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

目次

AWS Security Hub で事前定義された対応と修復アクションにより、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 4 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、次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の実行に必要なコストが知りたい場合。	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が知りたい場合。	クォータ
どの AWS リージョンでこのソリューションをサポートしているか知りたい場合。	サポートしている AWS リージョン
このソリューションに含まれている 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したい場合	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したい場合。	GitHub リポジトリ

セキュリティは進化し続けるため、データを保護するための積極的な対策が必要であり、セキュリティチームが対応するのが難しく、費用と時間がかかることがあります。AWS での自動化されたセキュリティ対応ソリューションは、業界のコンプライアンス基準とベストプラクティスに基づいて事前定義された応答と修復アクションを提供することにより、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) に合わせて調整するのに役立つ 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 のユーザーは、一般的なセキュリティの検出結果を解決し、AWS でのセキュリティ体制を改善することが容易になります。

特定のプレイブックを選択して、AWS Security Hub のプライマリアカウントにデプロイできます。各プレイブックには、単一の AWS アカウント内または複数の AWS 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、AWS 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、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 AWS Security Hub が管理するすべてのアカウントの検出結果を 1 回のアクションで修復できるようにします。例えば、AWS リソースを保護するためのコンプライアンス基準である Center for Internet Security (CIS) AWS Foundations Benchmark の推奨事項を適用して、パスワードの有効期限を 90 日以内にしたり、AWS に保存されたイベントログの暗号化を強制したりすることができます。

注記

修復は、早急な対処が必要な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 Management コンソールから開始した場合、または特定のコントロール用に 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、検出結果を修復するための変更を加えます。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。

AWS 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、スタックのリソースを定義するコードを変更し、スタックを更新して、スタックのリソースを修正してください。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、「CIS (Center for Internet Security) AWS Foundations Benchmark v1.2.0」、「CIS AWS Foundations Benchmark v1.4.0」、「AWS Foundational Security Best Practices (FSBP) v1.0.0」、「Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1」、「National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5」の一部として定義されているセキュリティ基準のプレイブックによる修復が含まれています。このソリューションには、AWS Security Hub の統合されたコントロールの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、「プレイブック」セクション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 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、AWS クラウドにおけるアーキテクチャの設計の実務経験がある IT インフラストラクチャアーキテクト、管理者、DevOps プロフェッショナルを対象としています。

機能とメリット

AWS での自動化されたセキュリティ対応では次の機能を提供しています。

特定のコントロールに関する検出結果を自動的に修復する

コントロール用の Amazon EventBridge ルールを有効にすると、そのコントロールの検出結果が AWS Security Hub に表示された直後に自動的に修正されます。

複数のアカウントとリージョンの修復を 1 か所から管理する

組織のアカウントとリージョンの集約先として設定している AWS Security Hub の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任意のアカウントとリージョンで検出結果の修復を開始します。

修復アクションと結果の通知を受け取る

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すると、修正が開始されたときや、修復が成功したかどうかが通知されます。

GovCloud パーティションと中国パーティションで AWSConfigRemediations を使用する

このソリューションに含まれる修復には、AWS が所有する AWSConifgRemediation ドキュメントの再パッケージ化がありますが、商用パーティションでは利用できますが、GovCloud や中国では利用できません。このソリューションをデプロイして、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してください。

カスタム修復とプレイブックの実装により、この AWS ソリューションを拡張する

このソリューションは、拡張可能でカスタマイズできるように設計されています。代替の修復実装を指定するには、カスタマイズされた AWS Systems Manager オートメーションドキュメントと AWS IAM ロールをデプロイします。ソリューションに実装されていない新しいコントロールセット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てください。

ユースケース

組織のアカウントとリージョン全体で基準への準拠を強制する

プレイブックを基準 (AWS 基本セキュリティベストプラクティスなど) にデプロイして、提供されている修復を利用できるようにします。ソリューションがデプロイされているアカウントやリージョンのリソースの修復を自動または手動で開始して、コンプライアンス違反のリソースを修正します。

組織のコンプライアンスニーズに合わせて、カスタム修復やプレイブックをデプロイする

提供されている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、主要な概念について説明し、このソリューション固有の用語を定義します。

アプリケーション

1 つのユニットとして運用する AWS リソースの論理グループ。

修復、修復ランブック

検出結果を解決するための一連の手順の実施。例えば、Security Control (SC) Lambda.1「Lambda 関数ポリシーではパブリックアクセスを禁止すべき」というコントロールの修復では、関連する AWS Lambda 関数のポリシーが修正され、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

オーケストレータが特定の統制に対して開始された修復を正しい修正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) オートメーションドキュメントの 1 つ。例えば、SC の Lambda.1 と AWS の基本的なセキュリティのベストプラクティス (FSBP) の Lambda.1 の修復は、同じ修復ランブックを使用して実装されます。オーケストレータは、各コントロールのコントロールランブックを起動します。コントロールランブックには、それぞれ ASR-AFSBP_Lambda.1 と ASR-SC_2.0.0_Lambda.1 という名前が付けられていま

す。各コントロールのランブックは同じ修復ランブック (この場合は ASR-RemoveLambdaPublicAccess) を起動します。

オーケストレーター

ソリューションによってデプロイされた Step Functions は、AWS Security Hub から検出された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起動します。また、オーケストレーターは、修復が開始されたときと修復が成功または失敗したときに、ソリューションの SNS トピックに通知します。

標準規格

コンプライアンスフレームワークの一部として組織によって定義されるコントロールのグループ。例えば、AWS Security Hub とこのソリューションでサポートしている基準の 1 つが AWS FSBP です。

コントロール

準拠するためにリソースに必要な、または持ってはいけないプロパティの説明。例えば、AWS FSBP Lambda.1というコントロールでは、AWS Lambda 関数はパブリックアクセスを禁止すべきであると記載されています。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。

統合された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 の機能の 1 つで、有効にすると、特定の基準に対応する ID ではなく、統合されたコントロール ID で検出結果が表示されます。例えば、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 のコントロールはすべて、統合された (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」にマップされます。 この機能を有効にすると、SC ランブックが使用されます。

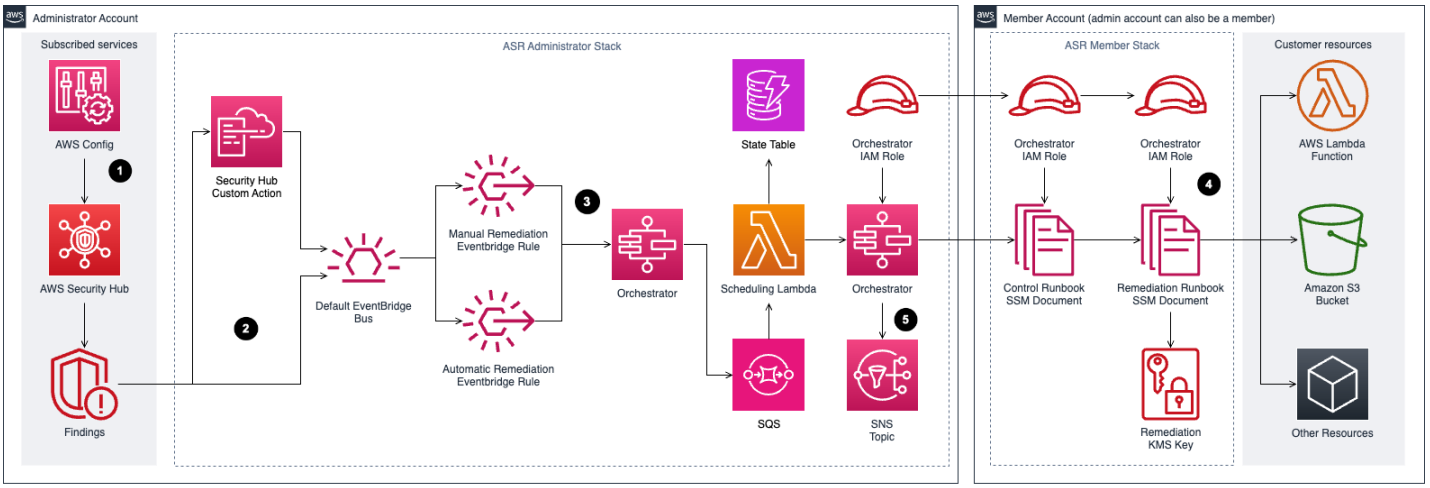
AWS 用語の一般的なリファレンスについては、「AWS 用語集」を参照してください。

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 での自動化されたセキュリティ対応のアーキテクチャ

> **注記**
> AWS CloudFormation のリソースは、AWS Cloud Development Kit (AWS CDK) のコンストラクトで作成されています。

AWS CloudFormation テンプレートを使用してデプロイされたこの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 を使用すると、セキュリティ体制を包括的に確認できるようになります。セキュリティ業界の基準とベストプラクティスに照らして環境を測定するのに役立ちます。機能するに際して、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基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表示されます。新しい検出結果は Amazon EventBridge 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 Amazon EventBridge イベントを開始できます。AWS Security Hub のカスタムアクションと Amazon EventBridge ルールにより、AWS プレイブックで自動セキュリティ対応が開始され、検出結果に対応できます。カスタムアクションイベントと一致するように 1 つの EventBridge ルールがデプロイされ、リアルタイム検出結果イベントと一致するように、サポートされている各コントロール (デフォルトでは無効化) に対して 1 つの Amazon EventBridge Event ルールがデプロイされます。AWS Security Hub 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するか、非本番環境で慎重にテストした後で自動修復を有効にすることができます。これは修復ごとに有効にできます。すべての修復で自動開始を有効にする必要はありません。

3. **オーケストレーション**: クロスアカウントの AWS Identity and Access Management (IAM) ロールを使用して、管理者アカウントの 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の修復を呼び出します。

4. **修復**: メンバーアカウントの AWS Systems Manager Automation ドキュメントは、AWS Lambda パブリックアクセスの無効化など、対象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。

5. **ログ**: プレイブックは結果を Amazon CloudWatch Logs グループにログを記録し、Amazon Simple Notification Service (Amazon SNS) トピックに通知を送信して、Security Hub の検出結果を更新します。実行されたアクションの監査証跡は、検出結果のメモに保持されます。AWS Security Hub のダッシュボードで、検出結果ワークフローのステータスが **NEW** から **NOTIFIED** または **RESOLVED** に変更されます。実行された修復を反映するように、セキュリティに関する検出結果のメモが更新されます。

AWS Well-Architected の設計に関する考慮事項

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に基づいて設計されました。これにより、ユーザーは信頼性が高く、安全で、効率的で、費用対効果の高いワークロードをクラウド上で設計し運用することができます。このセクションでは、このソリューションを構築する際に AWS 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どのように適用されたかを説明します。

運用上の優秀性

このセクションでは、このソリューションを設計する際に、運用上の優秀性の柱の原則とベストプラクティスをどのように適用したかを説明します。

- リソースは CloudFormation を使用して IaC として定義しました。

- 可能な限り、次の特性を考慮して対策を実施しました。
  - べき等性
  - エラー処理と報告
  - ロギング
  - 失敗時における既知の状態へのリソースの復元

セキュリティ

このセクションでは、このソリューションを設計する際に、セキュリティの柱の原則とベストプラクティスをどのように適用したかについて説明します。

- 認証と承認に IAM を使用しました。
- 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任意のリソースを操作するにはワイルドカードのアクセス許可が必要です。

信頼性

このセクションでは、このソリューションを設計する際に、信頼性の柱の原則とベストプラクティスをどのように適用したかを説明します。

- 検出結果の根本的な原因が修復によって解決されない場合、Security Hub は検出結果を作成し続けます。
- サーバーレスサービスにより、ソリューションは必要に応じてスケールできます。

パフォーマンス効率

このセクションでは、このソリューションを設計する際に、パフォーマンス効率の柱の原則とベストプラクティスをどのように適用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。

コストの最適化

このセクションでは、このソリューションを設計する際に、コスト最適化の柱の原則とベストプラクティスをどのように適用したかを説明します。

- サーバーレスサービスでは、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 自動化の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、このソリューションを設計する際に、持続可能性の柱の原則とベストプラクティスをどのように適用したかを説明します。

- サーバーレスサービスでは、必要に応じて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の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統合されます。AWS Security Hub コンソールのユーザーが **Findings for remediation** を選択すると、このソリューションでは AWS Step Functions を使用して、修復のために検出結果のレコードを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 のランブックは、`aws-sharr-member.template` と `aws-sharr-member-roles.template` の CloudFormation テンプレートを使用して、すべての AWS Security Hub のアカウント (管理者およびメンバー) 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」セクション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の自動修復が可能になります。

ユーザーは、Amazon CloudWatch Events 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。このオプションは、AWS Security Hub に報告されるとすぐに検出結果の完全自動修復を起動します。自動開始はデフォルトでオフに設定されています。このオプションは、AWS Security Hub の管理者アカウントで Amazon CloudWatch Events ルールをオンにすることで、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いつでも変更できます。

クロスアカウントの修復

AWS での自動化されたセキュリティ対応ソリューションでは、クロスアカウントのロールを使用して、プライマリアカウントとセカンダリアカウント間で動作します。これらのロールは、この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では、修復が必要なアカウントの修復用の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の AWS Systems Manager の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している修復方法については、「開発者ガイド」の「プレイブック」を参照してください。このソリューションでは、現在、次のプレイブックをサポートしています。

- セキュリティコントロール、AWS Security Hub の統合されたコントロールの検出結果機能と連携するプレイブック (2023 年 2 月 23 日公開)

  > **重要**
  > 統合されたコントロールの検出結果が Security Hub で有効になっている場合、このソリューションで有効にする必要があるのはこのプレイブックだけです。

- Center for Internet Security (CIS) Amazon Web Services Foundations benchmarks, version 1.2.0 (2018 年 5 月 18 日公開)
- Center for Internet Security (CIS) Amazon Web Services Foundations benchmarks, version 1.4.0 (2022 年 11 月 9 日公開)
- AWS Foundational Security Best Practices (FSBP) v1.0.0 (2021 年 3 月公開)
- Payment Card Industry Data Security Standards (PCI-DSS) version 3.2.1 (2018 年 5 月公開)
- National Institute of Standards and Technology (NIST) version 5.0.0 (2023 年 11 月公開)

統合ログ管理

AWS での自動化されたセキュリティ対応ソリューションでは、単一の Amazon CloudWatch Logs グループ (SO0111-SHARR) にログを記録します。これらのログには、この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に、詳細なロギングが含まれています。

通知

このソリューションでは、Amazon Simple Notification Service (Amazon SNS) トピックを使用して修復結果を発行します。このトピックのサブスクリプションを使用して、このソリューションの機能を拡張できます。例えば、メール通知を送信したり、トラブルチケットを更新したりできます。

このソリューションで使用している 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ています。この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を接続します。

AWS のサービス	説明
Amazon EventBridge	**コア。**検出内容が修正される際に、オーケストレーターステップ関数を起動するイベントをデプロイします。
AWS IAM	**コア。**さまざまなロールをデプロイして、さまざまなリソースでの修復を可能にします。
AWS Lambda	**コア。**オーケストレーターステップ関数が問題の修復に使用する複数の Lambda 関数をデプロイします。
AWS Security Hub	**コア。**ユーザーに AWS のセキュリティ状態を包括的に提供します。
AWS Step Functions	**コア。**AWS Systems Manager API コールを使用して修復ドキュメントを起動する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。
Amazon CloudWatch	**サポート。**さまざまなプレイブックが結果を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。メトリクスを収集して、アラーム付きのカスタムダッシュボードに表示します。
AWS DynamoDB	**サポート。**各アカウントとリージョンに最後に実行された修復を保存して、修復のスケジュールを最適化します。
Service Catalog AppRegistry	**サポート。**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て、コストと使用状況を追跡します。
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。**このソリューションが多数の修復を並行して実行できるように、修復のスケジュール設定を支援します。

デプロイの計画

このセクションでは、このソリューションをデプロイする前に、コスト、ネットワークセキュリティ、サポートしている AWS リージョン、クォータ、その他の考慮事項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。この改訂の時点で、米国東部 (バージニア北部) の AWS リージョンでこのソリューションをデフォルト設定で実行するための費用は、**1 か月あたり 300 回の修復で約 21.14 USD**、**1 か月あたり 3,000 回の修復で約 132.53 USD**、**1 か月あたり 30,000 回の修復で約 1270.60 USD** です。料金は変更される可能性があります。詳細については、このソリューションで使用される各 AWS サービスの料金表ページを参照してください。

