実装ガイド

AWS での自動化されたセキュリティ対応

AWS での自動化されたセキュリティ対応: 実装ガイド

Table of Contents

AWS Security Hub で事前定義された対応と修復アクションを使用して、セキュリティの脅威に自動的に対処する

公開日: 2020 年 8 月 (最終更新日: 2024 年 12 月)

この実装ガイドでは、AWS での自動化されたセキュリティ対応ソリューションの概要、そのリファレンスアーキテクチャとコンポーネント、デプロイを計画する際の考慮事項、AWS での自動化されたセキュリティ対応ソリューションを Amazon Web Services (AWS) クラウドにデプロイするための設定手順について説明します。

このナビゲーションテーブルを使用すると、以下の質問に対する回答をすばやく見つけることができます。

目的	参照先
このソリューションを実行するのに必要なコストを確認する。	コスト
このソリューションのセキュリティ上の考慮事項を理解する	セキュリティ
このソリューションのクォータを計画する方法を確認する	クォータ
このソリューションでサポートされている AWS リージョンを知る	サポートされている AWS リージョン
このソリューションに含まれている AWS CloudFormation テンプレートを表示またはダウンロードして、このソリューションのインフラストラクチャリソース (スタック) を自動的にデプロイする。	AWS CloudFormation テンプレート
ソースコードにアクセスし、オプションで AWS Cloud Development Kit (AWS CDK) を使用してソリューションをデプロイする	GitHub リポジトリ

セキュリティの継続的な進化には、データを保護するための予防的な手順が必要です。これにより、セキュリティチームが対応するのが困難になり、コストがかかり、時間もかかる可能性があります。AWS ソリューションでの自動化されたセキュリティ対応は、業界のコンプライアンス標準とベストプラクティスに基づいて事前定義された対応と修復アクションを提供することで、セキュリティ問題に迅速に対応するのに役立ちます。

AWS での自動化されたセキュリティ対応は、AWS Security Hub と連携してセキュリティを強化し、ワークロードを Well-Architected セキュリティの柱のベストプラクティス (SEC10) に合わせるのに役立つ AWS ソリューションです。このソリューションにより、AWS Security Hub のお客様は一般的なセキュリティ上の検出結果を簡単に解決し、AWS のセキュリティ体制を改善できます。

Security Hub のプライマリアカウントにデプロイする特定のプレイブックを選択できます。各プレイブックには、1 つの AWS アカウント内または複数のアカウント間で修復ワークフローを開始するために必要なカスタムアクション、Identity and Access Management (IAM) ロール、Amazon EventBridge ルール、AWS Systems Manager オートメーションドキュメント、AWS Lambda 関数、および AWS Step Functions が含まれています。修復は AWS Security Hub のアクションメニューから機能し、承認されたユーザーは 1 回のアクションで AWS Security Hub が管理するすべてのアカウントで検出結果を修復できます。例えば、AWS リソースを保護するためのコンプライアンス標準である Center for Internet Security (CIS) AWS Foundations Benchmark からのレコメンデーションを適用して、パスワードが 90 日以内に期限切れになるようにし、AWS に保存されているイベントログの暗号化を強制できます。

> **Note**
>
> 修復は、即時アクションを必要とする緊急事態を対象としています。このソリューションでは、AWS Security Hub マネジメントコンソールを介してユーザーが開始した場合、または特定のコントロールの Amazon EventBridge ルールを使用して自動修復が有効になっている場合にのみ、検出結果を修正するための変更を行います。これらの変更を元に戻すには、リソースを手動で元の状態に戻す必要があります。
>
> CloudFormation スタックの一部としてデプロイされた AWS リソースを修正する場合は、ドリフトが発生する可能性があることに注意してください。可能な場合は、スタックリソースを定義するコードを変更し、スタックを更新することで、スタックリソースを修正します。詳細については、「AWS CloudFormation ユーザーガイド」の「ドリフトとは」を参照してください。

AWS での自動化されたセキュリティ対応には、以下の一部として定義されたセキュリティ標準のプレイブック修正が含まれています。

- Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0
- CIS AWS Foundations Benchmark v1.4.0
- CIS AWS Foundations Benchmark v3.0.0
- AWS Foundational Security Best Practices (FSBP) v.1.0.0

- Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1
- 米国国立標準技術研究所 (NIST) SP 800-53 Rev. 5

このソリューションには、AWS Security Hub の統合コントロール検出結果機能用のセキュリティコントロール (SC) プレイブックも含まれています。詳細については、「Playbooks」を参照してください。

この実装ガイドでは、AWS クラウドに AWS での自動化されたセキュリティ対応ソリューションをデプロイするためのアーキテクチャ上の考慮事項と設定手順について説明します。セキュリティと可用性に関する AWS のベストプラクティスを使用して、このソリューションを AWS にデプロイするために必要な AWS のコンピューティング、ネットワーク、ストレージ、その他さまざまなサービスを起動、設定、実行する AWS CloudFormation テンプレートへのリンクが含まれています。

このガイドは、IT インフラストラクチャアーキテクト、管理者、および AWS クラウドでのアーキテクチャの設計の実務経験を持つ DevOps の専門家を対象としています。

特徴と利点

AWS での自動化されたセキュリティ対応には、次の機能があります。

特定のコントロールの検出結果を自動的に修正

コントロールの Amazon EventBridge ルールを有効にして、AWS Security Hub に表示された直後にそのコントロールの検出結果を自動的に修正します。

複数のアカウントとリージョンにわたる修復を 1 か所から管理

組織のアカウントとリージョンの集約先として設定された AWS Security Hub 管理者アカウントから、ソリューションがデプロイされているアカウントとリージョンで検出結果の修正を開始します。

修復アクションと結果の通知を受信

ソリューションによってデプロイされた Amazon SNS トピックをサブスクライブして、修復が開始されたときや修復が成功したかどうかの通知を受け取ります。

Jira や ServiceNow などのチケットシステムとの統合

組織が修復 (インフラストラクチャコードの更新など) に対応できるように、このソリューションはチケットを外部のチケットシステムにプッシュできます。

GovCloud および中国パーティションで AWSConfigRemediations を使用

ソリューションに含まれる修復は、商用パーティションで利用できるが GovCloud や中国では利用できない AWS が所有する AWSConfigRemediation ドキュメントの再パッケージです。これらのパーティションでこれらのドキュメントを利用するには、このソリューションをデプロイします。

カスタム修復とプレイブック実装でソリューションを拡張

このソリューションは、拡張可能でカスタマイズ可能なように設計されています。代替修復実装を指定するには、カスタマイズされた AWS Systems Manager Automation ドキュメントと AWS IAM ロールをデプロイします。ソリューションによって実装されていない新しい一連のコントロール全体をサポートするには、カスタムプレイブックをデプロイします。

ユースケース

組織のアカウントとリージョン全体で標準へのコンプライアンスを強制

標準 (AWS Foundational Security Best Practices など) のプレイブックをデプロイして、提供された修復を使用できます。コンプライアンス違反のリソースを修正するためにソリューションがデプロイされているアカウントとリージョンのリソースの修正を自動または手動で開始します。

組織のコンプライアンスニーズに合わせてカスタム修復またはプレイブックをデプロイ

提供されたオーケストレーターコンポーネントをフレームワークとして使用します。組織の特定のニーズに応じて、コンプライアンス違反のリソースに対処するためのカスタム修復を構築します。

概念と定義

このセクションでは、重要な概念について説明し、このソリューションに固有の用語を定義します。

アプリケーション

ユニットとして操作する AWS リソースの論理グループです。

修復、修復ランブック

検出結果を解決する一連のステップの実装です。例えば、コントロール Security Control (SC) Lambda.1 の「Lambda 関数ポリシーではパブリックアクセスを禁止する必要があります」を修正すると、関連する AWS Lambda 関数のポリシーが変更され、パブリックアクセスを許可するステートメントが削除されます。

コントロールランブック

オーケストレーターが特定のコントロールに対して開始された修復を正しい修復ランブックにルーティングするために使用する一連の AWS Systems Manager (SSM) 自動化ドキュメントの 1 つです。例えば、SC Lambda.1 と AWS Foundational Security Best Practices (FSBP) Lambda.1 の修復は、同じ修復ランブックで実装されます。オーケストレーターは、各コントロールのコントロールランブックを呼び出します。このランブックの名前は、それぞれ ASR-AFSBP_Lambda.1 と ASR-SC_2.0.0_Lambda.1 です。各コントロールランブックは同じ修復ランブックを呼び出します。この場合、ASR-RemoveLambdaPublicAccess になります。

オーケストレーター

AWS Security Hub から検出結果オブジェクトを入力として受け取り、ターゲットアカウントとリージョンで正しいコントロールランブックを呼び出すソリューションによってデプロイされた Step Functions です。また、オーケストレーターは、修復が開始されたとき、および修復が成功または失敗したときに、ソリューション SNS トピックに通知します。

標準

コンプライアンスフレームワークの一部として組織が定義するコントロールのグループです。例えば、AWS Security Hub とこのソリューションでサポートされている標準の 1 つは AWS FSBP です。

コントロール

準拠するためにリソースが持つべきプロパティ、または持つべきでないプロパティの説明です。例えば、コントロール AWS FSBP Lambda.1 では、AWS Lambda 関数はパブリックアクセスを禁止する必要があると規定されています。パブリックアクセスを許可する関数は、このコントロールに失敗します。

統合コントロールの検出結果、セキュリティコントロール、セキュリティコントロールビュー

AWS Security Hub の機能です。アクティブ化すると、特定の標準に対応する ID ではなく、統合されたコントロール ID とともに検出結果が表示されます。例えば、コントロール AWS FSBP S3.2、CIS v1.2.0 2.3、CIS v1.4.0 2.1.5.2、PCI-DSS v3.2.1 S3.1 はすべて、統合 (SC) コントロール S3.2 「S3 バケットはパブリック読み取りアクセスを禁止する必要があります」にマッピングします。この機能を有効にすると、SC ランブックが使用されます。

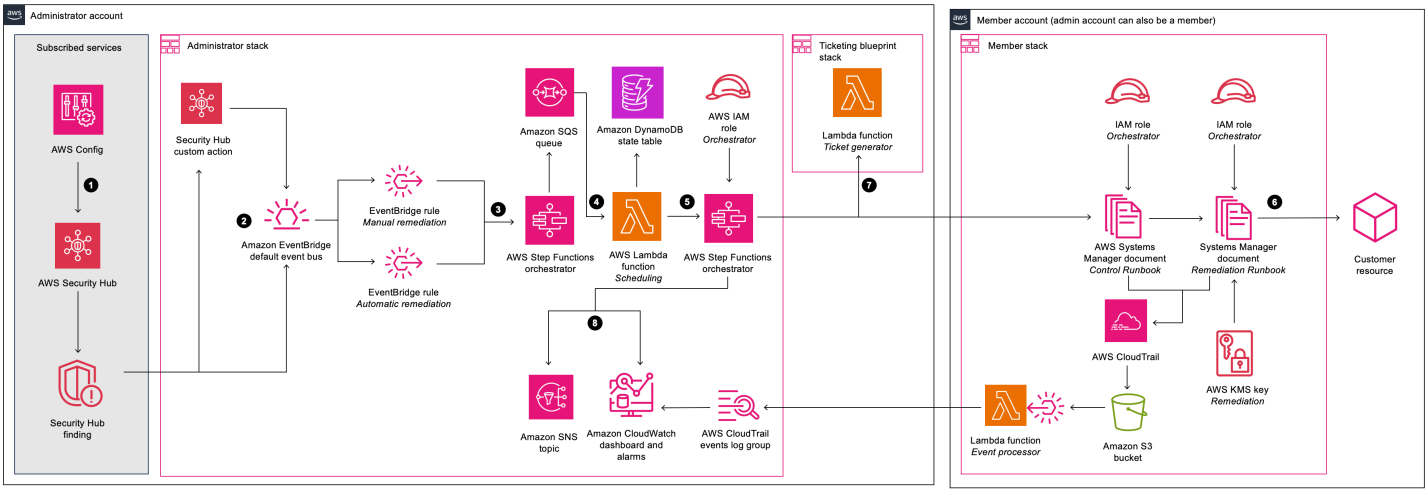
AWS の用語の一般的なリファレンスについては、「AWS 用語集」を参照してください。

アーキテクチャの概要

このセクションでは、このソリューションでデプロイされるコンポーネントのリファレンス実装のアーキテクチャ図を示します。

アーキテクチャ図

このソリューションをデフォルトのパラメータでデプロイすると、AWS クラウドに次の環境が構築されます。



AWS アーキテクチャでの自動セキュリティレスポンス

> **Note**
>
> AWS CloudFormation リソースは、AWS Cloud Development Kit (AWS CDK) コンストラクトから作成されます。

AWS CloudFormation テンプレートでデプロイされたソリューションコンポーネントの大まかなプロセスフローは次のとおりです。

1. 検出: AWS Security Hub は、AWS セキュリティの状態を包括的にお客様に提供します。これにより、セキュリティ業界の標準とベストプラクティスに照らして環境を測定できます。AWS Config、Amazon Guard Duty、AWS Firewall Manager などの他の AWS のサービスからイベントとデータを収集することで機能します。これらのイベントとデータは、CIS AWS Foundations Benchmark などのセキュリティ標準に照らして分析されます。例外は AWS Security Hub コン

ソールで検出結果としてアサートされます。新しい検出結果は Amazon EventBridge イベントとして送信されます。

2. 開始: カスタムアクションを使用して検出結果に対してイベントを開始できます。これにより、EventBridge イベントが発生します。AWS Security Hub カスタムアクションと EventBridge ルールは、検出結果に対応するために AWS プレイブックで自動セキュリティレスポンスを開始します。このソリューションは以下をデプロイします。

   a. カスタムアクションイベントに一致する 1 つの EventBridge ルール

   b. リアルタイム検出結果イベントに一致する、サポートされているコントロール (デフォルトでは無効) ごとに 1 つの EventBridge イベントルール

   Security Hub コンソールのカスタムアクションメニューを使用して、自動修復を開始できます。非本番環境で慎重にテストした後、自動修復をアクティブ化することもできます。個々の修復に対して自動化をアクティブ化できます。すべての修復で自動開始をアクティブ化する必要はありません。

3. 修復前: 管理者アカウントで、AWS Step Functions は修復イベントを処理し、スケジュールする準備をします。

4. スケジュール: このソリューションは、スケジューリング AWS Lambda 関数を呼び出して、修復イベントを Amazon DynamoDB 状態テーブルに配置します。

5. オーケストレーション: 管理者アカウントで、Step Functions はクロスアカウント AWS Identity and Access Management (IAM) ロールを使用します。Step Functions は、セキュリティ検出結果を生成したリソースを含むメンバーアカウントで修復を呼び出します。

6. 修復: メンバーアカウントのAWS Systems Manager 自動化ドキュメントは、Lambda パブリックアクセスの無効化など、ターゲットリソースの検出結果を修復するために必要なアクションを実行します。

   オプションで、EnableCloudTrailForASRActionLog パラメータを使用して、メンバースタックのアクションログ機能を有効にできます。この機能は、メンバーアカウントでソリューションによって実行されたアクションをキャプチャし、ソリューションの Amazon CloudWatch ダッシュボードに表示します。

7. (オプション) チケットの作成: TicketGenFunctionName パラメータを使用して管理者スタックでチケットを有効にすると、ソリューションは提供されたチケットジェネレーターの Lambda 関数を呼び出します。この Lambda 関数は、メンバーアカウントで修復が正常に実行された後に、チケット発行サービスにチケットを作成します。Jira および ServiceNow との統合用のスタックを提供しています。

8. 通知とログ: プレイブックは結果を CloudWatch ロググループにログ記録し、Amazon Simple Notification Service (Amazon SNS) トピックに通知を送信し、Security Hub の検出結果を更新します。このソリューションは、検出結果メモにアクションの監査証跡を保持します。

Well-Architected 設計上の考慮事項

このソリューションは、AWS Well-Architected フレームワークのベストプラクティスを使用して設計されています。これは、信頼性が高く、安全で、効率的で、コスト効率の高いワークロードをクラウドで設計および運用するのに役立ちます。このセクションでは、Well-Architected フレームワークの設計原則とベストプラクティスが、このソリューションの構築にどのように適用されているかについて説明します。

オペレーショナルエクセレンス

このセクションでは、運用上の優秀性の柱に関する原則とベストプラクティスを用いてこのソリューションをどのように設計したかを説明します。

- リソースは CloudFormation を使用して IaC として定義されます。
- 可能な場合は、次の特性を使用して修復を実装します。
  - 冪等性
  - エラー処理とレポート
  - ログ記録
  - 障害発生時のリソースの既知の状態への復元

セキュリティ

このセクションでは、セキュリティの柱に関する原則とベストプラクティスを用いてこのソリューションをどのように設計したかを説明します。

- 認証と認可に IAM を使用します。

- ロールのアクセス許可の範囲はできるだけ狭くしていますが、多くの場合、このソリューションではあらゆるリソースに対してアクションを実行するにはワイルドカードアクセス許可が必要です。

信頼性

このセクションでは、信頼性の柱に関する原則とベストプラクティスを用いてこのソリューションをどのように設計したかを説明します。

- Security Hub は、修復によって検出結果の根本的な原因が解決されない場合、検出結果の作成を継続します。
- サーバーレスサービスにより、必要に応じてソリューションをスケールできます。

パフォーマンス効率

このセクションでは、パフォーマンス効率の柱に関する原則とベストプラクティスを用いてこのソリューションをどのように設計したかを説明します。

- このソリューションは、オーケストレーションやアクセス許可を自分で実装しなくても拡張できるプラットフォームとして設計されています。

コスト最適化

このセクションでは、コスト最適化の柱に関する原則とベストプラクティスを用いてこのソリューションをどのように設計したかを説明します。

- サーバーレスサービスにより、使用した分だけ支払うことができます。
- すべてのアカウントで SSM オートメーションに無料利用枠を使用します。

持続可能性

このセクションでは、持続可能性の柱に関する原則とベストプラクティスを用いてこのソリューションをどのように設計したかを説明します。

- サーバーレスサービスにより、必要に応じてソリューションをスケールアップまたはスケールダウンできます。

アーキテクチャの詳細

このセクションでは、このソリューションを構成するコンポーネントと AWS のサービス、およびこれらのコンポーネントがどのように連携するかについてのアーキテクチャの詳細について説明します。

AWS Security Hub の統合

`aws-sharr-deploy` スタックをデプロイすると、AWS Security Hub のカスタムアクション機能との統合が作成されます。AWS Security Hub コンソールのユーザーが [修復のための検出結果] を選択すると、ソリューションは AWS Step Functions を使用して検出結果レコードを修復のためにルーティングします。

クロスアカウントのアクセス許可と AWS Systems Manager ランブックは、`aws-sharr-member.template` および `aws-sharr-member-roles.template` CloudFormation テンプレートを使用してすべての AWS Security Hub アカウント (管理者とメンバー) にデプロイする必要があります。詳細については、「プレイブック」を参照してください。このテンプレートを使用すると、ターゲットアカウントで自動修復が可能になります。

ユーザーは、Amazon CloudWatch Events のルールを使用して、修復ごとに自動修復を自動的に開始できます。このオプションにより、検出結果が AWS Security Hub に報告されるとすぐに、検出結果の完全自動修復がアクティブになります。デフォルトでは、自動開始はオフになっています。このオプションは、プレイブックのインストール中またはインストール後に、AWS Security Hub 管理者アカウントの CloudWatch Events ルールをオンにすることでいつでも変更できます。

クロスアカウント修復

AWS の自動セキュリティレスポンスは、クロスアカウントロールを使用して、プライマリアカウントとセカンダリアカウントをまたいで動作します。これらのロールは、ソリューションのインストール中にメンバーアカウントにデプロイされます。各修復には個別のロールが割り当てられます。プライマリアカウントの修復プロセスには、修復が必要なアカウントの修復ロールを引き受けるアクセス許可が付与されます。修復は、修復が必要なアカウントで実行されている AWS Systems Manager ランブックによって実行されます。

プレイブック

一連の修復は、プレイブックと呼ばれるパッケージにグループ化されます。プレイブックは、このソリューションのテンプレートを使用してインストール、更新、削除されます。各プレイブックでサポートされている修復の詳細については、「デベロッパーガイド -> プレイブック」を参照してください。このソリューションは現在、次のプレイブックをサポートしています。

- Security Control、2023 年 2 月 23 日に公開された AWS Security Hub の統合コントロール検出結果機能に沿ったプレイブック。

> **Important**
>
> Security Hub で統合コントロールの検出結果が有効になっている場合、ソリューションで有効にする必要があるプレイブックはこれだけです。

- Center for Internet Security (CIS) Amazon Web Services Foundations ベンチマーク、バージョン 1.2.0、2018 年 5 月 18 日公開。
- Center for Internet Security (CIS) Amazon Web Services Foundations ベンチマーク、バージョン 1.4.0、2022 年 11 月 9 日公開。
- Center for Internet Security (CIS) Amazon Web Services Foundations ベンチマーク、バージョン 3.0.0、2024 年 5 月 13 日公開。
- AWS Foundational Security Best Practices (FSBP) バージョン 1.0.0、2021 年 3 月発行。
- Payment Card Industry Data Security Standards (PCI-DSS) バージョン 3.2.1、2018 年 5 月発行。
- 米国国立標準技術研究所 (NIST) バージョン 5.0.0、2023 年 11 月発行。

集中ロギング

AWS の自動セキュリティレスポンスは、単一の CloudWatch Logs グループ SO0111-SHARR にログ記録されます。これらのログには、ソリューションのトラブルシューティングと管理のためのソリューションからの詳細なログ記録が含まれています。

通知

このソリューションは、Amazon Simple Notification Service (Amazon SNS) トピックを使用して修復結果を公開します。このトピックへのサブスクリプションを使用して、ソリューションの機能を拡張できます。例えば、E メール通知を送信したり、問題チケットを更新したりできます。

このソリューションの AWS のサービス

このソリューションでは、次のサービスを使用します。ソリューションを使用するにはコアサービスが必要であり、サポートサービスはコアサービスに接続します。

AWS のサービス	説明
Amazon EventBridge	コア。検出結果が修復されるときにオーケストレーターステップ関数を開始するイベントをデプロイします。
AWS IAM	コア。さまざまなリソースで修復できるように、多くのロールをデプロイします。
AWS Lambda	コア。ステップ関数オーケストレーターが問題を修復するために使用する複数の Lambda 関数をデプロイします。
AWS Security Hub	コア。AWS のセキュリティ状態を包括的に把握できます。
AWS Step Functions	コア。AWS Systems Manager API コールで修復ドキュメントを呼び出すオーケストレーターをデプロイします。
AWS Systems Manager	コア。実行される修復ロジックを含む System Manager ドキュメント (ドキュメントへのリンク) をデプロイします。
AWS CloudTrail	サポート。ソリューションが AWS リソースに加えた変更を記録し、CloudWatch ダッシュボードに表示します。
Amazon CloudWatch	サポート。さまざまなプレイブックが結果をログに記録するために使用するロググループをデプロイします。アラームを使用してカスタムダッシュボードに表示するメトリクスを収集します。

AWS のサービス	説明
AWS DynamoDB	サポート。修復のスケジュールを最適化するために、各アカウントとリージョンで最後に実行された修復を保存します。
Service Catalog AppRegistry	サポート。コストと使用状況を追跡するために、デプロイされたスタックにアプリケーションをデプロイします。
Amazon Simple Notification Service	サポート。修復が完了すると通知を受け取る SNS トピックをデプロイします。
AWS SQS	サポート。ソリューションが修復を並行して実行できるように、修復のスケジューリングを支援します。

デプロイを計画する

このセクションでは、ソリューションのデプロイ前に考慮すべきコスト、ネットワークセキュリティ、サポートされる AWS リージョン、およびクォータについて説明します。

コスト

このソリューションの実行中に使用した AWS サービスのコストは、お客様の負担となります。この改定時点で、米国東部 (バージニア北部) AWS リージョンのデフォルト設定でこのソリューションを実行する場合のコストは、1 か月あたり 300 回の修復で約 21.17 USD、1 か月あたり 3,000 回の修復で 134.86 USD、1 か月あたり 30,000 回の修復で 1,281.01 USD です。料金は変更されることがあります。詳細については、このソリューションで使用する各 AWS サービスの料金ページを参照してください。

> **Note**
>
> 多くの AWS サービスには無料利用枠が含まれています。これは、お客様が無料で使用できるサービスのベースライン量です。実際のコストは、提供されている料金例よりも多くなる場合も少なくなる場合もあります。

AWS Cost Explorer を使用して予算を作成することをお勧めします。これはコスト管理に役立ちます。料金は変更されることがあります。詳細については、このソリューションで使用する各 AWS サービスの料金ページを参照してください。

サンプルコスト表

このソリューションを実行するための総コストは、以下の要因によって異なります。

- AWS Security Hub メンバーアカウントの数
- 自動的に呼び出されるアクティブな修復の数
- 修復の頻度

このソリューションでは、以下の AWS コンポーネントを使用します。この設定に基づいてコストが発生します。料金の例は、小規模、中規模、大規模な組織を対象としています。

サービス	無料利用枠	料金 [USD]
AWS Systems Manager Automation - ステップ数	アカウントあたり 100,000 ステップ/月	無料利用枠を超えると、各基本ステップはステップあたり 0.002 USD が課金されます。マルチアカウントオートメーションの場合、子アカウントで実行されるステップを含むすべてのステップは、元のアカウントでのみカウントされます。
AWS Systems Manager Automation - ステップ期間	1 か月あたり 5,000 秒	無料利用枠を超えると、aws:executeScript の各アクションステップは、1 か月あたり 5,000 秒の無料利用枠の後に 1 秒あたり 0.00003 USD が課金されます。
AWS Systems Manager Automation - ストレージ	無料利用枠なし	1 か月あたり 0.046 USD/GB
AWS Systems Manager Automation - データ転送	無料利用枠なし	転送された GB あたり 0.900 USD (クロスアカウントまたはリージョン外の場合)
AWS Security Hub - セキュリティチェック	無料利用枠なし	最初の 100,000 件のチェックのアカウント/リージョン/月あたりのコストは、チェックあたり 0.0010 USD 次の 400,000 件のチェックのアカウント/リージョン/月あたりのコストは、チェックあたり 0.0008 USD 500,000 を超えるチェックのアカウント/リージョン/月あた

