ソフトウェアおよびコンフィギュレーション

この章では、Cisco ASA ソフトウェアおよびコンフィギュレーションの管理方法について説明します。

ソフトウェアのアップグレード

完全なアップグレードの手順については、『Cisco ASA Upgrade Guide』を参照してください。

ROMMON を使用したイメージのロード

ROMMON を使用して、新しいイメージをロードできます。

ROMMON を使用した ASA 5500-X シリーズのイメージのロード

TFTP を使用して ROMMON モードから ASA へソフトウェア イメージをロードするには、次の手順を実行します。

手順

ステップ 1 アプライアンス コンソールへのアクセスに従って、ASA のコンソール ポートに接続します。

ステップ 2 ASA の電源を切ってから、また電源をオンにします。

ステップ 3 スタートアップの間に、ROMMON モードに入るようにプロンプト表示されたら、**Escape** キーを押します。

ステップ 4 ROMMON モードで、IP アドレス、TFTP サーバ アドレス、ゲートウェイ アドレス、ソフトウェア イメージ ファイル、およびポートを含む、ASA に対するインターフェイス設定を次のように定義します。

```
rommon #1> interface gigabitethernet0/0
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
```

（注） ネットワークへの接続がすでに存在することを確認してください。

インターフェイス コマンドは ASA 5506-X、ASA 5508-X、および ASA 5516-X プラットフォームで無視されるため、これらのプラットフォームで Management 1/1 インターフェイスから TFTP リカバリを実行する必要があります。

ステップ 5 設定を検証します。

```
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

ステップ 6 TFTP サーバに ping を送信します。

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

ステップ 7 ネットワーク設定を、後で使用できるように保管しておきます。

```
rommon #8> sync
Updating NVRAM Parameters...
```

ステップ 8 システム ソフトウェア イメージをロードします。

```
rommon #9> tftpdnld
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21

Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2016

Loading...
```

ソフトウェア イメージが正常にロードされると、ASA は自動的に ROMMON モードを終了します。

ステップ 9 ROMMON モードから ASA を起動する場合、システム イメージはリロード間で保持されないため、やはりイメージをフラッシュ メモリにダウンロードする必要があります。ソフトウェアのアップグレード （1 ページ）を参照してください。

ROMMON を使用した ASASM のイメージのロード

TFTP を使用して ROMMON モードから ASASM へソフトウェア イメージをロードするには、次の手順を実行します。

手順

ステップ 1 ASA サービス モジュール コンソールへのアクセスに従って、ASA のコンソール ポートに接続します。

ステップ 2 ASASM イメージをリロードすることを確認してください。

ステップ 3 スタートアップの間に、ROMMON モードに入るようにプロンプト表示されたら、**Escape** キーを押します。

ステップ 4 ROMMON モードで、IP アドレス、TFTP サーバ アドレス、ゲートウェイ アドレス、ソフトウェア イメージ ファイル、ポートおよび VLAN を含む、ASASM に対するインターフェイス設定を次のように定義します。

```
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
rommon #5> interface Data0
rommon #6> vlan 1
Data0
Link is UP
MAC Address: 0012.d949.15b8
```

（注） ネットワークへの接続がすでに存在することを確認してください。

ステップ 5 設定を検証します。

```
rommon #7> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.4
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=Data0
  VLAN=1
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=2
  RETRY=20
```

ステップ 6 TFTP サーバに ping を送信します。

```
rommon #8> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 2 seconds:

Success rate is 100 percent (20/20)
```

ステップ 7 システム ソフトウェア イメージをロードします。

```
rommon #9> tftpdnld
Clearing EOBC receive queue ...
cmostime_set = 1
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=Data0
  VLAN=1
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

```
tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21
Starting download. Press ESC to abort.
```

ソフトウェア イメージが正常にロードされると、ASASM は自動的に ROMMON モードを終了します。

ステップ 8 ROMMON モードからモジュールを起動する場合、システム イメージはリロード間で保持されないため、やはりイメージをフラッシュ メモリにダウンロードする必要があります。ソフトウェアのアップグレード （1 ページ）を参照してください。

ROMMON イメージのアップグレード（ASA 5506-X、5508-X、および 5516-X）

ASA 5506-X シリーズ、ASA 5508-X、および ASA 5516-X の ROMMON イメージをアップグレードするには、次の手順に従います。システムの ROMMON バージョンは 1.1.8 以上でなければなりません。

始める前に

新バージョンへのアップグレードのみ可能です。ダウングレードはできません。現在のバージョンを確認するには、**show module** コマンドを入力して、MAC アドレス範囲テーブルの Mod 1 の出力で Fw バージョンを調べます。

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.5        9.4(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

手順

ステップ 1 Cisco.com から新しい ROMMON イメージを取得して、サーバ上に置いて ASA にコピーします。この手順では、TFTP コピーの方法を説明します。

次の URL からイメージをダウンロードします。

https://software.cisco.com/download/type.html?mdfid=286283326&flowid=77251

ステップ 2 ROMMON イメージを ASA フラッシュ メモリにコピーします。

copy tftp://*server_ip***/asa5500-firmware-***xxxx***.SPA disk0:asa5500-firmware-***xxxx***.SPA**

ステップ 3 ROMMON イメージをアップグレードします。

upgrade rommon disk0:asa5500-firmware-*xxxx***.SPA**

例：

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

ステップ 4 プロンプトが表示されたら、確認して ASA をリロードします。

ASA が ROMMON イメージをアップグレードした後、ASA の OS をリロードします。

ASA 5506W-X ワイヤレス アクセス ポイントのイメージの回復およびロード

TFTP を使用してソフトウェア イメージを回復して ASA 5506W-X にロードするには、次の手順を実行します。

手順

ステップ 1 アクセス ポイント（AP）へのセッションを確立し、AP ROMMON（ASA ROMMON ではなく）を開始します。

```
ciscoasa# hw-module module wlan recover image
```

ステップ 2 Cisco Aironet アクセス ポイント Cisco IOS ソフトウェア コンフィギュレーション ガイド [英語] の手順に従います。

ソフトウェアのダウングレード

ダウングレードでは、以下の機能を完了するためのショートカットが存在します。

- ブート イメージ コンフィギュレーションのクリア（**clear configure boot**）。
- 古いイメージへのブート イメージの設定（**boot system**）。
- （オプション）新たなアクティベーション キーの入力（**activation-key**）。
- 実行コンフィギュレーションのスタートアップへの保存（**write memory**）。これにより、BOOT 環境変数を古いイメージに設定します。このため、リロードすると古いイメージがロードされます。
- スタートアップ コンフィギュレーションへの古いコンフィギュレーションのコピー（**copy old_config_url startup-config**）。
- リロード（**reload**）。

始める前に

- クラスタリング用の公式のゼロ ダウンタイム ダウングレードのサポートはありません。ただし場合によっては、ゼロ ダウンタイム ダウングレードが機能します。ダウングレードに関する次の既知の問題を参照してください。この他の問題が原因でクラスタ ユニットのリロードが必要になることもあり、その場合はダウンタイムが発生します。
  - スマート ライセンスの 9.10(1) からのダウングレード - スマート エージェントの変更により、ダウン グレードする場合はデバイスを Cisco Smart Software Manager に再登録する必要があります。新しいスマート エージェントでは暗号化されたファイルを使用するため、再登録して古いスマート エージェントで必要な暗号化されていないファイルを使用する必要があります。
  - クラスタリングを含む 9.9(1) より前のリリースへのダウングレード：9.9(1) 以降では、バックアップの配布が改善されています。クラスタに 3 つ以上のユニットがある場合は、次の手順を実行する必要があります。
    1. クラスタからすべてのセカンダリ ユニットを削除します（クラスタはプライマリ ユニットのみで構成されます）。
    2. 1 つのセカンダリ ユニットをダウングレードし、クラスタに再参加させます。
    3. プライマリ ユニットでクラスタリングを無効にします。そのユニットをダウングレードし、クラスタに再参加させます。

