システム管理

管理 IP アドレスの変更

はじめる前に

FXOS CLI から Firepower 4100/9300 シャーシの管理 IP アドレスを変更できます。

（注） 管理 IP アドレスを変更した後、新しいアドレスを使用して Firepower Chassis Manager または FXOS CLI への接続を再確立する必要があります。

手順

ステップ 1 FXOS CLI に接続します（FXOS CLIへのアクセスを参照）。

ステップ 2 IPv4 管理 IP アドレスを設定するには、次の手順を実行します。

a) fabric-interconnect a のスコープを設定します。
Firepower-chassis# **scopefabric-interconnecta**

b) 現在の管理 IP アドレスを表示するには、次のコマンドを入力します。
Firepower-chassis /fabric-interconnect # **show**

c) 次のコマンドを入力して、新しい管理 IP アドレスとゲートウェイを設定します。
Firepower-chassis /fabric-interconnect # **setout-of-band staticip** *ip_address***netmask** *network_mask***gw** *gateway_ip_address*

d) トランザクションをシステムの設定に対して確定します。
Firepower-chassis /fabric-interconnect* # **commit-buffer**

ステップ 3 IPv6 管理 IP アドレスを設定するには、次の手順を実行します。

a) fabric-interconnect a のスコープを設定します。
Firepower-chassis# **scopefabric-interconnecta**

b) 管理 IPv6 設定のスコープを設定します。
Firepower-chassis /fabric-interconnect # **scopeipv6-config**

c) 現在の管理 IPv6 アドレスを表示するには、次のコマンドを入力します。
Firepower-chassis /fabric-interconnect/ipv6-config # **show ipv6-if**

d) 次のコマンドを入力して、新しい管理 IP アドレスとゲートウェイを設定します。
Firepower-chassis /fabric-interconnect/ipv6-config # **setout-of-band staticipv6** *ipv6_address***ipv6-prefix** *prefix_length***ipv6-gw** *gateway_address*

e) トランザクションをシステムの設定に対して確定します。
Firepower-chassis /fabric-interconnect/ipv6-config* # **commit-buffer**

次の例では、IPv4 管理インターフェイスとゲートウェイを設定します。

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    192.0.2.112     192.0.2.1       255.255.255.0   ::               ::
 64     Operable
Firepower-chassis /fabric-interconnect # set out-of-band static ip 192.0.2.111 netmask
255.255.255.0 gw 192.0.2.1
Warning: When committed, this change may disconnect the current CLI session
Firepower-chassis /fabric-interconnect* #commit-buffer
Firepower-chassis /fabric-interconnect #
```

次の例では、IPv6 管理インターフェイスとゲートウェイを設定します。

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                      Prefix     IPv6 Gateway
    --------------------------------- ---------- ------------
    2001::8998                        64         2001::1
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001::8999
 ipv6-prefix 64 ipv6-gw 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #
```

アプリケーション管理 IP の変更

FXOS CLI から Firepower 4100/9300 シャーシに接続されたアプリケーションの管理 IP アドレスは変更できます。そのためには、まずFXOSプラットフォーム レベルでIP情報を変更し、次にアプリケーション レベルで IP 情報を変更する必要があります。

（注） Firepower Chassis Manager を使用してこれらの変更を行おうとすると、サービスが中断される可能性があります。サービスが中断する可能性を避けるために、これらの変更は、FXOS CLI を使用して実行する必要があります。

手順

ステップ 1 FXOS CLI に接続します。（FXOS CLIへのアクセス を参照）。

ステップ 2 範囲を論理デバイスにします。
scopessa

scopelogical-device *logical_device_name*

ステップ 3 範囲を管理ブートストラップにし、新しい管理ブートストラップ パラメータを設定します。導入間で違いがあることに注意してください。
ASA 論理デバイスのスタンドアロンの設定の場合。

a) 論理デバイス管理ブートストラップを入力します。
scopemgmt-bootstrap *asa*

b) スロットを IP モードにします。
scope *ipv4_or_6 slot_number* default

c) （IPv4 のみ）新しい IP アドレスを設定します。
setip *ipv4_address***mask** *network_mask*

d) （IPv6 のみ）新しい IP アドレスを設定します。
setip *ipv6_address***prefix-length** *prefix_length_number*

