Cisco Security Cloud Control によるオンプレミス Firewall Management Center の管理

• Security Cloud Control による オンプレミス Firewall Management Center の管理 （i ページ）

Security Cloud Control によるオンプレミス Firewall Management Center の管理

オンプレミス Firewall Management Center について

オンプレミス Management Center 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、表示、ネットワークオブジェクトの管理、および関連付けられたデバイスとオブジェクトを管理するための オンプレミス Management Center UI のクロス起動に限定されます。その他の機能はまもなくサポート対象になる予定です。現時点で Security Cloud Control でサポートされていない可能性のある機能については、オンプレミス Management Center コンソールを使用する必要があります。オンプレミス Management Centerで提供される機能の詳細については、システムが実行しているバージョンの『Cisco Secure Firewall Management Center コンフィギュレーション ガイド』を参照してください。

オンプレミス Management Center はグラフィカル ユーザー インターフェイスを備えた中央管理コンソールであり、このコンソールを使って管理タスク、分析タスク、およびレポートタスクを実行できます。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。Security Cloud Control がサポートする オンプレミス Management Center 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、「Security Cloud Control 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

Security Cloud Control はバージョン 6.4 以降をサポートします。オンプレミス Management Center では、通常、メジャーバージョンをいくつか遡った古いデバイスを管理できます。たとえば、バージョン 6.6.0 を実行するデバイスでは、バージョン 6.4.0 のデバイスを管理できます。オンプレミス Management Center 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

Cisco Security Cloud Control による オンプレミス Firewall Management Center の管理

る場合、そのデバイスは[インベントリ（Inventory）] ページに表示されますが、Security Cloud Control 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。オンプレミス Management Center UI から変更を加えて展開する必要があります。

（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、Security Cloud Control の [インベントリ（Inventory）] 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。

Security Cloud Control と FMC の通信方法

Security Cloud Control は REST API クライアントとして機能し、オンプレミス Management Center に要求を送信します。次に オンプレミス Management Center 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デバイスが許可することはないため、管理者レベルの権限を持つ Security Cloud Control 通信専用の新しいユーザーを オンプレミス Management Center で作成することを推奨します。この新しいユーザーは、Security Cloud Control が指定する管理者、または [システム（system）] および [デバイス（devices）] 権限を持つカスタムユーザーロールのいずれかとして、Security Cloud Control で複製する必要があります。管理者ログインがないと、Security Cloud Control 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。

オンプレミス Management Center のオンボードまたは削除

オンプレミス Management Center はいつでもオンボードまたは削除できます。Security Cloud Control が オンプレミス Management Center 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。オンプレミス Management Center とその登録済みデバイスをオンボードするには、「FMC のオンボーディング」を参照してください。

オンプレミス Management Center のオンボーディングを終えてから、[サービス（Services）] ページで オンプレミス Management Center を選択し、右側のペインで [管理（Management）] の下にある [デバイス（Devices）] をクリックするか任意のアクションをクリックすると、[FMC クロス起動URLの確認（Verify FMC Cross Launch URL）] ウィザードが開き、管理センターのパブリック IP アドレスまたは FQDN およびポート番号を入力できます。[続行（Continue）] をクリックすると、入力した IP アドレスを使用して、新しいタブで選択した オンプレミス Management Center Web UI がクロス起動します。右側のペインの [外部リンク（External Links）] の下にある [外部リンクの追加（Add External Links）] オプションで、外部リンクを手動で追加することもできます。

Security Cloud Control テナントから オンプレミス Management Center を削除すると、その オンプレミス Management Center 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、「Security Cloud Control からの FMC の削除」を参照してください。オンボーディング後に オンプレミス Management Center のステータスが [無効なログイン情報（Invalid Credentials）] になった場合は、アプライアンスを**再接続**します。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。

Cisco Security Cloud Control によるオンプレミス Firewall Management Center の管理

（注） Firepower 6.6 を実行しているデバイスは、**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、オンプレミス Management Center を削除してアプライアンスを再度オンボードすることを推奨します。

オンプレミス Management Center 高可用性ペア

Security Cloud Control は、オンプレミス Management Center 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。オンプレミス Management Center 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 [サービス（Services）] ページに個々のアプライアンスとして表示されます。

オンプレミス Management Center による管理対象デバイス

オンプレミス Management Center の Security Cloud Controlへのオンボーディングを行うと、そのオンプレミス Management Center に登録されているすべてのデバイスも Security Cloud Control 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。オンプレミス Management Center は [サービス（Services）] ページに表示され、管理されるデバイスは [インベントリ（Inventory）] ページにリストされます。[サービス（Services）] ページでは、バージョン、管理対象デバイス、デバイスのタイプ、ステータスなどの情報を確認できます。FMC が管理するデバイスの数を表示する [サービス（Services）] ページのデバイスアイコンをクリックすると、デバイスフィルタが適用された状態で [インベントリ（Inventory）] ページが表示され、選択した オンプレミス Management Center によって管理されているすべてのデバイスが表示されます。

