AWS Firewall Manager のオートメーション

2020 年 *9* 月発行 *(*最終更新日 *2021* 年 *8* 月*)*

目次

はじめに

「AWS Firewall Manager のオートメーション」ソリューションを使用すると、AWS Organizations のアカウントとアプリケーションに対するファイアウォールルールを一元的に設定、管理、および監査するのに役立ちます。このソリューションでは AWS Firewall Manager を使用して、AWS Web Application Firewall (WAF) の一連のマネージドルールのセットを自動的にデプロイし、すべての該当する AWS アカウントに対して Amazon VPC セキュリティグループの監査チェックを行います。また、AWS Shield Advanced のユーザー向けに、分散サービス妨害 (DDoS) 保護をすべてのアカウントにデプロイするオプションも提供します。

AWS Firewall Manager でポリシーを定義してルールセットを設定するプロセスは、複雑で時間がかかる場合があります。このプロセスをシンプルにするために、このソリューションは AWS のマネージドファイアウォールのルールとセキュリティグループの監査チェックのセットをデプロイします。マネージドファイアウォールのルールは、Amazon CloudFront、Application Load Balancer、Amazon API Gateway で実行しているウェブアプリケーションを保護するために事前設定されている一連のルールです。セキュリティグループの監査チェックは、過度に許容的なセキュリティグループのルールを継続的にモニタリングおよび検出し、Amazon VPC のリソースを保護してファイアウォールの体制を強化します。

このソリューションは、AWS Firewall Manager のオンボーディングプロセスを自動化し、AWS Organizations アカウント内の特定の組織単位 (OU)、AWS リージョン、またはタグ付けされたリソースに対するポリシーを制限することで、AWS Organizations のベースラインルールと監査チェックを設定します。インストールされている AWS Systems Manager Parameter Store のパラメータを変更すると、このソリューションはポリシーを更新し、指定されたリソースにデプロイします。

このソリューションには、AWS CloudFormation の補足テンプレートも含まれています。このテンプレートを AWS Organizations の管理アカウントにデプロイすると、このソリューションは、AWS Organizations のすべての機能がアクティブになっていることを確認したり、アカウントを AWS Firewall Manager の管理者アカウントとして指定したりするなど、前提条件の設定を自動化します。このテンプレートでは、オプションで、組織全体で AWS Config を有効にするなどの前提条件の設定を

自動化することもできます。この補足テンプレートを使用して、このソリューションをプライマリアカウントにインストールすることもできます。

この実装ガイドでは、「AWS Firewall Manager のオートメーション」ソリューションをアマゾン ウェブ サービス (AWS) クラウド内にデプロイするためのアーキテクチャに関する考慮事項と設定手順について説明します。このガイドには、セキュリティと可用性に関する AWS のベストプラクティスを使用してこのソリューションをデプロイするために必要な AWS のサービスを起動および設定する 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 クラウド内でのアーキテクチャの設計経験がある IT 管理者や DevOps プロフェッショナルを対象としています。

コスト

このソリューションの実行中に使用した AWS のサービスのコストは、お客様の負担となります。このソリューションを実行する合計コストは、インストールしたポリシーの数、インストールしたルールセットとウェブ ACL の数、AWS Lambda 関数の数と実行時間、発行した Amazon EventBridge イベントの数によって異なります。

料金は変わる場合があります。詳細については、このソリューションで使用する AWS のサービス別の料金ウェブページを参照してください。

各ポリシーのコストは、**AWS リージョンごとのポリシーにつき 1 か月あたり 100 USD** です。例えば、2 つの Amazon CloudFront のグローバルポリシーと 1 つの AWS リージョンのポリシーの場合、ポリシーの合計コストは 3 つのポリシー x 100 USD = 300 USD / 月になります。このソリューションを実行する合計コストに影響する重要な要因は、管理するアカウントの数とインストールするポリシーの数です。2021 年 8 月時点で、米国東部 (バージニア北部) リージョンの小規模な組織でこのソリューションを実行するコストは、**1 か月あたり約 1,433.00 USD** です。

小規模な組織の月額コスト

前提:

- アカウント: 2 つの組織単位 (OU) で 12 個のアカウント
- AWS リージョンの数: 3
- AWS Shield Advanced のサブスクリプション: なし
- ポリシーの数: 13
  - Amazon CloudFront のグローバルポリシー: AWS WAF のグローバルポリシー (100 USD × 1 グローバルポリシー)
  - リージョンポリシー:
    - AWS WAF のリージョンポリシー (100 USD x 3 リージョン)
    - コンテンツ監査セキュリティグループポリシー (100 USD × 3 リージョン)
    - 使用状況監査セキュリティグループポリシー (100 USD x 3 リージョン)
    - Amazon Route 53 Resolver DNS Firewall ポリシー (100 USD x 3 リージョン)

AWS のサービス	コンポーネント	数量	アカウント	USD/月	月額合計
AWS Firewall Manager	ポリシー	13	該当なし	100.00 USD	**1,300.00 USD**
	AWS WAF ウェブ ACL	4	12	5.00 USD	**240.00 USD**
	AWS WAF ルール	4*4	12	1.00 USD	**192.00 USD**
その他のサービス*	該当なし	該当なし	12	1.00 USD 未満	**1.00 USD**
				合計:	**1,733.00 USD**

*** 注意:** その他の AWS のサービスには、AWS Lambda、AWS EventBridge、AWS CloudFormation StackSets、AWS Config、Amazon Route 53 Resolver DNS Firewall、AWS Systems Manager Parameter Store が含まれます。

大規模な組織の月額コスト

前提:

- アカウント: 20 個の OU 全体で 150 個のアカウント
- AWS リージョンの数: 10
- AWS Shield Advanced のサブスクリプション: なし
- ポリシーの数: 41
  - グローバルポリシー: AWS WAF のグローバルポリシー (100 USD × 1 グローバルポリシー)
  - リージョンポリシー:
    - AWS WAF のリージョンポリシー (100 USD x 10 AWS リージョン)
    - コンテンツ監査セキュリティグループポリシー (100 USD × 10 リージョン)
    - 使用状況監査セキュリティグループポリシー (100 USD x 10 リージョン)
    - Amazon Route 53 Resolver DNS Firewall ポリシー (100 USD x 10 リージョン)

AWS のサービス	コンポーネント	数量	アカウント	USD/月	月額合計
AWS Firewall Manager	ポリシー	41	該当なし	100.00 USD	**4,100.00 USD**
	AWS WAF ウェブ ACL	11	150	5.00 USD	**8,250.00 USD**
	AWS WAF ルール	4 x 11	150	1.00 USD	**6,600.00 USD**
その他のサービス*	該当なし	該当なし	150	1.00 USD 未満	**1.00 USD**
				合計:	**18, 951.00 USD**

*** 注意:** その他の AWS のサービスには、AWS Lambda、AWS EventBridge、AWS CloudFormation StackSets、AWS Config、Amazon Route 53 Resolver DNS Firewall、AWS Systems Manager Parameter Store が含まれます。

テーブルのコスト見積もりには、AWS Shield Advanced のサブスクリプションは含まれていません。AWS Shield Advanced のサブスクリプションには、AWS WAF 保護ポリシーのコストと、AWS WAF ウェブ ACL およびルールのコストが含まれます。詳細については、「AWS Firewall Manager の料金」ページを参照してください。

