Instalar certificados de administrador da Web nos switches Catalyst 9000

Contents

Introdução

Este documento descreve o processo para gerar, fazer download e instalar certificados nos Catalyst 9000 Series Switches.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Como configurar os switches da série Catalyst 9000
- Como assinar certificados usando o Microsoft Windows Server
- Infraestrutura de Chave Pública (PKI) e certificados digitais

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Switch Cisco Catalyst 9300, Cisco IOS® XE versão 17.12.4
- Microsoft Windows Server 2022

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento fornece um guia passo a passo para gerar uma CSR (Certificate Signing Request, solicitação de assinatura de certificado), obtê-la assinada por uma CA (Certification Authority, autoridade de certificação) e instalar o certificado resultante (juntamente com o certificado CA) em um switch Catalyst 9000.

O objetivo é permitir a administração segura da Web (HTTPS) do switch usando um certificado confiável, garantindo a compatibilidade com navegadores da Web modernos e a conformidade com políticas de segurança organizacionais.

Configurar

Esta seção fornece um fluxo de trabalho detalhado para gerar, assinar e instalar um certificado de administrador da Web em um switch Catalyst 9000. Cada etapa inclui comandos CLI relevantes, explicações e exemplos de saída.

Passo 1: Definir uma Chave

Gere um par de chaves RSA de uso geral e use-o para proteger o certificado. A chave deve ser exportável e pode ser dimensionada de acordo com as necessidades de segurança (1024 a 4096 bits).

<#root>

```
device(config)#
```

crypto key generate rsa general-keys label csr-key exportable

Exemplo de saída quando solicitado o tamanho do módulo:

<#root>

```
The name for the keys will be:
```

csr-key

```
Choose the size of the key modulus in the range of 512 to 4096 for your  General Purpose Keys. Choosing
How many bits in the modulus [1024]:
```

```
4096

% Generating 4096 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 4 seconds)
```

Passo 2: Gerar uma CSR (Certificate Signing Request, solicitação de assinatura de certificado)

Configure um ponto confiável no switch para o certificado de administrador da Web, especificando a inscrição via terminal, desabilitando a verificação de revogação e fornecendo informações de identificação (nome da entidade, chave e nomes alternativos da entidade).

<#root>

```
device(config)#

crypto pki trustpoint webadmin-TP

device(ca-trustpoint)#

enrollment terminal pem

device(ca-trustpoint)#

revocation-check none

device(ca-trustpoint)#

subject-name C=SJ, ST=CA, L=CA, O=TAC, OU=LANSW, CN=myc9300.local-domain

device(ca-trustpoint)#

rsakeypair csr-key

device(ca-trustpoint)#

subject-alt-name mywebadmin.com

device(ca-trustpoint)#exit
```

Registre o ponto confiável para gerar o CSR. Você deve ser solicitado a fornecer várias opções; fornecer "sim" ou "não" conforme necessário. A solicitação de certificado deve ser exibida no terminal.

```
device(config)#crypto pki enroll webadmin-TP
```

Saída de exemplo:

<#root>

```
% Start certificate enrollment ..
```

```
% The subject name in the certificate will include:
```

C=SJ, ST=CA, L=CA, O=TAC, OU=LANSW, CN=myc9300.local-domain

```
% The subject name in the certificate will include: C9300.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% Include an IP address in the subject name? [no]: yes
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
-----BEGIN CERTIFICATE REQUEST-----

-----END CERTIFICATE REQUEST-----
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]:
```

no

Parâmetros disponíveis para a configuração do nome do assunto:

- C : País, somente duas letras maiúsculas (EUA)
- ST: Nome do estado ou província
- I: Nome do local (cidade)
- O: Nome da organização (empresa)
- OU: Nome da unidade organizacional (departamento/seção)
- CN: Nome comum (FQDN ou endereço IP a ser acessado)

Passo 3: Enviar o CSR para a autoridade de certificação

Copie a sequência de caracteres CSR completa (incluindo as linhas BEGIN e END) e envie-a à sua CA para assinatura.

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

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

Se você usar uma CA do Microsoft Windows Server, baixe o certificado assinado no formato Base64. Normalmente, você recebe o certificado do dispositivo assinado e, possivelmente, um certificado de CA raiz.

Passo 4: Autenticar Certificado CA Base64 Raiz

Instale o certificado da CA (no formato Base64) no switch para estabelecer confiança na CA que emitiu o certificado do dispositivo.

