Firepower Threat Defense 論理デバイスのアップグレード

アップグレード チェックリスト：FMC を搭載した Firepower Threat Defense

Firepower Threat Defense のアップグレードを行う前にこのチェックリストを完了します。

（注） プロセス中は常に、展開の通信と正常性を維持してください。

ほとんどの場合、進行中のアップグレードを再開しないでください。ただし、バージョン6.7.0からのメジャーおよびメンテナンス FTD アップグレードを行った後は、失敗または進行中のアップグレードを手動でキャンセルし、失敗したアップグレードを再試行できます。[Device Management] ページおよびメッセージセンターからアクセスできる [Upgrade Status] ポップアップを使用するか、FTD CLI を使用してください。デフォルトでは、FTD はアップグレードが失敗すると自動的にアップグレード前の状態に戻ります（「自動キャンセル」）。失敗したアップグレードを手動でキャンセルまたは再試行できるようにするには、アップグレードを開始するときに自動キャンセルオプションを無効にします。パッチの自動キャンセルはサポートされていません。高可用性またはクラスタ展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1 つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。すべてのオプションを使い切った場合、または展開でキャンセルや再試行がサポートされていない場合は、Cisco TAC にお問い合わせください。

計画と実現可能性

誤りを避けるには、注意深い計画と準備が役立ちます。

表 *1*：

✓	アクション/チェック
	アップグレードパスを計画します。 これは、マルチアプライアンス展開、マルチホップアップグレード、または展開の互換性を常に維持しながらオペレーティングシステムまたはホスティング環境をアップグレードする必要がある状況では特に重要です。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常に確認します。 （注） FMC 展開では、通常、FMC をアップグレードしてから、管理対象デバイスをアップグレードします。ただし、場合によっては、最初にデバイスをアップグレードする必要があります。 アップグレードパスを参照してください。
	すべてのアップグレードのガイドラインを読み、設定の変更を計画します。 主要なアップグレードでは特に、アップグレードの前または後に、アップグレードにより重要な設定変更が発生することがあります。アップグレードの警告、動作の変更、新機能と廃止された機能、および既知の問題など、リリース固有の重要な情報を含むリリースノートから読み始めます。
	アプライアンスへのアクセスを確認します。 デバイスは、（インターフェイス設定に応じて）アップグレード中、またはアップグレードが失敗した場合に、トラフィックを渡すことを停止できます。アップグレードする前に、ユーザーの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。FMC の展開では、デバイスを経由せずに FMC 管理インターフェイスにアクセスできる必要もあります。
	帯域幅を確認します。 管理ネットワークに大量のデータ転送を実行するための帯域幅があることを確認します。FMC の展開では、アップグレードパケージをアップグレード時に管理対象デバイスに転送する場合は、帯域幅が不十分だとアップグレード時間が長くなったり、アップグレードがタイムアウトする原因となったりする可能性があります。デバイスのアップグレードを開始する前に、可能な場合は常に、アップグレードパッケージを管理対象デバイスにコピーします。 『Guidelines for Downloading Data from the Firepower Management Center to Managed Devices』（トラブルシューティング テクニカルノーツ）を参照してください。

✓	アクション/チェック
	メンテナンス時間帯をスケジュールします。 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。トラフィックフローおよびインスペクションへの影響、および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。また、ウィンドウで実行する必要があるタスクと、事前に実行できるタスクを検討します。 たとえば、メンテナンス時間帯で、アプライアンスへのアップグレードパッケージのコピー、準備状況チェックの実行、バックアップの作成などが行われるまで待機しないようにします。

アップグレードパッケージ

アップグレードパッケージは シスコ サポートおよびダウンロード サイトで入手できます。

表 2:

✓	アクション/チェック
	アップグレードパッケージを FMC または内部 Web サーバーにアップロードします。 バージョン 6.6.0 以降では、FTD アップグレードパッケージのソースとして FMC の代わりに内部 Web サーバーを設定できます。これは、FMC とそのデバイスの間の帯域幅が制限されている場合に役立ち、FMC の容量を節約することができます。 内部サーバへのアップロード（FMC を使用したバージョン 6.6.0 以降の FTD）を参照してください。
	アップグレードパッケージをデバイスにコピーします。 サポートされている場合、デバイスのアップグレードを開始する前に、管理対象デバイスにパッケージをコピー（プッシュ）することをお勧めします。 • バージョン 6.2.2 以前は、アップグレード前のコピーをサポートしていません。 • バージョン 6.2.3 では、FMC からアップグレードパッケージを手動でコピーできます。 • バージョン 6.6.0 では、アップグレードパッケージを内部 Web サーバーから手動でコピーする機能が追加されています。 • バージョン 7.0.0 では、アップグレードパッケージをコピーするように求める FTD アップグレードのワークフローが追加されています。 （注） Firepower 4100/9300 では、必要な付属の FXOS アップグレードを開始する前に、アップグレードパッケージをコピーすることを推奨（場合によっては必須）しています。 管理対象デバイスへのコピーを参照してください。

バックアップ

災害から回復する能力は、システム保守計画の重要な部分を占めます。

バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティやライセンスの問題を無視しないでください。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、使用する展開の設定ガイドを参照してください。

⚠

注意 アップグレードの前後に、安全な遠隔地にバックアップし、正常に転送が行われることを確認することを強くお勧めします。

表 *3:*

✓	アクション/チェック
	FTD をバックアップします。 FMC を使用してデバイスをバックアップします。すべての FTD プラットフォームおよび設定でバックアップがサポートされているわけではありません。バージョン 6.3.0 以降が必要です。 アップグレードの前後にバックアップします（サポートされている場合）。 • アップグレード前：アップグレードが致命的な失敗であった場合は、再イメージ化を実行し、復元する必要がある場合があります。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。最近のバックアップがある場合は、通常の操作にすばやく戻ることができます。 • アップグレード後：これにより、新しくアップグレードされた展開のスナップショットが作成されます。FMC の展開では、管理対象デバイスをアップグレードした後に FMC をバックアップして、新しい FMC バックアップファイルにデバイスがアップグレードされたことを「認識」させることをお勧めします。
	Firepower 4100/9300 の FXOS をバックアップします。 Firepower Chassis Manager または FXOS CLI を使用して、アップグレードの前後に、論理デバイス設定およびプラットフォーム設定を含むシャーシ設定をエクスポートします。