[インベントリ（Inventory）] の右側のペインにある [デバイスアクション（Device Actions）]、[モニタリング（Monitoring）]、[デバイス管理（Device Management）]、および [ポリシー（Policies）] パネルの関連オプションを使用して、各種アクションを実行できます。FMC によって現在管理されているデバイスを選択してこれらのオプションをクリックすると、Security Cloud Control は入力したクロス起動 URL を使って、デバイスを管理する オンプレミス Management Center 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、すべてのオンボード済みの オンプレミス Management Center 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。さらに、クラスタのデバイスを展開するか折りたたんで、個別に、またはグループとして選択してアクションを実行できます。

デバイスの正常性ステータス

Security Cloud Control では、[インベントリ（Inventory）] ページに Threat Defense デバイスの正常性ステータス（[正常（Normal）]、[エラー（Error）]、[警告（Warning）]、[無効（Disabled）] など）を表示します。デバイスのステータスをクリックすると、オンプレミス Management Centerユーザーインターフェイスでそのデバイスの [ヘルスモニタリング（Health Monitoring）] ページに移動できます。

Cisco Security Cloud Control によるオンプレミス Firewall Management Center の管理

（注） Security Cloud Control は 10 分ごとにデバイスの正常性ステータスを自動的に更新します。ただし、デバイスを選択して [変更の確認（Check for Changes）] をクリックすることで、手動でも実行できます。

Security Cloud Control のセキュリティポリシーの管理

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。Security Cloud Control 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

オンプレミス Management Center の Security Cloud Control へのオンボーディングが終わると、オンプレミス Management Center からオブジェクトを検出し、Security Cloud Control で管理できます。そのためには、**[ツールとサービス（Tools and Services）]** > **[Firewall Management Center]** に移動し、対象となる オンプレミス Management Center を選択し、[設定（Settings）] をクリックします。[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] トグルボタンをオンにできます。このオプションを有効にすると、Security Cloud Control は オンプレミス Management Center 管理対象デバイスからすべてのオブジェクトを Security Cloud Control に自動的に読み取ります。インポートされたオブジェクトは、Security Cloud Control から管理できます。[設定（Settings）] ボタンを使用するには、ネットワーク管理者または管理者ユーザーロールが必要です。

Security Cloud Control からオブジェクトの設定変更を行うと、変更が Security Cloud Control にステージングされ、[保留中の変更（Pending Changes）] で確認した後、オンプレミス Management Center に変更を手動でプッシュできます。さらに、オンプレミス Management Center ユーザーインターフェイスからオブジェクトの設定を変更すると、Security Cloud Control はそれらの変更を後から同期できるアウトオブバンドの変更として検出します。変更を オンプレミス Management Center と自動的に同期し、確認のためのステージングをしない場合は、[ネットワークオブジェクトの自動同期を有効にする（Enable automatic sync of network objects）] トグルをオンにします。

オンプレミス Management Center に割り当てる既存のオブジェクトが Security Cloud Control にある場合は、[サービス（Services）] ページで オンプレミス Management Center を選択し、右側のペインで [オブジェクトの割り当て（Assign Objects）] を選択します。Security Cloud Control に既存のすべてのオブジェクトが表示され、選択した オンプレミス Management Center に関連付けるオブジェクトを選択できます。これにより、Security Cloud Control の管理対象プラットフォーム間でネットワークオブジェクトの定義の一貫性が促進されます。[オブジェクトの割り当て（Assign Objects）] ボタンは、選択した オンプレミス Management Center の [ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] が有効になっている場合のみ使用できます。

Cisco Security Cloud Control による オンプレミス Firewall Management Center の管理

（注）

- 選択した オンプレミス Management Center に 1 つ以上の子ドメインがある場合、または変更管理ワークフローが有効になっている場合は、[ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] トグルをオンにできません。.
- [ネットワークオブジェクトの検出と管理（Discover & Manage Network Objects）] がオフの場合は、[ネットワークオブジェクトの自動同期を有効にする（Enable automatic sync of network objects）] トグルをオンにできません。

オンプレミス Management Center 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

オブジェクトの問題

Security Cloud Control は、重複、不整合、または未使用のオブジェクトを識別します。問題のステータスに基づいて問題をフィルタ処理できます。ただし、Security Cloud Control ではオブジェクトの問題を解決できません。

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、Security Cloud Control 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 Security Analytics and Logging

Cisco Security Analytics and Logging を使用すると、すべての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、Security Cloud Control の 1 か所で表示できます。

イベントは Cisco Cloud に保存され、Security Cloud Control 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 Cisco Secure Cloud Analytics 動的エンティティモデリングをイベントに適用し、動作モデリング分析を使用して Cisco 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、システムはデバイス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 Security Cloud Control からクロス起動できます。

Cisco Security Cloud Control による オンプレミス Firewall Management Center の管理

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。