料金は変わる場合があります。詳細については、このソリューションで使用する AWS のサービスごとの料金ウェブページを参照してください。

アーキテクチャの概要

このソリューションをデフォルトのパラメータを使用してデプロイすると、AWS クラウド内に次の環境が構築されます。

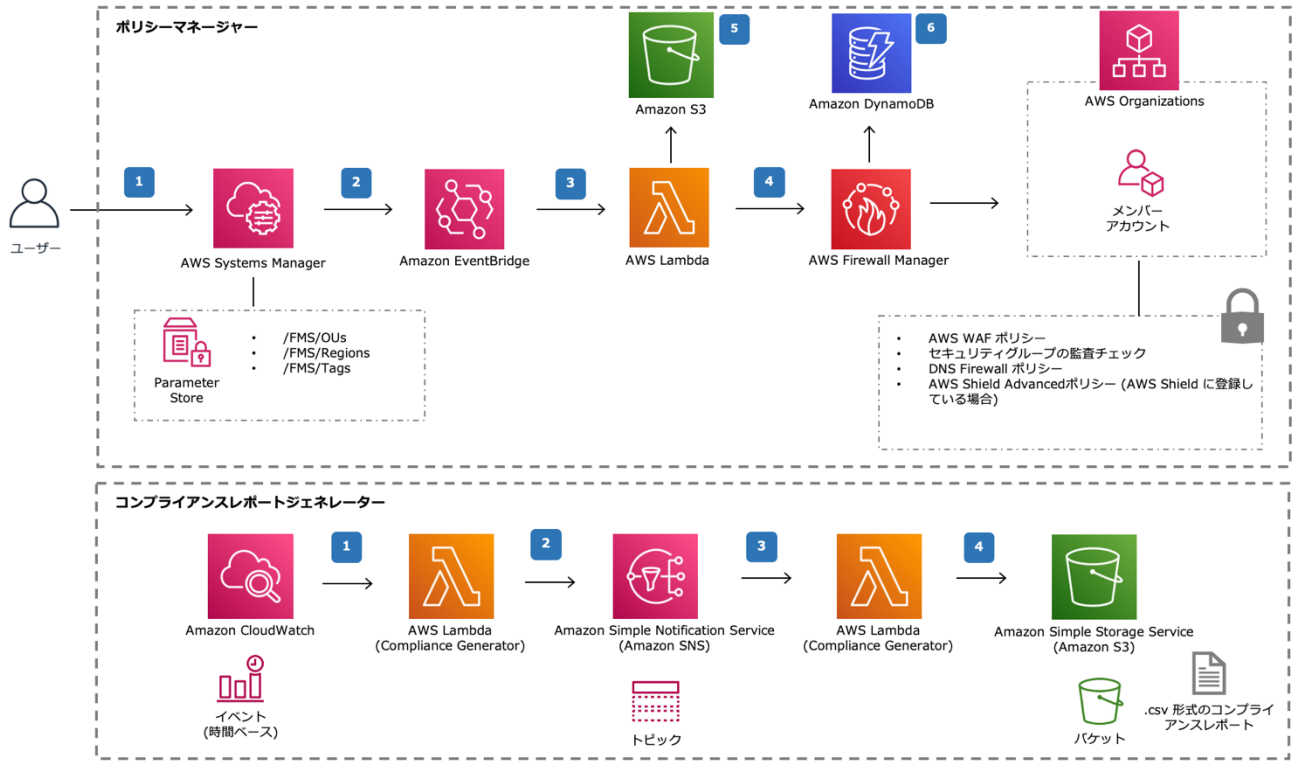

図 *1:*「*AWS Firewall Manager* のオートメーション」ソリューションのアーキテクチャ

このアーキテクチャは、ポリシーマネージャーとコンプライアンスレポートジェネレーターという 2 つの別個のワークフローにグループ化されています。

ポリシーマネージャー

AWS CloudFormation テンプレートをデプロイすると、3 つのパラメータを持つ AWS Systems Manager Parameter Store が作成され、各パラメータにはデフォルト値が設定されます。作成されるパラメータは、/FMS/OUs、/FMS/Regions、/FMS/Tags です。

1. これらのパラメータは、AWS Systems Manager を使用して更新できます。
    - /FMS/OUs パラメータでは、組織単位 ID を追加して、ポリシーとルールセットを複数の OU に適用します。
    - /FMS/Regions パラメータでは、AWS リージョン名を指定します。
    - /FMS/Tags パラメータでは、包含タグと除外タグを作成してアカウント内の特定のリソースに追加し、ポリシーやルールセットを適用するリソースと適用しないリソースを区別します。AWS System Manager Parameter Store のパラメータの設定については、「AWS Systems Manager のパラメータ設定用のシナリオ」を参照してください。
2. Amazon EventBridge ルールは、イベントパターンを使用して AWS System Manager Parameter Store の更新イベントをキャプチャします。
3. Amazon EventBridge ルールは AWS Lambda 関数を呼び出します。
4. この AWS Lambda 関数は、事前定義された AWS Firewall Manager のセキュリティポリシーのセットをユーザーが指定したすべての OU にインストールします。このポリシーには、AWS マネージドルールのセットで構成される AWS WAF ウェブ ACL と Amazon VPC のセキュリティグループの監査ポリシーが含まれます。さらに、AWS Shield Advanced のサブスクリプションを利用している場合は、このソリューションは AWS Shield Advanced のポリシーをデプロイして分散型サービス拒否 (DDoS) 攻撃から保護します。
5. AWS Lambda の `PolicyManager` 関数は、Amazon S3 バケットからこのポリシーのマニフェストファイルを取得し、このマニフェストファイルを使用して AWS Firewall Manager のセキュリティポリシーを作成します。
6. AWS Lambda は、ポリシーのメタデータを Amazon DynamoDB のテーブル内に保存します。

インストールされているポリシーとルールセットの詳細なリスト、推奨されるポリシーのデフォルトの結果、それらの格納場所については、「AWS System Manager のパラメータ設定用のシナリオ」を参照してください。

コンプライアンスレポートジェネレーター

AWS CloudFormation のスタックをデプロイすると、時間ベースの Amazon EventBridge ルール、AWS Lambda 関数、Amazon SNS トピック、Amazon S3 バケットが作成されます。

1. 時間ベースの Amazon EventBridge ルールは、AWS Lambda の `ComplianceGenerator` 関数を呼び出します。
2. AWS Lambda の `ComplianceGenerator` 関数は、各 AWS リージョンで AWS Firewall Manager のポリシーを取得し、ポリシー ID のリストを Amazon SNS トピックに発行します。
3. Amazon SNS トピックは、ペイロード `{PolicyId: string, Region: string}` を使用して AWS Lambda の `ComplianceGenerator` 関数を呼び出します。
4. コンプライアンスジェネレーターは、ポリシーごとにコンプライアンスレポートを生成し、そのレポートを CSV 形式で Amazon S3 バケットにアップロードします。

ソリューションのコンポーネント

AWS Lambda 関数

このソリューションは、AWS Lambda 関数を使用して、AWS Firewall Manager の前提条件チェックと、組織単位 (OU) のポリシーおよびルールセットのインストールをトリガーします。

このソリューションでは次の AWS Lambda 関数を使用します。

- **PreReqManager** ― この AWS Lambda 関数は次をチェックして検証します。
  - 前提条件スタックが AWS Organizations のプライマリアカウントにデプロイされている
  - AWS Organizations のすべての機能のオプションがアクティブになっている

- AWS Firewall Manager の管理者機能が設定されている
- 信頼されたアクセスが AWS Organizations と AWS CloudFormation StackSets との間でアクティブになっている
- AWS Config が AWS Organizations のすべてのメンバーアカウントに対してアクティブになっている

この AWS Lambda 関数のログ情報は、Amazon CloudWatch コンソールの CloudWatch Logs で、次のロググループからアクセスできます。

`/aws/lambda/<Stack-Name>-xxx-PreReqManager-xxx`

- **PolicyManager** ― この AWS Lambda 関数は、ポリシーの作成、更新、削除など、AWS Firewall Manager のポリシーの管理を担当します。この AWS Lambda 関数は、Amazon S3 バケットからポリシーのマニフェストファイルを取得し、このファイルを使用して AWS Firewall Manager のセキュリティポリシーを作成します。このマニフェストファイルは、ポリシー設定の要件に応じていつでも変更できます。ポリシーのマニフェストファイルの変更は、次回のポリシーの更新イベントで反映されます。また、この関数はポリシーのメタデータを Amazon DynamoDB のテーブル内に保存します。

  この AWS Lambda 関数のログ情報は、Amazon CloudWatch コンソールの CloudWatch Logs で、次のロググループからアクセスできます。

  `/aws/lambda/<Stack-Name>-xxx-PolicyManager-xxx`

- **ComplianceGenerator** ― この AWS Lambda 関数は、監査用のコンプライアンスレポートを生成します。このレポートは CSV 形式で生成され、Amazon S3 バケットに一時的に保存されます。

  この AWS Lambda 関数のログ情報は、Amazon CloudWatch コンソールの CloudWatch Logs で、次のロググループからアクセスできます。

  `/aws/lambda/<Stack-Name>-xxx-ComplianceGenerator-xxx`

AWS CloudFormation StackSets

このソリューションでは、サービスマネージド型の AWS CloudFormation StackSets でサービスマネージド型のアクセス許可を使用して、組織全体で AWS Config を有効にします。

> **注意**: AWS Config を有効にするのにかかる時間は、対象となるメンバーアカウントと AWS リージョンの数によって異なります。例えば、テストでは、2 つの OU で 6 つのアカウントと 16 の AWS リージョンで AWS Config を有効にするのに約 90 分かかりました。

AWS Firewall Manager の統合

このソリューションは、AWS Firewall Manager のポリシーとルールセットを自動的にインストールします。デフォルトでは、AWS WAF、セキュリティグループ、Amazon Route 53 Resolver DNS Firewall のセキュリティポリシーがインストールされます。さらに、AWS Shield Advanced のサブスクリプションを利用している場合は、AWS Shield のポリシーもインストールされます。

AWS Firewall Manager のポリシーは、AWS WAF と AWS Shield Advanced のポリシーに対してアクティブ化された自動修復を使用して設定されます。ポリシーのデプロイまたはこのソリューションの他の部分をカスタマイズする場合は、GitHub リポジトリの README.md ファイルを参照してください。

AWS Systems Manager Parameter Store

AWS Systems Manager Parameter Store は、このソリューションの設定パラメータを保存します。これらのパラメータを使用して OU、AWS リージョン、タグを指定できます。AWS Systems Manager Parameter Store のパラメータを使用すると、ポリシーとルールセットを複数の OU や AWS リージョンに簡単に拡張できます。また、これらのパラメータを使用して包含タグと除外タグを指定し、これらのタグをアカウント内の特定のリソースに適用することもできます。

