デベロッパーガイド

AWS Network Security Manager



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Network Security Manager: デベロッパーガイド

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

AWS Network Security Manager とは 1
AWS Network Security Manager の仕組みの概要 1
AWS Network Security Manager の機能 1
ユースケース 2
関連サービス 3
AWS Network Security Manager へのアクセス 3
料金 4
を初めてお使いになる方向けの情報 4
AWS Network Security Manager の仕組み 5
AWS Network Security Manager リソースモデル 5
AWS Network Security Manager リソースのライフサイクル、マージ、同期 6
ドラフトライフサイクルとアクティブライフサイクル 6
バージョニング 7
優先度ベースのポリシーマージ 8
Config AWS を使用したリソース検出 9
同期と修復 10
管理者アカウントとメンバーアカウント 11
サービスにリンクされたロール 12
AWS Network Security Manager のセットアップ 13
組織モデルを選択する 13
シングルアカウント使用のための のセットアップ 13
AWS Organizations でのマルチアカウント使用の設定 14
AWS Network Security Manager 管理者アカウントの作成 14
AWS Network Security Manager のアクセス許可を持つ IAM ID を作成する 16
にサインアップする AWS アカウント 18
デフォルトでは無効になっているリージョンでの AWS Network Security Manager の使用 18
チュートリアル: 最初のネットワークセキュリティ保護をデプロイする 19
前提条件 19
ステップ 1: ルールを作成する 20
ステップ 2: テンプレートを作成する 21
ステップ 3: ポリシーを作成する 22
ステップ 4: スコープを作成する 23
ステップ 5: デプロイを作成して公開する 24
ステップ 6: 同期ステータスをモニタリングする 24

ステップ 7: クリーンアップする 25
次の手順 26
ファイアウォールとセキュリティサービスの管理 28
AWS WAF ACLs の管理 28
AWS WAF の概念 28
AWS WAF のクイック作成 32
AWS WAF の標準作成プロセス 36
Shield Advanced の DDoS AWS 保護の管理 42
Shield Advanced AWS のクイック作成 43
Shield Advanced AWS の標準作成プロセス 46
AWS Network Security Manager と Firewall Manager 51
AWS Firewall Manager との共存 51
修復中の優先順位 51
AWS Firewall Manager からの計画された移行 51
セキュリティ 53
データ保護 54
保管中の暗号化 55
転送中の暗号化 55
キー管理 55
ID とアクセス管理 55
オーディエンス 55
アイデンティティを使用した認証 56
ポリシーを使用したアクセスの管理 57
AWS Network Security Manager と IAM の連携方法 59
アイデンティティベースのポリシーの例 65
トラブルシューティング 70
サービスリンクロール 72
サービスにリンクされたロールのアクセス許可 72
サービスにリンクされたロールの作成 83
サービスにリンクされたロールの編集 83
サービスにリンクされたロールの削除 83
サポート対象のリージョン 84
コンプライアンス検証 84
耐障害性 85
インフラストラクチャセキュリティ 85
セキュリティのベストプラクティス 86

予防的コントロール 86
「発見的コントロール」 86
AWS Network Security Manager のモニタリング 87
同期ステータスのモニタリング 87
同期ステータスオペレーション 87
同期ステータス値について 88
評価タイムスタンプについて 88
クロスアカウントの可視性 88
out-of-syncリソースの診断 89
CloudTrail ログ 89
AWS CloudTrail の Network Security Manager 情報 89
例: CreatePolicy イベント 91
クォータ 94
リソースクォータ 94
リソースコンポジションクォータ 94
スコープ設定クォータ 95
管理者アカウントのクォータ 95
API ページ分割クォータ 95
クォータの調整可能性 96
ドキュメント履歴 97
..... xcviii

AWS Network Security Manager とは

AWS Network Security Manager を使用すると、 AWS WAF や Shield Advanced AWS ルールなどのネットワークセキュリティ保護を組織内の 1 つ以上のアカウントとリソースに一元的に定義してデプロイできます。各リソースを個別に操作する代わりに、再利用可能なポリシーオブジェクト (ルール、テンプレート、ポリシー) を 1 回定義し、ポリシーのドリフトを検出して修正するための継続的なモニタリングを使用して、大規模なデプロイを行います。

AWS Network Security Manager の仕組みの概要

一連の階層ポリシーオブジェクトを定義し、ターゲットスコープに適用します。ポリシーオブジェクトの最下位レベルはルールです。ルールをテンプレートにグループ化し、優先度ベースの競合解決でポリシーに結合できます。次に、スコープで保護するアカウントとリソースを選択し、デプロイを公開してポリシーを適用します。

デプロイ後、 AWS Network Security Manager はスコープ環境とデプロイされたポリシーを継続的にモニタリングして、意図した定義と一致するかどうかを確認します。そうでない場合、 AWS Network Security Manager はオプションで、意図した設定から逸脱するリソースを修復できます。リソースモデル、ライフサイクル、アーキテクチャの詳細については、「」を参照してください AWS Network Security Manager の仕組み。

AWS Network Security Manager の機能

- 複数のファイアウォールタイプのサポート – AWS Network Security Manager は、ウェブ ACL 設定とルールグループの AWS WAF をサポートしています。保護されたリソースタイプには、Amazon CloudFront ディストリビューション、Application Load Balancer、Amazon API Gateway ステージが含まれます。 AWS Network Security Manager AWS は、Amazon CloudFront ディストリビューション、Application Load Balancer、Classic Load Balancer、Elastic IP アドレスの DDoS 保護のために Shield Advanced もサポートしています。
- 再利用可能なセキュリティ設定 – ポリシーオブジェクトを 1 回ルールとして定義し、テンプレートにグループ化して、リソースをターゲットとするスコープを作成します。ルール、テンプレート、スコープを複数のポリシーとデプロイで再利用します。
- 優先度ベースのポリシーマージ – 複数のポリシーが同じリソースを保護する場合、 AWS Network Security Manager はポリシーの優先度に基づいて設定をマージし、予測可能な競合解決を提供します。

- シングルアカウントとマルチ管理者のサポート – AWS Network Security Manager を 1 つのアカウントで使用するか、複数の管理者アカウントを指定します。各アカウントは優先度が高くなります。管理者のポリシーが重複すると、 AWS Network Security Manager はまず管理者の優先度によって競合を解決し、次に各アカウント内のポリシーの優先度によって競合を解決します。
- ドラフト状態とアクティブ状態 – ルール、テンプレート、ポリシー、スコープ、デプロイを含む各 AWS Network Security Manager リソースは、ドラフト状態とアクティブ状態をサポートします。ライブ保護に影響を与えずにリソースをドラフトとして保存し、適用する準備ができたら公開します。
- バージョン管理されたスナップショット – ルール、テンプレート、ポリシー、スコープ、デプロイを含む各 AWS Network Security Manager リソースは、イミュータブルなバージョン番号のスナップショットをサポートします。バージョニングを使用して、既知の正常な AWS Network Security Manager リソース設定を保持します。
- 保護されたリソースの同期診断 – スコープ内のリソースごとに、同期されていない設定とその理由を正確に確認し、各設定フィールドの実際の値と比較して予想される設定を確認します。
- 自動修復 – オプションで、 AWS Network Security Manager out-of-syncリソースを自動的に修復し、手動による介入なしで意図した設定に合わせることを可能にします。
- 自然言語ルールの生成 – `GenerateRuleConfiguration`オペレーションを使用してルールをプレーン言語で記述し、Amazon Bedrock を搭載した対応する設定 JSON を受け取ります。

ユースケース

AWS Network Security Manager の一般的なユースケースは次のとおりです。

- すべてのアカウントでベースライン AWS WAF ルールを適用する – すべてのインターネット向けアプリケーションが使用する必要がある一連の AWS WAF ルールグループを定義し、組織全体にデプロイします。 AWS Network Security Manager は、範囲内の新しいリソースにルールを自動的に適用します。
- 特定のリソース間で特定のカスタムまたは例外 AWS WAF ルールを作成する – 特定のリソースセットにのみ適用される一連の AWS WAF ルールを定義します。このセットは、 AWS アカウント ID、OU、タグ、または Amazon リソースネーム (ARNs) で識別する特定のビジネスユニットまたはアプリケーションにすることができます。
- インターネット向けリソースに対する DDoS 保護の検証 – パブリックリソースタイプを対象とする AWS Shield Advanced ポリシーを作成し、組織全体にデプロイして、重要なリソースで DDoS 保護が有効になっているようにします。

- 設定ドリフトの検出と修復 – 同期ステータスモニタリングを使用して、ファイアウォール設定が意図した状態からドリフトしたリソースを特定し、オプションで自動修復を有効にしてコンプライアンスに戻します。
- セキュリティ管理を複数のチームに委任する – 優先度レベルが異なる複数の管理者アカウントを指定し、特定のアカウント、組織単位、またはファイアウォールタイプへのスコープ付きアクセスを指定します。これにより、チームは定義された境界内で独自のセキュリティポリシーを管理できます。

関連サービス

- AWS WAF – AWS WAF を使用して、可用性に影響を与えたり、セキュリティを侵害したり、過剰なリソースを消費したりする可能性のある一般的なウェブエクスプロイトやボットからウェブアプリケーションと APIs を保護します。 AWS Network Security Manager は AWS WAF を使用して、単一のアカウント内または組織内のアカウント間でリソースのウェブ ACLs とルールグループを作成および管理します。
- AWS Shield Advanced – で実行されているアプリケーションに拡張された保護を提供するマネージド DDoS 保護サービス AWS。 AWS Network Security Manager は Shield Advanced を使用して、単一のアカウント内または組織内のアカウント間でリソースの DDoS 保護を提供します。
- AWS Organizations – AWS リソースの拡大とスケーリングに応じて、環境を一元管理できます。 AWS Network Security Manager では、 AWS Organizations がメンバーアカウント全体の保護を管理する必要があります。
- AWS Config – AWS リソースの設定を評価、監査、評価できるサービス。 AWS Network Security Manager は、サービスにリンクされた AWS Config レコーダーを使用して、メンバーアカウントのリソースを検出します。

AWS Network Security Manager へのアクセス

AWS Network Security Manager には、次のインターフェイスからアクセスできます。

AWS マネジメントコンソール

AWS Network Security Manager リソースを管理するためのウェブベースのインターフェイス。

https://console.aws.amazon.com/network-security-manager/ で AWS Network Security Manager コンソールを開きます。

AWS コマンドラインインターフェイス (AWS CLI)

AWS Network Security Manager オペレーションのコマンドを提供します。詳細については、「AWS CLI コマンドリファレンス」を参照してください。

AWS SDKs

AWS はSDKs を提供します。SDKs を使用すると、 AWS Network Security Manager へのプログラムによるアクセスを簡単に作成できます。詳細については、「Amazon ウェブ サービスのツール」を参照してください。

AWS Network Security Manager API

HTTPS 経由で JSON を使用する REST API。API エンドポイントの形式は ですnetwork-security-manager.*{region}*.api.aws。詳細については、AWS 「Network Security Manager API リファレンス」を参照してください。

AWS Network Security Manager の使用を開始するには、 AWS Network Security Manager のセットアップ「」および「」を参照してくださいチュートリアル: 最初のネットワークセキュリティ保護をデプロイする。

料金

AWS Network Security Manager がモニタリングおよび保護する対象範囲内のリソースごとに料金が発生します。 AWS WAF や AWS Shield Advanced など、デプロイする基盤となるセキュリティサービスには追加料金が適用されます。料金の詳細については、 AWS ウェブサイトのAWS 「Network Security Manager の料金」を参照してください。

を初めてお使いになる方向けの情報

AWS Network Security Manager を初めて使用する場合は、次のトピックを順番に読むことをお勧めします。

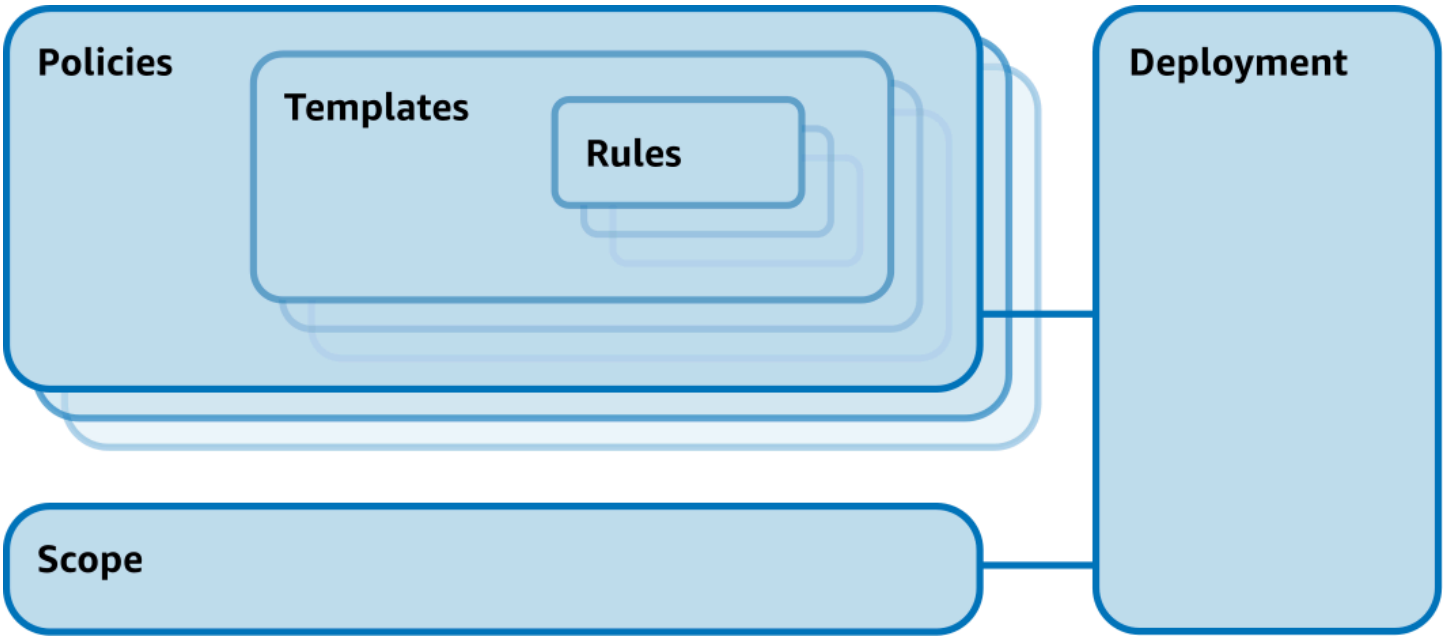
1. AWS Network Security Manager の仕組み – リソースモデル、ライフサイクル状態、ポリシーマージ、同期について説明します。
2. AWS Network Security Manager のセットアップ – AWS Network Security Manager を使用するための前提条件を完了します。
3. チュートリアル: 最初のネットワークセキュリティ保護をデプロイする – 最初のデプロイを作成するend-to-endのチュートリアルについて説明します。

AWS Network Security Manager の仕組み

AWS Network Security Manager リソースモデルを使用して、単一のアカウントまたは組織内の複数のアカウントにわたるリソースのネットワークセキュリティ保護を設計および管理します。この章では、5 つのリソースタイプ、それらが階層を形成する方法、およびそれらの動作を管理する主要な概念について説明します。

AWS Network Security Manager リソースモデル

AWS Network Security Manager は、構成階層に配置された 5 つのリソースタイプを使用します。



リソースは、階層を通じて相互参照します。ルールはテンプレートとポリシー内で使用されます。テンプレート、ルール、またはその両方がポリシー内で使用されます。スコープは、ポリシーがデプロイ内で保護するリソースを参照します。

以下のセクションでは、階層内の各リソースタイプについて説明します。

ルール – ネットワークセキュリティ設定のアトミックユニット。ルールには、トラフィック検査ルールとファイアウォール設定ルールの 2 種類があります。トラフィック検査では、セキュリティサービスがトラフィックにどのように対処するかに焦点を当てます。設定ルールは、トラフィック検査以外のシステムオペレーションを指定します。ルールの構造は、ファイアウォールのタイプによって異なります。

テンプレート – 1 つのファイアウォールタイプの順序付けされた再利用可能なルールのグループ。テンプレートを使用して、関連するルールをパッケージ化し、複数のポリシー間で共有します。テンプレートはオプションです。

ポリシー – 順序付けられたテンプレートとルールのセットを、ファイアウォールタイプの強制設定と組み合わせます。各ポリシーには優先度があります (数値が低いほど優先度が高いことを示します) 。複数のポリシーが同じリソースを保護する場合、優先度によって競合の解決方法が決まります。トラフィック検査ルールの場合、優先度によってルールが集約される順序が決まります。ファイアウォール設定ルールの場合、優先度によって各リソースとその範囲内ポリシーに適用される設定が決まります。

スコープ – 保護が適用される の宣言的な選択。スコープは保護するリソースタイプを指定し、オプションでタグまたは設定属性でリソースをフィルタリングできます。マルチアカウントモードでは、スコープは包含または除外するアカウントまたは OUs も指定します。シングルアカウントモードでは、スコープはアカウント自体に適用されます。スコープのモードは、作成時に修正されます。スコープをどちらの方向でもマルチアカウントモードとシングルアカウントモードの間で切り替えることはできないため、マルチアカウントスコープをシングルアカウントスコープにしたり、逆にしたりすることはできません。