4. 残りのセカンダリユニットをダウングレードし、それらを一度に1つずつクラスタに再参加させます。

- クラスタ サイトの冗長性を有効にする場合は、9.9(1) より前のリリースにダウングレードします。ダウングレードする場合（または9.9(1) より前のユニットをクラスタに追加する場合）は、サイトの冗長性を無効にする必要があります。そうしないと、古いバージョンを実行しているユニットにダミーの転送フローなどの副作用が発生します。
- クラスタリングおよび暗号マップを使用する場合に9.8(1) からダウングレードする：暗号マップが設定されている場合に 9.8 (1) からダウングレードすると、ゼロ ダウンタイム ダウングレードはサポートされません。ダウングレード前に暗号マップ設定をクリアし、ダウングレード後に設定をもう一度適用する必要があります。
- クラスタリング ユニットのヘルスチェックを 0.3 ～ 0.7 秒に設定した状態で 9.8(1) からダウングレードする：（**health-check holdtime**で）ホールド時間を 0.3 ～ 0.7 秒に設定した後で ASA ソフトウェアをダウングレードすると、新しい設定はサポートされないため、設定値はデフォルトの 3 秒に戻ります。
- クラスタリング（CSCuv82933）を使用している場合に9.5(2) 以降から9.5(1) 以前にダウングレードする：9.5(2) からダウングレードする場合、ゼロ ダウンタイム ダウングレードはサポートされません。ユニットがオンラインに戻ったときに新しいクラスタが形成されるように、すべてのユニットをほぼ同時にリロードする必要があります。ユニットが順番にリロードされるのを待つと、クラスタを形成できなくなります。
- クラスタリングを使用する場合に 9.2(1) 以降から 9.1 以前にダウングレードする：ゼロ ダウンタイム ダウングレードはサポートされません。

- PBKDF2（パスワード ベースのキー派生関数 2）ハッシュをパスワードで使用する場合に9.5 以前のバージョンにダウングレードする：9.6 より前のバージョンは PBKDF2 ハッシュをサポートしていません。9.6(1) では、32 文字より長い **enable** パスワードおよび **username** パスワードで PBKDF2 ハッシュを使用します。9.7(1) では、すべての新しいパスワードは、長さに関わらず PBKDF2 ハッシュを使用します（既存のパスワードは引き続き MD5 ハッシュを使用します）。ダウングレードすると、**enable** パスワードがデフォルト（空白）に戻ります。ユーザ名は正しく解析されず、**username** コマンドが削除されます。ローカル ユーザをもう一度作成する必要があります。
- ASAv 用のバージョン 9.5(2.200) からのダウングレード：ASAv はライセンス登録状態を保持しません。**license smart register idtoken id_token force** コマンドで再登録する必要があります（ASDM の場合、[Configuration] > [Device Management] > [Licensing] > [Smart Licensing] ページで [Force registration] オプションを使用）。Smart Software Manager から ID トークンを取得します。
- 設定を移行すると、ダウングレードの可否に影響を与える可能性があります。そのため、ダウングレード時に使用できる古い設定のバックアップを保持することを推奨します。8.3 へのアップグレード時には、バックアップが自動的に作成されます（<old_version>_startup_cfg.sav）。他の移行ではバックアップが作成されません。古いバージョンでは利用できなかったコマンドが新しい設定に含まれていると、設定がロードされ

たときにそれらのコマンドのエラーが表示されます。ただし、エラーは無視できます。各バージョンの設定の移行または廃止の詳細については、各バージョンのアップグレードガイドを参照してください。

- 元のトンネルがネゴシエートした暗号スイートをサポートしないソフトウェアバージョンをスタンバイ装置が実行している場合でも、VPNトンネルがスタンバイ装置に複製されます。このシナリオは、ダウングレード時に発生します。その場合、VPN接続を切断して再接続してください。

手順

ステップ1 **[Tools]** > **[Downgrade Software]** を選択します。

[Downgrade Software] ダイアログボックスが表示されます。

ステップ2 ASA イメージの場合、[Select Image File] をクリックします。

[Browse File Locations] ダイアログボックスが表示されます。

ステップ3 次のいずれかのオプション ボタンをクリックします。

- [Remote Server]：ドロップダウン リストで [ftp]、[smb]、[http] のいずれかを選択し、以前のイメージ ファイルのパスを入力します。
- [Flash File System]：[Browse Flash] をクリックして、ローカル フラッシュ ファイル システムにある以前のイメージ ファイルを選択します。

ステップ4 [Configuration] で [Browse Flash] をクリックし、移行前の設定ファイルを選択します。

ステップ5 （任意） バージョン 8.3 よりも前のアクティベーション キーに戻す場合は、[Activation Key] フィールドで以前のアクティベーション キーを入力します。

ステップ6 [Downgrade] をクリックします。

ファイルの管理

ASDM には、基本的なファイル管理タスクを実行するのに便利なファイル管理ツール セットが用意されています。ファイル管理ツールにより、フラッシュ メモリに保存されているファイルの表示、移動、コピー、および削除、ファイルの転送、およびリモート ストレージ デバイス（マウント ポイント）のファイルの管理を行うことができます。

（注） マルチコンテキスト モードの場合、このツールはシステムのセキュリティ コンテキストでだけ使用できます。

ファイル アクセスの設定

ASA では、FTP クライアント、セキュア コピー クライアント、または TFTP クライアントを使用できます。また、ASA をセキュア コピー サーバとして設定することもできるため、コンピュータでセキュア コピー クライアントを使用できます。

FTP クライアント モードの設定

ASA では、FTP サーバとの間で、イメージ ファイルやコンフィギュレーション ファイルのアップロードおよびダウンロードを実行できます。パッシブ FTP では、クライアントは制御接続およびデータ接続の両方を開始します。パッシブ モードではデータ接続の受け入れ側となるサーバは、今回の特定の接続においてリッスンするポート番号を応答として返します。

手順

ステップ 1 [Configuration] > [Device Management] > [Management Access] > [File Access] > [FTP Client] ペインで、[Specify FTP mode as passive] チェックボックスをオンにします。

ステップ 2 [Apply] をクリックします。

FTP クライアントのコンフィギュレーションが変更され、その変更内容が実行コンフィギュレーションに保存されます。

セキュア コピー サーバとしての ASA の設定

ASA 上でセキュア コピー（SCP）サーバをイネーブルにできます。SSH による ASA へのアクセスを許可されたクライアントだけが、セキュア コピー接続を確立できます。

始める前に

- サーバにはディレクトリ サポートがありません。ディレクトリ サポートがないため、ASA の内部ファイルへのリモート クライアント アクセスは制限されます。
- サーバでは、バナーまたはワイルドカードがサポートされていません。
- ASDM、Telnet、または SSH 用の ASA アクセスの設定 に従って、ASA で SSH を有効にします。
- SSH バージョン 2 接続をサポートするには、ASA のライセンスに強力な暗号化（3DES/AES）ライセンスが必要です。
- 特に指定されていないかぎり、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次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

- セキュア コピーのパフォーマンスは、使用する暗号化アルゴリズムにある程度依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。提示された暗号方式を変更するには、**[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]** ペインを使用します。たとえば、**[Custom]** を選択して aes128-cbc に設定します。

手順

ステップ 1 コンテキスト モードによって次のように異なります。

- シングル モードの場合、[Configuration] > [Device Management] > [Management Access] > [File Access] > [Secure Copy (SCP)] の順に選択します。
- マルチ モードの場合、[Configuration] > [Device Management] > [Device Administration] > [Secure Copy] の順に選択します。