さらに、管理者は一元化された場所でこのソリューションのパラメータを表示および変更できます。パラメータ値を追加、編集、削除することで、OU、AWS リージョン、タグ全体にわたって選択内容を変更できます。対応する AWS Firewall Manager のポリシーは、自動的に更新されます。

Amazon EventBridge

AWS Systems Manager Parameter Store で OU、AWS リージョン、タグが更新されると、このソリューションは Amazon EventBridge のルールを使用して AWS Lambda 関数を呼び出します。AWS

Lambda 関数がトリガーされると、ポリシーとルールセットが (ユーザーが更新した) OU と AWS リージョンにインストールされます。

Amazon Simple Storage Service

このソリューションは、アカウントに 2 つの Amazon S3 バケットを作成します。1 つのバケットは、ポリシーのマニフェストファイルをステージングするのに使用し、もう 1 つのバケットは、AWS Lambda の `ComplianceGenerator` 関数でコンプライアンスレポートを保存するのに使用します。

Amazon DynamoDB

このソリューションでは、AWS Firewall Manager のポリシーから作成したメタデータを Amazon DynamoDB に保存します。このメタデータは、指定した OU や AWS リージョン全体でポリシーを更新および削除するために使用します。AWS Firewall Manager のポリシーからメタデータのサンプルを次に示します。

```
{
"LastUpdatedAt": "2020-09-10T19:18:33.719Z",
"PolicyId": "abcd1234-ab12-cd34-b99b-ab01cde2fg34",
"PolicyName": "FMS-Shield-01",
"PolicyUpdateToken": "1:AbCde1fGH2iJKLM34nO5PQ==",
"Region": "Global"
}
```

重要：このテーブルは削除しないでください。このテーブルは、ポリシーに対する作成、更新、削除のアクションを実行するために使用します。

設計に関する考慮事項

デプロイ

AWS Organizations と AWS Firewall Manager はグローバルに利用できる AWS のサービスですが、どちらも `us-east-1` をデータプレーンとして使用しています。そのため、これらの AWS サービスのサービスクライアントは `us-east-1` のエンドポイントで作成する必要があります。別の AWS リー

ジョンにデプロイすることはできますが、AWS リージョン外へのトラフィック送信を制限する AWS Organizations のサービスコントロールポリシーやカスタマイズされたファイアウォールルールがある場合に、これらの API は失敗します。制限を設定している場合は、`us-east-1` の AWS リージョンにこのソリューションをデプロイすることをお勧めします。

ソリューションのアンインストール

このソリューションをアンインストールする前に、AWS Systems Manager Parameter Store に移動し、/FMS/OUs パラメータを delete に更新することをお勧めします。これにより、スタックの削除に先立って AWS Firewall Manager のセキュリティポリシーが削除されます。このソリューションによってデプロイされた他のすべてのリソースは、スタックを削除すると自動的に削除されます。カスタム定義のルールのみが自動的に削除されることはありません。詳細については、「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。

AWS CloudFormation テンプレート

このソリューションでは、AWS CloudFormation を使用して、AWS クラウドでの「AWS Firewall Manager のオートメーション」ソリューションのデプロイを自動化します。このソリューションには次の AWS CloudFormation テンプレートが含まれており、デプロイ前にダウンロードできます。

テンプレートを表示

aws-fms-automations.template: このテンプレートを使用して、ソリューションとすべての関連コンポーネントを起動します。デフォルト設定では、AWS Lambda 関数、Amazon EventBridge、AWS Systems Manager Parameter Store、Amazon DynamoDB、Amazon S3 バケット、AWS Firewall Manager のポリシーをデプロイします。

自動デプロイ

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、設定、セキュリティ、その他の考慮事項を確認して、ニーズに最適なインストール方法を判断してください。このセクションの手順に従い、AWS アカウントにソリューションを設定してデプロイします。

デプロイ所要時間: 約 3 分

前提条件

AWS Firewall Manager を AWS Organizations のプライマリアカウントに設定していない場合は、最初にこのソリューションの前提条件テンプレートをデプロイする必要があります。このテンプレートは、事前に、AWS Organizations のすべての機能オプションをアクティブにしてから、AWS Organizations の管理アカウントにデプロイする必要があります。

AWS Firewall Manager が AWS Organizations の管理アカウントに設定済みである場合は、前提条件テンプレートのインストールをスキップして「デプロイの概要」に進み、`aws-fms-automations` テンプレートを指定先の AWS Firewall Manager の管理者アカウントにインストールできます。

> **注意**: 前提条件テンプレートをインストールする場合は、組織内の別のアカウントを AWS Firewall Manager の管理者アカウントとして指定するオプションがあります。このオプションを選択した場合は、AWS Organizations の管理アカウントに前提条件テンプレートをインストールした後で、指定したアカウントに `aws-fms-automations` テンプレートを手動でインストールする必要があります。

詳細については、「前提条件テンプレートのインストール」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。手順の詳細については、各ステップのリンクを参照してください。

ステップ 1. スタックの起動

ステップ 2. FMS ポリシーの追加と管理

ステップ 1. スタックの起動

この自動化された AWS CloudFormation テンプレートは、AWS クラウドに「AWS Firewall Manager Automations for AWS Organizations」ソリューションをデプロイします。スタックを起動する前に、AWS Firewall Manager と AWS Organizations をアカウントに設定しておく必要があります（これらのサービスを設定する方法については、「前提条件」を参照してください）。

1. AWS マネジメントコンソールにサインインし、右側のボタンを使用して、`aws-fms-automations` AWS CloudFormation テンプレートを起動します。あるいは、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。

ソリューションの起動

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）リージョンで起動します。このソリューションを別の AWS リージョンで起動するには、コンソールのナビゲーションバーにあるリージョンセレクターを使用してください。
3. **スタックの作成**ページで、正しいテンプレート URL が **Amazon S3 URL** テキストボックスに表示されていることを確認し、[**次へ**] を選択します。
4. **スタックの詳細を指定**ページで、ソリューションスタックに名前を付け、*Compliance Reporting* パラメータの値を指定して [**次へ**] を選択します。

パラメータ	デフォルト	説明
Compliance Reporting	`Yes`	AWS Firewall Manager のセキュリティポリシーのコンプライアンスレポートを生成するかどうかを `Yes` または `No` で指定します。

5. **スタックオプションの設定**ページで、[**次へ**] を選択します。
6. **レビュー**ページで、設定を見直して確認します。テンプレートで AWS Identity and Access Management (IAM) リソースを作成することを確認するチェックボックスをオンにします。
7. [**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 3 分で CREATE_COMPLETE ステータスが表示されます。

ステップ 2. FMS ポリシーの追加と管理

ビジネスニーズに合わせて、FMS ポリシーを複数の OU や AWS リージョンに追加できます。AWS Systems Manager のパラメータを使用すると、ポリシーを作成または削除する AWS リージョンや OU を管理したり、Tag パラメータを使用してスコープ内のリソースを管理したりできます。各パラメータを更新するには、次の手順に従います。

1. AWS Systems Manager コンソールにサインインします。
2. 左側のメニューペインにある**アプリケーション管理**で、[**パラメータストア**] を選択します。
3. 更新するパラメータを選択し、[**編集**] を選択します。
4. 値を更新します。
5. [**変更を保存**] を選択します。

これらのパラメータは、ユースケースや、OU、AWS リージョン、タグのユーザー設定に合わせて、いつでも必要な回数だけ更新できます。これらのパラメータの形式は次のとおりです。

- `/FMS/<PolicyID>/OUs: <StringList>`
- `/FMS/<PolicyID>/Regions: <StringList>`
- `/FMS/<PolicyID>/Tags: <String>`

これらのパラメータを更新する例については、「AWS Systems Manager のパラメータ設定用のシナリオ」を参照してください。

AWS Systems Manager Parameter Store の履歴にアクセスする

AWS Systems Manager Parameter Store のパラメータの変更を呼び出したユーザーを確認するには、次の手順を実行します。

1. AWS Systems Manager コンソールにサインインします。
2. 左側のメニューペインにある**アプリケーション管理**で、[**パラメータストア**] を選択します。
3. パラメータを選択し、[**詳細**] を選択します。

4. [**履歴**] を選択します。

> **注意：**デフォルトのポリシーをカスタマイズする場合、または OU や AWS リージョン別に異なるポリシーを適用する場合は、「ポリシーのカスタマイズ」を参照してください。このセクションでは、`aws-fms-policy.template` を使用して、OU や AWS リージョン別に異なるポリシーセットを適用する方法について説明しています。

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では、ホストオペレーティングシステム、仮想化レイヤー、サービスを運用する施設の物理的なセキュリティなどのコンポーネントを AWS が運用、管理、制御するため、お客様の運用上の負担が軽減します。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。

AWS IAM ロール

AWS Identity and Access Management (IAM) のロールを使用すると、AWS クラウド内のサービスやユーザーに対して、きめ細かなアクセスポリシーと許可を割り当てることができます。このソリューションでは、AWS Lambda 関数に対して、リージョンリソースを作成するためのアクセスを許可する AWS IAM ロールを作成します。

