イメージ管理

イメージ管理について

Firepower 4100/9300 シャーシ では 2 つの基本タイプのイメージを使用します。

（注） すべてのイメージにデジタル署名が行われ、セキュア ブートによって検証されます。どのような場合も、イメージを変更しないでください。変更すると、検証エラーになります。

- プラットフォームバンドル：プラットフォームバンドルは、Supervisor および セキュリティ モジュール/エンジン で動作する、複数の独立したイメージの集まりです。プラットフォーム バンドルは、FXOS のソフトウェア パッケージです。
- アプリケーション：アプリケーションイメージは、Firepower 4100/9300 シャーシのセキュリティ モジュール/エンジンに導入するソフトウェア イメージです。アプリケーション イメージは、Cisco Secure Package ファイル（CSP）として提供されます。これは、論理デバイス作成時にセキュリティ モジュール/エンジンに展開されるまで（または以降の論理デバイス作成に備えて）スーパーバイザに保存されます。同じアプリケーション イメージ タイプの複数の異なるバージョンをスーパバイザに保存できます。

（注） プラットフォーム バンドル イメージと 1 つ以上のアプリケーション イメージの両方をアップグレードする場合、まずプラットフォーム バンドルをアップグレードする必要があります。

（注） デバイスに ASA アプリケーションをインストールする場合は、既存のアプリケーション Threat Defense のイメージを削除できます。その逆も同様です。すべての Threat Defense イメージを削除しようとすると、少なくとも 1 つのイメージの削除が拒否され、「`Invalid operation as no default Threat Defense /ASA APP will be left. Please select a new default Threat Defense app`」というエラーメッセージが表示されます。すべての Threat Defense イメージを削除するには、デフォルトイメージだけを残して、その他のイメージを削除し、最後にデフォルトイメージを削除する必要があります。

Cisco.com からのイメージのダウンロード

FXOS およびアプリケーションイメージをシャーシにアップロードできるように Cisco.com からダウンロードします。

始める前に

Cisco.com アカウントが必要です。

手順

ステップ 1 Web ブラウザを使用して、http://www.cisco.com/go/firepower9300-software または http://www.cisco.com/go/firepower4100-software にアクセスします。
Firepower 4100/9300 シャーシのソフトウェア ダウンロードページがブラウザに表示されます。

ステップ 2 該当するソフトウェア イメージを見つけて、ローカル コンピュータにダウンロードします。

セキュリティアプライアンスへのイメージのアップロード

FXOS およびアプリケーションイメージをシャーシにアップロードできます。

始める前に

アップロードするイメージがローカル コンピュータで使用可能であることを確認してください。

手順

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

ステップ 2 [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。

ステップ 3 [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。

ステップ 4 [Upload] をクリックします。
選択したイメージがFirepower 4100/9300 シャーシにアップロードされます。イメージのアップロード中、完了したアップロードの割合を示す進行状況バーが表示されます。

ステップ 5 特定のソフトウェア イメージについては、イメージをアップロードした後にエンドユーザ ライセンス契約書が表示されます。システムのプロンプトに従ってエンドユーザ契約書に同意します。

イメージの整合性の確認

イメージの整合性は、新しいイメージがFirepower 4100/9300 シャーシに追加されると自動的に確認されます。必要な場合に、手動でイメージの整合性を確認するには、次の手順を実行できます。

手順

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

ステップ 2 確認するイメージの [確認（Verify）]（チェックマーク アイコン）をクリックします。

システムはイメージの整合性を確認し、[イメージの整合性（Image Integrity）] フィールドにステータスを表示します。

FXOS プラットフォーム バンドルのアップグレード

始める前に

プラットフォーム バンドルのソフトウェア イメージを Cisco.com からダウンロードして（Cisco.com からのイメージのダウンロード （2 ページ）を参照）、そのイメージを Firepower 4100/9300 シャーシにアップロードします（セキュリティアプライアンスへのイメージのアップロード （2 ページ）を参照）。

（注） アップグレード プロセスには通常 20 ～ 30 分かかります。

スタンドアロン論理デバイスを実行中の Firepower 9300 または 4100 シリーズ セキュリティ アプライアンスをアップグレードしている場合、または シャーシ内クラスタを実行中の Firepower 9300 セキュリティアプライアンスをアップグレードしている場合、アップグレード中にはトラフィックがデバイスを通過しません。

シャーシ間クラスタに属する Firepower 9300 または 4100 シリーズ セキュリティ アプライアンスをアップグレードしている場合、アップグレード中には、アップグレード対象のデバイスをトラフィックが通過しません。ただし、クラスタ内の他のデバイスではトラフィックは通過し続けます。