e) ゲートウェイ アドレスを設定します。
setgateway *gateway_ip_address*

f) 設定を確定します。
commit-buffer

ASA 論理デバイスのクラスタ設定の場合。

a) クラスタ管理ブートストラップを入力します。
scopecluster-bootstrap *asa*

b) （IPv4 のみ）新しい仮想 IP を設定します。
setvirtualipv4 *ip_address***mask** *network_mask*

c) （IPv6 のみ）新しい仮想 IP を設定します。
setvirtualipv6 *ipv6_address***prefix-length** *prefix_length_number*

d) 新しい IP プールを設定します。
setippool *start_ip end_ip*

e) ゲートウェイ アドレスを設定します。
setgateway *gateway_ip_address*

f) 設定を確定します。
commit-buffer

Firepower Threat Defense のスタンドアロン設定およびクラスタ設定の場合。

a) 論理デバイス管理ブートストラップを入力します。
scopemgmt-bootstrap *ftd*

b) スロットを IP モードにします。
scope *ipv4_or_6 slot_number* firepower

c) （IPv4 のみ）新しい IP アドレスを設定します。
setip *ipv4_address***mask** *network_mask*

d) （IPv6 のみ）新しい IP アドレスを設定します。
setip *ipv6_address***prefix-length** *prefix_length_number*

e) ゲートウェイ アドレスを設定します。
setgateway *gateway_ip_address*

f) 設定を確定します。
commit-buffer

（注） クラスタ設定の場合、Firepower 4100/9300 シャーシに接続されているアプリケーションごとに新しい IP アドレスを設定する必要があります。シャーシ間クラスタまたは HA 設定の場合、両方のシャーシでアプリケーションごとにこれらのステップを繰り返す必要があります。

ステップ 4 アプリケーションごとに管理ブートストラップ情報をクリアします。

a) 範囲を ssa モードにします。
scopessa

b) 範囲をスロットにします。
scopeslot *slot_number*

c) 範囲をアプリケーション インスタンスにします。
scopeapp-instance *asa_or_ftd*

d) 管理ブートストラップ情報をクリアします。
clearmgmt-bootstrap

e) 設定を確定します。
commit-buffer

ステップ 5 アプリケーションを無効にします。
disable

commit-buffer

（注） クラスタ設定の場合、Firepower 4100/9300 シャーシに接続されているアプリケーションごとに管理ブートストラップ情報をクリアし、無効にする必要があります。シャーシ間クラスタまたはHA設定の場合、両方のシャーシでアプリケーションごとにこれらのステップを繰り返す必要があります。

ステップ 6 アプリケーションがオフラインで、スロットが再度オンラインになったときに、アプリケーションを再度有効にします。

a) 範囲を ssa モードに戻します。
scopessa

b) 範囲をスロットにします。
scopeslot *slot_number*

c) 範囲をアプリケーション インスタンスにします。
scopeapp-instance *asa_or_ftd*

d) アプリケーションを有効にします。
enable

e) 設定を確定します。
commit-buffer

（注） クラスタ設定の場合、これらのステップを繰り返して、Firepower 4100/9300 シャーシに接続されている各アプリケーションを再度有効にします。シャーシ間クラスタまたはHA 設定の場合、両方のシャーシでアプリケーションごとにこれらのステップを繰り返す必要があります。

Firepower 4100/9300 シャーシ 名前の変更

はじめる前に

Firepower 4100/9300 シャーシに使用する名前を FXOS CLI から変更することができます。

手順

ステップ 1 FXOS CLI に接続します（FXOS CLIへのアクセスを参照）。

ステップ 2 システム モードに入ります。
Firepower-chassis-A# **scopesystem**

ステップ 3 現在の名前を表示するには：
Firepower-chassis-A /system # **show**

ステップ 4 新しい名前を設定するには：
Firepower-chassis-A /system # **setname** *device_name*

ステップ 5 トランザクションをシステム設定に確定するには：
Firepower-chassis-A /fabric-interconnect* # **commit-buffer**

