



ASA のアップグレード

このドキュメントの手順に従って ASA をアップグレードします。

- [Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 のアップグレード \(1 ページ\)](#)
- [Firepower 4100/9300 のアップグレード \(43 ページ\)](#)
- [ASA 5500-X、ASA Virtual、ASASM、ISA 3000 のアップグレード \(81 ページ\)](#)

Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 のアップグレード

このドキュメントでは、Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 のスタンドアロン、フェールオーバー、またはクラスタリング展開用に、ASA、FXOS、および ASDM のアップグレードを計画し、実装する方法について説明します。

Firepower 2100 9.12 以前では、プラットフォームモードのみを使用できます。9.13 以降では、アプライアンスモードがデフォルトです。モードを確認するには、ASA CLI で `show fxos mode` コマンドを使用します。

Firepower 1000、2100（アプライアンスモード）、および Cisco Secure Firewall 3100/4200 のアップグレード

このドキュメントでは、Firepower 1000、2100（アプライアンスモード）、および Cisco Secure Firewall 3100/4200 のスタンドアロンまたはフェールオーバー展開用に、ASA、FXOS、および ASDM のアップグレードを計画し、実装する方法について説明します。バージョン 9.13 以前では、Firepower 2100 はプラットフォームモードのみをサポートしていました。9.14 以降では、アプライアンスモードがデフォルトです。9.14 以降では、ASA で `show fxos mode` コマンドを使用して現在のモードを決定します。プラットフォームモードの手順については、[プラットフォームモードでの Firepower 2100 のアップグレード \(22 ページ\)](#) を参照してください。

スタンドアロンユニットのアップグレード

スタンドアロンユニットをアップグレードするには CLI または ASDM を使用します。

CLI を使用したスタンドアロンユニットのアップグレード

この項では、アプライアンスモードの Firepower 1000 または Firepower 2100、Cisco Secure Firewall 3100/4200 に ASDM および ASA イメージをインストールする方法について説明します。

始める前に

この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバー タイプについては、『[ASA Command Reference](#)』の **copy** コマンドを参照してください。

手順

- ステップ 1** グローバル コンフィギュレーション モードで、デフォルト以外の ASDM イメージを以前に設定した場合は、イメージバンドルに付属のイメージにリセットします。

```
asdm image disk0:/asdm.bin
```

write memory

イメージバンドルには ASDM イメージが含まれていて、ASA バンドルをアップグレードすると、同じ名前 (**asdm.bin**) であるため、リロード後にバンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。アップロードした別の ASDM イメージ (たとえば **asdm-7191.bin**) を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のあるバージョンの ASDM が確実に実行されるようにするには、バンドルされている ASDM イメージを使用するように ASA を再設定する必要があります。

- ステップ 2** 特権 EXEC モード (最小限) で、ASA ソフトウェアをフラッシュメモリにコピーします。

```
copy ftp://[[user[:password]@]server[/path]]asa_image_name diskn:[/path]asa_image_name
```

例 :

```
ciscoasa# copy ftp://jcrichon:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA  
disk0:/cisco-asa-fp1k.9.14.1.SPA
```

- ステップ 3** グローバル コンフィギュレーション モードにアクセスします。

configure terminal

例 :

```
ciscoasa# configure terminal  
ciscoasa(config)#
```

- ステップ 4** 設定されている現在のブートイメージが存在している場合、これを表示します。

show running-config boot system

設定に **boot system** コマンドが存在しない場合があることに注意してください。たとえば、ROMMON からイメージをインストールした場合、新しいデバイスがある場合、またはコマンドを手動で削除した場合などです。

例 :

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

ステップ 5 **boot system** コマンドが設定されている場合は、新しいブートイメージを入力できるようにコマンドを削除します。

no boot system diskn:[/path]asa_image_name

boot system コマンドが設定されていない場合は、この手順をスキップします。

例 :

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

ステップ 6 ブートする ASA イメージを設定します (先ほどアップロードしたもの)。

boot system diskn:[/path]asa_image_name

boot system コマンドは 1 つだけ入力できます。 **boot system** コマンドは、入力時にアクションを実行します。システムはイメージを検証して解凍し、ブート場所 (FXOS によって管理される **disk0** の内部ロケーション) にコピーします。ASA をリロードすると、新しいイメージがロードされます。リロードの前に気が変わった場合は、**no boot system** コマンドを入力してブート場所から新しいイメージを削除し、現在のイメージを引き続き実行することができます。

例 :

```
ciscoasa(config)# boot system disk0:/cisco-asa-fp1k.9.14.1.SPA

The system is currently installed with security software package 9.13.1, which has:
  - The platform version: 2.7.1
  - The CSP (asa) version: 9.13.1
Preparing new image for install...
!!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.14.1 will do the following:
  - upgrade to the new platform version 2.8.1
  - upgrade to the CSP ASA version 9.14.1
After the installation is complete, reload to apply the new image.
Finalizing image install process...

Install_status: ready.....
Install_status: validating-images.....
Install_status: update-software-pack-completed
ciscoasa(config)#
```

ステップ 7 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

ステップ 8 ASA をリロードします。

reload

ASDM を使用したローカルコンピュータからのスタンドアロンユニットのアップグレード

Upgrade Software from Local Computer ツールにより、コンピュータからフラッシュファイルシステムにイメージファイルをアップロードし、アプライアンスモードの Firepower 1000 または Firepower 2100、Cisco Secure Firewall 3100/4200 の ASA をアップグレードできます。

手順

- ステップ 1** デフォルト以外の ASDM イメージを以前に設定した場合は、イメージバンドルに付属のイメージにリセットします。
- イメージバンドルには ASDM イメージが含まれていて、ASA バンドルをアップグレードすると、同じ名前 (**asdm.bin**) であるため、リロード後にバンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。アップロードした別の ASDM イメージ (たとえば **asdm-7191.bin**) を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のあるバージョンの ASDM が確実に実行されるようにするには、バンドルされている ASDM イメージを使用するように ASA を再設定する必要があります。
- メイン ASDM アプリケーションウィンドウで、**[設定 (Configuration)] > [デバイス管理 (Device Management)] > [システムイメージ/設定 (System Image/Configuration)] > [ブートイメージ/設定 (Boot Image/Configuration)]** を選択します。
 - [ASDM イメージファイルパス (ASDM Image File Path)]** に、**disk0:/asdm.bin** と入力します。
 - [適用 (Apply)]** をクリックします。
- ステップ 2** メイン ASDM アプリケーション ウィンドウで、**[Tools] > [Upgrade Software from Local Computer]** の順に選択します。
- ステップ 3** **[アップロードするイメージ (Image to Upload)]** ドロップダウンリストから、**[ASA]** を選択します。
- ステップ 4** **[Local File Path]** フィールドで **[Browse Local Files]** をクリックして PC 上のファイルを見つけます。
- ステップ 5** **[Flash File System Path]** フィールドで **[Browse Flash]** をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを見つけます。
- ステップ 6** **[イメージのアップロード (Upload Image)]** をクリックします。
- アップグレードプロセスには数分かかる場合があります。
- ステップ 7** このイメージを ASA イメージとして設定するように求められます。**[Yes]** をクリックします。
- ステップ 8** 新しいイメージを使用するために、ASA をリロードするよう求められます。**[OK]** をクリックします。
- アップグレードツールを終了します。
- ステップ 9** **[Tools] > [System Reload]** を選択して、ASA をリロードします。
- リロードの詳細の確認を求める新しいウィンドウが表示されます。

- a) [Save the running configuration at the time of reload] オプションボタン (デフォルト) をクリックします。
- b) リロードする時刻を選択します (たとえば、デフォルトの [Now]) 。
- c) [Schedule Reload] をクリックします。

リロードが開始されると、[Reload Status] ウィンドウにリロードの進行状況が表示されます。ASDM を終了するオプションも表示されます。

ステップ 10 ASA のリロード後、ASDM を再起動します。

コンソール ポートでリロードの状況を確認できます。または、数分待った後に ASDM を使用して、接続可能になるまで再試行することもできます。

ASDM Cisco.com ウィザードを使用したスタンドアロンユニットのアップグレード

アップライアンスモードの Firepower 1000 または 2100、Cisco Secure Firewall 3100 の場合、**Upgrade Software from Cisco.com Wizard** により、ASDM および ASA を最新のバージョンに自動的にアップグレードできます。

このウィザードでは、次の操作を実行できます。

- アップグレード用の ASA イメージファイルまたは ASDM イメージファイルを選択する。



(注) ASDM は最新のイメージバージョンをダウンロードし、そこにはビルド番号が含まれています。たとえば、9.9(1) をダウンロードする場合に、ダウンロードが 9.9(1.2) となる可能性があります。この動作は想定されているため、計画したアップグレードを続行できます。

- 実行したアップグレードの変更点を確認する。
- イメージをダウンロードし、インストールする。
- インストールのステータスを確認する。
- インストールが正常に完了した場合は、ASA をリロードして、コンフィギュレーションを保存し、アップグレードを完了する。

始める前に

内部的な変更により、このウィザードでは ASDM 7.10(1) 以降の使用のみがサポートされています。また、イメージの命名が変更されたため、ASA 9.10(1) 以降にアップグレードするには、ASDM 7.12(1) 以降を使用する必要があります。ASDM は ASA の以前のリリースと下位互換性があるため、実行している ASA バージョンを問わず、ASDM をアップグレードすることができます。

手順

- ステップ 1** [Tools] > [Check for ASA/ASDM Updates] を選択します。
- マルチコンテキストモードでは、システムからこのメニューにアクセスします。
- [Cisco.com Authentication] ダイアログボックスが表示されます。
- ステップ 2** Cisco.com のユーザー ID とパスワードを入力して、[Login] をクリックします。
- [Cisco.com Upgrade Wizard] が表示されます。
- (注) 利用可能なアップグレードがない場合は、ダイアログボックスが表示されます。ウィザードを終了するには、[OK] をクリックします。
- ステップ 3** [Next] をクリックして [Select Software] 画面を表示します。
- 現在の ASA バージョンおよび ASDM バージョンが表示されます。
- ステップ 4** ASA バージョンおよび ASDM バージョンをアップグレードするには、次の手順を実行します。
- [ASA] 領域で、[Upgrade to] チェックボックスをオンにしてから、アップグレードする ASA バージョンをドロップダウンリストから選択します。
 - [ASDM] 領域で、[Upgrade to] チェックボックスをオンにしてから、アップグレードする ASDM バージョンをドロップダウンリストから選択します。
- ステップ 5** [Next] をクリックして [Review Changes] 画面を表示します。
- ステップ 6** 次の項目を確認します。
- ダウンロードした ASA イメージ ファイルや ASDM イメージ ファイルが正しいファイルであること。
 - アップロードする ASA イメージ ファイルや ASDM イメージ ファイルが正しいファイルであること。
 - 正しい ASA ブート イメージが選択されていること。
- ステップ 7** [Next] をクリックして、アップグレード インストールを開始します。
- アップグレード インストールの進行状況を示すステータスを表示できます。
- [Results] 画面が表示され、アップグレード インストール ステータス（成功または失敗）など、追加の詳細が示されます。
- ステップ 8** アップグレード インストールが成功した場合に、アップグレード バージョンを有効にするには、[Save configuration and reload device now] チェックボックスをオンにして、ASA を再起動し、ASDM を再起動します。
- ステップ 9** [Finish] をクリックして、ウィザードを終了し、コンフィギュレーションに対して行った変更を保存します。
- (注) 次に高いバージョン（存在する場合）にアップグレードするには、ウィザードを再起動する必要があります。

ステップ 10 ASA のリロード後、ASDM を再起動します。

コンソール ポートでリロードの状況を確認できます。または、数分待った後に ASDM を使用して、接続可能になるまで再試行することもできます。

アクティブ/スタンバイ フェールオーバー ペアのアップグレード

アクティブ/スタンバイ フェールオーバー ペアをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、CLI または ASDM を使用します。

CLI を使用したアクティブ/スタンバイ フェールオーバー ペアのアップグレード

アプライアンスモードの Firepower 1000 または 2100、Cisco Secure Firewall 3100/4200 のアクティブ/スタンバイ フェールオーバー ペアをアップグレードするには、次の手順を実行します。

始める前に

- アクティブ装置で次の手順を実行します。SSH アクセスの場合、アクティブな IP アドレスに接続します。アクティブ装置は常にこの IP アドレスを保有しています。CLI に接続する場合は、ASA プロンプトを調べてフェールオーバー ステータスを確認します。フェールオーバー ステータスと優先順位（プライマリまたはセカンダリ）を表示するように ASA プロンプトを設定できます。これは、接続しているユニットを特定するのに役立ちます。[prompt](#) コマンドを参照してください。代わりに、**show failover** コマンドを入力して、このユニットのステータスと優先順位（プライマリまたはセカンダリ）を表示します。
- この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバータイプについては、『[ASA Command Reference](#)』の **copy** コマンドを参照してください。

手順

ステップ 1 グローバルコンフィギュレーションモードのプライマリユニットで、デフォルト以外の ASDM イメージを以前に設定した場合は、イメージバンドルに付属のイメージにリセットします。

```
asdm image disk0:/asdm.bin
```

```
write memory
```

イメージバンドルには ASDM イメージが含まれていて、ASA バンドルをアップグレードすると、同じ名前 (**asdm.bin**) であるため、リロード後にバンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。アップロードした別の ASDM イメージ（たとえば **asdm-7191.bin**）を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のあるバージョンの ASDM が確実に実行されるようにするには、バンドルされている ASDM イメージを使用するように ASA を再設定する必要があります。

ステップ 2 特権 EXEC モード（最小限）時にアクティブユニットで、ASA ソフトウェアをアクティブユニットのフラッシュメモリにコピーします。

```
copy ftp://[[user[:password]]@]server[/path]/asa_image_name diskn:[/path]/asa_image_name
```

例 :

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fplk.9.14.1.SPA
disk0:/cisco-asa-fplk.9.14.1.SPA
```

- ステップ 3** ソフトウェアをスタンバイ装置にコピーします。アクティブ装置で指定したのと同じパスを指定してください。

```
failover exec mate copy /noconfirm ftp://[[user[:password]]@]server[/path]/asa_image_name
diskn:[/path]/asa_image_name
```

例 :

```
asa/act# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fplk.9.14.1.SPA disk0:/cisco-asa-fplk.9.14.1.SPA
```

- ステップ 4** まだグローバルコンフィギュレーションモードを開始していない場合は、グローバルコンフィギュレーションモードを開始します。

```
configure terminal
```

- ステップ 5** 設定されている現在のブートイメージが存在している場合、これを表示します。

```
show running-config boot system
```

設定に **boot system** コマンドが存在しない場合があることに注意してください。たとえば、ROMMON からイメージをインストールした場合、新しいデバイスがある場合、またはコマンドを手動で削除した場合などです。

例 :

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fplk.9.13.1.SPA
```

- ステップ 6** **boot system** コマンドが設定されている場合は、新しいブートイメージを入力できるようにコマンドを削除します。

```
no boot system diskn:[/path]/asa_image_name
```

boot system コマンドが設定されていない場合は、この手順をスキップします。

例 :

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fplk.9.13.1.SPA
```

- ステップ 7** ブートする ASA イメージを設定します (先ほどアップロードしたもの)。

```
boot system diskn:[/path]/asa_image_name
```

boot system コマンドは 1 つだけ入力できます。**boot system** コマンドは、入力時にアクションを実行します。システムはイメージを検証して解凍し、ブート場所 (FXOS によって管理され

る disk0 の内部ロケーション) にコピーします。ASA をリロードすると、新しいイメージがロードされます。リロードの前に気が変わった場合は、**no boot system** コマンドを入力してブート場所から新しいイメージを削除し、現在のイメージを引き続き実行することができます。

例 :

```
ciscoasa(config)# boot system disk0:/cisco-asa-fplk.9.14.1.SPA

The system is currently installed with security software package 9.13.1, which has:
- The platform version: 2.7.1
- The CSP (asa) version: 9.13.1
Preparing new image for install...
!!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.14.1 will do the following:
- upgrade to the new platform version 2.8.1
- upgrade to the CSP ASA version 9.14.1
After the installation is complete, reload to apply the new image.
Finalizing image install process...

Install_status: ready.....
Install_status: validating-images.....
Install_status: update-software-pack-completed
ciscoasa(config)#
```

ステップ 8 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

これらの設定変更は、スタンバイ ユニットに自動的に保存されます。

ステップ 9 スタンバイ装置をリロードして新しいイメージを起動します。

failover reload-standby

スタンバイ装置のロードが完了するまで待ちます。**show failover** コマンドを使用して、スタンバイ ユニットが Standby Ready 状態かどうかを検証します。

ステップ 10 強制的にアクティブ装置からスタンバイ装置へのフェールオーバーを行います。

no failover active

SSH セッションから切断されている場合は、新しいアクティブ/元のスタンバイ ユニット上に現在あるメイン IP アドレスに再接続します。

ステップ 11 新しいアクティブ装置から、元のアクティブ装置 (今の新しいスタンバイ装置) をリロードします。

failover reload-standby

例 :

```
asa/act# failover reload-standby
```

- (注) 元のアクティブ ユニットのコンソール ポートに接続されている場合は、代わりに **reload** コマンドを入力して、元のアクティブユニットをリロードする必要があります。

ASDM を使用したアクティブ/スタンバイ フェールオーバー ペアのアップグレード

Upgrade Software from Local Computer ツールにより、コンピュータからフラッシュファイルシステムにイメージファイルをアップロードし、アプライアンスモードの Firepower 1000 または Firepower 2100、Cisco Secure Firewall 3100/4200 のアクティブ/スタンバイ フェールオーバー ペアをアップグレードできます。

手順

- ステップ 1** スタンバイ IP アドレスに接続して、*standby* ユニット上で ASDM を起動します。
- ステップ 2** メイン ASDM アプリケーションウィンドウで、**[Tools] > [Upgrade Software from Local Computer]** の順に選択します。
- [Upgrade Software] ダイアログボックスが表示されます。
- ステップ 3** [アップロードするイメージ (Image to Upload)] ドロップダウンリストから、[ASA] を選択します。
- ステップ 4** [Local File Path] フィールドにコンピュータ上のファイルへのローカルパスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを見つけます。
- ステップ 5** [Flash File System Path] フィールドにフラッシュファイルシステムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを検索します。
- ステップ 6** [イメージのアップロード (Upload Image)] をクリックします。アップグレードプロセスには数分かかる場合があります。
- このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。
- ステップ 7** メイン IP アドレスに接続して、ASDM をアクティブなユニットに接続します。
- ステップ 8** デフォルト以外の ASDM イメージを以前に設定した場合は、イメージバンドルに付属のイメージにリセットします。
- イメージバンドルには ASDM イメージが含まれていて、ASA バンドルをアップグレードすると、同じ名前 (**asdm.bin**) であるため、リロード後にバンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。アップロードした別の ASDM イメージ (たとえば **asdm-7191.bin**) を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のあるバージョンの ASDM が確実に実行されるようにするには、バンドルされている ASDM イメージを使用するように ASA を再設定する必要があります。

- a) [設定 (Configuration)] > [デバイス管理 (Device Management)] > [システムイメージ/設定 (System Image/Configuration)] > [ブートイメージ/設定 (Boot Image/Configuration)] を選択します。
- b) [ASDMイメージファイルパス (ASDM Image File Path)] に、**disk0:/asdm.bin** と入力します。
- c) [適用 (Apply)] をクリックします。

ステップ 9 スタンバイユニットで使用したのと同じファイルの場所を使用して、ASA ソフトウェアをアップロードします。

ステップ 10 このイメージを ASA イメージとして設定するように求められたら、[Yes] をクリックします。新しいイメージを使用するために、ASA をリロードするよう求められます。[OK] をクリックします。アップグレード ツールを終了します。

ステップ 11 コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。
これらの設定変更は、スタンバイ ユニットに自動的に保存されます。

ステップ 12 [Monitoring] > [Properties] > [Failover] > [Status] の順に選択し、[Reload Standby] をクリックして、スタンバイ装置をリロードします。
[System] ペインを開いたまま、スタンバイ ユニットがリロードされるのを確認します。

ステップ 13 スタンバイユニットがリロードしたら、[Monitoring] > [Properties] > [Failover] > [Status] の順に選択し、[Make Standby] をクリックして、アクティブユニットをスタンバイユニットにフェールオーバーします。
ASDM は新しいアクティブ ユニットに自動的に再接続されます。

ステップ 14 [Monitoring] > [Properties] > [Failover] > [Status] の順に選択し、[Reload Standby] をクリックして、(新しい) スタンバイユニットをリロードします。

アクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー ペアをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、CLI または ASDM を使用します。

CLI を使用したアクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー コンフィギュレーションの 2 つのユニットをアップグレードするには、アプライアンスモードの Firepower 1000 または 2100、Cisco Secure Firewall 3100/4200 で次の手順を実行します。

始める前に

- 標準出荷単位で次の手順を実行します。
- これらの手順をシステム実行スペースで実行します。

- この手順では、FTPを使用します。TFTP、HTTP、またはその他のサーバータイプについては、『[ASA Command Reference](#)』の **copy** コマンドを参照してください。

手順

- ステップ 1** グローバルコンフィギュレーションモードのプライマリユニットで、デフォルト以外の ASDM イメージを以前に設定した場合は、イメージバンドルに付属のイメージにリセットします。

