

Security Cloud ControlによるオンプレミスFMCからクラウド(cdFMC)への移行

内容

[お問い合わせ内容](#)

[環境](#)

[解決策](#)

[原因](#)

[関連コンテンツ](#)

- [お問い合わせ内容](#)
 - [環境](#)
 - [解決策](#)
 - [原因](#)
 - [関連コンテンツ](#)
-

お問い合わせ内容

ユーザは、実稼働のFirewall Management Center(FMCv300)仮想アプライアンスを、Security Cloud Control(SCC)テナントでクラウド提供のFMC(cdFMC)に移行する際の支援を必要としています。具体的な懸念事項は次のとおりです。

- 移行プロセスのどの部分でダウンタイムが発生し、生産への影響を最小限に抑える方法を理解します。
- 移行ワークフローの手順を説明します。
- 移行完了後のFMCv300の処理方法を決定します。
- ハイアベイラビリティ(HA)構成の複数のファイアウォール脅威対策(FTD)デバイスに対する段階的な移行アプローチを計画します。
- 移行ウィザードをトリガーする前に、オンプレミスのFMC設定をcdFMCに手動でインポートする必要があるかどうかを確認します。

環境

- ソースFMC:FMCv300仮想アプライアンス、バージョン7.6.5。他のハードウェア(HW)およびソフトウェア(SW)プラットフォームも導入できます。
- ターゲット： cdFMCテナントがプロビジョニングされました。
- 管理対象デバイスは、異なるHWおよびSWバージョンのFTDです。次に例を示します。
 - 2x Secure Firewall 3130、FTD 7.6.4、HAペアで設定
 - 2x Firepower 2130、FTD 7.4.4、HAペアで設定
 - 1x FTDv in Azure、7.6.4、スタンドアロン構成。

解決策

移行の前提条件とバージョンの検証

環境バージョンは、cdFMCへの移行の前提条件を満たしています。

- FMC 7.6.5は、移行ワークフローの文書化された最小要件を満たしています。
- FTDバージョン7.6.4および7.4.4は、文書化されている移行の最小要件を満たしています。
- cdFMCは、環境内のFTDリリーストレインをサポートします。

移行前の検証手順

移行を開始する前に、次の前提条件を検証します。

- FMCv300には保留中の展開はありません。
- 両方のHAペアが正常で同期している。
- FMCv300のバックアップが完了しました。
- 十分なFMCディスク領域 (少なくとも10%の空き領域) 。
- FTD管理パスから動作するDNS解決。
- 必要なクラウド管理ポート (TCP 443およびTCP 8305) 経由でFTD管理インターフェイスからcdFMCへのアウトバウンド接続が可能

- FMCv300にはSCCへの発信HTTPSアクセスがあります。

設定のインポートプロセス

移行ウィザードを実行する前に、オンプレミスのFMCv300設定をcdFMCに手動でインポートする必要はありません。「FTDをcdFMCに移行」ワークフローでは、移行ジョブの一部として設定のインポートを処理します。

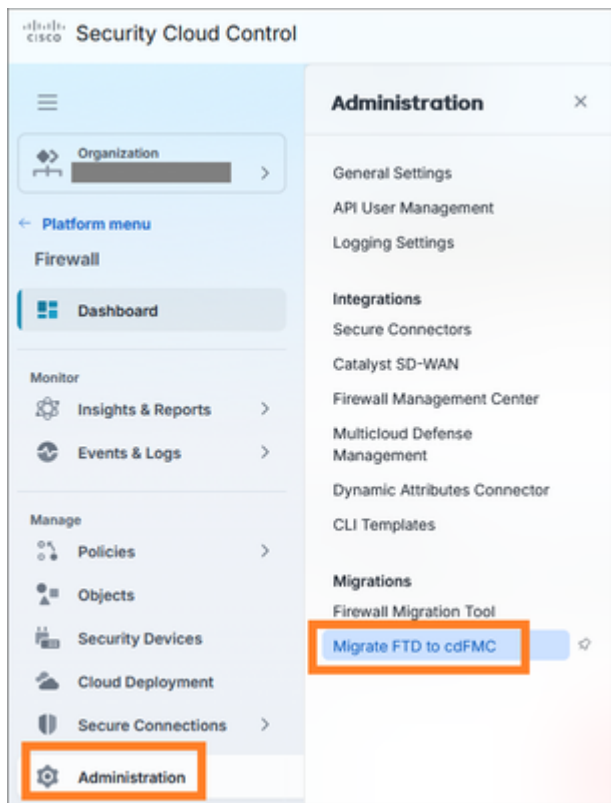
1. SCCはオンプレミスのFMCv300に接続します。
2. 関連する設定をオンプレミスのFMCからエクスポートする
3. 共有ポリシー/オブジェクトをcdFMCにインポートします。
4. インターフェイスやルーティングなど、デバイス固有の設定をインポートする。
5. 選択したFTDデバイスをcdFMCに登録します。
6. 14日間の評価期間は、移行の完了後に開始されます。

