],
 "EvaluateLowSampleCountPercentile": "evaluate",
 "EvaluationPeriods": 1,
 "ExtendedStatistic": "p99.9",
 "InsufficientDataActions": [
  "arn:aws:automate:region:ec2:stop"
 ],
 "MetricName": "Sample Metric",
 "Namespace": "YourNamespace",
 "OkActions": [
  "arn:aws:swf:region:account-id:action/actions/AWS_EC2.InstanceId.Stop/1.0"
```

```
 ],
 "Period": 1,
 "Statistic": "SampleCount",
 "Threshold": 12.3,
 "ThresholdMetricId": "t1",
 "TreatMissingData": "notBreaching",
 "Unit": "Kilobytes/Second"
}
```

ASFF の AwsCodeBuild リソース

`AwsCodeBuild` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsCodeBuildProject

`AwsCodeBuildProject` オブジェクトは、 AWS CodeBuild プロジェクトに関する情報を提供します。

以下は、 AWS Security Finding 形式 (ASFF) の `AwsCodeBuildProject` 検出の例です。`AwsCodeBuildProject` 属性の説明については、AWS Security Hub API リファレンスの「AwsCodeBuildProjectDetails」を参照してください。

例

```
"AwsCodeBuildProject": {
   "Artifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
   ],
   "SecondaryArtifacts": [
      {
          "ArtifactIdentifier": "string",
```

```
            "EncryptionDisabled": boolean,
            "Location": "string",
            "Name": "string",
            "NamespaceType": "string",
            "OverrideArtifactName": boolean,
            "Packaging": "string",
            "Path": "string",
            "Type": "string"
        }
    ],
    "EncryptionKey": "string",
    "Certificate": "string",
    "Environment": {
       "Certificate": "string",
       "EnvironmentVariables": [
            {
                 "Name": "string",
                 "Type": "string",
                 "Value": "string"
            }
       ],
    "ImagePullCredentialsType": "string",
    "PrivilegedMode": boolean,
    "RegistryCredential": {
        "Credential": "string",
        "CredentialProvider": "string"
    },
    "Type": "string"
    },
    "LogsConfig": {
         "CloudWatchLogs": {
              "GroupName": "string",
              "Status": "string",
              "StreamName": "string"
         },
         "S3Logs": {
              "EncryptionDisabled": boolean,
              "Location": "string",
              "Status": "string"
         }
    },
    "Name": "string",
    "ServiceRole": "string",
    "Source": {
```

```
        "Type": "string",
        "Location": "string",
        "GitCloneDepth": integer
    },
    "VpcConfig": {
        "VpcId": "string",
        "Subnets": ["string"],
        "SecurityGroupIds": ["string"]
    }
}
```

ASFF の AwsDms リソース

AwsDms リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsDmsEndpoint

AwsDmsEndpoint オブジェクトは、 AWS Database Migration Service （ AWS DMS) エンドポイントに関する情報を提供します。エンドポイントは、データストアに関する接続、データストアタイプ、および場所情報を提供します。

次の例は、 AwsDmsEndpoint オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsDmsEndpoint 属性の詳細については、AWS Security Hub API リファレンスの「AwsDmsEndpointDetails」を参照してください。

例

```
"AwsDmsEndpoint": {
    "CertificateArn": "arn:aws:dms:us-
east-1:123456789012:cert:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWFI",
    "DatabaseName": "Test",
    "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJVBNPK6MJQVFVQA",
    "EndpointIdentifier": "target-db",
    "EndpointType": "TARGET",
    "EngineName": "mariadb",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "Port": 3306,
```

```
    "ServerName": "target-db.exampletafyu.us-east-1.rds.amazonaws.com",
    "SslMode": "verify-ca",
    "Username": "admin"
}
```

AwsDmsReplicationInstance

`AwsDmsReplicationInstance` オブジェクトは、 AWS Database Migration Service（AWS DMS) レプリケーションインスタンスに関する情報を提供します。DMS はレプリケーション インスタンスを使用してソースデータストアに接続し、ソースデータを読み取り、ターゲットデータストアが使用できるようにデータをフォーマットします。

次の例は、 `AwsDmsReplicationInstance` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsDmsReplicationInstance` 属性の詳細については、AWS Security Hub API リファレンスの「AwsDmsReplicationInstanceDetails」を参照してください。

例

```
"AwsDmsReplicationInstance": {
    "AllocatedStorage": 50,
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1b",
    "EngineVersion": "3.5.1",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "MultiAZ": false,
    "PreferredMaintenanceWindow": "wed:08:08-wed:08:38",
    "PubliclyAccessible": true,
    "ReplicationInstanceClass": "dms.c5.xlarge",
    "ReplicationInstanceIdentifier": "second-replication-instance",
    "ReplicationSubnetGroup": {
        "ReplicationSubnetGroupIdentifier": "default-vpc-2344f44f"
    },
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-003a34e205138138b"
        }
    ]
}
```

AwsDmsReplicationTask

`AwsDmsReplicationTask` オブジェクトは、 AWS Database Migration Service （ AWS DMS) レプリケーションタスクに関する情報を提供します。レプリケーションタスクは、一連のデータをソースエンドポイントからターゲットエンドポイントに移動します。

次の例は、 `AwsDmsReplicationInstance` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsDmsReplicationInstance` 属性の詳細については、AWS Security Hub API リファレンスの「AwsDmsReplicationInstance」を参照してください。

例

```
"AwsDmsReplicationTask": {
    "CdcStartPosition": "2023-08-28T14:26:22",
    "Id": "arn:aws:dms:us-
east-1:123456789012:task:YDYUOHZIXWKQSUCBMUCQCNY44SJW74VJNB5DFWQ",
    "MigrationType": "cdc",
    "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4YOUGIMYJUI",
    "ReplicationTaskIdentifier": "test-task",
    "ReplicationTaskSettings": "{\"Logging\":{\"EnableLogging\":false,
\"EnableLogContext\":false,\"LogComponents\":[{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"TRANSFORMATION\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",
\"Id\":\"SOURCE_UNLOAD\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"IO\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TARGET_LOAD\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"PERFORMANCE\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SOURCE_CAPTURE\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SORTER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"REST_SERVER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id
\":\"VALIDATOR_EXT\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"TARGET_APPLY\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TASK_MANAGER
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TABLES_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"METADATA_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_FACTORY\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMON\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"ADDONS\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"DATA_STRUCTURE
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMUNICATION\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_TRANSFER\"}],\"CloudWatchLogGroup
\":null,\"CloudWatchLogStream\":null},\"StreamBufferSettings\":{\"StreamBufferCount
\":3,\"CtrlStreamBufferSizeInMB\":5,\"StreamBufferSizeInMB\":8},\"ErrorBehavior
\":{\"FailOnNoTablesCaptured\":true,\"ApplyErrorUpdatePolicy\":\"LOG_ERROR\",
\"FailOnTransactionConsistencyBreached\":false,\"RecoverableErrorThrottlingMax\":1800,
\"DataErrorEscalationPolicy\":\"SUSPEND_TABLE\",\"ApplyErrorEscalationCount\":0,
```

```
\"RecoverableErrorStopRetryAfterThrottlingMax\":true,\"RecoverableErrorThrottling
\":true,\"ApplyErrorFailOnTruncationDdl\":false,\"DataTruncationErrorPolicy\":
\"LOG_ERROR\",\"ApplyErrorInsertPolicy\":\"LOG_ERROR\",\"EventErrorPolicy\":
\"IGNORE\",\"ApplyErrorEscalationPolicy\":\"LOG_ERROR\",\"RecoverableErrorCount
\":-1,\"DataErrorEscalationCount\":0,\"TableErrorEscalationPolicy\":\"STOP_TASK
\",\"RecoverableErrorInterval\":5,\"ApplyErrorDeletePolicy\":\"IGNORE_RECORD\",
\"TableErrorEscalationCount\":0,\"FullLoadIgnoreConflicts\":true,\"DataErrorPolicy
\":\"LOG_ERROR\",\"TableErrorPolicy\":\"SUSPEND_TABLE\"},\"TTSettings
\":{\"TTS3Settings\":null,\"TTRecordSettings\":null,\"EnableTT\":false},
\"FullLoadSettings\":{\"CommitRate\":10000,\"StopTaskCachedChangesApplied
\":false,\"StopTaskCachedChangesNotApplied\":false,\"MaxFullLoadSubTasks
\":8,\"TransactionConsistencyTimeout\":600,\"CreatePkAfterFullLoad\":false,
\"TargetTablePrepMode\":\"DO_NOTHING\"},\"TargetMetadata\":{\"ParallelApplyBufferSize
\":0,\"ParallelApplyQueuesPerThread\":0,\"ParallelApplyThreads\":0,\"TargetSchema
\":\"\",\"InlineLobMaxSize\":0,\"ParallelLoadQueuesPerThread\":0,\"SupportLobs
\":true,\"LobChunkSize\":64,\"TaskRecoveryTableEnabled\":false,\"ParallelLoadThreads
\":0,\"LobMaxSize\":0,\"BatchApplyEnabled\":false,\"FullLobMode\":true,
\"LimitedSizeLobMode\":false,\"LoadMaxFileSize\":0,\"ParallelLoadBufferSize\":0},
\"BeforeImageSettings\":null,\"ControlTablesSettings\":{\"historyTimeslotInMinutes
\":5,\"HistoryTimeslotInMinutes\":5,\"StatusTableEnabled\":false,
\"SuspendedTablesTableEnabled\":false,\"HistoryTableEnabled\":false,\"ControlSchema
\":\"\",\"FullLoadExceptionTableEnabled\":false},\"LoopbackPreventionSettings
\":null,\"CharacterSetSettings\":null,\"FailTaskWhenCleanTaskResourceFailed
\":false,\"ChangeProcessingTuning\":{\"StatementCacheSize\":50,\"CommitTimeout
\":1,\"BatchApplyPreserveTransaction\":true,\"BatchApplyTimeoutMin\":1,
\"BatchSplitSize\":0,\"BatchApplyTimeoutMax\":30,\"MinTransactionSize\":1000,
\"MemoryKeepTime\":60,\"BatchApplyMemoryLimit\":500,\"MemoryLimitTotal\":1024},
\"ChangeProcessingDdlHandlingPolicy\":{\"HandleSourceTableDropped\":true,
\"HandleSourceTableTruncated\":true,\"HandleSourceTableAltered\":true},
\"PostProcessingRules\":null}",
    "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:TZPWV2VCXEGHYOKVKRNHAKJ4Q3RUXACNGFGYWRI",
    "TableMappings": "{\"rules\":[{\"rule-type\":\"selection\",\"rule-id\":
\"969761702\",\"rule-name\":\"969761702\",\"object-locator\":{\"schema-name\":\"%table
\",\"table-name\":\"%example\"},\"rule-action\":\"exclude\",\"filters\":[]}]}",
    "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:ABR8LBOQB3CZY33F7XV253NAJVBNPK6MJQVFVQA"
}
```


ASFF の AwsDynamoDB リソース

以下は、 AwsDynamoDBリソースの AWS Security Finding Format (ASFF) 構文の例です。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsDynamoDbTable

`AwsDynamoDbTable` オブジェクトは、Amazon DynamoDB テーブルに関する詳細を表示します。

以下は、 AWS Security Finding 形式 (ASFF) の `AwsDynamoDbTable` 検出の例です。`AwsDynamoDbTable` 属性の説明の詳細については、AWS Security Hub API リファレンスの「AwsDynamoDbTableDetails」を参照してください。

例

```
"AwsDynamoDbTable": {
    "AttributeDefinitions": [
        {
            "AttributeName": "attribute1",
            "AttributeType": "value 1"
        },
        {
            "AttributeName": "attribute2",
            "AttributeType": "value 2"
        },
        {
            "AttributeName": "attribute3",
            "AttributeType": "value 3"
        }
    ],
    "BillingModeSummary": {
        "BillingMode": "PAY_PER_REQUEST",
        "LastUpdateToPayPerRequestDateTime": "2019-12-03T15:23:10.323Z"
    },
    "CreationDateTime": "2019-12-03T15:23:10.248Z",
    "DeletionProtectionEnabled": true,
    "GlobalSecondaryIndexes": [
        {
            "Backfilling": false,
            "IndexArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
index/exampleIndex",
            "IndexName": "standardsControlArnIndex",
            "IndexSizeBytes": 1862513,
            "IndexStatus": "ACTIVE",
            "ItemCount": 20,
            "KeySchema": [
```

```
                {
                    "AttributeName": "City",
                    "KeyType": "HASH"
                },
                {
                    "AttributeName": "Date",
                    "KeyType": "RANGE"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
            "ProvisionedThroughput": {
                "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
                "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
                "NumberOfDecreasesToday": 0,
                "ReadCapacityUnits": 100,
                "WriteCapacityUnits": 50
            },
        }
    ],
    "GlobalTableVersion": "V1",
    "ItemCount": 2705,
    "KeySchema": [
        {
            "AttributeName": "zipcode",
            "KeyType": "HASH"
        }
     ],
     "LatestStreamArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
stream/2019-12-03T23:23:10.248",
     "LatestStreamLabel": "2019-12-03T23:23:10.248",
     "LocalSecondaryIndexes": [
        {
            "IndexArn": "arn:aws:dynamodb:us-east-1:111122223333:table/exampleGroup/
index/exampleId",
            "IndexName": "CITY_DATE_INDEX_NAME",
            "KeySchema": [
                {
                    "AttributeName": "zipcode",
                    "KeyType": "HASH"
                }
            ],
```

```
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
        }
    ],
    "ProvisionedThroughput": {
        "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
        "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
        "NumberOfDecreasesToday": 0,
        "ReadCapacityUnits": 100,
        "WriteCapacityUnits": 50
    },
    "Replicas": [
        {
            "GlobalSecondaryIndexes":[
                {
                    "IndexName": "CITY_DATE_INDEX_NAME",
                    "ProvisionedThroughputOverride": {
                        "ReadCapacityUnits": 10
                    }
                }
            ],
            "KmsMasterKeyId" : "KmsKeyId"
            "ProvisionedThroughputOverride": {
                "ReadCapacityUnits": 10
            },
            "RegionName": "regionName",
            "ReplicaStatus": "CREATING",
            "ReplicaStatusDescription": "replicaStatusDescription"
        }
    ],
    "RestoreSummary" : {
        "SourceBackupArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
backup/backup1",
        "SourceTableArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable",
        "RestoreDateTime": "2020-06-22T17:40:12.322Z",
        "RestoreInProgress": true
    },
    "SseDescription": {
        "InaccessibleEncryptionDateTime": "2018-01-26T23:50:05.000Z",
        "Status": "ENABLED",
        "SseType": "KMS",
        "KmsMasterKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key1"
```

```
    },
    "StreamSpecification" : {
        "StreamEnabled": true,
        "StreamViewType": "NEW_IMAGE"
    },
    "TableId": "example-table-id-1",
    "TableName": "example-table",
    "TableSizeBytes": 1862513,
    "TableStatus": "ACTIVE"
}
```

ASFF の AwsEc2 リソース

`AwsEc2` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsEc2ClientVpnEndpoint

`AwsEc2ClientVpnEndpoint` オブジェクトは、 AWS Client VPN エンドポイントに関する情報を提供します。クライアント VPN エンドポイントは、クライアント VPN セッションを有効にして管理するために作成して設定するリソースです。これは、すべてのクライアント VPN セッションの終了ポイントです。

次の例は、 `AwsEc2ClientVpnEndpoint` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEc2ClientVpnEndpoint` 属性の詳細については、「AWS Security Hub API リファレンス」の「AwsEc2ClientVpnEndpointDetails」を参照してください。

例

```
"AwsEc2ClientVpnEndpoint": {
    "AuthenticationOptions": [
        {
            "MutualAuthentication": {
                "ClientRootCertificateChainArn": "arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            },
            "Type": "certificate-authentication"
        }
    ],
    "ClientCidrBlock": "10.0.0.0/22",
```

```
    "ClientConnectOptions": {
        "Enabled": false
    },
    "ClientLoginBannerOptions": {
        "Enabled": false
    },
    "ClientVpnEndpointId": "cvpn-endpoint-00c5d11fc4729f2a5",
    "ConnectionLogOptions": {
        "Enabled": false
    },
    "Description": "test",
    "DnsServer": ["10.0.0.0"],
    "ServerCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "SecurityGroupIdSet": [
        "sg-0f7a177b82b443691"
    ],
    "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/endpoints/
cvpn-endpoint-00c5d11fc4729f2a5",
    "SessionTimeoutHours": 24,
    "SplitTunnel": false,
    "TransportProtocol": "udp",
    "VpcId": "vpc-1a2b3c4d5e6f1a2b3",
    "VpnPort": 443
}
```

AwsEc2Eip

`AwsEc2Eip` オブジェクトは、Elastic IP アドレスに関する情報を提供します。

次の例は、 `AwsEc2Eip` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEc2Eip` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEc2EipDetails」を参照してください。

例

```
"AwsEc2Eip": {
    "InstanceId": "instance1",
    "PublicIp": "192.0.2.04",
    "AllocationId": "eipalloc-example-id-1",
    "AssociationId": "eipassoc-example-id-1",
    "Domain": "vpc",
    "PublicIpv4Pool": "anycompany",
```

```
    "NetworkBorderGroup": "eu-central-1",
    "NetworkInterfaceId": "eni-example-id-1",
    "NetworkInterfaceOwnerId": "777788889999",
    "PrivateIpAddress": "192.0.2.03"
}
```

AwsEc2Instance

`AwsEc2Instance` オブジェクトは、Amazon EC2 インスタンスの詳細を提供します。

次の例は、 `AwsEc2Instance` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEc2Instance` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEc2InstanceDetails」を参照してください。

例

```
"AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
    "ImageId": "ami-1234",
    "IpV4Addresses": [ "1.1.1.1" ],
    "IpV6Addresses": [ "2001:db8:1234:1a2b::123" ],
    "KeyName": "my_keypair",
    "LaunchedAt": "2018-05-08T16:46:19.000Z",
    "MetadataOptions": {
     "HttpEndpoint": "enabled",
     "HttpProtocolIpv6": "enabled",
     "HttpPutResponseHopLimit": 1,
     "HttpTokens": "optional",
     "InstanceMetadataTags": "disabled",
    },
    "Monitoring": {
     "State": "disabled"
    },
    "NetworkInterfaces": [
      {
         "NetworkInterfaceId": "eni-e5aa89a3"
      }
    ],
    "SubnetId": "subnet-123",
    "Type": "i3.xlarge",
    "VpcId": "vpc-123"
}
```

AwsEc2LaunchTemplate

`AwsEc2LaunchTemplate` オブジェクトには、インスタンス設定情報を指定する Amazon Elastic Compute Cloud の起動テンプレートに関する詳細が含まれています。

次の例は、 `AwsEc2LaunchTemplate` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEc2LaunchTemplate` 属性の詳細については、「AWS Security Hub API リファレンス」の「AwsEc2LaunchTemplateDetails」を参照してください。

例

```
"AwsEc2LaunchTemplate": {
    "DefaultVersionNumber": "1",
    "ElasticGpuSpecifications": ["string"],
    "ElasticInferenceAccelerators": ["string"],
    "Id": "lt-0a16e9802800bdd85",
    "ImageId": "ami-0d5eff06f840b45e9",
    "LatestVersionNumber": "1",
    "LaunchTemplateData": {
     "BlockDeviceMappings": [{
      "DeviceName": "/dev/xvda",
      "Ebs": {
       "DeleteonTermination": true,
       "Encrypted": true,
       "SnapshotId": "snap-01047646ec075f543",
       "VolumeSize": 8,
       "VolumeType:" "gp2"
      }
     }],
     "MetadataOptions": {
      "HttpTokens": "enabled",
      "HttpPutResponseHopLimit" : 1
     },
     "Monitoring": {
      "Enabled": true,
     "NetworkInterfaces": [{
      "AssociatePublicIpAddress" : true,
     }],
    "LaunchTemplateName": "string",
    "LicenseSpecifications": ["string"],
    "SecurityGroupIds": ["sg-01fce87ad6e019725"],
    "SecurityGroups": ["string"],
    "TagSpecifications": ["string"]
```

```
}
```

AwsEc2NetworkAcl

`AwsEc2NetworkAcl` オブジェクトには、Amazon EC2 ネットワークアクセスコントロールリスト (ACL) の詳細が含まれています。

次の例は、 `AwsEc2NetworkAcl` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEc2NetworkAcl` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEc2NetworkAclDetails」を参照してください。

例

```
"AwsEc2NetworkAcl": {
    "IsDefault": false,
    "NetworkAclId": "acl-1234567890abcdef0",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234abcd",
    "Associations": [{
        "NetworkAclAssociationId": "aclassoc-abcd1234",
        "NetworkAclId": "acl-021345abcdef6789",
        "SubnetId": "subnet-abcd1234"
   }],
   "Entries": [{
        "CidrBlock": "10.24.34.0/23",
        "Egress": true,
        "IcmpTypeCode": {
            "Code": 10,
            "Type": 30
        },
        "Ipv6CidrBlock": "2001:DB8::/32",
        "PortRange": {
            "From": 20,
            "To": 40
        },
        "Protocol": "tcp",
        "RuleAction": "allow",
        "RuleNumber": 100
   }]
}
```

AwsEc2NetworkInterface

`AwsEc2NetworkInterface` オブジェクトは、Amazon EC2 ネットワークインターフェイスに関する情報を提供します。

次の例は、 `AwsEc2NetworkInterface` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEc2NetworkInterface` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEc2NetworkInterfaceDetails」を参照してください。

例

```
"AwsEc2NetworkInterface": {
    "Attachment": {
        "AttachTime": "2019-01-01T03:03:21Z",
        "AttachmentId": "eni-attach-43348162",
        "DeleteOnTermination": true,
        "DeviceIndex": 123,
        "InstanceId": "i-1234567890abcdef0",
        "InstanceOwnerId": "123456789012",
        "Status": 'ATTACHED'
    },
    "SecurityGroups": [
        {
            "GroupName": "my-security-group",
            "GroupId": "sg-903004f8"
        },
    ],
    "NetworkInterfaceId": 'eni-686ea200',
    "SourceDestCheck": false
}
```

AwsEc2RouteTable

`AwsEc2RouteTable` オブジェクトは、Amazon EC2 ルートテーブルに関する情報を提供します。

次の例は、 `AwsEc2RouteTable` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEc2RouteTable` 属性の詳細については、「AWS Security Hub API リファレンス」の「AwsEc2RouteTableDetails」を参照してください。

例

```
"AwsEc2RouteTable": {
    "AssociationSet": [{
```

```
      "AssociationSet": {
       "State": "associated"
         },
      "Main": true,
      "RouteTableAssociationId": "rtbassoc-08e706c45de9f7512",
      "RouteTableId": "rtb-0a59bde9cf2548e34",
     }],
     "PropogatingVgwSet": [],
     "RouteTableId": "rtb-0a59bde9cf2548e34",
     "RouteSet": [
      {
       "DestinationCidrBlock": "10.24.34.0/23",
       "GatewayId": "local",
       "Origin": "CreateRouteTable",
       "State": "active"
      },
      {
       "DestinationCidrBlock": "10.24.34.0/24",
       "GatewayId": "igw-0242c2d7d513fc5d3",
       "Origin": "CreateRoute",
       "State": "active"
      }
     ],
     "VpcId": "vpc-0c250a5c33f51d456"
}
```

AwsEc2SecurityGroup

`AwsEc2SecurityGroup` オブジェクトは、Amazon EC2 セキュリティグループについての説明を表示します。

次の例は、 `AwsEc2SecurityGroup` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEc2SecurityGroup` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEc2SecurityGroupDetails」を参照してください。

例

```
"AwsEc2SecurityGroup": {
    "GroupName": "MySecurityGroup",
    "GroupId": "sg-903004f8",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1a2b3c4d",
    "IpPermissions": [
```

```
        {
            "IpProtocol": "-1",
            "IpRanges": [],
            "UserIdGroupPairs": [
                {
                    "UserId": "123456789012",
                    "GroupId": "sg-903004f8"
                }
            ],
            "PrefixListIds": [
                {"PrefixListId": "pl-63a5400a"}
            ]
        },
        {
            "PrefixListIds": [],
            "FromPort": 22,
            "IpRanges": [
                {
                    "CidrIp": "203.0.113.0/24"
                }
            ],
            "ToPort": 22,
            "IpProtocol": "tcp",
            "UserIdGroupPairs": []
        }
    ]
}
```

AwsEc2Subnet

`AwsEc2Subnet`オブジェクトは、Amazon EC2 内のサブネットに関する情報を提供します。

次の例は、 `AwsEc2Subnet` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEc2Subnet` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEc2SubnetDetails」を参照してください。

例

```
AwsEc2Subnet: {
    "AssignIpv6AddressOnCreation": false,
    "AvailabilityZone": "us-west-2c",
    "AvailabilityZoneId": "usw2-az3",
    "AvailableIpAddressCount": 8185,
```

```
    "CidrBlock": "10.0.0.0/24",
    "DefaultForAz": false,
    "MapPublicIpOnLaunch": false,
    "OwnerId": "123456789012",
    "State": "available",
    "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/subnet-d5436c93",
    "SubnetId": "subnet-d5436c93",
    "VpcId": "vpc-153ade70",
    "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "subnet-cidr-assoc-EXAMPLE",
        "Ipv6CidrBlock": "2001:DB8::/32",
        "CidrBlockState": "associated"
   }]
}
```

AwsEc2TransitGateway

`AwsEc2TransitGateway` オブジェクトは、仮想プライベートクラウド (VPC) とオンプレミスネットワークを相互接続する Amazon EC2 トランジットゲートウェイに関する詳細を提供します。

AWS Security Finding 形式 (ASFF) の検出`AwsEc2TransitGateway`結果の例を次に示します。`AwsEc2TransitGateway` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEc2TransitGatewayDetails」を参照してください。

例

```
"AwsEc2TransitGateway": {
 "AmazonSideAsn": 65000,
 "AssociationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "AutoAcceptSharedAttachments": "disable",
 "DefaultRouteTableAssociation": "enable",
 "DefaultRouteTablePropagation": "enable",
 "Description": "sample transit gateway",
 "DnsSupport": "enable",
 "Id": "tgw-042ae6bf7a5c126c3",
 "MulticastSupport": "disable",
 "PropagationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "TransitGatewayCidrBlocks": ["10.0.0.0/16"],
 "VpnEcmpSupport": "enable"
}
```

AwsEc2Volume

`AwsEc2Volume` オブジェクトは、Amazon EC2 ボリュームに関する詳細を提供します。

次の例は、 `AwsEc2Volume` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEc2Volume` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEc2VolumeDetails」を参照してください。

例

```
"AwsEc2Volume": {
    "Attachments": [
      {
        "AttachTime": "2017-10-17T14:47:11Z",
        "DeleteOnTermination": true,
        "InstanceId": "i-123abc456def789g",
        "Status": "attached"
      }
     ],
    "CreateTime": "2020-02-24T15:54:30Z",
    "Encrypted": true,
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "Size": 80,
    "SnapshotId": "",
    "Status": "available"
}
```

AwsEc2Vpc

`AwsEc2Vpc` オブジェクトは、Amazon EC2 VPC の詳細を提供します。

次の例は、 `AwsEc2Vpc` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEc2Vpc` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEc2VpcDetails」を参照してください。

例

```
"AwsEc2Vpc": {
    "CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlock": "192.0.2.0/24",
```

```
            "CidrBlockState": "associated"
        }
    ],
    "DhcpOptionsId": "dopt-4e42ce28",
    "Ipv6CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlockState": "associated",
            "Ipv6CidrBlock": "192.0.2.0/24"
       }

    ],
    "State": "available"
}
```

AwsEc2VpcEndpointService

`AwsEc2VpcEndpointService` オブジェクトには、VPC エンドポイントサービスの設定に関する詳細が含まれています。

次の例は、 `AwsEc2VpcEndpointService` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEc2VpcEndpointService` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEc2VpcEndpointServiceDetails」を参照してください。

例

```
"AwsEc2VpcEndpointService": {
    "ServiceType": [
      {
        "ServiceType": "Interface"
      }
    ],
    "ServiceId": "vpce-svc-example1",
    "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example1",
    "ServiceState": "Available",
    "AvailabilityZones": [
      "us-east-1"
    ],
    "AcceptanceRequired": true,
    "ManagesVpcEndpoints": false,
    "NetworkLoadBalancerArns": [
      "arn:aws:elasticloadbalancing:us-east-1:444455556666:loadbalancer/net/my-network-
load-balancer/example1"
```

```
    ],
    "GatewayLoadBalancerArns": [],
    "BaseEndpointDnsNames": [
      "vpce-svc-04eec859668b51c34.us-east-1.vpce.amazonaws.com"
    ],
    "PrivateDnsName": "my-private-dns"
}
```

AwsEc2VpcPeeringConnection

`AwsEc2VpcPeeringConnection` オブジェクトは、2 つの VPC 間のネットワーク接続に関する詳細を表示します。

次の例は、 `AwsEc2VpcPeeringConnection` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEc2VpcPeeringConnection` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEc2VpcPeeringConnectionDetails」を参照してください。

例

```
"AwsEc2VpcPeeringConnection": {
 "AccepterVpcInfo": {
  "CidrBlock": "10.0.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "10.0.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
 },
 "ExpirationTime": "2022-02-18T15:31:53.161Z",
 "RequesterVpcInfo": {
  "CidrBlock": "192.168.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "192.168.0.0/28"
  }],
```

```
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
 },
 "Status": {
  "Code": "initiating-request",
  "Message": "Active"
 },
 "VpcPeeringConnectionId": "pcx-1a2b3c4d"
}
```

ASFF の AwsEcr リソース

`AwsEcr` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsEcrContainerImage

`AwsEcrContainerImage` オブジェクトは、Amazon ECR イメージに関する情報を提供します。

次の例は、 `AwsEcrContainerImage` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEcrContainerImage` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEcrContainerImageDetails」を参照してください。

例

```
"AwsEcrContainerImage": {
    "RegistryId": "123456789012",
    "RepositoryName": "repository-name",
    "Architecture": "amd64"
    "ImageDigest":
 "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
    "ImageTags": ["00000000-0000-0000-0000-000000000000"],
```

```
    "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

`AwsEcrRepository` オブジェクトは、Amazon Elastic Container Registry リポジトリに関する情報を提供します。

次の例は、 `AwsEcrRepository` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEcrRepository` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEcrRepositoryDetails」を参照してください。

例

```
"AwsEcrRepository": {
    "LifecyclePolicy": {
        "RegistryId": "123456789012",
    },
    "RepositoryName": "sample-repo",
    "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
    "ImageScanningConfiguration": {
        "ScanOnPush": true
    },
    "ImageTagMutability": "IMMUTABLE"
}
```

ASFF の AwsEcs リソース

`AwsEcs` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsEcsCluster

`AwsEcsCluster` オブジェクトは、Amazon Elastic Container Service クラスターに関する詳細を提供します。

次の例は、 `AwsEcsCluster` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEcsCluster` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEcsClusterDetails」を参照してください。

例

```
    "AwsEcsCluster": {
        "CapacityProviders": [],
        "ClusterSettings": [
            {
                "Name": "containerInsights",
                "Value": "enabled"
            }
        ],
        "Configuration": {
            "ExecuteCommandConfiguration": {
                "KmsKeyId": "kmsKeyId",
                "LogConfiguration": {
                    "CloudWatchEncryptionEnabled": true,
                    "CloudWatchLogGroupName": "cloudWatchLogGroupName",
                    "S3BucketName": "s3BucketName",
                    "S3EncryptionEnabled": true,
                    "S3KeyPrefix": "s3KeyPrefix"
                },
                "Logging": "DEFAULT"
            }
        }
        "DefaultCapacityProviderStrategy": [
            {
                "Base": 0,
                "CapacityProvider": "capacityProvider",
                "Weight": 1
            }
        ]
    }
```

AwsEcsContainer

`AwsEcsContainer` オブジェクトには、Amazon ECS コンテナの詳細が含まれています。

次の例は、 `AwsEcsContainer` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEcsContainer` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEcsContainerDetails」を参照してください。

例

```
"AwsEcsContainer": {
    "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
```

```
    "MountPoints": [{
        "ContainerPath": "/mnt/etc",
        "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
}
```

AwsEcsService

`AwsEcsService` オブジェクトは、Amazon ECS クラスター内のサービスに関する詳細を提供します。

次の例は、 `AwsEcsService` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEcsService` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEcsServiceDetails」を参照してください。

例

```
"AwsEcsService": {
    "CapacityProviderStrategy": [
        {
            "Base": 12,
            "CapacityProvider": "",
            "Weight": ""
        }
    ],
    "Cluster": "arn:aws:ecs:us-east-1:111122223333:cluster/example-ecs-cluster",
    "DeploymentConfiguration": {
        "DeploymentCircuitBreaker": {
            "Enable": false,
            "Rollback": false
        },
        "MaximumPercent": 200,
        "MinimumHealthyPercent": 100
    },
    "DeploymentController": "",
    "DesiredCount": 1,
    "EnableEcsManagedTags": false,
    "EnableExecuteCommand": false,
    "HealthCheckGracePeriodSeconds": 1,
    "LaunchType": "FARGATE",
    "LoadBalancers": [
```

```
        {
            "ContainerName": "",
            "ContainerPort": 23,
            "LoadBalancerName": "",
            "TargetGroupArn": ""
        }
    ],
    "Name": "sample-app-service",
    "NetworkConfiguration": {
        "AwsVpcConfiguration": {
            "Subnets": [
                "Subnet-example1",
                "Subnet-example2"
            ],
        "SecurityGroups": [
                "Sg-0ce48e9a6e5b457f5"
        ],
        "AssignPublicIp": "ENABLED"
        }
    },
    "PlacementConstraints": [
        {
            "Expression": "",
            "Type": ""
        }
    ],
    "PlacementStrategies": [
        {
            "Field": "",
            "Type": ""
        }
    ],
    "PlatformVersion": "LATEST",
    "PropagateTags": "",
    "Role": "arn:aws:iam::111122223333:role/aws-servicerole/ecs.amazonaws.com/
ServiceRoleForECS",
    "SchedulingStrategy": "REPLICA",
    "ServiceName": "sample-app-service",
    "ServiceArn": "arn:aws:ecs:us-east-1:111122223333:service/example-ecs-cluster/
sample-app-service",
    "ServiceRegistries": [
        {
            "ContainerName": "",
            "ContainerPort": 1212,
```

```
            "Port": 1221,
            "RegistryArn": ""
        }
    ],
    "TaskDefinition": "arn:aws:ecs:us-east-1:111122223333:task-definition/example-
taskdef:1"
}
```

AwsEcsTask

`AwsEcsTask` オブジェクトは、Amazon ECS タスクの詳細を提供します。

次の例は、 `AwsEcsTask` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEcsTask` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEcsTask」を参照してください。

例

```
"AwsEcsTask": {
 "ClusterArn": "arn:aws:ecs:us-west-2:123456789012:task/MyCluster/1234567890123456789",
 "CreatedAt": "1557134011644",
 "Group": "service:fargate-service",
 "StartedAt": "1557134011644",
 "StartedBy": "ecs-svc/1234567890123456789",
 "TaskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-definition/sample-
fargate:2",
 "Version": 3,
 "Volumes": [{
  "Name": "string",
  "Host": {
   "SourcePath": "string"
  }
 }],
 "Containers": {
  "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
   "ContainerPath": "/mnt/etc",
   "SourceVolume": "vol-03909e9"
  }],
  "Name": "knote",
  "Privileged": true
 }
```

```
}
```

AwsEcsTaskDefinition

`AwsEcsTaskDefinition` オブジェクトには、タスク定義に関する詳細が含まれています。タスク定義は、Amazon Elastic Container Service タスクのコンテナとボリューム定義について説明しています。

次の例は、 `AwsEcsTaskDefinition` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEcsTaskDefinition` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEcsTaskDefinitionDetails」を参照してください。

例

```
    "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [
            {
                "Command": ['ruby', 'hi.rb'],
                "Cpu":128,
                "Essential": true,
                "HealthCheck": {
                    "Command": ["CMD-SHELL", "curl -f http://localhost/ || exit 1"],
                    "Interval": 10,
                    "Retries": 3,
                    "StartPeriod": 5,
                    "Timeout": 20
                },
                "Image": "tongueroo/sinatra:latest",
                "Interactive": true,
                "Links": [],
                "LogConfiguration": {
                    "LogDriver": "awslogs",
                    "Options": {
                        "awslogs-group": "/ecs/sinatra-hi",
                        "awslogs-region": "ap-southeast-1",
                        "awslogs-stream-prefix": "ecs"
                    },
                    "SecretOptions": []

                },
                "MemoryReservation": 128,
                "Name": "web",
                "PortMappings": [
```

```
                    {
                        "ContainerPort": 4567,
                        "HostPort":4567,
                        "Protocol": "tcp"
                    }
                ],
                "Privileged": true,
                "StartTimeout": 10,
                "StopTimeout": 100,
            }
        ],
        "Family": "sinatra-hi",
        "NetworkMode": "host",
        "RequiresCompatibilities": ["EC2"],
        "Status": "ACTIVE",
        "TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
    }
```

ASFF の AwsEfs リソース

`AwsEfs` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsEfsAccessPoint

`AwsEfsAccessPoint` オブジェクトは Amazon Elastic File System に保存されているファイルに関する詳細を表示します。

次の例は、 `AwsEfsAccessPoint` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEfsAccessPoint` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEfsAccessPointDetails」を参照してください。

例

```
"AwsEfsAccessPoint": {
 "AccessPointId": "fsap-05c4c0e79ba0b118a",
 "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/
fsap-05c4c0e79ba0b118a",
 "ClientToken": "AccessPointCompliant-ASk06ZZSXsEp",
 "FileSystemId": "fs-0f8137f731cb32146",
```

```
 "PosixUser": {
  "Gid": "1000",
  "SecondaryGids": ["0", "4294967295"],
  "Uid": "1234"
 },
 "RootDirectory": {
  "CreationInfo": {
   "OwnerGid": "1000",
   "OwnerUid": "1234",
   "Permissions": "777"
  },
  "Path": "/tmp/example"
 }
}
```

ASFF の AwsEks リソース

以下は、 `AwsEks`リソースの AWS Security Finding Format (ASFF) 構文の例です。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsEksCluster

`AwsEksCluster` オブジェクトは、Amazon EKS クラスターに関する詳細を提供します。

次の例は、 `AwsEksCluster` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEksCluster` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEksClusterDetails」を参照してください。

例

```
{
  "AwsEksCluster": {
    "Name": "example",
    "Arn": "arn:aws:eks:us-west-2:222222222222:cluster/example",
    "CreatedAt": 1565804921.901,
    "Version": "1.12",
    "RoleArn": "arn:aws:iam::222222222222:role/example-cluster-
ServiceRole-1XWBQWYSFRE2Q",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": false,
      "SubnetIds": [
```

```
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    },
    "Logging": {
      "ClusterLogging": [
        {
          "Types": [
            "api",
            "audit",
            "authenticator",
            "controllerManager",
            "scheduler"
          ],
          "Enabled": true
        }
      ]
    },
    "Status": "CREATING",
    "CertificateAuthorityData": {},
  }
}
```

ASFF の AwsElasticBeanstalk リソース

`AwsElasticBeanstalk` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsElasticBeanstalkEnvironment

`AwsElasticBeanstalkEnvironment` オブジェクトには、 AWS Elastic Beanstalk 環境に関する詳細が含まれています。

次の例は、 `AwsElasticBeanstalkEnvironment` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsElasticBeanstalkEnvironment` 属性の詳細については、AWS Security Hub API リファレンスの「AwsElasticBeanstalkEnvironmentDetails」を参照してください。

例

```
"AwsElasticBeanstalkEnvironment": {
    "ApplicationName": "MyApplication",
    "Cname": "myexampleapp-env.devo-2.elasticbeanstalk-internal.com",
    "DateCreated": "2021-04-30T01:38:01.090Z",
    "DateUpdated": "2021-04-30T01:38:01.090Z",
    "Description": "Example description of my awesome application",
    "EndpointUrl": "eb-dv-e-p-AWSEBLoa-abcdef01234567890-021345abcdef6789.us-
east-1.elb.amazonaws.com",
    "EnvironmentArn": "arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/
MyApplication/myapplication-env",
    "EnvironmentId": "e-abcd1234",
    "EnvironmentLinks": [
        {
            "EnvironmentName": "myexampleapp-env",
            "LinkName": "myapplicationLink"
        }
    ],
    "EnvironmentName": "myapplication-env",
    "OptionSettings": [
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSize",
            "Value": "100"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "Timeout",
            "Value": "600"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSizeType",
            "Value": "Percentage"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "IgnoreHealthCheck",
            "Value": "false"
        },
        {
            "Namespace": "aws:elasticbeanstalk:application",
            "OptionName": "Application Healthcheck URL",
```

```
            "Value": "TCP:80"
        }
    ],
    "PlatformArn": "arn:aws:elasticbeanstalk:us-east-1::platform/Tomcat 8 with Java 8
 running on 64bit Amazon Linux/2.7.7",
    "SolutionStackName": "64bit Amazon Linux 2017.09 v2.7.7 running Tomcat 8 Java 8",
    "Status": "Ready",
    "Tier": {
        "Name": "WebServer"
       "Type": "Standard"
       "Version": "1.0"
    },
    "VersionLabel": "Sample Application"
}
```

ASFF の AwsElasticSearch リソース

`AwsElasticSearch` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsElasticSearchDomain

`AwsElasticSearchDomain` オブジェクトは、Amazon OpenSearch Service ドメインの詳細を表示します。

次の例は、 `AwsElasticSearchDomain` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsElasticSearchDomain` 属性の詳細については、AWS Security Hub API リファレンスの「AwsElasticSearchDomainDetails」を参照してください。

例

```
"AwsElasticSearchDomain": {
    "AccessPolicies": "string",
    "DomainStatus": {
           "DomainId": "string",
           "DomainName": "string",
           "Endpoint": "string",
           "Endpoints": {
                  "string": "string"
           }
    },
    "DomainEndpointOptions": {
```

```
            "EnforceHTTPS": boolean,
            "TLSSecurityPolicy": "string"
      },
      "ElasticsearchClusterConfig": {
            "DedicatedMasterCount": number,
            "DedicatedMasterEnabled": boolean,
            "DedicatedMasterType": "string",
            "InstanceCount": number,
            "InstanceType": "string",
            "ZoneAwarenessConfig": {
                  "AvailabilityZoneCount": number
            },
            "ZoneAwarenessEnabled": boolean
      },
      "ElasticsearchVersion": "string",
      "EncryptionAtRestOptions": {
            "Enabled": boolean,
            "KmsKeyId": "string"
      },
      "LogPublishingOptions": {
            "AuditLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
            },
            "IndexSlowLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
            },
            "SearchSlowLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
            }
      },
      "NodeToNodeEncryptionOptions": {
            "Enabled": boolean
      },
      "ServiceSoftwareOptions": {
            "AutomatedUpdateDate": "string",
            "Cancellable": boolean,
            "CurrentVersion": "string",
            "Description": "string",
            "NewVersion": "string",
            "UpdateAvailable": boolean,
            "UpdateStatus": "string"
```

```
    },
    "VPCOptions": {
           "AvailabilityZones": [
                 "string"
           ],
           "SecurityGroupIds": [
                 "string"
           ],
           "SubnetIds": [
                 "string"
           ],
          "VPCId": "string"
    }
}
```

ASFF の AwsElb リソース

`AwsElb` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsElbLoadBalancer

`AwsElbLoadBalancer` オブジェクトには、Classic Load Balancer に関する詳細が含まれます。

次の例は、 `AwsElbLoadBalancer` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsElbLoadBalancer` 属性の詳細については、AWS Security Hub API リファレンスの「AwsElbLoadBalancerDetails」を参照してください。

例

```
"AwsElbLoadBalancer": {
    "AvailabilityZones": ["us-west-2a"],
    "BackendServerDescriptions": [
         {
            "InstancePort": 80,
            "PolicyNames": ["doc-example-policy"]
        }
    ],
    "CanonicalHostedZoneName": "Z3DZXE0EXAMPLE",
    "CanonicalHostedZoneNameID": "my-load-balancer-444455556666.us-
west-2.elb.amazonaws.com",
    "CreatedTime": "2020-08-03T19:22:44.637Z",
```

```
    "DnsName": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
    "HealthCheck": {
        "HealthyThreshold": 2,
        "Interval": 30,
        "Target": "HTTP:80/png",
        "Timeout": 3,
        "UnhealthyThreshold": 2
    },
    "Instances": [
        {
            "InstanceId": "i-example"
        }
    ],
    "ListenerDescriptions": [
        {
            "Listener": {
                "InstancePort": 443,
                "InstanceProtocol": "HTTPS",
                "LoadBalancerPort": 443,
                "Protocol": "HTTPS",
                "SslCertificateId": "arn:aws:iam::444455556666:server-certificate/my-
server-cert"
            },
            "PolicyNames": ["ELBSecurityPolicy-TLS-1-2-2017-01"]
        }
    ],
    "LoadBalancerAttributes": {
        "AccessLog": {
            "EmitInterval": 60,
            "Enabled": true,
            "S3BucketName": "amzn-s3-demo-bucket",
            "S3BucketPrefix": "doc-example-prefix"
        },
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        },
        "ConnectionSettings": {
            "IdleTimeout": 30
        },
        "CrossZoneLoadBalancing": {
            "Enabled": true
        },
        "AdditionalAttributes": [{
```

```
            "Key": "elb.http.desyncmitigationmode",
            "Value": "strictest"
        }]

    },
    "LoadBalancerName": "example-load-balancer",
    "Policies": {
        "AppCookieStickinessPolicies": [
            {
                "CookieName": "",
                "PolicyName": ""
            }
        ],
        "LbCookieStickinessPolicies": [
            {
                "CookieExpirationPeriod": 60,
                "PolicyName": "my-example-cookie-policy"
            }
        ],
        "OtherPolicies": [
            "my-PublicKey-policy",
            "my-authentication-policy",
            "my-SSLNegotiation-policy",
            "my-ProxyProtocol-policy",
            "ELBSecurityPolicy-2015-03"
        ]
    },
    "Scheme": "internet-facing",
    "SecurityGroups": ["sg-example"],
    "SourceSecurityGroup": {
        "GroupName": "my-elb-example-group",
        "OwnerAlias": "444455556666"
    },
    "Subnets": ["subnet-example"],
    "VpcId": "vpc-a01106c2"
}
```

AwsElbv2LoadBalancer

`AwsElbv2LoadBalancer` オブジェクトは、ロードバランサーに関する情報を提供します。

次の例は、 `AwsElbv2LoadBalancer` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsElbv2LoadBalancer` 属性の詳細については、AWS Security Hub API リファレンスの「AwsElbv2LoadBalancerDetails」を参照してください。

例

```
"AwsElbv2LoadBalancer": {
                        "AvailabilityZones": {
                            "SubnetId": "string",
                            "ZoneName": "string"
                        },
                        "CanonicalHostedZoneId": "string",
                        "CreatedTime": "string",
                        "DNSName": "string",
                        "IpAddressType": "string",
                        "LoadBalancerAttributes": [
                            {
                                "Key": "string",
                                "Value": "string"
                            }
                        ],
                        "Scheme": "string",
                        "SecurityGroups": [ "string" ],
                        "State": {
                            "Code": "string",
                            "Reason": "string"
                        },
                        "Type": "string",
                        "VpcId": "string"
                    }
```

ASFF の AwsEventBridge リソース

以下は、 `AwsEventBridge`リソースの AWS Security Finding Format (ASFF) 構文の例です。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsEventSchemasRegistry

`AwsEventSchemasRegistry` このオブジェクトは、Amazon EventBridge スキーマレジストリに関する情報を提供します。スキーマは、EventBridge に送信されるイベントの構造を定義します。スキーマ レジストリは、スキーマを収集して論理的にグループ化するコンテナです。

次の例は、 AwsEventSchemasRegistry オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEventSchemasRegistry 属性の詳細については、「AWS Security Hub API リファレンス」の「AwsEventSchemasRegistry」を参照してください。

例

```
"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
    "RegistryName": "schema-registry"
}
```

AwsEventsEndpoint

この AwsEventsEndpoint オブジェクトは、Amazon EventBridge グローバルエンドポイントに関する情報を提供します。エンドポイントは、アプリケーションの可用性をリージョンフォールトトレラントにすることによって、アプリケーションの可用性を向上することができます。

次の例は、 AwsEventsEndpoint オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsEventsEndpoint 属性の詳細については、AWS Security Hub API リファレンスの「AwsEventsEndpointDetails」を参照してください。

例

```
"AwsEventsEndpoint": {
    "Arn": "arn:aws:events:us-east-1:123456789012:endpoint/my-endpoint",
    "Description": "This is a sample endpoint.",
    "EndpointId": "04k1exajoy.veo",
    "EndpointUrl": "https://04k1exajoy.veo.endpoint.events.amazonaws.com",
    "EventBuses": [
        {
            "EventBusArn": "arn:aws:events:us-east-1:123456789012:event-bus/default"
        },
        {
            "EventBusArn": "arn:aws:events:us-east-2:123456789012:event-bus/default"
        }
    ],
    "Name": "my-endpoint",
    "ReplicationConfig": {
        "State": "ENABLED"
    },
```

```
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/
Amazon_EventBridge_Invoke_Event_Bus_1258925394",
    "RoutingConfig": {
        "FailoverConfig": {
            "Primary": {
                "HealthCheck": "arn:aws:route53:::healthcheck/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
            },
            "Secondary": {
                "Route": "us-east-2"
            }
        }
    },
    "State": "ACTIVE"
}
```

AwsEventsEventbus

この `AwsEventsEventbus` オブジェクトは、Amazon EventBridge グローバルエンドポイントに関する情報を提供します。エンドポイントは、アプリケーションの可用性をリージョンフォールトトレラントにすることによって、アプリケーションの可用性を向上することができます。

次の例は、 `AwsEventsEventbus` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsEventsEventbus` 属性の詳細については、AWS Security Hub API リファレンスの「AwsEventsEventbusDetails」を参照してください。

例

```
"AwsEventsEventbus":
    "Arn": "arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus",
    "Name": "my-event-bus",
    "Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AllowAllAccountsFromOrganizationToPutEvents\",\"Effect\":\"Allow
\",\"Principal\":\"*\",\"Action\":\"events:PutEvents\",\"Resource\":
\"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\",\"Condition
\":{\"StringEquals\":{\"aws:PrincipalOrgID\":\"o-ki7yjtkjv5\"}}},{\"Sid\":
\"AllowAccountToManageRulesTheyCreated\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
\"arn:aws:iam::123456789012:root\"},\"Action\":[\"events:PutRule\",\"events:PutTargets
\",\"events:DeleteRule\",\"events:RemoveTargets\",\"events:DisableRule
\",\"events:EnableRule\",\"events:TagResource\",\"events:UntagResource\",
\"events:DescribeRule\",\"events:ListTargetsByRule\",\"events:ListTagsForResource\"],
```

```
\"Resource\":\"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\",\"Condition\":
{\"StringEqualsIfExists\":{\"events:creatorAccount\":\"123456789012\"}}}]}"
```

ASFF の AwsGuardDuty リソース

以下は、 `AwsGuardDuty`リソースの AWS Security Finding Format (ASFF) 構文の例です。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsGuardDutyDetector

`AwsGuardDutyDetector` オブジェクトは、Amazon GuardDuty ディテクターに関する情報を提供します。ディテクターは、GuardDuty サービスを表すオブジェクトです。ディテクターは動作するために、GuardDuty が必要です。

次の例は、 `AwsGuardDutyDetector` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsGuardDutyDetector` 属性の詳細については、「AWS Security Hub API リファレンス」の「AwsGuardDutyDetector」を参照してください。

例

```
"AwsGuardDutyDetector": {
    "FindingPublishingFrequency": "SIX_HOURS",
    "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Status": "ENABLED",
    "DataSources": {
        "CloudTrail": {
            "Status": "ENABLED"
        },
        "DnsLogs": {
            "Status": "ENABLED"
        },
        "FlowLogs": {
            "Status": "ENABLED"
        },
        "S3Logs": {
             "Status": "ENABLED"
         },
         "Kubernetes": {
             "AuditLogs": {
                "Status": "ENABLED"
```

```
            }
        },
        "MalwareProtection": {
            "ScanEc2InstanceWithFindings": {
               "EbsVolumes": {
                   "Status": "ENABLED"
                }
            },
           "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/malware-
protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    }
}
```

ASFF の AwsIam リソース

`AwsIam` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsIamAccessKey

`AwsIamAccessKey` オブジェクトには、結果に関連する IAM アクセスキーの詳細が含まれています。

次の例は、 `AwsIamAccessKey` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsIamAccessKey` 属性の詳細については、AWS Security Hub API リファレンスの「AwsIamAccessKeyDetails」を参照してください。

例

```
"AwsIamAccessKey": {
                        "AccessKeyId": "string",
                        "AccountId": "string",
                        "CreatedAt": "string",
                        "PrincipalId": "string",
                        "PrincipalName": "string",
                        "PrincipalType": "string",
                        "SessionContext": {
                            "Attributes": {
                                "CreationDate": "string",
                                "MfaAuthenticated": boolean
```

```
                            },
                            "SessionIssuer": {
                                "AccountId": "string",
                                "Arn": "string",
                                "PrincipalId": "string",
                                "Type": "string",
                                "UserName": "string"
                            }
                        },
                        "Status": "string"
                    }
```

AwsIamGroup

`AwsIamGroup` オブジェクトには IAM グループに関する詳細が含まれています。

次の例は、 `AwsIamGroup` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsIamGroup` 属性の詳細については、AWS Security Hub API リファレンスの「AwsIamGroupDetails」を参照してください。

例

```
"AwsIamGroup": {
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleManagedAccess",
            "PolicyName": "ExampleManagedAccess",
        }
    ],
    "CreateDate": "2020-04-28T14:08:37.000Z",
    "GroupId": "AGPA4TPS3VLP7QEXAMPLE",
    "GroupName": "Example_User_Group",
    "GroupPolicyList": [
        {
            "PolicyName": "ExampleGroupPolicy"
        }
    ],
    "Path": "/"
}
```

AwsIamPolicy

`AwsIamPolicy` オブジェクトは IAM 許可ポリシーを表します。

次の例は、 `AwsIamPolicy` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsIamPolicy` 属性の詳細については、AWS Security Hub API リファレンスの「AwsIamPolicyDetails」を参照してください。

例

```
"AwsIamPolicy": {
    "AttachmentCount": 1,
    "CreateDate": "2017-09-14T08:17:29.000Z",
    "DefaultVersionId": "v1",
    "Description": "Example IAM policy",
    "IsAttachable": true,
    "Path": "/",
    "PermissionsBoundaryUsageCount": 5,
    "PolicyId": "ANPAJ2UCCR6DPCEXAMPLE",
    "PolicyName": "EXAMPLE-MANAGED-POLICY",
    "PolicyVersionList": [
        {
            "VersionId": "v1",
            "IsDefaultVersion": true,
            "CreateDate": "2017-09-14T08:17:29.000Z"
        }
    ],
    "UpdateDate": "2017-09-14T08:17:29.000Z"
}
```

AwsIamRole

`AwsIamRole` オブジェクトには、IAM ロールに関する情報 (ロールのすべてのポリシーを含む) が含まれています。

次の例は、 `AwsIamRole` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsIamRole` 属性の詳細については、AWS Security Hub API リファレンスの「AwsIamRoleDetails」を参照してください。

例

```
"AwsIamRole": {
    "AssumeRolePolicyDocument": "{'Version': '2012-10-17','Statement': [{'Effect':
 'Allow','Action': 'sts:AssumeRole'}]}",
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExamplePolicy1",
```

```
            "PolicyName": "Example policy 1"
        },
        {
            "PolicyArn": "arn:aws:iam::444455556666:policy/ExamplePolicy2",
            "PolicyName": "Example policy 2"
        }
        ],
        "CreateDate": "2020-03-14T07:19:14.000Z",
        "InstanceProfileList": [
            {
                "Arn": "arn:aws:iam::333333333333:ExampleProfile",
                "CreateDate": "2020-03-11T00:02:27Z",
                "InstanceProfileId": "AIPAIXEU4NUHUPEXAMPLE",
                "InstanceProfileName": "ExampleInstanceProfile",
                "Path": "/",
                "Roles": [
                    {
                       "Arn": "arn:aws:iam::444455556666:role/example-role",
                        "AssumeRolePolicyDocument": "",
                        "CreateDate": "2020-03-11T00:02:27Z",
                        "Path": "/",
                        "RoleId": "AROAJ52OTH4H7LEXAMPLE",
                        "RoleName": "example-role",
                    }
                ]
            }
        ],
        "MaxSessionDuration": 3600,
        "Path": "/",
        "PermissionsBoundary": {
            "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
            "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
        },
        "RoleId": "AROA4TPS3VLEXAMPLE",
        "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
        "RolePolicyList": [
            {
                "PolicyName": "Example role policy"
            }
        ]
    }
```

AwsIamUser

`AwsIamUser` オブジェクトは、ユーザーに関する情報を提供します。

次の例は、 `AwsIamUser` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsIamUser` 属性の詳細については、AWS Security Hub API リファレンスの「AwsIamUserDetails」を参照してください。

例

```
"AwsIamUser": {
    "AttachedManagedPolicies": [
        {
            "PolicyName": "ExamplePolicy",
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleAccess"
        }
    ],
    "CreateDate": "2018-01-26T23:50:05.000Z",
    "GroupList": [],
    "Path": "/",
    "PermissionsBoundary" : {
        "PermissionsBoundaryArn" : "arn:aws:iam::aws:policy/AdministratorAccess",
        "PermissionsBoundaryType" : "PermissionsBoundaryPolicy"
    },
    "UserId": "AIDACKCEVSQ6C2EXAMPLE",
    "UserName": "ExampleUser",
    "UserPolicyList": [
        {
            "PolicyName": "InstancePolicy"
        }
    ]
}
```

ASFF の AwsKinesis リソース

`AwsKinesis` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsKinesisStream

`AwsKinesisStream` オブジェクトは、Amazon Kinesis Data Streams の詳細を表示します。

次の例は、 AwsKinesisStream オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsKinesisStream 属性の詳細については、AWS Security Hub API リファレンスの「AwsKinesisStreamDetails」を参照してください。

例

```
"AwsKinesisStream": {
 "Name": "test-vir-kinesis-stream",
 "Arn": "arn:aws:kinesis:us-east-1:293279581038:stream/test-vir-kinesis-stream",
 "RetentionPeriodHours": 24,
 "ShardCount": 2,
 "StreamEncryption": {
  "EncryptionType": "KMS",
  "KeyId": "arn:aws:kms:us-east-1:293279581038:key/849cf029-4143-4c59-91f8-
ea76007247eb"
 }
}
```

ASFF の AwsKms リソース

AwsKms リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsKmsKey

AwsKmsKey オブジェクトは、 に関する詳細を提供します AWS KMS key。

次の例は、 AwsKmsKey オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsKmsKey 属性の詳細については、AWS Security Hub API リファレンスの「AwsKmsKeyDetails」を参照してください。

例

```
"AwsKmsKey": {
                        "AWSAccountId": "string",
                        "CreationDate": "string",
                        "Description": "string",
                        "KeyId": "string",
                        "KeyManager": "string",
                        "KeyRotationStatus": boolean,
```

```
                        "KeyState": "string",
                        "Origin": "string"
                    }
```

AwsLambda

`AwsLambda` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsLambdaFunction

`AwsLambdaFunction` オブジェクトは、Lambda 関数の設定に関する詳細を提供します。

次の例は、 `AwsLambdaFunction` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsLambdaFunction` 属性の詳細については、AWS Security Hub API リファレンスの「AwsLambdaFunctionDetails」を参照してください。

例

```
"AwsLambdaFunction": {
    "Architectures": [
        "x86_64"
    ],
    "Code": {
        "S3Bucket": "amzn-s3-demo-bucket",
        "S3Key": "samplekey",
        "S3ObjectVersion": "2",
        "ZipFile": "myzip.zip"
    },
    "CodeSha256": "1111111111111abcdef",
    "DeadLetterConfig": {
        "TargetArn": "arn:aws:lambda:us-east-2:123456789012:queue:myqueue:2"
    },
    "Environment": {
        "Variables": {
            "Stage": "foobar"
         },
        "Error": {
            "ErrorCode": "Sample-error-code",
            "Message": "Caller principal is a manager."
         }
```

```
     },
    "FunctionName": "CheckOut",
    "Handler": "main.py:lambda_handler",
    "KmsKeyArn": "arn:aws:kms:us-west-2:123456789012:key/mykey",
    "LastModified": "2001-09-11T09:00:00Z",
    "Layers": {
        "Arn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:3",
        "CodeSize": 169
    },
    "PackageType": "Zip",
    "RevisionId": "23",
    "Role": "arn:aws:iam::123456789012:role/Accounting-Role",
    "Runtime": "go1.7",
    "Timeout": 15,
    "TracingConfig": {
        "Mode": "Active"
    },
    "Version": "$LATEST$",
    "VpcConfig": {
        "SecurityGroupIds": ["sg-085912345678492fb", "sg-08591234567bdgdc"],
         "SubnetIds": ["subnet-071f712345678e7c8", "subnet-07fd123456788a036"]
    },
    "MasterArn": "arn:aws:lambda:us-east-2:123456789012:\$LATEST",
    "MemorySize": 2048
}
```

AwsLambdaLayerVersion

`AwsLambdaLayerVersion` オブジェクトは、Lambda レイヤーのバージョンに関する詳細を提供します。

次の例は、 `AwsLambdaLayerVersion` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsLambdaLayerVersion` 属性の詳細については、AWS Security Hub API リファレンスの「AwsLambdaLayerVersionDetails」を参照してください。

例

```
"AwsLambdaLayerVersion": {
    "Version": 2,
    "CompatibleRuntimes": [
        "java8"
    ],
    "CreatedDate": "2019-10-09T22:02:00.274+0000"
```

```
}
```

ASFF の AwsMsk リソース

`AwsMsk` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsMskCluster

`AwsMskCluster` オブジェクトは Amazon Managed Streaming for Apache Kafka (Amazon MSK) クラスターに関する情報を提供します。

次の例は、 `AwsMskCluster` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsMskCluster` 属性の詳細については、AWS Security Hub API リファレンスの「AwsMskClusterDetails」を参照してください。

例

```
"AwsMskCluster": {
        "ClusterInfo": {
            "ClientAuthentication": {
                "Sasl": {
                    "Scram": {
                        "Enabled": true
                    },
                    "Iam": {
                        "Enabled": true
                    }
                },
                "Tls": {
                    "CertificateAuthorityArnList": [],
                    "Enabled": false
                },
                "Unauthenticated": {
                    "Enabled": false
                }
            },
            "ClusterName": "my-cluster",
            "CurrentVersion": "K2PWKAKR8XB7XF",
            "EncryptionInfo": {
                "EncryptionAtRest": {
```

```
                    "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
                "EncryptionInTransit": {
                    "ClientBroker": "TLS",
                    "InCluster": true
                }
            },
            "EnhancedMonitoring": "PER_TOPIC_PER_BROKER",
            "NumberOfBrokerNodes": 3
        }
}
```

ASFF の AwsNetworkFirewall リソース

以下は、 `AwsNetworkFirewall`リソースの AWS Security Finding Format (ASFF) 構文の例です。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsNetworkFirewallFirewall

`AwsNetworkFirewallFirewall` オブジェクトには AWS Network Firewall ファイアウォールに関する詳細が含まれています。

次の例は、 `AwsNetworkFirewallFirewall` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsNetworkFirewallFirewall` 属性の詳細については、AWS Security Hub API リファレンスの「AwsNetworkFirewallFirewallDetails」を参照してください。

例

```
"AwsNetworkFirewallFirewall": {
    "DeleteProtection": false,
    "FirewallArn": "arn:aws:network-firewall:us-east-1:024665936331:firewall/
testfirewall",
    "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
    "FirewallId": "dea7d8e9-ae38-4a8a-b022-672a830a99fa",
    "FirewallName": "testfirewall",
    "FirewallPolicyChangeProtection": false,
    "SubnetChangeProtection": false,
    "SubnetMappings": [
        {
```

```
            "SubnetId": "subnet-0183481095e588cdc"
        },
        {
            "SubnetId": "subnet-01f518fad1b1c90b0"
        }
    ],
    "VpcId": "vpc-40e83c38"
}
```

AwsNetworkFirewallFirewallPolicy

`AwsNetworkFirewallFirewallPolicy` オブジェクトは、ファイアウォールポリシーに関する詳細を提供します。ファイアウォールポリシーは、ネットワークファイアウォールの動作を定義します。

次の例は、 `AwsNetworkFirewallFirewallPolicy` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsNetworkFirewallFirewallPolicy` 属性の詳細については、AWS Security Hub API リファレンスの「AwsNetworkFirewallFirewallPolicyDetails」を参照してください。

例

```
"AwsNetworkFirewallFirewallPolicy": {
   "FirewallPolicy": {
    "StatefulRuleGroupReferences": [
        {
            "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/PatchesOnly"
        }
    ],
    "StatelessDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessRuleGroupReferences": [
       {
          "Priority": 1,
          "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1"
       }
     ]
   },
   "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
   "FirewallPolicyId": "9ceeda22-6050-4048-a0ca-50ce47f0cc65",
```

```
    "FirewallPolicyName": "InitialFirewall",
    "Description": "Initial firewall"
}
```

AwsNetworkFirewallRuleGroup

`AwsNetworkFirewallRuleGroup` オブジェクトは、 AWS Network Firewall ルールグループに関する詳細を提供します。ルールグループはネットワークトラフィックを検査および制御するために使用します。ステートレスルールグループは、個々のパケットに適用されます。ステートフルルールグループは、トラフィックフローのコンテキスト内のパケットに適用されます。

ルールグループは、ファイアウォールポリシーで参照されます。

次の例は、 `AwsNetworkFirewallRuleGroup` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsNetworkFirewallRuleGroup` 属性の詳細については、AWS Security Hub API リファレンスの「AwsNetworkFirewallRuleGroupDetails」を参照してください。

例 - ステートレスルールグループ

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 600,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1",
    "RuleGroupId": "fb13c4df-b6da-4c1e-91ec-84b7a5487493",
    "RuleGroupName": "Stateless-1"
    "Description": "Example of a stateless rule group",
    "Type": "STATELESS",
    "RuleGroup": {
        "RulesSource": {
            "StatelessRulesAndCustomActions": {
                "CustomActions": [],
                "StatelessRules": [
                    {
                        "Priority": 1,
                        "RuleDefinition": {
                            "Actions": [
                                "aws:pass"
                            ],
                            "MatchAttributes": {
                                "DestinationPorts": [
                                    {
                                        "FromPort": 443,
                                        "ToPort": 443
```

```
                                    }
                                ],
                                "Destinations": [
                                    {
                                        "AddressDefinition": "192.0.2.0/24"
                                    }
                                ],
                                "Protocols": [
                                            6
                                ],
                                "SourcePorts": [
                                    {
                                        "FromPort": 0,
                                        "ToPort": 65535
                                    }
                                ],
                                "Sources": [
                                    {
                                         "AddressDefinition": "198.51.100.0/24"
                                    }
                                ]
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

例 - ステートフルルールグループ

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 100,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/tupletest",
    "RuleGroupId": "38b71c12-da80-4643-a6c5-03337f8933e0",
    "RuleGroupName": "ExampleRuleGroup",
    "Description": "Example of a stateful rule group",
    "Type": "STATEFUL",
    "RuleGroup": {
        "RuleSource": {
             "StatefulRules": [
```

```
                {
                    "Action": "PASS",
                    "Header": {
                        "Destination": "Any",
                        "DestinationPort": "443",
                        "Direction": "ANY",
                        "Protocol": "TCP",
                        "Source": "Any",
                        "SourcePort": "Any"
                    },
                    "RuleOptions": [
                        {
                           "Keyword": "sid:1"
                        }
                    ]
                }
            ]
        }
    }
}
```

以下は、AwsNetworkFirewallRuleGroup 属性の、有効な値の例の一覧です。

- Action

  有効な値: PASS | DROP | ALERT
- Protocol

  有効な値: IP | TCP | UDP | ICMP | HTTP | FTP | TLS | SMB | DNS | DCERPC | SSH | SMTP | IMAP | MSN | KRB5 | IKEV2 | TFTP | NTP | DHCP
- Flags

  有効な値: FIN | SYN | RST | PSH | ACK | URG | ECE | CWR
- Masks

  有効な値: FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

ASFF の AwsOpenSearchService リソース

以下は、 AwsOpenSearchServiceリソースの AWS Security Finding Format (ASFF) 構文の例です。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsOpenSearchServiceDomain

`AwsOpenSearchServiceDomain` オブジェクトには、Amazon OpenSearch Service ドメインに関する情報が含まれています。

次の例は、 `AwsOpenSearchServiceDomain` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsOpenSearchServiceDomain` 属性の詳細については、AWS Security Hub API リファレンスの「AwsOpenSearchServiceDomainDetails」を参照してください。

例

