Cisco Defense Orchestrator を使用した AWS の管理

Cisco Defense Orchestrator を使用した AWS の管理

Cisco Defense Orchestrator を使用して AWS VPC の管理

CDO は、Amazon Web Services（AWS）仮想プライベートクラウド（VPC）向けの簡素化された管理インターフェイスを提供します。他のデバイスを管理するのと同じインターフェイスで、AWS VPC とそのコンポーネントを管理できます。

CDO を使用して、以下のタスクを実行できます。

- AWS VPC の導入準備
- VPC の詳細を表示する
- セキュリティグループを操作する
- AWS オブジェクトを他の管理対象デバイスと共有する
- AWS のサイト間 VPN 接続を監視する
- AWS デバイスへの変更をモニタリングする
- AWS のサイト間 VPN トンネルを表示する

以下は、CDO が将来サポートする予定の一般的な AWS の機能です。

- セキュリティグループに対するロードバランサー（エラスティック、ネットワーク、アプリケーション ロード バランサー）の関係を表示する
- セキュリティグループに対する自動スケーリンググループの関係を表示する

セキュリティグループの以下の側面を CDO で管理することはできません。

Cisco Defense Orchestrator を使用した AWS の管理

- セキュリティグループを作成する。
- セキュリティグループをインスタンスにリンクする。
- セキュリティグループをロードバランサーに割り当てる。
- VPC ピアリング。

AWS VPC の導入準備

CDO の導入準備ウィザードを使用して、AWS VPC の導入準備を開始します。詳細については、AWS VPC の導入準備を参照してください。

AWS VPC にタグが含まれている場合、これらのタグは、デバイスの導入準備時に CDO にインポートされる点に注意してください。CDOはタグを**ラベル**として表示します。セキュリティクラウド オブジェクトやルールとは異なり、ラベルは AWS VPC に自動的には同期されません。詳細については、「ラベルとフィルタ処理」を参照してください。

CDO コンソールを介して、AWS VPC のログイン情報と権限を処理します。正しいログイン情報または権限がないと、CDO は AWS VPC と通信できません。詳細については、AWS VPC 接続ログイン情報の更新 と「IAM ユーザーのアクセス許可の変更」を参照してください。

AWS VPC の詳細を表示する

AWS VPC が導入準備されると、AWS VPC の ID、リージョン、セキュリティグループ、セキュリティグループに割り当てられたルールとオブジェクトを表示できます。

セキュリティグループを操作する

セキュリティグループは、セキュリティグループに関連付けられているすべての AWS インスタンスおよびその他のエンティティへの、インバウンドおよびアウトバウンドのネットワークトラフィックを管理するルールのコレクションです。AWS VPC を CDO に対して導入準備すると、セキュリティグループはセキュリティ グループ オブジェクトとして CDO に保存されます。

CDO を使用すると、以下のタスクを実行できます。

- セキュリティグループに新しいルールを作成する
- セキュリティグループのルールの変更確認、編集、削除

現時点では、VPC に新しいセキュリティグループを作成することはできません。

詳細については、次のトピックを参照してください。

- AWS VPC セキュリティグループとインスタンス
- AWS VPC セキュリティグループのルールを管理する
- AWS と他の管理対象デバイス間でオブジェクトを共有する

Cisco Defense Orchestrator を使用した AWS の管理

AWS と他の管理対象デバイス間でオブジェクトを共有する

CDO は、ルールにおけるオブジェクトの使用をサポートしています。オブジェクトは値のコンテナです。たとえば、リソースの IP アドレスを含むネットワークオブジェクトを作成し、意味のある名前を付けることができます。その後、リソースのリテラル IP アドレスを使用するのではなく、ルールの送信元または接続先の一部としてアクセスルール内でそのオブジェクトを使用できます。また、そのオブジェクトを異なるルールで再利用することもできます。オブジェクトの値をいったん変更すると、そのオブジェクトを使用するすべてのルールが新しい値を使用し始めます。

AWS VPC の導入準備後、CDO は AWS の概念を、既存のセキュリティグループルールで見つかったセキュリティ グループ オブジェクト、ネットワークオブジェクト、およびサービスオブジェクトに変換します。

ネットワークオブジェクトとサービスオブジェクト（ポートオブジェクトと呼ばれることもある）は、AWS VPC と、CDO を使用して管理する他のデバイスとの間で共有できます。セキュリティ グループ オブジェクトは AWS に固有です。

詳細については、「AWS と他の管理対象デバイス間でオブジェクトを共有する」を参照してください。

AWS のサイト間 VPN 接続を監視する

AWS のサイト間 VPN は、AWS VPC をセキュアなトンネルを介してエンタープライズ ネットワークに接続します。詳細については、「AWS のサイト間 VPN の管理」を参照してください。

AWS VPC および AWS セキュリティグループへの変更をモニタリングする

ログの変更

変更ログは、CDO で行われた構成変更を継続的にキャプチャします。この単一のビューには、サポートされているすべてのデバイスとサービスにわたる変更が含まれます。変更ログの機能の一部を次に示します。

- デバイス構成に加えられた変更の対照比較。
- すべての変更ログエントリの平易な英語のラベル。
- デバイスの導入準備と削除の記録。
- CDO の外部で発生するポリシー変更の競合の検出。
- インシデントの調査またはトラブルシューティング中に、誰が、何を、いつに回答可能。

変更リクエスト管理

変更リクエスト管理により、サードパーティのチケットシステムで開かれた変更リクエストとそのビジネス上の正当性を、変更ログのイベントに関連付けることができます。変更リクエスト管理を使用して、CDO で変更リクエストを作成し、作成した変更リクエストを一意の名前で識別し、変更の説明を入力して、変更リクエストを変更ログイベントに関連付けます。後から変更リクエスト名を変更ログで検索できます。

Cisco Defense Orchestrator を使用した AWS の管理

一般的な管理者タスクのサポート

CDO は、以下の AWS セキュリティグループの一般的な管理タスクをサポートしています。

- デバイス設定の一括展開
- すべてのデバイス設定の読み取り
- アウトオブバンド変更の検出
- 競合検出
- 構成の競合の解決