FMCvのアップグレードとVMware ESXi 7.0からESXi 8.0への移行：段階的アプローチとベストプラクティス

内容

問題

VMware ESXi 7.0上でFirewall Management Center(FMCv)virtual(FMCv)バージョン7.3.1を実行している管理者が、FMCをサポートされる上位バージョンにアップグレードし、その後、FMCv仮想マシンを新しいVMware ESXi 8.0クラスタに移行することを計画している。この計画作業の間に、次の問題が発生しました。

- 最初にFMCvを7.3.1から7.4.2にアップグレードしてからVMをESXi 8.0クラスタに移行し、その後でアップグレードを実行するのが安全かどうか。
- バージョン7.3.1または7.4.2を実行するFMCvをVMware ESXi 8.0環境に移行する際に、互換性に関する既知の問題や制約があるかどうか。
- VMware vMotionを使用して、新しいVMインスタンスを作成せずに、FMCv仮想マシンから新しいクラスタへのシームレスな同じIP移行を実行できるかどうか。
- アップグレードまたは移行が失敗した場合に、VMwareスナップショットをバックアップおよびロールバックメカニズムとして使用できるかどうか。
- サポート可能なFMCの中で最も高いバージョンは、既存のマネージドデバイスの環境に関するものです。これには、バージョン7.2.8 ~ 7.4.2の範囲のファイアウォール脅威対策(FTD)デバイスが含まれます。
- 同じ管理IPアドレスとホスト名を維持したまま、新しいクラスタの新しいFMCvインスタンスに切り替えるときにIPアドレスの競合を回避する方法
- リスクとダウンタイムを最小限に抑える段階的なアップグレードおよび移行計画の運用の正しい順序

環境

- 製品：FMCv
- 現在のFMCソフトウェアバージョン：7.3.1
- 現在のハイパーバイザプラットフォーム：VMware ESXi 7.0
- ターゲットハイパーバイザプラットフォーム：VMware ESXi 8.0.3（新しいクラスタ）
- FMC導入タイプ：スタンドアロン（ハイアベイラビリティペアの一部ではない）
- 管理対象デバイス：バージョン7.2.8 ~ 7.4.2の複数のFTDデバイス

解決方法

この環境に推奨されるアプローチは、段階的な段階的アップグレードと移行計画です。この計画では、FMCソフトウェアのアップグレード、ハイパーバイザプラットフォームの移行、および以降のFMCバージョンのアップグレードを個別のメンテナンスイベントに分離します。このアプローチにより、各フェーズでのリスクが軽減され、ロールバックのポイントが明確になります。VMware vMotion、スナップショット、クローニング、またはVMレベルの直接移行を使用する方法は、クラスタ間またはバージョン間でFMCvを移行する方法としてサポートされていません。

重要：VMwareのスナップショット、vMotion、およびクローニングは、FMCv移行ではサポートされていません

この計画の任意のフェーズに進む前に、VMwareネイティブの移行方法に関する次の制約を理解することが重要です。

- VMwareスナップショットは、FMCvのアップグレードまたは移行でサポートされるバックアップ、リストア、またはロールバックの方法ではありません。FMCvをVMwareスナップショットに戻すと、データベースの破損、バージョンとコンテンツのアップデートの不一致、またはサポートされていないシステム状態が発生する可能性があります。
- VMware vMotion、クローニング、およびクラスタ間での仮想マシンの直接移行は、FMCvを新しいハイパーバイザプラットフォームに移行するためのサポートされている方法ではありません。これらのメソッドは、FMCの内部データ整合性メカニズムをバイパスします。
- FMCvを新しいクラスタまたはホストに移行する方法としてサポートされているのは、FMCのネイティブバックアップと復元ワークフローと、ターゲットプラットフォームへの新しいFMCvインスタンスの導入だけです。

カットオーバー後に検証が失敗した場合の正しいロールバック方法は、新しいFMCvインスタンスの電源をオフにして、元のFMCvをサービスに戻すことです。この場合、スナップショットの復帰に依存しないでください。