移行の前にcdFMCでFMCv300上の項目と同じ名前のポリシーまたはオブジェクトを手動で作成すると、移行ワークフローではオンプレミスのバージョンをインポートする代わりに既存のcdFMC項目を使用できるため、予期しない結果が生じる可能性があります。

推奨される移行シーケンス

フェーズ1：移行前設定

1. SCCテナントにcdFMCを展開します。
2. 現在のFMCv300をSCCにオンボードします。
3. cdFMCのスマートライセンスを確認します。
4. Firewall > Administration > Migrations > Migrations FTD to cdFMCの順に選択し、移行ワークフローを開始します。



5. 共有ポリシーのインポート後に確認のために一時停止するには、オプションを使用します。

The screenshot displays the Cisco Security Cloud Control interface for migrating FTDs to cdFMC. The left sidebar contains navigation links for Organization, Platform menu, Firewall, Dashboard, Monitor, and Manage. The main panel shows the 'Migrate FTD to cdFMC' workflow. Step 2, 'Select On-Prem FMC', is active, showing 'On-Prem FMC: FMC'. Step 3, 'Select Devices', is also active, prompting the user to select FTD device(s) to migrate. A search bar and a table with columns 'Name' and 'Domain' are present. The table lists one device, 'FTD3140-HA', with the domain 'Global'. Below the table, it indicates '0 device(s) selected'. Two checkboxes are shown: 'Pause migration to review imported shared policy' (checked) and 'Auto deploy to FTDs after successful migration'. A 'Migrate FTD to cdFMC' button is located at the bottom of the main panel.

フェーズ2：移行の実行

メンテナンスウィンドウでは、段階的なアプローチを使用してデバイスを移行します。

1. スタンドアロンのFTD (最も影響が小さい) から開始します。
2. 最初のHAペアを移行します。
3. デバイスの健全性と機能を検証する。
4. 2番目のHAペアを移行します。

フェーズ3：移行後の検証

各デバイスまたはHAペアの移行後：

1. cdFMCでデバイスの状態を確認します。
2. 必要に応じて、HA状態を確認します。
3. 展開のプレビュー/警告を確認します。
4. cdFMCから展開します。
5. トラフィックとイベントの可視性を検証します。

構成の固定を伴う3フェーズ移行計画

推奨されるアプローチでは、3つのフェーズでFTD移行を実行します。各フェーズは個別の日付で実行され、フェーズごとに最低3日間のカットオーバー後監視が行われます。このアプローチにより、リスクが軽減され、検証に時間を取ることができます。

- cdFMCからのポリシー展開。
- デバイスのヘルスステータス。
- 両方のHAペアのHAステータス。
- クラウドでのイベント/分析の可視化
- 次のフェーズに進む前の運用上の問題。

設定の凍結の実装

次のアプローチを使用して、移行/評価期間中に設定を固定します。

- 最適なオプション：各フェーズが検証およびコミットされるまで、FMCv300とcdFMC間のすべてのFTD関連の設定変更を凍結します。
- 最小オプション：移行中のデバイスと、移行されたデバイスと移行されていないデバイスの両方で使用されている共有ポリシー/オブジェクトを固定します。
- 段階的な移行時には、FMCv300とcdFMCの両方で同じ共有ポリシー/オブジェクトを編集しないでください。
- 評価期間中の大きな変更は避けてください。

緊急変更プロセス

移行中の緊急変更の場合：

- 変更は、そのデバイスの現在の権限のあるマネージャにのみ適用します。
 - 移行されていないデバイス：FMCv300
 - 移行済みデバイス：cdFMC
- 変更、影響を受けるポリシー/オブジェクト、タイムスタンプ、デバイスの範囲を文書化します。
- フェーズが完了した後で変更を調整します。特に、共有オブジェクトまたは共有ポリシーに影響を与える場合に調整します。

評価期間管理

14日間の評価期間に関する重要な考慮事項：

- 各移行フェーズ/ジョブの14日間の評価期間を追跡します。
- 意図せずに自動コミットに達するフェーズはありません。
- 3日間の監視が成功した場合は、14日間待機せずにフェーズを手動でコミットします。

FMCv300運用停止プロセス

デバイスの移行直後にFMCv300の電源をオフにしたり、取り外したりしないでください。FMCv300は次の期間まで使用可能な状態を維持：

- すべてのFTDデバイスが正常に移行されます。
- cdFMCの展開が成功しました。
- クラウド分析/イベントが確認されました。
- 移行がコミットされます。
- すべてのログ/イベント保存要件が満たされます。
- 最終のFMCv300バックアップは、組織のポリシーに従って保持されます。

これらの条件が満たされると、標準的な仮想マシンの廃棄プロセスに従って、FMCv300をアクティブな使用から削除し、使用を停止することができます。

原因

これは、オンプレミスのFMCからcdFMCへの移行計画です。この移行は、クラウドベースの管理機能を活用し、既存のFMCv300仮想アプライアンスを廃止する必要性によって推進されています。

関連コンテンツ

- [FTDのcdFMCへの移行：シスコのドキュメント](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。