関連するアップグレード

オペレーティングシステムとホスティング環境のアップグレードはトラフィックフローとインスペクションに影響を与える可能性があるため、メンテナンス時間帯で実行してください。

表 4：

✓	アクション/チェック
	仮想ホスティングをアップグレードします。 必要に応じて、任意の仮想アプライアンスのホスティング環境をアップグレードします。通常、古いバージョンの VMware を実行していて、デバイスのメジャーアップグレードを実行している場合、アップグレードが必要です。
	Firepower 4100/9300 の FXOS をアップグレードします。 必要に応じて、FTD をアップグレードする前に、FXOS をアップグレードします。これは通常、メジャーアップグレードの要件ですが、メンテナンスリリースやパッチの場合は要件になるのは非常にまれです。トラフィックフローとインスペクションでの中断を防ぐには、FTD 高可用性ペアおよびシャーシ間クラスタの FXOS を一度に 1 つずつアップグレードします。 （注） FXOS をアップグレードする前に、必ずすべてのアップグレードのガイドラインを読み、設定の変更を計画してください。FXOS リリースノート：Cisco Firepower 4100/9300 FXOS リリースノート を使用して開始します。

最終チェック

一連の最終チェックにより、 をアップグレードする準備が整います。

表 5：

✓	アクション/チェック
	設定を確認します。 必要なアップグレード前の設定変更を行っていることを確認し、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。
	NTP 同期を確認します。 時刻の提供に使用している NTP サーバーとすべてのアプライアンスが同期していることを確認します。同期されていないと、アップグレードが失敗する可能性があります。FMC 展開では、時刻のずれが 10 秒を超えている場合、ヘルスモニタからアラートが発行されますが、手動で確認する必要もあります。 時刻を確認するには、次の手順を実行します。 • FMC：[システム（System）] > [設定（Configuration）] > [時刻（Time）] を選択します。 • デバイス：**show time** CLI コマンドを使用します。

✓	アクション/チェック
	ディスク容量を確認します。 ソフトウェアアップグレードに関するディスク容量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。 対象バージョンの Cisco Firepower リリース ノート 内の「ソフトウェアのアップグレード」の章を参照してください。
	設定を展開します。 アップグレードする前に設定を展開すると、失敗する可能性が減少します。 一部の展開では、設定が古い場合、アップグレードがブロックされることがあります。FMC における高可用性の展開では、アクティブなピアから展開するだけで済みます。 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。 対象バージョンの Cisco Firepower リリース ノート 内の「ソフトウェアのアップグレード」の章を参照してください。
	準備状況チェックを実行します。 FMC がバージョン 6.1.0 以降を実行している場合は、互換性と準備状況のチェックの実施をお勧めします。これらのチェックにより、ソフトウェアをアップグレードするための準備状況を確認できます。バージョン 7.0.0 では、これらのチェックを完了するように求める新しい FTD アップグレードのワークフローが導入されています。 Firepower ソフトウェアの準備状況チェックを参照してください。
	実行中のタスクを確認します。 アップグレードする前に、デバイスの重要なタスク（最終展開を含む）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。また、アップグレード中に実行するようにスケジュールされたタスクを確認し、それらをキャンセルまたは延期することをお勧めします。

Firepower Threat Defense 論理デバイスを持つ Firepower 4100/9300 上の FXOS のアップグレード

Firepower 4100/9300 で、シャーシ間クラスタリングの Firepower またはハイアベイラビリティペアの構成がある場合でも、各シャーシの FXOS を個別にアップグレードします。FXOS CLI または Firepower Chassis Manager を使用できます。

FXOS をアップグレードするとシャーシが再起動します。導入によっては、トラフィックがドロップしたり、インスペクションなしにネットワークを通過する可能性があります。お使いのバージョンのCisco Firepower リリースノートを参照してください。

FXOSのアップグレード：FTDスタンドアロンデバイスとシャーシ間クラスタ

スタンドアロンの Firepower Threat Defense 論理デバイスの場合、または FTD シャーシ内クラスタ（同じシャーシ上のユニット）の場合は、最初にFXOSプラットフォームバンドルをアップグレードしてから、FTD論理デバイスをアップグレードします。Firepower Management Center を使用して、クラスタ化されたデバイスを 1 つのユニットとしてアップグレードします。

Firepower Chassis Manager を使用したスタンドアロンFTD論理デバイスまたはFTD シャーシ内クラスタ用の FXOS のアップグレード

このセクションでは、スタンドアロン Firepower 4100/9300 シャーシの FXOS プラットフォームバンドルをアップグレードする方法を説明します。

このセクションでは、次のタイプのデバイスのアップグレードプロセスについて説明します。

- FTD論理デバイスで構成されており、フェールオーバーペアまたはシャーシ間クラスタの一部ではない Firepower 4100 シリーズ シャーシ。
- フェールオーバーペアまたはシャーシ間クラスタの一部ではない1つまたは複数のスタンドアロン FTD 論理デバイスで構成されている Firepower 9300 シャーシ。
- シャーシ内クラスタ内の FTD 論理デバイスで構成されている Firepower 9300 シャーシ。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。

手順

ステップ 1 Firepower Chassis Manager で、**[システム（System）]** > **[更新（Updates）]** を選択します。
[使用可能な更新（Available Updates）] ページに、シャーシで使用可能な FXOS プラットフォームバンドルのイメージやアプリケーションのイメージのリストが表示されます。

ステップ 2 新しいプラットフォーム バンドル イメージをアップロードします。

a) [イメージのアップロード（Upload Image）] をクリックして、[イメージのアップロード（Upload Image）] ダイアログ ボックスを開きます。

b) [ファイルを選択（Choose File）] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
c) [Upload] をクリックします。
選択したイメージが Firepower 4100/9300 シャーシにアップロードされます。
d) 特定のソフトウェア イメージについては、イメージをアップロードした後にエンドユーザ ライセンス契約書が表示されます。システムのプロンプトに従ってエンドユーザ契約書に同意します。

ステップ 3 新しいプラットフォーム バンドル イメージが正常にアップロードされたら、アップグレードする FXOS プラットフォーム バンドルの [アップグレード（Upgrade）] をクリックします。

システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

ステップ 4 インストールの続行を確定するには [はい（Yes）] を、インストールをキャンセルするには [いいえ（No）] をクリックします。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 5 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレード プロセスをモニターできます。

a) **scope system** を入力します。
b) **show firmware monitor** を入力します。
c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「`Upgrade-Status: Ready`」と表示されるのを待ちます。

（注）
FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

ステップ 6 すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

a) **top** を入力します。
b) **scope ssa** を入力します。
c) **show slot** を入力します。
d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
e) **show app-instance** を入力します。
f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

FXOS CLI を使用したスタンドアロン FTD 論理デバイスまたは FTD シャーシ内クラスタ用の FXOS のアップグレード

このセクションでは、スタンドアロン Firepower 4100/9300 シャーシの FXOS プラットフォーム バンドルをアップグレードする方法を説明します。

このセクションでは、次のタイプのデバイスの FXOS のアップグレード プロセスについて説明します。

- FTD論理デバイスで構成されており、フェールオーバーペアまたはシャーシ間クラスタの一部ではない Firepower 4100 シリーズ シャーシ。
- フェールオーバーペアまたはシャーシ間クラスタの一部ではない1つまたは複数のスタンドアロン FTD デバイスで構成されている Firepower 9300 シャーシ。
- シャーシ内クラスタ内の FTD 論理デバイスで構成されている Firepower 9300 シャーシ。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。
- Firepower 4100/9300 シャーシにソフトウェア イメージをダウンロードするために必要な次の情報を収集します。
  - イメージのコピー元のサーバーの IP アドレスおよび認証クレデンシャル。
  - イメージ ファイルの完全修飾名。

手順

ステップ 1 FXOS CLI に接続します。

ステップ 2 新しいプラットフォーム バンドル イメージを Firepower 4100/9300 シャーシにダウンロードします。

a) ファームウェア モードに入ります。

Firepower-chassis-a # **scope firmware**

b) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

Firepower-chassis-a /firmware # **download image** *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

c) ダウンロード プロセスをモニタする場合：

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 3 必要に応じて、ファームウェア モードに戻ります。

Firepower-chassis-a /firmware/download-task # **up**

ステップ 4 auto-install モードにします。

Firepower-chassis-a /firmware # **scope auto-install**

ステップ 5 FXOS プラットフォーム バンドルをインストールします。

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number は、インストールする FXOS プラットフォーム バンドルのバージョン番号です（たとえば、2.3(1.58)）。

ステップ 6 システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

yes を入力して、検証に進むことを確認します。

ステップ 7 インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 8 アップグレード プロセスをモニタするには、次の手順を実行します。

a) **scope system** を入力します。
b) **show firmware monitor** を入力します。
c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「`Upgrade-Status: Ready`」と表示されるのを待ちます。

（注）
FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

ステップ 9 すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

a) **top** を入力します。
b) **scope ssa** を入力します。
c) **show slot** を入力します。

d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
e) **show app-instance** を入力します。
f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

FXOS のアップグレード：FTD 高可用性ペア

Firepower Threat Defense の高可用性展開では、どちらかの FTD 論理デバイスをアップグレードする前に、両方のシャーシでFXOSプラットフォームバンドルをアップグレードします。中断を最小限に抑えるため、スタンバイは常にアップグレードします。

Firepower Management Center の展開では、論理デバイスを 1 つのユニットとしてアップグレードします。

1. スタンバイの FXOS をアップグレードします。
2. ロールを切り替えます。
3. 新しいスタンバイの FXOS をアップグレードします。
4. FTD 論理デバイスをアップグレードします。

Firepower Chassis Manager を使用した FTD ハイアベイラビリティペアの FXOS のアップグレード

ハイアベイラビリティペアとして構成されている FTD 論理デバイスを備えた FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスがある場合、次の手順を使用して FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスの FXOS プラットフォームバンドルを更新します。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。

手順

ステップ 1 スタンバイの Firepower Threat Defense 論理デバイスを含む Firepower セキュリティアプライアンス上の Firepower Chassis Manager に接続します。

ステップ 2 Firepower Chassis Manager で、**[システム（System）] > [更新（Updates）]** を選択します。
[使用可能な更新（Available Updates）] ページに、シャーシで使用可能な FXOS プラットフォームバンドルのイメージやアプリケーションのイメージのリストが表示されます。

ステップ 3 新しいプラットフォーム バンドル イメージをアップロードします。

a) [イメージのアップロード（Upload Image）] をクリックして、[イメージのアップロード（Upload Image）] ダイアログ ボックスを開きます。
b) [ファイルを選択（Choose File）] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
c) [Upload] をクリックします。
選択したイメージが Firepower 4100/9300 シャーシにアップロードされます。
d) 特定のソフトウェア イメージについては、イメージをアップロードした後にエンドユーザ ライセンス契約書が表示されます。システムのプロンプトに従ってエンドユーザ契約書に同意します。

ステップ 4 新しいプラットフォーム バンドル イメージが正常にアップロードされたら、アップグレードする FXOS プラットフォーム バンドルの [アップグレード（Upgrade）] をクリックします。

システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

ステップ 5 インストールの続行を確定するには [はい（Yes）] を、インストールをキャンセルするには [いいえ（No）] をクリックします。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 6 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレード プロセスをモニターできます。

a) **scope system** を入力します。
b) **show firmware monitor** を入力します。
c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「`Upgrade-Status: Ready`」と表示されるのを待ちます。

（注）
FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
```

```
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

ステップ 7 すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

a) **top** を入力します。
b) **scope ssa** を入力します。
c) **show slot** を入力します。
d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
e) **show app-instance** を入力します。
f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

ステップ 8 アップグレードしたユニットをアクティブユニットにして、アップグレード済みのユニットにトラフィックが流れるようにします。

a) Firepower Management Center に接続します。
b) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。
c) アクティブ ピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン（  ）をクリックします。
d) ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、[はい（Yes）] をクリックします。

ステップ 9 新しいスタンバイの Firepower Threat Defense 論理デバイスを含む Firepower セキュリティアプライアンス上の Firepower Chassis Manager に接続します。

ステップ 10 Firepower Chassis Manager で、**[システム（System）]** > **[更新（Updates）]** を選択します。
[使用可能な更新（Available Updates）] ページに、シャーシで使用可能な FXOS プラットフォームバンドルのイメージやアプリケーションのイメージのリストが表示されます。