<#root>

```
device(config)#
```

crypto pki authenticate webadmin-TP

Cole o certificado da CA (incluindo as linhas BEGIN e END) quando solicitado. Exemplo:

<#root>

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
Certificate has attributes:
      Fingerprint MD5: C7224F3A A9B0426A FDCC50E6 8A04583E
      Fingerprint SHA1: 9B31C319 A515AC41 0114EA43 33716E8B 472A4EF5
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
%
```

Certificate successfully imported

Passo 5: Autenticar Certificado de Dispositivo Base64

Autentique o certificado assinado do dispositivo com o certificado de autoridade de certificação instalado.

<#root>

```
device(config)#
```

crypto pki trustpoint webadmin-TP

```
device(ca-trustpoint)#
```

chain-validation stop

```
device(ca-trustpoint)#
```

crypto pki authenticate webadmin-TP

Quando solicitado, cole no certificado do dispositivo:

<#root>

```
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
Certificate has the following attributes:
Fingerprint MD5: DD05391A 05B62573 A38C18DD CDA2337C
Fingerprint SHA1: 596DD2DC 4BF26768 CFB14546 BC992C3F F1408809
Certificate validated - Signed by existing trustpoint CA certificate.

Trustpoint CA certificate accepted.
```

```
% Certificate successfully imported
```

Passo 6: Importar certificado assinado do dispositivo no switch Catalyst 9000

Importe o certificado de dispositivo assinado Base64 para o ponto confiável.

<#root>

```
device(config)#
crypto pki import webadmin-TP certificate
```

Cole o certificado quando solicitado:

<#root>

```
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
< 9300 device certificate >
-----END CERTIFICATE-----

% Router Certificate successfully imported
```

Nesse ponto, o certificado do dispositivo é importado para o switch junto com todas as CAs relevantes e o certificado está pronto para uso, incluindo o acesso à GUI (HTTPS).

Passo 7: Usar o novo certificado

Associe o ponto confiável ao servidor seguro HTTP e habilite o acesso HTTPS no switch.

<#root>

```
device(config)#
ip http secure-trustpoint webadmin-TP
```

<#root>

```
device(config)#
no ip http secure-server
```

<#root>

device(config)#

ip http secure-server

Passo 8: Como garantir que o certificado seja confiável para navegadores da Web

- O Nome Comum (CN) do certificado ou um Nome Alternativo da Entidade (SAN) deve corresponder à URL acessada pelo navegador.
- O certificado deve estar dentro do seu período de validade.
- O certificado deve ser emitido por uma CA (ou cadeia de CAs) cuja raiz é confiável pelo navegador. O switch deve fornecer a cadeia completa de certificados (exceto a CA raiz, que normalmente já está presente no armazenamento do navegador).
- Se o certificado contiver listas de revogação, verifique se o navegador pode baixá-las e se o CN do certificado não está listado em nenhuma lista de revogação.

Verificar

Você pode usar estes comandos para verificar a configuração do certificado e o status atual:

Exibir os certificados instalados e seu status para um ponto confiável:

<#root>

device#

show crypto pki certificate webadmin-TP

Saída de exemplo:

<#root>

Certificate Status:

 Available

Certificate Serial Number (hex): 4700000129584BB4BAFA13EABB000000000129
Certificate Usage: General Purpose
Issuer:

cn=mitch-DC02-CA   dc=mitch   dc=local

Subject: Name:

C9300.cisco.com

            Serial Number: XXXXXXXXXX
            cn=

myc9300.local-domain

ou=LANSW
o=TAC
l=CA
st=CA
c=SJ

hostname=C9300.cisco.com

Validity Date:
    start date: 05:09:42 UTC Jun 12 2025
    end   date: 07:25:06 UTC Dec 16 2026
Associated Trustpoints:

webadmin-TP

CA Certificate Status: Available
Certificate Serial Number (hex): 101552448B9C2EBB488C40034C129F4A
Certificate Usage: Signature
Issuer: cn=mitch-DC02-CA   dc=mitch   dc=local
Subject: cn=mitch-DC02-CA   dc=mitch   dc=local

Validity Date:

    start date: 07:15:06 UTC Dec 16 2021

end   date: 07:25:06 UTC Dec 16 2026

Associated Trustpoints: webadmin-TP RootCA

Verifique o status do servidor HTTPS e o ponto de confiança associado:

<#root>

device#

show ip http server secure status

Saída de exemplo:

<#root>

HTTP secure server status: Enabled

HTTP secure server port: 443
HTTP secure server ciphersuite: rsa-aes-cbc-sha2 rsa-aes-gcm-sha2
                                 dhe-aes-cbc-sha2 dhe-aes-gcm-sha2
                                 ecdhe-rsa-aes-cbc-sha2
                                 ecdhe-rsa-aes-gcm-sha2 ecdhe-ecdsa-aes-gcm-sha2
HTTP secure server TLS version: TLSv1.2 TLSv1.1

