Vertrauenspunkte konfigurieren und Zertifikate auf MDS 9000-Switches installieren

Inhalt

Einleitung

In diesem Dokument werden die Konfigurationsschritte für die Konfiguration von Trustpoint und Zertifikaten in den MDS-Switches beschrieben.

Hintergrundinformationen

Die Unterstützung der Public Key Infrastructure (PKI) ermöglicht es Cisco Multilayer Director Switches (MDS) der 9000-Familie, digitale Zertifikate für die sichere Kommunikation im Netzwerk zu erhalten und zu verwenden. Die PKI-Unterstützung bietet Verwaltbarkeit und Skalierbarkeit für IP Security (IPsec), Internet Key Exchange (IKE) und Secure Shell (SSH).

Voraussetzungen

Sie müssen den Hostnamen und den IP-Domänennamen des Switches konfigurieren, wenn diese noch nicht konfiguriert sind.

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

Hinweis: Wenn Sie den IP-Hostnamen oder den IP-Domänennamen nach dem Generieren des Zertifikats ändern, wird das Zertifikat möglicherweise ungültig.

Verständnis einiger verwandter Schlüsselwörter

Vertrauenspunkt: Ein lokal konfiguriertes Objekt, das Informationen über eine vertrauenswürdige Zertifizierungsstelle (Certificate Authority, CA) enthält, einschließlich der lokalen RSA-Tastatur, der öffentlichen Zertifizierungsstellenzertifikate und des Identitätszertifikats, das von einer Zertifizierungsstelle an den Switch ausgegeben wird. Mehrere Vertrauenspunkte können konfiguriert werden, um Switch-Identitätszertifikate von mehreren Zertifizierungsstellen zu registrieren. Die vollständigen Identitätsinformationen eines Vertrauenspunkts können in eine Datei im kennwortgeschützten PKCS12-Standardformat exportiert werden. Er kann später auf denselben Switch (z. B. nach einem Systemabsturz) oder auf einen Ersatzswitch importiert werden. Die Informationen in einer PKCS12-Datei bestehen aus dem RSA-Schlüsselpaar, dem Identitätszertifikat und dem Zertifizierungsstellenzertifikat (oder der Kette).

Zertifizierungsstellenzertifikat: Dies ist das Zertifikat, das von der Zertifizierungsstelle (Certification Authority, CA) für sich selbst ausgestellt wird. In der Konfiguration kann eine Zwischen- oder untergeordnete Zertifizierungsstelle vorhanden sein. In diesem Fall kann dies auch auf das öffentliche Zertifikat der Zwischen- oder untergeordneten Zertifizierungsstelle verweisen.

Zertifizierungsstellen (Certificate Authorities, CAs): Geräte, die Zertifikatanforderungen verwalten und Identitätszertifikate an Einheiten wie Hosts, Netzwerkgeräte oder Benutzer ausstellen. CAs bieten ein zentrales Schlüsselmanagement für diese Einheiten.

RSA-Schlüsselpaar: Wird mit der CLI im Switch generiert und mit dem Vertrauenspunkt verknüpft. Für jeden auf dem Switch konfigurierten Trustpoint müssen Sie eine eindeutige RSA-Schlüsselpaar generieren und diese dem Trustpoint zuordnen.

Certification Signing Request (CSR) - Eine Anforderung, die vom Switch generiert und zur Signatur an die Zertifizierungsstelle gesendet wird. Für diesen CSR sendet die CA das Identitätszertifikat zurück.

Identitätszertifikat: Dies ist das Zertifikat, das von der Zertifizierungsstelle für den Switch signiert und ausgestellt wird, von dem der CSR generiert wird. Sobald ein CSR an eine CA übermittelt wurde, stellt die CA oder ein Administrator das Identitätszertifikat per E-Mail oder über einen Webbrowser bereit. Um ein Identitätszertifikat in einen MDS-Vertrauenspunkt einzufügen, muss es im Standard-PEM-Format (base64) vorliegen.

Anforderungen

Stammzertifizierungsstelle .

Sub-Zertifizierungsstellenzertifikate (Wenn die Identitätszertifikate von der Sub-Zertifizierungsstelle signiert werden) In diesem Fall müssen dem Switch auch Zertifizierungsstellenzertifikate der Sub-Zertifizierungsstelle hinzugefügt werden.

Identitätszertifikat

Konfigurieren

Schritt 1

Generieren eines RSA-Schlüsselpaars

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

(Gültige Modulwerte sind (Standard) 512, 768, 1024, 1536, 2048 und 4096)

Schritt 2

Erstellen eines Zertifizierungsstellen-Vertrauenspunkts und Zuordnen des RSA-Schlüsselpaars zum Vertrauenspunkt

Der FQDN des Switches wird als Standard-Schlüsselbezeichnung verwendet, wenn während der Schlüsselpaar-Generierung kein Schlüssel angegeben wird.