ステップ 11 新しいプラットフォーム バンドル イメージをアップロードします。

a) [イメージのアップロード（Upload Image）] をクリックして、[イメージのアップロード（Upload Image）] ダイアログ ボックスを開きます。
b) [ファイルを選択（Choose File）] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
c) [Upload] をクリックします。

選択したイメージが Firepower 4100/9300 シャーシにアップロードされます。

d) 特定のソフトウェア イメージについては、イメージをアップロードした後にエンドユーザ ライセンス契約書が表示されます。システムのプロンプトに従ってエンドユーザ契約書に同意します。

ステップ 12 新しいプラットフォーム バンドル イメージが正常にアップロードされたら、アップグレードする FXOS プラットフォーム バンドルの [アップグレード（Upgrade）] をクリックします。

システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

ステップ 13 インストールの続行を確定するには[はい（Yes）] を、インストールをキャンセルするには[いいえ（No）] をクリックします。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。アップグレード プロセスは、完了までに最大 30 分かかることがあります。

ステップ 14 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレード プロセスをモニターできます。

a) **scope system** を入力します。

b) **show firmware monitor** を入力します。

c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「`Upgrade-Status: Ready`」と表示されるのを待ちます。

（注）
FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

ステップ 15 すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

a) **top** を入力します。

b) **scope ssa** を入力します。
c) **show slot** を入力します。
d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
e) **show app-instance** を入力します。
f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

ステップ 16 アップグレードしたユニットを、アップグレード前のようにアクティブ ユニットにします。

a) Firepower Management Center に接続します。
b) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。
c) アクティブ ピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン（  ）をクリックします。
d) ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、[はい（Yes）] をクリックします。

FXOS CLI を使用した FTD ハイアベイラビリティペアの FXOS のアップグレード

ハイ アベイラビリティ ペアとして構成されている FTD 論理デバイスを備えた FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスがある場合、次の手順を使用して FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスの FXOS プラットフォームバンドルを更新します。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。
- Firepower 4100/9300 シャーシにソフトウェア イメージをダウンロードするために必要な次の情報を収集します。
  - イメージのコピー元のサーバーの IP アドレスおよび認証クレデンシャル。
  - イメージ ファイルの完全修飾名。

手順

ステップ 1 スタンバイの Firepower Threat Defense 論理デバイスを含む Firepower セキュリティ アプライアンス上の FXOS CLI に接続します。

ステップ 2 新しいプラットフォーム バンドル イメージを Firepower 4100/9300 シャーシにダウンロードします。

a) ファームウェア モードに入ります。

Firepower-chassis-a # **scope firmware**

b) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

Firepower-chassis-a /firmware # **download image** *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

c) ダウンロード プロセスをモニタする場合：

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 3 必要に応じて、ファームウェア モードに戻ります。

Firepower-chassis-a /firmware/download-task # **up**

ステップ 4 auto-install モードにします。

Firepower-chassis-a /firmware # **scope auto-install**

ステップ 5 FXOS プラットフォーム バンドルをインストールします。

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number は、インストールする FXOS プラットフォームバンドルのバージョン番号です（たとえば、2.3(1.58)）。

ステップ 6 システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

yes を入力して、検証に進むことを確認します。

ステップ 7 インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 8 アップグレード プロセスをモニタするには、次の手順を実行します。

a) **scope system** を入力します。
b) **show firmware monitor** を入力します。
c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「Upgrade-Status: Ready」と表示されるのを待ちます。

（注）
FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

ステップ 9 すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

a) **top** を入力します。
b) **scope ssa** を入力します。
c) **show slot** を入力します。
d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
e) **show app-instance** を入力します。

f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

ステップ 10 アップグレードしたユニットをアクティブユニットにして、アップグレード済みのユニットにトラフィックが流れるようにします。

a) Firepower Management Center に接続します。
b) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。
c) アクティブ ピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン（  ）をクリックします。
d) ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、[はい（Yes）] をクリックします。

ステップ 11 新しいスタンバイの Firepower Threat Defense 論理デバイスを含む Firepower セキュリティ アプライアンス上の FXOS CLI に接続します。

ステップ 12 新しいプラットフォーム バンドル イメージを Firepower 4100/9300 シャーシにダウンロードします。

a) ファームウェア モードに入ります。

Firepower-chassis-a # **scope firmware**

b) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

Firepower-chassis-a /firmware # **download image** *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

c) ダウンロード プロセスをモニタする場合：

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
```

```
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 13 必要に応じて、ファームウェア モードに戻ります。

Firepower-chassis-a /firmware/download-task # **up**

ステップ 14 auto-install モードにします。

Firepower-chassis-a /firmware # **scope auto-install**

ステップ 15 FXOS プラットフォーム バンドルをインストールします。

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number は、インストールする FXOS プラットフォームバンドルのバージョン番号です（たとえば、2.3(1.58)）。

ステップ 16 システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

yes を入力して、検証に進むことを確認します。

ステップ 17 インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 18 アップグレード プロセスをモニタするには、次の手順を実行します。

a) **scope system** を入力します。
b) **show firmware monitor** を入力します。
c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「`Upgrade-Status: Ready`」と表示されるのを待ちます。