デプロイ — 1 つ以上のポリシーをスコープにバインドします。デプロイを公開すると、適用が有効になります。 AWS Network Security Manager は、スコープ内のリソースを検出し、意図した設定を計算し、オプションでout-of-syncリソースを修復します。

リソース構成の制限については、「」を参照してくださいクォータ。

AWS Network Security Manager リソースのライフサイクル、マージ、同期

以下のセクションでは、 AWS Network Security Manager リソースを作成した後の動作とメカニズムについて説明します。

ドラフトライフサイクルとアクティブライフサイクル

ルール、テンプレート、ポリシー、スコープ、デプロイを含むすべての AWS Network Security Manager リソースのステータスは、ドラフトまたはアクティブです。

- アクティブ – デフォルトのステータス。リソースが公開され、使用できます。他のリソースはそれを参照でき、それを含むデプロイは設定を適用します。

- 下書き – リソースは保存されますが、まだアクティブではありません。ドラフトリソースは強制されず、他のリソースからは参照できません。リソースを作成または更新するときは、ドラフトを保存を選択してドラフトステータスのままにします。

デフォルトでは、 AWS Network Security Manager はリソースをアクティブとして作成します。API を使用してリソースをドラフトとして作成するには、作成または更新オペレーションfalseで isPublishedパラメータを に設定します。

リソースを更新すると、次のシナリオが適用されます。

現在の状態	アクション	結果
下書き	ドラフトの保存を選択する	ドラフトを更新する (ドラフトのまま)
下書き	発行を選択する	ドラフトを公開する (アクティブになる)
アクティブ	発行を選択する	更新してアクティブのままにする (アクティブ)
アクティブ	ドラフトの保存を選択する	ドラフトオーバーレイを作成する (下にアクティブリソースがあるドラフトになる)

hasPublishedVersion フィールドがリストに表示され、レスポンスを取得します。このフィールドは、公開された Active リソースがドラフトの下に存在するかどうかを示します。リソースのドラフトステータスが および の場合hasPublishedVersion: true、保留中のドラフトは、公開されているライブアクティブリソースの上に存在します。

別の Active リソースが参照する Active リソースを削除することはできません。

バージョニング

ルール、テンプレート、ポリシー、スコープ、デプロイを含むすべての AWS Network Security Manager リソースをバージョニングできます。アクティブリソースのバージョンを作成するには、リソースを選択し、アクションを選択し、バージョニングされたスナップショットの作成を選択します。バージョンは、すべての更新で自動的に作成されるわけではありません。

> **AWS CLI の代替**
>
> Active リソースの `Create{Resource}Snapshot` API オペレーションを使用してバージョンを作成することもできます。

キーバージョンのプロパティ:

- 各バージョンには、一意の数値 (シーケンシャル整数) とバージョン修飾 ARN (例:) がありますarn:aws:network-security-manager:us-east-1:123456789012:rule:abc123:3。
- バージョンはイミュータブルです。更新することはできません。
- リソースごとに最大 10 のバージョンを作成できます。
- バージョンはタグ付け可能です。

バージョンを使用して、必要な設定バリアントを保持します。リソースをロールバックするには、バージョンを読み、そのバージョンの必要な設定でライブリソースを更新します。

優先度ベースのポリシーマージ

複数のポリシーが同じリソースを保護する場合、 AWS Network Security Manager は設定を 1 つの結果にマージします。優先度の数値が低いほど、優先度が高いことを示します (優先度 1 が優先度 2 よりも優先されます)。 AWS Network Security Manager がトラフィック検査ルールを含むポリシーをマージすると、優先度によってルールが集約される順序が決まります。ファイアウォール設定ルールの場合、優先度の高いポリシーによって、適用される設定が決まります。

AWS Network Security Manager は、次の順序で 2 つのレベルで優先度を評価します。

1. 管理者の優先度 – AWS Network Security Manager は管理者の優先度を最初に評価します。「」で説明されているように、各組織管理者に優先度が割り当てられますthe section called “管理者アカウントとメンバーアカウント”。 AWS Network Security Manager がポリシーをマージすると、メンバーアカウント独自のシングルアカウントポリシーよりも高い管理者ポリシーがランク付けされます。管理者ポリシーとメンバーアカウントのシングルアカウントポリシーの両方がリソースに適用され、競合する場合、管理者ポリシーの設定が優先されます。メンバーアカウントは、管理者ポリシーをオプトアウト、上書き、または除外することはできません。
2. ポリシーの優先度 – 各アカウント内で、 AWS Network Security Manager はポリシーの優先度を使用して残りの競合を解決します。ポリシーの優先度値は 1 から始まる整数であり、アカウントごとに一意である必要があります。

管理者の優先度は、PutAdminAccountオペレーションpriorityの必須フィールド、1～10 の整数で設定します。優先度値は一意であるため、2 人の管理者が優先度を共有することはなく、タイブレークは必要ありません。詳細については、AWS 「Network Security Manager API リファレンス」を参照してください。

リソースに適用可能なすべてのポリシーのマージ結果は、有効なファイアウォール設定です。 AWS Network Security Manager は、この設定を計算し、リソースの実際の設定と比較し、差異を同期ステータスとして報告します。

ポリシーが競合すると、 AWS Network Security Manager は各属性を比較し、優先度の高いポリシーの値を適用します。優先度の高いポリシーが属性を定義しない場合、優先度の低いポリシー値が適用されます。有効な設定に一致するリソースは IN_SYNC です。優先度の低いポリシーによって保護され、優先度の高いポリシーによって設定が上書きされたリソースは、優先度の低いデプロイでは OUT_OF_SYNC としてレポートされます。これは失敗ではなく、予想される動作です。

Config AWS を使用したリソース検出

AWS Network Security Manager は、サービスにリンクされた Config AWS 設定レコーダーを使用して、アカウント内の保護されたリソースを検出します。このレコーダーは、そのアカウントがデプロイの範囲に入ると、各アカウントに自動的に作成されます。 AWS Firewall Manager とは異なり、追加のセットアップを実行する必要はありません。 AWS Network Security Manager による AWS Config の使用は AWS 、Network Security Manager のお客様に課金されません。

サービスにリンクされたレコーダーの主な特性:

- その名前は AWSConfigurationRecorderForNetworkSecurityManager です。
- これは、アカウントのカスタマー管理設定レコーダーとは別のものです。
- アクティブなスコープとデプロイに関連するリソースタイプのみを記録します。
- Config AWS をセットアップしたり、設定レコーダーを作成したりする必要はありません。 AWS Network Security Manager はこれを自動的に管理します。 AWS Network Security Manager による AWS Config の使用料は顧客に請求されません。
- レコーダーは使用中は変更または削除できません。 AWS Network Security Manager はライフサイクルを自動的に管理します。

AWS Network Security Manager が機能するために、Config AWS を手動で有効化または設定する必要はありません。デプロイを公開すると、サービスはリソース検出を自動的に処理します。

同期と修復

AWS Network Security Manager での強制は非同期で、結果整合性があります。デプロイを公開した後、またはリソースが変更されると、次のステージが発生します。

1. リソース検出 – AWS Network Security Manager は、サービスにリンクされた Config AWS レコーダーを使用して、範囲内のリソースを検出します。
2. 設定の計算 – AWS Network Security Manager は、検出されたリソースごとに、該当するすべてのポリシーを優先度別にマージして、有効なファイアウォール設定を計算します。
3. 同期評価 – AWS Network Security Manager は、有効な設定をリソースの実際の設定と比較し、同期ステータスを記録します。
4. 修復 (オプション) – ポリシー`remediationEnabled`で を設定すると、 AWS Network Security Manager out-of-syncリソースを有効な設定に合わせて修正します。

各ステージは非同期です。ワークフローの結果:

- デプロイの公開とリソースの保護には遅延があります。
- 範囲内の新しいリソースの作成と保護には遅延があります。
- 同期ステータスエントリの`Last Checked`タイムスタンプは、 AWS Network Security Manager がリソースを最後に評価した日時を示します。

修復とリソースのクリーンアップは、ポリシーレベルの設定です。`policyConfiguration` オブジェクトのポリシーごとに各ポリシーを設定します。

`remediationEnabled`

AWS Network Security Manager が非準拠のリソースを自動的に修復するかどうかを指定します。この設定を有効にすると、 AWS Network Security Manager はout-of-syncリソースを修正します。

`resourcesCleanUp`

AWS Network Security Manager が、不要になったときに作成したリソースを自動的に削除するかどうかを指定します。 AWS Network Security Manager は、デプロイを削除したとき、またはアカウントまたはリソースが範囲外になったときに作成したファイアウォールを削除します。

remediationEnabled と resourcesCleanUpの両方の設定はデフォルトで .false AWS Network Security Manager は、これらの設定を有効にするまでリソースを修復またはクリーンアップしません。policyConfiguration オブジェクトにはwafConfig、 AWS WAF ポリシーに適用される も保持されます。詳細については、AWS 「Network Security Manager API リファレンス」を参照してください。

リソースが同期されていない場合、同期ステータスには、実際の値と比較して予想される値を示す設定ごとの詳細を含むout-of-sync理由が含まれます。理由は、次のカテゴリに分類されます。

- missingFirewall – ファイアウォール保護はリソースに関連付けられていません。
- invalidFirewall – ファイアウォールは存在しますが、その設定は有効な設定とは異なります。これには、、incorrectSingleValueConfigurations、missingAppendableConfigurationValues、missingMergeableConfigurationValuesの 6 incorrectAppendableConfigurationOrderつの詳細バケットが含まれますunexpectedMergeableConfigurationValues。

修復が有効になっていても AWS Network Security Manager がリソースを修正できない場合、remediationIssuesフィールドにはissueType、、問題messageを説明する 、および解決方法correctiveActionを提案する が表示されます。

AWS Network Security Manager は、管理しない設定を評価しません。フィールドが寄与ルールに表示されない場合、 AWS Network Security Manager は同期評価中にフィールドを無視します。

管理者アカウントとメンバーアカウント

AWS Network Security Manager は、 AWS Organizations 上に構築されたクロスアカウント管理モデルを使用します。

- 管理者アカウント – AWS Network Security Manager リソース (ルール、テンプレート、ポリシー、スコープ、デプロイ) を作成および管理しているアカウント。優先度が 1 ~ 10 の管理者アカウントを 1 つ以上指定します。
- メンバーアカウント – AWS Network Security Manager がリソースを検出し、同期ステータスを評価し、オプションでout-of-sync設定を修正するアカウント。 AWS Network Security Manager は、サービスにリンクされたロールを介してメンバーアカウントで動作します。詳細については、「the section called “サービスにリンクされたロール”」を参照してください。

オプションで、各管理者をアカウント、OUs、ファイアウォールタイプのサブセットに絞り込むことができます。この機能を使用して、特定の分野の管理を異なるチームに委任します。

AWS Network Security Manager はリージョナルサービスです。クロスリージョンの依存関係なしで、リージョンごとにリソースとデプロイを作成します。

サービスにリンクされたロール

AWS Network Security Manager は、 という名前の IAM サービスにリンクされたロールAWSServiceRoleForNetworkSecurityManagerを使用して、ユーザーに代わって組織のメンバーアカウントで動作します。このロールはnetwork-security-manager.amazonaws.comサービスプリンシパルを信頼します。NetworkSecurityManagerServiceRolePolicy AWS 管理ポリシーを使用します。

AWS Network Security Manager は、サービスを有効にするとこのロールを自動的に作成するので、手動セットアップはありません。このロールにより、 AWS Network Security Manager は AWS WAF と AWS Shield Advanced の保護を管理し、Config AWS を通じて保護されたリソースを検出し、クロスアカウントオペレーションを実行できます。詳細については、「the section called “サービスリンクロール”」を参照してください。

AWS Network Security Manager のセットアップ

AWS Network Security Manager を使用すると、2 つの組織モデルで作業できます。1 つのアカウントで直接使用するか、 AWS Organizations で使用して、複数のアカウントにわたる保護を管理します。セットアップ手順は、選択したモデルによって異なります。

トピック

- 組織モデルを選択する
- シングルアカウント使用のための のセットアップ
- AWS Organizations でのマルチアカウント使用の設定
- AWS Network Security Manager 管理者アカウントの作成
- AWS Network Security Manager のアクセス許可を持つ IAM ID を作成する
- デフォルトでは無効になっているリージョンでの AWS Network Security Manager の使用

組織モデルを選択する

次の組織モデルから選択します。

- シングルアカウント – AWS Network Security Manager を使用して、1 つのアカウントのリソースを保護します。 AWS Organizations または管理者アカウントは必要ありません。 AWS Network Security Manager のアクセス許可を持つ IAM ID を作成し、直接サービスの使用を開始します。 AWS Network Security Manager は、 アカウントにサービスにリンクされたロールを自動的に作成します。
- マルチアカウント – Organizations で AWS AWS Network Security Manager を使用して、複数のアカウントにわたるリソースを保護します。このモードでは、 AWS Organizations の設定、信頼されたアクセスの有効化、管理者アカウントの作成が必要です。

シングルアカウント使用のための のセットアップ

1 つのアカウントで AWS Network Security Manager を使用するには、適切なアクセス許可を持つ IAM ID を作成し、サービスを直接使用を開始します。管理者アカウントを作成する必要はありません。 AWS Network Security Manager は、アカウントにサービスにリンクされたロールをバックグラウンドで自動的に作成します。「the section called “AWS Network Security Manager のアクセス許可を持つ IAM ID を作成する”」へ進んでください。

AWS Organizations でのマルチアカウント使用の設定

複数のアカウントで保護を管理するには、必要な AWS Organizations メンバーシップと設定を確立します。

1. 組織の AWS Network Security Manager 管理者として使用するアカウントを選択します。これは、 AWS Network Security Manager リソースを作成および管理するためのアカウントです。
2. 組織メンバーシップの確認 – 選択したアカウントがまだ組織のメンバーでない場合は、参加させます。「 Organizations ユーザーガイド」の「組織に参加する AWS アカウントを招待する」のガイダンスに従ってください。 AWS
3. 組織内のすべての機能を有効にする – AWS Organizations には、一括請求機能とすべての機能という 2 つの機能セットがあります。 AWS Network Security Manager を使用するには、すべての機能に対して組織を有効にする必要があります。組織が一括請求専用に設定されている場合は、AWS 「 Organizations ユーザーガイド」の「組織内のすべての機能を有効にする」のガイダンスに従ってください。
4. AWS Network Security Manager の信頼されたアクセスを有効にする – AWS Organizations の AWS Network Security Manager の信頼されたアクセスを有効にします。信頼されたアクセスを有効にすると、 AWS Network Security Manager はメンバーアカウントにサービスにリンクされたロールを作成し、メンバーアカウントに代わってリソースを管理できます。
5. 委任管理者アカウントを登録する – 選択したアカウントを AWS Organizations の AWS Network Security Manager の委任管理者として登録します。Organizations 管理アカウントを使用して、このステップを完了します。

> ⚠ 信頼されたアクセスをオフにすると、マルチアカウント保護が無効になります
>
> AWS Organizations で AWS Network Security Manager の信頼されたアクセスをオフにした場合、または委任管理者アカウントの登録を解除した場合、 AWS Network Security Manager はマルチアカウントのスコープとデプロイを `DISABLED`状態に設定し、管理する保護をクリーンアップします。

AWS Network Security Manager 管理者アカウントの作成

このステップは、マルチアカウントモードにのみ適用されます。 AWS Network Security Manager 管理者アカウントを作成できるのは、組織の管理アカウントのみです。

Organizations のセットアップが完了したら、アカウントを AWS Network Security Manager 管理者として登録します。これを行うには、 コンソールまたは コマンドラインインターフェイス (AWS CLI) AWS を使用します。

管理者アカウントを作成すると、 AWS Network Security Manager は組織内のすべてのアカウントにサービスにリンクされたロールを自動的に作成します。このロールにより、 AWS Network Security Manager はメンバーアカウントのリソースを検出し、保護を管理します。

AWS Network Security Manager を使用すると、組織のファイアウォールリソースを管理する複数の管理者を設定できます。組織内で複数の管理者を使用する場合は、各管理者に管理範囲条件を適用して、管理できるリソースを定義できます。これにより、組織内で異なる管理者ロールを持つ柔軟性が得られ、最小特権アクセスの原則を維持するのに役立ちます。たとえば、1 人の管理者が組織単位 (OUs) のセットを管理できます。別の管理者は、特定のポリシータイプのみを管理できます。

組織ごとに配置できる管理者の最大数については、「クォータ」を参照してください。

> **リージョン登録**
>
> AWS Network Security Manager 管理者アカウントを 1 つの AWS リージョンに登録します。追加のリージョンで AWS Network Security Manager を使用するには、各リージョンでこのステップを繰り返します。

コンソールを使用して管理者アカウントを作成するには

1. https://console.aws.amazon.com/network-security-manager/ で AWS Network Security Manager コンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。
3. 管理者の追加 を選択します。
4. アカウントを選択し、優先度の値 (1 ~ 10) を入力します。
5. 管理者の追加を選択して確認します。

CLI AWS を使用して管理者アカウントを作成するには

`PutAdminAccount` 操作を呼び出します。優先度値 (1 ~ 10) を指定する必要があります。

次の CLI AWS の例では、優先度 1 の AWS Network Security Manager 管理者としてアカウントを登録します。

```
aws network-security-manager put-admin-account \
    --account-id 123456789012 \
    --priority 1
```