> **注記**
> 多くの AWS のサービスには、無料で利用できるサービスの基準額である無料利用枠が含まれています。実際のコストは、提示しているコストの例よりも多い場合と少ない場合があります。

コスト管理を容易にするために、AWS Cost Explorer を使用して予算の作成を行うことを推奨しています。料金は変更される可能性があります。全体の詳細については、このソリューションで使用している各 AWS のサービスについて、料金のウェブ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、次の要因によって異なります。

- AWS Security Hub のメンバーアカウントの数
- 自動的に起動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、次の AWS コンポーネントを使用しており、設定に基づいてコストが発生します。小規模、中規模、大規模の組織向けのコスト例を示します。

AWS のサービス	無料利用枠	料金 [USD]
AWS Systems Manager Automation - ステップカウント	アカウントごと 1 か月あたり 100,000 ステップ	無料利用枠を超えると、基本ステップごとに 1 ステップあたり 0.002 USD が課金されます。複数のアカウントで自動化にする場合は、子 AWS 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、オリジナルアカウントでのみカウントされます。
AWS Systems Manager Automation - ステップの実行時間	1 か月あたり 5,000 秒	無料利用枠を超えると、aws:executeScript のアクションステップごとに、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 GB につき 1 か月あたり 0.046 USD
AWS Systems Manager Automation - データ転送	無料利用枠なし	転送される 1 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 件のチェックに対するコスト (1 つのアカウントごとで 1 つのリージョンにつき 1 か月あたり) は、1 件のチェックにつき 0.0010 USD 次の 400,000 件のチェックに対するコスト (1 つのアカウントごとで 1 つのリージョンにつき 1 か月あたり) は、1 件のチェックにつき 0.0008 USD 500,000 件を超えるチェックに対するコスト (1 つのアカウントごとで 1 つのリージョンにつき 1 か月あたり) は、1 件のチェックにつき 0.0005 USD
AWS Security Hub - 検出結果の取り込みイベント	最初の 10,000 件のイベント (1 つのアカウントごとで 1 つのリージョンにつき 1 か月あたり) は無料。AWS Security Hub のセキュリティに関連する検出結果の取り込みイベントをチェックします。	10,000 件を超えるイベントに対するコスト (1 つのアカウントごとで 1 つのリージョンにつき 1 か月あたり) は、1 件のイベントにつき 0.00003 USD
Amazon CloudWatch - メトリクス	基本モニタリングのメトリクス (5 分間隔) 10 件の詳細モニタリングのメトリクス (1 分間隔) 100 万件の API リクエスト (GetMetricData と	最初の 10,000 件のメトリクスのコストは、1 か月あたり 0.30 USD 次の 240,000 件のメトリクスのコストは、1 か月あたり 0.10 USD 次の 750,000 件のメトリクスのコストは、1 か月あたり 0.05 USD

AWS のサービス	無料利用枠	料金 [USD]
	GetMetricWidgetImage には適用なし)	1,000,000 件を超えるメトリクスのコストは、1 か月あたり 0.02 USD API コールのコストは 1,000 件のリクエストにつき 0.01 USD
Amazon CloudWatch - ダッシュボード	1 か月あたり最大 50 件のメトリクスに対応して、3 つのダッシュボード	1 か月あたり 1 つのダッシュボードごとに 3.00 USD
Amazon CloudWatch - アラーム	10 件のアラームメトリクス (高解像度のアラームには適用なし)	標準解像度 (60 秒) のコストは、アラームメトリクスごとに 0.10 USD 高解像度 (10 秒) のコストは、アラームメトリクスごとに 0.30 USD 標準解像度の異常検出のコストは、アラームごとに 0.30ドル 高解像度の異常検出のコストは、アラームごとに 0.90 USD 組み合わせた場合のコストは、アラームごとに 0.50 USD
Amazon CloudWatch - ログ収集	5 GB のデータ (取り込み、ストレージのアーカイブ、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 - ログのストレージ	5 GB のデータ (取り込み、ストレージのアーカイブ、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 1 GB あたり 0.005 USD
Amazon CloudWatch - イベント	カスタマイズされたイベントを除く、すべてのイベントが対象	カスタムイベントでは 100 万件のイベントにつき 1.00 USD、クロスアカウントイベントでは 100 万件のイベントにつき 1.00 USD
AWS Lambda - リクエスト	1 か月あたり 100 万件の無料リクエスト	100 万件のリクエストあたり 0.20 USD
AWS Lambda - 実行時間	1 か月あたり 400,000 GB / 秒のコンピューティング時間	1 GB / 秒ごとに 0.0000166667 USD実行時間に対する料金は、関数に割り当てたメモリ量により異なります。関数には、128 MB から 10,240 MB までの任意の量のメモリ

AWS のサービス	無料利用枠	料金 [USD]
		を 1 MB 単位の増分で割り当てることができます。
AWS Step Functions - 状態遷移	1 か月あたり 4,000 件の無料状態遷移	それ以後は、1,000 件の状態遷移につき 0.025 USD
Amazon EventBridge	AWS サービスが発行するすべての状態変更イベントは無料	カスタマイズされたイベントで、100 万件の発行されたイベントにつき 1.00 USD サードパーティ製 (SaaS) のイベントで、100 万件の発行されたイベントにつき 1.00 USD クロスアカウントイベントのコスト 送信されたクロスアカウントイベント 100 万件あたり 1.00 USD
Amazon SNS	最初の 100 万件 (1 か月あたり) の Amazon SNS リクエストは無料	それ以後は、100万件のリクエストにつき 0.50 USD
Amazon SQS	Amazon SQS リクエストのうち、毎月最初の 100 万件は無料	その後、100 万件から 1,000 億件のリクエストにつき 0.40 ドル
Amazon DynamoDB	最初の 25 GB のストレージは無料	それ以降、整合性のとれた読み取り/書き込みが 100 万回につき 2.00 USD

料金の例 (1 か月あたり)

例 1: 1 か月あたり 300 件の修復

- 10 個のアカウント、1 つのリージョン
- 1 つのアカウント / 1 つのリージョン / 1 か月につき 30 件の修復
- 総コストは、1 か月あたり 21.14 USD

AWS のサービス	前提	月額料金 [USD]
AWS Systems Manager Automation	ステップ: ~ 4 ステップ * 300 件の修復 * 0.002 USD = 2.40 USD 実行時間: 10秒 * 300 件の修復 * 0.00003 USD = 0.09 USD	2.49 USD
AWS Security Hub	請求可能なサービスの利用なし	0 USD

AWS のサービス	前提	月額料金 [USD]
Amazon CloudWatch Logs	300 件の修復 * 0.000002 USD = 0.0006 USD 0.0006 USD * 0.03 = 0.000018 USD	< 0.01 USD
AWS Lambda - リクエスト	300 件の修正 * 6 件のリクエスト = 1,800 件のリクエスト 0.20 USD * 1,000,000 万件のリクエスト = 0.20 USD	0.20 USD
AWS Lambda - 実行時間	256M: 1.875 GB 秒 * 300 件の修復 * 0.000167 USD = 0.009375 USD	< 0.01 USD
AWS Step Functions	15 件の状態遷移 * 300 件の修復 = 4,500 0.025 USD * (4,500/1,000) 状態遷移 = 0.1125 USD	< 0.12 USD
Amazon EventBridge ルール	ルールに対する課金なし	0 USD
AWS Key Management Service	1 つのキー * 10 個のアカウント * 1 つのリージョン * 1 ドル = 10 USD	10.00 USD
Amazon DynamoDB	2.00 USD * 1,000,000 件の読み取り / 書き込み = 2.00 USD	2.00 USD
Amazon SQS	0.40 USD * 1,000,000 件のリクエスト = 0.40 USD	0.40 USD
Amazon SNS	0.50 USD * 1,000,000 件の通知 = 0.50 USD	0.50 USD
Amazon CloudWatch - メトリクス	0.30 USD * 7 つのカスタムメトリックス = 2.10 USD 0.01 USD * (300 * 3 / 1,000) PUT メトリクスの API コール = 0.01 USD	2.11 USD
Amazon CloudWatch - ダッシュボード	3.00 USD * 1 つのダッシュボード = 3.00 USD	3.00 USD
Amazon CloudWatch - アラーム	0.10 USD * 3 つのアラーム = 0.30 USD	0.30 USD
合計		**21.14 USD**

例 2: 1 か月あたり 3,000 件の修復

- 100 個のアカウント、1 つのリージョン
- 1 つのアカウント / 1 つのリージョン / 1 か月につき 30 件の修復
- 総コストは、1 か月あたり 134.71 USD

AWS のサービス	前提	月額料金 [USD]
AWS Systems Manager Automation	ステップ: ~ 4 ステップ * 3,000 件の修復 * 0.002 USD = 24.00 USD 実行時間: 10 秒 * 3,000 件の修復 * 0.00003 USD = 0.90 USD	24.90 USD
AWS Security Hub	請求可能なサービスの利用なし	0 USD
Amazon CloudWatch Logs	3,000 件の修復 * 0.000002 USD = 0.006 USD 0.006 USD * 0.03 = 0.00018 USD	< 0.01 USD
AWS Lambda - リクエスト	3,000 件の修復 * 6 件のリクエスト = 18,000 件のリクエスト 0.20 USD * 1,000,000 万件のリクエスト = 0.20 USD	0.20 USD
AWS Lambda - 実行時間	256M: 1.875 GB 秒 * 3,000 件の修復 * 0.000167 USD = 0.09375 USD	0.09 USD
AWS Step Functions	15 件の状態遷移 * 3,000 件の修復 = 45,000 0.025 USD * (45,000 / 1,000) 状態遷移 = 1.125 USD	1.13 USD
Amazon EventBridge ルール	ルールに対する課金なし	0 USD
AWS Key Management Service	1 つのキー * 100 個のアカウント * 1 つのリージョン * 1 USD = 100 USD	100 USD
Amazon DynamoDB	2.00 USD * 1,000,000 件の読み取り / 書き込み = 2.00 USD	2.00 USD
Amazon SQS	0.40 USD * 1,000,000 件のリクエスト = 0.40 USD	0.40 USD
Amazon SNS	0.50 USD * 1,000,000 件の通知 = 0.50 USD	0.50 USD
Amazon CloudWatch - メトリクス	0.30 USD * 7 つのカスタムメトリックス = 2.10 USD 0.01 USD * (3000 * 3 / 1,000) PUT メトリクスの API コール = 0.09 USD	2.19 USD
Amazon CloudWatch - ダッシュボード	3.00 USD * 1 つのダッシュボード = 3.00 USD	3.00 USD
Amazon CloudWatch - アラーム	0.10 USD * 3 つのアラーム = 0.30 USD	0.30 USD
合計		**134.71 USD**

例 3: 1 か月あたり 30,000 件の修復

- 1000 個のアカウント、1 つのリージョン
- 1 つのアカウント / 1 つのリージョン / 1 か月につき 30 件の修復
- 総コストは、1 か月あたり 1270.60 USD

AWS のサービス	前提	月額料金 [USD]
AWS Systems Manager Automation	ステップ: ~ 4 ステップ * 30,000 件の修復 * 0.002 USD = 240.00 USD 実行時間: 10 秒 * 30,000 件の修復 * 0.00003 USD = 9.00 USD	249.00 USD
AWS Security Hub	請求可能なサービスの利用なし	0 USD
Amazon CloudWatch Logs	30,000 件の修復 * 0.000002 USD = 0.06 USD 0.06 USD * 0.03 = 0.0018 USD	< 0.01 USD
AWS Lambda - リクエスト	30,000 件の修正 * 6 件のリクエスト = 180,000 件のリクエスト 0.20 USD * 1,000,000 万件のリクエスト = 0.20 USD	0.20 USD
AWS Lambda - 実行時間	256M: 1.875 GB 秒 * 30,000 件の修復 * 0.000167 USD = 0.9375 USD	0.94 USD
AWS Step Functions	15 件の状態遷移 * 30,000 件の修復 = 450,000 0.025 USD * (450,000 / 1,000) 状態遷移 = 11.25 USD	11.25 USD
Amazon EventBridge ルール	ルールに対する課金なし	0 USD
AWS Key Management Service	1 つのキー * 1,000 個のアカウント * 1 つのリージョン * 1 USD = 1000 USD	1000 USD
Amazon DynamoDB	2.00 USD * 1,000,000 件の読み取り / 書き込み = 2.00 USD	2.00 USD
Amazon SQS	0.40 USD * 1,000,000 件のリクエスト = 0.40 USD	0.40 USD
Amazon SNS	0.50 USD * 1,000,000 件の通知 = 0.50 USD	0.50 USD
Amazon CloudWatch - メトリクス	0.30 USD * 7 つのカスタムメトリックス = 2.10 USD 0.01 USD * (30,000 * 3 / 1,000) PUT メトリクスの API コール = 0.90 USD	3.00 USD
Amazon CloudWatch - ダッシ	3.00 USD * 1 つのダッシュボード = 3.00 USD	3.00 USD

AWS のサービス	前提	月額料金 [USD]
ュボード		
Amazon CloudWatch - アラーム	0.10 USD * 3 つのアラーム = 0.30 USD	0.30 USD
合計		**1270.60 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場合、セキュリティ上の責任はお客様と AWS の間で共有されます。この責任共有モデルにより、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システムの物理的なセキュリティに至るまでのコンポーネントについて、AWS が運用、管理、および制御します。そのため、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) ロールにより、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詳細に割り当てることができます。このソリューションでは、各自動修復の機能ごとに、絞り込まれた範囲のアクセス許可を付与する IAM ロールを作成します。

管理者アカウントの AWS Step Functions には、SO0111-SHARR-Orchestrator-Admin ロールが割り当てられます。このロールのみが、各メンバーアカウントの SO0111-Orchestrator-Member を引き受けることが許可されています。メンバーロールは、各修復ロールが AWS Systems Manager サービスに渡して、特定の修復ランブックを実行することを許可されています。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になります。

サポートしている 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
米国東部 (バージニア北部)	us-east-1

リージョン名	リージョンコード
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
欧州 (ミラノ)	eu-south-1
欧州 (パリ)	eu-west-3
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 (UAE)	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

リージョン名	リージョンコード
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 アカウント用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。

次のリンクを使用すると、各サービスのページに移動できます。ページを切り替えずにドキュメント内のすべての AWS サービスのサービスクォータを表示するには、こちらの PDF にある「Service endpoints and quotas」ページの情報を確認してください。

AWS CloudFormation のクォータ

お使いの 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ような制限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 Amazon EventBridge ルールのクォータがあり、この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際に注意しておく必要があります。各プレイブックは、修正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と、ルールのクォータに達してしまう可能性があります。詳細については、**AWS 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 のセットアップに関する詳細は、**AWS Security Hub ユーザーガイド**の「AWS Security Hub のセットアップ」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 AWS Security Hub が動作するように設定されている必要があります。このソリューションは、AWS Security Hub のプライマリアカウントと同じ AWS アカウント (および AWS リージョン) にデプロイできます。各 Security Hub のプライマリアカウントとセカンダリアカウントで、アカウントで修復ランブックを実行するソリューションの AWS Step Functions に AssumeRole の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する必要もあります。

ソリューションの更新

このソリューションを v1.3.x 以前から最新バージョンにアップグレードするには、まずは既存のスタックを削除してから、最新バージョンのスタックを再インストールする必要があります。削除の手順については、「ソリューションのアンインストール」セクションを参照してください。ログデータはすべて保持され、運用データが失われることはありません。v1.4.x からアップグレードする場合は、「ソリューションのアップデート」を参照してください。

スタックと StackSets のデプロイメント

StackSets 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される場所と方法に基づいてリソースを分割することにより、StackSets を用いたデプロイをサポートします。マルチアカウントのユーザーで、特に AWS Organizations を利用している場合は、StackSets を使用して多数のアカウントにデプロイすることでメリットを得られます。これにより、ソリューションのインストールとメンテナンスに必要な労力が軽減されます。StackSets の詳細については、「AWS CloudFormation StackSets の使用」を参照してください。

ソリューションのデプロイ

重要

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は (**新規デプロイではこれがデフォルト**)、このソリューションをデプロイする際に、**セキュリティコントロール (SC) プレイブックのみを有効にしてください**。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基準のプレイブック**のみ**を有効にしてください。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してしまう可能性があります。