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

Schritt 3

Authentifizieren einer Zertifizierungsstelle für Vertrauenspunkte

Wenn es sich bei der authentifizierten Zertifizierungsstelle nicht um eine selbstsignierte Zertifizierungsstelle handelt, muss während des Zertifizierungsstellenauthentifizierungsschritts die vollständige Liste der Zertifizierungsstellenzertifikate aller Zertifizierungsstellen in der Zertifizierungskette eingegeben werden. Dies wird als Zertifizierungsstellen-Zertifikatkette der authentifizierten Zertifizierungsstelle bezeichnet. Die maximale Anzahl von Zertifikaten in einer Zertifizierungsstellenzertifikatkette beträgt 10.

Wenn nur eine Stammzertifizierungsstelle vorhanden ist

```
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
```

Bei Zwischen- oder untergeordneten Zertifizierungsstellen

Die Bescheinigungen sind wie folgt vorzulegen:

```
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-------
-----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
```

Blauer Text -> Dieser wird aus dem CA-Zertifikat kopiert (in einem Texteditor geöffnet) und eingefügt, wenn in der Switch-CLI dazu aufgefordert wird.

Red Color Text -> Dies ist einzugeben, um das Zertifikat zu beenden.

Jeder Fehler im Zertifikat führt dazu, dass

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

Wenn Sie versuchen, sich von einem Zertifikat der Sub-Zertifizierungsstelle aus zu authentifizieren, ohne das erhaltene Zertifikat der Root-Zertifizierungsstelle hinzuzufügen

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

Wenn alles gut ist

```
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
```

Schritt 4

Generieren von Zertifikatsignierungsanforderungen

NX-OS 8.4(1x) und frühere Version

```
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---
--
```

Das Challenge-Passwort wird bei der Konfiguration nicht gespeichert. Dieses Kennwort ist für den Fall erforderlich, dass Ihr Zertifikat widerrufen werden muss. Sie müssen sich dieses Kennwort daher merken.

Hinweis: Verwenden Sie nicht das Zeichen "$" für Ihr Kennwort. Dies führt zum Scheitern der CSR.

Kopieren Sie diese ab

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

Bis

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

Speichern Sie den Wert außerhalb des Switches. Diese muss per E-Mail oder auf andere Weise an die Stamm-CA oder Sub-CA weitergeleitet werden (je nachdem, welches signiert wird). Die Zertifizierungsstelle gibt ein signiertes Identitätszertifikat zurück.

NX-OS 8.4(1) und höher

Als Korrektur für den Cisco Bug CSCvo43832 wurden die Anmeldeaufforderungen in NX-OS 8.4(1) geändert.

Der Betreffname entspricht standardmäßig dem Namen des Switches.

Bei den Anmeldeaufforderungen sind auch ein Alternativer Betreffname und mehrere DN-Felder zulässig.

Hinweis: Das DN-Feld fordert eine Eingabe mit Zahlen an, da Beispiele jede Zeichenfolge mit diesem Zeichenbereich akzeptieren können. Die Eingabeaufforderung für den Status-DN lautet z. B.:

Geben Sie State [1-128] ein:

Es kann eine beliebige Zeichenkette zwischen 1 und 128 Zeichen enthalten.

```
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-----
```

Schritt 5

Installieren von Identitätszertifikaten

Hinweis: Sie können maximal 16 ID-Zertifikate für einen Switch konfigurieren.

```
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-----
```

Schritt 6

Speichern Sie die Konfiguration

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

Überprüfung

```
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>
================================================================================
========================
```

Einschränkungen und Hinweise

Maximale Grenzwerte für Zertifizierungsstelle und digitales Zertifikat

Funktion	Maximaler Grenzwer
Vertrauenswürdige Punkte, die für einen Switch deklariert wurden	16
Auf einem Switch erzeugte RSA-Schlüsselpaare	16
Größe des RSA-Schlüsselpaars	4096 Bit
Auf einem Switch konfigurierte Identitätszertifikate	16
Zertifikate in einer Zertifikatskette einer Zertifizierungsstelle	10
Vertrauenspunkte, die an eine bestimmte Zertifizierungsstelle authentifiziert wurden	10

Standardeinstellungen

Parameter	Standard
Vertrauenswürdiger Punkt	None
RSA-Schlüsselpaar	None
RSA-Schlüsselpaar-Label	Switch-FQDN
RSA-Schlüsselpaar-Modul	512
Exportierbares RSA-Schlüsselpaar	Ja
Widerrufskontrollmethode für Vertrauenspunkt	Sperrliste

Hinweise

Cisco Bug-ID CSCvo43832 - MDS 9000 Certificate Signing Request (CSR) enthält nicht alle Distinguished Name (DN)-Felder

Cisco Bug-ID CSCvt46531 - Es müssen PKI-"Trustpool"-Befehle dokumentiert werden.

Cisco Bug-ID CSCwa7156 - Cisco MDS 9000 Series Security Configuration Guide, Release 8.x Benötigt Aktualisierung des Kennwortzeichens

Cisco Bug-ID CSCwa54084 - 'Alternativer Betreff-Name' ist in der von NX-OS generierten CSR-Datei falsch

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.