（注）
FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
```

```
        Upgrade-Status: Ready

FP9300-A /system #
```

ステップ 19 すべてのコンポーネントが正常にアップグレードされたら、次のコマンドを入力して、セキュリティ モジュール/セキュリティエンジンおよびインストールされているアプリケーションの状態を確認します。

a) **top** を入力します。
b) **scope ssa** を入力します。
c) **show slot** を入力します。
d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
e) **show app-instance** を入力します。
f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」であることを確認します。

ステップ 20 アップグレードしたユニットを、アップグレード前のようにアクティブ ユニットにします。

a) Firepower Management Center に接続します。
b) **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択します。
c) アクティブ ピアを変更するハイ アベイラビリティ ペアの横にあるアクティブ ピア切り替えアイコン（  ）をクリックします。
d) ハイ アベイラビリティ ペアでスタンバイ デバイスをアクティブ デバイスにすぐに切り替える場合は、[はい（Yes）] をクリックします。

FXOS のアップグレード：FTD シャーシ間クラスタ

Firepower Threat Defense シャーシ間クラスタ（異なるシャーシのユニット）の場合、FTD 論理デバイスをアップグレードする前に、すべてのシャーシでFXOSプラットフォームバンドルをアップグレードします。中断を最小限に抑えるため、すべてデータユニットのシャーシ上の FXOS を常にアップグレードします。次に、Firepower Management Center を使用して、論理デバイスを 1 つのユニットとしてアップグレードします。

たとえば、2 つのシャーシがあるクラスタの場合：

1. すべてデータユニットのシャーシの FXOS をアップグレードします。
2. 制御モジュールをアップグレードしたシャーシに切り替えます。
3. 新しいすべてデータユニットのシャーシの FXOS をアップグレードします。
4. FTD 論理デバイスをアップグレードします。

Firepower Chassis Manager を使用した FTD シャーシ間クラスタの FXOS のアップグレード

シャーシ間クラスタとして構成されている FTD 論理デバイスを備えた FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスがある場合、次の手順を使用して FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスの FXOS プラットフォームバンドルを更新します。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。

手順

ステップ 1 次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

a) シャーシ #2 の FXOS CLI に接続します（これは制御ユニットを持たないシャーシである必要があります）。
b) **top** を入力します。
c) **scope ssa** を入力します。
d) **show slot** を入力します。
e) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
f) **show app-instance** を入力します。
g) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」、クラスタの状態が「In Cluster」であることを確認します。また、稼働バージョンとして表示されている FTD ソフトウェアのバージョンが正しいことを確認します。

重要
制御ユニットがこのシャーシ上にないことを確認します。「Master」に設定されているクラスタのロールを持つ Firepower Threat Defense インスタンスがあってはいけません。

h) Firepower 9300 appliance にインストールされているすべてのセキュリティ モジュール、または Firepower 4100 シリーズ アプライアンス上のセキュリティ エンジンについて、FXOS バージョンが正しいことを確認してください。

scope server 1/*slot_id* で、Firepower 4100 シリーズ セキュリティ エンジンの場合、*slot_id* は 1 です。

show versionを使用して無効にすることができます。

ステップ 2 シャーシ #2 の Firepower Chassis Manager に接続します（これは制御ユニットを持たないシャーシである必要があります）。

ステップ 3 Firepower Chassis Manager で、**[システム（System）] > [更新（Updates）]** を選択します。
[使用可能な更新（Available Updates）] ページに、シャーシで使用可能な FXOS プラットフォームバンドルのイメージやアプリケーションのイメージのリストが表示されます。

ステップ 4 新しいプラットフォーム バンドル イメージをアップロードします。

a) [イメージのアップロード（Upload Image）] をクリックして、[イメージのアップロード（Upload Image）] ダイアログ ボックスを開きます。
b) [ファイルを選択（Choose File）] をクリックして対象のファイルに移動し、アップロードするイメージを選択します。
c) [Upload] をクリックします。
選択したイメージが Firepower 4100/9300 シャーシにアップロードされます。
d) 特定のソフトウェア イメージについては、イメージをアップロードした後にエンドユーザ ライセンス契約書が表示されます。システムのプロンプトに従ってエンドユーザ契約書に同意します。

ステップ 5 新しいプラットフォーム バンドル イメージが正常にアップロードされたら、アップグレードする FXOS プラットフォーム バンドルの [アップグレード（Upgrade）] をクリックします。

システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

ステップ 6 インストールの続行を確定するには [はい（Yes）] を、インストールをキャンセルするには [いいえ（No）] をクリックします。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 7 Firepower Chassis Manager は、アップグレード中は使用できません。FXOS CLI を使用してアップグレード プロセスをモニターできます。

a) **scope system** を入力します。
b) **show firmware monitor** を入力します。
c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「`Upgrade-Status: Ready`」と表示されるのを待ちます。

（注）
FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

d) **top** を入力します。
e) **scope ssa** を入力します。
f) **show slot** を入力します。
g) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「`Ok`」、操作の状態が「`Online`」であることを確認します。
h) **show app-instance** を入力します。

i) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」、クラスタの状態が「In Cluster」、クラスタのロールが「Slave」であることを確認します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
FP9300-A /ssa #

FP9300-A /ssa # show app-instance
App Name   Slot ID    Admin State Oper State       Running Version Startup Version Profile Name
Cluster State   Cluster Role
---------- ---------- ----------- ---------------- --------------- --------------- ------------
--------------- ------------
ftd        1          Enabled     Online           6.2.2.81        6.2.2.81
In Cluster      Slave
ftd        2          Enabled     Online           6.2.2.81        6.2.2.81
In Cluster      Slave
ftd        3          Disabled    Not Available                    6.2.2.81
Not Applicable  None
FP9300-A /ssa #
```

ステップ 8 シャーシ #2 のセキュリティモジュールの 1 つを制御用として設定します。

シャーシ #2 のセキュリティモジュールの 1 つを制御用として設定すると、シャーシ #1 には制御ユニットが含まれなくなり、すぐにアップグレードすることができます。

ステップ 9 クラスタ内の他のすべてのシャーシに対して手順 1 ～ 7 を繰り返します。

ステップ 10 制御ロールをシャーシ #1 に戻すには、シャーシ #1 のセキュリティモジュールの 1 つを制御用として設定します。

FXOS CLI を使用した FTD シャーシ間クラスタの FXOS のアップグレード

シャーシ間クラスタとして構成されている FTD 論理デバイスを備えた FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスがある場合、次の手順を使用して FirePOWER 9300 または FirePOWER 4100 シリーズのセキュリティアプライアンスの FXOS プラットフォームバンドルを更新します。

始める前に

アップグレードを開始する前に、以下が完了していることを確認します。

- アップグレード先の FXOS プラットフォーム バンドル ソフトウェア パッケージをダウンロードします。
- FXOS と FTD の構成をバックアップします。
- Firepower 4100/9300 シャーシにソフトウェア イメージをダウンロードするために必要な次の情報を収集します。
  - イメージのコピー元のサーバーの IP アドレスおよび認証クレデンシャル。
  - イメージ ファイルの完全修飾名。

手順

ステップ 1 シャーシ #2 の FXOS CLI に接続します（これは制御ユニットを持たないシャーシである必要があります）。

ステップ 2 次のコマンドを入力して、セキュリティ モジュール/セキュリティ エンジンおよびインストールされているアプリケーションの状態を確認します。

a) **top** を入力します。
b) **scope ssa** を入力します。
c) **show slot** を入力します。
d) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「Ok」、操作の状態が「Online」であることを確認します。
e) **show app-instance** を入力します。
f) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「Online」、クラスタの状態が「In Cluster」であることを確認します。また、稼働バージョンとして表示されている FTD ソフトウェアのバージョンが正しいことを確認します。