このソリューションでは、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。

この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、次にデプロイ方法を決定します。

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 Stack または StackSet としてデプロイする方法について詳しく説明します。

各スタックをデプロイする場所の決定

3 つのテンプレートは次の名称で呼ばれており、それぞれ次のリソースが含まれています。

- 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、Security Hub カスタムアクション
- メンバースタック: 修復 SSM オートメーションドキュメント
- 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。ご自分の組織の Security Hub 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 の検出結果に基づいて動作するため、そのアカウントまたはリージョンが Security Hub の管理者アカウントとリージョンの検出結果を集約するように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、ある組織に us-east-1 と us-west-2 のリージョンで運用されているアカウントがあり、アカウント 111111111111 が us-east-1 リージョンの Security Hub 委任管理者になっているとします。222222222222 と 333333333333 のアカウントは、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。us-west-2 から us-east-1 までの検出結果を集約するには、3 つのアカウントすべてを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。

メンバースタックをデプロイする前に、まず管理者スタックのデプロイを完了する必要があります。これにより、メンバーアカウントからハブアカウントへの信頼関係を構築できます。

メンバースタックは、検出結果を修復したい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 の管理者スタックをデプロイした Security Hub の委任管理者アカウントが含まれる場合があります。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をメンバーアカウントで実行する必要があります。

前述の例を使用して、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、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 と 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、これにはアカウントごとに 1 回しかデプロイできない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ありません。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。

前述の例を使用して、メンバーロールスタックを us-east-1 の 3 つのアカウント (111111111111、222222222222、333333333333) すべて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の決定

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 (セルフマネージドのアクセス許可)
- CloudFormation StackSet (サービスマネージドのアクセス許可)

- CloudFormation スタック

サービスマネージドのアクセス許可を持つ StackSet は、独自のロールをデプロイする必要がなく、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、この方法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だけです。

組織全体にデプロイする場合、組織の管理アカウントは含まれないため、組織の管理アカウントで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ることに注意してください。

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、サービスマネージド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。そのため、このスタックはセルフマネージドのアクセス許可を持つ StackSets でデプロイすることをお勧めします。

管理者スタックは一度だけデプロイされるため、プレーンな CloudFormation スタックとして、または単一のアカウントとリージョンでセルフマネージド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

ご自分の組織のアカウントで、Security Hub の統合されたコントロールの検出結果機能をオンまたはオフに設定できます。**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。

> **重要**
> 有効になっている場合は、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」の基準では、管理者スタックとメンバースタックの両方をデプロイする必要があります。これにより、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、この機能がオンになったときに生成される統合されたコントロール ID で使用できるようになります。この機能を使用する場合、特定の基準 (例: AWS FSBP) に合わせ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。このテンプレートには、このソリューションのコアコンポーネント、AWS Step Functions のログ用のネストされたスタック、選択したセキュリティ基準ごとに 1 つのネストされたスタックがインストールされます。

使用するサービスには、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

次のテンプレートが AWS Security Hub の管理者アカウントにインストールされ、サポートするセキュリティ基準が有効になります。`aws-sharr-deploy.template` をインストールするときに、インストールするテンプレートを次の中から選択できます。

aws-sharr-orchestrator-log.template - オーケストレーターステップ関数用の CloudWatch ロググループの作成。

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 のルール。

CIS120Stack.template - CIS Amazon Web Services Foundations benchmarks, v1.2.0 のルール。

CIS140Stack.template - CIS Amazon Web Services Foundations benchmarks, v1.4.0 のルール。

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

NISTStack.template - National Institute of Standards and Technology (NIST), v5.0.0 のルール。

SCStack.template - SC v2.0.0 のルール。

メンバーアカウント

View template

aws-sharr-member.template - AWS Systems Manager のオートメーションランブックとアクセス許可を AWS Security Hub の各メンバーアカウント (管理者アカウントを含む) にインストールするためのコアソリューションをセットアップした後にこのテンプレートを使用します。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基準のプレイブックを選択できます。

`aws-sharr-member.template` では、選択内容に基づいて次のテンプレートがインストールされます。

aws-sharr-remediations.template - 1 つ以上のセキュリティ基準で使用されている共通の修復コード。

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、修復ランブック。

CIS120MemberStack.template - CIS Amazon Web Services Foundations benchmarks, v1.2.0 の設定、アクセス許可、修復ランブック。

CIS140MemberStack.template - CIS Amazon Web Services Foundations benchmarks, v1.4.0 の設定、アクセス許可、修復ランブック。

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

NISTMemberStack.template - National Institute of Standards and Technology (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、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 のメンバーアカウントに必要な修復ロールを定義します。

自動デプロイ - StackSets

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

このソリューションを起動する前に、このガイドで説明し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、設計上の考慮事項を確認してください。このセクションの手順に従ってソリューションを設定し、AWS Organizations 内にデプロイします。

デプロイ時間: StackSets パラメータによって、1 つのアカウントごとに約 30 分。

前提条件

AWS Organizations は、マルチアカウントの AWS 環境とリソースを一元的に管理するのに役立ちます。StackSets は AWS Organizations で最適に機能します。

既にこのソリューションの v1.3.x またはそれ以前のバージョンをデプロイしている場合は、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、「ソリューションのアップデート」セクション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 Organizations には、委任された Security Hub の管理者アカウントが必要です。
- Security Hub は、リージョン全体の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「クロスリージョン集約」を参照してください。
- AWS を使用する各リージョンで、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 の管理者アカウントと AWS Security Hub の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

注記
このソリューションの StackSets のデプロイでは、サービスマネージドとセルフマネージドの StackSets を組み合わせて使用しています。セルフマネージドの StackSets では、サービスマネージド StackSets ではまだサポートされていないネストされた StackSets を使用しているため、今のところは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 をデプロイしてください。

プランニング

次のフォームを使用して、StackSets のデプロイを支援することができます。データを準備し、デプロイ中に値をコピーして貼り付けてください。

```
AWS Organizations の管理者アカウント ID: _____________

Security Hub の管理者アカウント ID: _____________

CloudTrail のロググループ: _____________________________

メンバーアカウント ID (カンマ区切りリスト):

____________________,
____________________,
____________________,
____________________,
____________________
AWS Organizations の OU (カンマ区切りリスト):

____________________,
____________________,
____________________,
____________________,
____________________
```

ステップ 1: 委任された Security Hub の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 StackSets を使用して、AWS Security Hub の管理者と同じリージョンの AWS Security Hub の管理者アカウントで `aws-sharr-deploy.template` AWS CloudFormation テンプレートを起動します。このテンプレートでは、ネストされたスタックを使用しています。
- インストールするセキュリティ基準を選択します。デフォルトでは、SC のみが選択されています (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。前回のインストールで `SO0111-SHARR-Orchestrator` がすでに存在する場合は、`Yes` を選択します。

セルフマネージド 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 の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 のデプロイが完了するまで待ちます。

- サービスマネージド StackSets を使用して、AWS Organizations の各アカウントの単一の AWS 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。
- 組織に新しいアカウントが追加された時に、このテンプレートを自動的にインストールするように選択します。
- AWS Security Hub の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 の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 StackSets を使用して、同じ AWS Security Hub の管理者が管理する AWS Organizations のすべてのアカウントに AWS リソースがあるすべての AWS リージョンで、`aws-sharr-member.template` AWS CloudFormation テンプレートを起動します。

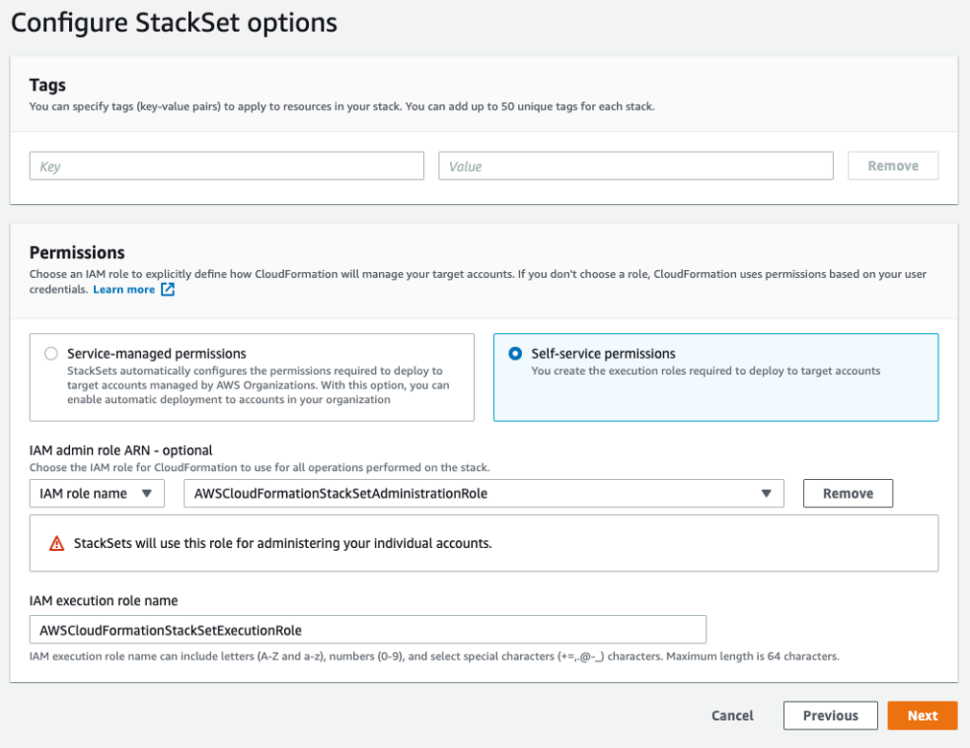
  > **注記**
  > サービスマネージド StackSets がネストされたスタックがサポートされるまでは、組織に加わる新しいアカウントに対してこの手順を実行する必要があります。

- インストールするセキュリティ基準の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 (一部の修復で使用します)。

- AWS Security Hub の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 1: 委任された Security Hub の管理者アカウントで管理者スタックを起動する

1. Security Hub の管理者アカウントで、管理者スタック (`aws-sharr-deploy.template`) をデプロイします。通常、単一のリージョンで組織ごとに 1 つ指定します。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 StackSets としてデプロイする必要があります。



StackSet のオプションを設定する

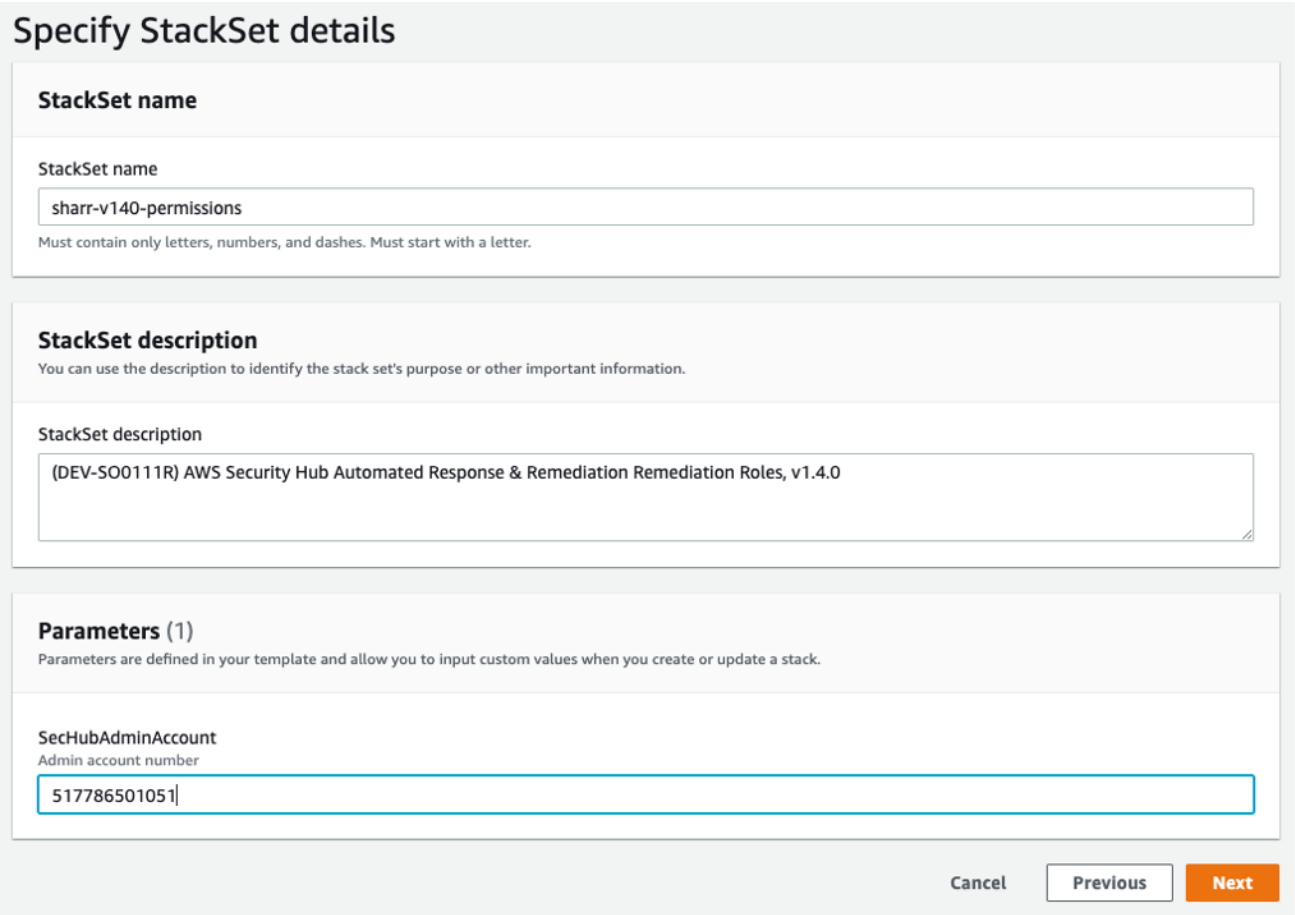
2. **Account numbers** パラメータに、AWS Security Hub の管理者アカウントのアカウント ID を入力します。

3. **Specify regions** パラメータで、Security Hub の管理者がオンになっているリージョンのみを選択します。この手順が完了するのを待ってから、ステップ 2 に進みます。

ステップ 2: 各 AWS Security Hub の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 StackSets を使用して、メンバーロールのテンプレート (`aws-sharr-member-roles.template`) をデプロイします。この StackSets 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 の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にこれらのアクセス許可が付与されるように、自動デプロイをオンにします。
3. **Specify regions** パラメータで、単一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 StackSets がデプロイされている間に、ステップ 3 に進むことができます。



StackSets の詳細を指定

ステップ 3: 各 AWS Security Hub の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

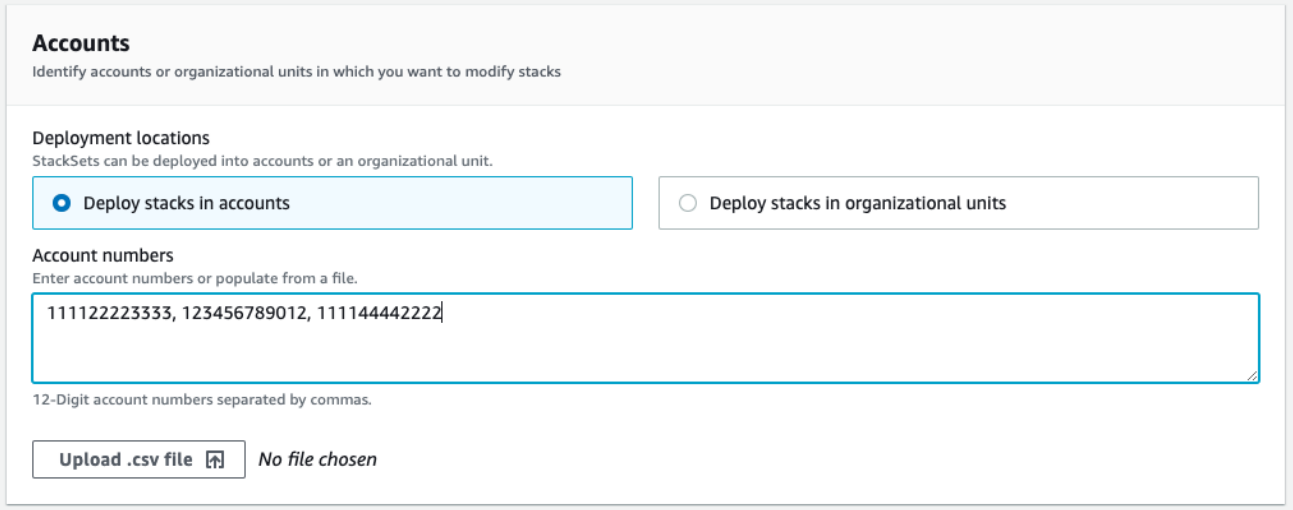
メンバースタックはネストされたスタックを使用するため、セルフマネージド StackSets としてデプロイする必要があります。AWS Organizations の新しいアカウントへの自動デプロイはサポートされていません。

