Firepower Management Center のアップグレード

アップグレード チェックリスト：Firepower Management Center

このチェックリストを使用して Firepower Management Center（FMCv を含む）をアップグレードします。ハイアベイラビリティペアの FMC をアップグレードする場合は、チェックリストをピアごとに完了します。

アップグレードを行うたびにチェックリストを完了します。ステップの実行を省略すると、アップグレードが失敗する場合があります。プロセスの間、展開環境内のアプライアンスが正常に通信していること、およびヘルスモニタによって報告された問題がないことを確認します。

アップグレードの計画

アップグレードパスを正しく計画し、そのパスに従うことによって、常に展開の互換性を保ちます。

✓	アクション/チェック	詳細
	アップグレードパスを確認する アップグレードパスにおける自分の位置を確認します。実行したアップグレードと次に実行するアップグレードを確認します。	アップグレードパス：Firepower Management Center （3 ページ）

✓	アクション/チェック	詳細
	バージョンを確認する FMC で現在のバージョンとターゲットバージョンを確認します。 • FirePOWER ソフトウェア • 仮想ホスティング環境（FMCv）	Firepower Management Center
	FMC の互換性を確認する FMC のアップグレード後に、その Firepower Management Center でデバイスを管理できるかどうか確認します。管理できない場合は、最初にデバイスをアップグレードするようアップグレードパスを修正します。	FMC デバイスのバージョン互換性を維持できるか
	リリースノートを読む 次のアップグレード/一連のアップグレードのリリースノートを読み、バージョン固有の警告とガイドラインに特に注意してください。	FirePOWER リリースノート

アップグレード前のアクションおよびチェック

メンテナンスウィンドウ外で事前チェックを実行することによって、中断を最小化します。

✓	アクション/チェック	詳細
	必要な設定変更を行う 必要なアップグレード前の設定変更を行うとともに、必要なアップグレード後の設定変更を行う準備をします。	FirePOWER リリースノート
	ディスク容量を確認する FirePOWER ソフトウェアアップグレード用の予備のディスク容量を確認します。	時間テストとディスク容量の要件
	アップグレードパッケージを取得する 正しいアップグレードパッケージを取得して、FMC にアップロードします。署名付きの（.tar）パッケージは解凍しないでください。	アップグレードパッケージの取得およびプッシュ
	準備状況チェックを実行する 準備状況チェックを実行します。バージョン 6.1+ が必要です。	準備状況チェックの実行

✓	アクション/チェック	詳細
	イベントと設定をバックアップする イベントデータと設定データをバックアップします。外部の場所にバックアップして、正常に転送されたことを確認します。デバイスのバックアップを FMC に保存する場合は、それらも外部にバックアップされていることを確認してください。FMC をアップグレードする際に、ローカルに保存されているバックアップは消去されます。	Firepower Management Center Configuration Guide
	メンテナンス時間帯をスケジュールする 影響が最小限になるメンテナンス時間帯をスケジュールします。実行する必要がある作業と、アップグレードにかかる可能性がある時間を考慮してください。	時間テストとディスク容量の要件

Firepower Management Centerのアップグレード

メンテナンスウィンドウでアップグレードを実行します。

✓	アクション/チェック	詳細
	ホスティングをアップグレードする 必要に応じて、ホスティング環境をアップグレードします（FMCv）。	ホスティング環境のドキュメンテーションを参照してください。
	FirePOWER ソフトウェアのアップグレード FirePOWER ソフトウェアをアップグレードします。	スタンドアロンの FMC のアップグレード （5 ページ） または ハイアベイラビリティ FMC のアップグレード （7 ページ）

アップグレードパス：Firepower Management Center

次の表に Firepower Management Center（FMCv を含む）のアップグレードパスを示します。 現在のバージョンから目的のバージョンに直接アップグレードできない場合は、指示に従ってアップグレードパスに中間バージョンを含める必要があります。

（注） バージョン 6.0.0 およびバージョン 6.0.1 へのアップグレードにはプレインストールパッケージが必要です。これは、一部のモデルでバージョン 6.2.0–6.2.3.7 からバージョン 6.3.0+ に直接アップグレードする場合と同様です。詳細については、「プレインストールパッケージの特定」を参照してください。