サービス	無料利用枠	料金 [USD]
		りのコストは、チェックあたり 0.0005 USD
AWS Security Hub - 取り込みイベントの検索	アカウント/リージョン/月あたりの最初の 10,000 イベントは無料です。Security Hub のセキュリティチェックに関連する取り込みイベントを検索します。	アカウント/リージョン/月あたりの 10,000 を超えるイベントのコストは、イベントあたり 0.00003 USD
Amazon CloudWatch - メトリクス	基本モニタリングメトリクス (5 分間隔) 10 詳細モニタリングメトリクス (1 分間隔) 100 万 API リクエスト (GetMetricData および GetMetricWidgetImage には適用されません)	最初の 10,000 メトリクスのコストは 0.30 USD/月 次の 240,000 メトリクスのコストは 0.10 USD/月 次の 750,000 メトリクスのコストは 0.05 USD/月 1,000,000 を超えるメトリクスのコストは 0.02 USD/月 API コールのコストは 1,000 リクエストあたり 0.01 USD
Amazon CloudWatch - ダッシュボード	1 か月あたり最大 50 のメトリクスに 3 つのダッシュボード	ダッシュボードあたり 3.00 USD/月

サービス	無料利用枠	料金 [USD]
Amazon CloudWatch - アラーム	10 アラームメトリクス (高解像度アラームには適用されません)	標準解像度 (60 秒) のコストはアラームメトリクスあたり 0.10 USD 高解像度 (10 秒) のコストはアラームメトリクスあたり 0.30 USD 標準解像度異常検出のコストはアラームあたり 0.30 USD 高解像度異常検出のコストはアラームあたり 0.90 USD 組み合わせる場合のコストはアラームあたり 0.50 USD
Amazon CloudWatch - ログコレクション	5 GB のデータ (取り込み、アーカイブストレージ、および Logs Insights クエリでスキャンされたデータ)	1 GB あたり 0.50 USD
Amazon CloudWatch - ログストレージ	5 GB のデータ (取り込み、アーカイブストレージ、および Logs Insights クエリでスキャンされたデータ)	スキャンされたデータの GB あたり 0.005 USD
Amazon CloudWatch -イベント	カスタムイベントを除くすべてのイベントが含まれます	カスタムイベントの場合は 100 万イベントあたり 1.00 USD。クロスアカウントイベントの場合は 100 万イベントあたり 1.00 USD
AWS Lambda - リクエスト	1 か月あたり 100 万の無料リクエスト	100 万リクエストあたり 0.20 USD

サービス	無料利用枠	料金 [USD]
AWS Lambda - 期間	1 か月あたり 400,000 GB 秒のコンピューティング時間	1 GB 秒あたり 0.0000166667 USD 期間の料金は、関数に割り当てるメモリの量によって異なります。関数には、128MB から 10,240 MB までの任意の量のメモリを 1MB 単位で割り当てることができます。
AWS Step Functions - 状態移行	1 か月あたり 4,000 回の無料の状態移行	その後、1,000 回の状態移行あたり 0.025 USD
Amazon EventBridge	AWS サービスによって発行されたすべての状態変更イベントは無料です	カスタムイベントには発行される 100 万 のカスタムイベントあたり 1.00 USD のコストがかかります サードパーティー (SaaS) イベントのコストは 100 万 の発行済みイベントあたり 1.00 USD クロスアカウントイベントのコストは送信された 100 万 のクロスアカウントイベントあたり 1.00 USD
Amazon SNS	1 か月あたり最初の 100 万件の Amazon SNS リクエストが無料	その後、100 万リクエストあたり 0.50 USD
Amazon SQS	1 か月あたり最初の 100 万件の Amazon SQS リクエストが無料	その後、100 万から 1,000 億リクエストあたり 0.40 USD

サービス	無料利用枠	料金 [USD]
Amazon DynamoDB	最初の 25GB のストレージは無料	その後、100 万回の整合性のある読み込みと書き込みあたり 2.00 USD

料金の例 (月額)

例 1: 1 か月あたり 300 回の修復

- 10 アカウント、1 リージョン
- アカウント/リージョン/月あたり 30 回の修復
- 合計コストは 21.17 USD/月

サービス	引き受け	月額料金 [USD]
AWS Systems Manager Automation	ステップ: ~4 ステップ x 300 回の修復 x 0.002 USD = 2.40 USD 期間: 10 秒 x 300 回の修復 x 0.00003 USD = 0.09 USD	2.49 USD
AWS Security Hub	請求対象サービスの使用なし	$0
Amazon CloudWatch Logs	300 回の修復 x 0.000002 USD = 0.0006 USD 0.0006 USD x 0.03 = 0.000018 USD	< 0.01 USD
AWS Lambda - リクエスト	300 回の修復 x 6 件のリクエスト = 1,800 件のリクエスト 0.20 USD x 1,000,000 件のリクエスト = 0.20 USD	0.20 USD

サービス	引き受け	月額料金 [USD]
AWS Lambda - 期間	256M: 1.875 GB 秒 x 300 回の修復 x 0.0000167 USD = 0.009375 USD	< 0.01 USD
AWS Step Functions	17 回の状態移行 x 300 回の修復 = 5,100 0.025 USD x (5,100/1,000) 回の状態移行 = 0.15 USD	0.15 USD
Amazon EventBridge ルール	ルールの料金は無料	$0
AWS Key Management Service	1 つのキー x 10 のアカウント x 1 リージョン x 1 USD = 10 USD	10.00 USD
Amazon DynamoDB	2.00 USD x 1,000,000 回の読み込みおよび書き込み = 2.00 USD	2.00 USD
Amazon SQS	0.40 USD x 1,000,000 件のリクエスト = 0.40 USD	0.40 USD
Amazon SNS	0.50 USD x 1,000,000 件の通知 = 0.50 USD	0.50 USD
Amazon CloudWatch - メトリクス	0.30 USD x 7 つのカスタムメトリクス = 2.10 USD 001 USD x (300 x 3 ÷ 1,000) の put メトリクス API コール = 0.01 USD	2.11 USD
Amazon CloudWatch - ダッシュボード	3.00 USD x 1 つのダッシュボード = 3.00 USD	3.00 USD

サービス	引き受け	月額料金 [USD]
Amazon CloudWatch - アラーム	0.10 USD x 3 つのアラーム = 0.30 USD	0.30 USD
合計		21.17 USD

例 2: 1 か月あたり 3,000 回の修復

- 100 アカウント、1 リージョン
- アカウント/リージョン/月あたり 30 回の修復
- 合計コスト 134.86 USD/月

サービス	引き受け	月額料金 [USD]
AWS Systems Manager Automation	ステップ: ~4 ステップ x 3,000 回の修復 x 0.002 USD = 24.00 USD 期間: 10 秒 x 3,000 回の修復 x 0.00003 USD = 0.90 USD	24.90 USD
AWS Security Hub	請求対象サービスの使用なし	$0
Amazon CloudWatch Logs	3,000 回の修復 x 0.000002 USD = 0.006 USD 0.006 USD x 0.03 = 0.00018 USD	< 0.01 USD
AWS Lambda - リクエスト	3,000 回の修復 x 6 件のリクエスト = 18,000 件のリクエスト 0.20 USD x 1,000,000 件のリクエスト = 0.20 USD	0.20 USD

サービス	引き受け	月額料金 [USD]
AWS Lambda - 期間	256M: 1.875 GB 秒 x 3,000 回の修復 x 0.000167 USD = 0.09375 USD	0.09 USD
AWS Step Functions	17 回の状態移行 x 3,000 回の修復 = 51,000 0.025 USD x (51,000 ÷ 1,000) 回の状態移行 = 1.275 USD	1.28 USD
Amazon EventBridge ルール	ルールの料金は無料	$0
AWS Key Management Service	1 つのキー x 100 のアカウント x 1 リージョン x 1 USD = 100 USD	100 USD
Amazon DynamoDB	2.00 USD x 1,000,000 回の読み込みおよび書き込み = 2.00 USD	2.00 USD
Amazon SQS	0.40 USD x 1,000,000 件のリクエスト = 0.40 USD	0.40 USD
Amazon SNS	0.50 USD x 1,000,000 件の通知 = 0.50 USD	0.50 USD
Amazon CloudWatch - メトリクス	0.30 USD x 7 つのカスタムメトリクス = 2.10 USD 0.01 USD x (3000 x 3 ÷ 1,000) の put メトリクス API コール = 0.09 USD	2.19 USD
Amazon CloudWatch - ダッシュボード	3.00 USD x 1 つのダッシュボード = 3.00 USD	3.00 USD

サービス	引き受け	月額料金 [USD]
Amazon CloudWatch - アラーム	0.10 USD x 3 つのアラーム = 0.30 USD	0.30 USD
合計		134.86 USD

例 3: 1 か月あたり 30,000 回の修復

- 1,000 アカウント、1 リージョン
- アカウント/リージョン/月あたり 30 回の修復
- 合計コスト 1,281.01 USD/月

サービス	引き受け	月額料金 [USD]
AWS Systems Manager Automation	ステップ: ~4 ステップ x 30,000 回の修復 x 0.002 USD = 240.00 USD 期間: 10 秒 x 30,000 回の修復 x 0.00003 USD = 9.00 USD	249.00 USD
AWS Security Hub	請求対象サービスの使用なし	$0
Amazon CloudWatch Logs	30,000 回の修復 x 0.000002 USD = 0.06 USD 0.06 USD x 0.03 = 0.0018 USD	< 0.01 USD
AWS Lambda - リクエスト	30,000 回の修復 x 6 件のリクエスト = 180,000 件のリクエスト 0.20 USD x 1,000,000 件のリクエスト = 0.20 USD	0.20 USD

サービス	引き受け	月額料金 [USD]
AWS Lambda - 期間	256M: 1.875 GB 秒 x 30,000 回の修復 x 0.000,167 USD = 0.9375 USD	0.94 USD
AWS Step Functions	17 回の状態移行 x 30,000 回の修復 = 510,000 0.025 USD x (510,000÷1,000) 回の状態移行 = 12.75 USD	12.75 USD
Amazon EventBridge ルール	ルールの料金は無料	$0
AWS Key Management Service	1 つのキー x 1,000 のアカウント x 1 リージョン x 1 USD = 1,000 USD	1,000 USD
Amazon DynamoDB	0.000002 USD x 1,000,000 回の読み込みおよび書き込み = 2.00 USD	2.00 USD
Amazon SQS	0.000004 USD x 1,000,000 件のリクエスト = 0.40 USD	0.40 USD
Amazon SNS	0.000005 USD x 1,000,000 件の通知 = 0.50 USD	0.50 USD
Amazon CloudWatch - メトリクス	0.30 USD x 6 つのカスタムメトリクス = 1.80 USD 0.01 USD x (30,000 x 3 ÷ 1,000) の put メトリクス API コール = 0.90 USD	2.70 USD
Amazon CloudWatch - ダッシュボード	3.00 USD x 1 つのダッシュボード = 3.00 USD	3.00 USD

サービス	引き受け	月額料金 [USD]
Amazon CloudWatch - アラーム	0.10 USD x 2 つのアラーム = 0.20 USD	0.20 USD
Amazon CloudWatch – Application Insights	0.10 USD x 40 アラーム (最大) = 4.00 USD 0.53 USD x 10 GB のログデータ (推定) = 5.30 USD 0.00267 USD x 5 OpsItems (推定) = ~0.01 USD	9.31 USD
合計		1,281.01 USD

オプション機能の追加コスト

このセクションでは、このソリューションのオプション機能に関連する追加コストについて説明します。

強化された CloudWatch メトリクス

管理スタックをデプロイするときに EnableEnhancedCloudWatchMetrics パラメータに `yes` を選択した場合、ソリューションはコントロール ID ごとに 2 つのカスタムメトリクスと 1 つのアラームを作成します。コストは、修復するコントロール ID の数によって異なります。次の表では、コストの上限を決定するために、1 か月あたり 96 の異なるコントロール ID をすべて修復することを前提としています。

サービス	引き受け 96 の ID x 2 = 192 のカスタムメトリクス	月額料金 [USD]
Amazon CloudWatch - メトリクス	0.30 USD x 192 のカスタムメトリクス = 57.60 USD	57.60 USD

サービス	引き受け	月額料金 [USD]
	96 の ID x 2 = 192 のカスタムメトリクス	
Amazon CloudWatch - アラーム	0.10 USD x 96 のアラーム = 9.60 USD	9.60 USD
合計		67.20 USD

CloudTrail アクションログ

アクションログ機能を有効にする各メンバーアカウントで、ソリューションはすべての書き込み管理イベントをログに記録する CloudTrail 証跡を作成します。Lambda 関数は、ソリューションに関連しないイベントを除外します。つまり、ソリューションに関連しないイベントは引き続き証跡によってキャプチャされ、Lambda 関数によって処理されるため、コストはアカウントの管理イベントの合計数に関連しています。

次の表では、アカウントで 1 か月あたり 150,000 件の管理イベントを想定しています。実際のコストは、アカウントの実際の管理イベントアクティビティによって異なります。

サービス	引き受け	月額料金 [USD]
AWS CloudTrail	150,000 x 2.00 USD ÷ 100,000 = 3.00 USD	3.00 USD
Lambda	150,000 x 0.2 x 0.125 = 3,750 GB 秒 3,750 x 0.0000166667 USD = 0.0625 USD の計算時間コスト 0.15 x 0.20 USD = 0.03 USD のリクエストコスト	0.0925 USD

サービス	引き受け	月額料金 [USD]
	0.0625 USD + 0.03 USD = Lambda の合計コスト 0.0952 USD	
合計		メンバーアカウントあたり 3.09 USD

セキュリティ

AWS インフラストラクチャでシステムを構築すると、お客様と AWS の間でセキュリティ上の責任が分担されます。この責任共有モデルにより、AWS がホストオペレーティングシステムと仮想化レイヤーからサービスが運用されている施設の物理的なセキュリティに至るまでのコンポーネントを運用、管理、および制御するため、お客様の運用上の負担を軽減するのに役立ちます。AWS セキュリティの詳細については、AWS クラウドのセキュリティを参照してください。

IAM ロール

AWS Identity and Access Management (IAM) ロールを使用すると、AWS クラウドのサービスとユーザーに対してアクセスポリシーとアクセス許可をきめ細かく割り当てることができます。このソリューションでは、ソリューションの自動関数に、各修復に固有のアクセス許可の狭い範囲のセット内で修復アクションを実行するためのアクセス権を付与する IAM ロールを作成します。

管理者アカウントの Step Function は、SO0111-SHARR-Orchestrator-Admin ロールに割り当てられます。このロールのみが、各メンバーアカウントで SO0111-Orchestrator-Member を引き受けることができます。メンバーロールは、各修復ロールによって AWS Systems Manager サービスに渡され、特定の修復ランブックを実行できます。修復ロール名は SO0111 で始まり、その後に修復ランブックの名前と一致する説明が続きます。例えば、SO0111-RemoveVPCDefaultSecurityGroupRules は、ASR-RemoveVPCDefaultSecurityGroupRules 修復ランブックのロールです。

サポートされている AWS リージョン

リージョン名	リージョンコード
米国東部 (オハイオ)	us-east-2

リージョン名	リージョンコード
米国東部 (バージニア北部)	us-east-1
米国西部 (北カリフォルニア)	us-west-1
米国西部 (オレゴン)	us-west-2
アフリカ (ケープタウン)	af-south-1
アジアパシフィック (香港)	ap-east-1
アジアパシフィック (ハイデラバード)	ap-south-2
アジアパシフィック (ジャカルタ)	ap-southeast-3
アジアパシフィック (メルボルン)	ap-southeast-4
アジアパシフィック (ムンバイ)	ap-south-1
アジアパシフィック (大阪)	ap-northeast-3
アジアパシフィック (ソウル)	ap-northeast-2
アジアパシフィック (シンガポール)	ap-southeast-1
アジアパシフィック (シドニー)	ap-southeast-2
アジアパシフィック (東京)	ap-northeast-1
カナダ (中部)	ca-central-1
欧州 (フランクフルト)	eu-central-1
欧州 (アイルランド)	eu-west-1
欧州 (ロンドン)	eu-west-2
ヨーロッパ (ミラノ)	eu-south-1
欧州 (パリ)	eu-west-3

リージョン名	リージョンコード
欧州 (スペイン)	eu-south-2
欧州 (ストックホルム)	eu-north-1
欧州 (チューリッヒ)	eu-central-2
中東 (バーレーン)	me-south-1
中東 (アラブ首長国連邦)	me-central-1
南米 (サンパウロ)	sa-east-1
AWS GovCloud (米国東部)	us-gov-east-1
AWS GovCloud (米国西部)	us-gov-east-2
中国 (北京)	cn-north-1
中国 (寧夏)	cn-northwest-1

クォータ

サービスクォータ (制限とも呼ばれます) は、AWS アカウントのサービスリソースまたはオペレーションの最大数です。

このソリューション内の AWS サービスのクォータ

このソリューションに実装されている各サービスに十分なクォータがあることを確認してください。詳細については、「AWS サービスクォータ」を参照してください。

次のリンクを使用して、そのサービスのページに移動します。ページを切り替えずに、ドキュメント内のすべての AWS サービスの Service Quotas を表示するには、PDF の「サービスエンドポイントとクォータ」ページの情報を参照してください。

AWS CloudFormation のクォータ

ご使用の AWS アカウントには AWS CloudFormation のクォータがあり、このソリューションでスタックを起動する際に注意する必要があります。これらのクォータを理解することで、このソ

リューションを正常にデプロイできなくなる、制限によるエラーを回避できます。詳細については、「AWS CloudFormation ユーザーガイド」の「AWS CloudFormation のクォータ」を参照してください。

Amazon EventBridge ルールのクォータ

AWS アカウントには、ソリューションでデプロイするプレイブックを選択するときに注意すべき Amazon EventBridge ルールのクォータがあります。各プレイブックは、修復できるコントロールごとに EventBridge ルールを作成します。複数のプレイブックをデプロイする場合、ルールのクォータに達する可能性があります。詳細については、「Amazon EventBridge ユーザーガイド」の「Amazon EventBridge クォータ」を参照してください。

AWS Security Hub のデプロイ

AWS Security Hub のデプロイと設定は、このソリューションの前提条件です。AWS Security Hub を設定する方法の詳細については、「AWS Security Hub ユーザーガイド」の「AWS Security Hub の設定」を参照してください。

少なくとも、プライマリアカウントで動作する Security Hub を設定する必要があります。このソリューションは、Security Hub プライマリアカウントと同じアカウント (および AWS リージョン) にデプロイできます。Security Hub のプライマリアカウントとセカンダリアカウントごとに、ソリューションの AWS Step Functions に AssumeRole アクセス許可を付与するメンバーテンプレートをデプロイして、アカウントで修復ランブックを実行する必要があります。

スタックと StackSets のデプロイの比較

スタックセットでは、1 つの AWS CloudFormation テンプレートを使用して、複数の AWS リージョンの AWS アカウントにスタックを作成できます。バージョン 1.4 以降、このソリューションは、デプロイ場所と方法に基づいてリソースを分割することでスタックセットのデプロイをサポートします。マルチアカウントのお客様、特に AWS Organizations を使用しているお客様は、多くのアカウントにまたがるデプロイにスタックセットを使用することによってベネフィットを得られます。これにより、ソリューションのインストールと保守に必要な労力を削減できます。StackSets の詳細については、「AWS CloudFormation StackSets の使用」を参照してください。

ソリューションをデプロイする

> **Important**
>
> Security Hub で統合されたコントロールの検出結果機能が有効になっている場合 (これは新しいデプロイではデフォルトです)、このソリューションをデプロイするときにのみセキュリティコントロール (CS) プレイブックを有効にします。この機能が有効になっていない場合は、Security Hub で有効になっているセキュリティ標準のプレイブックのみを有効にします。追加のプレイブックを有効にすると、EventBridge ルールのクォータに達する可能性があります。

このソリューションは、AWS CloudFormation テンプレートとスタックを使用してデプロイを自動化します。CloudFormation テンプレートは、このソリューションに含まれる AWS リソースとそのプロパティを指定します。CloudFormation スタックは、テンプレートに記述されているリソースをプロビジョニングします。

ソリューションが機能するには、3 つのテンプレートをデプロイする必要があります。まず、テンプレートをデプロイする場所を決定し、次にテンプレートをデプロイする方法を決定します。

この概要では、テンプレートと、テンプレートをデプロイする場所と方法を決定する方法について説明します。次のセクションでは、各スタックをスタックまたは StackSet としてデプロイする詳細な手順について説明します。

各スタックをデプロイする場所を決定する

3 つのテンプレートは次の名前で参照され、次のリソースが含まれます。

- 管理者スタック: オーケストレーターステップ関数、イベントルール、および Security Hub カスタムアクション。
- メンバースタック: SSM Automation ドキュメントを修復します。
- メンバーロールスタック: 修復用の IAM ロール。

管理者スタックは、1 つのアカウントと 1 つのリージョンに 1 回デプロイする必要があります。これは、組織の Security Hub の検出結果の集約先として設定したアカウントとリージョンにデプロイする必要があります。

このソリューションは Security Hub の検出結果で動作するため、Security Hub 管理者アカウントとリージョンで検出結果を集約するようにアカウントまたはリージョンが設定されていない場合、特定のアカウントとリージョンの検出結果を操作することはできません。

例えば、組織にはリージョン us-east-1 および us-west-2 で運用されているアカウントがあり、リージョン us-east-1 の Security Hub 委任管理者としてアカウント 111111111111 があります。アカウント 222222222222 および 333333333333 は、委任管理者アカウント 111111111111 の Security Hub メンバーアカウントである必要があります。3 つのアカウントはすべて、us-west-2 から us-east-1 に検出結果を集約するように設定する必要があります。管理者スタックは、us-east-1 のアカウント 111111111111 にデプロイする必要があります。

検出結果の集約の詳細については、Security Hub の「委任管理者アカウント」と「クロスリージョン集約」のドキュメントを参照してください。

管理者スタックは、メンバーアカウントからハブアカウントに信頼関係を作成できるように、メンバースタックをデプロイする前にデプロイを完了する必要があります。

メンバースタックは、検出結果を修復するすべてのアカウントとリージョンにデプロイする必要があります。これには、以前に ASR 管理者スタックをデプロイした Security Hub 委任管理者アカウントを含めることができます。SSM Automation の無料利用枠を使用するには、オートメーションドキュメントがメンバーアカウントで実行されている必要があります。

前の例を使用して、すべてのアカウントとリージョンの検出結果を修復する場合は、メンバースタックを 3 つのアカウントすべて (111111111111、222222222222、333333333333) と両方のリージョン (us-east-1 および us-west-2) にデプロイする必要があります。

メンバーロールスタックはすべてのアカウントにデプロイする必要がありますが、アカウントごとに 1 回のみデプロイできるグローバルリソース (IAM ロール) が含まれています。メンバーロールスタックをデプロイするリージョンは関係ないため、わかりやすくするために、管理者スタックがデプロイされているのと同じリージョンにデプロイすることをお勧めします。

前の例を使用して、メンバーロールスタックを us-east-1 の 3 つのアカウントすべて (111111111111、222222222222、および 333333333333) にデプロイすることをお勧めします。

各スタックのデプロイ方法を決定する

スタックをデプロイするためのオプションは次のとおりです。

- CloudFormation StackSet (セルフマネージド型のアクセス許可)

- CloudFormation StackSet (サービス管理型のアクセス許可)
- CloudFormation スタック

サービス管理型のアクセス許可を持つ StackSets は、独自のロールをデプロイする必要はなく、組織内の新しいアカウントに自動的にデプロイできるため、最も便利です。残念ながら、このメソッドは、管理者スタックとメンバースタックの両方で使用するネストされたスタックをサポートしていません。この方法でデプロイできるスタックは、メンバーロールスタックのみです。

組織全体にデプロイする場合、組織管理アカウントは含まれていないため、組織管理アカウントの検出結果を修復する場合は、このアカウントに個別にデプロイする必要があります。

メンバースタックはすべてのアカウントとリージョンにデプロイする必要がありますが、ネストされたスタックが含まれているため、サービス管理型のアクセス許可を持つ StackSets を使用してデプロイすることはできません。したがって、このスタックをセルフマネージド型のアクセス許可を持つ StackSets を使用してデプロイすることをお勧めします。

管理者スタックは 1 回のみデプロイされるため、1 つのアカウントとリージョンにプレーン CloudFormation スタックとして、またはセルフマネージド型のアクセス許可を持つ StackSet としてデプロイできます。

統合されたコントロールの検出結果

組織内のアカウントは、Security Hub の統合されたコントロールの検出結果機能を有効または無効に設定できます。「AWS Security Hub ユーザーガイド」の「統合されたコントロールの検出結果」を参照してください。

> **Important**
>
> 有効にした場合、ソリューションの v2.0.0 以降を使用する必要があります。さらに、「SC」または「セキュリティコントロール」標準のために、管理者とメンバーの両方のネストされたスタックをデプロイする必要があります。これにより、この機能がオンになっているときに生成された統合コントロール ID で使用するオートメーションドキュメントと EventBridge ルールがデプロイされます。この機能を使用する場合、特定の標準 (AWS FSBP など) に対して管理者またはメンバーのネストされたスタックをデプロイする必要はありません。

AWS CloudFormation テンプレート

View template

aws-sharr-deploy.template - このテンプレートを使用して、AWS での自動化されたセキュリティ対応ソリューションを起動します。テンプレートは、ソリューションのコアコンポーネント、AWS Step Functions ログのネストされたスタック、アクティブ化するセキュリティ標準ごとに 1 つのネストされたスタックをインストールします。

使用されるサービスには、Amazon Simple Notification Service、AWS Key Management Service、AWS Identity and Access Management、AWS Lambda、AWS Step Functions、Amazon CloudWatch Logs、Amazon S3、AWS Systems Manager などがあります。

管理者アカウントのサポート

以下のテンプレートは、サポートするセキュリティ標準を有効にするために AWS Security Hub 管理者アカウントにインストールされます。`aws-sharr-deploy.template` のインストール時にインストールするテンプレートを以下から選択できます。

aws-sharr-orchestrator-log.template - オーケストレーターステップ関数の CloudWatch ロググループを作成します。

AFSBPStack.template - AWS の基本的なセキュリティのベストプラクティス v1.0.0 ルール。

CIS120Stack.template - CIS Amazon Web Services Foundations Benchmark、v1.2.0 ルール。

CIS140Stack.template - CIS Amazon Web Services Foundations Benchmark、v1.4.0 ルール。

PCI321Stack.template - PCI-DSS v3.2.1 ルール。

NISTStack.template - 米国国立標準技術研究所 (NIST)、v5.0.0 ルール。

SCStack.template - SC v2.0.0 ルール。

メンバーアカウント

View template

aws-sharr-member.template - コアソリューションを設定した後、このテンプレートを使用して、AWS Systems Manager Automation ランブックとアクセス許可を各 AWS Security Hub メン