```
"AwsOpenSearchServiceDomain": {
    "AccessPolicies": "IAM_Id",
    "AdvancedSecurityOptions": {
        "Enabled": true,
        "InternalUserDatabaseEnabled": true,
        "MasterUserOptions": {
            "MasterUserArn": "arn:aws:iam::123456789012:user/third-master-use",
            "MasterUserName": "third-master-use",
            "MasterUserPassword": "some-password"
        }
    },
    "Arn": "arn:aws:Opensearch:us-east-1:111122223333:somedomain",
    "ClusterConfig": {
        "InstanceType": "c5.large.search",
        "InstanceCount": 1,
        "DedicatedMasterEnabled": true,
        "ZoneAwarenessEnabled": false,
        "ZoneAwarenessConfig": {
            "AvailabilityZoneCount": 2
        },
        "DedicatedMasterType": "c5.large.search",
        "DedicatedMasterCount": 3,
        "WarmEnabled": true,
        "WarmCount": 3,
        "WarmType": "ultrawarm1.large.search"
    },
    "DomainEndpoint": "https://es-2021-06-23t17-04-qowmgghud5vofgb5e4wmi.eu-
central-1.es.amazonaws.com",
    "DomainEndpointOptions": {
```

```
        "EnforceHTTPS": false,
        "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07",
        "CustomEndpointCertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/bda1bff1-79c0-49d0-abe6-50a15a7477d4",
        "CustomEndpointEnabled": true,
        "CustomEndpoint": "example.com"
    },
    "DomainEndpoints": {
        "vpc": "vpc-endpoint-h2dsd34efgyghrtguk5gt6j2foh4.us-east-1.es.amazonaws.com"
    },
    "DomainName": "my-domain",
    "EncryptionAtRestOptions": {
        "Enabled": false,
        "KmsKeyId": "1a2a3a4-1a2a-3a4a-5a6a-1a2a3a4a5a6a"
    },
    "EngineVersion": "7.1",
    "Id": "123456789012",
    "LogPublishingOptions": {
        "IndexSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-index-slow-logs",
            "Enabled": true
        },
        "SearchSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        },
        "AuditLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        }
    },
    "NodeToNodeEncryptionOptions": {
        "Enabled": true
    },
    "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "2022-04-28T14:08:37.000Z",
        "Cancellable": false,
        "CurrentVersion": "R20210331",
        "Description": "There is no software update available for this domain.",
        "NewVersion": "OpenSearch_1.0",
        "UpdateAvailable": false,
```

```
        "UpdateStatus": "COMPLETED",
        "OptionalDeployment": false
    },
    "VpcOptions": {
        "SecurityGroupIds": [
            "sg-2a3a4a5a"
        ],
        "SubnetIds": [
            "subnet-1a2a3a4a"
        ],
    }
}
```

ASFF の AwsRds リソース

AwsRds リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsRdsDbCluster

AwsRdsDbCluster オブジェクトは、Amazon RDS データベースクラスターの詳細を提供します。

次の例は、 AwsRdsDbCluster オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsRdsDbCluster 属性の詳細については、AWS Security Hub API リファレンスの「AwsRdsDbClusterDetails」を参照してください。

例

```
"AwsRdsDbCluster": {
    "ActivityStreamStatus": "stopped",
    "AllocatedStorage": 1,
    "AssociatedRoles": [
        {
        "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
        "Status": "PENDING"
        }
    ],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1c",
```

```
        "us-east-1e"
    ],
    "BackupRetentionPeriod": 1,
    "ClusterCreateTime": "2020-06-22T17:40:12.322Z",
    "CopyTagsToSnapshot": true,
    "CrossAccountClone": false,
    "CustomEndpoints": [],
    "DatabaseName": "Sample name",
    "DbClusterIdentifier": "database-3",
    "DbClusterMembers": [
        {
        "DbClusterParameterGroupStatus": "in-sync",
        "DbInstanceIdentifier": "database-3-instance-1",
        "IsClusterWriter": true,
        "PromotionTier": 1,
        }
    ],
    "DbClusterOptionGroupMemberships": [],
    "DbClusterParameterGroup": "cluster-parameter-group",
    "DbClusterResourceId": "cluster-example",
    "DbSubnetGroup": "subnet-group",
    "DeletionProtection": false,
    "DomainMemberships": [],
    "Status": "modifying",
    "EnabledCloudwatchLogsExports": [
        "audit",
        "error",
        "general",
        "slowquery"
    ],
    "Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
    "Engine": "aurora-mysql",
    "EngineMode": "provisioned",
    "EngineVersion": "5.7.mysql_aurora.2.03.4",
    "HostedZoneId": "ZONE1",
    "HttpEndpointEnabled": false,
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "MasterUsername": "admin",
    "MultiAz": false,
    "Port": 3306,
    "PreferredBackupWindow": "04:52-05:22",
    "PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
    "ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",
```

```
    "ReadReplicaIdentifiers": [],
    "Status": "Modifying",
    "StorageEncrypted": true,
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example-1"
        }
    ],
}
```

AwsRdsDbClusterSnapshot

`AwsRdsDbClusterSnapshot` オブジェクトには、Amazon RDS DB クラスタースナップショットに関する情報が含まれています。

次の例は、 `AwsRdsDbClusterSnapshot` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsRdsDbClusterSnapshot` 属性の詳細については、AWS Security Hub API リファレンスの「AwsRdsDbClusterSnapshotDetails」を参照してください。

例

```
"AwsRdsDbClusterSnapshot": {
    "AllocatedStorage": 0,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1d",
        "us-east-1e"
    ],
    "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
    "DbClusterIdentifier": "database-2",
    "DbClusterSnapshotAttributes": [{
        "AttributeName": "restore",
        "AttributeValues": ["123456789012"]
    }],
    "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
    "Engine": "aurora",
    "EngineVersion": "5.6.10a",
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "LicenseModel": "aurora",
    "MasterUsername": "admin",
    "PercentProgress": 100,
```

```
    "Port": 0,
    "SnapshotCreateTime": "2020-06-22T17:40:12.322Z",
    "SnapshotType": "automated",
    "Status": "available",
    "StorageEncrypted": true,
    "VpcId": "vpc-faf7e380"
}
```

AwsRdsDbInstance

`AwsRdsDbInstance` オブジェクトは、Amazon RDS DB インスタンスに関する詳細を提供します。

次の例は、 `AwsRdsDbInstance` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsRdsDbInstance` 属性の詳細については、AWS Security Hub API リファレンスの「AwsRdsDbInstanceDetails」を参照してください。

例

```
"AwsRdsDbInstance": {
    "AllocatedStorage": 20,
    "AssociatedRoles": [],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1d",
    "BackupRetentionPeriod": 7,
    "CaCertificateIdentifier": "certificate1",
    "CharacterSetName": "",
    "CopyTagsToSnapshot": true,
    "DbClusterIdentifier": "",
    "DbInstanceArn": "arn:aws:rds:us-east-1:111122223333:db:database-1",
    "DbInstanceClass": "db.t2.micro",
    "DbInstanceIdentifier": "database-1",
    "DbInstancePort": 0,
    "DbInstanceStatus": "available",
    "DbiResourceId": "db-EXAMPLE123",
    "DbName": "",
    "DbParameterGroups": [
        {
            "DbParameterGroupName": "default.mysql5.7",
            "ParameterApplyStatus": "in-sync"
        }
    ],
```

```
    "DbSecurityGroups": [],


    "DbSubnetGroup": {
        "DbSubnetGroupName": "my-group-123abc",
        "DbSubnetGroupDescription": "My subnet group",
        "VpcId": "vpc-example1",
        "SubnetGroupStatus": "Complete",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-123abc",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1d"
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-456def",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1c"
                },
                "SubnetStatus": "Active"
            }
      ],
        "DbSubnetGroupArn": ""
    },
    "DeletionProtection": false,
    "DomainMemberships": [],
    "EnabledCloudWatchLogsExports": [],
    "Endpoint": {
        "address": "database-1.example.us-east-1.rds.amazonaws.com",
        "port": 3306,
        "hostedZoneId": "ZONEID1"
    },
    "Engine": "mysql",
    "EngineVersion": "5.7.22",
    "EnhancedMonitoringResourceArn": "arn:aws:logs:us-east-1:111122223333:log-
group:Example:log-stream:db-EXAMPLE1",
    "IamDatabaseAuthenticationEnabled": false,
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "Iops": "",
    "KmsKeyId": "",
    "LatestRestorableTime": "2020-06-24T05:50:00.000Z",
    "LicenseModel": "general-public-license",
```

```
    "ListenerEndpoint": "",
    "MasterUsername": "admin",
    "MaxAllocatedStorage": 1000,
    "MonitoringInterval": 60,
    "MonitoringRoleArn": "arn:aws:iam::111122223333:role/rds-monitoring-role",
    "MultiAz": false,
    "OptionGroupMemberships": [
        {
            "OptionGroupName": "default:mysql-5-7",
            "Status": "in-sync"
        }
    ],
    "PreferredBackupWindow": "03:57-04:27",
    "PreferredMaintenanceWindow": "thu:10:13-thu:10:43",
    "PendingModifiedValues": {
        "DbInstanceClass": "",
        "AllocatedStorage": "",
        "MasterUserPassword": "",
        "Port": "",
        "BackupRetentionPeriod": "",
        "MultiAZ": "",
        "EngineVersion": "",
        "LicenseModel": "",
        "Iops": "",
        "DbInstanceIdentifier": "",
        "StorageType": "",
        "CaCertificateIdentifier": "",
        "DbSubnetGroupName": "",
        "PendingCloudWatchLogsExports": "",
        "ProcessorFeatures": []
    },
    "PerformanceInsightsEnabled": false,
    "PerformanceInsightsKmsKeyId": "",
    "PerformanceInsightsRetentionPeriod": "",
    "ProcessorFeatures": [],
    "PromotionTier": "",
    "PubliclyAccessible": false,
    "ReadReplicaDBClusterIdentifiers": [],
    "ReadReplicaDBInstanceIdentifiers": [],
    "ReadReplicaSourceDBInstanceIdentifier": "",
    "SecondaryAvailabilityZone": "",
    "StatusInfos": [],
    "StorageEncrypted": false,
    "StorageType": "gp2",
```

```
    "TdeCredentialArn": "",
    "Timezone": "",
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-example1",
            "Status": "active"
        }
    ]
}
```

AwsRdsDbSecurityGroup

`AwsRdsDbSecurityGroup` オブジェクトには、Amazon Relational Database Service に関する情報が含まれます。

次の例は、 `AwsRdsDbSecurityGroup` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsRdsDbSecurityGroup` 属性の詳細については、AWS Security Hub API リファレンスの「AwsRdsDbSecurityGroupDetails」を参照してください。

例

```
"AwsRdsDbSecurityGroup": {
    "DbSecurityGroupArn": "arn:aws:rds:us-west-1:111122223333:secgrp:default",
    "DbSecurityGroupDescription": "default",
    "DbSecurityGroupName": "mysecgroup",
    "Ec2SecurityGroups": [
        {
          "Ec2SecurityGroupuId": "myec2group",
          "Ec2SecurityGroupName": "default",
          "Ec2SecurityGroupOwnerId": "987654321021",
          "Status": "authorizing"
        }
    ],
    "IpRanges": [
        {
          "Cidrip": "0.0.0.0/0",
          "Status": "authorizing"
        }
    ],
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234567f"
}
```

AwsRdsDbSnapshot

AwsRdsDbSnapshot オブジェクトには、Amazon RDS DB クラスタースナップショットに関する詳細が含まれています。

次の例は、 AwsRdsDbSnapshot オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsRdsDbSnapshot 属性の詳細については、AWS Security Hub API リファレンスの「AwsRdsDbSnapshotDetails」を参照してください。

例

```
"AwsRdsDbSnapshot": {
    "DbSnapshotIdentifier": "rds:database-1-2020-06-22-17-41",
    "DbInstanceIdentifier": "database-1",
    "SnapshotCreateTime": "2020-06-22T17:41:29.967Z",
    "Engine": "mysql",
    "AllocatedStorage": 20,
    "Status": "available",
    "Port": 3306,
    "AvailabilityZone": "us-east-1d",
    "VpcId": "vpc-example1",
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "MasterUsername": "admin",
    "EngineVersion": "5.7.22",
    "LicenseModel": "general-public-license",
    "SnapshotType": "automated",
    "Iops": null,
    "OptionGroupName": "default:mysql-5-7",
    "PercentProgress": 100,
    "SourceRegion": null,
    "SourceDbSnapshotIdentifier": "",
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Encrypted": false,
    "KmsKeyId": "",
    "Timezone": "",
    "IamDatabaseAuthenticationEnabled": false,
    "ProcessorFeatures": [],
    "DbiResourceId": "db-resourceexample1"
}
```

AwsRdsEventSubscription

`AwsRdsEventSubscription` には、RDS イベント通知サブスクリプションの詳細が含まれています。サブスクリプションにより、RDS は SNS トピックにイベントを送信できます。

次の例は、 `AwsRdsEventSubscription` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsRdsEventSubscription` 属性の詳細については、AWS Security Hub API リファレンスの「AwsRdsEventSubscriptionDetails」を参照してください。

例

```
"AwsRdsEventSubscription": {
    "CustSubscriptionId": "myawsuser-secgrp",
    "CustomerAwsId": "111111111111",
    "Enabled": true,
    "EventCategoriesList": [
        "configuration change",
        "failure"
    ],
    "EventSubscriptionArn": "arn:aws:rds:us-east-1:111111111111:es:my-instance-events",
    "SnsTopicArn": "arn:aws:sns:us-east-1:111111111111:myawsuser-RDS",
    "SourceIdsList": [
        "si-sample",
        "mysqldb-rr"
    ],
    "SourceType": "db-security-group",
    "Status": "creating",
    "SubscriptionCreationTime": "2021-06-27T01:38:01.090Z"
}
```

ASFF の AwsRedshift リソース

`AwsRedshift` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsRedshiftCluster

`AwsRedshiftCluster` オブジェクトには、Amazon Redshift クラスターに関する詳細が含まれています。

次の例は、 `AwsRedshiftCluster` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsRedshiftCluster` 属性の詳細については、AWS Security Hub API リファレンスの「AwsRedshiftClusterDetails」を参照してください。

例

```
"AwsRedshiftCluster": {
    "AllowVersionUpgrade": true,
    "AutomatedSnapshotRetentionPeriod": 1,
    "AvailabilityZone": "us-west-2d",
    "ClusterAvailabilityStatus": "Unavailable",
    "ClusterCreateTime": "2020-08-03T19:22:44.637Z",
    "ClusterIdentifier": "redshift-cluster-1",
    "ClusterNodes": [
        {
            "NodeRole": "LEADER",
            "PrivateIPAddress": "192.0.2.108",
            "PublicIPAddress": "198.51.100.29"
        },
        {
            "NodeRole": "COMPUTE-0",
            "PrivateIPAddress": "192.0.2.22",
            "PublicIPAddress": "198.51.100.63"
        },
        {
             "NodeRole": "COMPUTE-1",
             "PrivateIPAddress": "192.0.2.224",
             "PublicIPAddress": "198.51.100.226"
        }
        ],
    "ClusterParameterGroups": [
        {
            "ClusterParameterStatusList": [
                {
                    "ParameterName": "max_concurrency_scaling_clusters",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "enable_user_activity_logging",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
```

```
                {
                    "ParameterName": "auto_analyze",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "query_group",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "datestyle",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "extra_float_digits",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "search_path",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "statement_timeout",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "wlm_json_configuration",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "require_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "use_fips_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
```

```
                }
            ],
            "ParameterApplyStatus": "in-sync",
            "ParameterGroupName": "temp"
        }
    ],
    "ClusterPublicKey": "JalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY Amazon-Redshift",
    "ClusterRevisionNumber": 17498,
    "ClusterSecurityGroups": [
        {
            "ClusterSecurityGroupName": "default",
            "Status": "active"
        }
    ],
    "ClusterSnapshotCopyStatus": {
        "DestinationRegion": "us-west-2",
        "ManualSnapshotRetentionPeriod": -1,
        "RetentionPeriod": 1,
        "SnapshotCopyGrantName": "snapshotCopyGrantName"
    },
    "ClusterStatus": "available",
    "ClusterSubnetGroupName": "default",
    "ClusterVersion": "1.0",
    "DBName": "dev",
    "DeferredMaintenanceWindows": [
        {
            "DeferMaintenanceEndTime": "2020-10-07T20:34:01.000Z",
            "DeferMaintenanceIdentifier": "deferMaintenanceIdentifier",
            "DeferMaintenanceStartTime": "2020-09-07T20:34:01.000Z"
        }
     ],
    "ElasticIpStatus": {
        "ElasticIp": "203.0.113.29",
        "Status": "active"
    },
    "ElasticResizeNumberOfNodeOptions": "4",
    "Encrypted": false,
    "Endpoint": {
        "Address": "redshift-cluster-1.example.us-west-2.redshift.amazonaws.com",
        "Port": 5439
    },
    "EnhancedVpcRouting": false,
    "ExpectedNextSnapshotScheduleTime": "2020-10-13T20:34:01.000Z",
    "ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
```

```
    "HsmStatus": {
        "HsmClientCertificateIdentifier": "hsmClientCertificateIdentifier",
        "HsmConfigurationIdentifier": "hsmConfigurationIdentifier",
        "Status": "applying"
    },
    "IamRoles": [
        {
             "ApplyStatus": "in-sync",
             "IamRoleArn": "arn:aws:iam::111122223333:role/RedshiftCopyUnload"
        }
    ],
    "KmsKeyId": "kmsKeyId",
    "LoggingStatus": {
        "BucketName": "amzn-s3-demo-bucket",
        "LastFailureMessage": "test message",
        "LastFailureTime": "2020-08-09T13:00:00.000Z",
        "LastSuccessfulDeliveryTime": "2020-08-08T13:00:00.000Z",
        "LoggingEnabled": true,
        "S3KeyPrefix": "/"
    },
    "MaintenanceTrackName": "current",
    "ManualSnapshotRetentionPeriod": -1,
    "MasterUsername": "awsuser",
    "NextMaintenanceWindowStartTime": "2020-08-09T13:00:00.000Z",
    "NodeType": "dc2.large",
    "NumberOfNodes": 2,
    "PendingActions": [],
    "PendingModifiedValues": {
        "AutomatedSnapshotRetentionPeriod": 0,
        "ClusterIdentifier": "clusterIdentifier",
        "ClusterType": "clusterType",
        "ClusterVersion": "clusterVersion",
        "EncryptionType": "None",
        "EnhancedVpcRouting": false,
        "MaintenanceTrackName": "maintenanceTrackName",
        "MasterUserPassword": "masterUserPassword",
        "NodeType": "dc2.large",
        "NumberOfNodes": 1,
        "PubliclyAccessible": true
    },
    "PreferredMaintenanceWindow": "sun:13:00-sun:13:30",
    "PubliclyAccessible": true,
    "ResizeInfo": {
        "AllowCancelResize": true,
```

```
        "ResizeType": "ClassicResize"
    },
    "RestoreStatus": {
        "CurrentRestoreRateInMegaBytesPerSecond": 15,
        "ElapsedTimeInSeconds": 120,
        "EstimatedTimeToCompletionInSeconds": 100,
        "ProgressInMegaBytes": 10,
        "SnapshotSizeInMegaBytes": 1500,
        "Status": "restoring"
    },
    "SnapshotScheduleIdentifier": "snapshotScheduleIdentifier",
    "SnapshotScheduleState": "ACTIVE",
     "VpcId": "vpc-example",
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example"
        }
    ]
}
```

ASFF の AwsRoute53 リソース

以下は、 `AwsRoute53`リソースの AWS Security Finding Format (ASFF) 構文の例です。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsRoute53HostedZone

この `AwsRoute53HostedZone` オブジェクトは、ホストゾーンに割り当てられた 4 つのネームサーバーを含む Amazon Route 53 ホストゾーンに関する情報を提供します。ホストゾーンは単一の親ドメイン名に属する、まとめて管理できるレコードの集合を表します。

次の例は、 `AwsRoute53HostedZone` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsRoute53HostedZone` 属性の詳細については、AWS Security Hub API リファレンスの「AwsRoute53HostedZoneDetails」を参照してください。

例

```
"AwsRoute53HostedZone": {
    "HostedZone": {
        "Id": "Z06419652JEMGO9TA2XKL",
```

```
        "Name": "asff.testing",
        "Config": {
            "Comment": "This is an example comment."
        }
    },
    "NameServers": [
        "ns-470.awsdns-32.net",
        "ns-1220.awsdns-12.org",
        "ns-205.awsdns-13.com",
        "ns-1960.awsdns-51.co.uk"
    ],
    "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-
group:asfftesting:*",
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "HostedZoneId": "Z00932193AF5H180PPNZD"
        }
    },
    "Vpcs": [
        {
            "Id": "vpc-05d7c6e36bc03ea76",
            "Region": "us-east-1"
        }
    ]
}
```

ASFF の AwsS3 リソース

`AwsS3` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsS3AccessPoint

`AwsS3AccessPoint` は、Amazon S3 アクセスポイントに関する情報を提供します。S3 アクセスポイントは、S3 バケットにアタッチされた名前付きのネットワークエンドポイントで、S3 オブジェクトのオペレーションを実行するために使用できます。

次の例は、 `AwsS3AccessPoint` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsS3AccessPoint` 属性の詳細については、「AWS Security Hub API リファレンス」の「AwsS3AccessPointDetails」を参照してください。

例

```
"AwsS3AccessPoint": {
        "AccessPointArn": "arn:aws:s3:us-east-1:123456789012:accesspoint/asff-access-
point",
        "Alias": "asff-access-point-hrzrlukc5m36ft7okagglf3gmwluquse1b-s3alias",
        "Bucket": "amzn-s3-demo-bucket",
        "BucketAccountId": "123456789012",
        "Name": "asff-access-point",
        "NetworkOrigin": "VPC",
        "PublicAccessBlockConfiguration": {
            "BlockPublicAcls": true,
            "BlockPublicPolicy": true,
            "IgnorePublicAcls": true,
            "RestrictPublicBuckets": true
        },
        "VpcConfiguration": {
            "VpcId": "vpc-1a2b3c4d5e6f1a2b3"
        }
}
```

AwsS3AccountPublicAccessBlock

`AwsS3AccountPublicAccessBlock` は、アカウントの Amazon S3 パブリックアクセスブロックに関する情報を提供します。

次の例は、 `AwsS3AccountPublicAccessBlock` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsS3AccountPublicAccessBlock` 属性の詳細については、AWS Security Hub API リファレンスの「AwsS3AccountPublicAccessBlockDetails」を参照してください。

例

```
"AwsS3AccountPublicAccessBlock": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": false,
    "RestrictPublicBuckets": true
}
```

AwsS3Bucket

`AwsS3Bucket` オブジェクトは、Amazon S3 バケットに関する詳細を提供します。

次の例は、 `AwsS3Bucket` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsS3Bucket` 属性の詳細については、AWS Security Hub API リファレンスの「AwsS3BucketDetails」を参照してください。

例

```
"AwsS3Bucket": {
    "AccessControlList": "{\"grantSet\":null,\"grantList\":[{\"grantee\":{\"id\":
\"4df55416215956920d9d056aa8b99803a294ea221222bb668b55a8c6bca81094\",\"displayName
\":null},\"permission\":\"FullControl\"},{\"grantee\":\"AllUsers\",\"permission\":
\"ReadAcp\"},{\"grantee\":\"AuthenticatedUsers\",\"permission\":\"ReadAcp\"}",,
    "BucketLifecycleConfiguration": {
       "Rules": [
           {
               "AbortIncompleteMultipartUpload": {
                   "DaysAfterInitiation": 5
               },
               "ExpirationDate": "2021-11-10T00:00:00.000Z",
               "ExpirationInDays": 365,
               "ExpiredObjectDeleteMarker": false,
               "Filter": {
                   "Predicate": {
                       "Operands": [
                           {
                               "Prefix": "tmp/",
                               "Type": "LifecyclePrefixPredicate"
                           },
                           {
                               "Tag": {
                                   "Key": "ArchiveAge",
                                   "Value": "9m"
                               },
                               "Type": "LifecycleTagPredicate"
                           }
                       ],
                       "Type": "LifecycleAndOperator"
                   }
               },
               "ID": "Move rotated logs to Glacier",
               "NoncurrentVersionExpirationInDays": -1,
               "NoncurrentVersionTransitions": [
                   {
                       "Days": 2,
```

```
                        "StorageClass": "GLACIER"
                    }
                ],
                "Prefix": "rotated/",
                "Status": "Enabled",
                "Transitions": [
                    {
                        "Date": "2020-11-10T00:00:00.000Z",
                        "Days": 100,
                        "StorageClass": "GLACIER"
                    }
                ]
            }
        ]
    },
    "BucketLoggingConfiguration": {
     "DestinationBucketName": "s3serversideloggingbucket-123456789012",
     "LogFilePrefix": "buckettestreadwrite23435/"
    },
    "BucketName": "amzn-s3-demo-bucket",
    "BucketNotificationConfiguration": {
     "Configurations": [{
      "Destination": "arn:aws:lambda:us-east-1:123456789012:function:s3_public_write",
      "Events": [
       "s3:ObjectCreated:Put"
      ],
      "Filter": {
       "S3KeyFilter": {
        "FilterRules": [
        {
         "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.PREFIX",
         "Value": "pre"
        },
        {
         "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.SUFFIX",
         "Value": "suf"
        },
        ]
       }
      },
      "Type": "LambdaConfiguration"
     }]
    },
    "BucketVersioningConfiguration": {
```

```
      "IsMfaDeleteEnabled": true,
      "Status": "Off"
     },
     "BucketWebsiteConfiguration": {
      "ErrorDocument": "error.html",
      "IndexDocumentSuffix": "index.html",
      "RedirectAllRequestsTo": {
       "HostName": "example.com",
       "Protocol": "http"
      },
      "RoutingRules": [{
       "Condition": {
        "HttpErrorCodeReturnedEquals": "Redirected",
        "KeyPrefixEquals": "index"
          },
       "Redirect": {
        "HostName": "example.com",
        "HttpRedirectCode": "401",
        "Protocol": "HTTP",
        "ReplaceKeyPrefixWith": "string",
        "ReplaceKeyWith": "string"
       }
      }]
     },
     "CreatedAt": "2007-11-30T01:46:56.000Z",
     "ObjectLockConfiguration": {
      "ObjectLockEnabled": "Enabled",
      "Rule": {
       "DefaultRetention": {
        "Days": null,
        "Mode": "GOVERNANCE",
        "Years": 12
       },
      },
     },
     "OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
     "OwnerName": "s3bucketowner",
     "PublicAccessBlockConfiguration": {
         "BlockPublicAcls": true,
         "BlockPublicPolicy": true,
         "IgnorePublicAcls": true,
         "RestrictPublicBuckets": true,
     },
     "ServerSideEncryptionConfiguration": {
```

```
        "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "AES256",
                    "KMSMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
                }
            }
        ]
    }
}
```

AwsS3Object

`AwsS3Object` オブジェクトは、Amazon S3 オブジェクトに関する情報を提供します。

次の例は、 `AwsS3Object` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsS3Object` 属性の詳細については、AWS Security Hub API リファレンスの「AwsS3ObjectDetails」を参照してください。

例

```
"AwsS3Object": {
    "ContentType": "text/html",
    "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
    "LastModified": "2012-04-23T18:25:43.511Z",
    "ServerSideEncryption": "aws:kms",
    "SSEKMSKeyId": "arn:aws:kms:us-west-2:123456789012:key/4dff8393-e225-4793-
a9a0-608ec069e5a7",
    "VersionId": "ws31OurgOOjH_HHllIxPE35P.MELYaYh"
}
```

ASFF の AwsSageMaker リソース

`AwsSageMaker` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsSageMakerNotebookInstance

`AwsSageMakerNotebookInstance` オブジェクトは、Jupyter Notebook App を実行する機械学習コンピューティングインスタンスである Amazon SageMaker AI ノートブックインスタンスに関する情報を提供します。

次の例は、 `AwsSageMakerNotebookInstance` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsSageMakerNotebookInstance` 属性の詳細については、「AWS Security Hub API リファレンス」の「AwsSageMakerNotebookInstanceDetails」を参照してください。

例

```
"AwsSageMakerNotebookInstance": {
    "DirectInternetAccess": "Disabled",
    "InstanceMetadataServiceConfiguration": {
     "MinimumInstanceMetadataServiceVersion": "1",
    },
    "InstanceType": "ml.t2.medium",
    "LastModifiedTime": "2022-09-09 22:48:32.012000+00:00",
    "NetworkInterfaceId": "eni-06c09ac2541a1bed3",
    "NotebookInstanceArn": "arn:aws:sagemaker:us-east-1:001098605940:notebook-instance/
sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm",
    "NotebookInstanceName":
 "SagemakerNotebookInstanceRootAccessDisabledComplia-8MYjcyofZiXm",
    "NotebookInstanceStatus": "InService",
    "PlatformIdentifier": "notebook-al1-v1",
    "RoleArn": "arn:aws:iam::001098605940:role/sechub-SageMaker-1-scenar-
SageMakerCustomExecution-1R0X32HGC38IW",
    "RootAccess": "Disabled",
    "SecurityGroups": [
     "sg-06b347359ab068745"
    ],
    "SubnetId": "subnet-02c0deea5fa64578e",
    "Url":
 "sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm.notebook.us-
east-1.sagemaker.aws",
    "VolumeSizeInGB": 5
}
```

ASFF の AwsSecretsManager リソース

以下は、 `AwsSecretsManager`リソースの AWS Security Finding Format (ASFF) 構文の例です。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsSecretsManagerSecret

`AwsSecretsManagerSecret` オブジェクトは、Secrets Manager シークレットの詳細を提供します。

次の例は、 `AwsSecretsManagerSecret` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsSecretsManagerSecret` 属性の詳細については、AWS Security Hub API リファレンスの「AwsSecretsManagerSecretDetails」を参照してください。

例

```
"AwsSecretsManagerSecret": {
    "RotationRules": {
        "AutomaticallyAfterDays": 30
    },
    "RotationOccurredWithinFrequency": true,
    "KmsKeyId": "kmsKeyId",
    "RotationEnabled": true,
    "RotationLambdaArn": "arn:aws:lambda:us-
west-2:777788889999:function:MyTestRotationLambda",
    "Deleted": false,
    "Name": "MyTestDatabaseSecret",
    "Description": "My test database secret"
}
```

ASFF の AwsSns リソース

`AwsSns` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsSnsTopic

`AwsSnsTopic` オブジェクトには、Amazon Simple Notification Service トピックの詳細が含まれています。

次の例は、 `AwsSnsTopic` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsSnsTopic` 属性の詳細については、AWS Security Hub API リファレンスの「AwsSnsTopicDetails」を参照してください。

例

```
"AwsSnsTopic": {
    "ApplicationSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
ApplicationSuccessFeedbackRoleArn",
    "FirehoseFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseFailureFeedbackRoleArn",
    "FirehoseSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseSuccessFeedbackRoleArn",
    "HttpFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpFailureFeedbackRoleArn",
    "HttpSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpSuccessFeedbackRoleArn",
    "KmsMasterKeyId": "alias/ExampleAlias",
    "Owner": "123456789012",
    "SqsFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsFailureFeedbackRoleArn",
    "SqsSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsSuccessFeedbackRoleArn",
    "Subscription": {
         "Endpoint": "http://sampleendpoint.com",
         "Protocol": "http"
    },
    "TopicName": "SampleTopic"
}
```

ASFF の AwsSqs リソース

AwsSqs リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsSqsQueue

AwsSqsQueue オブジェクトには、Amazon Simple Queue Service キューに関する情報が含まれています。

次の例は、 AwsSqsQueue オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。AwsSqsQueue 属性の詳細については、AWS Security Hub API リファレンスの「AwsSqsQueueDetails」を参照してください。

例

```
"AwsSqsQueue": {
```

```
    "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
    "KmsDataKeyReusePeriodSeconds": 60,,
    "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "QueueName": "sample-queue"
}
```

ASFF の AwsSsm リソース

以下は、 `AwsSsm`リソースの AWS Security Finding Format (ASFF) 構文の例です。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsSsmPatchCompliance

`AwsSsmPatchCompliance` オブジェクトは、インスタンスにパッチを適用する際に使用したパッチベースラインに基づいて、インスタンスのパッチの状態に関する情報を提供します。

次の例は、 `AwsSsmPatchCompliance` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsSsmPatchCompliance` 属性の詳細については、AWS Security Hub API リファレンスの「AwsSsmPatchComplianceDetails」を参照してください。

例

```
"AwsSsmPatchCompliance": {
    "Patch": {
        "ComplianceSummary": {
            "ComplianceType": "Patch",
            "CompliantCriticalCount": 0,
            "CompliantHighCount": 0,
            "CompliantInformationalCount": 0,
            "CompliantLowCount": 0,
            "CompliantMediumCount": 0,
            "CompliantUnspecifiedCount": 461,
            "ExecutionType": "Command",
            "NonCompliantCriticalCount": 0,
            "NonCompliantHighCount": 0,
            "NonCompliantInformationalCount": 0,
            "NonCompliantLowCount": 0,
            "NonCompliantMediumCount": 0,
            "NonCompliantUnspecifiedCount": 0,
            "OverallSeverity": "UNSPECIFIED",
```

```
            "PatchBaselineId": "pb-0c5b2769ef7cbe587",
            "PatchGroup": "ExamplePatchGroup",
            "Status": "COMPLIANT"
        }
    }
}
```

ASFF の AwsStepFunctions リソース

`AwsStepFunctions` リソースの AWS Security Finding Format (ASFF) 構文の例を次に示します。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsStepFunctionStateMachine

`AwsStepFunctionStateMachine` このオブジェクトは、 AWS Step Functions 一連のイベント駆動型ステップで構成されるワークフローであるステートマシンに関する情報を提供します。

次の例は、 `AwsStepFunctionStateMachine` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsStepFunctionStateMachine` 属性の詳細については、「AWS Security Hub API リファレンス」の「AwsStepFunctionStateMachine」を参照してください。

例

```
"AwsStepFunctionStateMachine": {
    "StateMachineArn": "arn:aws:states:us-
east-1:123456789012:stateMachine:StepFunctionsLogDisableNonCompliantResource-
fQLujTeXvwsb",
    "Name": "StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
    "Status": "ACTIVE",
    "RoleArn": "arn:aws:iam::123456789012:role/teststepfunc-
StatesExecutionRole-1PNM71RVO1UKT",
    "Type": "STANDARD",
    "LoggingConfiguration": {
        "Level": "OFF",
        "IncludeExecutionData": false
    },
    "TracingConfiguration": {
        "Enabled": false
    }
}
```

ASFF の AwsWaf リソース

以下は、 `AwsWaf`リソースの AWS Security Finding Format (ASFF) 構文の例です。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsWafRateBasedRule

`AwsWafRateBasedRule` オブジェクトには、グローバルリソースの AWS WAF レートベースのルールに関する詳細が含まれています。 AWS WAF レートベースのルールは、リクエストを許可、ブロック、またはカウントするタイミングを示す設定を提供します。レートベースのルールには、指定した期間に届くリクエストの数が含まれます。

次の例は、 `AwsWafRateBasedRule` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsWafRateBasedRule` 属性の詳細については、AWS Security Hub API リファレンスの「AwsWafRateBasedRuleDetails」を参照してください。

例

```
"AwsWafRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRateBasedRule

`AwsWafRegionalRateBasedRule` オブジェクトには、リージョンリソースのレートベースのルールに関する詳細が含まれています。レートベースのルールは、リクエストを許可、ブロック、またはカウントするタイミングを示す設定を提供します。レートベースのルールには、指定した期間に届くリクエストの数が含まれます。

次の例は、 `AwsWafRegionalRateBasedRule` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsWafRegionalRateBasedRule` 属性の詳細については、AWS Security Hub API リファレンスの「AwsWafRegionalRateBasedRuleDetails」を参照してください。

例

```
"AwsWafRegionalRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRule

`AwsWafRegionalRule` オブジェクトは、 AWS WAF リージョンルール に関する詳細を提供します。このルールは、許可、ブロック、またはカウントするウェブリクエストを識別します。

次の例は、 `AwsWafRegionalRule` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsWafRegionalRule` 属性の詳細については、AWS Security Hub API リファレンスの「AwsWafRegionalRuleDetails」を参照してください。

例

```
"AwsWafRegionalRule": {
    "MetricName": "SampleWAF_Rule__Metric_1",
    "Name": "bb-waf-regional-rule-not-empty-conditions-compliant",
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de95fe",
    "PredicateList": [{
        "DataId": "127d9346-e607-4e93-9286-c1296fb5445a",
        "Negated": false,
        "Type": "GeoMatch"
    }]
}
```

AwsWafRegionalRuleGroup

`AwsWafRegionalRuleGroup` オブジェクトは、 AWS WAF リージョンルールグループに関する詳細を表示します。ルールグループは、ウェブアクセスコントロールリスト (ウェブ ACL) に追加される事前定義済みルールのコレクションです。

次の例は、 `AwsWafRegionalRuleGroup` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsWafRegionalRuleGroup` 属性の詳細については、AWS Security Hub API リファレンスの「AwsWafRegionalRuleGroupDetails」を参照してください。

例

```
"AwsWafRegionalRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFClassicRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW"
        }
    }],
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
}
```

AwsWafRegionalWebAcl

`AwsWafRegionalWebAcl` は、 AWS WAF リージョン別ウェブアクセスコントロールリスト (ウェブ ACL) の詳細を提供します。ウェブ ACL には、許可、ブロック、またはカウントするリクエストを識別するルールが含まれています。

以下は、 AWS Security Finding 形式 (ASFF) の `AwsWafRegionalWebAcl` 検出の例です。`AwsApiGatewayV2Stage` 属性の詳細については、AWS Security Hub API リファレンスの「AwsWafRegionalWebAclDetails」を参照してください。

例

```
"AwsWafRegionalWebAcl": {
    "DefaultAction": "ALLOW",
    "MetricName" : "web-regional-webacl-metric-1",
```

```
    "Name": "WebACL_123",
    "RulesList": [
        {
            "Action": {
                "Type": "Block"
            },
            "Priority": 3,
            "RuleId": "24445857-852b-4d47-bd9c-61f05e4d223c",
            "Type": "REGULAR",
            "ExcludedRules": [
                {
                    "ExclusionType": "Exclusion",
                    "RuleId": "Rule_id_1"
                }
            ],
            "OverrideAction": {
                "Type": "OVERRIDE"
            }
        }
    ],
    "WebAclId": "443c76f4-2e72-4c89-a2ee-389d501c1f67"
}
```

AwsWafRule

`AwsWafRule` は、 AWS WAF ルールに関する情報を提供します。 AWS WAF ルールは、許可、ブロック、またはカウントするウェブリクエストを識別します。

Security AWS Finding Format (ASFF) `AwsWafRule`の結果の例を次に示します。`AwsApiGatewayV2Stage` 属性の詳細については、AWS Security Hub API リファレンスの「AwsWafRuleDetails」を参照してください。

例

```
"AwsWafRule": {
    "MetricName": "AwsWafRule_Metric_1",
    "Name": "AwsWafRule_Name_1",
    "PredicateList": [{
        "DataId": "cdd225da-32cf-4773-1dc2-3bca3ed9c19c",
        "Negated": false,
        "Type": "GeoMatch"
    }],
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de953e"
```

```
}
```

AwsWafRuleGroup

`AwsWafRuleGroup` は、 AWS WAF ルールグループに関する情報を提供します。 AWS WAF ルールグループは、ウェブアクセスコントロールリスト (ウェブ ACL) に追加される事前定義済みルールのコレクションです。

Security Finding 形式 (ASFF) AWS の検出`AwsWafRuleGroup`結果の例を次に示します。`AwsApiGatewayV2Stage` 属性の詳細については、AWS Security Hub API リファレンスの「AwsWafRuleGroupDetails」を参照してください。

例

```
"AwsWafRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW",
        },
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
    }]
}
```

AwsWafv2RuleGroup

`AwsWafv2RuleGroup` オブジェクトは、 AWS WAF V2 ルールグループに関する詳細を提供します。

次の例は、 `AwsWafv2RuleGroup` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsWafv2RuleGroup` 属性の詳細については、「AWS Security Hub API リファレンス」の「AwsWafv2RuleGroupDetails」を参照してください。

例

```
"AwsWafv2RuleGroup": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/wafv2rulegroupasff/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
    "Capacity": 1000,
    "Description": "Resource for ASFF",
    "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "wafv2rulegroupasff",
    "Rules": [{
     "Action": {
     "Allow": {
      "CustomRequestHandling": {
       "InsertHeaders": [
        {
        "Name": "AllowActionHeader1Name",
        "Value": "AllowActionHeader1Value"
        },
        {
        "Name": "AllowActionHeader2Name",
        "Value": "AllowActionHeader2Value"
        }
       ]
      }
     },
     "Name": "RuleOne",
     "Priority": 1,
     "VisibilityConfig": {
      "CloudWatchMetricsEnabled": true,
      "MetricName": "rulegroupasff",
      "SampledRequestsEnabled": false
     }
    }],
    "VisibilityConfig": {
     "CloudWatchMetricsEnabled": true,
     "MetricName": "rulegroupasff",
     "SampledRequestsEnabled": false
    }
}
```

AwsWafWebAcl

`AwsWafWebAcl` オブジェクトは、 AWS WAF ウェブ ACL に関する詳細を提供します。

次の例は、 `AwsWafWebAcl` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsWafWebAcl` 属性の詳細については、AWS Security Hub API リファレンスの「AwsWafWebAclDetails」を参照してください。

例

```
"AwsWafWebAcl": {
    "DefaultAction": "ALLOW",
    "Name": "MyWafAcl",
    "Rules": [
        {
            "Action": {
                "Type": "ALLOW"
            },
            "ExcludedRules": [
                {
                    "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98"
                }
            ],
            "OverrideAction": {
                "Type": "NONE"
            },
            "Priority": 1,
            "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98",
            "Type": "REGULAR"
        }
    ],
    "WebAclId": "waf-1234567890"
}
```

AwsWafv2WebAcl

`AwsWafv2WebAcl` オブジェクトは、 AWS WAF V2 ウェブ ACL の詳細を提供します。

次の例は、 `AwsWafv2WebAcl` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsWafv2WebAcl` 属性の詳細については、「AWS Security Hub API リファレンス」の「AwsWafv2WebAclDetails」を参照してください。

例

```
"AwsWafv2WebAcl": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/WebACL-RoaD4QexqSxG/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1326,
    "CaptchaConfig": {
     "ImmunityTimeProperty": {
      "ImmunityTime": 500
     }
```

```
    },
    "DefaultAction": {
     "Block": {}
    },
    "Description": "Web ACL for JsonBody testing",
    "ManagedbyFirewallManager": false,
    "Name": "WebACL-RoaD4QexqSxG",
    "Rules": [{
     "Action": {
      "RuleAction": {
       "Block": {}
      }
     },
     "Name": "TestJsonBodyRule",
     "Priority": 1,
     "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "JsonBodyMatchMetric"
     }
    }],
    "VisibilityConfig": {
     "SampledRequestsEnabled": true,
     "CloudWatchMetricsEnabled": true,
     "MetricName": "TestingJsonBodyMetric"
    }
}
```

ASFF の AwsXray リソース

以下は、 `AwsXray`リソースの AWS Security Finding Format (ASFF) 構文の例です。

AWS Security Hub は、さまざまなソースから ASFF に検出結果を正規化します。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

AwsXrayEncryptionConfig

`AwsXrayEncryptionConfig` オブジェクトには、 の暗号化設定に関する情報が含まれています AWS X-Ray。

次の例は、 `AwsXrayEncryptionConfig` オブジェクト AWS のセキュリティ検出結果形式 (ASFF) を示しています。`AwsXrayEncryptionConfig` 属性の詳細については、AWS Security Hub API リファレンスの「AwsXrayEncryptionConfigDetails」を参照してください。

例

```
"AwsXRayEncryptionConfig":{
    "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
    "Status": "UPDATING",
    "Type":"KMS"
}
```

CodeRepository ASFF の オブジェクト

`CodeRepository` オブジェクトは、 AWS リソースに接続し、脆弱性をスキャンするように Amazon Inspector を設定した外部コードリポジトリに関する情報を提供します。

次の例は、 `CodeRepository` オブジェクトの AWS Security Finding Format (ASFF) 構文を示しています。`CodeRepository` 属性の説明を表示するには、 AWS Security Hub API リファレンスのCodeRepositoryDetails」を参照してください。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

例

```
"CodeRepository": {
    "ProviderType": "GITLAB_SELF_MANAGED",
    "ProjectName": "projectName",
    "CodeSecurityIntegrationArn": "arn:aws:inspector2:us-
east-1:123456789012:codesecurity-integration/00000000-0000-0000-0000-000000000000"
}
```

Container ASFF の オブジェクト

次の例は、 `Container` オブジェクトの AWS Security Finding Format (ASFF) 構文を示しています。`Container` 属性の詳細については、AWS Security Hub API リファレンスの「ContainerDetails」を参照してください。ASFF の背景情報については、「AWS Security Finding 形式 (ASFF)」を参照してください。

例

```
"Container": {
    "ContainerRuntime": "docker",
    "ImageId": "image12",
    "ImageName": "1111111/
knotejs@sha256:372131c9fef111111111111115f4ed3ea5f9dce4dc3bd34ce21846588a3",
    "LaunchedAt": "2018-09-29T01:25:54Z",
```

```
    "Name": "knote",
    "Privileged": true,
    "VolumeMounts": [{
        "Name": "vol-03909e9",
        "MountPath": "/mnt/etc"
    }]
}
```

Other ASFF の オブジェクト

AWS Security Finding Format (ASFF) では、 `Other` オブジェクトはカスタムフィールドと値を指定します。ASFF の詳細については、AWS Security Finding 形式 (ASFF) を参照してください。

`Other` オブジェクトを使用すると、リソースのカスタムフィールドと値を指定できます。オブジェクトは、`Other`次の場合に使用できます。

- リソースタイプに対応する `Details` オブジェクトがない場合。リソースの詳細を指定するには、`Other` オブジェクトを使用します。
- リソースタイプの `Details` オブジェクトには、指定するすべての属性が含まれているわけではありません。この場合、リソースタイプの `Details` オブジェクトを使用して、使用可能な属性を指定します。`Other` オブジェクトを使用して、タイプ固有の`Details`オブジェクトにない属性を指定します。
- リソースタイプが提供されたタイプのいずれでもない場合。この場合、 `Resource.Type`を に設定`Other`し、 `Other` オブジェクトを使用して詳細を指定します。

[Type]: (タイプ) 最大 50 個のキーバリューペアのマップ

各キーバリューペアは、次の要件を満たしている必要があります。

- キーは 128 文字未満である必要があります。
- 値は 1,024 文字未満である必要があります。

Security Hub CSPM でのインサイトの表示

AWS Security Hub CSPM では、インサイトは関連する検出結果のコレクションです。インサイトは、注意と介入が必要な特定のセキュリティ領域を特定できます。たとえば、インサイトによって、不十分なセキュリティ慣行を示す結果の対象として EC2 インスタンスが指摘される場合があります。インサイトには、複数の提供元からの結果がまとめられます。

各インサイトは、group by ステートメントとオプションのフィルターによって定義されます。group by ステートメントは、一致する結果をグループ化する方法を示し、インサイトが適用される項目のタイプを識別します。たとえば、インサイトがリソース識別子によってグループ化されている場合、インサイトによってリソース識別子のリストが生成されます。オプションのフィルターは、インサイトの一致する結果を特定します。例えば、特定のプロバイダーからの結果または特定のタイプのリソースに関連付けられた結果のみが、表示されるようにできます。

Security Hub CSPM には、いくつかの組み込みマネージドインサイトが用意されています。マネージド型インサイトを変更または削除することはできません。 AWS 環境と使用状況に固有のセキュリティ問題を追跡するには、カスタムインサイトを作成できます。

AWS Security Hub CSPM コンソールのインサイトページには、使用可能なインサイトのリストが表示されます。

デフォルトでは、リストにはマネージド型インサイトとカスタムインサイトの両方が表示されます。インサイトタイプに基づいてインサイトリストをフィルタリングするには、フィルターフィールドの横にあるドロップダウンメニューからインサイトタイプを選択します。

- 使用できるインサイトをすべて表示するには、[All insights] (すべてのインサイト) を選択します。これがデフォルトのオプションです。
- マネージドインサイトのみを表示するには、Security Hub CSPM マネージドインサイトを選択します。
- カスタムインサイトのみを表示するには、[Custom insights] (カスタムインサイト) を選択します。

インサイトの名前に基づいてインサイトリストをフィルタリングすることもできます。これを行うために、フィルターフィールドに、リストのフィルタリングに使用するテキストを入力します。フィルターでは、大文字と小文字は区別されません。フィルターは、インサイト名の全体または一部にそのテキストが含まれているインサイトを検索します。

インサイトは、一致する結果を生成する統合または標準を有効にしている場合にのみ、結果を返します。たとえば、マネージド型インサイト 29 などです。Top resources by counts of failed CIS checks (失敗した CIS チェック数でのトップリソース) は、Center for Internet Security (CIS) AWS Foundations Benchmark 標準のバージョンを有効にした場合にのみ、結果を返します。

Security Hub CSPM でのインサイトの確認と対応

インサイトごとに、 AWS Security Hub CSPM はまずフィルター条件に一致する検出結果を決定し、次にグループ化属性を使用して一致する検出結果をグループ化します。

コンソールの [インサイト] ページで、結果と検出結果を表示して、それらに基づいてアクションを実行できます。

クロスリージョン集約を有効にすると、集約リージョンでは、マネージド型インサイトの結果 (集約リージョンにサインしている場合) には、集約リージョンとリンクされたリージョンの検出結果が含まれます。カスタムインサイトの結果では、インサイトがリージョンでフィルタリングされない場合、集約リージョンとリンクされたリージョン (集約リージョンにサインしている場合) の検出結果も含まれます。他のリージョンでは、インサイト結果に含まれるのはそのリージョンの結果のみです。

クロスリージョン集約の詳細については、「the section called “リージョン間のデータの集約”」を参照してください。

インサイト結果の表示とアクションの実行

インサイト結果は、インサイトの結果をグループ化したリストで構成されます。例えば、インサイトがリソース識別子に基づいてグループ化されている場合、インサイト結果はリソース識別子のリストになります。結果のリストの各項目は、その項目に一致する結果の数を示します。

検出結果が、リソース識別子またはリソースタイプでグループ化されている場合、結果には、一致する検出結果のすべてのリソースが含まれます。これには、フィルター条件で指定されたリソースタイプとは異なるタイプのリソースが含まれます。例えば、インサイトでは S3 バケットに関連付けられている結果が識別されます。一致する検出結果に S3 バケットリソースと IAM アクセスキーリソースの両方が含まれている場合、インサイト結果には両方のリソースが含まれます。

Security Hub CSPM コンソールでは、結果リストは一致する検出結果の多くから少なくソートされます。Security Hub CSPM は 100 件の結果のみを表示できます。グループ化値の数が 100 を超える場合、最初の 100 個のみが表示されます。

インサイト結果には、結果のリストに加えて、次の属性に一致した結果の数を要約した一連のチャートが表示されます。

- 重要度ラベル - 各重要度ラベルの結果の数
- AWS アカウント ID – 一致する結果の上位 5 つのアカウント IDs
- リソースタイプ - 一致する結果の上位 5 つのリソースタイプ
- リソース ID - 一致する結果の上位 5 つのリソース ID
- 製品名 - 一致する結果の上位 5 つの結果プロバイダー

カスタムアクションを設定している場合、選択した結果をカスタムアクションに送信できます。アクションは、`Security Hub Insight Results` イベントタイプの Amazon CloudWatch ルールに関連付けられている必要があります。詳細については、「the section called “自動応答および自動修復”」を参照してください。カスタムアクションを設定していない場合は、[アクション] メニューは無効です。

Security Hub CSPM console

インサイト結果を表示してアクションを実行するには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで、[Insights] (インサイト) を選択します。
3. インサイト結果のリストを表示するには、インサイト名を選択します。
4. カスタムアクションに送信する結果ごとにチェックボックスを選択します。
5. [Actions] (アクション) メニューから、カスタムアクションを選択します。

Security Hub CSPM API, AWS CLI

インサイト結果を表示してアクションを実行するには (API、 AWS CLI)

インサイト結果を表示するには、Security Hub CSPM API の >GetInsightResultsオペレーションを使用します。を使用する場合は AWS CLI、 get-insight-results コマンドを実行します。

インサイトを特定して結果を返すには、インサイト ARN が必要です。カスタムインサイトのインサイト ARN を取得するには、 `GetInsights` API オペレーションまたは get-insight-results コマンドを使用します。

次の例では、指定されたインサイトの結果を取得します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

プログラムでカスタムアクションを作成する方法については、「カスタムアクションを使用して結果とインサイト結果を EventBridge に送信する」を参照してください。

インサイト結果の検出結果の表示とアクションの実行 (コンソール)

Security Hub CSPM コンソールのインサイト結果リストから、各結果の結果のリストを表示できます。

インサイトの結果を表示して、アクションを実行するには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで、[Insights] (インサイト) を選択します。
3. インサイト結果のリストを表示するには、インサイト名を選択します。
4. インサイト結果の結果のリストを表示するには、インサイト結果のリストからその項目を選択します。結果リストには、ワークフローステータスが `NEW` または `NOTIFIED` で、選択されたインサイト結果のアクティブな結果が表示されます。

結果リストから、以下のアクションを実行できます。

- Security Hub CSPM での検出結果のフィルタリング
- 検出結果の詳細と履歴の確認
- Security Hub CSPM での検出結果のワークフローステータスの設定
- カスタム Security Hub CSPM アクションに結果を送信する

Security Hub CSPM のマネージド型インサイト

AWS Security Hub CSPM は、いくつかのマネージド型インサイトを提供します。

Security Hub CSPM マネージドインサイトを編集または削除することはできません。インサイトの結果と検出結果を表示し、それらに対してアクションを実行できます。また、マネージド型インサイトを新しいカスタムインサイトのベースとして使用することができます。

すべてのインサイトと同様、マネージド型インサイトは、一致する結果をする製品統合またはセキュリティ標準が有効にされている場合にのみ、結果を返します。

リソース識別子でグループ化されたインサイトの場合、結果には、一致する結果のすべてのリソースの識別子が含まれます。これには、フィルター条件のリソースタイプとは異なるタイプのリソースが含まれます。例えば、次のリストのインサイト 2 では Amazon S3 バケットに関連付けられている結

果が識別されます。一致する検出結果に S3 バケットリソースと IAM アクセスキーリソースの両方が含まれている場合、インサイト結果には両方のリソースが含まれます。

Security Hub CSPM は現在、以下のマネージドインサイトを提供しています。

1.検出結果が最も多い AWS リソース

ARN: `arn:aws:securityhub:::insight/securityhub/default/1`

グループ化の基準: リソース識別子

結果フィルター:

- レコードの状態が `ACTIVE`
- ワークフローステータスが `NEW` または `NOTIFIED`

2. パブリック書き込みまたは読み取り許可を含む S3 バケット

ARN: `arn:aws:securityhub:::insight/securityhub/default/10`

グループ化の基準: リソース識別子

結果フィルター:

- タイプが `Effects/Data Exposure` で始まる
- リソースタイプが `AwsS3Bucket`
- レコードの状態が `ACTIVE`
- ワークフローステータスが `NEW` または `NOTIFIED`

3. 最も多くの結果を生成している AMI

ARN: `arn:aws:securityhub:::insight/securityhub/default/3`

グループ化の基準: EC2 インスタンスイメージ ID

結果フィルター:

- リソースタイプが `AwsEc2Instance`
- レコードの状態が `ACTIVE`
- ワークフローステータスが `NEW` または `NOTIFIED`

4. 既知の戦略、手法、および手順 (TTP) に含まれる EC2 インスタンス

ARN: `arn:aws:securityhub:::insight/securityhub/default/14`

グループ化の基準: リソース ID

結果フィルター:

- タイプが TTPs で始まる
- リソースタイプが AwsEc2Instance
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

5.疑わしいアクセスキーアクティビティを持つ AWS プリンシパル

ARN: arn:aws:securityhub:::insight/securityhub/default/9

グループ化の基準: IAM アクセスキーのプリンシパル名

結果フィルター:

- リソースタイプが AwsIamAccessKey
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

6. セキュリティ標準/ベストプラクティスを満たさないインスタンスを AWS リソース化する

ARN: arn:aws:securityhub:::insight/securityhub/default/6

グループ化の基準: リソース ID

結果フィルター:

- タイプが Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

7.潜在的なデータ流出に関連する AWS リソース

ARN: arn:aws:securityhub:::insight/securityhub/default/7

グループ化の基準: リソース ID

結果フィルター:

- タイプが Effects/Data Exfiltration/ で始まる
- レコードの状態が ACTIVE

- ワークフローステータスが NEW または NOTIFIED

8.不正な AWS リソース消費に関連するリソース

ARN: `arn:aws:securityhub:::insight/securityhub/default/8`

グループ化の基準: リソース ID

結果フィルター:

- タイプが `Effects/Resource Consumption` で始まる
- レコードの状態が `ACTIVE`
- ワークフローステータスが `NEW` または `NOTIFIED`

9. セキュリティ標準/ベストプラクティスを満たさない S3 バケット

ARN: `arn:aws:securityhub:::insight/securityhub/default/11`

グループ化の基準: リソース ID

結果フィルター:

- リソースタイプが `AwsS3Bucket`
- タイプが `Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices`
- レコードの状態が `ACTIVE`
- ワークフローステータスが `NEW` または `NOTIFIED`

10. 機密データを含む S3 バケット

ARN: `arn:aws:securityhub:::insight/securityhub/default/12`

グループ化の基準: リソース ID

結果フィルター:

- リソースタイプが `AwsS3Bucket`
- タイプが `Sensitive Data Identifications/` で始まる
- レコードの状態が `ACTIVE`
- ワークフローステータスが `NEW` または `NOTIFIED`

11. 漏洩した可能性がある認証情報

ARN: `arn:aws:securityhub:::insight/securityhub/default/13`

グループ化の基準: リソース ID

結果フィルター:

- タイプが `Sensitive Data Identifications/Passwords/` で始まる
- レコードの状態が `ACTIVE`
- ワークフローステータスが `NEW` または `NOTIFIED`

12. 重要な脆弱性のセキュリティパッチが欠落している EC2 インスタンス

ARN: `arn:aws:securityhub:::insight/securityhub/default/16`

グループ化の基準: リソース ID

結果フィルター:

- タイプが `Software and Configuration Checks/Vulnerabilities/CVE` で始まる
- リソースタイプが `AwsEc2Instance`
- レコードの状態が `ACTIVE`
- ワークフローステータスが `NEW` または `NOTIFIED`

13. 一般的な異常な動作に関連する EC2 インスタンス

ARN: `arn:aws:securityhub:::insight/securityhub/default/17`

グループ化の基準: リソース ID

結果フィルター:

- タイプが `Unusual Behaviors` で始まる
- リソースタイプが `AwsEc2Instance`
- レコードの状態が `ACTIVE`
- ワークフローステータスが `NEW` または `NOTIFIED`

14. インターネットからアクセス可能なポートを持つ EC2 インスタンス

ARN: `arn:aws:securityhub:::insight/securityhub/default/18`

グループ化の基準: リソース ID

結果フィルター:

- タイプが `Software and Configuration Checks/AWS Security Best Practices/Network Reachability` で始まる

- リソースタイプが AwsEc2Instance
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

15. セキュリティ標準/ベストプラクティスを満たさない EC2 インスタンス

    ARN: arn:aws:securityhub:::insight/securityhub/default/19

    グループ化の基準: リソース ID

    結果フィルター:

    - タイプが次のいずれかで始まる。
      - Software and Configuration Checks/Industry and Regulatory Standards/
      - Software and Configuration Checks/AWS Security Best Practices
    - リソースタイプが AwsEc2Instance
    - レコードの状態が ACTIVE
    - ワークフローステータスが NEW または NOTIFIED

16. インターネットに開放されている EC2 インスタンス

    ARN: arn:aws:securityhub:::insight/securityhub/default/21

    グループ化の基準: リソース ID

    結果フィルター:

    - タイプが Software and Configuration Checks/AWS Security Best Practices/Network Reachability で始まる
    - リソースタイプが AwsEc2Instance
    - レコードの状態が ACTIVE
    - ワークフローステータスが NEW または NOTIFIED

17. 敵対的な偵察に関連付けられている EC2 インスタンス

    ARN: arn:aws:securityhub:::insight/securityhub/default/22

    グループ化の基準: リソース ID

    結果フィルター:

    - タイプが TTPs/Discovery/Recon で始まる

- リソースタイプが AwsEc2Instance
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

18. マルウェアに関連付けられている AWS リソース

ARN: arn:aws:securityhub:::insight/securityhub/default/23

グループ化の基準: リソース ID

結果フィルター:

- タイプが次のいずれかで始まる。
  - Effects/Data Exfiltration/Trojan
  - TTPs/Initial Access/Trojan
  - TTPs/Command and Control/Backdoor
  - TTPs/Command and Control/Trojan
  - Software and Configuration Checks/Backdoor
  - Unusual Behaviors/VM/Backdoor
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

19. 暗号通貨の問題に関連する AWS リソース

ARN: arn:aws:securityhub:::insight/securityhub/default/24

グループ化の基準: リソース ID

結果フィルター:

- タイプが次のいずれかで始まる。
  - Effects/Resource Consumption/Cryptocurrency
  - TTPs/Command and Control/CryptoCurrency
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

20. 不正アクセスを試みる AWS リソース

ARN: arn:aws:securityhub:::insight/securityhub/default/25

グループ化の基準: リソース ID

結果フィルター:

- タイプが次のいずれかで始まる。
  - `TTPs/Command and Control/UnauthorizedAccess`
  - `TTPs/Initial Access/UnauthorizedAccess`
  - `Effects/Data Exfiltration/UnauthorizedAccess`
  - `Unusual Behaviors/User/UnauthorizedAccess`
  - `Effects/Resource Consumption/UnauthorizedAccess`
- レコードの状態が `ACTIVE`
- ワークフローステータスが `NEW` または `NOTIFIED`

21. 先週ヒット数が最も多かった脅威インテリジェンス指標

    ARN: `arn:aws:securityhub:::insight/securityhub/default/26`

    結果フィルター:

    - 過去 7 日以内に作成

22. 結果数による上位アカウント

    ARN: `arn:aws:securityhub:::insight/securityhub/default/27`

    グループ化基準： AWS アカウント ID

    結果フィルター:

    - レコードの状態が `ACTIVE`
    - ワークフローステータスが `NEW` または `NOTIFIED`

23. 結果数による上位製品

    ARN: `arn:aws:securityhub:::insight/securityhub/default/28`

    グループ化の基準: 製品名

    結果フィルター:

    - レコードの状態が `ACTIVE`
    - ワークフローステータスが `NEW` または `NOTIFIED`

24. 結果数による重要度

    ARN: `arn:aws:securityhub:::insight/securityhub/default/29`

    グループ化の基準: 重要度ラベル

    結果フィルター:

    - レコードの状態が `ACTIVE`
    - ワークフローステータスが `NEW` または `NOTIFIED`
25. 結果数による上位 S3 バケット

    ARN: `arn:aws:securityhub:::insight/securityhub/default/30`

    グループ化の基準: リソース ID

    結果フィルター:

    - リソースタイプが `AwsS3Bucket`
    - レコードの状態が `ACTIVE`
    - ワークフローステータスが `NEW` または `NOTIFIED`
26. 結果数による上位 EC2 インスタンス

    ARN: `arn:aws:securityhub:::insight/securityhub/default/31`

    グループ化の基準: リソース ID

    結果フィルター:

    - リソースタイプが `AwsEc2Instance`
    - レコードの状態が `ACTIVE`
    - ワークフローステータスが `NEW` または `NOTIFIED`
27. 結果数による上位 AMI

    ARN: `arn:aws:securityhub:::insight/securityhub/default/32`

    グループ化の基準: EC2 インスタンスイメージ ID

    結果フィルター:

    - リソースタイプが `AwsEc2Instance`
    - レコードの状態が `ACTIVE`

- ワークフローステータスが NEW または NOTIFIED

28. 結果数による上位 IAM ユーザー

    ARN: arn:aws:securityhub:::insight/securityhub/default/33

    グループ化の基準: IAM アクセスキー ID

    結果フィルター:

    - リソースタイプが AwsIamAccessKey
    - レコードの状態が ACTIVE
    - ワークフローステータスが NEW または NOTIFIED

29. 失敗した CIS チェック数による上位リソース

    ARN: arn:aws:securityhub:::insight/securityhub/default/34

    グループ化の基準: リソース ID

    結果フィルター:

    - ジェネレーター ID が arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule で始まる
    - 最終日に更新
    - コンプライアンス状況が FAILED
    - レコードの状態が ACTIVE
    - ワークフローステータスが NEW または NOTIFIED

30. 調査数による上位統合

    ARN: arn:aws:securityhub:::insight/securityhub/default/35

    グループ化の基準: 製品 ARN

    結果フィルター:

    - レコードの状態が ACTIVE
    - ワークフローステータスが NEW または NOTIFIED

31. セキュリティチェックの失敗が最も多いリソース

    ARN: arn:aws:securityhub:::insight/securityhub/default/36

    グループ化の基準: リソース ID

結果フィルター:

- 最終日に更新
- コンプライアンス状況が FAILED
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

32。不審なアクティビティに関連する IAM ユーザー

ARN: arn:aws:securityhub:::insight/securityhub/default/37

グループ化の基準: IAM ユーザー

結果フィルター:

- リソースタイプが AwsIamUser
- レコードの状態が ACTIVE
- ワークフローステータスが NEW または NOTIFIED

33。 AWS Health 検出結果が最も多いリソース

ARN: arn:aws:securityhub:::insight/securityhub/default/38

グループ化の基準: リソース ID

結果フィルター:

- ProductNameがHealth

34。 AWS Config 検出結果が最も多いリソース

ARN: arn:aws:securityhub:::insight/securityhub/default/39

グループ化の基準: リソース ID

結果フィルター:

- ProductNameがConfig

35。最も検出結果の多いアプリケーション

ARN: arn:aws:securityhub:::insight/securityhub/default/40

グループ化の基準: ResourceApplicationArn

結果フィルター:

- `RecordState`が`ACTIVE`
- `Workflow.Status` が `NEW` または `NOTIFIED`

Security Hub CSPM のカスタムインサイトについて

AWS Security Hub CSPM マネージドインサイトに加えて、Security Hub CSPM でカスタムインサイトを作成して、環境に固有の問題を追跡できます。カスタムインサイトは、問題のキュレーションされたサブセットを追跡するのに役立ちます。

以下に、設定に役立つカスタムインサイトの例をいくつか示します。

- 管理者アカウントを所有している場合は、カスタムインサイトを設定して、メンバーアカウントに影響を与えているクリティカルな結果および重要度の高い結果を追跡できます。
- 特定の統合 AWS サービスに依存している場合は、カスタムインサイトを設定して、そのサービスからの重大度の高い検出結果を追跡できます。
- サードパーティー統合に依存する場合、カスタムインサイトを設定して、その統合された製品からクリティカルな結果と重大度が高い結果を追跡できます。

まったく新しいカスタムインサイトを作成するか、既存のカスタムインサイトまたはマネージド型インサイトから作成を開始できます。

各インサイトは、次のオプションを使用して設定できます。

- Grouping attribute (グループ化属性) - グループ化属性によって、インサイト結果リストに表示される項目が決定します。例えば、グループ化属性が [製品名] の場合、インサイト結果には、各検出結果プロバイダー関連付けられている結果の数が表示されます。
- Optional filters (オプションのフィルター) - フィルターにより、インサイトの一致する結果が絞り込まれます。

  検出結果は、提供されたすべてのフィルターに一致する場合にのみインサイト結果に含まれます。例えば、フィルターが「製品名が GuardDuty」と「リソースタイプが `AwsS3Bucket`」である場合、一致となる検出結果はこれらの両方の条件に一致する必要があります。

  ただし、Security Hub CSPM は、同じ属性を使用するが値が異なるフィルターにブール OR ロジックを適用します。例えば、フィルターが「製品名が GuardDuty」と「製品名が Amazon Inspector」である場合、検出結果は、Amazon GuardDuty または Amazon Inspector のいずれかによって生成されていれば一致となります。

リソース識別子またはリソースタイプをグループ化属性として使用する場合、インサイト結果には、一致する検出結果のすべてのリソースが含まれます。このリストは、リソースタイプフィルターに一致するリソースに限定されません。例えば、インサイトは S3 バケットに関連付けられている結果を特定し、それらの結果をリソース識別子でグループ化します。一致する結果には、S3 バケットリソースと IAM アクセスキーリソースの両方が含まれます。インサイト結果には、両方のリソースが含まれます。

クロスリージョン集約 を有効にしていて、カスタムインサイトを作成すると、インサイトは集約リージョンとリンクされたリージョンでの一致する検出結果に適用されます。ただし、インサイトにリージョンフィルターが含まれている場合は例外です。

カスタムインサイトの作成

AWS Security Hub CSPM では、カスタムインサイトを使用して特定の検出結果を収集し、環境に固有の問題を追跡できます。カスタムインサイトの背景情報については、「Security Hub CSPM のカスタムインサイトについて」を参照してください。

任意の方法を選択し、手順に従って Security Hub CSPM でカスタムインサイトを作成します。

Security Hub CSPM console

カスタムインサイトを作成するには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで、[Insights] (インサイト) を選択します。
3. [Create insight] (インサイトの作成) を選択します。
4. インサイトのグループ化属性を選択するには:
   a. 検索ボックスを選択して、フィルターオプションを表示します。
   b. [Group by] (グループ化の条件) を選択します。
   c. このインサイトに関連付けられている結果をグループ化するのに使用する属性を選択します。
   d. [Apply] (適用) を選択します。
5. 必要に応じて、このインサイトに使用する追加のフィルターを選択します。フィルターごとに、フィルター条件を定義し、[Apply] (適用) を選択します。
6. [Create insight] (インサイトの作成) を選択します。

7. [インサイトの名前] を入力し、[インサイトの作成] を選択します。

Security Hub CSPM API

カスタムインサイトを作成するには (API)

1. カスタムインサイトを作成するには、Security Hub CSPM API の CreateInsightオペレーションを使用します。を使用する場合は AWS CLI、 create-insight コマンドを実行します。
2. `Name` パラメータにカスタムインサイトの名前を指定します。
3. `Filters` パラメーターを入力して、インサイトに含める結果を指定します。
4. `GroupByAttribute` パラメーターを入力して、インサイトに含まれる結果をグループ化するために使用する属性を指定します。
5. オプションで、特定のフィールドで調査結果をソートする `SortCriteria` パラメーターを指定します。

次の例では、`AwsIamRole` リソースタイプで重要な検出結果を含むカスタムインサイトを作成します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub create-insight --name "Critical role findings" --filters
 '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

カスタムインサイトを作成するには (PowerShell)

1. `New-SHUBInsight` コマンドレットを使用します。
2. `Name` パラメータにカスタムインサイトの名前を指定します。
3. `Filter` パラメーターを入力して、インサイトに含める結果を指定します。
4. `GroupByAttribute` パラメーターを入力して、インサイトに含まれる結果をグループ化するために使用する属性を指定します。

クロスリージョン集約を有効にしていて、集約リージョンからこのコマンドレットを使用すると、インサイトは集約とリンクされたリージョンでの一致する結果に適用されます。

例

