Installeer een betrouwbaar certificaat voor FXOS Chassis Manager

Inhoud

Inleiding

In dit document wordt beschreven hoe u een CSR kunt genereren en het identiteitscertificaat kunt installeren voor gebruik met Chassis Manager voor FXOS op apparaten uit de FP 4100/9300-serie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower eXtensible Operating System (FXOS) configureren vanuit de opdrachtregel
- Aanvraag voor gebruik van certificaat-ondertekening (CSR)
- Private Key Infrastructure (PKI)-concepten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firepower (FP) 4100 en 9300 Series hardware
- FXOS versies 2.10

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Na de eerste configuratie wordt een zelfondertekend SSL-certificaat gegenereerd voor gebruik met de Chassis Manager-webtoepassing. Aangezien dat certificaat zelf-ondertekend is, wordt het niet automatisch

vertrouwd door clientbrowsers. De eerste keer dat een nieuwe clientbrowser toegang heeft tot de webinterface van Chassis Manager, geeft de browser een SSL-waarschuwing die vergelijkbaar is met uw verbinding dat deze niet privé is, en vereist dat de gebruiker het certificaat accepteert voordat u de Chassis Manager opent. Dit proces maakt het mogelijk om een certificaat te installeren dat is ondertekend door een vertrouwde certificeringsinstantie, waardoor een clientbrowser de verbinding kan vertrouwen en de web-interface zonder waarschuwingen kan openen.

Configureren

MVO genereren

Voer deze stappen uit om een certificaat te verkrijgen dat het IP-adres of de volledig gekwalificeerde domeinnaam (FQDN) van het apparaat bevat (waarmee een clientbrowser de server correct kan identificeren):

- Maak een sleutelring en selecteer de modulusgrootte van de privé-sleutel.

Opmerking: de naam van de sleutelhanger kan worden ingevoerd. In deze voorbeelden wordt **firepower_cert** gebruikt.

In dit voorbeeld wordt een sleutelring gemaakt met een sleutelgrootte van 1024 bits:

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

- De CSR-velden configureren. MVO kan worden gegenereerd met alleen basisopties zoals een onderwerpnaam. Dit vraagt ook om een wachtwoord voor een certificaataanvraag.

In dit voorbeeld wordt een certificaataanvraag gemaakt en weergegeven met een IPv4-adres voor een sleutelring, met basisopties:

```
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
```

- MVO kan ook worden gegenereerd met geavanceerdere opties waarmee informatie zoals locale en organisatie in het certificaat kan worden ingebed.

```
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
```

- Exporteer de CSR om deze door te geven aan uw certificeringsinstantie. Kopieert de uitvoer die begint met (en omvat) -----BEGIN CERTIFICAAT VERZOEK----- eindigt met (en omvat) -----END CERTIFICAAT VERZOEK-----.

```
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-----
```

Importeer de certificaatketen van de certificeringsinstantie

Opmerking: alle certificaten moeten in Base64-formaat zijn om in FXOS te worden geïmporteerd. Als het certificaat of de ketting die van de Certificaatautoriteit wordt ontvangen in een ander formaat is, moet u het eerst converteren met een SSL-tool zoals OpenSSL.

- Maak een nieuw trustpoint om de certificaatketen te houden.

Opmerking: De trustpoint naam kan elke invoer zijn. In de voorbeelden is FirePOWER_chain het resultaat.

```
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
```

> **Opmerking**: Voor een certificeringsinstantie die gebruik maakt van tussencertificaten, moeten de basiscertificaten en de tussencertificaten worden gecombineerd. In het tekstbestand plakt u het basiscertificaat bovenaan, gevolgd door elk tussenliggend certificaat in de keten (dat alle begin- en EINDCERTIFICAAT-vlaggen omvat). Plakt het hele bestand vervolgens vóór de ENDOFBUF-afbakening.

Het ondertekende identiteitscertificaat voor de server importeren

- Associeer het trustpoint dat in de vorige stap is gemaakt met de sleutelring die is gemaakt voor de MVO.

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

- Plakt de inhoud van het door de certificeringsinstantie verstrekte identiteitsbewijs.

```
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 configureren om het nieuwe certificaat te gebruiken

Het certificaat is nu geïnstalleerd, maar de webservice is nog niet geconfigureerd om het te gebruiken.

```
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
```

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

- **https tonen -** Uitvoer geeft de sleutelring weer die aan de HTTPS-server is gekoppeld. Het kan de naam weerspiegelen die in de eerder genoemde stappen is gemaakt. Als het nog steeds standaard is, is het niet bijgewerkt om het nieuwe certificaat te gebruiken.

<#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
```

- **toon sleutelring <keyring_name> detail -** Output toont de inhoud van het certificaat dat wordt ingevoerd, en toont als het of niet geldig is.

<#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
```

- Voer **https://<FQDN_or_IP>/** in de adresbalk van een webbrowser in en blader naar de Firepower Chassis Manager en controleer of het nieuwe vertrouwde certificaat wordt weergegeven.

Waarschuwing: Browsers verifiëren ook de onderwerpnaam van een certificaat aan de ingang in de adresbalk, dus als het certificaat wordt afgegeven aan de volledig gekwalificeerde domeinnaam, moet het op die manier in de browser worden benaderd. Als het via IP-adres wordt benaderd, wordt een andere SSL-fout geworpen (algemene naam ongeldig), zelfs als het vertrouwde certificaat wordt gebruikt.

Problemen oplossen

Er is momenteel geen specifieke informatie beschikbaar om deze configuratie problemen op te lossen.

Gerelateerde informatie

- **De FXOS CLI gebruiken**
- **Technische ondersteuning en documentatie â€“ Cisco Systems**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.