Configurazione di Trustpoint e installazione di certificati sugli switch MDS 9000

Sommario

Introduzione

In questo documento viene descritto come configurare Trustpoint e certificati negli switch MDS.

Premesse

Il supporto PKI (Public Key Infrastructure) consente agli switch della famiglia MDS (Cisco Multilayer Director Switch) 9000 di ottenere e utilizzare certificati digitali per comunicazioni protette nella rete. Il supporto PKI fornisce gestibilità e scalabilità per IP Security (IPsec), Internet Key Exchange (IKE) e Secure Shell (SSH).

Prerequisiti

Ènecessario configurare il nome dell'host e il nome del dominio IP dello switch, se non sono già stati configurati.

```
switch# configuration terminal
switch(config)# switchname <switchName>
SwitchName(config)# ip domain-name example.com
```

Nota: la modifica del nome dell'host IP o del nome di dominio IP dopo la generazione del certificato può invalidare il certificato.

Informazioni su alcune parole chiave correlate

Trustpoint: oggetto configurato localmente contenente informazioni su un'Autorità di certificazione (CA) attendibile, tra cui la coppia di chiavi RSA locale, i certificati pubblici della CA e il certificato di identità rilasciato allo switch da una CA. È possibile configurare più trust point per registrare certificati di identità switch da più CA. Le informazioni complete sull'identità in un trust point possono essere esportate in un file nel formato standard PKCS12 protetto da password. Può essere successivamente importato sullo stesso switch (ad esempio, in seguito a un arresto anomalo del sistema) o su uno switch sostitutivo. Le informazioni contenute in un file PKCS12 sono costituite dalla coppia di chiavi RSA, dal certificato di identità e dal certificato (o catena) CA.

Certificato CA : Si tratta del certificato rilasciato dall'Autorità di certificazione (CA) in relazione a se stessa. Nell'installazione potrebbe essere presente una CA intermedia o subordinata. In tal caso, potrebbe anche fare riferimento al certificato pubblico della CA intermedia o subordinata.

Autorità di certificazione (CA) : Dispositivi che gestiscono le richieste di certificati e rilasciano certificati di identità a entità quali host, dispositivi di rete o utenti. Le CA forniscono la gestione centralizzata delle chiavi per tali entità.

KeyPair RSA : Generato con la CLI nello switch e associato al trust point. Per ciascun trust point configurato sullo switch, è necessario generare una coppia di chiavi RSA univoca e associarla al trust point.

Richiesta di firma della certificazione (CSR) Si tratta di una richiesta generata dallo switch e inviata alla CA per la firma. A fronte di questo CSR, la CA restituisce il certificato di identità.

Certificato di identità : Si tratta del certificato firmato e rilasciato dall'Autorità di certificazione per lo switch da cui viene generato il CSR. Dopo l'invio di un CSR a una CA, la CA o un amministratore fornisce il certificato di identità tramite posta elettronica o tramite un browser Web. Per incollare un certificato di identità in un trust point MDS, è necessario che sia in formato PEM (base64) standard.

Requisiti

CA radice.

Se i certificati di identità sono firmati dalla CA secondaria, è necessario aggiungere nello switch anche i certificati CA della CA secondaria.

Certificato di identità

Configurazione

Passaggio 1

Generare una coppia di chiavi RSA

```
switchName# configure terminal
switchName(config)# crypto key generate rsa label <rsaKeyPairName> exportable modulus xxx
```

I valori validi per il modulo sono (default) 512, 768, 1024, 1536, 2048 e 4096

Passaggio 2

Creare un trust point CA e associare la coppia di chiavi RSA al trust point

L'FQDN dello switch viene utilizzato come etichetta di chiave predefinita quando non ne viene specificata alcuna durante la generazione della coppia di chiavi.

```
switchName(config)# crypto ca trustpoint <trustpointName>
switchName(config-trustpoint)# enroll terminal
switchName(config-trustpoint)# rsakeypair <rsaKeyPairName>
```

Passaggio 3

Autenticazione di un'Autorità di certificazione del punto di attendibilità

Se la CA da autenticare non è una CA autofirmata, è necessario immettere l'elenco completo dei certificati CA di tutte le CA nella catena di certificazione durante la fase di autenticazione della CA. Tale catena è denominata catena di certificati CA della CA da autenticare. Il numero massimo di certificati in una catena di certificati CA è 10.