次の例では、デバイス名を変更します。

```
Firepower-chassis-A# scope system
Firepower-chassis-A /system # set name New-name
Warning: System name modification changes FC zone name and redeploys them non-disruptively
Firepower-chassis-A /system* # commit-buffer
Firepower-chassis-A /system # show

Systems:
    Name       Mode        System IP Address System IPv6 Address
    ---------- ----------- ------------------ -------------------
    New-name   Stand Alone 192.168.100.10     ::
New-name-A /system #
```

ログイン前バナー

ログイン前バナーでは、ユーザが Firepower Chassis Manager にログインするとシステムにバナーテキストが表示されます。ユーザ名とパスワードのシステム プロンプトの前に、メッセージの画面で[OK]をクリックする必要があります。ログイン前バナーを設定しないと、システムはユーザ名とパスワードのプロンプトにすぐに進みます。

ユーザが FXOS CLI にログインすると、設定されている場合はシステムがパスワードのプロンプトの前にログイン バナー テキストを表示します。

ログイン前バナーの作成

手順

ステップ 1 FXOS CLI に接続します（FXOS CLIへのアクセスを参照）。

ステップ 2 セキュリティ モードに入ります。
Firepower-chassis# **scopesecurity**

ステップ 3 バナー セキュリティ モードに入ります。
Firepower-chassis /security # **scopebanner**

ステップ 4 次のコマンドを入力して、ログイン前バナーを作成します。
Firepower-chassis /security/banner # **create pre-login-banner**

ステップ 5 Firepower Chassis Manager または FXOS CLI へのログイン前のユーザに FXOS が表示するメッセージを指定します。
Firepower-chassis /security/banner/pre-login-banner* # **set message**

ログイン前バナー メッセージのテキストを入力するためのダイアログを開始します。

ステップ 6 プロンプトで、ログイン前バナー メッセージを入力します。このフィールドには、標準の ASCII 文字を入力できます。複数行のテキストを入力できますが、各行の最大文字数は 192 文字です。行の区切りで Enter キーを押します。

入力内容の次の行に ENDOFBUF と入力し、Enter キーを押して終了します。

[メッセージの設定（set message）] ダイアログをキャンセルするには、Ctrl+C キーを押します。

ステップ 7 トランザクションをシステムの設定に対して確定します。
Firepower-chassis /security/banner/pre-login-banner* # **commit-buffer**

次の例は、ログイン前バナーを作成します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # create pre-login-banner
Firepower-chassis /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

ログイン前バナーの変更

手順

ステップ 1 FXOS CLI に接続します（FXOS CLIへのアクセスを参照）。

ステップ 2 セキュリティ モードに入ります。
Firepower-chassis# **scopesecurity**

ステップ 3 バナー セキュリティ モードに入ります。
Firepower-chassis /security # **scopebanner**

ステップ 4 ログイン前バナーのバナー セキュリティ モードに入ります。
Firepower-chassis /security/banner # **scope pre-login-banner**

ステップ 5 Firepower Chassis Manager または FXOS CLI へのログイン前のユーザに FXOS が表示するメッセージを指定します。
Firepower-chassis /security/banner/pre-login-banner # **set message**

ログイン前バナー メッセージのテキストを入力するためのダイアログを開始します。

ステップ 6 プロンプトで、ログイン前バナー メッセージを入力します。このフィールドには、標準の ASCII 文字を入力できます。複数行のテキストを入力できますが、各行の最大文字数は 192 文字です。行の区切りで Enter キーを押します。
入力内容の次の行に ENDOFBUF と入力し、Enter キーを押して終了します。

[メッセージの設定（set message）] ダイアログをキャンセルするには、Ctrl+C キーを押します。

ステップ 7 トランザクションをシステムの設定に対して確定します。
Firepower-chassis /security/banner/pre-login-banner* # **commit-buffer**

次に、ログイン前バナーを変更する例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # scope pre-login-banner
Firepower-chassis /security/banner/pre-login-banner # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

ログイン前バナーの削除

手順

ステップ 1 FXOS CLI に接続します（FXOS CLIへのアクセスを参照）。

ステップ 2 セキュリティ モードに入ります。
Firepower-chassis# **scopesecurity**

ステップ 3 バナー セキュリティ モードに入ります。
Firepower-chassis /security # **scopebanner**

ステップ 4 システムからログイン前バナーを削除します。
Firepower-chassis /security/banner # **delete pre-login-banner**

