



Firepower 4100/9300 の FXOS アップグレード

Firepower 4100/9300 の場合、Threat Defense のメジャーアップグレードには FXOS のアップグレードも必要です。Threat Defense のメジャーバージョンには特別に認定および推奨されている付随の FXOS バージョンがあります。シスコではこれらの組み合わせの拡張テストを実施するため、可能な限りこれらの組み合わせを使用してください。メンテナンスリリースとパッチで FXOS のアップグレードが必要になることはほとんどありませんが、最新の FXOS ビルドにアップグレードして、解決済みの問題を有効に活用することもできます。

- [FXOS のアップグレードパッケージ \(1 ページ\)](#)
- [FXOS のアップグレードガイドライン \(1 ページ\)](#)
- [FXOS のアップグレードパス \(4 ページ\)](#)
- [Chassis Manager を使用した FXOS のアップグレード \(9 ページ\)](#)
- [CLI を使用した FXOS のアップグレード \(18 ページ\)](#)

FXOS のアップグレードパッケージ

FXOS イメージはシスコ サポートおよびダウンロードサイトで入手できます。

- Firepower 4100 シリーズ : <http://www.cisco.com/go/firepower4100-software>
- Firepower 9300 : <http://www.cisco.com/go/firepower9300-software>

正しい FXOS イメージを見つけるには、デバイス モデルを選択または検索し、対象バージョンとビルドの *Firepower Extensible Operating System* のダウンロードページを参照します。FXOS イメージ (fxos-k9.version.SPA) は、リカバリおよび MIB パッケージとともにリストされます。

FXOS のアップグレードガイドライン

重要なリリース固有のアップグレードガイドライン、新機能および廃止された機能、未解決のバグおよび解決済みのバグについては、[Cisco Firepower 4100/9300 FXOS リリースノート](#) を参照してください。

Threat Defense をアップグレードするために必要な FXOS の最小バージョン

バージョン 7.2 を実行するために必要な FXOS の最小バージョンは、FXOS 2.12.0.31 です。

FXOS をアップグレードするために必要な FXOS の最小バージョン

FXOS 2.2.2 から、それ以降の任意の FXOS バージョンにアップグレードできます。

FXOS アップグレードの所要時間

FXOS のアップグレードには最長 45 分かかることがあり、トラフィックフローやインスペクションに影響を与える場合があります。詳細については、[FXOS のアップグレードでのトラフィックフローとインスペクション \(3 ページ\)](#) を参照してください。

Threat Defense 高可用性/スケーラビリティを備えた FXOS のアップグレード順序

高可用性や拡張性を導入する場合でも、各シャーシの FXOS を個別にアップグレードします。中断を最小限に抑えるには、1 つずつシャーシの FXOS をアップグレードします。Threat Defense のアップグレードの場合、グループ化されたデバイスが 1 つずつ自動的にアップグレードされます。

表 1: Threat Defense 高可用性/スケーラビリティを備えた FXOS のアップグレード順序

展開	アップグレード順序
スタンドアロンデバイス	<ol style="list-style-type: none"> 1. FXOS をアップグレードします。 2. Threat Defense をアップグレードします。
ハイ アベイラビリティ	<p>FTD をアップグレードする前に、両方のシャーシで Threat Defense 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。</p> <ol style="list-style-type: none"> 1. スタンバイデバイスを備えたシャーシの FXOS をアップグレードします。 2. ロールを切り替えます。 3. 新しいスタンバイデバイスを備えたシャーシの FXOS をアップグレードします。 4. Threat Defense をアップグレードします。
シャーシ内クラスタ (同じシャーシ上のユニット)	<ol style="list-style-type: none"> 1. FXOS をアップグレードします。 2. Threat Defense をアップグレードします。

展開	アップグレード順序
シャーシ内クラスタ（異なるシャーシ上のユニット）	<p>Threat Defense をアップグレードする前に、すべてのシャーシの FXOS 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を常にアップグレードします。</p> <ol style="list-style-type: none"> 1. すべての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. 残りのシャーシの FXOS をアップグレードします。 4. Threat Defense をアップグレードします。

FTD および ASA 論理デバイスを搭載した FXOS のアップグレード

Firepower 9300 に Threat Defense および ASA 論理デバイスが設定されている場合は、この章の手順を使用して FXOS と Threat Defense をアップグレードします。FXOS をアップグレードしても、どちらのタイプの論理デバイスとの互換性も失われないことを確認する必要があります（[Threat Defense および ASA を使用した FXOS のアップグレードパス（7ページ）](#) を参照）。