ステップ 2 [Enable secure copy server] チェック ボックスをオンにします。

ステップ 3 （オプション）ASA は接続先の各 SCP サーバの SSH ホストキーを保存します。必要に応じて、ASA データベースから手動でサーバとそのキーを追加または削除できます。

キーを追加するには、次の手順を実行します。

a) 新しいサーバの [Add] をクリックするか、または信頼できる SSH ホストのテーブルからサーバを選択し、[Edit] をクリックします。
b) 新しいサーバの [Host] フィールドに、サーバの IP アドレスを入力します。
c) [Add public key for the trusted SSH host] チェックボックスをオンにします。
d) 次のいずれかのキーを指定します。
   - フィンガープリント：すでにハッシュされているキーを入力します。たとえば、**show** コマンドの出力からコピーしたキーです。
   - キー：SSH ホストの公開キーまたはハッシュ値を入力します。キー ストリングはリモート ピアの Base64 で符号化された RSA 公開キーです。オープン SSH クライアントから（言い換えると .ssh/id_rsa.pub ファイルから）公開キー値を取得できます。Base64 で符号化された公開キーを送信した後、SHA-256 によってそのキーがハッシュされます。

キーを削除するには、信頼できる SSH ホストのテーブルからサーバを選択し、[Delete] をクリックします。

ステップ 4 （オプション）新しいホストキーが検出されたときに通知を受け取るには、[Inform me when a new host key is detected] チェックボックスをオンにします。

デフォルトで、このオプションは有効になっています。このオプションがイネーブルになっている場合、ASA にまだ格納されていないホストキーを許可または拒否するように求められま

す。このオプションがディセーブルになっている場合、ASA は過去に保存されたことがないホストキーを自動的に許可します。

ステップ 5 [Apply] をクリックします。

例

外部ホストのクライアントから、SCP ファイル転送を実行します。たとえば、Linux では次のコマンドを入力します。

scp -v -pw *password source_filename username@asa_address*:{**disk0**|**disk1**}:/*dest_filename*

-v は冗長を表します。**-pw** が指定されていない場合は、パスワードの入力を求めるプロンプトが表示されます。

ASA TFTP クライアントのパス設定

TFTP は、単純なクライアント/サーバ ファイル転送プロトコルで、RFC 783 および RFC 1350 Rev. 2 で規定されています。TFTP サーバとの間でファイルをコピーできるように、ASA を TFTP クライアントとして設定できます。これにより、コンフィギュレーション ファイルをバックアップし、それらを複数の ASA にプロパゲートできます。

ここでは、TFTP サーバへのパスを事前定義できるため、**copy** および **configure net** などのコマンドで入力する必要がなくなります。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[File Access]** > **[TFTP Client]** の順に選択し、[Enable] チェックボックスをオンにします。

ステップ 2 [Interface Name] ドロップダウン リストから、TFTP クライアントとして使用するインターフェイスを選択します。

ステップ 3 コンフィギュレーション ファイルの保存先とする TFTP サーバの IP アドレスを [IP Address] フィールドに入力します。

ステップ 4 コンフィギュレーション ファイルの保存先とする TFTP サーバへのパスを [Path] フィールドに入力します。

例：/tftpboot/asa/config3

ステップ 5 **Apply** をクリックします。

マウント ポイントの追加

CIFS マウント ポイントまたは FTP マウント ポイントを追加できます。

CIFS マウント ポイントの追加

共通インターネット ファイル システム（CIFS）マウント ポイントを定義するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[File Access]** > **[Mount-Points]** の順に選択し、**[Add]** > **[CIFS Mount Point]** の順にクリックします。

[Add CIFS Mount Point] ダイアログボックスが表示されます。

ステップ 2 [Enable mount point] チェックボックスをオンにします。

これにより、ASA 上の CIFS ファイル システムが UNIX のファイル ツリーに接続されます。

ステップ 3 [Mount Point Name] フィールドに、既存の CIFS が存在する位置の名前を入力します。

ステップ 4 [Server Name] フィールドまたは [IP Address] フィールドに、マウント ポイントを配置するサーバの名前または IP アドレスを入力します。

ステップ 5 [Share Name] フィールドに、CIFS サーバ上のフォルダの名前を入力します。

ステップ 6 [NT Domain Name] フィールドに、サーバが常駐する NT ドメインの名前を入力します。

ステップ 7 サーバに対するファイル システムのマウントを認可されているユーザの名前を、[User Name] フィールドに入力します。

ステップ 8 サーバに対するファイルシステムのマウントを認可されているユーザのパスワードを、[Password] フィールドに入力します。

ステップ 9 [Confirm Password] フィールドにパスワードを再入力します。

ステップ 10 [OK] をクリックします。

[Add CIFS Mount Point] ダイアログボックスが閉じます。

ステップ 11 [Apply] をクリックします。

FTP マウント ポイントの追加

FTP マウント ポイントの場合、FTP サーバには UNIX のディレクトリ リスト スタイルが必要です。Microsoft FTP サーバには、デフォルトで MS-DOS ディレクトリ リスト スタイルがあります。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Management Access]** > **[File Access]** > **[Mount-Points]** の順に選択し、**[Add]** > **[FTP Mount Point]** の順にクリックします。

[Add FTP Mount Point] ダイアログボックスが表示されます。

ステップ 2 [Enable] チェックボックスを選択します。

これにより、ASA 上の FTP ファイル システムが UNIX のファイル ツリーに接続されます。

ステップ 3 [Mount Point Name] フィールドに、既存の FTP が存在する位置の名前を入力します。

ステップ 4 [Server Name] フィールドまたは [IP Address] フィールドに、マウント ポイントを配置するサーバの名前または IP アドレスを入力します。

ステップ 5 [Mode] フィールドで、オプション ボタン（[Active] または [Passive]）をクリックして FTP モードを選択します。[Passive] モードを選択した場合、クライアントでは、FTP コントロール接続とデータ接続がともに起動します。サーバは、この接続をリッスンするポートの番号で応答します。

ステップ 6 FTP ファイル サーバへのディレクトリ パス名を [Path to Mount] フィールドに入力します。

ステップ 7 サーバに対するファイル システムのマウントを認可されているユーザの名前を、[User Name] フィールドに入力します。

ステップ 8 サーバに対するファイルシステムのマウントを認可されているユーザのパスワードを、[Password] フィールドに入力します。

ステップ 9 [Confirm Password] フィールドにパスワードを再入力します。

ステップ 10 [OK] をクリックします。

[Add FTP Mount Point] ダイアログボックスが閉じます。

ステップ 11 [Apply] をクリックします。

ファイル管理ツールへのアクセス

ファイル管理ツールを使用するには、次の手順を実行します。

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]** > **[File Management]** の順に選択します。

[File Management] ダイアログボックスが表示されます。

- [Folders] ペインには、ディスク上にあるフォルダが表示されます。
- [Flash Space] は、フラッシュ メモリの合計容量と、使用可能なメモリ容量を示します。
- [Files] 領域には、選択したフォルダのファイルについて次の情報が表示されます。
  - パス
  - ファイル名
  - サイズ（バイト単位）
  - 修正時刻

- 選択したファイルの種類（ブート コンフィギュレーション、ブート イメージ ファイル、ASDM イメージ ファイル、SVC イメージ ファイル、CSD イメージ ファイル、または APCF イメージ ファイル）を示す、ステータス

ステップ 2 選択したファイルをブラウザに表示するには、[View] をクリックします。

ステップ 3 選択したファイルを切り取って別のディレクトリに貼り付けるには、[Cut] をクリックします。

ステップ 4 選択したファイルをコピーして別のディレクトリに貼り付けるには、[Copy] をクリックします。

ステップ 5 コピーしたファイルを選択した場所に貼り付けるには、[Paste] をクリックします。

ステップ 6 選択したファイルをフラッシュ メモリから削除するには、[Delete] をクリックします。

ステップ 7 ファイルの名前を変更するには、[Rename] をクリックします。

ステップ 8 ファイルを保存するディレクトリを新規作成するには、[New Directory] をクリックします。

ステップ 9 [File Transfer] ダイアログボックスを開くには、[File Transfer] をクリックします。詳細については、「ファイルの転送 （15 ページ）」を参照してください。