Solo se è presente una CA radice

```
switchName# configure terminal

switchName(config)# crypto ca authenticate <trustpointName>

input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIDmjCCAoKgAwIBAgIGAVTGvpxRMA0GCSqGSIb3DQEBCwUAMF0xCzAJBgNVBAYT
AkFVMSUwIwYDVQQKDBxDaXNjbyBTeXN0ZW1zIEluYy4gQXVzdHJhbGlhMRIwEAYD
VQQLDAlDaXNjbyBUQUMxEzARBgNVBAMMCk5pa29sYXkgQ0EwHhcNMTYwNTE5MDIw
MTAxWhcNMjYwNTIwMDIwMTE0WjBdMQswCQYDVQQGEwJBVTElMCMGA1UECgwcQ2lz
Y28gU3lzdGVtcyBJbmMuIEF1c3RyYWxpYTESMBAGA1UECwwJQ2lzY28gVEFDMRMw
EQYDVQQDDApOaWtvbGF5IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAm6onXi3JRfIe2NpQ53CDBCUTn8cHGU67XSyqgL7MlYBhH032QaVrT3b98KcW
55UoqQW15kAnJhNTIQ+f0f8oj9A5UbwcQwIXQuHGkDZvJULjidM37tGF90ZVLJs7
sMxsnVSPIe05w71B9Zuvgh3b7QEdW0DMevNwhuYgaZ0TWrkRR0SoG+6l60DWVzfT
GX0I7MCpLE8JevHZmwfutkQcbVlozcu9sueemvL3v/nEmKP+GlxboR9EqFhXQeyy
/qkhr7Oj/pPHJbvTSuf09VgVRi5c03u7R1Xcc0taNZxSENWovyy/EXkEYjbWaFr7
u+Npt5/6H3XNQKJ0PCSuoOdWPwIDAQABo2AwXjAfBgNVHSMEGDAWgBSE/uqXmcfx
DeH/OVLB6G3ARtAvYzAdBgNVHQ4EFgQUhP7ql5nH8Q3h/zlSwehtwEbQL2MwDgYD
VR0PAQH/BAQDAgGGMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAH9J
a89CFrIUIGGQFg6L2CrYmuOE0bv69UnuodvzG/qEy4GwWUNkUCNu8wNfx3RAgJ8R
KHUbeQY0HjGRaThY8z7Qx8ugA6pDEiwf/BMKPNBPkfhMEGL2Ik02uRThXruA82Wi
OdLY0E3+fx0KULVKS5VvO9Iu5sGXa8t4riDwGWLkfQo2AMLzc+SP4T3udEpG/9BD
nwGOseiz5a/kTAsMircoN2TcqoMBf5LQoA52DJf6MAHd2QZxcnm9ez8igKhzvMG1
OiopI3jTQ38Y9fqCK8E30wUwCozaY3jT0G3F57BfPCfBkkdz1a/Lw7en991xtBcp
```

```
0iptGTDJSt7TruaTvDs=
-----END CERTIFICATE-----
END OF INPUT ---> press Enter
```