ステップ 5 トランザクションをシステムの設定に対して確定します。
Firepower-chassis /security/banner* # **commit-buffer**

次に、ログイン前バナーを削除する例を示します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # delete pre-login-banner
Firepower-chassis /security/banner* # commit-buffer
Firepower-chassis /security/banner #
```

Firepower 4100/9300 シャーシ の再起動

手順

ステップ 1 シャーシ モードに入ります。
scope chassis 1

ステップ 2 次のコマンドを入力して、シャーシをリブートします。

reboot [理由] **[no-prompt]**

（注） **[no-prompt]** キーワードを使用した場合、コマンドを入力するとシャーシはすぐにリブートします。**[no-prompt]** キーワードを使用しない場合、システムはユーザが **commit-buffer** コマンドを入力するまでリブートしません。

システムはそのシステム上で構成されているすべての論理デバイスをグレースフルにシャットダウンし、最終的に Firepower 4100/9300 シャーシの電源をオフにして再始動する前に、セキュリティモジュール/エンジンの電源を個別にオフにします。このプロセスには約 15 ～ 20 分かかります。

ステップ 3 リブート プロセスをモニタするには、次の手順を実行します。
scope chassis 1
show fsm status

Firepower 4100/9300 シャーシの電源オフ

手順

ステップ 1 シャーシ モードに入ります。
scope chassis 1

ステップ 2 次のコマンドを入力して、シャーシを電源オフにします。
shutdown [理由] **[no-prompt]**

（注） **[no-prompt]** キーワードを使用した場合、コマンドを入力するとシャーシはすぐにシャットダウンします。**[no-prompt]** キーワードを使用しない場合、システムはユーザが **commit-buffer** コマンドを入力するまでシャットダウンしません。

システムはそのシステム上で構成されているすべての論理デバイスをグレースフルにシャットダウンし、最終的に Firepower 4100/9300 シャーシの電源をオフにする前に、セキュリティ モジュール/エンジンの電源を個別にオフにします。このプロセスには約 15 ～ 20 分かかります。シャーシが正常にシャットダウンすれば、シャーシの電源コードを物理的に抜くことができます。

ステップ 3 シャットダウン プロセスをモニタするには、次の手順を実行します。
scope chassis 1
show fsm status

トラスト ID 証明書のインストール

初期設定後に、自己署名 SSL 証明書が Firepower 4100/9300 シャーシ Web アプリケーションで使用するために生成されます。その証明書は自己署名であるため、クライアント ブラウザが自動的に信頼することはありません。新しいクライアント ブラウザで Firepower 4100/9300 シャーシ Web インターフェイスに初めてアクセスするときに、ブラウザは SSL 警告をスローして、ユーザが

Firepower 4100/9300 シャーシ にアクセスする前に証明書を受け入れることを要求します。FXOS CLI を使用して証明書署名要求（CSR）を生成し、Firepower 4100/9300 シャーシ で使用する結果の ID 証明書をインストールするには、以下の手順を使用できます。この ID 証明書により、クライアントブラウザは接続を信頼し、警告なしで Web インターフェイスを起動できるようになります。

手順

ステップ 1 FXOS CLI に接続します。（FXOS CLIへのアクセス を参照）。

ステップ 2 セキュリティ モジュールを入力します。
scopesecurity

ステップ 3 キー リングを作成します。
createkeyring *keyring_name*

ステップ 4 秘密キーのモジュラス サイズを設定します。
setmodulus *size*

ステップ 5 設定を確定します。
commit-buffer

ステップ 6 CSR フィールドを設定します。証明書は、基本オプション（subject-name など）を指定して生成できます。さらに任意で、ロケールや組織などの情報を証明書に組み込むことができる詳細オプションを指定できます。CSR フィールドを設定する場合、システムにより証明書パスワードの入力が求められることに注意してください。
createcertreqcertreq *subject_name*

password

setcountry *country*

setstate *state*

setlocality *locality*

setorg-name *organization_name*

setorg-unit-name *organization_unit_name*

setsubject-name *subject_name*

ステップ 7 設定を確定します。
commit-buffer

ステップ 8 認証局に提供する CSR をエクスポートします。

a) 完全な CSR を表示します。
showcertreq

b) 「-----BEGIN CERTIFICATE REQUEST-----」から「-----END CERTIFICATE REQUEST-----」までの出力をコピーします。

例：
```
-----BEGIN CERTIFICATE REQUEST-----
MIIC6zCCAdMCAQAwdzELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWEx
```