重要
制御ユニットがこのシャーシ上にないことを確認します。「Master」に設定されているクラスタのロールを持つ Firepower Threat Defense インスタンスがあってはいけません。

g) Firepower 9300 appliance にインストールされているすべてのセキュリティ モジュール、または Firepower 4100 シリーズ アプライアンス上のセキュリティ エンジンについて、FXOS バージョンが正しいことを確認してください。

scope server 1/*slot_id* で、Firepower 4100 シリーズ セキュリティ エンジンの場合、*slot_id* は 1 です。

show versionを使用して無効にすることができます。

ステップ 3 新しいプラットフォーム バンドル イメージを Firepower 4100/9300 シャーシにダウンロードします。

a) **top** を入力します。

b) ファームウェア モードに入ります。

Firepower-chassis-a # **scope firmware**

c) FXOS プラットフォーム バンドル ソフトウェア イメージをダウンロードします。

Firepower-chassis-a /firmware # **download image** *URL*

次のいずれかの構文を使用してインポートされるファイルの URL を指定します。

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

d) ダウンロード プロセスをモニタする場合：

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

例：

次の例では、SCP プロトコルを使用してイメージをコピーします。

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

ステップ 4 必要に応じて、ファームウェア モードに戻ります。

Firepower-chassis-a /firmware/download-task # **up**

ステップ 5 auto-install モードにします。

Firepower-chassis /firmware # **scope auto-install**

ステップ 6 FXOS プラットフォーム バンドルをインストールします。

Firepower-chassis /firmware/auto-install # **install platform platform-vers** *version_number*

version_number は、インストールする FXOS プラットフォーム バンドルのバージョン番号です（たとえば、2.3(1.58)）。

ステップ 7 システムは、まずインストールするソフトウェア パッケージを確認します。そして現在インストールされているアプリケーションと指定した FXOS プラットフォーム ソフトウェア パッケージの間の非互換性を通知します。また既存のセッションを終了することやアップグレードの一部としてシステムをリブートする必要があることが警告されます。

yes を入力して、検証に進むことを確認します。

ステップ 8 インストールの続行を確定するには **yes** を、インストールをキャンセルするには **no** を入力します。

システムがバンドルを解凍し、コンポーネントをアップグレードまたはリロードします。

ステップ 9 アップグレード プロセスをモニタするには、次の手順を実行します。

a) **scope system** を入力します。
b) **show firmware monitor** を入力します。
c) すべてのコンポーネント（FPRM、ファブリック インターコネクト、およびシャーシ）で「`Upgrade-Status: Ready`」と表示されるのを待ちます。

（注）
FPRM コンポーネントをアップグレードすると、システムが再起動し、その他のコンポーネントのアップグレードを続行します。

d) **top** を入力します。
e) **scope ssa** を入力します。
f) **show slot** を入力します。
g) Firepower 4100 シリーズ アプライアンスのセキュリティ エンジン、または Firepower 9300 applianceのインストールされている任意のセキュリティ モジュールについて、管理状態が「`Ok`」、操作の状態が「`Online`」であることを確認します。
h) **show app-instance** を入力します。
i) シャーシにインストールされているすべての論理デバイスについて、操作の状態が「`Online`」、クラスタの状態が「`In Cluster`」、クラスタのロールが「`Slave`」であることを確認します。