```
asdm image disk0:/asdm.bin
```

```
write memory
```

イメージバンドルには ASDM イメージが含まれていて、ASA バンドルをアップグレードすると、同じ名前 (**asdm.bin**) であるため、リロード後にバンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。アップロードした別の ASDM イメージ (たとえば **asdm-7191.bin**) を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のあるバージョンの ASDM が確実に実行されるようにするには、バンドルされている ASDM イメージを使用するように ASA を再設定する必要があります。

- ステップ 2** 特権 EXEC モード (最小限) 時にプライマリユニットで、ASA ソフトウェアをフラッシュメモリにコピーします。

```
copy ftp://[[user[:password]]@]server[/path]/asa_image_name diskn:[/path]/asa_image_name
```

(注) ASDM は ASA イメージに含まれています。

例 :

```
asa/act/pri# copy ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA
disk0:/cisco-asa-fp1k.9.14.1.SPA
```

- ステップ 3** ソフトウェアをセカンダリ装置にコピーします。プライマリ装置で指定したのと同じパスを指定してください。

```
failover exec mate copy /noconfirm ftp://[[user[:password]]@]server[/path]/asa_image_name
diskn:[/path]/asa_image_name
```

例 :

```
asa/act/pri# failover exec mate copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA disk0:/cisco-asa-fp1k.9.14.1.SPA
```

- ステップ 4** まだグローバルコンフィギュレーションモードを開始していない場合は、グローバルコンフィギュレーションモードを開始します。

```
configure terminal
```

- ステップ 5** 設定されている現在のブートイメージが存在している場合、これを表示します。

show running-config boot system

設定に **boot system** コマンドが存在しない場合があることに注意してください。たとえば、ROMMON からイメージをインストールした場合、新しいデバイスがある場合、またはコマンドを手動で削除した場合などです。

例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

- ステップ 6** **boot system** コマンドが設定されている場合は、新しいブートイメージを入力できるようにコマンドを削除します。

no boot system disk:[/path]asa_image_name

boot system コマンドが設定されていない場合は、この手順をスキップします。

例：

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

- ステップ 7** ブートする ASA イメージを設定します（先ほどアップロードしたもの）。

boot system disk:[/path]asa_image_name

boot system コマンドは 1 つだけ入力できます。**boot system** コマンドは、入力時にアクションを実行します。システムはイメージを検証して解凍し、ブート場所（FXOS によって管理される **disk0** の内部ロケーション）にコピーします。ASA をリロードすると、新しいイメージがロードされます。リロードの前に気が変わった場合は、**no boot system** コマンドを入力してブート場所から新しいイメージを削除し、現在のイメージを引き続き実行することができます。

例：

```
ciscoasa(config)# boot system disk0:/cisco-asa-fp1k.9.14.1.SPA

The system is currently installed with security software package 9.13.1, which has:
  - The platform version: 2.7.1
  - The CSP (asa) version: 9.13.1
Preparing new image for install...
!!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.14.1 will do the following:
  - upgrade to the new platform version 2.8.1
  - upgrade to the CSP ASA version 9.14.1
After the installation is complete, reload to apply the new image.
Finalizing image install process...

Install_status: ready.....
Install_status: validating-images.....
Install_status: update-software-pack-completed
ciscoasa(config)#
```

- ステップ 8** 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

これらの設定変更は、セカンダリ ユニットに自動的に保存されます。

ステップ 9 プライマリ ユニットの両方のフェールオーバー グループをアクティブにします。

failover active group 1

failover active group 2

例 :

```
asa/act/pri(config)# failover active group 1
asa/act/pri(config)# failover active group 2
```

ステップ 10 セカンダリ装置をリロードして新しいイメージを起動します。

failover reload-standby

セカンダリ装置のロードが完了するまで待ちます。 **show failover** コマンドを使用して、両方のフェールオーバー グループが **Standby Ready** 状態であることを確認します。

ステップ 11 セカンダリ装置で、両方のフェールオーバー グループを強制的にアクティブにします。

no failover active group 1

no failover active group 2

例 :

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
asa/stby/pri(config)#
```

SSH セッションから切断されている場合は、セカンダリ ユニット上に現在あるフェールオーバー グループ 1 の IP アドレスに再接続します。

ステップ 12 プライマリ装置をリロードします。

failover reload-standby

例 :

```
asa/act/sec# failover reload-standby
```

(注) プライマリユニットのコンソールポートに接続されている場合は、代わりに **reload** コマンドを入力して、プライマリ ユニットの再ロードする必要があります。

SSH セッションから切断される場合があります。

ステップ 13 フェールオーバー グループは、**preempt** コマンドを使用して設定されている場合、プリエンブト遅延の経過後、指定された装置で自動的にアクティブになります。

ASDM を使用したアクティブ/アクティブ フェールオーバー ペアのアップグレード

Upgrade Software from Local Computer ツールにより、コンピュータからフラッシュファイルシステムにイメージファイルをアップロードし、アプライアンスモードの Firepower 1000 または Firepower 2100、Cisco Secure Firewall 3100/4200 のアクティブ/アクティブ フェールオーバー ペアをアップグレードできます。

始める前に

- これらの手順をシステム実行スペースで実行します。
- ローカル管理コンピュータに ASA イメージを配置します。

手順

-
- ステップ 1** フェールオーバー グループ 2 の管理アドレスに接続して、セカンダリ ユニットで ASDM を起動します。
- ステップ 2** メイン ASDM アプリケーションウィンドウで、[Tools] > [Upgrade Software from Local Computer] の順に選択します。
- [Upgrade Software] ダイアログボックスが表示されます。
- ステップ 3** [アップロードするイメージ (Image to Upload)] ドロップダウンリストから、[ASA] を選択します。
- ステップ 4** [Local File Path] フィールドにコンピュータ上のファイルへのローカルパスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを見つけます。
- ステップ 5** [Flash File System Path] フィールドにフラッシュファイルシステムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを検索します。
- ステップ 6** [イメージのアップロード (Upload Image)] をクリックします。アップグレードプロセスには数分かかる場合があります。
- このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。
- ステップ 7** フェールオーバーグループ 1 の管理 IP アドレスに接続して、ASDM をプライマリユニットに接続します。
- ステップ 8** デフォルト以外の ASDM イメージを以前に設定した場合は、イメージバンドルに付属のイメージにリセットします。

イメージバンドルには ASDM イメージが含まれていて、ASA バンドルをアップグレードすると、同じ名前 (**asdm.bin**) であるため、リロード後にバンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。アップロードした別の ASDM イメージ (たとえば **asdm-7191.bin**) を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のあるバージョンの ASDM が確実に実行されるようにするには、バンドルされている ASDM イメージを使用するように ASA を再設定する必要があります。

- a) [設定 (Configuration)] > [デバイス管理 (Device Management)] > [システムイメージ/設定 (System Image/Configuration)] > [ブートイメージ/設定 (Boot Image/Configuration)] を選択します。
- b) [ASDMイメージファイルパス (ASDM Image File Path)] に、**disk0:/asdm.bin** と入力します。
- c) [適用 (Apply)] をクリックします。

ステップ 9 セカンダリユニットで使用したのと同じファイルの場所を使用して、ASA ソフトウェアをアップロードします。

ステップ 10 このイメージを ASA イメージとして設定するように求められたら、[Yes] をクリックします。新しいイメージを使用するために、ASA をリロードするよう求められます。[OK] をクリックします。アップグレード ツールを終了します。

ステップ 11 コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。
これらの設定変更は、セカンダリ ユニットに自動的に保存されます。

ステップ 12 [Monitoring] > [Failover] > [Failover Group #] の順に選択して、プライマリユニット上の両方のフェールオーバーグループをアクティブにします。ここで # は、プライマリユニットに移動するフェールオーバーグループの数です。[Make Active] をクリックします。

ステップ 13 [Monitoring] > [Failover] > [System] の順に選択し、[Reload Standby] をクリックして、セカンダリユニットをリロードします。
[System] ペインを開いたまま、セカンダリ ユニットがリロードされるのを確認します。

ステップ 14 セカンダリユニットが起動したら、[Monitoring] > [Failover] > [Failover Group #] の順に選択して、セカンダリユニット上の両方のフェールオーバーグループをアクティブにします。ここで # は、セカンダリユニットに移動するフェールオーバーグループの数です。[Make Standby] をクリックします。
ASDM は、セカンダリ ユニット上のフェールオーバー グループ 1 の IP アドレスに自動的に再接続されます。

ステップ 15 [Monitoring] > [Failover] > [System] の順に選択し、[Reload Standby] をクリックして、プライマリユニットをリロードします。

ステップ 16 フェールオーバーグループは、[Preempt Enabled] を使用して設定されると、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。ASDM は、プライマリ ユニット上のフェールオーバー グループ 1 の IP アドレスに自動的に再接続されます。

ASA クラスタのアップグレード (Cisco Secure Firewall 3100/4200)

CLI を使用した ASA クラスタのアップグレード (Cisco Secure Firewall 3100/4200)

ASA クラスタ内のすべてのノードをアップグレードするには、次の手順を実行します。この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバータイプについては、『[ASA Command Reference](#)』の `copy` コマンドを参照してください。

始める前に

- 制御ノードで次の手順を実行します。クラスタノードと状態（制御またはデータ）を表示するように ASA プロンプトを設定できます。これは、接続しているノードを特定するのに役立ちます。 `prompt` コマンドを参照してください。代わりに、 `show cluster info` コマンドを入力して、各ノードのロールを表示します。
- コンソール ポートを使用する必要があります。クラスタリングのイネーブルまたはディセーブルを、リモート CLI 接続から行うことはできません。
- マルチ コンテキスト モードでは、システム実行スペースで後続の手順を実行します。

手順

- ステップ 1** グローバル コンフィギュレーション モードの制御ノードで、デフォルト以外の ASDM イメージを以前に設定した場合は、イメージバンドルに付属のイメージにリセットします。

```
asdm image disk0:/asdm.bin
```

write memory

イメージバンドルには ASDM イメージが含まれていて、ASA バンドルをアップグレードすると、同じ名前 (`asdm.bin`) であるため、リロード後にバンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。アップロードした別の ASDM イメージ（たとえば `asdm-7191.bin`）を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のあるバージョンの ASDM が確実に実行されるようにするには、バンドルされている ASDM イメージを使用するように ASA を再設定する必要があります。

- ステップ 2** 特権 EXEC モード（最小限）時に制御ノードで、ASA ソフトウェアをクラスタ内のすべてのノードにコピーします。

```
cluster exec copy /noconfirm ftp://[user[:password]@]server[/path]/asa_image_name  
diskn:[/path]asa_image_name
```

例 :

```
asa/unit1/control# cluster exec copy /noconfirm  
ftp://dwinchester:sam@10.1.1.1/cisco-asa-fp3k.9.19.1.SPA disk0:/cisco-asa-fp3k.9.19.1.SPA
```

- ステップ 3** まだグローバル コンフィギュレーション モードを開始していない場合は、ここで開始します。

```
configure terminal
```

例 :

```
asa/unit1/control# configure terminal
asa/unit1/control(config)#
```

ステップ 4 設定されている現在のブートイメージが存在している場合、これを表示します。

show running-config boot system

設定に **boot system** コマンドが存在しない場合があることに注意してください。たとえば、ROMMON からイメージをインストールした場合、新しいデバイスがある場合、またはコマンドを手動で削除した場合などです。

例 :

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fplk.9.17.1.SPA
```

ステップ 5 **boot system** コマンドが設定されている場合は、新しいブートイメージを入力できるようにコマンドを削除します。

no boot system diskn:[path]asa_image_name

boot system コマンドが設定されていない場合は、この手順をスキップします。

例 :

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fplk.9.17.1.SPA
```

ステップ 6 ブートする ASA イメージを設定します (先ほどアップロードしたもの)。

boot system diskn:[path]asa_image_name

boot system コマンドは 1 つだけ入力できます。**boot system** コマンドは、入力時にアクションを実行します。システムはイメージを検証して解凍し、ブート場所 (FXOS によって管理される disk0 の内部ロケーション) にコピーします。ASA をリロードすると、新しいイメージがロードされます。リロードの前に気が変わった場合は、**no boot system** コマンドを入力してブート場所から新しいイメージを削除し、現在のイメージを引き続き実行することができます。

例 :

```
ciscoasa(config)# boot system disk0:/cisco-asa-fplk.9.19.1.SPA
```

```
The system is currently installed with security software package 9.17.1, which has:
- The platform version: 2.11.1
- The CSP (asa) version: 9.17.1
Preparing new image for install...
!!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.19.1 will do the following:
- upgrade to the new platform version 2.13.1
- upgrade to the CSP ASA version 9.19.1
After the installation is complete, reload to apply the new image.
Finalizing image install process...
```

```
Install_status: ready.....
Install_status: validating-images.....
Install_status: update-software-pack-completed
ciscoasa(config)#
```

ステップ 7 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

これらの設定変更は、データノードに自動的に保存されます。

ステップ 8 リロードしてデータノードをアップグレードします。

(注) アップグレードプロセス中は、**cluster control-node unit** コマンドを使用して強制的にデータノードを制御に変更しないでください。ネットワークの接続性とクラスタの安定性に関連した障害が発生する恐れがあります。最初にすべてのデータノードをアップグレードしてリロードし、次にこの手順を実行すると、現在の制御ノードから新しい制御ノードへの移行をスムーズに行うことができます。

- a) 制御ノードでメンバー名を表示するには、**cluster exec unit ?** または **show cluster info** コマンドを入力します。
- b) データノードをリロードします。

cluster exec unit data-node reload noconfirm

例 :

```
asa/unit1/control# cluster exec unit node2 reload noconfirm
```

- c) 各データノードで繰り返します。

接続損失を回避し、トラフィックを安定させるために、各ノードが起動しクラスタに再接続するのを待ち (約 5 分)、次のノードにこれらの手順を繰り返します。ノードがクラスタに再接続したことを確認するには、**show cluster info** を入力します。

ステップ 9 リロードして制御ノードをアップグレードします。

- a) クラスタリングを無効にします。可能であれば、制御ノードのクラスタリングを手動で無効にすることを推奨します。これにより、新しい制御ノードをできるだけ迅速かつクリーンな状態で選定できます。

cluster group name

no enable

新しい制御ノードが選択され、トラフィックが安定するまで 5 分間待ちます。

リロード時にクラスタリングを有効にするために、この構成を保存しないでください。

例 :

```
asa/unit1/control(config)# cluster group cluster1
asa/unit1/control(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover
```

```
either enable clustering or remove cluster group configuration.
```

```
Cluster unit node1 transitioned from CONTROL to DISABLED
asa/unit1/ClusterDisabled(cfg-cluster)#
```

- b) このノードをリロードします。

reload noconfirm

元の制御ノードがクラスタに再接続すると、そのノードはデータノードになります。

ASDM を使用した ASA クラスタのアップグレード (Cisco Secure Firewall 3100/4200)

ASA クラスタ内のすべてのノードをアップグレードするには、次の手順を実行します。

始める前に

- 制御ノードで次の手順を実行します。
- マルチ コンテキスト モードでは、システム実行スペースで後続の手順を実行します。
- ローカル管理コンピュータに ASA イメージを配置します。

手順

- ステップ 1** メインクラスタ IP アドレスに接続して、制御ノードで ASDM を起動します。

この IP アドレスは、常に制御ノードに保持されます。

- ステップ 2** デフォルト以外の ASDM イメージを以前に設定した場合は、イメージバンドルに付属のイメージにリセットします。

イメージバンドルには ASDM イメージが含まれていて、ASA バンドルをアップグレードすると、同じ名前 (**asdm.bin**) であるため、リロード後にバンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。アップロードした別の ASDM イメージ (たとえば **asdm-7191.bin**) を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のあるバージョンの ASDM が確実に実行されるようにするには、バンドルされている ASDM イメージを使用するように ASA を再設定する必要があります。

- メイン ASDM アプリケーションウィンドウで、**[設定 (Configuration)] > [デバイス管理 (Device Management)] > [システムイメージ/設定 (System Image/Configuration)] > [ブートイメージ/設定 (Boot Image/Configuration)]** を選択します。
- [ASDM イメージファイルパス (ASDM Image File Path)]** に、**disk0:/asdm.bin** と入力します。
- [適用 (Apply)]** をクリックします。

- ステップ 3** メイン ASDM アプリケーションウィンドウで、[ツール (Tools)] > [ローカルコンピュータからのソフトウェアのアップグレード (Upgrade Software from Local Computer)] の順に選択します。
- [Upgrade Software from Local Computer] ダイアログボックスが表示されます。
- ステップ 4** [クラスタ内のすべてのデバイス (All devices in the cluster)] オプション ボタンをクリックします。
- [ソフトウェアのアップグレード (Upgrade Software)] ダイアログボックスが表示されます。
- ステップ 5** [アップロードするイメージ (Image to Upload)] ドロップダウンリストから、[ASA] を選択します。
- ステップ 6** [ローカル ファイル パス (Local File Path)] フィールドで [ローカル ファイルの参照 (Browse Local Files)] をクリックして、コンピュータ上のファイルを見つけます。
- ステップ 7** (任意) [フラッシュファイルシステムのパス (Flash File System Path)] フィールドにフラッシュファイルシステムへのパスを入力するか、[フラッシュの参照 (Browse Flash)] をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを検索します。
- デフォルトでは、このフィールドにはパス (**disk0:/filename**) が入力されています。
- ステップ 8** [イメージのアップロード (Upload Image)] をクリックします。アップグレードプロセスには数分かかる場合があります。
- ステップ 9** このイメージを ASA イメージとして設定するように求められます。[Yes] をクリックします。
- ステップ 10** 新しいイメージを使用するために、ASA をリロードするよう求められます。[OK] をクリックします。
- アップグレード ツールを終了します。
- ステップ 11** コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。
- これらの設定変更は、データノードに自動的に保存されます。
- ステップ 12** [構成 (Configuration)] > [デバイス管理 (Device Management)] > [ハイアベイラビリティとスケラビリティ (High Availability and Scalability)] > [ASA クラスタ (ASA Cluster)] > [クラスタメンバー (Cluster Members)] で、各ノードの個別の管理 IP アドレスをメモして、後で ASDM をデータノードに直接接続できるようにします。
- ステップ 13** リロードしてデータノードをアップグレードします。
- (注) アップグレードプロセス中は、強制的にデータノードを制御に変更するために [モニタリング (Monitoring)] > [ASA クラスタ (ASA Cluster)] > [クラスタの概要 (Cluster Summary)] ページを使用して制御ノードを変更しないでください。ネットワークの接続性とクラスタの安定性に関連した障害が発生する可能性があります。最初にすべてのデータノードをリロードし、次にこの手順を実行すると、現在の制御ノードから新しい制御ノードへの移行をスムーズに行うことができます。
- a) 制御ノードで、[ツール (Tools)] > [システムリロード (System Reload)] を選択します。
- b) [デバイス (Device)] ドロップダウンリストからデータノード名を選択します。