フェーズ1：アップグレード前の互換性チェック

FMCソフトウェアのアップグレードを開始する前に、環境内のすべての管理対象FTDデバイスの正確なソフトウェアバージョンを確認します。

- FMC 7.4.2では、バージョン7.0以降を実行するFTDデバイスの管理がサポートされています。
- FMC 7.6.6では、バージョン7.1以降を実行しているFTDデバイスの管理がサポートされています。
- 環境内の任意のFTDデバイスがバージョン< 7.0を実行している場合、FMC自体をアップグレードする前に、FMCをバージョン7.3.1のままにしたまま、そのデバイスをバージョン7.0以上にアップグレードする必要があります。
- このドキュメントに記載されている環境（FTDの範囲：7.2.8 ~ 7.4.2）では、管理対象デバイスはすべてFMC 7.4.2とFMC 7.6.6の両方の互換性範囲内にあります。この場合、FTDのアップグレード前は不要です。

次に進む前に、次の点も確認してください。

- FMCはスタンドアロンであり、ハイアベイラビリティ(HA)ペアの一部ではありません。
- 新しいクラスタに正確なVMware ESXi 8.0が構築されます（この環境ではESXi 8.0.3として確認されています）。
- FMCvリソースプロファイル（vCPU、メモリ、ディスク）は、ターゲットFMCリリースの要件を満たしています。4つのvCPU、32 GBのRAM、および250 GBのディスクの現在の仕様は、特にFMC 7.6.6にアップグレードする前に、現在の導入ガイドラインに照らして確認する必要があります。
- 移行後にFMC管理IPアドレスとホスト名が同じままかどうか（すべての管理対象FTDデバイスでマネージャアドレスの更新が必要とされないようにすることを強く推奨）。

フェーズ2：現在のESXi 7.0クラスタで既存のFMCvを7.3.1から7.4.2にアップグレードする

このフェーズでは、FMCvソフトウェアをバージョン7.4.2にアップグレードしますが、既存のESXi 7.0インフラストラクチャには残ります。FMCv 7.4.2では、フェーズ3のプラットフォーム移行の前に必要なVMware ESXi 8.0の明示的なサポートが追加されています。

ステップ1:アップグレードを開始する前に、FMCで現在実行中の保留中のポリシー展開、アクティブなバックアップジョブ、またはバックグラウンドタスクがないことを確認します。

手順2:FMC組み込みバックアップユーティリティを使用して、ネイティブFMCのフルバックアップを実行します。バックアップは、FMCv仮想マシンの外部の安全なリモートロケーションに保存します。続行する前に、バックアップが正常に完了することを確認します。

ステップ3:FMC 7.4アップグレード計画ガイドに記載されているように、すべてのアップグレード準備状況チェックを実行します。アップグレードを開始する前に、フラグが設定された問題を解決します。

手順4:既存のFMCvをバージョン7.3.1からバージョン7.4.2にアップグレードします。ここでは、サポートされているアップグレード移行パス7.3 → 7.4を使用します。

ステップ5:アップグレードが完了したら、アップグレード後の検証を実行します。

- 管理対象のすべてのFTDデバイスがFMCに再接続されたことを確認します。
- イベント取り込みがアクティブで、FMCにイベントが表示されていることを確認します。
- ライセンスのステータスが正しいことを確認します。
- 管理対象デバイスへのテストポリシーの展開を実行し、成功することを確認します。

アップグレードされたFMCv 7.4.2でアップグレード後のすべての検証手順が正常に完了するまで、フェーズ3に進まないでください。

フェーズ3：ネイティブバックアップおよび復元を使用したVMware ESXi 8.0.3クラスタへのFMCvの移行

このフェーズでは、FMCvを既存のESXi 7.0クラスタから新しいESXi 8.0.3クラスタに移行します。これを行うには、ターゲットクラスタに新しいFMCvインスタンスを導入し、ネイティブFMCバックアップを復元します。すべての管理対象FTDデバイスでマネージャアドレスを変更する必要がないように、同じ管理IPアドレスとホスト名が保持されます。

ステップ1:バージョン7.4.2でFMCvの安定性が確認されたら、新しいネイティブFMCバックアップを生成します。安全なリモートロケーションに保存します。続行する前に、バックアップが完了し、有効であることを確認してください。