手順

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

ステップ 2 アップグレードする FXOS プラットフォーム バンドルの [アップグレード（Upgrade）] をクリックします。

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

ステップ 3 インストールの続行を確定するには [はい（Yes）] を、インストールをキャンセルするには [いいえ（No）] をクリックします。

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。

Firepower 4100/9300 シャーシ への論理デバイスのソフトウェア イメージのダウンロード

FTP、HTTP/HTTPS、SCP、SFTP、または TFTP を使用して、論理デバイスのソフトウェアイメージを Firepower 4100/9300 シャーシ にコピーできます。

始める前に

コンフィギュレーション ファイルのインポート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の IP アドレスおよび認証クレデンシャル
- ソフトウェア イメージ ファイルの完全修飾名

（注） FXOS 2.8.1 以降のバージョンでは、ファームウェアおよびアプリケーションイメージのダウンロード用に HTTP/HTTPS プロトコルがサポートされています。

手順

ステップ 1 セキュリティ サービス モードを開始します。

Firepower-chassis # **scope ssa**

ステップ 2 アプリケーション ソフトウェア モードに入ります。

Firepower-chassis /ssa # **scope app-software**

ステップ 3 論理デバイスのソフトウェア イメージをダウンロードします。

Firepower-chassis /ssa/app-software # **download image** *URL*

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

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

ステップ 4 ダウンロード プロセスをモニタする場合：

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

ステップ 5 ダウンロード アプリケーションを表示するには、次のコマンドを使用します。

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

Firepower-chassis /ssa # **show app**

ステップ 6 特定のアプリケーションの詳細情報を表示するには、次のコマンドを使用します。

Firepower-chassis /ssa # **scope app** *application_type image_version*

Firepower-chassis /ssa/app # **show expand**

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

Firepower-chassis /ssa # scope app asa 9.4.1.65
Firepower-chassis /ssa/app # show expand

Application:
    Name: asa
    Version: 9.4.1.65
    Description: N/A
    Author:
    Deploy Type: Native
    CSP Type: Application
    Is Default App: Yes

    App Attribute Key for the Application:
        App Attribute Key Description
        ----------------- -----------
        cluster-role      This is the role of the blade in the cluster
        mgmt-ip           This is the IP for the management interface
        mgmt-url          This is the management URL for this application
```

```
    Net Mgmt Bootstrap Key for the Application:
        Bootstrap Key Key Data Type Is the Key Secret Description
        ------------- ------------- ----------------- -----------
        PASSWORD      String        Yes               The admin user password.

    Port Requirement for the Application:
        Port Type: Data
        Max Ports: 120
        Min Ports: 1

        Port Type: Mgmt
        Max Ports: 1
        Min Ports: 1

        Mgmt Port Sub Type for the Application:
            Management Sub Type
            -------------------
            Default

