

Installa un certificato attendibile per Gestione chassis FXOS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Genera aCSR](#)

[Importa catena di certificati dell'Autorità di certificazione](#)

[Importa il certificato di identità firmato per il server](#)

[Configurazione di Chassis Manager per l'utilizzo del nuovo certificato](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come generare un CSR e installare il certificato di identità da utilizzare con Chassis Manager per FXOS sui dispositivi serie FP 4100/9300.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di Firepower eXtensible Operating System (FXOS) dalla riga di comando
- Usa richiesta di firma del certificato (CSR)
- Nozioni base sull'infrastruttura a chiave privata (PKI)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Hardware Firepower (FP) serie 4100 e 9300
- FXOS versioni 2.10

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Dopo la configurazione iniziale, viene generato un certificato SSL autofirmato da utilizzare con l'applicazione Web Chassis Manager. Poiché il certificato è autofirmato, non viene considerato automaticamente attendibile dai browser client. La prima volta che un nuovo browser client accede all'interfaccia Web di Chassis Manager, il browser genera un avviso SSL simile alla connessione che indica che non è privata e richiede all'utente di accettare il certificato prima di accedere a Chassis Manager. Questo processo consente l'installazione di un certificato firmato da un'autorità di certificazione attendibile, che consente a un browser client di considerare attendibile la connessione e di visualizzare l'interfaccia Web senza visualizzare avvisi.

Configurazione

Genera un CSR

Per ottenere un certificato contenente l'indirizzo IP o il nome di dominio completo (FQDN) del dispositivo, che consente a un browser client di identificare correttamente il server, eseguire la procedura seguente:

- Creare una sequenza di chiavi e selezionare le dimensioni del modulo della chiave privata.



Nota: il nome del keyring può essere qualsiasi input. In questi esempi viene utilizzato `firepower_cert`.

In questo esempio viene creato un keyring con una dimensione della chiave di 1024 bit:

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

- Configurare i campi CSR. Il CSR può essere generato semplicemente con opzioni di base come il nome di un soggetto. In questo modo viene richiesta anche una password per la richiesta del certificato.

In questo esempio viene creata e visualizzata una richiesta di certificato con un indirizzo IPv4 per un anello di chiavi, con le opzioni di base seguenti:

```
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
```


- Il CSR può inoltre essere generato con opzioni più avanzate che consentono di incorporare nel certificato informazioni quali le impostazioni internazionali e l'organizzazione.

```
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 "bgl-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
```


- Esportare il CSR da fornire all'autorità di certificazione. Copiare l'output che inizia con (e include) —BEGIN CERTIFICATE REQUEST— termina con (e include) —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
gY0AMIGJAoGBALpKn1t8qMZ04UGqILKFXQQc2c8b/vW2rnRF80PhKbhghLA1YZ1F
JqcYEG5Y11+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1Wsy1wUWV4
Ore/zgTk/WCd56Rf0BvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWwMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAA0BgQCcsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHU003Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWICtWgHhH8Bim0b/00KuG8kwfIGGsED1Av
TTYvUP+BZ90FiPbRIA718S+V8ndXr1HejiQGx1DNqoN+odCXPc5kjoXD01ZTL09H
BA==
-----END CERTIFICATE REQUEST-----
```


Importa catena di certificati dell'Autorità di certificazione

 Nota: per poter essere importati in FXOS, tutti i certificati devono essere in formato Base64. Se il formato del certificato o della catena ricevuto dall'Autorità di certificazione è diverso, è necessario innanzitutto convertirlo con uno strumento SSL quale OpenSSL.

- Creare un nuovo trust point per contenere la catena di certificati.

 Nota: il nome del trust point può essere qualsiasi input. Negli esempi viene utilizzato `firepower_chain`.

```
Firepower-chassis# scope security
Firepower-chassis /security # create trustpoint tPoint10
Firepower-chassis /security/trustpoint* # set certchain
Enter lines one at a time. Enter END_OF_BUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGx1IE1uYy4xEzARBGNVBASt
> C1R1c3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgYOAMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQe0GHemdh66u2/XAoLx7YCCyU
> ZgAmivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgd4VBNKOND1
> GMbkPayV1QjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzC190306Mg51zq1zXcz75+VFj2I6rH9asckC1d3mk0Vx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfualtv1WvfhevskV0j6
> jtCEMYZ+f7+3yh421ido3n04MIGeBgNVHSMegZYwgZ0AFL1NjtcEMYZ+f7+3yh42
> 1ido3n04oXikdjBOMQswCQYDVQQGEwJVUzELMAKGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKEwJ0dW92YSBTeXN0ZW1zIE1uYy4xFDASBgNV
> BAsTC0VuZ21uZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GAQAwdAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAA0BgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wr4pYi04z42/j9Ijenh75tCKMhw51az8copP1EBm0cyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> END_OF_BUF
Firepower-chassis /security/trustpoint* # commit-buffer
```

 Nota: per un'Autorità di certificazione che utilizza certificati intermedi, è necessario combinare i certificati radice e intermedi. Nel file di testo, incollare il certificato radice nella parte superiore, seguito da ciascun certificato intermedio della catena (che include tutti i flag BEGIN CERTIFICATE e END CERTIFICATE). Incollare quindi l'intero file prima della definizione END_OF_BUF.

Importa il certificato di identità firmato per il server

- Associare il trust point creato nel passaggio precedente al keyring creato per il CSR.

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

- Incollare il contenuto del certificato di identità fornito dall'Autorità di certificazione.

```
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/zCCAwwCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGAlUE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGx1IEluYy4xEzARBgNVBASt
> ClRlc3Qgr3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWzXZJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
> GmbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bf5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl90306Mg51zq1zXcz75+VFj2I6rH9asckClD3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSSxretysOhqHmp9+CLv8FDuy1CDYfuaLtv1WvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L4317IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/keyring* # commit-buffer
```

Configurazione di Chassis Manager per l'utilizzo del nuovo certificato

Il certificato è stato installato, ma il servizio Web non è ancora configurato per utilizzarlo.

```
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
```

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

- `show https` - Output visualizza il keyring associato al server HTTPS. Può riflettere il nome creato nei passi menzionati in precedenza. Se viene ancora visualizzato il valore predefinito, significa che non è stato aggiornato per utilizzare il nuovo certificato.

<#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:+HI
```

- `show keyring <nome_keyring> detail`: l'output visualizza il contenuto del certificato importato e indica se è valido o meno.

<#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-----
```

```
MIIE8DCCBJagAwIBAgITRQAAAAreh1UWgiTzvgAAAAACjAKBggqhkJOPQDAjBT MRUwEwYKCZImiZPyLQGGRYFbG9jYWwxGDAWBg
```


```
-----END CERTIFICATE-----
```

```
Zeroized: No
```

- Immettere `https://<FQDN_or_IP>/` nella barra degli indirizzi di un browser Web, selezionare Firepower Chassis Manager e verificare che il nuovo certificato protetto sia stato presentato.



Avviso: i browser verificano anche il nome soggetto di un certificato in base all'input nella barra degli indirizzi, quindi se il certificato viene rilasciato al nome di dominio completo, è

 necessario accedervi nel browser. Se vi si accede tramite l'indirizzo IP, viene generato un errore SSL diverso (Nome comune non valido) anche se viene utilizzato il certificato attendibile.

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per risolvere i problemi relativi a questa configurazione.

Informazioni correlate

- [Accesso alla CLI di FXOS](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).