- c) [Schedule Reload] をクリックします。
- d) [Yes] をクリックしてリロードを続行します。
- e) 各データノードで繰り返します。

接続損失を回避し、トラフィックを安定させるために、各ノードが起動しクラスタに再接続するのを待ち（約 5 分）、次のノードにこれらの手順を繰り返します。ノードがクラスタに再接続したことを確認するには、[モニタリング (Monitoring)] > [ASA クラスタ (ASA Cluster)] > [クラスタの概要 (Cluster Summary)] ペインを表示します。

ステップ 14 リロードして制御ノードをアップグレードします。

- a) 制御ノードの ASDM で、[構成 (Configuration)] > [デバイス管理 (Device Management)] > [ハイアベイラビリティとスケーラビリティ (High Availability and Scalability)] > [ASA クラスタ (ASA Cluster)] > [クラスタの設定 (Cluster Configuration)] ペインを選択します。
- b) [ASA クラスタに参加 (Participate in ASA cluster)] チェックボックスをオフにして、[適用 (Apply)] をクリックします。

ASDM から出るように促されます。

- c) 新しい制御ノードが選択され、トラフィックが安定するまで最大 5 分間待ちます。
元の制御ノードがクラスタに再接続すると、そのノードはデータノードになります。
- d) 事前にメモした個別の管理 IP アドレスに接続して、ASDM を元の制御ノードに再接続します。

この時点で、メインクラスタ IP アドレスは新しい制御ノードに属しています。元の制御ノードは、その個別の管理 IP アドレスに引き続きアクセスできます。

- e) [Tools] > [System Reload] を選択します。
- f) [実行コンフィギュレーションを保存しないでリロードする (Reload without saving the running configuration)] オプション ボタンをクリックします。

このノードのリロード時にクラスタリングを有効にするために、この構成を保存しないようにします。

- g) [Schedule Reload] をクリックします。
- h) [Yes] をクリックしてリロードを続行します。

ASDM から出るように促されます。メインクラスタ IP アドレスで ASDM を再起動すると、新しい制御ノードに再接続されます。

プラットフォームモードでの Firepower 2100 のアップグレード

このドキュメントでは、プラットフォームモードでの Firepower 2100 のスタンドアロンまたはフェールオーバー展開用に、ASA、FXOS、および ASDM のアップグレードを計画し、実装する方法について説明します。バージョン 9.13 以前では、Firepower 2100 はプラットフォーム

モードのみをサポートしていました。9.14 以降では、アプライアンスモードがデフォルトです。9.14 以降では、ASA で **show fxos mode** コマンドを使用して現在のモードを決定します。アプライアンスモードの手順については、[Firepower 1000、2100 \(アプライアンスモード\)](#)、および [Cisco Secure Firewall 3100/4200 のアップグレード \(1 ページ\)](#) を参照してください。

スタンドアロンユニットのアップグレード

スタンドアロンユニットをアップグレードするには FXOS CLI または FirePOWER シャーシマネージャを使用します。

Firepower Chassis Manager を使用したスタンドアロンユニットのアップグレード

この項では、スタンドアロンユニットの (ASA と ASDM の両方を含む) ASA バンドルをアップグレードする方法を説明します。管理コンピュータからパッケージをアップロードします。

手順

ステップ 1 ASA の設定でデフォルト以外の ASDM イメージを以前に設定した場合は、イメージバンドルに付属のイメージにリセットします。

イメージバンドルには ASDM イメージが含まれていて、ASA バンドルをアップグレードすると、同じ名前 (**asdm.bin**) であるため、リロード後にバンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。アップロードした別の ASDM イメージ (たとえば **asdm-7191.bin**) を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のあるバージョンの ASDM が確実に実行されるようにするには、バンドルされている ASDM イメージを使用するように ASA を再設定する必要があります。

- メイン ASDM アプリケーションウィンドウで、**[設定 (Configuration)] > [デバイス管理 (Device Management)] > [システムイメージ/設定 (System Image/Configuration)] > [ブートイメージ/設定 (Boot Image/Configuration)]** を選択します。
- [ASDM イメージファイルパス (ASDM Image File Path)]** に、**disk0:/asdm.bin** と入力します。
- [適用 (Apply)]** をクリックします。
- コンフィギュレーションの変更を保存するには、ツールバーの **[Save]** アイコンをクリックします。
- ASDM を終了します。

ステップ 2 Firepower Chassis Manager に接続します。

ステップ 3 **[System] > [Updates]** を選択します。

[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。

ステップ 4 **[Upload Image]** をクリックして管理コンピュータから新しいパッケージをアップロードします。

ステップ 5 **[Choose File]** をクリックして対象のファイルに移動し、アップロードするパッケージを選択します。

ステップ 6 **[Upload]** をクリックします。

選択したパッケージがシャーシにアップロードされます。[Upload Image] のダイアログボックスにアップロードの状況が表示されます。[Success] のダイアログボックスが表示されたら [OK] をクリックします。アップロードが完了すると、イメージの整合性が自動的に検証されます。

ステップ 7 新しいパッケージの右側の [Upgrade] アイコンをクリックします。

ステップ 8 [Yes] をクリックして、インストールを続行することを確認します。

新しいパッケージが読み込まれていることを示すインジケータはありません。アップグレードプロセスの開始時には引き続き Firepower Chassis Manager が表示されます。システムのリブート時にログアウトされます。Firepower Chassis Manager にログインするには、システムのリブート完了を待つ必要があります。リブートプロセスには約 20 分かかります。リブート後、ログイン画面が表示されます。

FXOS CLI を使用したスタンドアロンユニットのアップグレード

この項では、スタンドアロンユニットの (ASA と ASDM の両方を含む) ASA バンドルをアップグレードする方法を説明します。パッケージを FirePOWER 2100 シャーシにコピーするには、FTP、SCP、SFTP、または TFTP を使用できます。

手順

ステップ 1 コンソールポート (推奨) または SSH を使用して、FXOS CLI に接続します。

ステップ 2 ASA の設定でデフォルト以外の ASDM イメージを以前に設定した場合は、イメージバンドルに付属のイメージにリセットします。

イメージバンドルには ASDM イメージが含まれていて、ASA バンドルをアップグレードすると、同じ名前 (**asdm.bin**) であるため、リロード後にバンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。アップロードした別の ASDM イメージ (たとえば **asdm-7191.bin**) を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のあるバージョンの ASDM が確実に実行されるようにするには、バンドルされている ASDM イメージを使用するように ASA を再設定する必要があります。

a) ASA に接続します。

connect asa

例 :

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

b) 特権 EXEC モードにアクセスしてから、グローバル コンフィギュレーション モードにアクセスします。

enable

configure terminal

- c) ASDM イメージを設定します。

```
asdm image disk0:/asdm.bin
```

- d) 設定を保存します。

```
write memory
```

- e) **Ctrl+a**、**d** を押して、FXOS コンソールに戻ります。

ステップ 3 FXOS で、シャーシにパッケージをダウンロードします。

- a) ファームウェア モードを入力します。

```
scope firmware
```

例 :

```
firepower-2110# scope firmware
firepower-2110 /firmware#
```

- b) パッケージをダウンロードします。

```
download image url
```

次のいずれかを使用してインポートするファイルの URL を指定します。

- **ftp://username@server/[path/]image_name**
- **scp://username@server/[path/]image_name**
- **sftp://username@server/[path/]image_name**
- **tftp://server[:port]/[path/]image_name**

例 :

```
firepower-2110 /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

- c) ダウンロード プロセスをモニターします。

```
show download-task
```

例 :

```
firepower-2110 /firmware # show download

Download task:
  File Name Protocol Server          Port    Userid    State
  -----
  cisco-asa-fp2k.9.8.2.SPA
    Tftp    10.88.29.181    0       0       Downloaded
  cisco-asa-fp2k.9.8.2.2.SPA
    Tftp    10.88.29.181    0       0       Downloading
firepower-2110 /firmware #
```

ステップ 4 新しいパッケージのダウンロードが終了 ([Downloaded] の状態) したら、パッケージを起動します。

- a) 新しいパッケージのバージョン番号を表示します。

show package

例 :

```
firepower-2110 /firmware # show package
Name                                     Package-Vers
-----
cisco-asa-fp2k.9.8.2.SPA                9.8.2
cisco-asa-fp2k.9.8.2.2.SPA              9.8.2.2
firepower-2110 /firmware #
```

- b) パッケージをインストールします。

scope auto-install

install security-pack version version

show package の出力で、**security-pack version** 番号の **Package-Vers** 値をコピーします。シャシーが ASA イメージをインストールして再起動します。

例 :

```
firepower-2110 /firmware # scope auto-install
firepower-2110 /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
  - The platform version: 2.2.2.52
  - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
  - upgrade to the new platform version 2.2.2.97
  - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no) :yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no) :yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
firepower-2110 /firmware/auto-install #
```

ステップ 5 シャシーのリブートが完了するのを待ちます (5 ~ 10 分)。

FXOS が起動しても、ASA が稼働するまで (5 分) 待機する必要があります。次のメッセージが表示されるまで待機します。

```
firepower-2110#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
```

```
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[...]
```

アクティブ/スタンバイ フェールオーバー ペアのアップグレード

アクティブ/スタンバイ フェールオーバー ペアをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、FXOS CLI または FirePOWER シャーシマネージャを使用します。

Firepower Chassis Manager を使用したアクティブ/スタンバイ フェールオーバー ペアのアップグレード

この項では、アクティブ/スタンバイ フェールオーバー ペアの (ASA と ASDM の両方を含む) ASA バンドルをアップグレードする方法を説明します。管理コンピュータからパッケージをアップロードします。

始める前に

アクティブになっているユニットとスタンバイになっているユニットを確認する必要があります。ASDM をアクティブな ASA の IP アドレスに接続します。アクティブ装置は、常にアクティブな IP アドレスを保有しています。次に、[**モニタリング (Monitoring)**] > [**プロパティ (Properties)**] > [**フェールオーバー (Failover)**] > [**ステータス (Status)**] の順に選択して、このユニットの優先順位 (プライマリまたはセカンダリ) を表示し、接続先のユニットを確認できるようにします。

手順

ステップ 1 ASA の設定でデフォルト以外の ASDM イメージを以前に設定した場合は、イメージバンドルに付属のイメージにリセットします。

イメージバンドルには ASDM イメージが含まれていて、ASA バンドルをアップグレードすると、同じ名前 (**asdm.bin**) であるため、リロード後にバンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。アップロードした別の ASDM イメージ (たとえば **asdm-7191.bin**) を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のあるバージョンの ASDM が確実に実行されるようにするには、バンドルされている ASDM イメージを使用するように ASA を再設定する必要があります。

- アクティブユニットの ASDM に接続します。
- メイン ASDM アプリケーションウィンドウで、[**設定 (Configuration)**] > [**デバイス管理 (Device Management)**] > [**システムイメージ/設定 (System Image/Configuration)**] > [**ブートイメージ/設定 (Boot Image/Configuration)**] を選択します。

- c) [ASDMイメージファイルパス (ASDM Image File Path)] に、**disk0:/asdm.bin** と入力します。
- d) [適用 (Apply)] をクリックします。
- e) コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。
- f) ASDM を終了します。

ステップ 2 スタンバイ装置をアップグレードします。

- a) スタンバイ装置の Firepower Chassis Manager に接続します。
- b) [システム (System)] > [更新 (Updates)] を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。
- c) [Upload Image] をクリックして管理コンピュータから新しいパッケージをアップロードします。
- d) [Choose File] をクリックして対象のファイルに移動し、アップロードするパッケージを選択します。
- e) [Upload] をクリックします。

選択したパッケージがシャーシにアップロードされます。[Upload Image] のダイアログボックスにアップロードの状況が表示されます。[Success] のダイアログボックスが表示されたら [OK] をクリックします。アップロードが完了すると、イメージの整合性が自動的に検証されます。

- f) 新しいパッケージの右側の [Upgrade] アイコンをクリックします。
- g) [Yes] をクリックして、インストールを続行することを確認します。

新しいパッケージが読み込まれていることを示すインジケータはありません。アップグレードプロセスの開始時には引き続き Firepower Chassis Manager が表示されます。システムのリブート時にログアウトされます。Firepower Chassis Manager にログインするには、システムのリブート完了を待つ必要があります。リブートプロセスには約 20 分かかります。リブート後、ログイン画面が表示されます。

ステップ 3 アップグレードした装置をアクティブ装置にして、アップグレード済みの装置にトラフィックが流れるようにします。

- a) スタンバイ ASA IP アドレスに接続して、スタンバイ装置で ASDM を起動します。
- b) [モニタリング (Monitoring)] > [プロパティ (Properties)] > [フェールオーバー (Failover)] > [ステータス (Status)] の順に選択し、[アクティブにする (Make Active)] をクリックして、スタンバイ装置を強制的にアクティブにします。

ステップ 4 以前のアクティブ装置をアップグレードします。

- a) 以前のアクティブ装置の Firepower Chassis Manager に接続します。
- b) [システム (System)] > [更新 (Updates)] を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。
- c) [Upload Image] をクリックして管理コンピュータから新しいパッケージをアップロードします。
- d) [Choose File] をクリックして対象のファイルに移動し、アップロードするパッケージを選択します。

- e) [Upload] をクリックします。

選択したパッケージがシャーシにアップロードされます。[Upload Image] のダイアログボックスにアップロードの状況が表示されます。[Success] のダイアログボックスが表示されたら [OK] をクリックします。アップロードが完了すると、イメージの整合性が自動的に検証されます。

- f) 新しいパッケージの右側の [Upgrade] アイコンをクリックします。

- g) [Yes] をクリックして、インストールを続行することを確認します。

新しいパッケージが読み込まれていることを示すインジケータはありません。アップグレードプロセスの開始時には引き続き Firepower Chassis Manager が表示されます。システムのリブート時にログアウトされます。Firepower Chassis Manager にログインするには、システムのリブート完了を待つ必要があります。リブートプロセスには約 20 分かかります。リブート後、ログイン画面が表示されます。

FXOS CLI を使用したアクティブ/スタンバイ フェールオーバー ペアのアップグレード

この項では、アクティブ/スタンバイ フェールオーバー ペアの (ASA と ASDM の両方を含む) ASA バンドルをアップグレードする方法を説明します。パッケージを FirePOWER 2100 シャーシにコピーするには、FTP、SCP、SFTP、または TFTP を使用できます。

始める前に

アクティブになっているユニットとスタンバイになっているユニットを確認する必要があります。フェールオーバー ステータスを確認するには、ASA プロンプトを調べます。フェールオーバー ステータスと優先順位 (プライマリまたはセカンダリ) を表示するように ASA プロンプトを設定できます。これは、接続しているユニットを特定するのに役立ちます。prompt コマンドを参照してください。ただし、FXOS プロンプトでは ASA フェールオーバー は認識されません。代わりに、ASA show failover コマンドを入力して、このユニットのステータスと優先順位 (プライマリまたはセカンダリ) を表示します。

手順

-
- ステップ 1** ASA の設定でデフォルト以外の ASDM イメージを以前に設定した場合は、イメージバンドルに付属のイメージにリセットします。

イメージバンドルには ASDM イメージが含まれていて、ASA バンドルをアップグレードすると、同じ名前 (asdm.bin) であるため、リロード後にバンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。アップロードした別の ASDM イメージ (たとえば asdm-7191.bin) を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のあるバージョンの ASDM が確実に実行されるようにするには、バンドルされている ASDM イメージを使用するように ASA を再設定する必要があります。

- a) コンソールポート（推奨）または SSH を使用して、アクティブユニットの FXOS CLI に接続します。
- b) ASA に接続します。

connect asa

例：

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

- c) 特権 EXEC モードにアクセスしてから、グローバル コンフィギュレーション モードにアクセスします。

enable

configure terminal

- d) ASDM イメージを設定します。

asdm image disk0:/asdm.bin

- e) 設定を保存します。

write memory

- f) **Ctrl+a**、**d** を押して、FXOS コンソールに戻ります。

ステップ 2 スタンバイ装置をアップグレードします。

- a) コンソールポート（推奨）または SSH を使用して、スタンバイ装置の FXOS CLI に接続します。
- b) ファームウェア モードを入力します。

scope firmware

例：

```
2110-sec# scope firmware
2110-sec /firmware#
```

- c) パッケージをダウンロードします。

download image url

次のいずれかを使用してインポートするファイルの URL を指定します。

- **ftp://username@server/[path/]image_name**
- **scp://username@server/[path/]image_name**
- **sftp://username@server/[path/]image_name**
- **tftp://server[:port]/[path/]image_name**

例：

```
2110-sec /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

- d) ダウンロードプロセスをモニターします。

show download-task

例 :

```
2110-sec /firmware # show download

Download task:
  File Name Protocol Server          Port    Userid    State
  -----
  cisco-asa-fp2k.9.8.2.SPA
    Tftp      10.88.29.181          0        0        Downloaded
  cisco-asa-fp2k.9.8.2.2.SPA
    Tftp      10.88.29.181          0        0        Downloading
2110-sec /firmware #
```

- e) 新しいパッケージのダウンロードが終了 ([Downloaded] の状態) したら、パッケージを起動します。新しいパッケージのバージョン番号を表示します。

show package

例 :

```
2110-sec /firmware # show package
Name                                     Package-Vers
-----
cisco-asa-fp2k.9.8.2.SPA                 9.8.2
cisco-asa-fp2k.9.8.2.2.SPA              9.8.2.2
2110-sec /firmware #
```

- f) パッケージをインストールします。

scope auto-install

install security-pack version *version*

show package の出力で、**security-pack version** 番号の **Package-Vers** 値をコピーします。シャーンが ASA イメージをインストールして再起動します。

例 :

```
2110-sec /firmware # scope auto-install
2110-sec /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
- The platform version: 2.2.2.52
- The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
- upgrade to the new platform version 2.2.2.97
- upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes
```

```
This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup
```

```
Do you want to proceed? (yes/no):yes
```

```
Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-sec /firmware/auto-install #
```

- g) シャーシのリポートが完了するのを待ちます (5 ~ 10 分)。

FXOS が起動しても、ASA が稼働するまで (5 分) 待機する必要があります。次のメッセージが表示されるまで待機します。

```
2110-sec#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[...]
```

ステップ 3 アップグレードした装置をアクティブ装置にして、アップグレード済みの装置にトラフィックが流れるようにします。

- a) FXOS からスタンバイ ASA CLI に接続します。

```
connect asa
```

```
enable
```

例 :

```
2110-sec# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
asa/stby/sec> enable
Password: *****
asa/stby/sec#
```

- b) スタンバイ装置を強制的にアクティブにします。

```
failover active
```

例 :

```
asa/stby/sec> failover active
asa/act/sec#
```

- c) FXOS コンソールに戻るには、**Ctrl+a**、**d** と入力します。

ステップ 4 以前のアクティブ装置をアップグレードします。

- a) コンソールポート（推奨）または SSH を使用して、以前のアクティブ装置の FXOS CLI に接続します。
- b) ファームウェア モードを入力します。

scope firmware

例：

```
2110-pri# scope firmware
2110-pri /firmware#
```

- c) パッケージをダウンロードします。

download image url

次のいずれかを使用してインポートするファイルの URL を指定します。

- **ftp://username@server/[path/]image_name**
- **scp://username@server/[path/]image_name**
- **sftp://username@server/[path/]image_name**
- **tftp://server[:port]/[path/]image_name**

例：

```
2110-pri /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

- d) ダウンロードプロセスをモニターします。

show download-task

例：

```
2110-pri /firmware # show download
```

```
Download task:
  File Name Protocol Server      Port      Userid      State
  -----
  cisco-asa-fp2k.9.8.2.SPA
    Tftp      10.88.29.181      0          Downloaded
  cisco-asa-fp2k.9.8.2.2.SPA
    Tftp      10.88.29.181      0          Downloading
2110-pri /firmware #
```

- e) 新しいパッケージのダウンロードが終了（[Downloaded] の状態）したら、パッケージを起動します。新しいパッケージのバージョン番号を表示します。

show package

例：