前提条件のスタックに必要なアクセス許可

前提条件を満たすには、適切な AWS IAM のアクセス許可が必要です。これらのアクセス許可には、AWS のサービスと AWS Organizations との信頼されたアクセスの有効化、メンバーアカウントに AWS Config を設定するスタックセットのインスタンスの作成と削除、AWS Firewall Manager の管理者設定、Amazon CloudWatch Logs への AWS Lambda のイベントの記録が含まれます。

プライマリスタックに必要なアクセス許可

AWS Firewall Manager のポリシーを管理する場合も、適切な AWS IAM のアクセス許可が必要です。これらのアクセス許可には、AWS WAF、AWS Shield、Amazon VPC のセキュリティグループ、

Amazon Route 53 Resolver DNS Firewall に対する AWS Firewall Manager のポリシーの作成と削除、ポリシーのメタデータを使用した Amazon DynamoDB テーブルの読み取りと書き込み、SSM のパラメータ情報の読み取り、Amazon CloudWatch Logs への AWS Lambda のイベントの記録が含まれます。さらに、AWS Lambda の ComplianceGenerator 関数には、すべての AWS Firewall Manager のポリシーを記述し、コンプライアンスレポートを生成して Amazon S3 バケットにアップロードするアクセス許可が必要です。

AWS Systems Manager Parameter Store

このソリューションでは、AWS Systems Manager Parameter Store を使用して AWS Firewall Manager のポリシーに対する作成、読み取り、更新、削除 (CRUD) 操作をトリガーします。このソリューションで作成した SSM のパラメータはセキュリティで保護する必要があります。アクセス権は、特定のプリンシパルまたはユーザーにのみ付与する必要があります。これらのパラメータにアクセスできる悪意のあるユーザーは、望ましくない AWS Firewall Manager のポリシー操作 (ポリシーの削除など) を引き起こす可能性があります。このような操作は、AWS Organizations の複数のメンバーアカウントでトリガーされる場合があります。

IAM ユーザー、ロール、またはフェデレーティッドユーザーは、デフォルトでアクセスが拒否されています。ユーザーには、アクションの実行を明示的に許可する必要があります。これらの SSM のパラメータにアクセスする明示的な許可を取得しない限り、このソリューションのパラメータを変更することはできません。さらに、次のサンプルポリシーに示すように、明示的な拒否を使用して、これらのリソースに対するさらなるアクセスを防止できます。このサンプルポリシーをユーザーに割り当てることで、Amazon DynamoDB テーブルおよび SSM のパラメータリソースへのアクセスを禁止できます。

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Action": [
        "dynamodb:*"
      ],
      "Resource": "arn:aws:dynamodb:<region>:<account-
id>:table/<table-name>",
      "Effect": "Deny",
      "Sid": "FMSDDBSecure"
    },
```

```
      {
        "Action": "ssm:*"
        "Resource": [
          "arn:aws:ssm:<region>:<account-id>:parameter/FMS/OUs",
          "arn:aws:ssm:<region>:<account-id>:parameter/FMS/Regions",
          "arn:aws:ssm:<region>:<account-id>:parameter/FMS/Tags"
        ],
        "Effect": "Deny",
        "Sid": "FMSSSMSecure"
      }
    ]
  }
  }
```

その他のリソース

AWS のサービス

- AWS Config
- AWS CloudFormation
- Amazon EventBridge
- AWS Firewall Manager
- AWS Lambda
- AWS Systems Manager
- AWS DynamoDB
- Amazon Simple Storage Service

その他の AWS WAF のソリューションとリソース

- 「AWS での WAF オートメーション」ソリューション
- AWS WAF のリソース

スタックの更新

旧バージョンのソリューションをデプロイしている場合は、次の手順に従って最新バージョンの「AWS Firewall Manager のオートメーション」ソリューションに安全に移行できます。

1. AWS CloudFormation コンソールにサインインし、`aws-fms-automations` テンプレートをデプロイします。「スタックの起動」を参照してください。

2. スタックを正常に作成したら、SSM Parameter Store のパラメータを変更して、OU、AWS リージョン、タグの値に応じた FMS ポリシーを作成します。「FMS ポリシーの追加と管理」を参照してください。
3. さらに、ポリシーのマニフェストファイルの値を変更することで、カスタム要件を満たすようにポリシーを設定できます。詳細については、「ポリシーのカスタマイズ」を参照してください。
4. 新しい FMS ポリシーをデプロイし、これらのポリシーが要件に準拠していることを確認したら、以前にデプロイしたバージョンのソリューションを削除できます。AWS CloudFormation コンソールにサインインし、既存の `aws-centralized-waf-and-security-group-management` AWS CloudFormation スタックを選択して、[**削除**] 選択します。

これで、このソリューションの最新バージョンおよびサポートされている FMS ポリシーに安全に移行できます。

AWS Systems Manager のパラメータ設定用のシナリオ

このソリューションでは、AWS Systems Manager の 3 つのパラメータを使用して、AWS Firewall Manager のポリシーの作成、更新、削除を開始します。次のシナリオを参考にして AWS Systems Manager の該当するタスクを設定してください。

- 2 つの組織単位 (OU) と 5 つの AWS リージョンにまたがるポリシーを作成する
- ポリシーからタグを削除する
- AWS リージョンのポリシーを削除する
- すべてのポリシーを削除する

各パラメータは *StringList* 型です。各文字列を区切るには、カンマを使用します。

シナリオ 1

2 つの OU と 5 つの AWS リージョンにまたがるポリシーを作成し、ポリシーの適用範囲を特定のタグ値に制限するには、次の手順に従います。

シナリオ情報:

- OU: `ou-xxxx-y1y1y1y1,ou-yyyy-x2x2x2x2`
- AWS リージョン: `us-east-1,us-east-2,us-west-1,us-west-2,eu-west-1`
- タグ:

```
{"ResourceTags":[{"Key":"Environment","Value":"Prod"}],"ExcludeResourceTags":false}
```

1. OU 値を使用して **/FMS/OUs** パラメータを更新します。
   `ou-xxxx-y1y1y1y1,ou-yyyy-x2x2x2x2`

   このアクションでは、AWS WAF および AWS Shield Advanced のグローバルポリシーを作成します。

2. 選択した AWS リージョンで **/FMS/Regions** パラメータを更新します。
   `us-east-1,us-east-2,us-west-1,us-west-2,eu-west-1`

   このアクションでは、リージョンポリシー (1 つの AWS WAF、1 つの AWS Shield、2 つのセキュリティグループ) を作成します。

3. タグ値を使用して **/FMS/Tags** パラメータを更新します。
   `{"ResourceTags":[{"Key":"Environment","Value":"Prod"}],"ExcludeResourceTags":false}`

   このアクションでは、すべてのポリシーを更新して指定したタグ値を反映します。

AWS Firewall Manager のポリシーは、次の手順に従って作成します。選択した各 AWS リージョンには、2 つのグローバルポリシーと 4 つのリージョンポリシーが必要です。このシナリオでは、(4*5) + 2 という式を使用して、合計 22 のポリシーを作成します。

シナリオ 2

ポリシーからタグを削除するには、次の値を使用して **/FMS/Tags** パラメータを更新します。

/FMS/Tags: `delete`

このアクションでは、すべてのポリシーを更新し、適用したタグを削除します。

シナリオ 3

すべてのリージョンポリシーを削除するには、次の値を使用して /FMS/Regions パラメータを更新します。

/FMS/Regions: `delete`

このアクションでは、すべてのリージョンポリシーを削除します。

シナリオ 4

すべてのポリシーを削除するには、次の値を使用して **/FMS/OUs** パラメータを更新します。

/FMS/OUs: `delete`

> **注意**: ポリシーのメタデータは Amazon DynamoDB テーブルに保存されています。このソリューションの使用中は、このテーブルを削除しないでください。

使用するポリシーとルールセットのリスト

一元的な AWS WAF のマネージドルールの自動化

AWS Firewall Manager をサポートするために、このソリューションでは AWS WAF 用の AWS マネージドルールをインストールします。組織単位 (OU) またはリソースタグに基づいて、適用範囲とするアカウントを設定できます。

インストールされている AWS マネージドルールの一覧を次に示します。

- **コアルールセット (CRS) ― ウェブ ACL キャパシティーユニット (WCU) 700 :** このグループには、ウェブアプリケーションに一般的に適用できるルールが含まれています。このグループは、OWASP に記載されている脆弱性を含め、さまざまな脆弱性の悪用に対する保護を提供します。
- **Amazon IP 評価リスト ― WCU 25 :** このグループには、Amazon の脅威インテリジェンスに基づくルールが含まれています。このリストは、ボットやその他の脅威に関連するソースをブロックする場合に役立ちます。
- **既知の不正な入力 (KBI) ― WCU 200 :** このグループには、無効であることがわかっており、脆弱性の悪用や発見に関連するリクエストパターンをブロックできるルールが含まれています。これらの入力は、悪意のある人物が脆弱なアプリケーションを発見するリスクを軽減するのに役立ちます。
- **SQL - WCU 200 :** このグループには、SQL インジェクション攻撃など、SQL データベースの悪用に関連するリクエストパターンをブロックできるルールが含まれています。これらのルールは、不正なクエリのリモートインジェクションを防ぐのに役立ちます。

デフォルトでは、これらのルールに基づく検出結果は AWS Firewall Manager によって自動修復されます。この設定を変更して自動修復を手動で実行するには、このソリューションのマニフェストファイルで選択内容を更新します。

一元的なセキュリティグループの監査チェック

このソリューションは、AWS Firewall Manager で、主要な管理者アカウントからすべての該当するアカウントの Amazon EC2 インスタンスに対して、Amazon VPC のセキュリティグループ用に事前設定された監査チェックをインストールします。アカウントの適用範囲は、OU またはリソースタグに基づいて設定できます。このソリューションでは、未使用および冗長なセキュリティグループの監査とクリーンアップを行います。

デフォルトでは、これらのルールに基づく検出結果は AWS Firewall Manager によって自動修復されません。

一元的な DDoS 保護の有効化

AWS Shield Advanced をアクティブにしている場合は、そのルールとポリシーを活用して一元的な DDoS 攻撃から保護できます。

デフォルトでは、これらのルールに基づく検出結果は AWS Firewall Manager によって自動修復されます。この設定を変更して自動修復を手動で実行するには、このソリューションのマニフェストファイルで選択内容を更新します。

一元的な Amazon Route 53 Resolver DNS Firewall ルールの自動化

このソリューションでは、Amazon Route 53 Resolver DNS Firewall ルールの一元管理をサポートするために、事前設定された Amazon Route 53 Resolver DNS Firewall のルールグループを AWS リージョンごとにインストールします。Amazon Route 53 Resolver DNS Firewall のルールグループは、AWS のマネージドドメインリストを使用します。

詳細については、*Amazon Route 53* デベロッパーガイドの「Route 53 Resolver DNS Firewall」を参照してください。

ポリシーのマニフェストファイル

このソリューションでは、JSON のマニフェストファイルを使用して AWS Firewall Manager のポリシーを作成します。このソリューションをデプロイすると、マニフェストファイルがアカウントの Amazon S3 バケット (`<Stack-Name>-xx-policymanifestbucket-xx`) にコピーされます。このマニフェストファイルは、ポリシー用に AWS で提供しているデフォルトのセットです。これらのデフォルトがユースケースに適していない場合は、次の手順に従ってマニフェストの設定を調整できます。

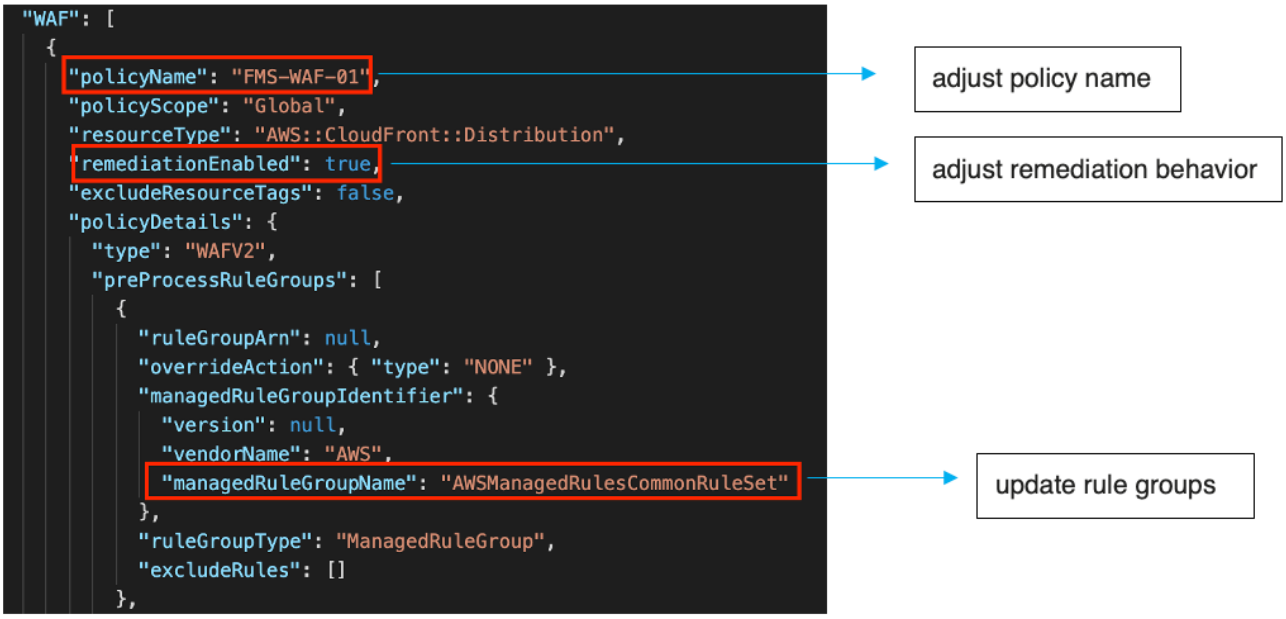

図 *2:* ポリシーのマニフェストファイルの例

マニフェストのスキーマ

ユースケースに合わせてマニフェストファイルを更新する前に、次のスキーマの詳細と定義を確認します。

```
{
  "default": {
    "<Policy-Type>": <Policy-Object>
  }
}
```

default: マニフェストのルートキー。変更**しません**。

Policy-Type: このソリューションでサポートしている AWS Firewall Manager のポリシー。サポートしているタイプは、次のとおりです。

- "WAF_GLOBAL"、
- "WAF_REGIONAL"、
- "SHIELD_GLOBAL"、"SHIELD_REGIONAL"、
- "SECURITY_GROUPS_USAGE_AUDIT"、

- "SECURITY_GROUPS_CONTENT_AUDIT"、
- "DNS_FIREWALL"。

Policy-Object

policyName: AWS Firewall Manager のポリシーの名前。

policyDetails: サービスタイプに固有のポリシー詳細 (JSON 形式)。さまざまなポリシータイプの詳細については、セキュリティサービスのポリシーデータを参照してください。

resourceType：ポリシーで保護されるか、ポリシーの適用範囲内で保護されるリソースのタイプ。この形式については、「AWS リソースおよびプロパティタイプのリファレンス」を参照してください。

resourceTypeList：resourceType のリスト。

remediationEnabled：ポリシーを自動的に新しいリソースに適用するかどうか、およびポリシーの検出結果を自動的に修復するかどうかを示します。

このソリューションのカスタマイズの詳細については、GitHub リポジトリの README.md ファイルを参照してください。

ポリシーのカスタマイズ

このソリューションでは、AWS Firewall Manager のセキュリティポリシーをデフォルト設定でデプロイします。ただし、OU や AWS リージョン別に、ポリシー設定を変更したり、異なるポリシーを適用したりできます。

AWS Firewall Manager のセキュリティポリシーのデフォルト設定を変更するには、このソリューションのインストール後に、次の手順に従ってください。

1. このソリューションのデプロイが正常に完了したら、Amazon S3 コンソールにサインインし、`<Stack-Name>-XX-policymanifestbucket-xx` の Amazon S3 バケットを選択します。
2. バケット内の `policy_manifest.json` ファイルを参照します。

3. マニフェストファイルをダウンロードし、ポリシーのマニフェストのデフォルト設定を調整します。詳細については、「ポリシーのマニフェストファイル」を参照してください。更新したマニフェストファイルを同じ場所にアップロードします。
4. SSM Parameter Store のパラメータを更新します。SSM パラメータ (OU、AWS リージョン、またはタグのパラメータ) を更新したら、FMS ポリシーも更新して、手順 3 で行った変更を反映する必要があります。

OU や AWS リージョン別に異なるポリシーを適用するには、次の手順に従ってください。

1. `aws-fms-policy.template` を使用して、OU や AWS リージョン別に異なるポリシーをサポートするために必要な追加のリソースを起動します。このテンプレートは、必要なポリシー設定の数に応じて繰り返し起動できます。
2. 次に、スタックのパラメータ値を指定します。

パラメータ	デフォルト	説明
Policy Identifier		ポリシーの固有の識別子。
Policy Table		ポリシーのメタデータを保存する Amazon DynamoDB テーブル。このテーブルは、プライマリテンプレートのデプロイの一部として作成されます。
UUID		スタックのデプロイごとの固有の識別子。UUID は、プライマリテンプレートのデプロイの一部として作成されます。 注意：このソリューションのエンドポイントに匿名メトリクスを送信しない場合は、このパラメータを空白にすることができます。
Metric Queue		このソリューションのエンドポイントに匿名メトリクスを送信するための Amazon SQS キュー。このキューは、プライマリテンプレートのデプロイの一部として作成されます。

注意：Policy Table、UUID、Metric Queue はプライマリスタックのデプロイの一部として作成されます。これらの値は、デプロイしたスタックの**出力**セクションで確認できます。プライマリスタックの**出力**セクションに表示されているのと同じ値であることを確認してください。

3. デプロイが正常に完了すると、さらに 3 つの SSM Parameter Store が AWS Systems Manager コンソールのパラメータストアに追加され、さらに 1 つの `<Stack-Name>-xx-policymanifestbucket-XX` バケットが Amazon S3 コンソールに追加されます。
4. これらの SSM Parameter Store の値は調整できます。SSM Parameter Store の値を反映した FMS ポリシーが作成されます。また、ポリシー設定は、マニフェストバケットの `policy_manifest.json` ファイルによって管理されます。`policy_manifest.json` はいつでも更新できます。

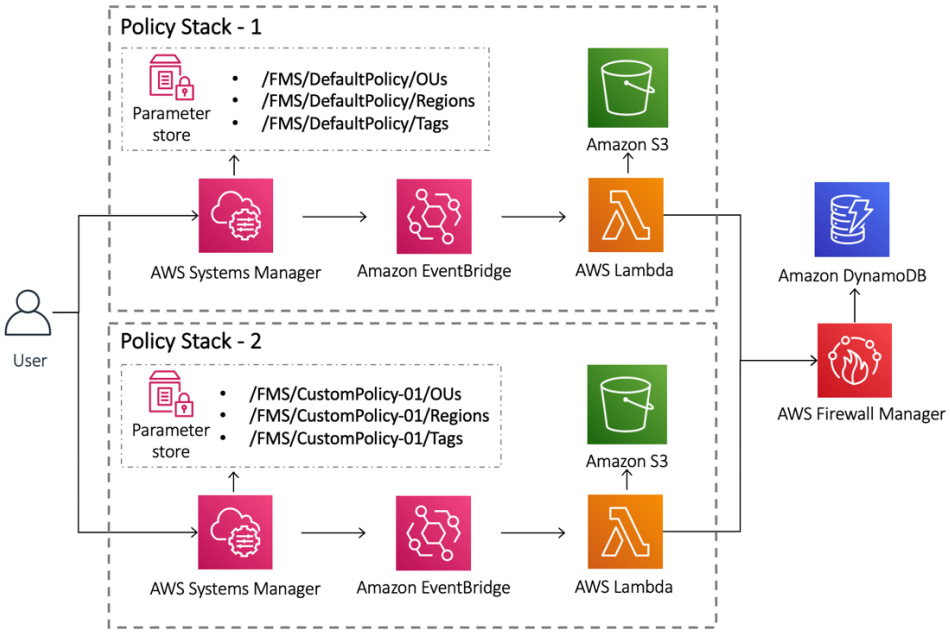

図 *3: AWS Firewall Manager* における複数のポリシースタックのデプロイ

ポリシー設定別のポリシースタックを必要な数だけ作成し、これらを各 OU や AWS リージョンに適用できます。

ポリシーのカスタマイズシナリオの例

ポリシーのマニフェストのスキーマについては、「マニフェストのスキーマ」を参照してください。ポリシーのマニフェストはさまざまな方法で設定できます。いくつかの一般的な方法を次に示します。

ポリシーの自動修復の動作を変更する

すべてのポリシーには、ポリシーのマニフェストファイル内にデフォルトの修復動作があります。これを要件ごとに `true` または `false` に調整できます。