ASA のアップグレード手順については、[Cisco Secure Firewall ASA アップグレードガイド](#) を参照してください。

論理デバイスを搭載していない FXOS のアップグレード

論理デバイスが設定されていない場合は、この章の手順を使用して、スタンドアロン型の Threat Defense デバイスの FXOS をアップグレードします。論理デバイスに関する指示は無視してください。または、必要な FXOS バージョンへのシャーシの完全な再イメージ化を実行します。

FXOS のアップグレードでのトラフィックフローとインスペクション

FXOS をアップグレードするとシャーシが再起動します。高可用性や拡張性を導入する場合でも、各シャーシの FXOS を個別にアップグレードします。中断を最小限に抑えるには、1 つずつシャーシをアップグレードします。

表 2: トラフィックフローとインスペクション: FXOS のアップグレード

導入	トラフィックの挙動	メソッド
スタンドアロン	廃棄	—

導入	トラフィックの挙動	メソッド
高可用性	影響なし。	ベストプラクティス ：スタンバイで FXOS を更新し、アクティブピアを切り替えて新しいスタンバイをアップグレードします。
	1 つのピアがオンラインになるまでドロップされる。	スタンバイでアップグレードが終了する前に、アクティブピアで FXOS をアップグレードします。
シャーシ間クラスタ	影響なし。	ベストプラクティス ：少なくとも 1 つのモジュールを常にオンラインにするため、一度に 1 つのシャーシをアップグレードします。
	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。	ある時点ですべてのモジュールを停止するため、シャーシを同時にアップグレードします。
シャーシ内クラスタ (FirePOWER 9300 のみ)	検査なしで受け渡される。	ハードウェアバイパス有効：[Bypass: Standby] または [Bypass-Force]。
	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。	ハードウェアバイパス無効：[Bypass: Disabled]。
	少なくとも 1 つのモジュールがオンラインになるまでドロップされる。	ハードウェアバイパスモジュールなし。

FXOS のアップグレードパス

展開に一致するアップグレードパスを選択します。

Threat Defense を使用する FXOS のアップグレードパス

次の表に、Firepower 4100/9300 の Threat Defense のアップグレードパスを示します。

現在の Threat Defense /Management Center のバージョンが対象のバージョンより後の日付にリリースされた場合、期待どおりにアップグレードできない可能性があります。このような場合、アップグレードはすぐに失敗し、2 つのバージョン間にデータストアの非互換性があることを説明するエラーが表示されます。現在のバージョンと対象のバージョンの両方に関するリリースノートには、特定の制限が掲載されています。

この表には、シスコにより特別に認定されたバージョンの組み合わせのみが掲載されています。最初に FXOS をアップグレードするため、サポートされている（ただし推奨されていない）組み合わせを短時間実行します。ここでは、FXOS が論理デバイスの「前」になります。

最小限のビルドおよびその他の詳細な互換性情報については、[Cisco Secure Firewall Threat Defense 互換性ガイド](#) を参照してください。

表 3: Firepower 4100/9300 での Threat Defense の直接アップグレード

現在のバージョン	対象のバージョン
Threat Defense 7.2 を搭載した FXOS 2.12	→ Threat Defense 7.2.x 以降のメンテナンスリリースを搭載した FXOS 2.12
Threat Defense 7.1 を搭載した FXOS 2.11.1	次のいずれかです。 → Threat Defense 7.2 を搭載した FXOS 2.12 → Threat Defense 7.1.x 以降のメンテナンスリリースを搭載した FXOS 2.11.1
Threat Defense 7.0 を搭載した FXOS 2.10.1	次のいずれかです。 → Threat Defense 7.2 を搭載した FXOS 2.12 → Threat Defense 7.1 を搭載した FXOS 2.11.1 → Threat Defense 7.0.x 以降のメンテナンスリリースを搭載した FXOS 2.10.1 (注) データストアの非互換性のため、をバージョン 7.0.4 以降からバージョン 7.1.0 にアップグレードすることができません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。 (注) クラウド提供型の管理センターは、バージョン 7.1 を実行している脅威防御デバイス、または任意のバージョンを実行しているデバイスを管理できません。クラウド管理を登録解除して無効にしない限り、クラウド提供型の管理センターに登録されている脅威防御デバイスをバージョン 7.0.x からバージョン 7.1 にアップグレードすることはできません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。