複数の管理者アカウントを指定でき、それぞれに異なる優先順位が付けられます。必要に応じて、adminScopeパラメータを指定することで、各管理者を特定のアカウント、OUs、またはファイアウォールタイプに制限できます。

コンソールを使用して管理者アカウントを削除するには

> ⚠ 管理者を削除するとマルチアカウント保護が無効になる
>
> 管理者アカウントを削除すると、 AWS Network Security Manager はマルチアカウントの範囲とデプロイを DISABLED状態に設定し、管理する保護をクリーンアップします。

1. https://console.aws.amazon.com/network-security-manager/ で AWS Network Security Manager コンソールを開きます。
2. ナビゲーションペインで [設定] を選択します。
3. 削除する管理者アカウントを選択します。
4. [Remove administrator] (管理者を削除) を選択します。
5. 確認するには、管理者の削除の確認を選択します。

AWS Network Security Manager のアクセス許可を持つ IAM ID を作成する

AWS Network Security Manager を使用するには、 AWS Network Security Manager オペレーションを呼び出すアクセス許可を持つ IAM ID (ユーザーまたはロール) が必要です。IAM アクションはプレフィックス を使用しますnetwork-security-manager。

次の IAM ポリシーの例には、3 つのステートメントが含まれています。最初のステートメントは、すべての AWS Network Security Manager オペレーションへのフルアクセスを許可します。2 番目のステートメントは、 AWS Network Security Manager が必要とする追加の AWS Organizations お

よび AWS WAF アクセス許可を付与します。 AWS Network Security Manager は、これらのアクセス許可を使用して、組織内のアカウントと組織単位 (OUs) を識別し、使用可能な WAF ルールグループとマネージド製品を一覧表示します。これらのアクセス許可により、 AWS Network Security Manager は信頼されたアクセスを有効にし、委任された管理者 AWS を Organizations に登録することもできます。3 番目のステートメントは、 AWS Network Security Manager がサービスにリンクされたロールを作成するために必要な`iam:CreateServiceLinkedRole`アクセス許可を付与します。これは、シングルアカウントとマルチアカウントの両方で必要です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "network-security-manager:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAccountsForParent",
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "wafv2:ListRuleGroups",
                "wafv2:ListAvailableManagedRuleGroups",
                "wafv2:DescribeAllManagedProducts"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*"
        }
    ]
}
```

本番稼働用には、必要な最小限のアクセス許可のみを付与することをお勧めします。詳細については、「the section called “ID とアクセス管理”」を参照してください。

にサインアップする AWS アカウント

の使用を開始するには AWS、 が必要です AWS アカウント。の作成の詳細については AWS アカウント、「 AWS アカウント管理 リファレンスガイド」の「 の開始方法 AWS アカウント」を参照してください。

デフォルトでは無効になっているリージョンでの AWS Network Security Manager の使用

デフォルトでは無効になっているリージョンで AWS Network Security Manager を使用するには、組織の管理アカウントと AWS Network Security Manager 管理者アカウントの両方でリージョンを有効にする必要があります。デフォルトでは無効になっているリージョンとその有効化方法については、AWS 「 全般のリファレンス」のAWS 「リージョンの管理」を参照してください。

無効にしたリージョンを有効にするには

Organizations 管理アカウントと AWS Network Security Manager 管理者アカウントの両方について、AWS 「 全般のリファレンス」の「リージョンの有効化」のガイダンスに従ってください。

最初のネットワークセキュリティ保護をデプロイする

このチュートリアルでは、 AWS Network Security Manager コンソールを使用して AWS WAF ウェブ ACL をデプロイする方法について説明します。次の手順を実行します。

1. ルールの作成
2. テンプレートを作成する
3. ポリシーの作成
4. スコープを作成する
5. デプロイを作成して公開する
6. 同期ステータスのモニタリング

このチュートリアルでは、選択したアカウント全体で Application Load Balancer を保護する AWS WAF ウェブ ACL を作成します。このプロセスは、 AWS Network Security Manager でサポートされているすべてのセキュリティサービスとファイアウォールでほぼ同じです。

完了までの時間: 約 10 分

コスト: このチュートリアルでは、料金が発生する可能性のある AWS サービスを使用します。現在の料金については、 AWS ウェブサイトのAWS 「Network Security Manager の料金」を参照してください。

前提条件

開始する前に、次の要件を満たしていることを確認してください。

- 「」の説明に従って、セットアップ手順を完了しました AWS Network Security Manager のセットアップ。
- AWS Network Security Manager のアクセス許可を持つ AWS Identity and Access Management (IAM) ID。
- すべての機能が有効になっている AWS Organizations 組織と、指定された AWS Network Security Manager 管理者アカウント (マルチアカウントデプロイに必要) 。
- AWS Network Security Manager コンソールへのアクセス。

ステップ 1: ルールを作成する

ルールは、セキュリティ設定の構成要素です。このステップでは、2 つの AWS WAF ルールを作成します。1 つはデフォルトのアクションを設定するルール、もう 1 つは可視性設定を設定するルールです。デフォルトのアクションと VisibilityConfig は AWS 、WAF ウェブ ACL の必須フィールドです。

デフォルトアクションルールを作成するには、次の手順に従います。

1. https://console.aws.amazon.com/network-security-manager/ で AWS Network Security Manager コンソールを開きます。
2. ナビゲーションペインで、[概要] を選択します。
3. 概要ページで、ルールの作成を選択します。
4. ルール名には、 などのわかりやすい名前を入力しますmy-default-action-rule。
5. ルール定義セクションのファイアウォールタイプで AWS WAF を選択します。
6. Select type of rule で、Configuration を選択します。
7. 「設定タイプの挿入」を選択し、「デフォルトアクション」を選択します。JSON エディタがデフォルト設定で表示されます。
8. JSON エディタで、 Blockセクションを削除し、 Allowセクションのみを保持します。
9. [ルールを作成] を選択します。

VisibilityConfig ルールを作成するには、次の手順に従います。

1. ナビゲーションペインで、[概要] を選択します。
2. 概要ページで、ルールの作成を選択します。
3. ルール名には、 などのわかりやすい名前を入力しますmy-visibility-config-rule。
4. ルール定義セクションのファイアウォールタイプで AWS WAF を選択します。
5. Select type of rule で、Configuration を選択します。
6. 設定タイプの挿入を選択し、VisibilityConfig を選択します。JSON エディタがデフォルト設定で表示されます。
7. [ルールを作成] を選択します。

AWS CLI の代替

CLI AWS を使用してルールを作成することもできます。

```
aws network-security-manager create-rule \
    --rule-name "my-default-action-rule" \
    --firewall-type WAF \
    --rule-type CONFIGURATION \
    --configuration '{"DefaultAction": {"Allow": {}}}' \
    --is-published true

aws network-security-manager create-rule \
    --rule-name "my-visibility-config-rule" \
    --firewall-type WAF \
    --rule-type CONFIGURATION \
    --configuration '{"VisibilityConfig": {"SampledRequestsEnabled": true,
 "CloudWatchMetricsEnabled": true, "MetricName": "my-web-acl-metric"}}' \
    --is-published true
```

ステップ 2: テンプレートを作成する

テンプレートは、ポリシー間で再利用するために 1 つ以上のルールをグループ化します。このステップでは、ステップ 1 のルールを含むテンプレートを作成します。

1. ナビゲーションペインで、[概要] を選択します。
2. 概要ページで、テンプレートの作成を選択します。
3. テンプレート名には、 などのわかりやすい名前を入力しますmy-waf-template。
4. ファイアウォールタイプで、AWS WAF を選択します。
5. ルールセクションで、ルールの追加を選択し、ステップ 1 で作成したルールを選択します。
6. [テンプレートを作成] をクリックします。

AWS CLI の代替

CLI AWS を使用してテンプレートを作成することもできます。

```
aws network-security-manager create-template \
```

```
    --template-name "my-waf-template" \
    --firewall-type WAF \
    --associated-rule-list '[{"ruleIdentifier": "rule-arn-from-step-1"}]' \
    --is-published true
```

ステップ 3: ポリシーを作成する

ポリシーは、テンプレートと強制設定を組み合わせます。このステップでは、テンプレートを参照し、自動修復を有効にするポリシーを作成します。

1. ナビゲーションペインで、[概要] を選択します。
2. 概要ページで、ポリシーの作成を選択します。
3. ポリシー名にわかりやすい名前 (my-waf-policy など) を入力します。
4. ファイアウォールタイプで、AWS WAF を選択します。
5. ポリシーの優先度セクションには、既存のポリシーとその優先度が表示されます。新しいポリシーの優先度を確認します。調整する必要がある場合は、優先度フィールドを選択し、値を 1 または未使用の優先度番号に変更します。
6. テンプレートとルールセクションで、テンプレートの追加を選択し、ステップ 2 で作成したテンプレートを選択します。
7. 修復 で、有効 を選択します。
8. 既存のカスタマーウェブ ACL 解決で、修正なしを選択します。
9. [Create policy] (ポリシーの作成) を選択します。

AWS CLI の代替

CLI AWS を使用してポリシーを作成することもできます。

```
aws network-security-manager create-policy \
    --policy-name "my-waf-policy" \
    --firewall-type WAF \
    --priority 1 \
    --associated-template-and-rule-list '[{"templateIdentifier": "template-arn-
from-step-2"}]' \
    --policy-configuration '{"remediationEnabled": true, "resourcesCleanUp":
 false, "wafConfig": {"existingCustomerWebACLResolution": "NO_REMEDIATION"}}' \
```

```
    --is-published true
```

ステップ 4: スコープを作成する

スコープは、保護が適用される場所を定義します。このステップでは、アカウントの Application Load Balancer をターゲットとするスコープを作成します。

1. ナビゲーションペインで、[概要] を選択します。
2. 概要ページで、スコープの作成を選択します。
3. スコープ名には、 などのわかりやすい名前を入力しますmy-alb-scope。
4. (オプション) アカウントと組織単位の選択セクションで、管理範囲を制御する方法を選択するで、 AWS 組織全体 (すべての OUs とアカウント) の範囲を選択します。シングルアカウントデプロイの場合は、このステップをスキップします。
5. リソースセクションのリソースタイプで、Application Load Balancer を選択します。
6. [Create scope] (スコープの作成) を選択します。

AWS CLI の代替

CLI AWS を使用してスコープを作成することもできます。

```
aws network-security-manager create-scope \
    --scope-name "my-alb-scope" \
    --scope-configuration '{
        "accountFilter": {"includeAll": {}},
        "resourceScopes": {
            "AWS::ElasticLoadBalancingV2::LoadBalancer::application": {
                "includeAll": true
            }
        }
    }' \
    --is-published true
```

ステップ 5: デプロイを作成して公開する

デプロイはポリシーをスコープにバインドし、適用を有効にします。デプロイを作成して公開するには:

1. ナビゲーションペインで、[概要] を選択します。
2. 概要ページで、デプロイの作成を選択します。
3. デプロイ名には、 などのわかりやすい名前を入力しますmy-first-deployment。
4. ポリシーセクションで、ポリシーの追加を選択し、ステップ 3 で作成したポリシーを選択します。
5. 「スコープ」セクションで「スコープの追加」を選択し、ステップ 4 で作成したスコープを選択します。
6. [デプロイの作成] を選択します。

AWS Network Security Manager は、リソースの検出と保護の適用を開始します。このプロセスは非同期であり、完了までに数分かかる場合があります。

AWS CLI の代替

AWS CLI を使用してデプロイを作成して公開することもできます。

```
aws network-security-manager create-deployment \
    --deployment-name "my-first-deployment" \
    --associated-policy-list '[{"policyIdentifier": "policy-arn-from-step-3"}]'
 \
    --associated-scope-list '[{"scopeIdentifier": "scope-arn-from-step-4"}]' \
    --deployment-configuration '{"enableCrossAccountVisibility": true}' \
    --is-published true
```

ステップ 6: 同期ステータスをモニタリングする

デプロイを公開すると、 AWS Network Security Manager はリソースを検出し、その設定を同期します。各リソースのステータスをモニタリングするには:

1. ナビゲーションペインで、[概要] を選択します。

2. [デプロイ] タブを選択します。
3. ステップ 5 で作成したデプロイを選択します。
4. 同期タブを選択します。
5. 各リソースの同期ステータスを確認します。
   - IN_SYNC – リソース設定は、意図した保護設定と一致します。
   - OUT_OF_SYNC – リソース設定が一致しません。 AWS Network Security Manager は、修復が有効になっていると、これを自動的に修復します。
   - NOT_APPLICABLE – リソースは範囲内ですが、このデプロイでは評価できません。

> AWS CLI の代替
>
> AWS CLI で同期ステータスを確認することもできます。
>
> ```
> aws network-security-manager list-resource-synchronization-statuses \
>     --deployment-identifier "deployment-arn-from-step-5"
> ```

ステップ 7: クリーンアップする

作成したリソースが不要になった場合は、逆の順序で削除して適用を停止し、範囲内のリソースから保護を削除します。

これらのリソースは相互を参照するため、逆の順序が重要です。削除する前にリソースに関連付けられているものを確認するには、そのリソースの ARN `ListResourceAssociations`を使用してを呼び出します。関連付けられた各リソースの ARN とリソースタイプを返します。詳細については、AWS 「Network Security Manager API リファレンス」を参照してください。

1. ナビゲーションペインで、[概要] を選択します。[デプロイ] タブを選択します。デプロイを選択し、アクションを選択し、削除を選択します。
2. スコープタブを選択します。スコープを選択し、アクションを選択し、削除を選択します。
3. [Policies] タブを選択します。ポリシーを選択し、アクションを選択し、削除を選択します。
4. [テンプレート] タブを選択します。テンプレートを選択し、アクションを選択し、削除を選択します。
5. [Rules] (ルール) タブを選択します。ルールを選択し、アクションを選択し、削除を選択します。

AWS CLI の代替

リソースを削除する前に、その関連付けを確認して削除順序を計画します。

```
aws network-security-manager list-resource-associations \
    --resource-arn "resource-arn"
```

リソースにまだ関連付けがある場合は、まず関連付けられたリソースを削除または削除します。
CLI AWS を使用してリソースを逆の順序で削除できます。

```
aws network-security-manager delete-deployment \
    --deployment-identifier "deployment-arn"

aws network-security-manager delete-scope \
    --scope-identifier "scope-arn"

aws network-security-manager delete-policy \
    --policy-identifier "policy-arn"

aws network-security-manager delete-template \
    --template-identifier "template-arn"