ステップ 10 [Manage Points] ダイアログボックスを開くには、[Mount Points] をクリックします。詳細については、「マウント ポイントの追加 （12 ページ）」を参照してください。

ファイルの転送

File Transfer ツールにより、ローカルにあるファイルとリモートにあるファイルを転送できます。PC またはフラッシュ ファイル システムのローカル ファイルを ASA との間で転送できます。HTTP、HTTPS、TFTP、FTP、または SMB を使用して、ASA との間でファイルを転送できます。

（注） IPS SSP ソフトウェア モジュールの場合、IPS ソフトウェアを disk0 にダウンロードする前に、フラッシュ メモリに少なくとも 50% の空きがあることを確認してください。IPS をインストールするときに、IPS のファイル システム用に内部フラッシュ メモリの 50% が予約されます。

ローカル PC とフラッシュ間でのファイル転送

ローカル PC とフラッシュ ファイル システムとの間でファイルを転送するには、次の手順を実行します。

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]** > **[File Management]** の順に選択します。

[File Management] ダイアログボックスが表示されます。

ステップ 2 [File Transfer] の横にある下矢印をクリックし、続いて [Between Local PC and Flash] をクリックします。

[File Transfer] ダイアログボックスが表示されます。

ステップ 3 ローカル PC またはフラッシュ ファイル システムのどちらかで、アップロードまたはダウンロードしたいファイルを選択し、目的の場所にドラッグします。または、ローカル PC またはフラッシュ ファイル システムのどちらかで、アップロードまたはダウンロードしたいファイルを選択し、右矢印または左矢印をクリックし、目的の場所にファイルを転送します。

ステップ 4 完了したら [Close] をクリックします。

リモート サーバとフラッシュ間でのファイル転送

リモート サーバとフラッシュ ファイル システムとの間でファイルを転送するには、次の手順を実行します。

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]** > **[File Management]** の順に選択します。

[File Management] ダイアログボックスが表示されます。

ステップ 2 [File Transfer] ドロップダウン リストで下矢印をクリックし、[Between Remote Server and Flash] をクリックします。

[File Transfer] ダイアログボックスが表示されます。

ステップ 3 リモート サーバからファイルを転送するには、[Remote server] オプションをクリックします。

ステップ 4 転送対象になるソース ファイルを定義します。

a) （オプション）ASA がサーバとの通信に使用するインターフェイスを指定します。インターフェイスを指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。

b) サーバの IP アドレスを含めたファイルの場所へのパスを選択します。

（注） ファイル転送は IPv4 および IPv6 のアドレスをサポートしています。

c) FTP の場合はリモート サーバのタイプを、HTTP または HTTPS の場合はリモート サーバのポート番号を入力します。有効な FTP タイプは次のとおりです。

- ap：パッシブ モードの ASCII ファイル
- an：非パッシブ モードの ASCII ファイル
- ip：パッシブ モードのバイナリ イメージ ファイル
- in：非パッシブ モードのバイナリ イメージ ファイル

ステップ 5 フラッシュ ファイル システムからファイルを転送するには、[Flash file system] オプションを選択します。

ステップ 6 ファイルの場所へのパスを入力するか、[Browse Flash] をクリックしてファイルの場所を指定します。

ステップ 7 また、CLIにより、スタートアップ コンフィギュレーション、実行コンフィギュレーション、または SMB ファイル システムからファイルをコピーすることもできます。**Copy** コマンドの使用方法については、CLI コンフィギュレーション ガイドを参照してください。

ステップ 8 転送するファイルの宛先を定義します。

a) フラッシュ ファイル システムにファイルを転送するには、[Flash file system] オプションを選択します。

b) ファイルの場所へのパスを入力するか、[Browse Flash] をクリックしてファイルの場所を指定します。

ステップ 9 リモート サーバにファイルを転送するには、[Remote server] オプションを選択します。

a) （オプション）ASA がサーバとの通信に使用するインターフェイスを指定します。インターフェイスを指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。

b) ファイルの場所へのパスを入力します。

c) FTP 転送の場合はタイプを入力します。有効なタイプは次のとおりです。

- ap：パッシブ モードの ASCII ファイル
- an：非パッシブ モードの ASCII ファイル
- ip：パッシブ モードのバイナリ イメージ ファイル
- in：非パッシブ モードのバイナリ イメージ ファイル

ステップ 10 [Transfer] をクリックしてファイル転送を開始します。

[Enter Username and Password] ダイアログボックスが表示されます。

ステップ 11 リモート サーバのユーザ名、パスワード、ドメイン（必要な場合）が表示されます。

ステップ 12 [OK] をクリックし、ファイル転送を続行します。

ファイル転送プロセスには数分かかる場合があります。必ず終了するまでお待ちください。

ステップ 13 ファイル転送が完了したら [Close] をクリックします。

ASA イメージ、ASDM、およびスタートアップ コンフィギュレーションの設定

複数の ASA または ASDM イメージがある場合は、ブートするイメージを指定する必要があります。イメージを設定しない場合はデフォルトのブートイメージが使用され、そのイメージは意図されたものではない可能性があります。スタートアップ コンフィギュレーションでは、コンフィギュレーション ファイルを任意で指定できます。

次のデフォルト設定を参照してください。

- ASA イメージ：
  - 物理 ASA：内部フラッシュ メモリ内で見つかった最初のアプリケーション イメージをブートします。
  - ASAv：最初に展開したときに作成された、読み取り専用の boot:/ パーティションにあるイメージをブートします。
  - Firepower 4100/9300 シャーシ 上の ASA：FXOS システムが、起動する ASA イメージを決定します。この手順を使用して ASA イメージを設定することはできません。
  - Firepower 2100：FXOS システムが、起動する ASA/FXOS パッケージを決定します。この手順を使用して ASA イメージを設定することはできません。
- すべての ASA の ASDM イメージ：内部フラッシュ メモリ内で見つかった（またはここにイメージがない場合は、外部フラッシュ メモリ内で見つかった）最初の ASDM イメージをブートします。
- スタートアップ コンフィギュレーション：デフォルトでは、ASA は、隠しファイルであるスタートアップ コンフィギュレーションからブートします。

始める前に

- Firepower 4100/9300 シャーシ：ASA のアップグレードは FXOS によって管理されます。ASA オペレーティング システム内で ASA をアップグレードすることはできません。したがって、この手順を ASA イメージに使用しないでください。ASA と FXOS を別々にアップグレードすることができ、FXOS ディレクトリ リストに別々にリストされます。ASA パッケージには常に ASDM が含まれています。
- Firepower 2100：ASA、ASDM、および FXOS のイメージは 1 つのパッケージにバンドルされています。パッケージ更新は FXOS によって管理されます。ASA オペレーティング システム内で ASA をアップグレードすることはできません。したがって、この手順を ASA イメージに使用しないでください。ASA と FXOS を個別にアップグレードすることはできません。常にバンドルされています。
- Firepower 2100 および Firepower 4100/9300 シャーシ の ASDM：ASDM は ASA オペレーティング システム内からアップグレードできるため、バンドルされた ASDM イメージのみを

使用する必要はありません。手動でアップロードする ASDM イメージは FXOS イメージ リストに表示されません。ASA から ASDM イメージを管理する必要があります。