現在のバージョン	対象のバージョン
Threat Defense 6.7 を搭載した FXOS 2.9.1	次のいずれかです。 → Threat Defense 7.2 を搭載した FXOS 2.12 → Threat Defense 7.1 を搭載した FXOS 2.11.1 → Threat Defense 7.0 を搭載した FXOS 2.10.1 → Threat Defense 6.7.x 以降のメンテナンスリリースを搭載した FXOS 2.9.1
Threat Defense 6.6 を搭載した FXOS 2.8.1	次のいずれかです。 → Threat Defense 7.2 を搭載した FXOS 2.12 → Threat Defense 7.1 を搭載した FXOS 2.11.1 → Threat Defense 7.0 を搭載した FXOS 2.10.1 → Threat Defense 6.7 を搭載した FXOS 2.9.1 → Threat Defense 6.6.x 以降のメンテナンスリリースを搭載した FXOS 2.8.1
Threat Defense 6.5 を搭載した FXOS 2.7.1	次のいずれかです。 → Threat Defense 7.1 を搭載した FXOS 2.11.1 → Threat Defense 7.0 を搭載した FXOS 2.10.1 → Threat Defense 6.7 を搭載した FXOS 2.9.1 → Threat Defense 6.6 を搭載した FXOS 2.8.1
Threat Defense 6.4 を搭載した FXOS 2.6.1	次のいずれかです。 → Threat Defense 7.0 を搭載した FXOS 2.10.1 → Threat Defense 6.7 を搭載した FXOS 2.9.1 → Threat Defense 6.6 を搭載した FXOS 2.8.1 → Threat Defense 6.5 を搭載した FXOS 2.7.1
Threat Defense 6.3 を搭載した FXOS 2.4.1	次のいずれかです。 → Threat Defense 6.7 を搭載した FXOS 2.9.1 → Threat Defense 6.6 を搭載した FXOS 2.8.1 → Threat Defense 6.5 を搭載した FXOS 2.7.1 → Threat Defense 6.4 を搭載した FXOS 2.6.1

現在のバージョン	対象のバージョン
Threat Defense 6.2.3 を搭載した FXOS 2.3.1	次のいずれかです。 → Threat Defense 6.6 を搭載した FXOS 2.8.1 → Threat Defense 6.5 を搭載した FXOS 2.7.1 → Threat Defense 6.4 を搭載した FXOS 2.6.1 → Threat Defense 6.3 を搭載した FXOS 2.4.1

Threat Defense および ASA を使用した FXOS のアップグレードパス

この表では、別のモジュールで実行されている Threat Defense および ASA 論理デバイスを搭載した Firepower 9300 シャーシのアップグレードパスを示します。



- (注) このドキュメントには、ASA 論理デバイスのアップグレード手順は記載されていません。アップグレード手順については、[Cisco Secure Firewall ASA アップグレードガイド](#)を参照してください。

現在の Threat Defense /Management Center のバージョンが対象のバージョンより後の日付にリリースされた場合、期待どおりにアップグレードできない可能性があります。このような場合、アップグレードはすぐに失敗し、2つのバージョン間にデータストアの非互換性があることを説明するエラーが表示されます。現在のバージョンと対象のバージョンの両方に関するリリースノートには、特定の制限が掲載されています。

この表には、シスコにより特別に認定されたバージョンの組み合わせのみが掲載されています。最初に FXOS をアップグレードするため、サポートされている（ただし推奨されていない）組み合わせを短時間実行します。ここでは、FXOS が論理デバイスの「前」になります。最小限のビルドおよびその他の詳細な互換性情報については、[Cisco Secure Firewall Threat Defense 互換性ガイド](#)を参照してください。

このタイプの展開では、FXOS をアップグレードしても、どちらのタイプの論理デバイスとの互換性も失われないことを確認する必要があります。複数のバージョンをスキップする必要がある場合、通常は Threat Defense がリミッタになります。FXOS と ASA は通常、1 ホップでさらにアップグレードできます。ターゲットの FXOS バージョンに達したら、どのタイプの論理デバイスからでもアップグレードを開始できます。

表 4: Firepower 9300 での Threat Defense および ASA の直接アップグレード

現在のバージョン	対象のバージョン
次を搭載した FXOS 2.11.1 • Threat Defense 7.1 • ASA 9.17(x)	→ ASA 9.18(x) および Threat Defense 7.2 を搭載した FXOS 2.12