```
ETAPBgNVBAcMCFNhbiBKb3NlMRYwFAYDVQQKDA1DaXNjbyBTeXN0ZW1zMQwwCgYD
VQQLDANUQUMxGjAYBgNVBAMMEWZwNDEyMC50ZXN0LmxvY2FsMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0ON5gagkfZ2fi4JVEANG+7YGgcHbnUt7LpV
yMChnKOPJjBwkUMNQA1mQsRQDcbJ232/sK0fMSnyqOL8JzC7itxeVEZRyz7/ax7W
GNveg/XP+zd03nt4GXM63FsrPcPmA7EwgqDSLoShtBEV10hhf4+Nw4pKCZ+eSSkS
JkTB1ZHaKV9bttYg3kf/UEUUgk/EyrVq3B+u2DsooPVq76mTm8BwYMqHbJEv4Pmu
RjWE88yEvVwH7JTEij9OvxbatjDjVSJHZBURtCanvyBvGuLP/Q/Nmv3Lo3G9ITbL
L5gIYZVatTxp6HTUezH2MIIzOavU6d1tB9rnyxgGth5dPV0dhQIDAQABoC8wLQYJ
KoZIhvcNAQkOMSAwHjAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDANBgkq
hkiG9w0BAQsFAAOCAQEAZUfCbwx9vt5aVDcL+tATu5xFE3LA310ck6GjlNv6W/6r
jBNLxusYi1rZZcW+CgnvNs4ArqYGyNVBySOavJO/VvQ1KfyxxJ1OIkyx3RzEjgK0
zzyoyrG+EZXC5ShiraS8HuWvE2wFM2wwWNtHWtvcQy55+/hDPD2Bv8pQOC2Zng3I
kLfG1dxWf1xAxLzf5J+AuIQ0CM5HzM9Zm8zREoWT+xHtLSqAqg/aCuomN9/vEwyU
OYfoJMvAqC6AZyUnMfUfCoyuLpLwgkxB0gyaRdnea5RhiGjYQ2lDXYDjEXp7rCx9
+6bvDl1n70JCegHdCWtP75SaNyaBEPkO0365rTckbw==
-----END CERTIFICATE REQUEST-----
```

ステップ 9 certreq モードを終了します。
exit

ステップ 10 キーリング モードを終了します。
exit

ステップ 11 （注） FXOS にインポートするすべての証明書は、Base64 形式でなければなりません。認証局から受信した証明書またはチェーンの形式が多様である場合は、まずそれを OpenSSL などの SSL ツールを使用して変換する必要があります。
証明書チェーンを保持する新規トラストポイントを作成します。
createtrustpoint *trustpoint_name*

ステップ 12 生成された CSR をトラストポイントで設定します。
setcertchain

ステップ 13 （注） 中間証明書を使用する認証局の場合は、ルートと中間証明書とを結合させる必要があります。テキストファイルで、ルート証明書を一番上にペーストし、それに続いてチェーン内の各中間証明書をペーストします。この場合、すべての BEGIN CERTIFICATE フラグと END CERTIFICATE フラグを含めます。この全体のテキスト ブロックを、トラストポイントにコピー アンド ペーストします。
画面に表示される指示に従って、手順 8 でコピーした CSR 出力を入力します。

例：