```

2110-pri /firmware # show package
Name                                     Package-Vers
-----
cisco-asa-fp2k.9.8.2.SPA                9.8.2
cisco-asa-fp2k.9.8.2.2.SPA              9.8.2.2
2110-pri /firmware #

```

- f) パッケージをインストールします。

scope auto-install

install security-pack version *version*

show package の出力で、**security-pack version** 番号の **Package-Vers** 値をコピーします。シャーシが ASA イメージをインストールして再起動します。

例 :

```

2110-pri /firmware # scope auto-install
2110-pri /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
- The platform version: 2.2.2.52
- The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
- upgrade to the new platform version 2.2.2.97
- upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-pri /firmware/auto-install #

```

- g) シャーシのリブートが完了するのを待ちます (5 ~ 10 分)。

FXOS が起動しても、ASA が稼働するまで (5分) 待機する必要があります。次のメッセージが表示されるまで待機します。

```

2110-pri#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.

```

[...]

アクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー ペアをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、FXOS CLI または FirePOWER シャーシマネージャを使用します。

Firepower Chassis Manager を使用したアクティブ/アクティブ フェールオーバー ペアのアップグレード

この項では、アクティブ/アクティブフェールオーバーペアの（ASA と ASDM の両方を含む）ASA バンドルをアップグレードする方法を説明します。管理コンピュータからパッケージをアップロードします。

手順

ステップ 1 プライマリ ユニットの両方のフェールオーバー グループをアクティブにします。

- フェールオーバー グループ 1 の管理アドレスに接続して、プライマリ ユニット（またはフェールオーバー グループ 1 がアクティブに設定されているユニット）で ASDM を起動します。
- [**モニタリング (Monitoring)**] > [**フェールオーバー (Failover)**] > [**フェールオーバー グループ 2 (Failover Group 2)**] の順に選択して、[**アクティブにする (Make Active)**] をクリックします。
- 後続の手順のために、このユニットの ASDM に接続したままにします。

ステップ 2 ASA の設定でデフォルト以外の ASDM イメージを以前に設定した場合は、イメージバンドルに付属のイメージにリセットします。

イメージバンドルには ASDM イメージが含まれていて、ASA バンドルをアップグレードすると、同じ名前 (**asdm.bin**) であるため、リロード後にバンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。アップロードした別の ASDM イメージ（たとえば **asdm-7191.bin**）を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のあるバージョンの ASDM が確実に実行されるようにするには、バンドルされている ASDM イメージを使用するように ASA を再設定する必要があります。

- プライマリユニットのメイン ASDM アプリケーションウィンドウで、[**設定 (Configuration)**] > [**デバイス管理 (Device Management)**] > [**システムイメージ/設定 (System Image/Configuration)**] > [**ブートイメージ/設定 (Boot Image/Configuration)**] を選択します。
- [**ASDM イメージファイルパス (ASDM Image File Path)**] に、**disk0:/asdm.bin** と入力します。
- [**適用 (Apply)**] をクリックします。
- コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。

ステップ 3 セカンダリ ユニットのアップグレードします。

- a) セカンダリ ユニットの Firepower Chassis Manager に接続します。
- b) **[System] > [Updates]** を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。
- c) **[Upload Image]** をクリックして管理コンピュータから新しいパッケージをアップロードします。
- d) **[Choose File]** をクリックして対象のファイルに移動し、アップロードするパッケージを選択します。
- e) **[Upload]** をクリックします。

選択したパッケージがシャーシにアップロードされます。[Upload Image] のダイアログボックスにアップロードの状況が表示されます。[Success] のダイアログボックスが表示されたら **[OK]** をクリックします。アップロードが完了すると、イメージの整合性が自動的に検証されます。

- f) 新しいパッケージの右側の **[Upgrade]** アイコンをクリックします。
- g) **[Yes]** をクリックして、インストールを続行することを確認します。

新しいパッケージが読み込まれていることを示すインジケータはありません。アップグレードプロセスの開始時には引き続き Firepower Chassis Manager が表示されます。システムのリブート時にログアウトされます。Firepower Chassis Manager にログインするには、システムのリブート完了を待つ必要があります。リブートプロセスには約 20 分かかります。リブート後、ログイン画面が表示されます。

ステップ 4 セカンダリ ユニットの両方のフェールオーバー グループをアクティブにします。プライマリユニットの ASDM で、**[Monitoring] > [Failover] > [Failover Group 1]** の順に選択して、**[Make Standby]** をクリックします。

ASDM は、セカンダリ ユニット上のフェールオーバー グループ 1 の IP アドレスに自動的に再接続されます。

ステップ 5 プライマリ ユニットのアップグレードします。

- a) プライマリ ユニットの Firepower Chassis Manager に接続します。
- b) **[System] > [Updates]** を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。
- c) **[Upload Image]** をクリックして管理コンピュータから新しいパッケージをアップロードします。
- d) **[Choose File]** をクリックして対象のファイルに移動し、アップロードするパッケージを選択します。
- e) **[Upload]** をクリックします。

選択したパッケージがシャーシにアップロードされます。[Upload Image] のダイアログボックスにアップロードの状況が表示されます。[Success] のダイアログボックスが表示されたら **[OK]** をクリックします。アップロードが完了すると、イメージの整合性が自動的に検証されます。

- f) 新しいパッケージの右側の **[Upgrade]** アイコンをクリックします。

- g) [Yes] をクリックして、インストールを続行することを確認します。

新しいパッケージが読み込まれていることを示すインジケータはありません。アップグレードプロセスの開始時には引き続き Firepower Chassis Manager が表示されます。システムのリブート時にログアウトされます。Firepower Chassis Manager にログインするには、システムのリブート完了を待つ必要があります。リブートプロセスには約 20 分かかります。リブート後、ログイン画面が表示されます。

- ステップ 6** フェールオーバーグループは、[Preempt Enabled] を使用して設定されると、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。[Preempt Enabled] でフェールオーバーグループが設定されていない場合は、[Monitoring] > [Failover] > [Failover Group #] ペインを使用して、指定された装置上でアクティブステータスに戻すことができます。

FXOS CLI を使用したアクティブ/アクティブ フェールオーバー ペアのアップグレード

この項では、アクティブ/アクティブフェールオーバーペアの（ASA と ASDM の両方を含む）ASA バンドルをアップグレードする方法を説明します。パッケージを FirePOWER 2100 シャーシにコピーするには、FTP、SCP、SFTP、または TFTP を使用できます。

手順

- ステップ 1** ASA の設定でデフォルト以外の ASDM イメージを以前に設定した場合は、イメージバンドルに付属のイメージにリセットします。

イメージバンドルには ASDM イメージが含まれていて、ASA バンドルをアップグレードすると、同じ名前 (**asdm.bin**) であるため、リロード後にバンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。アップロードした別の ASDM イメージ（たとえば **asdm-7191.bin**）を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のあるバージョンの ASDM が確実に実行されるようにするには、バンドルされている ASDM イメージを使用するように ASA を再設定する必要があります。

- a) コンソールポート（推奨）または SSH を使用して、プライマリユニットの FXOS CLI に接続します。
- b) ASA に接続します。

connect asa

例：

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

- c) 特権 EXEC モードにアクセスしてから、グローバル コンフィギュレーション モードにアクセスします。

enable

configure terminal

- d) ASDM イメージを設定します。

```
asdm image disk0:/asdm.bin
```

- e) 設定を保存します。

write memory

- f) **Ctrl+a**、**d** を押して、FXOS コンソールに戻ります。

ステップ 2 コンソール ポート（推奨）または SSH を使用して、セカンダリ ユニットの FXOS CLI に接続します。

ステップ 3 プライマリ ユニットの両方のフェールオーバー グループをアクティブにします。

- a) FXOS から ASA CLI に接続します。

connect asa**enable**

デフォルトで、イネーブルパスワードは空白です。

例：

```
2110-sec# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
asa/act/sec> enable
Password: <blank>
asa/act/sec#
```

- b) プライマリ ユニットの両方のフェールオーバー グループをアクティブにします。

no failover active group 1**no failover active group 2**

例：

```
asa/act/sec# no failover active group 1
asa/act/sec# no failover active group 2
```

- c) **Ctrl + a**、**d** を押下し、FXOS コンソールに戻ります。

ステップ 4 セカンダリ ユニットをアップグレードします。

- a) FXOS で、ファームウェア モードに入ります。

scope firmware

例：

```
2110-sec# scope firmware
2110-sec /firmware#
```

- b) パッケージをダウンロードします。

download image url

次のいずれかを使用してインポートするファイルの URL を指定します。

- **ftp://username@server/[path/]image_name**
- **scp://username@server/[path/]image_name**
- **sftp://username@server/[path/]image_name**
- **tftp://server[:port]/[path/]image_name**

例 :

```
2110-sec /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

- c) ダウンロードプロセスをモニターします。

show download-task

例 :

```
2110-sec /firmware # show download

Download task:
  File Name Protocol Server          Port      Userid      State
  -----
  cisco-asa-fp2k.9.8.2.SPA
    Tftp      10.88.29.181          0         0         Downloaded
  cisco-asa-fp2k.9.8.2.2.SPA
    Tftp      10.88.29.181          0         0         Downloading
2110-sec /firmware #
```

- d) 新しいパッケージのダウンロードが終了 ([Downloaded] の状態) したら、パッケージを起動します。新しいパッケージのバージョン番号を表示します。

show package

例 :

```
2110-sec /firmware # show package
Name                                     Package-Vers
-----
cisco-asa-fp2k.9.8.2.SPA                 9.8.2
cisco-asa-fp2k.9.8.2.2.SPA              9.8.2.2
2110-sec /firmware #
```

- e) パッケージをインストールします。

scope auto-install**install security-pack version version**

show package の出力で、**security-pack version** 番号の **Package-Vers** 値をコピーします。シャーンが ASA イメージをインストールして再起動します。

例 :

```
2110-sec /firmware # scope auto-install
2110-sec /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
- The platform version: 2.2.2.52
- The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
- upgrade to the new platform version 2.2.2.97
- upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-sec /firmware/auto-install #
```

- f) シャーシのリブートが完了するのを待ちます (5 ~ 10 分)。

FXOS が起動しても、ASA が稼働するまで (5分) 待機する必要があります。次のメッセージが表示されるまで待機します。

```
2110-sec#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[...]
```

ステップ 5 セカンダリ ユニットの両方のフェールオーバー グループをアクティブにします。

- a) FXOS から ASA CLI に接続します。

connect asa

enable

デフォルトで、イネーブルパスワードは空白です。

例 :

```
2110-sec# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
asa/stby/sec> enable
Password: <blank>
```



```
asa/stby/sec#
```

- b) セカンダリ ユニットの両方のフェールオーバー グループをアクティブにします。

```
failover active group 1
```

```
failover active group 2
```

例 :

```
asa/stby/sec# failover active group 1  
asa/act/sec# failover active group 2
```

- c) **Ctrl + a**、**d** を押下し、FXOS コンソールに戻ります。

ステップ 6 プライマリ ユニットのアップグレードします。

- a) コンソール ポート (推奨) または SSH を使用して、プライマリ ユニットの FXOS CLI に接続します。
- b) ファームウェア モードを入力します。

```
scope firmware
```

例 :

```
2110-pri# scope firmware  
2110-pri /firmware#
```

- c) パッケージをダウンロードします。

```
download image url
```

次のいずれかを使用してインポートするファイルの URL を指定します。

- **ftp://username@server/[path/]image_name**
- **scp://username@server/[path/]image_name**
- **sftp://username@server/[path/]image_name**
- **tftp://server[:port]/[path/]image_name**

例 :

```
2110-pri /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA  
Please use the command 'show download-task' or 'show download-task detail' to check  
download progress.
```

- d) ダウンロード プロセスをモニターします。

```
show download-task
```

例 :

```
2110-pri /firmware # show download  
  
Download task:
```

```

File Name Protocol Server          Port      Userid      State
-----
cisco-asa-fp2k.9.8.2.SPA
      Tftp      10.88.29.181          0          Downloaded
cisco-asa-fp2k.9.8.2.2.SPA
      Tftp      10.88.29.181          0          Downloading
2110-pri /firmware #

```

- e) 新しいパッケージのダウンロードが終了 ([Downloaded] の状態) したら、パッケージを起動します。新しいパッケージのバージョン番号を表示します。

show package

例 :

```

2110-pri /firmware # show package
Name                               Package-Vers
-----
cisco-asa-fp2k.9.8.2.SPA          9.8.2
cisco-asa-fp2k.9.8.2.2.SPA       9.8.2.2
2110-pri /firmware #

```

- f) パッケージをインストールします。

scope auto-install

install security-pack version *version*

show package の出力で、**security-pack version** 番号の **Package-Vers** 値をコピーします。シャーンシが ASA イメージをインストールして再起動します。

例 :

```

2110-pri /firmware # scope auto-install
2110-pri /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
- The platform version: 2.2.2.52
- The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
- upgrade to the new platform version 2.2.2.97
- upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-pri /firmware/auto-install #

```

- g) シャーンシのリポートが完了するのを待ちます (5 ~ 10 分)。

FXOS が起動しても、ASA が稼働するまで (5分) 待機する必要があります。次のメッセージが表示されるまで待機します。

```
2110-pri#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[...]
```

ステップ 7 フェールオーバー グループは、ASA **preempt** コマンドを使用して設定されている場合、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。フェールオーバーグループが **preempt** コマンドによって設定されていない場合は、ASA CLI に接続し、**failover active group** コマンドを使用して、指定された装置でそれらのステータスをアクティブに戻すことができます。

Firepower 4100/9300 のアップグレード

このドキュメントでは、Firepower 4100/9300 で ASA をアップグレードする方法について説明します。

FXOS および ASA スタンドアロン デバイスまたはシャーシ内クラスタのアップグレード

FXOS CLI または Firepower Chassis Manager を使用して、Firepower 9300 上の FXOS およびスタンドアロン ASA デバイスまたは ASA シャーシ内クラスタをアップグレードします。

Secure Firewall Chassis Manager を使用した FXOS および ASA スタンドアロンデバイスまたはシャーシ内クラスタのアップグレード

アップグレードプロセスは最大 45 分かかることがあります。アップグレード中、トラフィックはデバイスを通しません。適切なアップグレード活動の計画を行ってください。

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 および ASA ソフトウェアパッケージをダウンロードします。
- FXOS と ASA の構成をバックアップします。

手順

-
- ステップ 1** Secure Firewall シャーシマネージャ で、**[System] > [Updates]** を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。
- ステップ 2** 新しい FXOS プラットフォーム バンドルのイメージと ASA ソフトウェア イメージのアップロード：：
- [Upload Image] をクリックします。
 - [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シャーシにアップロードされます。
- ステップ 3** 新しい FXOS 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 **[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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。
- ステップ 4** [はい (Yes)] をクリックして、インストールを続行することを確認します。
- FXOS 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 ([アップグレード進行のモニター \(79 ページ\)](#) を参照してください)。
- 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、続行する前に、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 ([インストールの確認 \(80 ページ\)](#) を参照してください)。
- ステップ 7** [論理デバイス (Logical Devices)] を選択します。
[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。
- ステップ 8** アップグレードする各 ASA 論理デバイスごとに、以下を実行します。
- 更新する論理デバイスの **[Set Version]** アイコンをクリックして、**[Update Image Version]** ダイアログボックスを開きます。
 - [New Version] では、アップグレードしたいソフトウェア バージョンを選択します。
 - [OK] をクリックします。
- ステップ 9** アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。
- [論理デバイス (Logical Devices)] を選択します。
 - アプリケーションのバージョンと動作ステータスを確認します。
-

FXOS CLI を使用した FXOS および ASA スタンドアロン デバイスまたはシャーシ内クラスタのアップグレード

アップグレードプロセスは最大 45 分かかることがあります。アップグレード中、トラフィックはデバイスを通しません。適切なアップグレード活動の計画を行ってください。

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 および ASA ソフトウェアパッケージをダウンロードします。
- FXOS と ASA の構成をバックアップします。
- 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 モードを開始します。

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。

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

c) ダウンロード プロセスをモニターする場合 :

scope download-task image_name

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 # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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 新しい FXOS プラットフォームバンドルのイメージが正常にダウンロードされたら、FXOS バンドルをアップグレードします。

- a) 必要に応じて、ファームウェア モードに戻ります。

up

- b) 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をメモします。

show package

- c) auto-install モードにします。

scope auto-install

- d) FXOS プラットフォーム バンドルをインストールします。

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))。

- e) 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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

- f) 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。

FXOS 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。

- g) アップグレードプロセスをモニターするには、[アップグレード進行のモニター \(79 ページ\)](#) を参照してください。

ステップ 4 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、続行する前に、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（[インストールの確認 \(80 ページ\)](#) を参照してください）。

ステップ 5 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

- a) セキュリティ サービス モードを開始します。

top

scope ssa

- b) アプリケーション ソフトウェア モードを開始します。

scope app-software

- c) 論理デバイス ソフトウェア イメージをダウンロードします。

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@server/path**
- **scp://username@server/path**
- **sftp://username@server/path**
- **tftp://server:port-num/path**

- d) ダウンロード プロセスをモニターする場合：

show download-task

- e) ダウンロードしたアプリケーションを表示する場合：

up

show app

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

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 # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task
```

Downloads for Application Software:

File Name	Protocol	Server	Userid	State
cisco-asa.9.4.1.65.csp	Scp	192.168.1.1	user	Downloaded