例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
```

```
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
FP9300-A /ssa #

FP9300-A /ssa # show app-instance
App Name   Slot ID    Admin State Oper State       Running Version Startup Version Profile Name
Cluster State   Cluster Role
---------- ---------- ----------- ---------------- --------------- --------------- ------------
--------------- ------------
ftd        1          Enabled     Online           6.2.2.81        6.2.2.81
In Cluster      Slave
ftd        2          Enabled     Online           6.2.2.81        6.2.2.81
In Cluster      Slave
ftd        3          Disabled    Not Available                    6.2.2.81
Not Applicable  None
FP9300-A /ssa #
```

ステップ 10 シャーシ #2 のセキュリティモジュールの 1 つを制御用として設定します。

シャーシ #2 のセキュリティモジュールの 1 つを制御用として設定すると、シャーシ #1 には制御ユニットが含まれなくなり、すぐにアップグレードすることができます。

ステップ 11 クラスタ内の他のすべてのシャーシに対して手順 1 ～ 9 を繰り返します。

ステップ 12 制御ロールをシャーシ #1 に戻すには、シャーシ #1 のセキュリティモジュールの 1 つを制御用として設定します。

FMC を使用した Firepower Threat Defense のアップグレード（バージョン 7.0.0）

FMC には、FTD をアップグレードするためのウィザードが用意されています。アップグレードパッケージの場所をアップロードまたは指定するには、引き続き [システムの更新（System Updates）] ページ（**[システム（System）] > [更新（Updates）]**）を使用する必要があります。また、[システムの更新（System Updates）] ページを使用して、FMC 自体、および古い従来型デバイスをアップグレードする必要があります。

ウィザードでは、アップグレードするデバイスの選択、アップグレードパッケージのデバイスへのコピー、互換性と準備状況の確認など、アップグレード前の重要な段階を順を追って説明します。続行すると、選択したデバイスに関する基本情報と、現在のアップグレード関連のステータスが表示されます。表示内容には、アップグレードできない理由が含まれます。あるデバイスがウィザードの1つの段階に「合格」しない場合、そのデバイスは次の段階には表示されません。

ウィザードから移動しても、進行状況は保持されますが、管理者アクセス権を持つ他のユーザーはワークフローをリセット、変更、または続行できます（CAC でログインした場合を除きます。この場合、進行状況はログアウトしてから 24 時間後にクリアされます）。進行状況は、高可用性 FMC 間でも同期されます。

（注） バージョン 7.0.x では、[デバイスのアップグレード（Device Upgrade）] ページにクラスタまたは高可用性ペアのデバイスが正しく表示されません。これらのデバイスは1つのユニットとして選択してアップグレードする必要がありますが、ワークフローにはスタンドアロンデバイスとして表示されます。デバイスのステータスとアップグレードの準備状況は、個別に評価および報告されます。つまり、1 つのユニットが「合格」して次の段階に進んでいるように見えても、他のユニットは合格していない可能性があります。ただし、それらのデバイスはグループ化されたままです。1 つのユニットで準備状況チェックを実行すると、すべてのユニットで実行されます。1つユニットでアップグレードを開始すると、すべてのユニットで開始されます。

時間がかかるアップグレードの失敗を回避するには、[Next] をクリックする前に、すべてのグループメンバーがワークフローの次のステップに進む準備ができていることを手動で確認します。

注意 アップグレード中は、設定を変更または展開しないでください。システムが非アクティブに見えても、手動で再起動またはシャットダウンしないでください。ほとんどの場合、進行中のアップグレードを再開しないでください。ただし、バージョン 6.7.0 からのメジャーアップグレードおよびメンテナンスアップグレードでは、失敗したアップグレードまたは進行中のアップグレードを手動でキャンセルし、失敗したアップグレードを再試行できます。 [デバイス管理（Device Management）] ページおよびメッセージセンターからアクセスできる [アップグレードステータス（Upgrade Status）] ポップアップを使用するか、FTD CLI を使用します。

デフォルトでは、FTDはアップグレードが失敗すると自動的にアップグレード前の状態に戻ります（「自動キャンセル」）。失敗したアップグレードを手動でキャンセルまたは再試行できるようにするには、アップグレードを開始するときに自動キャンセルオプションを無効にします。パッチの自動キャンセルはサポートされていません。高可用性またはクラスタ展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1 つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。すべてのオプションを使い切った場合、または展開でキャンセルや再試行がサポートされていない場合は、Cisco TAC にお問い合わせください。

始める前に

事前アップグレードのチェックリストを完了します。展開したアプライアンスが正常で、きちんと通信していることを確認します。

手順

アップグレードするデバイスを選択します。

ステップ 1 [デバイス（Devices）] > [デバイス管理（Device Management）] を選択します。

ステップ 2 アップグレードするデバイスを選択します。

複数のデバイスを同時にアップグレードできます。デバイスクラスタとハイアベイラビリティペアのメンバーは、同時にアップグレードする必要があります。

重要
パフォーマンスの問題により、デバイスをアップグレードする場合は（バージョン 6.4.0.x から 6.6.x ではなく）、同時にアップグレードするデバイスは 5 つまでにすることを 強くお勧めします。

ステップ 3 [アクションの選択（Select Action）] または [一括アクションの選択（Select Bulk Action）] メニューから、[Firepower ソフトウェアをアップグレードする（Upgrade Firepower Software）] を選択します。

[デバイスのアップグレード（Device Upgrade）] ページが表示され、選択したデバイスの数が示され、対象のバージョンを選択するように求められます。 このページには、左側の [デバイスの選択（Device Selection）] と右側の [デバイスの詳細（Device Details）] の 2 つのペインがあります。[デバイスの選択（Device Selection）] でデバイスリンク（「4 つのデバイス」 など）をクリックして、デバイス詳細を表示します。

進行中のアップグレードワークフローがすでにある場合は、最初にデバイスをマージする（新しく選択したデバイスを以前に選択したデバイスに追加して続行する）か、リセットする（以前の選択を破棄し、新しく選択したデバイスのみを使用する）必要があることに注意してください。

ステップ 4 デバイスの選択内容を確認します。

追加のデバイスを選択するには、[デバイス管理（Device Management）] ページに戻ります。進行状況は失われません。デバイスを削除するには、[リセット（Reset）] をクリックしてデバイスの選択をクリアし、最初からやり直します。

アップグレードパッケージをデバイスにコピーします。

ステップ 5 [Upgrade to] メニューから、対象のバージョンを選択します。

システムは、選択したデバイスのどれをそのバージョンにアップグレードできるかを決定します。対象外のデバイスがある場合は、デバイスのリンクをクリックして理由を確認できます。削除したくなければ、不要なデバイスは削除する必要はありません。それらは次のステップには含まれません。

[Upgrade to] メニューの選択肢は、システムで利用可能なデバイスのアップグレードパッケージに対応していることに注意してください。対象のバージョンがリストにない場合は、[System] > [Updates] に移動し、正しいアップグレードパッケージの場所をアップロードまたは指定します。

ステップ 6 アップグレードパッケージがまだ必要なすべてのデバイスについて、[Copy Upgrade Packages] をクリックして、選択を確認します。

FTD をアップグレードするには、ソフトウェアアップグレードパッケージがアプライアンスにある必要があります。アップグレードの前にアップグレードパッケージをコピーすると、アップグレードのメンテナンス時間が短縮されます。

互換性、準備状況、およびその他の最終チェックを実行します。

ステップ 7 準備状況チェックに合格する必要があるすべてのデバイスについて、[Run Readiness Check] をクリックして、選択を確認します。

[Require passing compatibility and readiness checks option] オプションを無効にすることでチェックをスキップできますが、お勧めしません。すべてのチェックに合格すると、アップグレードが失敗する可能性が大幅に減少します。準備状況チェックの実行中は、デバイスに変更を展開したり、手動で再起動またはシャットダウンしたりしないでください。デバイスが準備状況チェックに失敗した場合は、問題を修正して、準備状況チェックを再度実行してください。準備状況チェックの結果、解決できない問題が見つかった場合は、アップグレードを開始しないでください。代わりに、Cisco TAC にお問い合わせください。