バーアカウント (管理者アカウントを含む) にインストールします。このテンプレートを使用すると、インストールするセキュリティ標準プレイブックを選択できます。

`aws-sharr-member.template` は、選択内容に基づいて次のテンプレートをインストールします。

aws-sharr-remediations.template - 1 つ以上のセキュリティ標準で使用される一般的な修復コード。

AFSBPMemberStack.template - AWS の基本的なセキュリティのベストプラクティス v1.0.0 の設定、アクセス許可、および修復ランブック。

CIS120MemberStack.template - CIS Amazon Web Services Foundations Benchmark、バージョン 1.2.0 の設定、アクセス許可、および修復ランブック。

CIS140MemberStack.template - CIS Amazon Web Services Foundations Benchmark、バージョン 1.4.0 の設定、アクセス許可、および修復ランブック。

PCI321MemberStack.template - PCI-DSS v3.2.1 の設定、アクセス許可、および修復ランブック。

NISTMemberStack.template - 米国国立標準技術研究所 (NIST)、v5.0.0 の設定、アクセス許可、修復ランブック。

SCMemberStack.template - セキュリティコントロールの設定、アクセス許可、および修復ランブック。

メンバーロール

View template

aws-sharr-member-roles.template - 各 AWS Security Hub メンバーアカウントに必要な修復ロールを定義します。

チケットシステム統合

次のいずれかのテンプレートを使用して、チケット発行システムと統合します。

View template

JiraBlueprintStack.template - Jira をチケット発行システムとして使用している場合はデプロイします。

View template

ServiceNowBlueprintStack.template - ServiceNow をチケット発行システムとして使用している場合はデプロイします。

別の外部チケットシステムを統合する場合は、これらのスタックのいずれかをブループリントとして使用して、独自のカスタム統合を実装する方法を理解できます。

自動デプロイ - StackSets

> **Note**
>
> StackSets を使用してデプロイすることをお勧めします。ただし、単一アカウントのデプロイ、テストまたは評価の目的の場合は、スタックのデプロイオプションを検討してください。

ソリューションを開始する前に、このガイドに記載されているアーキテクチャ、ソリューションコンポーネント、セキュリティ、設計に関する考慮事項を確認してください。このセクションのステップバイステップの手順に従って、ソリューションを設定して AWS Organizations にデプロイします。

デプロイ時間: StackSet パラメータに応じて、アカウントあたり約 30 分。

前提条件

AWS Organizations は、マルチアカウントの AWS 環境およびリソースの一元管理およびガバナンスを支援します。StackSets は AWS Organizations で最適に動作します。

以前に、このソリューションの v1.3.x 以前をデプロイしたことがある場合は、既存のソリューションをアンインストールする必要があります。詳細については、「ソリューションを更新する」を参照してください。

このソリューションをデプロイする前に、AWS Security Hub のデプロイを確認してください。

- AWS Organization には委任 Security Hub 管理者アカウントが必要です。
- Security Hub は、リージョン間で検出結果を集約するように設定する必要があります。詳細については、AWS Security Hub ユーザーガイドの「リージョン間の検出結果を集約する」を参照してください。
- AWS を使用している各リージョンで、組織の Security Hub を有効にする必要があります。

この手順では、AWS Organizations を使用する複数のアカウントがあり、AWS Organizations 管理者アカウントと AWS Security Hub 管理者アカウントを委任していることを前提としています。

デプロイの概要

> **Note**
>
> このソリューションの StackSets デプロイでは、サービスマネージド型とセルフマネージド型の StackSets の組み合わせを使用します。セルフマネージド型 StackSets は、サービスマネージド型 StackSets ではまだサポートされていないネストされた StackSets を使用するため、現在使用する必要があります。

AWS Organizations の委任管理者アカウントから StackSets をデプロイします。

計画

StackSets を使用したデプロイには、次のフォームを使用します。データを準備し、デプロイ中に値をコピーして貼り付けます。

```
AWS Organizations admin account ID: _________________
Security Hub admin account ID: _________________
CloudTrail Logs Group: ____________________________
Member account IDs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
____________________
AWS Organizations OUs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
____________________
```

(オプション) ステップ 0: チケット作成統合スタックをデプロイする

- チケット作成機能を使用する場合は、まずチケット作成統合スタックを Security Hub 管理者アカウントにデプロイします。

- このスタックから Lambda 関数名をコピーし、管理者スタックへの入力として指定します (ステップ 1 を参照)。

ステップ 1: 委任 Security Hub 管理者アカウントで管理者スタックを起動する

- セルフマネージド型 StackSet を使用して、Security Hub 管理者と同じリージョンの AWS Security Hub 管理者アカウントに `aws-sharr-deploy.template` AWS CloudFormation テンプレートを起動します。このテンプレートはネストされたスタックを使用します。
- インストールするセキュリティ標準を選択します。デフォルトでは、SC のみが選択されます (推奨)。
- 使用する既存のオーケストレーターロググループを選択します。以前のインストールからの `SO0111-SHARR- Orchestrator` が既に存在する場合は、`Yes` を選択します。

セルフマネージド型の StackSets の詳細については、「AWS CloudFormation ユーザーガイド」の「セルフマネージド型のアクセス許可を付与する」を参照してください。

ステップ 2: 各 AWS Security Hub メンバーアカウントに修復ロールをインストールする

ステップ 2 のテンプレートはステップ 1 で作成された IAM ロールを参照するため、ステップ 1 でデプロイが完了するまで待ちます。

- サービスマネージド型 StackSet を使用して、AWS Organizations の各アカウントの 1 つのリージョンで `aws-sharr-member-roles.template` AWS CloudFormation テンプレートを起動します。
- 新しいアカウントが組織に加わったときに、このテンプレートを自動的にインストールすることを選択します。
- AWS Security Hub 管理者アカウントのアカウント ID を入力します。

ステップ 3: 各 AWS Security Hub メンバーアカウントとリージョンでメンバースタックを起動する

- セルフマネージド型 StackSets を使用して、`aws-sharr-member.template` AWS CloudFormation テンプレートを、同じ Security Hub 管理者によって管理される AWS Organization のすべてのアカウントに AWS リソースがあるすべてのリージョンで起動します。

> **Note**
>
> サービスマネージド型 StackSets がネストされたスタックをサポートするまでは、組織に参加する新しいアカウントに対してこのステップを実行する必要があります。

- インストールするセキュリティ標準プレイブックを選択します。
- CloudTrail ロググループの名前を指定します (一部の修復で使用されます)。
- AWS Security Hub 管理者アカウントのアカウント ID を入力します。

(オプション) ステップ 0: チケットシステム統合スタックを起動する

1. チケット機能を使用する場合は、まずそれぞれの統合スタックを起動します。
2. Jira または ServiceNow 用に提供されている統合スタックを選択するか、独自のカスタム統合を実装するためのブループリントとして使用します。

   Jira スタックをデプロイするには:

   a. スタック名を入力します。

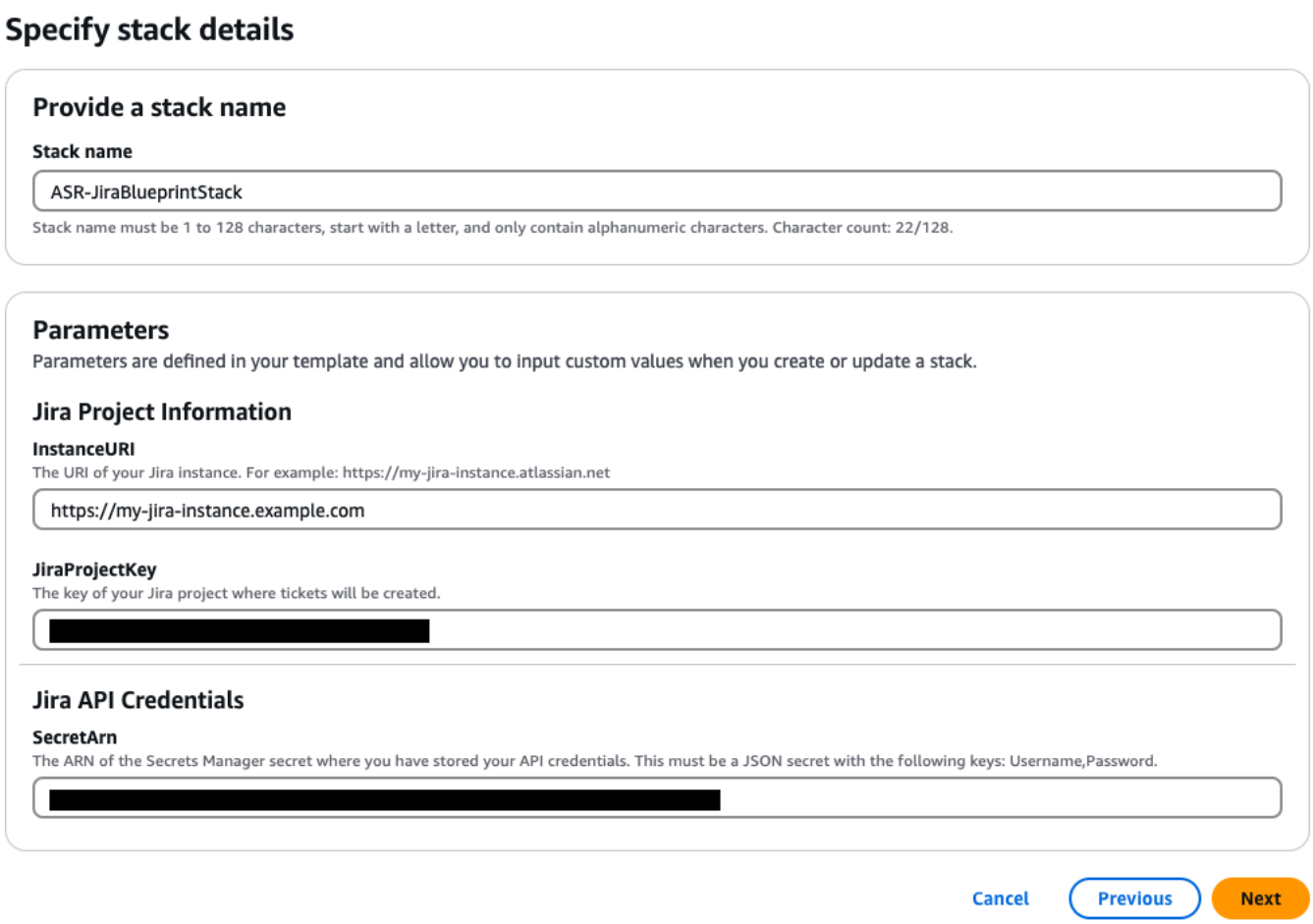
   b. Jira インスタンスに URI を指定します。

   c. チケットを送信する Jira プロジェクトのプロジェクトキーを指定します。

   d. Jira `Username` と `Password` を保持する新しいキーと値のシークレットを Secrets Manager に作成します。

   > **Note**
   >
   > ユーザー名を `Username` として、API キーを `Password` として指定することで、パスワードの代わりに Jira API キーを使用することを選択できます。

   e. このシークレットの ARN をスタックへの入力として追加します。



ServiceNow スタックをデプロイするには:

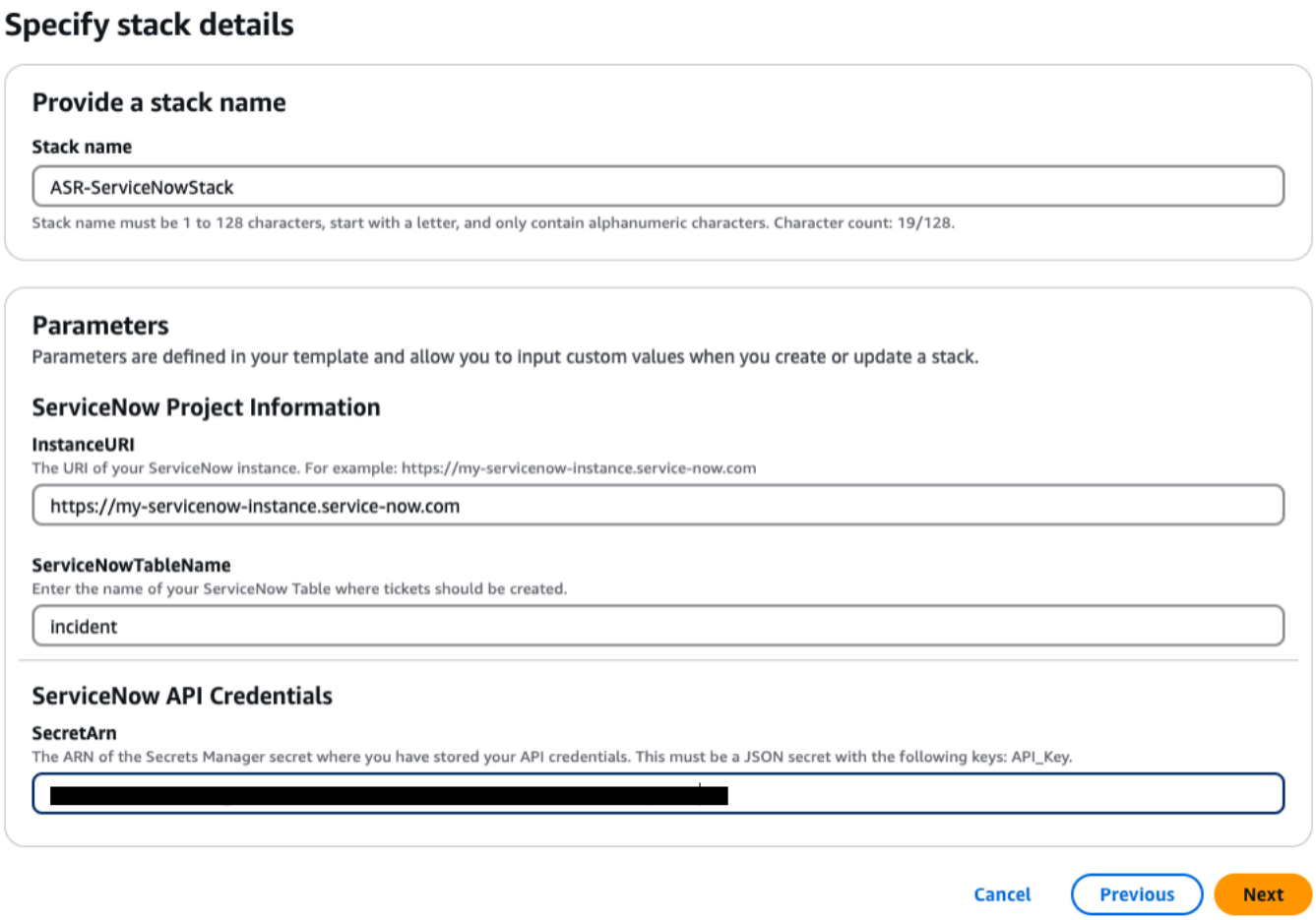
a. スタック名を入力します。

b. ServiceNow インスタンスの URI を指定します。

c. ServiceNow テーブル名を指定します。

d. 書き込み先のテーブルを変更するアクセス許可を持つ API キーを ServiceNow に作成します。

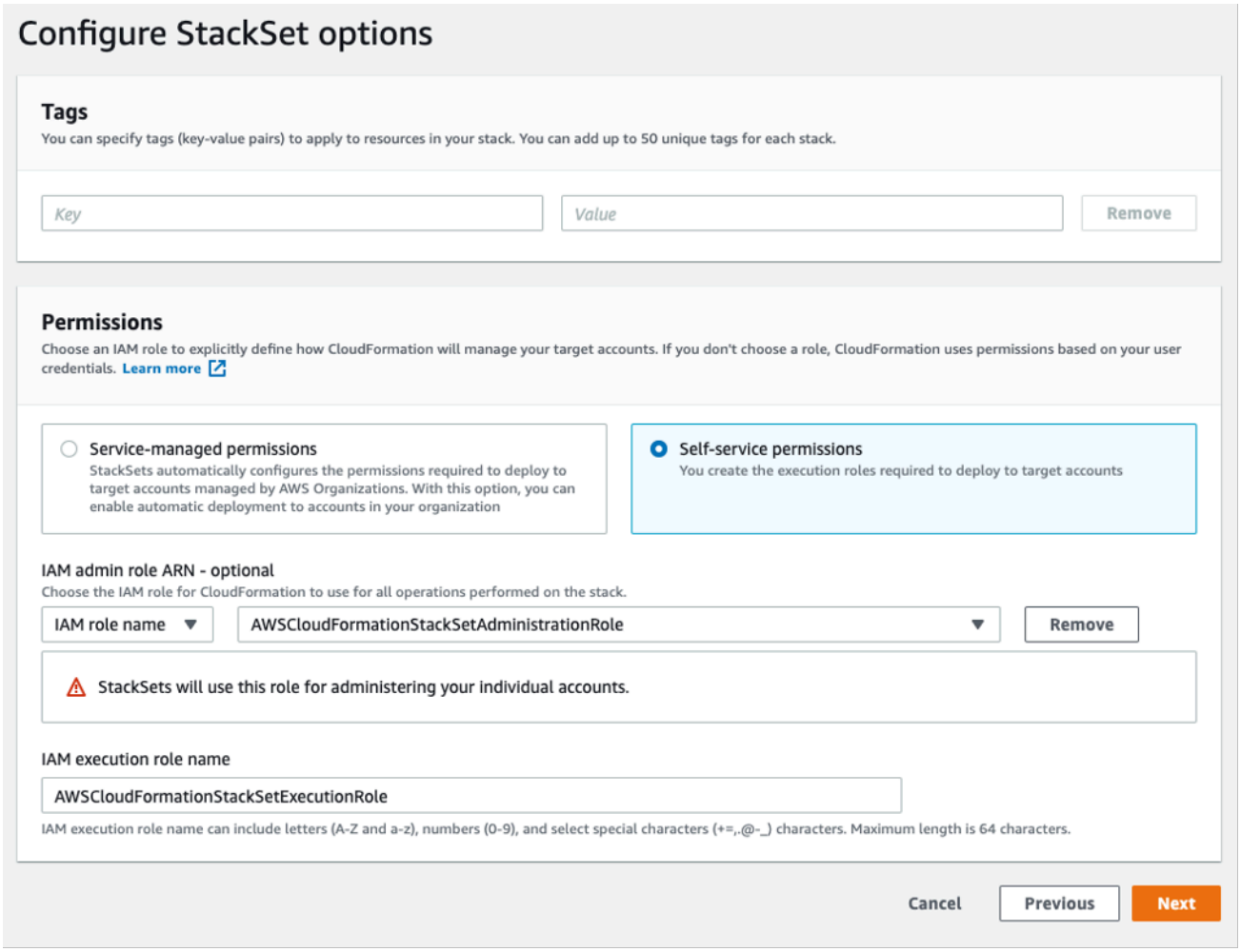
e. キー `API_Key` を使用して Secrets Manager でシークレットを作成し、そのシークレットの ARN をスタックへの入力として提供します。



カスタム統合スタックを作成するには: ソリューションオーケストレーター Step Functions が修復ごとに呼び出すことができる Lambda 関数を含めます。Lambda 関数は、Step Functions から提供された入力を受け取り、チケット発行システムの要件に従ってペイロードを構築し、システムにチケットの作成をリクエストする必要があります。

ステップ 1: 委任 Security Hub 管理者アカウントで管理者スタックを起動する

1. Security Hub 管理者アカウントを使用して、管理者スタック、`aws-sharr-deploy.template` を起動します。通常、1 つのリージョンの組織ごとに 1 つです。このスタックはネストされたスタックを使用するため、このテンプレートをセルフマネージド型の StackSet としてデプロイする必要があります。



StackSet オプションを設定する

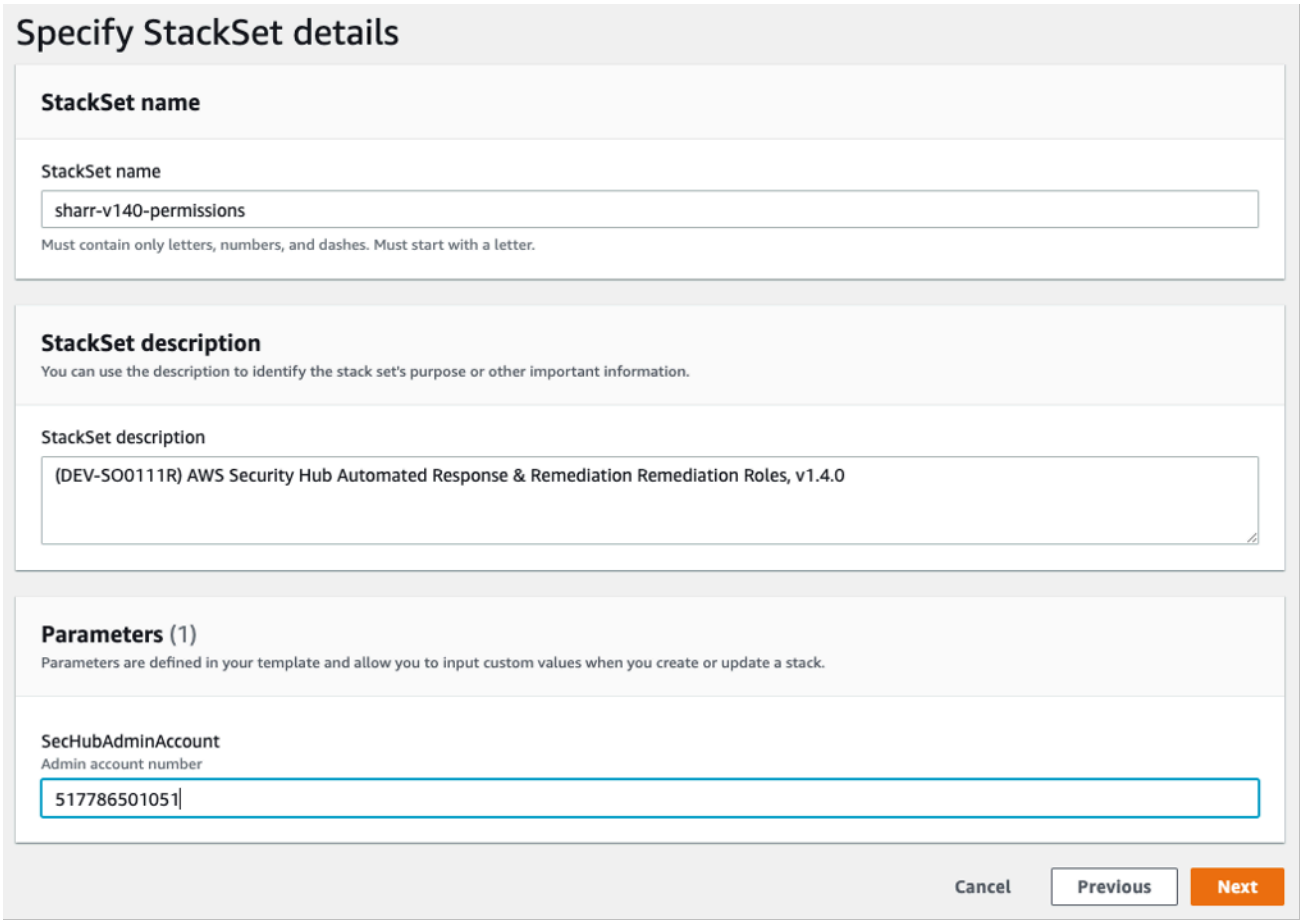
2. [アカウント番号] パラメータに、AWS Security Hub 管理者アカウントのアカウント ID を入力します。
3. [リージョンの指定] パラメータで、Security Hub 管理者が有効になっているリージョンのみを選択します。このステップが完了するまで待ってから、ステップ 2 に進みます。

ステップ 2: 各 AWS Security Hub メンバーアカウントに修復ロールをインストールする

サービスマネージド型 StackSets を使用して、メンバーロールテンプレート、`aws-sharr-member-roles.template` をデプロイします。この StackSet は、メンバーアカウントごとに 1 つのリージョンにデプロイする必要があります。SHARR オーケストレーターステップ関数からのクロスアカウント API コールを許可するグローバルロールを定義します。

1. 組織のポリシーに従って、組織全体 (通常) または組織単位にデプロイします。

2. AWS Organizations の新しいアカウントがこれらのアクセス許可を受け取るように、自動デプロイを有効にします。
3. [リージョンの指定] パラメータで、1 つのリージョンを選択します。IAM ロールはグローバルです。この StackSet のデプロイ中に、ステップ 3 に進むことができます。



StackSet の詳細を指定する

ステップ 3: 各 AWS Security Hub メンバーアカウントとリージョンでメンバースタックを起動する

メンバースタックはネストされたスタックを使用するため、セルフマネージド型の StackSet としてデプロイする必要があります。これは、AWS Organization の新しいアカウントへの自動デプロイをサポートしていません。

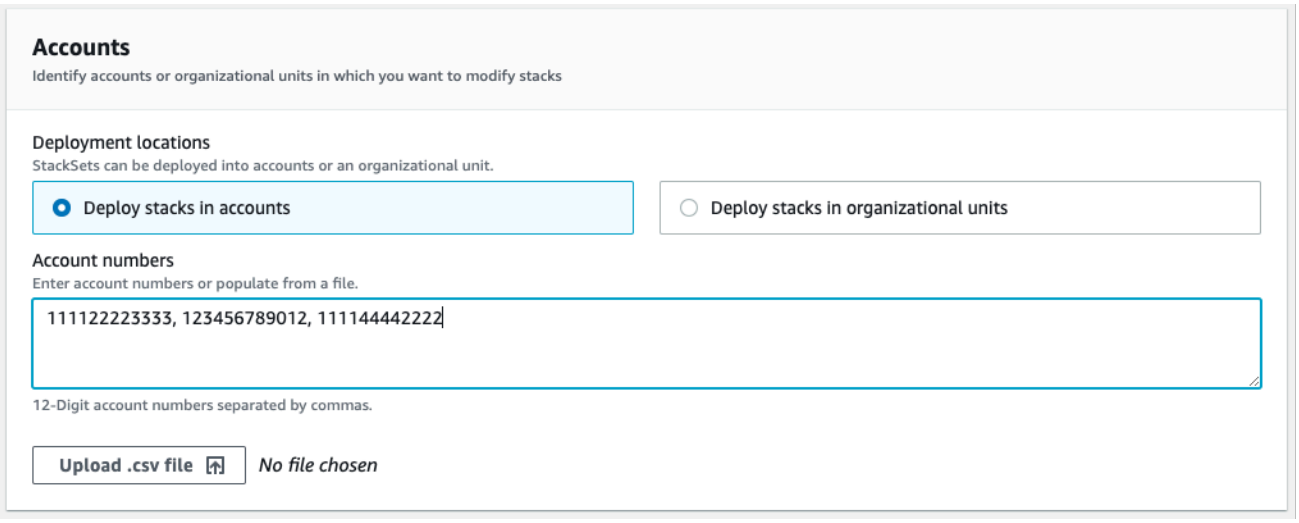
パラメータ

LogGroup 設定: CloudTrail ログを受信するロググループを選択します。存在しない場合、またはロググループがアカウントごとに異なる場合は、便利な値を選択します。アカウント管理者