パラメータ

LogGroup Configuration: CloudTrail ログを受信するロググループを選択します。存在していない場合、またはロググループがアカウントごとに異なる場合は、適切な値を選択してください。アカウント管理者は、CloudTrail ログ用に CloudWatch ロググループを作成した後に、AWS System Manager の Prameter Store で、/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のアラームを作成する修復に必要です。

Standards: メンバーアカウントに読み込むセキュリティ基準を選択します。これによってインストールされるのは AWS Systems Manager のランブックだけです。セキュリティ基準は有効になりません。

SecHubAdminAccount: この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 の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

Deployment locations: 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。

Specify regions: 検出結果を修復するリージョンをすべて選択します。アカウントとリージョンの数に応じて、デプロイのオプションを調整できます。リージョンの同時実行性は並列化できます。

自動デプロイ - スタック

> **注記**
> マルチアカウントのユーザーには、StackSets を使用したデプロイを強くお勧めします。

このソリューションを起動する前に、このガイドで説明し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、設計上の考慮事項を確認してください。このセクションの手順に従って、この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および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。既にこのソリューションをデプロイしている場合は、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、「ソリューションのアップデート」セクション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。

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 の管理者アカウントで起動します。
- インストールするセキュリティ基準を選択します。
- 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で `SO0111-SHARR-Orchestrator` が既に存在している場合は `Yes` を選択してください)。

ステップ 2: メンバースタックを起動する

- CIS 3.1-3.14 の修復で使用する CloudWatch ロググループの名前を指定します。CloudTrail ログを受け取る CloudWatch Logs の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。このロールは、アカウントごとに 1 回だけインストールしてください。
- インストールするプレイブックを選択します。
- AWS Security Hub の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: (オプション) 利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措置をすべて削除します。この手順はオプションです。

ステップ 1: 管理者スタックの起動する

重要
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。AWS ではこのデータを使用して、ユーザーがこのソリューション、関連サービスおよび製品をどのように使用しているかをよりよく理解し、提供するサービスや製品の改善に役立てます。AWS は、このアンケートを通じて収集されたデータを所有します。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て、AWS CloudFormation のマッピングセクションを変更し、AWS CloudFormation コンソールを使用してテンプレートをアップロードし、この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の収集」セクションを参照してください。

この自動化された 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、前提条件を確認する必要があります。

注記
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。詳細については、このガイドの「コスト」セクションで、このソリューションで使用されている各 AWS サービスの料金表ウェブ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の AWS マネジメントコンソールにサインインしてから、`aws-sharr-deploy.template` AWS CloudFormation テンプレートを起動するボタンを選択します。

   Launch solution

   独自にカスタマイズするためにテンプレートをダウンロードすることもできます。

2. このテンプレートは、デフォルトで米国東部 (バージニア北部) リージョンで起動されます。別の AWS リージョンでこのソリューションを起動するには、AWS マネージメントコンソールのナビゲーションバーでリージョンセレクターを使用します。

   注記
   このソリューションは AWS Systems Manager を使用していますが、現在こちらは特定の AWS リージョンのみで利用可能です。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 AWS リージョンで動作します。AWS リージョンごとで利用可能な AWS サービスの最新情報については、AWS リージョン別のサービスをご参照ください。

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入力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、この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 AWS STS クォータ」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
Load SC Admin Stack	`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。
Load AFSBP Admin Stack	`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。
Load CIS120 Admin Stack	`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。
Load CIS140 Admin Stack	`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。

パラメータ	デフォルト	説明
Load PC1321 Admin Stack	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。
Load NIST Admin Stack	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。
Reuse Orchestrator Log Group	no	既存の Amazon CloudWatch Logs の `SO0111-SHARR-Orchestrator` 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が簡単に行えます。v1.2 以降からアップグレードする場合は、`yes` を選択してください。
Use CloudWatch Metrics	yes	この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。
Use CloudWatch Metrics Alarms	yes	このソリューションの CloudWatch メトリッ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、この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。
State Machine Executions Alarm Threshold	1000	ステートマシン実行アラームのしきい値を指定します。これにより、実装に合わせてカスタマイズされたしきい値を選択して、予想範囲を超える修復の量を示すことができます。

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. **レビュー**ページで、設定を確認します。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承認するチェックボックスを必ずオンにします。
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。

スタックのステータスは、AWS CloudFormation コンソールの**ステータス**列で確認できます。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 の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` StackSets 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 の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. AWS Security Hub の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) ごとに AWS マネジメントコンソールにサインインします。`aws-sharr-member.template` AWS CloudFormation テンプレートを起動するボタンを選択します。独自にカスタマイズするためにテンプレートをダウンロードすることもできます。

2. このテンプレートは、デフォルトで米国東部 (バージニア北部) リージョンで起動されます。別の AWS リージョンでこのソリューションを起動するには、AWS マネージメントコンソールのナビゲーションバーで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入力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、このソリューションのスタックに名前を割り当てます。名前に使用する文字の制限に関する詳細については、**AWS Identity and Access Management ユーザーガイド**の「IAM および AWS STS クォータ」を参照してください。

5. **パラメータ**ページで、次のパラメータを指定して [**次へ**] を選択します。

パラメータ	デフォルト	説明
Sec Hub Account Admin	<入力が必須>	AWS Security Hub の管理者アカウントの 12 桁のアカウント ID を入力します。この値により、管理者アカウントのソリューションのロールにアクセス許可が付与されます。

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. **レビュー**ページで、設定を確認します。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承認するチェックボックスを必ずオンにします。

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。

スタックのステータスは、AWS CloudFormation コンソールの**ステータス**列で確認できます。約 5 分で CREATE_COMPLETE ステータスが表示されます。このスタックが読み込まれている間は、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

重要
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。AWS ではこのデータを使用して、ユーザーがこのソリューション、関連サービスおよび製品をどのように使用しているかをよりよく理解し、提供するサービスや製品の改善に役立てます。このアンケートを通じて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て、AWS CloudFormation のマッピングセクションを変更し、AWS CloudFormation コンソールを使用してテンプレートをアップロードし、この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 の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、このスタック経由で利用可能な修復をコントロールできます。

1. AWS Security Hub の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) ごとに AWS マネジメントコンソールにサインインします。`aws-sharr-member.template` AWS CloudFormation テンプレートを起動するボタンを選択します。

   Launch solution

   独自にカスタマイズするためにテンプレートをダウンロードすることもできます。

2. このテンプレートは、デフォルトで米国東部 (バージニア北部) リージョンで起動されます。別の AWS リージョンでこのソリューションを起動するには、AWS マネージメントコンソールのナビゲーションバーでリージョンセレクターを使用します。

> **注記**
> このソリューションでは AWS Systems Manager を使用します。このサービスは、現在、ほとんどの AWS リージョンで利用可能です。このソリューションは、これらの AWS サービスをサポートするすべての AWS リージョンで起動します。AWS リージョンごとで利用可能な AWS サービスの最新情報については、AWS リージョン別のサービスをご参照ください。

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入力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、この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 AWS STS クォータ」を参照してください。

5. **パラメータ**ページで、次のパラメータを指定して [**次へ**] を選択します。

パラメータ	デフォルト	説明
Provide the name of the LogGroup to be used to create Metric Filters and Alarms	<入力が必須>	CloudTrail が API コールを記録する CloudWatch ロググループの名前を指定します。これは CIS 3.1-3.14 の修復に使用されます。
Load SC Member Stack	`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。
Load AFSBP Member Stack	`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。
Load CIS120 Member Stack	`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。
Load CIS140 Member Stack	`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。
Load PC1321 Member Stack	`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。
Load NIST Member Stack	`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。
Create S3 Bucket For Redshift Audit Logging	`no`	FSBP Redshift.4 修復用に S3 バケットを作成する必要がある場合は、`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

パラメータ	デフォルト	説明
		Redshift.4 の修復を参照してください。
Sec Hub Admin Account	<入力が必須>	AWS Security Hub の管理者アカウントの 12 桁のアカウント ID を入力します。

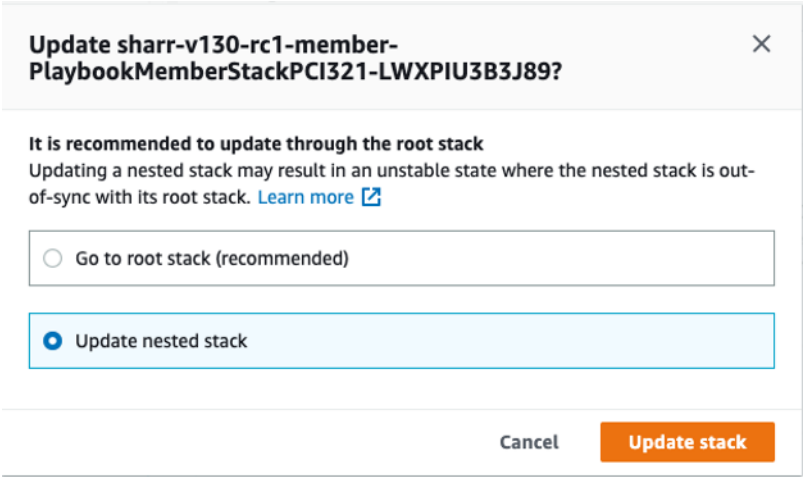
6. **スタックオプションの設定**ページで、[**次へ**] を選択します。
7. **レビュー**ページで、設定を確認します。テンプレートが AWS Identity and Access Management (IAM) リソースを作成することを承認するチェックボックスを必ずオンにします。
8. [**スタックの作成**] を選択してスタックをデプロイします。

スタックのステータスは、AWS CloudFormation コンソールの**ステータス**列で確認できます。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) 利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、ネストされたスタックをセキュリティ基準に合わせて更新することで削除できます。シンプルにするために、ネストされたスタックのオプションはルートスタックには伝播されません。

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



ネストされたスタックの更新

4. [**現在のテンプレートを使用**] 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。必要なコントロールの値は `Available` に、不要なコントロールは `Not available` に変更してください。

> **注記**
> 修復をオフにすると、セキュリティ基準とコントロール用のソリューションの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. **レビュー**ページで、設定を確認します。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承認するチェックボックスを必ずオンにします。
8. [**スタックの更新**] を選択します。

スタックのステータスは、AWS CloudFormation コンソールの**ステータス**列で確認できます。約 15 分で CREATE_COMPLETE ステータスが表示されます。

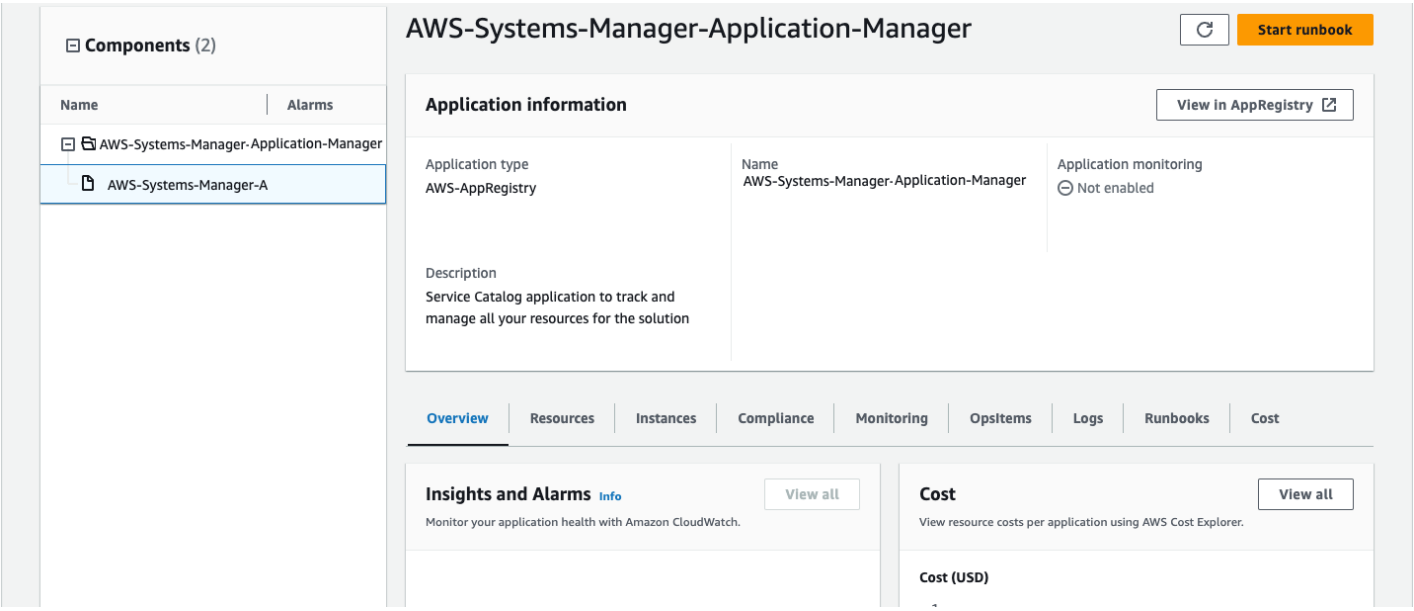
Service Catalog AppRegistry によるソリューションのモニタリング

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

AWS Systems Manager Application Manager は、このソリューションとリソースをアプリケーションレベルで確認できるため、次のようなことが可能になります。

- リソース、スタックや AWS アカウント全体でデプロイされたリソースのコスト、このソリューションに関連するログを一元的にモニタリングします。
- このソリューションのリソースの運用データ (デプロイステータス、CloudWatch アラーム、リソース設定、運用上の問題など) をアプリケーションのコンテキストで表示します。