（注） FXOS で 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、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。ただし、アップロードした別の ASDM イメージ（たとえば **asdm-782.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 ASDM バージョンを実行していることを確認するには、バンドルをアップグレードする前に ASDM をアップグレードするか、または ASA バンドルをアップグレードする直前に、バンドルされた ASDM イメージ（**asdm.bin**）を使用するように ASA を再設定する必要があります。

- ASAv：初期展開の ASAv パッケージでは、ASA イメージが読み取り専用 boot:/ パーティションに配置されます。ASAv をアップグレードするときは、フラッシュ メモリに別のイメージを指定します。後でコンフィギュレーションをクリアすると、ASAv は元の展開のイメージをロードするようになることに注意してください。初期展開の ASAv パッケージには、フラッシュ メモリに配置される ASDM イメージも含まれています。ASDM イメージを個別にアップグレードできます。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[System Image/Configuration]** > **[Boot Image/Configuration]** の順に選択します。

起動イメージとして使用するバイナリ イメージ ファイルは、ローカルから 4 つまで指定できます。また TFTP サーバのイメージを 1 つ指定し、そこからデバイスをブートできます。TFTP サーバに格納されているイメージを指定する場合は、そのファイルをリスト内の先頭に配置する必要があります。デバイスが、イメージのロード元の TFTP サーバに到達できない場合は、フラッシュ メモリに保存されているリスト内の次のイメージ ファイルのロードが試行されます。

ステップ 2 [Boot Image/Configuration] ペインで [Add] をクリックします。

ステップ 3 ブートするイメージを参照します。TFTP イメージの場合は、[File Name] フィールドに TFTP URL を入力します。[OK] をクリックします。

ステップ 4 上へ移動ボタンと下へ移動ボタンを使用してイメージの順番を並べ替えます。

ステップ 5 （オプション）[Boot Configuration File Path] フィールドで、[Browse Flash] をクリックしてコンフィギュレーションを選択してスタートアップ コンフィギュレーション ファイルを指定します。[OK] をクリックします。

ステップ 6 [ASDM Image File Path] フィールドで、[Browse Flash] をクリックしてイメージを選択して ASDM イメージを指定します。[OK] をクリックします。

ステップ 7 [Apply] をクリックします。

コンフィギュレーションまたはその他のファイルのバックアップおよび復元

システム障害から保護するために、コンフィギュレーションおよびその他のファイルの定期的なバックアップを実行することを推奨します。

完全なシステム バックアップまたは復元の実行

次の手順では、コンフィギュレーションおよびイメージの zipバックアップ zip ファイルへのバックアップおよび復元方法と、そのファイルのローカル コンピュータへの転送方法について説明します。

バックアップまた復元を開始する前に

- バックアップまたは復元を開始する前に、バックアップまたは復元場所に使用可能なディスク領域が少なくとも 300 MB ある必要があります。
- ASA は、シングル コンテキスト モードである必要があります。
- バックアップ中またはバックアップ後にコンフィギュレーションを変更した場合、その変更内容はバックアップに含められません。バックアップの実行後にコンフィギュレーションを変更してから復元を実行した場合、このコンフィギュレーションの変更は上書きされます。結果として、ASA は異なる挙動をすることもあります。
- 一度に開始できるバックアップまたは復元は 1 つだけです。
- コンフィギュレーションは、元のバックアップを実行したときと同じ ASA バージョンにのみ復元できます。復元ツールを使用して、ASA の異なるバージョン間でコンフィギュレーションを移行することはできません。コンフィギュレーションの移行が必要な場合、ASA は、新しい ASA OS をロードした時に常駐するスタートアップ コンフィギュレーションを自動的にアップグレードします。
- クラスタリングを使用する場合、バックアップまたは復元できるのは、スタートアップ コンフィギュレーション、実行コンフィギュレーション、およびアイデンティティ証明書のみです。ユニットごとに別々にバックアップを作成および復元する必要があります。
- フェールオーバーを使用する場合、バックアップの作成および復元は、アクティブユニットとスタンバイ ユニットに対して別々に行う必要があります。

- ASA にマスター パスフレーズを設定している場合は、この手順で作成したバックアップ コンフィギュレーションの復元時にそのマスター パスフレーズが必要となります。ASA のマスターパスフレーズが不明な場合は、マスターパスフレーズの設定を参照して、バックアップを続行する前に、マスター パスフレーズをリセットする方法を確認してください。
- PKCS12 データをインポート（**crypto ca trustpoint** コマンドを使用）する際にトラストポイントが RSA キーを使用している場合、インポートされたキー ペアにはトラストポイントと同じ名前が割り当てられます。この制約のため、ASDM コンフィギュレーションを復元した後でトラストポイントおよびそのキー ペアに別の名前を指定した場合、スタートアップ コンフィギュレーションは元のコンフィギュレーションと同じになるのに、実行コンフィギュレーションには異なるキー ペア名が含まれることになります。つまり、キー ペアとトラストポイントに別の名前を使用した場合は、元のコンフィギュレーションを復元できないということです。この問題を回避するため、トラストポイントとそのキーペアには必ず同じ名前を使用してください。
- CLI を使用してバックアップしてから ASDM を使用して復元したり、その逆を行うことはできません。
- 各バックアップ ファイルに含まれる内容は次のとおりです。
  - 実行コンフィギュレーション
  - スタートアップ コンフィギュレーション
  - すべてのセキュリティ イメージ

    Cisco Secure Desktop およびホスト スキャンのイメージ

    Cisco Secure Desktop およびホスト スキャンの設定

    AnyConnect（SVC）クライアントのイメージおよびプロファイル

    AnyConnect（SVC）のカスタマイズおよびトランスフォーム
  - アイデンティティ証明書（アイデンティティ証明書に関連付けられた RSA キー ペアは含まれるが、スタンドアロン キーは除外される）
  - VPN 事前共有キー
  - SSL VPN コンフィギュレーション
  - Application Profile Custom Framework（APCF）
  - Bookmarks
  - カスタマイゼーション
  - ダイナミック アクセス ポリシー（DAP）
  - プラグイン
  - 接続プロファイル用の事前入力スクリプト
  - プロキシ自動設定

- 変換テーブル
- Web コンテンツ
- バージョン情報

システムのバックアップ

この手順では、完全なシステム バックアップを実行する方法について説明します。

手順

ステップ 1 コンピュータ上にフォルダを作成し、バックアップ ファイルを保存します。こうすると、後で復元するときに探しやすくなります。

ステップ 2 **[Tools]** > **[Backup Configurations]** を選択します。

[Backup Configurations] ダイアログボックスが表示されます。[SSL VPN Configuration] 領域の下矢印をクリックし、SSL VPN コンフィギュレーションのバックアップ オプションを確認します。デフォルトでは、すべてのコンフィギュレーション ファイルがチェックされ、利用できる場合にはバックアップされます。リスト内のすべてのファイルをバックアップするには、手順 5 に進みます。

ステップ 3 バックアップするコンフィギュレーションを選択する場合は、[Backup All] チェックボックスをオフにします。

ステップ 4 バックアップするオプションの横にあるチェックボックスをオンにします。

ステップ 5 [Browse Local to specify a directory and file name for the backup .zip file] をクリックします。

ステップ 6 [Select] ダイアログボックスで、バックアップ ファイルを格納するディレクトリを選択します。

ステップ 7 [Select] をクリックします。[Backup File] フィールドにパスが表示されます。

ステップ 8 ディレクトリ パスの後にバックアップ ファイルの宛先の名前を入力します。バックアップ ファイルの名前の長さは、3 ～ 232 文字の間である必要があります。

ステップ 9 [Backup] をクリックします。証明書をバックアップする場合や、ASA でマスター パスフレーズを使用している場合を除き、すぐにバックアップが続行されます。