は、CloudTrail ログの CloudWatch Logs グループを作成した後、Systems Manager – Parameter Store /Solutions/SO0111/Metrics_LogGroupName パラメータを更新する必要があります。これは、API コールでメトリクスアラームを作成する修復に必要です。

標準: メンバーアカウントにロードする標準を選択します。これにより、AWS Systems Manager ランブックのみがインストールされます。セキュリティ標準は有効になりません。

SecHubAdminAccount: ソリューションの管理者テンプレートをインストールした AWS Security Hub 管理者アカウントのアカウント ID を入力します。



アカウント

デプロイ先: アカウント番号または組織単位のリストを指定できます。

リージョンの指定: 検出結果を修復するすべてのリージョンを選択します。デプロイオプションは、アカウントとリージョンの数に応じて調整できます。リージョンの同時実行は並列にすることができます。

自動デプロイ - スタック

> **Note**
>
> マルチアカウントのお客様の場合は、StackSets を使用してデプロイすることを強くお勧めします。

ソリューションを開始する前に、このガイドに記載されているアーキテクチャ、ソリューションコンポーネント、セキュリティ、設計に関する考慮事項を確認してください。このセクションのステップバイステップの手順に従って、ソリューションを設定してアカウントにデプロイします。

デプロイ時間: 約 30 分

前提条件

このソリューションをデプロイする前に、AWS Security Hub がプライマリアカウントとセカンダリアカウントと同じ AWS リージョンにあることを確認してください。以前にこのソリューションをデプロイしたことがある場合は、既存のソリューションをアンインストールする必要があります。詳細については、「ソリューションを更新する」を参照してください。

デプロイの概要

次の手順を使用して、このソリューションを AWS にデプロイします。

(オプション) ステップ 0: チケットシステム統合スタックを起動する

- チケット作成機能を使用する場合は、まずチケット作成統合スタックを Security Hub 管理者アカウントにデプロイします。
- このスタックから Lambda 関数名をコピーし、管理者スタックへの入力として指定します (ステップ 1 を参照)。

ステップ 1: 管理者スタックを起動する

- `aws-sharr-deploy.template` AWS CloudFormation テンプレートを AWS Security Hub 管理者アカウントに起動します。
- インストールするセキュリティ標準を選択します。
- 使用する既存のオーケストレーターロググループを選択します (以前のインストールからの `SO0111-SHARR-Orchestrator` が既に存在する場合は `Yes` 選択します)。

ステップ 2: 各 AWS Security Hub メンバーアカウントに修復ロールをインストールする

- メンバーアカウントごとに 1 つのリージョンで `aws-sharr-member-roles.template` AWS CloudFormation テンプレートを起動します。
- AWS Security Hub 管理者アカウントの 12 桁のアカウント IG を入力します。

ステップ 3: メンバースタックを起動する

- CIS 3.1 ~ 3.14 修復で使用する CloudWatch Logs グループの名前を指定します。これは、CloudTrail ログを受信する CloudWatch Logs ロググループの名前である必要があります。
- 修復ロールをインストールするかどうかを選択します。これらのロールは、アカウントごとに 1 回のみインストールします。
- インストールするプレイブックを選択します。
- AWS Security Hub 管理者アカウントのアカウント ID を入力します。

ステップ 4: (オプション) 使用可能な修復を調整する

- メンバーアカウントごとに修復を削除します。この手順は省略可能です。

(オプション) ステップ 0: チケットシステム統合スタックを起動する

1. チケット機能を使用する場合は、まずそれぞれの統合スタックを起動します。
2. Jira または ServiceNow 用に提供されている統合スタックを選択するか、独自のカスタム統合を実装するためのブループリントとして使用します。

   Jira スタックをデプロイするには:

   a. スタック名を入力します。

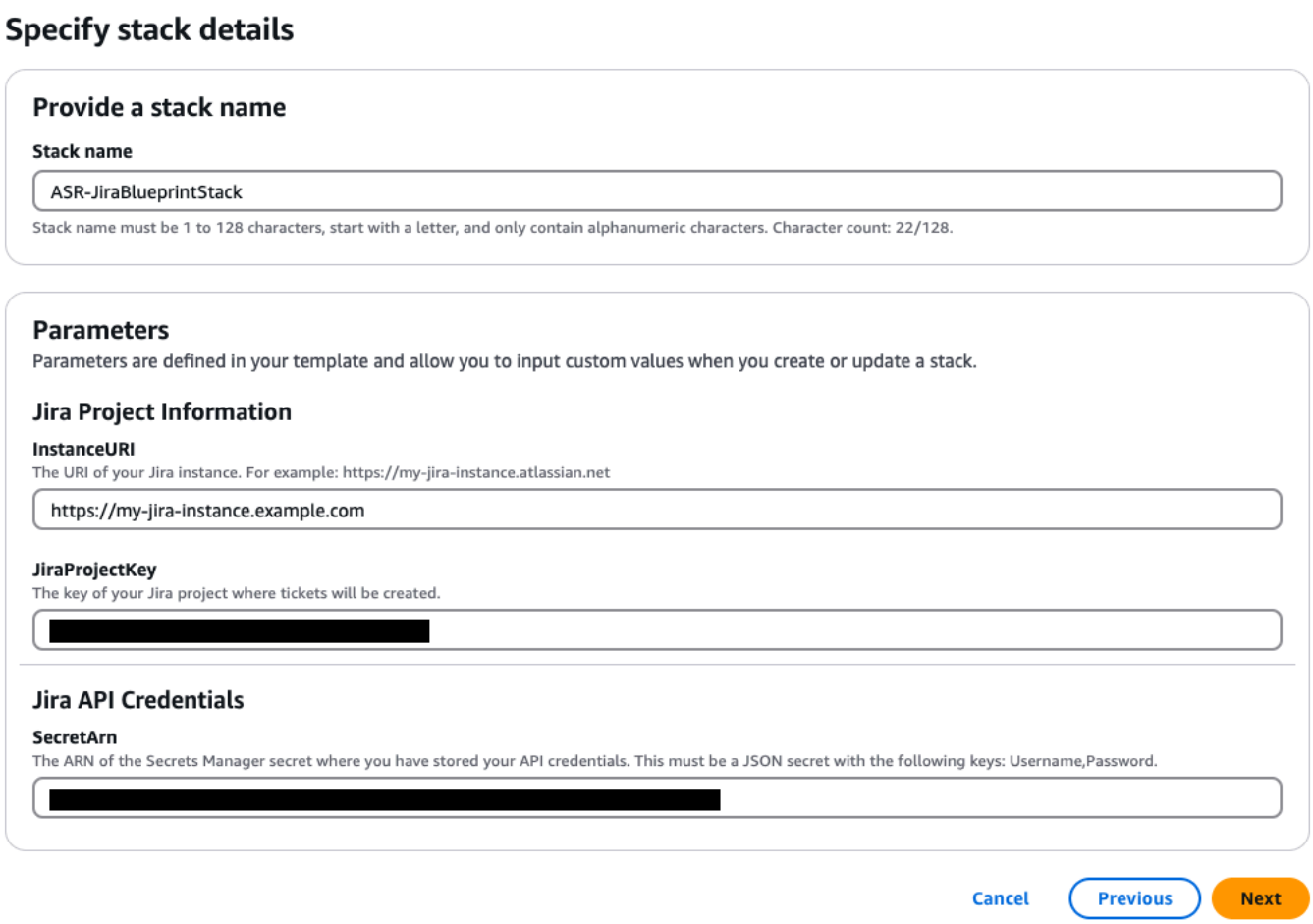
   b. Jira インスタンスに URI を指定します。

   c. チケットを送信する Jira プロジェクトのプロジェクトキーを指定します。

   d. Jira `Username` と `Password` を保持する新しいキーと値のシークレットを Secrets Manager に作成します。

   > **Note**
   >
   > ユーザー名を `Username` として、API キーを `Password` として指定することで、パスワードの代わりに Jira API キーを使用することを選択できます。

   e. このシークレットの ARN をスタックへの入力として追加します。



ServiceNow スタックをデプロイするには:

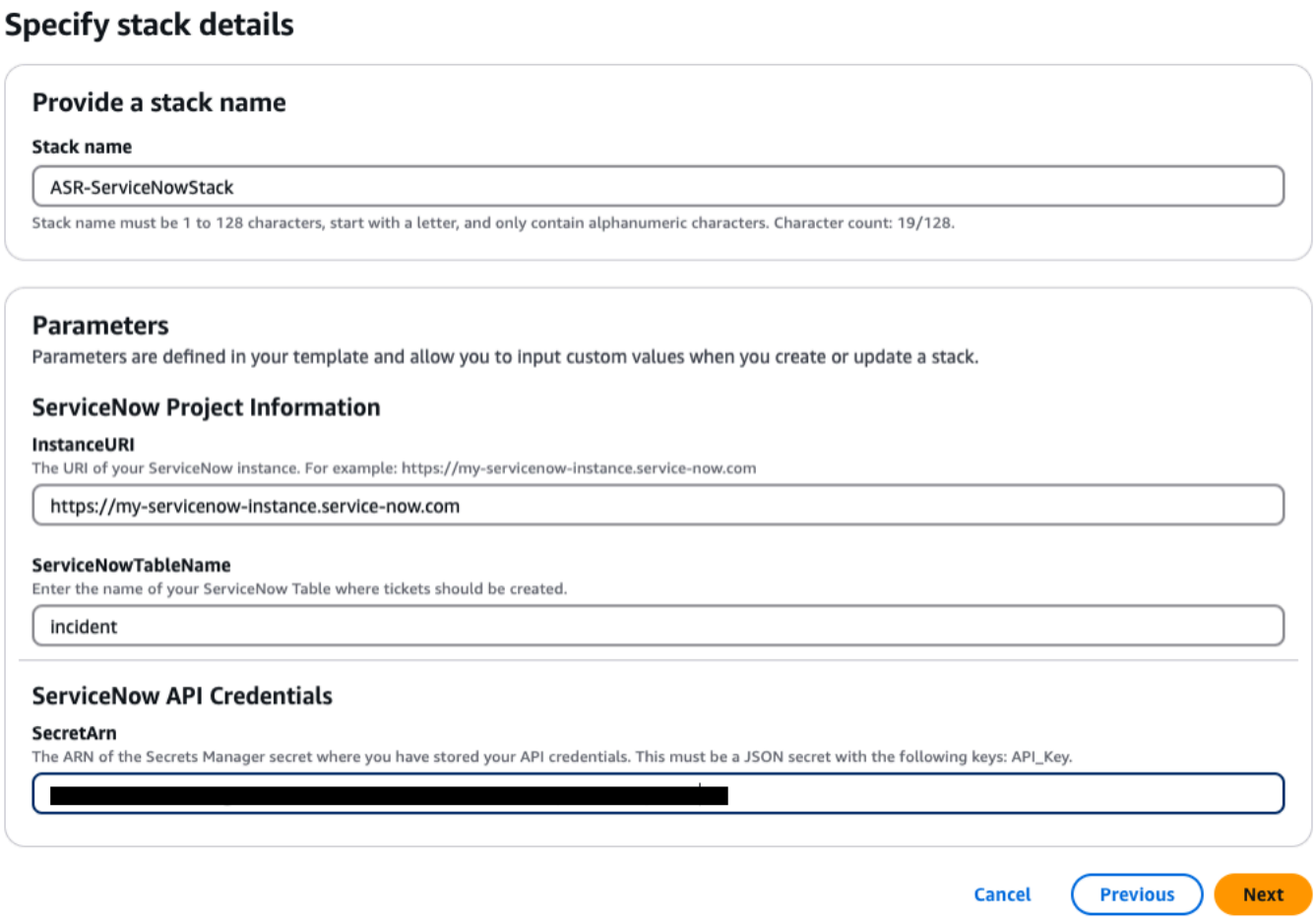
a. スタック名を入力します。

b. ServiceNow インスタンスの URI を指定します。

c. ServiceNow テーブル名を指定します。

d. 書き込み先のテーブルを変更するアクセス許可を持つ API キーを ServiceNow に作成します。

e. キー `API_Key` を使用して Secrets Manager でシークレットを作成し、そのシークレットの ARN をスタックへの入力として提供します。



カスタム統合スタックを作成するには: ソリューションオーケストレーター Step Functions が修復ごとに呼び出すことができる Lambda 関数を含めます。Lambda 関数は、Step Functions から提供された入力を受け取り、チケット発行システムの要件に従ってペイロードを構築し、システムにチケットの作成をリクエストする必要があります。

ステップ 1: 管理者スタックを起動する

> **Important**
>
> このソリューションには、匿名化された運用メトリクスを AWS に送信するオプションが含まれています。このデータを使用して、ユーザーがこのソリューションおよび関連サービスや製品をどのように使用しているかをよりよく理解します。このアンケートで収集されたデータは AWS が所有します。データ収集には、AWS プライバシー通知が適用されます。この機能を無効にするには、テンプレートをダウンロードし、AWS CloudFormation マッピングセクションを変更してから、AWS CloudFormation コンソールを使ってテンプレートを

アップロードし、ソリューションをデプロイします。詳細については、このガイドの「匿名化されたデータ収集」セクションを参照してください。

この自動化 AWS CloudFormation テンプレートは、AWS での自動化されたセキュリティ対応スソリューションを AWS クラウドにデプロイします。スタックを起動する前に Security Hub を有効にして、前提条件を完了しておく必要があります。

> **Note**
>
> このソリューションの実行中に使用した AWS サービスのコストは、お客様の負担となります。詳細は、このガイドの「コスト」セクションに移動して、このソリューションで使用する各 AWS のサービスのウェブ料金ページを参照してください。

1. AWS Security Hub が現在設定されているアカウントから AWS Management Console にサインインし、以下のボタンを使用して `aws-sharr-deploy.template` AWS CloudFormation テンプレートを起動します。

   Launch solution

   実装の開始点としてテンプレートをダウンロードすることもできます。

2. テンプレートはデフォルトで米国東部 (バージニア北部) リージョンで起動します。別の AWS リージョンでソリューションを起動するには、AWS Management Console ナビゲーションバーのリージョンセレクターを使用します。

   > **Note**
   >
   > このソリューションでは、現在特定の AWS リージョンでのみで利用できる AWS Systems Manager を使用します。このソリューションは、このサービスをサポートするすべてのリージョンで機能します。リージョン別の最新の可用性については、「AWS リージョンサービスリスト」を参照してください。

3. [スタックの作成] ページで、正しいテンプレート URL が [Amazon S3 URL] テキストボックスに表示されていることを確認し、[次へ] を選択します。

4. [スタックの詳細を指定] ページで、ソリューションのスタックに名前を割り当てます。名前の文字数制限に関する詳細は、「AWS Identity and Access Management ユーザーガイド」の「IAM および STS の制限」を参照してください。
5. [パラメータ] ページで [次へ] を選択します。

パラメータ	デフォルト	説明
SC 管理者スタックのロード	yes	SC コントロールの自動修復のために管理コンポーネントをインストールするかどうかを指定します。
AFSBP 管理スタックのロード	no	FSBP コントロールの自動修復のために管理コンポーネントをインストールするかどうかを指定します。
CIS120 管理者スタックのロード	no	CIS120 コントロールの自動修復のために管理コンポーネントをインストールするかどうかを指定します。
CIS140 管理者スタックのロード	no	CIS140 コントロールの自動修復のために管理コンポーネントをインストールするかどうかを指定します。
CIS300 管理者スタックのロード	no	CIS300 コントロールの自動修復のために管理コンポーネントをインストールするかどうかを指定します。
PC1321 管理者スタックのロード	no	PC1321 コントロールの自動修復のために管理コンポーネントをインストールするかどうかを指定します。

パラメータ	デフォルト	説明
NIST 管理スタックのロード	no	NIST コントロールの自動修復のために管理コンポーネントをインストールするかどうかを指定します。
オーケストレーターロググループの再利用	no	既存の `SO0111-SHARR-Orchestrator` CloudWatch Logs グループを再利用するかどうかを選択します。これにより、以前のバージョンのログデータを失うことなく、再インストールとアップグレードを簡素化できます。v1.2 以降からアップグレードする場合は、`yes` を選択します。
CloudWatch メトリクスを使用する	`yes`	ソリューションをモニタリングするために CloudWatch メトリクスを有効にするかどうかを指定します。これにより、メトリクスを表示するための CloudWatch ダッシュボードが作成されます。
CloudWatch メトリクスアラームを使用する	`yes`	ソリューションの CloudWatch メトリクスアラームを有効にするかどうかを指定します。これにより、ソリューションによって収集された特定のメトリクスのアラームが作成されます。

パラメータ	デフォルト	説明
RemediationFailure AlarmThreshold	5	コントロール ID あたりの修復失敗の割合のしきい値を指定します。例えば、5 と入力すると、コントロール ID が特定の日に 5% を超える修復に失敗すると、アラームが表示されます。 このパラメータは、アラームが作成された場合にのみ機能します (「CloudWatch メトリクスアラームを使用する」パラメータを参照)。
EnableEnhancedCloudWatchMetrics	no	yes の場合、追加の CloudWatch メトリクスを作成し、CloudWatch ダッシュボードで、CloudWatch アラームとして、すべてのコントロール ID を個別に追跡します。 これに伴う追加コストについては、「コスト」セクションを参照してください。
TicketGenFunctionName	(オプション入力)	オプション。チケット発行システムを統合しない場合は、空白のままにします。それ以外の場合は、ステップ 0 のスタック出力から Lambda 関数名を指定します。例: `SO0111-ASR-ServiceNow-TicketGenerator` 。

6. [スタックオプションの設定] ページで、[次へ] を選択します。
7. [確認] ページで、設定を確認して確定します。テンプレートが AWS Identity and Access Management (IAM) リソースを作成することを確認するボックスにチェックを入れてください。
8. [スタックの作成] を選択してスタックをデプロイします。

AWS CloudFormation コンソールの [Status] (ステータス) 欄でスタックのステータスを表示できます。約 15 分で CREATE_COMPLETE ステータスが表示されます。

ステップ 2: 各 AWS Security Hub メンバーアカウントに修復ロールをインストールする

`aws-sharr-member-roles.template` StackSet は、メンバーアカウントごとに 1 つのリージョンにのみデプロイする必要があります。SHARR オーケストレーターステップ関数からのクロスアカウント API コールを許可するグローバルロールを定義します。

1. 各 AWS Security Hub メンバーアカウント (メンバーでもある管理者アカウントを含む) の AWS マネジメントコンソールにサインインします。ボタンを選択すると、`aws-sharr-member-roles.template` AWS CloudFormation テンプレートが起動します。実装の開始点としてテンプレートをダウンロードすることもできます。

   Launch solution

2. テンプレートはデフォルトで米国東部 (バージニア北部) リージョンで起動します。別の AWS リージョンでソリューションを起動するには、AWS マネジメントコンソールナビゲーションバーのリージョンセレクターを使用します。
3. [スタックの作成] ページで、正しいテンプレート URL が Amazon S3 URL テキストボックスに表示されていることを確認し、[次へ] を選択します。
4. [スタックの詳細を指定] ページで、ソリューションのスタックに名前を割り当てます。名前の文字数制限に関する詳細は、「AWS Identity and Access Management ユーザーガイド」の「IAM および STS の制限」を参照してください。
5. [パラメータ] ページで、以下を入力し、[次へ] を選択します。

パラメータ	デフォルト	説明
名前空間	*<####>*	最大 9 文字の小文字の英数字の文字列を入力します。この文字列は IAM ロール名の一部になります。メンバースタックデプロイとメンバーロールスタックデプロイには同じ値を使用します。
Sec Hub アカウント管理者	*<####>*	AWS Security Hub 管理者アカウントの 12 桁のアカウント ID を入力します。この値は、管理者アカウントのソリューションロールにアクセス許可を付与します。

6. [スタックオプションの設定] ページで、[次へ] を選択します。
7. [確認] ページで、設定を確認して確定します。テンプレートが AWS Identity and Access Management (IAM) リソースを作成することを確認するボックスにチェックを入れてください。
8. [スタックの作成] を選択してスタックをデプロイします。

   AWS CloudFormation コンソールの [Status] (ステータス) 欄でスタックのステータスを表示できます。約 5 分で CREATE_COMPLETE のステータスが表示されます。このスタックのロード中に、次のステップに進むことができます。

ステップ 3: メンバースタックを起動する

> **Important**
>
> このソリューションには、匿名化された運用メトリクスを AWS に送信するオプションが含まれています。このデータを使用して、ユーザーがこのソリューションおよび関連サービスや製品をどのように使用しているかをよりよく理解します。このアンケートで収集されたデータは AWS が所有します。データ収集には、AWS プライバシーポリシーが適用されます。

この機能を無効にするには、テンプレートをダウンロードし、AWS CloudFormation マッピングセクションを変更してから、AWS CloudFormation コンソールを使ってテンプレートをアップロードし、ソリューションをデプロイします。詳細については、このガイドの「運用メトリクスの収集」セクションを参照してください。

`aws-sharr-member` スタックは、各 Security Hub メンバーアカウントにインストールする必要があります。このスタックは、自動修復用のランブックを定義します。各メンバーアカウントの管理者は、このスタックを介して利用可能な修復を制御できます。

1. 各 AWS Security Hub メンバーアカウント (メンバーでもある管理者アカウントを含む) の AWS Management Console にサインインします。ボタンを選択すると、`aws-sharr-member.template` AWS CloudFormation テンプレートが起動します。

   Launch solution

   実装の開始点としてテンプレートをダウンロードすることもできます。
2. テンプレートはデフォルトで米国東部 (バージニア北部) リージョンで起動します。別の AWS リージョンでソリューションを起動するには、AWS Management Console ナビゲーションバーのリージョンセレクターを使用します。

   > **Note**
   >
   > このソリューションでは、AWS Systems Manager を使用します。これは現在、ほとんどの AWS リージョンで利用できます。このソリューションは、これらのサービスをサポートするすべてのリージョンで機能します。リージョン別の最新の可用性については、「AWS リージョンサービスリスト」を参照してください。
3. [スタックの作成] ページで、正しいテンプレート URL が [Amazon S3 URL] テキストボックスに表示されていることを確認し、[次へ] を選択します。
4. [スタックの詳細を指定] ページで、ソリューションのスタックに名前を割り当てます。名前の文字数制限に関する詳細は、「AWS Identity and Access Management ユーザーガイド」の「IAM および STS の制限」を参照してください。
5. [パラメータ] ページで、以下を入力し、[次へ] を選択します。

パラメータ	デフォルト	説明
メトリクスフィルターとアラームの作成に使用する LogGroup の名前を指定する	<####>	CloudTrail が API コールをログに記録する CloudWatch Logs グループの名前を指定します。これは CIS 3.1 ~ 3.14 修復に使用されます。
SC メンバースタックのロード	yes	SC コントロールの自動修復のためにメンバーコンポーネントをインストールするかどうかを指定します。
AFSBP メンバースタックのロード	no	FSBP コントロールの自動修復のためにメンバーコンポーネントをインストールするかどうかを指定します。
CIS120 メンバースタックのロード	no	CIS120 コントロールの自動修復のためにメンバーコンポーネントをインストールするかどうかを指定します。
CIS140 メンバースタックのロード	no	CIS140 コントロールの自動修復のためにメンバーコンポーネントをインストールするかどうかを指定します。
CIS300 メンバースタックのロード	no	CIS300 コントロールの自動修復のためにメンバーコンポーネントをインストールするかどうかを指定します。
PC1321 メンバースタックのロード	no	PC1321 コントロールの自動修復のためにメンバーコンポーネントをインストールするかどうかを指定します。

パラメータ	デフォルト	説明
NIST メンバースタックのロード	no	NIST コントロールの自動修復のためにメンバーコンポーネントをインストールするかどうかを指定します。
Redshift 監査ログ作成用の S3 バケットを作成する	no	FSBP RedShift.4 修復のために S3 バケットを作成する場合は、yes を選択します。S3 バケットと修復の詳細については、「AWS Security Hub ユーザーガイド」の「Redshift.4 修復」を参照してください。
Sec Hub 管理者アカウント	*<####>*	AWS Security Hub 管理者アカウントの 12 桁のアカウント ID を入力します。
名前空間	*<####>*	最大 9 文字の小文字の英数字の文字列を入力します。この文字列は、IAM ロール名とアクションログ S3 バケットの一部になります。メンバースタックデプロイとメンバーロールスタックデプロイには同じ値を使用します。この文字列は、汎用 S3 バケットの Amazon S3 命名規則に従う必要があります。

パラメータ	デフォルト	説明
EnableCloudTrailForASRActionLog	no	CloudWatch ダッシュボードのソリューションによって実施される管理イベントをモニタリングする場合は、yes を選択します。このソリューションは、yes を選択した各メンバーアカウントに CloudTrail 証跡を作成します。これに伴う追加コストについては、「コスト」セクションを参照してください。