```
HTTP secure server client authentication: Disabled
HTTP secure server PIV authentication: Disabled
HTTP secure server PIV authorization only: Disabled

HTTP secure server trustpoint: webadmin-TP

HTTP secure server peer validation trustpoint:
HTTP secure server ECDHE curve: secp256r1
HTTP secure server active session modules: ALL
```

Troubleshooting

Se você encontrar problemas durante o processo de instalação do certificado, use esses comandos para ativar a depuração de transações PKI. Isso é especialmente útil para diagnosticar falhas durante a importação ou registro de certificados.

<#root>

```
device#

debug crypto pki transactions
```

Exemplo de uma saída de depuração de cenário bem-sucedida:

<#root>

```
*Jun 12 05:16:03.531: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named C9300.cisco.com has been generated or
*Jun 12 05:16:03.534:

 %CRYPTO-6-AUTOGEN: Generated new 2048 bit key pair

*Jun 12 05:16:03.556: CRYPTO_PKI: unlocked trustpoint RootCA, refcount is 0
*Jun 12 05:16:03.556: CRYPTO_PKI: using private key C9300.cisco.com for enrollment
*Jun 12 05:16:04.489: CRYPTO_PKI: Adding myc9300.local-domain to subject-alt-name field
*Jun 12 05:16:17.463: CRYPTO_PKI: using private key csr-key for enrollment
*Jun 12 05:18:32.378: CRYPTO_PKI: locked trustpoint webadmin-TP, refcount is 1
*Jun 12 05:19:15.464: CRYPTO_PKI: unlocked trustpoint webadmin-TP, refcount is 0
*Jun 12 05:19:15.470: CRYPTO_PKI: trustpoint webadmin-TP authentication status = 0
*Jun 12 05:19:15.472: CRYPTO_PKI: (A018E) Session started - identity not specified
*Jun 12 05:19:15.473: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
*Jun 12 05:19:15.473: CRYPTO_PKI: Found a subject match
*Jun 12 05:19:15.473: CRYPTO_PKI: (A018E) Check for identical certs
*Jun 12 05:19:15.473: CRYPTO_PKI: Found a issuer match
*Jun 12 05:19:15.473: CRYPTO_PKI: (A018E) Suitable trustpoints are: RootCA,
*Jun 12 05:19:15.473: CRYPTO_PKI: (A018E) Attempting to validate certificate using RootCA policy
*Jun 12 05:19:15.473: CRYPTO_PKI: (A018E)

Using RootCA to validate certificate

*Jun 12 05:19:15.474: CRYPTO_PKI(make trusted certs chain)
*Jun 12 05:19:15.474: CRYPTO_PKI:

Added 1 certs to trusted chain.

*Jun 12 05:20:05.555: CRYPTO_PKI: locked trustpoint webadmin-TP, refcount is 1
```

```
*Jun 12 05:20:25.734: CRYPTO_PKI: unlocked trustpoint webadmin-TP, refcount is 0
*Jun 12 05:20:25.735: CRYPTO_PKI(Cert Lookup)
```

issuer="cn=mitch-DC02-CA,dc=mitch,dc=local"

```
 serial number= 10 15 52 44 8B 9C 2E BB 48 8C 40 03 4C 12 9F 4A
*Jun 12 05:20:25.735: CRYPTO_PKI: crypto_pki_get_cert_record_by_cert()
*Jun 12 05:20:25.735: CRYPTO_PKI:
```

Found a cert match

```
*Jun 12 05:20:25.735: CRYPTO_PKI: crypto_pki_authenticate_tp_cert()
*Jun 12 05:20:25.735: CRYPTO_PKI: trustpoint webadmin-TP authentication status = 0
*Jun 12 05:20:32.094: PKI: Cert key-usage: Digital-Signature , Certificate-Signing , CRL-Signing
*Jun 12 05:20:32.096: CRYPTO_PKI:
```

Notify subsystem about new certificate.