```
$Filter = @{
    AwsAccountId = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "XXX"
    }
    ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = 'FAILED'
    }
}
New-SHUBInsight -Filter $Filter -Name TestInsight -GroupByAttribute ResourceId
```

マネージド型インサイトからのカスタムインサイトの作成 (コンソールのみ)

マネージド型インサイトに変更を保存したり、マネージド型インサイトを削除したりすることはできません。ただし、マネージド型インサイトをカスタムインサイトのベースとして使用することができます。これは Security Hub CSPM コンソールでのみ使用できます。

マネージド型インサイトからカスタムインサイトを作成するには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで、[Insights] (インサイト) を選択します。
3. 作成元になるマネージド型インサイトを選択します。
4. 必要に応じてインサイト設定を編集します。
   - インサイトで結果のグループ化に使用される属性を変更するには:
     a. 既存のグループ化を削除するには、[Group by] (グループ化の条件) 設定の横にある X を選択します。
     b. 検索ボックスを選択します。
     c. グループ化に使用する属性を選択します。
     d. [Apply] (適用) を選択します。
   - インサイトからフィルターを削除するには、フィルターの横にある円で囲まれた X を選択します。
   - インサイトにフィルターを追加するには:

a. 検索ボックスを選択します。

b. フィルターとして使用する属性と値を選択します。

c. [Apply] (適用) を選択します。

5. 更新が完了したら、[Create insight] (インサイトの作成) を選択します。
6. プロンプトが表示されたら、[Insight name] (インサイト名) に入力し、[Create insight] (インサイトの作成) を選択します。

カスタムインサイトの編集

既存のカスタムインサイトのグループ化値とフィルターを編集できます。変更後、元のインサイトのまま更新内容を保存するか、新しいインサイトとして更新されたバージョンを保存できます。

AWS Security Hub CSPM では、カスタムインサイトを使用して特定の検出結果を収集し、環境に固有の問題を追跡できます。カスタムインサイトの背景情報については、「Security Hub CSPM のカスタムインサイトについて」を参照してください。

カスタムインサイトを編集するには、希望の方法を選択し、手順に従います。

Security Hub CSPM console

カスタムインサイトを編集するには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで、[Insights] (インサイト) を選択します。
3. 変更するカスタムインサイトを選択します。
4. 必要に応じてインサイト設定を編集します。
   - インサイトで結果のグループ化に使用される属性を変更するには:
     a. 既存のグループ化を削除するには、[Group by] (グループ化の条件) 設定の横にある X を選択します。
     b. 検索ボックスを選択します。
     c. グループ化に使用する属性を選択します。
     d. [Apply] (適用) を選択します。
   - インサイトからフィルターを削除するには、フィルターの横にある円で囲まれた X を選択します。

- インサイトにフィルターを追加するには:

  a. 検索ボックスを選択します。

  b. フィルターとして使用する属性と値を選択します。

  c. [Apply] (適用) を選択します。

5. 更新が完了したら、[Save insight] (インサイトの保存) を選択します。
6. プロンプトが表示されたら、次のいずれかを実行します。

   - 既存のインサイトを更新して変更を反映させる場合は、[Update ***<Insight_Name>***] (<Insight_Name> を更新) を選択してから、[Save insight] (インサイトの保存) を選択します。
   - 更新内容を使用して新しいインサイトを作成する場合は、[Save new insight] (新しいインサイトの保存) を選択します。[Insight name] (インサイトの名前) に入力して、[Save insight] (インサイトの保存) を選択します。

Security Hub CSPM API

カスタムインサイト (API) を編集するには

1. Security Hub CSPM API の `UpdateInsight`オペレーションを使用します。を使用する場合は、 update-insight コマンド AWS CLI を実行します。
2. 更新するカスタムインサイトを特定するには、インサイトの Amazon リソースネーム (ARN) を指定します。カスタムインサイトの ARN を取得するには、`GetInsights` オペレーションまたは get-insights コマンドを実行します。
3. 必要に応じて、`Name`, `Filters` と `GroupByAttribute` パラメータを更新します。

次の例では、指定されたインサイトを更新します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub update-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value":
 "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' --
name "High severity role findings"
```

PowerShell

カスタムインサイトを編集するには (PowerShell)

1. `Update-SHUBInsight` コマンドレットを使用します。
2. カスタムインサイトを特定するには、インサイトの Amazon リソースネーム (ARN) を指定します。カスタムインサイトの ARN を取得するには、`Get-SHUBInsight`コマンドレットを使用します。
3. 必要に応じて、`Name`, `Filter` と `GroupByAttribute` パラメータを更新します。

例

```
$Filter = @{
    ResourceType = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "AwsIamRole"
    }
    SeverityLabel = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "HIGH"
    }
}

Update-SHUBInsight -InsightArn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" -Filter $Filter -Name "High severity role findings"
```

カスタムインサイトの削除

AWS Security Hub CSPM では、カスタムインサイトを使用して特定の検出結果を収集し、環境に固有の問題を追跡できます。カスタムインサイトの背景情報については、「Security Hub CSPM のカスタムインサイトについて」を参照してください。

カスタムインサイトの削除は、希望の方法を選択し、手順に従います。マネージド型インサイトを削除することはできません。

Security Hub CSPM console

カスタムインサイトを削除するには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで、[Insights] (インサイト) を選択します。
3. 削除するカスタムインサイトを見つけます。
4. そのインサイトで、その他のオプションを表示するためのアイコン (カードの右上隅にある 3 つのドット) を選択します。
5. [削除] を選択します。

Security Hub CSPM API

カスタムインサイトを削除するには (API)

1. Security Hub CSPM API の `DeleteInsight`オペレーションを使用します。を使用する場合は、 delete-insight コマンド AWS CLI を実行します。
2. 削除するカスタムインサイトを特定するには、インサイト ARN を指定します。カスタムインサイトの ARN を取得するには、`GetInsights` オペレーションまたは get-insights コマンドを実行します。

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

```
$ aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

PowerShell

カスタムインサイトを削除するには (PowerShell)

1. `Remove-SHUBInsight` コマンドレットを使用します。
2. カスタムインサイトを特定するには、インサイト ARN を指定します。カスタムインサイトの ARN を取得するには、`Get-SHUBInsight`コマンドレットを使用します。

例

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Security Hub CSPM の検出結果を自動的に変更して処理する

AWS Security Hub CSPM には、仕様に基づいて結果を自動的に変更してアクションを実行する機能があります。

Security Hub CSPM は現在、次の 2 種類のオートメーションをサポートしています。

- 自動化ルール — 定義した基準に基づいて、ほぼリアルタイムで検出結果を自動的に更新および非表示にします。
- 自動対応と修正 — 特定の検出結果やインサイトに対して実行する自動アクションを定義するカスタム Amazon EventBridge ルールを作成できます。

自動化ルールは、 AWS Security Finding 形式 (ASFF) で検出結果フィールドを自動的に更新する場合に役立ちます。例えば、自動化ルールを使用して、特定のサードパーティー統合の結果の重要度レベルまたはワークフローステータスを更新できます。自動化ルールを使用すると、このサードパーティー製品の各検出結果の重要度レベルまたはワークフローステータスを手動で更新する必要がなくなります。

EventBridge ルールは、特定の検出結果に関して Security Hub CSPM の外部でアクションを実行する場合や、修復や追加調査のために特定の検出結果をサードパーティーのツールに送信する場合に便利です。ルールを使用して、 AWS Lambda 関数の呼び出しや、特定の検出結果に関する Amazon Simple Notification Service (Amazon SNS) トピックの通知など、サポートされているアクションをトリガーできます。

自動化ルールは、EventBridge ルールが適用される前に有効になります。つまり、EventBridge が検出結果を受信する前に自動化ルールがトリガーされ、検出結果が更新されます。その後、EventBridge のルールが更新された検出結果に適用されます。

セキュリティコントロールの自動化を設定するときは、タイトルや説明ではなく、コントロール ID に基づいてフィルタリングすることをお勧めします。Security Hub CSPM はコントロールのタイトルと説明を更新することがありますが、コントロール IDsは変わりません。

トピック

- Security Hub CSPM のオートメーションルールについて
- EventBridge を使用した自動応答と修復

Security Hub CSPM のオートメーションルールについて

自動化ルールを使用して、 AWS Security Hub CSPM の結果を自動的に更新できます。検出結果を取り込む際に、Security Hub CSPM は検出結果の抑制、重要度の変更、メモの追加など、さまざまなルールアクションを適用できます。このようなルールアクションは、指定した条件に一致する検出結果を変更します。

自動化ルールの使用例には、次のようなものがあります。

- 検出結果のリソース ID がビジネス上重要なリソースを参照している場合、検出結果の重大度を `CRITICAL` に上げます。
- 検出結果が特定の本番稼働用アカウントのリソースに影響する場合は、検出結果の重要度を `HIGH` から `CRITICAL` に引き上げます。
- `INFORMATIONAL` 重要度を持つ `SUPPRESSED` ワークフローステータスの特定の検出結果を割り当てます。

Security Hub CSPM 管理者アカウントからのみ自動化ルールを作成および管理できます。

ルールは、新しい検出結果と更新された検出結果の両方に適用されます。カスタムルールを最初から作成することも、Security Hub CSPM が提供するルールテンプレートを使用することもできます。テンプレートから開始し、必要に応じて変更することもできます。

ルール基準とルールアクションの定義

Security Hub CSPM 管理者アカウントから、1 つ以上のルール条件と 1 つ以上のルールアクションを定義して、自動化ルールを作成できます。結果が定義された基準に一致すると、Security Hub CSPM はルールアクションを適用します。使用可能な条件とアクションの詳細については、「使用可能なルール基準とルールアクション」を参照してください。

Security Hub CSPM は現在、管理者アカウントごとに最大 100 個のオートメーションルールをサポートしています。

Security Hub CSPM 管理者アカウントは、オートメーションルールを編集、表示、削除することもできます。ルールは、管理者アカウントとすべてのメンバーアカウントの一致する検出結果に適用されます。ルール基準としてメンバーアカウント IDs を指定することで、Security Hub CSPM 管理者

はオートメーションルールを使用して、特定のメンバーアカウントの結果を更新または抑制することもできます。

自動化ルールは、作成された AWS リージョン にのみ適用されます。複数のリージョンにルールを適用するには、管理者がリージョンごとにルールを作成する必要があります。これは、Security Hub CSPM コンソール、Security Hub CSPM API、または を使用して実行できますAWS CloudFormation。マルチリージョンデプロイスクリプトを使用することもできます。

使用可能なルール基準とルールアクション

現在、自動化ルールの基準として、次の AWS Security Finding Format (ASFF) フィールドがサポートされています。

ルール基準	フィルター演算子	フィールドタイプ
`AwsAccountId`	`CONTAINS`, `EQUALS`, `PREFIX`, `NOT_CONTAINS`, `NOT_EQUALS`, `PREFIX_NOT_EQUALS`	String
`AwsAccountName`	`CONTAINS`, `EQUALS`, `PREFIX`, `NOT_CONTAINS`, `NOT_EQUALS`, `PREFIX_NOT_EQUALS`	文字列
`CompanyName`	`CONTAINS`, `EQUALS`, `PREFIX`, `NOT_CONTAINS`, `NOT_EQUALS`, `PREFIX_NOT_EQUALS`	文字列
`ComplianceAssociatedStandardsId`	`CONTAINS`, `EQUALS`, `PREFIX`, `NOT_CONTAINS`, `NOT_EQUALS`, `PREFIX_NOT_EQUALS`	文字列
`ComplianceSecurityControlId`	`CONTAINS`, `EQUALS`, `PREFIX`, `NOT_CONTAINS`, `NOT_EQUALS`, `PREFIX_NOT_EQUALS`	String

ルール基準	フィルター演算子	フィールドタイプ
ComplianceStatus	Is, Is Not	選択:[FAILED, NOT_AVAILABLE , PASSED, WARNING]
Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	数値
CreatedAt	Start, End, DateRange	日付 (形式例: 2022-12-01T21:47:39.269Z)
Criticality	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	数値
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
FirstObservedAt	Start, End, DateRange	日付 (形式例: 2022-12-01T21:47:39.269Z)
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
LastObservedAt	Start, End, DateRange	日付 (形式例: 2022-12-01T21:47:39.269Z)

ルール基準	フィルター演算子	フィールドタイプ
NoteText	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
NoteUpdatedAt	Start, End, DateRange	日付 (形式例: 2022-12-01T21:47:39.269Z)
NoteUpdatedBy	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
ProductName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列

ルール基準	フィルター演算子	フィールドタイプ
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	マッピング
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

ルール基準	フィルター演算子	フィールドタイプ
ResourceTags	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	マッピング
ResourceType	Is, Is Not	選択 (ASFF がサポートするリソースを参照)
SeverityLabel	Is, Is Not	選択: [CRITICAL, HIGH, MEDIUM, LOW, INFORMATIONAL]
SourceUrl	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Title	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	文字列
Type	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
UpdatedAt	Start, End, DateRange	日付 (形式例: 2022-12-01T21:47:39.269Z)
UserDefinedFields	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	マッピング

ルール基準	フィルター演算子	フィールドタイプ
VerificationState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
WorkflowStatus	Is, Is Not	選択: [NEW, NOTIFIED, RESOLVED, SUPPRESSED]

文字列フィールドとしてラベル付けされている条件の場合、同じフィールドで異なるフィルター演算子を使用すると、評価ロジックに影響します。詳細については、StringFilterSecurity Hub CSPM API リファレンスの「」を参照してください。 AWS

各基準は、一致する検出結果のフィルタリングに使用できる値の最大数をサポートしています。各基準の制限については、AWS Security Hub CSPM API リファレンスのAutomationRulesFindingFilters「」を参照してください。

現在、次の ASFF フィールドが自動化ルールのアクションとしてサポートされています。

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

特定の ASFF フィールドの詳細については、AWS 「Security Finding Format (ASFF) 構文」を参照してください。

> **Tip**
>
> Security Hub CSPM で特定のコントロールの検出結果の生成を停止する場合は、オートメーションルールを使用する代わりにコントロールを無効にすることをお勧めします。コントロールを無効にすると、Security Hub CSPM はセキュリティチェックの実行を停止し、検出結果の生成を停止するため、そのコントロールに対して料金が発生しません。自動化ルールを使用し、定義した条件に一致する検出結果に関して、特定の ASFF フィールド値を変更することをおすすめします。コントロールの無効化に関する詳細については、「Security Hub CSPM でのコントロールの無効化」を参照してください。

自動化ルールが評価する検出結果

自動化ルールは、ルールの作成後に Security Hub CSPM が BatchImportFindingsオペレーションを通じて生成または取り込む新規および更新された検出結果を評価します。Security Hub CSPM は、コントロールの検出結果を 12 ~ 24 時間ごと、または関連するリソースの状態が変更されたときに更新します。詳細については、「Schedule for running security checks」を参照してください。

自動化ルールは、プロバイダーが提供する元の検出結果を評価します。プロバイダーは、Security Hub CSPM API の `BatchImportFindings`オペレーションを通じて、新しい検出結果を提供し、既存の検出結果を更新できます。BatchUpdateFindings オペレーションを通じてルールを作成した後に検出結果フィールドを更新しても、ルールはトリガーされません。自動化ルールを作成し、同じ検出結果フィールドに影響する `BatchUpdateFindings` 更新を行うと、最後の更新によってそのフィールドの値を設定します。次の例を見てみましょう。

1. `BatchUpdateFindings` を使用して、検出結果の `Workflow.Status` フィールドを `NEW` から `NOTIFIED` に更新します。
2. `GetFindings` を呼び出すと、`Workflow.Status` フィールドの値が `NOTIFIED` になりました。
3. 検出結果の `Workflow.Status` フィールドを `NEW` から `SUPPRESSED` に変更する自動化ルールを作成します (`BatchUpdateFindings` で行われた更新を無視するルールを思い出してください)。
4. 検出結果プロバイダーは `BatchImportFindings` を使用して検出結果を更新し、`Workflow.Status` フィールドを `NEW` に変更します。
5. `GetFindings` を呼び出すと、自動化ルールが適用され、ルールが検出結果に対して最後に実行されたアクションであったため、`Workflow.Status` フィールドの値が `SUPPRESSED` になりました。

Security Hub CSPM コンソールでルールを作成または編集すると、コンソールにルール条件に一致する検出結果のベータが表示されます。自動化ルールは、検出結果プロバイダーによって送信された元の検出結果を評価しますが、コンソールベータは GetFindings API オペレーションへの応答 (つまり、ルールアクションやその他の更新が検出結果に適用された後) に表示されるため、検出結果を最終状態に反映します。

ルールの順序の仕組み

自動化ルールを作成するときは、各ルールに順序を割り当てます。これにより、Security Hub CSPM が自動化ルールを適用する順序が決まり、複数のルールが同じ検出結果または検出結果フィールドに関連する場合に重要になります。

複数のルールアクションが同じ検出結果または検出結果フィールドに関連する場合、ルール順序の数値が最も大きいルールが最後に適用され、最終的な結果となります。

Security Hub CSPM コンソールでルールを作成すると、Security Hub CSPM はルールの作成順序に基づいてルールの順序を自動的に割り当てます。最後に作成されたルールは、ルール順序の数値が最も小さいため、最初に適用されます。Security Hub CSPM は、後続のルールを昇順で適用します。

Security Hub CSPM API または を使用してルールを作成すると AWS CLI、Security Hub CSPM は`RuleOrder`最初に最も低い数値のルールを適用します。その後、後続のルールを昇順で適用します。複数の検出結果に同じ がある場合`RuleOrder`、Security Hub CSPM は、最初に`UpdatedAt`フィールドに以前の値を持つルールを適用します (つまり、最後に編集されたルールが適用されます) 。

ルールの順序はいつでも変更できます。

ルール順序の例:

ルール A (ルール順序は **1**):

- ルール A の基準
  - `ProductName` = `Security Hub CSPM`
  - `Resources.Type` は `S3 Bucket`
  - `Compliance.Status` = `FAILED`
  - `RecordState` は `NEW`
  - `Workflow.Status` = `ACTIVE`
- ルール A のアクション

- `Confidence` を 95 に更新
- `Severity` を `CRITICAL` に更新

ルール B (ルールの順序は **2**):

- ルール B の基準
  - `AwsAccountId` = `123456789012`
- ルール B のアクション
  - `Severity` を `INFORMATIONAL` に更新

ルール A アクションは、まずルール A 基準に一致する Security Hub CSPM の検出結果に適用されます。次に、ルール B アクションは、指定されたアカウント ID を持つ Security Hub CSPM の検出結果に適用されます。この例では、ルール B が最後に適用されるため、指定されたアカウント ID からの検出結果における `Severity` の最終値は `INFORMATIONAL` です。ルール A のアクションに基づくと、一致した検出結果の `Confidence` の最終値は 95 です。

自動化ルールの作成

自動化ルールを使用して、 AWS Security Hub CSPM の結果を自動的に更新できます。カスタムオートメーションルールを最初から作成することも、Security Hub CSPM コンソールで事前入力されたルールテンプレートを使用することもできます。自動化ルールの仕組みに関する背景情報については、「Security Hub CSPM のオートメーションルールについて」を参照してください。

一度に作成できる自動化ルールは 1 つだけです。複数の自動化ルールを作成するには、コンソールの手順を複数回実行するか、必要なパラメータを指定して API またはコマンドを複数回呼び出します。

ルールを検出結果に適用させる各リージョンとアカウントで自動化ルールを作成する必要があります。

Security Hub CSPM コンソールで自動化ルールを作成すると、ルールが適用される検出結果のベータ版が Security Hub CSPM に表示されます。ルール条件に CONTAINS または NOT_CONTAINS フィルターが含まれている場合、ベータは現在サポートされていません。これらのフィルターは、マッピングフィールドタイプと文字列フィールドタイプに対して選択できます。

> **Important**
>
> AWS では、ルール名、説明、またはその他のフィールドに個人を特定できる情報、機密情報、または機密情報を含めないことをお勧めします。

カスタム自動化ルールの作成

ご希望の方法を選択し、次の手順を完了させ、カスタム自動化ルールを作成します。

Console

カスタムオー自動化ルールを作成するには (コンソール)

1. Security Hub CSPM 管理者の認証情報を使用して、https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで [オートメーション] を選択します。
3. [ルールを作成] を選択します。ルールタイプ で、カスタムルールの作成 を選択します。
4. [ルール] セクションで、一意のルール名とルールの説明を入力します。
5. [基準] では、[キー]、[オペレータ]、および [値] のドロップダウンメニューを使用して、ルール条件を指定します。少なくとも 1 つのルール基準を指定する必要があります。

   選択した基準でサポートされている場合、コンソールには、基準に一致する検出結果のベータが表示されます。
6. [自動アクション] の場合は、ドロップダウンメニューを使用して、検出結果がルール条件に一致したときに更新する結果フィールドを指定します。少なくとも 1 つのルールアクションを指定する必要があります。
7. [ルールステータス] では、ルールを作成した後でそのルールを [有効] にするか [無効] にするかを選択します。
8. (オプション) [詳細設定] セクションを展開します。このルールをルール条件に一致する検出結果に適用する最後のルールにしたい場合は、[これらの条件に一致する検出結果については後続のルールを無視する] を選択します。
9. (オプション) [タグ] でタグをキーと値のペアとして追加すると、ルールを簡単に識別できるようになります。
10. [ルールを作成] を選択します。

API

カスタム自動化ルールを作成するには (API)

1. Security Hub CSPM 管理者アカウントCreateAutomationRuleから を実行します。この API は、特定の Amazon リソースネーム (ARN) を使用してルールを作成します。
2. ルールの名前と説明を入力します。
3. このルールを、ルール条件に一致する検出結果に適用する最後のルールにする場合は、IsTerminal パラメーターを true に設定します。
4. RuleOrder パラメータでは、ルールの順序を指定します。Security Hub CSPM は、このパラメータの数値が低いルールを最初に適用します。
5. RuleStatus パラメータで、Security Hub CSPM を有効にして、作成後の結果へのルールの適用を開始するかどうかを指定します。値を指定しない場合、デフォルトは ENABLED になります。値が DISABLED の場合、ルールは作成後に一時停止されます。
6. Criteria パラメータには、Security Hub CSPM が検出結果をフィルタリングするために使用する基準を指定します。ルールアクションは、条件に一致する検出結果に適用されます。サポートされている条件のリストについては、「使用可能なルール基準とルールアクション」を参照してください。
7. Actions パラメータには、検出結果と定義された基準が一致するときに Security Hub CSPM が実行するアクションを指定します。サポートされているアクションのリストについては、「使用可能なルール基準とルールアクション」 を参照してください。

次の AWS CLI コマンド例では、自動化ルールを作成し、ワークフローのステータスと一致する結果のメモを更新します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub create-automation-rule \
--actions '[{
 "Type": "FINDING_FIELDS_UPDATE",
 "FindingFieldsUpdate": {
 "Severity": {
 "Label": "HIGH"
 },
 "Note": {
 "Text": "Known issue that is a risk. Updated by automation rules",
 "UpdatedBy": "sechub-automation"
 }
 }
```

```
 }]' \
--criteria '{
 "SeverityLabel": [{
 "Value": "INFORMATIONAL",
 "Comparison": "EQUALS"
 }]
 }' \
--description "A sample rule" \
--no-is-terminal \
--rule-name "sample rule" \
--rule-order 1 \
--rule-status "ENABLED" \
--region us-east-1
```

テンプレートからの自動化ルールの作成 (コンソールのみ)

ルールテンプレートには、自動化ルールの一般的なユースケースが反映されています。現在、Security Hub CSPM コンソールのみがルールテンプレートをサポートしています。以下の手順を完了して、コンソールのテンプレートから自動化ルールを作成します。

テンプレートから自動化ルールを作成するには (コンソール)

1. Security Hub CSPM 管理者の認証情報を使用して、https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで [オートメーション] を選択します。
3. [ルールを作成] を選択します。ルールタイプ で、 テンプレートからルールを作成する を選択します。
4. ドロップダウンメニューからルールテンプレートを選択します。
5. (オプション) 使用状況の必要に応じて、[ルール]、[基準]、[自動化アクション] セクションを変更します。少なくとも 1 つのルール基準と 1 つのルールアクションを指定する必要があります。

   選択した基準でサポートされている場合、コンソールには、基準に一致する検出結果のベータが表示されます。
6. [ルールステータス] では、ルールを作成した後でそのルールを [有効] にするか [無効] にするかを選択します。
7. (オプション) [詳細設定] セクションを展開します。このルールをルール条件に一致する検出結果に適用する最後のルールにしたい場合は、[これらの条件に一致する検出結果については後続のルールを無視する] を選択します。

8. (オプション) [タグ] でタグをキーと値のペアとして追加すると、ルールを簡単に識別できるようになります。
9. [ルールを作成] を選択します。

自動化ルールを表示する

自動化ルールを使用して、 AWS Security Hub CSPM の結果を自動的に更新できます。自動化ルールの仕組みに関する背景情報については、「Security Hub CSPM のオートメーションルールについて」を参照してください。

ご希望の方法を選択し、手順に従って既存の自動化ルールと各ルールの詳細を確認してください。

自動化ルールによって検出結果がどのように変化したかの履歴を表示するには、「Security Hub CSPM での検出結果の詳細と履歴の確認」を参照してください。

Console

自動化ルールを表示するには (コンソール)

1. Security Hub CSPM 管理者の認証情報を使用して、https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで [オートメーション] を選択します。
3. ルール名を選択します。または、ルールを選択してください。
4. [アクション]、[ログの表示] の順に選択します。

API

自動化ルール (API) を表示するには

1. アカウントの自動化ルールを表示するには、Security Hub CSPM 管理者アカウント`ListAutomationRules`から を実行します。この API は、使用中のルールのルール ARN とその他のメタデータを返します。この API には入力パラメータは必要ありませんが、オプションで結果の数を制限するために `MaxResults` を指定したり、ページ区切りパラメータとして `NextToken` を指定したりできます。`NextToken` の初期値は `NULL` である必要があります。
2. ルールの基準やアクションなど、追加のルールの詳細については、Security Hub CSPM 管理者アカウント`BatchGetAutomationRules`から を実行します。詳細を指定する自動化ルールの ARN を指定します。

次の例では、指定した自動化ルールに関する詳細を取得します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub batch-get-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-
east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
 "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222"]' \
--region us-east-1
```

自動化ルールの編集

自動化ルールを使用して、 AWS Security Hub CSPM の結果を自動的に更新できます。自動化ルールの仕組みに関する背景情報については、「Security Hub CSPM のオートメーションルールについて」を参照してください。

自動化ルールを作成した後、委任 Security Hub CSPM 管理者はルールを編集できます。自動化ルールを編集すると、ルールの編集後に Security Hub CSPM が生成または取り込む新規および更新された検出結果に変更が適用されます。

ご希望の方法を選択し、手順に従って自動化ルールの内容を編集します。1 回のリクエストで 1 つ以上のルールを編集できます。ルール順序の編集方法については、「自動化ルールの順序の編集」を参照してください。

Console

自動化ルールを編集するには (コンソール)

1. Security Hub CSPM 管理者の認証情報を使用して、https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで [オートメーション] を選択します。
3. 編集するルールを選択します。[アクション]、[編集] の順に選択します。
4. 必要に応じてルールを変更し、[変更を保存] を選択します。

API

自動化ルール (API) を編集するには

1. Security Hub CSPM 管理者アカウントBatchUpdateAutomationRulesから を実行します。
2. RuleArn パラメータでは、編集するルールの ARN を指定します。
3. 編集するパラメータの新しい値を指定します。RuleArn 以外の任意のパラメータを編集できます。

次の例では、指定された自動化ルールを更新します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub batch-update-automation-rules \
--update-automation-rules-request-items '[
    {
      "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
          "Note": {
            "Text": "Known issue that is a risk",
            "UpdatedBy": "sechub-automation"
          },
          "Workflow": {
            "Status": "NEW"
          }
        }
      }],
      "Criteria": {
        "SeverityLabel": [{
         "Value": "LOW",
         "Comparison": "EQUALS"
        }]
      },
      "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "RuleOrder": 14,
      "RuleStatus": "DISABLED",
    }
  ]' \
```

```
--region us-east-1
```

自動化ルールの順序の編集

自動化ルールを使用して、 AWS Security Hub CSPM の結果を自動的に更新できます。自動化ルールの仕組みに関する背景情報については、「Security Hub CSPM のオートメーションルールについて」を参照してください。

自動化ルールを作成した後、委任 Security Hub CSPM 管理者はルールを編集できます。

ルール条件とアクションを同じままにし、Security Hub CSPM が自動化ルールを適用する順序を変更する場合は、ルールの順序のみを編集できます。ご希望の方法を選択し、手順に従ってルールの順序を編集します。

自動化ルールの基準またはアクションを編集する手順については、「自動化ルールの編集」を参照してください。

Console

自動化ルールの順序を編集するには (コンソール)

1. Security Hub CSPM 管理者の認証情報を使用して、https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで [オートメーション] を選択します。
3. 順序を変更するルールを選択します。[優先度を編集] を選択します。
4. ルールの優先度を 1 単位上げるには、[上に移動] を選択します。ルールの優先度を 1 単位下げるには、[下に移動] を選択します。ルールに [1] の順序を割り当てるには、[先頭に移動] を選択します (これにより、このルールが他の既存のルールよりも優先されます)。

> **Note**
>
> Security Hub CSPM コンソールでルールを作成すると、Security Hub CSPM はルールの作成順序に基づいてルールの順序を自動的に割り当てます。最後に作成されたルールは、ルール順序の数値が最も小さいため、最初に適用されます。

API

自動化ルールの順序を編集するには (API)

1. Security Hub CSPM 管理者アカウントの `BatchUpdateAutomationRules`オペレーションを使用します。
2. `RuleArn` パラメータでは、順序を編集するルールの ARN を指定します。
3. `RuleOrder` フィールドの値を変更します。

> **Note**
>
> 複数のルールに同じ がある場合`RuleOrder`、Security Hub CSPM は最初に`UpdatedAt`フィールドに以前の値を持つルールを適用します (つまり、最後に編集されたルールが最後に適用されます) 。

自動化ルールの削除または無効化

自動化ルールを使用して、 AWS Security Hub CSPM の結果を自動的に更新できます。自動化ルールの仕組みに関する背景情報については、「Security Hub CSPM のオートメーションルールについて」を参照してください。

自動化ルールを削除すると、Security Hub CSPM はアカウントから削除し、そのルールを結果に適用しなくなります。削除の代わりに、ルールを無効にすることもできます。これにより、ルールは将来の使用のために保持されますが、Security Hub CSPM は、有効にするまで、一致する結果にルールを適用しません。

ご希望の方法を選択し、手順に従って自動化ルールを削除します。1 回のリクエストで 1 つ以上のルールを削除できます。

Console

自動化ルールを削除または無効にするには (コンソール)

1. Security Hub CSPM 管理者の認証情報を使用して、https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで [オートメーション] を選択します。

3. 削除するルールを選択します。[アクション]、[削除] の順に選択します (ルールを保持しながら一時的に無効にするには、[無効] を選択します)。
4. 選択を確認して、[削除] をクリックします。

API

自動化ルール (API) を削除または無効にするには

1. Security Hub CSPM 管理者アカウントの BatchDeleteAutomationRulesオペレーションを使用します。
2. AutomationRulesArns パラメータでは、削除するルールの ARN を指定します (ルールを保持しながら一時的に無効にするには、RuleStatus パラメータの DISABLED を指定します)。

次の例は、指定された自動化ルールを削除します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub batch-delete-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"]' \
--region us-east-1
```

自動化ルールの例

このセクションでは、一般的な Security Hub CSPM ユースケースの自動化ルールの例を示します。これらの例は、Security Hub CSPM コンソールで使用できるルールテンプレートに対応しています。

S3 バケットなどの特定のリソースが危険にさらされている場合は、重要度を「重大」に引き上げます。

この例では、検出結果の ResourceId が特定の Amazon Simple Storage Service (Amazon S3) バケットである場合にルール条件が一致します。ルールアクションは、一致した検出結果の重要度を CRITICAL に変更することです。このテンプレートを変更して他のリソースに適用できます。

API リクエストの例:

```
{
    "IsTerminal": true,
    "RuleName": "Elevate severity of findings that relate to important resources",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity to CRITICAL when specific resource such as
 an S3 bucket is at risk",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub CSPM",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "ResourceId": [{
            "Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "This is a critical resource. Please review ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

CLI コマンドの例:

```
$
aws securityhub create-automation-rule \
--is-terminal \
--rule-name "Elevate severity of findings that relate to important resources" \
--rule-order 1 \
--rule-status "ENABLED" \

--description "Elevate finding severity to CRITICAL when specific resource such as an
 S3 bucket is at risk" \
--criteria '{
"ProductName": [{
"Value": "Security Hub CSPM",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"ResourceId": [{
"Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "This is a critical resource. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
```

```
}]' \
--region us-east-1
```

本番稼働用アカウントのリソースに関連する検出結果の重大度を上げます。

この例では、特定の本番稼働用アカウントで重要度 HIGH の検出結果が生成されると、ルール条件が一致します。ルールアクションは、一致した検出結果の重要度を CRITICAL に変更することです。

API リクエストの例:

```
{
    "IsTerminal": false,
    "RuleName": "Elevate severity for production accounts",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity from HIGH to CRITICAL for findings that
 relate to resources in specific production accounts",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub CSPM",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "HIGH",
            "Comparison": "EQUALS"
        }],
        "AwsAccountId": [
        {
            "Value": "111122223333",
            "Comparison": "EQUALS"
        },
```

```
        {
            "Value": "123456789012",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "A resource in production accounts is at risk. Please review
 ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

CLI コマンドの例:

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Elevate severity of findings that relate to resources in production
 accounts" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Elevate finding severity from HIGH to CRITICAL for findings that relate
 to resources in specific production accounts" \
--criteria '{
"ProductName": [{
"Value": "Security Hub CSPM",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
```

```
}],
"SeverityLabel": [{
"Value": "HIGH",
"Comparison": "EQUALS"
}],
"AwsAccountId": [
{
"Value": "111122223333",
"Comparison": "EQUALS"
},
{
"Value": "123456789012",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "A resource in production accounts is at risk. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

情報の検出結果を非表示にする

この例では、Amazon GuardDuty から Security Hub CSPM に送信されたINFORMATIONAL重要度の検出結果に対してルール基準が一致されます。ルールアクションは、一致した検出結果のワークフローステータスを SUPPRESSED に変更することです。

API リクエストの例:

```
{
    "IsTerminal": false,
    "RuleName": "Suppress informational findings",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Suppress GuardDuty findings with INFORMATIONAL severity",
```

```
    "Criteria": {
        "ProductName": [{
            "Value": "GuardDuty",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "INFORMATIONAL",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
                "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL
 severity",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

CLI コマンドの例:

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Suppress informational findings" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Suppress GuardDuty findings with INFORMATIONAL severity" \
--criteria '{
```

```
"ProductName": [{
"Value": "GuardDuty",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "INFORMATIONAL",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Workflow": {
"Status": "SUPPRESSED"
},
"Note": {
"Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

EventBridge を使用した自動応答と修復

Amazon EventBridge でルールを作成することで、 AWS Security Hub CSPM の検出結果に自動的に応答できます。Security Hub CSPM は、検出結果をイベントとして EventBridge にほぼリアルタイムで送信します。簡単なルールを記述して、注目するイベントと、イベントがルールに一致した場合に自動的に実行するアクションを指定できます。自動的にトリガーできるオペレーションには、以下が含まれます。

- AWS Lambda 関数の呼び出し
- Amazon EC2 Run Command の呼び出し
- Amazon Kinesis Data Streams へのイベントの中継
- AWS Step Functions ステートマシンのアクティブ化
- Amazon SNS トピックまたは Amazon SQS キューの通知
- サードパーティーのチケット発行、チャット、SIEM、またはインシデント対応および管理ツールへの結果の送信

Security Hub CSPM は、すべての新しい検出結果と既存の検出結果へのすべての更新を EventBridge イベントとして EventBridge に自動的に送信します。また、選択した結果とインサイト結果を EventBridge に送信できるカスタムアクションを作成することもできます。

次に、それぞれの種類のイベントに応答するように EventBridge ルールを設定します。

EventBridge の使用方法の詳細については、「Amazon EventBridge ユーザーガイド」を参照してください。

> **Note**
>
> ベストプラクティスとして、EventBridge にアクセスするためにユーザーに付与されたアクセス許可が、必要なアクセス許可のみを付与する最小特権 AWS Identity and Access Management (IAM) ポリシーを使用していることを確認してください。
> 詳細については、「Amazon EventBridge でのアイデンティティとアクセス管理」を参照してください。

クロスアカウント自動応答と修復用のテンプレートのセットは、 AWS ソリューションでも使用できます。このテンプレートでは、EventBridge イベントルールと Lambda 関数を利用します。 AWS CloudFormation および を使用してソリューションをデプロイします AWS Systems Manager。このソリューションによって、完全に自動化された応答と修復のアクションが作成されます。また、Security Hub CSPM カスタムアクションを使用して、ユーザーがトリガーするレスポンスと修復アクションを作成することもできます。ソリューションの設定方法と使用方法の詳細については、「AWSでの自動化されたセキュリティ対応」ソリューションページを参照してください。

トピック

- EventBridge の Security Hub CSPM イベントタイプ
- Security Hub CSPM の EventBridge イベント形式

- Security Hub CSPM 検出結果の EventBridge ルールの設定
- カスタムアクションを使用して結果とインサイト結果を EventBridge に送信する

EventBridge の Security Hub CSPM イベントタイプ

Security Hub CSPM は、次の Amazon EventBridge イベントタイプを使用して EventBridge と統合します。

Security Hub CSPM の EventBridge ダッシュボードでは、すべてのイベントにこれらのイベントタイプがすべて含まれています。

すべての結果 (Security Hub Findings - Imported)

Security Hub CSPM は、すべての新しい検出結果と既存の検出結果へのすべての更新をSecurity Hub Findings - Importedイベントとして EventBridge に自動的に送信します。各 Security Hub Findings - Imported イベントには 1 つの結果が含まれています。

どの `BatchImportFindings` および `BatchUpdateFindings` リクエストでも Security Hub Findings - Imported イベントがトリガーされます。

管理者アカウントの場合、EventBridge のイベントフィードには、管理者アカウントとメンバーアカウントの両方からの結果に関するイベントが含まれます。

集約リージョンでは、イベントフィードには、集約リージョンとリンクされたリージョンからの結果のイベントが含まれます。クロスリージョン結果は、ほぼリアルタイムでイベントフィードに追加されます。結果の集約を設定する方法については、「the section called “リージョン間のデータの集約”」を参照してください。

検出結果を自動的に修復ワークフロー、サードパーティーツール、またはその他のサポートされている EventBridge ターゲットにルーティングするルールを EventBridge で定義できます。ルールでは、結果に特定の属性値が含まれている場合にのみルールを適用するフィルターを指定できます。

このメソッドを使用して、すべての結果、または固有の特徴を持つすべての結果を応答または修復ワークフローに自動的に送信します。

「the section called “EventBridge ルールの設定”」を参照してください。

カスタムアクションの結果 (Security Hub Findings - Custom Action)

Security Hub CSPM は、カスタムアクションに関連付けられた検出結果をSecurity Hub Findings - Custom Actionイベントとして EventBridge に送信します。

これは、Security Hub CSPM コンソールを操作するアナリストが、特定の検出結果、または少数の検出結果をレスポンスまたは修復ワークフローに送信する場合に便利です。一度に最大 20 件の結果のカスタムアクションを選択できます。各結果は、個別の EventBridge イベントとして EventBridge に送信されます。

カスタムアクションを作成したら、カスタムアクションにカスタムアクション ID を割り当てます。この ID を使用すると、そのカスタムアクション ID に関連付けられた結果を受け取った後、指定されたアクションを実行する EventBridge ルールを作成できます。

「the section called “カスタムアクションの設定と使用方法”」を参照してください。

たとえば、 というカスタムアクションを Security Hub CSPM で作成できます`send_to_ticketing`。次に EventBridge で、`send_to_ticketing` カスタムアクション ID を含む結果を EventBridge が受信したときにトリガーされるルールを作成します。ルールには、結果をチケット発行システムに送信するロジックが含まれています。その後、Security Hub CSPM 内の検出結果を選択し、Security Hub CSPM のカスタムアクションを使用して、検出結果をチケット発行システムに手動で送信できます。

さらなる処理のために Security Hub CSPM の検出結果を EventBridge に送信する方法の例については、「 AWS パートナーネットワーク (APN) ブログ」のAWS 「Security Hub CSPM カスタムアクションを PagerDuty と統合する方法」およびAWS 「Security Hub CSPM でカスタムアクションを有効にする方法」を参照してください。

カスタムアクションのインサイト結果 (Security Hub Insight Results)

カスタムアクションを使用すると、インサイト結果のセットも Security Hub Insight Results イベントとして EventBridge に送信できます。インサイト結果は、インサイトに一致するリソースです。インサイト結果を EventBridge に送信するとき、結果を EventBridge に送信しているわけではないことに注意してください。インサイト結果に関連付けられたリソース識別子を送信しているだけです。最大 100 個のリソース識別子を一度に送信できます。

検出結果のカスタムアクションと同様に、まず Security Hub CSPM でカスタムアクションを作成し、次に EventBridge でルールを作成します。

「the section called “カスタムアクションの設定と使用方法”」を参照してください。

例えば、同僚と共有する必要がある特定のインサイト結果があるとします。この場合、カスタムアクションを使用して、チャットまたはチケット発行システム経由で、そのインサイト結果を同僚に送信できます。

Security Hub CSPM の EventBridge イベント形式

Security Hub Findings - Imported、Security Findings - Custom Action、および Security Hub Insight Results イベントタイプでは、次のイベント形式を使用します。

イベント形式は、Security Hub CSPM が EventBridge にイベントを送信するときに使用される形式です。

Security Hub Findings - Imported

Security Hub Findings - Imported Security Hub CSPM から EventBridge に送信されるイベントは、次の形式を使用します。

```
{
   "version":"0",
   "id":"CWE-event-id",
   "detail-type":"Security Hub Findings - Imported",
   "source":"aws.securityhub",
   "account":"111122223333",
   "time":"2019-04-11T21:52:17Z",
   "region":"us-west-2",
   "resources":[
      "arn:aws:securityhub:us-west-2::product/aws/macie/arn:aws:macie:us-
west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/
f2893b211841"
   ],
   "detail":{
      "findings": [{
         <finding content>
       }]
   }
}
```

<finding content> は、イベントによって送信される結果の JSON 形式のコンテンツです。各イベントは 1 つの結果を送信します。

結果の属性の詳細なリストについては、「AWS Security Finding 形式 (ASFF)」を参照してください。

このようなイベントによってトリガーされる EventBridge ルールを設定する方法については、「the section called “EventBridge ルールの設定”」を参照してください。

Security Hub Findings - Custom Action

Security Hub Findings - Custom Action Security Hub CSPM から EventBridge に送信されるイベントは、次の形式を使用します。各結果は個別のイベントで送信されます。

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Findings - Custom Action",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:securityhub:us-west-1:111122223333:action/custom/custom-action-name"
  ],
  "detail": {
    "actionName":"custom-action-name",
    "actionDescription": "description of the action",
    "findings": [
      {
        <finding content>
      }
    ]
  }
}
```

<finding content> は、イベントによって送信される結果の JSON 形式のコンテンツです。各イベントは 1 つの結果を送信します。

結果の属性の詳細なリストについては、「AWS Security Finding 形式 (ASFF)」を参照してください。

このようなイベントによってトリガーされる EventBridge ルールを設定する方法については、「the section called “カスタムアクションの設定と使用方法”」を参照してください。

Security Hub Insight Results

Security Hub Insight Results Security Hub CSPM から EventBridge に送信されるイベントは、次の形式を使用します。

```
{
  "version": "0",
```

```
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Insight Results",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [
      "arn:aws:securityhub:us-west-1:111122223333::product/aws/macie:us-
west-1:222233334444:test/trigger/1ec9cf700ef6be062b19584e0b7d84ec/alert/f2893b211841"
  ],
  "detail": {
    "actionName":"name of the action",
    "actionDescription":"description of the action",
    "insightArn":"ARN of the insight",
    "insightName":"Name of the insight",
    "resultType":"ResourceAwsIamAccessKeyUserName",
    "number of results":"number of results, max of 100",
    "insightResults": [
        {"result 1": 5},
        {"result 2": 6}
    ]
  }
}
```

このようなイベントによってトリガーされる EventBridge ルールを作成する方法については、「the section called “カスタムアクションの設定と使用方法”」を参照してください。

Security Hub CSPM 検出結果の EventBridge ルールの設定

Security Hub Findings - Imported イベントの受信時に実行するアクションを定義するルールを Amazon EventBridge で作成できます。Security Hub Findings - Imported イベントは、`BatchImportFindings` オペレーションと `BatchUpdateFindings` オペレーションの両方による更新によってトリガーされます。

各ルールには、ルールをトリガーするイベントを識別するイベントパターンが含まれています。イベントパターンにはイベントソース (`aws.securityhub`) とイベントタイプ (Security Hub Findings - Imported) が必ず含まれています。イベントパターンでは、ルールが適用される結果を識別するためのフィルターを指定することもできます。

次に、イベントルールによってルールターゲットが識別されます。ターゲットは、EventBridge が Security Hub Findings - Imported イベントを受信し、検索条件がフィルターと一致したときに実行されるアクションです。

ここで説明する手順では、EventBridge コンソールを使用します。このコンソールを使用すると、EventBridge による Amazon CloudWatch Logs への書き込みを有効にする必要なリソースベースポリシーが EventBridge によって自動的に作成されます。

また、EventBridge API の `PutRule` オペレーションを使用することもできます。ただし、EventBridge API を使用する場合は、リソースベースのポリシーを作成する必要があります。必要なポリシーの詳細については、「Amazon EventBridge ユーザーガイド」の「CloudWatch Logs の許可」を参照してください。

イベントパターンの形式

Security Hub Findings - Imported イベントのイベントパターンの形式は次のとおりです。

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source` は、Security Hub CSPM をイベントを生成するサービスとして識別します。
- `detail-type` は、イベントのタイプを示します。
- `detail` はオプションで、イベントパターンのフィルター値を提供します。イベントパターンに `detail` フィールドが含まれていない場合、すべての結果でルールがトリガーされます。

結果は、どの結果属性に基づいてもフィルタリングできます。属性ごとに、1 つ以上の値のカンマ区切りの配列を指定します。

```
"<attribute name>": [ "<value1>", "<value2>"]
```

属性に複数の値を指定すると、それらの値は OR で結合されます。結果にリストされている値が含まれている場合、結果は個々の属性のフィルターと一致しています。例えば、`Severity.Label` の値

として INFORMATIONAL と LOW の両方を指定した場合、結果に INFORMATIONAL または LOW の重要度ラベルが含まれていると、結果は一致となります。

属性が AND で結合されている場合、結果が、指定されたすべての属性のフィルター条件に一致すると、その結果は一致となります。

属性値を指定するときは、 AWS Security Finding Format (ASFF) 構造内のその属性の場所を反映する必要があります。

> **Tip**
>
> コントロールの検出結果をフィルタリングする場合は、Title または Description ではなく、SecurityControlId または SecurityControlArn ASFF フィールドをフィルターとして使用することをお勧めします。前者のフィールドは変更される可能性がありますが、コントロール ID と ARN は静的な識別子です。

次の例では、イベントパターンによって ProductArn と Severity.Label のフィルタ値が提供されています。したがって、Amazon Inspector が生成し、その重要度のラベルが INFORMATIONAL または LOW である場合は、結果が一致します。

```
{
    "source": [
        "aws.securityhub"
     ],
    "detail-type": [
        "Security Hub Findings - Imported"
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
    }
}
```

イベントルールの作成

定義済みのイベントパターンまたはカスタムのイベントパターンを使用して、EventBridge でルールを作成することができます。定義済みのパターンを選択した場合、EventBridge で `source` と `detail-type` が自動的に入力されます。EventBridge には、次の結果の属性のフィルター値を指定するフィールドもあります。

- `AwsAccountId`
- `Compliance.Status`
- `Criticality`
- `ProductArn`
- `RecordState`
- `ResourceId`
- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

EventBridge ルールを作成する (コンソール)

1. Amazon EventBridge コンソールの https://console.aws.amazon.com/events/ を開いてください。
2. 次の値を使用して、検索イベントをモニタリングする EventBridge ルールを作成します。
   - [ルールタイプ] で、[イベントパターンを持つルール] を選択してください。
   - イベントパターンの作成方法を選択します。

次を使用してイベントパターンを作成するには	手順	
テンプレート	[Event pattern] (イベントパターン) のセクションで、次のオプションを選択します。	

次を使用してイベントパターンを作成するには	手順	
	• [イベントソース] で、[AWS のサービス] を選択してください。 • [AWS のサービス] で、[Security Hub] を選択します。 • [Event type] (イベントタイプ)で、[Security Hub Findings - Imported] (Security Hub 調査結果 - インポート) を選択します。 • (オプション) ルールをより具体的にしたいときは、フィルタ値を追加します。例えば、ルールを、アクティブなレコード状態を持つ結果のみに限定するときは、[Specific Record state(s)] (特定のレコード状態) で [Active] (アクティブ) を選択します。	

次を使用してイベントパターンを作成するには	手順	
カスタムのイベントパターン (カスタムパターンは、EventBridge コンソールに表示されない属性に基づいて結果をフィルタリングするときに使用します)。	• [Event pattern] (イベントパターン) セクションで [Custom patterns (JSON editor)] (カスタムパターン (JSONエディター)) を選択し、次のイベントパターンをテキストエリアに貼付けます。 `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "<attribute name> ": [ "<value1>", "<value2>"] } } }` • イベントパターンを更新し、フィルタとして使用する属性および属性値を追加します。 例えば、検証状態が `TRUE_POSITIVE` である結果にのみルールを適用	

次を使用してイベントパターンを作成するには	手順	

	するときは、次のパターン例を使用します。
	
	{
	"source": [
	"aws.secu
	rityhub"
	],
	"detail-type": [
	"Security
	Hub Findings -
	Imported"
	],
	"detail": {
	"findings": {
	"Verifica
	tionState":
	["TRUE_POSITIVE"]
	}
	}
	}	

- ターゲットタイプでAWS サービスを選択し、ターゲットの選択で Amazon SNS トピックや AWS Lambda 関数などのターゲットを選択します。ターゲットは、ルールで定義したイベントパターンに一致するイベントが返されたときにトリガーされます。

ルールの作成に関する詳細については、「Amazon EventBridge ユーザーガイド」の「イベントに反応する Amazon EventBridge ルールの作成」を参照してください。

カスタムアクションを使用して結果とインサイト結果を EventBridge に送信する

AWS Security Hub CSPM カスタムアクションを使用して検出結果またはインサイト結果を Amazon EventBridge に送信するには、まず Security Hub CSPM でカスタムアクションを作成します。次に、EventBridge でカスタムアクションに適用されるルールを定義できます。

最大 50 個のカスタムアクションを作成できます。

クロスリージョン集約を有効にし、集約リージョンの結果を管理する場合は、集約リージョンでカスタムアクションを作成します。

EventBridge のルールでは、カスタムアクションの Amazon リソースネーム (ARN)が使用されます。

カスタムアクションを作成する

AWS Security Hub CSPM でカスタムアクションを作成するときは、その名前、説明、一意の識別子を指定します。

カスタムアクションは、EventBridge イベントが EventBridge ルールと一致するときに実行するアクションを指定します。Security Hub CSPM は、各検出結果をイベントとして EventBridge に送信します。

ご希望の方法を選択し、次の手順を従ってカスタムアクションを作成します。

Console

Security Hub CSPM でカスタムアクションを作成するには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで、[Settings] (設定) を選択して、[Custom actions] (カスタムアクション) を選択します。
3. [Create custom action] (カスタムアクションの作成) を選択します。
4. アクションの [Name] (名前)、[Description] (説明)、および [Custom action ID] (カスタムアクション ID) を指定します。

   [Name] (名前) は 20 文字未満で指定する必要があります。

   [Custom action ID] (カスタムアクション ID) は AWS アカウントごとに一意にする必要があります。
5. [Create custom action] (カスタムアクションの作成) を選択します。
6. [Custom action ARN] (カスタムアクション ARN) を書き留めます。この ARN は、EventBridge でルールを作成してこのアクションに関連付けるときに使用する必要があります。

API

カスタムアクションを作成するには (API)

CreateActionTarget 操作を使用します。を使用している場合は AWS CLI、create-action-target コマンドを実行します。

次の例では、カスタムアクションを作成して、検出結果を修復ツールに送信します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub create-action-target --name "Send to remediation" --description
 "Action to send the finding for remediation tracking" --id "Remediation"
```

EventBridge でルールを定義する

Amazon EventBridge でカスタムアクションをトリガーするには、EventBridge で対応するルールを作成する必要があります。ルールの定義には、カスタムアクションの Amazon リソースネーム (ARN) が含まれます。

Security Hub Findings - Custom Action イベントのイベントパターンの形式は次のとおりです。

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Security Hub Insight Results イベントのイベントパターンの形式は次のとおりです。

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

どちらのパターンでも、`<custom action ARN>` がカスタムアクションの ARN です。したがって、複数のカスタムアクションに適用されるルールを構成できます。

ここで説明する手順では、EventBridge コンソールを使用します。このコンソールを使用すると、EventBridge による CloudWatch Logs への書き込みを有効にする必要なリソースベースポリシーが EventBridge によって自動的に作成されます。

また、EventBridge API の `PutRule` API オペレーションを使用することもできます。ただし、EventBridge API を使用する場合は、リソースベースのポリシーを作成する必要があります。必要なポリシーの詳細については、「Amazon EventBridge ユーザーガイド」の「CloudWatch Logs の許可」を参照してください。

EventBridge でルールを定義するには (EventBridge コンソール)

1. Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) を開きます。
2. ナビゲーションペインで ルール] を選択します。
3. [ルールの作成] を選択します。
4. ルールの名前と説明を入力します。
5. イベントバス] では、このルールに関連付けるイベントバスを選択します。このルールをアカウントからのイベントと一致させるには、[default] (デフォルト) を選択します。アカウントの AWS サービスがイベントを発行すると、常にアカウントのデフォルトのイベントバスに移動します。
6. [Rule type] (ルールタイプ) では、[Rule with an event pattern] (イベントパターンを持つルール) を選択します。
7. [Next] (次へ) を選択します。
8. [Event source] (イベントソース) で、[AWS events] (イベント) を選択します。
9. [イベントパターン] で、[イベントパターンフォーム] を選択します。
10. [イベントパターンフォーム] では、AWS [サービス] を選択します。
11. [AWS のサービス] で、[Security Hub] を選択します。
12. [イベントタイプ] の場合は、次のいずれかの操作を実行します。
    - 結果をカスタムアクションに送信するときに適用するルールを作成するには、[Security Hub Findings - Custom Action] (Security Hub 結果 - カスタムアクション) を選択します。
    - インサイト結果をカスタムアクションに送信するときに適用するルールを作成するには、[Security Hub Insight Results] (Security Hub インサイト結果) を選択します。

13. [Specific custom action ARNs] (特定のカスタムアクション ARN) を選択し、カスタムアクション ARN を追加します。

    このルールを複数のカスタムアクションに適用する場合は、[Add] (追加) を選択し、カスタムアクション ARN をさらに追加します。
14. [次へ] を選択します。
15. [Select targets] (ターゲットの選択) で、このルールが一致した場合に呼び出すターゲットを選択し設定します。
16. [次へ] を選択します。
17. (オプション) ルールに 1 つ以上のタグを入力します。詳細については、Amazon EventBridge ユーザーガイドのAmazon EventBridge のタグを参照してください。
18. 次へをクリックします。
19. ルールの詳細を確認し、ルールの作成 を選択します。

    アカウントで、結果またはインサイト結果に対してカスタムアクションを実行すると、EventBridge でイベントが生成されます。

結果とインサイト結果のカスタムアクションを選択する

AWS Security Hub CSPM カスタムアクションと Amazon EventBridge ルールを作成したら、検出結果とインサイト結果を EventBridge に送信して、自動管理と処理を行うことができます。

イベントは、そのイベントが表示されているアカウントでのみ、EventBridge に送信されます。管理者アカウントを使用して結果を表示すると、イベントは管理者アカウントで EventBridge に送信されます。

AWS API コールを有効にするには、ターゲットコードの実装でロールをメンバーアカウントに切り替える必要があります。つまり、切り替えるロールは、アクションが必要な各メンバーにもデプロイされる必要があります。

検出結果を EventBridge に送信するには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. 結果のリストを表示します。

    - [Findings] (結果) では、有効になっているすべての製品の統合とコントロールの結果を表示できます。

- [セキュリティ標準] では、特定のコントロールから生成された検出結果のリストに移動できます。詳細については、「Security Hub CSPM でのコントロールの詳細の確認」を参照してください。
- [Integrations] (統合) では、有効にした統合によって生成された結果のリストに移動できます。詳細については、「Security Hub CSPM 統合からの検出結果の表示」を参照してください。
- [Insights] (インサイト) では、インサイト結果のリストに移動できます。詳細については、「Security Hub CSPM でのインサイトの確認と対応」を参照してください。

3. 結果を選択して、EventBridge に送信します。一度に最大 20 件の結果を選択できます。
4. [Actions] (アクション) ドロップダウンから、適用する EventBridge ルールと一致するカスタムアクションを選択します。

   Security Hub CSPM は、検出結果ごとに個別の Security Hub 検出結果 - カスタムアクションイベントを送信します。

インサイト結果を EventBridge に送信するには (コンソール)

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで、[Insights] (インサイト) を選択します。
3. [Insights] (インサイト) ページで、EventBridge に送信する結果が含まれているインサイトを選択します。
4. EventBridge に送信するインサイト結果を選択します。一度に最大 20 件の結果を選択できます。
5. [Actions] (アクション) ドロップダウンから、適用する EventBridge ルールと一致するカスタムアクションを選択します。

Security Hub CSPM でのダッシュボードの操作

Security Hub コンソールの概要ページには、リスク、攻撃シーケンス、セキュリティカバレッジの概要が表示されます。このページは、重大度とさまざまなセキュリティ機能のアカウントカバレッジに基づいて、リスクと攻撃シーケンスを特定するのに役立ちます。このページをカスタマイズするには、さまざまなセキュリティウィジェットを追加および削除し、フィルター条件を設定して特定のタイプのデータを取得します。

このページのカスタマイズは、将来の使用のために保存されます。アカウントのユーザーがこのページをカスタマイズすると、カスタマイズ設定はカスタマイズ設定とは別に保存されます。

アカウントが組織の委任管理者アカウントである場合、データにはアカウントとメンバーアカウントの結果が含まれます。アカウントがメンバーアカウントまたはスタンドアロンアカウントである場合、データにはアカウントの結果のみが含まれます。

Security Hub CSPM でクロスリージョン集約を設定すると、このページに集約の結果が表示されます。

> **Note**
>
> このページを開くたびに、自動的に更新されます。ただし、セキュリティスコアとコントロールステータスは 24 時間ごとに更新されます。

リスク概要ウィジェット

このウィジェットには、重大度に基づいてすべてのリスクが表示されます。重要度の高いリスクが最初に表示されます。リスクは、Security Hub CSPM やその他の の検出結果と特性の分析に基づいています AWS のサービス。

脅威の概要ウィジェット

このウィジェットには、重大度に基づいてすべての攻撃シーケンスが表示されます。重要度の高い攻撃シーケンスが最初に表示されます。攻撃シーケンスは一連のイベントに関連しており、環境内の潜在的な脅威を特定します。また、GuardDuty を起点としています。

セキュリティカバレッジウィジェット

[概要] ダッシュボードで利用できるウィジェット

概要ダッシュボードには、最新のクラウドセキュリティ脅威の状況を反映したウィジェットが含まれており、 AWS 顧客のセキュリティオペレーションとエクスペリエンスに導かれています。ウィジェットには、デフォルトで表示されるものもあれば、表示されないものもあります。ウィジェットを追加または削除することで、ダッシュボードの表示をカスタマイズできます。

ウィジェットを追加するには、[概要] ページの右上にある [ウィジェットを追加] を選択します。検索バーに、ウィジェットのタイトルを入力します。ウィジェットをダッシュボードにドラッグアンドドロップします。

デフォルトで表示されるウィジェット

デフォルトでは、[概要] ダッシュボードには以下のウィジェットが表示されます。

上位の脅威シーケンス

最も高い重要度の脅威シーケンスを表示します。Amazon GuardDuty の攻撃シーケンスの検出結果と呼ばれる脅威シーケンスの検出結果は、複数のイベントを関連付けて AWS 、環境に対する潜在的な脅威を特定します。脅威シーケンスには、環境内の進行中または最近の攻撃動作 (24 時間以内) が含まれる場合があり、さらに侵害される可能性があります。Security Hub CSPM で脅威シーケンスの検出結果を受信するには、GuardDuty と GuardDuty S3 Protection が有効になっている必要があります。

トップリスク

環境内の上位リスクの概要を表示します。ウィジェットの上部には、各重要度レベルのリスクの数が表示されます。重要度レベルを選択して、選択した重要度レベルにフィルタリングされたリスクを含むリスクページに移動できます。環境で最も発生頻度の高いリスクが最初に表示されます。このウィジェットは、軽減するリスクの優先順位付けに役立ちます。

セキュリティカバレッジ

カバレッジコントロールの検出結果に基づいて、セキュリティカバレッジの範囲を要約します。カバレッジコントロールは、特定の AWS のサービス とその機能が有効になっているかどうかを確認します (例: [Macie.1] Amazon Macie を有効にする必要があります) 。このウィジェットは、カバレッジコントロールPASSEDの結果があることを確認するのに役立ちます。Security Hub CSPM コンソールには、欠落しているセキュリティ機能を有効にするために、このウィジェットからのリンクが用意されています。中央設定を使用して、複数の AWS アカウント と で欠落しているセキュリティ機能を有効にすることをお勧めします AWS リージョン。詳細については、「Security Hub CSPM の中央設定について」を参照してください。

セキュリティ標準

最新の概要セキュリティスコアと各 Security Hub CSPM 標準のセキュリティスコアを表示します。セキュリティスコア (0 ~ 100%) は、有効になっているすべてのコントロールに対する合格したコントロールの割合を表します。スコアの詳細については、「セキュリティスコアの計算方法」を参照してください。このウィジェットは、全体的なセキュリティ体制を把握するのに役立ちます。

セキュリティ標準

最新の概要セキュリティスコアと各 Security Hub CSPM 標準のセキュリティスコアを表示します。セキュリティスコア (0 ~ 100%) は、有効になっているすべてのコントロールに対する合格

したコントロールの割合を表します。スコアの詳細については、「セキュリティスコアの計算方法」を参照してください。このウィジェットは、全体的なセキュリティ体制を把握するのに役立ちます。

最も検出結果の多いアセット

検出結果が最も多いリソース、アカウント、アプリケーションの概要を示します。リストは、検出結果の数によって降順にソートされます。ウィジェットの各タブには、そのカテゴリの上位 6 つの項目が重大度とリソースタイプ別にグループ化されて表示されます。Total findings 列で数値を選択すると、Security Hub CSPM がアセットの検出結果を示すページを開きます。このウィジェットは、どのコアアセットに潜在的なセキュリティ脅威があるかをすばやく特定するのに役立ちます。

リージョン別の検出結果

Security Hub CSPM が有効になっている各 の検出結果の合計数 AWS リージョン を重要度別にグループ化して表示します。このウィジェットは、特定のリージョンに影響を与える可能性のあるセキュリティ問題を特定するのに役立ちます。集約リージョンでダッシュボードを開くと、このウィジェットはリンクされたリージョンごとに発生する可能性のあるセキュリティ問題をモニタするのに役立ちます。

最も一般的な脅威のタイプ

AWS 環境内の最も一般的な 10 種類の脅威の内訳を提供します。これには、権限のエスカレーションや、公開されている認証情報の使用、悪意のある IP アドレスでの通信などの脅威が含まれます。

このデータを表示するには、Amazon GuardDuty が有効になっている必要があります。有効になっている場合は、このウィジェットで脅威の種類を選択して GuardDuty コンソールを開き、この脅威に関連する検出結果を確認します。このウィジェットは、他のセキュリティ問題との関連で潜在的な脅威を評価するのに役立ちます。

エクスプロイトを伴うソフトウェアの脆弱性

AWS 環境に存在し、既知のエクスプロイトがあるソフトウェアの脆弱性の概要を提供します。また、修正できる脆弱性と修正できない脆弱性の内訳を確認することもできます。

このデータを表示するには、Amazon Inspector が有効になっている必要があります。有効になっている場合は、このウィジェットで統計を選択して Amazon Inspector コンソールを開き、脆弱性に関する詳細を確認します。このウィジェットは、他のセキュリティ問題との関連でソフトウェアの脆弱性を評価するのに役立ちます。

時間の経過に伴う新しい検出結果の数

過去 90 日間の新しい日次検出結果の数の傾向を示します。データを重大度別またはプロバイダー別に分類して、さらに詳しい情報を得ることができます。このウィジェットは、過去 90 日間の特定の時期に検出結果の数が急増または減少したかどうかを把握するのに役立ちます。

最も検出結果の多いリソース

最も多くの検出結果を生成したリソースの概要を、Amazon Simple Storage Service (Amazon S3) バケット、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、および AWS Lambda 関数のリソースタイプ別に示します。

ウィジェットの各タブは、上記のリソースタイプの 1 つに焦点を当て、最も多くの検出結果を生成した 10 個のリソースインスタンスを一覧表示します。特定のリソースの検出結果を確認するには、リソースインスタンスを選択します。このウィジェットは、一般的な AWS リソースに関連付けられているセキュリティ検出結果をトリアージするのに役立ちます。