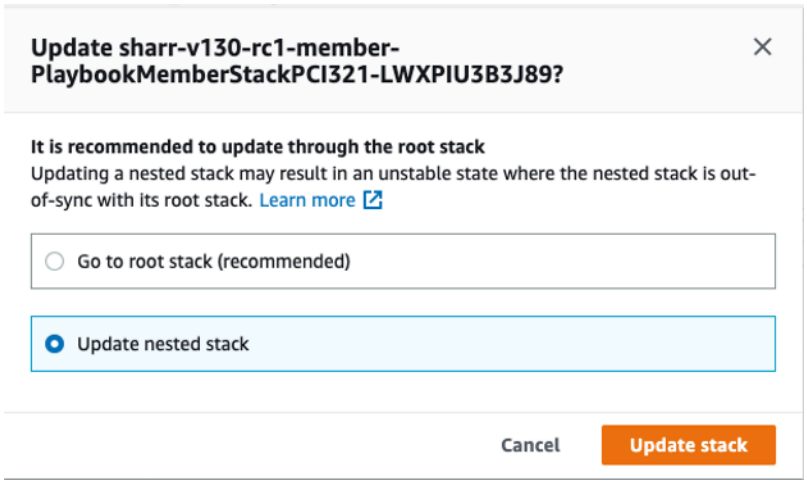
6. [スタックオプションの設定] ページで、[次へ] を選択します。
7. [確認] ページで、設定を確認して確定します。テンプレートが AWS Identity and Access Management (IAM) リソースを作成することを確認するボックスにチェックを入れてください。
8. [スタックの作成] を選択してスタックをデプロイします。

AWS CloudFormation コンソールの [Status] (ステータス) 欄でスタックのステータスを表示できます。約 15 分で CREATE_COMPLETE ステータスが表示されます。

ステップ 4: (オプション) 使用可能な修復を調整する

メンバーアカウントから特定の修復を削除する場合は、セキュリティ標準のネストされたスタックを更新することで削除できます。わかりやすくするために、ネストされたスタックオプションはルートスタックに伝達されません。

1. AWS CloudFormation コンソールにサインインし、ネストされたスタックを選択します。
2. [Update] (更新) を選択します。
3. [ネストされたスタックを更新する] を選択し、[スタックの更新] を選択します。



ネストされたスタックを更新する

4. [現在のテンプレートの使用] を選択し、[次へ] を選択します。
5. 利用可能な修復を調整します。目的のコントロールの値を `Available` に変更し、不要なコントロールを `Not available` に変更します。

> **Note**
>
> 修復を無効にすると、セキュリティ標準とコントロールのソリューション修復ランブックが削除されます。

6. [スタックオプションの設定] ページで、[次へ] を選択します。
7. [確認] ページで、設定を確認して確定します。テンプレートが AWS Identity and Access Management (IAM) リソースを作成することを確認するボックスにチェックを入れてください。
8. [スタックを更新]を選択します。

AWS CloudFormation コンソールの [ステータス] 列でスタックのステータスを表示できます。約 15 分で CREATE_COMPLETE ステータスが表示されます。

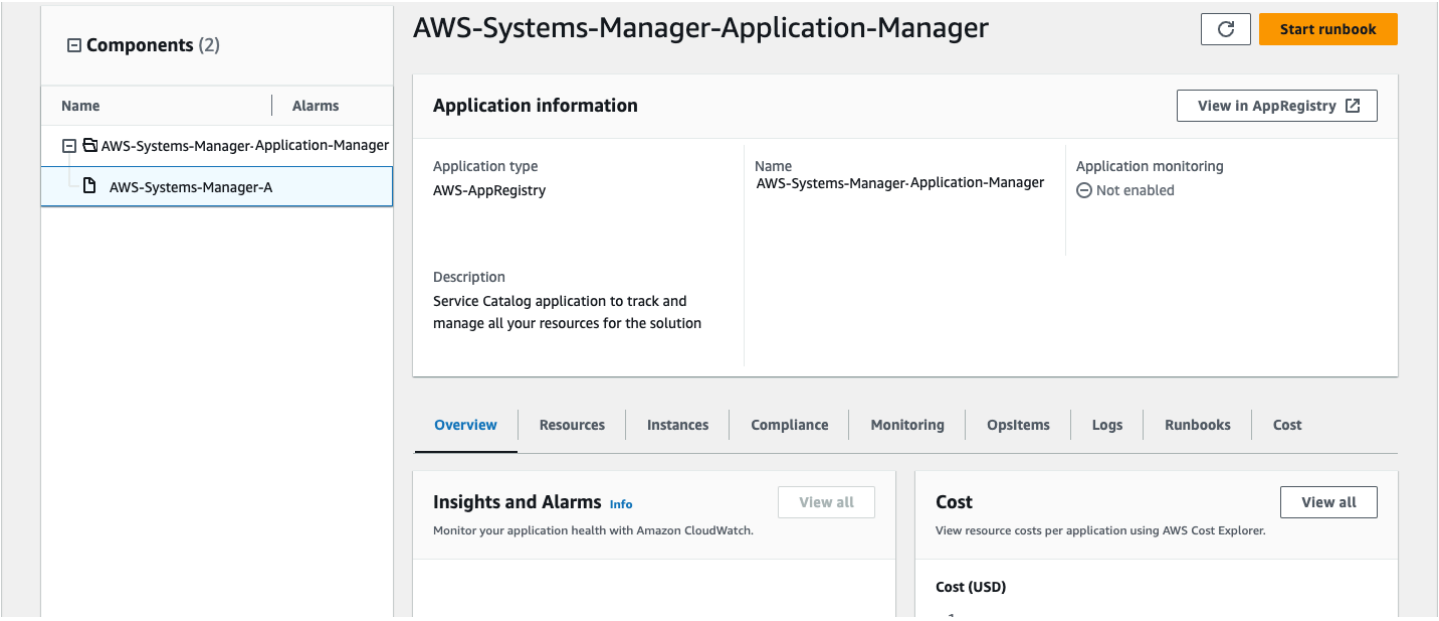
Service Catalog AppRegistry によるソリューションのモニタリング

このソリューションには、Service Catalog AppRegistry および AWS Systems Manager Application Manager の両方でアプリケーションとして、CloudFormation テンプレートと基礎となるリソースを登録するための Service Catalog AppRegistry リソースが含まれています。

AWS Systems Manager Application Manager では、このソリューションとそのリソースをアプリケーションレベルで表示できるため、以下の操作を行うことができます。

- リソース、スタックと AWS アカウント にデプロイされたリソースのコスト、およびソリューションに関連するログを、一元化された場所からモニタリングします。
- アプリケーションのコンテキストで、このソリューションのリソース (デプロイ状況、CloudWatch アラーム、リソース設定、運用上の問題) に関するオペレーションデータを表示します。

  次の図は、Application Manager のソリューションスタックに関するアプリケーションビューの例を示しています。



Application Manager のソリューションスタック

CloudWatch Application Insights を使用する

このソリューションは、デプロイ時に CloudWatch Application Insights と自動的に統合されます。CloudWatch Application Insights は、以下によってソリューションの状態とパフォーマンスを確認および理解するのに役立ちます。

- 主要なアプリケーションリソースを自動的に検出およびモニタリングします。
- 潜在的な問題を事前に特定するためのカスタムアラームを作成します。
- 異常または障害が検出されると、Systems Manager OpsItems を自動的に生成します。これらの OpsItems は、ソリューションに影響する問題を迅速に知らせる実用的な通知として機能します。

CloudWatch Application Insights のモニタリングダッシュボードを表示するには、次のステップに従います。ダッシュボードでは、事前設定されたダッシュボードとアラームを使用して、ソリューションの状態を表示し、主要コンポーネントを表示できます。

1. [CloudWatch console] (CloudWatch のコンソール) に移動する。
2. [Insights] タブを選択し、[Application Insights] を選択します。
3. [アプリケーション] タブを選択し、ソリューションに関連付けられているアプリケーションを選択します。

ソリューションの CloudWatch ダッシュボードをインポートして、ソリューションの状態のモニタリングを統合することもできます。CloudWatch Application Insights のソリューションのアプリケーションダッシュボードで、次のステップに従います。

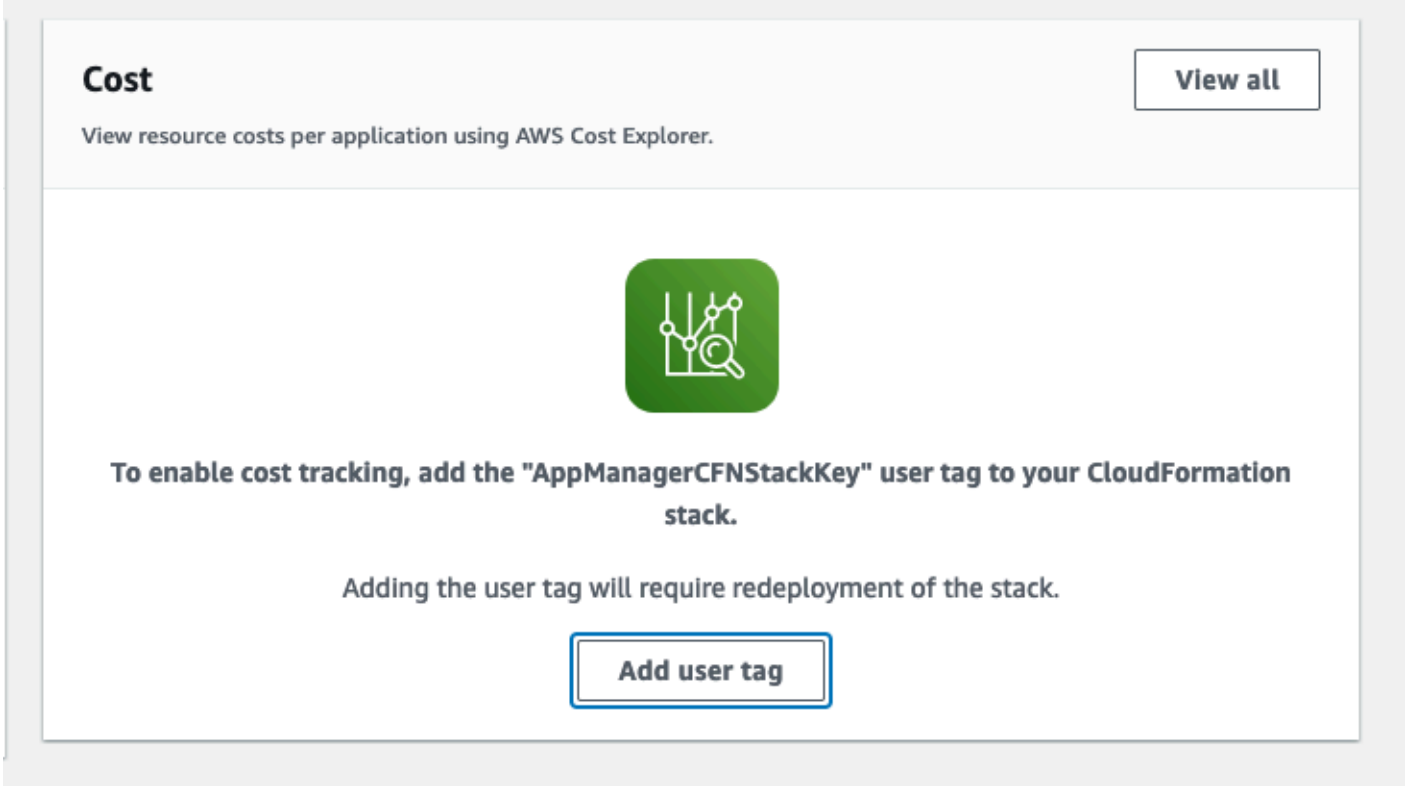
1. [カスタム CloudWatch ダッシュボード] タブを選択します。
2. [CloudWatch ダッシュボードをインポートする] を選択します。
3. 検索ボックスに「`ASR-Remediation-Metrics-Dashboard`」と入力し、AWS ダッシュボードで [自動化されたセキュリティ対応] を選択します。
4. [インポート] を選択します。

これで、CloudWatch Application Insights のダッシュボードとソリューションのカスタムダッシュボードの両方を CloudWatch Application Insights のコンソールで表示でき、ページを切り替える必要はなくなりました。

ソリューションに関連するコストタグを確認する

このソリューションに関連するコスト配分タグをアクティブ化した後、コスト配分タグを確認して、このソリューションのコストをチェックする必要があります。コスト配分タグを確認するには:

1. Systems Manager コンソールにサインインします。
2. [Application Manager] を選択します。
3. [アプリケーション] で、このソリューションのアプリケーション名を検索して選択します。
4. [概要] タブの [コスト] で、[ユーザータグを追加] を選択します。



5. [ユーザータグを追加] ページで、「`confirm`」と入力し、[ユーザータグを追加] を選択します。

アクティベーションプロセスが完了して、タグデータが表示されるまでに最大 24 時間かかることがあります。

ソリューションに関連するコスト配分タグをアクティブ化する

このソリューションに関連するコストタグを確認したら、コスト配分タグをアクティブにして、このソリューションのコストをチェックする必要があります。コスト配分タグは、組織の管理アカウントからのみアクティブ化できます。

コスト配分タグをアクティブ化するには:

1. AWS Billing and Cost Management コンソールにサインインします。
2. ナビゲーションペインで、[コスト配分タグ] を選択します。
3. [コスト配分タグ] ページで、`AppManagerCFNStackKey` タグを使ってフィルターし、表示された結果からタグを選択します。
4. [有効化] を選択します。

AWS Cost Explorer

アプリケーションとそのコンポーネントに関連するコストの概要は、AWS Cost Explorer との統合を通じて、Application Manager コンソール内で確認できます。Cost Explorer では、AWS リソースのコストと使用状況を時系列で表示することで、コストを管理できます。

1. AWS Cost Management コンソールにサインインします。
2. ナビゲーションメニューで [Cost Explorer] を選択し、ソリューションの経時的なコストと使用状況を表示します。

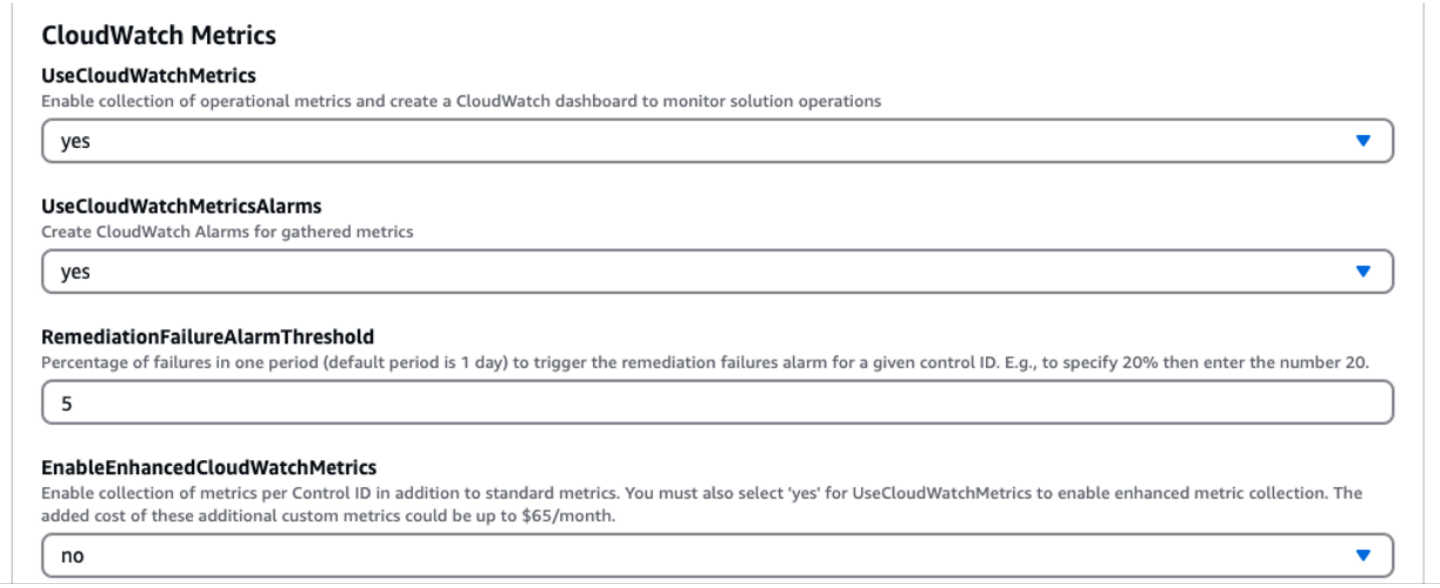
Amazon CloudWatch ダッシュボードでソリューションのオペレーションをモニタリングする

このソリューションには、Amazon CloudWatch ダッシュボードに表示されるカスタムメトリクスとアラームが含まれます。

CloudWatch ダッシュボードとアラームは、ソリューションのオペレーションをモニタリングし、潜在的な問題が発生した場合にアラートを送信します。

CloudWatch メトリクス、アラーム、ダッシュボードの有効化

CloudWatch 機能には 4 つの CloudFormation テンプレートパラメータがあります。



1. UseCloudWatchMetrics – これを yes に設定すると、オペレーションメトリクスの収集が可能になり、これらのメトリクスを表示する CloudWatch ダッシュボードが作成されます。
2. UseCloudWatchAlarms – これを yes に設定すると、ソリューションのデフォルトアラームが有効になります。
3. RemediationFailureAlarmThreshold – アラームを発生させる期間内に失敗した修復の割合。
4. EnableEnhancedCloudWatchMetrics – このパラメータを yes に設定して、コントロール ID ごとに個々のメトリクスを収集します。デフォルトでは、このパラメータは no に設定されているため、すべてのコントロール ID にわたる修復の合計数に関するメトリクスのみが収集されます。コントロール ID ごとの個々のメトリクスとアラームには、追加料金が発生します。

CloudWatch ダッシュボードの使用

ダッシュボードを表示するには:

1. Amazon CloudWatch に移動し、次に [ダッシュボード] に移動します。
2. 「ASR-Remediation-Metrics-Dashboard」という名前のダッシュボードを選択します。

CloudWatch ダッシュボードには、以下がセクションが含まれています。

1. 成功した修復の合計 — ソリューションによって正常に修復された Security Hub の検出結果の数に関するインサイトを提供します。
2. 修復失敗 — 失敗した修復の数を、合計とパーセンテージの両方で示し、失敗の原因を示します。失敗の数が多い場合は、ソリューションに技術的な問題があることを示唆している可能性があり、詳細に調査する必要があります。
3. コントロール ID による修復の成功/失敗 – デプロイ時に拡張メトリクスを有効にした場合、このセクションにはコントロール ID 別の修復結果が一覧表示されます。修復失敗セクションに全体的に高い失敗率が表示されている場合、このセクションには、失敗が多くのコントロール ID に分散されているかどうか、または特定のコントロール ID のみが失敗しているかが表示されます。
4. ランブックロールの引き受けの失敗 – ソリューションメンバーロールがインストールされていないアカウントで修復が試行されたために発生した失敗の数を示します。ロールの不足が原因で自動修復の試行が繰り返し失敗すると、不要なコストが発生します。この問題を軽減するには、関連するアカウントにメンバーロールスタックをインストールするか、ソリューションによって作成されたすべての EventBridge ルールを無効にするか、Security Hub でアカウントの関連付けを解除します。
5. ASR による Cloud Trail 管理アクション – デプロイ時に EnableCloudTrailForASRActionLog パラメータを使用してアクションログを有効にしたすべてのメンバーアカウントのソリューション別の管理アクションを一覧表示します。いずれかの AWS アカウントで予期しないリソースの変更が発生した場合、このウィジェットは、リソースがソリューションによって変更されたかどうかを理解するのに役立ちます。

CloudWatch ダッシュボードには、一般的なオペレーションエラーを警告する事前定義されたアラームも付属しています。

1. 24 時間で 1,000 を超えるステートマシン実行。
   a. 修復実行の急増は、イベントルールが意図したよりも頻繁に開始されていることを示している可能性があります。

b. しきい値は CloudFormation パラメータを使用して変更できます。

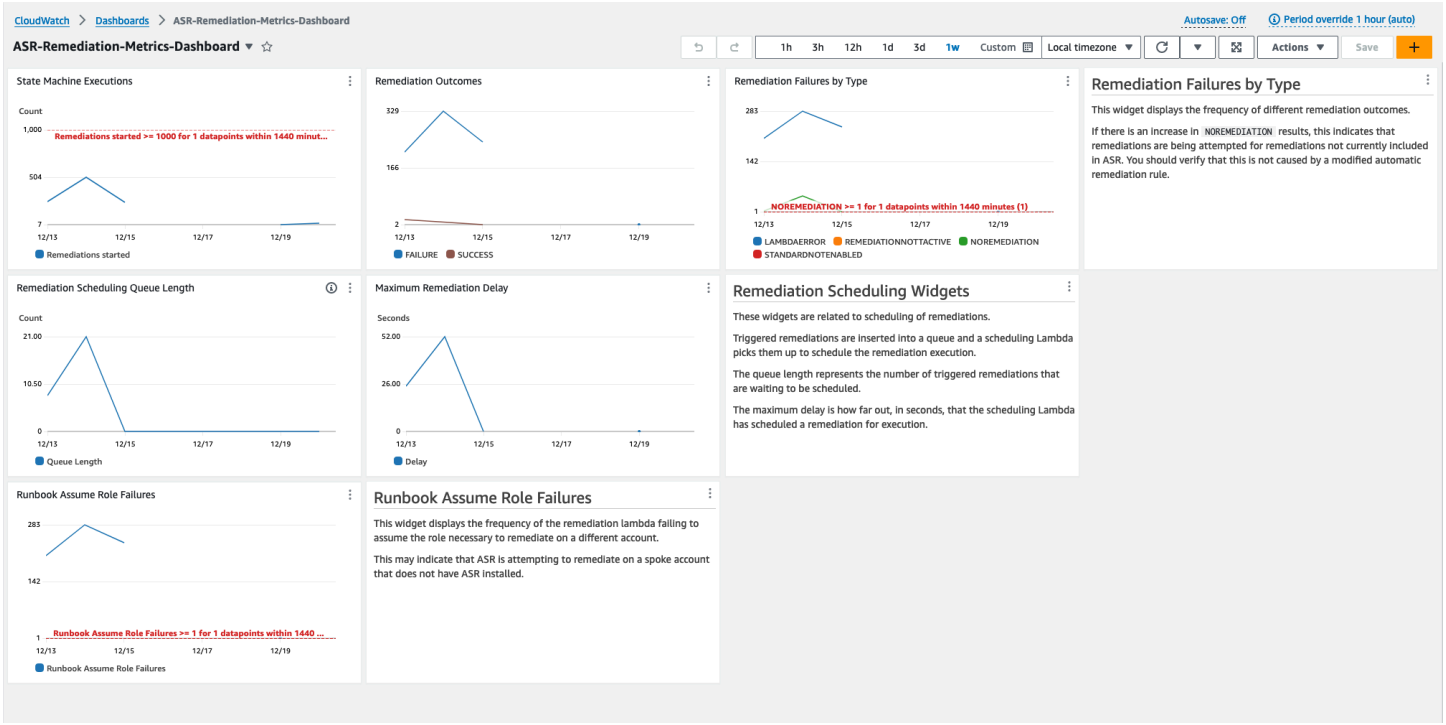
2. タイプ別の修復失敗 = NOREMEDIATION > 0

a. ASR に含まれていない修復に対して修復が試行されています。これは、イベントルールが変更され、意図した以上の修復が含まれていることを示している可能性があります。

3. ランブックロール引き継ぎ失敗数 > 0

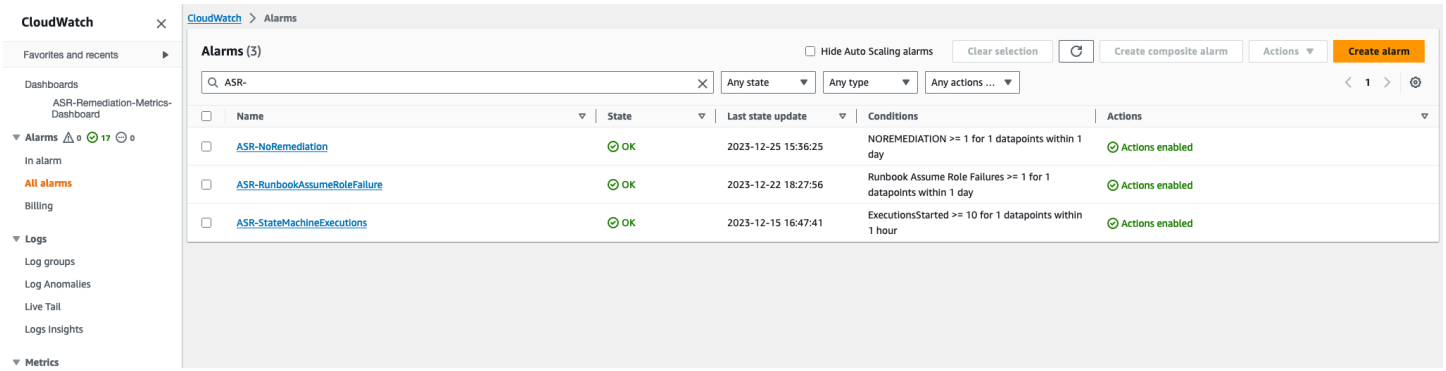
a. ソリューションが適切にデプロイされていないアカウントまたはリージョンに対して修復が試行されています。これは、イベントルールが変更され、意図した以上のアカウントが含まれるようになったことを示している可能性があります。