ステップ 10 ASA でマスター パスフレーズを設定し、イネーブルにしている場合、バックアップを続行する前に、マスターパスフレーズが不明な場合は変更することを推奨する警告メッセージが表示されます。マスター パスフレーズがわかっている場合は、[Yes] をクリックしてバックアップを続行します。ID 証明書をバックアップする場合を除き、すぐにバックアップが続行されます。

ステップ 11 ID 証明書をバックアップする場合は、証明書を PKCS12 形式でエンコーディングするために使用する別のパスフレーズを入力するように求められます。パスフレーズを入力するか、またはこの手順をスキップすることができます。

（注） このプロセスで ID 証明書はバックアップされますが、認証局の証明書はバックアップされません。CA 証明書のバックアップ手順については、ローカル CA サーバのバックアップ （24 ページ）を参照してください。

- 証明書を暗号化するには、[Certificate Passphrase] ダイアログボックスで証明書のパスフレーズを入力および確認し、[OK] をクリックします。証明書の復元時に必要となるため、このダイアログボックスに入力したパスワードを覚えておく必要があります。
- [Cancel] をクリックすると、この手順がスキップされ、証明書はバックアップされません。

[OK] または [Cancel] をクリックすると、すぐにバックアップが開始されます。

ステップ 12 バックアップが完了すると、ステータス ウィンドウが閉じ、[Backup Statistics] ダイアログボックスが表示され、成功または失敗のメッセージが示されます。

（注） バックアップの「失敗」メッセージは多くの場合、指定されたタイプの既存のコンフィギュレーションが存在しない場合に表示されます。

ステップ 13 [OK] をクリックし、[Backup Statistics] ダイアログボックスを閉じます。

バックアップの復元

zip tar.gz ファイルからローカル PC に復元するコンフィギュレーションやイメージを指定します。

手順

ステップ 1 **[Tools]** > **[Restore Configurations]** を選択します。

ステップ 2 [Restore Configurations] ダイアログボックスで、[Browse Local Directory] をクリックし、ローカル コンピュータ上の、復元するコンフィギュレーションが含まれている zip ファイルを選択し、[Select] をクリックします。[Local File] フィールドにパスと zip ファイル名が表示されます。

復元する zip ファイルは、[Tools] > [Backup Configurations] オプションを選択して作成したものである必要があります。

ステップ 3 [Next] をクリックします。2 つ目の [Restore Configuration] ダイアログボックスが表示されます。復元するコンフィギュレーションの横にあるチェックボックスをオンにします。使用可能なすべての SSL VPN コンフィギュレーションがデフォルトで選択されています。

ステップ 4 [Restore] をクリックします。

ステップ 5 バックアップ ファイルの作成時に、証明書の暗号化に使用する証明書パスフレーズを指定している場合は、このパスフレーズを入力するように ASDM から求められます。

ステップ 6 実行コンフィギュレーションの復元を選択した場合、実行コンフィギュレーションを結合するか、実行コンフィギュレーションを置換するか、または復元プロセスのこの部分をスキップするかを尋ねられます。

- コンフィギュレーションの結合では、現在の実行コンフィギュレーションとバックアップされた実行コンフィギュレーションが結合されます。

- 実行コンフィギュレーションの置換では、バックアップされた実行コンフィギュレーションのみが使用されます。
- この手順をスキップすると、バックアップされた実行コンフィギュレーションは復元されません。

ASDM では、復元操作が完了するまでステータス ダイアログボックスが表示されます。

ステップ 7 実行コンフィギュレーションを置換または結合した場合は、ASDM を閉じてから再起動します。実行コンフィギュレーションを復元しなかった場合は、ASDMセッションをリフレッシュして、変更を有効にします。

ローカル CA サーバのバックアップ

ASDM バックアップを実行した場合、ローカル CA サーバ データベースは含まれていないため、サーバ上の CA 証明書はバックアップされません。ローカル CA サーバをバックアップする場合は、ASA CLI による次の手動プロセスを使用します。

手順

ステップ 1 **show run crypto ca server** コマンドを入力します。

```
crypto ca server
 keysize server 2048
 subject-name-default OU=aa,O=Cisco,ST=ca,
 issuer-name CN=xxx,OU=yyy,O=Cisco,L=Bxb,St=Mass
 smtp from-address abcd@cisco.com
 publish-crl inside 80
 publish-crl outside 80
```

ステップ 2 **crypto ca import** コマンドを使用して、ローカル CA PKCS12 ファイルをインポートして LOCAL-CA-SERVER トラストポイントを作成し、キーペアを復元します。

```
crypto ca import LOCAL-CA-SERVER pkcs12 <passphrase> (paste the pkcs12
base64 data here)
```

（注） この手順では、正確な名前「LOCAL-CA-SERVER」を必ず使用してください。

ステップ 3 LOCAL-CA-SERVER ディレクトリが存在しない場合、**mkdir LOCAL-CA-SERVER** を入力して作成する必要があります。

ステップ 4 ローカル CA ファイルを LOCAL-CA-SERVER ディレクトリにコピーします。

```
copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.ser
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.cdb
```

```
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.udb
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.crl
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.p12
disk0:/LOCAL-CA-SERVER/
```

ステップ 5 **crypto ca server** コマンドを入力して、ローカル CA サーバをイネーブルにします。

```
crypto ca server
 no shutdown
```

ステップ 6 **show crypto ca server** コマンドを入力して、ローカル CA サーバが起動し、動作していることを確認します。

ステップ 7 設定を保存します。

TFTP サーバへの実行コンフィギュレーションの保存

この機能により、現在の実行コンフィギュレーション ファイルのコピーを TFTP サーバに保存します。

手順

ステップ 1 **[File]** > **[Save Running Configuration to TFTP Server]** を選択します。

[Save Running Configuration to TFTP Server] ダイアログボックスが表示されます。

ステップ 2 TFTP サーバの IP アドレスと、コンフィギュレーション ファイルの保存先となる TFTP サーバ上のファイル パスを入力して、[Save Configuration] をクリックします。

（注） デフォルトの TFTP 設定を行うには、[Configuration] > [Device Management] > [Management Access] > [File Access] > [TFTP Client] の順に選択します。この設定を行った後は、このダイアログボックスに、TFTP サーバの IP アドレスと TFTP サーバ上でのファイル パスが自動的に表示されます。

システム再起動のスケジュール

System Reload ツールにより、システムの再起動をスケジュールしたり、現在の再起動をキャンセルしたりできます。

手順

ステップ 1 **[Tools]** > **[System Reload]** を選択します。

ステップ 2 [Reload Scheduling] 領域で、次の設定を定義します。

a) [Configuration State] では、再起動時に実行コンフィギュレーションを保存するか、破棄するかのどちらかを選択します。

b) [Reload Start Time] では、次のオプションから選択します。

- 再起動をただちに実行するには、[Now] をクリックします。
- 指定した時間だけ再起動を遅らせるには、[Delay by] をクリックします。再起動開始までの時間を、時間と分単位、または分単位だけで入力します。
- 指定した時刻と日付に再起動を実行するようにスケジュールするには、[Schedule at] をクリックします。再起動の実行時刻を入力し、再起動のスケジュール日を選択します。

c) [Reload Message] フィールドに、再起動時に開いている ASDM インスタンスに送信するメッセージを入力します。

d) 再起動を再試行するまでの経過時間を時間と分単位で、または分単位だけで表示するには、[On reload failure force immediate reload after] チェックボックスをオンにします。

e) 設定に従って再起動をスケジュールするには、[Schedule Reload] をクリックします。

[Reload Status] 領域には、再起動のステータスが表示されます。

ステップ 3 次のいずれかを選択します。

- スケジュールされた再起動を停止するには、[Cancel Reload] をクリックします。
- スケジュールされた再起動の終了後に [Reload Status] 表示をリフレッシュするには、[Refresh] をクリックします。
- スケジュールされた再起動の詳細を表示するには、[Details] をクリックします。