手順2:新しいFMCvインスタンスをESXi 8.0.3クラスタに導入します。この新しいインスタンスのソフトウェアバージョンとビルドは、バックアップ元のFMCv(FMCv 7.4.2)のバージョン（パッチとホットフィックスを含む）と正確に一致している必要があります。 新しいインスタンスが同等以上のリソース（vCPU、メモリ、ディスク）で設定されていること、およびネットワーク設定がステージングされているが、この時点で本番管理のIPアドレスが新しいインスタンスにまだ割り当てられていないことを確認します。

手順3:ネイティブFMCのバックアップをESXi 8.0.3の新しいFMCvインスタンスに復元します。

手順4:実稼働管理のIPアドレスとホスト名を使用して新しいFMCvをオンラインにする前に、元のFMCvの電源を完全にオフにするか、ネットワークから切断します。これは、重複したIP状態を防ぎ、2つのFMCインスタンスが同じ管理対象FTDデバイスと同時に通信しようとするのを防ぐために必須のステップです。

元のFMCvの電源がオフになり、新しいFMCvがオンラインになる前の期間は、管理対象FTDデバイスでは次の動作が予想されます。

- トラフィック転送：FTDデバイスは、FMCとは独立してデータプレーンを操作し、ここで説明されている場合を除いて、トラフィックをシームレスに転送し、最後に正常に導入されたアクセスコントロールポリシーを適用します。
- 管理と可視性の変更：ポリシーの導入、設定の調整、FMCヘルスアラート、およびデバイス管理の可視性がまったく利用できなくなります。
- イベントのバッファリングと損失の可能性：FMCでのリアルタイムのイベント可視性が一時停止しています。FTDはセキュリティと接続のイベントを一時的な統合ファイルにローカルで記録しようとしますが、これらのファイルには厳格なストレージ制限があり、循環オーバーライトに基づいて動作します。拡張移行ウィンドウ中に大量の接続ログが上書きまたは失われる可能性があります。ローカルバッファに残っているイベントは、新しいFMCがオンラインになると、そのFMCにストリーミングされます。
- マルウェア(AMP)ルール：キャッシュされていないファイルのリアルタイムクラウドルックアップ要求は、FMCがレピュテーションクエリをAMPクラウドにプロキシするため、一時的に使用できません。FTDは、ローカルのオンボックス廃棄キャッシュにすでに保存されているファイルに対してのみ、引き続きブロックまたは許可のルールを適用します。キャッシュされていないファイルはクラウド分析をバイパスし、ポリシーのフェールセーフ設定（通常はトラフィックの中断を防ぐためにフェールオープン）を使用します。 Threat Gridおよびレトロスペクティブアラートへのサンドボックス送信は、新しいFMCが稼働するまで一時停止されます。

- IDベースのルール：FTDはアクティブマッピングをローカルメモリに保持するため、すでにログインしてIPアドレスにマッピングされているユーザに対しても、割り込みは発生しません。ただし、FMCはアイデンティティソース（たとえば、Cisco ISEまたはActive Directoryエージェント）のブローカとして機能するため、このウィンドウ中の新しいユーザログインまたはIPの変更はFTDによって学習されません。これらの不明なセッションは、ポリシーのデフォルトまたはゲストルールにフォールバックします。

- URLフィルタリング：FMCがCisco Talosクラウドに不明なURL要求をプロキシするため、完全に不明なWebサイトのライブクラウド検索が一時的に使用できません。FTDは、プッシュされたローカルデータセットまたはアクティブなローカルメモリキャッシュ内ですでに検出されたWebサイトに対してのみ、引き続きポリシーを完全にフィルタリングして適用します。キャッシュされていない未知のURLに到達するWebトラフィックは、クラウドの分類をバイパスし、分類されていないトラフィック（通常は許可される）に対するポリシーのフォールバック設定に一致します。 URLデータベースパッケージの更新は、新しいFMCがオンラインになるまで一時停止されます。

手順5:ESXi 8.0.3で復元されたFMCvに実稼働管理のIPアドレスとホスト名を割り当て、オンラインにします。同じIPアドレスとホスト名が使用されるため、管理対象のFTDデバイスは、個々のFTDデバイス上でマネージャアドレスを変更することなく、自動的にFMCに再接続できます。