すべてのアラームしきい値は、個々のデプロイニーズに合わせて変更できます。

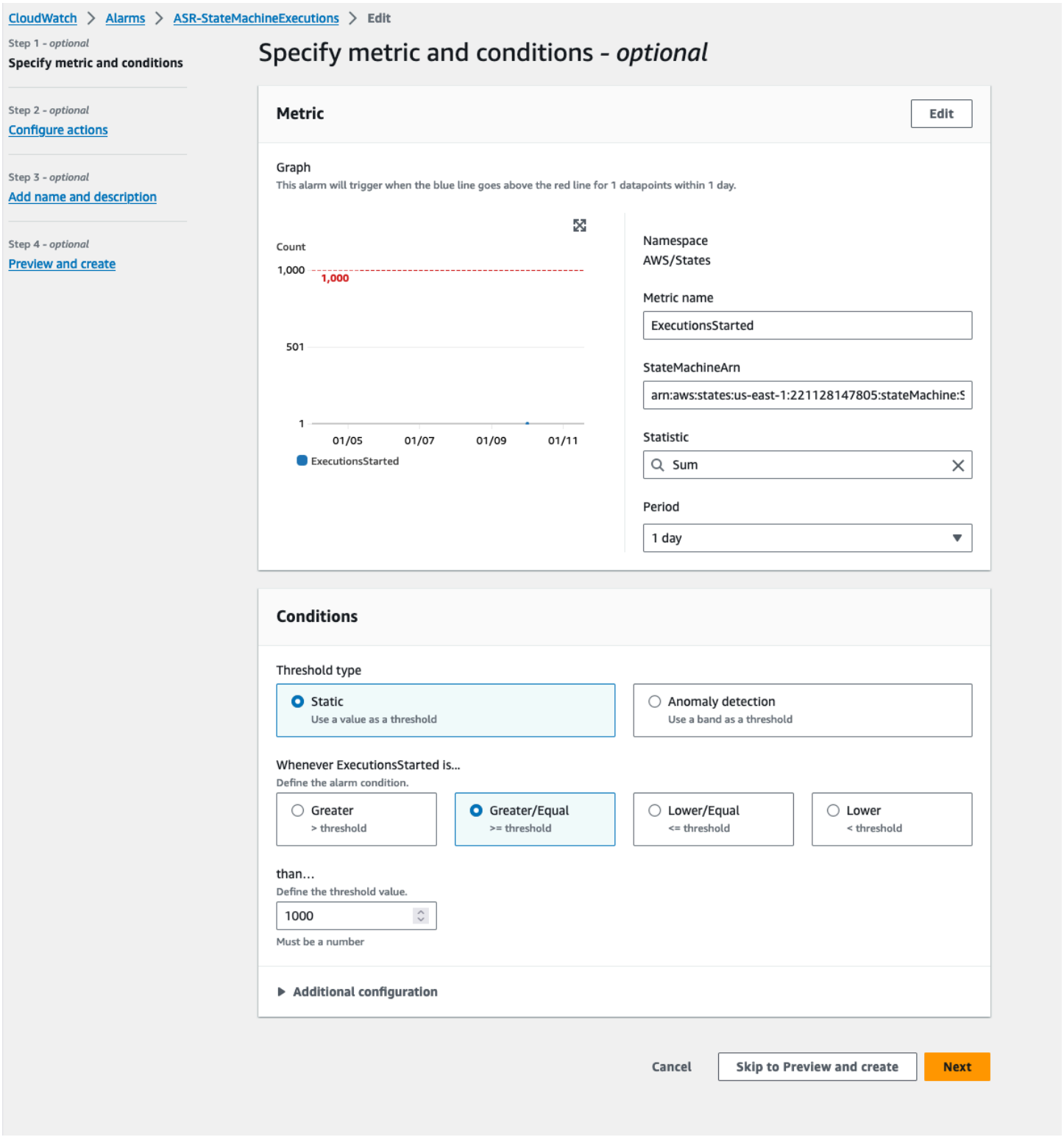


アラームしきい値の変更

1. [Amazon CloudWatch] -> [アラーム] -> [すべてのアラーム] に移動します。
2. 変更するアラームを選択し、[アクション] -> [編集] を選択します。



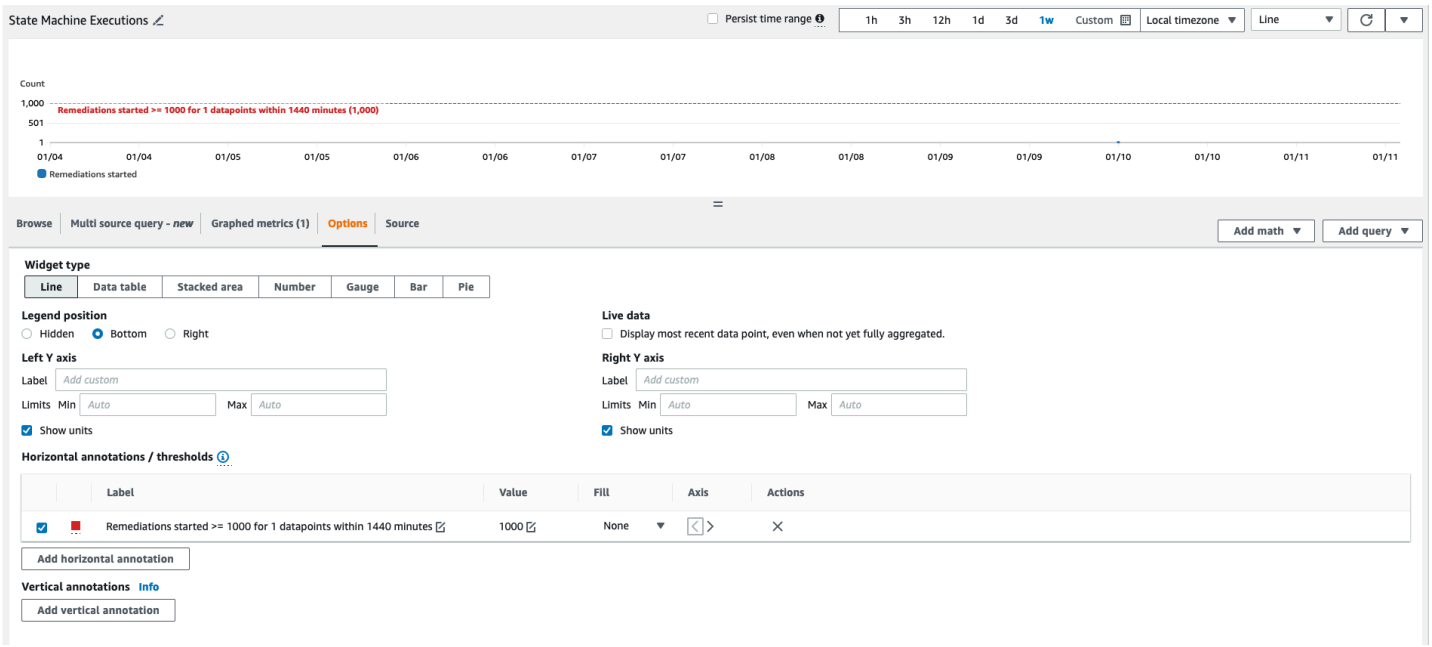
3. しきい値を希望の値に変更して保存します。



4. CloudWatch ダッシュボードに移動して、新しい設定に合わせてチャートを変更します。
   a. 対応するウィジェットの右上にある省略記号を選択します。
   b. [編集] を選択します。

c. [オプション] タブに変更します。

d. 新しい設定に合わせてアラーム注釈を変更します。



アラーム通知にサブスクライブする

管理者アカウントで、管理スタックによって作成された Amazon SNS トピック SO0111-ASR_Alarm_Topic をサブスクライブします。これにより、アラームが ALARM 状態になると通知されます。

ソリューションを更新する

v1.4 より前のバージョンからのアップグレード

以前に v1.4.x より前のソリューションをデプロイしたことがある場合は、アンインストールしてから最新バージョンをインストールします。

1. 以前にデプロイしたソリューションをアンインストールします。「Uninstall the solution」を参照してください。
2. 最新のテンプレートを起動します。「Deploy the solution」を参照してください。

> **Note**
>
> v1.2.1 以前から v1.3.0 以降にアップグレードする場合は、[既存のオーケストレーターロググループを使用する] を No に設定します。v1.3.0 以降を再インストールする場合は、このオプションの Yes を選択できます。このオプションを使用すると、オーケストレーター Step Functions の同じロググループに引き続きログを記録できます。

v1.4 以降からのアップグレード

v1.4.x からアップグレードする場合は、次のようにすべてのスタックまたは StackSets を更新します。

1. 最新のテンプレートを使用して、Security Hub 管理者アカウントのスタックを更新します。
2. 各メンバーアカウントで、最新のテンプレートからアクセス許可を更新します。
3. 現在デプロイされているすべてのリージョンの各メンバーアカウントで、最新のテンプレートからメンバースタックを更新します。

v2.0.x からのアップグレード

v2.0.x からアップグレードする場合は、v2.1.2 以降にアップグレードします。CloudFormation で v2.1.0 - v2.1.1 への更新は失敗します。

トラブルシューティング

既知の問題解決には、既知のエラーを軽減する手順が記載されています。これらの手順で問題が解決しない場合は、「AWS サポートへのお問い合わせ」で、このソリューションの AWS サポートケースの作成手順を確認してください。

ソリューションログ

このセクションには、このソリューションのトラブルシューティング情報が含まれています。トピックの左ナビゲーションを参照してください。

このソリューションは、AWS Systems Manager で実行される修復ランブックから出力を収集し、その結果を AWS Security Hub 管理者アカウントの CloudWatch ロググループ `SO0111-SHARR` に記録します。コントロールごとに 1 日あたり 1 つのストリームがあります。

Orchestrator Step Functions は、AWS Security Hub 管理者アカウントの `SO0111-SHARR-Orchestrator` CloudWatch ロググループへのすべてのステップ移行を記録します。このログは、Step Functions の各インスタンスの状態移行を記録するための監査証跡です。Step Functions の実行ごとに 1 つのログストリームがあります。

両方のロググループは、AWS KMS カスタマー管理キー (CMK) を使用して暗号化されます。

次のトラブルシューティング情報では、`SO0111-SHARR` ロググループを使用します。このログと、AWS Systems Manager Automation コンソール、自動化実行ログ、Step Function コンソール、Lambda ログを使用して、問題のトラブルシューティングを行います。

修復に失敗すると、次のようなメッセージが `SO0111-SHARR` の標準、コントロール、日付のログストリームに記録されます。例: CIS-2.9-2021-08-12

```
ERROR: a4cbb9bb-24cc-492b-a30f-1123b407a6253: Remediation failed for CIS control
 2.9 in account 123412341234: See Automation Execution output for details (AwsEc2Vpc
 vpc-0e92bbe911cf08acb)
```

ここで示しているメッセージで、さらに詳しく学習できます。この出力は、セキュリティ標準とコントロールの SHARR ランブックからのものです。例: SHARR-CIS_1.2.0_2.9

```
Step fails when it is Execution complete: verified. Failed to run automation with
 executionId: eecdef79-9111-4532-921a-e098549f5259 Failed :
```

```
{Status=[Failed], Output=[No output available yet because the step is not successfully
 executed], ExecutionId=[eecdef79-9111-4532-921a-e098549f5259]}. Please refer to
 Automation Service Troubleshooting Guide for more diagnosis details.
```

この情報は、失敗を示します。この場合、メンバーアカウントで実行されている子自動化です。この問題のトラブルシューティングを行うには、メンバーアカウントの AWS Management Console にログインし (上記のメッセージから)、AWS Systems Manager に移動して自動化に移動し、実行 ID `eecdef79-9111-4532-921a-e098549f525` のログ出力を確認する必要があります。

既知の問題解決

- 問題: ソリューションのデプロイが失敗し、リソースが Amazon CloudWatch で既に利用可能であることを示すエラーが表示される。

  解決策: CloudFormation リソース/イベントセクションで、ロググループが既に存在することを示すエラーメッセージを確認します。SHARR デプロイテンプレートを使用すると、既存のロググループを再利用できます。再利用が選択されていることを確認します。

- 問題: EventBridge ルールの作成に失敗するプレイブックのネストされたスタックで、ソリューションがエラーでデプロイされない

  解決策: EventBridge ルールのクォータに達し、プレイブックの数がデプロイされている可能性があります。これを回避するには、Security Hub の統合されたコントロールの検出結果をこのソリューションの SC プレイブックと組み合わせて使用するか、使用する標準用のプレイブックのみをデプロイするか、EventBridge ルールクォータの引き上げをリクエストします。

- 問題: 同じアカウントの複数のリージョンで Security Hub を実行しています。このソリューションを複数のリージョンにデプロイしたいです。

  解決策: Security Hub 管理者と同じアカウントとリージョンに管理者スタックをデプロイします。Security Hub メンバーが設定されている各アカウントとリージョンにメンバーテンプレートをインストールします。Security Hub で集約を有効にします。

- 問題: SO0111-SHARR-Orchestrator を展開した直後に、Get Automation Document State で失敗し、以下の 502 エラーが発生します。「KMSアクセスが拒否されたため、Lambda が環境変数を復号できませんでした 関数の KMS キー設定を確認してください。KMS の例外: UnrecognizedClientExceptionKMS メッセージ: リクエストに含まれるセキュリティトークンが無効です。(サービス: AWSLambda、ステータスコード: 502、エラーコード: KMSAccessDeniedException、リクエスト ID: ...」

解決策: 修復を実行する前に、ソリューションを約 10 分間安定させます。問題が解決しない場合は、サポートチケットまたは GitHub の問題を開きます。

- 問題: 検出結果を修復しようとしましたが、何も起こりませんでした。

  解決策: 検出結果のメモに修復されなかった理由がないか確認してください。一般的な原因は、検出結果に自動修復がないことです。現時点では、メモ以外の修復が存在しない場合に、ユーザーに直接フィードバックを提供する方法はありません。ソリューションログを確認します。コンソールで CloudWatch ログを開きます。SO0111-SHARR CloudWatch ログ グループを検索します。リストをソートして、最近更新されたストリームが最初に表示されるようにします。実行を試みた結果のログストリームを選択します。そこにエラーがあります。失敗の原因には、検出結果のコントロールと修復コントロールの不一致、クロスアカウント修復 (まだサポートされていない)、検出結果が既に修復されていることなどがあります。失敗の理由を特定できない場合は、ログを収集してサポートチケットを開いてください。

- 問題: 修復を開始した後、Security Hub コンソールのステータスが更新されていません。

  解決策: Security Hub コンソールは自動的に更新されません。現在のビューを更新します。結果のステータスが更新されます。検出結果が失敗から成功に移行するまでに数時間かかる場合があります。検出結果は、AWS Config などの他のサービスから AWS Security Hub に送信されたイベントデータから作成されます。ルールが再評価されるまでの時間は、基盤となるサービスによって異なります。それでも問題が解決しない場合は、前述の解決策「検出結果を修復しようとしましたが、何も起こりませんでした」を参照してください。

- 問題: オーケストレーターステップ関数が「Get Automation Document State: AssumeRole オペレーションを呼び出すときにエラー (AccessDenied) が発生しました」で失敗します。

  解決策: SHARR が検出結果の修復を試みているメンバーアカウントにメンバーテンプレートがインストールされていません。メンバーテンプレートのデプロイの手順に従います。

- 問題: レコーダーまたは配信チャネルが既に存在するため、Config.1 ランブックが失敗します。

  解決策: AWS Config 設定を注意深く調べて、Config が正しく設定されていることを確認します。自動修復では、場合によっては既存の AWS Config 設定を修正できません。

- 問題: 修復は成功したが、`"No output available yet because the step is not successfully executed."` メッセージが返される

  解決策: これは、特定の修復ランブックがレスポンスを返さないこのリリースの既知の問題です。修復ランブックは適切に失敗し、機能しない場合にソリューションに通知します。

- 問題: 解決策が失敗し、スタックトレースが送信されました。

解決策: エラー状態を処理する機会を逃し、エラーメッセージではなくスタックトレースにつながることがあります。トレースデータから問題のトラブルシューティングを試みます。サポートが必要な場合は、サポートチケットを開きます。

- 問題: カスタムアクションリソースで v1.3.0 スタックの削除に失敗しました。

  解決策: 管理者テンプレートの削除は、カスタムアクションの削除で失敗することがあります。これは、次のリリースで修正される既知の問題です。これが発生した場合、以下を実行します。

  1. AWS Security Hub マネジメントコンソールにサインインします。
  2. 管理者アカウントで、[設定] に移動します。
  3. [カスタムアクション] タブを選択します。
  4. エントリ Remediate with SHARR を手動で削除します。
  5. スタックを再度削除します。
- 問題: 管理者スタックを再デプロイした後、ステップ関数が `AssumeRole` で失敗しています。

  解決策: 管理者スタックを再デプロイすると、管理者アカウントの管理者ロールとメンバーアカウントのメンバーロールとの間の信頼接続が切断されます。すべてのメンバーアカウントにメンバーロールスタックを再デプロイする必要があります。
- 問題: CIS 3.x の修復が 24 時間以上 `PASSED` を表示しない。

  解決策: これは、メンバーアカウントに `SO0111-SHARR_LocalAlarmNotification` SNS トピックへのサブスクリプションがない場合によく発生します。

特定の修復に関する問題

SetSSLBucketPolicy が AccessDenied エラーで失敗する

関連するコントロール: AWS FSBP v1.0.0 S3.5、PCI v3.2.1 PCI.S3.5、CIS v1.4.0 2.1.2、SC v2.0.0 S3.5

問題: SetSSLBucketPolicy が AccessDenied エラーで失敗します。

PutBucketPolicy オペレーションを呼び出すときにエラー (AccessDenied) が発生しました: アクセスが拒否されました。

バケットに対してパブリックアクセスブロック設定が有効になっている場合、パブリックアクセスを許可するステートメントを含むバケットポリシーの配置を試みると、このエラーで失敗します。この

状態は、このようなステートメントを含むバケットポリシーを配置し、そのバケットのパブリックアクセスブロックを有効にすることで生じます。

ConfigureS3BucketPublicAccessBlock の修復 (関連するコントロール: AWS FSBP v1.0.0 S3.2、PCI v3.2.1 PCI.S3.2、CIS v1.4.0 2.1.5.2、SC v2.0.0 S3.2) は、バケットポリシーを変更せずにパブリックアクセスブロック設定を設定するため、バケットをこの状態にすることもできます。

SetSSLBucketPolicy は、SSL を使用しないリクエストを拒否するステートメントをバケットポリシーに追加します。ポリシー内の他のステートメントは変更されないため、パブリックアクセスを許可するステートメントがある場合、修復は、それらのステートメントがまだ含まれている変更されたバケットポリシーの配置を試み、失敗します。

解決策: バケットポリシーを変更して、バケットのパブリックアクセスブロック設定と競合するパブリックアクセスを許可するステートメントを削除します。

PutS3BucketPolicyDeny が失敗する

関連するコントロール: AWS FSBP v1.0.0 S3.6、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

問題: PutS3BucketPolicyDeny で次のエラーが発生します。

```
Unable to create an explicit deny statement for {bucket_name}.
```

ターゲットバケットのすべてのポリシーのプリンシパルが「*」の場合、ソリューションでは、すべてのプリンシパルのすべてのバケットアクションがブロックされるため、ターゲットバケットに拒否ポリシーを追加できません。

解決策: バケットポリシーを変更して、「*」プリンシパルを使用する代わりに特定のアカウントにアクションを許可し、拒否されたアクションを制限します。

ソリューションを無効にする方法

インシデントが発生した場合、インフラストラクチャを削除せずにソリューションを無効にする必要がある場合があります。これらのシナリオでは、ソリューション内のさまざまなコンポーネントを無効にする方法を詳しく説明します。

シナリオ 1: 1 つのコントロールの自動修復を無効にします。

1. AWS CloudFormation コンソール の EventBridge に移動します。
2. サイドバーで [ルール] を選択します。

3. デフォルトのイベントバスを選択し、無効にするコントロールを検索します。
4. ルールを選択し、[無効にする] ボタンを選択します。

シナリオ 2: すべてのコントロールの自動修復を無効にする。

1. コンソール の EventBridge に移動します。
2. サイドバーで [ルール] を選択します。
3. 「デフォルト」イベントバスを選択し、以下のすべてのルールを選択します。
4. 「無効にする」ボタンを選択します。ルールの複数のページでこれを行う必要がある場合があります。

シナリオ 3: アカウントの手動修復を無効にする

1. コンソール の EventBridge に移動します。
2. サイドバーで [ルール] を選択します。
3. 「デフォルト」イベントバスを選択し、「Remediate_with_SHARR_CustomAction」を検索します。
4. ルールを選択し、「無効にする」ボタンを選択します。

AWS Supportに問い合わせる

AWS デベロッパーサポート、AWS ビジネスサポート、または AWS エンタープライズサポートをご利用の場合は、サポートセンターを利用して、このソリューションに関する工キスパートのサポートを受けることができます。次のセクションで、その方法を説明します。

ケースの作成

1. サポートセンターにサインインします。
2. [ケースを作成] を選択します。

どのようなサポートをご希望ですか?

1. [技術] を選択します。

2. サービスで、[ソリューション] を選択します。
3. [カテゴリ] で、[その他のソリューション] を選択します。
4. 重要度で、ユースケースに最も適したオプションを選択します。
5. サービス、カテゴリ、重要度を入力すると、インターフェースに一般的なトラブルシューティングの質問へのリンクが表示されます。これらのリンクを使用しても問題を解決できない場合は、[次のステップ: 追加情報] を選択します。

追加情報

1. 件名に、質問または問題を要約したテキストを入力します。
2. 説明に、問題の詳細を入力します。
3. [ファイルを添付] を選択します。
4. AWS Support がリクエストを処理するために必要な情報を添付します。

ケースの迅速な解決にご協力ください

1. 必要な情報を記入します。
2. [次のステップ: 今すぐ解決またはお問い合わせ] を選択します。

今すぐ解決またはお問い合わせ

1. 今すぐ解決の解決策を確認します。
2. これらの解決策で問題を解決できない場合は、[お問い合わせ] を選択し、必要な情報を入力して [送信] を選択します。

ソリューションをアンインストールする

次の手順に従って、AWS Management Console を使用してソリューションをアンインストールします。

V1.0.0-V1.2.1

リリース v1.0.0 から v1.2.1 の場合は、Service Catalog を使用して CIS および/または FSBP プレイブックをアンインストールします。v1.3.0 では、Service Catalog は使用されなくなりました。

1. AWS CloudFormation コンソールにサインインし、Security Hub のプライマリアカウントに移動します。
2. [Service Catalog] を選択して、プロビジョニングされたプレイブックを終了し、セキュリティグループ、ロール、またはユーザーを削除します。
3. Security Hub メンバーアカウントからスポーク `CISPermissions.template` テンプレートを削除します。
4. Security Hub 管理者アカウントとメンバーアカウントからスポーク `AFSBPMemberStack.template` テンプレートを削除します。
5. Security Hub のプライマリアカウントに移動し、ソリューションのインストールスタックを選択し、[削除] を選択します。

> **Note**
>
> CloudWatch Logs のグループログは保持されます。これらのログは、組織のログ保持ポリシーの必要に応じて保持することをお勧めします。

V1.3.x

1. 各メンバーアカウントから `aws-sharr-member.template` を削除します。
2. 管理者アカウントから `aws-sharr-admin.template` を削除します。

> **Note**
>
> v1.3.0 で管理者テンプレートを削除すると、カスタムアクションの削除に失敗する可能性があります。これは、次のリリースで修正される既知の問題です。この問題を修正するには、以下の手順に従います。
>
> 1. AWS Security Hub マネジメントコンソールにサインインします。
> 2. 管理者アカウントで、[設定] に移動します。
> 3. [カスタムアクション] タブを選択します。
> 4. エントリ Remediate with SHARR を手動で削除します。
> 5. スタックを再度削除します。

V1.4.0 以降

スタックのデプロイ

1. 各メンバーアカウントから `aws-sharr-member.template` を削除します。
2. 管理者アカウントから `aws-sharr-admin.template` を削除します。

StackSet デプロイ

StackSet ごとにスタックを削除し、デプロイの逆の順序で StackSet を削除します。

テンプレートが削除された場合でも、`aws-sharr-member-roles.template` の IAM ロールは保持されることに注意してください。これは、これらのロールを使用した修復が引き続き機能するようにするためです。これらの SO0111-* ロールは、CloudTrail から CloudWatch へのログ記録や RDS 拡張モニタリングなどのアクティブな修復で使用されなくなったことを確認した後に、手動で削除できます。

管理者ガイド

ソリューションの一部の有効化と無効化

ソリューション管理者は、ソリューションのどの機能を有効にするかについて、次の制御を行うことができます。

メンバースタックとメンバーロールスタックがデプロイされる場所:

- 管理者スタックは、メンバーおよびメンバーロールスタックがパラメータ値として指定された管理者アカウント番号でデプロイされているアカウントでのみ (カスタムアクションまたは完全に自動化された EventBridge ルールを使用して)、修復を開始できます。
- アカウントまたはリージョンをソリューションの制御から完全に除外するには、メンバースタックまたはメンバーロールスタックをそれらのアカウントまたはリージョンにデプロイしないでください。

Security Hub でのアカウントとリージョンの検出結果の集約設定:

- 管理者スタックは、管理者アカウントとリージョンに到着した検出結果に対してのみ (カスタムアクションまたは完全に自動化された EventBridge ルールを使用して) 修復を開始できます。
- アカウントまたはリージョンをソリューションの制御から完全に除外するには、それらのアカウントまたはリージョンを、管理スタックがデプロイされているのと同じ管理者アカウントとリージョンに検出結果を送信する対象に含めないでください。

どの標準ネストスタックがデプロイされるか:

- 管理スタックは、ターゲットメンバーアカウントとリージョンにコントロールランブックがデプロイされているコントロールに対してのみ (カスタムアクションまたは完全に自動化された EventBridge ルールを使用して) 修復を開始できます。これらは、各標準のメンバースタックによってデプロイされます。
- 管理スタックは、その標準の管理スタックによってルールがデプロイされているコントロールに対してのみ、EventBridge ルールを使用して完全に自動化された修復を開始できます。これらは管理者アカウントにデプロイされます。
- 分かりやすいように、管理者アカウントとメンバーアカウント間で標準を一貫してデプロイすることをお勧めします。AWS FSBP と CIS v1.2.0 を優先する場合は、これら 2 つのネストされた管理

者スタックを管理者アカウントにデプロイし、これら 2 つのネストされたメンバースタックを各メンバーアカウントとリージョンにデプロイします。

ネストされた各メンバースタックにどのコントロールランブックがデプロイされるか:

- 管理スタックは、各標準のメンバースタックによってターゲットメンバーアカウントとリージョンにコントロールランブックがデプロイされているコントロールに対してのみ (カスタムアクションまたは完全に自動化された EventBridge ルールを使用して) 修復を開始できます。
- 特定の標準に対してコントロールが有効になっているかをよりきめ細かく制御するために、標準の各ネストされたスタックには、コントロールランブックをデプロイするためのパラメータがあります。コントロールのパラメータを「使用不可」の値に設定して、そのコントロールランブックのデプロイを解除します。

標準を有効または無効にするための SSM パラメータ:

- 管理スタックは、標準管理スタックによってデプロイされた SSM パラメータを介して有効になっている標準に対してのみ (カスタムアクションまたは完全に自動化された EventBridge ルールを使用して) 修復を開始できます。
- 標準を無効にするには、パスが「/Solutions/SO0111/<standard_name>/<standard_version>/status」の SSM パラメータの値を「いいえ」に設定します。

SNS 通知の例

修復が開始されたとき


```
{
  "severity": "INFO",
  "message": "00000000-0000-0000-0000-000000000000: Remediation queued for SC control
 RDS.13 in account 111111111111",
  "finding": {
    "finding_id": "22222222-2222-2222-2222-222222222222",
    "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
    "standard_name": "security-control",
    "standard_version": "2.0.0",
    "standard_control": "RDS.13",
    "title": "RDS automatic minor version upgrades should be enabled",
```

```
    "region": "us-east-1",
    "account": "111111111111",
    "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
  }
}
```