現在のバージョン	対象のバージョン
次を搭載した FXOS 2.10.1 <ul style="list-style-type: none"> • Threat Defense 7.0 • ASA 9.16(x) 	次のいずれかです。 <ul style="list-style-type: none"> → ASA 9.18(x) および Threat Defense 7.2 を搭載した FXOS 2.12 → ASA 9.17(x) および Threat Defense 7.1 を搭載した FXOS 2.11.1 (注) データストアの非互換性のため、をバージョン 7.0.4 以降からバージョン 7.1.0 にアップグレードすることができません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。 (注) クラウド提供型の管理センターは、バージョン 7.1 を実行している脅威防御デバイス、または任意のバージョンを実行しているデバイスを管理できません。クラウド管理を登録解除して無効にしない限り、クラウド提供型の管理センターに登録されている脅威防御デバイスをバージョン 7.0.x からバージョン 7.1 にアップグレードすることはできません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。
次を搭載した FXOS 2.9.1 : <ul style="list-style-type: none"> • Threat Defense 6.7 • ASA 9.15(x) 	次のいずれかです。 <ul style="list-style-type: none"> → ASA 9.18(x) および Threat Defense 7.2 を搭載した FXOS 2.12 → ASA 9.17(x) および Threat Defense 7.1 を搭載した FXOS 2.11.1 → ASA 9.16(x) および Threat Defense 7.0 を搭載した FXOS 2.10.1
次を搭載した FXOS 2.8.1 : <ul style="list-style-type: none"> • Threat Defense 6.6 • ASA 9.14(x) 	次のいずれかです。 <ul style="list-style-type: none"> → ASA 9.18(x) および Threat Defense 7.2 を搭載した FXOS 2.12 → ASA 9.17(x) および Threat Defense 7.1 を搭載した FXOS 2.11.1 → ASA 9.16(x) および Threat Defense 7.0 を搭載した FXOS 2.10.1 → ASA 9.15(x) および Threat Defense 6.7 を搭載した FXOS 2.9.1

現在のバージョン	対象のバージョン
次を搭載した FXOS 2.7.1 : <ul style="list-style-type: none"> • Threat Defense 6.5 • ASA 9.13(x) 	次のいずれかです。 <ul style="list-style-type: none"> → ASA 9.17(x) および Threat Defense 7.1 を搭載した FXOS 2.11.1 → ASA 9.16(x) および Threat Defense 7.0 を搭載した FXOS 2.10.1 → ASA 9.15(x) および Threat Defense 6.7 を搭載した FXOS 2.9.1 → ASA 9.14(x) および Threat Defense 6.6 を搭載した FXOS 2.8.1
次を搭載した FXOS 2.6.1 : <ul style="list-style-type: none"> • Threat Defense 6.4 • ASA 9.12(x) 	次のいずれかです。 <ul style="list-style-type: none"> → ASA 9.16(x) および Threat Defense 7.0 を搭載した FXOS 2.10.1 → ASA 9.15(x) および Threat Defense 6.7 を搭載した FXOS 2.9.1 → ASA 9.14(x) および Threat Defense 6.6 を搭載した FXOS 2.8.1 → ASA 9.13(x) および Threat Defense 6.5 を搭載した FXOS 2.7.1

Chassis Manager を使用した FXOS のアップグレード

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。

-
- 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ポ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。
- top** を入力します。
 - scope ssa** を入力します。
 - show slot** を入力します。
 - 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。
 - show app-instance** を入力します。
 - 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。

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。

- 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。
- 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）。
 - top** を入力します。
 - scope ssa** を入力します。
 - show slot** を入力します。
 - 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。
 - show app-instance** を入力します。
 - 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なりません。
- 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。
- [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。
 - [ファイルを選択 (ChooseFile)] 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。
 - [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。
 - 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。

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。

- 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。
- [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。
 - [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。
 - [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。
 - 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。
- scope system** を入力します。
 - show firmware monitor** を入力します。
 - 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。
- top** を入力します。
 - scope ssa** を入力します。
 - show slot** を入力します。
 - 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。
 - show app-instance** を入力します。
 - 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。
- Firepower Management Center に接続します。
 - [**デバイス (Devices)**] > [**デバイス管理 (Device Management)**] を選択します。
 - 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。
 - 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。
- [**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。
 - [**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。
 - [**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。
 - 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。

CLI を使用した FXOS のアップグレード

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。

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 インターコネクタ、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 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。

-
- 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:
```

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

```

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。

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。

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。
- top** を入力します。
 - scope ssa** を入力します。
 - show slot** を入力します。
 - 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。
 - show app-instance** を入力します。
 - 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。
- Firepower Management Center に接続します。
 - [**デバイス (Devices)**] > [**デバイス管理 (Device Management)**] を選択します。
 - 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。
 - 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。
- ファームウェア モードに入ります。
Firepower-chassis-a # **scope firmware**
 - 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。

- top** を入力します。
- scope ssa** を入力します。
- show slot** を入力します。
- 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。
- show app-instance** を入力します。
- 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。

- Firepower Management Center に接続します。
- [**デバイス (Devices)**] > [**デバイス管理 (Device Management)**] を選択します。
- 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。
- 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。

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。