Quando sono presenti CA intermedie o subordinate

I certificati devono essere forniti come indicato di seguito:

```
switchName# configure terminal
switchName(config)# crypto ca authenticate <trustpointName>

Input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIDmjCCAoKgAwIBAgIGAVTGvpxRMA0GCSqGSIb3DQEBCwUAMF0xCzAJBgNVBAYT
AkFVMSUwIwYDVQQKDBxDaXNjbyBTeXN0ZW1zIEluYy4gQXVzdHJhbGlhMRIwEAYD
VQQLDAlDaXNjbyBUQUMxEzARBgNVBAMMCk5pa29sYXkgQ0EwHhcNMTYwNTE5MDIw
MTAxWhcNMjYwNTIwMDIwMTE0WjBdMQswCQYDVQQGEwJBVTElMCMGA1UECgwcQ2lz
Y28gU3lzdGVtcyBJbmMuIEF1c3RyYWxpYTESMBAGA1UECwwJQ2lzY28gVEFDMRMw
EQYDVQQDDApOaWtvbGF5IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAm6onXi3JRfIe2NpQ53CDBCUTn8cHGU67XSyqgL7MlYBhH032QaVrT3b98KcW
55UoqQW15kAnJhNTIQ+f0f8oj9A5UbwcQwIXQuHGkDZvJULjidM37tGF90ZVLJs7
sMxsnVSPIe05w71B9Zuvgh3b7QEdW0DMevNwhuYgaZ0TWrkRR0SoG+6l60DWVzfT
GX0I7MCpLE8JevHZmwfutkQcbVlozcu9sueemvL3v/nEmKP+GlxboR9EqFhXQeyy
/qkhr7Oj/pPHJbvTSuf09VgVRi5c03u7R1Xcc0taNZxSENWovyy/EXkEYjbWaFr7
u+Npt5/6H3XNQKJ0PCSuoOdWPwIDAQABo2AwXjAfBgNVHSMEGDAWgBSE/uqXmcfx
DeH/OVLB6G3ARtAvYzAdBgNVHQ4EFgQUhP7ql5nH8Q3h/zlSwehtwEbQL2MwDgYD
VR0PAQH/BAQDAgGGMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAH9J
a89CFrIUIGGQFg6L2CrYmuOE0bv69Unuodvz G/qEy4GwWUNkUCNu8wNfx3RAgJ8R
KHUbeQY0HjGRaThY8z7Qx8ugA6pDEiwf/BMKPNBPkfhMEGL2Ik02uRThXruA82Wi
OdLY0E3+fx0KULVKS5VvO9Iu5sGXa8t4riDwGWLkfQo2AMLzc+SP4T3udEpG/9BD
nwGOseiz5a/kTAsMircoN2TcqoMBf5LQoA52DJf6MAHd2QZxcnm9ez8igKhzvMG1
OiopI3jTQ38Y9fqCK8E30wUwCozaY3jT0G3F57BfPCfBkkdz1a/Lw7en991xtBcp
0iptGTDJSt7TruaTvDs=
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO
MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----
END OF INPUT ---> press Enter
```

Testo in blu -> Viene copiato dal certificato CA (aperto in qualsiasi editor di testo) e incollato quando richiesto nella CLI dello switch.

Testo in rosso -> Da immettere per terminare il certificato.

Qualsiasi errore nel certificato genera questo

```
failed to load or parse certificate
could not perform CA authentication
```

Se si tenta di eseguire l'autenticazione da un certificato CA secondaria senza aggiungere il certificato CA radice, si ottiene

```
incomplete chain (no selfsigned or intermediate cert)
could not perform CA authentication
```

Se tutto è buono

```
Fingerprint(s): SHA1 Fingerprint=E1:37:5F:23:FA:82:0C:63:40:9C:AD:C7:7A:83:C9:6A:EA:54:9A:7A
Do you accept this certificate? [yes/no]:yes
```

Passaggio 4

Generazione delle richieste di firma dei certificati

NX-OS 8.4(1x) e versioni precedenti

```
switchName# configure terminal
switchName(config)# crytpo ca enroll <trustpointName>
Create the certificate request.. Create a challenge password. You need to verbally provide this
password to the CA Administrator in order to revoke your certificate. For security reasons your
password not be saved in the configuration. Please make a note of it. Password: abcdef1234 -----
>(Keep a note of this password that you are entering) The subject name in the certificate be the
name of the switch. Include the switch serial number in the subject name? [yes/no]: no Include
an IP address in the subject name [yes/no]: yes ip address: 192.168.x.x The certificate request
be displayed... -----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0= -----END CERTIFICATE REQUEST---
--
```

La password richiesta di verifica non viene salvata con la configurazione. Questa password è necessaria nel caso in cui sia necessario revocare il certificato, pertanto è necessario ricordarla.

Nota: non utilizzare il carattere '$' per la password. Provoca il fallimento della RSI.