aws network-security-manager delete-rule \
    --rule-identifier "rule-arn"
```

次の手順

正常にデプロイされたので、次の方法を調べてネットワークセキュリティ保護を拡張します。

- のリソースモデルとライフサイクルについて説明します AWS Network Security Manager の仕組み。
- ドラフト/公開ワークフローを使用して、変更が有効になる前にステージングします。詳細については、「the section called “ドラフトライフサイクルとアクティブライフサイクル”」を参照してください。
- スナップショットを作成して、既知の正常な設定を保持します。詳細については、「the section called “バージョニング”」を参照してください。

- を使用してGenerateRuleConfiguration、自然言語の説明からルールを作成します。詳細については、AWS 「Network Security Manager API リファレンス」を参照してください。
- 組織全体での AWS WAF および AWS Shield Advanced 保護の管理について説明します。詳細については、「ファイアウォールとセキュリティサービスの管理」を参照してください。

ファイアウォールとセキュリティサービスの管理

AWS Network Security Manager では、複数のファイアウォールとセキュリティサービスのセキュリティポリシーを定義してデプロイします。一般的な要素は AWS ネットワークセキュリティポートフォリオにまたがりますが、 AWS Network Security Manager 内で対処する必要がある重要なバリエーションがあります。

以下のサブセクションでは、サポートされているネットワークセキュリティサービスごとに、クイック作成と標準の詳細作成プロセスの両方の固有の要素と手順について説明します。

AWS WAF ACLs の管理

AWS Network Security Manager を使用すると、組織内のアカウントとリソース間で AWS WAF ウェブアクセスコントロールリスト (ウェブ ACLs) を一元的に設定してデプロイできます。 AWS WAF の AWS Network Security Manager ルールを定義し、保護テンプレートにグループ化して、 AWS Network Security Manager のポリシーとデプロイを通じて大規模に適用できます。

AWS WAF の概念

以下の概念は、 AWS WAF での AWS Network Security Manager の使用に固有のものです。 AWS Network Security Manager の仕組みの詳細については、「」を参照してください AWS Network Security Manager の仕組み。

AWS WAF ルールタイプ

AWS WAF の場合、ルールは 2 つのタイプのいずれかです。

- 検査 – (ユーザー定義ルールの前に実行されるルール) または `PreProcessFirewallManagerRuleGroups` (後に実行されるPostProcessFirewallManagerRuleGroupsルール) を使用するルールグループ定義が含まれます。
- CONFIGURATION – 単一のウェブ ACL 設定が含まれます。設定 JSON には、サポートされている設定
  (、Description、、DefaultAction、VisibilityConfig、、、、、TokenDomains、、など) に一致する最上位キーが 1 LoggingConfiguration CaptchaConfig ChallengeConfig CustomResponseBodies DataProtectionConfig

AssociationConfig OnSourceDDoSProtectionConfigつだけ含まれている必要がありますMonetizationConfig。

ほとんどのウェブ ACL 設定は、 AWS WAF CreateWebACLオペレーションのパラメータに対応しています。これらの設定とその定義の詳細については、AWS 「 WAF API リファレンス」のCreateWebACL」を参照してください。

例外は、個別に設定LoggingConfigurationする です。詳細については、「the section called “ログ記録”」を参照してください。

AWS WAF ポリシーのマージ

AWS WAF の場合、各設定は次のいずれかのマージ戦略を使用します。

SingleValue

1 つの値のみを持つことができる設定。優先度が最も高いポリシーが優先されます。優先度値は一意であるため、2 つのポリシーで同じ優先度で異なる値を定義することはできません。AWS Network Security Manager が優先度を解決する方法の詳細については、「」を参照してくださいthe section called “優先度ベースのポリシーマージ”。SingleValue を使用する設定は、DefaultAction、、VisibilityConfig、CaptchaConfig、ChallengeConfig、OnSourceDおよび ですDescription。

追加 (および AppendAndSort)

すべてのポリシーからのエントリは、優先度順にリストに追加されます。TokenDomainsおよび DataProtectionConfig.DataProtectionsは、追加を使用します。 PreProcessFirewallManagerRuleGroups および は、すべてのポリシーからルールグループを追加し、優先度でソートする AppendAndSort PostProcessFirewallManagerRuleGroupsを使用します。 AWS WAF はルールグループを順番に評価するので、順序は重要です。

Merge (マージ)

すべてのポリシーからのエントリは、優先度に関係なく 1 つのセットにマージされます。CustomResponseBodiesと はマージAssociationConfig.RequestBodyを使用します。

Append、AppendAndSort、Merge 戦略は、重複するエントリを削除します。2 つのポリシーが同じ設定を提供する場合、 AWS Network Security Manager は優先度の高いポリシーからエントリを保持

します。したがって、有効な設定には、寄与ポリシーごとに 1 つのコピーではなく、そのエントリの 1 つのコピーが含まれます。

既存のウェブ ACL 解決

AWS WAF ポリシーの `existingCustomerWebACLResolution`設定を使用して、 AWS Network Security Manager が既にカスタマーマネージドウェブ ACL を持つリソースを処理する方法を指定します。

- `RETROFIT` – 有効な設定に合わせて既存のウェブ ACL を更新します。
- `OVERRIDE_ASSOCIATION` – AWS Network Security Manager によって管理されるウェブ ACL を代わりにリソースに関連付けます。
- `NO_REMEDIATION` – ウェブ ACL が存在する場合は修復しないでください。

のウェブ ACL トラフィックのログ記録

ポリシーの `LoggingConfiguration`設定でウェブ ACL ログ記録を制御します。 AWS Network Security Manager は AWS 、WAF `PutLoggingConfiguration`オペレーションを使用してこの設定を適用します。Web ACL ごとに 1 つのログ記録先を定義できます。詳細については、AWS「 WAF API リファレンス」のPutLoggingConfiguration」を参照してください。

ポリシーが管理するすべての対象範囲内のウェブ ACL は、ポリシーが指定した宛先にログを送信します。これにより、組織内のアカウント全体でログ記録を一元化できます。これを使用して、ウェブ ACLs が組織全体で分析するトラフィックに関する詳細情報を取得します。

複数のアカウントを一元的にログ記録するには、Amazon S3 バケットまたは Amazon Data Firehose 配信ストリームにログを送信できます。各送信先タイプには追加の設定が必要です。これは、 AWS Network Security Manager が範囲内のリソースとアカウント全体で AWS WAF ログ記録を管理する前に完了する必要があります。送信先名は で始まる必要がありますaws-waf-logs-。

Amazon Data Firehose

次の特性を持つ配信ストリームを作成します。

- AWS Network Security Manager 管理者アカウントを使用して作成
- で始まる名前`aws-waf-logs-`。例: `aws-waf-logs-network-security-manager-central`
- PUT ソース

- 運用しているリージョンで作成、または Amazon CloudFront のログをキャプチャする場合は米国東部 (バージニア北部) リージョンで作成

配信ストリームを使用する前に、それをテストして、組織のログに十分なスループットがあることを確認します。詳細については、「Amazon Data Firehose デベロッパーガイド」の「Amazon Data Firehose 配信ストリームの作成」を参照してください。

Amazon S3

AWS WAF デベロッパーガイドの Amazon S3 ガイダンスに従ってバケットを作成します。また、ログ配信に書き込みを許可するアクセス許可でバケットを設定する必要があります。次のバケットポリシーは、これらのアクセス許可を付与します。

```
{
    "Version":"2012-10-17",
    "Id": "AWSLogDeliveryForNetworkSecurityManager",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheckNetworkSecurityManager",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-logs-bucket-suffix"
        },
        {
            "Sid": "AWSLogDeliveryWriteNetworkSecurityManager",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::aws-waf-logs-bucket-suffix/policy-id/AWSLogs/
*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

bucket-suffix を独自のバケット名のサフィックスに置き換え、*policy-id* をポリシーの ID に置き換えます。

> **CloudWatch Logs はシングルアカウントの使用のみをサポートします**
>
> 複数のアカウントで AWS Network Security Manager を使用する場合、Amazon CloudWatch Logs ロググループを ログ記録先として使用することはできません。ロググループは、ウェブ ACL と同じ AWS アカウントとリージョンに存在する必要があります。マルチアカウントデプロイの場合は、代わりに Amazon S3 バケットまたは Amazon Data Firehose 配信ストリームを使用します。

AWS WAF のクイック作成

クイック作成では、単一のガイド付きワークフローで AWS WAF 保護を定義してデプロイします。1 つのセッションでのデプロイを通じてルールからの完全なウェブ ACL 保護を設定する場合は、クイック作成を使用します。

クイック作成で AWS WAF 保護を定義してデプロイするには、次の手順を順番に実行します。

ポリシーを作成して保護を追加するには

1. https://console.aws.amazon.com/network-security-manager/ で AWS Network Security Manager コンソールを開きます。
2. ナビゲーションペインで、[概要] を選択します。
3. 概要ページの右上で、クイック作成とデプロイを選択します。クイック作成およびデプロイページが複数のペインで表示されます。
4. ポリシーの詳細ペインの「名前」にポリシー名を入力します。(オプション) [説明] に説明を入力します。
5. 保護の定義ペインで、使用するファイアウォールタイプを選択します。AWS WAF を選択します。テンプレートとルールのサブペインが表示され、ルールまたはテンプレートを追加できます。
6. ルールを追加するには、ルールの追加または管理を選択します。表示されるウィンドウで、ルールタイプの選択で、次のいずれかを選択します。
   - AWS マネージドルール – テーブルには、 AWS WAF がサポートするすべての AWS マネージドルールが表示されます。

- ルール – テーブルには、 AWS マネージドルール以外の所有する AWS WAF ルールグループが表示されます。

  ポリシーに追加するルールのチェックボックスをオンにします。次に、ルールの追加を選択します。

7. テンプレートを追加するには、テンプレートの追加を選択します。表示されるテンプレートの追加ウィンドウで、使用可能なテンプレートがテーブルに表示されます。ポリシーに含めるバージョンとともに、必要なテンプレートを選択します。次に、テンプレートの追加を選択します。

ポリシーを設定するには

1. テンプレートとルール表で選択内容を確認します。Position 列の整数は、ルールとテンプレートの評価順序を決定します。評価の順序を変更するには、Position 列で position 値を選択します。矢印を使用して値を変更します。変更を受け入れるには、確認を選択します。変更を元に戻すには、キャンセルを選択します。
2. 保護の定義ペインのポリシー設定で、 AWS Network Security Manager が対象範囲内で実行する自動アクションを決定します。
   - 修復は、 AWS Network Security Manager で説明されている目的の状態とセキュリティ状態が同期されていないリソースに、定義されたポリシーを適用します。
   - リソースクリーンアップは、デプロイが削除されたとき、またはアカウントまたはリソースが範囲外になったときに、 AWS Network Security Manager がリソース用に作成したファイアウォールを削除します。
   - 既存のカスタマー WebACL 解決により、定義しているポリシーと既にデプロイされているポリシー間の競合を解決する方法が決まります。メニューから、次のいずれかのオプションを選択します。
     - ウェブ ACL が既に存在するリソースでは、修復はスキップされません。
     - 関連付けを上書きすると、既存のウェブ ACL が AWS Network Security Manager が作成したウェブ ACL に置き換えられます。
     - Retrofit は、既存の各ウェブ ACL にルールを改良し、リソースに関連付けられたウェブ ACL を保持します。
3. ポリシーの優先度ペインで、優先度を設定します。 AWS Network Security Manager は優先度に従ってポリシーを評価し、競合を解決します。低い位置 (低い整数) の方が優先度が高くなります。優先度を編集するには、位置の値を選択します。次に、矢印で増分するか、値を直接入力

します。選択を確認するには、確認を選択します。変更を破棄するには、キャンセルを選択します。

スコープを設定するには

1. スコープの設定ペインで、ポリシーが適用されるアセットのセットを定義します。スコープ名には、名前を入力します。(オプション) [説明] に説明を入力します。
2.

> **マルチアカウントモードのみ**
>
> このステップは、マルチアカウントモードにのみ適用されます。マルチアカウントモードでは、アカウントと組織単位の選択サブペインを使用して、含めるまたは除外するアカウントまたは OUs を選択します。シングルアカウントモードでは、このサブペインはコンソールに表示されないため、このステップはスキップします。

アカウントと組織単位の選択サブペインで、次のいずれかのオプションを選択します。

- AWS 組織全体にスコープします。これ以上の定義は必要ありません。
- AWS 組織全体にスコープしますが、特定の OUs。組織単位サブペインとアカウントサブペインが表示されます。組織単位を除外するには、OUs の追加を選択します。組織ツリー内の組織単位を選択し、OUs の追加を選択します。個々のアカウントを除外するには、アカウントの追加を選択します。組織ツリー内のアカウントを選択し、アカウントの追加を選択します。
- Organization 全体を対象とするのではなく AWS 、特定の OUsとアカウントのみを含めます。同じ OUs の追加 および アカウントの追加 メカニズムを使用して、必要な組織単位とアカウントを含めます。

3. リソースサブペインのリソースタイプで、すべてまたは特定の AWS WAF リソースタイプを選択します。オプションは、次のいずれかまたは複数です。
   - Application Load Balancer
   - Amazon API Gateway REST API
   - CloudFront ディストリビューション

> **CloudFront リージョンの要件**
>
> CloudFront Distribution リソースを保護するには、米国東部 (バージニア北部) リージョン () を使用しますus-east-1。

> **グローバルリソースタイプとリージョンリソースタイプ**
>
> グローバルリソースタイプ (CloudFront ディストリビューション) またはリージョンリソースタイプ (Application Load Balancer と Amazon API Gateway REST API) を選択できますが、両方を選択することはできません。リソースタイプを選択した後、設定を更新するときに CloudFront Distribution とリージョンリソースタイプを切り替えることはできません。

> **アンマネージド CloudFront リソース**
>
> AWS Network Security Manager は、CloudFront 定額料金プランまたは CloudFront ステージングディストリビューションを使用する CloudFront ディストリビューションを管理しません。これらのリソースは同期外に表示されます。

4. 選択したリソースタイプごとに、次のいずれかの相互に排他的なオプションを選択します。
   - [すべてのリソースを含める]
   - 特定のリソースを含める
   - 特定のリソースを除外する
5. 特定のリソースを含めるを選択した場合は、次のいずれかの式タイプを選択し、タグまたは ARNs。
   - 単一の条件
   - すべての条件に一致 (AND)
   - 任意の条件に一致 (OR)
   - NOT

   すべてのリソースタイプには、タグと ARN の包含基準があります。タグを選択した場合は、キーとオプションの値を入力します。複数のタグを識別できます。リソースタイプが Application Load Balancer の場合、追加の設定条件が表示されます。設定内で、インターネット向けまたは内部用のオプションがあるスキームを選択します。

ポリシーを確認してデプロイするには

1. 確認とデプロイペインで、デプロイ名に名前を入力します。(オプション) [説明] に説明を入力します。デプロイのコンテンツが組織内の他のアカウントに表示されるかどうかを確認するには、このデプロイのクロスアカウント可視性を有効にするを選択します。
2. (オプション) リソースにタグを追加するには、新しいタグを追加を選択し、キーとオプションの値の組み合わせを入力します。
3. 定義したものを実行するには、作成とデプロイを選択します。プロセスが完了すると、デプロイページが表示され、作成された内容の詳細を確認できます。

> ⚠ デプロイには料金が発生する場合があります
>
> デプロイでは、ネットワークセキュリティサービスを作成し、保護されたリソースにアタッチします。 AWS Network Security Manager は、保護されたリソースに対して課金します。セキュリティサービス自体がリソースを保護し、追加料金が発生します。デプロイする前に、AWS Network Security Manager の料金ページと AWS WAF の料金ページを確認してください。

AWS WAF の標準作成プロセス

標準の作成プロセスでは、ルール、テンプレート、ポリシー、スコープ、デプロイなどの各 AWS WAF コンポーネントを個別に作成して、完全に制御します。このアプローチは、再利用可能なコンポーネントを作成し、必要に応じて組み合わせる場合に使用します。

AWS Network Security Manager AWS WAF ポリシーには、ルールとテンプレートを含めることができます。ポリシーを適用すると、 AWS Network Security Manager は対象範囲内の各アカウントにウェブ ACL を作成します。

ルールを作成するには (コンソール)

1. AWS Network Security Manager 管理者アカウントを使用して AWS マネジメントコンソールにサインインし、https://console.aws.amazon.com/network-security-manager/ で AWS Network Security Manager コンソールを開きます。

> **管理者アカウントのセットアップ**
>
> AWS Network Security Manager 管理者アカウントの設定については、「」を参照してください AWS Network Security Manager のセットアップ。

2. ナビゲーションペインで、AWS Network Security Manager を選択し、概要を選択します。
3. 概要ペインで、ルールの作成を選択します。わかりやすい名前を入力し、オプションの Description を入力します。
4. ルール定義ペインのファイアウォールタイプで AWS WAF を選択します。
5. ルールのタイプ で、検査または設定を選択します。

   Inspection を選択すると、ルールグループ参照の定義という名前の JSON エディタペインが以下のオプションとともに表示されます。

   - テンプレートを挿入 – 最初の (前処理) ルールまたは最後の (後処理) ルールの JSON テンプレートを選択します。選択を行うと、 AWS Network Security Manager は対応する JSON をエディタに挿入し、テンプレートを完了するために入力が必要な場合は警告アイコンも挿入します。
   - ルールグループを挿入 – 次の 3 つのオプションによって駆動される選択リストを表示します。
     - AWS マネージドルール (AMR) ルールグループ
     - 既存のカスタムルールグループ
     - AWS Marketplace ルールグループ

     AWS Network Security Manager は、選択したルールグループを表示し、包含する 1 つのインスタンスを選択できます。選択したら、ルールグループの選択を選択します。 AWS Network Security Manager は、正しい構文で検査ルールへの参照を JSON エディタに挿入します。
   - AI で挿入 – AI 設定ジェネレーターという名前のオーバーレイウィンドウを開きます。このツールを使用してルールをプレーン言語で記述すると、 AWS Network Security Manager は関連する JSON をエディタで生成します。その後、生成されたコードを確認し、出力を承認、変更、または削除することを選択できます。
6. (オプション) JSON ルール定義が完了したら、タグをルールに関連付けることができます。これを行うには、[Add new tag] (タグの追加) を選択してから、キーとオプションの値を入力します。
7. 定義が完了したら、ドラフトを保存を選択して非アクティブで不完全なオブジェクトを保存するか、ルールを作成します。

> ⚠ ウェブ ACL 名は永続的です
>
> 作成後にウェブ ACL 名を変更することはできません。ポリシーの名前を更新しても、AWS Network Security Manager は関連付けられたウェブ ACL 名を更新しません。 AWS Network Security Manager で別の名前のウェブ ACL を作成するには、新しいポリシーを作成する必要があります。

テンプレートを作成するには (コンソール)

テンプレートは、ポリシー内で評価するためのルールを優先度順にアセンブルします。ルールタイプをセキュリティ目標に沿ったグループに整理できます。また、さまざまなチームが各自の責任とスキルに合ったセキュリティコントロールステートメントを構築することもできます。

1. 概要ページの概要ペインで、テンプレートの作成を選択します。テンプレートの作成ページで、テンプレート名を入力し、オプションの 説明を入力し、ファイアウォールタイプ (この場合は AWS WAF) を選択します。
2. ファイアウォールタイプを選択すると、ルールペインが表示されます。2 つのルールの追加ボタンのいずれかを選択して、使用可能なルールのリストを開きます。ルール名の左側にあるチェックボックスをオンにして、テンプレートに追加します。ルールの特定のバージョンを選択するには、ルールのバージョンフィールドを選択します。複数のバージョンが利用可能な場合は、必要なバージョンを選択し、確認を選択します。
3. (オプション) テンプレートのタグを作成します。完了したら、ドラフトの保存またはテンプレートの作成を選択します。ポリシーの作成を続行するには、テンプレートの作成を選択します。

- ポリシーを作成するには (コンソール)

これは、ポリシー定義とデプロイの準備の最終ステップです。

1. 概要ページの概要ペインで、ポリシーの作成を選択します。ポリシーの作成ページで、名前とオプションの説明を入力し、ファイアウォールタイプ (この場合は AWS WAF) を選択します。
2. ポリシーの優先度ペインで、優先度を設定します。 AWS Network Security Manager は優先度に従ってポリシーを評価し、競合を解決します。低い位置 (低い整数) の方が優先度が高くなります。優先度を編集するには、位置の値を選択します。次に、矢印で増分するか、値を直接入力し

