Installazione dei certificati Web Admin sugli switch Catalyst 9000

Sommario

Introduzione

In questo documento viene descritto il processo di generazione, download e installazione dei certificati sugli switch Catalyst serie 9000.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Come configurare gli switch Catalyst serie 9000
- Come firmare i certificati utilizzando Microsoft Windows Server
- Infrastruttura a chiave pubblica (PKI) e certificati digitali

Componenti usati

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

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

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

Questo documento offre una guida dettagliata alla generazione di una richiesta di firma di un certificato (CSR), alla firma di un'Autorità di certificazione (CA) e all'installazione del certificato risultante (insieme al certificato CA) su uno switch Catalyst 9000.

L'obiettivo è quello di abilitare l'amministrazione sicura sul Web (HTTPS) dello switch utilizzando un certificato attendibile, garantendo la compatibilità con i browser Web più recenti e la conformità con i criteri di sicurezza aziendali.

Configurazione

In questa sezione viene descritto in dettaglio il flusso di lavoro per la generazione, la firma e l'installazione di un certificato amministratore Web su uno switch Catalyst 9000. Ogni passaggio include comandi CLI, spiegazioni e output di esempio rilevanti.

Passaggio 1: Definisci una chiave

Generare una coppia di chiavi RSA generica e utilizzarla per proteggere il certificato. La chiave deve essere esportabile e può essere ridimensionata in base alle esigenze di sicurezza (da 1024 a 4096 bit).

<#root>

```
device(config)#
```

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

Output di esempio quando viene richiesto di specificare le dimensioni del modulo:

<#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)
```

Passaggio 2: Genera una richiesta di firma del certificato (CSR)

Configurare un trust point sullo switch per il certificato di amministratore Web, specificando la registrazione tramite il terminale, disattivando il controllo delle revoche e fornendo informazioni di identificazione (nome soggetto, chiave e nomi alternativi soggetto).

<#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
```

Registrare il trust point per generare il CSR. È necessario specificare diverse opzioni; fornendo "sì" o "no" a seconda delle necessità. La richiesta di certificato deve essere visualizzata sul terminale.

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

Output di esempio:

<#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

Parametri disponibili per la configurazione del nome soggetto:

- C: Nazione, solo due lettere maiuscole (Stati Uniti)
- ST: Nome provincia
- L: Nome località (città)
- O: Nome organizzazione (società)
- Unità organizzativa: Nome unità organizzativa (reparto/sezione)
- CN: Nome comune (FQDN o indirizzo IP a cui accedere)

Passaggio 3: Invia CSR all'Autorità di certificazione (CA)

Copiare l'intera stringa CSR (incluse le righe BEGIN e END) e inviarla alla CA per la firma.

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

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

Se si utilizza una CA di Microsoft Windows Server, scaricare il certificato firmato in formato Base64. In genere si riceve il certificato del dispositivo firmato e, se possibile, un certificato della CA radice.

Passaggio 4: Autentica certificato CA radice Base64

Installare il certificato della CA (in formato Base64) sullo switch per stabilire l'attendibilità della CA che ha emesso il certificato del dispositivo.

<#root>

```
device(config)#
```

crypto pki authenticate webadmin-TP

Quando richiesto, incollare il certificato CA (incluse le righe BEGIN e END). Esempio:

<#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

Passaggio 5: Autentica certificato base64 dispositivo

Autentica il certificato firmato del dispositivo in base al certificato CA installato.

<#root>

```
device(config)#
```

crypto pki trustpoint webadmin-TP

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

chain-validation stop

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

crypto pki authenticate webadmin-TP

Quando richiesto, incollare il certificato del 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

Passaggio 6: Importazione del certificato firmato dal dispositivo sullo switch Catalyst 9000

Importare il certificato del dispositivo firmato Base64 nel trust point.

<#root>

```
device(config)#
```

crypto pki import webadmin-TP certificate

Incollare il certificato quando richiesto:

<#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

A questo punto, il certificato del dispositivo viene importato nello switch insieme a tutte le CA rilevanti e il certificato è pronto per l'uso, incluso l'accesso GUI (HTTPS).