デフォルトでは非表示のウィジェット

[概要] ダッシュボードでは以下のウィジェットも使用できますが、デフォルトでは非表示になっています。

最も検出結果の多い AMI

最も多くの検出結果が得られた 10 個の Amazon マシンイメージ (AMI) のリストを表示します。このデータは、アカウントで Amazon EC2 が有効になっている場合にのみ利用できます。どの AMI が潜在的なセキュリティリスクをもたらすかを特定するのに役立ちます。

最も検出結果の多い IAM プリンシパル

最も多くの検出結果を生成した 10 AWS Identity and Access Management (IAM) ユーザーのリストを提供します。このウィジェットは、管理タスクや請求タスクを実行するのに役立ちます。どのユーザーが Security Hub CSPM の使用に最も貢献しているかを示します。

最も検出結果の多いアカウント (重大度別)

最も多くの検出結果が得られた 10 個のアカウントのグラフを、重大度別にグループ化して表示します。このウィジェットは、分析と対策の取り組みをどのアカウントに集中させるかを判断するのに役立ちます。

最も検出結果の多いアカウント (リソースタイプ別)

最も多くの結果が得られた 10 個のアカウントのグラフを、リソースタイプ別にグループ化して表示します。このウィジェットは、どのアカウントとリソースタイプを分析と対策で優先するかについて判断するのに役立ちます。

インサイト

Security Hub CSPM マネージドインサイト 5 つと、それらが生成した検出結果の数を一覧表示します。インサイトは、注意が必要な特定のセキュリティ領域を識別します。

AWS 統合の最新の検出結果

統合 AWS のサービスから Security Hub CSPM で受け取った検出結果の数を表示します。また、各統合サービスから最近の検出結果を取得した日時も表示されます。このウィジェットは、複数の から統合された結果データを提供します AWS のサービス。ドリルダウンするには、統合サービスを選択します。Security Hub CSPM は、そのサービスのコンソールを開きます。

Security Hub CSPM での概要ダッシュボードのフィルタリング

AWS Security Hub CSPM コンソールで概要ダッシュボードをキュレートして、最も関連性の高いセキュリティデータのみを含めることができます。例えば、アプリケーションチームのメンバーであれば、本稼働環境にある重要なアプリケーション専用のビューを作成できます。セキュリティチームのメンバーであれば、重大度の高い検出結果に焦点を当てるのに役立つ専用ビューを作成するとよいでしょう。

これらのキュレートされたビューを作成するには、ダッシュボードの上にあるフィルターボックスにフィルター条件を入力します。フィルター条件を適用すると、その条件は [インサイト] ウィジェットと [セキュリティ基準] ウィジェット内のデータを除く、ダッシュボード上のすべてのデータとウィジェットに適用されます。ダッシュボードで使用可能なウィジェットのリストについては、「[概要] ダッシュボードで利用できるウィジェット」を参照してください。

以下のフィールドを使用してデータをフィルタリングできます。

- アカウント名
- アカウント ID
- アプリケーションの Amazon リソースネーム (ARN)
- アプリケーション名
- 製品名 (Security Hub CSPM に結果を送信する AWS のサービス またはサードパーティー製品の場合)

- レコードの状態
- リージョン
- リソースタグ
- 緊急度
- ワークフローステータス

デフォルトでは、`Workflow.Status` が `NOTIFIED` または `NEW`、`RecordState` が `ACTIVE` という条件を使用してダッシュボードデータをフィルタリングします。これらの条件は、ダッシュボードの上、フィルターボックスの下に表示されます。これらの条件を削除するには、削除する条件のフィルタートークンで [X] を選択します。

再使用するフィルター条件を適用する場合は、フィルターセットとして保存できます。フィルターセットは一連のフィルター条件であり、[概要] ダッシュボードでデータを確認するときに再適用するために作成し保存します。

> **Note**
> アプリケーション ARN、アプリケーション名、リソースタグの各フィールドはフィルターセットの一部として保存できません。

フィルターセットの作成と保存

フィルターセットを作成して保存するには、以下の手順に従います。

フィルターセットを作成して保存するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで 概要を選択します。
3. [概要] ダッシュボードの上にあるフィルターボックスに、フィルターセットのフィルター条件を入力します。
4. [フィルターをクリア] メニューで、[新しいフィルターセットを保存] を選択します。
5. [フィルターセットを保存] ダイアログボックスで、フィルターセットの名前を入力します。
6. (オプション) [概要] ページを開くたびにこのフィルターセットをデフォルトで使用するには、このオプションを選択してデフォルトビューとして設定します。

7. [保存] を選択します。

作成して保存したフィルターセットを切り替えるには、[概要] ダッシュボードの上にある [フィルターセットを選択] メニューを使用します。フィルターセットを選択すると、Security Hub CSPM はフィルターセットの基準をダッシュボードのデータに適用します。

フィルターセットの更新または削除

既存のフィルターセットを更新または削除するには、以下の手順を実行します。概要ダッシュボードのデフォルトビューとして現在設定されているフィルターセットを削除すると、デフォルトビューはデフォルトの Security Hub CSPM ビューにリセットされます。

フィルターセットを更新または削除するには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで 概要を選択します。
3. [概要] ページの上にある [フィルターセットを選択] メニューで、フィルターセットを選択します。
4. [フィルターをクリア] メニューで、以下のいずれかを実行します。
   - フィルターセットを更新するには、[現在のフィルターセットを更新] を選択します。次に、表示されるダイアログボックスに変更内容を入力します。
   - フィルターセットを削除するには、[現在のフィルターセットを削除] を選択します。次に、表示されたダイアログボックスで、[削除] を選択します。

Security Hub CSPM での概要ダッシュボードのカスタマイズ

AWS Security Hub CSPM コンソールの 概要ダッシュボードは、いくつかの方法でカスタマイズできます。例えば、ダッシュボードにウィジェットを追加したり、削除したりできます。ダッシュボード上のウィジェットの配置やサイズを変更することもできます。ダッシュボードで使用可能なウィジェットのリストについては、「[概要] ダッシュボードで利用できるウィジェット」を参照してください。

ダッシュボードをカスタマイズすると、Security Hub CSPM は変更をすぐに適用し、新しいダッシュボード設定を保存します。変更は、すべての AWS リージョン およびブラウザのダッシュボードのビューに適用されます。

[概要] ダッシュボードをカスタマイズするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで 概要を選択します。
3. 次のいずれかを実行します。
   - ウィジェットを追加するには、ページの右上隅の [ウィジェットを追加] を選択します。検索バーに、追加するウィジェットのタイトルを入力します。次に、ウィジェットを目的の位置にドラッグします。
   - ウィジェットを削除するには、ウィジェットの右上隅にある 3 つのドットを選択します。
   - ウィジェットを移動するには、ウィジェットの左上隅にあるハンドルを選択し、ウィジェットを目的の位置にドラッグします。
   - ウィジェットのサイズを変更するには、ウィジェットの右下隅にあるリサイズハンドルを選択します。ウィジェットの端を、希望のサイズになるまでドラッグします。

後で元の設定に戻すには、ページ上部の [デフォルトのレイアウトにリセット] を選択します。

Security Hub CSPM のリージョン制限

一部の AWS Security Hub CSPM 機能は、特定の でのみ使用できます AWS リージョン。以下のセクションでは、これらのリージョン制限を示します。Security Hub CSPM が現在利用可能なすべてのリージョンの完全なリストについては、のAWS 「Security Hub エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。

クロスリージョン集約の制限

では AWS GovCloud (US) Regions、クロスリージョン集約は、 の検出結果、検出結果の更新、インサイト AWS GovCloud (US) Regions に対してのみ使用できます。具体的には、 AWS GovCloud (米国東部) リージョンと GovCloud AWS GovCloud (米国西部) リージョン間でのみ、検出結果、検出結果の更新、インサイトを集約できます。

中国リージョンでは、クロスリージョン集約は、中国リージョンの結果、結果の更新、インサイトにのみ使用できます。具体的には、中国 (北京) と中国 (寧夏) リージョン間でのみ、検出結果、検出結果の更新、インサイトを集約できます。

デフォルトでは無効になっているリージョンを集約リージョンとして使用することはできません。デフォルトで無効になっているリージョンのリストについては、「 AWS アカウント管理 リファレンスガイド」の「アカウント AWS リージョン で有効または無効にする」を参照してください。

リージョン別の統合の可用性

一部の統合は、すべてで利用できるわけではありません AWS リージョン。Security Hub CSPM コンソールでは、統合が現在サインインしているリージョンで利用できない場合、統合は統合ページに表示されません。

中国 (北京) および中国 (寧夏) リージョンでサポートされている統合

中国 (北京) および中国 (寧夏) リージョンでは、Security Hub CSPM は との次の統合 AWS のサービスのみをサポートしています。

- AWS Firewall Manager
- Amazon GuardDuty
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender
- AWS Systems Manager Explorer
- AWS Systems Manager OpsCenter
- AWS Systems Manager パッチマネージャー

中国 (北京) および中国 (寧夏) リージョンでは、Security Hub CSPM は次のサードパーティー統合のみをサポートしています。

- Cloud Custodian
- FireEye Helix
- Helecloud
- IBM QRadar
- PagerDuty
- Palo Alto Networks Cortex XSOAR
- Palo Alto Networks VM-Series
- Prowler

- RSA Archer
- Splunk Enterprise
- Splunk Phantom
- ThreatModeler

AWS GovCloud (米国東部) リージョンと AWS GovCloud (米国西部) リージョンでサポートされている統合

AWS GovCloud (米国東部) および AWS GovCloud (米国西部) リージョンでは、Security Hub CSPM は との次の統合 AWS のサービスのみをサポートします。

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty
- AWS Health
- IAM Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender

AWS GovCloud (米国東部) および AWS GovCloud (米国西部) リージョンでは、Security Hub CSPM は次のサードパーティー統合のみをサポートしています。

- Atlassian Jira Service Management
- Atlassian Jira Service Management Cloud
- Atlassian OpsGenie
- Caveonix Cloud
- Cloud Custodian
- Cloud Storage Security Antivirus for Amazon S3
- CrowdStrike Falcon
- FireEye Helix
- Forcepoint CASB

- Forcepoint DLP
- Forcepoint NGFW
- Fugue
- Kion
- MicroFocus ArcSight
- NETSCOUT Cyber Investigator
- PagerDuty
- Palo Alto Networks – Prisma Cloud Compute
- Palo Alto Networks – Prisma Cloud Enterprise
- Palo Alto Networks – VM-Series (AWS GovCloud (米国西部) でのみ利用できます)
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer
- SecureCloudDb
- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

リージョン別の標準の有無

AWS Control Tower サービスマネージド標準は、 を含む がサポート AWS リージョン する AWS Control Tower でのみ使用できます AWS GovCloud (US) Regions。が AWS Control Tower 現在サポートしているリージョンのリストについては、「 AWS Control Tower ユーザーガイド」の「 の AWS リージョン 仕組み AWS Control Tower」を参照してください。

AWS リソースタグ付け標準は、アジアパシフィック (台北) 、アジアパシフィック (タイ) 、メキシコ (中部) の各リージョンでは使用できません。

その他のセキュリティ標準は、Security Hub CSPM が現在利用可能なすべてのリージョンで利用できます。

リージョン別のコントロールの可用性

一部の Security Hub CSPM コントロールは、一部のリージョンでは使用できません。各リージョンで使用できないコントロールのリストについては、「」を参照してくださいSecurity Hub CSPM コントロールのリージョン制限。

Security Hub CSPM コンソールでは、現在サインインしているリージョンで使用できない場合、コントロールはコントロールのリストに表示されません。例外は集約リージョンです。集約リージョンを設定し、そのリージョンにサインインすると、コンソールに集約リージョンまたは 1 つ以上のリンクされたリージョンで使用できるコントロールが表示されます。

Security Hub CSPM コントロールのリージョン制限

一部の AWS Security Hub CSPM コントロールは、すべてで利用できるわけではありません AWS リージョン。このページでは、特定のリージョンで使用できないコントロールを指定します。

Security Hub CSPM コンソールでは、現在サインインしているリージョンで使用できない場合、コントロールはコントロールのリストに表示されません。例外は集約リージョンです。集約リージョンを設定し、そのリージョンにサインインすると、コンソールに集約リージョンまたは 1 つ以上のリンクされたリージョンで使用できるコントロールが表示されます。

AWS リージョン

- 米国東部 (バージニア北部)
- 米国東部 (オハイオ)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- アフリカ (ケープタウン)
- アジアパシフィック (香港)
- アジアパシフィック (ハイデラバード)
- アジアパシフィック (ジャカルタ)
- アジアパシフィック (マレーシア)
- アジアパシフィック (メルボルン)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (大阪)
- アジアパシフィック (ソウル)

- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- アジアパシフィック (台北)
- アジアパシフィック (タイ)
- アジアパシフィック (東京)
- カナダ (中部)
- カナダ西部 (カルガリー)
- 中国 (北京)
- 中国 (寧夏)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (ミラノ)
- 欧州 (パリ)
- 欧州 (スペイン)
- 欧州 (ストックホルム)
- 欧州 (チューリッヒ)
- イスラエル (テルアビブ)
- メキシコ (中部)
- 中東 (バーレーン)
- 中東 (アラブ首長国連邦)
- 南米 (サンパウロ)
- AWS GovCloud (米国東部)
- AWS GovCloud (米国西部)

米国東部 (バージニア北部)

米国東部 (バージニア北部) リージョンでは、以下のコントロールはサポートされていません。

- [ElastiCache.4] ElastiCache レプリケーショングループは保管中に暗号化する必要があります
- [ElastiCache.5] ElastiCache レプリケーショングループは転送時に暗号化する必要があります

- [ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります
- [ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります

米国東部 (オハイオ)

米国東部 (オハイオ) リージョンでは、以下のコントロールはサポートされていません。

- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります

- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です

- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

米国西部 (北カリフォルニア)

米国西部 (北カリフォルニア) リージョンでは、以下のコントロールはサポートされていません。

- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります

- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DocumentDB.6] Amazon DocumentDB クラスターは転送中に暗号化する必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります

- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [Redshift.18] Redshift クラスターでは、マルチ AZ 配置を有効にする必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります

- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

米国西部 (オレゴン)

米国西部 (オレゴン) リージョンでは、以下のコントロールはサポートされていません。

- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります

- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

アフリカ (ケープタウン)

アフリカ (ケープタウン) リージョンでは、以下のコントロールはサポートされていません。

- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります

- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DocumentDB.6] Amazon DocumentDB クラスターは転送中に暗号化する必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします

- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります
- [EC2.179] EC2 トラフィックミラーターゲットにはタグを付ける必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります

- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [RDS.1] RDS スナップショットはプライベートである必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [RedshiftServerless.3] Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります
- [RedshiftServerless.4] Redshift Serverless 名前空間はカスタマーマネージドで暗号化する必要があります AWS KMS keys

- [RedshiftServerless.5] Redshift Serverless 名前空間では、デフォルトの管理者ユーザー名を使用しないでください
- [RedshiftServerless.6] Redshift Serverless 名前空間は CloudWatch Logs にログをエクスポートする必要があります
- [RedshiftServerless.7] Redshift Serverless 名前空間はデフォルトのデータベース名を使用しないでください
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

アジアパシフィック (香港)

アジアパシフィック (香港) リージョンでは、以下のコントロールはサポートされていません。

- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります

- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります

- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります

- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

アジアパシフィック (ハイデラバード)

アジアパシフィック (ハイデラバード) リージョンでは、以下のコントロールはサポートされていません。

- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります

- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります
- [AppConfig.1] AWS AppConfig アプリケーションにはタグを付ける必要があります
- [AppConfig.2] AWS AppConfig 設定プロファイルにはタグを付ける必要があります
- [AppConfig.3] AWS AppConfig 環境にはタグを付ける必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります

- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットが一般公開されていないことを確認します
- [CloudTrail.7] CloudTrail S3 バケットで、S3 バケットアクセスログ記録が有効であることを確認します
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります
- [Cognito.2] Cognito ID プールは認証されていない ID を許可しないでください
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [Detective.1] 検出動作グラフにはタグを付ける必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにはタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります

- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります
- [DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.34] EC2 Transit Gateway ルートテーブルにはタグを付ける必要があります
- [EC2.40] EC2 NAT ゲートウェイにはタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.170] EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.175] EC2 起動テンプレートにはタグを付ける必要があります
- [EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります
- [EC2.179] EC2 トラフィックミラーターゲットにはタグを付ける必要があります
- [EC2.180] EC2 ネットワークインターフェイスでは、送信元/送信先チェックを有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS

- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります
- [ELB.18] Application and Network Load Balancer リスナーは、安全なプロトコルを使用して転送中のデータを暗号化する必要があります
- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります
- [ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください
- [ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。
- [ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります
- [ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.4] AWS Glue Spark ジョブは、サポートされているバージョンの AWS Glue で実行する必要があります
- [GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください

- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [Inspector.1] Amazon Inspector EC2 スキャンを有効にする必要があります
- [Inspector.2] Amazon Inspector ECR スキャンを有効にする必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [Inspector.4] Amazon Inspector Lambda 標準スキャンを有効にする必要があります
- [IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります

- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [Lambda.7] Lambda 関数では AWS X-Ray アクティブなトレースを有効にする必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 機密データ自動検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります
- [MQ.3] Amazon MQ ブローカーでは、自動マイナーバージョンアップグレードが有効になっている必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.4] MSK クラスターではパブリックアクセスを無効にする必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります

- [MSK.6] MSK クラスターは認証されていないアクセスを無効にする必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- [Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインはにはタグを付ける必要があります
- [Opensearch.10] OpenSearch ドメインには、最新のソフトウェアアップデートがインストールされている必要があります
- [Opensearch.11] OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります

- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.37] Aurora PostgreSQL DB クラスターでは、ログを CloudWatch Logs に発行する必要があります
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.18] Redshift クラスターでは、マルチ AZ 配置を有効にする必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [RedshiftServerless.3] Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります
- [RedshiftServerless.4] Redshift Serverless 名前空間はカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 名前空間では、デフォルトの管理者ユーザー名を使用しないでください
- [RedshiftServerless.6] Redshift Serverless 名前空間は CloudWatch Logs にログをエクスポートする必要があります
- [RedshiftServerless.7] Redshift Serverless 名前空間はデフォルトのデータベース名を使用しないでください
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.6] S3 汎用バケットポリシーは、他の へのアクセスを制限する必要があります AWS アカウント
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります
- [SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- [SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません
- [SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります

- [SageMaker.6] SageMaker アプリのイメージ設定にはタグを付ける必要があります
- [SageMaker.7] SageMaker イメージにはタグを付ける必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [SSM.6] SSM Automation では CloudWatch ログ記録が有効になっている必要があります
- [SSM.7] SSM ドキュメントでは、パブリック共有ブロック設定を有効にする必要があります
- [Transfer.3] Transfer Family コネクタではログ記録が有効になっている必要があります
- [Transfer.4] Transfer Family 契約にはタグを付ける必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

アジアパシフィック (ジャカルタ)

アジアパシフィック (ジャカルタ) リージョンでは、以下のコントロールはサポートされていません。

- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります

- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります

- [CodeBuild.1] CodeBuild Bitbucket ソースリポジトリの URL には機密認証情報を含めないでください
- [CodeBuild.2] CodeBuild プロジェクト環境変数にクリアテキストの認証情報を含めることはできません
- [CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- [CodeBuild.4] CodeBuild AWS Configプロジェクト環境にはログ記録設定が必要です
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [Detective.1] 検出動作グラフにはタグを付ける必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにはタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります

- [DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DocumentDB.6] Amazon DocumentDB クラスターは転送中に暗号化する必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります
- [EC2.179] EC2 トラフィックミラーターゲットにはタグを付ける必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります

- [ELB.18] Application and Network Load Balancer リスナーは、安全なプロトコルを使用して転送中のデータを暗号化する必要があります
- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります
- [ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください
- [ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。
- [ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- [IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります

- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 機密データ自動検出を有効にする必要があります
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります

- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

アジアパシフィック (マレーシア)

アジアパシフィック (マレーシア) リージョンでは、以下のコントロールはサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [Account.1] のセキュリティ連絡先情報は に提供する必要があります AWS アカウント
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります
- [AppConfig.1] AWS AppConfig アプリケーションにはタグを付ける必要があります
- [AppConfig.2] AWS AppConfig 設定プロファイルにはタグを付ける必要があります
- [AppConfig.3] AWS AppConfig 環境にはタグを付ける必要があります
- [AppConfig.4] AWS AppConfig 拡張機能の関連付けにはタグを付ける必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.2] AWS AppSync フィールドレベルのログ記録を有効にする必要があります
- [AppSync.4] AWS AppSync GraphQL APIsにはタグを付ける必要があります
- [AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります

- [Athena.2] Athena データカタログにはタグを付ける必要があります
- [Athena.3] Athena ワークグループにはタグを付ける必要があります
- [Athena.4] Athena ワークグループではログ記録が有効になっている必要があります
- [AutoScaling.2] Amazon EC2 Auto Scaling グループは、複数のアベイラビリティーゾーンをカバーする必要があります
- [AutoScaling.3] Auto Scaling グループ起動設定は、EC2 インスタンスを、インスタンスメタデータサービスバージョン 2 (IMDSv2) を必要とするように設定する必要があります
- [AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります
- [AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.2] AWS Backup 復旧ポイントにはタグを付ける必要があります
- [Backup.3] AWS Backup ボールトにはタグを付ける必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [Backup.5] AWS Backup バックアッププランにはタグを付ける必要があります
- 〔バッチ.1] バッチジョブキューにはタグを付ける必要があります
- [Batch.2] バッチスケジューリングポリシーにはタグを付ける必要があります
- [Batch.3] バッチコンピューティング環境にはタグを付ける必要があります
- [Batch.4] マネージドバッチコンピューティング環境のコンピューティングリソースプロパティにはタグを付ける必要があります
- [CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります

- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットが一般公開されていないことを確認します
- [CloudTrail.7] CloudTrail S3 バケットで、S3 バケットアクセスログ記録が有効であることを確認します
- [CloudTrail.10] CloudTrail Lake イベントデータストアはカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [CloudWatch.17] CloudWatch アラームアクションをアクティブにする必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeBuild.1] CodeBuild Bitbucket ソースリポジトリの URL には機密認証情報を含めないでください
- [CodeBuild.2] CodeBuild プロジェクト環境変数にクリアテキストの認証情報を含めることはできません
- [CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- [CodeBuild.4] CodeBuild AWS Configプロジェクト環境にはログ記録設定が必要です
- [CodeBuild.7] CodeBuild レポートグループのエクスポートは保管時に暗号化する必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります

- [Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります
- [Cognito.2] Cognito ID プールは認証されていない ID を許可しないでください
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DataSync.1] DataSync タスクではログ記録が有効になっている必要があります
- [DataSync.2] DataSync タスクにはタグを付ける必要があります
- [Detective.1] 検出動作グラフにはタグを付ける必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにはタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります
- [DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません

- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DocumentDB.6] Amazon DocumentDB クラスターは転送中に暗号化する必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.6] DynamoDB テーブルで、削除保護が有効になっている必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.33] EC2 Transit Gateway アタッチメントにはタグを付ける必要があります
- [EC2.34] EC2 Transit Gateway ルートテーブルにはタグを付ける必要があります
- [EC2.40] EC2 NAT ゲートウェイにはタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.52] EC2 Transit Gateway にはタグを付ける必要があります
- [EC2.53] EC2 セキュリティグループが 0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可することがないようにする必要があります
- [EC2.54] EC2 セキュリティグループは ::/0 からリモートサーバー管理ポートへの入力を許可しない必要があります
- [EC2.55] VPCs は ECR API のインターフェイスエンドポイントで設定する必要があります
- [EC2.56] VPCsは Docker Registry のインターフェイスエンドポイントで設定する必要があります

- [EC2.57] VPCsは Systems Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.170] EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.171] EC2 VPN 接続では、ログ記録が有効になっている必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.174] EC2 DHCP オプションセットにはタグを付ける必要があります
- [EC2.175] EC2 起動テンプレートにはタグを付ける必要があります
- [EC2.176] EC2 プレフィックスリストにはタグを付ける必要があります
- [EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります
- [EC2.178] EC2 トラフィックミラーフィルターにはタグを付ける必要があります
- [EC2.179] EC2 トラフィックミラーターゲットにはタグを付ける必要があります
- [EC2.180] EC2 ネットワークインターフェイスでは、送信元/送信先チェックを有効にする必要があります
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECR.5] ECR リポジトリはカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください
- [ECS.4] ECS コンテナは、非特権として実行する必要があります
- [ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。
- [ECS.8] シークレットは、コンテナ環境の変数として渡さないでください

- [ECS.9] ECS タスク定義にはログ設定が必要です。
- [ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。
- [ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります
- [ECS.16] ECS タスクセットはパブリック IP アドレスを自動的に割り当てないでください。
- [ECS.17] ECS タスク定義はホストネットワークモードを使用しないでください
- [EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります
- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EFS .5] EFS アクセスポイントにはタグを付ける必要があります
- [EFS.6] EFS マウントターゲットは、起動時にパブリック IP アドレスを割り当てるサブネットに関連付けるべきではありません
- [EFS .7] EFS ファイルシステムでは、自動バックアップが有効になっている必要があります
- [EFS .8] EFS ファイルシステムは保管中に暗号化する必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [EKS.6] EKS クラスターにはタグを付ける必要があります
- [EKS.7] EKS ID プロバイダーの設定にはタグを付ける必要があります
- [EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります
- [ELB.10] Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります
- [ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります

- [ELB.18] Application and Network Load Balancer リスナーは、安全なプロトコルを使用して転送中のデータを暗号化する必要があります
- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElastiCache.2] ElastiCache クラスターでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [ElastiCache.3] ElastiCache (Redis OSS) レプリケーショングループでは、自動フェイルオーバーを有効にする必要があります
- [ElastiCache.4] ElastiCache レプリケーショングループは保管中に暗号化する必要があります
- [ElastiCache.5] ElastiCache レプリケーショングループは転送時に暗号化する必要があります
- [ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります
- [ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください
- [ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。
- [ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります
- [ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります
- [EMR.3] Amazon EMR セキュリティ設定は保管時に暗号化する必要があります
- [EMR.4] Amazon EMR セキュリティ設定は転送中に暗号化する必要があります
- [ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります
- [ES.9] Elasticsearch ドメインにはタグを付ける必要があります
- [EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります
- [EventBridge.3] Amazon EventBridge カスタムイベントバスにリソースポリシーがアタッチされている必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります

- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムでは、タグをバックアップにコピーするように設定する必要があります
- [FSx.3] FSx for OpenZFS ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [FSx.4] FSx for NetApp ONTAP ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [FSx.5] FSx for Windows File Server ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.1] AWS Glue ジョブにはタグを付ける必要があります
- [Glue.3] AWS Glue 機械学習変換は保管時に暗号化する必要があります
- [Glue.4] AWS Glue Spark ジョブは、サポートされているバージョンの AWS Glue で実行する必要があります
- [GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- [GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- [GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [GuardDuty.5] GuardDuty EKS 監査ログモニタリングを有効にする必要があります
- [GuardDuty.6] GuardDuty Lambda Protection を有効にする必要があります
- [GuardDuty.7] GuardDuty EKS ランタイムモニタリングを有効にする必要があります
- [GuardDuty.8] GuardDuty Malware Protection for EC2 を有効にする必要があります
- [GuardDuty.9] GuardDuty RDS Protection を有効にする必要があります
- [GuardDuty.10] GuardDuty S3 Protection を有効にする必要があります
- [GuardDuty.11] GuardDuty Runtime Monitoring を有効にする必要があります
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring を有効にする必要があります
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring を有効にする必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください

- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.10] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します
- [IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します
- [IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します
- [IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します
- [IAM.15] IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認します
- [IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています
- [IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します
- [IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.23] IAM Access Analyzer アナライザーにはタグを付ける必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [IAM.28] IAM Access Analyzer 外部アクセスアナライザーを有効にする必要があります

- [Inspector.1] Amazon Inspector EC2 スキャンを有効にする必要があります
- [Inspector.2] Amazon Inspector ECR スキャンを有効にする必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [Inspector.4] Amazon Inspector Lambda 標準スキャンを有効にする必要があります
- [IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります

- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [Kinesis.2] Kinesis ストリームにはタグを付ける必要があります
- [Kinesis.3] Kinesis ストリームには適切なデータ保持期間が必要です
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [KMS.5] KMS キーはパブリックにアクセスしないでください
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Lambda.7] Lambda 関数では AWS X-Ray アクティブなトレースを有効にする必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 機密データ自動検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります
- [MQ.3] Amazon MQ ブローカーでは、自動マイナーバージョンアップグレードが有効になっている必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.4] MSK クラスターではパブリックアクセスを無効にする必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [MSK.6] MSK クラスターは認証されていないアクセスを無効にする必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります

- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.1] Network Firewall ファイアウォールを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.2] Network Firewall ログ記録を有効にする必要があります
- [Network Firewall.3] Network Firewall ポリシーには、1 つ以上のルールグループが関連付けられている必要があります
- [NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、完全なパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、断片化されたパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.6] ステートレス Network Firewall のルールグループを空にしないでください
- [NetworkFirewall.9] Network Firewall は削除保護を有効にする必要があります
- [NetworkFirewall.10] Network Firewall ファイアウォールでは、サブネット変更保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインはにはタグを付ける必要があります

- [Opensearch.10] OpenSearch ドメインには、最新のソフトウェアアップデートがインストールされている必要があります
- [Opensearch.11] OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です
- [PCA.1] AWS Private CA ルート認証機関を無効にする必要があります
- [PCA.2] AWS プライベート CA 認証機関にはタグを付ける必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.18] RDS インスタンスは VPC 内にデプロイする必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RDS.34] Aurora MySQL DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.36] RDS for PostgreSQL DB は CloudWatch Logs にログを発行する必要があります
- [RDS.37] Aurora PostgreSQL DB クラスターでは、ログを CloudWatch Logs に発行する必要があります
- [RDS.38] RDS for PostgreSQL DB インスタンスは転送中に暗号化する必要があります
- [RDS.39] RDS for MySQL DB インスタンスは転送中に暗号化する必要があります
- [RDS.40] RDS for SQL Server DB インスタンスは CloudWatch Logs にログを発行する必要があります
- [RDS.41] RDS for SQL Server DB インスタンスは転送中に暗号化する必要があります
- [RDS.42] RDS for MariaDB DB インスタンスは CloudWatch Logs にログを発行する必要があります
- [RDS.44] RDS for MariaDB DB インスタンスは転送中に暗号化する必要があります
- [RDS.45] Aurora MySQL DB クラスターでは、監査ログ記録を有効にする必要があります
- [PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります
- [Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります

- [Redshift.6] Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります
- [Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください
- [Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.11] Redshift クラスターにはタグを付ける必要があります
- [Redshift.13] Redshift クラスタースナップショットにはタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの入力を許可する必要があります
- [Redshift.16] Redshift クラスターサブネットグループには、複数のアベイラビリティーゾーンからのサブネットが必要です
- [Redshift.17] Redshift クラスターパラメータグループにはタグを付ける必要があります
- [Redshift.18] Redshift クラスターでは、マルチ AZ 配置を有効にする必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [RedshiftServerless.3] Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります
- [RedshiftServerless.4] Redshift Serverless 名前空間はカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 名前空間では、デフォルトの管理者ユーザー名を使用しないでください
- [RedshiftServerless.6] Redshift Serverless 名前空間は CloudWatch Logs にログをエクスポートする必要があります
- [RedshiftServerless.7] Redshift Serverless 名前空間はデフォルトのデータベース名を使用しないでください
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.7] S3 汎用バケットでクロスリージョンレプリケーションを使用する必要があります
- [S3.10] バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です

- [S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります
- [S3.12] ACL は、S3 汎用バケットへのユーザーアクセスの管理に使用しないでください。
- [S3.13] S3 汎用バケットにはライフサイクル設定が必要です
- [S3.19] S3 アクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります
- [S3.22] S3 汎用バケットはオブジェクトレベルの書き込みイベントをログに記録する必要があります
- [S3.23] S3 汎用バケットはオブジェクトレベルの読み取りイベントをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります
- [SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- [SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません
- [SageMaker.4] SageMaker エンドポイントの本番稼働バリアントの初期インスタンス数は 1 より大きい必要があります
- [SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります
- [SageMaker.6] SageMaker アプリのイメージ設定にはタグを付ける必要があります
- [SageMaker.7] SageMaker イメージにはタグを付ける必要があります
- [SageMaker.8] SageMaker ノートブックインスタンスは、サポートされているプラットフォームで実行する必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- [ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SNS.4] SNS トピックアクセスポリシーはパブリックアクセスを許可しないでください
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください

- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [SSM.4] SSM ドキュメントはパブリックにしないでください
- [SSM.5] SSM ドキュメントにはタグを付ける必要があります
- [SSM.6] SSM Automation では CloudWatch ログ記録が有効になっている必要があります
- [SSM.7] SSM ドキュメントでは、パブリック共有ブロック設定を有効にする必要があります
- [StepFunctions.1] Step Functions ステートマシンではログ記録がオンになっている必要があります
- [StepFunctions.2] Step Functions アクティビティにはタグを付ける必要があります
- [Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [Transfer.3] Transfer Family コネクタではログ記録が有効になっている必要があります
- [Transfer.4] Transfer Family 契約にはタグを付ける必要があります
- [Transfer.5] Transfer Family 証明書にはタグを付ける必要があります
- [Transfer.6] Transfer Family コネクタにはタグを付ける必要があります
- [Transfer.7] Transfer Family プロファイルにはタグを付ける必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.2] AWS WAF Classic リージョンルールには少なくとも 1 つの条件が必要です
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です
- [WAF.4] AWS WAF Classic Regional Web ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

アジアパシフィック (メルボルン)

アジアパシフィック (メルボルン) リージョンでは、以下のコントロールはサポートされていません。

- [APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.2] AWS AppSync フィールドレベルのログ記録を有効にする必要があります
- [AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- 〔バッチ.1] バッチジョブキューにはタグを付ける必要があります
- [Batch.3] バッチコンピューティング環境にはタグを付ける必要があります
- [Batch.4] マネージドバッチコンピューティング環境のコンピューティングリソースプロパティにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります

- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [Detective.1] 検出動作グラフにはタグを付ける必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにはタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。

- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります
- [DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DocumentDB.6] Amazon DocumentDB クラスターは転送中に暗号化する必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.18] セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可することをお勧めします
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.34] EC2 Transit Gateway ルートテーブルにはタグを付ける必要があります
- [EC2.40] EC2 NAT ゲートウェイにはタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります

- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.170] EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.175] EC2 起動テンプレートにはタグを付ける必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります
- [ELB.18] Application and Network Load Balancer リスナーは、安全なプロトコルを使用して転送中のデータを暗号化する必要があります
- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElastiCache.2] ElastiCache クラスターでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [ElastiCache.3] ElastiCache (Redis OSS) レプリケーショングループでは、自動フェイルオーバーを有効にする必要があります
- [ElastiCache.4] ElastiCache レプリケーショングループは保管中に暗号化する必要があります
- [ElastiCache.5] ElastiCache レプリケーショングループは転送時に暗号化する必要があります
- [ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります
- [ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください
- [ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。
- [ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります

- [ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.3] FSx for OpenZFS ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.4] AWS Glue Spark ジョブは、サポートされているバージョンの AWS Glue で実行する必要があります
- [GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.10] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します
- [IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します
- [IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します
- [IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します

- [IAM.15] IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認します
- [IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています
- [IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します
- [IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [Inspector.1] Amazon Inspector EC2 スキャンを有効にする必要があります
- [Inspector.2] Amazon Inspector ECR スキャンを有効にする必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [Inspector.4] Amazon Inspector Lambda 標準スキャンを有効にする必要があります
- [IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります

- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 機密データ自動検出を有効にする必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります

- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- [Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインはにはタグを付ける必要があります
- [Opensearch.10] OpenSearch ドメインには、最新のソフトウェアアップデートがインストールされている必要があります
- [Opensearch.11] OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です
- [RDS.1] RDS スナップショットはプライベートである必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.37] Aurora PostgreSQL DB クラスターでは、ログを CloudWatch Logs に発行する必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります

- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [RedshiftServerless.3] Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります
- [RedshiftServerless.4] Redshift Serverless 名前空間はカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 名前空間では、デフォルトの管理者ユーザー名を使用しないでください
- [RedshiftServerless.6] Redshift Serverless 名前空間は CloudWatch Logs にログをエクスポートする必要があります
- [RedshiftServerless.7] Redshift Serverless 名前空間はデフォルトのデータベース名を使用しないでください
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります
- [SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- [SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません
- [SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります
- [SageMaker.6] SageMaker アプリのイメージ設定にはタグを付ける必要があります
- [SageMaker.7] SageMaker イメージにはタグを付ける必要があります
- [SageMaker.8] SageMaker ノートブックインスタンスは、サポートされているプラットフォームで実行する必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください

- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [SSM.4] SSM ドキュメントはパブリックにしないでください
- [SSM.7] SSM ドキュメントでは、パブリック共有ブロック設定を有効にする必要があります
- [StepFunctions.1] Step Functions ステートマシンではログ記録がオンになっている必要があります
- [Transfer.3] Transfer Family コネクタではログ記録が有効になっている必要があります
- [Transfer.4] Transfer Family 契約にはタグを付ける必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

アジアパシフィック (ムンバイ)

アジアパシフィック (ムンバイ) リージョンでは、以下のコントロールはサポートされていません。

- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります

- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります

- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

アジアパシフィック (大阪)

アジアパシフィック (大阪) リージョンでは、以下のコントロールはサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります

- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [Detective.1] 検出動作グラフにはタグを付ける必要があります
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります

- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DocumentDB.6] Amazon DocumentDB クラスターは転送中に暗号化する必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.20] AWS Site-to-Site VPN トンネルが稼働している必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.55] VPCs は ECR API のインターフェイスエンドポイントで設定する必要があります
- [EC2.56] VPCsは Docker Registry のインターフェイスエンドポイントで設定する必要があります
- [EC2.57] VPCsは Systems Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager

- [ELB.3] Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります
- [ELB.4] Application Load Balancer は、無効な http ヘッダーを削除するように設定する必要があります
- [ELB.6] アプリケーション、ゲートウェイ、および Network Load Balancer で削除保護を有効にする必要があります
- [ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な uration AWS Configを持つ事前定義されたセキュリティポリシーを使用する必要があります
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください
- [ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。
- [ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります

- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [RedshiftServerless.3] Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります

- [RedshiftServerless.4] Redshift Serverless 名前空間はカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 名前空間では、デフォルトの管理者ユーザー名を使用しないでください
- [RedshiftServerless.6] Redshift Serverless 名前空間は CloudWatch Logs にログをエクスポートする必要があります
- [RedshiftServerless.7] Redshift Serverless 名前空間はデフォルトのデータベース名を使用しないでください
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

アジアパシフィック (ソウル)

アジアパシフィック (ソウル) リージョンでは、以下のコントロールはサポートされていません。

- [AppRunner.1] App Runner サービスにはタグを付ける必要があります

- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.2] Cognito ID プールは認証されていない ID を許可しないでください
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります

- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.180] EC2 ネットワークインターフェイスでは、送信元/送信先チェックを有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ELB.18] Application and Network Load Balancer リスナーは、安全なプロトコルを使用して転送中のデータを暗号化する必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.4] AWS Glue Spark ジョブは、サポートされているバージョンの で実行する必要があります AWS Glue
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [Lambda.7] Lambda 関数では AWS X-Ray アクティブなトレースを有効にする必要があります
- [MSK.4] MSK クラスターではパブリックアクセスを無効にする必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [MSK.6] MSK クラスターは認証されていないアクセスを無効にする必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [Redshift.18] Redshift クラスターでは、マルチ AZ 配置を有効にする必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります

- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SSM.6] SSM Automation では CloudWatch ログ記録が有効になっている必要があります
- [SSM.7] SSM ドキュメントでは、パブリック共有ブロック設定を有効にする必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

アジアパシフィック (シンガポール)

アジアパシフィック (シンガポール) リージョンでは、以下のコントロールはサポートされていません。

- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください

- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

アジアパシフィック (シドニー)

アジアパシフィック (シドニー) リージョンでは、以下のコントロールはサポートされていません。

- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります

- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

アジアパシフィック (台北)

アジアパシフィック (台北) リージョンでは、以下のコントロールはサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [ACM.3] ACM 証明書にはタグを付ける必要があります
- [Account.1] のセキュリティ連絡先情報は に提供する必要があります AWS アカウント
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.1] API Gateway REST および WebSocket API 実行ログ記録を有効にする必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります
- [APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります
- [APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります
- [APIGateway.5] API Gateway REST API のキャッシュデータは、保管中に暗号化する必要があります
- [APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります

- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります
- [AppConfig.1] AWS AppConfig アプリケーションにはタグを付ける必要があります
- [AppConfig.2] AWS AppConfig 設定プロファイルにはタグを付ける必要があります
- [AppConfig.3] AWS AppConfig 環境にはタグを付ける必要があります
- [AppConfig.4] AWS AppConfig 拡張機能の関連付けにはタグを付ける必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.2] AWS AppSync フィールドレベルのログ記録を有効にする必要があります
- [AppSync.4] AWS AppSync GraphQL APIsにはタグを付ける必要があります
- [AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [Athena.2] Athena データカタログにはタグを付ける必要があります
- [Athena.3] Athena ワークグループにはタグを付ける必要があります
- [Athena.4] Athena ワークグループではログ記録が有効になっている必要があります
- [AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要がある
- [AutoScaling.2] Amazon EC2 Auto Scaling グループは、複数のアベイラビリティーゾーンをカバーする必要があります
- [AutoScaling.3] Auto Scaling グループ起動設定は、EC2 インスタンスを、インスタンスメタデータサービスバージョン 2 (IMDSv2) を必要とするように設定する必要があります
- [AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります
- [AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります
- [AutoScaling.10] EC2 Auto Scaling グループにタグを付ける必要があります
- [Autoscaling.5] Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません

- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.2] AWS Backup 復旧ポイントにはタグを付ける必要があります
- [Backup.3] AWS Backup ボールトにはタグを付ける必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [Backup.5] AWS Backup バックアッププランにはタグを付ける必要があります
- 〔バッチ.1] バッチジョブキューにはタグを付ける必要があります
- [Batch.2] バッチスケジューリングポリシーにはタグを付ける必要があります
- [Batch.3] バッチコンピューティング環境にはタグを付ける必要があります
- [Batch.4] マネージドバッチコンピューティング環境のコンピューティングリソースプロパティにはタグを付ける必要があります
- [CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります

- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットが一般公開されていないことを確認します
- [CloudTrail.7] CloudTrail S3 バケットで、S3 バケットアクセスログ記録が有効であることを確認します
- [CloudTrail.9] CloudTrail 証跡にはタグを付ける必要があります
- [CloudTrail.10] CloudTrail Lake イベントデータストアはカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [CloudWatch.17] CloudWatch アラームアクションをアクティブにする必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeBuild.1] CodeBuild Bitbucket ソースリポジトリの URL には機密認証情報を含めないでください
- [CodeBuild.2] CodeBuild プロジェクト環境変数にクリアテキストの認証情報を含めることはできません
- [CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- [CodeBuild.4] CodeBuild AWS Configプロジェクト環境にはログ記録設定が必要です
- [CodeBuild.7] CodeBuild レポートグループのエクスポートは保管時に暗号化する必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります
- [Cognito.2] Cognito ID プールは認証されていない ID を許可しないでください
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DataSync.1] DataSync タスクではログ記録が有効になっている必要があります
- [DataSync.2] DataSync タスクにはタグを付ける必要があります

- [Detective.1] 検出動作グラフにはタグを付ける必要があります
- [DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにはタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります
- [DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DocumentDB.6] Amazon DocumentDB クラスターは転送中に暗号化する必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.5] DynamoDB テーブルにはタグを付ける必要があります
- [DynamoDB.6] DynamoDB テーブルで、削除保護が有効になっている必要があります

- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.10] Amazon EC2 サービス用に作成された VPC エンドポイントを使用するようにAmazon EC2 を設定することをお勧めします
- [EC2.19] セキュリティグループは、リスクの高いポートへの無制限アクセスを許可してはいけません
- [EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.33] EC2 Transit Gateway アタッチメントにはタグを付ける必要があります
- [EC2.34] EC2 Transit Gateway ルートテーブルにはタグを付ける必要があります
- [EC2.35] EC2 ネットワークインターフェイスにはタグを付ける必要があります
- [EC2.36] EC2 カスタマーゲートウェイにはタグを付ける必要があります
- [EC2.37] EC2 Elastic IP アドレスにはタグを付ける必要があります
- [EC2.38] EC2 インスタンスにはタグを付ける必要があります
- [EC2.39] EC2 インターネットゲートウェイにはタグを付ける必要があります
- [EC2.40] EC2 NAT ゲートウェイにはタグを付ける必要があります
- [EC2.41] EC2 ネットワーク ACL にはタグを付ける必要があります
- [EC2.42] EC2 ルートテーブルにはタグを付ける必要があります
- [EC2.43] EC2 セキュリティグループにはタグを付ける必要があります
- [EC2.44] EC2 サブネットにはタグを付ける必要があります
- [EC2.45] EC2 ボリュームにはタグを付ける必要があります
- [EC2.46] Amazon VPC にはタグを付ける必要があります
- [EC2.47] Amazon VPC エンドポイントサービスはタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります

- [EC2.49] Amazon VPC ピアリング接続にはタグを付ける必要があります
- [EC2.50] EC2 VPN ゲートウェイにはタグを付ける必要があります
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.52] EC2 Transit Gateway にはタグを付ける必要があります
- [EC2.53] EC2 セキュリティグループが 0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可することがないようにする必要があります
- [EC2.54] EC2 セキュリティグループは ::/0 からリモートサーバー管理ポートへの入力を許可しない必要があります
- [EC2.55] VPCs は ECR API のインターフェイスエンドポイントで設定する必要があります
- [EC2.56] VPCsは Docker Registry のインターフェイスエンドポイントで設定する必要があります
- [EC2.57] VPCsは Systems Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.170] EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.171] EC2 VPN 接続では、ログ記録が有効になっている必要があります
- [EC2.172] EC2 VPC ブロックパブリックアクセス設定はインターネットゲートウェイトラフィックをブロックする必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.174] EC2 DHCP オプションセットにはタグを付ける必要があります
- [EC2.175] EC2 起動テンプレートにはタグを付ける必要があります
- [EC2.176] EC2 プレフィックスリストにはタグを付ける必要があります
- [EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります
- [EC2.178] EC2 トラフィックミラーフィルターにはタグを付ける必要があります
- [EC2.179] EC2 トラフィックミラーターゲットにはタグを付ける必要があります
- [EC2.180] EC2 ネットワークインターフェイスでは、送信元/送信先チェックを有効にする必要があります

- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECR.5] ECR リポジトリはカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。
- [ECS.2] ECS サービスには、パブリック IP アドレスを自動で割り当てないでください
- [ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください
- [ECS.4] ECS コンテナは、非特権として実行する必要があります
- [ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。
- [ECS.8] シークレットは、コンテナ環境の変数として渡さないでください
- [ECS.9] ECS タスク定義にはログ設定が必要です。
- [ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。
- [ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります
- [ECS.13] ECS サービスにはタグを付ける必要があります
- [ECS.14] ECS クラスターにはタグを付ける必要があります
- [ECS.15] ECS タスク定義にはタグを付ける必要があります
- [ECS.16] ECS タスクセットはパブリック IP アドレスを自動的に割り当てないでください。
- [ECS.17] ECS タスク定義はホストネットワークモードを使用しないでください
- [EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります
- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EFS .5] EFS アクセスポイントにはタグを付ける必要があります

- [EFS.6] EFS マウントターゲットは、起動時にパブリック IP アドレスを割り当てるサブネットに関連付けるべきではありません
- [EFS .7] EFS ファイルシステムでは、自動バックアップが有効になっている必要があります
- [EFS .8] EFS ファイルシステムは保管中に暗号化する必要があります
- [EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [EKS.6] EKS クラスターにはタグを付ける必要があります
- [EKS.7] EKS ID プロバイダーの設定にはタグを付ける必要があります
- [EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.3] Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります
- [ELB.7] Classic Load Balancers は、Connection Draining を有効にする必要があります
- [ELB.8] SSL リスナーを使用する Classic Load Balancer は、強力な uration AWS Configを持つ事前定義されたセキュリティポリシーを使用する必要があります
- [ELB.10] Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります
- [ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- [ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります
- [ELB.18] Application and Network Load Balancer リスナーは、安全なプロトコルを使用して転送中のデータを暗号化する必要があります

- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElastiCache.2] ElastiCache クラスターでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [ElastiCache.3] ElastiCache (Redis OSS) レプリケーショングループでは、自動フェイルオーバーを有効にする必要があります
- [ElastiCache.4] ElastiCache レプリケーショングループは保管中に暗号化する必要があります
- [ElastiCache.5] ElastiCache レプリケーショングループは転送時に暗号化する必要があります
- [ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります
- [ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください
- [ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。
- [ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります
- [ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります
- [EMR.3] Amazon EMR セキュリティ設定は保管時に暗号化する必要があります
- [EMR.4] Amazon EMR セキュリティ設定は転送中に暗号化する必要があります
- [ES.1] Elasticsearch ドメインは、保管中の暗号化を有効にする必要があります
- [ES.2] Elasticsearch ドメインがパブリックにアクセスできないようにする必要があります
- [ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります
- [ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります
- [ES.5] Elasticsearch ドメインで監査ログ記録が有効になっている必要があります
- [ES.6] Elasticsearch ドメインには少なくとも 3 つのデータノードが必要です
- [ES.7] Elasticsearch ドメインは、少なくとも 3 つの専用マスターノードを設定する必要があります。
- [ES.8] Elasticsearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります

- [ES.9] Elasticsearch ドメインにはタグを付ける必要があります
- [EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります
- [EventBridge.3] Amazon EventBridge カスタムイベントバスにリソースポリシーがアタッチされている必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムでは、タグをバックアップにコピーするように設定する必要があります
- [FSx.3] FSx for OpenZFS ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [FSx.4] FSx for NetApp ONTAP ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [FSx.5] FSx for Windows File Server ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.1] AWS Glue ジョブにはタグを付ける必要があります
- [Glue.3] AWS Glue 機械学習変換は保管時に暗号化する必要があります
- [Glue.4] AWS Glue Spark ジョブは、サポートされているバージョンの AWS Glue で実行する必要があります
- [GuardDuty.1] GuardDuty を有効にする必要があります
- [GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- [GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- [GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [GuardDuty.5] GuardDuty EKS 監査ログモニタリングを有効にする必要があります
- [GuardDuty.6] GuardDuty Lambda Protection を有効にする必要があります
- [GuardDuty.7] GuardDuty EKS ランタイムモニタリングを有効にする必要があります
- [GuardDuty.8] GuardDuty Malware Protection for EC2 を有効にする必要があります

- [GuardDuty.9] GuardDuty RDS Protection を有効にする必要があります
- [GuardDuty.10] GuardDuty S3 Protection を有効にする必要があります
- [GuardDuty.11] GuardDuty Runtime Monitoring を有効にする必要があります
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring を有効にする必要があります
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring を有効にする必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.10] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します
- [IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します
- [IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します
- [IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します
- [IAM.15] IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認します
- [IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています
- [IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します
- [IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません

- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.23] IAM Access Analyzer アナライザーにはタグを付ける必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [IAM.28] IAM Access Analyzer 外部アクセスアナライザーを有効にする必要があります
- [Inspector.1] Amazon Inspector EC2 スキャンを有効にする必要があります
- [Inspector.2] Amazon Inspector ECR スキャンを有効にする必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [Inspector.4] Amazon Inspector Lambda 標準スキャンを有効にする必要があります
- [IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります

- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [Kinesis.2] Kinesis ストリームにはタグを付ける必要があります
- [Kinesis.3] Kinesis ストリームには適切なデータ保持期間が必要です
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [KMS.3] AWS KMS keys を意図せずに削除しないでください
- [KMS.5] KMS キーはパブリックにアクセスしないでください
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Lambda.6] Lambda 関数にはタグを付ける必要があります
- [Lambda.7] Lambda 関数では AWS X-Ray アクティブなトレースを有効にする必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 機密データ自動検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります
- [MQ.3] Amazon MQ ブローカーでは、自動マイナーバージョンアップグレードが有効になっている必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります

- [MSK.4] MSK クラスターではパブリックアクセスを無効にする必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [MSK.6] MSK クラスターは認証されていないアクセスを無効にする必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.1] Network Firewall ファイアウォールを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.2] Network Firewall ログ記録を有効にする必要があります
- [Network Firewall.3] Network Firewall ポリシーには、1 つ以上のルールグループが関連付けられている必要があります
- [NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、完全なパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、断片化されたパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.6] ステートレス Network Firewall のルールグループを空にしないでください
- [NetworkFirewall.7] Network Firewall ファイアウォールにはタグを付ける必要があります
- [NetworkFirewall.8] Network Firewall ファイアウォールポリシーにはタグを付ける必要があります
- [NetworkFirewall.9] Network Firewall は削除保護を有効にする必要があります
- [NetworkFirewall.10] Network Firewall ファイアウォールでは、サブネット変更保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります

- [Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインはにはタグを付ける必要があります
- [Opensearch.10] OpenSearch ドメインには、最新のソフトウェアアップデートがインストールされている必要があります
- [Opensearch.11] OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です
- [PCA.1] AWS Private CA ルート認証機関を無効にする必要があります
- [PCA.2] AWS プライベート CA 認証機関にはタグを付ける必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.16] Aurora DB クラスターは、タグを DB スナップショットにコピーするように設定する必要があります
- [RDS.17] RDS DB インスタンスは、タグをスナップショットにコピーするように設定する必要があります
- [RDS.18] RDS インスタンスは VPC 内にデプロイする必要があります
- [RDS.19] 重大なクラスターイベントについて、既存の RDS イベント通知サブスクリプションを設定する必要があります
- [RDS.20] 重大なデータベースインスタンスイベントに対して、既存の RDS イベント通知サブスクリプションを設定する必要があります
- [RDS.21] 重大なデータベースパラメータグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります
- [RDS.22] 重大なデータベースセキュリティグループイベントに対して RDS イベント通知サブスクリプションを設定する必要があります
- [RDS.23] RDS インスタンスはデータベースエンジンのデフォルトポートを使用しないようにする必要があります

- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [RDS.28] RDS DB クラスターにはタグを付ける必要があります
- [RDS.29] RDS DB クラスタースナップショットにはタグを付ける必要があります
- [RDS.30] RDS DB インスタンスにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RDS.32] RDS DB スナップショットにはタグを付ける必要があります
- [RDS.33] RDS DB サブネットグループにはタグを付ける必要があります
- [RDS.34] Aurora MySQL DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.36] RDS for PostgreSQL DB は CloudWatch Logs にログを発行する必要があります
- [RDS.37] Aurora PostgreSQL DB クラスターでは、ログを CloudWatch Logs に発行する必要があります
- [RDS.38] RDS for PostgreSQL DB インスタンスは転送中に暗号化する必要があります
- [RDS.39] RDS for MySQL DB インスタンスは転送中に暗号化する必要があります
- [RDS.40] RDS for SQL Server DB インスタンスは CloudWatch Logs にログを発行する必要があります
- [RDS.41] RDS for SQL Server DB インスタンスは転送中に暗号化する必要があります
- [RDS.42] RDS for MariaDB DB インスタンスは CloudWatch Logs にログを発行する必要があります
- [RDS.44] RDS for MariaDB DB インスタンスは転送中に暗号化する必要があります
- [RDS.45] Aurora MySQL DB クラスターでは、監査ログ記録を有効にする必要があります
- [PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります
- [Redshift.2] Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります
- [Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります

- [Redshift.4] Amazon Redshift クラスターでは、監査ログ記録が有効になっている必要があります
- [Redshift.6] Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります
- [Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります
- [Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください
- [Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.11] Redshift クラスターにはタグを付ける必要があります
- [Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります
- [Redshift.13] Redshift クラスタースナップショットにはタグを付ける必要があります
- [Redshift.14] Redshift クラスターサブネットグループにはタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの入力を許可する必要があります
- [Redshift.16] Redshift クラスターサブネットグループには、複数のアベイラビリティーゾーンからのサブネットが必要です
- [Redshift.17] Redshift クラスターパラメータグループにはタグを付ける必要があります
- [Redshift.18] Redshift クラスターでは、マルチ AZ 配置を有効にする必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [RedshiftServerless.3] Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります
- [RedshiftServerless.4] Redshift Serverless 名前空間はカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 名前空間では、デフォルトの管理者ユーザー名を使用しないでください
- [RedshiftServerless.6] Redshift Serverless 名前空間は CloudWatch Logs にログをエクスポートする必要があります
- [RedshiftServerless.7] Redshift Serverless 名前空間はデフォルトのデータベース名を使用しないでください

- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.7] S3 汎用バケットでクロスリージョンレプリケーションを使用する必要があります
- [S3.10] バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です
- [S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります
- [S3.12] ACL は、S3 汎用バケットへのユーザーアクセスの管理に使用しないでください。
- [S3.13] S3 汎用バケットにはライフサイクル設定が必要です
- [S3.17] S3 汎用バケットは保管時に で暗号化する必要があります AWS KMS keys
- [S3.19] S3 アクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります
- [S3.22] S3 汎用バケットはオブジェクトレベルの書き込みイベントをログに記録する必要があります
- [S3.23] S3 汎用バケットはオブジェクトレベルの読み取りイベントをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります
- [SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- [SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません
- [SageMaker.4] SageMaker エンドポイントの本番稼働バリアントの初期インスタンス数は 1 より大きい必要があります
- [SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります
- [SageMaker.6] SageMaker アプリのイメージ設定にはタグを付ける必要があります
- [SageMaker.7] SageMaker イメージにはタグを付ける必要があります
- [SageMaker.8] SageMaker ノートブックインスタンスは、サポートされているプラットフォームで実行する必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります

- [SecretsManager.1] Secrets Manager のシークレットは、自動ローテーションを有効にする必要があります
- [SecretsManager.2] 自動ローテーションを設定した Secrets Manager のシークレットは正常にローテーションする必要があります
- [SecretsManager.3] 未使用の Secrets Manager のシークレットを削除します
- [SecretsManager.4] Secrets Manager のシークレットは、指定された日数以内にローテーションする必要があります
- [SecretsManager.5] Secrets Manager のシークレットにはタグを付ける必要があります
- [ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SNS.3] SNS トピックにはタグを付ける必要があります
- [SNS.4] SNS トピックアクセスポリシーはパブリックアクセスを許可しないでください
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください
- [SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [SSM.4] SSM ドキュメントはパブリックにしないでください
- [SSM.5] SSM ドキュメントにはタグを付ける必要があります
- [SSM.6] SSM Automation では CloudWatch ログ記録が有効になっている必要があります
- [SSM.7] SSM ドキュメントでは、パブリック共有ブロック設定を有効にする必要があります
- [StepFunctions.1] Step Functions ステートマシンではログ記録がオンになっている必要があります
- [StepFunctions.2] Step Functions アクティビティにはタグを付ける必要があります
- [Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [Transfer.3] Transfer Family コネクタではログ記録が有効になっている必要があります
- [Transfer.4] Transfer Family 契約にはタグを付ける必要があります
- [Transfer.5] Transfer Family 証明書にはタグを付ける必要があります

- [Transfer.6] Transfer Family コネクタにはタグを付ける必要があります
- [Transfer.7] Transfer Family プロファイルにはタグを付ける必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.2] AWS WAF Classic リージョンルールには少なくとも 1 つの条件が必要です
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です
- [WAF.4] AWS WAF Classic Regional Web ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります
- [WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

アジアパシフィック (タイ)

アジアパシフィック (タイ) リージョンでは、以下のコントロールはサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [Account.1] のセキュリティ連絡先情報は に提供する必要があります AWS アカウント
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります

- [AppConfig.1] AWS AppConfig アプリケーションにはタグを付ける必要があります
- [AppConfig.2] AWS AppConfig 設定プロファイルにはタグを付ける必要があります
- [AppConfig.3] AWS AppConfig 環境にはタグを付ける必要があります
- [AppConfig.4] AWS AppConfig 拡張機能の関連付けにはタグを付ける必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.2] AWS AppSync フィールドレベルのログ記録を有効にする必要があります
- [AppSync.4] AWS AppSync GraphQL APIsにはタグを付ける必要があります
- [AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [Athena.2] Athena データカタログにはタグを付ける必要があります
- [Athena.3] Athena ワークグループにはタグを付ける必要があります
- [Athena.4] Athena ワークグループではログ記録が有効になっている必要があります
- [AutoScaling.2] Amazon EC2 Auto Scaling グループは、複数のアベイラビリティーゾーンをカバーする必要があります
- [AutoScaling.3] Auto Scaling グループ起動設定は、EC2 インスタンスを、インスタンスメタデータサービスバージョン 2 (IMDSv2) を必要とするように設定する必要があります
- [AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります
- [AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.2] AWS Backup 復旧ポイントにはタグを付ける必要があります
- [Backup.3] AWS Backup ボールトにはタグを付ける必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [Backup.5] AWS Backup バックアッププランにはタグを付ける必要があります
- 〔バッチ.1] バッチジョブキューにはタグを付ける必要があります
- [Batch.2] バッチスケジューリングポリシーにはタグを付ける必要があります
- [Batch.3] バッチコンピューティング環境にはタグを付ける必要があります

- [Batch.4] マネージドバッチコンピューティング環境のコンピューティングリソースプロパティにはタグを付ける必要があります
- [CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットが一般公開されていないことを確認します
- [CloudTrail.7] CloudTrail S3 バケットで、S3 バケットアクセスログ記録が有効であることを確認します
- [CloudTrail.10] CloudTrail Lake イベントデータストアはカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [CloudWatch.17] CloudWatch アラームアクションをアクティブにする必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります

- [CodeBuild.1] CodeBuild Bitbucket ソースリポジトリの URL には機密認証情報を含めないでください
- [CodeBuild.2] CodeBuild プロジェクト環境変数にクリアテキストの認証情報を含めることはできません
- [CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- [CodeBuild.4] CodeBuild AWS Configプロジェクト環境にはログ記録設定が必要です
- [CodeBuild.7] CodeBuild レポートグループのエクスポートは保管時に暗号化する必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります
- [Cognito.2] Cognito ID プールは認証されていない ID を許可しないでください
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DataSync.1] DataSync タスクではログ記録が有効になっている必要があります
- [DataSync.2] DataSync タスクにはタグを付ける必要があります
- [Detective.1] 検出動作グラフにはタグを付ける必要があります
- [DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにはタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。

- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります
- [DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DocumentDB.6] Amazon DocumentDB クラスターは転送中に暗号化する必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.6] DynamoDB テーブルで、削除保護が有効になっている必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.33] EC2 Transit Gateway アタッチメントにはタグを付ける必要があります
- [EC2.34] EC2 Transit Gateway ルートテーブルにはタグを付ける必要があります

- [EC2.40] EC2 NAT ゲートウェイにはタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.52] EC2 Transit Gateway にはタグを付ける必要があります
- [EC2.53] EC2 セキュリティグループが 0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可することがないようにする必要があります
- [EC2.54] EC2 セキュリティグループは ::/0 からリモートサーバー管理ポートへの入力を許可しない必要があります
- [EC2.55] VPCs は ECR API のインターフェイスエンドポイントで設定する必要があります
- [EC2.56] VPCsは Docker Registry のインターフェイスエンドポイントで設定する必要があります
- [EC2.57] VPCsは Systems Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.170] EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.171] EC2 VPN 接続では、ログ記録が有効になっている必要があります
- [EC2.172] EC2 VPC ブロックパブリックアクセス設定はインターネットゲートウェイトラフィックをブロックする必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.174] EC2 DHCP オプションセットにはタグを付ける必要があります
- [EC2.175] EC2 起動テンプレートにはタグを付ける必要があります
- [EC2.176] EC2 プレフィックスリストにはタグを付ける必要があります
- [EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります
- [EC2.178] EC2 トラフィックミラーフィルターにはタグを付ける必要があります
- [EC2.179] EC2 トラフィックミラーターゲットにはタグを付ける必要があります
- [EC2.180] EC2 ネットワークインターフェイスでは、送信元/送信先チェックを有効にする必要があります

- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECR.5] ECR リポジトリはカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください
- [ECS.4] ECS コンテナは、非特権として実行する必要があります
- [ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。
- [ECS.8] シークレットは、コンテナ環境の変数として渡さないでください
- [ECS.9] ECS タスク定義にはログ設定が必要です。
- [ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。
- [ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります
- [ECS.16] ECS タスクセットはパブリック IP アドレスを自動的に割り当てないでください。
- [ECS.17] ECS タスク定義はホストネットワークモードを使用しないでください
- [EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります
- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EFS .5] EFS アクセスポイントにはタグを付ける必要があります
- [EFS.6] EFS マウントターゲットは、起動時にパブリック IP アドレスを割り当てるサブネットに関連付けるべきではありません
- [EFS .7] EFS ファイルシステムでは、自動バックアップが有効になっている必要があります
- [EFS .8] EFS ファイルシステムは保管中に暗号化する必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。

- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [EKS.6] EKS クラスターにはタグを付ける必要があります
- [EKS.7] EKS ID プロバイダーの設定にはタグを付ける必要があります
- [EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります
- [ELB.10] Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります
- [ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります
- [ELB.18] Application and Network Load Balancer リスナーは、安全なプロトコルを使用して転送中のデータを暗号化する必要があります
- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElastiCache.2] ElastiCache クラスターでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [ElastiCache.3] ElastiCache (Redis OSS) レプリケーショングループでは、自動フェイルオーバーを有効にする必要があります
- [ElastiCache.4] ElastiCache レプリケーショングループは保管中に暗号化する必要があります
- [ElastiCache.5] ElastiCache レプリケーショングループは転送時に暗号化する必要があります
- [ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります
- [ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください
- [ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。
- [ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります
- [ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります

- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります
- [EMR.3] Amazon EMR セキュリティ設定は保管時に暗号化する必要があります
- [EMR.4] Amazon EMR セキュリティ設定は転送中に暗号化する必要があります
- [ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります
- [ES.9] Elasticsearch ドメインにはタグを付ける必要があります
- [EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります
- [EventBridge.3] Amazon EventBridge カスタムイベントバスにリソースポリシーがアタッチされている必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムでは、タグをバックアップにコピーするように設定する必要があります
- [FSx.3] FSx for OpenZFS ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [FSx.4] FSx for NetApp ONTAP ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [FSx.5] FSx for Windows File Server ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.1] AWS Glue ジョブにはタグを付ける必要があります
- [Glue.3] AWS Glue 機械学習変換は保管時に暗号化する必要があります
- [Glue.4] AWS Glue Spark ジョブは、サポートされているバージョンの AWS Glue で実行する必要があります
- [GuardDuty.1] GuardDuty を有効にする必要があります

- [GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- [GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- [GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [GuardDuty.5] GuardDuty EKS 監査ログモニタリングを有効にする必要があります
- [GuardDuty.6] GuardDuty Lambda Protection を有効にする必要があります
- [GuardDuty.7] GuardDuty EKS ランタイムモニタリングを有効にする必要があります
- [GuardDuty.8] GuardDuty Malware Protection for EC2 を有効にする必要があります
- [GuardDuty.9] GuardDuty RDS Protection を有効にする必要があります
- [GuardDuty.10] GuardDuty S3 Protection を有効にする必要があります
- [GuardDuty.11] GuardDuty Runtime Monitoring を有効にする必要があります
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring を有効にする必要があります
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring を有効にする必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.10] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します
- [IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します
- [IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します
- [IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します
- [IAM.15] IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認します

- [IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています
- [IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します
- [IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.23] IAM Access Analyzer アナライザーにはタグを付ける必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [IAM.28] IAM Access Analyzer 外部アクセスアナライザーを有効にする必要があります
- [Inspector.1] Amazon Inspector EC2 スキャンを有効にする必要があります
- [Inspector.2] Amazon Inspector ECR スキャンを有効にする必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [Inspector.4] Amazon Inspector Lambda 標準スキャンを有効にする必要があります
- [IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります

- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [Kinesis.2] Kinesis ストリームにはタグを付ける必要があります
- [Kinesis.3] Kinesis ストリームには適切なデータ保持期間が必要です
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [KMS.5] KMS キーはパブリックにアクセスしないでください
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Lambda.7] Lambda 関数では AWS X-Ray アクティブなトレースを有効にする必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 機密データ自動検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります
- [MQ.3] Amazon MQ ブローカーでは、自動マイナーバージョンアップグレードが有効になっている必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります

- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.4] MSK クラスターではパブリックアクセスを無効にする必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [MSK.6] MSK クラスターは認証されていないアクセスを無効にする必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.1] Network Firewall ファイアウォールを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.2] Network Firewall ログ記録を有効にする必要があります
- [Network Firewall.3] Network Firewall ポリシーには、1 つ以上のルールグループが関連付けられている必要があります
- [NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、完全なパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、断片化されたパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.6] ステートレス Network Firewall のルールグループを空にしないでください

- [NetworkFirewall.9] Network Firewall は削除保護を有効にする必要があります
- [NetworkFirewall.10] Network Firewall ファイアウォールでは、サブネット変更保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインはにはタグを付ける必要があります
- [Opensearch.10] OpenSearch ドメインには、最新のソフトウェアアップデートがインストールされている必要があります
- [Opensearch.11] OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です
- [PCA.1] AWS Private CA ルート認証機関を無効にする必要があります
- [PCA.2] AWS プライベート CA 認証機関にはタグを付ける必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.18] RDS インスタンスは VPC 内にデプロイする必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RDS.34] Aurora MySQL DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります

- [RDS.36] RDS for PostgreSQL DB は CloudWatch Logs にログを発行する必要があります
- [RDS.37] Aurora PostgreSQL DB クラスターでは、ログを CloudWatch Logs に発行する必要があります
- [RDS.38] RDS for PostgreSQL DB インスタンスは転送中に暗号化する必要があります
- [RDS.39] RDS for MySQL DB インスタンスは転送中に暗号化する必要があります
- [RDS.40] RDS for SQL Server DB インスタンスは CloudWatch Logs にログを発行する必要があります
- [RDS.41] RDS for SQL Server DB インスタンスは転送中に暗号化する必要があります
- [RDS.42] RDS for MariaDB DB インスタンスは CloudWatch Logs にログを発行する必要があります
- [RDS.44] RDS for MariaDB DB インスタンスは転送中に暗号化する必要があります
- [RDS.45] Aurora MySQL DB クラスターでは、監査ログ記録を有効にする必要があります
- [PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります
- [Redshift.2] Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります
- [Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります
- [Redshift.6] Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります
- [Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります
- [Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください
- [Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.11] Redshift クラスターにはタグを付ける必要があります
- [Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります
- [Redshift.13] Redshift クラスタースナップショットにはタグを付ける必要があります
- [Redshift.14] Redshift クラスターサブネットグループにはタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの入力を許可する必要があります
- [Redshift.16] Redshift クラスターサブネットグループには、複数のアベイラビリティーゾーンからのサブネットが必要です

- [Redshift.17] Redshift クラスターパラメータグループにはタグを付ける必要があります
- [Redshift.18] Redshift クラスターでは、マルチ AZ 配置を有効にする必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [RedshiftServerless.3] Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります
- [RedshiftServerless.4] Redshift Serverless 名前空間はカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 名前空間では、デフォルトの管理者ユーザー名を使用しないでください
- [RedshiftServerless.6] Redshift Serverless 名前空間は CloudWatch Logs にログをエクスポートする必要があります
- [RedshiftServerless.7] Redshift Serverless 名前空間はデフォルトのデータベース名を使用しないでください
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.7] S3 汎用バケットでクロスリージョンレプリケーションを使用する必要があります
- [S3.10] バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です
- [S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります
- [S3.12] ACL は、S3 汎用バケットへのユーザーアクセスの管理に使用しないでください。
- [S3.13] S3 汎用バケットにはライフサイクル設定が必要です
- [S3.19] S3 アクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります
- [S3.22] S3 汎用バケットはオブジェクトレベルの書き込みイベントをログに記録する必要があります
- [S3.23] S3 汎用バケットはオブジェクトレベルの読み取りイベントをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です

- [SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります
- [SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- [SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません
- [SageMaker.4] SageMaker エンドポイントの本番稼働バリアントの初期インスタンス数は 1 より大きい必要があります
- [SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります
- [SageMaker.6] SageMaker アプリのイメージ設定にはタグを付ける必要があります
- [SageMaker.7] SageMaker イメージにはタグを付ける必要があります
- [SageMaker.8] SageMaker ノートブックインスタンスは、サポートされているプラットフォームで実行する必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- [ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SNS.4] SNS トピックアクセスポリシーはパブリックアクセスを許可しないでください
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [SSM.4] SSM ドキュメントはパブリックにしないでください
- [SSM.5] SSM ドキュメントにはタグを付ける必要があります
- [SSM.6] SSM Automation では CloudWatch ログ記録が有効になっている必要があります
- [SSM.7] SSM ドキュメントでは、パブリック共有ブロック設定を有効にする必要があります
- [StepFunctions.1] Step Functions ステートマシンではログ記録がオンになっている必要があります
- [StepFunctions.2] Step Functions アクティビティにはタグを付ける必要があります
- [Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [Transfer.3] Transfer Family コネクタではログ記録が有効になっている必要があります

- [Transfer.4] Transfer Family 契約にはタグを付ける必要があります
- [Transfer.5] Transfer Family 証明書にはタグを付ける必要があります
- [Transfer.6] Transfer Family コネクタにはタグを付ける必要があります
- [Transfer.7] Transfer Family プロファイルにはタグを付ける必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.2] AWS WAF Classic リージョンルールには少なくとも 1 つの条件が必要です
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です
- [WAF.4] AWS WAF Classic Regional Web ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります
- [WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

アジアパシフィック (東京)

アジアパシフィック (東京) リージョンでは、以下のコントロールはサポートされていません。

- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります

- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です

- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

カナダ (中部)

以下のコントロールは、カナダ (中部) リージョンではサポートされていません。

- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります

- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Kinesis.3] Kinesis ストリームには適切なデータ保持期間が必要です
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります

- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

カナダ西部 (カルガリー)

以下のコントロールは、カナダ西部 (カルガリー) リージョンではサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [Account.1] のセキュリティ連絡先情報は に提供する必要があります AWS アカウント
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります
- [AppConfig.1] AWS AppConfig アプリケーションにはタグを付ける必要があります
- [AppConfig.2] AWS AppConfig 設定プロファイルにはタグを付ける必要があります
- [AppConfig.3] AWS AppConfig 環境にはタグを付ける必要があります
- [AppConfig.4] AWS AppConfig 拡張機能の関連付けにはタグを付ける必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります

- [AppSync.2] AWS AppSync フィールドレベルのログ記録を有効にする必要があります
- [AppSync.4] AWS AppSync GraphQL APIsにはタグを付ける必要があります
- [AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [Athena.4] Athena ワークグループではログ記録が有効になっている必要があります
- [AutoScaling.2] Amazon EC2 Auto Scaling グループは、複数のアベイラビリティーゾーンをカバーする必要があります
- [AutoScaling.3] Auto Scaling グループ起動設定は、EC2 インスタンスを、インスタンスメタデータサービスバージョン 2 (IMDSv2) を必要とするように設定する必要があります
- [AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります
- [AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- 〔バッチ.1] バッチジョブキューにはタグを付ける必要があります
- [Batch.3] バッチコンピューティング環境にはタグを付ける必要があります
- [Batch.4] マネージドバッチコンピューティング環境のコンピューティングリソースプロパティにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります

- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットが一般公開されていないことを確認します
- [CloudTrail.7] CloudTrail S3 バケットで、S3 バケットアクセスログ記録が有効であることを確認します
- [CloudTrail.10] CloudTrail Lake イベントデータストアはカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [CloudWatch.17] CloudWatch アラームアクションをアクティブにする必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeBuild.1] CodeBuild Bitbucket ソースリポジトリの URL には機密認証情報を含めないでください
- [CodeBuild.2] CodeBuild プロジェクト環境変数にクリアテキストの認証情報を含めることはできません
- [CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- [CodeBuild.4] CodeBuild AWS Configプロジェクト環境にはログ記録設定が必要です
- [CodeBuild.7] CodeBuild レポートグループのエクスポートは保管時に暗号化する必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります
- [Cognito.2] Cognito ID プールは認証されていない ID を許可しないでください
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります

- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DataSync.1] DataSync タスクではログ記録が有効になっている必要があります
- [Detective.1] 検出動作グラフにはタグを付ける必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにはタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります
- [DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DocumentDB.6] Amazon DocumentDB クラスターは転送中に暗号化する必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります

- [DynamoDB.6] DynamoDB テーブルで、削除保護が有効になっている必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.33] EC2 Transit Gateway アタッチメントにはタグを付ける必要があります
- [EC2.34] EC2 Transit Gateway ルートテーブルにはタグを付ける必要があります
- [EC2.40] EC2 NAT ゲートウェイにはタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.53] EC2 セキュリティグループが 0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可することがないようにする必要があります
- [EC2.54] EC2 セキュリティグループは ::/0 からリモートサーバー管理ポートへの入力を許可しない必要があります
- [EC2.55] VPCs は ECR API のインターフェイスエンドポイントで設定する必要があります
- [EC2.56] VPCsは Docker Registry のインターフェイスエンドポイントで設定する必要があります
- [EC2.57] VPCsは Systems Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.170] EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします

- [EC2.171] EC2 VPN 接続では、ログ記録が有効になっている必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.175] EC2 起動テンプレートにはタグを付ける必要があります
- [EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります
- [EC2.179] EC2 トラフィックミラーターゲットにはタグを付ける必要があります
- [EC2.180] EC2 ネットワークインターフェイスでは、送信元/送信先チェックを有効にする必要があります
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECR.5] ECR リポジトリはカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください
- [ECS.4] ECS コンテナは、非特権として実行する必要があります
- [ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。
- [ECS.8] シークレットは、コンテナ環境の変数として渡さないでください
- [ECS.9] ECS タスク定義にはログ設定が必要です。
- [ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。
- [ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります
- [ECS.16] ECS タスクセットはパブリック IP アドレスを自動的に割り当てないでください。
- [ECS.17] ECS タスク定義はホストネットワークモードを使用しないでください
- [EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります

- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EFS.6] EFS マウントターゲットは、起動時にパブリック IP アドレスを割り当てるサブネットに関連付けるべきではありません
- [EFS .7] EFS ファイルシステムでは、自動バックアップが有効になっている必要があります
- [EFS .8] EFS ファイルシステムは保管中に暗号化する必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [EKS.6] EKS クラスターにはタグを付ける必要があります
- [EKS.7] EKS ID プロバイダーの設定にはタグを付ける必要があります
- [EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.10] Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります
- [ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります
- [ELB.18] Application and Network Load Balancer リスナーは、安全なプロトコルを使用して転送中のデータを暗号化する必要があります
- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElastiCache.2] ElastiCache クラスターでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [ElastiCache.3] ElastiCache (Redis OSS) レプリケーショングループでは、自動フェイルオーバーを有効にする必要があります
- [ElastiCache.4] ElastiCache レプリケーショングループは保管中に暗号化する必要があります

- [ElastiCache.5] ElastiCache レプリケーショングループは転送時に暗号化する必要があります
- [ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります
- [ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください
- [ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。
- [ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります
- [ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります
- [ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります
- [EventBridge.3] Amazon EventBridge カスタムイベントバスにリソースポリシーがアタッチされている必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムでは、タグをバックアップにコピーするように設定する必要があります
- [FSx.3] FSx for OpenZFS ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [FSx.4] FSx for NetApp ONTAP ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [FSx.5] FSx for Windows File Server ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります

- [Glue.3] AWS Glue 機械学習変換は保管時に暗号化する必要があります
- [Glue.4] AWS Glue Spark ジョブは、サポートされているバージョンの AWS Glue で実行する必要があります
- [GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- [GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- [GuardDuty.5] GuardDuty EKS 監査ログモニタリングを有効にする必要があります
- [GuardDuty.6] GuardDuty Lambda Protection を有効にする必要があります
- [GuardDuty.7] GuardDuty EKS ランタイムモニタリングを有効にする必要があります
- [GuardDuty.8] GuardDuty Malware Protection for EC2 を有効にする必要があります
- [GuardDuty.9] GuardDuty RDS Protection を有効にする必要があります
- [GuardDuty.10] GuardDuty S3 Protection を有効にする必要があります
- [GuardDuty.11] GuardDuty Runtime Monitoring を有効にする必要があります
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring を有効にする必要があります
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring を有効にする必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.10] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します
- [IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します
- [IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します
- [IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します

- [IAM.15] IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認します
- [IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています
- [IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します
- [IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [IAM.28] IAM Access Analyzer 外部アクセスアナライザーを有効にする必要があります
- [Inspector.1] Amazon Inspector EC2 スキャンを有効にする必要があります
- [Inspector.2] Amazon Inspector ECR スキャンを有効にする必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [Inspector.4] Amazon Inspector Lambda 標準スキャンを有効にする必要があります
- [IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります

- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [Kinesis.2] Kinesis ストリームにはタグを付ける必要があります
- [Kinesis.3] Kinesis ストリームには適切なデータ保持期間が必要です
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [KMS.5] KMS キーはパブリックにアクセスしないでください
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Lambda.7] Lambda 関数では AWS X-Ray アクティブなトレースを有効にする必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 機密データ自動検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります
- [MQ.3] Amazon MQ ブローカーでは、自動マイナーバージョンアップグレードが有効になっている必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります

- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.4] MSK クラスターではパブリックアクセスを無効にする必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [MSK.6] MSK クラスターは認証されていないアクセスを無効にする必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.1] Network Firewall ファイアウォールを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.2] Network Firewall ログ記録を有効にする必要があります
- [Network Firewall.3] Network Firewall ポリシーには、1 つ以上のルールグループが関連付けられている必要があります
- [NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、完全なパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、断片化されたパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.6] ステートレス Network Firewall のルールグループを空にしないでください

- [NetworkFirewall.9] Network Firewall は削除保護を有効にする必要があります
- [NetworkFirewall.10] Network Firewall ファイアウォールでは、サブネット変更保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインはにはタグを付ける必要があります
- [Opensearch.10] OpenSearch ドメインには、最新のソフトウェアアップデートがインストールされている必要があります
- [Opensearch.11] OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です
- [PCA.1] AWS Private CA ルート認証機関を無効にする必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.18] RDS インスタンスは VPC 内にデプロイする必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RDS.34] Aurora MySQL DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.36] RDS for PostgreSQL DB は CloudWatch Logs にログを発行する必要があります

- [RDS.37] Aurora PostgreSQL DB クラスターでは、ログを CloudWatch Logs に発行する必要があります
- [RDS.38] RDS for PostgreSQL DB インスタンスは転送中に暗号化する必要があります
- [RDS.39] RDS for MySQL DB インスタンスは転送中に暗号化する必要があります
- [RDS.40] RDS for SQL Server DB インスタンスは CloudWatch Logs にログを発行する必要があります
- [RDS.41] RDS for SQL Server DB インスタンスは転送中に暗号化する必要があります
- [RDS.42] RDS for MariaDB DB インスタンスは CloudWatch Logs にログを発行する必要があります
- [RDS.44] RDS for MariaDB DB インスタンスは転送中に暗号化する必要があります
- [RDS.45] Aurora MySQL DB クラスターでは、監査ログ記録を有効にする必要があります
- [Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります
- [Redshift.6] Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります
- [Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください
- [Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの入力を許可する必要があります
- [Redshift.16] Redshift クラスターサブネットグループには、複数のアベイラビリティーゾーンからのサブネットが必要です
- [Redshift.18] Redshift クラスターでは、マルチ AZ 配置を有効にする必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [RedshiftServerless.3] Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります
- [RedshiftServerless.4] Redshift Serverless 名前空間はカスタマーマネージドで暗号化する必要があります AWS KMS keys

- [RedshiftServerless.5] Redshift Serverless 名前空間では、デフォルトの管理者ユーザー名を使用しないでください
- [RedshiftServerless.6] Redshift Serverless 名前空間は CloudWatch Logs にログをエクスポートする必要があります
- [RedshiftServerless.7] Redshift Serverless 名前空間はデフォルトのデータベース名を使用しないでください
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.7] S3 汎用バケットでクロスリージョンレプリケーションを使用する必要があります
- [S3.10] バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です
- [S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります
- [S3.12] ACL は、S3 汎用バケットへのユーザーアクセスの管理に使用しないでください。
- [S3.13] S3 汎用バケットにはライフサイクル設定が必要です
- [S3.19] S3 アクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります
- [S3.22] S3 汎用バケットはオブジェクトレベルの書き込みイベントをログに記録する必要があります
- [S3.23] S3 汎用バケットはオブジェクトレベルの読み取りイベントをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります
- [SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- [SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません
- [SageMaker.4] SageMaker エンドポイントの本番稼働バリアントの初期インスタンス数は 1 より大きい必要があります
- [SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります
- [SageMaker.6] SageMaker アプリのイメージ設定にはタグを付ける必要があります

- [SageMaker.7] SageMaker イメージにはタグを付ける必要があります
- [SageMaker.8] SageMaker ノートブックインスタンスは、サポートされているプラットフォームで実行する必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- [ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SNS.4] SNS トピックアクセスポリシーはパブリックアクセスを許可しないでください
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [SSM.4] SSM ドキュメントはパブリックにしないでください
- [SSM.6] SSM Automation では CloudWatch ログ記録が有効になっている必要があります
- [SSM.7] SSM ドキュメントでは、パブリック共有ブロック設定を有効にする必要があります
- [StepFunctions.1] Step Functions ステートマシンではログ記録がオンになっている必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [Transfer.3] Transfer Family コネクタではログ記録が有効になっている必要があります
- [Transfer.4] Transfer Family 契約にはタグを付ける必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.2] AWS WAF Classic リージョンルールには少なくとも 1 つの条件が必要です
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です
- [WAF.4] AWS WAF Classic Regional Web ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

中国 (北京)

以下のコントロールは、中国 (北京) リージョンではサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります
- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります
- [AppConfig.1] AWS AppConfig アプリケーションにはタグを付ける必要があります
- [AppConfig.2] AWS AppConfig 設定プロファイルにはタグを付ける必要があります
- [AppConfig.3] AWS AppConfig 環境にはタグを付ける必要があります
- [AppConfig.4] AWS AppConfig 拡張機能の関連付けにはタグを付ける必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [AutoScaling.10] EC2 Auto Scaling グループにタグを付ける必要があります
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- 〔バッチ.1] バッチジョブキューにはタグを付ける必要があります

- [Batch.2] バッチスケジューリングポリシーにはタグを付ける必要があります
- [Batch.3] バッチコンピューティング環境にはタグを付ける必要があります
- [Batch.4] マネージドバッチコンピューティング環境のコンピューティングリソースプロパティにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CloudTrail.10] CloudTrail Lake イベントデータストアはカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります

- [Cognito.2] Cognito ID プールは認証されていない ID を許可しないでください
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DataSync.2] DataSync タスクにはタグを付ける必要があります
- [Detective.1] 検出動作グラフにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにはタグを付ける必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります
- [DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.20] AWS Site-to-Site VPN トンネルが稼働している必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.33] EC2 Transit Gateway アタッチメントにはタグを付ける必要があります

- [EC2.34] EC2 Transit Gateway ルートテーブルにはタグを付ける必要があります
- [EC2.35] EC2 ネットワークインターフェイスにはタグを付ける必要があります
- [EC2.36] EC2 カスタマーゲートウェイにはタグを付ける必要があります
- [EC2.42] EC2 ルートテーブルにはタグを付ける必要があります
- [EC2.46] Amazon VPC にはタグを付ける必要があります
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.53] EC2 セキュリティグループが 0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可することがないようにする必要があります
- [EC2.54] EC2 セキュリティグループは ::/0 からリモートサーバー管理ポートへの入力を許可しない必要があります
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.171] EC2 VPN 接続では、ログ記録が有効になっている必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.174] EC2 DHCP オプションセットにはタグを付ける必要があります
- [EC2.175] EC2 起動テンプレートにはタグを付ける必要があります
- [EC2.176] EC2 プレフィックスリストにはタグを付ける必要があります
- [EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります
- [EC2.178] EC2 トラフィックミラーフィルターにはタグを付ける必要があります
- [EC2.179] EC2 トラフィックミラーターゲットにはタグを付ける必要があります
- [EC2.180] EC2 ネットワークインターフェイスでは、送信元/送信先チェックを有効にする必要があります
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS.6] EFS マウントターゲットは、起動時にパブリック IP アドレスを割り当てるサブネットに関連付けるべきではありません

- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [EKS.6] EKS クラスターにはタグを付ける必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- [ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります
- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります
- [EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります
- [EMR.3] Amazon EMR セキュリティ設定は保管時に暗号化する必要があります
- [EMR.4] Amazon EMR セキュリティ設定は転送中に暗号化する必要があります
- [ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムでは、タグをバックアップにコピーするように設定する必要があります
- [FSx.5] FSx for Windows File Server ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- [GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [GuardDuty.5] GuardDuty EKS 監査ログモニタリングを有効にする必要があります
- [GuardDuty.6] GuardDuty Lambda Protection を有効にする必要があります

- [GuardDuty.7] GuardDuty EKS ランタイムモニタリングを有効にする必要があります
- [GuardDuty.8] GuardDuty Malware Protection for EC2 を有効にする必要があります
- [GuardDuty.9] GuardDuty RDS Protection を有効にする必要があります
- [GuardDuty.10] GuardDuty S3 Protection を有効にする必要があります
- [GuardDuty.11] GuardDuty Runtime Monitoring を有効にする必要があります
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring を有効にする必要があります
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.23] IAM Access Analyzer アナライザーにはタグを付ける必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [IAM.28] IAM Access Analyzer 外部アクセスアナライザーを有効にする必要があります
- [Inspector.1] Amazon Inspector EC2 スキャンを有効にする必要があります
- [Inspector.2] Amazon Inspector ECR スキャンを有効にする必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [Inspector.4] Amazon Inspector Lambda 標準スキャンを有効にする必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります

- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 機密データ自動検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.1] Network Firewall ファイアウォールを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.2] Network Firewall ログ記録を有効にする必要があります

- [Network Firewall.3] Network Firewall ポリシーには、1 つ以上のルールグループが関連付けられている必要があります
- [NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、完全なパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、断片化されたパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.6] ステートレス Network Firewall のルールグループを空にしないでください
- [NetworkFirewall.7] Network Firewall ファイアウォールにはタグを付ける必要があります
- [NetworkFirewall.9] Network Firewall は削除保護を有効にする必要があります
- [NetworkFirewall.10] Network Firewall ファイアウォールでは、サブネット変更保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.11] OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です
- [PCA.1] AWS Private CA ルート認証機関を無効にする必要があります
- [PCA.2] AWS プライベート CA 認証機関にはタグを付ける必要があります
- [RDS.7] RDS クラスターでは、削除保護が有効になっている必要があります
- [RDS.12] IAM 認証は RDS クラスター用に設定する必要があります
- [RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります

- [RDS.16] Aurora DB クラスターは、タグを DB スナップショットにコピーするように設定する必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [RDS.28] RDS DB クラスターにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RDS.32] RDS DB スナップショットにはタグを付ける必要があります
- [RDS.34] Aurora MySQL DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.37] Aurora PostgreSQL DB クラスターでは、ログを CloudWatch Logs に発行する必要があります
- [RDS.42] RDS for MariaDB DB インスタンスは CloudWatch Logs にログを発行する必要があります
- [RDS.44] RDS for MariaDB DB インスタンスは転送中に暗号化する必要があります
- [RDS.45] Aurora MySQL DB クラスターでは、監査ログ記録を有効にする必要があります
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの入力を許可する必要があります
- [Redshift.17] Redshift クラスターパラメータグループにはタグを付ける必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [RedshiftServerless.3] Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります

- [S3.22] S3 汎用バケットはオブジェクトレベルの書き込みイベントをログに記録する必要があります
- [S3.23] S3 汎用バケットはオブジェクトレベルの読み取りイベントをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります
- [SageMaker.4] SageMaker エンドポイントの本番稼働バリアントの初期インスタンス数は 1 より大きい必要があります
- [SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります
- [SageMaker.6] SageMaker アプリのイメージ設定にはタグを付ける必要があります
- [SageMaker.7] SageMaker イメージにはタグを付ける必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- [ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SSM.5] SSM ドキュメントにはタグを付ける必要があります
- [SSM.6] SSM Automation では CloudWatch ログ記録が有効になっている必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [Transfer.4] Transfer Family 契約にはタグを付ける必要があります
- [Transfer.5] Transfer Family 証明書にはタグを付ける必要があります
- [Transfer.6] Transfer Family コネクタにはタグを付ける必要があります
- [Transfer.7] Transfer Family プロファイルにはタグを付ける必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

中国 (寧夏)

中国 (寧夏) リージョンでは、以下のコントロールはサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります
- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります
- [AppConfig.1] AWS AppConfig アプリケーションにはタグを付ける必要があります
- [AppConfig.2] AWS AppConfig 設定プロファイルにはタグを付ける必要があります
- [AppConfig.3] AWS AppConfig 環境にはタグを付ける必要があります
- [AppConfig.4] AWS AppConfig 拡張機能の関連付けにはタグを付ける必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [AutoScaling.10] EC2 Auto Scaling グループにタグを付ける必要があります
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- 〔バッチ.1] バッチジョブキューにはタグを付ける必要があります
- [Batch.2] バッチスケジューリングポリシーにはタグを付ける必要があります
- [Batch.3] バッチコンピューティング環境にはタグを付ける必要があります

- [Batch.4] マネージドバッチコンピューティング環境のコンピューティングリソースプロパティにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CloudTrail.10] CloudTrail Lake イベントデータストアはカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります

- [Cognito.2] Cognito ID プールは認証されていない ID を許可しないでください
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DataSync.2] DataSync タスクにはタグを付ける必要があります
- [Detective.1] 検出動作グラフにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにはタグを付ける必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります
- [DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.20] AWS Site-to-Site VPN トンネルが稼働している必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.33] EC2 Transit Gateway アタッチメントにはタグを付ける必要があります
- [EC2.34] EC2 Transit Gateway ルートテーブルにはタグを付ける必要があります
- [EC2.35] EC2 ネットワークインターフェイスにはタグを付ける必要があります
- [EC2.36] EC2 カスタマーゲートウェイにはタグを付ける必要があります
- [EC2.42] EC2 ルートテーブルにはタグを付ける必要があります

- [EC2.46] Amazon VPC にはタグを付ける必要があります
- [EC2.50] EC2 VPN ゲートウェイにはタグを付ける必要があります
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.171] EC2 VPN 接続では、ログ記録が有効になっている必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.174] EC2 DHCP オプションセットにはタグを付ける必要があります
- [EC2.175] EC2 起動テンプレートにはタグを付ける必要があります
- [EC2.176] EC2 プレフィックスリストにはタグを付ける必要があります
- [EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります
- [EC2.178] EC2 トラフィックミラーフィルターにはタグを付ける必要があります
- [EC2.179] EC2 トラフィックミラーターゲットにはタグを付ける必要があります
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります
- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EFS.6] EFS マウントターゲットは、起動時にパブリック IP アドレスを割り当てるサブネットに関連付けるべきではありません
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [EKS.6] EKS クラスターにはタグを付ける必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- [ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります

- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります
- [EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります
- [EMR.3] Amazon EMR セキュリティ設定は保管時に暗号化する必要があります
- [EMR.4] Amazon EMR セキュリティ設定は転送中に暗号化する必要があります
- [ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムでは、タグをバックアップにコピーするように設定する必要があります
- [FSx.5] FSx for Windows File Server ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.3] AWS Glue 機械学習変換は保管時に暗号化する必要があります
- [GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- [GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [GuardDuty.5] GuardDuty EKS 監査ログモニタリングを有効にする必要があります
- [GuardDuty.6] GuardDuty Lambda Protection を有効にする必要があります
- [GuardDuty.7] GuardDuty EKS ランタイムモニタリングを有効にする必要があります
- [GuardDuty.8] GuardDuty Malware Protection for EC2 を有効にする必要があります
- [GuardDuty.9] GuardDuty RDS Protection を有効にする必要があります
- [GuardDuty.10] GuardDuty S3 Protection を有効にする必要があります
- [GuardDuty.11] GuardDuty Runtime Monitoring を有効にする必要があります
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring を有効にする必要があります

- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.23] IAM Access Analyzer アナライザーにはタグを付ける必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [IAM.28] IAM Access Analyzer 外部アクセスアナライザーを有効にする必要があります
- [Inspector.1] Amazon Inspector EC2 スキャンを有効にする必要があります
- [Inspector.2] Amazon Inspector ECR スキャンを有効にする必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [Inspector.4] Amazon Inspector Lambda 標準スキャンを有効にする必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります

- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります
- [Lambda.2] Lambda 関数はサポートされているランタイムを使用する必要があります
- [Lambda.3] Lambda 関数は VPC 内に存在する必要があります
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Lambda.6] Lambda 関数にはタグを付ける必要があります
- [Lambda.7] Lambda 関数では AWS X-Ray アクティブなトレースを有効にする必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 機密データ自動検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [NetworkFirewall.1] Network Firewall ファイアウォールを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.2] Network Firewall ログ記録を有効にする必要があります
- [Network Firewall.3] Network Firewall ポリシーには、1 つ以上のルールグループが関連付けられている必要があります
- [NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、完全なパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、断片化されたパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.6] ステートレス Network Firewall のルールグループを空にしないでください
- [NetworkFirewall.7] Network Firewall ファイアウォールにはタグを付ける必要があります
- [NetworkFirewall.9] Network Firewall は削除保護を有効にする必要があります
- [NetworkFirewall.10] Network Firewall ファイアウォールでは、サブネット変更保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります

- [Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.11] OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です
- [PCA.1] AWS Private CA ルート認証機関を無効にする必要があります
- [PCA.2] AWS プライベート CA 認証機関にはタグを付ける必要があります
- [RDS.13] RDS 自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.28] RDS DB クラスターにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RDS.32] RDS DB スナップショットにはタグを付ける必要があります
- [RDS.34] Aurora MySQL DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.42] RDS for MariaDB DB インスタンスは CloudWatch Logs にログを発行する必要があります
- [RDS.44] RDS for MariaDB DB インスタンスは転送中に暗号化する必要があります

- [RDS.45] Aurora MySQL DB クラスターでは、監査ログ記録を有効にする必要があります
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの入力を許可する必要があります
- [Redshift.17] Redshift クラスターパラメータグループにはタグを付ける必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [RedshiftServerless.3] Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります
- [SageMaker.4] SageMaker エンドポイントの本番稼働バリアントの初期インスタンス数は 1 より大きい必要があります
- [SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります
- [SageMaker.6] SageMaker アプリのイメージ設定にはタグを付ける必要があります
- [SageMaker.7] SageMaker イメージにはタグを付ける必要があります
- [ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SSM.5] SSM ドキュメントにはタグを付ける必要があります
- [SSM.7] SSM ドキュメントでは、パブリック共有ブロック設定を有効にする必要があります
- [StepFunctions.2] Step Functions アクティビティにはタグを付ける必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [Transfer.4] Transfer Family 契約にはタグを付ける必要があります
- [Transfer.5] Transfer Family 証明書にはタグを付ける必要があります

- [Transfer.6] Transfer Family コネクタにはタグを付ける必要があります
- [Transfer.7] Transfer Family プロファイルにはタグを付ける必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

欧州 (フランクフルト)

欧州 (フランクフルト) リージョンでは、以下のコントロールはサポートされていません。

- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります

- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

欧州 (アイルランド)

欧州 (アイルランド) リージョンでは、以下のコントロールはサポートされていません。

- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります

- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です

- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

欧州 (ロンドン)

欧州 (ロンドン) リージョンでは、以下のコントロールはサポートされていません。

- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります

- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります

- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

欧州 (ミラノ)

欧州 (ミラノ) リージョンでは、以下のコントロールはサポートされていません。

- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります

- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります

- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります

- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- [RDS.1] RDS スナップショットはプライベートである必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [RedshiftServerless.3] Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります
- [RedshiftServerless.4] Redshift Serverless 名前空間はカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 名前空間では、デフォルトの管理者ユーザー名を使用しないでください

- [RedshiftServerless.6] Redshift Serverless 名前空間は CloudWatch Logs にログをエクスポートする必要があります
- [RedshiftServerless.7] Redshift Serverless 名前空間はデフォルトのデータベース名を使用しないでください
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SSM.2] Systems Manager によって管理される Amazon EC2 インスタンスは、パッチのインストール後に、パッチコンプライアンスのステータスが COMPLIANT である必要があります
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

欧州 (パリ)

欧州 (パリ) リージョンでは、以下のコントロールはサポートされていません。

- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります

- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります

- [FSx.5] FSx for Windows File Server ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です

- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

欧州 (スペイン)

欧州 (スペイン) リージョンでは、以下のコントロールはサポートされていません。

- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります
- [AppConfig.1] AWS AppConfig アプリケーションにはタグを付ける必要があります
- [AppConfig.2] AWS AppConfig 設定プロファイルにはタグを付ける必要があります
- [AppConfig.3] AWS AppConfig 環境にはタグを付ける必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります

- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります
- [Cognito.2] Cognito ID プールは認証されていない ID を許可しないでください
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [Detective.1] 検出動作グラフにはタグを付ける必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにはタグを付ける必要があります

- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります
- [DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DocumentDB.6] Amazon DocumentDB クラスターは転送中に暗号化する必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.1] Amazon EBS スナップショットはパブリックに復元できないようにすることをお勧めします
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.34] EC2 Transit Gateway ルートテーブルにはタグを付ける必要があります

- [EC2.40] EC2 NAT ゲートウェイにはタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.170] EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.175] EC2 起動テンプレートにはタグを付ける必要があります
- [EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります
- [EC2.179] EC2 トラフィックミラーターゲットにはタグを付ける必要があります
- [EC2.180] EC2 ネットワークインターフェイスでは、送信元/送信先チェックを有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります
- [ELB.18] Application and Network Load Balancer リスナーは、安全なプロトコルを使用して転送中のデータを暗号化する必要があります
- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります

- [ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください
- [ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。
- [ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります
- [ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.4] AWS Glue Spark ジョブは、サポートされているバージョンの で実行する必要があります AWS Glue
- [GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- [GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります

- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [Inspector.1] Amazon Inspector EC2 スキャンを有効にする必要があります
- [Inspector.2] Amazon Inspector ECR スキャンを有効にする必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [Inspector.4] Amazon Inspector Lambda 標準スキャンを有効にする必要があります
- [IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります

- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [Lambda.1] Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります
- [Lambda.7] Lambda 関数では AWS X-Ray アクティブなトレースを有効にする必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 機密データ自動検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります
- [MQ.3] Amazon MQ ブローカーでは、自動マイナーバージョンアップグレードが有効になっている必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.4] MSK クラスターではパブリックアクセスを無効にする必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [MSK.6] MSK クラスターは認証されていないアクセスを無効にする必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります

- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- [Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインはにはタグを付ける必要があります
- [Opensearch.10] OpenSearch ドメインには、最新のソフトウェアアップデートがインストールされている必要があります
- [Opensearch.11] OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です
- [RDS.1] RDS スナップショットはプライベートである必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.37] Aurora PostgreSQL DB クラスターでは、ログを CloudWatch Logs に発行する必要があります
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.18] Redshift クラスターでは、マルチ AZ 配置を有効にする必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります

- [S3.6] S3 汎用バケットポリシーは、他の へのアクセスを制限する必要があります AWS アカウント
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります
- [SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- [SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません
- [SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [SSM.6] SSM Automation では CloudWatch ログ記録が有効になっている必要があります
- [SSM.7] SSM ドキュメントでは、パブリック共有ブロック設定を有効にする必要があります
- [Transfer.3] Transfer Family コネクタではログ記録が有効になっている必要があります
- [Transfer.4] Transfer Family 契約にはタグを付ける必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

欧州 (ストックホルム)

欧州 (ストックホルム) リージョンでは、以下のコントロールはサポートされていません。

- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります

- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DocumentDB.6] Amazon DocumentDB クラスターは転送中に暗号化する必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります

- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

欧州 (チューリッヒ)

欧州 (チューリッヒ) リージョンでは、以下のコントロールはサポートされていません。

- [APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります

- [AppConfig.1] AWS AppConfig アプリケーションにはタグを付ける必要があります
- [AppConfig.2] AWS AppConfig 設定プロファイルにはタグを付ける必要があります
- [AppConfig.3] AWS AppConfig 環境にはタグを付ける必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります

- [CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットが一般公開されていないことを確認します
- [CloudTrail.7] CloudTrail S3 バケットで、S3 バケットアクセスログ記録が有効であることを確認します
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります
- [Cognito.2] Cognito ID プールは認証されていない ID を許可しないでください
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [Detective.1] 検出動作グラフにはタグを付ける必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにはタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります

- [DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DocumentDB.6] Amazon DocumentDB クラスターは転送中に暗号化する必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.170] EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.175] EC2 起動テンプレートにはタグを付ける必要があります
- [EC2.180] EC2 ネットワークインターフェイスでは、送信元/送信先チェックを有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS

- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります
- [ELB.18] Application and Network Load Balancer リスナーは、安全なプロトコルを使用して転送中のデータを暗号化する必要があります
- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります
- [ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください
- [ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。
- [ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります
- [ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.4] AWS Glue Spark ジョブは、サポートされているバージョンの で実行する必要があります AWS Glue

- [GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- [GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります

- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [Lambda.7] Lambda 関数では AWS X-Ray アクティブなトレースを有効にする必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 機密データ自動検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります
- [MQ.3] Amazon MQ ブローカーでは、自動マイナーバージョンアップグレードが有効になっている必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.4] MSK クラスターではパブリックアクセスを無効にする必要があります

- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [MSK.6] MSK クラスターは認証されていないアクセスを無効にする必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- [Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインはにはタグを付ける必要があります
- [Opensearch.10] OpenSearch ドメインには、最新のソフトウェアアップデートがインストールされている必要があります
- [Opensearch.11] OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です
- [RDS.1] RDS スナップショットはプライベートである必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります

- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [Redshift.18] Redshift クラスターでは、マルチ AZ 配置を有効にする必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります
- [SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- [SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません
- [SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります
- [SageMaker.6] SageMaker アプリのイメージ設定にはタグを付ける必要があります
- [SageMaker.7] SageMaker イメージにはタグを付ける必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [SSM.6] SSM Automation では CloudWatch ログ記録が有効になっている必要があります
- [SSM.7] SSM ドキュメントでは、パブリック共有ブロック設定を有効にする必要があります
- [Transfer.3] Transfer Family コネクタではログ記録が有効になっている必要があります
- [Transfer.4] Transfer Family 契約にはタグを付ける必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です

- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

イスラエル (テルアビブ)

イスラエル (テルアビブ) リージョンでは、以下のコントロールはサポートされていません。

- [APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.2] AWS AppSync フィールドレベルのログ記録を有効にする必要があります
- [AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- 〔バッチ.1] バッチジョブキューにはタグを付ける必要があります
- [Batch.3] バッチコンピューティング環境にはタグを付ける必要があります
- [Batch.4] マネージドバッチコンピューティング環境のコンピューティングリソースプロパティにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります

- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.2] Cognito ID プールは認証されていない ID を許可しないでください
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります

- [DMS.5] DMS レプリケーションサブネットグループにはタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります
- [DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DocumentDB.6] Amazon DocumentDB クラスターは転送中に暗号化する必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.20] AWS Site-to-Site VPN トンネルが稼働している必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします

- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.33] EC2 Transit Gateway アタッチメントにはタグを付ける必要があります
- [EC2.34] EC2 Transit Gateway ルートテーブルにはタグを付ける必要があります
- [EC2.40] EC2 NAT ゲートウェイにはタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.55] VPCs は ECR API のインターフェイスエンドポイントで設定する必要があります
- [EC2.56] VPCsは Docker Registry のインターフェイスエンドポイントで設定する必要があります
- [EC2.57] VPCsは Systems Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.170] EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.175] EC2 起動テンプレートにはタグを付ける必要があります
- [EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります
- [EC2.179] EC2 トラフィックミラーターゲットにはタグを付ける必要があります
- [EC2.180] EC2 ネットワークインターフェイスでは、送信元/送信先チェックを有効にする必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECR.5] ECR リポジトリはカスタマーマネージドで暗号化する必要があります AWS KMS keys

- [ECS.16] ECS タスクセットはパブリック IP アドレスを自動的に割り当てないでください。
- [EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります
- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EFS .8] EFS ファイルシステムは保管中に暗号化する必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.6] EKS クラスターにはタグを付ける必要があります
- [EKS.7] EKS ID プロバイダーの設定にはタグを付ける必要があります
- [EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります
- [ELB.2] SSL/HTTPS リスナーを使用する Classic Load Balancer は、 が提供する証明書を使用する必要があります AWS Certificate Manager
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります
- [ELB.18] Application and Network Load Balancer リスナーは、安全なプロトコルを使用して転送中のデータを暗号化する必要があります
- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElastiCache.2] ElastiCache クラスターでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [ElastiCache.3] ElastiCache (Redis OSS) レプリケーショングループでは、自動フェイルオーバーを有効にする必要があります
- [ElastiCache.4] ElastiCache レプリケーショングループは保管中に暗号化する必要があります
- [ElastiCache.5] ElastiCache レプリケーショングループは転送時に暗号化する必要があります
- [ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります
- [ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください

- [ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。
- [ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります
- [ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.4] AWS Glue Spark ジョブは、サポートされているバージョンの AWS Glue で実行する必要があります
- [GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- [GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.10] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します

- [IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します
- [IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します
- [IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します
- [IAM.15] IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認します
- [IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています
- [IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します
- [IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [IAM.28] IAM Access Analyzer 外部アクセスアナライザーを有効にする必要があります
- [Inspector.1] Amazon Inspector EC2 スキャンを有効にする必要があります
- [Inspector.2] Amazon Inspector ECR スキャンを有効にする必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [Inspector.4] Amazon Inspector Lambda 標準スキャンを有効にする必要があります
- [IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります

- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [Kinesis.2] Kinesis ストリームにはタグを付ける必要があります
- [Kinesis.3] Kinesis ストリームには適切なデータ保持期間が必要です
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Lambda.7] Lambda 関数では AWS X-Ray アクティブなトレースを有効にする必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります
- [MQ.3] Amazon MQ ブローカーでは、自動マイナーバージョンアップグレードが有効になっている必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります

- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.4] MSK クラスターではパブリックアクセスを無効にする必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [MSK.6] MSK クラスターは認証されていないアクセスを無効にする必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [NetworkFirewall.10] Network Firewall ファイアウォールでは、サブネット変更保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインはにはタグを付ける必要があります
- [Opensearch.10] OpenSearch ドメインには、最新のソフトウェアアップデートがインストールされている必要があります
- [Opensearch.11] OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です
- [RDS.1] RDS スナップショットはプライベートである必要があります
- [RDS.4] RDS クラスタースナップショットとデータベーススナップショットは保管中に暗号化する必要があります

- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.29] RDS DB クラスタースナップショットにはタグを付ける必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.37] Aurora PostgreSQL DB クラスターでは、ログを CloudWatch Logs に発行する必要があります
- [Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります
- [Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください
- [Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください
- [Redshift.18] Redshift クラスターでは、マルチ AZ 配置を有効にする必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります
- [SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- [SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません
- [SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります
- [ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります

- [SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [SSM.4] SSM ドキュメントはパブリックにしないでください
- [SSM.6] SSM Automation では CloudWatch ログ記録が有効になっている必要があります
- [SSM.7] SSM ドキュメントでは、パブリック共有ブロック設定を有効にする必要があります
- [StepFunctions.1] Step Functions ステートマシンではログ記録がオンになっている必要があります
- [Transfer.3] Transfer Family コネクタではログ記録が有効になっている必要があります
- [Transfer.4] Transfer Family 契約にはタグを付ける必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

メキシコ (中部)

以下のコントロールは、メキシコ (中部) リージョンではサポートされていません。

- [ACM.1] インポートされ ACM によって発行された証明書は、一定期間後に更新する必要があります
- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [Account.1] のセキュリティ連絡先情報は に提供する必要があります AWS アカウント
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.1] API Gateway REST および WebSocket API 実行ログ記録を有効にする必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります

- [APIGateway.3] API Gateway REST API ステージでは、 AWS X-Ray トレースを有効にする必要があります
- [APIGateway.4] API Gateway は、WAF ウェブ ACL に関連付けられている必要があります
- [APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります
- [AppConfig.1] AWS AppConfig アプリケーションにはタグを付ける必要があります
- [AppConfig.2] AWS AppConfig 設定プロファイルにはタグを付ける必要があります
- [AppConfig.3] AWS AppConfig 環境にはタグを付ける必要があります
- [AppConfig.4] AWS AppConfig 拡張機能の関連付けにはタグを付ける必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.2] AWS AppSync フィールドレベルのログ記録を有効にする必要があります
- [AppSync.4] AWS AppSync GraphQL APIsにはタグを付ける必要があります
- [AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [Athena.2] Athena データカタログにはタグを付ける必要があります
- [Athena.3] Athena ワークグループにはタグを付ける必要があります
- [Athena.4] Athena ワークグループではログ記録が有効になっている必要があります
- [AutoScaling.2] Amazon EC2 Auto Scaling グループは、複数のアベイラビリティーゾーンをカバーする必要があります
- [AutoScaling.3] Auto Scaling グループ起動設定は、EC2 インスタンスを、インスタンスメタデータサービスバージョン 2 (IMDSv2) を必要とするように設定する必要があります
- [AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります
- [AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります

- [Backup.2] AWS Backup 復旧ポイントにはタグを付ける必要があります
- [Backup.3] AWS Backup ボールトにはタグを付ける必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [Backup.5] AWS Backup バックアッププランにはタグを付ける必要があります
- 〔バッチ.1] バッチジョブキューにはタグを付ける必要があります
- [Batch.2] バッチスケジューリングポリシーにはタグを付ける必要があります
- [Batch.3] バッチコンピューティング環境にはタグを付ける必要があります
- [Batch.4] マネージドバッチコンピューティング環境のコンピューティングリソースプロパティにはタグを付ける必要があります
- [CloudFormation.2] CloudFormation スタックにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります

- [CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットが一般公開されていないことを確認します
- [CloudTrail.7] CloudTrail S3 バケットで、S3 バケットアクセスログ記録が有効であることを確認します
- [CloudTrail.10] CloudTrail Lake イベントデータストアはカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [CloudWatch.17] CloudWatch アラームアクションをアクティブにする必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeBuild.1] CodeBuild Bitbucket ソースリポジトリの URL には機密認証情報を含めないでください
- [CodeBuild.2] CodeBuild プロジェクト環境変数にクリアテキストの認証情報を含めることはできません
- [CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- [CodeBuild.4] CodeBuild AWS Configプロジェクト環境にはログ記録設定が必要です
- [CodeBuild.7] CodeBuild レポートグループのエクスポートは保管時に暗号化する必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります
- [Cognito.2] Cognito ID プールは認証されていない ID を許可しないでください
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります
- [DataSync.1] DataSync タスクではログ記録が有効になっている必要があります
- [DataSync.2] DataSync タスクにはタグを付ける必要があります
- [Detective.1] 検出動作グラフにはタグを付ける必要があります
- [DMS.1] Database Migration Service のレプリケーションインスタンスは非パブリックである必要があります

- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにはタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります
- [DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DocumentDB.6] Amazon DocumentDB クラスターは転送中に暗号化する必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります
- [DynamoDB.6] DynamoDB テーブルで、削除保護が有効になっている必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります
- [EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします

- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.33] EC2 Transit Gateway アタッチメントにはタグを付ける必要があります
- [EC2.34] EC2 Transit Gateway ルートテーブルにはタグを付ける必要があります
- [EC2.40] EC2 NAT ゲートウェイにはタグを付ける必要があります
- [EC2.48] Amazon VPC フローログにはタグを付ける必要があります
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.52] EC2 Transit Gateway にはタグを付ける必要があります
- [EC2.53] EC2 セキュリティグループが 0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可することがないようにする必要があります
- [EC2.54] EC2 セキュリティグループは ::/0 からリモートサーバー管理ポートへの入力を許可しない必要があります
- [EC2.55] VPCs は ECR API のインターフェイスエンドポイントで設定する必要があります
- [EC2.56] VPCsは Docker Registry のインターフェイスエンドポイントで設定する必要があります
- [EC2.57] VPCsは Systems Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.170] EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.171] EC2 VPN 接続では、ログ記録が有効になっている必要があります
- [EC2.172] EC2 VPC ブロックパブリックアクセス設定はインターネットゲートウェイトラフィックをブロックする必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります

- [EC2.174] EC2 DHCP オプションセットにはタグを付ける必要があります
- [EC2.175] EC2 起動テンプレートにはタグを付ける必要があります
- [EC2.176] EC2 プレフィックスリストにはタグを付ける必要があります
- [EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります
- [EC2.178] EC2 トラフィックミラーフィルターにはタグを付ける必要があります
- [EC2.179] EC2 トラフィックミラーターゲットにはタグを付ける必要があります
- [EC2.180] EC2 ネットワークインターフェイスでは、送信元/送信先チェックを有効にする必要があります
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECR.5] ECR リポジトリはカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください
- [ECS.4] ECS コンテナは、非特権として実行する必要があります
- [ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。
- [ECS.8] シークレットは、コンテナ環境の変数として渡さないでください
- [ECS.9] ECS タスク定義にはログ設定が必要です。
- [ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。
- [ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります
- [ECS.16] ECS タスクセットはパブリック IP アドレスを自動的に割り当てないでください。
- [ECS.17] ECS タスク定義はホストネットワークモードを使用しないでください
- [EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります

- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EFS .5] EFS アクセスポイントにはタグを付ける必要があります
- [EFS.6] EFS マウントターゲットは、起動時にパブリック IP アドレスを割り当てるサブネットに関連付けるべきではありません
- [EFS .7] EFS ファイルシステムでは、自動バックアップが有効になっている必要があります
- [EFS .8] EFS ファイルシステムは保管中に暗号化する必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります
- [EKS.6] EKS クラスターにはタグを付ける必要があります
- [EKS.7] EKS ID プロバイダーの設定にはタグを付ける必要があります
- [EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります
- [ELB.10] Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります
- [ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります
- [ELB.18] Application and Network Load Balancer リスナーは、安全なプロトコルを使用して転送中のデータを暗号化する必要があります
- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElastiCache.2] ElastiCache クラスターでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [ElastiCache.3] ElastiCache (Redis OSS) レプリケーショングループでは、自動フェイルオーバーを有効にする必要があります
- [ElastiCache.4] ElastiCache レプリケーショングループは保管中に暗号化する必要があります
- [ElastiCache.5] ElastiCache レプリケーショングループは転送時に暗号化する必要があります

- [ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります
- [ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください
- [ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。
- [ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります
- [ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります
- [EMR.3] Amazon EMR セキュリティ設定は保管時に暗号化する必要があります
- [EMR.4] Amazon EMR セキュリティ設定は転送中に暗号化する必要があります
- [ES.3] Elasticsearch ドメインは、ノード間で送信されるデータを暗号化する必要があります
- [ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります
- [ES.9] Elasticsearch ドメインにはタグを付ける必要があります
- [EventBridge.2] EventBridge イベントバスにはタグを付ける必要があります
- [EventBridge.3] Amazon EventBridge カスタムイベントバスにリソースポリシーがアタッチされている必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムでは、タグをバックアップにコピーするように設定する必要があります
- [FSx.3] FSx for OpenZFS ファイルシステムは、マルチ AZ 配置用に設定する必要があります

- [FSx.4] FSx for NetApp ONTAP ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [FSx.5] FSx for Windows File Server ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.1] AWS Glue ジョブにはタグを付ける必要があります
- [Glue.3] AWS Glue 機械学習変換は保管時に暗号化する必要があります
- [Glue.4] AWS Glue Spark ジョブは、サポートされているバージョンの AWS Glue で実行する必要があります
- [GuardDuty.1] GuardDuty を有効にする必要があります
- [GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- [GuardDuty.3] GuardDuty IPSets にはタグを付ける必要があります
- [GuardDuty.4] GuardDuty ディテクターにはタグを付ける必要があります
- [GuardDuty.5] GuardDuty EKS 監査ログモニタリングを有効にする必要があります
- [GuardDuty.6] GuardDuty Lambda Protection を有効にする必要があります
- [GuardDuty.7] GuardDuty EKS ランタイムモニタリングを有効にする必要があります
- [GuardDuty.8] GuardDuty Malware Protection for EC2 を有効にする必要があります
- [GuardDuty.9] GuardDuty RDS Protection を有効にする必要があります
- [GuardDuty.10] GuardDuty S3 Protection を有効にする必要があります
- [GuardDuty.11] GuardDuty Runtime Monitoring を有効にする必要があります
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring を有効にする必要があります
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring を有効にする必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.7] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります

- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.10] IAM ユーザーのパスワードポリシーには強力な設定が必要です
- [IAM.11] IAM パスワードポリシーで少なくとも 1 文字の大文字が要求されていることを確認します
- [IAM.12] IAM パスワードポリシーで少なくとも 1 文字の小文字が要求されていることを確認します
- [IAM.13] IAM パスワードポリシーで少なくとも 1 文字の記号が要求されていることを確認します
- [IAM.14] IAM パスワードポリシーで少なくとも 1 文字の数字が要求されていることを確認します
- [IAM.15] IAM パスワードポリシーで 14 文字以上の長さが要求されていることを確認します
- [IAM.16] IAM パスワードポリシーはパスワードの再使用を禁止しています
- [IAM.17] IAM パスワードポリシーでパスワードが 90 日以内に有効期限切れとなることを確認します
- [IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.23] IAM Access Analyzer アナライザーにはタグを付ける必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [IAM.28] IAM Access Analyzer 外部アクセスアナライザーを有効にする必要があります
- [Inspector.1] Amazon Inspector EC2 スキャンを有効にする必要があります
- [Inspector.2] Amazon Inspector ECR スキャンを有効にする必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [Inspector.4] Amazon Inspector Lambda 標準スキャンを有効にする必要があります
- [IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります
- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります

- [IoT.4] AWS IoT Core オーソライザーにはタグを付ける必要があります
- [IoT.5] AWS IoT Core ロールエイリアスにはタグを付ける必要があります
- [IoT.6] AWS IoT Core ポリシーにはタグを付ける必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [Kinesis.2] Kinesis ストリームにはタグを付ける必要があります
- [Kinesis.3] Kinesis ストリームには適切なデータ保持期間が必要です
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [KMS.5] KMS キーはパブリックにアクセスしないでください

- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Lambda.7] Lambda 関数では AWS X-Ray アクティブなトレースを有効にする必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 機密データ自動検出を有効にする必要があります
- [MQ.2] ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります
- [MQ.3] Amazon MQ ブローカーでは、自動マイナーバージョンアップグレードが有効になっている必要があります
- [MQ.4] Amazon MQ ブローカーにはタグを付ける必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.4] MSK クラスターではパブリックアクセスを無効にする必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [MSK.6] MSK クラスターは認証されていないアクセスを無効にする必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.1] Network Firewall ファイアウォールを複数のアベイラビリティーゾーンにデプロイする必要があります

- [NetworkFirewall.2] Network Firewall ログ記録を有効にする必要があります
- [Network Firewall.3] Network Firewall ポリシーには、1 つ以上のルールグループが関連付けられている必要があります
- [NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、完全なパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、断片化されたパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.6] ステートレス Network Firewall のルールグループを空にしないでください
- [NetworkFirewall.9] Network Firewall は削除保護を有効にする必要があります
- [NetworkFirewall.10] Network Firewall ファイアウォールでは、サブネット変更保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインはにはタグを付ける必要があります
- [Opensearch.10] OpenSearch ドメインには、最新のソフトウェアアップデートがインストールされている必要があります
- [Opensearch.11] OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です
- [PCA.1] AWS Private CA ルート認証機関を無効にする必要があります
- [PCA.2] AWS プライベート CA 認証機関にはタグを付ける必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.18] RDS インスタンスは VPC 内にデプロイする必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります

- [RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります
- [RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RDS.34] Aurora MySQL DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.36] RDS for PostgreSQL DB は CloudWatch Logs にログを発行する必要があります
- [RDS.37] Aurora PostgreSQL DB クラスターでは、ログを CloudWatch Logs に発行する必要があります
- [RDS.38] RDS for PostgreSQL DB インスタンスは転送中に暗号化する必要があります
- [RDS.39] RDS for MySQL DB インスタンスは転送中に暗号化する必要があります
- [RDS.40] RDS for SQL Server DB インスタンスは CloudWatch Logs にログを発行する必要があります
- [RDS.41] RDS for SQL Server DB インスタンスは転送中に暗号化する必要があります
- [RDS.42] RDS for MariaDB DB インスタンスは CloudWatch Logs にログを発行する必要があります
- [RDS.44] RDS for MariaDB DB インスタンスは転送中に暗号化する必要があります
- [RDS.45] Aurora MySQL DB クラスターでは、監査ログ記録を有効にする必要があります
- [PCI.Redshift.1] Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります
- [Redshift.2] Amazon Redshift クラスターへの接続は転送中に暗号化する必要があります
- [Redshift.3] Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります
- [Redshift.4] Amazon Redshift クラスターでは、監査ログ記録が有効になっている必要があります
- [Redshift.6] Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります
- [Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります
- [Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください
- [Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください

- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.11] Redshift クラスターにはタグを付ける必要があります
- [Redshift.12] Redshift イベント通知サブスクリプションにはタグを付ける必要があります
- [Redshift.13] Redshift クラスタースナップショットにはタグを付ける必要があります
- [Redshift.14] Redshift クラスターサブネットグループにはタグを付ける必要があります
- [Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの入力を許可する必要があります
- [Redshift.16] Redshift クラスターサブネットグループには、複数のアベイラビリティーゾーンからのサブネットが必要です
- [Redshift.17] Redshift クラスターパラメータグループにはタグを付ける必要があります
- [Redshift.18] Redshift クラスターでは、マルチ AZ 配置を有効にする必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [RedshiftServerless.3] Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります
- [RedshiftServerless.4] Redshift Serverless 名前空間はカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 名前空間では、デフォルトの管理者ユーザー名を使用しないでください
- [RedshiftServerless.6] Redshift Serverless 名前空間は CloudWatch Logs にログをエクスポートする必要があります
- [RedshiftServerless.7] Redshift Serverless 名前空間はデフォルトのデータベース名を使用しないでください
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.7] S3 汎用バケットでクロスリージョンレプリケーションを使用する必要があります
- [S3.10] バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です
- [S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります
- [S3.12] ACL は、S3 汎用バケットへのユーザーアクセスの管理に使用しないでください。
- [S3.13] S3 汎用バケットにはライフサイクル設定が必要です

- [S3.19] S3 アクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります
- [S3.22] S3 汎用バケットはオブジェクトレベルの書き込みイベントをログに記録する必要があります
- [S3.23] S3 汎用バケットはオブジェクトレベルの読み取りイベントをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります
- [SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- [SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません
- [SageMaker.4] SageMaker エンドポイントの本番稼働バリアントの初期インスタンス数は 1 より大きい必要があります
- [SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります
- [SageMaker.6] SageMaker アプリのイメージ設定にはタグを付ける必要があります
- [SageMaker.7] SageMaker イメージにはタグを付ける必要があります
- [SageMaker.8] SageMaker ノートブックインスタンスは、サポートされているプラットフォームで実行する必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- [SecretsManager.1] Secrets Manager のシークレットは、自動ローテーションを有効にする必要があります
- [SecretsManager.2] 自動ローテーションを設定した Secrets Manager のシークレットは正常にローテーションする必要があります
- [SecretsManager.3] 未使用の Secrets Manager のシークレットを削除します
- [SecretsManager.4] Secrets Manager のシークレットは、指定された日数以内にローテーションする必要があります
- [ServiceCatalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります
- [SNS.4] SNS トピックアクセスポリシーはパブリックアクセスを許可しないでください

- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります
- [SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください
- [SSM.3] Systems Manager によって管理される Amazon EC2 インスタンスの関連付けコンプライアンスのステータスは COMPLIANT である必要があります
- [SSM.4] SSM ドキュメントはパブリックにしないでください
- [SSM.5] SSM ドキュメントにはタグを付ける必要があります
- [SSM.6] SSM Automation では CloudWatch ログ記録が有効になっている必要があります
- [SSM.7] SSM ドキュメントでは、パブリック共有ブロック設定を有効にする必要があります
- [StepFunctions.1] Step Functions ステートマシンではログ記録がオンになっている必要があります
- [StepFunctions.2] Step Functions アクティビティにはタグを付ける必要があります
- [Transfer.1] AWS Transfer Family ワークフローにはタグを付ける必要があります
- [Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください
- [Transfer.3] Transfer Family コネクタではログ記録が有効になっている必要があります
- [Transfer.4] Transfer Family 契約にはタグを付ける必要があります
- [Transfer.5] Transfer Family 証明書にはタグを付ける必要があります
- [Transfer.6] Transfer Family コネクタにはタグを付ける必要があります
- [Transfer.7] Transfer Family プロファイルにはタグを付ける必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.2] AWS WAF Classic リージョンルールには少なくとも 1 つの条件が必要です
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です
- [WAF.4] AWS WAF Classic Regional Web ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります

- [WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

中東 (バーレーン)

中東 (バーレーン) リージョンでは、以下のコントロールはサポートされていません。

- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります

- [CloudTrail.10] CloudTrail Lake イベントデータストアはカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DocumentDB.6] Amazon DocumentDB クラスターは転送中に暗号化する必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.20] AWS Site-to-Site VPN トンネルが稼働している必要があります
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECR.5] ECR リポジトリはカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [ECS.17] ECS タスク定義はホストネットワークモードを使用しないでください

- [ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [FSx.3] FSx for OpenZFS ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [FSx.4] FSx for NetApp ONTAP ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [FSx.5] FSx for Windows File Server ファイルシステムは、マルチ AZ 配置用に設定する必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.4] AWS Glue Spark ジョブは、サポートされているバージョンの AWS Glue で実行する必要があります
- [GuardDuty.11] GuardDuty Runtime Monitoring を有効にする必要があります
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring を有効にする必要があります
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring を有効にする必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります

- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [NetworkFirewall.10] Network Firewall ファイアウォールでは、サブネット変更保護を有効にする必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RDS.41] RDS for SQL Server DB インスタンスは転送中に暗号化する必要があります
- [RDS.42] RDS for MariaDB DB インスタンスは CloudWatch Logs にログを発行する必要があります
- [RDS.44] RDS for MariaDB DB インスタンスは転送中に暗号化する必要があります
- [RDS.45] Aurora MySQL DB クラスターでは、監査ログ記録を有効にする必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [RedshiftServerless.3] Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります
- [RedshiftServerless.4] Redshift Serverless 名前空間はカスタマーマネージドで暗号化する必要があります AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 名前空間では、デフォルトの管理者ユーザー名を使用しないでください
- [RedshiftServerless.6] Redshift Serverless 名前空間は CloudWatch Logs にログをエクスポートする必要があります

- [RedshiftServerless.7] Redshift Serverless 名前空間はデフォルトのデータベース名を使用しないでください
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SageMaker.8] SageMaker ノートブックインスタンスは、サポートされているプラットフォームで実行する必要があります
- [SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください
- [Transfer.3] Transfer Family コネクタではログ記録が有効になっている必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

中東 (アラブ首長国連邦)

中東 (UAE) リージョンでは、以下のコントロールはサポートされていません。

- [APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります
- [AppConfig.1] AWS AppConfig アプリケーションにはタグを付ける必要があります
- [AppConfig.2] AWS AppConfig 設定プロファイルにはタグを付ける必要があります
- [AppConfig.3] AWS AppConfig 環境にはタグを付ける必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります

- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [AutoScaling.1] ロードバランサーに関連付けられた Auto Scaling グループは ELB ヘルスチェックを使用する必要がある
- [Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CloudTrail.6] CloudTrail ログの保存に使用される S3 バケットが一般公開されていないことを確認します
- [CloudWatch.16] CloudWatch ロググループは指定した期間保持する必要があります

- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります
- [Cognito.2] Cognito ID プールは認証されていない ID を許可しないでください
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [Detective.1] 検出動作グラフにはタグを付ける必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.3] DMS イベントサブスクリプションにはタグを付ける必要があります
- [DMS.4] DMS レプリケーションインスタンスにはタグを付ける必要があります
- [DMS.5] DMS レプリケーションサブネットグループにはタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります
- [DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります
- [DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.4] 停止した EC2 インスタンスは、指定した期間後に削除する必要があります

- [EC2.12] 未使用の Amazon EC2 EIP を削除することをお勧めします
- [EC2.14] セキュリティグループは、0.0.0.0/0 または ::/0 からポート 3389 への入力を許可しないようにする必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.170] EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.175] EC2 起動テンプレートにはタグを付ける必要があります
- [EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります
- [EC2.179] EC2 トラフィックミラーターゲットにはタグを付ける必要があります
- [EC2.180] EC2 ネットワークインターフェイスでは、送信元/送信先チェックを有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.1] Amazon ECS タスク定義には、セキュアなネットワークモードとユーザー定義が必要です。
- [EFS.1] Elastic File System は、 を使用して保管中のファイルデータを暗号化するように設定する必要があります AWS KMS
- [EFS.2] Amazon EFS ボリュームは、バックアッププランに含める必要があります
- [ELB.3] Classic Load Balancer のリスナーは、HTTPS または TLS ターミネーションで設定する必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります

- [ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります
- [ELB.18] Application and Network Load Balancer リスナーは、安全なプロトコルを使用して転送中のデータを暗号化する必要があります
- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElastiCache.2] ElastiCache クラスターでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [ElastiCache.3] ElastiCache (Redis OSS) レプリケーショングループでは、自動フェイルオーバーを有効にする必要があります
- [ElastiCache.4] ElastiCache レプリケーショングループは保管中に暗号化する必要があります
- [ElastiCache.5] ElastiCache レプリケーショングループは転送時に暗号化する必要があります
- [ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります
- [ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください
- [ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。
- [ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります
- [ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります
- [EMR.1] Amazon EMR クラスタープライマリノードは、パブリック IP アドレスを未設定にする必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.4] AWS Glue Spark ジョブは、サポートされているバージョンの AWS Glue で実行する必要があります

- [GuardDuty.2] GuardDuty フィルターにはタグを付ける必要があります
- [IAM.1] IAM ポリシーでは、完全な「*」管理者権限を許可しないでください
- [IAM.2] IAM ユーザーには IAM ポリシーを添付しないでください
- [IAM.3] IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります
- [IAM.4] IAM ルートユーザーアクセスキーが存在してはいけません
- [IAM.5] コンソールパスワードを使用するすべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.8] 未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.18] AWS サポートでインシデントを管理するためのサポートロールが作成されていることを確認します
- [IAM.19] すべての IAM ユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.22] 45 日間未使用の IAM ユーザー認証情報は削除する必要があります
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください
- [Inspector.1] Amazon Inspector EC2 スキャンを有効にする必要があります
- [Inspector.2] Amazon Inspector ECR スキャンを有効にする必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [Inspector.4] Amazon Inspector Lambda 標準スキャンを有効にする必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります

- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [KMS.1] IAM カスタマー管理ポリシーでは、すべての KMS キーの復号アクションを許可しないでください
- [KMS.2] IAM プリンシパルは、すべての KMS キーで復号アクションを許可する IAM インラインポリシーを使用しないでください
- [KMS.4] AWS KMS キーローテーションを有効にする必要があります
- [Lambda.7] Lambda 関数では AWS X-Ray アクティブなトレースを有効にする必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 機密データ自動検出を有効にする必要があります
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.4] MSK クラスターではパブリックアクセスを無効にする必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [MSK.6] MSK クラスターは認証されていないアクセスを無効にする必要があります
- [Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です

- [Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [Opensearch.9] OpenSearch ドメインはにはタグを付ける必要があります
- [Opensearch.10] OpenSearch ドメインには、最新のソフトウェアアップデートがインストールされている必要があります
- [Opensearch.11] OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [Redshift.18] Redshift クラスターでは、マルチ AZ 配置を有効にする必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります
- [SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- [SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません
- [SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります
- [SQS.1] Amazon SQS キューは保管中に暗号化する必要があります
- [SQS.2] SQS キューにはタグを付ける必要があります