ます。選択を確認するには、確認 を選択します。変更を破棄するには、キャンセルを選択します。

3. ポリシー設定ペインで、 AWS Network Security Manager が対象範囲内で実行する自動アクションを決定します。
   - 修復は、 AWS Network Security Manager で説明されている目的の状態とセキュリティ状態が同期されていないリソースに、定義されたポリシーを適用します。
   - リソースクリーンアップは、デプロイが削除されたとき、またはアカウントまたはリソースが範囲外になったときに、 AWS Network Security Manager がリソース用に作成したファイアウォールを削除します。
   - 既存のカスタマー WebACL 解決により、定義しているポリシーと既にデプロイされているポリシー間の競合を解決する方法が決まります。メニューから、次のいずれかのオプションを選択します。
     - ウェブ ACL が既に存在するリソースでは、修復はスキップされません。
     - 関連付けを上書きすると、既存のウェブ ACL が AWS Network Security Manager が作成したウェブ ACL に置き換えられます。
     - Retrofit は、既存の各ウェブ ACL にルールを改良し、リソースに関連付けられたウェブ ACL を保持します。
4. これらの設定が完了したら、ポリシーに追加するルールとテンプレートを選択します。テンプレートとルールペインで、ルールの追加またはテンプレートの追加を選択してポリシーを入力します。どちらのプロセスも、このセクションで前述したルール選択プロセスと同じ方法で動作するウィンドウを開きます。

スコープを作成するには (コンソール)

1. このステップは、概要ページまたはツール内の他の領域から開始できます。スコープの詳細ペインで、スコープ名とオプションの説明を入力します。
2. **マルチアカウントモードのみ**

   このステップは、マルチアカウントモードにのみ適用されます。マルチアカウントモードでは、アカウントと組織単位の選択サブペインを使用して、含めるまたは除外するアカウントまたは OUs を選択します。シングルアカウントモードでは、このサブペインはコンソールに表示されないため、このステップはスキップします。

アカウントと組織単位の選択ペインで、管理範囲を制御する 3 つの方法のいずれかを選択します。

- AWS 組織全体 (すべての OUs とアカウント) を対象とする – これ以上の定義は必要ありません。
- AWS 組織全体を対象とするが、特定の OUsとアカウントを除外する – 2 つのサブペインが表示されます。1 つは組織単位用、もう 1 つはアカウント用です。OUs の追加OUs の追加 ウィンドウを開き、組織ツリーから必要な組織単位を選択し、OUs」を選択します。個々のアカウントを追加するには、アカウントサブペインでアカウントの追加を選択し、組織ツリーからアカウントを選択し、アカウントの追加を選択します。
- Organization 全体を対象とするのではなく AWS 、特定の OUs とアカウントのみを含める – 同じサブペインを使用して、前述のオプションで説明したのと同じメカニズムを持つ OUs またはアカウントを追加します。

3. 次に、リソースサブペインでリソースを選択します。リソースタイプの選択ボックスで、すべてまたは特定の AWS WAF リソースタイプを選択します。 AWS WAF の場合、オプションは次のいずれかまたはすべてです。
   - Application Load Balancer
   - Amazon API Gateway REST API
   - CloudFront ディストリビューション

> **CloudFront リージョンの要件**
>
> CloudFront Distribution リソースを保護するには、米国東部 (バージニア北部) リージョン () を使用しますus-east-1。

> **グローバルリソースタイプとリージョンリソースタイプ**
>
> グローバルリソースタイプ (CloudFront ディストリビューション) またはリージョンリソースタイプ (Application Load Balancer と Amazon API Gateway REST API) を選択できますが、両方を選択することはできません。リソースタイプを選択した後、設定を更新するときに CloudFront Distribution とリージョンリソースタイプを切り替えることはできません。

> **アンマネージド CloudFront リソース**
>
> AWS Network Security Manager は、CloudFront 定額料金プランまたは CloudFront ステージングディストリビューションを使用する CloudFront ディストリビューションを管理しません。これらのリソースは同期外に表示されます。

4. 選択したリソースタイプごとに、次のいずれかの相互に排他的なオプションを選択します。
   - [すべてのリソースを含める]
   - 特定のリソースを含める
   - 特定のリソースを除外する
5. 特定のリソースを含める を選択した場合は、次のいずれかの式タイプを選択します。
   - 単一の条件
   - すべての条件に一致 (AND)
   - 任意の条件に一致 (OR)
   - NOT
6. 各式タイプは、単一または複数の包含基準と ARNs をサポートしているため、タグまたは ARNs の組み合わせを構築できます。すべてのリソースタイプは、タグと ARN の包含基準をサポートしています。タグを選択した場合は、キーとオプションの値を指定します。複数のタグを識別できます。
7. Application Load Balancer の場合、追加の設定条件が表示されます。設定内では、インターネット向けまたは内部のオプションを使用してスキームを設定できます。

デプロイを作成するには (コンソール)

デプロイはポリシーをスコープにバインドし、適用をアクティブ化します。これにより、 AWS Network Security Manager は WAF AWS ルールをスコープ内のリソースに適用します。

1. 概要ページの概要ペインで、デプロイの作成を選択します。ツール内の他の領域からこのステップを開始することもできます。
2. デプロイするポリシーを選択します。
3. AWS Network Security Manager がポリシーを適用するアカウントとリソースを定義するスコープを選択します。

4. デプロイ名に名前を入力します。(オプション) [説明] に説明を入力します。
5. (オプション) デプロイを組織内の他のアカウントに表示するには、このデプロイのクロスアカウント可視性を有効にするを選択します。
6. (オプション) タグを追加するには、新しいタグを追加を選択し、キーとオプションの値の組み合わせを入力します。
7. [Create and deploy] (作成してデプロイ) を選択します。デプロイページが表示され、 AWS Network Security Manager が作成した内容の詳細を確認できます。

> ⚠ デプロイには料金が発生する場合があります
>
> デプロイでは、ネットワークセキュリティサービスを作成し、保護されたリソースにアタッチします。 AWS Network Security Manager は、保護されたリソースに対して課金します。セキュリティサービス自体がリソースを保護し、追加料金が発生します。デプロイする前に、AWS Network Security Manager の料金ページと AWS WAF の料金ページを確認してください。

Shield Advanced の DDoS AWS 保護の管理

AWS Network Security Manager を使用すると、組織内のアカウントとリソース間で AWS Shield Advanced 保護を一元的に設定してデプロイできます。DDoS 保護ポリシーを定義し、 AWS Network Security Manager のポリシーとデプロイを通じて大規模に適用できます。

> ⓘ AWS Network Security Manager は個別に請求されます
>
> AWS Network Security Manager は Shield Advanced AWS オファーの一部ではありません。料金の詳細については、AWS 「Network Security Manager の料金」およびAWS 「Shield Advanced の料金」を参照してください。

> ⚠ AWS Shield Advanced サブスクリプション
>
> アクティブなデプロイにそのスコープにアカウントが含まれている場合、 AWS Network Security Manager はそのアカウントを Shield Advanced AWS にサブスクライブします。AWS Network Security Manager は、アカウントがスコープを離れるか、デプロイを削除してもサブスクリプションをキャンセルしません。 AWS Shield Advanced サブスクリプショ

ンをキャンセルするには、「 WAF デベロッパーガイド」の「Shield Advanced AWS へのサブスクライブ」を参照してください。 AWS

Shield Advanced AWS のクイック作成

クイック作成では、Shield Advanced AWS 保護を定義して単一のガイド付きワークフローにデプロイします。1 つのセッションでのデプロイを通じてポリシーからの DDoS 保護を設定する場合は、クイック作成を使用します。

クイック作成で AWS Shield Advanced 保護を定義してデプロイするには、次の手順を順番に実行します。

ポリシーを作成して保護を設定するには

以下のステップを実行します。

1. https://console.aws.amazon.com/network-security-manager/ で AWS Network Security Manager コンソールを開きます。
2. ナビゲーションペインで、[概要] を選択します。
3. 概要ページで、クイック作成とデプロイを選択します。クイック作成およびデプロイページが複数のペインで表示されます。
4. ポリシーの詳細ペインで、名前にポリシー名を入力します。(オプション) [説明] に説明を入力します。
5. 保護の定義ペインで、使用するファイアウォールタイプを選択します。AWS Shield Advanced を選択します。
6. 保護の定義ペインのポリシー設定で、 AWS Network Security Manager が対象範囲内で実行する自動アクションを決定します。
   - 修復は、セキュリティ状態が AWS Network Security Manager が記述する目的の状態と一致しないリソースに、定義されたポリシーを適用します。
   - リソースクリーンアップは、デプロイが削除されたとき、またはアカウントまたはリソースが範囲外になったときに、 AWS Network Security Manager がリソース用に作成した DDoS 保護を削除します。
   - 既存のお客様の DDoS 解決により、定義しているポリシーと既にデプロイされているポリシー間の競合を解決する方法が決まります。メニューから、次のいずれかのオプションを選択します。

- DDoS DDoS 保護がすでにあるリソースに対する修復は、修復をスキップしません。
- 関連付けを上書きすると、既存の DDoS 保護が AWS Network Security Manager が作成した DDoS 保護に置き換えられます。
- Retrofit は、既存の各 DDoS 保護にルールを改良し、リソースに関連付けられた DDoS 保護を維持します。

7. ポリシーの優先度ペインで、優先度を設定します。 AWS Network Security Manager は優先度に従ってポリシーを評価し、競合を解決します。低い位置 (低い整数) の方が優先度が高くなります。

   優先度を編集するには、位置の値を選択します。次に、矢印で増分するか、値を直接入力します。選択を確認するには、確認を選択します。変更を破棄するには、キャンセルを選択します。

スコープを設定するには

以下のステップを実行します。

1. スコープの設定ペインで、ポリシーが適用されるアセットのセットを定義します。スコープ名に名前を入力します。(オプション) [説明] に説明を入力します。
2.

   > **マルチアカウントモードのみ**
   >
   > このステップは、マルチアカウントモードにのみ適用されます。マルチアカウントモードでは、アカウントと組織単位の選択サブペインを使用して、含めるまたは除外するアカウントまたは OUs を選択します。シングルアカウントモードでは、このサブペインはコンソールに表示されないため、このステップはスキップします。

   アカウントと組織単位の選択サブペインで、次のいずれかのオプションを選択します。

   - AWS 組織全体にスコープします。これ以上の定義は必要ありません。
   - Organization 全体を対象とし AWS ますが、特定の OUsとアカウントを除外します。組織単位サブペインとアカウントサブペインが表示されます。組織単位を除外するには、OUs」を選択します。組織ツリーで組織単位を選択し、OUs の追加を選択します。個々のアカウントを除外するには、アカウントの追加を選択します。組織ツリー内のアカウントを選択し、アカウントの追加を選択します。

- Organization 全体を対象とするのではなく AWS 、特定の OUsとアカウントのみを含めます。同じ OUs の追加とアカウントの追加メカニズムを使用して、必要な組織単位とアカウントを含めます。

3. リソースサブペインのリソースタイプで、すべてまたは特定の AWS Shield Advanced リソースタイプを選択します。オプションは、次のいずれかまたは複数です。
   - Application Load Balancer
   - CloudFront ディストリビューション
   - Classic Load Balancer
   - Elastic IP アドレス
4. 選択したリソースタイプごとに、次のいずれかの相互に排他的なオプションを選択します。
   - [すべてのリソースを含める]
   - 特定のリソースを含める
   - 特定のリソースを除外する
5. 特定のリソースを含めるを選択した場合は、次のいずれかの式タイプを選択し、タグまたはARNs。
   - 単一の条件
   - すべての条件に一致 (AND)
   - 任意の条件に一致 (OR)
   - NOT

   すべてのリソースタイプには、タグと ARN の包含基準があります。タグを選択した場合は、キーとオプションの値を入力します。複数のタグを識別できます。

> **CloudFront リージョンの要件**
>
> CloudFront Distribution リソースを保護するには、米国東部 (バージニア北部) リージョン () を使用しますus-east-1。

ポリシーを確認してデプロイするには

以下のステップを実行します。

1. 確認とデプロイペインで、デプロイ名に名前を入力します。(オプション) [説明] に説明を入力します。デプロイのコンテンツが組織内の他のアカウントに表示されるかどうかを確認するには、このデプロイのクロスアカウント可視性を有効にするを選択します。
2. (オプション) リソースにタグを追加するには、新しいタグを追加を選択し、キーとオプションの値の組み合わせを入力します。
3. ポリシーとスコープを作成してデプロイするには、作成してデプロイを選択します。プロセスが完了すると、デプロイページが表示され、 AWS Network Security Manager が作成した内容の詳細を確認できます。

> ⚠ デプロイには料金が発生する場合があります
>
> デプロイでは、ネットワークセキュリティサービスを作成し、保護されたリソースにアタッチします。 AWS Network Security Manager は、保護されたリソースに対して課金します。セキュリティサービス自体がリソースを保護し、追加料金が発生します。デプロイする前に、AWS Network Security Manager の料金ページと AWS Shield Advanced の料金ページを確認してください。

Shield Advanced AWS の標準作成プロセス

標準の作成プロセスでは、ポリシー、スコープ、デプロイなどの各 AWS Shield Advanced コンポーネントを個別にセットアップして、完全な制御を行います。このアプローチは、再利用可能なコンポーネントを作成し、必要に応じて組み合わせる場合に使用します。

AWS Shield Advanced ポリシーはシンプルで、ルール、ルールグループ、テンプレートは含まれません。ポリシーを適用すると、 AWS Network Security Manager は範囲内の各アカウントに AWS Shield Advanced DDoS 保護を作成します。 AWS Network Security Manager の仕組みについては、「」を参照してください AWS Network Security Manager の仕組み。

- ポリシーを作成するには (コンソール)

以下のステップを実行します。

1. AWS Network Security Manager 管理者アカウントを使用して AWS マネジメントコンソールにサインインし、https://console.aws.amazon.com/network-security-manager/ で AWS Network Security Manager コンソールを開きます。

> **管理者アカウントの設定**
>
> AWS Network Security Manager 管理者アカウントの設定については、「」を参照してください AWS Network Security Manager のセットアップ。

2. ナビゲーションペインで、AWS Network Security Manager を選択し、概要を選択します。
3. 概要ペインで、ポリシーの作成を選択します。名前とオプションの説明を入力し、ファイアウォールタイプ (この場合は AWS Shield Advanced) を選択します。
4. ポリシーの優先度ペインで、優先度を設定します。 AWS Network Security Manager は優先度に従ってポリシーを評価し、競合を解決します。低い位置 (低い整数) の方が優先度が高くなります。

   優先度を編集するには、位置の値を選択します。次に、矢印で増分するか、値を直接入力します。選択を確認するには、確認を選択します。変更を破棄するには、キャンセルを選択します。
5. ポリシー設定ペインで、 AWS Network Security Manager が対象範囲内で実行する自動アクションを決定します。
   - 修復は、定義されたポリシーを、 AWS Network Security Manager が記述する目的の状態とセキュリティ状態が一致しないすべてのリソースに適用します。
   - リソースクリーンアップは、デプロイが削除されたとき、またはアカウントまたはリソースが範囲外になったときに、 AWS Network Security Manager がリソース用に作成した DDoS 保護を削除します。
   - 既存のお客様の DDoS 解決により、定義しているポリシーと既にデプロイされているポリシー間の競合を解決する方法が決まります。メニューから、次のいずれかのオプションを選択します。
     - DDoS DDoS 保護がすでに存在するリソースに対する修復は、修復をスキップしません。
     - 関連付けを上書きすると、既存の DDoS 保護が AWS Network Security Manager が作成した DDoS 保護に置き換えられます。
     - Retrofit は、既存の各 DDoS 保護にルールを改良し、リソースに関連付けられた DDoS 保護を維持します。

スコープを作成するには (コンソール)

以下のステップを実行します。

1. スコープの詳細ペインで、スコープ名とオプションの説明を入力します。
2. **マルチアカウントモードのみ**

   このステップは、マルチアカウントモードにのみ適用されます。マルチアカウントモードでは、アカウントと組織単位の選択サブペインを使用して、含めるまたは除外するアカウントまたは OUsを選択します。シングルアカウントモードでは、このサブペインはコンソールに表示されないため、このステップはスキップします。

   アカウントと組織単位の選択ペインで、管理範囲を制御する 3 つの方法のいずれかを選択します。

   - AWS 組織全体 (すべての OUs とアカウント) を対象とする – これ以上の定義は必要ありません。
   - AWS 組織全体を対象とするが、特定の OUs とアカウントを除外する – 2 つのサブペインが表示されます。1 つは組織単位用、もう 1 つはアカウント用です。OUs の追加 を選択して OUs の追加 ウィンドウを開き、必要な組織単位を選択し、OUs の追加 を選択します。個々のアカウントを追加するには、「アカウント」サブペインで「アカウントの追加」を選択し、「アカウントの追加」を選択します。
   - AWS Organization 全体を対象とするのではなく、特定の OUs とアカウントのみを含める – 同じサブペインを使用して OUs またはアカウントを追加します。
3. 次に、リソースサブペインでリソースを選択します。リソースタイプの選択ボックスで、すべてまたは特定の AWS Shield Advanced リソースタイプを選択します。 AWS Shield Advanced の場合、オプションは次のいずれかまたはすべてです。
   - Application Load Balancer
   - CloudFront ディストリビューション
   - Classic Load Balancer
   - Elastic IP アドレス
4. 選択したリソースタイプごとに、次のいずれかの相互に排他的なオプションを選択します。
   - [すべてのリソースを含める]
   - 特定のリソースを含める
   - 特定のリソースを除外する
5. 特定のリソースを含める を選択した場合は、次のいずれかの式タイプを選択します。
   - 単一の条件