```
"remediationEnabled": false
```

AWS WAF Bot Control のルールグループを追加する

マニフェストファイル内の **WAF Global** ポリシーまたは **WAF Regional** ポリシーをカスタマイズして、AWS マネージドの AWS WAF Bot Control のルールグループを追加できます。WAF ポリシーの `preProcessRuleGroups` セクションまたは `postProcessRuleGroups` セクションは、次のように更新できます。

```
"postProcessRuleGroups": [{
    "ruleGroupArn": null,
    "overrideAction": {
        "type": "NONE"
    },
    "managedRuleGroupIdentifier": {
        "version": null,
        "vendorName": "AWS",
        "managedRuleGroupName": "AWSManagedRulesBotControlRuleSet"
    },
    "ruleGroupType": "ManagedRuleGroup",
    "excludeRules": []
}]
```

AWS WAF Bot Control のマネージドルールグループの詳細については、*AWS WAF* デベロッパーガイドの「*AWS マネージドルールのルールグループリスト*」を参照してください。

特定のポリシータイプをデプロイする

サポートされている次のポリシーから FMS ポリシーをデプロイすることもできます。

- WAF_GLOBA
- WAF_REGIONAL
- SHIELD_GLOBAL
- SHIELD_REGIONAL

- SECURITY_GROUPS_USAGE_AUDIT
- SECURITY_GROUPS_CONTENT_AUDIT
- DNS_FIREWALL

FMS ポリシーのタイプごとに JSON オブジェクトがあり、ポリシー設定を制御するマニフェストのスキーマで定義されています。特定のポリシーが必要ない場合は、この JSON オブジェクトをマニフェストファイルから削除できます。

このソリューションによって既にポリシーが作成されている場合は、次の手順に従って該当するポリシータイプを削除してください。

1. デプロイ済みの FMS ポリシータイプを削除します。
    a. AWS Firewall Manager の管理者アカウントにログインします。
    b. 削除するポリシーを特定します。
    c. このポリシーを選択し、[**Delete**] を選択します。
    d. ポップアップウィンドウで [**Delete all policy resources**]、[**Delete**] の順に選択します。
2. Amazon S3 バケット内のポリシーのマニフェストファイルを更新します。詳細については、「ポリシーのマニフェストファイル」を参照してください。
3. SSM Parameter Store パラメータを更新します。詳細については、「ステップ 2. FMS ポリシーの追加と管理」を参照してください。

コンプライアンスレポート

このソリューションでは、AWS Firewall Manager のポリシーごとに 2 つのレポートを生成します。

1. **アカウントコンプライアンスレポート**：このレポートは、ポリシーの適用範囲内のすべてのメンバーアカウントと、これらのアカウントのコンプライアンスステータスを一覧表示しま

す。このレポートは、`<timestamp>_account_compliance_<policy-id>` の命名スキーマを使用した Amazon S3 バケット内にあります。

MEMBER_ACCOUNT	COMPLIANCE_STATUS
[redacted]	COMPLIANT
[redacted]	COMPLIANT
[redacted]	{"AWSCONFIG":"Cannot create config rule resource for member account [redacted]. Please ensure AWS Config Recorder is enabled and the Config resource limits are not exceeded."}

図 *4:* アカウントコンプライアンスレポートの例

2. **リソース違反レポート**：このレポートは、ポリシーの適用範囲内のすべての AWS リソースのうち、コンプライアンスに違反しているリソースを一覧表示します。このレポートは、`<timestamp>_resource_violator_<policy-id>` の命名スキーマを使用した Amazon S3 バケット内にあります。

MEMBER_ACCOUNT	RESOURCE_ID	RESOURCE_TYPE	VIOLATION_REASON
[redacted]	[redacted]	AWS::EC2::SecurityGroup	RESOURCE_VIOLATES_AUDIT_SECURITY_GROUP
[redacted]	[redacted]	AWS::EC2::SecurityGroup	RESOURCE_VIOLATES_AUDIT_SECURITY_GROUP

図 *5:* リソース違反レポートの例

レポートが含まれている Amazon S3 バケットは、パブリックアクセスがブロックされ、暗号化されています。また、バージョニングが有効になっています。さらに、このバケットのオブジェクトの削除に対しては多要素認証 (MFA) を有効にすること、これらのレポートを表示または削除するための昇格された特権をユーザーに付与しない (最小特権の設計原則に準拠する) ことをお勧めします。詳細については、*Amazon S3* ユーザーガイドの「MFA 削除の設定」を参照してください。

Amazon CloudWatch Logs Insights

このソリューションは、AWS Lambda 関数のエラー、警告、情報、デバッグの各メッセージをログに記録します。ログに記録するメッセージのタイプを選択するには、AWS Lambda コンソールで該当する関数を見つけ、その **LOG_LEVEL** 環境変数を該当するメッセージのタイプに変更します。

Level	Description
ERROR	Logs will include information on anything that causes an operation to fail.
WARNING	Logs will include information on anything that can potentially cause inconsistencies in the function but might not necessarily cause the operation to fail. Logs will also include ERROR messages.
INFO	Logs will include high-level information about how the function is operating. Logs will also include ERROR and WARN messages.
DEBUG	Logs will include information that might be helpful when debugging a problem with the function. Logs will also include ERROR, WARNING, and INFO messages.

ログレベルを調整して、「トラブルシューティング」で特定した問題のトラブルシューティングに役立てることができます。

Amazon CloudWatch Logs Insights を追加する

次の手順に従って、このソリューションに Amazon CloudWatch Logs Insights を追加します。

1. Amazon CloudWatch コンソールに移動します。
2. 左のメニューペインにある**ログ**で、[**ログのインサイト**] を選択します。
3. **ログのインサイト**ページで、[**ログ**] タブを選択します。
4. [**/aws/lambda/FMS-Stack-policyManager-xxxx**] を選択します。このロググループには、ポリシーの作成、更新、削除に関連するログイベントが含まれています。
5. 次のサンプルクエリのいずれかをコピーし、クエリフィールドに貼り付けます。
   - エラーイベントを特定する場合:

```
fields @message
| parse @message "[*] [*] *" as loggingType, microService,
loggingMessage
| filter loggingType = "ERROR"
| display loggingType, microService, loggingMessage
```

- ポリシー作成の成功イベントを特定する場合:

```
fields @message
| parse @message "[*] [*] *" as loggingType, microService,
loggingMessage
| filter loggingMessage like "FMS policy saved successfully"
| display loggingType, microService, loggingMessage
```

- ポリシー作成の失敗イベントを特定する場合:

```
fields @message
| parse @message "[*] [*] *" as loggingType, microService,
loggingMessage
| filter loggingMessage like "failed to save policy"
| display loggingType, microService, loggingMessage
```

6. 時間の設定を選択し、[**クエリの実行**] を選択します。これらのクエリは、今後使用できるように保存しておきます。

トラブルシューティング

次の一般的なエラーに対処する前に、Amazon CloudWatch Logs の詳細レベルを調整することができます。詳細については、「Amazon CloudWatch Logs Insights」を参照してください。

一般的なエラー

1. 前提条件スタックで AWS Config を有効化できない

問題: このソリューションの aws-fms-prereq.template をデプロイする際に、**Enable Config** パラメータを `Yes` に設定すると、次のエラーが発生します。

PreReqManagerCR	⊗ CREATE_FAILED	Received response status [FAILED] from custom resource. Message returned: stack set instance creation failed .ogs: /aws/lambda/tc04-3-PreReqManagerFunction80D2ED4C-X8xz06V4RXIx at sendResponse (/var/task/index.js:155:15) at Runtime.exports.handler (/var/task/index.js:132:18) at processTicksAndRejections (internal/process/task_queues.js:95:5) (RequestId: 3ed6460e-2b8f-4dcf-87cb-8476cda9cb2f)

図 *6: StackSets* 作成の失敗

原因：AWS CloudFormation StackSets との信頼されたアクセスは、AWS CloudFormation コンソールを通じて**のみ**有効にすることができます。*AWS Organizations* ユーザーガイドの「AWS CloudFormation StackSets との信頼されたアクセスの有効化」を参照してください。

解決策:

1. AWS CloudFormation コンソールに移動し、[**信頼されたアクセスを有効にする**] を選択します。**(登録済み委任管理者**の指定はオプションです)

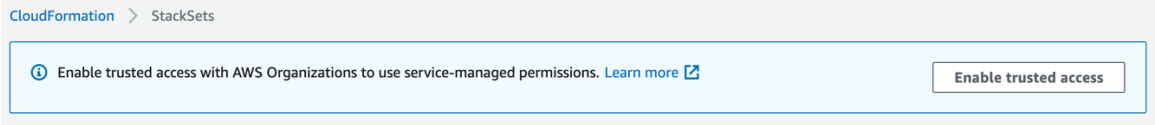

図 *7:* 信頼されたアクセスを有効にする

2. `aws-fms-prereq.template` を再度デプロイすると、今度は成功するはずです。

2. 設定レコーダーの作成時に、AWS CloudFormation StackSets を使用した AWS Config のアクティブ化に失敗する

問題：AWS CloudFormation StackSets コンソールで次のエラーが発生します。

```
ResourceLogicalId:ConfigRecorder, ResourceType:AWS::Config::ConfigurationRecorder, ResourceStatusReason:Failed to put configuration recorder 'StackSet-FMS-EnableConfig-CloudFront-2765adb1-71a9-4a3e-9bbb-535c4efdf35e-ConfigRecorder-1V0GK1MU9SVGJ' because maximum number of configuration recorders: 1 is reached. (Service: AmazonConfig; Status Code: 400; Error Code: MaxNumberOfConfigurationRecordersExceededException; Request ID: 4d48abd6-380a-4037-ab8e-51f239d203cc; Proxy: null).
```

図 *8: AWS CloudFormation StackSets* のエラーメッセージ

原因：各 AWS リージョンでサポートする設定レコーダーは 1 つのみです。レコーダーが既に存在する場合、AWS CloudFormation StackSets は AWS アカウント/AWS リージョンにスタックのインスタンスを作成できません。このエラーは、その AWS リージョンで AWS Config を現在使用しているか、過去に使用していた場合に発生します。詳細については、*AWS Config* デベロッパーガイドの「設定レコーダー」を参照してください。

解決策：該当する AWS リージョンで AWS Config をアクティブにして、必要なリソースタイプを記録グループに確実に含めます。詳細については、*AWS WAF*、*AWS Firewall Manager*、および *AWS Shield Advanced* デベロッパーガイドの「AWS Config の有効化」を参照してください。

3. AWS Config がメンバーアカウントでアクティブになっていない

問題： AWS Config がメンバーアカウントでアクティブになっていない場合は、AWS Firewall Manager コンソールに次のエラーメッセージが表示されます。

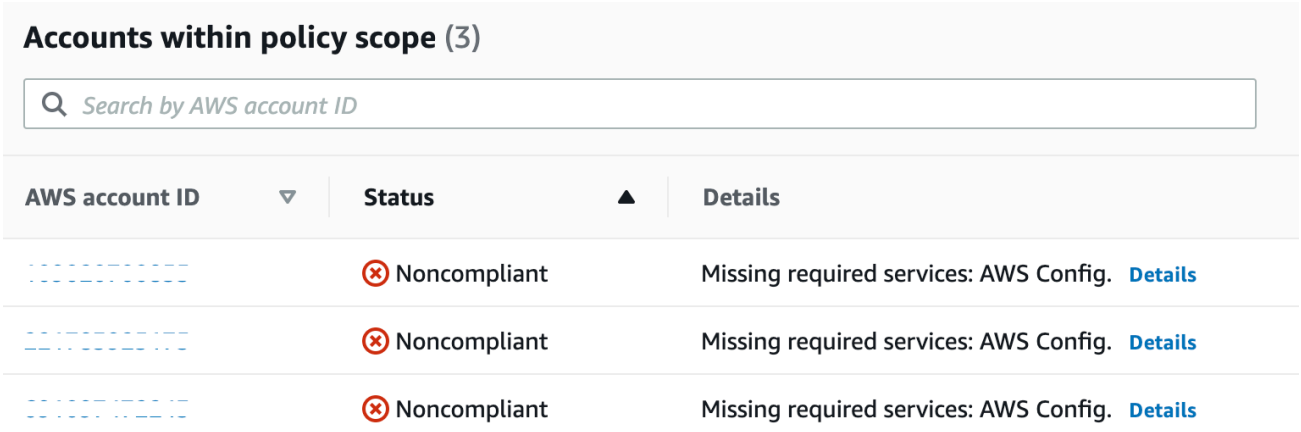

図 *9: AWS Config* のメンバーアカウント

解決策：このソリューションの前提条件テンプレートを使用して AWS Config をアクティブにした場合、これは一時的な問題です。AWS Config がアクティブになってから AWS Organizations の該当するアカウント全体に反映されるまでに時間がかかります。更新の処理が完了するまで少し待ちます。このソリューションの前提条件テンプレートを使用していない場合は、各アカウントにアクセスして AWS Config を手動でアクティブにします。詳細については、*AWS WAF*、*AWS Firewall Manager*、および *AWS Shield Advanced* デベロッパーガイドの「AWS Config の有効化」を参照してください。

4. FMS の管理者アカウント ID が AWS Firewall Manager コンソールに表示されない

問題：AWS CloudFormation スタックで指定した管理者アカウント ID が FMS 設定に反映されていません。

解決策：コンソールで変更を反映して更新するまでに最大 5 分かかる場合があります。

5. AWS CloudFormation StackSets インスタンスが Outdated と表示される

問題：AWS CloudFormation StackSets インスタンスのステータスが **Outdated** と表示されます。

eu-west-1	OUTDATED	User initiated operation
eu-west-2	OUTDATED	User initiated operation
eu-west-3	OUTDATED	User initiated operation
sa-east-1	OUTDATED	User initiated operation
us-east-2	OUTDATED	User initiated operation
us-west-1	OUTDATED	User initiated operation
us-west-2	OUTDATED	User initiated operation

図 *10: AWS CloudFormation StackSets の Outdated ステータス*

解決策：Outdated は一時的なステータスです。StackSets の操作完了後に、AWS CloudFormation StackSets が最終状態に更新されるまでしばらく待ちます。複数の AWS アカウントや AWS リージョンにわたって AWS CloudFormation StackSets インスタンスを作成するプロセスは、時間がかかります。例えば、約 18 の AWS リージョンにわたる 6 つの AWS アカウントの場合、StackSets の操作完了には約 90 分かかります。

6. InternalErrorException が AWS Firewall Manager でポリシーを作成する際に発生する

問題： `InternalErrorException` が原因で、AWS Firewall Manager がポリシーの作成に失敗します。

```
▼ 2020-09-10T13:47:18.041-04:0...  [ERROR] [fmsHelper/putPolicy] {"message":null,"code":"InternalErrorException","time":"2020-09-10
[ERROR] [fmsHelper/putPolicy]
{
    "message": null,
    "code": "InternalErrorException",
    "time": "2020-09-10T17:47:18.041Z",
    "requestId": "b8c75083-ec51-4cc0-a92c-5135abb1faf1",
    "statusCode": 400,
    "retryable": false,
    "retryDelay": 80.23010098902039
}