```
Firepower-chassis /ssa/app-software # up
Firepower-chassis /ssa # show app

Application:
-----
Name          Version      Description Author      Deploy Type CSP Type      Is Default App
-----
asa           9.4.1.41    N/A
asa           9.4.1.65    N/A
Native       Application No
Native       Application Yes
```

ステップ 6 アップグレードする各 ASA 論理デバイスごとに、以下を実行します。

- a) セキュリティ サービス モードを開始します。

top

scope ssa

- b) スコープを更新するセキュリティ モジュールに設定します。

scope slotslot_number

- c) スコープを更新する ASA アプリケーションに設定します。

scope app-instance asa instance_name

- d) スタートアップ バージョンを新しい ASA ソフトウェアのバージョンに設定します。

set startup-version version_number

ステップ 7 設定を確定します。

commit-buffer

トランザクションをシステム設定にコミットします。アプリケーションイメージが更新され、アプリケーションが再起動します。

ステップ 8 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するには、[インストールの確認 \(80 ページ\)](#) を参照してください。

FXOS および ASA アクティブ/スタンバイ フェールオーバー ペアのアップグレード

FXOS CLI または Firepower Chassis Manager を使用して、FXOS および ASA アクティブ/スタンバイ フェールオーバー ペアをアップグレードします。

Secure Firewall Chassis Manager を使用した FXOS および ASA アクティブ/スタンバイ フェールオーバー ペアのアップグレード

アップグレード プロセスはシャーンごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

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。

- アクティブになっているユニットとスタンバイになっているユニットを確認する必要があります。ASDM をアクティブな ASA の IP アドレスに接続します。アクティブ装置は、常にアクティブな IP アドレスを保有しています。次に、[**モニタリング (Monitoring)**] > [**プロパティ (Properties)**] > [**フェールオーバー (Failover)**] > [**ステータス (Status)**] の順に選択して、このユニットの優先順位 (プライマリまたはセカンダリ) を表示し、接続先のユニットを確認できるようにします。
- アップグレード先の FXOS および ASA ソフトウェアパッケージをダウンロードします。
- FXOS と ASA 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 ASA 論理デバイスが含まれているシャーシでは、新しい FXOS プラットフォームバンドルイメージと ASA ソフトウェアイメージをアップロードします。
- a) Secure Firewall シャーシマネージャで、[**System**] > [**Updates**] を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。
 - b) [**Upload Image**] をクリックします。
 - c) [**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。
 - d) [**Upload**] をクリックします。
選択したイメージがシャーシにアップロードされます。
- ステップ 2** 新しい FXOS 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後に、スタンバイ ASA 論理デバイスが含まれているシャーシの FXOS バンドルをアップグレードします。
- a) アップグレードする FXOS プラットフォームバンドルの [**Upgrade**] アイコンをクリックします。

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。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。ASA パーティションが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。
 - b) [**はい (Yes)**] をクリックして、インストールを続行することを確認します。

FXOS 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 3** アップグレード中は Secure Firewall シャーシマネージャを使用できません。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 ([アップグレード進行のモニター \(79 ページ\)](#) を参照してください)。

- ステップ 4** 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、続行する前に、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（[インストールの確認（80 ページ）](#) を参照してください）。
- ステップ 5** ASA 論理デバイス イメージのアップグレード：
- [Logical Devices] を選択して [Logical Devices] ページを開きます。
[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。
 - 更新する論理デバイスの [Set Version] アイコンをクリックして、[Update Image Version] ダイアログボックスを開きます。
 - [New Version] では、更新後のソフトウェア バージョンを選択します。
 - [OK] をクリックします。
- ステップ 6** アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。
- [論理デバイス (Logical Devices)] を選択します。
 - アプリケーションのバージョンと動作ステータスを確認します。
- ステップ 7** 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。
- スタンバイ ASA IP アドレスに接続して、スタンバイ装置で ASDM を起動します。
 - [モニタリング (Monitoring)] > [プロパティ (Properties)] > [フェールオーバー (Failover)] > [ステータス (Status)] の順に選択し、[アクティブにする (Make Active)] をクリックして、スタンバイ装置を強制的にアクティブにします。
- ステップ 8** 新しいスタンバイ ASA 論理デバイスが含まれているシャーシでは、新しい FXOS プラットフォーム バンドル イメージと ASA ソフトウェア イメージをアップロードします。
- Secure Firewall シャーシマネージャ で、[System] > [Updates] を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。
 - [Upload Image] をクリックします。
 - [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シャーシにアップロードされます。
- ステップ 9** 新しい FXOS 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後に、新しいスタンバイ ASA 論理デバイスが含まれているシャーシの FXOS バンドルをアップグレードします。
- アップグレードする FXOS プラットフォーム バンドルの [Upgrade] アイコンをクリックします。

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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

- b) [はい (Yes)] をクリックして、インストールを続行することを確認します。

FXOS 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 10 アップグレード中は Secure Firewall シャーシマネージャ を使用できません。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 ([アップグレード進行のモニター \(79 ページ\)](#) を参照してください)。

ステップ 11 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、続行する前に、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 ([インストールの確認 \(80 ページ\)](#) を参照してください)。

ステップ 12 ASA 論理デバイス イメージのアップグレード:

- a) [論理デバイス (Logical Devices)] を選択します。
[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。論理デバイスが設定されていない場合は、これを通知するメッセージが代わりに表示されます。
- b) 更新する論理デバイスの [Set Version] アイコンをクリックして、[Update Image Version] ダイアログボックスを開きます。
- c) [New Version] では、更新後のソフトウェア バージョンを選択します。
- d) [OK] をクリックします。

ステップ 13 アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。

- a) [論理デバイス (Logical Devices)] を選択します。
- b) アプリケーションのバージョンと動作ステータスを確認します。

ステップ 14 (オプション) 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) スタンバイ ASA IP アドレスに接続して、スタンバイ装置で ASDM を起動します。
- b) [モニタリング (Monitoring)] > [プロパティ (Properties)] > [フェールオーバー (Failover)] > [ステータス (Status)] の順に選択し、[アクティブにする (Make Active)] をクリックして、スタンバイ装置を強制的にアクティブにします。

FXOS CLI を使用した FXOS および ASA アクティブ/スタンバイ フェールオーバー ペアのアップグレード

アップグレードプロセスはシャーシごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

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。

- どのユニットがアクティブで、どのユニットがスタンバイかを特定する必要があります。シャーシで ASA コンソールに接続し、**show failover** コマンドを入力してユニットのアクティブ/スタンバイステータスを表示します。

- アップグレード先の FXOS および ASA ソフトウェアパッケージをダウンロードします。
- FXOS と ASA の構成をバックアップします。
- 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 ASA 論理デバイスが含まれているシャーシでは、新しい FXOS プラットフォームバンドル イメージをダウンロードします。

- a) FXOS CLI に接続します。
- b) ファームウェア モードを開始します。

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。

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

- d) ダウンロードプロセスをモニターする場合 :

scope download-task image_name

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 # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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 2 新しいFXOSプラットフォームバンドルのイメージが正常にダウンロードされたら、FXOS バンドルをアップグレードします。

- a) 必要に応じて、ファームウェア モードに戻ります。

up

- b) 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をメモします。

show package

- c) auto-install モードにします。

scope auto-install

- d) FXOS プラットフォーム バンドルをインストールします。

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))。

- e) 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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

- f) 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。

FXOS 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。

- g) アップグレードプロセスをモニターするには、[アップグレード進行のモニター \(79 ページ\)](#) を参照してください。

ステップ 3 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、続行する前に、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 ([インストールの確認 \(80 ページ\)](#) を参照してください)。

ステップ 4 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

- a) セキュリティ サービス モードを開始します。

top

scope ssa

- b) アプリケーション ソフトウェア モードを開始します。

scope app-software

- c) 論理デバイス ソフトウェア イメージをダウンロードします。

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@server/path**
- **scp://username@server/path**
- **sftp://username@server/path**
- **tftp://server:port-num/path**

- d) ダウンロードプロセスをモニターする場合 :

show download-task

- e) ダウンロードしたアプリケーションを表示する場合 :

up

show app

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

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 # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task
```

```
Downloads for Application Software:
```

File Name	Protocol	Server	Userid	State
cisco-asa.9.4.1.65.csp	Scp	192.168.1.1	user	Downloaded

```
Firepower-chassis /ssa/app-software # up
Firepower-chassis /ssa # show app
```

```
Application:
```

Name	Version	Description	Author	Deploy Type	CSP Type	Is Default	App
asa	9.4.1.41	N/A		Native	Application	No	
asa	9.4.1.65	N/A		Native	Application	Yes	

ステップ 5 ASA 論理デバイス イメージのアップグレード :

- a) セキュリティ サービス モードを開始します。

top

scope ssa

- b) スコープを更新するセキュリティ モジュールに設定します。

scope slots*slot_number*

- c) スコープを更新する ASA アプリケーションに設定します。

scope app-instance asa *instance_name*

- d) スタートアップ バージョンを更新するバージョンに設定します。

set startup-version *version_number*

- e) 設定を確定します。

commit-buffer

トランザクションをシステム設定にコミットします。アプリケーションイメージが更新され、アプリケーションが再起動します。

ステップ 6 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するには、[インストールの確認 \(80 ページ\)](#) を参照してください。

ステップ 7 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) スタンバイ ASA 論理デバイスが含まれるシャーシで、コンソール接続または Telnet 接続を使用してモジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

例 :

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```

```
CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>
```

- b) アプリケーションのコンソールに接続します。

connect asa

例 :

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>
```

- c) この装置をアクティブにします。

failover active

- d) 設定を保存します。

write memory

- e) ユニットがアクティブであることを確認します。

show failover

ステップ 8 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

Ctrl-a, d と入力します。

ステップ 9 FXOS CLI のスーパーバイザ レベルに戻ります。

コンソールを終了します。

- a) ~ と入力

Telnet アプリケーションに切り替わります。

- b) Telnet アプリケーションを終了するには、次を入力します。

telnet>quit

Telnet セッションを終了します。

- a) **Ctrl-], .** と入力

ステップ 10 新しいスタンバイ ASA 論理デバイスが含まれているシャーシでは、新しい FXOS プラットフォーム バンドル イメージをダウンロードします。

- a) FXOS CLI に接続します。

- b) ファームウェア モードを開始します。

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。

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@server/path/image_name**

• **scp://username@server/path/image_name**

• **sftp://username@server/path/image_name**

• **tftp://server:port-num/path/image_name**

- d) ダウンロードプロセスをモニターする場合 :

scope download-task image_name

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 # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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 11 新しいFXOS プラットフォーム バンドルのイメージが正常にダウンロードされたら、FXOS バンドルをアップグレードします。

a) 必要に応じて、ファームウェア モードに戻ります。

up

b) 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をメモします。

show package

c) auto-install モードにします。

scope auto-install

d) FXOS プラットフォーム バンドルをインストールします。

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))。

e) 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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

f) 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。

FXOS 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。

g) アップグレードプロセスをモニターするには、[アップグレード進行のモニター \(79 ページ\)](#) を参照してください。

ステップ 12 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、続行する前に、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（[インストールの確認（80 ページ）](#) を参照してください）。

ステップ 13 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

a) セキュリティ サービス モードを開始します。

```
top
```

```
scope ssa
```

b) アプリケーション ソフトウェア モードを開始します。

```
scope app-software
```

c) 論理デバイス ソフトウェア イメージをダウンロードします。

```
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@server/path`

- `scp://username@server/path`

- `sftp://username@server/path`

- `tftp://server:port-num/path`

d) ダウンロードプロセスをモニターする場合：

```
show download-task
```

e) ダウンロードしたアプリケーションを表示する場合：

```
up
```

```
show app
```

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

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 # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task
```

```
Downloads for Application Software:
```

File Name	Protocol	Server	Userid	State
cisco-asa.9.4.1.65.csp	Scp	192.168.1.1	user	Downloaded

```
Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
-----
Name          Version      Description Author      Deploy Type CSP Type      Is Default App
-----
asa           9.4.1.41    N/A
asa           9.4.1.65    N/A
Native       Application No
Native       Application Yes
```

ステップ 14 ASA 論理デバイス イメージのアップグレード:

- a) セキュリティ サービス モードを開始します。

top

scope ssa

- b) スコープを更新するセキュリティ モジュールに設定します。

scope slotslot_number

- c) スコープを更新する ASA アプリケーションに設定します。

scope app-instance asa instance_name

- d) スタートアップ バージョンを更新するバージョンに設定します。

set startup-version version_number

- e) 設定を確定します。

commit-buffer

トランザクションをシステム設定にコミットします。アプリケーションイメージが更新され、アプリケーションが再起動します。

ステップ 15 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するには、[インストールの確認 \(80 ページ\)](#) を参照してください。

ステップ 16 (オプション) 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) スタンバイ ASA 論理デバイスが含まれるシャーシで、コンソール接続または Telnet 接続を使用してモジュール CLI に接続します。

connect module slot_number {console | telnet}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

例:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```

```
CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

- b) アプリケーションのコンソールに接続します。

connect asa

例 :

```
Firepower-module1> connect asa
Connecting to asa(asal) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>
```

- c) この装置をアクティブにします。

failover active

- d) 設定を保存します。

write memory

- e) ユニットがアクティブであることを確認します。

show failover

FXOS および ASA アクティブ/アクティブ フェールオーバー ペアのアップグレード

FXOS CLI または Firepower Chassis Manager を使用して、FXOS および ASA アクティブ/アクティブ フェールオーバー ペアをアップグレードします。

Secure Firewall Chassis Manager を使用した FXOS および ASA アクティブ/アクティブ フェールオーバー ペアのアップグレード

アップグレードプロセスはシャーンごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

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。

- どのユニットがプライマリ ユニットか特定する必要があります。ASDM に接続し、**[Monitoring] > [Properties] > [Failover] > [Status]** の順に選択して、このユニットの優先順位 (プライマリまたはセカンダリ) を表示し、接続先のユニットを確認できるようにします。
- アップグレード先の FXOS および ASA ソフトウェアパッケージをダウンロードします。

- FXOS と ASA の構成をバックアップします。

手順

- ステップ 1** プライマリ ユニットの両方のフェールオーバー グループをアクティブにします。
- フェールオーバー グループ 1 の管理アドレスに接続して、プライマリ ユニット（またはフェールオーバー グループ 1 がアクティブに設定されているユニット）で ASDM を起動します。
 - [**モニタリング (Monitoring)**] > [**フェールオーバー (Failover)**] > [**フェールオーバー グループ 2 (Failover Group 2)**] の順に選択して、[**アクティブにする (Make Active)**] をクリックします。
 - 後続の手順のために、このユニットの ASDM に接続したままにします。
- ステップ 2** セカンダリ ASA 論理デバイスが含まれているシャーシでは、新しい FXOS プラットフォームバンドル イメージと ASA ソフトウェア イメージをアップロードします。
- セカンダリユニットの Secure Firewall Chassis Manager に接続します。
 - [**システム (System)**] > [**更新 (Updates)**] を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。
 - [**Upload Image**] をクリックします。
 - [**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シャーシにアップロードされます。
- ステップ 3** 新しい FXOS 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後に、セカンダリ ASA 論理デバイスが含まれているシャーシの FXOS バンドルをアップグレードします。
- アップグレードする FXOS プラットフォームバンドルの [**Upgrade**] アイコンをクリックします。

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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。
 - [**はい (Yes)**] をクリックして、インストールを続行することを確認します。

FXOS 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 4** アップグレード中は Secure Firewall Chassis Manager を使用できません。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 ([アップグレード進行のモニター \(79 ページ\)](#) を参照してください)。

- ステップ 5** 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、続行する前に、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（[インストールの確認（80 ページ）](#) を参照してください）。
- ステップ 6** ASA 論理デバイス イメージのアップグレード：
- [論理デバイス (Logical Devices)] を選択します。
[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。
 - 更新する論理デバイスの [Set Version] アイコンをクリックして、[Update Image Version] ダイアログボックスを開きます。
 - [New Version] では、更新後のソフトウェア バージョンを選択します。
 - [OK] をクリックします。
- ステップ 7** アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。
- [論理デバイス (Logical Devices)] を選択します。
 - アプリケーションのバージョンと動作ステータスを確認します。
- ステップ 8** セカンダリ ユニットの両方のフェールオーバー グループをアクティブにします。
- フェールオーバー グループ 1 の管理アドレスに接続して、プライマリ ユニット（またはフェールオーバー グループ 1 がアクティブに設定されているユニット）で ASDM を起動します。
 - [Monitoring] > [Failover] > [Failover Group 1] の順に選択して、[Make Standby] をクリックします。
 - [Monitoring] > [Failover] > [Failover Group 2] の順に選択して、[Make Standby] をクリックします。
- ASDM は、セカンダリ ユニット上のフェールオーバー グループ 1 の IP アドレスに自動的に再接続されます。
- ステップ 9** プライマリ ASA 論理デバイスが含まれているシャーシでは、新しい FXOS プラットフォーム バンドル イメージと ASA ソフトウェア イメージをアップロードします。
- プライマリ ユニットの Secure Firewall Chassis Manager に接続します。
 - [システム (System)] > [更新 (Updates)] を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。
 - [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。
選択したパッケージが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ー 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ー契約書に同意します。
- ステップ 10** 新しい FXOS 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後に、プライマリ ASA 論理デバイスが含まれているシャーシの FXOS バンドルをアップグレードします。

- a) アップグレードする FXOS プラットフォーム バンドルの [Upgrade] アイコンをクリックします。

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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

- b) [はい (Yes)] をクリックして、インストールを続行することを確認します。

FXOS 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 11 アップグレード中は Secure Firewall Chassis Manager を使用できません。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 ([アップグレード進行のモニター \(79 ページ\)](#) を参照してください)。

ステップ 12 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、続行する前に、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 ([インストールの確認 \(80 ページ\)](#) を参照してください)。

ステップ 13 ASA 論理デバイス イメージのアップグレード:

- a) [論理デバイス (Logical Devices)] を選択します。
[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。
- b) 更新する論理デバイスの [Set Version] アイコンをクリックして、[Update Image Version] ダイアログボックスを開きます。
- c) [New Version] では、更新後のソフトウェア バージョンを選択します。
- d) [OK] をクリックします。

ステップ 14 アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。

- a) [論理デバイス (Logical Devices)] を選択します。
- b) アプリケーションのバージョンと動作ステータスを確認します。

ステップ 15 フェールオーバー グループは、[Preempt Enabled] を使用して設定されると、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。[Preempt Enabled] でフェールオーバー グループが設定されていない場合は、[Monitoring] > [Failover] > [Failover Group #] ペインを使用して、指定された装置上でアクティブ ステータスに戻すことができます。

FXOS CLI を使用した FXOS および ASA アクティブ/アクティブ フェールオーバー ペアのアップグレード

アップグレードプロセスはシャーシごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

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。

- どのユニットがプライマリかを特定する必要があります。シャーシで ASA コンソールに接続し、**show failover** コマンドを入力してユニットの状態と優先順位（プライマリまたはセカンダリ）を表示します。
- アップグレード先の FXOS および ASA ソフトウェアパッケージをダウンロードします。
- FXOS と ASA の構成をバックアップします。
- 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 コンソール ポート（推奨）または SSH を使用して、セカンダリ ユニットの FXOS CLI に接続します。

ステップ 2 プライマリ ユニットの両方のフェールオーバー グループをアクティブにします。

a) コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

connect module slot_number { console | telnet }

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```

```
CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>
```

b) アプリケーションのコンソールに接続します。

connect asa

例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D to return to bootCLI
[...]
```



```
asa>
```

- c) プライマリ ユニットの両方のフェールオーバー グループをアクティブにします。

enable

デフォルトで、イネーブルパスワードは空白です。

no failover active group 1

no failover active group 2

例 :

```
asa> enable
Password: <blank>
asa# no failover active group 1
asa# no failover active group 2
```

- ステップ 3** アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

Ctrl-a, d と入力します。

- ステップ 4** FXOS CLI のスーパーバイザ レベルに戻ります。

コンソールを終了します。

- a) ~ と入力

Telnet アプリケーションに切り替わります。

- b) Telnet アプリケーションを終了するには、次を入力します。

```
telnet>quit
```

Telnet セッションを終了します。

- a) **Ctrl-], .** と入力

- ステップ 5** セカンダリ ASA 論理デバイスが含まれているシャーシでは、新しい FXOS プラットフォームバンドルイメージと ASA ソフトウェアイメージをダウンロードします。

- a) FXOS CLI に接続します。

- b) ファームウェア モードを開始します。

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。

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

- d) ダウンロードプロセスをモニターする場合：

```
scope download-task image_name
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 # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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 6 新しいFXOS プラットフォームバンドルのイメージが正常にダウンロードされたら、FXOS バンドルをアップグレードします。

- a) 必要に応じて、ファームウェア モードに戻ります。

```
top
scope firmware
```

- b) 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をメモします。

```
show package
```

- c) auto-install モードにします。

```
scope auto-install
```

- d) FXOS プラットフォーム バンドルをインストールします。

```
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))。

- e) 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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

- f) 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。

FXOS 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。

- g) アップグレードプロセスをモニターするには、[アップグレード進行のモニター \(79 ページ\)](#) を参照してください。

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、続行する前に、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 ([インストールの確認 \(80 ページ\)](#) を参照してください)。

ステップ 8 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

- a) セキュリティ サービス モードを開始します。

top

scope ssa

- b) アプリケーション ソフトウェア モードを開始します。

scope app-software

- c) 論理デバイス ソフトウェア イメージをダウンロードします。

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@server/path**
- **scp://username@server/path**
- **sftp://username@server/path**
- **tftp://server:port-num/path**

- d) ダウンロード プロセスをモニターする場合 :

show download-task

- e) ダウンロードしたアプリケーションを表示する場合 :

up

show app

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

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 # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
```

```

Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
  File Name                Protocol  Server                Userid                State
-----
  cisco-asa.9.4.1.65.csp    Scp       192.168.1.1          user
Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
  Name      Version  Description Author      Deploy Type  CSP Type  Is Default App
-----
  asa       9.4.1.41  N/A                Native      Application No
  asa       9.4.1.65  N/A                Native      Application Yes

```

ステップ 9 ASA 論理デバイス イメージのアップグレード:

- a) セキュリティ サービス モードを開始します。

top

scope ssa

- b) スコープを更新するセキュリティ モジュールに設定します。

scope slotslot_number

- c) スコープを更新する ASA アプリケーションに設定します。

scope app-instance asa instance_name

- d) スタートアップ バージョンを更新するバージョンに設定します。

set startup-version version_number

- e) 設定を確定します。

commit-buffer

トランザクションをシステム設定にコミットします。アプリケーションイメージが更新され、アプリケーションが再起動します。

ステップ 10 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するには、[インストールの確認 \(80 ページ\)](#) を参照してください。

ステップ 11 セカンダリ ユニットの両方のフェールオーバー グループをアクティブにします。

- a) コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

connect module slot_number {console | telnet}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

例:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

- b) アプリケーションのコンソールに接続します。

connect asa

例 :

```
Firepower-module1> connect asa
Connecting to asa(asal) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>
```

