Cisco Defense Orchestrator を使用した FMC の管理

Cisco Defense Orchestrator を使用した FMC の管理

Firepower Management Center について

Firepower Management Center（FMC）のサポートは、オンボーディング、管理対象デバイスの表示、FMC に関連付けられたオブジェクトの表示、およびバージョン 6.4 以降を実行している FMC の FMC UI へのクロス起動に限定されています。追加の FMC 機能がまもなくサポート対象になる予定です。現時点で CDO でサポートされていない可能性のある機能については、FMC コンソールを使用する必要があります。システムが実行しているバージョンの『Firepower Management Center Configuration Guide』を参照してください。

Firepower Management Center（FMC）は、管理、分析、レポートのタスクを実行できるグラフィカル ユーザー インターフェイスを備えた集中管理コンソールです。ASDM および FDM と同等の管理コンソールですが、同一ではありません。CDO がサポートする FMC デバイスとソフトウェアバージョンのリストについては、「CDO でサポートされるソフトウェアとハードウェア」を参照してください。

バージョン サポート

CDO は、バージョン 6.4 以降を実行する FMC をサポートします。FMC で古いデバイスを管理できます。通常は、メジャーバージョンをいくつか遡ることができます。たとえば、バージョン 6.6.0 の FMC では、バージョン 6.4.0 のデバイスを管理できます。FMC が 6.4 より前のバージョンを実行しているデバイスを管理している場合、そのデバイスは[インベントリ]ページに表示されますが、CDO に展開することも、そのポリシーを CDO から変更することもできません。FMC UI から変更を加えて展開する必要があります。

Cisco Defense Orchestrator を使用した FMC の管理

（注） 管理対象デバイスが無効になっているか、アクセスできない状態になっている場合、CDO の [インベントリ]ページにそのデバイスが表示されたとしても、要求を正常に送信したり、デバイス情報を表示したりすることはできません。

CDO と FMC の通信方法

CDO は REST API クライアントとして機能し、FMC に要求を送信します。次に FMC は、指定されたクライアントを使用して、要求を管理対象デバイスに送信します。同じログイン情報を使用した複数のログインを FMC が許可することはないため、管理者レベルの権限を持つ CDO 通信専用の新しいユーザーを FMC で作成することを推奨します。この新しいユーザーは、CDO が指定する管理者、または**システム**と**デバイス**に対する権限を持つカスタムユーザーロールのいずれかとして、CDO で複製する必要があります。管理者ログインがないと、CDO は、REST API コマンドを正常に使用してポリシー、ルール、またはオブジェクトを変更または作成することができません。

FMC の導入準備または削除

FMC はいつでも導入準備または削除できます。CDO が FMC とその登録済みデバイスを読み取るには、少なくともバージョン 6.4 が実行されている必要があります。FMC とその登録済みデバイスを導入準備するには、詳細について「FMC の導入準備」を参照してください。FMC が導入準備された後、[インベントリ] ページから FMC または FMC 管理対象デバイスを選択すると、選択した FMC Web UI が新しいタブとして自動的にクロス起動します。CDO テナントから FMC を削除すると、その FMC に登録されているデバイスも削除されます。詳細については、「CDO からの FMC の削除」を参照してください。

導入準備後に FMC のステータスが [無効なログイン情報] になった場合は、アプライアンスを**再接続**できます。導入準備詳細については、「無効なログイン情報のトラブルシュート」を参照してください。

（注） Firepower 6.6 を実行している FMC は、再接続機能をサポートしていません。アプライアンスを再接続する必要がある場合は、FMC を削除してアプライアンスを再度導入準備することを推奨します。

FMC 高可用性ペア

CDO は、FMC アプライアンスの高可用性（HA）機能をサポートしていません。FMC アプライアンスのペアが HA 用に設定されている場合、そのペアは [インベントリ] ページに個々のアプライアンスとして表示されます。

FMC によって管理されるデバイス

FMC の CDO への導入準備を行うと、その FMC に登録されているすべてのデバイスも CDO に読み込まれます。[インベントリ]ページから、名前、IP アドレス、デバイスのタイプ、ソフト

Cisco Defense Orchestrator を使用した FMC の管理

ウェアバージョン、状態などのデバイス情報を表示できます。FMC によって現在管理されているデバイスをクリックして選択すると、CDO はデバイスを管理する FMC コンソールを自動的に起動します。

フィルタアイコンを使用して、[インベントリ]ページをさらに整理できます。ここで、すべての導入準備済みの FMC または FMC によって管理されるデバイス、およびその他のサポート対象デバイスタイプを表示することを選択できます。

セキュリティ ポリシー管理

セキュリティポリシーは、目的の宛先へのトラフィックを許可するか、セキュリティ脅威が特定された場合にトラフィックをドロップすることを最終的な目標として、ネットワークトラフィックを検査します。CDO を使用して、さまざまな種類のデバイスでセキュリティポリシーを設定できます。

オブジェクト

FMC の CDO への導入準備を行うと、CDO は FMC 管理対象の FTD デバイスからオブジェクトをインポートします。CDO にインポートされると、オブジェクトは読み取り専用になります。FMC オブジェクトは読み取り専用ですが、CDO を使用すると、FMC によって管理されていないテナント上の他のデバイスにオブジェクトのコピーを適用できます。コピーは元のオブジェクトとの関連付けが解除されるため、FMC からインポートされたオブジェクトの値を変更せずにコピーを編集できます。FMC オブジェクトは、そのオブジェクトタイプをサポートする管理対象の任意のデバイスで使用できます。詳細については、「FMC オブジェクト」を参照してください。

FMC は、次のオブジェクトタイプをサポートします。

- ネットワーク オブジェクト
- ネットワークグループ オブジェクト
- サービス/ポートオブジェクト
- URL/URL グループオブジェクト

オブジェクトの問題

CDO は、FMC 上の重複、不整合、または未使用のオブジェクトを識別しません。これらの問題の状態に基づいてオブジェクトをフィルタ処理することはできません。

イベント（Eventing）

特定のイベントの履歴イベントテーブルとライブイベントテーブルの検索とフィルタ処理は、CDO で他の情報を検索してフィルタ処理する場合と同様に機能します。詳細については、『Firepower Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide』を参照してください。

Cisco Defense Orchestrator を使用した FMC の管理

Cisco Security Analytics and Logging

Cisco Security Analytics and Logging を使用すると、すべての Firepower Threat Defense（FTD）デバイスからの接続、侵入、ファイル、マルウェア、セキュリティインテリジェンスのイベントをキャプチャし、Cisco Defense Orchestrator（CDO）の 1 か所で表示できます。

イベントは Cisco Cloud に保存され、CDO の [イベントロギング（Event Logging）] ページから表示できます。イベントをフィルタリングして確認し、ネットワークでトリガーされているセキュリティルールを明確に理解できます。それらの機能は、**Logging and Troubleshooting** パッケージで提供されます。

Firewall Analytics and Monitoring パッケージを使用すると、システムは Secure Cloud Analytics 動的エンティティモデリングを FTD イベントに適用し、動作モデリング分析を使用して Secure Cloud Analytics の観測値とアラートを生成できます。**Total Network Analytics and Monitoring** パッケージを使用すると、システムは FTD イベントとネットワークトラフィックの両方に動的エンティティモデリングを適用し、観測値とアラートを生成します。Cisco Single Sign-On を使用して、プロビジョニングされた Cisco Secure Cloud Analytics ポータルを CDO からクロス起動できます。