表 *1*：推奨されるアップグレードパス：*Firepower Management Center*

現在のバージョン	ターゲットバージョン								
	6.5.0	**6.4.0**	**6.3.0**	**6.2.3**	**6.2.2**	**6.2.0**	**6.1.0**	**6.0.1**	**6.0.0**
6.4.0 MC750、1500、3500 の最終サポート。	直接	—	—	—	—	—	—	—	—
6.3.0	直接	直接	—	—	—	—	—	—	—
6.2.3	直接	直接	直接	—	—	—	—	—	—
6.2.2	→6.4.0 → 6.5.0	直接	直接	直接	—	—	—	—	—
6.2.1	→6.4.0 → 6.5.0	直接	直接	直接	直接	—	—	—	—
6.2.0	→6.4.0 → 6.5.0	直接	直接	直接	直接	—	—	—	—
6.1.0	→6.4.0 → 6.5.0	直接	直接	直接	→ 6.2.0 → 6.2.2	直接	—	—	—
6.0.1	→ 6.1.0 →6.4.0 → 6.5.0	→ 6.1.0 →6.4.0	→ 6.1.0 → 6.3.0	→ 6.1.0 → 6.2.3	→ 6.1.0 → 6.2.0 → 6.2.2	→ 6.1.0 → 6.2.0	直接	—	—
6.0.0	→ 6.0.1 → 6.1.0 →6.4.0 → 6.5.0	→ 6.0.1 → 6.1.0 →6.4.0	→ 6.0.1 → 6.1.0 → 6.3.0	→ 6.0.1 → 6.1.0 → 6.2.3	→ 6.0.1 → 6.1.0 → 6.2.0 → 6.2.2	→ 6.0.1 → 6.1.0 → 6.2.0	→ 6.0.1 → 6.1.0	直接	—

現在のバージョン	ターゲットバージョン								
	6.5.0	**6.4.0**	**6.3.0**	**6.2.3**	**6.2.2**	**6.2.0**	**6.1.0**	**6.0.1**	**6.0.0**
5.4. x*	→ 6.0.0 → 6.0.1 → 6.1.0 →6.4.0 → 6.5.0	→ 6.0.0 → 6.0.1 → 6.1.0 →6.4.0	→ 6.0.0 → 6.0.1 → 6.1.0 → 6.3.0	→ 6.0.0 → 6.0.1 → 6.1.0 → 6.2.3	→ 6.0.0 → 6.0.1 → 6.1.0 → 6.2.0 → 6.2.2	→ 6.0.0 → 6.0.1 → 6.1.0 → 6.2.0	→ 6.0.0 → 6.0.1 → 6.1.0	→ 6.0.0 → 6.0.1	直接

*バージョン6.0.0にアップグレードするには、バージョン5.4.1.1以降を実行している必要があります。

スタンドアロンの FMC のアップグレード

この手順を使用して、Firepower Management Center Virtual を含め、スタンドアロンの Firepower Management Center をアップグレードします。

注意 アップグレードしているアプライアンスとの間での変更の展開、またはアップグレードしているアプライアンスの手動での再起動やシャットダウンは行わないでください。進行中のアップグレードを再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

始める前に

ホスティング環境および管理対象デバイスのアップグレードを含め、アップグレードパス内の場所を確認します。この手順のために完全に計画および準備されていることを確認します。

ステップ 1 構成が古い管理対象デバイスに展開します。

メニューバーで、[展開（Deploy）] をクリックします。FMCデバイスを選択し、[展開（Deploy）] をもう一度クリックします。アップグレードする前に展開すると、失敗する可能性が減少します。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。詳細については、を参照してください。トラフィックフロー、検査、およびデバイス動作

ステップ 2 アップグレード前の最終的なチェックを実行します。

- 正常性のチェック：メッセージセンターを使用します（メニューバーの[システムステータス（System Status）] アイコンをクリックします）。導入環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。
- タスクの実行：また、メッセージセンターで、必須タスクが完了していることを確認します。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。後で失敗ステータスメッセージを手動で削除できます。
- ディスク容量のチェック：最終的なディスク容量のチェックを実行します。空きディスク容量が十分でない場合、アップグレードは失敗します。ディスク容量の要件については、「時間テストとディスク容量の要件」を参照してください。

ステップ 3 **[システム（System）] > [更新（Updates）]** を選択します。

ステップ 4 使用するアップグレードパッケージの横にある[インストール（Install）] アイコンをクリックして、FMC を選択します。

ステップ 5 [インストール（Install）] をクリックすると、アップグレードが開始されます。

アップグレードして、FMC を再起動することを確認します。

ステップ 6 ログアウトするまで、メッセージ センターで事前チェックの進行状況をモニタします。

FMC のアップグレード中は、構成に変更を加えたり、デバイスに構成を展開したりしないでください。メッセージ センターに進行状況が数分間表示されない、またはアップグレードが失敗したことが示されている場合でも、アップグレードを再開したり、FMC を再起動したりしないでください。代わりに、Cisco TAC にお問い合わせください。

ステップ 7 可能なときに、FMC に再度ログインします。

- マイナーアップグレード（パッチとホットフィックス）：アップグレードが完了し、FMC が再起動した後にログインできます。
- メジャー アップグレード：アップグレードが完了する前にログインできます。アップグレードの進行状況をモニタし、アップグレードログとエラーメッセージを確認するために使用できるページが FMC に表示されます。アップグレードが完了し、FMC が再起動すると再度ログアウトされます。リブート後に、再ログインしてください。

ステップ 8 プロンプトが表示されたら、エンド ユーザ ライセンス契約書（EULA）を確認し、承認します。

ステップ 9 アップグレードが成功したことを確認します。

ログイン時に、FMC からアップグレードの成功メッセージが表示されない場合は、**[ヘルプ（Help）] > [バージョン情報（About）]** を選択して、現在のソフトウェアのバージョン情報を表示します。