Passaggio 7: Usa il nuovo certificato

Associare il trust point al server sicuro HTTP e abilitare l'accesso HTTPS sullo 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
```

Passaggio 8: Verifica dell'attendibilità del certificato da parte dei browser Web

- Il nome comune (CN) o il nome alternativo del soggetto (SAN) del certificato deve corrispondere all'URL a cui si accede dal browser.
- Il certificato deve rientrare nel suo periodo di validità.
- Il certificato deve essere rilasciato da una CA (o catena di CA) la cui radice è considerata attendibile dal browser. Lo switch deve fornire l'intera catena di certificati (ad eccezione della CA radice, che in genere è già presente nell'archivio del browser).
- Se il certificato contiene elenchi di revoche, verificare che il browser sia in grado di scaricarli e che il CN del certificato non sia elencato in alcun elenco di revoche.

Verifica

È possibile utilizzare questi comandi per verificare la configurazione del certificato e lo stato corrente:

Visualizzare i certificati installati e il relativo stato per un trust point:

<#root>

```
device#
show crypto pki certificate webadmin-TP
```

Output di esempio:

<#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

Verificare lo stato del server HTTPS e il trust point associato:

<#root>

device#

show ip http server secure status

Output di esempio:

<#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
```

Risoluzione dei problemi

Se si verificano problemi durante il processo di installazione del certificato, utilizzare questi comandi per abilitare il debug delle transazioni PKI. Ciò risulta particolarmente utile per diagnosticare gli errori durante l'importazione o la registrazione di certificati.

<#root>

```
device#

debug crypto pki transactions
```

Esempio di output del comando debug per uno scenario con esito positivo:

<#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:
```

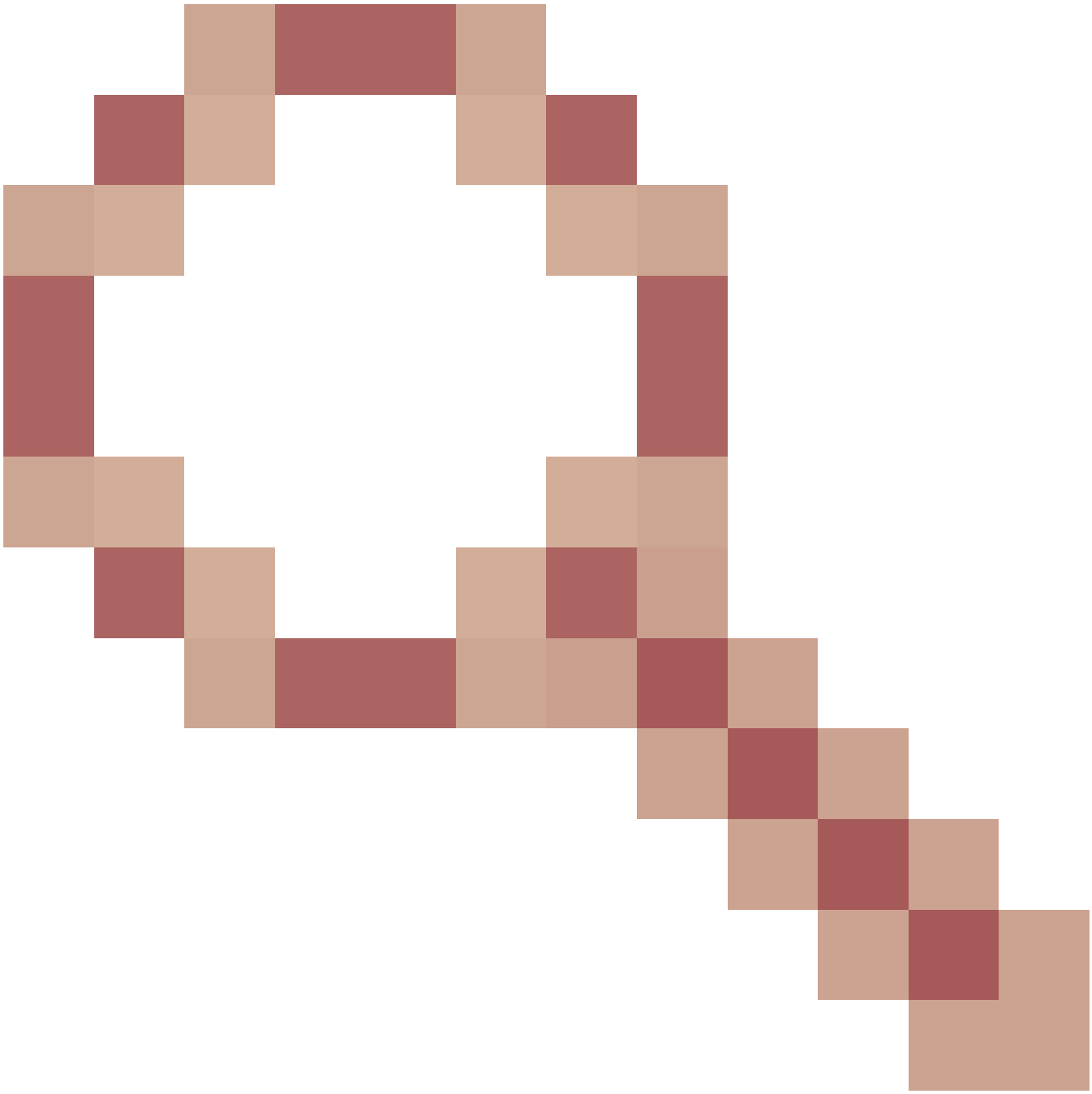
using private key csr-key for enrollment

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

make trustedCerts list for webadmin-TP

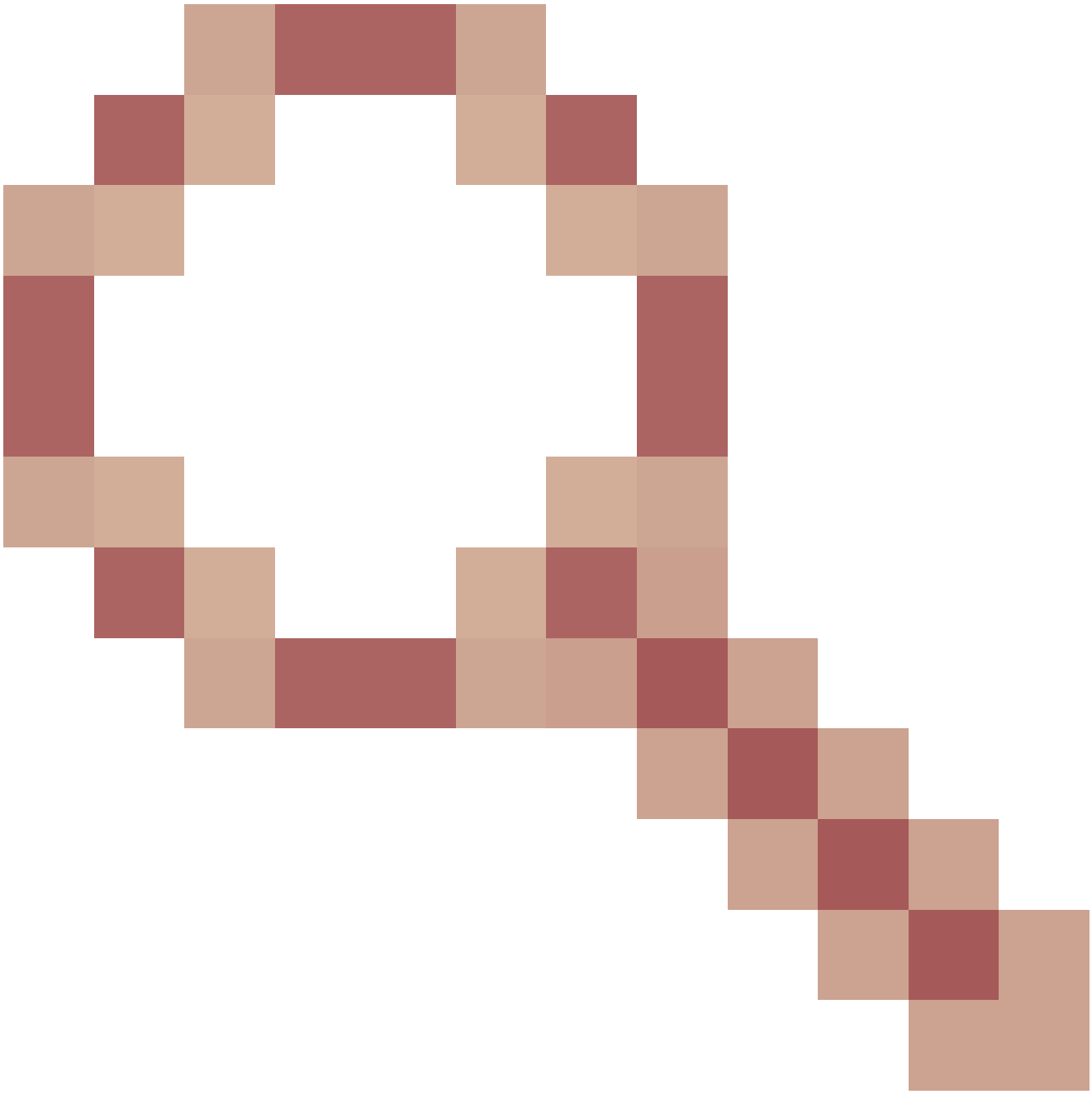
Note e limitazioni

- Cisco IOS® XE non supporta certificati CA con validità superiore a 2099 (ID bug Cisco CSCvp64208)



).

- Cisco IOS® XE non supporta i bundle PKCS 12 message digest SHA256 (sono supportati i certificati SHA256, ma non se il bundle PKCS12 è firmato con SHA256) (ID bug Cisco CSCvz41428)



). Questo problema è stato risolto nella versione 17.12.1.

Informazioni correlate

- Supporto tecnico Cisco e download

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).