- すべての条件に一致 (AND)
- 任意の条件に一致 (OR)
- NOT

6. 各式タイプは、単一または複数の包含基準と ARNs をサポートしているため、タグまたは ARNs の組み合わせを構築できます。すべてのリソースタイプは、タグと ARN の包含基準をサポートしています。タグを選択した場合は、キーとオプションの値を指定します。複数のタグを識別できます。

> **CloudFront リージョンの要件**
>
> CloudFront Distribution リソースを保護するには、米国東部 (バージニア北部) リージョン () を使用しますus-east-1。

デプロイを作成するには (コンソール)

デプロイはポリシーをスコープにバインドし、適用を有効にします。 AWS Network Security Manager AWS は、Shield Advanced DDoS 保護をスコープ内のリソースに適用します。

以下のステップを実行します。

1. 概要ページの概要ペインで、デプロイの作成を選択します。
2. デプロイするポリシーを選択します。
3. AWS Network Security Manager がポリシーを適用するアカウントとリソースを定義するスコープを選択します。
4. デプロイ名に名前を入力します。(オプション) [説明] に説明を入力します。
5. (オプション) デプロイを組織内の他のアカウントに表示するには、このデプロイのクロスアカウント可視性を有効にするを選択します。
6. (オプション) タグを追加するには、新しいタグを追加を選択し、キーとオプションの値の組み合わせを入力します。
7. [Create and deploy] (作成してデプロイ) を選択します。デプロイページが表示され、 AWS Network Security Manager が作成した内容の詳細を確認できます。

⚠ デプロイには料金が発生する場合があります

デプロイでは、ネットワークセキュリティサービスを作成し、保護されたリソースにアタッチします。 AWS Network Security Manager は、保護されたリソースに対して課金します。セキュリティサービス自体がリソースを保護し、追加料金が発生します。デプロイする前に、AWS Network Security Manager の料金ページと AWS Shield Advanced の料金ページを確認してください。

AWS Network Security Manager と AWS Firewall Manager

AWS Network Security Manager は、 AWS Firewall Manager を置き換えるサービスです。これら 2 つは完全に独立したサービスであり、それぞれに固有の機能と異なる料金モデルがあります。現在 AWS Firewall Manager を使用している場合は、何もする必要はありません。既存のファイアウォールとポリシーは引き続き機能します。この章では、2 つのサービスの共存方法、両方を使用する場合の優先順位、および利用可能になったときの移行の仕組みについて説明します。

AWS Network Security Manager と AWS Firewall Manager は、並行して、互いに独立して動作します。ある時点で、 AWS Firewall Manager は販売を停止し、その後動作を停止します。

AWS Firewall Manager との共存

AWS Network Security Manager は、変更するアクションを開始しない限り、 AWS Firewall Manager で作成したファイアウォールには影響しません。Firewall Manager で AWS 作成したファイアウォールとポリシーは、終了しない限り引き続き動作します。これは、 AWS Firewall Manager が廃止された後でも当てはまります。

修復中の優先順位

両方のサービスが動作している間、 AWS Firewall Manager で作成したファイアウォールに影響を与えるアクションを実行できます。 AWS Network Security Manager ポリシーを作成するときは、一連のターゲットリソースであるスコープに適用します。そのスコープに AWS Firewall Manager ポリシーが既に対処しているリソースが含まれている場合、修復中に AWS Network Security Manager が優先されます。この場合、 AWS Network Security Manager ポリシーとスコープは、既存の AWS Firewall Manager ファイアウォールとポリシーを上書きします。特定の動作は、選択した解決オプションによって異なります。

AWS Firewall Manager からの計画された移行

AWS Firewall Manager から AWS Network Security Manager に移行すると、ファイアウォール管理が 1 つのサービスに統合され、その機能を使用できます。移行は計画されていますが、まだ利用できません。移行が利用可能になると、 AWS Firewall Manager ポリシーを AWS Network Security Manager に移動できるようになります。移行するには、まだ導入されていない両方のサービスで新しいアクションが必要です。

計画されたプロセスでは、選択したポリシーを AWS Firewall Manager からコピーし、 AWS Network Security Manager に転送して、新しいポリシー構造に変換します。このプロセスは、 AWS Firewall Manager の元のポリシーまたは関連するファイアウォールには影響しません。

AWS Network Security Manager のセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを活用できます。

セキュリティは、 AWS とお客様の間の責任共有です。責任共有モデル では、これをクラウドのセキュリティとクラウド内 のセキュリティとして説明しています：

- クラウドのセキュリティ – AWS は、 で AWS サービスを実行するインフラストラクチャを保護する責任を担います AWS クラウド。 は、お客様が安全に使用できるサービス AWS も提供します。サードパーティーの監査者は、AWS コンプライアンスプログラムコンプライアンスプログラムの一環として、当社のセキュリティの有効性を定期的にテストおよび検証。 AWS Network Security Manager に適用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、 AWS Network Security Manager を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するように AWS Network Security Manager を設定する方法について説明します。また、 AWS Network Security Manager リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- AWS Network Security Manager でのデータ保護
- AWS Network Security Manager の Identity and Access Management
- AWS Network Security Manager のサービスにリンクされたロールの使用
- AWS Network Security Manager のコンプライアンス検証
- AWS Network Security Manager の耐障害性
- AWS Network Security Manager のインフラストラクチャセキュリティ
- AWS Network Security Manager のセキュリティのベストプラクティス

AWS Network Security Manager でのデータ保護

責任共有モデル、 AWS Network Security Manager AWS でのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「Data Privacy FAQChina」を参照してください。 欧州におけるデータ保護に関する情報については、General Data Protection Regulation (GDPR) Center を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM アイデンティティセンターまたは AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、または SDK を使用して AWS Network Security Manager AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

保管中の暗号化

AWS Network Security Manager は、 AWS Key Management Service (AWS KMS) キーを使用して保管中のすべてのデータを暗号化します。サービスマネージド KMS キーは、リソース設定、デプロイ状態、同期データを保護します。これらのキーを設定または管理する必要はありません。

転送中の暗号化

AWS Network Security Manager は、Transport Layer Security (TLS) を使用して転送中のすべてのデータを暗号化します。すべての API リクエストには TLS 1.2 以降が必要です。 AWS Network Security Manager API エンドポイントへの接続では、HTTPS のみが使用されます。

キー管理

AWS Network Security Manager は、保管時の暗号化にサービスマネージド AWS KMS キーを使用します。現時点では、独自の KMS キーを指定することはできません。

AWS Network Security Manager の Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS Network Security Manager リソースの使用を許可する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

トピック

- オーディエンス
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- AWS Network Security Manager と IAM の連携方法
- AWS Network Security Manager のアイデンティティベースのポリシーの例
- AWS Network Security Manager の ID とアクセスのトラブルシューティング

オーディエンス

AWS Identity and Access Management (IAM) の使用方法は、ロールによって異なります。

- サービスユーザー - 機能にアクセスできない場合は、管理者にアクセス許可をリクエストします (「AWS Network Security Manager の ID とアクセスのトラブルシューティング」を参照)。
- サービス管理者 - ユーザーアクセスを決定し、アクセス許可リクエストを送信します (「AWS Network Security Manager と IAM の連携方法」を参照)
- IAM 管理者 - アクセスを管理するためのポリシーを作成します (「AWS Network Security Manager のアイデンティティベースのポリシーの例」を参照)

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。、IAM ユーザー AWS アカウントのルートユーザー、または IAM ロールを引き受けることで認証される必要があります。

AWS IAM アイデンティティセンター (IAM Identity Center)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーティッド ID としてサインインできます。サインインの詳細については、「AWS サインイン ユーザーガイド」の「AWS アカウントにサインインする方法」を参照してください。

プログラムによるアクセスの場合、 は SDK と CLI AWS を提供してリクエストを暗号化して署名します。詳細については、「IAM ユーザーガイド」の「API リクエストに対するAWS 署名バージョン 4」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、まず、すべての AWS のサービス および リソースへの完全なアクセス権を持つ AWS アカウント root ユーザーと呼ばれる 1 つのサインインアイデンティティから始めます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザー認証情報を必要とするタスクについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーテッドアイデンティティ

ベストプラクティスとして、人間のユーザーが一時的な認証情報 AWS のサービス を使用して にアクセスするには、ID プロバイダーとのフェデレーションを使用する必要があります。

フェデレーティッド ID は、エンタープライズディレクトリ、ウェブ ID プロバイダー、または ID ソースの認証情報 AWS のサービス を使用して Directory Service にアクセスするユーザーです。フェデレーテッドアイデンティティは、一時的な認証情報を提供するロールを引き受けます。

アクセスを一元管理する場合は、 AWS IAM アイデンティティセンターをお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「IAM アイデンティティセンターとは」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、特定の個人やアプリケーションに対する特定のアクセス許可を持つアイデンティティです。長期認証情報を持つ IAM ユーザーの代わりに一時的な認証情報を使用することをお勧めします。詳細については、IAM ユーザーガイドの「ID プロバイダーとのフェデレーションを使用して にアクセスすることを人間 AWS のユーザーに要求する」を参照してください。

IAM グループは、IAM ユーザーの集合を指定し、大量のユーザーに対するアクセス許可の管理を容易にします。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可を持つアイデンティであり、一時的な認証情報を提供します。ユーザーから IAM ロール (コンソール) に切り替えるか、 または API オペレーションを呼び出すことで、ロールを引き受けることができます。 AWS CLI AWS 詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーのアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行するアプリケーションに役立ちます。詳細については、IAM ユーザーガイド の IAM でのクロスアカウントリソースアクセス を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは、アイデンティティまたはリソースに関連付けられている場合のアクセス許可を定義します。 は、プリンシパルがリクエストを行うときにこれらのポリシー AWS を評価します。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は、ポリシーを使用して、どのプリンシパルがどのリソースに対して、どのような条件でアクションを実行できるかを定義することで、誰が何にアクセスできるかを指定します。

デフォルトでは、ユーザーやロールにアクセス許可はありません。IAM 管理者は IAM ポリシーを作成してロールに追加し、このロールをユーザーが引き受けられるようにします。IAM ポリシーは、オペレーションの実行方法を問わず、アクセス許可を定義します。

アイデンティティベースのポリシー

アイデンティティベースのポリシーは、アイデンティティ (ユーザー、グループ、またはロール) にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、アイデンティティがどのリソースに対してどのような条件下でどのようなアクションを実行できるかを制御します。アイデンティティベースポリシーの作成方法については、IAM ユーザーガイド の カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する を参照してください。

アイデンティティベースのポリシーは、インラインポリシー (単一の ID に直接埋め込む) または管理ポリシー (複数の ID にアタッチされたスタンドアロンポリシー) にすることができます。管理ポリシーとインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。例としては、IAM ロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

その他のポリシータイプ

AWS は、より一般的なポリシータイプによって付与されるアクセス許可の上限を設定できる追加のポリシータイプをサポートしています。

- アクセス許可の境界 – アイデンティティベースのポリシーで IAM エンティティに付与することのできるアクセス許可の数の上限を設定します。詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可境界」を参照してください。
- サービスコントロールポリシー (SCP) - AWS Organizations内の組織または組織単位の最大のアクセス許可を指定します。詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。

- リソースコントロールポリシー (RCP) – は、アカウント内のリソースで利用できる最大数のアクセス許可を定義します。詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。
- セッションポリシー – ロールまたはフェデレーションユーザーの一時セッションを作成する際にパラメータとして渡される高度なポリシーです。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成されるアクセス許可を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

AWS Network Security Manager と IAM の連携方法

IAM を使用して AWS Network Security Manager へのアクセスを管理する前に、 AWS Network Security Manager で使用できる IAM 機能を確認してください。

IAM 機能	AWS Network Security Manager のサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	あり
ポリシー条件キー	あり
ACL	なし
ABAC (ポリシー内のタグ)	あり
一時的な認証情報	あり
プリンシパルアクセス権限	あり

IAM 機能	AWS Network Security Manager のサポート
サービスロール	あり
サービスリンクロール	はい

AWS Network Security Manager およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要については、IAM ユーザーガイドのAWS 「IAM と連携する のサービス」を参照してください。

AWS Network Security Manager のアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

AWS Network Security Manager 内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーで、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、全体のアカウント、または別のアカウントの IAM エンティティを、リソースベースのポリシーのプリンシパルとして指定します。詳細については、IAM ユーザーガイドのIAM でのクロスアカウントリソースアクセスを参照してください。

AWS Network Security Manager はリソースベースのポリシーをサポートしていません。

AWS Network Security Manager のポリシーアクション

ポリシーアクションのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

AWS Network Security Manager アクションのリストを確認するには、「サービス認可リファレンス」のAWS 「Network Security Manager で定義されるアクション」を参照してください。

AWS Network Security Manager のポリシーアクションは、アクションの前に次のプレフィックスを使用します。

```
network-security-manager
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "network-security-manager:action1",
      "network-security-manager:action2"
         ]
```

AWS Network Security Manager は、リソースタイプ全体で IAM アクションを定義します。これには、ルール、テンプレート、ポリシー、スコープ、デプロイの作成、読み取り、更新、削除 (CRUD) オペレーション、スナップショット、タグ付け、管理、同期ステータス、リソース関連付けオペレーションが含まれます。

AWS Network Security Manager のポリシーリソース

ポリシーリソースのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Resource JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。リソースレベルのアクセス許可をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

AWS Network Security Manager リソースタイプとその ARNsAWS 「Network Security Manager で定義されるリソース」を参照してください。 各リソースの ARN を指定できるアクションについては、AWS 「Network Security Manager で定義されるアクション」を参照してください。

AWS Network Security Manager は、各リソースの IAM リソースタイプ (ルール、テンプレート、ポリシー、スコープ、デプロイ) と、各リソースのスナップショットタイプ (例:) を定義しますrule-snapshot。ARN 形式は以下です:

```
arn:aws:network-security-manager:{region}:{account}:{resource-type}:{resource-id}
```

ドラフト ARNsバージョン番号 (例:) を追加:DRAFTし、スナップショット ARNs はバージョン番号を追加します:3。

ドラフトは個別の IAM リソースタイプではありません。承認の場合、ドラフトは親であるアクティブなリソースの子として扱われます。:DRAFT修飾 ARN はアクティブなリソースに対して を許可するため、ドラフトを操作するアクセス許可は、そのアクティブなリソースを操作するアクセス許可から取得されます。

スナップショットはドラフトとは異なります。各スナップショットは独自の IAM リソースタイプであるため、バージョン修飾 ARN は親アクティブリソースではなく、そのスナップショットリソースタイプに対して直接認可します。

AWS Network Security Manager のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素は、定義された基準に基づいてステートメントが実行される時期を指定します。イコールや未満などの条件演算子を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「グローバル条件コンテキストキー」を参照してください。

AWS Network Security Manager の条件キーのリストを確認するには、「サービス認可リファレンス」のAWS 「Network Security Manager の条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、AWS 「Network Security Manager で定義されるアクション」を参照してください。

AWS Network Security Manager は、属性ベースのアクセスコントロール (ABAC) で次の AWS グローバルタグ条件キーをサポートしています。

- aws:ResourceTag/${TagKey}
- aws:RequestTag/${TagKey}
- aws:TagKeys

タグベースの条件キーは、アクティブなリソースとスナップショットに適用されます。ドラフトリソースはタグ付けできず、aws:ResourceTag条件をサポートしていません。

AWS Network Security Manager ACLs

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするためのアクセス許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

AWS Network Security Manager は、アクセスコントロールリスト (ACLsをサポートしていません。

AWS Network Security Manager での ABAC

ABAC (ポリシー内のタグ) のサポート: あり

属性ベースのアクセス制御 (ABAC) は、タグと呼ばれる属性に基づいてアクセス許可を定義する認可戦略です。IAM エンティティと AWS リソースにタグをアタッチし、プリンシパルのタグがリソースのタグと一致するときにオペレーションを許可するように ABAC ポリシーを設計できます。

タグに基づいてアクセスを管理するには、aws:ResourceTag/*key-name*、aws:RequestTag/*key-name*、または aws:TagKeys の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセス制御 (ABAC) を使用する」を参照してください。

AWS Network Security Manager は、3 つの AWS グローバルタグ条件キーすべてを使用した属性ベースのアクセスコントロールをサポートしています。 AWS Network Security Manager リソースへのアクセスは、それらのリソースにアタッチされたタグに基づいて制限できます。

AWS Network Security Manager での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一時的な認証情報は AWS 、リソースへの短期的なアクセスを提供し、フェデレーションまたはスイッチロールの使用時に自動的に作成されます。長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成 AWS することをお勧めします。詳細については、「IAM ユーザーガイド」の「IAM の一時的な認証情報」および「AWS のサービス と IAM との連携」を参照してください。

AWS Network Security Manager のクロスサービスプリンシパルのアクセス許可

転送アクセスセッション (FAS) のサポート: あり

転送アクセスセッション (FAS) は、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする を使用します。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