```
*Jun 12 05:20:32.097: CRYPTO_PKI: unlocked trustpoint webadmin-TP, refcount is 0
*Jun 12 05:21:50.789: CRYPTO_PKI:
```

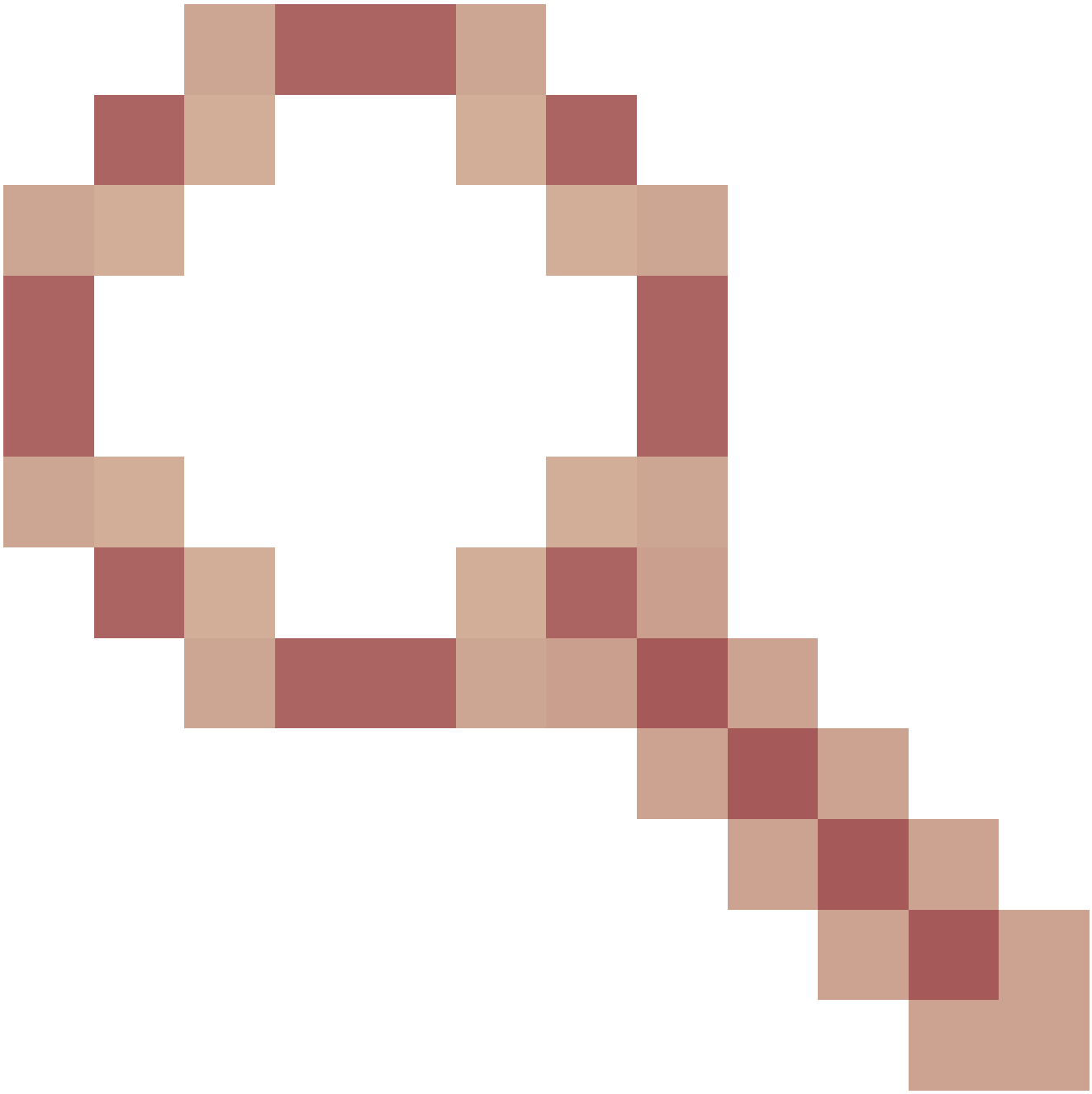
using private key csr-key for enrollment