        Port Type: Cluster
        Max Ports: 1
        Min Ports: 0
Firepower-chassis /ssa/app #
```

論理デバイスのイメージ バージョンの更新

この手順を使用して、新しいバージョンに ASA アプリケーションイメージをアップグレードするか、Threat Defense アプリケーションイメージをディザスタ リカバリ シナリオで使用される新しいスタートアップバージョンに設定します。

シャーシマネージャまたは FXOS CLIを使用して Threat Defense 論理デバイスでスタートアップバージョンを変更しても、アプリケーションはすぐに新しいバージョンにアップグレードされません。論理デバイス スタートアップ バージョンは、Threat Defense がディザスタ リカバリ シナリオで再インストールされるバージョンです。Threat Defense 論理デバイスの初期作成後には、Threat Defense 論理デバイスを、シャーシマネージャまたはFXOS CLI を使用してアップグレードすることはありません。Threat Defense 論理デバイスをアップグレードするには、Management Center を使用する必要があります。詳細については、次のサイトにあるシステム リリースノートを参照してください。http://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html

さらに、Threat Defense 論理デバイスへの更新は、シャーシマネージャの **[論理デバイス（Logical Devices）]** > **[編集（Edit）]** ページおよび **[システム（System）]** > **[更新（Updates）]** ページには反映されないことに注意してください。これらのページで、表示されるバージョンは、Threat Defense 論理デバイスを作成するために使用されたソフトウェア バージョン（CSP イメージ）を示します。

（注） Threat Defense のスタートアップバージョンを設定すると、アプリケーションのスタートアップバージョンが更新されます。したがって、アプリケーションを手動で再インストールするか、ブレードを再初期化して、選択したバージョンを適用する必要があります。この手順は、Threat Defense ソフトウェアのアップグレードまたはダウングレードとは異なり、完全な再インストール（再イメージ化）です。そのため、アプリケーションが削除され、既存の設定が失われます。

ASA 論理デバイスでスタートアップ バージョンを変更すると、ASA はこのバージョンにアップグレードされ、すべての設定が復元されます。設定に応じて ASA スタートアップ バージョンを変更するには、次のワークフローを使用します。

（注） ASA のスタートアップバージョンを設定すると、アプリケーションが自動的に再起動されます。この手順は、ASA ソフトウェアのアップグレードまたはダウングレードと同様です（既存の設定は保持されます）。

ASA ハイ アベイラビリティ：

1. スタンバイ ユニットで論理デバイス イメージ バージョンを変更します。
2. スタンバイ ユニットをアクティブにします。
3. 他のユニットでアプリケーション バージョンを変更します。

ASA シャーシ間クラスタ：

1. データユニットでスタートアップバージョンを変更します。
2. データユニットを制御ユニットにします。
3. 元の制御ユニット（ここではデータユニット）でスタートアップバージョンを変更します。

始める前に

論理デバイスに使用するアプリケーション イメージを Cisco.com からダウンロードして（Cisco.com からのイメージのダウンロード （2 ページ）を参照）、そのイメージを Firepower 4100/9300 シャーシにアップロードします（セキュリティアプライアンスへのイメージのアップロード （2 ページ）を参照）。

プラットフォーム バンドル イメージと 1 つ以上のアプリケーション イメージの両方をアップグレードする場合、まずプラットフォーム バンドルをアップグレードする必要があります。

手順

ステップ 1 [論理デバイス（Logical Devices）] を選択して、[論理デバイス（Logical Devices）] ページを開きます。
[論理デバイス（Logical Devices）] ページに、シャーシに設定されている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。

ステップ 2 更新する論理デバイスの [Update Version] をクリックして、[Update Image Version] ダイアログボックスを開きます。

ステップ 3 [New Version] では、ソフトウェア バージョンを選択します。

ステップ 4 [OK] をクリックします。

ファームウェア アップグレード

Firepower 4100/9300 シャーシでファームウェアをアップグレードする方法については、『*Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイド*』を参照してください。

バージョン 2.0.1 以下への手動ダウングレード

セキュリティモジュールに CIMC イメージを手動でダウングレードするには、次の CLI 手順に従います。

（注） この手順は、バージョン 2.1.1 以降からバージョン 2.0.1 以前にダウングレードする際に使用します。

始める前に

ダウングレード対象のアプリケーションイメージが Firepower 4100/9300 シャーシにダウンロードされていることを確認します（「Cisco.com からのイメージのダウンロード （2 ページ）」および「Firepower 4100/9300 シャーシへの論理デバイスのソフトウェア イメージのダウンロード （5 ページ）」を参照）。

手順

ステップ 1 CIMC イメージをダウングレードする前に、イメージバージョンの比較を無効にします。

デフォルトのプラットフォーム イメージ バージョンを消去するには、次の例の手順に従います。

例：

```
firepower# scope org
firepower /org # scope fw-platform-pack default
firepower /org/fw-platform-pack # set platform-bundle-version ""
Warning: Set platform version to empty will result software/firmware incompatibility
issue.
firepower /org/fw-platform-pack* # commit-buffer
firepower /org/fw-platform-pack #
```

ステップ 2 モジュールイメージをダウングレードします。

CIMC イメージを変更するには、次の例の手順に従います。

例：

```
firepower# scope server 1/1
firepower /chassis/server # scope cimc
firepower /chassis/server/cimc # update firmware <version_num>
firepower /chassis/server/cimc* # activate firmware <version_num>
firepower /chassis/server/cimc* # commit-buffer
firepower /chassis/server/cimc #
```

他のモジュールを更新するには、必要に応じてこの手順を繰り返します。

ステップ 3 新しいファームウェアバンドルをインストールします。

ダウングレードイメージをインストールするには、次の例の手順に従います。

例：

```
firepower# scope firmware
firepower /firmware # scope auto-install
firepower /firmware/auto-install # install platform platform-vers <version_num>
The currently installed FXOS platform software package is <version_num>

WARNING: If you proceed with the upgrade, the system will reboot.

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):
```

次のタスク

`firmware/auto-install` モードで **show fsm status expand** コマンドを使用すると、インストールプロセスをモニタできます。

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。