Copia a partire da

```
-----BEGIN CERTIFICATE REQUEST-----
```

Fino a

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

Salvarlo all'esterno dello switch. che deve essere inoltrata alla CA radice o alla CA secondaria (a seconda del tipo di firma) tramite e-mail o con un altro metodo. La CA restituisce un certificato di identità firmato.

NX-OS 8.4(1) e versioni successive.

Per risolvere il problema relativo all'ID bug Cisco CSCvo43832, le richieste di registrazione sono state modificate in NX-OS 8.4(1).

Per impostazione predefinita, il nome del soggetto è uguale al nome dello switch.

Le richieste di iscrizione consentono inoltre di specificare un nome soggetto alternativo e più campi DN.

Nota: il campo DN richiede l'immissione di numeri come esempi e può accettare qualsiasi stringa con tale intervallo di caratteri. Ad esempio, il prompt DN stato indica:

Enter State[1-128]:

Richiede qualsiasi stringa da 1 a 128 caratteri.

```
switchName# configure terminal
switchName(config)# crypto ca enroll <trustpointName>
Create the certificate request ..
Create a challenge password. You need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password not be saved in the configuration.
Please make a note of it.
Password:abcdef1234
The subject name in the certificate is the name of the switch.
Change default subject name? [yes/no]:yes
Enter Subject Name:customSubjectName
Include the switch serial number in the subject name? [yes/no]:yes
The serial number in the certificate is: XXXXXXXXXXX
Include an IP address in the subject name [yes/no]:yes
ip address:192.168.x.x
Include the Alternate Subject Name ? [yes/no]:yes
Enter Alternate Subject Name:AltName
Include DN fields? [yes/no]:yes
Include Country Name ? [yes/no]:yes
Enter Country Code [XX]:US
Include State ? [yes/no]:yes
Enter State[1-128]:NC
Include Locality ? [yes/no]:yes
Enter Locality[1-128]:RTP
Include the Organization? [yes/no]:yes
Enter Organization[1-64]:TAC
Include Organizational Unit ? [yes/no]:yes
Enter Organizational Unit[1-64]:sanTeam
The certificate request is displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIDEjCCAfoCAQAwbzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk5DMQwwCgYDVQQH
DANSVFAxDDAKBgNVBAoMA1RBQzEQMA4GA1UECwwHc2FuVGVhbTElMCMGA1UEAwwc
RjI0MS0xNS0xMC05MTQ4VC0yLmNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAJxGBpaX7j1S5rtLfZhttgvcvDPeXrtFCwOwrSSshPnJfzKN
ZFxzqTtyTSZpTUApfhd2QEDu+rdz+5RB4LF6cP5YNJeiYwQattf65QFfxWffFEuk
BSSvkBwx7y0Bna0fW7rMhDgVF5c9Cj2qNItwkO4Wxx56Guzn/iQGbGQ8Ak3YA/mZ
6lwl4x8Xj15jHwPrg57HB0IJoVFta0SV7DRsCwguq7Vq3CxViQSgdlOn4op699fn
7mENvOFHUfZhPF+YgsUakGeTcJpebu524kg4nZH1eiu9mlrs9VrU0d2qG7Ez+Goi
+GFD0NrauCQSvREpk7dv7l8jMk+tYR6u3ETFYYUCAwEAAaBeMBkGCSqGSIb3DQEJ
BzEMDAphYmNkZWYxMjM0MEEGCSqGSIb3DQEJDjE0MDIwMHYDVR0RAQH/BCYwJIIc
RjI0MS0xNS0xMC05MTQ4VC0yLmNpc2NvLmNvbYcEwKgBCjANBgkqhkiG9w0BAQsF
```

```
AAOCAQEAcBrh5xObTI/SOJ7DLm9sf5rfYFaJ0/1BafKqi2Dp3QPLMIa1jydZwz4q
NdNj7Igb4vZPVv/KBrJCibdjEJUn/YiGMST9PFQLys/Qm0fhQmsWcDxDX5xkE+/x
jZ+/8o5W/p6fPV4xT6sGDydjhA5McYr1o3grj0iPWloP+BaDpZgLpIoUHQygk8RB
SJbRR48QKl6pOVwcLPMXWy4w9Yp24hoJ8LI4Ll10D+urpyeEu0IpXywQdOJShQ3S
LWDEgVQSOhFQ+L7c+GGhnrXNXBD37K5hQ2mwrSIqI0FjDQMfzsBDe8bnDqx/HlLa
EP0sjBxo5AxmGon3ZEdlj6ivoyCA/A==
-----END CERTIFICATE REQUEST-----
```