▼ 2020-09-10T13:47:18.041-04:0...  [ERROR] [PolicyManager/saveShieldPolicy-Regional] failed to save policy
[ERROR] [PolicyManager/saveShieldPolicy-Regional] failed to save policy
```

図 *11: InternalErrorException* エラー

解決策：この問題は本来一時的なものであり、AWS Lambda 関数を再度呼び出すと問題が解決します。例えば、**/FMS/Regions** パラメータを更新したら、更新を再度呼び出す手順を実行します。次の手順に従って、イベントを再度呼び出してください。

1. AWS Systems Manager Parameter Store コンソールに移動します。
2. **/FMS/Regions** パラメータを選択し、[**Edit**] を選択します。
3. デフォルト値のままにして、[**Save changes**] を選択します。

AWS Lambda の `policyManager` 関数が、同じ値を使用して再度呼び出されます。FMS ポリシーが正常に作成されるはずです。

7. AWS API でのスロットリング例外

問題：このソリューションで多数の AWS Firewall Manager のポリシーや AWS アカウントを処理している場合、AWS API スロットリングが発生する可能性があります。

次のエラーが Amazon CloudWatch Logs に記録されます。

```
[ERROR] [ComplianceGenerator/getComplianceDetails] ThrottlingException: Rate exceeded
```

解決策：AWS Lambda 関数には `MAX_ATTEMPTS` 環境変数が含まれており、この変数を調整して問題を解決できます。`MAX_ATTEMPTS` 変数は、このソリューションで API リクエストを再試行する回数を制御します。

前提条件テンプレートのインストール

前提条件 (オプション)

AWS Organizations のプライマリアカウントでデフォルトパラメータを使用して AWS Firewall Manager の前提条件テンプレートをインストールすると、AWS クラウド内に次の環境が構築されます。

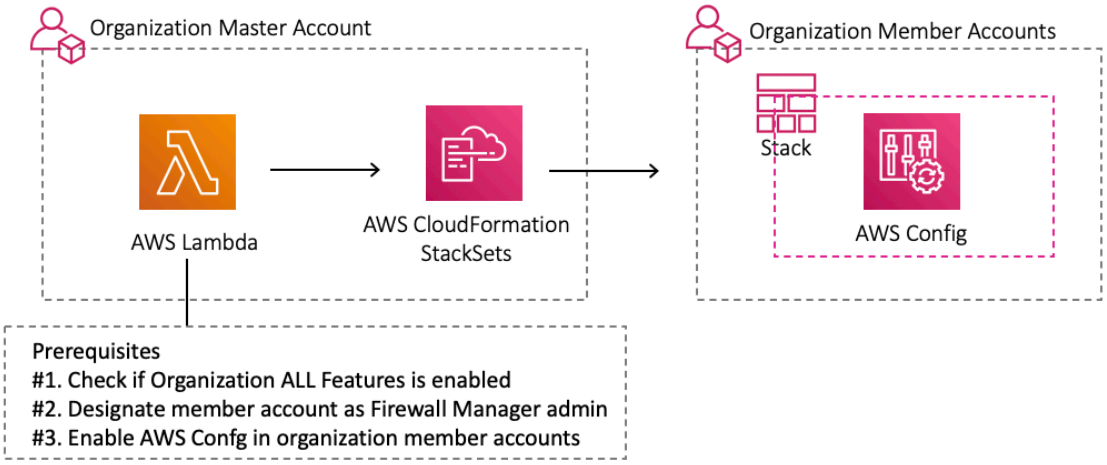

図 *12:* アーキテクチャ*:* 前提条件の有効化

このテンプレートを AWS Organizations のプライマリアカウントにデプロイすると、AWS Lambda 関数は次の前提条件を確認します。

1. **AWS Organizations のすべての機能**がアクティブになっている
2. AWS Firewall Manager の管理者が設定されている
3. オプション: AWS Config がアクティブになっている

> **注意：**この確認は、前提条件テンプレートのデプロイ時に AWS Config をアクティブにする (`Yes` に設定する) と実行されます。

AWS Lambda 関数は前提条件をインストールします。前提条件のインストール中にエラーがあると、スタックのロールバックが発生し、エラーメッセージが表示されます。

AWS Firewall Manager を使用するための前提条件については、「前提条件」を参照してください。

テンプレートを表示

aws-fms-prereq.template: このテンプレートを使用して、ソリューションの前提条件テンプレートを起動します。デフォルト設定では、AWS Lambda 関数、AWS CloudFormation StackSets、AWS Config リソースをデプロイします。

ステップ 1. 前提条件スタックの起動

この自動化された AWS CloudFormation テンプレートは、AWS Firewall Manager の前提条件テンプレートを AWS クラウド内にデプロイします。

> **注意：**このソリューションの実行中に使用した AWS の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」セクションに移動し、このソリューションで使用する AWS のサービス別の料金ウェブページを参照してください。

1. AWS マネジメントコンソールにサインインし、右側のボタンを使用して `aws-fms-prereq` AWS CloudFormation テンプレートを起動します。または、テンプレートをダウンロードし、これを土台にして独自の実装を開始することもできます。

ソリューションの起動

2. **スタックの作成**ページで、正しいテンプレート URL が **Amazon S3 URL** テキストボックスに表示されていることを確認し、[**次へ**] を選択します。
3. **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付けます。
4. **パラメータ**で、このソリューションのテンプレートのパラメータを確認し、必要に応じて変更します。このソリューションでは、次のデフォルト値を使用します。

パラメータ	デフォルト	説明
FMS Admin Account ID	<入力が必須>	FMS 管理者アカウントを既に設定している場合は、AWS Firewall Manager サービスの管理者アカウント ID を追加します。まだ設定していない場合は、AWS Firewall Manager の管理者アカウントとして指定する AWS Organizations のメンバーアカウント ID を選択します。
Enable Config	`Yes`	AWS Firewall Manager が必要とするリソースに対して、組織全体で AWS Config をアクティブにします。AWS Config を既にアクティブにしている場合は、`No` を選択します。

5. [**次へ**] を選択します。
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、設定を見直して確認します。テンプレートで AWS Identity and Access Management (IAM) リソースを作成することを確認するチェックボックスをオンにします。
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 10 分で CREATE_COMPLETE ステータスが表示されます。

ステップ 2. AWS Firewall Manager のアクティブ化

AWS Organizations で AWS Firewall Manager をアクティブにするには、次の手順に従います。

1. **AWS Organizations のすべての機能**をアクティブにします。
2. AWS Organizations のすべてのメンバーアカウントで **AWS Config** をアクティブにします。
3. 1 つのメンバーアカウントを **AWS Firewall Manager の管理者**として指定します。

AWS Firewall Manager を有効にするための詳細については、*AWS WAF*、*AWS Firewall Manager*、および *AWS Shield Advanced* デベロッパーガイドの「AWS Firewall Manager の前提条件」を参照してください。

ソリューションのアンインストール

このソリューションをアンインストールして、すべてのポリシーを確実に削除するには、AWS Systems Manager Parameter Store に移動し、**/FMS/<Policy-Id>/OU** パラメータを `delete` に変更する必要があります。次のいずれかの方法を使用してスタックを削除できます。

AWS マネジメントコンソールの使用

1. AWS CloudFormation コンソールにサインインします。
2. このソリューションのインストール用のスタックを選択します。
3. [**削除**] を選択します。

AWS Command Line Interface の使用

AWS Command Line Interface (AWS CLI) がご自分の環境で使用できるかどうかを確認します。インストール手順については、*AWS CLI* ユーザーガイドの「AWS Command Line Interface とは」を参照してください。AWS CLI が使用できることを確認したら、次のコマンドを実行します。

```
$ aws cloudformation delete-stack --stack-name <specify-your-stack-name>
```

注意：このソリューションでは、スタックとこのソリューションがデプロイしたすべてのリソースを完全に削除できます。カスタム定義のルールと Amazon S3 バケット (コンプライアンスレポートを含む) のみが残ります。

運用メトリクスの収集

このソリューションには、匿名の運用メトリクスを AWS に送信するオプションが含まれています。当社はこのデータを使用して、お客様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。アクティブにすると、次の情報が収集され、AWS に送信されます。

- **Solution ID :** AWS ソリューション識別子
- **Unique ID (UUID) :** ソリューションのデプロイごとにランダムに生成された固有の識別子
- **Timestamp :** データ収集タイムスタンプ

このアンケートを通じて収集したデータは 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、次のタスクを実行します。

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。

変更前:

```
"Send" : {
   "AnonymousUsage" : { "Data" : "Yes" }
},
```

変更後:

```
"Send" : {
   "AnonymousUsage" : { "Data" : "No" }
},
```

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、カスタマイズした結果を他のユーザーと共有できます。

改訂

日付	変更
2020 年 9 月	初回リリース
2021 年 8 月	リリースバージョン 1.1: Amazon Route 53 Resolver DNS Firewall ポリシーについて、FMS ポリシーに関するコンプライアンスレポートの生成と、複数のカスタムポリシースタックのデプロイに対するサポートを追加しました。また、ソースコードを `aws-sdk-js-v3` に移行しました。詳細については、CHANGELOG.md ファイルを参照してください。

寄稿者

- Garvit Singh
- Rakshana Balakrishnan

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 Firewall Manager のオートメーション」ソリューションは、Apache Software Foundation で入手可能な Apache ライセンスバージョン 2.0 の条件に基づいてライセンスされます。