FXOS Chassis Managerの信頼できる証明書のインストール

内容

はじめに

このドキュメントでは、FP 4100/9300シリーズデバイス上のFXOS用シャーシマネージャで使用するCSRを生成し、ID証明書をインストールする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- コマンドラインからのFirepowereXtensible Operating System(FXOS)の設定
- 証明書署名要求(CSR)の使用
- Private Key Infrastructure(PKI)の概念

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Firepower(FP)4100および9300シリーズハードウェア
- FXOSバージョン2.10

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

初期設定の後、Chassis Manager Webアプリケーションで使用する自己署名SSL証明書が生成されます。この証明書は自己署名されるため、クライアントブラウザによって自動的に信頼されることはありません。新しいクライアントブラウザがChassis ManagerのWebインターフェイスに初めてアクセスすると、ブラウザはプライベートではないという接続同様のSSL警告をスローし、Chassis Managerにアクセスする前に証明書を受け入れるようにユーザに要求します。このプロセスでは、信頼できる認証局によって署名された証明書をインストールできます。これにより、クライアントブラウザは接続を信頼でき、Webインターフェイスを警告なしで起動できます。

設定

CSR の生成

デバイスのIPアドレスまたは完全修飾ドメイン名(FQDN)を含む証明書を取得するには、次の手順を実行します（これにより、クライアントブラウザがサーバを正しく識別できます）。

- キーリングを作成し、秘密キーのモジュールサイズを選択します。

注：キーリング名は任意の入力にすることができます。次の例では、firepower_certが使用されています。

この例では、キーサイズが1024ビットのキーリングを作成します。

```
Firepower-chassis# scope security
Firepower-chassis /security # create keyring kr220
Firepower-chassis /security/keyring* # set modulus mod1024
Firepower-chassis /security/keyring* # commit-buffer
```

- CSRフィールドを設定します。CSRは、サブジェクト名などの基本オプションだけで生成できます。証明書要求パスワードの入力も求められます。

次の例では、キーリングのIPv4アドレスと基本オプションを使用して証明書要求を作成し、表示しています。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq ip 192.168.200.123 subject-name sjc04
Certificate request password:
Confirm certificate request password:
Firepower-chassis /security/keyring* # commit-buffer
```

- CSRは、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より高度なオプションを使用して生成することもできます。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq
Firepower-chassis /security/keyring/certreq* # set "ip 192.168.200.123"
Firepower-chassis /security/keyring/certreq* #  set subject-name "sjc04"
Firepower-chassis /security/keyring/certreq* # set country "US"
Firepower-chassis /security/keyring/certreq* # set dns "bg1-samc-15A"
Firepower-chassis /security/keyring/certreq* # set email "test@cisco.com"
Firepower-chassis /security/keyring/certreq* # set locality "new york city"
Firepower-chassis /security/keyring/certreq* # set org-name "Cisco Systems"
Firepower-chassis /security/keyring/certreq* # set org-unit-name "Testing"
Firepower-chassis /security/keyring/certreq* # set state "new york"
Firepower-chassis /security/keyring/certreq* # commit-buffer
```

- CSRをエクスポートして、認証局に提供します。-----BEGIN CERTIFICATE REQUEST-----ends with (and includes) -----END CERTIFICATE REQUEST-----で始まる出力をコピーします。

```
Firepower-chassis /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name: test@cisco.com
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
Ore/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/OOKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXDOlZTL09H
BA==
-----END CERTIFICATE REQUEST-----
```

認証局(CA)証明書チェーンのインポート

注:FXOSにインポートするには、すべての証明書がBase64形式である必要があります。認証局から受信した証明書またはチェーンが異なる形式の場合は、まず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しいトラストポイントを作成します。

注：トラストポイント名は任意の入力にすることができます。この例では、firepower_chainが使用されています。

```
Firepower-chassis# scope security
Firepower-chassis /security # create trustpoint tPoint10
Firepower-chassis /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl9O3O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc4OwhuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/trustpoint* # commit-buffer
```

注：中間証明書を使用する認証局の場合、ルート証明書と中間証明書を組み合わせる必要があります。テキストファイルで、ルート証明書を先頭に貼り付け、チェーン内の各中間証明書（すべてのBEGIN CERTIFICATEフラグとEND CERTIFICATEフラグを含む）に続けて貼り付けます。次に、そのファイル全体をENDOFBUFの線引きの前に貼り付けます。

サーバの署名付きID証明書のインポート

- 前の手順で作成したトラストポイントを、CSR用に作成したキーリングに関連付けます。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # set trustpoint tPoint10
```

- 認証局から提供されたID証明書の内容を貼り付けます。

```
Firepower-chassis /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/keyring* # commit-buffer
```

新しい証明書を使用するためのシャーシマネージャの設定

これで証明書がインストールされましたが、Webサービスはまだ証明書を使用するように構成されていません。

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # enable https
Firepower-chassis /system/services* # set https port 443
Warning: When committed, this closes all the web sessions.
Firepower-chassis /system/services* # set https keyring kring7984
Firepower-chassis /system/services* # set https cipher-suite-mode high
Firepower-chassis /system/services* # commit-buffer
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

- show https：出力には、HTTPSサーバに関連付けられたキーリングが表示されます。前に説明した手順で作成した名前を反映できます。それでもdefaultが表示される場合は、新しい証明書を使用するように更新されていません。

```
Firepower-chassis /system/services #
show https
 Name: https Admin State: Enabled Port: 443 Operational port: 443 Key Ring: kring7984
 Cipher suite mode: Medium Strength Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HI
```

- show keyring <keyring_name> detail：出力には、インポートされた証明書の内容が表示され、証明書が有効かどうかが示されます。

<#root>

```
fp4120 /security #
scope security
fp4120 /security #
show keyring kring7984
 detail
 Keyring
kring7984
: RSA key modulus: Mod2048 Trustpoint CA: tPoint10

 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:
-----BEGIN CERTIFICATE-----
MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAAACjAKBggqhkjOPQQDAjBT MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBg
-----END CERTIFICATE-----
 Zeroized: No
```

- Webブラウザのアドレスバーにhttps://<FQDN_or_IP>/と入力し、Firepower Chassis Managerを表示して、新しい信頼できる証明書が表示されることを確認します。

警告：ブラウザでは、証明書のサブジェクト名がアドレスバーの入力と照合されることも確認されます。そのため、証明書が完全修飾ドメイン名(FQDN)に対して発行された場合は、ブラウザで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場合でも、別のSSLエラー(Common Name Invalid)がスローされます。

トラブルシュート

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- FXOS CLIへのアクセス
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。