手順6:移行後の検証を実行します。

- 管理対象のすべてのFTDデバイスが新しいFMCvインスタンスに再接続したことを確認します。

- ライセンスステータスを確認し、すべてのライセンスが正しく適用されていることを確認します。

- イベントフローとすべての外部統合が正常に機能していることを確認します。

- 管理対象デバイスへの制御されたポリシー展開を実行し、成功することを確認します。

このフェーズのいずれかの時点で検証が失敗した場合は、新しいFMCvインスタンスの電源をオフにし、ESXi 7.0上の元のFMCvをサービスに復元し、移行を再試行する前にトラブルシューティングを行います。ロールバックメカニズムとしてVMwareスナップショットの復元を使用しないでください。

フェーズ4:FMCvを7.4.2から7.6.6にアップグレードする（移行が安定していることを確認した後）

FMCvからESXi 8.0.3への移行が完全に検証され、安定していることが確認されたら、FMC

7.6.6へのアップグレードを検討できます。ハイパーバイザプラットフォームの移行（フェーズ3）と、この追加のFMCバージョンのアップグレードを1つのメンテナンスイベントに組み合わせることは強く推奨します。移行を開始する前に、まず移行を完了することで、クリーンでリスクの低いチェックポイントが得られます。

7.6.6へのアップグレードを開始する前に、次の前提条件を確認します。

- 環境内の管理対象FTDデバイスはすべて、バージョン7.1以降を実行しています。FMC 7.6.6では、FTDデバイス< version 7.1の管理はサポートされていません。文書化された環境（FTDの範囲：7.2.8 ~ 7.4.2）では、すべてのデバイスがこの要件を満たしています。
- FMCvリソースプロファイル（4 vCPU、32 GB RAM、250 GBディスク）は、この環境における管理対象デバイス総数とイベント保持要件の合計について、FMC 7.6.6導入ガイドラインに照らして検証されています。
- サポートされているアップグレード移行パスが確認されました：7.4 → 7.6。
- FMCはスタンドアロンとして確認されています（ハイアベイラビリティペアの一部ではありません）。

手順1:ESXi 8.0.3上の安定したFMCv 7.4.2インスタンスから新しいネイティブFMCのバックアップを作成して確認します。安全なリモートロケーションに保存します。

手順2:FMCvをバージョン7.4.2からバージョン7.6.6にアップグレードします。

手順3:アップグレード後の最終検証を実行します。

- 管理対象のすべてのFTDデバイスがFMCに再接続されたことを確認します。
- イベント処理とイベント取り込みが正常に機能していることを確認します。
- ライセンスのステータスが正しいことを確認します。
- 制御されたポリシー展開を実行して、ポリシーの適用が正常に行われたことを確認します。

アップグレードパスと移行シーケンスの概要

次の表に、ステージングされた計画全体、サポートされているアップグレード移行および各フェーズでの主なアクションをまとめます。

フェ	アクション	FMCバージョ	ハイパー	サポートされる移行

ーズ		ン	バイザ	
フェーズ1	アップグレード前の互換性チェック、FTDバージョン、FMC HAステータス、およびリソースプロファイルの確認	7.3.1（現在）	ESXi 7.0	該当なし – 準備のみ
フェーズ2	FMCvソフトウェアのアップグレード、ネイティブバックアップの実行、管理対象デバイスとポリシー展開の検証	7.3.1 → 7.4.2	ESXi 7.0	7.3 → 7.4（サポート）
フェーズ3	ESXi 8.0.3への新しいFMCvの導入、ネイティブバックアップの復元、同じIP/ホスト名を使用したカットオーバー、検証	7.4.2（バージョン変更なし）	ESXi 7.0 → ESXi 8.0.3	ネイティブ・バックアップ/リストア：サポートされている方法
フェーズ4	安定した移行後：FMCvをアップグレードし、デバイスの接続、ライセンス、イベント、ポリシーを検証	7.4.2 → 7.6.6	ESXi 8.0.3	7.4 → 7.6（サポート）