- c) セカンダリ ユニットの両方のフェールオーバー グループをアクティブにします。

enable

デフォルトで、イネーブルパスワードは空白です。

failover active group 1

failover active group 2

例 :

```
asa> enable
Password: <blank>
asa# failover active group 1
asa# failover active group 2
```

ステップ 12 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

Ctrl-a, d と入力します。

ステップ 13 FXOS CLI のスーパーバイザ レベルに戻ります。

コンソールを終了します。

- a) ~ と入力

Telnet アプリケーションに切り替わります。

- b) Telnet アプリケーションを終了するには、次を入力します。

```
telnet>quit
```

Telnet セッションを終了します。

- a) **Ctrl-], .** と入力

ステップ 14 プライマリ ASA 論理デバイスが含まれているシャーシでは、新しい FXOS プラットフォームバンドル イメージと ASA ソフトウェア イメージをダウンロードします。

- a) FXOS CLI に接続します。
- b) ファームウェア モードを開始します。

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。

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

- d) ダウンロードプロセスをモニターする場合 :

scope download-task image_name

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 # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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 15 新しい FXOS プラットフォームバンドルのイメージが正常にダウンロードされたら、FXOS バンドルをアップグレードします。

- a) 必要に応じて、ファームウェア モードに戻ります。

up

- b) 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をメモします。

show package

- c) auto-install モードにします。

scope auto-install

- d) FXOS プラットフォーム バンドルをインストールします。

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))。

- e) 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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

- f) 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。

FXOS 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。

- g) アップグレードプロセスをモニターするには、[アップグレード進行のモニター \(79 ページ\)](#) を参照してください。

ステップ 16 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、続行する前に、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 ([インストールの確認 \(80 ページ\)](#) を参照してください)。

ステップ 17 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

- a) セキュリティ サービス モードを開始します。

top

scope ssa

- b) アプリケーション ソフトウェア モードを開始します。

scope app-software

- c) 論理デバイス ソフトウェア イメージをダウンロードします。

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@server/path**
- **scp://username@server/path**
- **sftp://username@server/path**
- **tftp://server:port-num/path**

- d) ダウンロード プロセスをモニターする場合 :

show download-task

- e) ダウンロードしたアプリケーションを表示する場合：

up

show app

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

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 # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task
```

Downloads for Application Software:				
File Name	Protocol	Server	Userid	State
cisco-asa.9.4.1.65.csp	Scp	192.168.1.1	user	Downloaded

```
Firepower-chassis /ssa/app-software # up
Firepower-chassis /ssa # show app
```

Application:							
Name	Version	Description	Author	Deploy Type	CSP Type	Is Default	App
asa	9.4.1.41	N/A		Native	Application	No	
asa	9.4.1.65	N/A		Native	Application	Yes	

ステップ 18 ASA 論理デバイス イメージのアップグレード：

- a) セキュリティ サービス モードを開始します。

top

scope ssa

- b) スコープを更新するセキュリティ モジュールに設定します。

scope slotslot_number

- c) スコープを更新する ASA アプリケーションに設定します。

scope app-instance asa instance_name

- d) スタートアップ バージョンを更新するバージョンに設定します。

set startup-version version_number

- e) 設定を確定します。

commit-buffer

トランザクションをシステム設定にコミットします。アプリケーションイメージが更新され、アプリケーションが再起動します。

- ステップ 19** 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するには、[インストールの確認 \(80 ページ\)](#) を参照してください。
- ステップ 20** フェールオーバー グループは、[Preempt Enabled] を使用して設定されると、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。[Preempt Enabled] でフェールオーバー グループが設定されていない場合は、[Monitoring] > [Failover] > [Failover Group #] ペインを使用して、指定された装置上でアクティブ ステータスに戻すことができます。

FXOS および ASA シャーシ間クラスタのアップグレード

FXOS CLI または Firepower Chassis Manager を使用して、シャーシ間クラスタ内のすべてのシャーシの FXOS と ASA をアップグレードします。

Secure Firewall Chassis Manager を使用した FXOS および ASA シャーシ間クラスタのアップグレード

アップグレードプロセスはシャーシごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

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 および ASA ソフトウェアパッケージをダウンロードします。
- FXOS と ASA の構成をバックアップします。

手順

- ステップ 1** どのシャーシに制御ノードがあるかを決定します。このシャーシは最後にアップグレードします。
- a) Secure Firewall シャーシマネージャ に接続します。
 - b) [論理デバイス (Logical Devices)] を選択します。
 - c) クラスタに含まれるセキュリティ モジュールの属性を表示するには、プラス記号 (+) をクリックします。
 - d) 制御ノードがこのシャーシ上にあることを確認します。 **CLUSTER-ROLE** が "Control" に設定されている ASA インスタンスがあるはずです。
- ステップ 2** 制御ノードがないクラスタ内のシャーシの Secure Firewall シャーシマネージャ に接続します。
- ステップ 3** 新しい FXOS プラットフォーム バンドルのイメージと ASA ソフトウェア イメージのアップロード:

- a) Secure Firewall シャーシマネージャ で、[システム (System)] > [更新 (Updates)] を選択します。
[Available Updates] の画面に、シャーシで使用可能なパッケージのリストが表示されます。
- b) [Upload Image] をクリックします。
- c) [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。
- d) [Upload] をクリックします。
選択したイメージがシャーシにアップロードされます。
- e) 続行する前に、イメージが正常にアップロードされるまで待ちます。

ステップ 4 FXOS バンドルのアップグレード :

- a) [System] > [Updates] を選択します。
- b) アップグレードする FXOS プラットフォーム バンドルの [Upgrade] アイコンをクリックします。

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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。
- c) [はい (Yes)] をクリックして、インストールを続行することを確認します。
FXOS 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 アップグレード中は Secure Firewall シャーシマネージャ を使用できません。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 ([アップグレード進行のモニター \(79 ページ\)](#) を参照してください)。

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、続行する前に、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 ([インストールの確認 \(80 ページ\)](#) を参照してください)。

ステップ 7 各セキュリティモジュールでの ASA 論理デバイス イメージのアップグレード :

- a) [論理デバイス (Logical Devices)] を選択します。
[Logical Devices] ページに、シャーシに設定された論理デバイスのリストが表示されます。
- b) 更新する論理デバイスの [Set Version] アイコンをクリックして、[Update Image Version] ダイアログボックスを開きます。
- c) [New Version] では、更新後のソフトウェア バージョンを選択します。
- d) [OK] をクリックします。

ステップ 8 アップグレードプロセスが完了したら、アプリケーションがオンラインであり、正常にアップグレードされたことを確認します。

- a) [論理デバイス (Logical Devices)] を選択します。
- b) アプリケーションのバージョンと動作ステータスを確認します。

- ステップ 9** 制御ノードがないクラスタ内の残りのすべてのシャーシで、手順 [ステップ 2 \(73 ページ\)](#) ～ [ステップ 8 \(74 ページ\)](#) を繰り返します。
- ステップ 10** 制御ノードがないクラスタ内のすべてのシャーシをアップグレードしたら、**制御ノードがある** シャーシで手順 [ステップ 2 \(73 ページ\)](#) ～ [ステップ 8 \(74 ページ\)](#) を繰り返します。新しい制御ノードが、以前にアップグレードされたシャーシのいずれかから選択されます。
- ステップ 11** 分散型 VPN クラスタリングモードでは、クラスタが安定したら、制御ノードで ASA コンソールを使用して、クラスタ内のすべてのモジュール間でアクティブセッションを再配布することができます。

```
cluster redistribute vpn-sessiondb
```

次のタスク

シャーシのサイト ID を設定します。シャーシのサイト ID を設定する方法の詳細については、Cisco.com で『Deploying a Cluster for ASA for the Firepower 4100/9300 for Scalability and High Availability』の「Inter-Site Clustering」トピックを参照してください。

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

アップグレードプロセスはシャーシごとに最大 45 分かかることがあります。適切なアップグレード活動の計画を行ってください。

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 および ASA ソフトウェアパッケージをダウンロードします。
- FXOS と ASA の構成をバックアップします。
- 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** どのシャーシに制御ノードがあるかを決定します。このシャーシは最後にアップグレードします。
- a) FXOS CLI に接続します。
 - b) 制御ノードがこのシャーシ上にあることを確認します。Cluster Role が "Control" に設定されている ASA インスタンスがあるはずです。

```
scope ssa
```

show app-instance

ステップ 2 制御ノードがないクラスタ内のシャーシの FXOS CLI に接続します。

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

a) ファームウェア モードを開始します。

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。

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

c) ダウンロードプロセスをモニターする場合 :

scope download-task image_name**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 # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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 FXOS バンドルをアップグレードします。

a) 必要に応じて、ファームウェア モードに戻ります。

top**scope firmware**

b) 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をメモします。

show package

- c) auto-install モードにします。

scope auto-install

- d) FXOS プラットフォーム バンドルをインストールします。

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))。

- e) 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。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。ASA バージョンが互換性テーブルにアップグレード可能としてリストされている限り、これらの警告を無視できます。

yes を入力して、検証に進むことを確認します。

- f) 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。

FXOS 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。

- g) アップグレードプロセスをモニターするには、[アップグレード進行のモニター \(79 ページ\)](#) を参照してください。

ステップ 5 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、続行する前に、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 ([インストールの確認 \(80 ページ\)](#) を参照してください)。

ステップ 6 シャーシに新しい ASA ソフトウェア イメージをダウンロードします。

- a) セキュリティ サービス モードを開始します。

top

scope ssa

- b) アプリケーション ソフトウェア モードを開始します。

scope app-software

- c) 論理デバイス ソフトウェア イメージをダウンロードします。

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@server/path**
- **scp://username@server/path**
- **sftp://username@server/path**
- **tftp://server:port-num/path**

- d) ダウンロード プロセスをモニターする場合 :

show download-task

- e) ダウンロードしたアプリケーションを表示する場合：

up

show app

ダウンロードしたソフトウェアパッケージの ASA のバージョンをメモします。後の手順でアプリケーションを有効にするために、正確なバージョン文字列を使用する必要があります。

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 # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task
```

Downloads for Application Software:				
File Name	Protocol	Server	Userid	State
cisco-asa.9.4.1.65.csp	Scp	192.168.1.1	user	Downloaded

```
Firepower-chassis /ssa/app-software # up
Firepower-chassis /ssa # show app
```

Application:						
Name	Version	Description	Author	Deploy Type	CSP Type	Is Default App
asa	9.4.1.41	N/A		Native	Application	No
asa	9.4.1.65	N/A		Native	Application	Yes

ステップ 7 ASA 論理デバイス イメージのアップグレード：

- a) セキュリティ サービス モードを開始します。

top

scope ssa

- b) スコープを更新するセキュリティ モジュールに設定します。

scope slotslot_number

- c) スコープを更新する ASA アプリケーションに設定します。

scope app-instance asa instance_name

- d) スタートアップ バージョンを更新するバージョンに設定します。

set startup-version version_number

- e) 設定を確定します。

commit-buffer

トランザクションをシステム設定にコミットします。アプリケーションイメージが更新され、アプリケーションが再起動します。

- ステップ 8 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するには、[インストールの確認 \(80 ページ\)](#) を参照してください。
- ステップ 9 制御ノードがないクラスタ内の残りのすべてのシャーシで、手順 [ステップ 2 \(76 ページ\)](#) ~ [ステップ 8 \(79 ページ\)](#) を繰り返します。
- ステップ 10 制御ノードがないクラスタ内のすべてのシャーシをアップグレードしたら、**制御ノードがある** シャーシで手順 [ステップ 2 \(76 ページ\)](#) ~ [ステップ 8 \(79 ページ\)](#) を繰り返します。新しい制御ノードが、以前にアップグレードされたシャーシのいずれかから選択されます。
- ステップ 11 分散型 VPN クラスタリングモードでは、クラスタが安定したら、制御ノードで ASA コンソールを使用して、クラスタ内のすべてのモジュール間でアクティブセッションを再配布することができます。

cluster redistribute vpn-sessiondb

次のタスク

シャーシのサイト ID を設定します。シャーシのサイト ID を設定する方法の詳細については、Cisco.com で『Deploying a Cluster for ASA for the Firepower 4100/9300 for Scalability and High Availability』の「Inter-Site Clustering」トピックを参照してください。

アップグレード進行のモニター

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。

手順

- ステップ 1 FXOS CLI に接続します。
- ステップ 2 **scope system** を入力します。
- ステップ 3 **show firmware monitor** を入力します。
- ステップ 4 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

```

Firepower-chassis# scope system
Firepower-chassis /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

```

インストールの確認

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。

手順

ステップ 1 FXOS CLI に接続します。

ステップ 2 **top** を入力します。

ステップ 3 **scope ssa** を入力します。

ステップ 4 **show slot** を入力します。

ステップ 5 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。

例：

ステップ 6 **show app-instance** を入力します。

ステップ 7 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」であり、正しいバージョンがリストされていることを確認します。

このシャーシがクラスタの一部である場合、シャーシ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で、クラスタ動作状態が「In-Cluster」であることを確認します。また、制御ユニットがアップグレードするシャーシ上にないことを確認します。Cluster Role が「Master」に設定されているインスタンスがあってはなりません。

例

```

Firepower-chassis# scope ssa
Firepower-chassis /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
Firepower-chassis /ssa #
Firepower-chassis /ssa # show app-instance
App Name      Identifier Slot ID      Admin State Oper State      Running Version Startup
Version Cluster State Cluster Role
-----
asa           asal      1           Enabled      Online          9.10.0.85      9.10.0.85
              Not Applicable None
asa           asa2      2           Enabled      Online          9.10.0.85      9.10.0.85
              Not Applicable None
Firepower-chassis /ssa #

```

ASA 5500-X、ASA Virtual、ASASM、ISA 3000 のアップグレード

このドキュメントでは、スタンドアロン、フェールオーバー、またはクラスタリング導入用に ASA 5500-X、ASA Virtual、ASASM、または ISA 3000 の ASA および ASDM アップグレードを計画し、実装する方法について説明します。

スタンドアロンユニットのアップグレード

スタンドアロンユニットをアップグレードするには CLI または ASDM を使用します。

CLI を使用したスタンドアロンユニットのアップグレード

ここでは、ASDM イメージおよび ASA イメージをインストールする方法について説明します。また、ASA FirePower モジュールをアップグレードするタイミングについても説明します。

始める前に

この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバー タイプについては、『[ASA Command Reference](#)』の `copy` コマンドを参照してください。

手順

ステップ 1 特権 EXEC モードで、ASA ソフトウェアをフラッシュメモリにコピーします。

```
copy ftp://[[user[:password]]@]server[/path]/asa_image_name diskn:[/path]/asa_image_name
```

例 :

```
ciscoasa# copy ftp://jcrichon:aeryn@10.1.1.1/asa-9-12-1-smp-k8.bin
disk0:/asa-9-12-1-smp-k8.bin
```

ステップ 2 ASDM イメージをフラッシュメモリにコピーします。

```
copy ftp://[[user[:password]]@]server[/path]/asdm_image_name diskn:[/path]/asdm_image_name
```

例 :

```
ciscoasa# copy ftp://jcrichon:aeryn@10.1.1.1/asdm-7121.bin disk0:/asdm-7121.bin
```

ステップ 3 グローバル コンフィギュレーション モードにアクセスします。

```
configure terminal
```

例 :

```
ciscoasa# configure terminal
ciscoasa(config)#
```

ステップ 4 設定されている現在のブート イメージを表示します (最大 4 個)。

```
show running-config boot system
```

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。

例 :

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ステップ 5 既存のブートイメージコンフィギュレーションがある場合は削除します。新しいブートイメージを最初の選択肢として入力できるようにするためです。

```
no boot system diskn:[/path]/asa_image_name
```

例 :

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa931-smp-k8.bin
```

ステップ 6 ブートする ASA イメージを設定します (先ほどアップロードしたもの)。

```
boot system diskn:[/path]/asa_image_name
```

このイメージが使用できない場合に使用するバックアップイメージに対して、このコマンドを繰り返します。たとえば、先ほど削除したイメージを再入力できます。

例：

```
ciscoasa(config)# boot system disk0:/asa-9-12-1-smp-k8.bin
```

ステップ 7 使用する ASDM イメージを設定します（先ほどアップロードしたもの）。

asdm image disk:[/path/]asdm_image_name

使用するよう設定できる ASDM イメージは1つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

例：