AWS Network Security Manager のサービスロール

サービスロールのサポート: あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細につい

ては、IAM ユーザーガイドの AWS のサービスに許可を委任するロールを作成するを参照してください。

> **Warning**
>
> サービスロールのアクセス許可を変更すると、 AWS Network Security Manager の機能が破損する可能性があります。 AWS Network Security Manager が指示する場合にのみ、サービスロールを編集します。

AWS Network Security Manager のサービスにリンクされたロール

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

AWS Network Security Manager は、サービスにリンクされたロールを使用して、組織のメンバーアカウントで動作します。サービスを有効にすると、 AWS Network Security Manager によってサービスにリンクされたロールが自動的に作成されます。このロールは、 AWS WAF および Shield Advanced リソースを管理するアクセス許可を AWS Network Security Manager AWS に付与します。このロールは、リソース検出用の AWS Config へのアクセスと、クロスアカウントオペレーションを実行するアクセス許可も付与します。

AWS Network Security Manager のサービスにリンクされたロールの作成と管理の詳細については、「」を参照してくださいthe section called “サービスリンクロール”。

AWS Network Security Manager のアイデンティティベースのポリシーの例

デフォルトでは、ユーザーとロールには AWS Network Security Manager リソースを作成または変更するアクセス許可はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。

これらのサンプルの JSON ポリシードキュメントを使用して IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーを作成する (コンソール)」を参照してください。

各リソースタイプの ARN の形式など、 AWS Network Security Manager で定義されるアクションとリソースタイプの詳細については、「サービス認可リファレンス」のAWS 「Network Security Manager のアクション、リソース、および条件キー」を参照してください。 ARNs

トピック

- ポリシーに関するベストプラクティス
- AWS Network Security Manager コンソールの使用
- 自分の権限の表示をユーザーに許可する
- AWS Network Security Manager への読み取り専用アクセス
- ルールとテンプレートのみを管理する

ポリシーに関するベストプラクティス

ID ベースのポリシーは、アカウント内で誰かが AWS Network Security Manager リソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションでは、 AWS アカウントに費用が発生する場合があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、IAM ユーザーガイド の AWS マネージドポリシー または ジョブ機能のAWS マネージドポリシー を参照してください。
- 最小特権を適用する – IAM ポリシーでアクセス許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイド の IAM でのポリシーとアクセス許可 を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する – ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます CloudFormation。詳細については、IAM ユーザーガイド の IAM JSON ポリシー要素:条件 を参照してください。

- IAM アクセスアナライザー を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する – IAM アクセスアナライザー は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイド の IAM Access Analyzer でポリシーを検証する を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、MFA をオンにしてセキュリティを強化します。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイド の MFA を使用した安全な API アクセス を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイド の IAM でのセキュリティのベストプラクティス を参照してください。

AWS Network Security Manager コンソールの使用

AWS Network Security Manager コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の AWS Network Security Manager リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

AWS Network Security Manager コンソールにアクセスするには、プリンシパルに `network-security-manager:List*`および `network-security-manager:Get*`アクションに対する最小限のアクセス許可が必要です。

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Network Security Manager への読み取り専用アクセス

次のポリシーは、すべての AWS Network Security Manager リソースへの読み取り専用アクセスをプリンシパルに付与します。これは、変更を加えずに設定と同期ステータスを表示する必要がある監査者またはモニタリングロールに役立ちます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "network-security-manager:Get*",
                "network-security-manager:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

ルールとテンプレートのみを管理する

次のポリシーでは、ポリシー、スコープ、デプロイへのアクセスを許可せずに、プリンシパルがルールとテンプレートを作成、更新、削除することを許可します。これは、セキュリティ設定を作成するが、適用を制御しないチームに役立ちます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "network-security-manager:CreateRule",
                "network-security-manager:GetRule",
                "network-security-manager:UpdateRule",
                "network-security-manager:DeleteRule",
                "network-security-manager:ListRules",
                "network-security-manager:CreateRuleSnapshot",
                "network-security-manager:ListRuleSnapshots",
                "network-security-manager:CreateTemplate",
                "network-security-manager:GetTemplate",
                "network-security-manager:UpdateTemplate",
                "network-security-manager:DeleteTemplate",
                "network-security-manager:ListTemplates",
                "network-security-manager:CreateTemplateSnapshot",
                "network-security-manager:ListTemplateSnapshots",
                "network-security-manager:TagResource",
                "network-security-manager:UntagResource",
                "network-security-manager:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Network Security Manager の ID とアクセスのトラブルシューティング

以下の情報は、 AWS Network Security Manager と IAM の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちます。

トピック

- AWS Network Security Manager でアクションを実行する権限がない
- iam:PassRole を実行する権限がありません
- 自分の 以外のユーザーに AWS Network Security Manager リソース AWS アカウント へのアクセスを許可したい

AWS Network Security Manager でアクションを実行する権限がない

アクションを実行する権限がないというエラーが表示された場合は、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要な network-security-manager:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 network-security-manager:GetWidget on resource: my-example-widget
```

この場合、network-security-manager:*GetWidget* アクションを使用して *my-example-widget* リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がありません

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、 AWS ポリシーを更新して Network Security Manager にロールを渡すことができるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡すアクセス許可が必要です。

次の例のエラーは、 という IAM ユーザーがコンソールを使用して AWS Network Security Manager `marymajor` でアクションを実行しようとすると発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与されたアクセス許可が必要です。Mary には、ロールをサービスに渡すアクセス許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに `iam:PassRole` アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

自分の 以外のユーザーに AWS Network Security Manager リソース AWS アカウントへのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- AWS Network Security Manager がこれらの機能をサポートしているかどうかを確認するには、「」を参照してくださいAWS Network Security Manager と IAM の連携方法。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、「IAM ユーザーガイド」の「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティーが所有する へのアクセスを提供する AWS アカウント」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイド の 外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可 を参照してください。

- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

AWS Network Security Manager のサービスにリンクされたロールの使用

AWS Network Security Manager は、IAM サービスにリンクされたロールを使用します。サービスにリンクされたロールは、 AWS Network Security Manager に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは AWS Network Security Manager によって事前定義されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、 AWS Network Security Manager の設定が簡単になります。 AWS Network Security Manager は、サービスにリンクされたロールのアクセス許可を定義します。特に定義されている場合を除き、AWS Network Security Manager のみがそのロールを引き受けることができます。定義された許可には、信頼ポリシーと許可ポリシーが含まれます。そのアクセス許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスにリンクされたロールを削除できるのは、関連するリソースを最初に削除した後のみです。これにより、リソースへのアクセス許可が誤って削除されないため、 AWS Network Security Manager リソースが保護されます。

サービスにリンクされたロールをサポートする他のサービスについては、AWS 「IAM と連携するサービス」を参照し、「サービスにリンクされたロール」列で「はい」を含むサービスを探してください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

AWS Network Security Manager のサービスにリンクされたロールのアクセス許可

AWS Network Security Manager は、 という名前のサービスにリンクされたロールを使用しますAWSServiceRoleForNetworkSecurityManager。このサービスにリンクされたロールは、network-security-manager.amazonaws.comサービスプリンシパルを信頼してロールを引き受けます。

という名前のロールアクセス許可ポリシーNetworkSecurityManagerServiceRolePolicyは、AWS AWS Network Security Manager が指定されたリソースに対するアクションを完了できるようにする マネージドポリシーです。

次の信頼ポリシーは、network-security-manager.amazonaws.comサービスプリンシパルがロールを引き受けることを許可します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "network-security-manager.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

> **Note**
>
> サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するにはアクセス許可を設定する必要があります。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールのアクセス権限」() を参照してください。

アクセス許可の詳細

AWS Network Security Manager では、アカウントと組織全体のリソースを保護して検出するためのアクセス許可の各グループが必要です。NetworkSecurityManagerServiceRolePolicy 管理ポリシーは、サービスごとにグループ化された次のアクセス許可を付与します。

- wafv2 – ウェブ ACLs。保護されたリソースとのウェブ ACLs関連付けと関連付け解除。ウェブ ACL ログ記録設定とルールグループのアクセス許可ポリシーを管理します。 リソースのタグ付けおよびタグ付け解除を行う。 AWS Network Security Manager のウェブ ACL とルール設定を検証します。
- shield – Shield Advanced AWS 保護を作成、説明、一覧表示、削除します。Shield Advanced AWS サブスクリプションを作成して記述します。

- elasticloadbalancing – Application Load Balancer とタグについて説明します。Application Load Balancer でウェブ ACL 関連付けを作成、削除、および設定します。
- cloudfront – Amazon CloudFront ディストリビューション、設定、タグを取得して一覧表示します。ディストリビューションウェブ ACLs関連付けと関連付け解除。VPC オリジンの読み取り。
- apigateway – Amazon API Gateway REST APIs、ステージ、タグを読み込みます。API ステージでウェブ ACL を設定します。
- ec2 – Amazon EC2 Verified Access インスタンスのウェブ ACLsと関連付けを読み取ります。Shield Advanced 保護用の AWS Elastic IP アドレスについて説明します。
- cognito-idp、apprunner、appsync、amplify、 bedrock-agentcore- Amazon Cognito ユーザープール、 AWS App Runner サービス AWS AppSync 、GraphQL APIs、 AWS Amplify アプリケーション、Amazon Bedrock AgentCore ゲートウェイのウェブ ACL 関連付けを読み取り、AWS Network Security Manager が保護されたリソースを検出できるようにします。
- config – リソース設定を選択し、 AWS Network Security Manager が対象範囲内のリソースを検出するために使用するサービスにリンクされた AWS Config 設定レコーダーを管理します。
- organizations – AWS Network Security Manager が組織全体で運用できるように、組織、アカウント、ルート、組織単位、委任された管理者を読み取ります。
- logs – ウェブ ACL ログ記録のログ配信を作成、読み取り、更新、削除、一覧表示します。
- s3 – 名前が で始まる Amazon S3 バケットにバケットポリシーを取得して配置aws-waf-logs-し、ウェブ ACL ログを配信できるようにします。
- iam – Shield Advanced AWS Config、および AWS WAF AWS が必要とするサービスにリンクされたロールを、 iam:AWSServiceName条件キーでスコープして作成します。

次の JSON は、完全なNetworkSecurityManagerServiceRolePolicyアクセス許可ポリシーを示しています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LogsGeneral",
      "Effect": "Allow",
      "Action": [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
```

```
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3LogBucketGeneral",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource": "arn:aws:s3:::aws-waf-logs-*"
    },
    {
      "Sid": "CloudfrontVpcOriginAccess",
      "Effect": "Allow",
      "Action": [
        "cloudfront:GetVpcOrigin"
      ],
      "Resource": "arn:aws:cloudfront::*:vpcorigin/*"
    },
    {
      "Sid": "ConfigUnscoped",
      "Effect": "Allow",
      "Action": [
        "config:SelectResourceConfig"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DescribeOrganizationUnScoped",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    },
```

```
    {
      "Sid": "DescribeAccountScoped",
      "Effect": "Allow",
      "Action": "organizations:DescribeAccount",
      "Resource": "arn:aws:organizations::*:account/o-*/*"
    },
    {
      "Sid": "DescribeOrganizationUnitScoped",
      "Effect": "Allow",
      "Action": "organizations:DescribeOrganizationalUnit",
      "Resource": "arn:aws:organizations::*:ou/o-*/ou-*"
    },
    {
      "Sid": "ListDelegatedAdministratorsScoped",
      "Effect": "Allow",
      "Action": "organizations:ListDelegatedAdministrators",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "network-security-manager.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "LoadBalancerNonMutationApiAccess",
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeWebACLAssociation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "LoadBalancerGetWebACLScoped",
      "Effect": "Allow",
      "Action": "elasticloadbalancing:GetLoadBalancerWebACL",
      "Resource": "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid": "CloudFrontDistributionNonMutationApiAccess",
      "Effect": "Allow",
```

```
      "Action": [
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListTagsForResource"
      ],
      "Resource": "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid": "ApiGatewayStageNonMutationApiAccess",
      "Effect": "Allow",
      "Action": "apigateway:GET",
      "Resource": [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*"
      ]
    },
    {
      "Sid": "Wafv2General",
      "Effect": "Allow",
      "Action": [
        "wafv2:TagResource",
        "wafv2:ListResourcesForWebACL",
        "wafv2:AssociateWebACL",
        "wafv2:ListTagsForResource",
        "wafv2:UntagResource",
        "wafv2:GetWebACL",
        "wafv2:DisassociateFirewallManager",
        "wafv2:DeleteWebACL",
        "wafv2:DisassociateWebACL",
        "wafv2:ValidateNetworkSecurityManagerWebACLConfiguration",
        "wafv2:ValidateNetworkSecurityManagerRuleConfiguration"
      ],
      "Resource": "arn:aws:wafv2:*:*:*/webacl/*"
    },
    {
      "Sid": "Wafv2WebAclAndRuleGroupMutation",
      "Effect": "Allow",
      "Action": [
        "wafv2:UpdateWebACL",
        "wafv2:CreateWebACL",
        "wafv2:DeleteFirewallManagerRuleGroups",
        "wafv2:PutFirewallManagerRuleGroups"
```

```
      ],
      "Resource": [
        "arn:aws:wafv2:*:*:*/webacl/*",
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/ipset/*",
        "arn:aws:wafv2:*:*:regional/ipset/*",
        "arn:aws:wafv2:*:*:global/regexpatternset/*",
        "arn:aws:wafv2:*:*:regional/regexpatternset/*"
      ]
    },
    {
      "Sid": "Wafv2Logging",
      "Effect": "Allow",
      "Action": [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource": "arn:aws:wafv2:*:*:*/webacl/*"
    },
    {
      "Sid": "Wafv2ListLogging",
      "Effect": "Allow",
      "Action": "wafv2:ListLoggingConfigurations",
      "Resource": "*"
    },
    {
      "Sid": "Wafv2ListWebACLs",
      "Effect": "Allow",
      "Action": "wafv2:ListWebACLs",
      "Resource": "*"
    },
    {
      "Sid": "Wafv2PermissionPolicy",
      "Effect": "Allow",
      "Action": [
        "wafv2:PutPermissionPolicy",
        "wafv2:GetPermissionPolicy",
        "wafv2:DeletePermissionPolicy"
      ],
      "Resource": [
```

```
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*"
      ]
    },
    {
      "Sid": "Wafv2WebaclDescribe",
      "Effect": "Allow",
      "Action": "wafv2:GetWebACLForResource",
      "Resource": "arn:aws:wafv2:*:*:*/webacl/*"
    },
    {
      "Sid": "CloudFrontListDistributions",
      "Effect": "Allow",
      "Action": [
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListDistributions"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudFrontDistributionMutation",
      "Effect": "Allow",
      "Action": [
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:DisassociateDistributionWebACL"
      ],
      "Resource": "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid": "ElbWebAclRemediationScoped",
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:CreateWebACLAssociation",
        "elasticloadbalancing:DeleteWebACLAssociation"
      ],
      "Resource": "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid": "ElbSetWebAcl",
      "Effect": "Allow",
      "Action": "elasticloadbalancing:SetWebACL",
      "Resource": "*"
    },
    {
```

```
      "Sid": "ApiGatewayWebAclRemediation",
      "Effect": "Allow",
      "Action": "apigateway:SetWebACL",
      "Resource": "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
    {
      "Sid": "CognitoWebAclIntegration",
      "Effect": "Allow",
      "Action": [
        "cognito-idp:GetWebACLForResource",
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AppRunnerWebAclIntegration",
      "Effect": "Allow",
      "Action": [
        "apprunner:DescribeWebAclForService",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource": "*"
    },
    {
      "Sid": "VerifiedAccessWebAclIntegration",
      "Effect": "Allow",
      "Action": [
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AppSyncWebAclIntegration",
      "Effect": "Allow",
      "Action": [
        "appsync:GetWebACLForResource",
        "appsync:ListResourcesForWebACL"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AmplifyWebAclIntegration",
      "Effect": "Allow",
```

```
      "Action": [
        "amplify:GetWebACLForResource",
        "amplify:ListResourcesForWebACL"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ShieldGeneral",
      "Effect": "Allow",
      "Action": [
        "shield:CreateProtection",
        "shield:DeleteProtection",
        "shield:DescribeProtection",
        "shield:ListProtections",
        "shield:CreateSubscription",
        "shield:DescribeSubscription",
        "shield:GetSubscriptionState",
        "ec2:DescribeAddresses",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ShieldSlrCreation",
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/shield.amazonaws.com/*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "shield.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowConfigRecorderList",
      "Effect": "Allow",
      "Action": "config:ListConfigurationRecorders",
      "Resource": "*"
    },
    {
      "Sid": "AllowPutServiceLinkedConfigRecorder",
      "Effect": "Allow",
      "Action": "config:PutServiceLinkedConfigurationRecorder",
```

```
      "Resource": "*"
    },
    {
      "Sid": "AllowConfigRecorderScopedAccess",
      "Effect": "Allow",
      "Action": [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:AssociateResourceTypes",
        "config:DisassociateResourceTypes"
      ],
      "Resource": "arn:aws:config:*:*:configuration-recorder/*"
    },
    {
      "Sid": "AllowCreateConfigServiceLinkedRole",
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "config.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowListActionsForAgentCoreGateway",
      "Effect": "Allow",
      "Action": [
        "bedrock-agentcore:GatewayListResourcesForWebACL"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowGetActionForAgentCoreGateway",
      "Effect": "Allow",
      "Action": [
        "bedrock-agentcore:GatewayGetWebACLForResource"
      ],
      "Resource": "arn:aws:bedrock-agentcore:*:*:gateway/*"
    },
    {
      "Sid": "WafV2LoggingSlrCreation",
      "Effect": "Allow",
```

```
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/wafv2.amazonaws.com/*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "wafv2.amazonaws.com"
        }
      }
    }
  ]
}
```