- [SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください
- [SSM.1] Amazon EC2 インスタンスは によって管理する必要があります AWS Systems Manager
- [SSM.6] SSM Automation では CloudWatch ログ記録が有効になっている必要があります
- [SSM.7] SSM ドキュメントでは、パブリック共有ブロック設定を有効にする必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

南米 (サンパウロ)

以下のコントロールは、南米 (サンパウロ) リージョンではサポートされていません。

- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります

- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [IoT.1] AWS IoT Device Defender セキュリティプロファイルにはタグを付ける必要があります
- [IoT.2] AWS IoT Core 緩和アクションにはタグを付ける必要があります

- [IoT.3] AWS IoT Core ディメンションにはタグを付ける必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です

AWS GovCloud (米国東部)

以下のコントロールは、 AWS GovCloud (米国東部) リージョンではサポートされていません。

- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります
- [Account.1] のセキュリティ連絡先情報は に提供する必要があります AWS アカウント
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります
- [APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります
- [AppConfig.1] AWS AppConfig アプリケーションにはタグを付ける必要があります
- [AppConfig.2] AWS AppConfig 設定プロファイルにはタグを付ける必要があります
- [AppConfig.3] AWS AppConfig 環境にはタグを付ける必要があります
- [AppConfig.4] AWS AppConfig 拡張機能の関連付けにはタグを付ける必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.2] AWS AppSync フィールドレベルのログ記録を有効にする必要があります
- [AppSync.4] AWS AppSync GraphQL APIsにはタグを付ける必要があります
- [AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [AutoScaling.2] Amazon EC2 Auto Scaling グループは、複数のアベイラビリティーゾーンをカバーする必要があります
- [AutoScaling.3] Auto Scaling グループ起動設定は、EC2 インスタンスを、インスタンスメタデータサービスバージョン 2 (IMDSv2) を必要とするように設定する必要があります
- [AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります

- [AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- 〔バッチ.1] バッチジョブキューにはタグを付ける必要があります
- [Batch.2] バッチスケジューリングポリシーにはタグを付ける必要があります
- [Batch.3] バッチコンピューティング環境にはタグを付ける必要があります
- [Batch.4] マネージドバッチコンピューティング環境のコンピューティングリソースプロパティにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CloudWatch.17] CloudWatch アラームアクションをアクティブにする必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります

- [CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- [CodeBuild.4] CodeBuild AWS Configプロジェクト環境にはログ記録設定が必要です
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります
- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります
- [Cognito.2] Cognito ID プールは認証されていない ID を許可しないでください
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります
- [DataSync.2] DataSync タスクにはタグを付ける必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります

- [EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします
- [EC2.47] Amazon VPC エンドポイントサービスはタグを付ける必要があります
- [EC2.52] EC2 Transit Gateway にはタグを付ける必要があります
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.170] EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.174] EC2 DHCP オプションセットにはタグを付ける必要があります
- [EC2.175] EC2 起動テンプレートにはタグを付ける必要があります
- [EC2.176] EC2 プレフィックスリストにはタグを付ける必要があります
- [EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります
- [EC2.178] EC2 トラフィックミラーフィルターにはタグを付ける必要があります
- [EC2.179] EC2 トラフィックミラーターゲットにはタグを付ける必要があります
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください

- [ECS.4] ECS コンテナは、非特権として実行する必要があります
- [ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。
- [ECS.8] シークレットは、コンテナ環境の変数として渡さないでください
- [ECS.9] ECS タスク定義にはログ設定が必要です。
- [ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。
- [ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります
- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります
- [ELB.10] Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります
- [ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElastiCache.2] ElastiCache クラスターでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [ElastiCache.3] ElastiCache (Redis OSS) レプリケーショングループでは、自動フェイルオーバーを有効にする必要があります
- [ElastiCache.4] ElastiCache レプリケーショングループは保管中に暗号化する必要があります
- [ElastiCache.5] ElastiCache レプリケーショングループは転送時に暗号化する必要があります
- [ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります

- [ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください
- [ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。
- [ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります
- [ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります
- [EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります
- [EMR.3] Amazon EMR セキュリティ設定は保管時に暗号化する必要があります
- [EMR.4] Amazon EMR セキュリティ設定は転送中に暗号化する必要があります
- [ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります
- [EventBridge.3] Amazon EventBridge カスタムイベントバスにリソースポリシーがアタッチされている必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムでは、タグをバックアップにコピーするように設定する必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [Glue.3] AWS Glue 機械学習変換は保管時に暗号化する必要があります
- [GuardDuty.7] GuardDuty EKS ランタイムモニタリングを有効にする必要があります
- [GuardDuty.8] GuardDuty Malware Protection for EC2 を有効にする必要があります
- [GuardDuty.9] GuardDuty RDS Protection を有効にする必要があります
- [GuardDuty.11] GuardDuty Runtime Monitoring を有効にする必要があります
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring を有効にする必要があります
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring を有効にする必要があります

- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーにはタグを付ける必要があります
- [IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります
- [IAM.28] IAM Access Analyzer 外部アクセスアナライザーを有効にする必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります
- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [KMS.5] KMS キーはパブリックにアクセスしないでください

- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 機密データ自動検出を有効にする必要があります
- [MQ.3] Amazon MQ ブローカーでは、自動マイナーバージョンアップグレードが有効になっている必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります
- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.1] Network Firewall ファイアウォールを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.2] Network Firewall ログ記録を有効にする必要があります
- [Network Firewall.3] Network Firewall ポリシーには、1 つ以上のルールグループが関連付けられている必要があります
- [NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、完全なパケットに対してドロップまたは転送される必要があります。

- [NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、断片化されたパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.6] ステートレス Network Firewall のルールグループを空にしないでください
- [NetworkFirewall.9] Network Firewall は削除保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります
- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [PCA.1] AWS Private CA ルート認証機関を無効にする必要があります
- [PCA.2] AWS プライベート CA 認証機関にはタグを付ける必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [RDS.31] RDS DB セキュリティグループにはタグを付ける必要があります
- [RDS.34] Aurora MySQL DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.45] Aurora MySQL DB クラスターでは、監査ログ記録を有効にする必要があります
- [Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください

- [Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.17] Redshift クラスターパラメータグループにはタグを付ける必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です
- [RedshiftServerless.3] Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります
- [RedshiftServerless.6] Redshift Serverless 名前空間は CloudWatch Logs にログをエクスポートする必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.10] バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です
- [S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります
- [S3.12] ACL は、S3 汎用バケットへのユーザーアクセスの管理に使用しないでください。
- [S3.13] S3 汎用バケットにはライフサイクル設定が必要です
- [S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SageMaker.1] Amazon SageMaker ノートブックインスタンスは、インターネットに直接アクセスできないようにする必要があります
- [SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- [SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません
- [SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります
- [SageMaker.6] SageMaker アプリのイメージ設定にはタグを付ける必要があります
- [SageMaker.7] SageMaker イメージにはタグを付ける必要があります
- [SES.1] SES 連絡先リストにはタグを付ける必要があります
- [SES.2] SES 設定セットにはタグを付ける必要があります

- [SNS.4] SNS トピックアクセスポリシーはパブリックアクセスを許可しないでください
- [SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください
- [SSM.4] SSM ドキュメントはパブリックにしないでください
- [SSM.5] SSM ドキュメントにはタグを付ける必要があります
- [SSM.6] SSM Automation では CloudWatch ログ記録が有効になっている必要があります
- [StepFunctions.1] Step Functions ステートマシンではログ記録がオンになっている必要があります
- [StepFunctions.2] Step Functions アクティビティにはタグを付ける必要があります
- [Transfer.4] Transfer Family 契約にはタグを付ける必要があります
- [Transfer.5] Transfer Family 証明書にはタグを付ける必要があります
- [Transfer.6] Transfer Family コネクタにはタグを付ける必要があります
- [Transfer.7] Transfer Family プロファイルにはタグを付ける必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります
- [WAF.2] AWS WAF Classic リージョンルールには少なくとも 1 つの条件が必要です
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です
- [WAF.4] AWS WAF Classic Regional Web ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります
- [WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります
- [WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります

AWS GovCloud (米国西部)

以下のコントロールは、 AWS GovCloud (米国西部) リージョンではサポートされていません。

- [ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります

- [Account.1] のセキュリティ連絡先情報は に提供する必要があります AWS アカウント
- [Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります
- [APIGateway.2] API Gateway REST API ステージでは、バックエンド認証に SSL 証明書を使用するように設定する必要があります
- [APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります
- [APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります
- [Amplify.1] Amplify アプリにはタグを付ける必要があります
- [Amplify.2] Amplify ブランチにはタグを付ける必要があります
- [AppConfig.1] AWS AppConfig アプリケーションにはタグを付ける必要があります
- [AppConfig.2] AWS AppConfig 設定プロファイルにはタグを付ける必要があります
- [AppConfig.3] AWS AppConfig 環境にはタグを付ける必要があります
- [AppConfig.4] AWS AppConfig 拡張機能の関連付けにはタグを付ける必要があります
- [AppFlow.1] Amazon AppFlow フローにはタグを付ける必要があります
- [AppRunner.1] App Runner サービスにはタグを付ける必要があります
- [AppRunner.2] App Runner VPC コネクタにはタグを付ける必要があります
- [AppSync.1] AWS AppSync API キャッシュは保管時に暗号化する必要があります
- [AppSync.2] AWS AppSync フィールドレベルのログ記録を有効にする必要があります
- [AppSync.4] AWS AppSync GraphQL APIsにはタグを付ける必要があります
- [AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください
- [AppSync.6] AWS AppSync API キャッシュは転送中に暗号化する必要があります
- [AutoScaling.2] Amazon EC2 Auto Scaling グループは、複数のアベイラビリティーゾーンをカバーする必要があります
- [AutoScaling.3] Auto Scaling グループ起動設定は、EC2 インスタンスを、インスタンスメタデータサービスバージョン 2 (IMDSv2) を必要とするように設定する必要があります
- [AutoScaling.6] Auto Scaling グループは、複数のアベイラビリティーゾーンで複数のインスタンスタイプを使用する必要があります
- [AutoScaling.9] Amazon EC2 Auto Scaling グループは Amazon EC2 起動テンプレートを使用する必要があります
- [Backup.4] AWS Backup レポートプランにはタグを付ける必要があります
- 〔バッチ.1] バッチジョブキューにはタグを付ける必要があります

- [Batch.2] バッチスケジューリングポリシーにはタグを付ける必要があります
- [Batch.3] バッチコンピューティング環境にはタグを付ける必要があります
- [Batch.4] マネージドバッチコンピューティング環境のコンピューティングリソースプロパティにはタグを付ける必要があります
- [CloudFront.1] CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります
- [CloudFront.3] CloudFront ディストリビューションでは、転送中に暗号化が必要となります
- [CloudFront.4] CloudFront ディストリビューションでは、オリジンフェイルオーバーが設定されている必要があります
- [CloudFront.5] CloudFront ディストリビューションでは、ログ記録を有効にする必要があります
- [CloudFront.6] CloudFront ディストリビューションでは、WAF を有効にする必要があります
- [CloudFront.7] CloudFront ディストリビューションでは、カスタム SSL/TLS 証明書を使用する必要があります
- [CloudFront.8] CloudFront ディストリビューションでは、SNI を使用して HTTPS リクエストを処理する必要があります
- [CloudFront.9] CloudFront ディストリビューションでは、カスタムオリジンへのトラフィックを暗号化する必要があります
- [CloudFront.10] CloudFront ディストリビューションは、エッジロケーションとカスタムオリジン間に非推奨の SSL プロトコルを使用しないでください
- [CloudFront.12] CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります
- [CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります
- [CloudFront.14] CloudFront ディストリビューションにはタグを付ける必要があります
- [CloudFront.15] CloudFront ディストリビューションは、推奨される TLS セキュリティポリシーを使用する必要があります
- [CloudWatch.17] CloudWatch アラームアクションをアクティブにする必要があります
- [CodeArtifact.1] CodeArtifact リポジトリにはタグを付ける必要があります
- [CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります
- [CodeBuild.4] CodeBuild AWS Configプロジェクト環境には口グ記録設定が必要です
- [CodeGuruProfiler.1] CodeGuru Profiler プロファイリンググループにはタグを付ける必要があります

- [CodeGuruReviewer.1] CodeGuru Reviewer リポジトリの関連付けにはタグを付ける必要があります
- [Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります
- [Connect.1] Amazon Connect Customer Profiles オブジェクトタイプにはタグを付ける必要があります
- [DataSync.2] DataSync タスクにはタグを付ける必要があります
- [DMS.2] DMS 証明書にはタグを付ける必要があります
- [DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。
- [DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。
- [DMS.9] DMS エンドポイントは SSL を使用する必要があります。
- [DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります
- [DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です
- [DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません
- [DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります
- [DynamoDB.3] DynamoDB Accelerator (DAX) クラスターは、保管中に暗号化する必要があります
- [DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります
- [EC2.21] ネットワーク ACL は、0.0.0.0/0 からポート 22、またはポート 3389 への侵入を許可しないようにする必要があります
- [EC2.22] 未使用の Amazon EC2 セキュリティグループを削除することをお勧めします
- [EC2.23] Amazon EC2 Transit Gateway が VPC アタッチメントリクエストを自動的に受け付けないようにすることをお勧めします
- [EC2.24] Amazon EC2 準仮想化インスタンスタイプを使用しないことをお勧めします
- [EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします

- [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします
- [EC2.38] EC2 インスタンスにはタグを付ける必要があります
- [EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります
- [EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります
- [EC2.170] EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします
- [EC2.173] 起動パラメータを持つ EC2 スポットフリートリクエストは、アタッチされた EBS ボリュームの暗号化を有効にする必要があります
- [EC2.174] EC2 DHCP オプションセットにはタグを付ける必要があります
- [EC2.175] EC2 起動テンプレートにはタグを付ける必要があります
- [EC2.176] EC2 プレフィックスリストにはタグを付ける必要があります
- [EC2.177] EC2 トラフィックミラーセッションにはタグを付ける必要があります
- [EC2.178] EC2 トラフィックミラーフィルターにはタグを付ける必要があります
- [EC2.179] EC2 トラフィックミラーターゲットにはタグを付ける必要があります
- [ECR.1] ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります
- [ECR.2] ECR プライベートリポジトリでは、タグのイミュータビリティが設定されている必要があります
- [ECR.3] ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーが設定されている必要があります
- [ECR.4] ECR パブリックリポジトリにはタグを付ける必要があります
- [ECS.3] ECS タスクの定義では、ホストのプロセス名前空間を共有しないでください
- [ECS.4] ECS コンテナは、非特権として実行する必要があります
- [ECS.5] ECS コンテナは、ルートファイルシステムへの読み取り専用アクセスに制限する必要があります。
- [ECS.8] シークレットは、コンテナ環境の変数として渡さないでください
- [ECS.9] ECS タスク定義には ログ設定が必要です。
- [ECS.10] ECS Fargate サービスは、最新の Fargate プラットフォームバージョンで実行する必要があります。

- [ECS.12] ECS クラスターはコンテナインサイトを使用する必要があります
- [EFS.3] EFS アクセスポイントは、ルートディレクトリを適用する必要があります
- [EFS.4] EFS アクセスポイントは、ユーザー ID を適用する必要があります
- [EKS.2] EKS クラスターは、サポートされている Kubernetes バージョンで実行する必要があります。
- [EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります
- [ELB.10] Classic Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.12] Application Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで構成する必要があります
- [ELB.13] Application、Network、Gateway Load Balancer は、複数のアベイラビリティーゾーンにまたがっている必要があります
- [ELB.14] Classic Load Balancer は、防御モードまたは最も厳密な非同期緩和モードで設定する必要があります
- [ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります
- [ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります
- [ElastiCache.2] ElastiCache クラスターでは、マイナーバージョンの自動アップグレードを有効にする必要があります
- [ElastiCache.3] ElastiCache (Redis OSS) レプリケーショングループでは、自動フェイルオーバーを有効にする必要があります
- [ElastiCache.4] ElastiCache レプリケーショングループは保管中に暗号化する必要があります
- [ElastiCache.5] ElastiCache レプリケーショングループは転送時に暗号化する必要があります
- [ElastiCache.6] 以前のバージョンの ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります
- [ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください
- [ElasticBeanstalk.1] Elastic Beanstalk 環境では、拡張ヘルスレポートを有効にする必要があります。
- [ElasticBeanstalk.2] Elastic Beanstalk のマネージドプラットフォームの更新を有効にする必要があります
- [ElasticBeanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります

- [EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります
- [EMR.3] Amazon EMR セキュリティ設定は保管時に暗号化する必要があります
- [EMR.4] Amazon EMR セキュリティ設定は転送中に暗号化する必要があります
- [ES.4] CloudWatch Logs への Elasticsearch ドメインエラーログ記録を有効にする必要があります
- [EventBridge.3] Amazon EventBridge カスタムイベントバスにリソースポリシーがアタッチされている必要があります
- [EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります
- [FraudDetector.1] Amazon Fraud Detector エンティティタイプにはタグを付ける必要があります
- [FraudDetector.2] Amazon Fraud Detector ラベルにはタグを付ける必要があります
- [FraudDetector.3] Amazon Fraud Detector の結果にはタグを付ける必要があります
- [FraudDetector.4] Amazon Fraud Detector 変数にはタグを付ける必要があります
- [FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります
- [FSx.2] FSx for Lustre ファイルシステムでは、タグをバックアップにコピーするように設定する必要があります
- [GlobalAccelerator.1] Global Accelerator アクセラレーターにはタグを付ける必要があります
- [GuardDuty.7] GuardDuty EKS ランタイムモニタリングを有効にする必要があります
- [GuardDuty.8] GuardDuty Malware Protection for EC2 を有効にする必要があります
- [GuardDuty.9] GuardDuty RDS Protection を有効にする必要があります
- [GuardDuty.11] GuardDuty Runtime Monitoring を有効にする必要があります
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring を有効にする必要があります
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring を有効にする必要があります
- [IAM.6] ルートユーザーに対してハードウェア MFA を有効にする必要があります
- [IAM.9] ルートユーザーに対して MFA を有効にする必要があります
- [IAM.21] 作成する IAM カスタマーマネージドポリシーにはサービスのワイルドカードアクションを許可してはいけません
- [IAM.24] IAM ロールにはタグを付ける必要があります
- [IAM.25] IAM ユーザーにはタグを付ける必要があります
- [IAM.28] IAM Access Analyzer 外部アクセスアナライザーを有効にする必要があります
- [Inspector.3] Amazon Inspector Lambda コードスキャンを有効にする必要があります

- [IoTEvents.1] AWS IoT Events 入力にはタグを付ける必要があります
- [IoTEvents.2] AWS IoT Events ディテクターモデルにはタグを付ける必要があります
- [IoTEvents.3] AWS IoT Events アラームモデルにはタグを付ける必要があります
- [IoTSiteWise.1] AWS IoT SiteWise アセットモデルにはタグを付ける必要があります
- [IoTSiteWise.2] AWS IoT SiteWise ダッシュボードにはタグを付ける必要があります
- [IoTSiteWise.3] AWS IoT SiteWise ゲートウェイにはタグを付ける必要があります
- [IoTSiteWise.4] AWS IoT SiteWise ポータルにはタグを付ける必要があります
- [IoTSiteWise.5] AWS IoT SiteWise プロジェクトにはタグを付ける必要があります
- [IoTTwinMaker.1] AWS IoT TwinMaker 同期ジョブにはタグを付ける必要があります
- [IoTTwinMaker.2] AWS IoT TwinMaker ワークスペースにはタグを付ける必要があります
- [IoTTwinMaker.3] AWS IoT TwinMaker シーンにはタグを付ける必要があります
- [IoTTwinMaker.4] AWS IoT TwinMaker エンティティにはタグを付ける必要があります
- [IoTWireless.1] AWS IoT Wireless マルチキャストグループにはタグを付ける必要があります
- [IoTWireless.2] AWS IoT Wireless サービスプロファイルにはタグを付ける必要があります
- [IoTWireless.3] AWS IoT FUOTA タスクにはタグを付ける必要があります
- [IVS.1] IVS 再生キーペアにはタグを付ける必要があります
- [IVS.2] IVS 記録設定にはタグを付ける必要があります
- [IVS.3] IVS チャネルにはタグを付ける必要があります
- [Keyspaces.1] Amazon Keyspaces キースペースにはタグを付ける必要があります
- [Kinesis.1] Kinesis ストリームは、保管中に暗号化する必要があります
- [KMS.5] KMS キーはパブリックにアクセスしないでください
- [Lambda.5] VPC Lambda 関数は複数のアベイラビリティーゾーンで運用する必要があります
- [Macie.1] Amazon Macie を有効にする必要があります
- [Macie.2] Macie 機密データ自動検出を有効にする必要があります
- [MQ.3] Amazon MQ ブローカーでは、自動マイナーバージョンアップグレードが有効になっている必要があります
- [MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります
- [MQ.6] RabbitMQ ブローカーはクラスターデプロイメントモードを使用する必要があります。
- [MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります

- [MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります
- [MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります
- [MSK.5] MSK コネクタではログ記録が有効になっている必要があります
- [Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります
- [Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください
- [Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります
- [Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります
- [Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります
- [Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります
- [Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります
- [Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.1] Network Firewall ファイアウォールを複数のアベイラビリティーゾーンにデプロイする必要があります
- [NetworkFirewall.2] Network Firewall ログ記録を有効にする必要があります
- [Network Firewall.3] Network Firewall ポリシーには、1 つ以上のルールグループが関連付けられている必要があります
- [NetworkFirewall.4] Network Firewall ポリシーのデフォルトのステートレスアクションは、完全なパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.5] Network Firewall ポリシーのデフォルトのステートレスアクションは、断片化されたパケットに対してドロップまたは転送される必要があります。
- [NetworkFirewall.6] ステートレス Network Firewall のルールグループを空にしないでください
- [NetworkFirewall.9] Network Firewall は削除保護を有効にする必要があります
- [Opensearch.1] OpenSearch ドメインは保管中の暗号化を有効にする必要があります
- [Opensearch.2] OpenSearch ドメインがパブリックにアクセスできないようにする必要があります
- [Opensearch.3] OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります
- [Opensearch.4] CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります

- [Opensearch.5] OpenSearch ドメインでは、監査ログ記録を有効にする必要があります
- [Opensearch.6] OpenSearch ドメインには少なくとも 3 つのデータノードが必要です
- [Opensearch.7] OpenSearch ドメインは、きめ細かなアクセスコントロールを有効にする必要があります
- [Opensearch.8] OpenSearch ドメインへの接続は最新の TLS セキュリティポリシーを使用して暗号化する必要があります
- [PCA.1] AWS Private CA ルート認証機関を無効にする必要があります
- [PCA.2] AWS プライベート CA 認証機関にはタグを付ける必要があります
- [RDS.14] Amazon Aurora クラスターはバックトラッキングを有効にする必要があります
- [RDS.15] RDS DB クラスターを複数のアベイラビリティーゾーンに対して設定する必要があります
- [RDS.24] RDS データベースクラスターはカスタム管理者ユーザー名を使用する必要があります
- [RDS.25] RDS データベースインスタンスはカスタム管理者ユーザーネームを使用する必要があります
- [RDS.27] RDS DB クラスターは保管中に暗号化する必要があります
- [RDS.34] Aurora MySQL DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります
- [RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります
- [RDS.45] Aurora MySQL DB クラスターでは、監査ログ記録を有効にする必要があります
- [Redshift.7] Redshift クラスターは拡張 VPC ルーティングを使用する必要があります
- [Redshift.8] Amazon Redshift クラスターはデフォルトの管理者ユーザーネームを使用しないでください
- [Redshift.9] Redshift クラスターでは、デフォルトのデータベース名を使用しないでください
- [Redshift.10] Redshift クラスターは保存時に暗号化する必要があります
- [Redshift.11] Redshift クラスターにはタグを付ける必要があります
- [Redshift.13] Redshift クラスタースナップショットにはタグを付ける必要があります
- [Redshift.17] Redshift クラスターパラメータグループにはタグを付ける必要があります
- [RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります
- [RedshiftServerless.2] SSL を使用するには、Redshift Serverless ワークグループへの接続が必要です

- [RedshiftServerless.3] Redshift Serverless ワークグループはパブリックアクセスを禁止する必要があります
- [RedshiftServerless.6] Redshift Serverless 名前空間は CloudWatch Logs にログをエクスポートする必要があります
- [Route53.1] Route 53 ヘルスチェックにはタグを付ける必要があります
- [Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります
- [S3.10] バージョニングが有効になっている S3 汎用バケットにはライフサイクル設定が必要です
- [S3.11] S3 汎用バケットでは、イベント通知を有効にする必要があります
- [S3.12] ACL は、S3 汎用バケットへのユーザーアクセスの管理に使用しないでください。
- [S3.13] S3 汎用バケットにはライフサイクル設定が必要です
- [S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります
- [S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります
- [S3.25] S3 ディレクトリバケットにはライフサイクル設定が必要です
- [SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります
- [SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません
- [SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります
- [SageMaker.6] SageMaker アプリのイメージ設定にはタグを付ける必要があります
- [SageMaker.7] SageMaker イメージにはタグを付ける必要があります
- [SNS.4] SNS トピックアクセスポリシーはパブリックアクセスを許可しないでください
- [SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください
- [SSM.4] SSM ドキュメントはパブリックにしないでください
- [SSM.5] SSM ドキュメントにはタグを付ける必要があります
- [StepFunctions.1] Step Functions ステートマシンではログ記録がオンになっている必要があります
- [StepFunctions.2] Step Functions アクティビティにはタグを付ける必要があります
- [Transfer.4] Transfer Family 契約にはタグを付ける必要があります
- [Transfer.5] Transfer Family 証明書にはタグを付ける必要があります
- [Transfer.6] Transfer Family コネクタにはタグを付ける必要があります
- [Transfer.7] Transfer Family プロファイルにはタグを付ける必要があります
- [WAF.1] AWS WAF Classic Global Web ACL ログ記録を有効にする必要があります

- [WAF.2] AWS WAF Classic リージョンルールには少なくとも 1 つの条件が必要です
- [WAF.3] AWS WAF Classic リージョンルールグループには少なくとも 1 つのルールが必要です
- [WAF.4] AWS WAF Classic Regional Web ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.6] AWS WAF Classic グローバルルールには少なくとも 1 つの条件が必要です
- [WAF.7] AWS WAF Classic グローバルルールグループには少なくとも 1 つのルールが必要です
- [WAF.8] AWS WAF Classic グローバルウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です
- [WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります

CloudFormation を使用した Security Hub CSPM リソースの作成

AWS Security Hub CSPM は と統合されています。これは AWS CloudFormation、 AWS リソースとインフラストラクチャの作成と管理に費やす時間を短縮できるように、リソースのモデル化とセットアップに役立つサービスです。必要なすべての AWS リソース (オートメーションルールなど) を記述するテンプレートを作成し、それらのリソースを AWS CloudFormation プロビジョニングして設定します。

を使用すると AWS CloudFormation、テンプレートを再利用して Security Hub CSPM リソースを一貫して繰り返しセットアップできます。リソースを 1 回記述し、複数の AWS アカウント およびリージョンで同じリソースを何度もプロビジョニングします。

Security Hub CSPM と AWS CloudFormation テンプレート

Security Hub CSPM および関連サービスのリソースをプロビジョニングおよび設定するには、AWS CloudFormation テンプレートの仕組みを理解する必要があります。テンプレートは、JSON または YAML 形式のテキストファイルです。これらのテンプレートは、 AWS CloudFormation スタックでプロビジョニングするリソースを記述します。

JSON または YAML に慣れていない場合は、 AWS CloudFormation Designer を使用して AWS CloudFormation テンプレートの使用を開始できます。詳細については、 AWS CloudFormation ユーザーガイドのAWS CloudFormation 「デザイナーとは」を参照してください。

次のタイプの Security Hub CSPM リソースの AWS CloudFormation テンプレートを作成できます。

- Security Hub CSPM の有効化
- 組織の委任 Security Hub CSPM 管理者の指定
- Security Hub CSPM で組織を設定する方法を指定する
- セキュリティ標準の有効化
- クロスリージョン集約の有効化
- 中央設定ポリシーを作成し、アカウント、組織単位 (OU)、またはルートに関連付ける
- カスタムインサイトの作成
- 自動化ルールの作成
- コントロールパラメータのカスタマイズ
- サードパーティー製品統合のサブスクライブ

リソースの JSON テンプレートと YAML テンプレートの例を含む詳細については、AWS CloudFormation 「 ユーザーガイド」のAWS 「Security Hub CSPM リソースタイプのリファレンス」を参照してください。

の詳細 AWS CloudFormation

詳細については AWS CloudFormation、次のリソースを参照してください。

- AWS CloudFormation
- AWS CloudFormation ユーザーガイド
- AWS CloudFormation API リファレンス
- AWS CloudFormation コマンドラインインターフェイスユーザーガイド

Amazon SNS で Security Hub CSPM の発表をサブスクライブする

このセクションでは、 AWS Security Hub CSPM に関する通知を受信するために、Amazon Simple Notification Service (Amazon SNS) を使用して Security Hub CSPM の発表をサブスクライブする方法について説明します。

サブスクライブした後、次のイベントに関する通知を受信するようになります (各イベントに対応する `AnnouncementType` を以下に示します)。

- `GENERAL` – Security Hub CSPM サービスに関する一般的な通知。

- `UPCOMING_STANDARDS_CONTROLS` – 指定された Security Hub CSPM コントロールまたは標準が間もなくリリースされます。このタイプの発表は、リリースに先立って対応と修正のワークフローを準備するのに役立ちます。
- `NEW_REGIONS` – Security Hub CSPM のサポートは、新しい で利用できます AWS リージョン。
- `NEW_STANDARDS_CONTROLS` – 新しい Security Hub CSPM コントロールまたは標準が追加されました。
- `UPDATED_STANDARDS_CONTROLS` – 既存の Security Hub CSPM コントロールまたは標準が更新されました。
- `RETIRED_STANDARDS_CONTROLS` – 既存の Security Hub CSPM コントロールまたは標準が廃止されました。
- `UPDATED_ASFF` – AWS Security Finding Format (ASFF) の構文、フィールド、または値が更新されました。
- `NEW_INTEGRATION` – 他の AWS サービスまたはサードパーティー製品との新しい統合が利用可能になりました。
- `NEW_FEATURE` – 新しい Security Hub CSPM 機能が利用可能になりました。
- `UPDATED_FEATURE` – 既存の Security Hub CSPM 機能が更新されました。

Amazon SNS がサポートするすべての形式で通知を使用できます。Security Hub CSPM の発表は、Security AWS リージョン Hub CSPM が利用可能なすべての でサブスクライブできます。

Amazon SNS トピックにサブスクライブするには、ユーザーは、`Subscribe` 許可が必要です。これは、Amazon SNS ポリシー、IAM ポリシー、またはその両方で実現できます。詳細については、「IAM and Amazon SNS policies together」(IAM と Amazon SNS のポリシーを一緒に) の「Amazon Simple 通知サービス デベロッパーガイド」を参照してください。

> **Note**
>
> Security Hub CSPM は、Security Hub CSPM サービスの更新に関する Amazon SNS 発表を、サブスクライブしている に送信します AWS アカウント。Security Hub CSPM の検出結果に関する通知を受け取るには、「」を参照してくださいSecurity Hub CSPM での検出結果の詳細と履歴の確認。

Amazon SNS トピックについて Amazon Simple Queue Service (Amazon SQS) キューをサブスクライブできますが、同じリージョンにある Amazon SNS トピックの Amazon リソースネーム (ARN)

を使用する必要があります。詳細については、Amazon SNSトピックへのキューのサブスクライブ」を参照してください。

AWS Lambda 関数を使用して、通知を受信したときにイベントを呼び出すこともできます。サンプル関数コードを含む詳細については、「 AWS Lambda デベロッパーガイド」の「チュートリアル: Amazon Simple Notification Service AWS Lambda での の使用」を参照してください。

各リージョンの Amazon SNS トピックの ARN は次のとおりです。

AWS リージョン	Amazon SNS トピックの ARN
米国東部(オハイオ)	`arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements`
米国東部 (バージニア北部)	`arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements`
米国西部 (北カリフォルニア)	`arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements`
米国西部 (オレゴン)	`arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`
アフリカ (ケープタウン)	`arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements`
アジアパシフィック (香港)	`arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements`
アジアパシフィック (ハイデラバード)	`arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements`

AWS リージョン	Amazon SNS トピックの ARN
アジアパシフィック (ジャカルタ)	arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements
アジアパシフィック (ムンバイ)	arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements
アジアパシフィック (大阪)	arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements
アジアパシフィック (ソウル)	arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements
アジアパシフィック (シンガポール)	arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements
アジアパシフィック (シドニー)	arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements
アジアパシフィック (東京)	arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements
カナダ (中部)	arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements
中国 (北京)	arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements

AWS リージョン	Amazon SNS トピックの ARN
中国 (寧夏)	arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements
欧州 (フランクフルト)	arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements
欧州 (アイルランド)	arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements
欧州 (ロンドン)	arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements
欧州 (ミラノ)	arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements
欧州 (パリ)	arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements
欧州 (スペイン)	arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements
欧州 (ストックホルム)	arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements
欧州 (チューリッヒ)	arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements

AWS リージョン	Amazon SNS トピックの ARN
イスラエル (テルアビブ)	`arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements`
中東 (バーレーン)	`arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements`
中東 (アラブ首長国連邦)	`arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements`
南米 (サンパウロ)	`arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements`
AWS GovCloud (米国東部)	`arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements`
AWS GovCloud (米国西部)	`arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements`

メッセージは通常、パーティション内のリージョン間で同じであるため、各パーティションの 1 つのリージョンにサブスクライブすれば、そのパーティションのすべてのリージョンに影響する発表を受け取ることができます。メンバーアカウントに関連する発表は、管理者アカウントではレプリケートされません。その結果、管理者アカウントを含む各アカウントには、各発表のコピーが 1 つだけ存在することになります。Security Hub CSPM 発表のサブスクライブに使用するアカウントを決定できます。

Security Hub CSPM の発表をサブスクライブするコストについては、Amazon SNS料金」を参照してください。

Security Hub CSPM の発表をサブスクライブする (コンソール)

1. Amazon SNS コンソールのhttps://console.aws.amazon.com/sns/v3/homeを開いてください。
2. リージョンリストで、Security Hub CSPM の発表をサブスクライブするリージョンを選択します。この例では、`us-west-2` リージョンを使用します。
3. ナビゲーションペインで、[Subscriptions] (サブスクリプション) を選択して、[Create subscription] (サブスクリプションの作成) を選択します。
4. [Topic ARN] (トピック ARN) ボックスにトピック ARN を入力します。例えば、`arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`。
5. Protocol で、Security Hub CSPM のお知らせを受け取る方法を選択します。[Email] (E メール) を選択した場合、[Endpoint] (エンドポイント) で、発表の受信に使用する E メールアドレスを入力します。
6. [Create subscription] を選択してください。
7. サブスクリプションを確認します。例えば、E メールプロトコルを選択した場合、指定した E メールに Amazon SNS からサブスクリプションの確認メッセージが送信されます。

Security Hub CSPM の発表をサブスクライブする (AWS CLI)

1. 次のコマンドを実行してください。

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. サブスクリプションを確認します。例えば、E メールプロトコルを選択した場合、指定した E メールに Amazon SNS からサブスクリプションの確認メッセージが送信されます。

Amazon SNS メッセージ形式

次の例は、新しいセキュリティコントロールの導入に関する Amazon SNS からの Security Hub CSPM の発表を示しています。メッセージの内容は発表のタイプによって異なりますが、形式はすべての発表タイプで同じです。オプションで、発表に関する詳細を指定する `Link` フィールドを含めることができます。

例: 新しいコントロールに関する Security Hub CSPM の発表 (E メールプロトコル)

```
{
```

```
"AnnouncementType":"NEW_STANDARDS_CONTROLS",
"Title":"[New Controls] 36 new Security Hub CSPM controls added to the AWS Foundational
 Security Best Practices standard",
"Description":"We have added 36 new controls to the AWS Foundational Security Best
 Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3,
 AutoScaling.4, AutoScaling.6), AWS CloudFormation (CloudFormation.1), Amazon
 CloudFront (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23,
 EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon
 Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12),
 Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes
 Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon
 Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3, NetworkFirewall.4,
 NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift
 (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
 (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
 Foundational Security Best Practices standard in an account and configured Security
 Hub CSPM to automatically enable new controls, these controls are enabled by default.
 Availability of controls can vary by Region. "
}
```

例: 新しいコントロールに対する Security Hub CSPM の発表 (email-JSON プロトコル)

```
{
  "Type" : "Notification",
  "MessageId" : "d124c9cf-326a-5931-9263-92a92e7af49f",
  "TopicArn" : "arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements",
  "Message" : "{\"AnnouncementType\":\"NEW_STANDARDS_CONTROLS\",\"Title\":\"[New
 Controls] 36 new Security Hub CSPM controls added to the AWS Foundational Security
 Best Practices standard\",\"Description\":\"We have added 36 new controls to the
 AWS Foundational Security Best Practices standard. These include controls for Amazon
 Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), AWS CloudFormation
 (CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud
 (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR)
 (ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5,
 ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon
 Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12,
 ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3,
 NetworkFirewall.4, NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7),
 Amazon Redshift (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
 (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
 Foundational Security Best Practices standard in an account and configured SSecurity
```

```
 Hub CSPM to automatically enable new controls, these controls are enabled by default.
 Availability of controls can vary by Region. \"}",
  "Timestamp" : "2022-08-04T19:11:12.652Z",
  "SignatureVersion" : "1",
  "Signature" :
 "HTHgNFRYMetCvisulgLM4CVySvK9qCXFPHQDxYl9tuCFQuIrd7YO4m4YFR28XKMgzqrF20YP
+EilipUm2SOTpEEtOTekU5bn74+YmNZfwr4aPFx0vUuQCVOshmHl37hjkiLjhCg/t53QQiLfP7MH
+MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUsOG8yiJVCBEJhJ1yS
+gkwJdhRk2UQab9RcAmE6COK3hRWcjDwqTXz5nR6Ywv1ZqZfLIl7gYKslt+jsyd/k+7kOqGmOJRDr7qhE7H
+7vaGRLOptsQnbW8VmeYnDbahEO8FV+Mp1rpV+7Qg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-56e67fcb41f6fec09b0196692625d385.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements:9d0230d7-d582-451d-9f15-0c32818bf61f"
}
```


Security Hub CSPM の無効化

AWS Security Hub CSPM コンソールまたは Security Hub API を使用して、Security Hub CSPM を無効にすることができます。Security Hub CSPM を無効にすると、後で再度有効にできます。

組織が中央設定を使用している場合、委任 Security Hub CSPM 管理者は、特定のアカウントと組織単位 (OUs) に対して Security Hub CSPM を有効にしておくことができます。設定ポリシーは、ホームリージョンとリンクされたすべてのリージョンに影響します。詳細については、「Security Hub CSPM の中央設定について」を参照してください。

アカウントの Security Hub CSPM を無効にすると、以下が発生します。

- アカウントでは、すべての Security Hub CSPM 標準とコントロールが無効になっています。
- Security Hub CSPM は、アカウントの結果の生成、更新、取り込みを停止します。
- 30 日後、Security Hub CSPM はアカウントの既存のアーカイブされた検出結果をすべて完全に削除します。Security Hub CSPM を使用して検出結果を復元することはできません。
- 90 日後、Security Hub CSPM はアカウントの既存のアクティブな検出結果をすべて完全に削除します。Security Hub CSPM を使用して検出結果を復元することはできません。
- 90 日後、Security Hub CSPM はアカウントの既存のインサイトと Security Hub CSPM 設定をすべて完全に削除します。データおよび設定は復元できません。

既存の検出結果を保持するには、Security Hub CSPM を無効にする前に、検出結果を S3 バケットにエクスポートできます。これを行うには、Amazon EventBridge ルールでカスタムアクションを使用します。詳細については、「EventBridge を使用した自動応答と修復」を参照してください。

アカウントの Security Hub CSPM を無効にしてから 90 日以内に再度有効にすると、既存のアクティブな検出結果、およびアカウントのインサイトと Security Hub CSPM 設定へのアクセスが回復します。30 日以内に Security Hub CSPM を再度有効にすると、アカウントの既存のアーカイブされた検出結果へのアクセスも回復します。ただし、Security Hub CSPM を無効にすると AWS 環境の状態が反映されるため、既存の検出結果は不正確になる可能性があります。さらに、個々の標準とコントロールを再度有効にすると、Security Hub CSPM は、有効にする標準とコントロールに応じて、最初に特定の AWS リソースに対して重複した検出結果を生成することがあります。このような理由から、次のいずれかを実行することをお勧めします。

- Security Hub CSPM を無効にするRESOLVED前に、既存のすべての検出結果のワークフローステータスを に変更します。詳細については、「結果のワークフローステータスを設定する」を参照してください。
- Security Hub CSPM を無効にする少なくとも 6 日前に、すべての標準を無効にします。その後、Security Hub CSPM は、すべての既存の検出結果をベストエフォートベースでアーカイブします。通常は 3~5 日以内にアーカイブします。詳細については、「セキュリティ標準の無効化」を参照してください。

以下の場合、Security Hub CSPM を無効にすることはできません。

- アカウントは、組織の委任 Security Hub CSPM 管理者アカウントです。中央設定を使用する場合、委任管理者アカウントの Security Hub CSPM を無効にする設定ポリシーを関連付けることはできません。関連付けは他のアカウントで成功できますが、Security Hub CSPM は委任管理者アカウントにポリシーを適用しません。
- アカウントは招待による Security Hub CSPM 管理者アカウントであり、メンバーアカウントがあります。Security Hub CSPM を無効にする前に、すべてのメンバーアカウントの関連付けを解除する必要があります。この方法の詳細は、「the section called “メンバーアカウントの関連付けを解除する”」を参照してください。

メンバーアカウントの所有者が Security Hub CSPM を無効にするには、アカウントと管理者アカウントの関連付けを解除する必要があります。組織アカウントでは、管理者アカウントのみがメンバーアカウントの関連付けを解除できます。詳細については、「the section called “組織メンバーアカウントの関連付けを解除する”」を参照してください。手動で招待されたアカウントの場合、管理者アカウントまたはメンバーアカウントのいずれかがアカウントの関連付けを解除できます。詳細につい

ては、the section called “メンバーアカウントの関連付けを解除する”またはthe section called “管理者アカウントから関連付けを解除する”を参照してください。Security Hub CSPM 管理者は特定のメンバーアカウントの Security Hub CSPM を無効にするポリシーを作成できるため、中央設定を使用する場合、関連付けを解除する必要はありません。

アカウントの Security Hub CSPM を無効にすると、現在の でのみ無効になります AWS リージョン。ただし、中央設定を使用して特定のアカウントの Security Hub CSPM を無効にすると、ホームリージョンとリンクされたすべてのリージョンで無効になります。

Security Hub CSPM を無効にするには、任意の方法を選択し、ステップに従います。

Security Hub CSPM console

コンソールを使用して Security Hub CSPM を無効にするには、次の手順に従います。

Security Hub CSPM を無効にするには

1. https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. ナビゲーションペインで [Settings] の [General] を選択します。
3. Security Hub CSPM の無効化セクションで、Security Hub CSPM の無効化を選択します。
4. 確認を求められたら、Security Hub CSPM を無効にするを選択します。

Security Hub API

Security Hub CSPM をプログラムで無効にするには、 AWS Security Hub API の DisableSecurityHub オペレーションを使用します。または、 を使用している場合は AWS CLI、disable-security-hub コマンドを実行します。たとえば、次のコマンドは、現在の で Security Hub CSPM を無効にします AWS リージョン。

```
$ aws securityhub disable-security-hub
```

のセキュリティ AWS Security Hub

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを活用できます。

セキュリティは、 AWS お客様とお客様の間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ – クラウドで AWS AWS サービスを実行するインフラストラクチャを保護する AWS 責任があります。 AWS また、 では、安全に使用できるサービスも提供しています。「AWS 」 コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。「 AWS Security Hub」 に適用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラムによる対象範囲内の「AWS 」 のサービス」を参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、ユーザーは、データの機密性、企業要件、および適用法令と規制などのその他要因に対する責任も担います。

このドキュメントは、Security Hub を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために Security Hub を設定する方法を説明します。また、Security Hub リソースのモニタリングと保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- でのデータ保護 AWS Security Hub
- AWS Security Hub の Identity and Access Management
- のコンプライアンス検証 AWS Security Hub
- AWS Security Hub の耐障害性
- のインフラストラクチャセキュリティ AWS Security Hub
- AWS Security Hub およびインターフェイス VPC エンドポイント (AWS PrivateLink)

でのデータ保護 AWS Security Hub

責任 AWS 共有モデル、 でのデータ保護に適用されます AWS Security Hub。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があ

ります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、データプライバシーに関するよくある質問を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された AWS 責任共有モデルおよび GDPR のブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、または SDK を使用して Security Hub AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

Security Hub はマルチテナント型サービスを提供します。データ保護を確実に行うために、Security Hub は保管中のデータとコンポーネントサービス間で転送中のデータを暗号化します。

AWS Security Hub の Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰を認可する (Security Hub リソースの使用を許可する) かを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- Security Hub と IAM の連携方法
- AWS Security Hubのアイデンティティベースのポリシーの例
- のサービスにリンクされたロール AWS Security Hub
- AWS Security Hub の マネージドポリシー
- AWS Security Hub ID とアクセスのトラブルシューティング

対象者

AWS Identity and Access Management (IAM) の使用方法は、Security Hub で行う作業によって異なります。

サービスユーザー - ユーザーがジョブを実行するために Security Hub サービスを使用する場合は、管理者から必要な認証情報と許可がそのユーザーに提供されます。作業を行うためにさらに多くの Security Hub の機能を使用する場合、追加の許可が必要になる可能性があります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。Security Hub の機能にアクセスできない場合は、「AWS Security Hub ID とアクセスのトラブルシューティング」を参照してください。

サービス管理者 - お客様が社内の Security Hub リソースを担当している場合は、通常 Security Hub に完全にアクセスすることができます。サービスユーザーがどの Security Hub 機能およびリソースにアクセスする必要があるかを決定するのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を確認して、IAM の基本概念を理解してください。お客様の会社で Security Hub で IAM を利用する方法の詳細については、「Security Hub と IAM の連携方法」を参照してください。

IAM 管理者 - IAM 管理者は、Security Hub へのアクセスを管理するポリシーの作成方法を詳しく確認する必要がある場合があります。IAM で使用できる Security Hub のアイデンティティベースのポリシーの例を表示するには、「AWS Security Hubのアイデンティティベースのポリシーの例」を参照してください。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けることによって、認証 (にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook 認証情報は、フェデレーション ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーの種類に応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 AWS サインイン ユーザーガイド」の「 へのサインイン AWS アカウント方法」を参照してください。

AWS プログラムで にアクセスする場合、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストを暗号化して署名します。AWS ツールを使用しない場合は、自分でリクエストに署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。たとえば、 では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用する AWS ことをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「IAM のAWS 多要素認証」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強く

お勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、ID プロバイダーとのフェデレーションを使用して一時的な認証情報 AWS のサービス を使用して にアクセスすることを要求します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、、AWS Directory Serviceアイデンティティセンターディレクトリ、または ID ソースを介して提供された認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID がにアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成するか、独自の ID ソースのユーザーとグループのセットに接続して同期し、すべての AWS アカウント とアプリケーションで使用できます。IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内の ID です。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユー

ザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内の ID です。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。で IAM ロールを一時的に引き受けるには AWS Management Console、ユーザーから IAM ロール (コンソール) に切り替えることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールについては、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。
- クロスサービスアクセス – 一部の は他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。

- 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用してアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする と組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
- サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」を参照してください。
- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 インスタンスに AWS ロールを割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメ

ント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プ

リンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、および Amazon VPC は AWS WAF、ACLs。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的でない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) の最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、ビジネスが所有する複数の をグループ化して一元管理するためのサービス AWS アカウント です。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。
- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定する

ために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースのアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。RCP をサポートする のリストを含む Organizations と RCP の詳細については、AWS Organizations RCPs「リソースコントロールポリシー (RCPs」を参照してください。 AWS のサービス

- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

Security Hub と IAM の連携方法

AWS Identity and Access Management (IAM) を使用して へのアクセスを管理する前に AWS Security Hub、Security Hub で使用できる IAM 機能を確認してください。

で使用できる IAM 機能 AWS Security Hub

IAM の機能	Security Hub のサポート
アイデンティティベースポリシー	はい
リソースベースのポリシー	いいえ
ポリシーアクション	はい
ポリシーリソース	いいえ
ポリシー条件キー	あり
アクセスコントロールリスト (ACL)	なし

IAM の機能	Security Hub のサポート
属性ベースのアクセス制御 (ABAC) – ポリシー内のタグ	あり
一時的な認証情報	あり
転送アクセスセッション (FAS)	あり
サービスロール	いいえ
サービスリンクロール	あり

Security Hub およびその他の がほとんどの IAM 機能と AWS のサービス 連携する方法の概要については、「IAM ユーザーガイド」のAWS のサービス 「IAM と連携する 」を参照してください。

Security Hub のアイデンティティベースのポリシー

ID ベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。ID ベースのポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

Security Hub は、アイデンティティベースのポリシーをサポートします。詳細については、「AWS Security Hubのアイデンティティベースのポリシーの例」を参照してください。

Security Hub のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「IAM ユーザーガイド」の「IAM でのクロスアカウントリソースアクセス」を参照してください。

Security Hub では、リソースベースのポリシーはサポートされていません。IAM ポリシーを Security Hub リソースに直接アタッチすることはできません。

Security Hub のポリシーアクション

ポリシーアクションのサポート:あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

Security Hub のポリシーアクションでは、アクションの前に次のプレフィックスが使用されます。

```
securityhub:
```

例えば、Security Hub API の `EnableSecurityHub` オペレーションに対応するアクションである Security Hub を有効にするアクセス許可をユーザーに付与するには、ポリシーに `securityhub:EnableSecurityHub` アクションを含めます。ポリシーステートメントには、`Action` または `NotAction` 要素を含める必要があります。Security Hub では、このサービスで実行できるタスクを記述する独自のアクションのセットを定義します。

```
"Action": "securityhub:EnableSecurityHub"
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。例:

```
"Action": [
      "securityhub:EnableSecurityHub",
      "securityhub:BatchEnableStandards"
```

ワイルドカード (*) を使用して複数のアクションを指定することもできます。例えば、`Get` という単語で始まるすべてのアクションを指定するには次のアクションを含めます。

```
"Action": "securityhub:Get*"
```

ただしベストプラクティスとして、最小特権 の原則に準拠したポリシーを作成してください。別の言い方をすると、特定タスクの実行にのみ必要とされる権限のみが含まれたポリシーを作成してください。

`BatchGetSecurityControls`、`BatchGetStandardsControlAssociations`、および `ListStandardsControlAssociations` にアクセスするには、ユーザーが `DescribeStandardsControl` オペレーションにアクセスできる必要があります。

`BatchUpdateStandardsControlAssociations` および `UpdateSecurityControl` にアクセスするには、ユーザーが `UpdateStandardsControls` オペレーションにアクセスできる必要があります。

Security Hub アクションのリストについては、「サービス認可リファレンス」の「AWS Security Hubで定義されるアクション」を参照してください。Security Hub アクションを指定するポリシーの例については、AWS Security Hubのアイデンティティベースのポリシーの例 を参照してください。

Security Hub のポリシーリソース

ポリシーリソースのサポート: なし

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

`Resource` JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ステートメントには`Resource` または `NotResource` 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

Security Hub は以下のリソースタイプを定義しています。

- [Hub] (ハブ)
- 製品
- クロスリージョンアグリゲーターとも呼ばれるアグリゲーターの検出
- 自動化ルール
- 設定ポリシー

ARN を使用して、ポリシーでこれらのタイプのリソースを指定できます。

Security Hub リソースタイプのリストとそれぞれの ARN 構文については、「サービス認可リファレンス」の「AWS Security Hubによって定義されたリソースタイプ」を参照してください。リソースタイプごとに指定できるアクションについては、「サービス認可リファレンス」の「AWS Security Hubで定義されるアクション」を参照してください。リソースを指定するポリシーの例については、AWS Security Hubのアイデンティティベースのポリシーの例を参照してください。

Security Hub のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「グローバル条件コンテキストキー」を参照してください。

Security Hub の条件キーのリストについては、「サービス認可リファレンス」の「AWS Security Hubの条件キー」を参照してください。どのアクションおよびリソースで条件キーを使用できるかについては、「AWS Security Hubで定義されるアクション」を参照してください。条件キーを使用するポリシーの例については、「AWS Security Hubのアイデンティティベースのポリシーの例」を参照してください。

Security Hub のアクセスコントロールリスト (ACL)

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Security Hub は ACL をサポートしていないため、Security Hub リソースに ACL をアタッチすることはできません。

Security Hub での属性ベースのアクセスコントロール (ABAC)

ABAC (ポリシー内のタグ) のサポート: あり

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。では AWS、これらの属性はタグと呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用する」を参照してください。

Security Hub リソースにタグをアタッチできます。ポリシーの `Condition` 要素にタグ情報を指定することで、リソースへのアクセスを制御することもできます。

Security Hub リソースのタグ付けの詳細については、 Security Hub リソースのタグ付け を参照してください。タグに基づいてリソースへのアクセスを制御するアイデンティティベースのポリシーの例については、AWS Security Hubのアイデンティティベースのポリシーの例をご参照ください。

Security Hub で一時的なセキュリティ認証情報を使用する

一時的な認証情報のサポート: あり

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報 AWS のサービス を使用する場合などの詳細については、IAM ユーザーガイドAWS のサービス の「IAM と連携する 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。たとえば、会社のシングルサインオン (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ユーザーから IAM ロールに切り替える (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用して アクセスできます AWS。長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成 AWS することをお勧めします。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

一時的な認証情報を使用して、フェデレーションでサインインする、IAM 役割を引き受ける、またはクロスアカウント役割を引き受けることができます。一時的なセキュリティ認証情報を取得するには、AssumeRole や GetFederationToken などの AWS STS API オペレーションを呼び出します。

Security Hub は、一時的な認証情報の使用をサポートしています。

Security Hub の転送アクセスセッション

転送アクセスセッション (FAS) のサポート: あり

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする と組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

例えば、Security Hub を と統合 AWS のサービス するとき、 AWS Organizations および Organizations 内の組織の委任 Security Hub 管理者アカウントを指定するときに、Security Hub はダウンストリームに FAS リクエストを実行します。

他のタスクでは、Security Hub は、サービスリンクロールを使用して、ユーザーに代わってアクションを実行します。このロールの詳細については、のサービスにリンクされたロール AWS Security Hubを参照してください。

Security Hub のサービスロール

Security Hub はサービスロールを引き受けたり使用したりしません。ユーザーに代わってアクションを実行するために、Security Hub はサービスリンクロールを使用します。このロールの詳細については、のサービスにリンクされたロール AWS Security Hubを参照してください。

> **Warning**
> サービスロールの権限を変更すると、Security Hub を使用する際に運用上の問題が発生する可能性があります。Security Hub がそのためのガイダンスを提供している場合にのみ、サービス ロールを編集してください。

Security Hub のサービスリンクロール

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

Security Hub は、ユーザーに代わってアクションを実行するためにサービスリンクロールを使用します。このロールの詳細については、のサービスにリンクされたロール AWS Security Hubを参照してください。

AWS Security Hubのアイデンティティベースのポリシーの例

デフォルトでは、ユーザーおよびロールには、Security Hub リソースを作成または変更する許可はありません。また、 AWS Management Console、 AWS CLI、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、指定されたリソースで特定の API 操作を実行するための許可をユーザーとロールに付与する IAM ポリシーを作成する必要があります。続いて、管理者はそれらのアクセス許可が必要なユーザーまたはグループにそのポリシーをアタッチします。

JSON ポリシードキュメントのこれらの例を使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「JSON タブでのポリシーの作成」を参照してください。

トピック

- ポリシーに関するベストプラクティス
- Security Hub コンソールの使用
- 例: ユーザーにそれぞれのアクセス権限の表示を許可する
- 例: ユーザーに設定ポリシーの作成と管理を許可する
- 例: ユーザーに検出結果の表示を許可する
- 例: ユーザーに自動化ルールの作成と管理を許可する

ポリシーに関するベストプラクティス

ID ベースのポリシーは、あるユーザーがアカウント内で Security Hub リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行 – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能の AWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサ

ポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer でポリシーを検証する」を参照してください。

- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、MFA をオンにしてセキュリティを強化します。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA を使用した安全な API アクセス」を参照してください。

IAM でのベストプラクティスの詳細については、「IAM ユーザーガイド」の「IAM でのセキュリティのベストプラクティス」を参照してください。

Security Hub コンソールの使用

AWS Security Hub コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の Security Hub リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

これらのユーザーとロールが Security Hub コンソールを使用できるようにするには、次の AWS 管理ポリシーもエンティティにアタッチします。詳細については、IAM ユーザーガイド」の「ユーザーへの許可の追加」を参照してください。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
```

```
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

例: ユーザーにそれぞれのアクセス権限の表示を許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

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

```
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

例: ユーザーに設定ポリシーの作成と管理を許可する

この例では、ユーザーが設定ポリシーを作成、表示、更新、削除できるようにする IAM ポリシーを作成する方法を示します。このポリシー例では、ポリシーの関連付けを開始、停止、表示することもできます。この IAM ポリシーが機能するには、ユーザーが組織の委任された Security Hub 管理者である必要があります。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateConfigurationPolicy",
                "securityhub:UpdateConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetConfigurationPolicy",
                "securityhub:ListConfigurationPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
```

```
                "securityhub:DeleteConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetConfigurationPolicyAssociations",
                "securityhub:GetConfigurationPolicyAssociation",
                "securityhub:ListConfigurationPolicyAssociations"
            ],
            "Resource": "*"
        },
        {
            "Sid": "UpdateConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:StartConfigurationPolicyAssociation",
                "securityhub:StartConfigurationPolicyDisassociation"
            ],
            "Resource": "*"
        }
    ]
}
```

例: ユーザーに検出結果の表示を許可する

この例では、ユーザーに Security Hub 検出結果データの表示を許可する IAM ポリシーを作成する方法を示しています。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindings"
```

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

例: ユーザーに自動化ルールの作成と管理を許可する

この例では、Security Hub 自動化ルールの作成、表示、更新、削除をユーザーに許可する IAM ポリシーを作成する方法を示します。この IAM ポリシーを使用するには、ユーザーが Security Hub 管理者である必要があります。アクセス許可を制限するには、例えば、ユーザーに自動化ルールの表示のみを許可するには、作成、更新、削除のアクセス許可を削除できます。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateAutomationRule",
                "securityhub:BatchUpdateAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetAutomationRules",
                "securityhub:ListAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchDeleteAutomationRules"
```

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

のサービスにリンクされたロール AWS Security Hub

AWS Security Hub は、 という名前の AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用しますAWSServiceRoleForSecurityHub。このサービスリンクロールは、Security Hub に直接リンクされている IAM ロールです。これは Security Hub によって事前定義されており、Security Hub がユーザーに代わって他の を呼び出し AWS のサービス て AWS リソースをモニタリングするために必要なすべてのアクセス許可が含まれています。Security Hub は、Security Hub AWS リージョン が利用可能なすべての で、このサービスにリンクされたロールを使用します。

サービスにリンクされたロールを使用することで、必要な許可を手動で追加する必要がなくなるため、Security Hub の設定が簡単になります。Security Hub は、サービスにリンクされたロールのアクセス許可を定義します。特に定義されている場合を除き、Security Hub のみがロールを引き受けることができます。定義される許可には、信頼ポリシーや許可ポリシーなどがあり、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスにリンクされたロールの詳細を確認するには、Security Hub コンソールを使用できます。ナビゲーションペインで、「設定」の「全般」を選択します。次に、「サービスアクセス許可」セクションで「サービスアクセス許可の表示」を選択します。

Security Hub サービスにリンクされたロールを削除できるのは、Security Hub が有効になっているすべてのリージョンで Security Hub を無効にした後のみです。これにより、アクセスに必要な許可を誤って削除してしまうことがなくなり、Security Hub リソースは保護されます。

サービスにリンクされたロールをサポートする他のサービスの詳細については、AWS 「IAM ユーザーガイド」の「IAM と連携するサービス」を参照し、「サービスにリンクされたロール」列で「はい」を持つサービスを見つけます。 サービスリンクロールに関するドキュメントをサービスで表示するには、[Yes] (はい) リンクを選択します。

トピック

- Security Hub のサービスにリンクされたロールの許可
- Security Hub のサービスにリンクされたロールの作成

- Security Hub 向けのサービスにリンクされたロールの編集
- Security Hub 向けのサービスにリンクされたロールの削除

Security Hub のサービスにリンクされたロールの許可

Security Hub では、`AWSServiceRoleForSecurityHub` という名前のサービスにリンクされたロールを使用します。これは、 が リソースにアクセス AWS Security Hub するために必要なサービスにリンクされたロールです。このサービスにリンクされたロールにより、Security Hub は他の からの検出結果の受信 AWS のサービス や、コントロールのセキュリティチェックを実行するために必要な AWS Config インフラストラクチャの設定などのタスクを実行できます。`AWSServiceRoleForSecurityHub` サービスにリンクされたロールは、ロールを継承するために `securityhub.amazonaws.com` のサービスを信頼します。

`AWSServiceRoleForSecurityHub` サービスにリンクされたロールは、マネージドポリシーである `AWSSecurityHubServiceRolePolicy` を使用します。

IAM アイデンティティ (ロール、グループ、ユーザーなど) に、サービスにリンクされたロールの作成、編集、削除を許可する設定をする必要があります。`AWSServiceRoleForSecurityHub` サービスにリンクされたロールを適切に作成するには、Security Hub を使用する IAM アイデンティティに、必要な許可が付与されている必要があります。必要な許可を付与するには、次のポリシーを IAM アイデンティティにアタッチします。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
```

```
                }
            }
        }
    ]
}
```

Security Hub のサービスにリンクされたロールの作成

`AWSServiceRoleForSecurityHub` サービスにリンクされたロールは、Security Hub を初めて有効にするか、以前に有効にしたことがないリージョンで Security Hub を有効にすると、自動的に作成されます。IAM コンソール、IAM CLI、または IAM API を使用して、`AWSServiceRoleForSecurityHub`サービスにリンクされたロールを手動で作成することもできます。IAM ロールを手動で作成する方法の詳細は、「IAM ユーザーガイド」の「サービスにリンクされたロールを作成する」を参照してください。

> **Important**
>
> Security Hub 管理者アカウント用に作成されたサービスにリンクされたロールは、関連する Security Hub メンバーアカウントには適用されません。

Security Hub 向けのサービスにリンクされたロールの編集

Security Hub では、`AWSServiceRoleForSecurityHub` サービスにリンクされたロールの編集は許可されていません。サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用してロールの説明の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの編集」を参照してください。

Security Hub 向けのサービスにリンクされたロールの削除

サービスにリンクされたロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。これにより、使用していないエンティティがアクティブにモニタリングされたり、メンテナンスされたりすることがなくなります。

Security Hub を無効にすると、Security Hub は`AWSServiceRoleForSecurityHub`サービスにリンクされたロールを自動的に削除しません。Security Hub を再度有効にすると、サービスは既存のサービスにリンクされたロールの使用を再開できます。Security Hub を使用する必要がなくなった場合は、サービスにリンクされたロールを手動で削除できます。

> **Important**
>
> `AWSServiceRoleForSecurityHub` サービスにリンクされたロールを削除する前に、そのロールが有効になっているすべてのリージョンで Security Hub を無効にする必要があります。詳細については、「Security Hub CSPM の無効化」を参照してください。サービスにリンクされたロールを削除しようとしたときに、Security Hub が無効になっていない場合、削除することはできません。

`AWSServiceRoleForSecurityHub` サービスにリンクされたロールを削除するには、IAM コンソール、IAM CLI、または IAM API を使用できます。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの削除」を参照してください。

AWS Security Hub の マネージドポリシー

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。 AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS 管理ポリシーを更新する可能性が最も高くなります。

詳細については「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWS 管理ポリシー: AWSSecurityHubFullAccess

`AWSSecurityHubFullAccess` ポリシーを IAM アイデンティティにアタッチできます。

このポリシーは、すべての Security Hub CSPM アクションへのフルアクセスをプリンシパルに許可する管理アクセス許可を付与します。このポリシーは、アカウントで Security Hub CSPM を手動で有効にする前に、プリンシパルにアタッチする必要があります。例えば、これらの許可を持つプリン

シパルは、結果のステータスを表示および更新できます。また、カスタムインサイトの設定、統合の有効化、標準とコントロールの有効化と無効化を行うこともできます。管理者アカウントのプリンシパルは、メンバーアカウントを管理することもできます。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `securityhub` – プリンシパルにすべての Security Hub CSPM アクションへのフルアクセスを許可します。
- `guardduty` – Amazon GuardDuty のアカウントステータスに関する情報の取得をプリンシパルに許可します。
- `iam` – プリンシパルが Security Hub CSPM と Security Hub のサービスにリンクされたロールを作成できるようにします。
- `inspector` – Amazon Inspector のアカウントステータスに関する情報の取得をプリンシパルに許可します。
- `pricing` – プリンシパルが AWS のサービス および 製品の料金表を取得できるようにします。

このポリシーのアクセス許可を確認するには、AWS 「 マネージドポリシーリファレンスガイドAWSSecurityHubFullAccess」の「」を参照してください。

AWS 管理ポリシー: AWSSecurityHubReadOnlyAccess

`AWSSecurityHubReadOnlyAccess` ポリシーを IAM アイデンティティにアタッチできます。

このポリシーは、ユーザーが Security Hub CSPM で情報を表示できるようにする読み取り専用アクセス許可を付与します。このポリシーがアタッチされているプリンシパルは、Security Hub CSPM で更新を行うことはできません。例えば、これらの許可を持つプリンシパルは、アカウントに関連付けられた結果のリストを表示できますが、結果のステータスを変更することはできません。インサイトの結果を表示することはできますが、カスタムインサイトを作成したり設定したりすることはできません。コントロールや製品統合を設定することはできません。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `securityhub` – ユーザーが項目のリストまたは項目の詳細を返すアクションを実行できるようにします。これには、`Get`、`List`、または `Describe` で始まる API オペレーションが含まれます。

このポリシーのアクセス許可を確認するには、AWS 「 マネージドポリシーリファレンスガイドAWSSecurityHubReadOnlyAccess」の「」を参照してください。

AWS 管理ポリシー: AWSSecurityHubOrganizationsAccess

`AWSSecurityHubOrganizationsAccess` ポリシーを IAM アイデンティティにアタッチできます。

このポリシーは、 の組織の Security Hub と Security Hub CSPM を有効化および管理するための管理アクセス許可を付与します AWS Organizations。このポリシーのアクセス許可により、組織管理アカウントは Security Hub と Security Hub CSPM の委任管理者アカウントを指定できます。また、委任管理者アカウントが組織アカウントをメンバーアカウントとして有効にすることもできます。

このポリシーは、 のアクセス許可のみを提供します AWS Organizations。組織管理アカウントと委任管理者アカウントには、関連するアクションに対するアクセス許可も必要です。これらの許可は、`AWSSecurityHubFullAccess` マネージドポリシーを使用して付与することができます。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `organizations:ListAccounts` - 組織に属するアカウントリストの取得をプリンシパルに許可します。
- `organizations:DescribeOrganization` - 組織に関する情報の取得をプリンシパルに許可します。
- `organizations:ListRoots` - 組織ルートの一覧表示をプリンシパルに許可します。
- `organizations:ListDelegatedAdministrators` - 組織の委任管理者の一覧表示をプリンシパルに許可します。
- `organizations:ListAWSServiceAccessForOrganization` – プリンシパル AWS のサービス が、組織が使用する を一覧表示できるようにします。
- `organizations:ListOrganizationalUnitsForParent` - 親 OU の子組織単位 (OU) の一覧表示をプリンシパルに許可します。
- `organizations:ListAccountsForParent` - 親 OU の子アカウントの一覧表示をプリンシパルに許可します。
- `organizations:ListParents` – 指定された子 OUs) を一覧表示します。
- `organizations:DescribeAccount` - 組織内のアカウントに関する情報の取得をプリンシパルに許可します。