修復が成功した場合

```
{
  "severity": "INFO",
  "message": "00000000-0000-0000-0000-000000000000: Remediation succeeded for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
  "finding": {
    "finding_id": "22222222-2222-2222-2222-222222222222",
    "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
    "standard_name": "security-control",
    "standard_version": "2.0.0",
    "standard_control": "RDS.13",
    "title": "RDS automatic minor version upgrades should be enabled",
    "region": "us-east-1",
    "account": "111111111111",
    "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
  }
}
```

修復が失敗した場合

```
{
  "severity": "ERROR",
  "message": "00000000-0000-0000-0000-000000000000: Remediation failed for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
  "finding": {
    "finding_id": "22222222-2222-2222-2222-222222222222",
```

```
    "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
    "standard_name": "security-control",
    "standard_version": "2.0.0",
    "standard_control": "RDS.13",
    "title": "RDS automatic minor version upgrades should be enabled",
    "region": "us-east-1",
    "account": "111111111111",
    "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
  }
}
```

ソリューションを使用する

これは、ASR の最初のデプロイについて説明するチュートリアルです。ソリューションのデプロイの前提条件から始まり、メンバーアカウントでの検出結果例の修復で終了します。

チュートリアル: AWS での自動化されたセキュリティ対応の開始方法

これは、最初のデプロイについて説明するするチュートリアルです。ソリューションのデプロイの前提条件から始まり、メンバーアカウントでの検出結果例の修復で終了します。

アカウントを準備する

ソリューションのクロスアカウントおよびクロスリージョン修復機能をデモンストレーションするために、このチュートリアルでは 2 つのアカウントを使用します。ソリューションを 1 つのアカウントにデプロイすることもできます。

次の例では、アカウント 111111111111 とアカウント 222222222222 を使用してソリューションをデモンストレーションします。111111111111 は管理者アカウント、222222222222 はメンバーアカウントです。リージョン us-east-1 および us-west-2 のリソースに関する検出結果を修正するソリューションをセットアップします。

以下の表は、各アカウントとリージョンの各ステップで実行するアクションを示す例です。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	[なし]	[なし]
222222222222	メンバー	[なし]	[なし]

管理者アカウントは、ソリューションの管理アクションを実行するアカウントであり、つまり、修復を手動で開始したり、EventBridge ルールを使用して完全自動修復を有効にしたりします。このアカウントは、検出結果を修正するすべてのアカウントの Security Hub 委任管理者アカウントでもある必要がありますが、アカウントが属する AWS Organizations の AWS Organizations 管理者アカウントである必要はありません。

AWS Config の有効化

次のドキュメントを確認してください。

- AWS Config ドキュメント
- AWS Config の料金
- AWS Config の有効化

両方のアカウントとリージョンで AWS Config を有効にします。これには料金が発生します。

> **Important**
>
> 「グローバルリソース (AWS IAM リソースなど) を含める」オプションを必ず選択してください。AWS Config を有効にするときにこのオプションを選択しないと、グローバルリソース (AWS IAM リソースなど) に関連する検出結果は表示されません。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	AWS Config の有効化	AWS Config の有効化
222222222222	メンバー	AWS Config の有効化	AWS Config の有効化

AWS Security Hub を有効にする

次のドキュメントを確認してください。

- AWS Security Hub ドキュメント
- AWS Security Hub の料金
- AWS Security Hub の有効化

両方のアカウントとリージョンで AWS Security Hub を有効にします。これには料金が発生します。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	AWS Security Hub を有効にする	AWS Security Hub を有効にする
222222222222	メンバー	AWS Security Hub を有効にする	AWS Security Hub を有効にする

統合されたコントロールの検出結果を有効にする

次のドキュメントを確認してください。

- コントロールの検出結果を生成および更新する

このチュートリアルでは、推奨される設定である AWS Security Hub の統合コントロール検出結果機能を有効にした状態で、ソリューションの使用方法を示します。執筆時点でこの機能をサポートしていないパーティションでは、SC (セキュリティコントロール) ではなく、標準固有のプレイブックをデプロイする必要があります。

両方のアカウントとリージョンで統合コントロール検出結果を有効にします。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	統合されたコントロールの検出結果を有効にする	統合されたコントロールの検出結果を有効にする
222222222222	メンバー	統合されたコントロールの検出結果を有効にする	統合されたコントロールの検出結果を有効にする

新機能で検出結果が生成されるまでに時間がかかる場合があります。チュートリアルを進むことはできますが、新機能なしで生成された検出結果を修正することはできません。新機能で生成された検

出結果は、GeneratorId フィールド値 security-control/<control_id> によって識別できます。

クロスリージョン検出結果の集約を設定する

次のドキュメントを確認してください。

- クロスリージョン集約
- クロスリージョン集約を有効にする

両方のアカウントで us-west-2 から us-east-1 への検出結果の集約を設定します。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	us-west-2 からの集約を設定する	[なし]
222222222222	メンバー	us-west-2 からの集約を設定する	[なし]

検出結果が集約リージョンに反映されるまでに時間がかかる場合があります。チュートリアルを進むことはできますが、集約リージョンに表示され始めるまでは、他のリージョンの検出結果を修正することはできません。

Security Hub 管理者アカウントを指定する

次のドキュメントを確認してください。

- AWS Security Hub でのアカウントの管理
- 組織メンバーアカウントの管理
- 招待によるメンバーアカウントの管理

前述の例では、手動の招待方法を使用します。一連の本番稼働用アカウントについては、AWS Organizations を通じて Security Hub の委任管理者を管理することをお勧めします。

管理者アカウント (111111111111) の AWS Security Hub コンソールから、メンバーアカウント (222222222222) を招待し、管理者アカウントを Security Hub 委任管理者として受け入れます。メンバーアカウントから招待を受け入れます。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	メンバーアカウントを招待する	[なし]
222222222222	メンバー	招待を受け入れる	[なし]

検出結果が管理者アカウントに反映されるまでに時間がかかる場合があります。チュートリアルを進むことはできますが、メンバーアカウントからの検出結果が管理者アカウントに表示され始めるまでは修正できません。

セルフマネージド型の StackSets アクセス許可のロールを作成する

次のドキュメントを確認してください。

- 「AWS CloudFormation StackSets」
- セルフマネージド型のアクセス許可を付与する

CloudFormation スタックを複数のアカウントにデプロイするため、StackSets を使用します。管理スタックとメンバースタックには、サービスでサポートされていないネストされたスタックがあるため、サービス管理型のアクセス許可は使用できません。そのため、セルフマネージド型のアクセス許可を使用する必要があります。

StackSet オペレーションの基本的なアクセス許可のためにスタックをデプロイします。本番稼働用アカウントの場合は、「高度なアクセス許可オプション」ドキュメントに従ってアクセス許可を絞り込むことができます。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	StackSet 管理者ロールスタックをデプロイする StackSet 実行ロールスタックをデプロイする	[なし]
222222222222	メンバー	StackSet 実行ロールスタックをデプロイする	[なし]

検出結果の例を生成する安全でないリソースを作成する

次のドキュメントを確認してください。

- Security Hub コントロールのリファレンス
- AWS Lambda コントロール

次のリソース例では、修復をデモンストレーションするために安全でない設定を使用しています。コントロール例は Lambda.1 です。Lambda 関数ポリシーでは、パブリックアクセスを禁止する必要があります。

> **Important**
>
> 安全でない設定のリソースを意図的に作成します。コントロールの性質を確認し、環境でそのようなリソースを作成するリスクを評価してください。組織がこのようなリソースを検出して報告するために備えているツールに注意し、必要に応じて例外をリクエストしてください。選択したコントロールの例が不適切な場合は、ソリューションがサポートする別のコントロールを選択します。

メンバーアカウントの 2 番目のリージョンで、AWS Lambda コンソールに移動し、最新の Python ランタイムで関数を作成します。[設定] > [アクセス許可] で、認証なしで URL から関数を呼び出すことを許可するポリシーステートメントを追加します。

コンソールページで、関数がパブリックアクセスを許可していることを確認します。ソリューションがこの問題を修正したら、アクセス許可を比較して、パブリックアクセスが取り消されたことを確認します。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	[なし]	[なし]
222222222222	メンバー	[なし]	安全でない設定で Lambda 関数を作成する

AWS Config が安全でない設定を検出するまでに時間がかかる場合があります。チュートリアルを進むことはできますが、Config が検出するまで検出結果を修正することはできません。

関連するコントロールの CloudWatch ロググループを作成する

次のドキュメントを確認してください。

- Monitoring CloudTrail Log Files with Amazon CloudWatch Logs
- CloudTrail コントロール

ソリューションでサポートされているさまざまな CloudTrail コントロールには、マルチリージョン CloudTrail の送信先である CloudWatch ロググループが必要です。次の例では、プレースホルダーロググループを作成します。本番稼働用アカウントでは、CloudWatch Logs との CloudTrail 統合を適切に設定する必要があります。

各アカウントとリージョンに同じ名前のロググループ (例: `asr-log-group`) を作成します。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	ロググループの作成	ロググループの作成
222222222222	メンバー	ロググループの作成	ロググループの作成

ソリューションをチュートリアルアカウントにデプロイする

管理者、メンバー、およびメンバーロールスタックの 3 つの Amazon S3 URL を収集します。

管理者スタックをデプロイする

View template

aws-sharr-deploy.template

管理者アカウントで、CloudFormation コンソールに移動し、管理者スタックを Security Hub の検出結果集約リージョンにデプロイします。

「SC」または「Security Control」スタックを除く、ネストされた管理者スタックをロードするためのすべてのパラメータの値として [No] を選択します。このスタックには、アカウントで設定した統合されたコントロールの検出結果のリソースが含まれています。

以前にこのソリューションをこのアカウントとリージョンにデプロイしていない限り、オーケストレーターロググループを再利用する場合は [No] を選択します。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	管理者スタックをデプロイする	[なし]
222222222222	メンバー	[なし]	[なし]

管理者スタックがデプロイを完了するまで待ってから続行し、メンバーアカウントから管理者アカウントへの信頼関係を作成できるようにします。

メンバースタックをデプロイする

View template

aws-sharr-member.template

管理者アカウントで、CloudFormation StackSets コンソールに移動し、メンバースタックを各アカウントとリージョンにデプロイします。このチュートリアルで作成した StackSets 管理者ロールと実行ロールを使用します。

作成したロググループの名前をロググループ名のパラメータの値として入力します。

「SC」または「セキュリティコントロール」スタックを除く、ネストされたメンバースタックをロードするためのすべてのパラメータの値として [No] を選択します。このスタックには、アカウントで設定した統合されたコントロールの検出結果のリソースが含まれています。

管理者アカウント番号のパラメータの値として、管理者アカウントの ID を入力します。この例では、111111111111 となります。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	メンバー StackSet をデプロイする/メンバースタックがデプロイされたことを確認する	メンバースタックがデプロイされたことを確認する
222222222222	メンバー	メンバースタックがデプロイされたことを確認する	メンバースタックがデプロイされたことを確認する

メンバーロールスタックをデプロイする

View template

aws-sharr-member-roles.template

管理者アカウントで、CloudFormation StackSets コンソールに移動し、メンバースタックを各アカウントにデプロイします。このチュートリアルで作成した StackSets 管理者ロールと実行ロールを使用します。管理者アカウント番号のパラメータの値として、管理者アカウントの ID を入力します。この例では、111111111111 となります。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	メンバー StackSet をデプロイする/メンバースタックがデプロイされたことを確認する	[なし]
222222222222	メンバー	メンバースタックがデプロイされたことを確認する	[なし]

続行することはできますが、CloudFormation StackSets がデプロイを完了するまで検出結果を修正することはできません。

SNS トピックをサブスクライブする

修復の更新

トピック - SO0111-SHARR_Topic

管理者アカウントで、管理者スタックによって作成された Amazon SNS トピックをサブスクライブします。これにより、修復が開始されたとき、および成功または失敗したときに通知されます。

アラーム

トピック - SO0111-ASR_Alarm_Topic

管理者アカウントで、管理者スタックによって作成された Amazon SNS トピックをサブスクライブします。これにより、メトリクスアラームが開始されたときに通知されます。

検出結果の例を修正する

管理者アカウントで、Security Hub コンソールに移動し、このチュートリアルの一部として作成した安全でない設定のリソースの検出結果を見つけます。

これには、いくつかの方法があります。

1. 統合されたコントロールの検出結果機能をサポートするパーティションでは、[コントロール] とラベル付けされたページで、統合されたコントロール ID によって検出結果を見つけることができます。
2. [セキュリティ標準] ページで、どの標準に属するかによってコントロールを見つけることができます。
3. すべての検出結果を [検出結果] ページで表示し、属性で検索できます。

作成したパブリック Lambda 関数の統合されたコントロールの ID は Lambda.1 です。

修復を開始する

作成したリソースに関連する検出結果の左側にあるチェックボックスをオンにします。[アクション] ドロップダウンメニューで、[Remediate with ASR] を選択します。検出結果が Amazon EventBridge に送信されたという通知が表示されます。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	修復を開始する	[なし]
222222222222	メンバー	[なし]	[なし]

修復によって検出結果が解決されたことを確認する

2 つの SNS 通知を受信します。1 つ目は修復が開始されたことを示し、2 つ目は修復が成功したことを示します。2 つ目の通知を受け取ったら、メンバーアカウントの Lambda コンソールに移動し、パブリックアクセスが取り消されたことを確認します。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	[なし]	[なし]
222222222222	メンバー	[なし]	修復が成功したことを確認する

修復の実行をトレースする

ソリューションの仕組みを理解するために、修復の実行をトレースできます。

EventBridge ルール

管理者アカウントで、Remediate_with_SHARR_CustomAction という名前の EventBridge ルールを見つけます。このルールは、Security Hub から送信した検出結果と一致し、オーケストレーター Step Functions に送信します。

Step Functions の実行

管理者アカウントで、SO0111-SHARR-Orchestrator という名前の AWS Step Functions を見つけます。このステップ関数は、ターゲットアカウントとリージョンの SSM Automation ドキュメントを呼び出します。この AWS Step Functions の実行履歴で修復の実行をトレースできます。

SSM Automation

メンバーアカウントで、SSM Automation コンソールに移動します。「ASR-SC_2.0.0_Lambda.1」という名前のドキュメントの実行が 2 つと「ASR-RemoveLambdaPublicAccess」という名前のドキュメントの実行が 1 つあります。

最初の実行は、ターゲットアカウントのオーケストレーターステップ関数からのものです。2 つ目の実行はターゲットリージョンで発生しますが、検出結果の発生元のリージョンではない場合があります。最終の実行は、Lambda 関数からパブリックアクセスポリシーを取り消す修復です。

CloudWatch ロググループ

管理者アカウントで、CloudWatch ログコンソールに移動し、SO0111-SHARR という名前のロググループを見つけます。このロググループは、オーケストレーター Step Functions からの高レベルログの送信先です。

完全に自動化された修復を有効にする

ソリューションのもう 1 つのオペレーションモードは、Security Hub に検出結果が届くたびにを自動的に修復を行うことです。

この検出結果が誤って適用される可能性のあるリソースがないことを確認する

自動修復を有効にすると、有効にしたコントロール (Lambda.1) に一致するすべてのリソースで修復が開始されます。

> **Important**
>
> ソリューションのスコープ内のすべてのパブリック Lambda 関数で、このアクセス許可を取り消されることを確認します。完全に自動化された修復は、作成した関数に範囲が限定されません。このソリューションは、インストールされているアカウントとリージョンのいずれかで検出された場合、このコントロールを修正します。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	必要なパブリック関数がないことを確認する	必要なパブリック関数がないことを確認する
222222222222	メンバー	必要なパブリック関数がないことを確認する	必要なパブリック関数がないことを確認する

ルールを有効にする

管理者アカウントで、SC_2.0.0_Lambda.1_AutoTrigger という名前の EventBridge ルールを見つけて有効にします。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	自動修復ルールを有効にする	[なし]
222222222222	メンバー	[なし]	[なし]

リソースの設定

メンバーアカウントで、パブリックアクセスを許可するように Lambda 関数を再設定します。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	[なし]	[なし]
222222222222	メンバー	[なし]	パブリックアクセスを許可するように Lambda 関数を設定する

修復によって検出結果が解決されたことを確認する

Config が安全でない設定を再度検出するまでに時間がかかる場合があります。2 つの SNS 通知を受信します。1 つ目は、修復が開始されたことを示します。2 つ目は、修復が成功したことを示します。2 つ目の通知を受け取ったら、メンバーアカウントの Lambda コンソールに移動し、パブリックアクセスが取り消されたことを確認します。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	自動修復ルールを有効にする	[なし]

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
222222222222	メンバー	[なし]	修復が成功したことを確認する

クリーンアップ

サンプルリソースを削除する

メンバーアカウントで、作成したサンプル Lambda 関数を削除します。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	[なし]	[なし]
222222222222	メンバー	[なし]	サンプル Lambda 関数を削除する

管理者スタックを削除する

管理者アカウントで、管理者スタックを削除します。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	管理者スタックを削除する	[なし]
222222222222	メンバー	[なし]	[なし]

メンバースタックを削除する

管理者アカウントで、メンバー StackSet を削除します。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	メンバー StackSet を削除する メンバースタックが削除されたことを確認する	メンバースタックが削除されたことを確認する
222222222222	メンバー	メンバースタックが削除されたことを確認する	メンバースタックが削除されたことを確認する

メンバーロールスタックを削除する

管理者アカウントで、メンバーロール StackSet を削除します。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	メンバーロール StackSet を削除する メンバーロールスタックが削除されたことを確認する	[なし]
222222222222	メンバー	メンバーロールスタックが削除されたことを確認する	[なし]

保持されたロールを削除する

各アカウントで、保持されている IAM ロールを削除します。

重要: これらのロールは、ロールを必要とする修復が機能し続けるために保持されます (例: VPC フローログ記録)。削除する前に、これらのロールの継続的な機能が必要でないことを確認してください。

SO0111- というプレフィックスが付いたロールをすべて削除します。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	保持されたロールを削除する	[なし]
222222222222	メンバー	保持されたロールを削除する	[なし]

保持された KMS キーの削除をスケジュールする

管理者スタックとメンバースタックは、どちらも KMS キーを作成して保持します。これらのキーを保持すると、料金が発生します。

これらのキーは、ソリューションによって暗号化されたリソースにアクセスできるようにするために保持されます。削除をスケジュールする前に、それらが必要でないことを確認してください。

ソリューションによって作成された、または CloudFormation 履歴からの工イリアスを使用して、ソリューションによってデプロイされたキーを特定します。それらを削除するようスケジュールします。

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	管理者キーを特定して削除をスケジュールする メンバーキーを特定して削除をスケジュールする	メンバーキーを特定して削除をスケジュールする

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
222222222222	メンバー	メンバーキーを特定して削除をスケジュールする	メンバーキーを特定して削除をスケジュールする

セルフマネージド型の StackSets アクセス許可のスタックを削除する

セルフマネージド型の StackSets アクセス許可を許可するために作成されたスタックを削除する

アカウント	目的	us-east-1 でのアクション	us-west-2 でのアクション
111111111111	管理	StackSet 管理者ロールスタックを削除する	[なし]
222222222222	メンバー	StackSet 実行ロールスタックを削除する	[なし]

開発者ガイド

このセクションでは、このソリューションのソースコードと追加のカスタマイズについて説明します。

ソースコード

GitHub リポジトリでは、このソリューションのテンプレートとスクリプトをダウンロードし、カスタマイズ内容を他のユーザーと共有できます。

プレイブック

このソリューションには、Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v3.0.0、AWS Foundational Security Best Practices (FSBP) v.1.0.0、Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1、および National Institute of Standards and Technology (NIST) の一部として定義されたセキュリティ標準のプレイブック修復が含まれています。

統合されたコントロールの検出結果を有効にしている場合、それらの統制はすべての標準でサポートされています。この機能が有効になっている場合は、SC プレイブックのみをデプロイする必要があります。そうでない場合、プレイブックは前述の標準でサポートされています。

> **Important**
>
> サービスクォータに達しないように、有効な標準のプレイブックのみをデプロイします。

特定の修復の詳細については、アカウントのソリューションによってデプロイされた名前の Systems Manager オートメーションドキュメントを参照してください。AWS Systems Manager コンソールに移動し、ナビゲーションペインで [ドキュメント] を選択します。

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
合計修復	63	34	29	33	65	19	90

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableAutoScalingGroupELBHealthCheck ロードバランサーに関連付けられた Auto Scaling グループは、ロードバランサーのヘルスチェックを使用する必要があります。	Autoscaling.1		Autoscaling.1		Autoscaling.1		Autoscaling.1

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-CreateMultiRegionTrail CloudTrail を有効にし、少なくとも 1 つのマルチリージョンの証跡で設定する必要があります。	CloudTrail.1	2.1	CloudTrail.2	3.1	CloudTrail.1	3.1	CloudTrail.1
ASR-EnableEncryption CloudTrail は保管時の暗号化を有効にする必要があります。	CloudTrail.2	2.7	CloudTrail.1	37	CloudTrail.2	3.5	CloudTrail.2

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableLogFileValidation CloudTrail のログファイル検証が有効であることを確認します。	CloudTrail.4	2.2	CloudTrail.3	3.2	CloudTrail.4		CloudTrail.4
ASR-EnableCloudTrailToCloudWatchLogging CloudTrail 追跡が Amazon CloudWatch Logs と統合されていることを確認します。	CloudTrail.5	2.4	CloudTrail.4	3.4	CloudTrail.5		CloudTrail.5

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-ConfigureS3BucketLogging S3 バケットアクセスログ記録が CloudTrail S3 バケットで有効になっていることを確認します		2.6		3.6		3.4	CloudTrail.7

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-ReplaceCodeBuildClearTextCredentials CodeBuild プロジェクト環境変数に、クリアテキストの認証情報を含めるべきでない	CodeBuild.2		CodeBuild.2		CodeBuild.2		CodeBuild.2
ASR-EnableAWSConfig AWS Config が有効になっていることを確認します。	Config.1	2.5	Config.1	3.5	Config.1	3.3	Config.1

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-MakeEBSSnapshotsPrivate Amazon EBS スナップショットはパブリックに復元できないようにすることをお勧めします。	EC2.1		EC2.1		EC2.1		EC2.1

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-RemoveVPCDefaultSecurityGroupRules VPC のデフォルトのセキュリティグループで、インバウンドトラフィックとアウトバウンドトラフィックを禁止する必要があります。	EC2.2	4.3	EC2.2	5.3	EC2.2	5.4	EC2.2

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableVPCFlowLogs すべての VPC で VPC フローログ記録を有効にする必要があります	EC2.6	2.9	EC2.6	3.9	EC2.6	37	EC2.6
ASR-EnableEbsEncryptionByDefault EBS のデフォルト暗号化を有効にする必要があります。	EC2.7	2.2.1			EC2.7	2.2.1	EC2.7

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-RevokeUnrotatedKeys ユーザーのアクセスキーは 90 日以内ごとに更新する必要があります。	IAM.3	1.4		1.14	IAM.3	1.14	IAM.3
ASR-SetIAMPasswordPolicy IAM のデフォルトのパスワードポリシー	IAM.7	1.5 ~ 1.11	IAM.8	1.8	IAM.7	1.8	IAM.7

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-RevokeUnusedIAMUserCredentials 90 日以内に使用しない場合は、ユーザー認証情報をオフにする必要があります。	IAM.8	1.3	IAM.7		IAM.8		IAM.8

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-RevokeUnusedIAMUserCredentials 45 日以内に使用しない場合は、ユーザー認証情報をオフにする必要があります。				1.12		1.12	IAM.22
ASR-RemoveLambdaPublicAccess Lambda 関数では、パブリックアクセスを禁止する必要があります。	Lambda.1		Lambda.1		Lambda.1		Lambda.1

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-MakeRDSSnapshotPrivate RDS スナップショットでパブリックアクセスを禁止する必要があります。	RDS.1		RDS.1		RDS.1		RDS.1
ASR-DisablePublicAccessToRDSInstance RDS DB インスタンスでパブリックアクセスを禁止する必要があります。	RDS.2		RDS.2		RDS.2	2.3.3	RDS.2

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EncryptRDSSnapshot RDS クラスターのスナップショットとデータベースのスナップショットは保管中に暗号化する必要があります	RDS.4				RDS.4		RDS.4

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableMultiAZOnRDSInstance RDS DB インスタンスは、複数のアベイラビリティーゾーンで設定する必要があります	RDS.5				RDS.5		RDS.5

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableEnhancedMonitoringOnRDSInstance RDS DB インスタンスとクラスターの拡張モニタリングを設定する必要があります。	RDS.6				RDS.6		RDS.6

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableRDSClusterDeletionProtection RDS クラスターでは、削除保護が有効になっている必要があります。	RDS.7				RDS.7		RDS.7

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableRDSInstanceDeletionProtection RDS DB インスタンスで、削除保護が有効になっている必要があります。	RDS.8				RDS.8		RDS.8

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableMinorVersionUpgradeOnRDSDBInstance RDS 自動マイナーバージョンアップグレードを有効にする必要があります。	RDS.13				RDS.13	2.3.2	RDS.13

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableCopyTagsToSnapshotOnRDSCluster タグをスナップショットにコピーするように RDS DB クラスターを設定する必要があります	RDS.16				RDS.16		RDS.16

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-DisablePublicAccessToRedshiftCluster Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります	Redshift.1		Redshift.1		Redshift.1		Redshift.1

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableAutomaticSnapshotsOnRedshiftCluster Amazon Redshift クラスターでは、自動スナップショットが有効になっている必要があります。	Redshift.3				Redshift.3		Redshift.3

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableRedshiftClusterAuditLogging Amazon Redshift クラスターでは、監査ログ記録が有効になっている必要があります。	Redshift.4				Redshift.4		Redshift.4

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableAutomaticVersionUpgradeOnRedshiftCluster Amazon Redshift でメジャーバージョンへの自動アップグレードが有効になっている必要があります。	Redshift.6				Redshift.6		Redshift.6

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-ConfigureS3PublicAccessBlock S3 ブロックパブリックアクセス設定を有効にする必要があります。	S3.1	2.3	S3.6	2.1.5.1	S3.1	2.1.4	S3.1
ASR-ConfigureS3BucketPublicAccessBlock S3 バケットではパブリック読み取りアクセスを禁止する必要があります	S3.2		S3.2	2.1.5.2	S3.2		S3.2