AWS Network Security Manager のサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。 AWS Network Security Manager を有効にすると、 AWS Network Security Manager がサービスにリンクされたロールを作成します。実行する手動ステップはありません。

このサービスにリンクされたロールを削除し、再度作成する必要がある場合、 AWS Network Security Manager は次回サービスを使用するときにロールを再作成します。何もする必要はありません。

詳細については、IAM ユーザーガイドの「サービスリンクロールの作成」を参照してください。

AWS Network Security Manager のサービスにリンクされたロールの編集

`AWSServiceRoleForNetworkSecurityManager` サービスにリンクされたロールのアクセス許可は変更できません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。

詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

AWS Network Security Manager のサービスにリンクされたロールの削除

AWS Network Security Manager を使用する必要がなくなった場合
は、`AWSServiceRoleForNetworkSecurityManager`サービスにリンクされたロールを削除することをお勧めします。

サービスにリンクされたロールを削除する前に、 AWS Network Security Manager が管理するリソースをクリーンアップします。 AWS Network Security Manager を無効にし、ポリシーとスコープを削

除して、 AWS Network Security Manager が管理するリソースがアカウントに残らないようにします。その後、ロールを手動で削除できます。

> **Note**
>
> リソースを削除しようとしたときに AWS Network Security Manager がロールを使用している場合、削除が失敗する可能性があります。その場合は、数分待ってからオペレーションを再試行してください。

IAM を使用してサービスリンクロールを手動で削除するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで Roles (ロール) を選択してください。
3. 検索ボックスに と入力しAWSServiceRoleForNetworkSecurityManager、ロールを選択します。
4. [削除] を選択します。
5. 削除を確認するには、ロール名を入力し、削除を選択します。

詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの削除」を参照してください。

AWS Network Security Manager のサービスにリンクされたロールでサポートされているリージョン

AWS Network Security Manager は、 AWS Network Security Manager が利用可能なすべての AWS リージョンで、サービスにリンクされたロールの使用をサポートしています。

AWS Network Security Manager のコンプライアンス検証

新しい AWS サインアップエクスペリエンスは、規制されたワークロード向けには設計されていません。新しい AWS サインアップエクスペリエンスを使用しているが、規制対象のワークロード AWS に を使用する場合は、 AWS (アドバンスド) にサインアップするか、 AWS 環境の高度な機能をアクティブ化できます。

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、AWS のサービス 「コンプライアンスプログラムによるスコープ」の「コンプライアンス」を

参照して、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「Downloading Reports in AWS Artifact」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。を使用する際のコンプライアンス責任の詳細については AWS のサービス、AWS 「 セキュリティドキュメント」を参照してください。

AWS Network Security Manager の耐障害性

AWS グローバルインフラストラクチャは、 AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。 は、低レイテンシー、高スループット、高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティーゾーン AWS リージョン を提供します。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェールオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、フォールトトレランス、および拡張性が優れています。

AWS リージョン およびアベイラビリティーゾーンの詳細については、AWS 「グローバルインフラストラクチャ」を参照してください。

AWS グローバルインフラストラクチャに加えて、 AWS Network Security Manager には、データの耐障害性とバックアップのニーズをサポートするのに役立つ機能がいくつか用意されています。

AWS Network Security Manager のインフラストラクチャセキュリティ

マネージドサービスである AWS Network Security Manager は、ホワイトペーパー「Amazon Web Services: セキュリティプロセスの概要」に記載されている AWS グローバルネットワークセキュリティ手順で保護されています。

AWS 公開された API コールを使用して、ネットワーク経由で AWS Network Security Manager にアクセスします。クライアントで Transport Layer Security (TLS) 1.0 以降がサポートされている必要があります。TLS 1.2 以降が推奨されています。また、DHE (Ephemeral Diffie-Hellman) や ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) などの Perfect Forward Secrecy (PFS) を使用した暗号ス

イートもクライアントでサポートされている必要があります。これらのモードは Java 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

AWS Network Security Manager のセキュリティのベストプラクティス

以下のベストプラクティスは、Network AWS Security Manager の安全な設定を維持するのに役立ちます。

予防的コントロール

- IAM 最小権限を使用する -- 各ユーザーまたはロールが AWS Network Security Manager タスクを実行するために必要なアクセス許可のみを付与します。IAM 条件キーを使用して、可能な場合は特定のリソースへのアクセスを制限します。
- サービスにリンクされたロールを使用する -- AWS Network Security Manager は、サービスにリンクされたロールを使用してユーザーに代わってアクションを実行します。これらのロールには、最低限必要なアクセス範囲の事前定義されたアクセス許可があります。
- スコープを慎重に設定する -- 保護が必要なアカウントとリソースタイプのみを対象とするスコープ設定を定義します。範囲が広すぎると、意図しない適用につながる可能性があります。

「発見的コントロール」

- AWS CloudTrail ログ記録を有効にする -- CloudTrail はすべての AWS Network Security Manager API コールを記録します。これらのログを確認して、セキュリティ設定に誰がいつ変更したかを監査します。
- 同期ステータスのモニタリング -- デプロイの同期ステータスを定期的にチェックして、意図したセキュリティ体制と同期していないリソースを特定します。

AWS Network Security Manager のモニタリング

AWS Network Security Manager のモニタリングは、リソースが意図したとおりに保護されているかどうかを理解するのに役立ちます。 AWS Network Security Manager には、次のモニタリング機能が用意されています。

- 同期ステータス APIs -- デプロイ全体の個々のリソースの保護状態をクエリします。
- AWS CloudTrail -- 監査、コンプライアンス、運用上のトラブルシューティングのためのすべての AWS Network Security Manager API コールを記録します。

同期ステータスのモニタリング

リソースが保護されているかどうかをモニタリングする主な方法は、同期ステータス APIs を使用することです。 AWS Network Security Manager は、範囲内の各リソースを評価し、実際のファイアウォール設定が意図した設定と一致するかどうかを記録します。

同期ステータスオペレーション

AWS Network Security Manager には、同期ステータスをクエリするための 2 つのオペレーションがあります。

ListResourceSynchronizationStatuses

特定のデプロイのリソースごとのステータスを返します。`deploymentIdentifier` パラメータが必要です。オプションで `synchronizationStatus` (IN_SYNC、OUT_OF_SYNC、または NOT_APPLICABLE) でフィルタリングします。

ListAggregateResourceSynchronizationStatuses

すべてのデプロイでリソースごとの集計ステータスを返します。オプションで でフィルタリングしますsynchronizationStatus。このオペレーションは、各リソースに適用されるすべてのポリシーを組み合わせた結果を表示します。

どちらのオペレーションも、 `maxResults` (1 ~ 100) と によるページ分割をサポートしていますnextToken。

同期ステータス値について

IN_SYNC

リソースの実際のファイアウォール設定は、該当するすべてのポリシーから計算された有効な設定と一致します。

OUT_OF_SYNC

リソースの実際の設定は、有効な設定とは異なります。outOfSyncReasons フィールドには、予想される値と実際の値を示す設定ごとの詳細が表示されます。

NOT_APPLICABLE

リソースのアカウントとリソースタイプはスコープ内ですが、リソース自体がスコープフィルターと一致しません (たとえば、タグフィルターでは除外されます) 。アクションは不要です。

リソースが結果にまったく表示されない場合、アカウントまたはリソースタイプはデプロイの対象外です。スコープ設定を確認します。

評価タイムスタンプについて

各同期ステータスエントリには、次の 2 つのタイムスタンプが含まれます。

- evaluatedAt -- AWS Network Security Manager がリソースの設定を最後に評価したとき。古いevaluatedAt値は、最近の変更に対して評価がまだ実行されていないことを示します。
- updatedAt -- 同期ステータスレコード自体が最後に変更された日時。updatedAt が より古い場合evaluatedAt、ステータスは前回の評価以降安定しています。

クロスアカウントの可視性

複数の管理者が同じリソースを保護する場合、集約同期ステータスの可視性は、各デプロイenableCrossAccountVisibilityの設定によって異なります。

- リソースを対象とするすべてのデプロイでクロスアカウント可視性が有効になっている場合、管理者は完全な集計ステータスとout-of-sync理由を確認できます。
- デプロイでクロスアカウント可視性が無効になっている場合、他の管理者には詳細な理由ではなくNOT_VISIBLEマーカーが表示されます。これは、別の管理者もリソースを保護しているが、可視性を共有していないことを示します。

out-of-syncリソースの診断

リソースが OUT_OF_SYNC を報告すると、 `outOfSyncReasons`フィールドは特定の設定の違いを識別します。最上位の理由は次のいずれかです。

- `missingFirewall` -- ファイアウォール保護はリソースに関連付けられていません。
- `invalidFirewall` -- ファイアウォールは存在しますが、その設定が想定と一致しません。特定の違いは、分類されたバケットに一覧表示されます。

修復が有効になっていてもリソースを修正できない場合、 `remediationIssues`フィールドには、問題を手動で解決する方法に関するガイダンス`correctiveAction`が表示されます。修復は、デフォルトでオフになっているポリシーレベルの設定です。詳細については、「the section called “同期と修復”」を参照してください。

異なる設定を持つ複数のデプロイは、同じリソースをターゲットにできます。この場合、デプロイごとの同期ステータスは OUT_OF_SYNC で、集計同期ステータスは IN_SYNC です。これは失敗ではなく、予想される動作です。マージ中に優先度の高いポリシーの設定が優先されました。その結果、リソースは優先度の低いデプロイの設定と一致しなくても、有効な設定と一致します。

を使用した AWS Network Security Manager API コールのログ記録 AWS CloudTrail

AWS Network Security Manager は、ユーザー AWS CloudTrail、ロール、または のサービスによって実行されたアクションを記録する AWS サービスである と統合されています。CloudTrail は、AWS Network Security Manager のすべての API コールを管理イベントとしてキャプチャします。キャプチャされた呼び出しには、 AWS Network Security Manager コンソールからの呼び出しと AWS 、Network Security Manager API オペレーションへのプログラムによる呼び出しが含まれます。

証跡を作成する場合は、 AWS Network Security Manager のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

AWS CloudTrail の Network Security Manager 情報

CloudTrail は、アカウントの作成 AWS アカウント 時に で有効になります。 AWS Network Security Manager でアクティビティが発生すると、そのアクティビティはイベント履歴の他の AWS サービ

スイベントとともに CloudTrail イベントに記録されます。で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。詳細については、「CloudTrail イベント履歴でのイベントの表示」を参照してください。

AWS Network Security Manager のイベントなど AWS アカウント、 のイベントの継続的な記録については、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。証跡は、パーティション内のすべてのリージョンからのイベントを AWS ログに記録します。指定した Amazon S3 バケットにログファイルを配信します。CloudTrail ログで収集されたイベントデータをさらに分析して処理するように、他の AWS サービスを設定できます。詳細については、次を参照してください:

- 追跡を作成するための概要
- CloudTrail がサポートされているサービスと統合
- 「CloudTrail の Amazon SNS 通知の設定」

すべての AWS Network Security Manager オペレーションは CloudTrail によってログに記録されます。パブリックオペレーションには以下が含まれます。

- ルール、テンプレート、ポリシー、スコープ、デプロイの作成、読み取り、更新、削除 (CRUD) オペレーション
- スナップショットオペレーション
- タグ付けオペレーション
- 管理者アカウントのオペレーション
- 同期ステータスオペレーション
- リソースの関連付けオペレーション
- ルール生成オペレーション

すべてのイベントエントリには、次の情報が含まれます。

- イベントソース: `network-security-manager.amazonaws.com`
- API オペレーション名であるイベント名 (例: `CreatePolicy`または `ListDeployments`)
- ARN とリソースタイプによって識別される、影響を受けるリソース

読み取り専用オペレーション (GetPolicy、、 などListResourceSynchronizationStatuses) は でログに記録readOnly: trueされListRules、レスポンス要素は含まれません。ミューテーションオペレーションには、リクエストパラメータとレスポンス要素が含まれます。

> **Note**
>
> CloudTrail は、イベントレコードの機密フィールドを編集します。例えば、CloudTrail は GenerateRuleConfigurationオペレーションで promptパラメータを編集します。

例: CreatePolicy イベント

次の例は、CreatePolicy オペレーションの CloudTrail ログエントリを示しています。

```
{
  "eventVersion": "1.09",
  "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AROAEXAMPLEID:my-session",
      "arn": "arn:aws:sts::123456789012:assumed-role/AdminRole/my-session",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
          "sessionIssuer": {
              "type": "Role",
              "principalId": "AROAEXAMPLEID",
              "arn": "arn:aws:iam::123456789012:role/AdminRole",
              "accountId": "123456789012",
              "userName": "AdminRole"
          },
          "attributes": {
              "creationDate": "2026-08-10T18:22:41Z",
              "mfaAuthenticated": "false"
          }
      }
  },
  "eventTime": "2026-08-10T18:24:03Z",
  "eventSource": "network-security-manager.amazonaws.com",
  "eventName": "CreatePolicy",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.44",
  "userAgent": "aws-cli/2.17.0 Python/3.12.4 Darwin/24.6.0",
```

```
  "requestParameters": {
      "clientToken": "550e8400-e29b-41d4-a716-446655440001",
      "policyName": "production-web-acl-policy",
      "firewallType": "WAF",
      "priority": 1,
      "associatedTemplateAndRuleList": [
          {
              "templateIdentifier": "arn:aws:network-security-manager:us-
east-1:123456789012:template:t1a2b3c4d5"
          }
      ],
      "policyConfiguration": {
          "remediationEnabled": true,
          "resourcesCleanUp": false,
          "wafConfig": {
              "existingCustomerWebACLResolution": "RETROFIT",
              "conflictResolution": "MERGE_WHERE_APPLICABLE"
          }
      },
      "isPublished": true
  },
  "responseElements": {
      "policyId": "p9z8y7x6w5v4u3t2",
      "policyArn": "arn:aws:network-security-manager:us-
east-1:123456789012:policy:p9z8y7x6w5v4u3t2",
      "policyName": "production-web-acl-policy",
      "status": "ACTIVE",
      "version": "1"
  },
  "requestID": "b1c2d3e4-5f67-4890-a1b2-c3d4e5f6a7b8",
  "eventID": "f0e1d2c3-b4a5-4968-8776-5a4b3c2d1e0f",
  "readOnly": false,
  "resources": [
      {
          "accountId": "123456789012",
          "type": "AWS::NetworkSecurityManager::Policy",
          "ARN": "arn:aws:network-security-manager:us-
east-1:123456789012:policy:p9z8y7x6w5v4u3t2"
      }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management"
```

```
}
```

AWS Network Security Manager のクォータ

AWS アカウント には、 AWS Network Security Manager の次のデフォルトクォータがあります。特に明記されていない限り、各クォータはアカウントごと、リージョンごとです。

リソースクォータ

次の表に、各リージョンでアカウントごとに作成できる AWS Network Security Manager リソースの最大数を示します。

[リソース]	デフォルトのクォータ	調整可能
アカウントごとのルールの数	200	いいえ
アカウントごとのテンプレートの種類	100	いいえ
ポリシー/アカウント	100	いいえ
アカウントあたりのスコープ	100	いいえ
アカウントあたりのデプロイ	100	いいえ
リソースあたりのスナップショット	10	いいえ

リソースコンポジションクォータ

次の表に、 AWS Network Security Manager リソースがリソース階層内で相互に参照する方法のクォータを示します。

クォータ	値
テンプレートあたりのルール	1 ~ 50
AWS WAF ポリシーあたりのテンプレート	1 ~ 2

クォータ	値
AWS WAF ポリシーごとに組み合わせられたルールとテンプレート	1 ~ 100
Shield Advanced AWS ポリシーあたりのテンプレートまたはルール	0 (空にする必要があります)
デプロイあたりのポリシー	1 ~ 2
デプロイあたりのスコープ	1 (正確に 1)

スコープ設定クォータ

次の表に、スコープ設定式のクォータを示します。

クォータ	値
スコープあたりのリソースタイプスコープ	20
スコープ式の深さ (ネストされたレベル)	2
スコープ式の幅 (レベルあたりの基準)	20

管理者アカウントのクォータ

次の表に、 AWS Network Security Manager 管理者アカウントの優先度レベルのクォータを示します。

クォータ	値
管理者の優先度レベル	1 ~ 10

API ページ分割クォータ

次の表に、リストオペレーションのページ分割制限を示します。

クォータ	値
ページあたりの最大結果 (`maxResults`)	100
ページあたりの最小結果 (`maxResults`)	1

クォータの調整可能性

前のセクションに記載されているクォータは固定されており、現時点では引き上げることはできません。

AWS Network Security Manager デベロッパーガイドのドキュメント履歴

次の表に、 AWS Network Security Manager のドキュメントリリースを示します。

変更	説明	日付
初回リリース	AWS Network Security Manager デベロッパーガイドの初回リリース。	2026 年 8 月 1 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。