使用する前に

タスク フロー

次に、Firepower 4100/9300 シャーシを設定する際に実行する必要がある基本的なタスクの手順を示します。

手順

ステップ 1 Firepower 4100/9300 シャーシ ハードウェアを設定します（『*Cisco Firepower Security Appliance Hardware Installation Guide*』を参照）。

ステップ 2 初期設定を完了します（初期設定 （2 ページ）を参照）。

ステップ 3 Firepower Chassis Manager にログインします（Firepower Chassis Manager のログイン/ログアウト （5 ページ）を参照）。

ステップ 4 日付と時刻を設定します（日時の設定を参照）。

ステップ 5 DNS サーバを設定します（DNS サーバの設定を参照）。

ステップ 6 製品ライセンスを登録します（ASA のライセンス管理を参照）。

ステップ 7 ユーザを設定します（User Managementを参照）。

ステップ 8 必要に応じてソフトウェア アップデートを実行します（イメージ管理を参照）。

ステップ 9 追加のプラットフォーム設定を行います（Platform Settingsを参照）。

ステップ 10 インターフェイスを設定します（インターフェイス管理を参照）。

ステップ 11 論理デバイスを作成します（論理デバイスを参照）。

初期設定

システムの設定と管理に Firepower Chassis Manager または FXOS CLI を使用するには、まず、コンソール ポートを介してアクセスした FXOS CLI を使用して初期設定タスクを実行する必要があります。FXOS CLI を使用して Firepower 4100/9300 シャーシに初めてアクセスすると、システムの設定に使用できるセットアップ ウィザードが表示されます。

システム設定を既存のバックアップ ファイルから復元するか、セットアップ ウィザードを実行してシステムを手動でセットアップするか、選択できます。システムを復元する場合は、バックアップ ファイルが、管理ネットワークから到達可能な場所に存在する必要があります。

Firepower 4100/9300 シャーシの単一の管理ポートには、1 つのみの IPv4 アドレス、ゲートウェイ、サブネット マスク、または 1 つのみの IPv6 アドレス、ゲートウェイ、ネットワーク プレフィックスを指定する必要があります。管理ポートの IP アドレスに対して IPv4 または IPv6 アドレスのいずれかを設定できます。

始める前に

1. Firepower 4100/9300 シャーシの次の物理接続を確認します。
   - コンソール ポートがコンピュータ端末またはコンソール サーバに物理的に接続されている。
   - 1 Gbps イーサネット管理ポートが外部ハブ、スイッチ、またはルータに接続されている。

   詳細については、『*Cisco Firepower Security Appliance Hardware Installation Guide*』を参照してください。
2. コンソール ポートに接続しているコンピュータ端末（またはコンソール サーバ）でコンソール ポート パラメータが次のとおりであることを確認します。
   - 9600 ボー
   - 8 データ ビット
   - パリティなし
   - 1 ストップ ビット

手順

ステップ 1 コンソール ポートに接続します。

ステップ 2 Firepower 4100/9300 シャーシの電源を入れます。

Firepower 4100/9300 シャーシが起動すると、電源投入時セルフテスト メッセージが表示されます。

ステップ 3 未設定のシステムが起動すると、セットアップ ウィザードでシステム設定に必要な次の情報の入力を求められます。

- セットアップ モード（フル システム バックアップからの復元または初期セットアップ）
- 強力なパスワードの適用ポリシー（強力なパスワードのガイドラインについては、ユーザアカウントを参照）
- admin パスワード
- システム名
- 管理ポートの IPv4 アドレスとサブネット マスク、または IPv6 アドレスとプレフィックス
- デフォルトのゲートウェイの IPv4 アドレスまたは IPv6 アドレス
- SSH アクセス用 IP ブロック アドレス
- SSH アクセス用 IPv4 または IPv6 ブロック ネットマスク
- HTTPS アクセス用 IP ブロック アドレス
- HTTPS アクセス用 IPv4 または IPv6 ブロック ネットマスク
- DNS サーバの IPv4 または IPv6 アドレス
- デフォルトのドメイン名