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-ConfigureS3BucketPublicAccessBlock S3 バケットはパブリック書き込みアクセスを禁止する必要があります		S3.3					S3.3
ASR-EnableDefaultEncryptionS3 S3 バケットでは、サーバー側の暗号化を有効にする必要があります。	S3.4		S3.4	2.1.1	S3.4		S3.4

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-SetSSLBucketPolicy S3 バケットではリクエストに SSL を使用する必要があります。	S3.5		S3.5	2.1.2	S3.5	2.1.1	S3.5
ASR-S3BlockDenylist バケットポリシー内で別の AWS アカウントに付与された Amazon S3 許可は制限する必要があります。	S3.6				S3.6		S3.6

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
S3 ブロックパブリックアクセス設定は、バケットレベルで有効にする必要があります。	S3.8				S3.8		S3.8
ASR-ConfigureS3BucketPublicAccessBlock S3 バケット CloudTrail ログが一般に公開されていないことを確認します。		2.3					CloudTrail.6

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-CreateAccessLoggingBucket S3 バケットアクセスログ記録が CloudTrail S3 バケットで有効になっていることを確認します。		2.6					CloudTrail.7

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableKeyRotation カスタマー作成の CMK のローテーションが有効になっていることを確認します。		2.8	KMS.1	3.8	KMS.4	3.6	KMS.4

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-CreateLogMetricFilterAndAlarm 不正な API コールに対するログメトリクスフィルターとアラームが存在することを確認する		3.1		4.1			Cloudwatch.1

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-CreateLogMetricFilterAndAlarm MFA なしの AWS Management Console サインインに対するログメトリクスフィルターとアラームが存在することを確認する		3.2		4.2			Cloudwatch.2

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-CreateLogMetricFilterAndAlarm 「ルート」ユーザーに使用するログメトリクスフィルターとアラームが存在することを確認します。		3.3	CW.1	4.3			Cloudwatch.3

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-CreateLogMetricFilterAndAlarm MFA なしの IAM ポリシーの変更に対してログメトリクスフィルターとアラームが存在することを確認します。		3.4		4.4			Cloudwatch.4

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-CreateLogMetricFilterAndAlarm CloudTrail の設定の変更に対するログメトリクスフィルターとアラームが存在することを確認します。		3.5		4.5			Cloudwatch.5

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-CreateLogMetricFilterAndAlarm AWS Management Console 認証の失敗に対してログメトリックフィルターとアラームが存在することを確認する		3.6		4.6			Cloudwatch.6

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-CreateLogMetricFilterAndAlarm カスタマー作成の CMK の無効化またはスケジュールされた削除に対してログメトリクスフィルターとアラームが存在することを確認します		37		4.7			Cloudwatch.7

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-CreateLogMetricFilterAndAlarm S3 バケットの変更に対してログメトリクスフィルターとアラームが存在することを確認します		3.8		4.8			Cloudwatch.8

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-CreateLogMetricFilterAndAlarm AWS Config 設定の変更に対してログメトリックフィルターとアラームが存在することを確認する		3.9		4.9			Cloudwatch.9

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-CreateLogMetricFilterAndAlarm セキュリティグループの変更に対するメトリクスフィルターとアラームが存在することを確認します		3.10		4.10			Cloudwatch.10

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-CreateLogMetricFilterAndAlarm ネットワークアクセスコントロールリスト (NACL) への変更に対するログメトリクスとアラームが存在することを確認します		3.11		4.11			Cloudwatch.11

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-CreateLogMetricFilterAndAlarm ネットワークゲートウェイへの変更に対するログメトリクスとアラームが存在することを確認します		3.12		4.12			Cloudwatch.12

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-CreateLogMetricFilterAndAlarm ルートテーブルの変更に対してログメトリクスフィルターとアラームが存在することを確認します		3.13		4.13			Cloudwatch.13

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-CreateLogMetricFilterAndAlarm VPC の変更に対してログメトリクスフィルターとアラームが存在することを確認します		3.14		4.14			Cloudwatch.14

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
AWS-DisablePublicAccessForSecurityGroup どのセキュリティグループでも 0.0.0.0/0 からポート 22 への入力を許可していないことを確認する		4.1	EC2.5		EC2.13		EC2.13

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
AWS-DisablePublicAccessForSecurityGroup どのセキュリティグループでも 0.0.0.0/0 からポート 3389 への入力を許可しないことを確認する		4.2			EC2.14		EC2.14
ASR-ConfigureSNSTopicForStack	CloudFormation.1				CloudFormation.1		CloudFormation.1
ASR-CreateIAMSupportRole		1.20		1.17		1.17	IAM.18

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-DisablePublicIPAutoAssign Amazon EC2 サブネットは、パブリック IP アドレスを自動的に割り当てないことをお勧めします	EC2.15				EC2.15		EC2.15
ASR-EnableCloudTrailLogFileValidation	CloudTrail.4	2.2	CloudTrail.3	3.2			CloudTrail.4
ASR-EnableEncryptionForSNSTopic	SNS.1				SNS.1		SNS.1

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableDeliveryStatusLoggingForSNSTopic トピックに送信される通知メッセージでは、配信ステータスのログ記録を有効にする必要があります	SNS.2				SNS.2		SNS.2
ASR-EnableEncryptionForSQSQueue	SQS.1				SQS.1		SQS.1

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-MakeRDSSnapshotPrivate RDS スナップショットはプライベートである必要があります	RDS.1		RDS.1				RDS.1
ASR-BlockSSMDocumentPublicAccess SSM ドキュメントはパブリックにしないでください。	SSM.4				SSM.4		SSM.4

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableCloudFrontDefaultRootObject CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります	CloudFront.1				CloudFront.1		CloudFront.1

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-SetCloudFrontOriginDomain CloudFront ディストリビューションは、存在しない S3 オリジンをポイントしない必要があります。	CloudFront.12				CloudFront.12		CloudFront.12

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-RemoveCodeBuildPrivilegedMode CodeBuild プロジェクト環境には ログ記録の AWS Config 設定が必要です。	CodeBuild.5				CodeBuild.5		CodeBuild.5
ASR-TerminateEC2Instance 停止した EC2 インスタンスは、指定した期間後に削除する必要があります	EC2.4				EC2.4		EC2.4

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnablelMDSV2OInstance EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用する必要があります	EC2.8				EC2.8	5.6	EC2.8

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-RevokeUnauthorizedInboundRules セキュリティグループは、許可されたポートに対して無制限の着信トラフィックのみを許可する必要があります。	EC2.18				EC2.18		EC2.18

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-DisableUnrestrictedToHighRiskPorts セキュリティグループは、リスクの高いポートへの無制限アクセスを許可しないでください	EC2.19				EC2.19		EC2.19

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-DisableTGWAutoAcceptSharedAttachments Amazon EC2 Transit Gateway は VPC アタッチメントリクエストを自動的に受け付けないようにする必要があります。	EC2.23				EC2.23		EC2.23

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableEPrivateRepositoryScanning ECR プライベートリポジトリでは、イメージスキャニングが設定されている必要があります	ECR.1				ECR.1		ECR.1
ASR-EnableGuardDuty GuardDuty を有効にする必要があります	GuardDuty.1		GuardDuty.1		GuardDuty.1		GuardDuty.1

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-ConfigureS3BucketLogging S3 バケットサーバーアクセスログ記録を有効にする必要があります	S3.9				S3.9		S3.9
ASR-EnableBucketEventNotifications S3 バケットでは、イベント通知を有効にする必要があります	S3.11				S3.11		S3.11

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-SetS3LifecyclePolicy S3 バケットでは、ライフサイクルポリシーを設定する必要があります	S3.13				S3.13		S3.13
ASR-EnableAutoSecretRotation Secrets Manager のシークレットは、自動ローテーションを有効にする必要があります	SecretsManager.1				SecretsManager.1		SecretsManager.1

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-RemoveUnusedSecret 未使用の Secrets Manager のシークレットを削除します	SecretsManager.3				SecretsManager.3		SecretsManager.3
ASR-UpdateSecretRotationPeriod Secrets Manager のシークレットは、指定された日数以内にローテーションする必要があります	SecretsManager.4				SecretsManager.4		SecretsManager.4

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableAPIGatewayCacheDataEncryption API Gateway REST API のキャッシュデータは、保管中に暗号化する必要があります					APIGateway.5		APIGateway.5

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-SetLogGroupRetentionDays CloudWatch ロググループは指定された期間保持する必要があります					CloudWatch.16		CloudWatch.16

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-AttachServiceVPCEndpoint Amazon EC2 サービス用に作成された VPC エンドポイントを使用するように Amazon EC2 を設定する必要があります	EC2.10				EC2.10		EC2.10

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-TagGuardDutyResource GuardDuty フィルターにはタグを付ける必要があります							GuardDuty.2
ASR-TagGuardDutyResource GuardDuty ディテクターにはタグを付ける必要があります							GuardDuty.4

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-AttachSSMPermissionsToEC2 Amazon EC2 インスタンスは Systems Manager によって管理される必要があります。	SSM.1		SSM.3				SSM.1

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-ConfigureLaunchConfigNoPublicIPDocument Auto Scaling グループの起動設定を使用して起動した Amazon EC2 インスタンスは、パブリック IP アドレスを含みません。					Autoscaling.5		Autoscaling.5
ASR-EnableAPIGatewayExecutionLogs	APIGateway.1						APIGateway.1

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	セキュリティコントロール ID
ASR-EnableMacie Amazon Macie を有効にする必要があります	Macie.1				Macie.1		Macie.1
ASR-EnableAthenaWorkGroupLogging Athena ワークグループではログ記録が有効になっている必要があります	Athena.4						Athena.4

新しい修復の追加

既存のプレイブックに新しい修復を追加する場合、ソリューション自体を変更する必要はありません。

> **Note**
>
> 以降の手順では、ソリューションによってインストールされたリソースを開始点として活用します。慣例により、ほとんどのソリューションリソース名には SHARR や SO0111 が含まれており、簡単に見つけて識別できます。

概要

AWS での自動化されたセキュリティ対応ランブックは、次の標準命名に従う必要があります。

ASR-*<standard>*-*<version>*-*<control>*

標準: セキュリティ標準の略語。これは SHARR でサポートされている標準と一致する必要があります。「CIS」、「AFSBP」、「PCI」、「NIST」、または「SC」のいずれかである必要があります。

バージョン: 標準のバージョン。繰り返しになりますが、これは SHARR でサポートされているバージョンと検出結果データ内のバージョンと一致する必要があります。

コントロール: 修復するコントロールのコントロール ID。これは検出結果データと一致する必要があります。

1. メンバーアカウント (複数可) にランブックを作成します。
2. メンバーアカウント (複数可) に IAM ロールを作成します。
3. (オプション) 管理者アカウントに自動修復ルールを作成します。

ステップ 1. メンバーアカウント (複数可) にランブックを作成する

1. AWS Systems Manager コンソールにサインインし、検出結果 JSON の例を取得します。
2. 検出結果を修復するオートメーションランブックを作成します。[自分が所有] タブで、[ドキュメント] タブの ASR- ドキュメントのいずれかを開始点として使用します。
3. 管理者アカウントの AWS Step Functions がランブックを実行します。ランブックを呼び出すときに渡すには、ランブックで修復ロールを指定する必要があります。

ステップ 2. メンバーアカウント (複数可) に IAM ロールを作成する

1. AWS Identity and Access Management コンソール にサインインします。
2. IAM SO0111 ロールから例を取得し、新しいロールを作成します。ロール名は「`SO0111-Remediate-<standard>-<version>-<control>`」で始まる必要があります。例えば、CIS v1.2.0 コントロール 5.6 を追加する場合、ロールは `SO0111-Remediate-CIS-1.2.0-5.6` である必要があります。
3. この例を使用して、修復の実行に必要な API コールのみを許可する、適切なスコープのロールを作成します。

この時点で、修復はアクティブになり、AWS Security Hub の SHARR カスタムアクションから自動修復が可能になります。

ステップ 3: (オプション) 管理者アカウントに自動修復ルールを作成する

自動 (「自動化」ではない) 修復は、AWS Security Hub が検出結果を受け取った時点での修復の即時実行です。このオプションを使用する前に、リスクを慎重に検討してください。

1. CloudWatch Events で同じセキュリティ標準のルール例を表示します。ルールの命名基準は `standard_control_**AutoTrigger**` です。
2. 使用する例からイベントパターンをコピーします。
3. 検出結果 JSON の `GeneratorId` と一致するように `GeneratorId` の値を変更します。
4. ルールを保存してアクティブ化します。

新しいプレイブックの追加

AWS での自動化されたセキュリティ対応ソリューションプレイブックとデプロイソースコードを GitHub リポジトリからダウンロードします。

AWS CloudFormation リソースは AWS CDK コンポーネントから作成され、リソースには新しいプレイブックの作成と設定に使用できるプレイブックテンプレートコードが含まれています。プロジェクトのセットアップとプレイブックのカスタマイズの詳細については、GitHub の「README.md」ファイルを参照してください。

AWS Systems Manager Parameter Store

AWS での自動化されたセキュリティ対応は、AWS Systems Manager Parameter Store を使用して運用データを保存します。以下のパラメータは Parameter Store に保存されます。

名前	値	使用アイテム
/Solutions/SO0111/CMK_REMEDIATION_ARN	FSBP 修復のデータを暗号化する AWS KMS キー	修復の一環としての CloudTrail ログなどの顧客データの暗号化
/Solutions/SO0111/CMK_ARN	SHARR がデータの暗号化に使用する AWS KMS キー	ソリューションデータの暗号化
/Solutions/SO0111/SNS_Topic_ARN	ソリューションの Amazon SNS トピックの ARN	修復イベントの通知
/Solutions/SO0111/SNS_Topic_Config.1	AWS Config 更新の SNS トピック	Config.1 修復
/Solutions/SO0111/sendAnonymousMetrics	Yes	匿名化されたメトリクスの収集
/Solutions/SO0111/version	ソリューションバージョン	
/Solutions/SO0111/*<security standard long name>*/*<version>*/status	enabled	ソリューションで標準がアクティブかどうかを示します。これを disabled に変更することで、自動修復のために標準を無効にすることができます。
/Solutions/SO0111/*<security standard long name>*/shortname	String	セキュリティ標準の短縮名。例:「CIS」、「AFSBP」、「PCI」

名前	値	使用アイテム
/Solutions/SO0111/ <security standard long name>/<version> /<control> /remap	String	あるコントロールが別のコントロールと同じ修復を使用する場合、これらのパラメータは再マッピングを実行します。

Amazon SNS トピック - 修復の進行状況

AWS での自動化されたセキュリティ対応は、Amazon SNS トピック SO0111-SHARR_Topic を作成します。このトピックは、修復の進行状況に関する更新を投稿するために使用されます。このトピックに送信される可能性のある 3 つの通知を次に示します。

```
Remediation queued for <standard> control <control_ID> in account <account_ID>
```

```
Remediation failed for <standard> control <control_ID> in account <account_ID>
```

```
<control_ID> remediation was successfully invoke via AWS Systems Manager in
 account <account_ID>
```

これは完了メッセージです。これは、修復がエラーなしで完了したことを示します。ただし、修復が成功するための最終的なテストは、AWS Config チェックおよび/または手動検証です。

SNS トピックサブスクリプションのフィルタリング

Amazon SNS サブスクリプションフィルターポリシー:

1. SNS トピックのサブスクリプションに移動します。
2. サブスクリプションフィルターポリシーで、「編集」を選択します。
3. 「サブスクリプションフィルターポリシー」を展開し、「サブスクリプションフィルターポリシー」オプションを切り替えてフィルターを有効にします。
4. 「メッセージ本文」スコープを選択します。
5. JSON エディタにポリシーを追加します。
6. 変更の保存。

ポリシーの例:

アカウントでフィルタリングする

```
{
    "finding": {
      "account": [
        "111111111111",
        "222222222222"
      ]
    }
```

エラーでフィルタリングする

```
{
    "severity": ["ERROR"]
    }
```

コントロールでフィルタリングする

```
{
    "finding": {
       "standard_control": ["S3.9","S3.6"]
      }
   }
```

Amazon SNS トピック – CloudWatch アラーム

このソリューションでは、Amazon SNS トピック、SO0111-ASR_Alarm_Topic を作成します。このトピックは、アラームアラートを投稿するために使用されます。

ALARM 状態に入るアラームの詳細は、このトピックに送信されます。

Config 検出結果でランブックを開始する

このソリューションは、カスタム AWS Config の検出結果に基づいてランブックを開始できます。これを行うには、以下を行う必要があります。

1. 修復する AWS Config ルール名を見つけます。これは、AWS Config または Security Hub がこのルールに対して生成する検出結果のいずれかにあります。
2. AWS Systems Manager Parameter Store に移動し、パラメータの作成を選択します。
3. ルールの名前は `/Solutions/SO0111/Rule name from Step 1` である必要があります。
4. 値は次のようにフォーマットする必要があります。

```
{

"RunbookName":"Name of SSM runbook",

"RunbookRole": "Role that Orchestrator will assume"

}
```

5. RunbookName は必須フィールドであり、この Config ルールを修復するときに実行されるランブックになります。RunbookRole は、オーケストレーターがこのロールを実行するときに引き受けるロールです。これは必須フィールドではなく、省略すると、オーケストレーターはデフォルトでアカウントのメンバーロールを使用します。
6. これが完了したら、Security Hub にある「Remediate with ASR」カスタムアクションを使用して Config ルールを修復できます。

リファレンス

このセクションでは、このソリューション固有のメトリクスを収集するためのオプション機能に関する情報、関連リソースへのポインタ、およびこのソリューションに貢献したビルダーのリストが含まれています。

匿名化されたデータ収集

このソリューションには、匿名化された運用メトリクスを AWS に送信するオプションが含まれています。このデータを使用して、ユーザーがこのソリューションおよび関連サービスや製品をどのように使用しているかをよりよく理解します。有効にすると、以下の情報が収集され AWS に送信されます。

- ソリューション ID - AWS ソリューションの ID
- 一意の ID (UUID): 各 AWS Security Hub 応答および修復デプロイごとにランダムに生成された一意の識別子
- タイムスタンプ - データ収集のタイムスタンプ
- インスタンスデータ - このスタックデプロイに関する情報
- CloudWatchMetricsDashboardEnabled - "Yes" デプロイ中に CloudWatch メトリクスとダッシュボードが有効になっている場合
- ステータス - デプロイステータス (合格または不合格のソリューション) または (合格または不合格の修復)
- エラーメッセージ - ステータスフィールドの一般的なエラーメッセージ
- Generator_id - Security Hub のルール情報
- タイプ - 修復タイプと名前
- productArn - Security Hub がデプロイされているリージョン
- finding_triggered_by - 実行された修復のタイプ (カスタムアクションまたは自動トリガー)

このアンケートで収集されたデータは AWS が所有します。データ収集には、AWS プライバシー通知が適用されます。この機能を無効にするには、AWS CloudFormation テンプレートを起動する前に次のステップを実行します。

1. AWS CloudFormation テンプレートをローカルハードドライブにダウンロードします。
2. テキストエディタで AWS CloudFormation テンプレートを開きます。

3. AWS CloudFormation テンプレートマッピングセクションの変更元:

```
Mappings:
  Solution:
    Data:
      SendAnonymizedUsageData: 'Yes'
```

変更先:

```
  Mappings:
    Solution:
      Data:
        SendAnonymizedUsageData: 'No'
```

4. AWS CloudFormation コンソールにサインインします。
5. [スタックの作成] を選択します。
6. [スタックの作成] ページの [テンプレートの指定] セクションで、[テンプレートファイルのアップロード] を選択します。
7. [テンプレートファイルのアップロード] で、[ファイルを選択] を選択してから、編集したテンプレートをローカルドライブから選択します。
8. [次へ] を選択してから、本ガイドの「自動デプロイ」セクションにある「スタックを起動する」のステップに従ってください。

関連リソース

- 自動化された応答および AWS Security Hub を使用した修復
- CIS Amazon Web Services Foundations ベンチマーク、バージョン 1.2.0
- AWS の基本的なセキュリティのベストプラクティス標準
- Payment Card Industry Data Security Standard (PCI DSS)
- 米国国立標準技術研究所 (NIST) SP 800-53 Rev. 5

寄稿者

このドキュメントの寄稿者は次のとおりです。

- Mike O’Brien
- Nikhil Reddy
- Chandini Penmetsa
- Chaitanya Deolankar
- Max Granat
- Tim Mekari
- Aaron Schuetter
- Andrew Yankowsky
- Josh Moss
- Ryan Garay
- Thiemo Belmega

リビジョン

日付	変更
2020 年 8 月	初回リリース
2020 年 10 月	付録 C にトラブルシューティング情報を追加しました。
2020 年 11 月	中国リージョンのデプロイ手順を追加しました。Security Hub 管理者アカウントのソリューションデプロイ手順を更新しました。詳細については、GitHub リポジトリの CHANGELOG.md ファイルを参照してください。
2021 年 4 月	リリース v1.2.0: 新しいプレイブックアーキテクチャと新しい FSBP 修復を追加しました。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。
2021 年 5 月	リリース v1.2.1: EC2.2 および EC2.7 に影響する問題のバグ修正。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。
2021 年 8 月	リリース v1.3.0: PCI DSS v3.2.1 プレイブックを追加しました。CIS v1.2.0 に 17 件の新しい修復を追加しました。FSBP に 4 つの新しい修復を追加しました。SSM ランブックにもとづく新しいプレイブックアーキテクチャを使用するように CIS を変換しました。お客様が定義した修復で既存のプレイブックを拡張する手順を追加しました。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。

日付	変更
2021 年 9 月	リリース v1.3.1: `CreateLogMetricFilterAndAlarm.py` が変更されてアクションがアクティブになり、`SO0111-SHARR-LocalAlarmNotification` に SNS 通知が追加されました。新しい検出結果データ形式に合わせて CIS 2.8 の修復が変更されました。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。
2021 年 11 月	リリース v1.3.2: CIS v1.2.0 コントロール 3.1 ~ 3.14 のバグ修正。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。
2021 年 12 月	リリース v1.4.0: StackSets を使用してソリューションをデプロイできるようになりました。クロスアカウントに加えて、クロスリージョン修復がサポートされるようになりました。スタックが削除されても、メンバーアカウントの IAM ロールが保持されるようになりました。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。
2022 年 1 月	リリース v1.4.1: バグ修正。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。
2022 年 1 月	リリース v1.4.2: バグ修正。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。
2022 年 6 月	リリース v1.5.0: 追加の修復。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。

日付	変更
2022 年 12 月	リリース 1.5.1 SSM ドキュメントの作成をカスタムリソース Lambda から `CfnDocument` に切り替えるための変更。SSM ドキュメント名のプレフィックスは、SHARR ではなく ASR で始まるように更新されました。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。
2023 年 3 月	リリース 2.0.0: セキュリティコントロールと CIS v1.4.0 標準のサポート、FSBP 標準に対する 5 つの新しい修復、CIS v1.2.0 標準に対する 1 つの新しい修復、サービスカタログ AppRegistry 統合、SSM ドキュメントスロットリングによるデプロイの失敗を回避するための追加の保護が追加されました。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。
2023 年 4 月	リリース 2.0.1: すべての新しい S3 バケットの S3 オブジェクト所有権の新しいデフォルト設定 (ACL 無効) による影響を軽減しました。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。
2023 年 5 月	ドキュメントの更新: Well-Architected 定義の更新、各スタックのデプロイ場所に関するガイダンスの追加、特定の修復に関する問題のトラブルシューティングエディションの追加、SNS 通知のコード例の更新をしました。
2023 年 7 月	ドキュメントの更新: ワークフローのアーキテクチャ図とソリューションコンポーネントを更新しました。

日付	変更
2023 年 10 月	リリース 2.0.2: セキュリティの脆弱性を解決するためにパッケージバージョンを更新しました。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。
2023 年 11 月	ドキュメントの更新: 「AWS Service Catalog AppRegistry によるソリューションのモニタリング」セクションに「ソリューションに関連するコストタグを確認する」を追加しました。
2024 年 3 月	リリース 2.1.0: NIST 標準のサポートを追加、FSBP 標準に 17 件の新しい修復を追加、ソリューションのモニタリング用の CloudWatch ダッシュボードを追加、アーキテクチャにスロットリングハンドラーを追加、Security Hub のカスタマイズ可能な入力パラメータのサポートを追加、Config の検出結果の修復のサポートを追加しました。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。
2024 年 4 月	リリース 2.1.1: CloudFormation パラメータの順序とデフォルト値を更新し、ドキュメントを更新しました。NIST 標準への参照を追加しました。EventBridge ルールの Service Quotas に関する情報を追加しました。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。
2024 年 6 月	リリース 2.1.2: ソリューションの更新時にエラーが発生しないように、特定のプレイブックの AppRegistry を無効にしました。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。

日付	変更
2024 年 9 月	リリース 2.1.3: EC2.18 および EC2.19 の修復スクリプトで、IpProtocol を -1 に設定した場合のセキュリティグループルールが誤って無視される問題を解決しました。修復 SSM ドキュメントのすべての Python ランタイムを Python 3.8 から Python 3.11 にアップグレードしました。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。
2024 年 11 月	リリース 2.1.4: すべてのコントロールランブックの Python ランタイムを Python 3.8 から Python 3.11 にアップグレードしました。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。
2024 年 12 月	リリース 2.2.0: チケットシステム統合、CloudTrail アクションログ、CIS 3.0.0 プレイブックを追加しました。ダッシュボードと通知を強化しました。詳細については、GitHub リポジトリ内の CHANGELOG.md ファイルを参照してください。

注意

お客様は、本書に記載されている情報を独自に評価する責任を負うものとします。本書は、(a) 情報提供のみを目的とし、(b) AWS の現行製品と慣行について説明しており、これらは予告なしに変更されることがあり、(c) AWS およびその関連会社、サプライヤー、またはライセンサーからの契約上の義務や保証をもたらすものではありません。AWS の製品やサービスは、明示または黙示を問わず、一切の保証、表明、条件なしに「現状のまま」提供されます。お客様に対する AWS の責任は、AWS 契約により規定されます。本書は、AWS とお客様の間で行われるいかなる契約の一部でもなく、そのような契約の内容を変更するものでもありません。

AWS の自動化されたセキュリティ応答は、Apache Software Foundation で利用可能な Apache License Version 2.0 の条項に基づいてライセンスされます。