Auto Update の設定

Auto Update は、Auto Update サーバがコンフィギュレーションおよびソフトウェア イメージを多数の ASA にダウンロードすることを許可し、中央からの ASA の基本的なモニタリングを提供するプロトコル仕様です。

Auto Update について

この項では、Auto Update の実装方法と Auto Update が必要になる理由について説明します。

Auto Update クライアントまたはサーバ

ASA は、クライアントまたはサーバとして設定できます。Auto Update クライアントとして動作する場合は、ソフトウェアイメージおよびコンフィギュレーション ファイルへのアップデートのため、Auto Update サーバを定期的にポーリングします。Auto Update サーバとして動作する場合は、Auto Update クライアントとして設定された ASA のアップデートを発行します。

Auto Update の利点

Auto Update は、次のように、管理者が ASA の管理で直面するさまざまな問題を解決できる便利な機能です。

- ダイナミック アドレッシングおよび NAT に関する問題点の解決。
- コンフィギュレーションの変更を 1 つのアクションでコミット。
- ソフトウェア更新用の信頼度の高い方式の提供。
- ハイ アベイラビリティ用の十分実績のある方式の活用（フェールオーバー）。
- オープン インターフェイスによる柔軟性の提供。
- サービス プロバイダー環境のセキュリティ ソリューションの簡素化。

Auto Update 仕様は、中央、または複数の場所から、リモート管理アプリケーションにより ASA のコンフィギュレーションやソフトウェアイメージをダウンロードしたり、基本的な監視機能を実行したりする場合に必要なインフラストラクチャです。

Auto Update 仕様に従うと、Auto Update サーバから ASA にコンフィギュレーション情報をプッシュしたり、要求を送信して情報を取得したりすることも、ASA から Auto Update サーバに定期的にポーリングすることによって、最新のコンフィギュレーション情報を引き出す（プルする）こともできます。また、Auto Update サーバはいつでも ASA にコマンドを送信し、ただちにポーリング要求を送信させることもできます。Auto Update サーバと ASA の通信では、通信パスとローカル CLI コンフィギュレーションをすべての ASA に設定する必要があります。

フェールオーバー設定での Auto Update サーバ サポート

Auto Update サーバを使用して、ソフトウェア イメージとコンフィギュレーション ファイルを、アクティブ/スタンバイ フェールオーバー コンフィギュレーションの ASA に配置できます。アクティブ/スタンバイ フェールオーバー コンフィギュレーションで Auto Update をイネーブルにするには、フェールオーバー ペアのプライマリ装置に Auto Update サーバのコンフィギュレーションを入力します。

フェールオーバー コンフィギュレーションの Auto Update サーバ サポートには、次の制限と動作が適用されます。

- アクティブ/スタンバイ コンフィギュレーションがサポートされるのは、シングル モードだけです。
- 新しいプラットフォーム ソフトウェア イメージをロードする際、フェールオーバー ペアはトラフィックの転送を停止します。

- LAN ベースのフェールオーバーを使用する場合、新しいコンフィギュレーションによってフェールオーバー リンクのコンフィギュレーションが変更されてはいけません。フェールオーバー リンクのコンフィギュレーションが変更されると、装置間の通信は失敗します。
- Auto Update サーバへの Call Home を実行するのはプライマリ装置だけです。Call Home を実行するには、プライマリ装置がアクティブ状態である必要があります。そうでない場合、ASA は自動的にプライマリ装置にフェールオーバーします。
- ソフトウェアイメージまたはコンフィギュレーションファイルをダウンロードするのは、プライマリ装置だけです。その後、ソフトウェアイメージまたはコンフィギュレーションファイルはセカンダリ装置にコピーされます。
- インターフェイス MAC アドレスとハードウェアのシリアル番号は、プライマリ装置のものです。
- Auto Update サーバまたは HTTP サーバに保存されたコンフィギュレーション ファイルは、プライマリ装置専用です。

Auto Update プロセスの概要

次に、フェールオーバー コンフィギュレーションでの Auto Update プロセスの概要を示します。このプロセスは、フェールオーバーがイネーブルであり、動作していることを前提としています。装置がコンフィギュレーションを同期化している場合、SSM カードの不具合以外の理由でスタンバイ装置に障害が発生している場合、または、フェールオーバー リンクがダウンしている場合、Auto Update プロセスは実行できません。

1. 両方の装置は、プラットフォームおよび ASDM ソフトウェア チェックサムとバージョン情報を交換します。
2. プライマリ装置は Auto Update サーバにアクセスします。プライマリ装置がアクティブ状態でない場合、ASA はプライマリ装置にフェールオーバーした後、Auto Update サーバにアクセスします。
3. Auto Update サーバは、ソフトウェア チェックサムと URL 情報を返します。
4. プライマリ装置が、アクティブまたはスタンバイ装置のプラットフォーム イメージ ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
    1. プライマリ装置は、Auto Update サーバの URL を使用して、HTTP サーバから適切なファイルを取得します。
    2. プライマリ装置は、そのイメージをスタンバイ装置にコピーしてから、自身のイメージをアップデートします。
    3. 両方の装置に新しいイメージがある場合は、セカンダリ（スタンバイ）装置が最初にリロードされます。
        - セカンダリ装置のブート時にヒットレス アップグレードが可能な場合は、セカンダリ装置がアクティブ装置になり、プライマリ装置がリロードされます。リロードが終了すると、プライマリ装置がアクティブ装置になります。

- スタンバイ装置のブート時にヒットレス アップグレードができない場合は、両方の装置が同時にリロードされます。

4. セカンダリ（スタンバイ）装置だけに新しいイメージがある場合は、セカンダリ装置だけがリロードされます。プライマリ装置は、セカンダリ装置のリロードが終了するまで待機します。
5. プライマリ（アクティブ）装置だけに新しいイメージがある場合は、セカンダリ装置がアクティブ装置になり、プライマリ装置がリロードされます。
6. もう一度アップデート プロセスが手順 1 から開始されます。

5. ASA が、プライマリまたはセカンダリ装置の ASDM ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
   1. プライマリ装置は、Auto Update サーバから提供された URL を使用して、HTTP サーバから ASDM イメージ ファイルを取得します。
   2. プライマリ装置は、必要に応じてそのイメージをスタンバイ装置にコピーします。
   3. プライマリ装置は、自身の ASDM イメージをアップデートします。
   4. もう一度アップデート プロセスが手順 1 から開始されます。
6. プライマリ装置が、コンフィギュレーション ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
   1. プライマリ装置は、指定された URL を使用して、からコンフィギュレーション ファイルを取得します。
   2. 両方の装置で同時に、古いコンフィギュレーションが新しいコンフィギュレーションに置換されます。
   3. もう一度アップデート プロセスが手順 1 から開始されます。
7. チェックサムがすべてのイメージおよびコンフィギュレーション ファイルと一致している場合、アップデートは必要ありません。このプロセスは、次のポーリング時間まで中断されます。

Auto Update のガイドライン

コンテキスト モード

Auto Update は、シングル コンテキスト モードでのみサポートされます。

クラスタ

クラスタリングはサポートされません。

モデル

次のモデルではサポートされません。

- ASA 5506-X、5508-X、5516-X
- Firepower 2100、4100、および 9300
- ASAv

その他のガイドライン

- Auto Update サーバから ASA のコンフィギュレーションが更新されても、ASDM には通知されません。**[Refresh]** または **[File] > [RefreshASDM** with the Running Configuration on the Device] を選択して、最新のコンフィギュレーションを取得する必要があります。また、ASDM でコンフィギュレーションに加えた変更は失われます。
- Auto Update サーバと通信するためのプロトコルとして HTTPS が選択されている場合は、ASA は SSL を使用します。これは、ASA による DES または 3DES ライセンスの保有が必須です。