```
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
>-----BEGIN CERTIFICATE-----
>MIICDTCCAbOgAwIBAgIQYIutxPDPw6BOp3uKNgJHZDAKBggqhkjOPQQDAjBTMRUw
>EwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>MB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTUwNzI4MTc1NjU2
>WhcNMjAwNzI4MTgwNjU2WjBTMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJ
>kiaJk/IsZAEZFghuYWF1c3RpbjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4t
>UEMtQ0EwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASvEA27V1Enq1gMtLkvJ6rx
>GXRpXWIEyuiBM4eQRoqZKnkeJUkm1xmqlubaDHPJ5TMGfJQYszLBRJPq+mdrKcDl
>o2kwZzATBgkrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0T
>AQH/BAUwAwEB/zAdBgNVHQ4EFgQUyInbDHPrFwEEBcbxGSgQW7pOVIkwEAYJKwYB
>BAGCNxUBBAMCAQAwCgYIKoZIzj0EAwIDSAAwRQIhAP++QJTUmniB/AxPDDN63Lqy
>18odMDoFTkG4p3Tb/2yMAiAtMYhlsv1gCxsQVOw0xZVRugSdoOak6n7wCjTFX9jr
>RA==
>-----END CERTIFICATE-----
>ENDOFBUF
```

ステップ 14 設定を確定します。
commit-buffer

ステップ 15 トラストポイント モードを終了します。
exit

ステップ 16 キーリング モードに入ります。
scopekeyring *keyring_name*

ステップ 17 ステップ 13 で作成されたトラストポイントを、CSR に作成されたキーリングに関連付けます。
settrustpoint *trustpoint_name*

ステップ 18 サーバの署名付き ID 証明書をインポートします。
setcert

ステップ 19 認証局により提供された ID 証明書の内容をペーストします。

例：

```
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
>-----BEGIN CERTIFICATE-----
>MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkjOPQQDAjBT
>MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
>bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
>OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs
>aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoTDUNpc2NvIFN5c3Rl
>bXMxDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
>MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
>BwdudS3sulXIwKGco48mMHCRQw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
>RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
>ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
>yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
>/cujcb0hNssvmAhhlVq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2Hl09XR2FAgMB
>AAGjggJYMIICVDAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
>FgQU/1WpstiEYExs8DlZWcuHZwPtu5QwHwYDVR0jBBgwFoAUyInbDHPrFwEEBcbx
>GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
>dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
>YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
>b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlz
>dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHMBggrBgEF
>BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
>QVVTVElOLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
>Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
>P2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0
>aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBlAGIAUwBlAHIAdgBlAHIwDgYDVR0P
>AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
>IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
>sgoIK60akbjotOTvUdUd9b6K1Uw=
>-----END CERTIFICATE-----
>ENDOFBUF
```

ステップ 20 キーリング モードを終了します。
exit

ステップ 21 セキュリティ モードを終了します。
exit

ステップ 22 システム モードに入ります。
scopesystem

ステップ 23 サービス モードに入ります。
scopeservices

ステップ 24 新しい証明書を使用するように FXOS Web サービスを設定します。
sethttpskeyring *keyring_name*

ステップ 25 設定を確定します。
commit-buffer

ステップ 26 HTTPS サーバに関連付けられているキーリングを表示します。これにはこの手順の手順 3 で作成したキーリングの名前が反映されることになります。画面出力にデフォルトのキーリング名が表示される場合には、HTTPS サーバはまだ、新しい証明書を使用するように更新されていません。
showhttps

例：

```
fp4120 /system/services # show https
Name: https
    Admin State: Enabled
    Port: 443
    Operational port: 443
    Key Ring: firepower_cert
    Cipher suite mode: Medium Strength
   Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL
```

ステップ 27 インポートされた証明書の内容を表示し、[証明書のステータス（Certificate Status）]**Certificate Status**値が [有効（Valid）]**Valid**と表示されることを確認します。
scopesecurity

showkeyring *keyring_name***detail**

例：