ステップ 4 設定の要約を確認し、設定を保存および適用する場合は **yes** を入力し、セットアップ ウィザードをやり直して設定を変更する場合は **no** を入力します。

セットアップ ウィザードのやり直しを選択した場合は、以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

例

次の例では、IPv4 管理アドレスを使用して設定します。

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) [y]: n
Enter the password for "admin": adminpassword%958
Confirm the password for "admin": adminpassword%958
Enter the system name: foo
Physical Switch Mgmt0 IP address : 192.168.10.10
Physical Switch Mgmt0 IPv4 netmask: 255.255.255.0
IPv4 address of the default gateway: 192.168.10.1
Do you want to configure IP block for ssh access? (yes/no) [y]: y
  SSH IPv4 block netmask: 0.0.0.0
Do you want to configure IP block for https access? (yes/no) [y]: y
  HTTPS IP block address: 0.0.0.0
  HTTPS IPv4 block netmask: 0.0.0.0
Configure the DNS Server IP address (yes/no) [n]:y
  DNS IP address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: y
```

```
  Default domain name: domainname.com
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Enforce Strong Password=no
  Physical Switch Mgmt0 IP Address=192.168.10.10
  Physical Switch Mgmt0 IP Netmask=255.255.255.0
  Default Gateway=192.168.10.1
  IPv6 value=0
  SSH Access Configured=yes
      SSH IP Address=0.0.0.0
      SSH IP Netmask=0.0.0.0
  HTTPS Access Configured=yes
      HTTPS IP Address=0.0.0.0
      HTTPS IP Netmask=0.0.0.0
  DNS Server=20.10.20.10
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

次の例では、IPv6 管理アドレスを使用して設定します。

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) [y]: n
Enter the password for "admin": adminpassword%652
Confirm the password for "admin": adminpassword%652
Enter the system name: foo
Physical Switch Mgmt0 IP address :  2001::107
Physical Switch Mgmt0 IPv6 prefix: 64
IPv6 address of the default gateway: 2001::1
Do you want to configure IP block for ssh access? (yes/no) [y]: y
  SSH IPv6 block netmask: 0.0.0.0
Do you want to configure IP block for https access? (yes/no) [y]: y
  HTTPS IP block address: 0.0.0.0
  HTTPS IPv6 block netmask: 0.0.0.0
Configure the DNS Server IPv6 address? (yes/no) [n]: y
  DNS IP address: 2001::101
Configure the DNS Server IP address (yes/no) [n]:
Configure the default domain name? (yes/no) [n]: y
  Default domain name: domainname.com
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Enforced Strong Password=no
  Physical Switch Mgmt0 IPv6 Address=2001::107
  Physical Switch Mgmt0 IPv6 Prefix=64
  Default Gateway=2001::1
  Ipv6 value=1
  SSH Access Configured=yes
      SSH IP Address=0.0.0.0
      SSH IP Netmask=0.0.0.0
  HTTPS Access Configured=yes
      HTTPS IP Address=0.0.0.0
      HTTPS IP Netmask=0.0.0.0
  DNS Server=2001::101
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

Firepower Chassis Manager のログイン/ログアウト

Firepower Chassis Manager を使用して Firepower 4100/9300 シャーシ を設定するには、その前に、有効なユーザ アカウントを使用してログオンする必要があります。ユーザ アカウントの詳細については、User Managementを参照してください。

一定期間にわたって操作がない場合は、自動的にシステムからログアウトされます。デフォルトでは、10 分間にわたり操作を行わないと自動的にログアウトします。このタイムアウト設定を変更するには、セッション タイムアウトの設定を参照してください。 また、セッションがアクティブな場合でも、一定時間の経過後にユーザをシステムからログオフさせるように絶対タイムアウトを設定することもできます。絶対タイムアウトを設定するには、絶対セッション タイムアウトの設定を参照してください。

システムを変更した結果、Firepower Chassis Manager から自動的にログアウトされる場合の一覧については、セッション変更により Firepower Chassis Manager セッションが閉じる場合を参照してください。