```
ciscoasa(config)# asdm image disk0:/asdm-7121.bin
```

ステップ 8 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

ステップ 9 ASA をリロードします。

reload

ステップ 10 ASA FirePOWER モジュールをアップグレードする場合は、ASA REST API を無効にします。無効にしない場合アップグレードは失敗します。

no rest-api agent

次のコマンドを実行して、アップグレード後に REST API を再度有効にすることができます。

rest-api agent

(注) FirePOWER モジュールのバージョン 6.0 以降を実行している場合、ASA 5506-X シリーズは ASA の REST API をサポートしません。

ステップ 11 ASA FirePOWER モジュールをアップグレードします。

ASDM を使用したローカルコンピュータからのスタンドアロンユニットのアップグレード

Upgrade Software from Local Computer ツールにより、コンピュータからフラッシュファイルシステムにイメージファイルをアップロードし、ASA をアップグレードできます。

手順

ステップ 1 メイン ASDM アプリケーションウィンドウで、[Tools]>[Upgrade Software from Local Computer]の順に選択します。

[Upgrade Software] ダイアログボックスが表示されます。

- ステップ 2** [アップロードするイメージ (Image to Upload)] ドロップダウン リストから、[ASDM] を選択します。
- ステップ 3** [Local File Path] フィールドで [Browse Local Files] をクリックして PC 上のファイルを見つけます。
- ステップ 4** [Flash File System Path] フィールドで [Browse Flash] をクリックしてフラッシュ ファイルシステム上のディレクトリまたはファイルを見つけます。
- ステップ 5** [イメージのアップロード (Upload Image)] をクリックします。
アップグレード プロセスには数分かかる場合があります。
- ステップ 6** このイメージを ASDM イメージとして設定するように求められます。[Yes] をクリックします。
- ステップ 7** ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。
アップグレード ツールを終了します。注：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM を終了して再接続します。
- ステップ 8** これらの手順を繰り返し、[Image to Upload] ドロップダウンリストで [ASA] を選択します。この手順は、その他のタイプのファイルのアップロードでも同じです。
- ステップ 9** [Tools] > [System Reload] を選択して、ASA をリロードします。
リロードの詳細の確認を求める新しいウィンドウが表示されます。
- [Save the running configuration at the time of reload] オプション ボタン (デフォルト) をクリックします。
 - リロードする時刻を選択します (たとえば、デフォルトの [Now]) 。
 - [Schedule Reload] をクリックします。
- リロードが開始されると、[Reload Status] ウィンドウにリロードの進行状況が表示されます。ASDM を終了するオプションも表示されます。
- ステップ 10** ASA のリロード後、ASDM を再起動します。
コンソール ポートでリロードの状況を確認できます。または、数分待った後に ASDM を使用して、接続可能になるまで再試行することもできます。
- ステップ 11** ASA FirePOWER モジュールをアップグレードする場合は、[ツール (Tools)] > [コマンドライン インターフェイス (Command Line Interface)] を選択し、**no rest-api agent** を入力して ASA REST API を無効にします。
REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。次のコマンドを実行して、アップグレード後に REST API を再度有効にすることができます。

rest-api agent

- (注) FirePOWER モジュールのバージョン 6.0 以降を実行している場合、ASA 5506-X シリーズは ASA の REST API をサポートしません。

ステップ 12 ASA FirePOWER モジュールをアップグレードします。

ASDM Cisco.com ウィザードを使用したスタンドアロンユニットのアップグレード

Upgrade Software from Cisco.com Wizard により、ASDM および ASA を最新のバージョンに自動的にアップグレードできます。

このウィザードでは、次の操作を実行できます。

- アップグレード用の ASA イメージファイルまたは ASDM イメージファイルを選択する。



(注) ASDM は最新のイメージバージョンをダウンロードし、そこにはビルド番号が含まれています。たとえば、9.9(1) をダウンロードする場合に、ダウンロードが 9.9(1.2) となる可能性があります。この動作は想定されているため、計画したアップグレードを続行できます。

- 実行したアップグレードの変更点を確認する。
- イメージをダウンロードし、インストールする。
- インストールのステータスを確認する。
- インストールが正常に完了した場合は、ASA をリロードして、コンフィギュレーションを保存し、アップグレードを完了する。

始める前に

内部的な変更により、このウィザードでは ASDM 7.10(1) 以降の使用のみがサポートされています。また、イメージの命名が変更されたため、ASA 9.10(1) 以降にアップグレードするには、ASDM 7.12(1) 以降を使用する必要があります。ASDM は ASA の以前のリリースと下位互換性があるため、実行している ASA バージョンを問わず、ASDM をアップグレードすることができます。

手順

ステップ 1 [Tools] > [Check for ASA/ASDM Updates] を選択します。

マルチコンテキストモードでは、システムからこのメニューにアクセスします。

[Cisco.com Authentication] ダイアログボックスが表示されます。

ステップ 2 Cisco.com のユーザー ID とパスワードを入力して、[Login] をクリックします。

[Cisco.com Upgrade Wizard] が表示されます。

(注) 利用可能なアップグレードがない場合は、ダイアログボックスが表示されます。ウィザードを終了するには、[OK] をクリックします。

ステップ 3 [Next] をクリックして [Select Software] 画面を表示します。

現在の ASA バージョンおよび ASDM バージョンが表示されます。

ステップ 4 ASA バージョンおよび ASDM バージョンをアップグレードするには、次の手順を実行します。

- a) [ASA] 領域で、[Upgrade to] チェックボックスをオンにしてから、アップグレードする ASA バージョンをドロップダウン リストから選択します。
- b) [ASDM] 領域で、[Upgrade to] チェックボックスをオンにしてから、アップグレードする ASDM バージョンをドロップダウン リストから選択します。

ステップ 5 [Next] をクリックして [Review Changes] 画面を表示します。

ステップ 6 次の項目を確認します。

- ダウンロードした ASA イメージ ファイルや ASDM イメージ ファイルが正しいファイルであること。
- アップロードする ASA イメージ ファイルや ASDM イメージ ファイルが正しいファイルであること。
- 正しい ASA ブート イメージが選択されていること。

ステップ 7 [Next] をクリックして、アップグレード インストールを開始します。

アップグレード インストールの進行状況を示すステータスを表示できます。

[Results] 画面が表示され、アップグレード インストール ステータス（成功または失敗）など、追加の詳細が表示されます。

ステップ 8 アップグレード インストールが成功した場合に、アップグレード バージョンを有効にするには、[Save configuration and reload device now] チェックボックスをオンにして、ASA を再起動し、ASDM を再起動します。

ステップ 9 [Finish] をクリックして、ウィザードを終了し、コンフィギュレーションに対して行った変更を保存します。

(注) 次に高いバージョン（存在する場合）にアップグレードするには、ウィザードを再起動する必要があります。

ステップ 10 ASA のリロード後、ASDM を再起動します。

コンソール ポートでリロードの状況を確認できます。または、数分待った後に ASDM を使用して、接続可能になるまで再試行することもできます。

ステップ 11 ASA FirePOWER モジュールをアップグレードする場合は、[ツール (Tools)] > [コマンドライン インターフェイス (Command Line Interface)] を選択し、**no rest-api agent** を入力して ASA REST API を無効にします。

REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。次のコマンドを実行して、アップグレード後に REST API を再度有効にすることができます。

rest-api agent

(注) FirePOWER モジュールのバージョン 6.0 以降を実行している場合、ASA 5506-X シリーズは ASA の REST API をサポートしません。

ステップ 12 ASA FirePOWER モジュールをアップグレードします。

アクティブ/スタンバイ フェールオーバー ペアのアップグレード

アクティブ/スタンバイ フェールオーバー ペアをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、CLI または ASDM を使用します。

CLI を使用したアクティブ/スタンバイ フェールオーバー ペアのアップグレード

アクティブ/スタンバイ フェールオーバー ペアをアップグレードするには、次の手順を実行します。

始める前に

- アクティブ装置で次の手順を実行します。SSH アクセスの場合、アクティブな IP アドレスに接続します。アクティブ装置は常にこの IP アドレスを保有しています。CLI に接続する場合は、ASA プロンプトを調べてフェールオーバー ステータスを確認します。フェールオーバー ステータスと優先順位（プライマリまたはセカンダリ）を表示するように ASA プロンプトを設定できます。これは、接続しているユニットを特定するのに役立ちます。[prompt](#) コマンドを参照してください。代わりに、**show failover** コマンドを入力して、このユニットのステータスと優先順位（プライマリまたはセカンダリ）を表示します。
- この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバータイプについては、『[ASA Command Reference](#)』の **copy** コマンドを参照してください。

手順

ステップ 1 特権 EXEC モード時にアクティブ装置で、ASA ソフトウェアをアクティブ装置のフラッシュメモリにコピーします。

copy ftp://[[user[:password]]@]server[/path]/asa_image_name disk:[/path]/asa_image_name

例 :

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin
disk0:/asa9-15-1-smp-k8.bin
```

- ステップ 2** ソフトウェアをスタンバイ装置にコピーします。アクティブ装置で指定したのと同じパスを指定してください。

```
failover exec mate copy /noconfirm ftp://[[user[:password]]@]server[/path]/asa_image_name
diskn:[/path]/asa_image_name
```

例 :

```
asa/act# failover exec mate copy /noconfirm
ftp://jcrichon:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin disk0:/asa9-15-1-smp-k8.bin
```

- ステップ 3** ASDM イメージをアクティブ装置のフラッシュ メモリにコピーします。

```
copy ftp://[[user[:password]]@]server[/path]/asdm_image_name diskn:[/path]/asdm_image_name
```

例 :

```
asa/act# copy ftp://jcrichon:aeryn@10.1.1.1/asdm-77171417151.bin
disk0:/asdm-77171417151.bin
```

- ステップ 4** ASDM イメージをスタンバイ装置にコピーします。アクティブ装置で指定したのと同じパスを指定してください。

```
failover exec mate copy /noconfirm ftp://[[user[:password]]@]server[/path]/asdm_image_name
diskn:[/path]/asdm_image_name
```

例 :

```
asa/act# failover exec mate copy /noconfirm
ftp://jcrichon:aeryn@10.1.1.1/asdm-77171417151.bin disk0:/asdm-77171417151.bin
```

- ステップ 5** まだグローバルコンフィギュレーションモードを開始していない場合は、グローバルコンフィギュレーション モードを開始します。

```
configure terminal
```

- ステップ 6** 設定されている現在のブート イメージを表示します (最大 4 個)。

```
show running-config boot system
```

例 :

```
asa/act(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。

- ステップ 7** 既存のブートイメージコンフィギュレーションがある場合は削除します。新しいブートイメージを最初の選択肢として入力できるようにするためです。

no boot system disk:[path]asa_image_name

例 :

```
asa/act(config)# no boot system disk0:/cdisk.bin
asa/act(config)# no boot system disk0:/asa931-smp-k8.bin
```

ステップ 8 ブートする ASA イメージを設定します (先ほどアップロードしたもの)。

boot system disk:[path]asa_image_name

例 :

```
asa/act(config)# boot system disk0://asa9-15-1-smp-k8.bin
```

このイメージが使用できない場合に使用するバックアップイメージに対して、このコマンドを繰り返します。たとえば、先ほど削除したイメージを再入力できます。

ステップ 9 使用する ASDM イメージを設定します (先ほどアップロードしたもの)。

asdm image disk:[path]asdm_image_name

例 :

```
asa/act(config)# asdm image disk0:/asdm-77171417151.bin
```

使用するように設定できる ASDM イメージは1つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

ステップ 10 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

これらの設定変更は、スタンバイ ユニットに自動的に保存されます。

ステップ 11 ASA FirePOWER モジュールをアップグレードする場合は、ASA REST API を無効にします。無効にしない場合アップグレードは失敗します。

no rest-api agent

ステップ 12 スタンバイ装置の ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をスタンバイ管理 IP アドレスに接続します。アップグレードが完了するまで待ちます。

ステップ 13 スタンバイ装置をリロードして新しいイメージを起動します。

failover reload-standby

スタンバイ装置のロードが完了するまで待ちます。 **show failover** コマンドを使用して、スタンバイ ユニットが Standby Ready 状態かどうかを検証します。

ステップ 14 強制的にアクティブ装置からスタンバイ装置へのフェールオーバーを行います。

no failover active

SSH セッションから切断されている場合は、新しいアクティブ/元のスタンバイ ユニット上に現在あるメイン IP アドレスに再接続します。

ステップ 15 以前のアクティブ装置の ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をスタンバイ管理 IP アドレスに接続します。アップグレードが完了するまで待ちます。

ステップ 16 新しいアクティブ装置から、元のアクティブ装置（今の新しいスタンバイ装置）をリロードします。

failover reload-standby

例：

```
asa/act# failover reload-standby
```

(注) 元のアクティブ ユニットのコンソールポートに接続されている場合は、代わりに **reload** コマンドを入力して、元のアクティブユニットをリロードする必要があります。

ASDM を使用したアクティブ/スタンバイ フェールオーバー ペアのアップグレード

アクティブ/スタンバイ フェールオーバー ペアをアップグレードするには、次の手順を実行します。

始める前に

ローカル管理コンピュータに ASA と ASDM のイメージを配置します。

手順

- ステップ 1** スタンバイ IP アドレスに接続して、*standby* ユニット上で ASDM を起動します。
- ステップ 2** メイン ASDM アプリケーションウィンドウで、**[Tools]>[Upgrade Software from Local Computer]** の順に選択します。
[Upgrade Software] ダイアログボックスが表示されます。
- ステップ 3** [アップロードするイメージ (Image to Upload)] ドロップダウン リストから、[ASDM] を選択します。
- ステップ 4** [Local File Path] フィールドにコンピュータ上のファイルへのローカルパスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを見つけます。
- ステップ 5** [Flash File System Path] フィールドにフラッシュファイルシステムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを検索します。

- ステップ 6** [イメージのアップロード (Upload Image)] をクリックします。アップグレードプロセスには数分かかる場合があります。
- このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。
- ステップ 7** これらの手順を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。
- このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレード ツールを終了します。
- ステップ 8** メイン IP アドレスに接続して ASDM をアクティブなユニットに接続し、スタンバイ ユニットで使用したのと同じファイルの場所を使用して、ASDM ソフトウェアをアップロードします。
- ステップ 9** このイメージを ASDM イメージとして設定するように求められたら、[Yes] をクリックします。
- ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。アップグレード ツールを終了します。注：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM をリロードします。
- ステップ 10** スタンバイ ユニットで使用したのと同じファイルの場所を使用して、ASA ソフトウェアをアップロードします。
- ステップ 11** このイメージを ASA イメージとして設定するように求められたら、[Yes] をクリックします。
- 新しいイメージを使用するために、ASA をリロードするよう求められます。[OK] をクリックします。アップグレード ツールを終了します。
- ステップ 12** コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。
- これらの設定変更は、スタンバイ ユニットに自動的に保存されます。
- ステップ 13** ASA FirePOWER モジュールをアップグレードする場合は、[ツール (Tools)] > [コマンドライン インターフェイス (Command Line Interface)] を選択し、**no rest-api enable** を入力して ASA REST API を無効にします。
- REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。
- ステップ 14** スタンバイ装置の ASA FirePOWER モジュールをアップグレードします。
- ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をスタンバイ管理 IP アドレスに接続します。アップグレードの完了を待ってから、ASDM をアクティブ装置に接続します。
- ステップ 15** [モニタリング (Monitoring)] > [プロパティ (Properties)] > [フェールオーバー (Failover)] > [ステータス (Status)] の順に選択し、[スタンバイのリロード (Reload Standby)] をクリックして、スタンバイ装置をリロードします。
- [システム (System)] ペインを開いたまま、スタンバイ ユニットがリロードされるのを確認します。

ステップ 16 スタンバイ ユニットがリロードしたら、**[Monitoring] > [Properties] > [Failover] > [Status]** の順に選択し、**[Make Standby]** をクリックして、アクティブなユニットをスタンバイ ユニットにフェールオーバーします。

ASDM は新しいアクティブ ユニットに自動的に再接続されます。

ステップ 17 以前のアクティブ装置の ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をスタンバイ管理 IP アドレスに接続します。アップグレードの完了を待ってから、ASDM をアクティブ装置に接続します。

ステップ 18 **[モニタリング (Monitoring)] > [プロパティ (Properties)] > [フェールオーバー (Failover)] > [ステータス (Status)]** の順に選択し、**[スタンバイのリロード (Reload Standby)]** をクリックして、(新しい) スタンバイユニットをリロードします。

アクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー ペアをアップグレードしてゼロ ダウンタイムアップグレードを実現するには、CLI または ASDM を使用します。

CLI を使用したアクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー コンフィギュレーションの 2 つの装置をアップグレードするには、次の手順を実行します。

始める前に

- 標準出荷単位で次の手順を実行します。
- これらの手順をシステム実行スペースで実行します。
- この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバータイプについては、『[ASA Command Reference](#)』の **copy** コマンドを参照してください。

手順

ステップ 1 特権 EXEC モード時にプライマリ ユニットで、ASA ソフトウェアをフラッシュ メモリにコピーします。

copy ftp://[[user[:password]]@]server[[/path]]asa_image_name diskn:[[path]]asa_image_name

例 :

```
asa/act/pri# copy ftp://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin
disk0:/asa9-15-1-smp-k8.bin
```

- ステップ 2** ソフトウェアをセカンダリ装置にコピーします。プライマリ装置で指定したのと同じパスを指定してください。

```
failover exec mate copy /noconfirm ftp://[[user[:password]]@]server[/path]/asa_image_name  
diskn:[/path]/asa_image_name
```

例 :

```
asa/act/pri# failover exec mate copy /noconfirm  
ftp://jcrichon:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin disk0:/asa9-15-1-smp-k8.bin
```

- ステップ 3** ASDM イメージをプライマリ装置のフラッシュ メモリにコピーします。

```
copy ftp://[[user[:password]]@]server[/path]/asdm_image_name diskn:[/path]/asdm_image_name
```

例 :

```
asa/act/pri# ciscoasa# copy ftp://jcrichon:aeryn@10.1.1.1/asdm-77171417151.bin  
disk0:/asdm-77171417151.bin
```

- ステップ 4** ASDM イメージをセカンダリ装置にコピーします。標準出荷単位で指定したのと同じパスを指定してください。

```
failover exec mate copy /noconfirm ftp://[[user[:password]]@]server[/path]/asdm_image_name  
diskn:[/path]/asdm_image_name
```

例 :

```
asa/act/pri# failover exec mate copy /noconfirm  
ftp://jcrichon:aeryn@10.1.1.1/asdm-77171417151.bin disk0:/asdm-77171417151.bin
```

- ステップ 5** まだグローバルコンフィギュレーションモードを開始していない場合は、グローバルコンフィギュレーション モードを開始します。

```
configure terminal
```

- ステップ 6** 設定されている現在のブート イメージを表示します (最大 4 個)。

```
show running-config boot system
```

例 :

```
asa/act/pri(config)# show running-config boot system  
boot system disk0:/cdisk.bin  
boot system disk0:/asa931-smp-k8.bin
```

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。

- ステップ 7** 既存のブートイメージコンフィギュレーションがある場合は削除します。新しいブートイメージを最初の選択肢として入力できるようにするためです。

no boot system diskn:[path]asa_image_name

例 :

```
asa/act/pri(config)# no boot system disk0:/cdisk.bin
asa/act/pri(config)# no boot system disk0:/asa931-smp-k8.bin
```

ステップ 8 ブートする ASA イメージを設定します (先ほどアップロードしたもの)。

boot system diskn:[path]asa_image_name

例 :

```
asa/act/pri(config)# boot system disk0://asa9-15-1-smp-k8.bin
```

このイメージが使用できない場合に使用するバックアップイメージに対して、このコマンドを繰り返します。たとえば、先ほど削除したイメージを再入力できます。

ステップ 9 使用する ASDM イメージを設定します (先ほどアップロードしたもの)。

asdm image diskn:[path]asdm_image_name

例 :

```
asa/act/pri(config)# asdm image disk0:/asdm-77171417151.bin
```

使用するように設定できる ASDM イメージは1つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

ステップ 10 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

これらの設定変更は、セカンダリ ユニットに自動的に保存されます。

ステップ 11 ASA FirePOWER モジュールをアップグレードする場合は、ASA REST API を無効にします。無効にしない場合アップグレードは失敗します。

no rest-api agent

ステップ 12 プライマリ装置の両方のフェールオーバー グループをアクティブにします。

failover active group 1

failover active group 2

例 :

```
asa/act/pri(config)# failover active group 1
asa/act/pri(config)# failover active group 2
```

ステップ 13 セカンダリ ユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をフェールオーバーグループ 1 または 2 のスタンバイ管理 IP アドレスに接続します。アップグレードが完了するまで待ちます。

ステップ 14 セカンダリ装置をリロードして新しいイメージを起動します。

failover reload-standby

セカンダリ装置のロードが完了するまで待ちます。**show failover** コマンドを使用して、両方のフェールオーバーグループが Standby Ready 状態であることを確認します。

ステップ 15 セカンダリ装置で、両方のフェールオーバーグループを強制的にアクティブにします。

no failover active group 1

no failover active group 2

例 :

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
asa/stby/pri(config)#
```

SSH セッションから切断されている場合は、セカンダリユニット上に現在あるフェールオーバーグループ 1 の IP アドレスに再接続します。

ステップ 16 プライマリユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をフェールオーバーグループ 1 または 2 のスタンバイ管理 IP アドレスに接続します。アップグレードが完了するまで待ちます。

ステップ 17 プライマリ装置をリロードします。

failover reload-standby

例 :

```
asa/act/sec# failover reload-standby
```

(注) プライマリユニットのコンソールポートに接続されている場合は、代わりに **reload** コマンドを入力して、プライマリユニットをリロードする必要があります。

SSH セッションから切断される場合があります。

ステップ 18 フェールオーバーグループは、**preempt** コマンドを使用して設定されている場合、プリエンブト遅延の経過後、指定された装置で自動的にアクティブになります。

ASDM を使用したアクティブ/アクティブ フェールオーバー ペアのアップグレード

アクティブ/アクティブ フェールオーバー コンフィギュレーションの 2 つの装置をアップグレードするには、次の手順を実行します。

始める前に

- これらの手順をシステム実行スペースで実行します。
- ローカル管理コンピュータに ASA と ASDM のイメージを配置します。

手順

-
- ステップ 1** フェールオーバー グループ 2 の管理アドレスに接続して、セカンダリ ユニットで ASDM を起動します。
- ステップ 2** メイン ASDM アプリケーションウィンドウで、**[Tools]>[Upgrade Software from Local Computer]** の順に選択します。
- [Upgrade Software] ダイアログボックスが表示されます。
- ステップ 3** [アップロードするイメージ (Image to Upload)] ドロップダウン リストから、[ASDM] を選択します。
- ステップ 4** [Local File Path] フィールドにコンピュータ上のファイルへのローカルパスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを見つけます。
- ステップ 5** [Flash File System Path] フィールドにフラッシュファイルシステムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを検索します。
- ステップ 6** [イメージのアップロード (Upload Image)] をクリックします。アップグレードプロセスには数分かかる場合があります。
- このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレードツールを終了します。
- ステップ 7** これらの手順を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。
- このイメージを ASA イメージとして設定するように求められる場合は、[No] をクリックします。アップグレードツールを終了します。
- ステップ 8** フェールオーバー グループ 1 の管理 IP アドレスに接続して ASDM をプライマリ ユニットに接続し、セカンダリ ユニットで使用したのと同じファイルの場所を使用して、ASDM ソフトウェアをアップロードします。
- ステップ 9** このイメージを ASDM イメージとして設定するように求められたら、[Yes] をクリックします。
- ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。アップグレードツールを終了します。**注** : ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM をリロードします。
- ステップ 10** セカンダリ ユニットで使用したのと同じファイルの場所を使用して、ASA ソフトウェアをアップロードします。
- ステップ 11** このイメージを ASA イメージとして設定するように求められたら、[Yes] をクリックします。