主な考慮事項

- アップグレードパスのコンプライアンス：完全なアップグレードシーケンス(7.3.1 → 7.4.2 → 7.6.6)では、サポートされているFMCアップグレード移行パス（7.3 → 7.4および7.4 → 7.6）が使用されます。 中間バージョンをスキップしたり、複数のフェーズを1つのイベントに結合したりすることは推奨されません。
- FMC-FTDの互換性：FMC 7.6.6では、バージョン7.2.8 ~ 7.4.2が稼働するFTDデバイスとの完全な管理互換性が維持されています。FMC 7.6では、管理対象のすべてのFTDデバイスがバージョン7.1以降である必要があります。
- 同じIPアドレスカットオーバー：交換用のFMCvを実稼働管理IPアドレスでオンラインにする前に、元のFMCvの電源を完全にオフにするか、ネットワークから切断する必要があります。これにより、IPの重複状態が防止され、2つの管理センターが同じFTDデバイスと同時に通信しようとする事態が回避されます。復元されたFMCvが同じIPアドレスとホスト名で戻ると、管理対象のFTDデバイスはマネージャアドレスを変更せずに再接続できます。
- 7.6.6より前のリソース検証：FMCvリソースプロファイル（4 vCPU、32 GB RAM、250 GBディスク）は、FMC 7.6.6にアップグレードする前に、環境の管理対象デバイス総数とイベント保持要件を考慮して、現在の導入ガイドラインに照らして確認する必要があります。
- ネイティブバックアップの検証：ネイティブFMCバックアップが作成される各フェーズで

、バックアップが完了して有効であることを確認してから続行する必要があります。バックアップは、FMCv仮想マシンの外部の安全なリモートロケーションに保存する必要があります。

- 移行とアップグレードを組み合わせないでください。プラットフォームの移行（フェーズ3）と、それに続く7.6.6へのFMCバージョンのアップグレード（フェーズ4）は、別個のメンテナンスイベントとして実行する必要があります。これにより、ESXi 8.0.3上のFMCv 7.4.2にクリーンチェックポイントが存在することが確認され、その後に変更が行われます。

原因

これは、ソフトウェアの不具合や設定ミスによる故障修理の問題ではありません。このガイダンスを必要とする根本的な原因は、バージョン互換性要件と、VMware上のCisco FMCvに固有のプラットフォーム移行制限の組み合わせにあります。

- FTD 7.4.2とのFMCバージョンの互換性：バージョン7.4.2が稼働する管理対象FTDデバイスが環境内に存在する場合、以前のFMCバージョンではFMC自体よりも高いバージョンのFTDデバイスを管理できないため、FMCをバージョン7.4.2以上にアップグレードする必要があります。
- VMware ESXi 8.0のFMCvサポート： FMCv 7.3.1は、VMware ESXi 8.0をハイパーバイザプラットフォームとしてサポートしていません。FMCvをESXi 8.0.xに導入または運用するには、バージョン7.4.2以降にアップグレードする必要があります。最初にFMCソフトウェアをアップグレードせずにFMCv 7.3.1 VMをESXi 8.0に直接移行しようとすると、互換性リスクが発生します。
- サポートされていないVM移行方法：VMware vMotion、スナップショット、クローニング、およびVMの直接移行は、クラスタ間またはハイパーバイザバージョン間でのFMCvの移行ではサポートされていません。これらのメソッドは、データベースの破損、バージョンの不一致、またはサポートされていないシステム状態を引き起こす可能性があります。サポートされている唯一の移行パスは、FMCネイティブのバックアップおよび復元ワークフローと、ターゲットプラットフォームでの新しいFMCvの導入を組み合わせたものです。

関連コンテンツ

- Cisco Secure Firewall Management Centerアップグレードガイド、バージョン7.4：アップグレードの計画とサポートされるパス

- Cisco Secure Firewall Management Centerアップグレードガイド、バージョン7.6：アップグレードの計画とサポートされるパス
- Cisco Secure Firewall Management Center互換性ガイド（FMCおよびFTD互換性マトリックス）
- リリース別のCisco Secure Firewall Management Center新機能：バージョン7.4.2
- Cisco Firepower Management Centerアップグレードガイド：アップグレード計画
- 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。