Configurar pontos confiáveis e instalar certificados em switches MDS 9000

Contents

Introduction

Este documento descreve as etapas de configuração para a configuração de pontos confiáveis e certificados nos switches MDS.

Informações de Apoio

O suporte à Public Key Infrastructure (PKI) fornece os meios para que os switches da família Cisco Multilayer Diretor Switch (MDS) 9000 obtenham e usem certificados digitais para comunicação segura na rede. O suporte a PKI fornece capacidade de gerenciamento e escalabilidade para IP Security (IPsec), Internet Key Exchange (IKE) e Secure Shell (SSH).

Prerequisites

Você deve configurar o nome de host e o nome de domínio IP do switch, caso ainda não estejam configurados.

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

Observação: alterar o nome do host IP ou o nome do domínio IP após gerar o certificado pode invalidar o certificado.

Compreensão de poucas palavras-chave relacionadas

Ponto confiável : um objeto configurado localmente que contém informações sobre uma Autoridade de Certificação (CA) confiável, incluindo o par de chaves RSA local, os certificados públicos da CA e o certificado de identidade emitido para o switch por uma CA. Vários pontos confiáveis podem ser configurados para registrar certificados de identidade do switch de várias CAs. As informações de identidade completas em um ponto de confiança podem ser exportadas para um arquivo no formato padrão PKCS12 protegido por senha. Ele pode ser importado posteriormente para o mesmo switch (por exemplo, após um travamento do sistema) ou para um switch de substituição. As informações em um arquivo PKCS12 consistem no par de chaves RSA, no certificado de identidade e no certificado (ou cadeia) de CA.

Certificado CA : este é o certificado emitido pela Autoridade de Certificação (CA) em relação a si mesmo. Pode haver uma CA Intermediária ou Subordinada na configuração. Nesse caso, isso também pode se referir ao certificado público da CA subordinada ou intermediária.

Autoridades de Certificação (CAs) : dispositivos que gerenciam solicitações de certificado e emitem certificados de identidade para entidades como hosts, dispositivos de rede ou usuários. As autoridades de certificação fornecem um gerenciamento centralizado de chaves a essas entidades.

Par de chaves RSA : gerado com cli no switch e associado ao ponto de confiança. Para cada ponto confiável configurado no switch, você deve gerar um par de chaves RSA exclusivo e associá-lo ao ponto confiável.

Solicitação de Assinatura de Certificação (CSR) Esta é uma solicitação que é gerada a partir do switch e enviada para a CA para ser assinada. Em relação a esse CSR, a CA envia de volta o certificado de identidade.

Certificado de Identidade : este é o certificado que é assinado e emitido pela Autoridade de Certificação para o switch a partir do qual o CSR é gerado. Quando um CSR é enviado a uma CA, a CA ou o administrador fornece o Certificado de identidade por e-mail ou por meio de um navegador da Web. Para colar um Certificado de Identidade em um ponto de confiança MDS, ele deve estar no formato PEM padrão (base64).

Requirements

CA raiz.

Certificados da Sub CA (se os certificados de identidade forem assinados pela Sub CA) Nesse caso, os certificados da Sub CA também precisam ser adicionados ao switch.

Certificado de identidade

Configurar

Passo 1

Gerar um par de chaves RSA

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

(Os valores de módulo válidos são (padrão) 512, 768, 1024, 1536, 2048 e 4096)

Passo 2

Crie um CA Trust Point e associe o par de chaves RSA ao ponto confiável

O FQDN do switch é usado como um rótulo de chave padrão quando nenhum é especificado durante a geração do par de chaves.

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

Etapa 3

Autenticando uma Autoridade de Certificação de Ponto de Confiança

Se a CA que está sendo autenticada não for uma CA autoassinada, a lista completa dos certificados de CA de todas as CAs na cadeia de certificação precisará ser inserida durante a etapa de autenticação da CA. Isso é chamado de cadeia de certificados CA da CA que está sendo autenticada. O número máximo de certificados em uma cadeia de certificados de CA é 10.

Quando somente há CA raiz

```
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 houver CAs intermediárias ou subordinadas

Os certificados devem ser fornecidos da seguinte forma:

```
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
```

Texto em azul -> É copiado do certificado da CA (aberto em qualquer editor de texto) e colado quando solicitado na CLI do switch.

Texto em vermelho -> Deve ser inserido para encerrar o certificado.

Qualquer erro no certificado resulta nesta

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

Se você tentar autenticar de um certificado Sub CA sem adicionar o certificado Root CA, você obterá

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

Se tudo estiver bem

```
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
```

Passo 4

Gerando Solicitações de Assinatura de Certificado

NX-OS 8.4(1x) e anterior

```
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---
--
```

A senha de desafio não é salva com a configuração. Essa senha é necessária caso o certificado precise ser revogado, portanto, lembre-se dessa senha.

Observação: não use o caractere '$' como senha. Causa falha no CSR.

Copiar isto a partir de

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

Até

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

Salve-o fora do switch. Isso precisa ser encaminhado para a CA raiz ou sub CA (o que for indicado por um sinal) por e-mail ou outro método. A CA retorna um Certificado de Identidade assinado.

NX-OS 8.4(1) e posterior.

Como uma correção para o bug da Cisco ID CSCvo43832 , os prompts de inscrição foram alterados no NX-OS 8.4(1).

Por padrão, o Nome do assunto é igual ao nome do switch.

Os prompts de inscrição também permitem um Nome de Assunto Alternativo e vários campos DN.

Observação: Os prompts do campo DN com números como exemplos podem aceitar qualquer string com essa faixa de caracteres. Por exemplo, o prompt de DN de estado diz:

Insira o estado[1-128]:

Ele aceita qualquer sequência de caracteres de 1 a 128 caracteres.

```
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-----
```

Etapa 5

Instalando certificados de identidade

Observação: o número máximo de certificados de identificação que você pode configurar em um switch é 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-----
```

Etapa 6

Salve a configuração

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

Verificar

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

Limitações e caveats

Limites Máximos para AC e Certificado Digital

Recurso	Limite máximo
Pontos de confiança declarados em um switch	16
Pares de chaves RSA gerados em um switch	16
Tamanho do par de chaves RSA	4096 bits
Certificados de identidade configurados em um switch	16
Certificados em uma cadeia de certificados CA	10
Pontos de confiança autenticados para uma autoridade de certificação específica	10

Configurações padrão

Parâmetros	Padrão
Ponto de confiança	Nenhum
par de chaves RSA	Nenhum
Rótulo de par de chaves RSA	FQDN do Switch
Módulo de par de chaves RSA	512

par de chaves RSA exportável	Yes
Método de verificação de revogação do ponto de confiança	CRL

Caveats

O bug da Cisco ID CSCvo43832 - MDS 9000 Certificate Signing Request (CSR) não inclui todos os campos Distinguished Name (DN)

ID de bug Cisco CSCvt46531 - É necessário documentar os comandos 'trustpool' de PKI

ID de bug Cisco CSCwa7156 - Guia de Configuração de Segurança Cisco MDS 9000 Series, Versão 8.x Precisa de Atualização no Caractere de Senha

ID de bug da Cisco CSCwa54084 - 'Nome alternativo do assunto' está incorreto no CSR gerado pelo NX-OS

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.