次の図では、Application Manager のソリューションスタックでのアプリケーションビューの例を示しています。

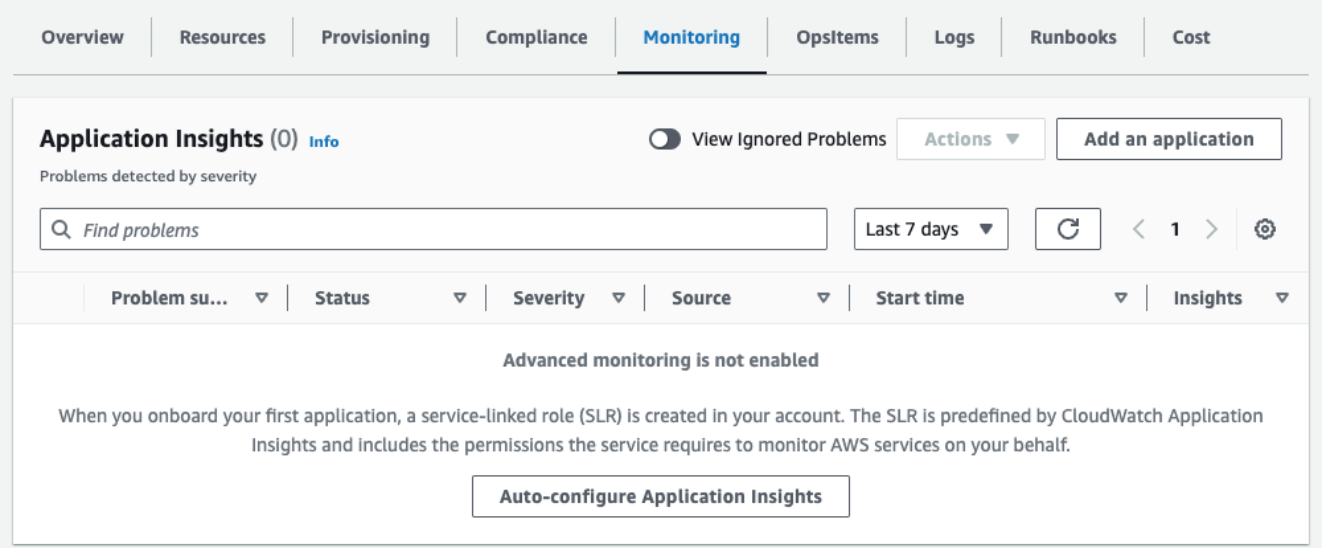


Application Manager でのソリューションスタック

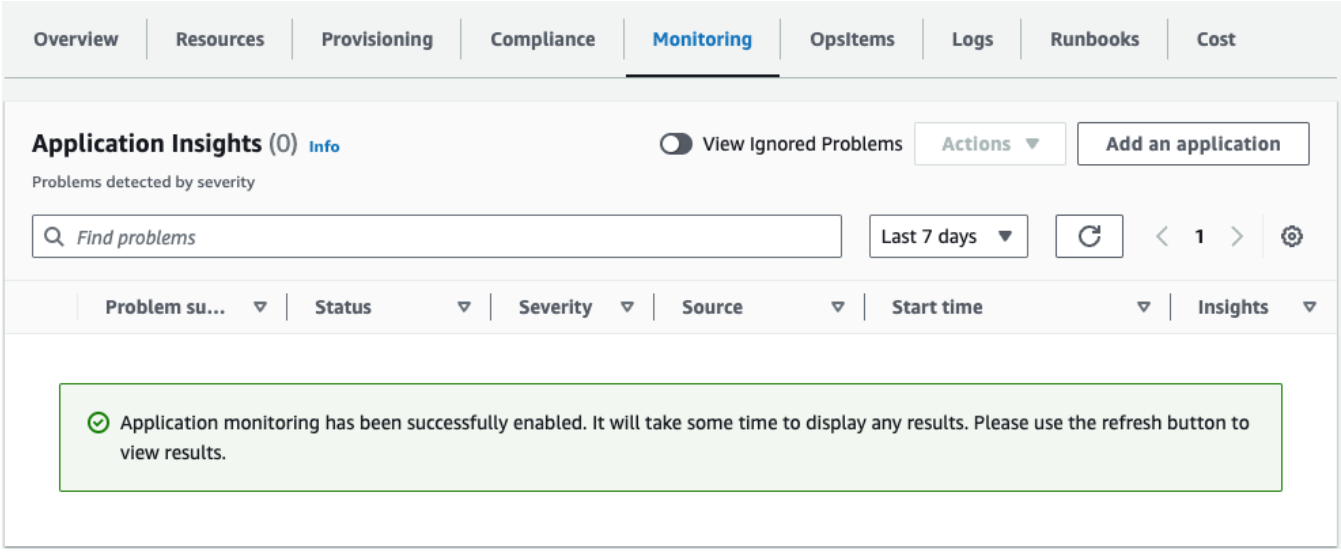
Amazon CloudWatch Application Insights の有効化

1. Systems Manager コンソールにログインします。
2. ナビゲーションペインで、[**アプリケーションマネージャー**] を選択します。
3. **Applications** 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。

   アプリケーション名の**アプリケーションソース**列には App Registry と表示され、ソリューション名、リージョン、アカウント ID、またはスタック名が組み合わされます。
4. **コンポーネント**ツリーで、有効化したいアプリケーションスタックを選択します。
5. **モニタリング**タブの **Application Insights** で、[**Auto-configure Application Insights**] を選択します。



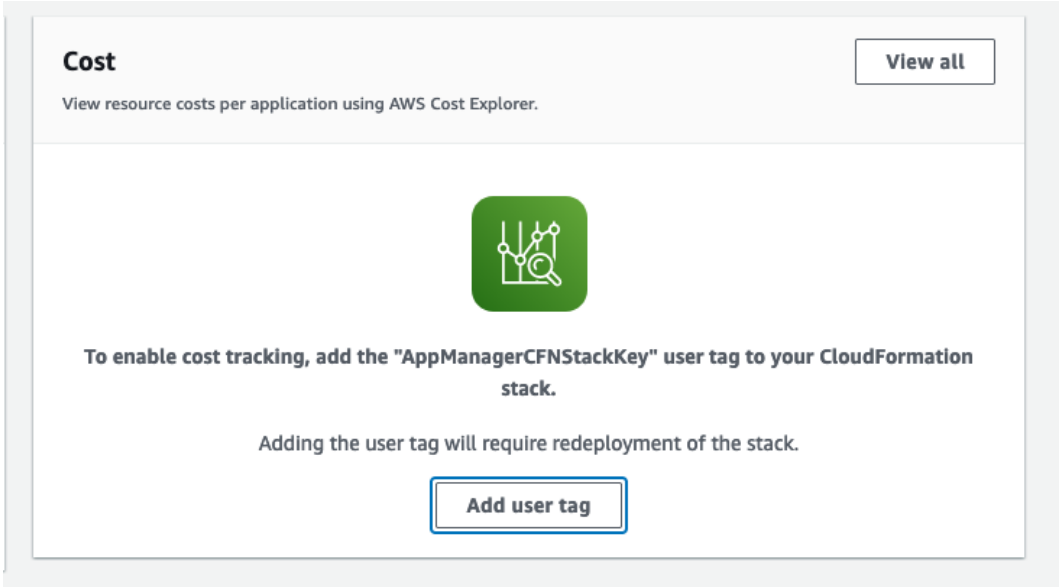
アプリケーションのモニタリングが有効になり、次のステータスボックスが表示されます。



ソリューションに関連するコストタグを確認する

ソリューションに関連するコスト配分タグを有効にしたら、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確認する必要があります。次の手順で、コスト配分タグを確認します。

1. Systems Manager コンソールにログインします。
2. ナビゲーションペインで、[**アプリケーションマネージャー**] を選択します。
3. **Applications** で、このソリューションのアプリケーション名を選択します。
4. **概要**タブの**コスト**で、[**Add user tag**] を選択します。



5. **Add user tag** ページで confirm と入力し、[**Add user tag**] 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 時間かかる場合があります。

ソリューションに関連するコスト配分タグの有効化

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、コスト配分タグを有効にしてこのソリューションのコストを確認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有効にできます。

次の手順で、コスト配分タグを有効にします。

1. 請求とコスト管理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` タグでフィルタリングし、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

AWS Cost Explorer との統合により、アプリケーションおよびアプリケーションコンポーネントに関連するコストの概要を Application Manager コンソールで確認できます。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 マネジメント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**] を選択して、ソリューションのコストと使用状況を時系列で表示します。

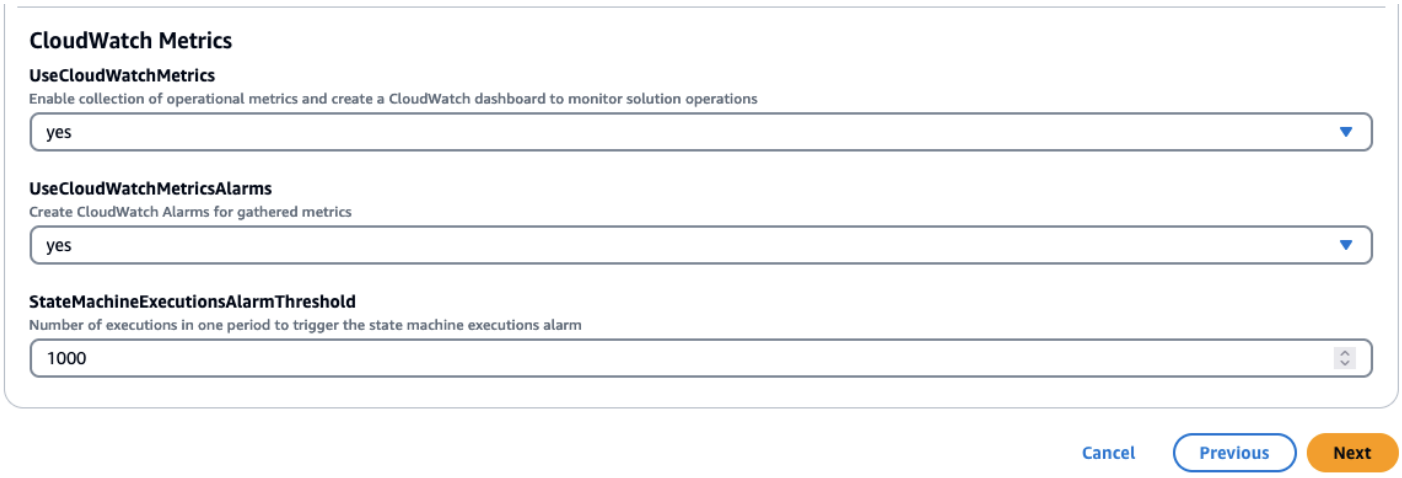
Amazon CloudWatch ダッシュボードを使用してソリューションのオペレーションをモニタリング

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ときにアラートを出します。

CloudWatch のメトリクス、アラーム、ダッシュボードを有効にする

CloudWatch の機能には 3 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、運用メトリクスの収集が有効になり、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. StateMachineExecutionsAlarmThreshold — ステートマシンの実行アラームを起動するある一定期間の実行回数。

CloudWatch ダッシュボードを使用する

ダッシュボードを表示するには:

1. Amazon CloudWatch 、ダッシュボードの順に移動します。
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、さまざまなメトリクスを表示する定義済みのウィジェットが付属しています。メトリクスのデフォルトの収集期間は 24 時間です。

1. State Machine Executions — ステートマシンによって開始された修復の数。
2. Remediation Outcomes — SUCCESS と FAILURE 別にグループ化された修復結果の数。
3. Remediation Failures by Type — 修復が失敗したさまざまな理由の数。
4. Remediation Scheduling Queue Length — 修復をスケジュールするためのキューの最大長。
5. Maximum Remediation Delay — 修復のスケジュール設定から実行までの最大遅延時間。
6. Runbook Assue Role Failures — 適切なロールを引き受けられなかったために失敗した修復の数。これは、ソリューションがターゲットアカウントに正しくデプロイされていないことを示しています。

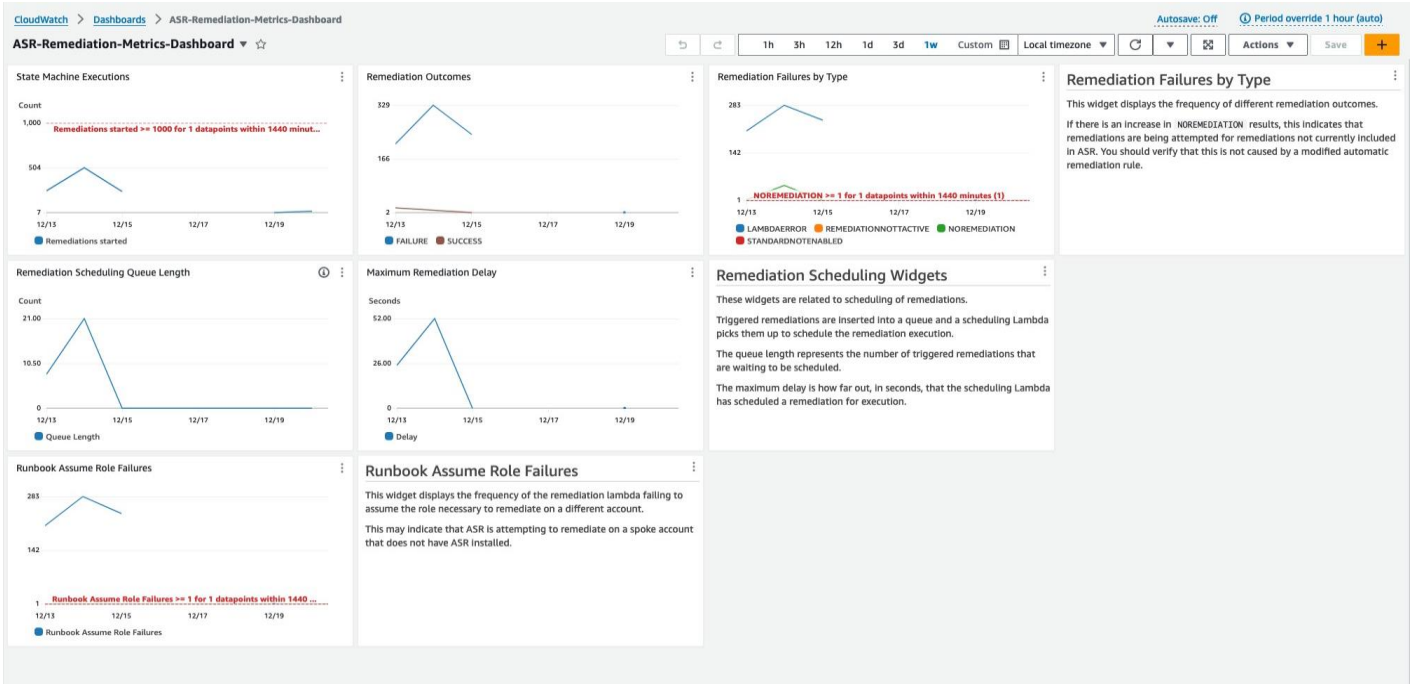
CloudWatch ダッシュボードには、一般的なオペレーションエラーを警告する定義済みのアラームも付属しています。

1. State Machine executions > 1000 (24 時間以内)
    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 パラメーターを使用して変更できます。
2. Remediation Failures by Type = NOREMEDIATION > 0
    a. ASR に含まれていない修復に対して修復が試みられています。これは、イベントルールが意図した以上の修復を含むように変更されたことを示している可能性があります。

3. Runbook Assume Role Failures > 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で修正が試みられています。これは、イベントルールが意図したよりも多くのアカウントを含むように変更されたことを示している可能性があります。