互換性チェックは自動的に行われることに注意してください。たとえば、Firepower 4100/9300 で FXOS をアップグレードする必要がある場合、または管理対象デバイスに展開する必要がある場合、システムはすぐに警告します。

ステップ 8 アップグレード前の最終的なチェックを実行します。

アップグレード前のチェックリストを再確認します。関連するすべてのタスク、特に最終チェックを完了していることを確認してください。

ステップ 9 必要に応じて、[Device Upgrade] ページに戻ります。

進行状況は保持されています。保持されていない場合は、管理者アクセス権を持つ他の誰かがワークフローをリセット、変更、または完了した可能性があります。

ステップ 10 [Next] をクリックします。

アップグレードします。

ステップ 11 デバイスの選択と対象のバージョンを確認します。

ステップ 12 ロールバックオプションを選択します。

メジャーおよびメンテナンスアップグレードの場合、**アップグレードに失敗すると自動的にキャンセルされ、1つ前のバージョンにロールバックされます**。オプションを有効にすると、アップグレードが失敗した場合、デバイスは自動的にアップグレード前の状態に戻ります。失敗したアップグレードを手動でキャンセルまたは再試行できるようにする場合は、このオプションを無効にします。高可用性またはクラスタ展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。

このオプションは、パッチではサポートされていません。

ステップ 13 [Start Upgrade] をクリックし、アップグレードして、デバイスを再起動することを確認します。

メッセージセンターでアップグレードの進行状況をモニタします。アップグレード中のトラフィック処理については、リリースノートの「ソフトウェアのアップグレード」の章を参照してください。

アップグレード中にデバイスが 2 回再起動する場合があります。これは想定されている動作です。

成功を確認し、アップグレード後のタスクを完了します。

ステップ 14 アップグレードが成功したことを確認します。

アップグレードが完了したら、**[Devices]** > **[Device Management]** を選択し、アップグレードしたデバイスのソフトウェアバージョンが正しいことを確認します。

ステップ 15 （オプション）高可用性および拡張性の展開では、デバイスのロールを調べます。

アップグレードプロセスは、常にスタンバイデバイスまたはデータユニットをアップグレードするようにデバイスのロールを切り替えます。デバイスをアップグレード前のロールに戻すことはありません。特定のデバイスに優先するロールがある場合は、それらの変更を今すぐ行ってください。

ステップ 16 侵入ルール（SRU/LSP）および脆弱性データベース（VDB）を更新します。

シスコ サポートおよびダウンロードサイトで利用可能なコンポーネント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。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 17 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 18 アップグレードしたデバイスに構成を再度展開します。

次のタスク

（オプション）[Device Upgrade] ページに戻り、[Finish] をクリックして、ウィザードをクリアします。これを行うまで、[Device Upgrade] ページには、実行したばかりのアップグレードに関する詳細が引き続き表示されます。

FMC を使用した Firepower Threat Defense のアップグレード（バージョン 6.0.1 ～ 6.7.0）

この手順を使用して、FMC の [システムアップデート（System Updates）] ページから FTD をアップグレードします。このページで、複数のデバイスで同じアップグレードパッケージを使用する場合にのみ、複数のデバイスを同時にアップグレードできます。デバイス クラスタとハイ アベイラビリティ ペアのメンバーは、同時にアップグレードする必要があります。

始める前に

- この手順を使用するかどうかを決定します。バージョン 7.0.x への FTD アップグレードについては、代わりにアップグレードウィザードを使用することをお勧めします。FMC を使用した Firepower Threat Defense のアップグレード（バージョン 7.0.0） （28 ページ）を参照してください。

- 事前アップグレードのチェックリストを完了します。展開したアプライアンスが正常で、きちんと通信していることを確認します。
- （任意）高可用性デバイスのペアのアクティブ/スタンバイの役割を切り替えます。**[Devices]** > **[Device Management]** を選択し、ペアの横にある [Switch Active Peer] アイコンをクリックして、選択内容を確認します。

  ハイ アベイラビリティ ペアのスタンバイ デバイスが最初にアップグレードされます。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレードプロセスによって元の役割に切り替わります。

手順

ステップ 1 **[システム（System）]** > **[更新（Updates）]** を選択します。

ステップ 2 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、アップグレードするデバイスを選択します。

アップグレードするデバイスがリストに表示されない場合は、間違ったアップグレード パッケージを選択しています。

（注）
[システムの更新（System Update）] ページから同時にアップグレードするデバイスは 5 台までにすることを強く推奨します。選択したすべてのデバイスがそのプロセスを完了するまで、アップグレードを停止することはできません。いずれかのデバイスのアップグレードに問題がある場合、問題を解決する前に、すべてのデバイスのアップグレードを完了する必要があります。

ステップ 3 （バージョン 6.7.0 以降）ロールバック オプション を選択します。

メジャーおよびメンテナンスアップグレードの場合、**アップグレードに失敗すると自動的にキャンセルされ、1つ前のバージョンにロールバックされます**。オプションを有効にすると、アップグレードが失敗した場合、デバイスは自動的にアップグレード前の状態に戻ります。失敗したアップグレードを手動でキャンセルまたは再試行できるようにする場合は、このオプションを無効にします。高可用性またはクラスタ展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1 つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。 パッチの自動キャンセルはサポートされていません。

ステップ 4 [Install] をクリックし、アップグレードして、デバイスを再起動することを確認します。

一部のデバイスは、アップグレード時に 2 回再起動することがありますが、これは想定内の動作です。トラフィックは、デバイスの設定および展開方法に応じて、アップグレードの間ドロップするか、検査なしでネットワークを通過します。 詳細については、対象バージョンの Cisco Firepower リリース ノート 内の「ソフトウェアのアップグレード」の章を参照してください。

ステップ 5 アップグレードの進捗状況 をモニタします。

注意

アップグレード中のデバイスへの変更の展開、手動での再起動、シャットダウンは行わないでください。

ほとんどの場合、進行中のアップグレードを再開しないでください。ただし、バージョン 6.7.0 からのメジャーおよびメンテナンス FTD アップグレードを行った後は、失敗または進行中のアップグレードを手動でキャンセルし、失敗したアップグレードを再試行できます。[Device Management] ページおよびメッセージセンターからアクセスできる [Upgrade Status] ポップアップを使用するか、FTD CLI を使用してください。デフォルトでは、FTD はアップグレードが失敗すると自動的にアップグレード前の状態に戻ります（「自動キャンセル」）。失敗したアップグレードを手動でキャンセルまたは再試行できるようにするには、アップグレードを開始するときに自動キャンセルオプションを無効にします。パッチの自動キャンセルはサポートされていません。高可用性またはクラスタ展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1 つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。すべてのオプションを使い切った場合、または展開でキャンセルや再試行がサポートされていない場合は、Cisco TAC にお問い合わせください。

ステップ 6 アップグレードが成功したことを確認します。

アップグレードが完了したら、**[Devices]** > **[Device Management]** を選択し、アップグレードしたデバイスのソフトウェアバージョンが正しいことを確認します。

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

シスコ サポートおよびダウンロード サイト で利用可能なコンポーネント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。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 アップグレードしたデバイスに構成を再度展開します。

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。