Installieren eines vertrauenswürdigen Zertifikats für den FXOS-Chassis-Manager

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie einen CSR erstellen und das Identitätszertifikat zur Verwendung mit dem Chassis Manager für FXOS auf den Geräten der Serien FP 4100/9300 installieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfigurieren von FirePOWER eXtensible Operating System (FXOS) über die Befehlszeile
- Zertifikatsignierungsanforderung (CSR) verwenden
- PKI-Konzepte (Private Key Infrastructure)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Firepower (FP) der Serien 4100 und 9300 - Hardware
- FXOS-Versionen 2.10

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Nach der Erstkonfiguration wird ein selbstsigniertes SSL-Zertifikat für die Verwendung mit der Chassis

Manager-Webanwendung generiert. Da es sich um ein selbstsigniertes Zertifikat handelt, wird es von Clientbrowsern nicht automatisch als vertrauenswürdig eingestuft. Wenn ein neuer Client-Browser zum ersten Mal auf die Chassis Manager-Webschnittstelle zugreift, löst der Browser eine SSL-Warnung aus, die der Ihrer Verbindung ähnelt und nicht privat ist. Er fordert den Benutzer auf, das Zertifikat zu akzeptieren, bevor Sie auf den Chassis Manager zugreifen. Auf diese Weise kann ein von einer vertrauenswürdigen Zertifizierungsstelle signiertes Zertifikat installiert werden, das einem Clientbrowser die Vertrauenswürdigkeit der Verbindung ermöglicht und die Webschnittstelle ohne Warnungen aufruft.

Konfigurieren

CSR erstellen

Führen Sie die folgenden Schritte aus, um ein Zertifikat zu erhalten, das die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) des Geräts enthält (anhand derer der Client-Browser den Server richtig identifizieren kann):

- Erstellen Sie einen Keyring, und wählen Sie die Modulgröße des privaten Schlüssels aus.

Hinweis: Der Keyring-Name kann beliebig eingegeben werden. In diesen Beispielen wird **firepower_cert** verwendet.

In diesem Beispiel wird ein Keyring mit einer Schlüssellänge von 1024 Bit erstellt:

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

- Konfigurieren der CSR-Felder Die CSR-Anfrage kann mit einfachen Optionen wie einem Betreff erstellt werden. Daraufhin wird auch ein Kennwort für die Zertifikatsanforderung eingegeben.

In diesem Beispiel wird eine Zertifikatsanforderung mit einer IPv4-Adresse für einen Keyring erstellt und angezeigt, mit grundlegenden Optionen:

```
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
```

- Der CSR kann auch mit erweiterten Optionen generiert werden, mit denen Informationen wie Gebietsschema und Organisation in das Zertifikat eingebettet werden können.

```
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
```

- Exportieren Sie den CSR, um ihn Ihrer Zertifizierungsstelle bereitzustellen. Kopieren Sie die Ausgabe, die mit beginnt (und enthält) -----BEGIN CERTIFICATE REQUEST----- endet mit (und enthält) -----END CERTIFICATE REQUEST-----.

```
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
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----
```

Zertifikatskette der Zertifizierungsstelle importieren

Hinweis: Alle Zertifikate müssen das Base64-Format aufweisen, damit sie in FXOS importiert werden können. Wenn das von der Zertifizierungsstelle empfangene Zertifikat oder die Kette ein anderes Format aufweist, müssen Sie es zuerst mit einem SSL-Tool wie OpenSSL konvertieren.

- Erstellen Sie einen neuen Vertrauenspunkt für die Zertifikatskette.

Hinweis: Der Name des Vertrauenspunkts kann eine beliebige Eingabe sein. In den Beispielen wird firepower_chain verwendet.

```
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
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/trustpoint* # commit-buffer
```

Hinweis: Für eine Zertifizierungsstelle, die Zwischenzertifikate verwendet, müssen das Stamm- und Zwischenzertifikat kombiniert werden. Fügen Sie in der Textdatei oben das Stammzertifikat ein, gefolgt von jedem Zwischenzertifikat in der Kette (das alle Flags BEGIN CERTIFICATE und END CERTIFICATE enthält). Fügen Sie dann die gesamte Datei vor die ENDOFBUF-Abgrenzung ein.

Importieren des signierten Identitätszertifikats für den Server

- Ordnen Sie den im vorherigen Schritt erstellten Vertrauenspunkt dem Keyring zu, der für den CSR erstellt wurde.

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

- Fügen Sie den Inhalt des von der Zertifizierungsstelle bereitgestellten Identitätszertifikats ein.

```
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
```

Chassis-Manager für die Verwendung des neuen Zertifikats konfigurieren

Das Zertifikat wurde jetzt installiert, aber der Webdienst ist noch nicht für seine Verwendung konfiguriert.

```
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
```

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

- **show https - In** der Ausgabe wird der Keyring angezeigt, der dem HTTPS-Server zugeordnet ist. Er kann den Namen wiedergeben, der in den oben genannten Schritten erstellt wurde. Wenn es immer noch Standard zeigt, dann wurde es nicht aktualisiert, um das neue Zertifikat zu verwenden.

<#root>

```
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:+HIG
```

- **show keyring <keyring_name> detail -** Die Ausgabe zeigt den Inhalt des Zertifikats an, das importiert wird, und zeigt an, ob es gültig ist oder nicht.

<#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:00:00:00:00:0
-----BEGIN CERTIFICATE-----
MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAAACjAKBggqhkjOPQQDAjBT MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgo
-----END CERTIFICATE-----
 Zeroized: No
```

- Geben Sie **https://<FQDN_or_IP>/** in die Adressleiste eines Webbrowsers ein, navigieren Sie zum FirePOWER Chassis Manager, und überprüfen Sie, ob das neue vertrauenswürdige Zertifikat angezeigt wird.

Warnung: Browser überprüfen auch den Subjektnamen eines Zertifikats anhand der Eingabe in der Adressleiste. Wenn das Zertifikat also für den vollqualifizierten Domänennamen ausgestellt wird, muss es auf diese Weise im Browser geöffnet werden. Wenn über eine IP-Adresse auf die Datei zugegriffen wird, wird ein anderer SSL-Fehler ausgegeben (Common Name Invalid), auch wenn das vertrauenswürdige Zertifikat verwendet wird.

Fehlerbehebung

Es sind derzeit keine spezifischen Informationen zur Fehlerbehebung für diese Konfiguration verfügbar.

Zugehörige Informationen

- **Zugriff auf die FXOS-CLI**
- **Technischer Support und Dokumentation für Cisco Systeme**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.