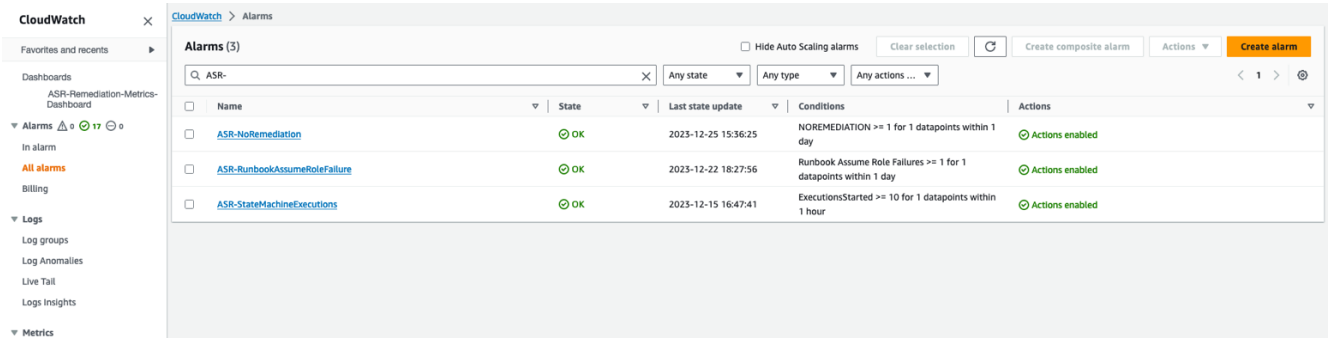
すべてのアラームしきい値は、個々のデプロイのニーズに合わせて変更できます。



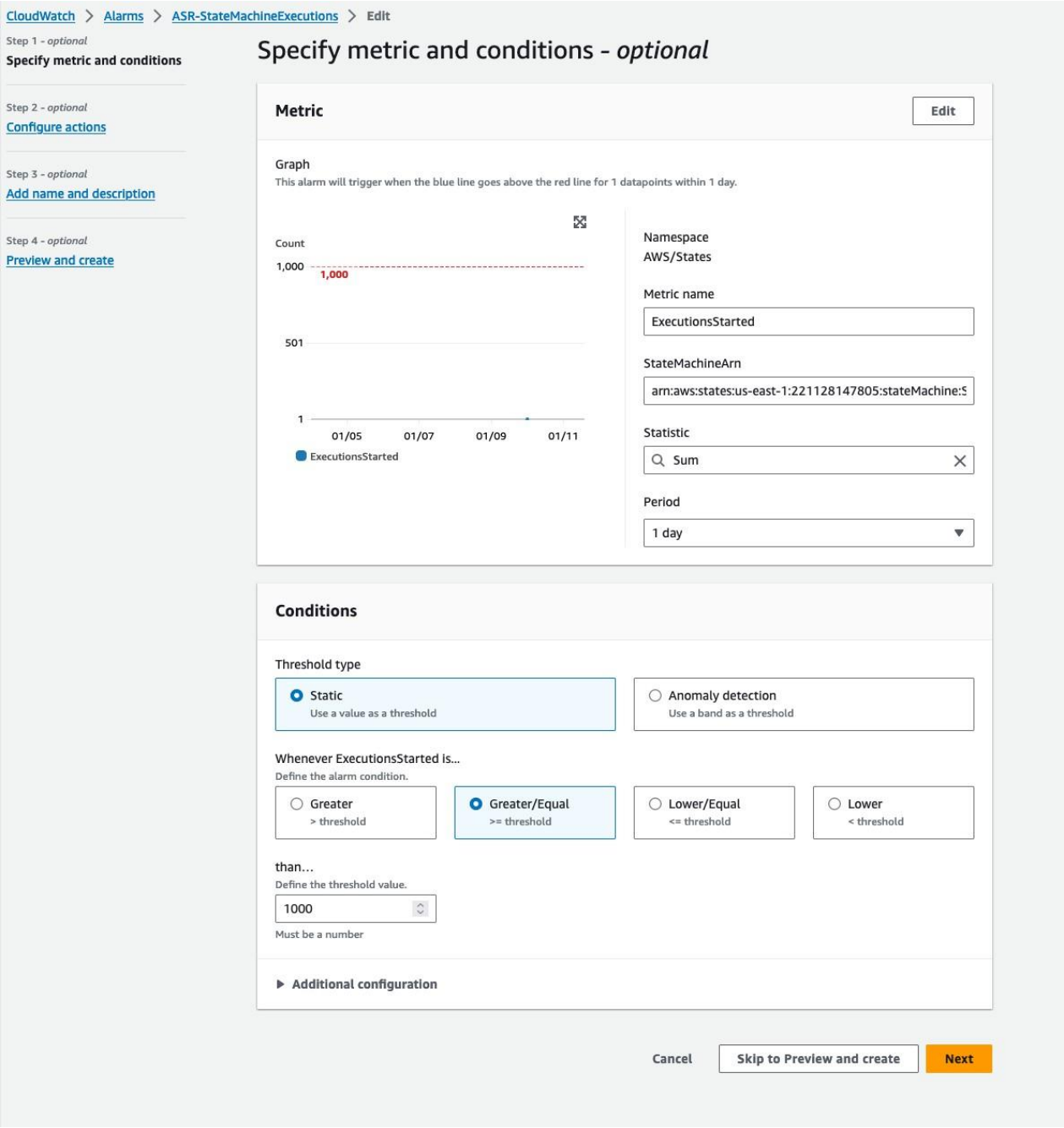
アラームのしきい値を変更する

1. Amazon CloudWatch -> アラーム -> すべてのアラーム の順に移動します。

2. 変更するアラームを選択し、[アクション] -> [編集] の順に選択します。



3. しきい値を希望の値に変更して保存します。



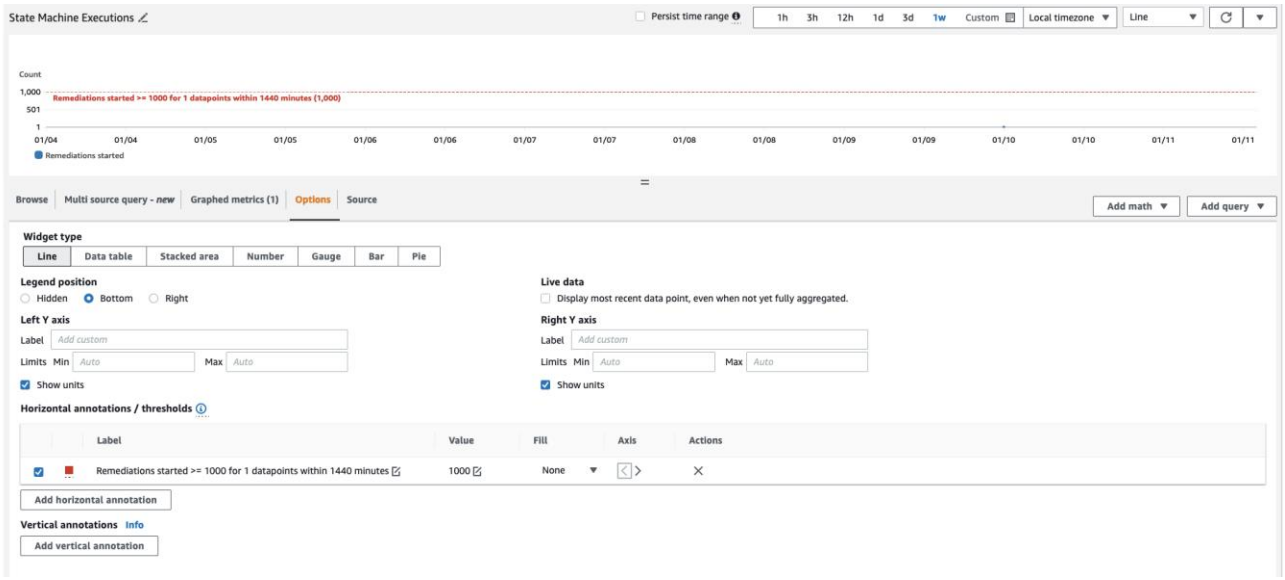
4. CloudWatch ダッシュボードに移動して、新しい設定と一致するようにグラフを変更します。

   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] をクリックします。

   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の注釈を修正します。



アラーム通知をサブクスライブする

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 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 状態になったときに通知されます。

ソリューションのアップデート

v1.4 以前のバージョンからのアップグレード

v1.4.x 以前のソリューションをデプロイしている場合は、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てください。

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。「ソリューションのアンインストール」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。「ソリューションのデプロイ」を参照してください。

> **注記**
> 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、**Use existing Orchestrator Log Group** 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、このオプションで `Yes` を選択します。このオプションを使用すると、オーケストレーターステップ関数と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、すべてのスタックまたは StackSets を次のように更新します。

1. 最新のテンプレートを使用して、AWS Security Hub の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のアクセス許可を更新します。
3. 現在デプロイし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のメンバースタックを更新します。

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ための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」に、このソリューションに関する AWS サポートのケースを開く方法が記載されています。

ソリューションのログ

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。トピックについては左側の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 の管理者アカウントの Amazon CloudWatch Logs グループ (`SO0111-SHARR`) に記録します。コントロールおよび日ごとに 1 つのストリームが作成されます。

オーケストレーターステップ関数は、AWS Security Hub の管理者アカウントで `SO0111-SHARR-Orchestrator` の CloudWatch ロググループにすべてのステップの遷移を記録します。このログは、ステップ関数の各インスタンスの状態遷移を記録する監査証跡です。ステップ関数の実行ごとに 1 つのログストリームが作成されます。

どちらのロググループも AWS KMS key 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ています。このログに加えて、AWS Systems Manager Automation コンソール、オートメーションの実行ログ、AWS Step Functions コンソール、AWS Lambda のログを使用して、問題のトラブルシューティングを行います。

修復が失敗すると、次のようなメッセージが `SO0111-SHARR` に基準、コントロール、日付用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)
```

次のメッセージに詳細が記載されています。この出力は、セキュリティ基準とコントロールに関する SHARR の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.
```

この情報は失敗箇所を示しています。この場合は、メンバーアカウントで実行されている子オートメーションになります。この問題をトラブルシューティングするには、(上記のメッセージより) メンバーアカウントで AWS マネジメントコンソールにログインし、AWS Systems Manager に移動して **Automation** に移動し、実行 ID (`eecdef79-9111-4532-921a-e098549f525`) のログ出力を調べる必要があります。

既知の問題解決

- **問題:** このソリューションのデプロイは、リソースが Amazon CloudWatch で既に使用可能であることを示すエラーで失敗します。

  解決策: CloudFormation のリソース / イベントのセクションで、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がないか確認します。SHARR のデプロイ用の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。再利用を選択したことを確認します。

- **問題:** プレイブックのネストされたスタックで EventBridge ルールを作成できないというエラーが発生し、ソリューションのデプロイに失敗します。

  解決策: デプロイされたプレイブックの数により、EventBridgeのルールが上限に達した可能性があります。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、使用されている基準のプレイブックのみをデプロイするか、EventBridge ルールのクォータの引き上げをリクエストしてください。

- **問題**: 同じアカウントで、Security Hub を複数のリージョンで実行しています。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 の管理者と同じアカウントおよびリージョンに管理者スタックをデプロイする必要があります。Security Hub のメンバーが設定されている各アカウントと AWS 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**: デプロイ直後に、**SO0111-SHARR-Orchestrator** が次の 502 エラーで Get Automation Document State で失敗します。「*Lambda was unable to decrypt the environment variables because KMS access was denied. Please check the function's KMS key settings. KMS Exception: UnrecognizedClientExceptionKMS Message: The security token included in the request is invalid.(Service: AWSLambda; Status Code: 502; Error Code: KMSAccessDeniedException; Request ID: …*」

  解決策: 修復を実行する前に、このソリューションが安定するまで約 10 分待ちます。問題が解決しない場合は、サポートチケットを切るか、GitHub の Issue に登録してください。

- **問題**: 検出結果の修復を試みましたが、何も起こりませんでした。

  解決策: 修復されなかった理由がないか、検出結果のメモを確認してください。一般的な原因は、この検出結果に自動修復機能がないことです。現時点では、メモ以外に修復が存在しない場合は、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。このソリューションのログを確認してください。コンソールで CloudWatch Logs を開いてください。SO0111-SHARR CloudWatch ロググループを見つけます。最近更新されたストリームが最初に表示されるようにリストを並べ替えてください。実行しようとした検出結果のログストリームを選択します。そこでエラーが見つかるはずです。失敗の原因としては、検出結果の制御と修復の制御の不一致、クロスアカウントの修復 (まだサポートされていない)、または検出結果がすでに修正されていることが考えられます。失敗の原因を特定できなかった場合は、ログを収集し、サポートチケットを切ってください。

- **問題**: 修復を開始した後に、AWS 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: AWS Security Hub コンソールでは、自動的に更新されません。現在のビューを更新してください。検出結果のステータスが更新されます。検出結果が **Failed** から **Passed** 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。これで問題が解決しない場合は、上記の「検出結果の修復を試みましたが、何も起こりませんでした」の解決方法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で、**Get Automation Document State** が失敗します。「*An error occurred (AccessDenied) when calling the AssumeRole operation*.」

  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の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をデプロイするための手順に従ってください。

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

  解決策: AWS Config の設定を慎重に調べて、AWS Config が正しくセットアップされていることを確認してください。自動修復では、場合によって、既存の AWS Config の設定を修正できません。

- **問題**: 修復は成功しているが、`"No output available yet because the step is not successfully executed."` の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」というこのリリースの既知の問題です。修復ランブックは正常に失敗し、動作しない場合にこのソリューションに通知します。

- **問題**: 解決に失敗して、スタックトレースが送信される

  解決策: 場合によっては、エラーメッセージではなくスタックトレースになるエラー状態に対処する機会を逃すことがあります。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てください。サポートが必要な場合は、サポートチケットを切ってください。

- **問題**: カスタムアクションのリソースで v1.3.0 のスタックを削除できませんでした。

  解決策: カスタムアクションを削除すると、管理者用テンプレートの削除が失敗することがあります。これは既知の問題で、次のリリースで修正される予定です。このような場合は、次のようになります。

  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. 管理者用のアカウントで、**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. 「**Remediate with SHARR**」のエントリを手動で削除します。
  5. 再度、スタックを削除します。

- **問題**: 管理者スタックを再度デプロイした後に、`AssumeRole` で AWS Step Functions が失敗します。

  解決策: 管理者スタックを再度デプロイすると、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間の信頼関係が切断されます。メンバーロールスタックをすべてのメンバーアカウントに再度デプロイする必要があります。

- **問題:** 24 時間を超えても CIS 3.x の修復が `PASSED` と表示されません。

  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。

特定の修復方法に関する問題

SetSSLBucketPolicy が AccessDenied エラーで失敗する

関連コントロール: 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 オペレーションをコールするとエラー (AccessDenied) が発生した: AccessDenied

ブロックパブリックアクセス設定がバケットで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を設定しようとすると、このエラーで失敗します。このような状態にするには、そのようなステートメントを含むバケットポリシーを設定し、そのバケットのパブリックアクセスブロックを有効にします。

ConfigureS3BucketPublicAccessBlock (関連コントロール: 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) の修復でも、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行うため、バケットをこの状態にすることができます。

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修正されないため、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は、それらのステートメントがまだ含まれている修正されたバケットポリシーを追加しようとしても、修復は失敗します。

解決策: バケットのパブリックアクセスをブロックする設定と矛盾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するようにバケットポリシーを修正します。

PutS3BucketPolicyDeny が失敗する

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

問題: PutS3BucketPolicyDeny で、次のエラーが表示されます。

```
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をブロックするため、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修正して、「*」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。

この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、このソリューションのさまざまなコンポーネントを無効にする方法について詳しく説明します。

シナリオ 1: 単一のコントロールに対する自動修復を無効にする。

1. AWS CloudFormation コンソールで、EventBridge に移動します。
2. サイドバーにある [**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て、無効にするコントロールを検索します。
4. ルールを選択して、[**無効化**] ボタンを選択します。

シナリオ 2: すべてのコントロールに対する自動修復を無効にする。

1. コンソールで EventBridge に移動します。
2. サイドバーにある [**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て、その下にあるすべてのルールを選択します。
4. [**無効化**] ボタンを選択します。複数ページのルールでこれを行う必要がある場合があることに注意してください。

シナリオ 3: アカウントに対する手動修復を無効にする。

1. コンソールで EventBridge に移動します。
2. サイドバーにある [**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て、「**Remediate_with_SHARR_CustomAction**」を検索します。
4. ルールを選択して、[**無効化**] ボタンを選択します。

AWS サポートへのお問い合わせ

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エ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。

ケースを作成

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、[**Solutions**] を選択します。
3. **カテゴリ**で、[**Other Solutions**] を選択します。
4. **緊急度**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**、**緊急度**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**] を選択してください。

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 サポート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**] で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。

ソリューションのアンインストール

AWS マネジメントコンソールでこのソリューションをアンインストールするには、次の手順を使用します。

V1.0.0-V1.2.1

リリース v1.0.0 ～ v1.2.1 では、サービスカタログを使用して CIS または FSBP の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. AWS Security Hub のメンバーアカウントからスポークの `CISPermissions.template` テンプレートを削除します。
4. Security Hub の管理者およびメンバーアカウントからスポークの `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、このソリューションのインストールスタックを選択して、[**削除**] を選択します。

> **注記**
> CloudWatch ロググループのログは保持されます。組織のログ保持ポリシーの要求に応じて、これらのログを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。

注記

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場合があります。これは既知の問題で、次のリリースで修正される予定です。次の手順を使用して、この問題を解決してください。

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. 管理者用のアカウントで、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. Remediate with SHARR のエントリを手動で削除します。
5. 再度、スタックを削除します。

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。

StackSets のデプロイ

StackSets ごとにスタックを削除してから、デプロイとは逆の順序で StackSets を削除します。

テンプレートが削除されても `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ようにしています。この SO0111-* のロールは、CloudTrail から CloudWatch へのロギングや RDS の拡張モニタリングなどのアクティブな修復で使用されていない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を有効または無効にする

ソリューションの管理者は、ソリューションのどの機能を有効にするかを次のようにコントロールできます。

メンバーとメンバーロールのスタックがデプロイされる場所:

- 管理者スタックは、パラメーター値として指定された管理者アカウント番号を使用して、メンバーとメンバーロールのスタックが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 ルールを通じて）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、メンバーまたはメンバーロールの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届い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 ルールを通じて）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、管理者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アカウントまたはリージョンを含めないでください。

どの基準のネストされたスタックがデプロイされているか:

- 管理者スタックは、対象となる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 ルールを通じて）修復を開始できます。これらは各基準のメンバースタックによってデプロイされます。
- 管理者スタックで完全に自動化された修復を開始できるのは、管理者スタックによってその基準のルールが適用されているコントロールの EventBridge ルールのみとなります。これらは管理者アカウントにデプロイされます。

- わかりやすくするために、管理者アカウントとメンバーアカウント全体で一貫して基準をデプロイすることをおすすめします。AWS FSBP と CIS v1.2.0 を取り扱う場合は、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て、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。

どのコントロールランブックが各ネストされたメンバースタックにデプロイされているか:

- 管理者スタックは、各スタンダードのメンバースタックによって対象となる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 ルールを通じて）修復を開始できます。
- 特定の基準でどのコントロールを有効にするかをよりきめ細かくコントロールするために、基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がデプロイされるパラメーターがあります。コントロールのパラメーターを「NOT Available」の値に設定して、そのコントロールランブックをアンデプロイします。

基準を有効または無効にするためのSSMパラメータ:

- 管理者スタックは、標準の管理者スタックによってデプロイされた SSM パラメータを通じて有効化された基準の修復のみを (カスタムアクションまたは完全に自動化された EventBridge ルールを通じて) 開始できます。
- 基準を無効にするには、/Solutions/SO0111/<standard_name>/<standard_version>/status パスの SSM パラメータの値を No に設定します。

SNS 通知の例

修復が開始された場合