新しいイメージを使用するために、ASA をリロードするよう求められます。[OK] をクリックします。アップグレード ツールを終了します。

- ステップ 12** コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。
- これらの設定変更は、セカンダリ ユニットに自動的に保存されます。
- ステップ 13** ASA FirePOWER モジュールをアップグレードする場合は、[ツール (Tools)] > [コマンドライン インターフェイス (Command Line Interface)] を選択し、**no rest-api enable** を入力して ASA REST API を無効にします。
- REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。
- ステップ 14** [Monitoring] > [Failover] > [Failover Group #] の順に選択して、プライマリ ユニット上の両方のフェールオーバー グループをアクティブにします。ここで # は、プライマリ ユニットに移動するフェールオーバー グループの数です。[Make Active] をクリックします。
- ステップ 15** セカンダリ ユニットの ASA FirePOWER モジュールをアップグレードします。
- ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をフェールオーバー グループ 1 または 2 のスタンバイ管理 IP アドレスに接続します。アップグレードの完了を待ってから、ASDM をプライマリ ユニットに接続します。
- ステップ 16** [Monitoring] > [Failover] > [System] の順に選択し、[Reload Standby] をクリックして、セカンダリ ユニットの ASA FirePOWER モジュールをリロードします。
- [System] ペインを開いたまま、セカンダリ ユニットがリロードされるのを確認します。
- ステップ 17** セカンダリ ユニットが起動したら、[Monitoring] > [Failover] > [Failover Group #] の順に選択して、セカンダリ ユニット上の両方のフェールオーバー グループをアクティブにします。ここで # は、セカンダリ ユニットに移動するフェールオーバー グループの数です。[Make Standby] をクリックします。
- ASDM は、セカンダリ ユニット上のフェールオーバー グループ 1 の IP アドレスに自動的に再接続されます。
- ステップ 18** プライマリ ユニットの ASA FirePOWER モジュールをアップグレードします。
- ASDM によって管理される ASA FirePOWER モジュールの場合、ASDM をフェールオーバー グループ 1 または 2 のスタンバイ管理 IP アドレスに接続します。アップグレードの完了を待ってから、ASDM をセカンダリ ユニットに接続します。
- ステップ 19** [Monitoring] > [Failover] > [System] の順に選択し、[Reload Standby] をクリックして、プライマリ ユニットの ASA FirePOWER モジュールをリロードします。
- ステップ 20** フェールオーバー グループは、[Preempt Enabled] を使用して設定されると、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。ASDM は、プライマリ ユニット上のフェールオーバー グループ 1 の IP アドレスに自動的に再接続されます。

ASA クラスタのアップグレード

ASA クラスタをアップグレードしてゼロ ダウンタイム アップグレードを実現するには、CLI または ASDM を使用します。

CLI を使用した ASA クラスタのアップグレード

ASA クラスタ内のすべての装置をアップグレードするには、次の手順を実行します。この手順では、FTP を使用します。TFTP、HTTP、またはその他のサーバータイプについては、『[ASA Command Reference](#)』の **copy** コマンドを参照してください。

始める前に

- 制御ユニットで次の手順を実行します。ASA FirePOWER モジュールもアップグレードしている場合は、各データユニットへのコンソールアクセスまたは ASDM アクセスが必要です。クラスタ ユニットと状態（制御またはデータ）を表示するように ASA プロンプトを設定できます。これは、接続しているユニットを特定するのに役立ちます。prompt コマンドを参照してください。代わりに、**show cluster info** コマンドを入力して、各ユニットの役割を表示します。
- コンソール ポートを使用する必要があります。クラスタリングのイネーブルまたはディセーブルを、リモート CLI 接続から行うことはできません。
- マルチ コンテキスト モードでは、システム実行スペースで後続の手順を実行します。

手順

- ステップ 1** 特権 EXEC モード時に制御ユニットで、ASA ソフトウェアをクラスタ内のすべてのユニットにコピーします。

```
cluster exec copy /noconfirm ftp://[[user[:password]@]server[/path]]asa_image_name
diskn:[/path]asa_image_name
```

例 :

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichon:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin disk0:/asa9-15-1-smp-k8.bin
```

- ステップ 2** ASDM イメージをクラスタ内のすべての装置にコピーします。

```
cluster exec copy /noconfirm ftp://[[user[:password]@]server[/path]]asdm_image_name
diskn:[/path]asdm_image_name
```

例 :

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichon:aeryn@10.1.1.1/asdm-77171417151.bin disk0:/asdm-77171417151.bin
```

- ステップ 3** まだグローバルコンフィギュレーションモードを開始していない場合は、ここで開始します。

configure terminal

例 :

```
asa/unit1/master# configure terminal
asa/unit1/master(config)#
```

ステップ 4 設定されている現在のブート イメージを表示します (最大 4 個)。

show running-config boot system

例 :

```
asa/unit1/master(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。

ステップ 5 既存のブートイメージコンフィギュレーションがある場合は削除します。新しいブートイメージを最初の選択肢として入力できるようにするためです。

no boot system disk:[path]asa_image_name

例 :

```
asa/unit1/master(config)# no boot system disk0:/cdisk.bin
asa/unit1/master(config)# no boot system disk0:/asa931-smp-k8.bin
```

ステップ 6 ブートする ASA イメージを設定します (先ほどアップロードしたもの)。

boot system disk:[path]asa_image_name

例 :

```
asa/unit1/master(config)# boot system disk0://asa9-15-1-smp-k8.bin
```

このイメージが使用できない場合に使用するバックアップイメージに対して、このコマンドを繰り返します。たとえば、先ほど削除したイメージを再入力できます。

ステップ 7 使用する ASDM イメージを設定します (先ほどアップロードしたもの)。

asdm image disk:[path]asdm_image_name

例 :

```
asa/unit1/master(config)# asdm image disk0:/asdm-77171417151.bin
```

使用するように設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。

ステップ 8 新しい設定をスタートアップ コンフィギュレーションに保存します。

write memory

これらの設定変更は、データユニットに自動的に保存されます。

ステップ 9 ASA FirePOWER モジュールをアップグレードする場合は、ASA REST API を無効にします。無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。

no rest-api agent

ステップ 10 ASDM によって管理されている ASA FirePOWER モジュールをアップグレードする場合、ASDM を個別の管理 IP アドレスに接続する必要があります。このため、各ユニットの IP アドレスをメモしておく必要があります。

show running-config interface management_interface_id

使用されている **cluster-pool** プール名をメモします。

show ip[v6] local pool poolname

クラスタ ユニットの IP アドレスをメモします。

例：

```
asa/unit2/slave# show running-config interface gigabitethernet0/0
!
interface GigabitEthernet0/0
  management-only
  nameif inside
  security-level 100
  ip address 10.86.118.1 255.255.252.0 cluster-pool inside-pool
asa/unit2/slave# show ip local pool inside-pool
Begin      End      Mask      Free      Held      In use
10.86.118.16  10.86.118.17  255.255.252.0    0         0         2

Cluster Unit      IP Address Allocated
unit2              10.86.118.16
unit1              10.86.118.17
asa1/unit2/slave#
```

ステップ 11 データユニットをアップグレードします。

ASA FirePOWER モジュールもアップグレードするかどうかによって、以下の手順を選択します。ASA FirePOWER モジュールもアップグレードする場合、ASA FirePOWER プロシージャは ASA のリロードの回数を最小化します。以下の手順では、データコンソールまたは ASDM を使用するよう選択できます。すべてのコンソールポートへのアクセスは準備できていないが、ASDM にネットワーク経由でアクセスできる場合は、コンソールではなく ASDM を使用することを推奨します。

(注) アップグレードプロセス中は、**cluster master unit** コマンドを使用して強制的にデータユニットを制御に変更しないでください。ネットワークの接続性とクラスタの安定性に関連した障害が発生する恐れがあります。最初にすべてのデータユニットをアップグレードしてリロードし、次にこの手順を実行すると、現在の制御ユニットから新しい制御ユニットへの移行をスムーズに行うことができます。

ASA FirePOWER モジュールをアップグレードしない場合 :

- a) 制御ユニットでメンバー名を表示するには、**cluster exec unit ?** または **show cluster info** コマンドを入力します。
- b) データユニットをリロードします。

cluster exec unit data-unit reload noconfirm

例 :

```
asa/unit1/master# cluster exec unit unit2 reload noconfirm
```

- c) 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約 5 分）、次の装置にこれらの手順を繰り返します。装置がクラスタに再接続したことを確認するには、**show cluster info** を入力します。

ASA FirePOWER モジュールもアップグレードする場合（データコンソールを使用） :

- a) データユニットのコンソールポートに接続し、グローバル コンフィギュレーション モードに入ります。

enable

configure terminal

例 :

```
asa/unit2/slave> enable
Password:
asa/unit2/slave# configure terminal
asa/unit2/slave(config)#
```

- b) クラスタリングを無効にします。

cluster group name

no enable

リロード時にクラスタリングを有効にするために、この構成を保存しないでください。複数の障害やアップグレード処理中の再参加を避けるために、クラスタリングを無効にする必要があります。このユニットでは、すべてのアップグレードとリロードが完了した後に再参加のみする必要があります。

例 :

```
asa/unit2/slave(config)# cluster group cluster1
asa/unit2/slave(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover
  either enable clustering or remove cluster group configuration.

Cluster unit unit2 transitioned from SLAVE to DISABLED
asa/unit2/ClusterDisabled(cfg-cluster)#
```

- c) このデータユニットの ASA FirePOWER モジュールをアップグレードします。
ASDM によって管理される ASA FirePOWER モジュールの場合、事前にメモした個別の管理 IP アドレスに ASDM を接続します。アップグレードが完了するまで待ちます。
- d) データユニットをリロードします。
reload noconfirm
- e) 各データユニットに対して手順を繰り返します。
接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約 5 分）、次の装置にこれらの手順を繰り返します。装置がクラスタに再接続したことを確認するには、**show cluster info** を入力します。

ASA FirePOWER モジュールのアップグレードもある場合（ASDM を使用）：

- a) 事前にメモしたこのデータユニットの「個別」の管理 IP アドレスに ASDM を接続します。
- b) **[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration]** の順に選択します。
- c) **[ASA クラスタに参加 (Participate in ASA cluster)]** チェックボックスをオフにします。
複数の障害やアップグレード処理中の再参加を避けるために、クラスタリングを無効にする必要があります。このユニットでは、すべてのアップグレードとリロードが完了した後に再参加のみする必要があります。
[Configure ASA cluster settings] チェックボックスをオフにしないでください。オフにすると、すべてのクラスタ コンフィギュレーションがクリアされ、ASDM が接続されている管理インターフェイスを含むすべてのインターフェイスもシャットダウンします。この場合、接続を復元するには、コンソールポートで CLI にアクセスする必要があります。
(注) ASDM の以前のバージョンは、この画面でのクラスタの無効化をサポートしていません。この場合、**[Tools] > [Command Line Interface]** ツールを使用します。**[Multiple Line]** ラジオボタンをクリックして、**cluster group name** と **no enable** を入力します。クラスタ グループ名は、**[Home] > [Device Dashboard] > [Device Information] > [ASA Cluster]** エリアで確認できます。
- d) **[適用 (Apply)]** をクリックします。
- e) ASDM から出るように促されます。同じ IP アドレスに ASDM を再接続します。
- f) ASA FirePOWER モジュールをアップグレードします。
アップグレードが完了するまで待ちます。
- g) ASDM で、**[Tools] > [System Reload]** を選択します。
- h) **[実行コンフィギュレーションを保存しないでリロードする (Reload without saving the running configuration)]** オプション ボタンをクリックします。
この装置のリロード時にクラスタリングを有効にするために、この構成を保存しないようにします。
- i) **[Schedule Reload]** をクリックします。

- j) [Yes] をクリックしてリロードを続行します。
- k) 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約 5 分）、次の装置にこれらの手順を繰り返します。装置がクラスタに再接続したことを確認するには、制御ユニットの [Monitoring]>[ASA Cluster]>[Cluster Summary] ペインを確認します。

ステップ 12 制御ユニットをアップグレードします。

- a) クラスタリングを無効にします。

```
cluster group name
```

```
no enable
```

新しい制御ユニットが選択され、トラフィックが安定するまで 5 分間待ちます。

リロード時にクラスタリングを有効にするために、この構成を保存しないでください。

可能であれば、制御ユニットのクラスタを手動で無効にすることを推奨します。これにより、新しい制御ユニットを迅速かつできるだけクリーンな状態で選定できます。

例：

```
asa/unit1/master(config)# cluster group cluster1
asa/unit1/master(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover
  either enable clustering or remove cluster group configuration.

Cluster unit unit1 transitioned from MASTER to DISABLED
asa/unit1/ClusterDisabled(cfg-cluster)#
```

- b) このユニットの ASA FirePOWER モジュールをアップグレードします。

ASDM によって管理される ASA FirePOWER モジュールの場合、事前にメモした個別の管理 IP アドレスに ASDM を接続します。この時点で、メインクラスタ IP アドレスは新しい制御ユニットに属しています。元の制御ユニットは、その個別の管理 IP アドレスに引き続きアクセスできます。

アップグレードが完了するまで待ちます。

- c) このユニットをリロードします。

```
reload noconfirm
```

元の制御ユニットがクラスタに再接続すると、そのユニットはデータユニットになります。

ASDM を使用した ASA クラスタのアップグレード

ASA クラスタ内のすべての装置をアップグレードするには、次の手順を実行します。

始める前に

- 制御ユニットで次の手順を実行します。ASA FirePOWER モジュールもアップグレードしている場合は、各データユニットへの ASDM アクセスが必要です。
- マルチ コンテキスト モードでは、システム実行スペースで後続の手順を実行します。
- ローカル管理コンピュータに ASA と ASDM のイメージを配置します。

手順

- ステップ 1** メインクラスタ IP アドレスに接続して、「制御」ユニットで ASDM を起動します。
この IP アドレスは、常に制御ユニットに保持されます。
- ステップ 2** メイン ASDM アプリケーションウィンドウで、[Tools]>[Upgrade Software from Local Computer] の順に選択します。
[Upgrade Software from Local Computer] ダイアログボックスが表示されます。
- ステップ 3** [クラスタ内のすべてのデバイス (All devices in the cluster)] オプションボタンをクリックします。
[ソフトウェアのアップグレード (Upgrade Software)] ダイアログボックスが表示されます。
- ステップ 4** [アップロードするイメージ (Image to Upload)] ドロップダウンリストから、[ASDM] を選択します。
- ステップ 5** [ローカル ファイルパス (Local File Path)] フィールドで [ローカル ファイルの参照 (Browse Local Files)] をクリックして、コンピュータ上のファイルを見つけます。
- ステップ 6** (任意) [フラッシュファイルシステムのパス (Flash File System Path)] フィールドにフラッシュファイルシステムへのパスを入力するか、[フラッシュの参照 (Browse Flash)] をクリックしてフラッシュファイルシステム上のディレクトリまたはファイルを検索します。
デフォルトでは、このフィールドにはパス (`disk0:/filename`) が入力されています。
- ステップ 7** [イメージのアップロード (Upload Image)] をクリックします。アップグレードプロセスには数分かかる場合があります。
- ステップ 8** このイメージを ASDM イメージとして設定するように求められます。[Yes] をクリックします。
- ステップ 9** ASDM を終了して、コンフィギュレーションを保存したことを確認します。[OK] をクリックします。
アップグレードツールを終了します。注：ASA ソフトウェアをアップグレードした後で、設定を保存し、ASDM をリロードします。
- ステップ 10** これらの手順を繰り返し、[アップロードするイメージ (Image to Upload)] ドロップダウンリストから [ASA] を選択します。
- ステップ 11** コンフィギュレーションの変更を保存するには、ツールバーの [Save] アイコンをクリックします。

これらの設定変更は、データユニットに自動的に保存されます。

ステップ 12 [Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Members] で、各ユニットの個別の管理 IP アドレスをメモして、後で ASDM をデータユニットに直接接続できるようにします。

ステップ 13 ASA FirePOWER モジュールをアップグレードする場合は、[ツール (Tools)] > [コマンドラインインターフェイス (Command Line Interface)] を選択し、**no rest-api enable** を入力して ASA REST API を無効にします。

REST API を無効にしない場合、ASA FirePOWER モジュールのアップグレードは失敗します。

ステップ 14 データユニットをアップグレードします。

ASA FirePOWER モジュールもアップグレードするかどうかによって、以下の手順を選択します。ASA FirePOWER モジュールもアップグレードする場合、ASA FirePOWER プロシージャは ASA のリロードの回数を最小化します。

(注) アップグレードプロセス中は、強制的にデータユニットを制御に変更するために [Monitoring] > [ASA Cluster] > [Cluster Summary] ページを使用して制御ユニットを変更しないでください。ネットワークの接続性とクラスタの安定性に関連した障害が発生する可能性があります。最初にすべてのデータユニットをリロードし、次にこの手順を実行すると、現在の制御ユニットから新しい制御ユニットへの移行をスムーズに行うことができます。

ASA FirePOWER モジュールをアップグレードしない場合：

- 制御ユニットで、[Tools] > [System Reload] を選択します。
- [Device] ドロップダウンリストからデータユニット名を選択します。
- [Schedule Reload] をクリックします。
- [Yes] をクリックしてリロードを続行します。
- 各データユニットに対して手順を繰り返します。

接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち (約 5 分)、次の装置にこれらの手順を繰り返します。ユニットがクラスタに再接続したことを確認するには、[Monitoring] > [ASA Cluster] > [Cluster Summary] ペインを表示します。

ASA FirePOWER モジュールのアップグレードもある場合：

- 制御ユニットで、[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Members] を選択します。
- アップグレードするデータユニットを選択して [Delete] をクリックします。
- [適用 (Apply)] をクリックします。
- ASDM を終了し、事前にメモした「個別」の管理 IP アドレスに接続して、ASDM をデータユニットに接続します。
- ASA FirePOWER モジュールをアップグレードします。

アップグレードが完了するまで待ちます。

- f) ASDM で、**[Tools] > [System Reload]** を選択します。
- g) **[実行コンフィギュレーションを保存しないでリロードする (Reload without saving the running configuration)]** オプション ボタンをクリックします。
この装置のリロード時にクラスタリングを有効にするために、この構成を保存しないようにします。
- h) **[Schedule Reload]** をクリックします。
- i) **[Yes]** をクリックしてリロードを続行します。
- j) 各データユニットに対して手順を繰り返します。
接続損失を回避し、トラフィックを安定させるために、各装置が起動しクラスタに再接続するのを待ち（約 5 分）、次の装置にこれらの手順を繰り返します。ユニットがクラスタに再接続したことを確認するには、**[Monitoring] > [ASA Cluster] > [Cluster Summary]** ペインを表示します。

ステップ 15 制御ユニットをアップグレードします。

- a) 制御ユニットの ASDM で、**[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] > [Cluster Configuration]** ペインを選択します。
- b) **[ASA クラスタに参加 (Participate in ASA cluster)]** チェックボックスをオフにして、**[適用 (Apply)]** をクリックします。
ASDM から出るように促されます。
- c) 新しい制御ユニットが選択され、トラフィックが安定するまで最大 5 分間待機します。
元の制御ユニットがクラスタに再接続すると、そのユニットはデータユニットになります。
- d) 事前にメモした「個別」の管理 IP アドレスに接続して、ASDM を元の制御ユニットに再接続します。
この時点で、メインクラスタ IP アドレスは新しい制御ユニットに属しています。元の制御ユニットは、その個別の管理 IP アドレスに引き続きアクセスできます。
- e) ASA FirePOWER モジュールをアップグレードします。
アップグレードが完了するまで待ちます。
- f) **[Tools] > [System Reload]** を選択します。
- g) **[実行コンフィギュレーションを保存しないでリロードする (Reload without saving the running configuration)]** オプション ボタンをクリックします。
この装置のリロード時にクラスタリングを有効にするために、この構成を保存しないようにします。
- h) **[Schedule Reload]** をクリックします。
- i) **[Yes]** をクリックしてリロードを続行します。

ASDM から出るように促されます。メインクラスター IP アドレスで ASDM を再起動すると、新しい制御ユニットに再接続されます。

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。