Auto Update サーバとの通信の設定

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[System Image/Configuration]** > **[Auto Update]** を選択します。

[Auto Update] ペインには、[Auto Update Servers] テーブルの他に [Timeout] 領域と [Polling] 領域があります。

[Auto Update Servers] テーブルで、Auto Update サーバにすでに設定されているパラメータを確認できます。ASA は、テーブルの一番上にあるサーバを最初にポーリングします。

ステップ 2 テーブル内のサーバの順序を変更するには、[Move Up] または [Move Down] をクリックします。

[Auto Update Servers] テーブルには次のカラムがあります。

- [Server]：Auto Update サーバの名前または IP アドレス。
- [User Name]：Auto Update サーバのアクセス時に使用されるユーザ名。
- [Interface]：Auto Update サーバへの要求送信時に使用されるインターフェイス。
- [Verify Certificate]：Auto Update サーバが返した証明書を、ASA で CA のルート証明書と照合して確認するかどうかを指定します。Auto Update サーバおよび ASA は同じ CA を使用する必要があります。

ステップ 3 [Auto Update Server] テーブルの行のいずれかをダブルクリックすると、[Edit Auto Update Server] ダイアログボックスが開き、Auto Update サーバのパラメータを変更できます。ここで行った変更はただちにテーブルに反映されますが、コンフィギュレーションに保存するには [Apply] をクリックする必要があります。

ステップ 4 [Timeout] エリアでは、ASA が Auto Update サーバのタイムアウトを待つ時間を設定できます。[Timeout] 領域には次のフィールドがあります。

- [Enable Timeout Period]：ASA が Auto Update サーバから応答を受信しなかった場合にタイムアウトするには、オンにします。
- [Timeout Period (Minutes)]：Auto Update サーバから応答がなかった場合の ASA のタイムアウト時間（分単位）を指定します。

ステップ 5 [Polling] エリアで、ASA から Auto Update サーバの情報をポーリングする頻度を設定できます。[Polling] 領域には次のフィールドがあります。

- [Polling Period (minutes)]：ASA から Auto Update サーバに新しい情報をポーリングするときの待ち時間（分単位）。
- [Poll on Specified Days]：ポーリングのスケジュールを指定します。
- [Set Polling Schedule]：[Set Polling Schedule] ダイアログボックスが表示され、Auto Update サーバをポーリングする日付と時刻を設定できます。
- [Retry Period (minutes)]：サーバのポーリングに失敗した場合、ASA から Auto Update サーバに新しい情報をポーリングするまでの待ち時間（分単位）。
- [Retry Count]：ASA から Auto Update サーバに新しい情報をポーリングするときの再試行回数。

ステップ 6 ポーリング スケジュールの設定

[Set Polling Schedule] ダイアログボックスでは、ASA から Auto Update サーバをポーリングする特定の日付と時刻を設定できます。

[Set Polling Schedule] ダイアログボックスには次のフィールドがあります。

[Days of the Week]：ASA から Auto Update サーバをポーリングする曜日のチェックボックスを選択します。

[Daily Update] ペイン グループでは、ASA が Auto Update サーバをポーリングする時刻を設定できます。次のフィールドがあります。

- [Start Time]：Auto Update のポーリング開始時刻を入力します。
- [Enable randomization]：ASA から Auto Update サーバをランダムに選択した時刻にポーリングするには、オンにします。

Auto Update のモニタリング

Auto Update プロセスのモニタリング

debug auto-update client または **debug fover cmd-exe** コマンドを使用して、Auto Update プロセスで実行される処理を表示できます。次に、**debug auto-update client** コマンドの出力例を示します。**debug**ターミナル セッションからコマンドを実行します。

```
Auto-update client: Sent DeviceDetails to /cgi-bin/dda.pl of server 192.168.0.21
Auto-update client: Processing UpdateInfo from server 192.168.0.21
   Component: asdm, URL: http://192.168.0.21/asdm.bint, checksum:
0x94bced0261cc992ae710faf8d244cf32
   Component: config, URL: http://192.168.0.21/config-rms.xml, checksum:
0x67358553572688a805a155af312f6898
   Component: image, URL: http://192.168.0.21/cdisk73.bin, checksum:
0x6d091b43ce96243e29a62f2330139419
Auto-update client: need to update img, act: yes, stby yes
name
ciscoasa(config)# Auto-update client: update img on stby unit...
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 9001, len = 1024
auto-update: Fover file copy waiting at clock tick 6129280
fover_parse: Rcvd file copy ack, ret = 0, seq = 4
auto-update: Fover filecopy returns value: 0 at clock tick 6150260, upd time 145980 msecs
Auto-update client: update img on active unit...
fover_parse: Rcvd image info from mate
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
Beginning configuration replication: Sending to mate.
auto-update: HA safe reload: reload active waiting with mate state: 50
```

```
auto-update: HA safe reload: reload active waiting with mate state: 50

auto-update: HA safe reload: reload active waiting with mate state: 80
        Sauto-update: HA safe reload: reload active unit at clock tick: 6266860
Auto-update client: Succeeded: Image, version: 0x6d091b43ce96243e29a62f2330139419
```

Auto Update プロセスが失敗すると、次の syslog メッセージが生成されます。

```
%ASA4-612002: Auto Update failed: file version: version reason: reason
```

file は、失敗したアップデートに応じて “image”、“asdm”、または “configuration” になります。*version* は、アップデートのバージョン番号です。*reason* は、アップデートが失敗した原因です。

ソフトウェアとコンフィギュレーションの履歴

機能名	プラットフォーム リリース	機能情報
セキュア コピー クライアント	9.1(5)/9.2(1)	SCP サーバとの間でファイルを転送するため、ASA は Secure Copy（SCP）クライアントをサポートするようになりました。 次の画面が変更されました。 [Tools] > [File Management] > [File Transfer] > [Between Remote Server and Flash] [Configuration] > [Device Management] > [Management Access] > [File Access] > [Secure Copy (SCP) Server]
設定可能な SSH 暗号機能と整合性アルゴリズム	9.1(7)/9.4(3)/9.5(3)/9.6(1)	ユーザは SSH 暗号化を管理するときに暗号化モードを選択し、さまざまなキー交換アルゴリズムに対して HMAC と暗号化を設定できます。アプリケーションに応じて、暗号の強度を強くしたり弱くする必要がある場合があります。セキュアなコピーのパフォーマンスは暗号化アルゴリズムに一部依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。たとえば、提示された暗号方式に変更するには、**ssh cipher encryption custom aes128-cbc** を使用します。 次の画面が導入されました。**[Configuration]** > **[Device Management]** > **[Advanced]** > **[SSH Ciphers]**

機能名	プラットフォーム リリース	機能情報
デフォルトでイネーブルになっている Auto Update サーバ証明書の検証	9.2(1)	Auto Update サーバ証明書の検証がデフォルトでイネーブルになりました。新しいコンフィギュレーションでは証明書の検証を明示的にディセーブルにする必要があります。証明書の確認をイネーブルにしていなかった場合に、以前のリリースからアップグレードしようとすると、証明書の確認はイネーブルではなく、次の警告が表示されます。 `WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.` 設定を移行する場合は、次のように確認なしを明示的に設定します。 次の画面が変更されました。[Configuration] > [Device Management] > [System/Image Configuration] > [Auto Update] > [Add Auto Update Server]。
CLI を使用したシステムのバックアップと復元	9.3(2)	CLI を使用してイメージや証明書を含む完全なシステムコンフィギュレーションをバックアップおよび復元できるようになりました。 変更された ASDM 画面はありません。
新しい ASA 5506W-X イメージの回復およびロード	9.4(1)	新しい ASA 5506W-X イメージのリカバリおよびロードがサポートされています。 変更された ASDM 画面はありません。