```
{
  "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"
  }
}
```

修復に失敗した場合

```
{
  "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"
  }
}
```

ソリューションの使用

このチュートリアルでは、ASR を初めてデプロイする手順を説明します。まず、このソリューションを導入するための前提条件を説明し、最後にメンバーアカウントの検出結果の例を修復します。

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

このチュートリアルでは、初めてデプロイする手順を説明します。まず、このソリューションを導入するための前提条件を説明し、最後にメンバーアカウントの検出結果の例を修復します。

アカウントを準備する

この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の修復機能のデモを行うために、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。このソリューションを単一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 `222222222222` を使用してこのソリューションのデモを行います。`111111111111` は管理者アカウントになり、`222222222222` はメンバーアカウントになります。`us-east-1` と `us-west-2` のリージョンのリソースに関する検出結果を修復するソリューションを設定します。

次の表は、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-east-2 でのアクション
`111111111111`	管理者	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す。具体的には、手動で修復を開始したり、EventBridge ルールを使用して完全に自動化された修復を有効にしたりします。このアカウントは、検出結果を修復したいすべてのアカウントの Security Hub の委任管理者アカウントでもなければなりませんが、ご自分の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なく、またそうである必要もありません。

AWS Config を有効にする

次のドキュメントを確認します。

- 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両方のリージョンで AWS Config を有効にします。これには料金が発生します。

> **重要**
> 必ず「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が表示されません。

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

AWS Security Hub を有効にする

次のドキュメントを確認します。

- 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両方のリージョンで 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-east-2 でのアクション
111111111111	管理者	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ます。

- コントロールの検出結果の生成と更新

このチュートリアルでは、推奨構成である AWS Security Hub の統合されたコントロールの検出結果機能を有効にしたソリューションの使用方法を示します。この記事を書いている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) ではなく基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両方のリージョンで統合されたコントロールの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-east-2 でのアクション
111111111111	管理者	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、しばらく時間がかかる場合があります。このチュートリアルを続行することはできますが、新機能がないと生成された検出結果を修復することはできません。この新機能で生成された結果は、`GeneratorID` フィールド値の `security-control/<control_id>` で識別できます。

クロスリージョンの検出結果の集約を設定する

次のドキュメントを確認します。

- クロスリージョン集約
- クロスリージョン集約の有効化

両方のアカウントで us-west-2 から us-east-1 までの検出結果の集計を設定します。

アカウント	目的	us-east-1 でのアクション	us-east-2 でのアクション
111111111111	管理者	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	なし

アカウント	目的	us-east-1 でのアクション	us-east-2 でのアクション
		する	

検出結果が集約リージョンに反映されるまでにはしばらく時間がかかる場合があります。チュートリアルを続行することはできますが、他のリージョンの検出結果を集約リージョンに表示し始めるまで修復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ます。

- AWS Security Hub でのアカウントの管理
- 組織の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

次の例では、手動での招待方法を使用します。本番稼働アカウントのセットについては、AWS Organizations を使用し Security Hub の委任管理を行う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`) を招待して、Security Hub の委任管理者として管理者アカウントを承諾します。メンバーアカウントから、招待を承諾します。

アカウント	目的	us-east-1 でのアクション	us-east-2 でのアクション
`111111111111`	管理者	メンバーアカウントを招待する	なし
`222222222222`	メンバー	招待を承諾する	なし

検出結果が管理者アカウントに反映されるまでにはしばらく時間がかかる場合があります。チュートリアルを続行することはできますが、管理者アカウントに表示され始めるまで、メンバーアカウントからの検出結果を修復することはできません。

セルフマネージド StackSets アクセス許可用のロールを作成する

次のドキュメントを確認します。

- AWS CloudFormation StackSets

- セルフマネージドのアクセス許可の付与

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

スタックをデプロイして StackSet オペレーションの基本的なアクセス許可を取得します。本番稼働アカウントの場合は、「高度な権限オプション」のドキュメントに従ってアクセス許可を絞り込むことをお勧めします。

アカウント	目的	us-east-1 でのアクション	us-east-2 でのアクション
111111111111	管理者	StackSet の管理者ロールスタックをデプロイする StackSet の実行ロールスタックをデプロイする	なし
222222222222	メンバー	StackSet の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はないリソースを作成する

次のドキュメントを確認します。

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

修復のデモを行うために、安全ではない設定のリソースを次に示します。コントロールの例は Lambda.1 です。Lambda 関数の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。

> **重要**
> 安全では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、ご自分の環境でこのようなリソースが作成されるリスクをご自分で評価してください。このようなリソースを検出して報告するために組織に用意されている可能性のあるツールをすべて把握し、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適切でない場合は、この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てください。

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。構成 -> アクセス許可 で、認証なしで URL から関数を起動する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。ソリューションによってこの問題が解決されたら、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-east-2 でのアクション
111111111111	管理者	なし	なし
222222222222	メンバー	なし	安全ではない設定で Lambda 関数を作成する

AWS Config が安全ではない設定を検出するまでにはしばらく時間がかかる場合があります。チュートリアルを続行することはできますが、Config が検出するまでは検出結果を修復できません。

関連するコントロール用の CloudWatch ロググループを作成する

次のドキュメントを確認します。

- Amazon CloudWatch Logs による CloudTrail ログファイルのモニタリング
- CloudTrail コントロール

このソリューションがサポートするさまざまな CloudTrail コントロールでは、マルチリージョン CloudTrail の送信先となる 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。本番稼働アカウントの場合は、CloudTrail と CloudWatch Logs の統合を正しく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を作成します (例: `asr-log-group`)。

アカウント	目的	us-east-1 でのアクション	us-east-2 でのアクション
111111111111	管理者	ロググループを作成する	ロググループを作成する
222222222222	メンバー	ロググループを作成する	ロググループを作成する

チュートリアルアカウントにこのソリューションをデプロイする

管理、メンバー、メンバーロールのスタックの 3 つの Amazon S3 URL を集約します。

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 の検出結果の集約リージョンにデプロイします。

「SC」または「セキュリティコントロール」スタックを除く、ロードネスト管理者スタックのすべてのパラメータの値で `No` を選択します。このスタックには、アカウントに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。

以前にこのアカウントとリージョンにこのソリューションをデプロイしたことがある場合を除き、オーケストレータ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-east-2 でのアクション
111111111111	管理者	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

管理者スタックのデプロイが完了するまで待ってから続行すると、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 の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、ロードネストメンバースタックのすべてのパラメータの値で No を選択します。このスタックには、アカウントに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、これは `111111111111` です。

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

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 の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、これは `111111111111` です。

アカウント	目的	us-east-1 でのアクション	us-east-2 でのアクション
`111111111111`	管理者	メンバーの StackSet をデプロイする / メンバースタックがデプロイされていることを確認する	なし
`222222222222`	メンバー	メンバースタックがデプロイされていることを確認する	なし

SNS トピックにサブスクライブする

修復アップデート

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 トピックに登録します。これにより、修復が開始されたとき、および修正が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 トピックに登録します。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。

検出結果例の修復

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はない設定のリソースの検索結果を探します。

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、「Controls」というラベルの付いたページから、統合されたコントロール ID で検出結果を検索できます。
2. 「セキュリティ基準」ページでは、そのコントロールがどの基準に属しているかを確認できます。
3. 「検出結果」ページですべての検出結果を表示し、属性で検索できます。

作成されたパブリック Lambda 関数の統合されたコントロール 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選択します。[アクション] の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 に送信されたことを示す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-east-2 でのアクション
111111111111	管理者	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 通知を受け取るはずです。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 回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-east-2 でのアクション
111111111111	管理者	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

修復の実行状況を追跡する

ソリューションがどのように機能するかをよりよく理解するには、修復の実行を追跡します。

EventBridge ルール

管理者アカウントで、**Remediate_with_SHARR_CustomAction** という名前の EventBridge ルールを探します。このルールは Security Hub から送信した結果と一致し、オーケストレーターステップ関数に送信します。

ステップ関数の実行

管理者アカウントで、**SO0111-SHARR-Orchestrator** という名前のステップ関数を探します。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。修復の実行は、このステップ関数の実行履歴で追跡できます。

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が 2 回実行され、**ASR-RemoveLambdaPublicAccess** という名前のドキュメントが 1 回実行されているのを確認します。

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行われます。2 回目の実行はターゲットリージョンで行われますが、そのリージョンは検出結果の元のリージョンではない場合があります。最後の実行は、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 Logs 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ステップ関数からのハイレベルなログの保存先です。

完全に自動化された修復を有効にする

このソリューションのもう 1 つの運用方法は、検出結果が Security Hub に到着したら自動的に修復することです。

この検出結果を誤って適用す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) と一致するすべてのリソースで修復が開始されます。

重要

ソリューションの範囲内のすべてのパブリック Lambda 関数に対してこのアクセス許可を取り消せることを確認してください。完全に自動化された修復は、作成した関数の範囲に限定されません。このコントロールが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、ソリューションは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-east-2 でのアクション
111111111111	管理者	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-east-2 でのアクション
111111111111	管理者	自動修復ルールを有効にする	なし
222222222222	メンバー	なし	なし

リソースを設定する

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-east-2 でのアクション
111111111111	管理者	なし	なし
222222222222	メンバー	なし	Lambda 関数がパブリックアクセスを許可できるように設定する

修復によって検出結果が解決したことを確認する

Config が安全ではない設定を再度検出するまでにはしばらく時間がかかる場合があります。2 つの SNS 通知を受け取るはずです。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 回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-east-2 でのアクション
111111111111	管理者	自動修復ルールを有効にする	なし
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、作成したサンプルの 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-east-2 でのアクション
111111111111	管理者	なし	なし
222222222222	メンバー	なし	サンプルの 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-east-2 でのアクション
111111111111	管理者	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-east-2 でのアクション
111111111111	管理者	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-east-2 でのアクション
111111111111	管理者	メンバーロール StackSet を削除する メンバーロールスタックの削除を確認する	なし
222222222222	メンバー	メンバーロールスタックの削除を確認する	なし

保持されているロールを削除する

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、修復が引き続き機能 (例: VPC フローログ) するためにロールが必要な修復でも維持されます。削除する前に、これらのロールの機能を継続する必要が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-east-2 でのアクション
111111111111	管理者	保持されたロールを削除する	なし

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

保持している KMS キーを削除するようにスケジュールする

管理とメンバーのスタックはどちらも KMS キーを作成して保持します。これらのキーを保管すると料金が発生します。

これらのキーは、このソリューションによって暗号化されたすべてのリソースにアクセスできるように保持されます。削除をスケジュールする前に、それらが不要であることを確認してください。

このソリューションで作成されたエイリアスまたは CloudFormation の履歴から、この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。削除するように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-east-2 でのアクション
111111111111	管理者	削除用の管理者キーを特定してスケジュールする 削除用のメンバーキーを特定してスケジュールする	削除用のメンバーキーを特定してスケジュールする
222222222222	メンバー	削除用のメンバーキーを特定してスケジュールする	削除用のメンバーキーを特定してスケジュールする

セルフマネージド StackSets アクセス許可用のスタックを削除する

セルフマネージド StackSets アクセス許可用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-east-2 でのアクション
111111111111	管理者	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

デベロッパーガイド

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 リポジトリにアクセスして、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、カスタマイズした上で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」、「AWS Foundational Security Best Practices (FSBP) v.1.0.0」、「Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1」、「National Institute of Standards and Technology (NIST)」の一部として定義されているセキュリティ基準のプレイブックの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は、それらのコントロールはすべての基準でサポートされます。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基準でサポートされます。

> **重要**
> サービスクォータに達しないように、有効な基準のプレイブックのみをデプロイしてください。

特定の修復の詳細については、アカウントにこのソリューションによってデプロイされた名前を持つ 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**] を選択してください。

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	セキュリティコントロール ID
修復の総計	60	33	27	31	61	81
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します。	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	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します。	CloudTrail.1	2.1	CloudTrail.2	3.1	CloudTrail.1	CloudTrail.1
ASR-EnableEncryption CloudTrail は、保管時の暗号化を有効にします。	CloudTrail.2	2.7	CloudTrail.1	3.7	CloudTrail.2	CloudTrail.2
ASR-EnableLogFileValidation CloudTrail ログファイルの整合性検証が有効になっていることを確認します。	CloudTrail.4	2.2	CloudTrail.3	3.2	CloudTrail.4	CloudTrail.4
ASR-EnableCloudTrailToCloudWatchLogging CloudTrail の追跡が 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
ASR-ReplaceCodeBuildClearTextCredentials CodeBuild プロジェクトの環境変数に平文の認証情報を含ませません。	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	Config.1
ASR-MakeEBSSnapshotsPrivate Amazon EBS のスナップショットをパブリックで復元可能にしません。	EC2.1		EC2.1		EC2.1	EC2.1
ASR-RemoveVPCDefaultSecurityGroupRules VPC のデフォルトセキュリティグループでインバウンドとアウトバウンドのトラフィックを禁止します。	EC2.2	4.3	EC2.2	5.3	EC2.2	EC2.2
ASR-EnableVPCFlowLogs VPC フローログをすべての VPC で有効にします。	EC2.6	2.9	EC2.6	3.9	EC2.6	EC2.6
ASR-EnableEbsEncryptionByDefault EBS の暗号化をデフォルトで有効にします。	EC2.7	2.2.1			EC2.7	EC2.7
ASR-RevokeUnrotatedKeys ユーザーのアクセスキーを 90 日以内でローテーションさせます。	IAM.3	1.4		1.14	IAM.3	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	IAM.7
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
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		IAM.22
ASR-RemoveLambdaPublicAccess Lambda 関数のパブリックアクセスを禁止します。	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	セキュリティコントロール ID
ASR-MakeRDSSnapshotPrivate RDS スナップショットのパブリックアクセスを禁止します。	RDS.1		RDS.1		RDS.1	RDS.1
ASR-DisablePublicAccessToRDSInstance RDS の DB インスタンスのパブリックアクセスを禁止します。	RDS.2		RDS.2		RDS.2	RDS.2
ASR-EncryptRDSSnapshot RDS のクラススナップショットとデータベーススナップショットを保管時に暗号化します。	RDS.4				RDS.4	RDS.4
ASR-EnableMultiAZOnRDSInstance RDS の DB インスタンスを複数のアベイラビリティーゾーンに設定します。	RDS.5				RDS.5	RDS.5
ASR-EnableEnhancedMonitoringOnRDSInstance 拡張モニタリングを RDS の DB インスタンスとクラスターに設定します。	RDS.6				RDS.6	RDS.6
ASR-EnableRDSClusterDeletionProtection RDS クラスターの削除保護を有効にします。	RDS.7				RDS.7	RDS.7
ASR-EnableRDSInstanceDeletionProtection RDS の DB インスタンスの削除保護を有効します。	RDS.8				RDS.8	RDS.8
ASR-EnableMinorVersionUpgradDSDBInstance RDS の自動マイナーバージョンアップグレードを有効にします。	RDS.13				RDS.13	RDS.13
ASR-EnableCopyTagsToSnapshotOnRDSCluster RDS DB クラスターのタグをスナップショットにコピーするよう設定します。	RDS.16				RDS.16	RDS.16
ASR-DisablePublicAccessToRedshiftCluster Amazon Redshift クラスターのパブリックアクセスを禁止します。	Redshift.1		Redshift.1		Redshift.1	Redshift.1
ASR-EnableAutomaticSnapshotsOnRedshiftCluster Amazon Redshift クラスターの自動スナップショットを有効にします。	Redshift.3				Redshift.3	Redshift.3
ASR-EnableRedshiftClusterAuditLogging Amazon Redshift クラスターの監査ログを有効にします。	Redshift.4				Redshift.4	Redshift.4
ASR-EnableAutomaticVersionUpgradeOnRedshiftCluster Amazon Redshift のメジャーバージョンへの自動アップグレードを有効にします。	Redshift.6				Redshift.6	Redshift.6
ASR-ConfigureS3PublicAccessBlock S3 のパブリックアクセスをブロックする設定を有効にします。	S3.1	2.3	S3.6	2.1.5.1	S3.1	S3.1
ASR-ConfigureS3BucketPublicAccessBlock S3 バケットのパブリックの読み取りアクセスを禁止します。	S3.2		S3.2	2.1.5.2	S3.2	S3.2
ASR-ConfigureS3BucketPublicAccessBlock		S3.3				S3.3

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	セキュリティコントロール ID
S3 バケットのパブリックの書き込みアクセスを禁止します。						
ASR-EnableDefaultEncryptionS3 S3 バケットのサーバーサイドの暗号化を有効にします。	S3.4		S3.4	2.1.1	S3.4	S3.4
ASR-SetSSLBucketPolicy S3 バケットは、リクエストに SSL を利用することを要求します。	S3.5		S3.5	2.1.2	S3.5	S3.5
ASR-S3BlockDenylist バケットポリシーで他の AWS アカウントに付与される Amazon S3 のアクセス許可を制限します。	S3.6				S3.6	S3.6
S3 の Block Public Access 設定をバケットレベルで有効にします。	S3.8				S3.8	S3.8
ASR-ConfigureS3BucketPublicAccessBlock CloudTrail のログ用の S3 バケットがパブリックにアクセスできないようにします。		2.3				CloudTrail.6
ASR-CreateAccessLoggingBucket CloudTrail で、S3 バケットのアクセスログが有効になっていることを確認します。		2.6				CloudTrail.7
ASR-EnableKeyRotation ユーザーが作成したカスタマーマネージドキー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	KMS.4
ASR-CreateLogMetricFilterAndAlarm 不正な API コールに関するログメトリクスのフィルタとアラームが存在することを確認します。		3.1		4.1		Cloudwatch.1
ASR-CreateLogMetricFilterAndAlarm MFA を使用しない AWS マネジメントコンソールへのサインインに関するログメトリクスのフィルタとアラームが存在することを確認します。		3.2		4.2		Cloudwatch.2
ASR-CreateLogMetricFilterAndAlarm ルートユーザーの使用に関するログメトリクスのフィルタ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
ASR-CreateLogMetricFilterAndAlarm IAM ポリシーの変更に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.4		4.4		Cloudwatch.4
ASR-CreateLogMetricFilterAndAlarm CloudTrail の設定変更に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.5		4.5		Cloudwatch.5
ASR-CreateLogMetricFilterAndAlarm AWS マネジメントコンソールの認証の失敗に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.6		4.6		Cloudwatch.6
ASR-CreateLogMetricFilterAndAlarm ユーザーが作成したカスタマーマネージドキーを無効にしたり、		3.7		4.7		Cloudwatch.7

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	セキュリティコントロール ID
定期的に削除したりするためのログメトリックスフィルターとアラームが存在することを確認してください。						
ASR-CreateLogMetricFilterAndAlarm S3 バケットのポリシー変更に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.8		4.8		Cloudwatch.8
ASR-CreateLogMetricFilterAndAlarm AWS Config の設定変更に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.9		4.9		Cloudwatch.9
ASR-CreateLogMetricFilterAndAlarm セキュリティグループの変更に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.10		4.10		Cloudwatch.10
ASR-CreateLogMetricFilterAndAlarm ネットワークアクセスコントロールリスト (NACL) の変更に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.11		4.11		Cloudwatch.11
ASR-CreateLogMetricFilterAndAlarm ネットワークゲートウェイに対する変更に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.12		4.12		Cloudwatch.12
ASR-CreateLogMetricFilterAndAlarm ルートテーブルの変更に関するログメトリックフィルタとアラームが存在することを確認します。		3.13		4.13		Cloudwatch.13
ASR-CreateLogMetricFilterAndAlarm VPC の変更に関するログメトリクスのフィルタとアラームが存在することを確認します。		3.14		4.14		Cloudwatch.14
AWS-DisablePublicAccessForSecurityGroup セキュリティグループが、0.0.0.0/0 からポート 22 へのインバウンドアクセスを許可しないことを確認します。		4.1	EC2.5		EC2.13	EC2.13
AWS-DisablePublicAccessForSecurityGroup セキュリティグループが、0.0.0.0/0 からポート 3389 へのインバウンドアクセスを許可しないことを確認します。		4.2			EC2.14	EC2.14
ASR-ConfigureSNSTopicForStack	CloudFormation.1				CloudFormation.1	CloudFormation.1
ASR-CreateIAMSupportRole		1.20		1,17		IAM.18
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るべきではありません。	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
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ギングを有効にする必要があります。	SNS.2				SNS.2	SNS.2

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	セキュリティコントロール ID
ASR-EnableEncryptionForSQSQueue	SQS.1				SQS.1	SQS.1
ASR-MakeRDSSnapshotPrivate RDS スナップショットはプライベートにする必要があります。	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ようにします。	SSM.4				SSM.4	SSM.4
ASR-EnableCloudFrontDefaultRootObject CloudFront ディストリビューションには、デフォルトのルートオブジェクトが設定されている必要があります。	CloudFront.1				CloudFront.1	CloudFront.1
ASR-SetCloudFrontOriginDomain CloudFront ディストリビューションが存在しない S3 オリジンを指定しないようにします。	CloudFront.12				CloudFront.12	CloudFront.12
ASR-RemoveCodeBuildPrivilegedMode CodeBuildプロジェクト環境にはロギング用の AWS の設定が必要です。	CodeBuild.5				CodeBuild.5	CodeBuild.5
ASR-TerminateEC2Instance 停止した EC2 インスタンスは、一定期間後に削除する必要があります。	EC2.4				EC2.4	EC2.4
ASR-EnableIMDSV2OnInstance 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	EC2.8
ASR-RevokeUnauthorizedInboudRules セキュリティグループは、許可されたポートへの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
ASR-DisableUnrestrictessToHighRiskPorts 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のアクセスを許可しません。	EC2.19				EC2.19	EC2.19
ASR-DisableTGWAutoAcceptSharedAttachments Amazon EC2 Transit Gateways が VPC アタッチメントリクエストを自動的に受け付けないようにします。	EC2.23				EC2.23	EC2.23
ASR-EnablePrivateRepositoryScanning ECR プライベートリポジトリにはイメージスキャン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
ASR-ConfigureS3BucketLogging S3 バケットサーバーアクセスロギング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が有効になっている必要があります。	S3.11				S3.11	S3.11

説明	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	セキュリティコントロール ID
ASR-SetS3LifecyclePolicy S3 バケットに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
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
ASR-DisablePublicSSMDocument SSM ドキュメントはパブリックにしないようにします。	SSM.4				SSM.4	SSM.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ために、このソリューション自体を変更する必要はありません。

> **注記**
> この後の説明では、この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のリソース名には **SHARR** や **SO0111** が含まれ、見つけやすく、識別し易いようになっています。

概要

AWS での自動化されたセキュリティ対応のランブックは、次の標準的な命名規則に従う必要があります。