ステップ 10 メッセージ センターを使用して、導入環境に問題がないことを再度確認します。

ステップ 11 侵入ルール（SRU）および脆弱性データベース（VDB）を更新します。

シスコ サポート & ダウンロード サイトで利用可能な SRU や VDB が現在実行中のバージョンより新しい場合は、新しいバージョンをインストールします。詳細については、Firepower Management Center Configuration Guideを参照してください。侵入ルールを更新する場合、ポリシーを自動的に再適用する必要はありません。後で適用します。

ステップ 12 リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

ステップ 13 構成を再展開します。

すべての管理対象デバイスに再展開します。 デバイスに構成を展開しない場合、最終的なアップグレードが失敗し、イメージの再作成が必要になることがあります。

ハイ アベイラビリティ FMC のアップグレード

この手順を使用して、ハイ アベイラビリティ ペアに含まれる Firepower Management Center の FirePOWER ソフトウェアをアップグレードします。

一度に 1 つのピアをアップグレードします。同期を一時停止して、まずスタンバイをアップグレードしてから、アクティブにします。スタンバイ FMC で事前チェックが開始されると、ステータスがスタンバイからアクティブに切り替わり、両方のピアがアクティブになります。この一時的な状態は *split-brain* と呼ばれていて、アップグレード中を除き、サポートされていません。ペアが split-brain の状況で、構成の変更または展開を行わないでください。同期の再開後は変更内容が失われます。

⚠

注意 アップグレードしているアプライアンスとの間での変更の展開、またはアップグレードしているアプライアンスの手動での再起動やシャットダウンは行わないでください。進行中のアップグレードを再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

始める前に

管理対象デバイスのアップグレードを含め、アップグレードパス内の場所を確認します。この手順のために完全に計画および準備されていることを確認します。

ステップ 1 アクティブな FMC で、構成が古い管理対象デバイスに展開します。

メニューバーで、[展開（Deploy）] をクリックします。FMCデバイスを選択し、[展開（Deploy）] をもう一度クリックします。アップグレードする前に展開すると、失敗する可能性が減少します。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、いくつかの設定を展開することで Snort が再起動されます。これにより、トラフィックのインスペクションが中断し、デバイスのトラフィックの処理方法によっては、再起動が完了するまでトラフィックが中断する場合があります。詳細については、を参照してください。トラフィックフロー、検査、およびデバイス動作

ステップ 2 同期を一時停止する前に、メッセージ センターを使用して導入環境に問題がないことを確認します。

FMC メニュー バーで、[システム ステータス（System Status）] アイコンをクリックして、メッセージ センターを表示します。導入環境内のアプライアンスが正常に通信していること、およびヘルス モニタによって報告された問題がないことを確認します。

ステップ 3 同期を一時停止します。

a) **[システム（System）] > [統合（Integration）]**を選択します。
b) [ハイ アベイラビリティ（High Availability）] タブで、[同期の一時停止（Pause Synchronization）] をクリックします。

ステップ 4 FMC を一度に 1 つずつアップグレード： 最初はスタンバイ、次はアクティブです。

「スタンドアロンの FMC のアップグレード （5 ページ）」の手順に従います。ただし、初期の展開は省略し、各 FMC で更新が成功したことを確認したら停止します。要約すると、それぞれの FMC で以下の手順を実行します。

a) 最終的なアップグレード前チェック（健全性、実行中のタスク、ディスク容量）を実行します。
b) **[システム（System）] > [更新（Updates）]** ページで、アップグレードをインストールします。
c) ログアウトするまで進行状況をモニタし、可能な場合な再度ログインします（これは主なアップグレードで 2 回行われます）。
d) アップグレードが成功したことを確認します。

ペアが split-brain の状況で、構成の変更または展開を行わないでください。

ステップ 5 アクティブ ピアにする FMC で、同期を再開します。

a) **[システム（System）] > [統合（Integration）]** の順に選択します。
b) [ハイ アベイラビリティ（High Availability）] タブで、[アクティブにする（Make-Me-Active）] をクリックします。
c) 同期が再開し、その他の FMC がスタンバイ モードに切り替わるまで待ちます。

ステップ 6 メッセージ センターを使用して、導入環境に問題がないことを再度確認します。

ステップ 7 侵入ルール（SRU）および脆弱性データベース（VDB）を更新します。

シスコ サポート & ダウンロード サイトで利用可能な SRU や VDB が現在実行中のバージョンより新しい場合は、新しいバージョンをインストールします。詳細については、Firepower Management Center Configuration Guideを参照してください。侵入ルールを更新する場合、ポリシーを自動的に再適用する必要はありません。後で適用します。

ステップ 8 リリース ノートに記載されているアップグレード後の構成の変更をすべて完了します。

ステップ 9 構成を再展開します。

すべての管理対象デバイスに再展開します。 デバイスに構成を展開しない場合、最終的なアップグレードが失敗し、イメージの再作成が必要になることがあります。