- `organizations:DescribeOrganizationalUnit` - 組織内の OU に関する情報の取得をプリンシパルに許可します。
- `organizations:ListPolicies` – 指定されたタイプの組織内のすべてのポリシーのリストを取得します。
- `organizations:ListPoliciesForTarget` – 指定されたターゲットルート、組織単位 (OU)、またはアカウントに直接アタッチされているポリシーを一覧表示します。
- `organizations:ListTargetsForPolicy` – 指定されたポリシーがアタッチされているすべてのルート、組織単位 (OUs)、およびアカウントを一覧表示します。
- `organizations:EnableAWSServiceAccess` – プリンシパルが Organizations との統合を有効にすることを許可します。
- `organizations:RegisterDelegatedAdministrator` – プリンシパルが委任管理者アカウントを指定できるようにします。
- `organizations:DeregisterDelegatedAdministrator` – プリンシパルが委任管理者アカウントを削除できるようにします。
- `organizations:DescribePolicy` – ポリシーに関する情報を取得します。
- `organizations:DescribeEffectivePolicy` – 指定されたポリシータイプとアカウントの有効なポリシーの内容を返します。
- `organizations:CreatePolicy` – ルート、組織単位 (OU)、または個々の AWS アカウントにアタッチできる、指定されたタイプのポリシーを作成します。
- `organizations:UpdatePolicy` – 既存のポリシーを新しい名前、説明、またはコンテンツで更新します。
- `organizations:DeletePolicy` – 指定されたポリシーを組織から削除します。
- `organizations:AttachPolicy` – ルート、組織単位 (OU)、または個々のアカウントにポリシーをアタッチします。
- `organizations:DetachPolicy` – ターゲットルート、組織単位 (OU)、またはアカウントからポリシーをデタッチします。
- `organizations:EnablePolicyType` – ルート内のポリシータイプを有効にします。
- `organizations:DisablePolicyType` – ルート内の組織ポリシータイプを無効にします。
- `organizations:TagResource` – 指定されたリソースに 1 つ以上のタグを追加します。
- `organizations:UntagResource` – 指定されたリソースから指定されたキーを持つタグを削除します。
- `organizations:ListTagsForResource` – 指定されたリソースにアタッチされているタグを一覧表示します。

このポリシーのアクセス許可を確認するには、AWS 「 マネージドポリシーリファレンスガイドAWSSecurityHubOrganizationsAccess」の「」を参照してください。

AWS 管理ポリシー: AWSSecurityHubServiceRolePolicy

IAM エンティティに `AWSSecurityHubServiceRolePolicy` をアタッチすることはできません。このポリシーは、Security Hub CSPM がユーザーに代わってアクションを実行できるようにするサービスにリンクされたロールにアタッチされます。詳細については、「the section called “サービスにリンクされた役割”」を参照してください。

このポリシーは、サービスにリンクされたロールが Security Hub CSPM コントロールのセキュリティチェックの実行などのタスクを実行できるようにする管理アクセス許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `cloudtrail` - CloudTrail 追跡に関する情報を取得します。
- `cloudwatch` – 現在の CloudWatch アラームを取得します。
- `logs` – CloudWatch ログのメトリクスフィルターを取得します。
- `sns` - SNS トピックのサブスクリプションリストを取得します。
- `config` – 設定レコーダー、リソース、および AWS Config ルールに関する情報を取得します。また、サービスにリンクされたロールに AWS Config ルールの作成と削除、およびルールに対する評価の実行も許可します。
- `iam` – アカウントの認証情報レポートを取得して生成します。
- `organizations` — 組織のアカウントおよび組織単位 (OU) 情報を取得します。
- `securityhub` – Security Hub CSPM サービス、標準、コントロールの設定方法に関する情報を取得します。
- `tag`— リソースタグに関する情報を取得します。

このポリシーのアクセス許可を確認するには、AWS 「 マネージドポリシーリファレンスガイドAWSSecurityHubServiceRolePolicy」の「」を参照してください。

AWS 管理ポリシー: AWSSecurityHubV2ServiceRolePolicy

> **Note**
>
> Security Hub はプレビューリリースであり、変更される可能性があります。

このポリシーにより、Security Hub は組織およびユーザーに代わって AWS Config ルールと Security Hub リソースを管理できます。このポリシーは、ユーザーに代わってサービスがアクションを実行することを許可する、サービスリンクロールにアタッチされます。このポリシーは IAM アイデンティティにはアタッチできません。詳細については、「the section called “サービスにリンクされた役割”」を参照してください。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `config` – Security Hub リソースのサービスにリンクされた設定レコーダーを管理します。
- `iam` – のサービスにリンクされたロールを作成します AWS Config。
- `organizations` — 組織のアカウントおよび組織単位 (OU) 情報を取得します。
- `securityhub` – Security Hub の設定を管理します。
- `tag`— リソースタグに関する情報を取得します。

このポリシーのアクセス許可を確認するには、AWS 「 マネージドポリシーリファレンスガイドAWSSecurityHubV2ServiceRolePolicy」の「」を参照してください。

AWS マネージドポリシーに対する Security Hub の更新

次の表は、このサービスがこれらの変更の追跡を開始してからの AWS Security Hub および Security Hub CSPM の AWS マネージドポリシーの更新に関する詳細を示しています。ポリシーの更新に関する自動アラートについては、Security Hub ドキュメント履歴ページの RSS フィードにサブスクライブしてください。

変更	説明	日付
AWSSecurityHubOrganizationsAccess – 既存のポリシーの更新	Security Hub がポリシーに新しいアクセス許可を追加しました。アクセス許可により、組織管理者は組織の Security Hub と Security Hub CSPM を有効化および管理できます。	2025 年 6 月 17 日
AWSSecurityHubFullAccess – 既存のポリシーの更新	Security Hub CSPM に、プリンシパルが Security Hub のサービスにリンクされたロールを作成できるようにする新しいアクセス許可が追加されました。	2025 年 6 月 17 日
AWSSecurityHubV2ServiceRolePolicy – 新しいポリシー	Security Hub は、Security Hub が顧客の組織および顧客に代わって AWS Config ルールと Security Hub リソースを管理できるようにする新しいポリシーを追加しました。Security Hub はプレビューリリースであり、変更される可能性があります。	2025 年 6 月 17 日
AWSSecurityHubFullAccess — 既存のポリシーの更新	Security Hub CSPM は、AWS のサービス および 製品の料金詳細を取得するようにポリシーを更新しました。	2024 年 4 月 24 日
AWSSecurityHubReadOnlyAccess – 既存のポリシーの更新	Security Hub CSPM は、`Sid`フィールドを追加してこの管理ポリシーを更新しました。	2024 年 2 月 22 日
AWSSecurityHubFullAccess — 既存のポリシーの更新	Security Hub CSPM は、Amazon GuardDuty と	2023 年 11 月 16 日

変更	説明	日付
	Amazon Inspector がアカウントで有効になっているかどうかを判断できるようにポリシーを更新しました。これにより、お客様は複数の からセキュリティ関連情報をまとめることができます AWS のサービス。	
AWSSecurityHubOrganizationsAccess — 既存のポリシーの更新	Security Hub CSPM は、委任された管理者機能への読み取り専用アクセスを許可する追加のアクセス許可を付与するように AWS Organizations ポリシーを更新しました。これには、ルート、組織単位 (OU)、アカウント、組織構造、およびサービスアクセスなどの詳細が含まれます。	2023 年 11 月 16 日
AWSSecurityHubServiceRolePolicy — 既存のポリシーに対する更新	Security Hub CSPM は`BatchGetSecurityControls` 、カスタマイズ可能なセキュリティコントロールプロパティを読み取って更新するための 、`DisassociateFromAdministratorAccount` 、および アクセス`UpdateSecurityControl` 許可を追加しました。	2023 年 11 月 26 日

変更	説明	日付
AWSSecurityHubServiceRolePolicy — 既存のポリシーに対する更新	Security Hub CSPM は、検出結果に関連するリソースタグを読み取るアクセス`tag:GetResources` 許可を追加しました。	2023 年 11 月 7 日
AWSSecurityHubServiceRolePolicy — 既存のポリシーに対する更新	Security Hub CSPM は、標準のコントロールの有効化ステータスに関する情報を取得する`BatchGetStandardsControlAssociations` アクセス許可を追加しました。	2023 年 9 月 27 日
AWSSecurityHubServiceRolePolicy — 既存のポリシーに対する更新	Security Hub CSPM は、標準やコントロールなど、 AWS Organizations データを取得し、Security Hub CSPM 設定の読み取りと更新を行うための新しいアクセス許可を追加しました。	2023 年 9 月 20 日
AWSSecurityHubServiceRolePolicy — 既存のポリシーに対する更新	Security Hub CSPM は、既存の`config:DescribeConfigRuleEvaluationStatus` アクセス許可をポリシー内の別のステートメントに移動しました。これにより、`config:DescribeConfigRuleEvaluationStatus` 許可がすべてのリソースに適用されます。	2023 年 3 月 17 日

変更	説明	日付
AWSSecurityHubServiceRolePolicy — 既存のポリシーに対する更新	Security Hub CSPM は、既存の`config:PutEvaluations` アクセス許可をポリシー内の別のステートメントに移動しました。これにより、`config:PutEvaluations` 許可がすべてのリソースに適用されます。	2021 年 7 月 14 日
AWSSecurityHubServiceRolePolicy — 既存のポリシーに対する更新	Security Hub CSPM に、サービスにリンクされたロールが評価結果を配信できるようにする新しいアクセス許可が追加されました AWS Config。	2021 年 6 月 29 日
AWSSecurityHubServiceRolePolicy — マネージドポリシーのリストに追加	Security Hub CSPM サービスにリンクされたロールで使用される管理ポリシー AWSSecurityHubServiceRolePolicy に関する情報を追加しました。	2021 年 6 月 11 日
AWSSecurityHubOrganizationsAccess — 新しいポリシー	Security Hub CSPM に、Security Hub CSPM と Organizations の統合に必要なアクセス許可を付与する新しいポリシーが追加されました。	2021 年 3 月 15 日
Security Hub CSPM が変更の追跡を開始しました	Security Hub CSPM は、AWS 管理ポリシーの変更の追跡を開始しました。	2021 年 3 月 15 日

AWS Security Hub ID とアクセスのトラブルシューティング

次の情報は、 および IAM の使用時に発生する可能性がある一般的な問題の診断 AWS Security Hub と修正に役立ちます。

トピック

- Security Hub でアクションを実行することが認可されていない
- iam:PassRole を実行する権限がない
- Security Hub にプログラム的にアクセスしたい
- 管理者として Security Hub へのアクセスを他のユーザーに許可したい
- 自分の 以外のユーザーに Security Hub リソース AWS アカウント へのアクセスを許可したい

Security Hub でアクションを実行することが認可されていない

がアクションを実行する権限がないと AWS Management Console 通知した場合は、管理者に連絡してサポートを依頼する必要があります。管理者は、サインイン認証情報を提供した担当者です。

以下の例のエラーは、`mateojackson` ユーザーがコンソールを使用して、*######*の詳細を表示しようとしているが、 `securityhub:`*`GetWidget`* アクセス許可がない場合に発生します。

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

この場合、Mateo は、`securityhub:`*`GetWidget`* アクションを使用して *`my-example-widget`* リソースにアクセスできるように、管理者にポリシーの更新を依頼します。

iam:PassRole を実行する権限がない

`iam:PassRole` アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Security Hub にロールを渡すことができるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、既存のロールをそのサービスに渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

以下の例のエラーは、`marymajor` という IAM ユーザーがコンソールを使用して Security Hub でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、

サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

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

この場合、Mary のポリシーを更新してメアリーに `iam:PassRole` アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

Security Hub にプログラム的にアクセスしたい

ユーザーが の AWS 外部で を操作する場合は、プログラムによるアクセスが必要です AWS Management Console。プログラムによるアクセスを許可する方法は、 がアクセスするユーザーのタイプによって異なります AWS。

ユーザーにプログラマチックアクセス権を付与するには、以下のいずれかのオプションを選択します。

プログラマチックアクセス権を必要とするユーザー	目的	方法
ワークフォースアイデンティティ (IAM アイデンティティセンターで管理されているユーザー)	一時的な認証情報を使用して AWS CLI、、 AWS SDKs、または AWS APIs。	使用するインターフェイスの指示に従ってください。 • については AWS CLI、「 AWS Command Line Interface ユーザーガイド」の「 を使用する AWS CLI ように AWS IAM Identity Centerを設定する」を参照してください。 • AWS SDKs、ツール、API については、 AWS APIs「 SDK およびツールリファレンスガイド」の「IAM ア

プログラマチックアクセス権を必要とするユーザー	目的	方法
		イデンティティセンター認証」を参照してください。 AWS SDKs
IAM	一時的な認証情報を使用して AWS CLI、、 AWS SDKs、または AWS APIs。	「IAM ユーザーガイド」の「 AWS リソースでの一時的な認証情報の使用」の手順に従います。
IAM	(非推奨) 長期認証情報を使用して、AWS CLI、 AWS SDKs、または AWS APIs。	使用するインターフェイスの指示に従ってください。 • については AWS CLI、「 AWS Command Line Interface ユーザーガイド」の「IAM ユーザー認証情報を使用した認証」を参照してください。 • AWS SDKs「 SDK とツールリファレンスガイド」の「長期認証情報を使用した認証」を参照してください。 AWS SDKs • API AWS APIs「IAM ユーザーのアクセスキーの管理」を参照してください。

管理者として Security Hub へのアクセスを他のユーザーに許可したい

アクセス権限を付与するにはユーザー、グループ、またはロールにアクセス許可を追加します。

- 以下のユーザーとグループ AWS IAM Identity Center：

  アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」の手順に従ってください。

- IAM 内で、ID プロバイダーによって管理されているユーザー:

  ID フェデレーションのロールを作成します。詳細については「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。

- IAM ユーザー:
  - ユーザーが担当できるロールを作成します。手順については「IAM ユーザーガイド」の「IAM ユーザーのロールの作成」を参照してください。
  - (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加します。詳細については「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス権限の追加」を参照してください。

自分の 以外のユーザーに Security Hub リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください。

- Security Hub でこれらの機能がサポートされるかどうかを確認するには、「Security Hub と IAM の連携方法」を参照してください。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、「IAM ユーザーガイド」の「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、「IAM ユーザーガイド」の「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

のコンプライアンス検証 AWS Security Hub

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、AWS のサービス 「コンプライアンスプログラムによる対象範囲内」を参照して、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「 Compliance ProgramsAssurance」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「Downloading Reports in AWS Artifact」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 は、コンプライアンスに役立つ以下のリソース AWS を提供します。

- セキュリティのコンプライアンスとガバナンス – これらのソリューション実装ガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスの機能をデプロイする手順を示します。
- HIPAA 対応サービスのリファレンス – HIPAA 対応サービスの一覧が提供されています。すべての AWS のサービス が HIPAA の対象となるわけではありません。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド – コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) など) にわたるセキュリティコントロールを保護および AWS のサービス マッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が内部プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に把握できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールの一覧については、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – 不審なアクティビティや悪意のあるアクティビティがないか環境をモニタリングすることで AWS アカウント、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。GuardDuty を使用すると、特定のコンプライアンスフレームワー

クで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。

- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

AWS Security Hub の耐障害性

AWS グローバルインフラストラクチャは、 AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。リージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立および隔離されたアベイラビリティーゾーンがあります。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョン およびアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

のインフラストラクチャセキュリティ AWS Security Hub

マネージドサービスである AWS Security Hub は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「セキュリティの柱 AWS Well-Architected フレームワーク」の「インフラストラクチャの保護」を参照してください。

AWS が公開した API コールを使用して、ネットワーク経由で Security Hub にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードはJava 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

AWS Security Hub およびインターフェイス VPC エンドポイント (AWS PrivateLink)

VPC と の間にプライベート接続を確立するには、インターフェイス VPC エンドポイント AWS Security Hub を作成します。インターフェイスエンドポイントは AWS PrivateLink テクノロジーを利用しています。このテクノロジーは Security Hub API にプライベートにアクセスでき、インターネットゲートウェイ、NAT デバイス、VPN 接続、 AWS Direct Connect 接続のいずれも必要としません。VPC のインスタンスは、パブリック IP アドレスがなくても Security Hub API と通信できます。VPC と Security Hub との間のトラフィックは、Amazon ネットワークを離れません。

各インターフェイスエンドポイントは、サブネット内の 1 つ以上の Elastic Network Interface によって表されます。詳細については、Amazon Virtual Private Cloud ガイド」の「インターフェイス VPC エンドポイント AWS のサービス を使用して にアクセスする」を参照してください。

Security Hub VPC エンドポイントに関する考慮事項

Security Hub のインターフェイス VPC エンドポイントを設定する前に、Amazon Virtual Private Cloud Guide の前提条件とその他の情報を確認してください。

Security Hub では、VPC からのすべての API アクションの呼び出しをサポートしています。

Security Hub 用のインターフェイス VPC エンドポイントの作成

Security Hub サービスの VPC エンドポイントは、Amazon VPC コンソールまたは AWS Command Line Interface () を使用して作成できますAWS CLI。詳細については、Amazon Virtual Private Cloud Guide」の「Create a VPC endpoint」を参照してください。

Security Hub 用の VPC エンドポイントを作成するには、次のサービス名を使用します。

```
com.amazonaws.region.securityhub
```

ここで、*#####*は該当する AWS リージョンのリージョンコードです。

エンドポイントのプライベート DNS を有効にすると、`securityhub.us-east-1.amazonaws.com`米国東部 (バージニア北部) リージョンなど、 リージョンのデフォルトの DNS 名を使用して Security Hub に API リクエストを行うことができます。

Security Hub 用の VPC エンドポイントポリシーの作成

VPC エンドポイントに Security Hub へのアクセスをコントロールするエンドポイントポリシーをアタッチできます。このポリシーでは、以下の情報を指定します。

- アクションを実行できるプリンシパル。
- 実行可能なアクション。
- アクションを実行できるリソース。

詳細については、Amazon Virtual Private Cloud Guide」の「Control access to VPC endpoints using endpoint policies」を参照してください。

例: Security Hub アクションの VPC エンドポイントポリシー

以下は、Security Hub のエンドポイントポリシーの例です。このポリシーは、エンドポイントに添付されると、すべてのリソースのすべてのプリンシパルに対して、登録されている Security Hub アクションへのアクセスが許可されます。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

共有サブネット

自分と共有されているサブネットで VPC エンドポイントを作成、説明、変更、または削除することはできません。ただし、VPC エンドポイントを使用することはできます。VPC 共有の詳細については、Amazon Virtual Private Cloud Guide」の「Share your VPC subnets with other accounts」を参照してください。

CloudTrail を使用した Security Hub API コールのログ記録

AWS Security Hub CSPM は AWS CloudTrail、Security Hub CSPM のユーザー、ロール、または サービスによって実行されたアクションを記録する AWS サービスである と統合されています。CloudTrail は、Security Hub CSPM の API コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、Security Hub CSPM コンソールからの呼び出しと、Security Hub CSPM API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、Security Hub CSPM のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、CloudTrail コンソールの [Event history (イベント履歴)] で最新のイベントを表示できます。CloudTrail が収集する情報を使用して、Security Hub CSPM に対して行われたリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

設定や有効化の方法など、CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

CloudTrail の Security Hub CSPM 情報

CloudTrail は、アカウントの作成 AWS アカウント 時に で有効になります。Security Hub CSPM でサポートされているイベントアクティビティが発生すると、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。最近のイベントは、アカウントで表示、検索、ダウンロードできます。詳細については、「CloudTrail Event 履歴でのイベントの表示」を参照してください。

Security Hub CSPM のイベントなど、アカウントのイベントの継続的な記録については、証跡を作成します。追跡を有効にすることで、CloudTrail でログファイルを Amazon S3 バケットに送信できるようになります。デフォルトでは、コンソールで追跡を作成すると、すべての AWS リージョンに追跡が適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集したイベントデータをより詳細に分析し、それに基づいて対応するため、他の AWS サービスを構成できます。詳細については、次を参照してください:

- 追跡を作成するための概要
- 「CloudTrail がサポートされているサービスと統合」
- 「CloudTrail の Amazon SNS 通知の設定」
- 複数のリージョンから CloudTrail ログファイルを受け取るおよび複数のアカウントから CloudTrail ログファイルを受け取る

Security Hub CSPM は、すべての Security Hub CSPM API アクションを CloudTrail ログのイベントとしてログ記録することをサポートしています。Security Hub CSPM オペレーションのリストを表示するには、「Security Hub CSPM API リファレンス」を参照してください。

次のアクションのアクティビティが CloudTrail にログ記録されると、`responseElements` の値は `null` に設定されます。これにより、機密性の高い情報が CloudTrail ログに含まれることがなくなります。

- `BatchImportFindings`
- `GetFindings`
- `GetInsights`
- `GetMembers`
- `UpdateFindings`

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか
- リクエストが、ロールとフェデレーティッドユーザーのどちらの一時的なセキュリティ認証情報を使用して送信されたか
- リクエストが別の AWS サービスによって行われたかどうか

詳細については、「CloudTrail userIdentity エレメント」を参照してください。

例: Security Hub CSPM ログファイルエントリ

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどの情報を含みます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、`CreateInsight` アクションを示す CloudTrail ログエントリです。この例では、`Test Insight` というインサイトが作成されます。`ResourceId` 属性は、[Group by] (グループ化の条件) アグリゲータとして指定され、このインサイトに対するオプションのフィルターは指定されません。

インサイトの詳細については、「Security Hub CSPM でのインサイトの表示」を参照してください。


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJK6U5DS22IAVUI7BW",
        "arn": "arn:aws:iam::012345678901:user/TestUser",
        "accountId": "012345678901",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "TestUser"
    },
    "eventTime": "2018-11-25T01:02:18Z",
    "eventSource": "securityhub.amazonaws.com",
    "eventName": "CreateInsight",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
    "requestParameters": {
        "Filters": {},
        "ResultField": "ResourceId",
        "Name": "Test Insight"
    },
    "responseElements": {
        "InsightArn": "arn:aws:securityhub:us-west-2:0123456789010:insight/custom/
f4c4890b-ac6b-4c26-95f9-e62cc46f3055"
    },
    "requestID": "c0fffccd-f04d-11e8-93fc-ddcd14710066",
    "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "012345678901"
}
```

Security Hub リソースのタグ付け

タグは、特定のタイプの AWS Security Hub CSPM AWS リソースなど、リソースを定義して割り当てることができるオプションのラベルです。タグを使用することで、目的、所有者、環境、その他の条件など、さまざまな方法でリソースを分類および管理できます。例えば、タグを使用して、リソースを区別したり、特定のコンプライアンス要件やワークフローをサポートするリソースを識別したり、コストを割り当てたりできます。

次のタイプの Security Hub CSPM リソースにタグを追加できます。

- 自動化ルール
- 設定ポリシー
- Hub リソース:

タグ付けの基本

リソースには、最大 50 個のタグを含めることができます。タグはそれぞれ、1 つの必須タグキーとオプションの 1 つのタグ値で設定されており、どちらもお客様側が定義します。タグキーは、より具体的なタグ値のカテゴリとして動作する一般的なラベルです。タグ値は、タグキーの記述子として機能します。

例えば、環境ごとに異なる自動化ルール (テスト用と本番用の自動化ルール) を作成する場合、それらのルールに `Environment` タグキーを割り当てます。関連するタグ値は、テストアカウントに関連付けられているルール用の `Test` でも、本番用アカウントと OU に関連するルール用の `Prod` でもかまいません。

AWS Security Hub CSPM リソースを定義してタグを割り当てるときは、次の点に注意してください。

- 各リソースには、最大 50 個のタグを設定できます。
- リソースごとに、各タグ キーは一意である必要があり、タグ値は 1 つだけ持つことができます。
- タグのキーと値では、大文字と小文字が区別されます。タグに大文字を使用する場合の戦略を決定し、その戦略をすべてのリソースにわたって一貫して実装することをベストプラクティスとして推奨します。
- タグキーは最大 128 文字 (UTF-8) です。タグキーは最大 256 文字 (UTF-8) です。文字には、文字、数字、スペース、または記号 (_ . : / = + - @) を使用できます。

- `aws:` プレフィックスは が使用するために予約されています AWS。定義したどのタグキーやタグ値にも使用できません。さらに、このプレフィックスを使用するタグキーまたは値は変更または削除できません。このプレフィックスを使用するタグは、リソースあたりのタグ数のクォータ (50 個) にはカウントされません。
- 割り当てたタグは、 AWS アカウント と、割り当てた AWS リージョン でのみ使用できます。
- Security Hub CSPM を使用してリソースにタグを割り当てる場合、タグは、該当する の Security Hub CSPM に直接保存されているリソースにのみ適用されます AWS リージョン。これらは、Security Hub CSPM が他の で作成、使用、または維持する、関連するサポートリソースには適用されません AWS のサービス。例えば、Amazon Simple Storage Service (Amazon S3) に関連する検出結果を更新するオートメーションルールにタグを割り当てると、タグは指定されたリージョンの Security Hub CSPM のオートメーションルールにのみ適用されます。S3 バケットには適用されません。関連付けられたリソースにタグを割り当てるには、SAmazon S3S3 など、リソース AWS のサービス を保存する AWS Resource Groups または を使用できます。関連付けられたリソースにタグを割り当てると、Security Hub CSPM リソースのサポートリソースを特定するのに役立ちます。
- リソースを削除すると、リソースに関連付けられているすべてのタグも削除されます。

> **Important**
>
> 機密データやその他の機密データをタグに保存しないでください。タグには AWS のサービス、 を含む多くの からアクセスできます AWS Billing and Cost Management。それらは機密データに使用することを目的としていません。

Security Hub CSPM リソースのタグを追加および管理するには、Security Hub CSPM コンソール、Security Hub CSPM API、または AWS Resource Groups Tagging API を使用できます。Security Hub CSPM を使用すると、リソースの作成時にリソースにタグを追加できます。また、既存のリソースごとにタグを追加、管理することもできます。Resource Groups を使用すると、Security Hub CSPM など AWS のサービス、複数の にまたがる複数の既存のリソースに対してタグを一括で追加および管理できます。

タグ付けのその他のヒントとベストプラクティスについては、「 AWS リソースのタグ付けユーザーガイド」の「 AWS リソースのタグ付け」を参照してください。

IAMポリシーでタグを使用する

リソースのタグ付けを開始した後、タグベースのリソースレベルのアクセス許可を AWS Identity and Access Management (IAM) ポリシーで定義できます。この方法でタグを使用することで、リソースを作成およびタグ付けするアクセス許可 AWS アカウント を持つ のユーザーとロール、およびタグをより一般的に追加、編集、削除するアクセス許可を持つユーザーとロールをきめ細かく制御できます。タグに基づいてアクセスを制御するには、IAM ポリシーの条件要素でタグ関連の条件キーを使用できます。

たとえば、リソースの`Owner`タグでユーザー名が指定されている場合、すべての AWS Security Hub CSPM リソースへのフルアクセスをユーザーに許可する IAM ポリシーを作成できます。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner":
 "${aws:username}"}
            }
        }
    ]
}
```

タグをベースにしてリソースレベルでアクセス許可を定義した場合、そのアクセス許可は即座に反映されます。つまり、リソースが作成されるとすぐにリソースの安全性が増し、新しいリソースにタグの使用をすぐに強制できるようになります。リソースレベルのアクセス許可を使用して、新しいリソースと既存のリソースに、どのタグキーと値を関連付けるかを制御することもできます。詳細については、IAM ユーザーガイドの「タグを使用した AWS リソースへのアクセスの制御」を参照してください。

Security Hub CSPM リソースへのタグの追加

タグは、特定のタイプの AWS Security Hub CSPM AWS リソースなど、リソースを定義して割り当てることができるラベルです。タグを使用すると、目的、所有者、環境、その他の条件など、さまざまな方法でリソースを識別、分類、管理できます。例えば、タグを使用してポリシーを適用したり、コストを割り当てたり、リソースのバージョンを区別したり、特定のコンプライアンス要件やワークフローをサポートするリソースを識別したりできます。

次のタイプの Security Hub CSPM リソースにタグを追加できます。

- 自動化ルール
- 設定ポリシー
- Hub リソース:

リソースには、最大 50 個のタグを含めることができます。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグキーは、より具体的なタグ値のカテゴリとして動作する一般的なラベルです。タグ値は、タグキーの記述子として機能します。タグ付けのオプションおよび要件の詳細は、「タグ付けの基本」を参照してください。

Security Hub CSPM リソースにタグを追加するには、Security Hub CSPM コンソールまたは Security Hub CSPM API を使用できます。ただし、コンソールは Hub リソースへのタグの追加をサポートしていません。

タグを追加したら、タグを編集し、タグキーまたはタグ値を変更できます。

複数の Security Hub CSPM リソースのタグを同時に追加または編集するには、タグ付け AWS Resource Groups API のタグ付けオペレーションを使用します。

> **Important**
>
> リソースにタグを追加すると、リソースへのアクセスに影響を与える可能性があります。リソースにタグを追加する前に、タグを使用してリソースへのアクセスを制御する可能性のある AWS Identity and Access Management (IAM) ポリシーを確認してください。

Console

Security Hub CSPM リソースにタグを追加するには (コンソール)

自動化ルールまたは設定ポリシーを作成すると、Security Hub CSPM コンソールにタグを追加するためのオプションが表示されます。タグキーとタグ値はタグセクションで指定できます。

Security Hub CSPM API

Security Hub CSPM リソースにタグを追加するには (API)

リソースを作成して 1 つ以上のタグをプログラムで追加するには、作成するリソースのタイプに適した操作を使用します。

- 設定ポリシーを作成して 1 つまたは複数のタグを追加するには、CreateConfigurationPolicy API を呼び出すか、 AWS CLIを使用している場合は create-configuration-policy コマンドを実行します。
- 自動化ルールを作成して 1 つ以上のタグを追加するには、CreateAutomationRule API を呼び出すか、 AWS CLIを使用している場合は create-automation-rule コマンドを実行します。
- Security Hub CSPM を有効にしてHubリソースに 1 つ以上のタグを追加するには、EnableSecurityHub API を呼び出すか、 AWS Command Line Interface （ AWS CLI) を使用している場合は enable-security-hub コマンドを実行します。

リクエストでは、`tags` パラメータを使用して、リソースに追加する各タグのタグキーとオプションのタグ値を指定します。`tags` パラメータは、オブジェクトの配列を指定します。各オブジェクトはタグキーとそれに関連するタグ値を指定します。

既存のリソースに 1 つ以上のタグを追加するには、Security Hub CSPM API の TagResource オペレーションを使用するか、 を使用している場合は tag-resource コマンド AWS CLIを実行します。リクエストでは、タグを追加するリソースの Amazon リソースネーム (ARN) を指定します。`tags` パラメータを使用して、追加する各タグのタグキー (`key`) とオプションのタグ値 (`value`) を指定します。`tags` パラメータは、オブジェクトの配列、各タグキーに 1 つのオブジェクト、および関連するタグ値を指定します。

たとえば、次の AWS CLI コマンドは、指定された設定ポリシーに`Environment`タグ値を持つ`Prod`タグキーを追加します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

CLI コマンドの例:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
```

```
--tags '{"Environment":"Prod"}'
```

コードの説明は以下のとおりです。

- `resource-arn` ではタグを追加する設定ポリシーの ARN を指定します。
- *`Environment`* はルールに追加するタグのタグキーです。
- *`Prod`* は指定されたタグキー (*`Environment`*) のタグ値です。

次の例では、コマンドは設定ポリシーに複数のタグを追加します。

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Prod", "CostCenter":"12345", "Owner":"jane-doe"}'
```

`tags`配列内の各オブジェクトには、`key``value`との引数の両方が必要です。ただし、`value`引数の値は空の文字列とすることができます。タグ値をタグキーに関連付けない場合、`value` 引数の値を指定しないでください。たとえば、以下のコマンドは、関連付けられたタグ値を含まない`Owner`タグキーを追加します。

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

タグ付けオペレーションが成功すると、Security Hub CSPM は空の HTTP 200 レスポンスを返します。それ以外の場合、Security Hub CSPM は、オペレーションが失敗した理由を示す HTTP 4xx または 500 レスポンスを返します。

Security Hub CSPM リソースのタグの編集

環境または要件が時間の経過とともに変化すると、 AWS Security Hub CSPM リソースの既存のタグを評価し、必要に応じてタグを変更できます。タグは、特定のタイプの Amazon Macie リソースなど 1 つ以上の AWS リソースを定義して割り当てることができるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグキーは、より具体的なタグ値のカテゴリとして動作する一般的なラベルです。タグ値は、タグキーの記述子として機能します。

タグを使用することで、目的、所有者、環境、その他の条件など、さまざまな方法でリソースを分類および管理できます。例えば、タグを使用してポリシーを適用したり、コストを割り当てたり、リソースのバージョンを区別したり、特定のコンプライアンス要件やワークフローをサポートするリソースを識別したりできます。

次のタイプの Security Hub CSPM リソースにタグを追加できます。

- 自動化ルール
- 設定ポリシー
- Hub リソース:

Security Hub CSPM リソースのタグキーまたはタグ値を編集するには、Security Hub CSPM API を使用できます。Security Hub CSPM コンソールは現在タグ編集をサポートしていません。

> **Important**
> リソースのタグを編集すると、リソースへのアクセスに影響する可能性があります。リソースのタグを編集する前に、タグを使用してリソースへのアクセスを制御する可能性のある AWS Identity and Access Management (IAM) ポリシーを確認してください。

Security Hub CSPM API

Security Hub CSPM リソースのタグを編集するには (API)

リソースのタグをプログラムで編集すると、既存のタグが新しい値に上書きされます。したがって、タグを編集する最適な方法は、タグキー、タグ値、またはその両方を編集するかどうかによって異なります。タグキーを編集するには、現在のタグを削除して、新しいタグを追加します。

タグキーに関連付けられているタグ値のみを編集または削除するには、Security Hub CSPM API の TagResource オペレーションを使用して既存の値を上書きします。 AWS CLIを使用している場合は、tag-resource コマンドを実行します。リクエストでは、タグ値を編集または削除するリソースの Amazon リソースネーム (ARN) を指定します。

タグ値を編集するには、`tags` パラメータを使用して、タグ値を変更したいタグキーを指定します。キーには新しいタグ値も指定する必要があります。たとえば、次の AWS CLI コマンドは、指定された自動化ルールに割り当てられたタグキー`Test`の`Environment`タグ値を `Prod`から に

変更します。この例は Linux、macOS、または Unix 用にフォーマットされており、読みやすさを向上させるためにバックスラッシュ (\) の行継続文字を使用しています。

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Test"}'
```

コードの説明は以下のとおりです。

- `resource-arn` では設定ポリシーの ARN を指定します。
- *`Environment`*は、変更するタグ値に関連付けられているタグキーです。
- *`Test`*は、指定したタグキー (*`Environment`*) に使用する新しいタグ値です。

タグキーからタグ値を削除するには、`tags`パラメーターのキーの`value`引数の値を指定しないでください。例:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

オペレーションが成功すると、Security Hub CSPM は空の HTTP 200 レスポンスを返します。それ以外の場合、Security Hub CSPM は、オペレーションが失敗した理由を示す HTTP 4xx または 500 レスポンスを返します。

Security Hub CSPM リソースのタグの確認

AWS Security Hub CSPM リソースのタグを追加または編集すると、リソースに現在あるタグキーとタグ値を表示できます。タグは、特定のタイプの Amazon Macie リソースなど 1 つ以上の AWS リソースを定義して割り当てることができるラベルです。各タグは、必要なタグキーとオプションのタグ値で設定されています。タグキーは、より具体的なタグ値のカテゴリとして動作する一般的なラベルです。タグ値は、タグキーの記述子として機能します。

タグを使用することで、目的、所有者、環境、その他の条件など、さまざまな方法でリソースを分類および管理できます。例えば、タグを使用してポリシーを適用したり、コストを割り当てたり、リソースのバージョンを区別したり、特定のコンプライアンス要件やワークフローをサポートするリソースを識別したりできます。

次のタイプの Security Hub CSPM リソースにタグを追加できます。

- 自動化ルール
- 設定ポリシー
- Hub リソース:

Security Hub CSPM コンソールまたは Security Hub CSPM API を使用して、Security Hub CSPM 自動化ルールまたは設定ポリシーのタグを確認できます。コンソールは Hub リソースのタグの確認をサポートしていません。プログラムにより、任意のリソースのタグを確認できます。

複数の Security Hub CSPM リソースのタグを同時に確認するには、タグ付け AWS Resource Groups API のタグ付けオペレーションを使用します。

Console

Security Hub CSPM リソースのタグを確認するには (コンソール)

1. Security Hub CSPM 管理者の認証情報を使用して、https://console.aws.amazon.com/securityhub/ で AWS Security Hub CSPM コンソールを開きます。
2. タグを追加するリソースのタイプに応じて、次のいずれかを実行します。
   - 自動化ルールのタグを確認するには、ナビゲーションペインで [自動化] を選択します。次に、自動化ルールを選択します。
   - 設定ポリシーのタグを確認するには、ナビゲーションペインで [設定] を選択します。次に、[ポリシー] タブで設定ポリシーの横にあるオプションを選択します。サイドパネルが開き、ポリシーに割り当てられたタグの数が表示されます。[タグ] ヘッダーを展開すると、タグキーとタグ値が表示されます。

Tags セクションには、現在リソースに割り当てられているすべてのタグが一覧表示されます。

Security Hub CSPM API

Security Hub CSPM リソースのタグを確認するには (API)

既存のリソースのタグを取得して確認するには、ListTagsForResource API を呼び出します。リクエストでは、`resourceArn` パラメータを使用してリソースの Amazon リソースネーム (ARN) を指定します。

を使用している場合は AWS CLI、list-tags-for-resource コマンドを実行し、 `resource-arn`パラメータを使用してリソースの ARN を指定します。例:

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

オペレーションが成功すると、Security Hub CSPM は`tags`配列を返します。配列内の各オブジェクトは、現在リソースに割り当てられているタグ (タグキーとタグ値の両方) を指定します。例:

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Prod"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

ここで`Environment`、`CostCenter`、`Owner`は、リソースに割り当てられるタグキーです。`Prod`は、`Environment`タグキーに関連付けられているタグ値です。 `12345`は、`CostCenter`タグキーに関連付けられているタグ値です。`Owner`タグキーには、関連するタグ値はありません。

タグを持つすべての Security Hub CSPM リソースと、それらの各リソースに割り当てられたすべてのタグのリストを取得するには、 AWS Resource Groups Tagging API の GetResources オペレーションを使用します。リクエストでは、`ResourceTypeFilters` パラメータの値を `securityhub` に設定します。を使用してこれを行うには AWS CLI、get-resources コマンドを実行し、 `resource-type-filters`パラメータの値を に設定します`securityhub`。例:

```
$ aws resourcegroupstaggingapi get-resources -\-resource-type-filters "securityhub"
```

オペレーションが成功すると、Resource Groups は `ResourceTagMappingList` 配列を返します。配列には、タグを持つ Security Hub CSPM リソースごとに 1 つのオブジェクトが含まれます。各オブジェクトは、Security Hub CSPM リソースの ARN、およびリソースに割り当てられたタグキーと値を指定します。

Security Hub CSPM リソースからのタグの削除

AWS Security Hub CSPM リソースにタグを追加すると、その後 1 つ以上のタグを削除できます。タグは、特定のタイプの Security Hub CSPM AWS リソースなど、リソースを定義して割り当てるラベルです。オートメーションルール、設定ポリシー、リソースの Security Hub CSPM リソースのタイプからタグを追加、編集、削除できますHub。

個々の AWS Security Hub CSPM リソースからタグを削除するには、Security Hub CSPM API を使用できます。Security Hub CSPM コンソールは現在、タグの削除をサポートしていません。

複数の Security Hub CSPM リソースからタグを同時に削除するには、タグ付け AWS Resource Groups API のタグ付けオペレーションを使用します。

> **Important**
>
> リソースからタグを削除すると、リソースへのアクセスに影響を与える可能性があります。タグを削除する前に、タグを使用してリソースへのアクセスを制御する可能性のある AWS Identity and Access Management (IAM) ポリシーを確認してください。

Security Hub CSPM API

Security Hub CSPM リソースからタグを削除するには (API)

プログラムでリソースから 1 つ以上のタグを削除するには、Security Hub CSPM API の UntagResource オペレーションを使用します。リクエストで、`resourceArn`パラメーターを使用して、タグを削除するリソースの Amazon リソースネーム (ARN) を指定します。`tagKeys`パラメータを使用して、削除するタグのタグキーを指定します。複数のタグを削除するには、削除する各タグの`tagKeys`パラメーターと引数をアンパサンド (&) で区切って追加します (例: `tagKeys=`*`key1`*`&tagKeys=`*`key2`*)。リソースから特定のタグ値 (タグキーではない) のみを削除するには、タグを削除する代わりにタグを編集します。

を使用している場合は AWS CLI、untag-resource コマンドを実行して、リソースから 1 つ以上のタグを削除します。`resource-arn`パラメータには、タグを削除するリソースの ARN を指定し

ます。tag-keysパラメータを使用して、削除するタグのタグキーを指定します。例えば、次のコマンドは、指定した設定ポリシーから Environment タグ (タグキーとタグ値の両方) を削除します。

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

ここで resource-arn ではタグを削除する設定ポリシーの ARN を指定し、*Environment* は削除するタグのタグキーです。

リソースから複数のタグを削除するには、追加の各タグ キーを tag-keys パラメーターの引数として追加します。例:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment Owner
```

オペレーションが成功すると、Security Hub CSPM は空の HTTP 200 レスポンスを返します。それ以外の場合、Security Hub CSPM は、オペレーションが失敗した理由を示す HTTP 4xx または 500 レスポンスを返します。

Security Hub のクォータ

AWS アカウント には、それぞれについて、以前は制限と呼ばれていた特定のデフォルトクォータがあります AWS のサービス。これらのクォータは、アカウントのサービスリソースまたはオペレーションの最大数です。このトピックでは、アカウントの AWS Security Hub リソースとオペレーションに適用されるクォータにリンクします。特に明記されていない限り、クォータはそれぞれの AWS リージョンのアカウントに適用されます。

クォータによっては、引き上げることができないものもあります。クォータの引き上げをリクエストするには、Service Quotas コンソール を使用します。クォータの引き上げをリクエストする方法についての説明は、Service Quotas ユーザーガイド のクォータ引き上げリクエストを参照してください。Service Quotas コンソールでクォータを使用できない場合は、 のサービス制限の引き上げフォームを使用してクォータの引き上げを AWS Support Center Console リクエストします。

最大クォータ

AWS Security Hub リソースに適用されるクォータのリストについては、のAWS 「Security Hub エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。

レートクォータ

AWS Security Hub API オペレーションに適用されるクォータのリストについては、AWS Security Hub API リファレンスを参照してください。

Security Hub CSPM でクロスリージョン集約を設定すると、 を 1 回呼び出す`BatchImportFindings`と、リンクされたリージョンと集約リージョン`BatchUpdateFindings`に影響します。`GetFindings` オペレーションは、リンクされたリージョンと集約リージョンから結果を取得します。ただし、`BatchEnableStandards` と `UpdateStandardsControl` オペレーションはリージョンに固有です。

AWS Security Hub ユーザーガイドのドキュメント履歴

次の表は、Security Hub と AWS Security Hub CSPM の前回のリリース以降のドキュメントの重要な変更点を示しています。新しい CSPM セキュリティコントロールのリリースの場合、日付は、サポートされている でコントロールが利用可能になるタイミングを指定します AWS リージョン。サポートされているすべてのリージョンでコントロールが使用可能になるまでに 1～2 週間かかる場合があります。

AWS Security Hub ユーザーガイドの更新に関する通知については、RSS フィードをサブスクライブできます。

変更	説明	日付
セキュリティ標準とコントロールの更新	Amazon Redshift の制限により、Redshift.9 および RedshiftServerless.7 コントロールを廃止し、2025 年 9 月 15 日に該当するすべての標準から削除する予定です。現在、これらのコントロールは AWS Foundational Security Best Practices (FSBP) 標準と NIST SP 800-53 Rev. 5 標準に適用されます。Redshift.9 コントロールは、AWS Control Tower サービスマネージド標準にも適用されます。	2025 年 8 月 15 日
ASFF の新しいリソース詳細オブジェクト	AWS Security Finding 形式 (ASFF) に`CodeRepository` リソースオブジェクトが含まれるようになりました。このオブジェクトは、AWS リソースに接続し、脆弱性をスキャンするように Amazon Inspector を設定した	2025 年 8 月 1 日

	外部コードリポジトリに関する詳細を提供します。	
リージョナルな可用性	Security Hub CSPM がアジアパシフィック (台北) リージョンで利用可能になりました。Security Hub CSPM が現在利用可能な AWS リージョン の完全なリストについては、のAWS 「Security Hub エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。	2025 年 7 月 23 日
新しいサードパーティー統合	Dynatrace は、Security Hub CSPM から検出結果を受信できる新しいサードパーティー統合です。	2025 年 7 月 18 日

新しいセキュリティコントロール	Security Hub CSPM は 13 の新しいコントロールをリリースしました。ほとんどのコントロールは、 AWS Foundational Security Best Practices (FSBP) 標準をサポートしています。一部のコントロールは、NIST SP 800-53 Rev. 5 の要件をサポートしています。 • AWS FSBP 標準では、該当するコントロールIDs は CloudFront.15、Cognito.2、EC2.180、ELB.18、MSK.4、MSK.5、MSK.6、RDS.45、Redshift.18、S3.25、SSM.6、SSM.7 です。 • NIST SP 800-53 Rev. 5 の場合、該当するコントロール IDs は Lambda.7 と RDS.45 です。	2025 年 7 月 15 日
コントロール検出結果の生成の更新	コンプライアンスの変更を追跡しやすくするために、Security Hub CSPM は、個々のリソースのコンプライアンスステータスに変更があった場合に、新しい検出結果を生成する代わりに既存のコントロール検出結果を更新するようになりました。つまり、個々の検出結果から提供されたデータを使用して、特定のコントロールに対する特定のリソースのコンプライアンス変更を追跡できます。	2025 年 7 月 3 日

セキュリティ標準とコントロールの更新	PCI DSS v4.0.1 標準から IAM.13 コントロールを削除しました。また、NIST SP 800-171 Revision 2 標準から IAM.17 コントロールを削除しました。標準では、これらのコントロールが提供するチェックが明示的に必要ありません。また、IAM パスワードポリシーをチェックする特定のコントロールについて、IAM.7 および IAM.10 から IAM.17 まで、これらの標準に関連する要件の詳細を更新しました。	2025 年 6 月 30 日
結果の保持の更新	Security Hub CSPM は、90 日ではなく 30 日間アーカイブされた検出結果を保存するようになりました。これにより、検出結果のノイズを減らすことができます。長期間保持するには、Amazon EventBridge ルールでカスタムアクションを使用して、結果を S3 バケットにエクスポートできます。	2025 年 6 月 20 日

既存のマネージドポリシーの更新	Security Hub CSPM は、 という名前AWS の管理ポリシーに新しいアクセス許可を追加しましたAWSSecurityHubOrganizationsAccess 。アクセス許可により、組織管理者は組織内で Security Hub と Security Hub CSPM を有効化および管理できます。Security Hub CSPM は、 という名前の管理 AWS ポリシーに新しいアクセス許可も追加しましたAWSSecurityHubFullAccess 。アクセス許可により、プリンシパルは Security Hub のサービスにリンクされたロールを作成できます。	2025 年 6 月 18 日
Security Hub のパブリックプレビューリリースと新しい管理ポリシー	AWS Security Hub のパブリックプレビューリリースと AWS Security Hub ユーザーガイド。このリリースには、新しい AWS 管理ポリシー が含まれていますAWSSecurityHubV2ServiceRolePolicy 。このポリシーにより、Security Hub はお客様の組織内およびお客様に代わって AWS Config ルールと Security Hub リソースを管理できます。Security Hub はプレビューリリースであり、変更される可能性があります。	2025 年 6 月 17 日

セキュリティ標準とコントロールの更新	PCI DSS v4.0.1 標準から IAM.10 コントロールを削除しました。このコントロールは、IAM ユーザーのアカウントパスワードポリシーが、パスワードの最小長 7 文字を含む最小要件を満たしているかどうかをチェックします。PCI DSS v4.0.1 では、パスワードを 8 文字以上にする必要があります。IAM.10 コントロールは、異なるパスワード要件を持つ PCI DSS v3.2.1 標準に引き続き適用されます。	2025 年 5 月 30 日
新しいセキュリティ標準	Security Hub CSPM は、NIST SP 800-171 Revision 2 サイバーセキュリティとコンプライアンスフレームワークに沿ったセキュリティ標準を提供するようになりました。この新しい標準には、60 を超える既存のセキュリティコントロールが含まれています。コントロールは、フレームワークで定義された要件のサブセットへの準拠について、特定の AWS のサービス および リソースを評価する自動チェックを実行します。	2025 年 5 月 29 日

セキュリティコントロールの更新	Security Hub CSPM は、すべてのコントロールのリリースをロールバックしました AWS リージョン。[RDS.46] RDS DB インスタンスは、インターネットゲートウェイへのルートを持つパブリックサブネットにデプロイしないでください。 以前は、このコントロールは AWS Foundational Security Best Practices (FSBP) 標準をサポートしていました。	2025 年 5 月 8 日

新しいセキュリティコントロール	Security Hub CSPM は 9 つの新しいコントロールをリリースしました。ほとんどのコントロールは、 AWS Foundational Security Best Practices (FSBP) 標準をサポートしています。一部のコントロールは、NIST SP 800-53 Rev. 5 の要件をサポートしています。 • AWS FSBP 標準では、該当するコントロールIDs は DocumentDB.6、RDS.44、RedshiftServerless.2、RedshiftServerless.3、RedshiftServerless.5、RedshiftServerless.6、RedshiftServerless.7 です。 • NIST SP 800-53 Rev. 5 の場合、該当するコントロールIDs は CloudTrail.10、RedshiftServerless.4、RedshiftServerless.7 です。	2025 年 5 月 7 日

新しいセキュリティコントロール	Security Hub CSPM が 24 の新しいコントロールをリリースしました。ほとんどのコントロールは、 AWS Foundational Security Best Practices (FSBP) または AWS Resource Tagging 標準をサポートしています。一部のコントロールは、NIST SP 800-53 Rev. 5 の要件をサポートしています。 • AWS FSBP 標準では、該当するコントロールIDs は EC2.173、RDS.41、RDS.42、SageMaker.8 です。 • AWS リソースタグ付け標準の場合、該当するコントロールIDs は、Amplify.1、Amplify.2、Batch.4、DataSync.2、EC2.174、EC2.175、EC2.176、EC2.177、EC2.178、EC2.179、R17、SageMaker.6、SageMaker.7、SSM.5、Transfer.4、Transfer.5、Transfer.6、Transfer.7 です。 • NIST SP 800-53 Rev. 5 の場合、該当するコントロールIDs は ECS.17 と RDS.42 です。	2025 年 4 月 16 日

新しいセキュリティコントロール	Security Hub CSPM はAWS 、Foundational Security Best Practices 標準の 4 つの新しいコントロールをリリースしました。コントロールは次のとおりです。 • the section called “[FSx.3] FSx for OpenZFS ファイルシステムは、マルチ AZ 配置用に設定する必要があります” • the section called “[FSx.4] FSx for NetApp ONTAP ファイルシステムは、マルチ AZ 配置用に設定する必要があります” • the section called “[FSx.5] FSx for Windows File Server ファイルシステムは、マルチ AZ 配置用に設定する必要があります” • the section called “[RedshiftServerless.1] Amazon Redshift Serverless ワークグループは拡張 VPC ルーティングを使用する必要があります”	2025 年 3 月 18 日

セキュリティ標準とコントロールの更新	RDS.18 セキュリティコントロールを AWS Foundational Security Best Practices 標準から削除し、NIST SP 800-53 Rev. 5 要件の自動チェックを削除しました。Amazon EC2-Classic ネットワークは廃止されたため、Amazon Relational Database Service (Amazon RDS) インスタンスは VPC の外部にデプロイできなくなります。コントロールは引き続きAWS Control Tower サービスマネージド標準の一部です。	2025 年 3 月 7 日
コントロールの検出結果の更新	Security Hub CSPM は、コントロールがチェックするリソースのタイプ AWS Config でリソース記録が有効になっていない場合、有効なコントロール`WARNING`の検出結果を生成するようになりました。これにより、セキュリティコントロールチェックで潜在的な設定ギャップを特定して対処できます。	2025 年 2 月 25 日

新しいセキュリティコントロール	Security Hub CSPM が 11 の新しいコントロールをリリースしました。コントロールは次のとおりです。 • the section called “[Connect.2] Amazon Connect インスタンスでは CloudWatch ログ記録が有効になっている必要があります” • the section called “[ECR.5] ECR リポジトリはカスタマーマネージドで暗号化する必要があります AWS KMS keys” • the section called “[ELB.17] リスナーを使用するアプリケーションおよび Network Load Balancer は、推奨されるセキュリティポリシーを使用する必要があります” • the section called “[Glue.4] AWS Glue Spark ジョブは、サポートされているバージョンの で実行する必要があります AWS Glue” • the section called “[GuardDuty.11] GuardDuty Runtime Monitoring を有効にする必要があります” • the section called “[GuardDuty.12] GuardDuty ECS Runtime Monitoring を有効にする必要があります”	2025 年 2 月 24 日

- the section called “[GuardDuty.13] GuardDuty EC2 Runtime Monitoring を有効にする必要があります”
- the section called “[Network Firewall.10] Network Firewall ファイアウォールでは、サブネット変更保護を有効にする必要があります”
- the section called “[RDS.40] RDS for SQL Server DB インスタンスは CloudWatch Logs にログを発行する必要があります”
- the section called “[SQS.3] SQS キューアクセスポリシーはパブリックアクセスを許可しないでください”
- the section called “[Transfer.3] Transfer Family コネクタではログ記録が有効になっている必要があります”

新しいセキュリティコントロール	Security Hub CSPM は、AWS Resource Tagging Standard 用に 37 の新しいコントロールをリリースしました。Security Hub CSPM は、次の新しいコントロールもリリースしました。 • the section called “[EMR.3] Amazon EMR セキュリティ設定は保管時に暗号化する必要があります” • the section called “[EMR.4] Amazon EMR セキュリティ設定は転送中に暗号化する必要があります” • the section called “[SageMaker.5] SageMaker モデルでは、ネットワーク分離を有効にする必要があります”	2025年 1 月 22 日
新しいセキュリティコントロール	Security Hub CSPM がリリースした EC2.172 EC2 VPC パブリックアクセスブロック設定は、インターネットゲートウェイトラフィックをブロックする必要があります。	2025年 1 月 15 日

新しいセキュリティコントロール	次の新しい Security Hub CSPM コントロールが利用可能になりました。 • the section called “[Cognito.1] Cognito ユーザープールでは、標準認証の完全な関数強制モードで脅威保護を有効にする必要があります” • the section called “[RDS.38] RDS for PostgreSQL DB インスタンスは転送中に暗号化する必要があります” • the section called “[RDS.39] RDS for MySQL DB インスタンスは転送中に暗号化する必要があります” • the section called “[Redshift.16] Redshift クラスターサブネットグループには、複数のアベイラビリティーゾーンからのサブネットが必要です”	2024 年 12 月 17 日
Security Hub CSPM が PCI DSS v4.0.1 をサポート	Security Hub CSPM が Payment Card Industry Data Security Standard (PCI DSS) の v4.0.1 をサポートするようになりました。標準とその標準に適用されるコントロールの詳細については、Security Hub CSPM の「PCI DSS」を参照してください。	2024 年 12 月 11 日

Security Hub CSPM が GuardDuty 攻撃シーケンスの検出結果を受け取る	Security Hub CSPM は、Amazon GuardDuty 拡張脅威検出から攻撃シーケンスの検出結果を受信するようになりました。攻撃シーケンスの検出結果の詳細は、 AWS Security Finding 形式 (ASFF) の検出オブジェクトで確認できます。	2024 年 12 月 1 日
新しい でサポートされている Security Hub CSPM AWS リージョン	Security Hub CSPM がアジアパシフィック (マレーシア) リージョンで利用可能になりました。一部のセキュリティコントロールには、リージョンの制限があります。このリージョンで利用できないコントロールのリストについては、「Security Hub CSPM コントロールのリージョン制限」を参照してください。	2024 年 11 月 22 日
Config.1 の変更	Security Hub CSPM は、Config.1 コントロールの重要度を から `MEDIUM`に増やし`CRITICAL`、Config.1 の検出に失敗した新しいステータスコードとステータス理由を追加しました。変更の詳細については、Security Hub CSPM コントロールの変更ログの 2024 年 11 月 20 日のエントリを参照してください。	2024 年 11 月 20 日

新しいセキュリティコントロール	次の新しい Security Hub CSPM コントロールが利用可能になりました。これらのコントロールは、 AWS Foundational Security Best Practices および NIST SP 800-53 Rev. 5 の一部であり、管理する仮想プライベートクラウド (VPC) に AWS のサービス または AWS リソースのインターフェイス VPC エンドポイントがあるかどうかを評価します。 • the section called “[EC2.55] VPCs は ECR API のインターフェイスエンドポイントで設定する必要があります” • the section called “[EC2.56] VPCsは Docker Registry のインターフェイスエンドポイントで設定する必要があります” • the section called “[EC2.57] VPCsは Systems Manager のインターフェイスエンドポイントで設定する必要があります” • the section called “[EC2.58] VPCs は、Systems Manager Incident Manager Contacts のインターフェイスエンドポイントで設定する必要があります”	2024 年 11 月 15 日

- the section called “[EC2.60] VPCsは Systems Manager Incident Manager のインターフェイスエンドポイントで設定する必要があります”

新しいセキュリティコントロール	次の新しい Security Hub CSPM コントロールが利用可能になりました。 • the section called “[AppSync .1] AWS AppSync API キャッシュは保管時に暗号化する必要があります” • the section called “[AppSync .6] AWS AppSync API キャッシュは転送中に暗号化する必要があります” • the section called “[EC2.170] EC2 起動テンプレートは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用することをお勧めします” • the section called “[EC2.171] EC2 VPN 接続では、ログ記録が有効になっている必要があります” • the section called “[EFS .8] EFS ファイルシステムは保管中に暗号化する必要があります” • the section called “[KMS.5] KMS キーはパブリックにアクセスしないでください” • the section called “[SNS.4] SNS トピックアクセスポリシーはパブリックアクセスを許可しないでください”	2024 年 10 月 18 日

新しいセキュリティコントロール	次の新しい Security Hub CSPM コントロールが利用可能になりました。 • the section called “[ECS.16] ECS タスクセットはパブリック IP アドレスを自動的に割り当てないでください。” • the section called “[GuardDuty.7] GuardDuty EKS ランタイムモニタリングを有効にする必要があります” • the section called “[Kinesis.3] Kinesis ストリームには適切なデータ保持期間が必要です” • the section called “[MSK.3] MSK Connect コネクタは転送中に暗号化する必要があります” • the section called “[RDS.36] RDS for PostgreSQL DB は CloudWatch Logs にログを発行する必要があります” • the section called “[RDS.37] Aurora PostgreSQL DB クラスターでは、ログを CloudWatch Logs に発行する必要があります” • the section called “[S3.24] S3 マルチリージョンアクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります”	2024 年 10 月 3 日

新しいセキュリティコントロール	次の新しい Security Hub CSPM コントロールが利用可能になりました。 • the section called “[Athena.4] Athena ワークグループでは口グ記録が有効になっている必要があります” • the section called “[CodeBuild.7] CodeBuild レポートグループのエクスポートは保管時に暗号化する必要があります” • the section called “[DataSync.1] DataSync タスクでは口グ記録が有効になっている必要があります” • the section called “[EFS .7] EFS ファイルシステムでは、自動バックアップが有効になっている必要があります” • Glue.2 (廃止) • the section called “[Glue.3] AWS Glue 機械学習変換は保管時に暗号化する必要があります” • the section called “[WorkSpaces.1] WorkSpaces ユーザーボリュームは保管中に暗号化する必要があります” • the section called “[WorkSpaces.2] WorkSpaces ルートボリュームは保管中に暗号化する必要があります”	2024 年 8 月 30 日

新しい検出結果パネル	Security Hub CSPM コンソールの新しい検出結果パネルは、検出結果に対する迅速なアクションの実行、リソースの詳細と検出結果履歴の確認、検出結果に関するその他の関連情報の検索に役立ちます。	2024 年 8 月 16 日
Config.1 コントロールの更新	Config.1 コントロール AWS Config は、 が有効になっているかどうかをチェックし、サービスにリンクされたロールを使用し、有効なコントロールのリソースを記録します。Security Hub CSPM に、 という名前のカスタムコントロールパラメータが追加されましたincludeConfigServiceLinkedRoleCheck 。このパラメータを false に設定することで、AWS Config がサービスにリンクされたロールを使用するかどうかの確認をオプトアウトできます。	2024 年 8 月 15 日
リンクされたリージョンのないホームリージョンを指定する	結果アグリゲータを作成し、ホームリージョン AWS リージョン にリンクせずにホームリージョンを確立できるようになりました。これにより、リンクされたリージョンを指定せずに中央設定を有効にすることができます。	2024 年 7 月 25 日

他のリージョンで使用できるコントロールを選択する	米国東部 (バージニア北部) や米国東部 (オハイオ) など AWS リージョン、次のコントロールが追加で利用可能になりました。 • the section called “[DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります” • the section called “[DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります” • the section called “[DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります” • the section called “[DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります” • the section called “[DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります” • the section called “[EFS.6] EFS マウントターゲットは、起動時にパブリック IP アドレスを割り当てるサブネットに関連付けるべきではありません”	2024 年 7 月 15 日

- the section called “[EKS.3] EKS クラスターは暗号化された Kubernetes シークレットを使用する必要があります”
- the section called “[FSx.2] FSx for Lustre ファイルシステムでは、タグをバックアップにコピーするように設定する必要があります”
- the section called “[MQ.2] ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります”
- the section called “[MQ.3] Amazon MQ ブローカーでは、自動マイナーバージョンアップグレードが有効になっている必要があります”
- the section called “[Opensearch.11] OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です”
- the section called “[Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの入力を許可する必要があります”
- the section called “[SageMaker.4] SageMaker エンドポイントの本番稼働バリアントの初期インスタ

ンス数は 1 より大きい必要があります”

- the section called “[Service Catalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります”
- the section called “[Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください”

新しいセキュリティコントロール	次の新しい Security Hub CSPM コントロールが利用可能になりました。 • the section called “[GuardDuty.5] GuardDuty EKS 監査ログモニタリングを有効にする必要があります” • the section called “[GuardDuty.6] GuardDuty Lambda Protection を有効にする必要があります” • the section called “[GuardDuty.8] GuardDuty Malware Protection for EC2 を有効にする必要があります” • the section called “[GuardDuty.9] GuardDuty RDS Protection を有効にする必要があります” • the section called “[GuardDuty.10] GuardDuty S3 Protection を有効にする必要があります” • the section called “[Inspector.1] Amazon Inspector EC2 スキャンを有効にする必要があります” • the section called “[Inspector.2] Amazon Inspector ECR スキャンを有効にする必要があります” • the section called “[Inspector.3] Amazon Inspector	2024 年 7 月 11 日

Lambda コードスキャンを有効にする必要があります”

- the section called “[Inspector.4] Amazon Inspector Lambda 標準スキャンを有効にする必要があります”

CIS AWS Foundations Benchmark v3.0.0 のリリース	Security Hub CSPM が Center for Internet Security (CIS) AWS Foundations Benchmark v3.0.0 をリリースしました。このリリースには、以下の新しいコントロールと、いくつかの既存のコントロールへのマッピングが含まれています。 • the section called “[EC2.53] EC2 セキュリティグループが 0.0.0.0/0 からリモートサーバー管理ポートへの入力を許可することがないようにする必要があります” • the section called “[EC2.54] EC2 セキュリティグループは ::/0 からリモートサーバー管理ポートへの入力を許可しない必要があります” • the section called “[IAM.26] IAM で管理されている期限切れの SSL/TLS 証明書は削除する必要があります” • the section called “[IAM.27] IAM ID に AWSCloudShellFullAccess ポリシーをアタッチしないでください” • the section called “[IAM.28] IAM Access Analyzer 外部アクセスアナライザーを有効にする必要があります” • the section called “[S3.22] S3 汎用バケットはオブジェ	2024 年 5 月 13 日

クトレベルの書き込みイベントをログに記録する必要があります”

- the section called “[S3.23] S3 汎用バケットはオブジェクトレベルの読み取りイベントをログに記録する必要があります”

新しいセキュリティコントロール	次の新しい Security Hub CSPM コントロールが利用可能になりました。 • the section called “[DataFirehose.1] Firehose 配信ストリームは保管時に暗号化する必要があります” • the section called “[DMS.10] Neptune データベースの DMS エンドポイントでは、IAM 認証が有効になっている必要があります” • the section called “[DMS.11] MongoDB の DMS エンドポイントでは、認証メカニズムが有効になっている必要があります” • the section called “[DMS.12] Redis OSS の DMS エンドポイントでは TLS が有効になっている必要があります” • the section called “[DynamoDB.7] DynamoDB Accelerator クラスターは、保管中に暗号化する必要があります” • the section called “[EFS.6] EFS マウントターゲットは、起動時にパブリック IP アドレスを割り当てるサブネットに関連付けるべきではありません” • the section called “[EKS.3] EKS クラスターは暗号化さ	2024 年 5 月 3 日

れた Kubernetes シークレットを使用する必要があります”

- the section called “[FSx.2] FSx for Lustre ファイルシステムでは、タグをバックアップにコピーするように設定する必要があります”
- the section called “[MQ.2] ActiveMQ ブローカーは監査ログを CloudWatch にストリーミングする必要があります”
- the section called “[MQ.3] Amazon MQ ブローカーでは、自動マイナーバージョンアップグレードが有効になっている必要があります”
- the section called “[Opensearch.11] OpenSearch ドメインには少なくとも 3 つの専用プライマリノードが必要です”
- the section called “[Redshift.15] Redshift セキュリティグループは、制限されたオリジンからのみクラスターポートへの入力を許可する必要があります”
- the section called “[SageMaker.4] SageMaker エンドポイントの本番稼働バリアントの初期インスタンス数は 1 より大きい必要があります”

	• the section called “[Service Catalog.1] Service Catalog ポートフォリオは AWS 組織内でのみ共有する必要があります” • the section called “[Transfer.2] Transfer Family サーバーはエンドポイント接続に FTP プロトコルを使用しないでください”	
AWS リソースタグ付け標準	Security Hub CSPM のAWS リソースタグ付け標準が、標準に適用される新しいコントロールとともに一般公開されました。	2024 年 4 月 30 日
既存のマネージドポリシーの更新	Security Hub CSPM は、AWS のサービス と 製品の料金詳細を取得`AmazonSecurityHubFullAccess` するために、 という名前の AWS マネージドポリシーを更新しました。	2024 年 4 月 24 日
コントロールパラメータのコンテキスト内の設定	中央設定を使用する場合、Security Hub CSPM コンソールのコントロールの詳細ページから、コンテキストでコントロールパラメータを設定できるようになりました。	2024 年 3 月 29 日
既存のマネージドポリシーの更新	Security Hub CSPM は、 `Sid` フィールドを追加して という名前の管理AWS ポリシーを更新`AWSSecurityHubReadOnlyAccess` しました。	2024 年 2 月 22 日

新しいセキュリティコントロール	コントロール [Macie.2] Macie 自動機密データ検出を有効にすることができるようになりました。このコントロールのリージョン制限については、「リージョン別のコントロールの可用性」を参照してください。	2024 年 2 月 19 日
Security Hub CSPM がカナダ西部 (カルガリー) で利用可能に	Security Hub CSPM がカナダ西部 (カルガリー) で利用可能になりました。特定のセキュリティコントロールを除き、すべての Security Hub CSPM 機能がこのリージョンで利用可能になりました。詳細については、「リージョン別のコントロールの可用性」を参照してください。	2023 年 12 月 20 日

新しいセキュリティコントロール	次の新しい Security Hub CSPM コントロールが利用可能になりました。 • the section called “[Backup.1] AWS Backup 復旧ポイントは保管時に暗号化する必要があります” • the section called “[DynamoDB.6] DynamoDB テーブルで、削除保護が有効になっている必要があります” • the section called “[EC2.51] EC2 Client VPN エンドポイントでは、クライアント接続ログ記録が有効になっている必要があります” • the section called “[EKS.8] EKS クラスターでは、監査ログ記録が有効になっている必要があります” • the section called “[EMR.2] Amazon EMR ブロックパブリックアクセス設定を有効にする必要があります” • the section called “[FSx.1] FSx for OpenZFS ファイルシステムでは、タグをバックアップとボリュームにコピーするように設定する必要があります” • the section called “[Macie.1] Amazon Macie を有効にする必要があります”	2023 年 12 月 14 日