```
fp4120 /security #  scope security
fp4120 /security #  show keyring firepower_cert detail
Keyring firepower_cert:
    RSA key modulus: Mod2048
    Trustpoint CA: firepower_chain
    Certificate status: Valid
    Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            45:00:00:00:0a:de:86:55:16:82:24:f3:be:00:00:00:00:00:0a
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: DC=local, DC=naaustin, CN=naaustin-NAAUSTIN-PC-CA
        Validity
            Not Before: Apr 28 13:09:54 2016 GMT
            Not After : Apr 28 13:09:54 2018 GMT
        Subject: C=US, ST=California, L=San Jose, O=Cisco Systems, OU=TAC,
CN=fp4120.test.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b3:43:8d:e6:06:a0:91:f6:76:7e:2e:09:54:40:
                    0d:1b:ee:d8:1a:07:07:6e:75:2d:ec:ba:55:c8:c0:
                    a1:9c:a3:8f:26:30:70:91:43:0d:40:0d:66:42:c4:
                    50:0d:c6:c9:db:7d:bf:b0:ad:1f:31:29:f2:a8:e2:
                    fc:27:30:bb:8a:dc:5e:54:46:51:cb:3e:ff:6b:1e:
                    d6:18:db:de:83:f5:cf:fb:37:74:de:7b:78:19:73:
                    3a:dc:5b:2b:3d:c3:e6:03:b1:30:82:a0:d2:2e:84:
                    a1:b4:11:15:d7:48:61:7f:8f:8d:c3:8a:4a:09:9f:
                    9e:49:29:12:26:44:c1:d5:91:da:29:5f:5b:b6:d6:
                    20:de:47:ff:50:45:14:82:4f:c4:ca:b5:6a:dc:1f:
                    ae:d8:3b:28:a0:f5:6a:ef:a9:93:9b:c0:70:60:ca:
```

```
                    87:6c:91:2f:e0:f9:ae:46:35:84:f3:cc:84:bd:5c:
                    07:ec:94:c4:8a:3f:4e:bf:16:da:b6:30:e3:55:22:
                    47:64:15:11:b4:26:a7:bf:20:6f:1a:e2:cf:fd:0f:
                    cd:9a:fd:cb:a3:71:bd:21:36:cb:2f:98:08:61:95:
                    5a:b5:3c:69:e8:74:d4:7b:31:f6:30:82:33:39:ab:
                    d4:e9:dd:6d:07:da:e7:cb:18:06:b6:1e:5d:3d:5d:
                    1d:85
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:fp4120.test.local
            X509v3 Subject Key Identifier:
                FF:55:A9:B2:D8:84:60:4C:6C:F0:39:59:59:CB:87:67:03:ED:BB:94
            X509v3 Authority Key Identifier:
                keyid:C8:89:DB:0C:73:EB:17:01:04:05:C6:F1:19:28:10:5B:BA:4E:54:89
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=naaustin-pc,CN=CDP,
                    CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
                  DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=AIA,
                  CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
                  DC=local?cACertificate?base?objectClass=certificationAuthority
            1.3.6.1.4.1.311.20.2:
                ...W.e.b.S.e.r.v.e.r
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
    Signature Algorithm: ecdsa-with-SHA256
         30:45:02:20:57:b0:ec:d7:09:8a:b1:2d:15:1b:f2:c6:39:10:
         e3:f7:55:a3:6a:08:e8:24:41:df:4f:16:41:b6:07:35:4b:bf:
         02:21:00:ed:47:4e:6e:24:89:04:6f:cf:05:98:e6:b2:0a:08:
         2b:ad:1a:91:b8:e8:b4:e4:ef:51:d5:1d:f5:be:8a:d5:4c
-----BEGIN CERTIFICATE-----
MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkjOPQQDAjBT
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWFlc3Rp
bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs
aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoTDUNpc2NvIFN5c3Rl
bXMxDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
BwdudS3sulXIwKGco48mMHCRQw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
/cujcb0hNssvmAhhlVq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2Hl09XR2FAgMB
AAGjggJYMIICVDAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
FgQU/1WpstiEYExs8DlZWcuHZwPtu5QwHwYDVR0jBBgwFoAUyInbDHPrFwEEBcbx
GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlz
dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHMBggrBgEF
BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
QVVTVElOLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
P2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0
aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBlAGIAUwBlAHIAdgBlAHIwDgYDVR0P
AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
IFew7NcJirEtFRvyxjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
sgoIK60akbjotOTvUdUd9b6K1Uw=
-----END CERTIFICATE-----

    Zeroized: No
```

次の作業

新しい信頼できる証明書が存在していることを確認するには、Web ブラウザのアドレス バーに *https://<FQDN_or_IP>/* と入力して、Firepower Chassis Manager に移動します。

（注） ブラウザはさらに、アドレス バーの入力内容に照らして証明書のサブジェクト名を確認します。証明書が完全修飾ドメイン名に対して発行されている場合、ブラウザでもそのようにアクセスする必要があります。IP アドレスを使用してアクセスすると、信頼できる証明書が使用されているとしても、別の SSL エラー（共通名が無効）がスローされます。