```
ASR-<standard>-<version>-<control>
```

Standard: セキュリティ基準の略称です。これは SHARR がサポートするセキュリティ基準に一致する必要があります。CIS、AFSBP、PCI、NIST、または SC のいずれかでなければなりません。

Version: セキュリティ基準のバージョン。この場合も、SHARR がサポートするバージョンと検出結果データのバージョンが一致している必要があります。

Control: 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でランブックを作成します。
2. メンバーアカウントで IAM ロールを作成します。
3. (オプション) 管理者アカウントで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で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、JSON の検出結果の例を取得します。
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。**自己所有** タブで、**ドキュメント**セクションの下にある任意の ASR- ドキュメント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。ランブックをコールしたときにロールを渡すために、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で 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 ロールの **SO0111** から例を取得し、新しいロールを作成します。このロール名は `SO0111-Remediate-<standard>-<version>-<control>` で始まる必要があります。例えば、CIS v1.2.0 のコントロール 5.6 を追加する場合、このロールは `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、修復の実行するための必要な API 呼び出しのみを許可する、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の自動修復が可能になります。

ステップ 3: (オプション) 管理者アカウントで自動修復ルールを作成する

自動修復 (「自動化」ではない) とは、AWS Security Hub が検出結果を受け取るとすぐに修復を実行することです。このオプションを使用する前に、慎重にリスクを検討するようにしてください。

1. CloudWatch Events で同じセキュリティ基準のルール例を確認してください。ルールの命名規則は、`standard_control_AutoTrigger` になります。
2. 使用する例からイベントパターンをコピーします。
3. `GeneratorId` の値を、JSON の検出結果の `GeneratorId` と一致するように変更します。
4. ルールを保存して有効にします。

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のプレイブックとデプロイ用のソースコードを GitHub リポジトリからダウンロードしてください。

AWS CloudFormation のリソースは AWS CDK のコンポーネントから作成され、そのリソースには、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の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 をご参照ください。

AWS Systems Manager Parameter Store

AWS での自動化されたセキュリティ対応では、運用データの格納に AWS Systems Manager Parameter Store を使用しています。次のパラメータが Parameter Store に格納されます。

名前	値	用途
`/Solutions/SO0111/CMK_REMEDIATION_ARN`	FSBP の修復でデータを暗号化する AWS KMS key	修復の一環として、CloudTrail ログなどのユーザーデータを暗号化します。
`/Solutions/SO0111/CMK_ARN`	SHARR がデータの暗号化に使用する AWS KMS key	ソリューションのデータを暗号化します。
`/Solutions/SO0111/SNS_Topic_ARN`	このソリューションの Amazon SNS トピックの ARN	修復イベントを通知します。
`/Solutions/SO0111/SNS_Topic_Config.1`	AWS Config の更新に関する SNS トピック	Config.1 の修復
`/Solutions/SO0111/sendAnonymousMetrics`	`Yes`	匿名化されたメトリクスの収集
`/Solutions/SO0111/version`	このソリューションのバージョン	

名前	値	用途
/Solutions/SO0111/*<security standard long name>*/*<version>*/status	enabled	セキュリティ基準がこのソリューションで有効かどうかを示します。これを disabled に変更すると、自動修復に関するセキュリティ基準を無効にできます。
/Solutions/SO0111/*<security standard long name>*/shortname	String	セキュリティ基準の略称。 (例: CIS、AFSBP、PCI)
/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している場合は、これらのパラメータによって再分類が行われます。

Amazon SNS トピック - 修復の進捗状況

AWS での自動化されたセキュリティ対応では、Amazon SNS トピック (SO0111-SHARR_Topic) が作成されます。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します。このトピックに送信される可能性のある通知は、次の 3 つになります。

```
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。修復がエラーなしで完了したことを示していますが、修復を成功させるための決定的なテストは、AWS Config のチェックまたは手動検証になります。

SNS トピックのサブスクリプションをフィルタリングする

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」のスコープを選択します。
5. JSON エディターにポリシーを追加します。
6. 変更を保存します。

サンプルポリシー:

アカウントでフィルター

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

エラーのフィルター

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

コントロールでフィルター

```
    {
        "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の投稿に使用されます。

ALARM 状態になったアラームの詳細は、このトピックに送信されます。

Config の検出結果に関するランブックを開始する

このソリューションでは、カスタム AWS Config 検出結果に基づいてランブックを開始できます。そのためには、次のことを行う必要があります。

1. 修復したい AWS Config ルール名を見つけます。これは、AWS Config または Security Hub がこのルール用に生成した検出結果のいずれかにあります。
2. AWS Systems Manager のパラメータストアに移動して、[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`* になります。
4. 値は次のような形式に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、この Config ルールを修復する際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ありません。省略した場合、オーケストレータ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。

参照資料

このセクションには、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、関連リソースへのポインタ、このソリューションに貢献したビルダーのリストに関する情報が含まれています。

匿名化されたデータの収集

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。AWS ではこのデータを使用して、ユーザーがこのソリューション、関連サービスおよび製品をどのように使用しているかをよりよく理解し、提供するサービスや製品の改善に役立てます。有効にすると、次の情報が収集され、AWS に送信されます。

- **Solution ID** - AWS ソリューションの識別子
- **Unique ID (UUID)** - AWS Security Hub の対応と修復のデプロイごとにランダムに生成された一意の識別子
- **Timestamp** - データ収集タイムスタンプ
- **Instance Data** - このスタックのデプロイに関する情報
- **CloudWatchMetricsDashboardEnabled** - 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は、Yes。
- **Status** - デプロイのステータス (ソリューションの成功または失敗) または (修復の成功または失敗)
- **Error message** - ステータスのフィールドに表示される一般的なエラーメッセージ
- **Generator_id** - Security Hub のルール情報
- **Type** - 修復のタイプと名前
- **productArn** - Security Hub がデプロイされているリージョン
- **finding_triggered_by** - 実行される修復のタイプ (カスタムアクションまたは自動トリガー)

AWS は、このアンケートを通じて収集されたデータを所有します。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、次の手順を実施してください。

1. AWS CloudFormation テンプレートをローカルの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 テンプレートのマッピングセクションを次のように変更します。

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

を次に変更します。

```
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、[**ファイルの選択**] を選択し、ローカルドライブから編集したテンプレートを選択します。
8. [**次へ**] を選択し、このガイドの「自動デプロイ」セクションの「スタックの起動」の手順に従います。

関連リソース

- AWS Security Hub による自動対応と修復
- CIS Amazon Web Services Foundations benchmarks, version 1.2.0
- AWS Foundational Security Best Practices 標準
- Payment Card Industry Data Security Standard (PCI DSS)
- National Institute of Standards and Technology (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

改訂

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。
2020 年 11 月	中国リージョンのデプロイ手順を追加。Security Hub の管理者アカウント用のソリューションのデプロイ手順を更新。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のアーキテクチャと新しい FSBP の修復を追加。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 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。CIS v1.2.0 に 17 の新しい修復を追加。FSBP に 4 つの新しい修復を追加。SSM のランブックに基づく新しいプレイブックのアーキテクチャを使用するように CIS を変換。既存のプレイブックをユーザー定義の修復で拡張する手順を追加。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 9 月	リリース v1.3.1: CreateLogMetricFilterAndAlarm.py を変更して、アクションを有効にするように変更し、SNS 通知を SO0111-SHARR-LocalAlarmNotification に追加。CIS 2.8 の修復を新しい検出結果のデータ形式に一致するように変更。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 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 を使用してこのソリューションが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、クロスリージョンの修復もサポートしています。スタックが削除されてもメンバーアカウントの IAM ロールは保持されます。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。
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: その他の修正。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。
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 に切り替えるように変更。SSM ドキュメント名のプレフィックスを SHARR ではなく ASR で始まるように更新。詳細に

日付	変更
	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。
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 基準のサポート、FSBP 基準に対する 5 つの新しい修復、CIS v1.2.0 基準に対する 1 つの新しい修復、サービスカタログの AppRegistry の統合、および 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保護機能を追加。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。
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。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。
2023 年 5 月	Well-Architected 定義の更新、各スタックをデプロイする場所に関するガイダンスの追加、特定の修復を含む問題のトラブルシューティング版の追加、および SNS 通知のコード例を更新。
2023 年 7 月	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。
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。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。
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の確認」を追加。
2024 年 3 月	リリース 2.1.0: NIST 基準サポートの追加、FSBP 基準に 17 の新しい修正を追加、モニタリングソリューション用の CloudWatch ダッシュボードの追加、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、および Config の検出結果を修正するためのサポートを追加。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。
2024 年 4 月	リリース 2.1.1: CloudFormation パラメータの順番とデフォルト値の更新。ドキュメンテーションの更新: NIST 基準へのリファレンスを追加。EventBridge ルールのサービスクォータに関する情報を追加。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。

注意

お客様は、この文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。このドキュメントは、(a) 情報提供のみを目的としており、(b) AWS の現行製品とプラクティスを表したものであり、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義務や確約を意味するものではありません。AWS の製品やサービスは、明示または暗示を問わず、いかなる保証、表明、条件を伴うことなく「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 での自動化されたセキュリティ対応ソリューションは、Apache Software Foundation で閲覧可能な Apache ライセンスバージョン 2.0 の条項に基づいてライセンスされています。