（注） 指定した時間でユーザがシステムからロックアウトされる前に、ログイン試行の失敗を特定の数だけ許可するように Firepower Chassis Manager を任意で設定できます。詳細については、ログイン試行の最大回数の設定を参照してください。

手順

ステップ 1 Firepower Chassis Manager にログインするには、次の手順を実行します。

a) サポートされているブラウザを使用して、アドレス バーに次の URL を入力します。

```
https://<chassis_mgmt_ip_address>
```

ここで、<*chassis_mgmt_ip_address*> は、初期設定時に入力した Firepower 4100/9300 シャーシ の IP アドレスまたはホスト名です。

（注） サポートされるブラウザの詳細については、使用しているバージョンのリリース ノートを参照してください（http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list を参照）。

b) ユーザ名とパスワードを入力します。

c) [Login] をクリックします。

ログインすると Firepower Chassis Manager が開き、[Overview] ページが表示されます。

ステップ 2 Firepower Chassis Manager からログアウトするには、ナビゲーション バーに表示されている自分のユーザ名をポイントし、[Logout] を選択します。
Firepower Chassis Manager からログアウトすると、ログイン画面に戻ります。

FXOS CLIへのアクセス

FXOS CLIには、コンソール ポートに繋いだ端末を使って接続します。コンソール ポートに接続しているコンピュータ端末（またはコンソール サーバ）でコンソール ポート パラメータが次のとおりであることを確認します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

SSH と Telnet を使用しても FXOS CLI に接続できます。Firepower eXtensible Operating System は最大 8 つの SSH 接続を同時にサポートできます。SSH で接続するには、Firepower 4100/9300 シャーシ のホスト名または IP アドレスが必要になります。

次のいずれかの構文例を使用して SSH、Telnet または Putty でログインします。

（注） SSH ログインでは大文字と小文字が区別されます。

Linux 端末からは以下の SSH を使用します。

- **ssh ucs-***auth-domain**username*@{*UCSM-ip-address* | *UCMS-ipv6-address*}

  ```
  ssh ucs-example\\jsmith@192.0.20.11
  ssh ucs-example\\jsmith@2001::1
  ```

- **ssh -l ucs-***auth-domain**username* {*UCSM-ip-address*| *UCSM-ipv6-address*| *UCSM-host-name*}

  ```
  ssh -l ucs-example\\jsmith 192.0.20.11
  ssh -l ucs-example\\jsmith 2001::1
  ```

- **ssh** {*UCSM-ip-address* | *UCSM-ipv6-address* | *UCSM-host-name*} **-l ucs-***auth-domain**username*

  ```
  ssh 192.0.20.11 -l ucs-example\\jsmith
  ssh 2001::1 -l ucs-example\\jsmith
  ```

- **ssh ucs-***auth-domain**username*@{*UCSM-ip-address* | *UCSM-ipv6-address*}

  ```
  ssh ucs-ldap23\\jsmith@192.0.20.11
  ssh ucs-ldap23\\jsmith@2001::1
  ```

Linux 端末からは以下の Telnet を使用します。

（注） Telnet はデフォルトでディセーブルです。Telnet を有効化する手順については、Telnet の設定を参照してください。

- **telnet ucs-***UCSM-host-name* **ucs-***auth-domain**username*

```
telnet ucs-qa-10
login: ucs-ldap23\blradmin
```

- **telnet ucs-**{*UCSM-ip-address* | *UCSM-ipv6-address*}*ucs-auth-domain**username*

```
telnet 10.106.19.12 2052
ucs-qa-10-A login: ucs-ldap23\blradmin
```

Putty クライアントから：

- **ucs-***auth-domain**username* でログインします。

```
Login as: ucs-example\jsmith
```

（注） デフォルトの認証がローカルに設定され、コンソール認証がLDAPに設定されている場合は、**ucs-local\admin**（admin はローカル アカウント名）を使用して Putty クライアントからファブリック インターコネクトにログインできます。