- the section called “[MSK.2] MSK クラスターでは、拡張モニタリングを設定する必要があります”
- the section called “[Neptune.9] Neptune DB クラスターを複数のアベイラビリティーゾーンにデプロイする必要があります”
- the section called “[Network Firewall.1] Network Firewall ファイアウォールを複数のアベイラビリティーゾーンにデプロイする必要があります”
- the section called “[Network Firewall.2] Network Firewall ログ記録を有効にする必要があります”
- the section called “[Opensearch.10] OpenSearch ドメインには、最新のソフトウェアアップデートがインストールされている必要があります”
- the section called “[PCA.1] AWS Private CA ルート認証機関を無効にする必要があります”
- the section called “[S3.19] S3 アクセスポイントでは、ブロックパブリックアクセス設定を有効にする必要があります”

	• the section called “[S3.20] S3 汎用バケットでは MFA 削除が有効になっている必要があります”	
検出結果の強化	Security Hub CSPM は、新しい検出結果フィールド `AwsAccountName` 、`ApplicationArn` 、 `ApplicationName` を AWS Security Finding 形式 (ASFF) に追加しました。	2023 年 11 月 27 日
[概要] ダッシュボードの機能強化	Security Hub CSPM コンソールの 概要ページでさらに多くのダッシュボードウィジェットにアクセスし、ダッシュボードフィルターセットを保存して特定のセキュリティ問題にすばやく焦点を合わせ、ダッシュボードレイアウトをカスタマイズできるようになりました。	2023 年 11 月 27 日
中央設定	中央設定は利用が可能になりました。中央設定では、Security Hub CSPM の委任管理者は、複数の組織アカウント、組織単位 (OUs)、リージョンにわたって Security Hub CSPM、標準、コントロールを設定できます。	2023 年 11 月 27 日

マネージドポリシーの更新	Security Hub CSPM は、Security Hub CSPM がカスタマイズ可能なセキュリティコントロールプロパティを読み取って更新できるようにする新しいアクセス許可を `AWSSecurityHubServiceRolePolicy` マネージドポリシーに追加しました。	2023 年 11 月 26 日
カスタムコントロールパラメータ	選択した Security Hub CSPM コントロールのパラメータ値をカスタマイズできるようになりました。これにより、特定のコントロールの検出結果をビジネス要件やセキュリティ上の期待とより関連性のあるものにすることができます。	2023 年 11 月 26 日
マネージドポリシーの更新	Security Hub CSPM は、それぞれ Security Hub CSPM 機能と との統合を使用できると `AWSSecurityHubFullAccess` `AWSSecurityHubOrganizationsAccess` 管理ポリシーを更新しました AWS Organizations。	2023 年 11 月 16 日

サービスマネージドスタンダードに追加された既存のセキュリティコントロール：AWS Control Tower	以下の既存の Security Hub CSPM コントロールがサービスマネージドスタンダードに追加されました AWS Control Tower。 • ACM.2 • AppSync.5 • CloudTrail.6 • DMS.9 • DocumentDB.3 • DynamoDB.3 • EC2.23 • EKS.1 • ElastiCache.3 • ElastiCache.4 • ElastiCache.5 • ElastiCache.6 • EventBridge.3 • KMS.4 • Lambda.3 • MQ.5 • MQ.6 • MSK.1 • RDS.12 • RDS.15 • S3.17	2023 年 11 月 14 日

マネージドポリシーの更新	Security Hub CSPM は、Security Hub CSPM が検出結果に関連するリソースタグを読み取ることを許可する新しいタグ付けアクセス許可を `AWSSecurityHubServiceRolePolicy` マネージドポリシーに追加しました。	2023 年 11 月 7 日

新しいセキュリティコントロール	次の新しい Security Hub CSPM コントロールが利用可能になりました。 • the section called “[AppSync.5] AWS AppSync GraphQL APIsは API キーで認証しないでください” • the section called “[DMS.6] DMS レプリケーションインスタンスでは、マイナーバージョンの自動アップグレードが有効になっている必要があります。” • the section called “[DMS.7] ターゲットデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。” • the section called “[DMS.8] ソースデータベースの DMS レプリケーションタスクでは、ロギングが有効になっている必要があります。” • the section called “[DMS.9] DMS エンドポイントは SSL を使用する必要があります。” • the section called “[DocumentDB.3] Amazon DocumentDB 手動クラスタースナップショットはパブリックにできません”	2023 年 10 月 10 日

- the section called “[DocumentDB.4] Amazon DocumentDB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります”
- the section called “[DocumentDB.5] Amazon DocumentDB では、削除保護が有効になっている必要があります”
- the section called “[ECS.9] ECS タスク定義にはログ設定が必要です。”
- the section called “[EventBridge.3] Amazon EventBridge カスタムイベントバスにリソースポリシーがアタッチされている必要があります”
- the section called “[EventBridge.4] EventBridge グローバルエンドポイントでは、イベントの複製が有効になっている必要があります”
- the section called “[MSK.1] MSK クラスターはブローカーノード間の転送時に暗号化される必要があります”
- the section called “[MQ.5] ActiveMQ ブローカーはアクティブ/スタンバイデプロイメントモードを使用する必要があります”
- the section called “[MQ.6] RabbitMQ ブローカーはク

ラスターデプロイメントモードを使用する必要があります。”

- the section called “[Network Firewall.9] Network Firewall は削除保護を有効にする必要があります”
- the section called “[RDS.34] Aurora MySQL DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります”
- the section called “[RDS.35] RDS DB クラスターは自動マイナーバージョンアップグレードを有効にする必要があります”
- the section called “[Route53.2] Route 53 のパブリックホストゾーンは DNS クエリをログに記録する必要があります”
- the section called “[WAF.12] AWS WAF ルールでは CloudWatch メトリクスを有効にする必要があります”

マネージドポリシーの更新	Security Hub CSPM がアカウントおよび組織単位 (OU) 情報を取得できるようにする新しい Organizations アクションを `AWSSecurityHubServiceRolePolicy` 管理ポリシーに追加しました。また、Security Hub CSPM が標準やコントロールなどのサービス設定を読み取って更新できるようにする新しい Security Hub CSPM アクションを追加しました。	2023 年 9 月 27 日

サービスマネージドスタンダードに追加された既存のセキュリティコントロール：AWS Control Tower	以下の既存の Security Hub CSPM コントロールがサービスマネージドスタンダードに追加されました AWS Control Tower。 • the section called “[Athena.1] Athena ワークグループは、保管中に暗号化する必要があります” • the section called “[DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります” • the section called “[DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です” • the section called “[Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります” • the section called “[Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります” • the section called “[Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください” • the section called “[Neptune.4] Neptune DB クラスター	2023 年 9 月 26 日

では、削除保護が有効になっている必要があります”

- the section called “[Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります”
- the section called “[Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります”
- the section called “[Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります”
- the section called “[Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります”
- the section called “[RDS.27] RDS DB クラスターは保管中に暗号化する必要があります”

統合されたコントロールビューと統合されたコントロールの検出結果が AWS GovCloud (US)で利用可能に	統合されたコントロールビューと統合されたコントロールの検出結果が AWS GovCloud (US) Regionで利用できるようになりました。Security Hub CSPM コンソールのコントロールページには、標準全体のすべてのコントロールが表示されます。各コントロールは、標準全体で同じコントロール ID を持ちます。統合されたコントロールの検出結果を有効にすると、コントロールが複数の有効な標準に適用される場合でも、セキュリティチェックごとに 1 つの検出結果を受け取ります。	2023 年 9 月 6 日
統合されたコントロールビューと統合されたコントロールの検出結果が中国リージョンで利用可能に	統合されたコントロールビューと統合されたコントロールの検出結果が中国リージョンで利用できるようになりました。Security Hub CSPM コンソールのコントロールページには、標準全体のすべてのコントロールが表示されます。各コントロールは、標準全体で同じコントロール ID を持ちます。統合されたコントロールの検出結果を有効にすると、コントロールが複数の有効な標準に適用される場合でも、セキュリティチェックごとに 1 つの検出結果を受け取ります。	2023 年 8 月 28 日

Security Hub CSPM がイスラエル (テルアビブ) リージョンで利用可能に	Security Hub CSPM がイスラエル (テルアビブ) で利用可能になりました。特定のセキュリティコントロールを除き、すべての Security Hub CSPM 機能がこのリージョンで利用可能になりました。詳細については、「リージョン別のコントロールの可用性」を参照してください。	2023 年 8 月 8 日

新しいセキュリティコントロール	次の新しい Security Hub CSPM コントロールが利用可能になりました。 • the section called “[Athena.1] Athena ワークグループは、保管中に暗号化する必要があります” • the section called “[DocumentDB.1] Amazon DocumentDB クラスターは、保管中に暗号化する必要があります” • the section called “[DocumentDB.2] Amazon DocumentDB クラスターには、適切なバックアップ保持期間が必要です” • the section called “[Neptune.1] Neptune DB クラスターは、保管中に暗号化する必要があります” • the section called “[Neptune.2] Neptune DB クラスターでは、監査ログを CloudWatch Logs に発行する必要があります” • the section called “[Neptune.3] Neptune DB クラスタースナップショットはパブリックにしないでください” • the section called “[Neptune.4] Neptune DB クラスターでは、削除保護が有効になっている必要があります”	2023 年 7 月 28 日

	• the section called “[Neptune.5] Neptune DB クラスターでは、自動バックアップが有効になっている必要があります” • the section called “[Neptune.6] Neptune DB クラスタースナップショットは、保管中に暗号化する必要があります” • the section called “[Neptune.7] Neptune DB クラスターでは、IAM データベース認証が有効になっている必要があります” • the section called “[Neptune.8] Neptune DB クラスターでは、タグをスナップショットにコピーするように設定する必要があります” • the section called “[RDS.27] RDS DB クラスターは保管中に暗号化する必要があります”	
自動化ルール基準の新しい演算子	自動化ルールのマッピングおよび文字列条件に対して、CONTAINS 比較演算子と NOT_CONTAINS 比較演算子を使用できるようになりました。	2023 年 7 月 25 日

自動化ルール	Security Hub CSPM では、指定した基準に基づいて結果を自動的に更新する自動化ルールが提供されるようになりました。	2023 年 6 月 13 日
新しいサードパーティー統合	Snyk は、Security Hub CSPM に結果を送信する新しいサードパーティー統合です。	2023 年 6 月 12 日

サービスマネージドスタンダードに追加された既存のセキュリティコントロール：AWS Control Tower	以下の既存の Security Hub CSPM コントロールがサービスマネージドスタンダードに追加されました AWS Control Tower。 • the section called “[Account.1] のセキュリティ連絡先情報は に提供する必要があります AWS アカウント” • the section called “[APIGateway.8] API Gateway ルートには認可タイプを指定する必要があります” • the section called “[APIGateway.9] API Gateway V2 ステージにアクセスロギングを設定する必要があります” • the section called “[CodeBuild.3] CodeBuild S3 ログは暗号化する必要があります” • the section called “[EC2.25] Amazon EC2 起動テンプレートがパブリック IP をネットワークインターフェイスに割り当てないようにすることをお勧めします” • the section called “[ELB.1] Application Load Balancer は、すべての HTTP リクエストを HTTPS にリダイレクトするように設定する必要があります” • the section called “[Redshift.10] Redshift クラスターは	2023 年 6 月 12 日

保存時に暗号化する必要があります”

- the section called “[SageMaker.2] SageMaker ノートブックインスタンスはカスタム VPC で起動する必要があります”
- the section called “[SageMaker.3] ユーザーは SageMaker ノートブックインスタンスのルートアクセス権を付与されてはなりません”
- the section called “[WAF.10] AWS WAF ウェブ ACLs には、少なくとも 1 つのルールまたはルールグループが必要です”

新しいセキュリティコントロール	次の新しい Security Hub CSPM コントロールが利用可能になりました。 • the section called “[ACM.2] ACM によって管理される RSA 証明書は、少なくとも 2,048 ビットのキーの長さを使用する必要があります” • the section called “[AppSync.2] AWS AppSync フィールドレベルのログ記録を有効にする必要があります” • the section called “[CloudFront.13] CloudFront ディストリビューションでは、オリジンアクセスコントロールを有効にする必要があります” • the section called “[Elastic Beanstalk.3] Elastic Beanstalk は CloudWatch にログをストリーミングする必要があります” • the section called “[S3.17] S3 汎用バケットは保管時にで暗号化する必要があります AWS KMS keys” • the section called “[StepFunctions.1] Step Functions ステートマシンではログ記録がオンになっている必要があります”	2023 年 6 月 6 日

アジアパシフィック (メルボルン) で Security Hub CSPM が利用可能に	Security Hub CSPM がアジアパシフィック (メルボルン) で利用可能になりました。特定のセキュリティコントロールを除き、すべての Security Hub CSPM 機能がこのリージョンで利用可能になりました。詳細については、「リージョン別のコントロールの可用性」を参照してください。	2023 年 5 月 25 日
検出結果の履歴	Security Hub CSPM は、過去 90 日間の検出結果の履歴を追跡できるようになりました。	2023 年 5 月 4 日

新しいセキュリティコントロール	次の新しい Security Hub CSPM コントロールが利用可能になりました。 • the section called “[EKS.1] EKS クラスターエンドポイントがパブリックにアクセスできないようにする必要があります” • the section called “[ELB.16] Application Load Balancer は AWS WAF ウェブ ACL に関連付ける必要があります” • the section called “[Redshift.10] Redshift クラスターは保存時に暗号化する必要があります” • the section called “[S3.15] S3 汎用バケットでは Object Lock が有効になっている必要があります”	2023 年 3 月 29 日
統合されたコントロールの検出結果のサポートを拡大	v2.0.0 AWS の自動セキュリティレスポンスは、統合コントロールの検出結果をサポートするようになりました。	2023 年 3 月 24 日
Security Hub CSPM が新しいで利用可能に AWS リージョン	Security Hub CSPM が、アジアパシフィック (ハイデラバード) 、欧州 (スペイン) 、欧州 (チューリッヒ) で利用可能になりました。これらのリージョンでは、利用できるコントロールに制限があります。	2023 年 3 月 21 日

マネージドポリシーの更新	Security Hub CSPM は、`AWSSecurityHubServiceRolePolicy` マネージドポリシーの既存のアクセス許可を更新しました。	2023 年 3 月 17 日

NIST 800-53 標準の新しいセキュリティコントロール	Security Hub CSPM には、NIST 800-53 標準に適用される以下のセキュリティコントロールが追加されました。 • the section called “[Account.2] AWS アカウント は AWS Organizations 組織の一部である必要があります” • the section called “[CloudWatch.15] CloudWatch アラームには、指定されたアクションが設定されている必要があります” • the section called “[CloudWatch.16] CloudWatch ロググループは指定した期間保持する必要があります” • the section called “[CloudWatch.17] CloudWatch アラームアクションをアクティブにする必要があります” • the section called “[DynamoDB.4] DynamoDB テーブルはバックアッププランにある必要があります” • the section called “ [EC2.28] EBS ボリュームをバックアッププランの対象にすることをお勧めします” • EC2.29 — EC2 インスタンスは VPC で起動する必要があります (廃止)	2023 年 3 月 3 日

	• the section called “[RDS.26] RDS DB インスタンスはバックアッププランで保護する必要があります” • the section called “[S3.14] S3 汎用バケットではバージョニングが有効になっている必要があります” • the section called “[WAF.11] AWS WAF ウェブ ACL ログ記録を有効にする必要があります”	
米国国立標準技術研究所 (NIST) 800-53 リビジョン 5	Security Hub CSPM は、200 を超える適用可能なセキュリティコントロールを持つ NIST 800-53 Rev. 5 標準をサポートするようになりました。	2023 年 2 月 28 日
統合コントロールビューとコントロールの検出結果	統合コントロールビューのリリースでは、Security Hub CSPM コンソールのコントロールページに、標準全体のすべてのコントロールが表示されます。各コントロールは、標準全体で同じコントロール ID を持ちます。統合されたコントロールの検出結果を有効にすると、コントロールが複数の有効な標準に適用される場合でも、セキュリティチェックごとに 1 つの検出結果を受け取ります。	2023 年 2 月 23 日

新しいセキュリティコントロール	次の新しい Security Hub CSPM コントロールが利用可能になりました。一部、リージョン別の制限があるコントロールがあります。 • the section called “[ElastiCache.1] ElastiCache (Redis OSS) クラスターでは自動バックアップを有効にする必要があります” • the section called “[ElastiCache.2] ElastiCache クラスターでは、マイナーバージョンの自動アップグレードを有効にする必要があります” • the section called “[ElastiCache.3] ElastiCache (Redis OSS) レプリケーショングループでは、自動フェイルオーバーを有効にする必要があります” • the section called “[ElastiCache.4] ElastiCache レプリケーショングループは保管中に暗号化する必要があります” • the section called “[ElastiCache.5] ElastiCache レプリケーショングループは転送時に暗号化する必要があります” • the section called “[ElastiCache.6] 以前のバージョンの	2023 年 2 月 16 日

	ElastiCache (Redis OSS) レプリケーショングループでは Redis OSS AUTH を有効にする必要があります” • the section called “[ElastiCache.7] ElastiCache クラスターでは、デフォルトのサブネットグループを使用しないでください”	
新しい ASFF フィールド	Security Hub CSPM は ProductFields.ArchivalReasons:0/Description および ProductFields.ArchivalReasons:0/ReasonCode を AWS Security Finding Format (ASFF) に追加しました。	2023 年 2 月 8 日
新しい ASFF フィールド	Security Hub CSPM に Compliance.AssociatedStandards と Compliance.SecurityControlId が AWS Security Finding Format (ASFF) に追加されました。	2023 年 1 月 31 日
脆弱性の詳細が公開されました	Amazon Inspector が Security Hub CSPM に送信する検出結果について、Security Hub CSPM コンソールで脆弱性の詳細を表示できるようになりました。	2023 年 1 月 14 日
Security Hub CSPM が中東 (UAE) で利用可能に	Security Hub CSPM が中東 (UAE) で利用可能になりました。一部、リージョン別の制限があるコントロールがあります。	2023 年 1 月 12 日

MetricStream とのサードパーティ統合を追加	Security Hub CSPM は、中国と を除くすべてのリージョンMetricStreamで とのサードパーティー統合をサポートするようになりました AWS GovCloud (US)。	2023 年 1 月 11 日
組織アカウント上限の引き上げ	Security Hub CSPM は、リージョンごとに Security Hub CSPM 管理者アカウントごとに最大 11,000 のメンバーアカウントをサポートするようになりました。	2022 年 12 月 27 日
ElasticBeanstalk.3 のロールバック	Security Hub CSPM は、コントロール [ElasticBeanstalk.3] をロールバックしました。Elastic Beanstalk は、すべてのリージョンで FSBP 標準から CloudWatch にログをストリーミングする必要があります。	2022 年 12 月 21 日
Security Hub CSPM が新しいセキュリティコントロールを追加	FSBP 標準を有効にしたお客様は、新しい Security Hub CSPM コントロールを利用できます。一部、リージョン別の制限があるコントロールがあります。	2022 年 12 月 15 日

今後予定されている機能についてのガイダンス	Security Hub CSPM は、統合コントロールビューと統合コントロール検出結果の 2 つの新機能をリリースする予定です。これらの今後予定されている機能は、統制結果フィールドや値に依存する既存のワークフローに影響を与える可能性があります。	2022 年 12 月 9 日
Amazon Security Lake の統合の提供を開始	Security Lake は、Security Hub CSPM の検出結果を受信することで、Security Hub CSPM と統合されるようになりました。	2022 年 11 月 29 日
サービスマネージドスタンダードのサポート： AWS Control Tower	Security Hub CSPM は、Service-Managed Standard: という新しいセキュリティ標準をサポートしています AWS Control Tower。AWS Control Tower はこの標準を管理します。	2022 年 11 月 28 日
CIS AWS Foundations Benchmark v1.4.0 が中国リージョンで利用可能に	Security Hub CSPM は、中国リージョンで CIS AWS Foundations Benchmark v1.4.0 をサポートするようになりました。	2022 年 11 月 18 日
Jira Service Management Cloud の統合の提供を開始	Jira Service Management Cloud は、中国リージョンを除くすべての利用可能なリージョンで Security Hub CSPM の検出結果を受け取るようになりました。	2022 年 11 月 17 日

AWS IoT Device Defender 統合が利用可能に	AWS IoT Device Defender は、使用可能なすべてのリージョンで Security Hub CSPM に検出結果を送信するようになりました。	2022 年 11 月 17 日
CIS AWS Foundations Benchmark v1.4.0 のサポート	Security Hub CSPM は、CIS AWS Foundations Benchmark v1.4.0 をサポートするセキュリティコントロールを提供するようになりました。この標準は、中国リージョンを除くすべての利用可能なリージョンで利用できます。	2022 年 11 月 9 日
での Security Hub CSPM の発表のサポート AWS GovCloud (US)	AWS GovCloud (米国東部) および GovCloud (米国西部) の Amazon Simple Notification Service (Amazon SNS) で Security Hub CSPM の発表をサブスクライブして、Security Hub CSPM に関する通知を受信できるようになりました。AWS GovCloud	2022 年 10 月 3 日
AWS Security Hub CSPM が新しいセキュリティコントロールを追加	新しい Security Hub CSPM コントロール AutoScaling.9 は、FSBP 標準を有効にしているお客様が利用できます。コントロールにはリージョン別の制限がある場合があります。	2022 年 9 月 1 日

Security Hub CSPM の発表をサブスクライブする	Amazon Simple Notification Service (Amazon SNS) で Security Hub CSPM の発表をサブスクライブして、Security Hub CSPM に関する通知を受信できるようになりました。	2022 年 8 月 29 日
クロスリージョン集約のためのリージョン拡張	クロスリージョン集約を AWS GovCloud (US)の結果、結果の更新、インサイトに使用できるようになりました。	2022 年 8 月 2 日
新しいサードパーティー製品の統合	Fortinet - FortiCNP は Security Hub CSPM の検出結果を受け取るサードパーティー統合であり、JFrog は Security Hub CSPM に検出結果を送信するサードパーティー統合です。	2022 年 7 月 26 日
EC2.27 は廃止されました	Security Hub CSPM は EC2.27 を廃止しました。EC2 インスタンスの実行には、Foundational Security Best Practices (FSBP) 標準の以前のコントロールであるキーペアを使用しないでください。AWS	2022 年 7 月 20 日
Lambda.2 は python3.6 をサポートしなくなりました	Security Hub CSPM は、Lambda.2 のパラメータとして python3.6 をサポートしなくなりました。- Lambda 関数は、 Foundational Security Best Practices (FSBP) 標準のコントロールであるサポートされているランタイムを使用する必要があります。 AWS	2022 年 7 月 19 日

AWS Security Hub CSPM が新しいセキュリティコントロールを追加	FSBP 標準を有効にしたお客様は、新しい Security Hub CSPM コントロールを利用できます。一部、リージョン別の制限があるコントロールがあります。	2022 年 6 月 22 日
AWS Security Hub CSPM が新しいリージョンをサポート	Security Hub CSPM がアジアパシフィック (ジャカルタ) で利用可能になりました。このリージョンでは、一部のコントロールが使用できません。	2022 年 6 月 7 日
AWS Security Hub CSPM との統合を改善 AWS Config	Security Hub CSPM ユーザーは、 AWS Config ルール評価の結果を Security Hub CSPM の結果として表示できます。	2022 年 6 月 6 日
自動で有効化された標準をオプトアウトする機能が追加されました	と統合したユーザーの場合 AWS Organizations、この機能を使用すると、Security Hub CSPM 管理者アカウントにログインし、新しいメンバーアカウントを自動有効化標準からオプトアウトできます。	2022 年 4 月 25 日
クロスリージョン集約が拡張されました	コントロールステータスとセキュリティスコアにクロスリージョン集約が追加されました。	2022 年 4 月 20 日
CompanyName と ProductName がトップレベルの属性になりました	カスタムインテグレーションに関連付けられた会社名および製品名を設定するための、新しいトップレベル属性が追加されました	2022 年 4 月 1 日

AWS Foundational Security Best Practices 標準に新しいコントロールを追加	AWS Foundational Security Best Practices 標準に 5 つの新しいコントロールを追加しました。	2022 年 3 月 31 日
新しいリソースの詳細オブジェクトが ASFF に追加されました	`AwsRdsDbSecurityGroup` リソースタイプが ASFF に追加されました。	2022 年 3 月 25 日
ASFF に新しいリソースの詳細が追加されました	その他の詳細が `AwsAutoScalingScalingGroup` 、`AwsElbLoadBalancer` 、`AwsRedshiftCluster` 、`AwsCodeBuildProject` に追加されました。	2022 年 3 月 25 日
AWS Foundational Security Best Practices 標準に新しいコントロールを追加	AWS Foundational Security Best Practices 標準に 15 の新しいコントロールを追加しました。	2022 年 3 月 16 日
AWS Foundational Security Best Practices 標準と Payment Card Industry Data Security Standard (PCI DSS) に新しいコントロールを追加	Amazon OpenSearch Service、Amazon RDS、Amazon EC2、Elastic Load Balancing、CloudFront の新しいコントロールが AWS Foundational Security Best Practices 標準に追加されました。また、OpenSearch Service の 2 つの新しいコントロールが PCI DSS に追加されました。	2022 年 2 月 15 日
ASFF に新しいフィールドを追加	次の新しいフィールドが追加されました: Sample。	2022 年 1 月 26 日

との統合を追加 AWS Health	AWS Health はservice-to-serviceイベントメッセージングを使用して、結果を Security Hub CSPM に送信します。	2022 年 1 月 19 日
との統合を追加 AWS Trusted Advisor	Trusted Advisor は、チェックの結果を Security Hub CSPM の検出結果として Security Hub CSPM に送信します。Security Hub CSPM は、 AWS 基本的なセキュリティのベストプラクティスチェックの結果を に送信します Trusted Advisor。	2022 年 1 月 18 日
ASFF のリソースの詳細オブジェクトを更新	`MixedInstancesPolicy` および `AvailabilityZones` が `AwsAutoScalingAutoScalingGroup` に追加されました。`MetadataOptions` が `AwsAutoScalingLaunchConfiguration` に追加されました。`BucketVersioningConfiguration` が `AwsS3Bucket` に追加されました。	2021 年 12 月 20 日

ASFF ドキュメントの出力を更新	ASFF 属性の説明は、以前は 1 つのトピックにまとめられていました。各最上位レベルのオブジェクトと各リソースの詳細オブジェクトが、独自のトピックに移動されました。ASFF 構文のトピックには、これらのトピックへのリンクが含まれています。	2021 年 12 月 20 日
の ASFF に新しいリソース詳細オブジェクトを追加 AWS Network Firewall	に AWS Network Firewall、、`AwsNetworkFirewallFirewall` 、`AwsNetworkFireFirewallPolicy` および のリソース詳細オブジェクトが追加されましたAwsNetworkFirewall`RuleGroup` 。	2021 年 12 月 20 日
Amazon Inspector の新しいバージョンのサポートの追加	Security Hub CSPM は、新しいバージョンの Amazon Inspector および Amazon Inspector Classic と統合されています。Amazon Inspector は Security Hub CSPM に結果を送信します。	2021 年 11 月 29 日
EC2.19 の重要度を変更	EC2.19 (セキュリティグループが、リスクの高いポートへの無制限アクセスを許可しない) の重要度 が「高」から「重大」に変更されました。	2021 年 11 月 17 日

Sonrai Dig との新しい統合	Security Hub CSPM が との統合を提供するようになりましたSonrai Dig。 はクラウド環境をSonrai Digモニタリングしてセキュリティリスクを特定します。 は Security Hub CSPM に結果Sonrai Digを送信します。	2021 年 11 月 12 日
CIS 2.1 および CloudTrail.1 コントロールのチェックを更新	CIS 2.1 と CloudTrail.1 では、少なくとも 1 つのマルチリージョン CloudTrail 追跡が設定されていることを確認する以外に、少なくとも 1 つのマルチリージョン CloudTrail 追跡で `ExcludeManagementEventSources` パラメータが空であることもチェックします。	2021 年 11 月 9 日
VPC エンドポイントのサポートを追加	Security Hub CSPM が と統合 AWS PrivateLink され、VPC エンドポイントがサポートされるようになりました。	2021 年 11 月 3 日
AWS Foundational Security Best Practices 標準にコントロールを追加	Elastic Load Balancing (ELB.2 および ELB.8) と AWS Systems Manager (SSM.4) の新しいコントロールを追加しました。	2021 年 11 月 2 日

EC2.19 コントロールのチェックにポートを追加	EC2.19 では、セキュリティグループが次のポートへの無制限の入力アクセスを許可しないこともチェックするようになりました: 3000 (Go、Node.js、および Ruby の ウェブ開発フレームワーク)、5000 (Python ウェブ開発フレームワーク)、8088 (レガシー HTTP ポート)、8888 (代替 HTTP ポート)	2021 年 10 月 27 日
Logz.io クラウド SIEM との統合を追加	Logz.io は、セキュリティチームがリアルタイムでセキュリティの脅威を検出、分析、対応できるように、ログとイベントデータの高度な相関を提供する Cloud SIEM のプロバイダです。Logz.io は Security Hub CSPM から検出結果を受け取ります。	2021 年 10 月 25 日
リージョン間の結果集約のサポートを追加	クロスリージョン集約では、リージョンを変更しなくても、すべての結果を確認できます。管理者アカウントによって、集約リージョンとリンクされたリージョンが選択されます。管理者アカウントとそのメンバーアカウントの結果が、リンクされたリージョンから集約リージョンに集約されます。	2021 年 10 月 20 日

ASFF のリソースの詳細オブジェクトを更新	ビューワーの証明書の詳細が AwsCloudFrontDistribution に追加されました。その他の詳細が AwsCodeBuildProject に追加されました。ロードバランサーの属性が AwsElbV2LoadBalancer に追加されました。S3 バケット所有者のアカウント識別子が AwsS3Bucket に追加されました。	2021 年 10 月 8 日
新しいリソースの詳細オブジェクトを ASFF に追加	次の新しいリソースの詳細オブジェクトが ASFF に追加されました: AwsEc2VpcEndpointService 、AwsEcrRepository 、AwsEksCluster 、AwsOpenSearchServiceDomain 、AwsWafRateBasedRule 、AwsWafRegionalRateBasedRule 、AwsXrayEncryptionConfig	2021 年 10 月 8 日
Lambda.2 コントロールから非推奨のランタイムを削除	AWS Foundational Security Best Practices 標準で、 は [Lambda.2] Lambda 関数からdotnetcore2.1 ランタイムを削除し、サポートされているランタイムを使用する必要があります。	2021 年 10 月 6 日

Check Point 統合の新しい名前	Check Point Dome9 アークとの統合が Check Point CloudGuard Posture Management になりました。統合 ARN は変更されませんでした。	2021 年 10 月 1 日
Alcide との統合を削除	Alcide kAudit との統合は中止されます。	2021 年 9 月 30 日
EC2.19 の重要度を変更	「[EC2.19] セキュリティグループが、リスクの高いポートへの無制限アクセスを許可しない」の重要度が「中」から「高」に変更されました。	2021 年 9 月 30 日
との統合 AWS Organizations が中国リージョンでサポートされるようになりました	Security Hub CSPM と Organizations の統合が、中国 (北京) と中国 (寧夏) でサポートされるようになりました。	2021 年 9 月 20 日
S3.1 および PCI.S3.6 コントロールの新しい AWS Config ルール	S3.1 と PCI.S3.6 の両方で、Amazon S3 ブロックパブリックアクセスの設定が有効になっていることが確認されます。これらのコントロールの AWS Config ルールが から `s3-account-level-public-access-blocks` に変更されました`s3-account-level-public-access-blocks-periodic` 。	2021 年 9 月 14 日

Lambda.2 コントロールから非推奨のランタイムを削除	AWS Foundational Security Best Practices 標準で、 は [Lambda.2] Lambda 関数から `nodejs10.x` および `ruby2.5`ランタイムを削除し、サポートされているランタイムを使用する必要があります。	2021 年 9 月 13 日
CIS 2.2 コントロールの重要度を変更	CIS AWS Foundations Benchmark 標準では、2.2 の重要度。-「CloudTrailのログファイル検証が有効であることを確認する」の重要度が「低」から「中」に変更されました。	2021 年 9 月 13 日
AWS Foundational Security Best Practices 標準の ECS.1、Lambda.2、SSM.1 を更新	AWS Foundational Security Best Practices 標準では、ECS.1 に に設定された`SkipInactiveTaskDefinitions` パラメータが追加されました`true`。これにより、コントロールはアクティブなタスク定義のみをチェックします。Lambda.2 では、Python 3.9 がランタイムのリストに追加されました。SSM.1 は、停止中および実行中の両方のインスタンスをチェックするようになりました。	2021 年 9 月 7 日

PCI.Lambda.2 コントロールによって Lambda @Edge リソースを除外	Payment Card Industry Data Security Standard (PCI DSS) では、PCI.Lambda.2 コントロールによって Lambda @Edge リソースが除外されるようになりました。	2021 年 9 月 7 日
HackerOne Vulnerability Intelligence との統合を追加	Security Hub CSPM が との統合を提供するようになりましたHackerOne Vulnerability Intelligence。統合は Security Hub CSPM に結果を送信します。	2021 年 9 月 7 日
ASFF のリソースの詳細オブジェクトを更新	`AwsKmsKey` には、`KeyRotationStatus` が追加されました。`AwsS3Bucket` には、`AccessControlList` 、`BucketLoggingConfiguration` 、`BucketNotificationConfiguration` 、および `BucketWebsiteConfiguration` が追加されました。	2021 年 9 月 2 日
新しいリソースの詳細オブジェクトを ASFF に追加	次の新しいリソースの詳細オブジェクトが ASFF に追加されました: `AwsAutoScalingLaunchConfiguration` 、`AwsEc2VpnConnection` 、および `AwsEcrContainerImage` 。	2021 年 9 月 2 日

ASFF で Vulnerabilities オブジェクトに詳細を追加	Cvss では、Adjustments と Source が追加されました。VulnerablePackages では、ファイルパスとパッケージマネージャーが追加されました。	2021 年 9 月 2 日
Systems Manager Explorer および OpsCenter の統合が中国リージョンでサポートされるようになります	Security Hub CSPM と SSM Explorer および OpsCenter の統合が、中国 (北京) および中国 (寧夏) でサポートされるようになりました。	2021 年 8 月 31 日
Lambda.4 コントロールの廃止	Security Hub CSPM はコントロール [Lambda.4] Lambda 関数のデッドレターキューを設定する必要があります。コントロールが廃止されると、コンソールに表示されなくなり、Security Hub CSPM はコントロールに対してチェックを実行しません。	2021 年 8 月 31 日
PCI.EC2.3 コントロールの廃止	Security Hub CSPM はコントロールを廃止しています [PCI.EC2.3] 未使用の EC2 セキュリティグループを削除する必要があります。コントロールが廃止されると、コンソールに表示されなくなり、Security Hub CSPM はコントロールに対してチェックを実行しません。	2021 年 8 月 27 日

Security Hub CSPM がカスタムアクションに結果を送信する方法への変更	カスタムアクションに結果を送信すると、Security Hub CSPM は個別のSecurity Hub Findings - Custom Actionイベントで各結果を送信するようになりました。	2021 年 8 月 20 日
カスタム Lambda ランタイムの新しいコンプライアン状況理由コードを追加	新しい `LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE` コンプライアンス状況理由コードが追加されました。この理由コードは、Security Hub CSPM がカスタム Lambda ランタイムに対してチェックを実行できなかったことを示します。	2021 年 8 月 20 日
AWS Firewall Manager 統合が中国リージョンでサポートされるようになりました	Security Hub CSPM と Firewall Manager の統合が、中国 (北京) および中国 (寧夏) でサポートされるようになりました。	2021 年 8 月 19 日
Caveonix Cloud および Forcepoint Cloud Security Gateway との新しい統合	Security Hub CSPM が Caveonix Cloudおよび との統合を提供するようになりましたForcepoint Cloud Security Gateway。どちらの統合も Security Hub CSPM に結果を送信します。	2021 年 8 月 10 日

ASFF に新しい CompanyName 、ProductName 、および Region 属性を追加	ASFF の最上位レベルに CompanyName 、ProductName 、および Region フィールドが追加されました。これらのフィールドは自動的に入力され、カスタム製品統合を除き、BatchImportFindings または BatchUpdateFindings を使用して更新することはできません。コンソールでは、検索フィルターによってこれらの新しいフィールドが使用されます。API では、CompanyName および ProductName フィルターによって ProductFields の属性が使用されます。	2021 年 7 月 23 日
ASFF のリソースの詳細オブジェクトを追加および更新	新しい AwsRdsEventSubscription リソースタイプと新しいリソースの詳細が追加されました。AwsEcsService リソースタイプのリソースの詳細が追加されました。AwsElasticsearchDomain リソースの詳細オブジェクトに属性が追加されました	2021 年 7 月 23 日

AWS Foundational Security Best Practices 標準にコントロールを追加	Amazon API Gateway (APIGateway.5)、Amazon EC2 (EC2.19)、Amazon ECS (ECS.2)、Elastic Load Balancing (ELB.7)、Amazon OpenSearch Service (ES.5 ~ ES.8)、Amazon RDS (RDS.16 ~ RDS.23)、Amazon Redshift (Redshift.4)、Amazon SQS (SQS.1) の新しいコントロールが追加されました。	2021 年 7 月 20 日
サービスにリンクされたロールマネージドポリシー内の許可を移動	マネージドポリシー `AWSSecurityHubServiceRolePolicy` 内の `config:PutEvaluations` 許可が移動され、すべてのリソースに適用されるようになりました。	2021 年 7 月 14 日
AWS Foundational Security Best Practices 標準にコントロールを追加	Amazon API Gateway (APIGateway.4)、Amazon CloudFront (CloudFront.5 および CloudFront.6)、Amazon EC2 (EC2.17 および EC2.18)、Amazon ECS (ECS.1)、Amazon OpenSearch Service (ES.4)、AWS Identity and Access Management (IAM.21)、Amazon RDS (RDS.15)、Amazon S3 (S3.8) の新しいコントロールが追加されました。	2021 年 7 月 8 日

統制結果の新しいコンプライアンス状況の理由コードを追加	`INTERNAL_SERVICE_ERROR` は、不明なエラーが発生したことを示します。`SNS_TOPIC_CROSS_ACCOUNT` は、SNS トピックが別のアカウントによって所有されていることを示します。`SNS_TOPIC_INVALID` は、関連付けられた SNS トピックが無効であることを示します。	2021 年 7 月 6 日
チャットアプリケーションで Amazon Q Developer との統合を追加	チャットアプリケーションで Amazon Q Developer との統合を追加しました。Security Hub CSPM は、チャットアプリケーションで Amazon Q Developer に検出結果を送信します。	2021 年 6 月 30 日
サービスにリンクされたロールマネージドポリシーに新しい許可を追加	マネージドポリシー `AWSSecurityHubServiceRolePolicy` に新しい許可が追加され、サービスにリンクされたロールで AWS Configに評価結果を提供できるようになりました。	2021 年 6 月 29 日

ASFF の新規および更新されたリソース詳細オブジェクト	ECS クラスタおよび ECS タスク定義の新しいリソースの詳細オブジェクトが追加されました。EC2 インスタンスオブジェクトが更新されて、関連付けられているネットワークインターフェイスが一覧表示されるようになりました。API Gateway V2 のステージのクライアント証明書 ID が追加されました。S3 バケットのライフサイクル設定が追加されました。	2021 年 6 月 24 日
集約されたコントロールステータスと標準のセキュリティスコアの計算を更新	Security Hub CSPM は、全体的なコントロールステータスと標準セキュリティスコアを 24 時間ごとに計算するようになりました。管理者アカウントの場合、アカウントごとに各コントロールが有効または無効かどうかがスコアに反映されるようになりました。	2021 年 6 月 23 日
停止されたアカウントの Security Hub CSPM 処理に関する情報を更新しました	Security Hub CSPM が で停止されているアカウントを処理する方法に関する情報を追加しました AWS。	2021 年 6 月 23 日

個々の管理者アカウントの有効化/無効化されたコントロールを表示するタブを追加	管理者アカウントの場合、標準の詳細ページのメインタブに、アカウント間で集約された情報が表示されます。新しい [Enabled for this account] (このアカウントでは有効) および [Disabled for this account] (このアカウントでは無効) タブには、個々の管理者アカウントに対して有効または無効になっているアカウントが一覧表示されます。	2021 年 6 月 23 日
`Lambda.2` のパラメータに `java8.al2` を追加	AWS Foundational Security Best Practices 標準で、`Lambda.2`コントロールでサポートされているランタイム`java8.al2` に が追加されました。	2021 年 6 月 8 日
MicroFocus ArcSight および NETSCOUT Cyber Investigator との新しい統合	MicroFocus ArcSight および NETSCOUT Cyber Investigator との統合が追加されました。MicroFocus ArcSight は Security Hub CSPM から検出結果を受け取ります。Netscout Cyber investigator は、結果を Security Hub CSPM に送信します。	2021 年 6 月 7 日
`AWSSecurityHubServiceRolePolicy` の詳細を追加	マネージドポリシーセクションを更新し`AWSSecurityHubServiceRolePolicy` 、Security Hub CSPM サービスリンクロールで使用される既存のマネージドポリシー の詳細を追加しました。	2021 年 6 月 4 日

Jira サービス管理との新しい統合	AWS Service Management Connector for Jira は検出結果を Jira に送信し、それを使用して Jira の問題を作成します。Jira の問題が更新されると、Security Hub CSPM の対応する検出結果も更新されます。	2021 年 5 月 26 日
アジアパシフィック (大阪) リージョンでサポートされているコントロールリストを更新	CIS AWS Foundations 標準と Payment Card Industry Data Security Standard (PCI DSS) を更新し、アジアパシフィック (大阪) でサポートされていないコントロールを示しました。	2021 年 5 月 21 日
Sysdig Secure for cloud との新しい統合	Sysdig Secure for cloud との統合が追加されました。統合は Security Hub CSPM に結果を送信します。	2021 年 5 月 14 日

AWS Foundational Security Best Practices 標準にコントロールを追加	Amazon API Gateway (APIGateway.2 および APIGateway.3), AWS CloudTrail 、 (CloudTrail.4 および CloudTrail.5),、Amazon EC2 (EC2.15 および EC2.16) AWS Elastic Beanstalk 、(ElasticBeanstalk.1 および ElasticBeanstalk.2), AWS Lambda 、(Lambda.4)、Amazon RDS (RDS.12 – RDS.14)、Amazon Redshift (Redshift.7) AWS Secrets Manager 、(SecretsManager.3 および SecretsManager.4),、および AWS WAF (WAF.1) の新しいコントロールを追加しました。	2021 年 5 月 10 日
GuardDuty および Amazon RDS コントロールの更新	`GuardDuty.1` および `PCI.GuardDuty.1` の重要度が「中」から「高」に変更されました。`databaseEngines` パラメータが `RDS.8` に追加されました。	2021 年 5 月 4 日
新しいリソースの詳細を ASFF に追加	に`Resources.Details` 、Amazon EC2 ネットワーク ACLs、Amazon EC2 サブネット、 AWS Elastic Beanstalk 環境の新しいリソース詳細オブジェクトが追加されました。	2021 年 5 月 3 日

Amazon EventBridge ルールのフィルター値を指定するコンソールフィールドを追加	Security Hub CSPM EventBridge ルールの新しい定義済みフィルターパターンには、フィルター値を指定するために使用できるコンソールフィールドが用意されています。	2021 年 4 月 30 日
AWS Systems Manager Explorer および OpsCenter との統合を追加	Security Hub CSPM が Systems Manager Explorer および OpsCenter との統合をサポートするようになりました。統合は、Security Hub CSPM から検出結果を受け取り、Security Hub CSPM でそれらの検出結果を更新します。	2021 年 4 月 26 日
製品統合の新しいタイプ	新しい統合タイプは`UPDATE_FINDINGS_IN_SECURITY_HUB`、製品統合が Security Hub CSPM から受け取った検出結果を更新することを示します。	2021 年 4 月 22 日
「マスターアカウント」という用語を「管理者アカウント」に変更	「マスターアカウント」という用語が「管理者アカウント」に変更されました。この用語は、Security Hub CSPM コンソールと API でも変更されています。	2021 年 4 月 22 日

HTTP を Websocket に置き換えるように APIGateway.1 を更新	APIGateway.1 のタイトル、説明、および修正が更新されました。コントロールは、HTTP API 実行ログではなく Websocket API 実行ログをチェックするようになりました。	2021 年 4 月 9 日
Amazon GuardDuty の統合が中国 (北京と寧夏) でサポートされるようになります	Security Hub CSPM と GuardDuty の統合が、中国 (北京) および中国 (寧夏) リージョンでサポートされるようになりました。	2021 年 4 月 5 日
Lambda.2 コントロールのサポートされているランタイムに `nodejs14.x` を追加	Foundational Security Best Practices 標準の Lambda.2 コントロールでは、`nodejs14.x` ランタイムがサポートされるようになりました。	2021 年 3 月 30 日
Security Hub CSPM がアジアパシフィック (大阪) で利用可能に	Security Hub CSPM がアジアパシフィック (大阪) リージョンで利用可能になりました。	2021 年 3 月 29 日
結果の詳細に結果プロバイダーフィールドを追加	結果の詳細パネルの新しい [Finding Provider Fields] (結果プロバイダフィールド) セクションには、信頼度、重大度、関連する結果、重要度、およびタイプの結果プロバイダー値が含まれています。	2021 年 3 月 24 日
Amazon Macie から機密性の高い結果を受け取るオプションを追加	Macie との統合で、機密の検出結果を Security Hub CSPM に送信するように設定できるようになりました。	2021 年 3 月 23 日

アカウント管理 AWS Organizations のための への移行	メンバーアカウントを持つ既存の管理アカウントのお客様について、招待によるアカウント管理から Organizations を使用したアカウント管理への変更方法に関する新しい情報が追加されました。	2021 年 3 月 22 日
Amazon S3 パブリックアクセスブロックの設定に関する情報の ASFF の新しいオブジェクト	`Resources` では、新しい `AwsS3AccountPublicAccessBlock` リソースタイプと詳細オブジェクトによって、アカウントの Amazon S3 パブリックアクセスブロック設定に関する情報が提供されます。`AwsS3Bucket` リソースの詳細オブジェクトでは、`PublicAccessBlockConfiguration` オブジェクトによって、S3 バケットのパブリックアクセスブロック設定が提供されます。	2021 年 3 月 18 日
ASFF の新しいオブジェクトを使用して、結果プロバイダーによる特定のフィールドの更新を許可	ASFF の新しい `FindingProviderFields` オブジェクトが `BatchImportFindings` で使用され、`Confidence` 、`Criticality` 、`RelatedFindings` 、`Severity`、`Types` の値が指定されます。元のフィールドは、`BatchUpdateFindings` を使用してのみ更新されます。	2021 年 3 月 18 日

ASFF のリソースの新規 DataClassification オブジェクト	ASFF の新規 Resources.DataClassification オブジェクトは、リソースで検出された機密データに関する情報を提供するために使用されます。	2021 年 3 月 18 日
使用可能なコンプライアンス状況コードに CONFIG_RETURNS_NOT_APPLICABLE 値を追加	NOT_AVAILABLE コンプライアンス状況について、理由コード RESOURCE_NO_LONGER_EXISTS が削除され、理由コード CONFIG_RETURNS_NOT_APPLICABLE が追加されました。	2021 年 3 月 16 日
と統合するための新しいマネージドポリシー AWS Organizations	新しい管理ポリシーはAWSSecurityHubOrganizationsAccess 、組織管理アカウントと委任 Security Hub CSPM 管理者アカウントに必要な Organizations アクセス許可を提供します。	2021 年 3 月 15 日
マネージドポリシーとサービスにリンクされたロール情報が「セキュリティ」の章に移動	マネージドポリシーに関する情報が改訂され、拡張されます。マネージドポリシー情報とサービスにリンクされたロールに関する情報は、「セキュリティ」の章に移動しました。	2021 年 3 月 15 日

SecureCloudDB との新しい統合	SecureCloudDB がサードパーティの統合のリストに追加されました。SecureCloudDB は、内部および外部のセキュリティ体制とアクティビティを包括的に可視化するクラウドネイティブデータベースセキュリティツールです。SecureCloudDB は Security Hub CSPM に結果を送信します。	2021 年 3 月 4 日
CIS 1.1 および CIS 3.1 ~ CIS 3.14 コントロールの重要度を改訂	CIS 1.1 および CIS 3.1 ~ CIS 3.14 コントロールの重要度が「低」に変更されます。	2021 年 3 月 3 日
RDS.11 コントロールを削除	Foundational Security Best Practices 標準から RDS.11 コントロールを削除	2021 年 3 月 3 日
Turbot の統合を更新	結果を送受信するように Turbot 統合が更新されます。	2021 年 2 月 26 日
Foundational Security Best Practices 標準にコントロールを追加	Amazon API Gateway (APIGateway.1)、Amazon EC2 (EC2.9 および EC2.10)、Amazon Elastic File System (EFS.2)、Amazon OpenSearch Service (ES2 および ES3)、Elastic Load Balancing (ELB.6)、 AWS Key Management Service (AWS KMS) (KMS.3) の新しいコントロールが追加されました。	2021 年 2 月 11 日

DescribeProducts API にオプションの ProductArn フィルターを追加	DescribeProducts API オペレーションにオプションの ProductArn パラメータが含まれるようになりました。ProductArn パラメータは、特定の製品の統合を識別して詳細を返すために使用されます。	2021 年 2 月 3 日
クラウドストレージセキュリティからの Amazon S3 用アンチウイルスとの新しい統合	Amazon S3 のウイルス対策との統合により、検出結果としてウイルススキャン結果が Security Hub CSPM に送信されます。	2021 年 1 月 27 日
管理アカウントのセキュリティスコア計算プロセスを更新	管理者アカウントの場合、Security Hub CSPM は別のプロセスを使用してセキュリティスコアを計算します。新しいプロセスでは、メンバーアカウントでは有効であるが、管理アカウントでは無効になっているコントロールがスコアに含まれます。	2021 年 1 月 21 日
ASFF の新しいフィールドとオブジェクト	新しい Action オブジェクトが追加され、リソースに対して発生したアクションを追跡します。フィールドが AwsEc2NetworkInterface オブジェクトに追加され、DNS 名と IP アドレスを追跡します。新しい AwsSsmPatchCompliance オブジェクトがリソースの詳細に追加されました。	2021 年 1 月 21 日

Foundational Security Best Practices 標準にコントロールを追加	Amazon CloudFront (CloudFront.1 ~ CloudFront.4)、Amazon DynamoDB (DynamoDB.1 ~ DynamoDB.3)、Elastic Load Balancing (ELB.3 ~ ELB.5)、Amazon RDS (RDS.9 ~ RDS.11)、Amazon Redshift (Redshift.1 ~ Redshift.6)、Amazon SNS (SNS.1) の新しいコントロールが追加されました。	2021 年 1 月 15 日
ワークフローステータスは、レコードの状態またはコンプライアン状況に基づいてリセットされます	Security Hub CSPM は、`RESOLVED``NEW`アーカイブされた検出結果がアクティブになった場合、`NOTIFIED`または検出結果のコンプライアンスステータスが から `FAILED`、、または `PASSED`のいずれかに変わった場合`WARNING`、ワークフローステータスを または に自動的にリセットします`NOT_AVAILABLE` 。このような変更は、追加の調査が必要であることを示しています。	2021 年 1 月 7 日
コントロールベースの結果の `ProductFields` の情報を追加	コントロールから生成された検出結果については、 オブジェクトのコンテンツに関する情報を `ProductFields` AWS Security Finding Format (ASFF) に追加しました。	2020 年 12 月 29 日

マネージド型インサイトの更新	インサイト 5 のタイトルが変更されました。疑わしいアクティビティにかかわっている IAM ユーザーをチェックする新しいインサイト 32 が追加されました。	2020 年 12 月 22 日
IAM.7 および Lambda.1 コントロールの更新	AWS Foundational Security Best Practices 標準で、IAM.7 のパラメータを更新しました。Lambda.1 のタイトルと説明が更新されました。	2020 年 12 月 22 日
ServiceNow ITSM との統合を拡張	ServiceNow ITSM 統合により、Security Hub CSPM の検出結果を受信すると、ユーザーはインシデントまたは問題を自動的に作成できます。これらのインシデントまたは問題を更新すると、Security Hub CSPM の結果が更新されます。	2020 年 12 月 11 日
AWS Audit Manager との新しい統合	Security Hub CSPM が AWS Audit Manager との統合を提供するようになりました。この統合により、Audit Manager は Security Hub CSPM からコントロールベースの検出結果を受け取ることができます。	2020 年 12 月 8 日
Aqua Security Kube-Bench との新しい統合	Security Hub CSPM に Aqua Security Kube-bench との統合が追加されました。統合は Security Hub CSPM に結果を送信します。	2020 年 11 月 24 日

Cloud Custodian が、中国リージョンで利用可能になります	Cloud Custodian との統合が中国 (北京) および中国 (寧夏) リージョンで利用可能になりました。	2020 年 11 月 24 日
追加フィールドを更新するために BatchImportFindings を使用できるようになります	これまでは、BatchImportFindings を使用して Confidence 、Criticality 、RelatedFindings 、Severity、および Types フィールドを更新できませんでした。今後は、これらのフィールドが BatchUpdateFindings によって更新されていない場合は、BatchImportFindings によって更新できます。フィールドが BatchUpdateFindings によって更新された場合、BatchImportFindings では更新できません。	2020 年 11 月 24 日
Security Hub CSPM が と統合されました AWS Organizations	お客様が Organizations アカウント設定を使用して、メンバーアカウントを管理できるようになりました。組織管理アカウントは、Security Hub CSPM で有効にする組織アカウントを決定する Security Hub CSPM 管理者アカウントを指定します。手動招待プロセスは、組織に含まれていないアカウントでも使用できます。	2020 年 11 月 23 日

大量のコントロールの個々の結果リストを削除	コントロールの結果リストでは、結果が非常に多い場合、[Findings] (結果) のページ形式が使用されなくなりました。	2020 年 11 月 19 日
新しいサードパーティの統合と更新されたサードパーティの統合	Security Hub CSPM は、cloudtamer.io、3C ORESec、Prowler、および StackRox Kubernetes Security との統合をサポートするようになりました。IBM QRadar は結果を送信しなくなりました。結果を受け取ることはできます。	2020 年 10 月 30 日
コントロールの詳細ページから結果のリストをダウンロードするオプションが追加されました。	コントロールの詳細ページで、新しい [Download] (ダウンロード) オプションを使用すると、検索リストを .csv ファイル形式でダウンロードできます。ダウンロードされたリストは、リストに含まれるすべてのフィルターを優先します。特定の結果を選択した場合、ダウンロードされたリストにはそれらの結果のみが含まれます。	2020 年 10 月 26 日

標準の詳細ページからコントロールのリストをダウンロードするオプションが追加されました。	標準の詳細ページで、新しいオプションの [Download] (ダウンロード) オプションを使用すると、コントロールリストを .csv ファイルにダウンロードできます。ダウンロードされたリストは、リストに含まれるすべてのフィルターを優先します。特定のコントロールを選択した場合、ダウンロードされたファイルにはそのコントロールのみが含まれます。	2020 年 10 月 26 日
新しいパートナーの統合と更新されたパートナーの統合	Security Hub CSPM が ThreatModeler と統合されました。新しい製品名を反映するように、次のパートナーの統合が更新されました。Twistlock Enterprise Edition は Palo Alto Networks - Prisma Cloud Compute になりました。Palo Alto Networks ではさらに、Demisto が Cortex XSOAR に名称変更されると共に、Redlock が Prisma Cloud Enterprise に名称変更され、機能強化されました。	2020 年 10 月 23 日
Security Hub CSPM が中国 (北京) と中国 (寧夏) で利用可能に	Security Hub CSPM が中国 (北京) および中国 (寧夏) リージョンで利用可能になりました。	2020 年 10 月 21 日

ASFF 属性およびサードパーティー統合のフォーマットを改訂	ASFF の属性およびパートナーの統合のリストでテーブルの代わりにリストベースの形式が使用されるようになりました。ASFF の構文、属性、およびタイプ分類が別々のトピックになりました。	2020 年 10 月 15 日
標準の詳細ページを再設計	有効な標準の標準の詳細ページに、コントロールのタブ付きリストが表示されるようになりました。タブは、コントロールステータスに基づいてコントロールリストをフィルタリングします。	2020 年 10 月 7 日
CloudWatch イベントを EventBridge に置き換える	Amazon CloudWatch Events への参照を Amazon EventBridge に置き換えました。	2020 年 10 月 1 日
Blue Hexagon for AWS、Alcide kAudit、Palo Alto Networks VM シリーズとの新しい統合。	Security Hub CSPM が Blue Hexagon for AWS、Alcide kAudit、Palo Alto Networks VM シリーズと統合されました。 AWS および kAudit 用の Blue Hexagon は、結果を Security Hub CSPM に送信します。VM-Series は Security Hub CSPM から検出結果を受け取ります。	2020 年 9 月 30 日

ASFF の新規および更新されたリソース詳細オブジェクト	AwsApiGatewayRestApi 、AwsApiGatewayStage 、AwsApiGatewayV2Api 、AwsApiGatewayV2Stage 、AwsCertificateManagerCertificate 、AwsElbLoadBalancer 、AwsIamGroup 、AwsRedshiftCluster の新しい Resources.Details オブジェクトが追加されました。AwsCloudFrontDistribution 、AwsIamRole 、AwsIamAccessKey オブジェクトに詳細が追加されました。	2020 年 9 月 30 日
ASFF のリソースの新しい ResourceRole 属性で、リソースがアクターであるか、ターゲットであるかを追跡します。	リソースの ResourceRole 属性は、リソースが結果アクティビティの対象であるか、検索アクティビティの被対象であるかを示します。有効な値は ACTOR および TARGET です。	2020 年 9 月 30 日
利用可能な AWS サービス統合に AWS Systems Manager Patch Manager を追加	AWS Systems Manager Patch Manager が Security Hub CSPM と統合されました。Patch Manager は、お客様のフリート内のインスタンスがパッチコンプライアンス標準に準拠していない場合、結果を Security Hub CSPM に送信します。	2020 年 9 月 22 日

AWS Foundational Security Best Practices 標準に新しいコントロールを追加	次のサービスの新しいコントロールが追加されました: Amazon EC2 (EC2.7 および EC2.8)、Amazon EMR (EMR.1)、IAM (IAM.8)、Amazon RDS (RDS.4 ~ RDS.8)、Amazon S3 (S3.6)、AWS Secrets Manager (SecretsManager.1 および SecretsManager.2)	2020 年 9 月 15 日
IAM ポリシーの新しいコンテキストキーによって `BatchUpdateFindings` フィールドへのアクセスを制御	IAM ポリシーを設定して、`BatchUpdateFindings` の使用時に、フィールドとフィールド値へのアクセスを制限できるようになりました。	2020 年 9 月 10 日
メンバーアカウントの `BatchUpdateFindings` へのアクセスを拡張	デフォルトで、メンバーアカウントが、`BatchUpdateFindings` に対して管理アカウントと同じアクセス権を持つようになりました。	2020 年 9 月 10 日
Foundational Security Best Practices Standard AWS KMS の の新しいコントロール	Foundational Security Best Practices 標準に 2 つの新しいコントロール (KMS.1 と KMS.2) が追加されました。新しいコントロールは、IAM ポリシーが復 AWS KMS 号アクションへのアクセスを制限するかどうかをチェックします。	2020 年 9 月 9 日

コントロールのアカウントレベルの結果を削除	Security Hub CSPM は、コントロールのアカウントレベルの検出結果を生成しなくなりました。生成されるのはリソースレベルの結果のみです。	2020 年 9 月 1 日
ASFF の新しい PatchSummary オブジェクト	ASFF に `PatchSummary` オブジェクトが追加されました。`PatchSummary` オブジェクトは、選択したコンプライアンス標準に関連するリソースのパッチコンプライアンスに関する情報を提供します。	2020 年 9 月 1 日
コントロールの詳細ページを再設計	コントロールの詳細ページが再設計されました。統制結果リストには、コンプライアンスステータスに基づいてリストをすばやくフィルタリングできるタブがあります。また、非表示の結果をすばやく確認することもできます。各エントリは、検出結果リソース、 AWS Config ルール、および検出結果ノートに関する追加の詳細へのアクセスを提供します。	2020 年 8 月 28 日

結果の新しいフィルターオプション	結果フィルターでは、is not フィルターを使用すると、フィールド値がフィルター値と等しくない結果を検索できます。does not start with を使用すると、指定したフィルター値でフィールド値が開始しない結果を検索できます。	2020 年 8 月 28 日
ASFF の新規リソース詳細オブジェクト	次のリソースタイプの新しい `Resources.Details` オブジェクトが追加されました: `AwsDynamoDbTable` 、`AwsEc2Eip` 、`AwsIamPolicy` 、`AwsIamUser` 、`AwsRdsDbCluster` 、`AwsRdsDbClusterSnapshot` 、`AwsRdsDbSnapshot` 、`AwsSecretsManagerSecret`	2020 年 8 月 18 日
RSA Archer との新しい統合	Security Hub CSPM が RSA Archer と統合されました。RSA Archer は Security Hub CSPM から検出結果を受け取ります。	2020 年 8 月 18 日
AwsKmsKey の新しい説明フィールド	`Resources.Details` の `AwsKmsKey` オブジェクトに `Description` フィールドが追加されました。	2020 年 8 月 18 日

AwsRdsDbInstance にフィールドを追加	`Resources.Details` の `AwsRdsDbInstance` オブジェクトに複数の属性が追加されました。	2020 年 8 月 18 日
Security Hub CSPM がコントロールの全体的なステータスを決定する方法を更新	結果がないコントロールの場合、ステータスは [Unknown] (不明) の代わりに [No data] (データなし) となります。コントロールステータスには、アカウントレベルの結果とリソースレベルの結果の両方が含まれます。コントロールステータスでは、非表示の結果を無視することを除き、結果のワークフローステータスが使用されません。	2020 年 8 月 13 日
Security Hub CSPM が標準のセキュリティスコアを計算する方法を更新	標準のセキュリティスコアを計算するときに、Security Hub CSPM は、ステータスがデータなしのコントロールを無視するようになりました。セキュリティスコアは、データがないコントロールを除いた、有効なコントロールに対する合格コントロールの割合です。	2020 年 8 月 13 日
有効な標準で新しいコントロールを自動的に有効にする新しいオプション	有効な標準の新しいコントロールを自動的に有効にする [Settings] (設定) オプションが追加されました。`UpdateSecurityHubConfiguration` API オペレーションを使用しても、このオプションを設定できます。	2020 年 7 月 31 日

Payment Card Industry Data Security Standard (PCI DSS) 標準の新しいコントロール	PCI DSS 標準に新しいコントロールが追加されました。新しいコントロールの識別子は、PCI.DMS.1、PCI.EC2.5、PCI.EC2.6、PCI.ELBV2.1、PCI.GuardDuty.1、PCI.IAM.7、PCI.IAM.8、PCI.S3.5、PCI.S3.6、PCI.SageMaker.1、PCI.SSM.2 .SSM.3 です。	2020 年 7 月 29 日
Foundational Security Best Practices 標準の新しいコントロールと更新	Foundational Security Best Practices 標準に新しいコントロールが追加されました。新しいコントロールの識別子は、AutoScaling.1、DMS.1、EC2.4、EC2.6、S3.5、SSM.3 です。ACM.1 のタイトルが更新され、`daysToExpiration` パラメータの値が 30 に変更されました。	2020 年 7 月 29 日
ASFF の新しい `Vulnerabilities` オブジェクト	`Vulnerabilities` オブジェクトが追加されました。このオブジェクトは、結果に関連付けられた脆弱性に関する情報を提供します。	2020 年 7 月 1 日
Auto Scaling グループ、EC2 ボリューム、および EC2 VPC の ASFF の新しい `Resource.Details` オブジェクト	`AwsAutoScalingAutoScalingGroup` 、`AWSEc2Volume` 、および `AwsEc2Vpc` オブジェクトが `Resource.Details` に追加されました。	2020 年 7 月 1 日

ASFF の新しい NetworkPath オブジェクト	NetworkPath オブジェクトが追加されました。このオブジェクトは、結果に関連するネットワークパスに関する情報を提供します。	2020 年 7 月 1 日
Compliance.Status が PASSED のときに結果を自動的に解決	コントロールの検出結果の場合、 Compliance.Status が の場合PASSED、Security Hub CSPM は自動的に Workflow.Status を に設定しますRESOLVED。	2020 年 6 月 24 日
AWS Command Line Interface 例	いくつかの Security Hub CSPM タスクの AWS CLI 構文と例を追加しました。Security Hub CSPM の有効化、インサイトの管理、標準とコントロールの管理、製品統合の管理、Security Hub CSPM の無効化が含まれます。	2020 年 6 月 24 日
ASFF の新しい Severity.Original 属性	Severity.Original 属性が追加されました。これの属性は、結果プロバイダーからの元の重要度です。これにより、廃止された Severity.Product 属性が置き換えられます。	2020 年 5 月 20 日
コントロールのステータスの詳細に関する ASFF の新しい Compliance.StatusReasons オブジェクト	Compliance.StatusReasons オブジェクトが追加されました。これのオブジェクトは、コントロールの現在のステータスに関する追加のコンテキストを提供します。	2020 年 5 月 20 日

AWS 新しい基本的なセキュリティのベストプラクティス標準	新しい AWS Foundational Security Best Practices 標準を追加しました。これは、デプロイされたアカウントとリソースがセキュリティのベストプラクティスから逸脱したときを検出する一連のコントロールです。	2020 年 4 月 22 日
結果のワークフローステータスを更新する新しいコンソールオプション	Security Hub のコンソールまたは API を使用して結果のワークフローステータスを設定する方法の情報が追加されました。	2020 年 4 月 16 日
結果のお客様による更新の新しい `BatchUpdateFindings` API	`BatchUpdateFindings` を使用して結果の調査プロセスに関連する情報を更新する方法の情報が追加されました。`BatchUpdateFindings` は `UpdateFindings` に置き換えられますが、これは非推奨です。	2020 年 4 月 16 日

AWS Security Finding 形式 (ASFF) の更新	複数の新しいリソースタイプが追加されました。Label オブジェクトに新しい Severity 属性が追加されました。Label は Normalized フィールドを置き換えることを目的としています。結果の調査プロセスを追跡する新しい Workflow オブジェクトが追加されました。Workflow には、既存の Status 属性を置き換える Workflowstate 属性が含まれています。	2020 年 3 月 12 日
[Integrations] (統合) ページを更新	[Integrations] (統合) ページの変更を反映するように更新されました。各統合について、このページには統合カテゴリと、各統合が Security Hub CSPM に検出結果を送受信するかどうかが表示されるようになりました。また、各統合を有効にするために必要な特定の手順も示されています。	2020 年 2 月 26 日
新しいサードパーティー製品の統合	次の新しい製品の統合が追加されました: Cloud Custodian、FireEye Helix、Forcepoint CASB、Forcepoint DLP、Forcepoint NGFW、Rackspace Cloud Native Security、Vectra.ai Cognito Detect。	2020 年 2 月 21 日

Payment Card Industry Data Security Standard (PCI DSS) の新しいセキュリティ標準	Payment Card Industry Data Security Standard (PCI DSS) の Security Hub CSPM セキュリティ標準を追加しました。この標準を有効にすると、Security Hub CSPM は PCI DSS 要件に関連するコントロールに対して自動チェックを実行します。	2020 年 2 月 13 日
AWS Security Finding 形式 (ASFF) の更新	標準コントロールの関連要件のフィールドが追加されました。新しいリソースタイプと新しいリソースの詳細が追加されました。ASFF で、最大 32 のリソースを指定できるようになりました。	2020 年 2 月 5 日
個々のセキュリティ標準コントロールを無効にする新しいオプション	個々のセキュリティ標準コントロールを有効にするかどうかを制御する方法に関する情報が追加されました。	2020 年 1 月 15 日
Security Hub CSPM の概念の更新	一部の説明を更新し、Security Hub CSPM の概念に新しい用語を追加しました。	2019 年 9 月 21 日
AWS Security Hub CSPM の一般提供リリース	ベータ期間中に Security Hub CSPM に加えられた改善を反映するコンテンツの更新。	2019 年 6 月 25 日
CIS AWS Foundations チェックの修正手順を追加	AWS Security Hub CSPM でサポートされているセキュリティ標準に修復手順を追加しました。	2019 年 4 月 15 日

AWS Security Hub CSPM のベータリリース	AWS Security Hub CSPM ユーザーガイドのベータリリースバージョンを公開しました。	2018 年 11 月 18 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。