```
*Jun 12 05:22:12.947: CRYPTO_PKI:
```

make trustedCerts list for webadmin-TP

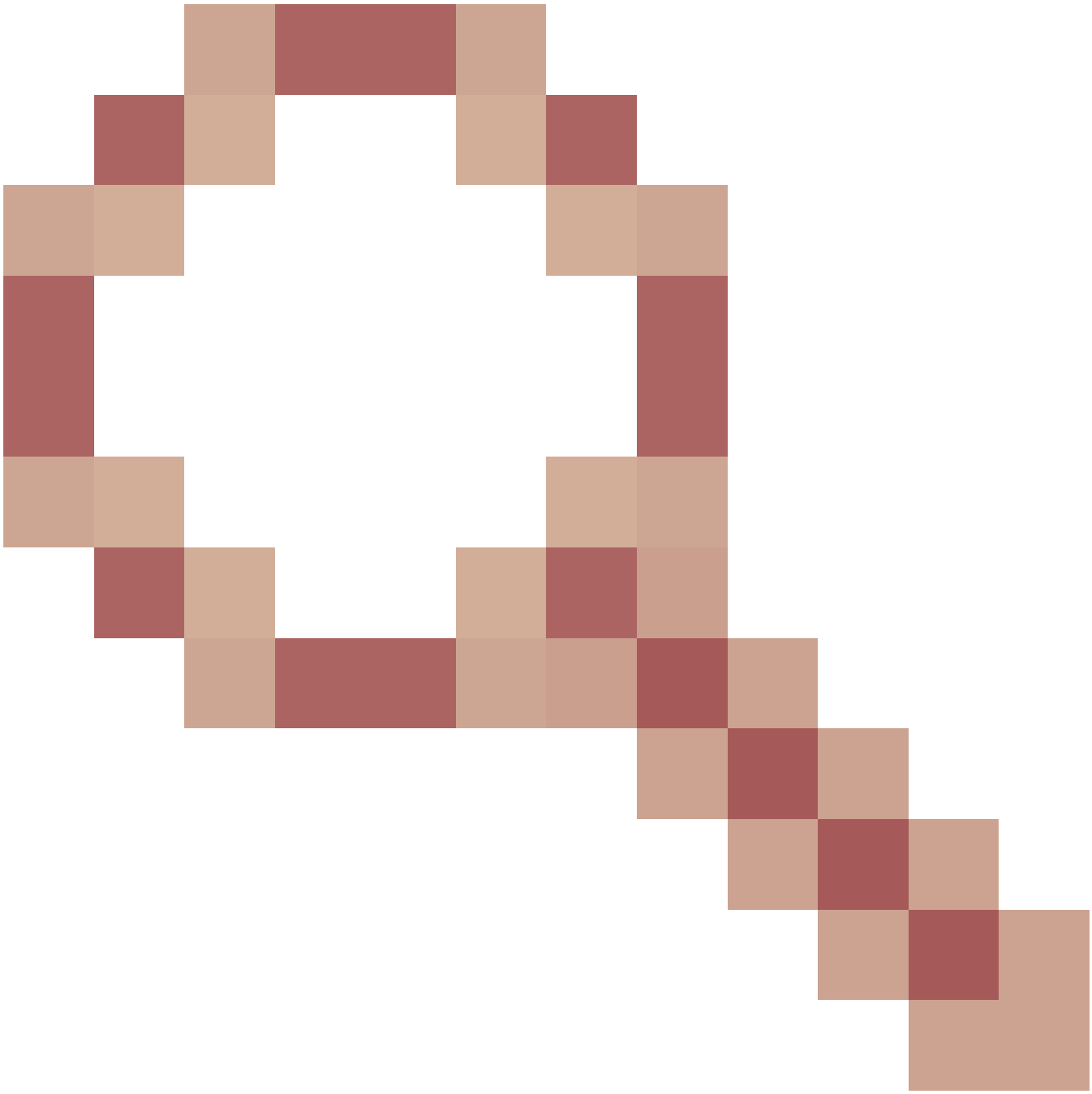
Notas e limitações

- O Cisco IOS® XE não suporta certificados CA com validade superior a 2099 (ID de bug Cisco CSCvp64208



).

- O Cisco IOS® XE não suporta pacotes SHA256 message digest PKCS 12 (certificados SHA256 são suportados, mas não se o próprio pacote PKCS12 for assinado com SHA256) (ID de bug Cisco CSCvz41428



). Isso foi corrigido em 17.12.1.

Informações Relacionadas

- Suporte técnico e downloads da Cisco

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.