Passaggio 5

Installazione dei certificati di identità

Nota: il numero massimo di certificati di identificazione che è possibile configurare su uno switch è 16.

```
switch# configure terminal
switch(config)# crypto ca import <trustpointName> certificate
input (cut & paste) certificate in PEM format: -----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD
VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz
Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu
Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XENlcnRFbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw E36cIZu4WsExREqxbTk8ycx7V5o= --
---END CERTIFICATE-----
```

Passaggio 6

Salvare la configurazione

```
switch# copy running-config startup-config
```

Verifica

```
switchName# show crypto ca certificates

Trustpoint: <trustpointName>

certificate: ---> Identity Certificate
subject= /CN=CP-SAND-MDS-A.example.com
issuer= /C=GB/O=England/CN=Utility CA1
serial=16D34BA800004441C69D
notBefore=Nov 15 08:11:47 2021 GMT
```

```
notAfter=Nov 14 08:11:47 2023 GMT
SHA1 Fingerprint=03:E0:73:FE:31:C5:4A:84:C0:77:21:0F:3A:A0:05:29:55:FF:9B:7E
purposes: sslserver sslclient ike

CA certificate 0: ---> CA Certificate of Sub CA
subject= /C=GB/O=England/CN=Eng Utility CA1
issuer= /C=GB/O= England/CN=EngRoot CA
serial=616F2990AB000078776000002
notBefore=Aug 14 11:22:48 2012 GMT
notAfter=Aug 14 11:32:48 2022 GMT
SHA1 Fingerprint=DF:41:1D:E7:B7:AD:6F:3G:05:F4:E9:99:B2:9F:9C:80:73:83:1D:B4
purposes: sslserver sslclient ike

CA certificate 1: ---> CA Certificate of Root CA
subject= /C=GB/O=England/CN=Eng Root CA
issuer= /C=GB/O=Bank of England/CN=Eng Root CA
serial=435218BABA57D57774BFA7A37A4E54D52
notBefore=Aug 14 10:08:30 2012 GMT
notAfter=Aug 14 10:18:09 2032 GMT
SHA1 Fingerprint=E3:F9:85:AC:1F:66:22:7C:G5:36:2D:89:5A:B4:3C:06:0E:2A:DB:13
purposes: sslserver sslclient ike

switchName# show crypto key mypubkey rsa
key label: <rsaKeyPairName>
key size: 2048
exportable: yes
key-pair already generated

switchName# show crypto ca crl <trustpointName>
Trustpoint: <trustpointName>
```

==========

Limitazioni e avvertenze

Limiti massimi per CA e certificato digitale

Funzionalità	Limite massimo
Trust point dichiarati su uno switch	16
Coppie di chiavi RSA generate su uno switch	16
Coppia di chiavi RSA	4096 bit
Certificati di identità configurati in uno switch	16
Certificati in una catena di certificati CA	10
Punti di attendibilità autenticati per una CA specifica	10

Impostazioni predefinite

Parametri	Predefinito
Trust point	Nessuna
coppia di chiavi RSA	Nessuna
Etichetta coppia di chiavi RSA	FQDN switch
Modulo RSA key-pair	512
coppia di chiavi RSA esportabile	Sì
Metodo di verifica revoca del trust point	CRL

Avvertenze

ID bug Cisco CSCvo43832 - La richiesta di firma del certificato (CSR) MDS 9000 non include tutti i campi del nome distinto (DN)

ID bug Cisco CSCvt46531 - È necessario documentare i comandi 'trustpool' dell'infrastruttura a chiave pubblica (PKI)

ID bug Cisco CSCwa77156 - Guida alla configurazione della sicurezza di Cisco MDS serie 9000, versione 8.x da aggiornare con il carattere della password

ID bug Cisco CSCwa54084 - Il nome soggetto alternativo non è corretto nel CSR generato da NX-OS

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).