在Catalyst 9000交換器上安裝Web管理憑證

目錄

簡介

本檔案介紹在Catalyst 9000系列交換器上產生、下載和安裝憑證的程式。

必要條件

需求

思科建議您瞭解以下主題：

- 如何設定Catalyst 9000系列交換器
- 如何使用Microsoft Windows Server對證書進行簽名
- 公開金鑰基礎架構(PKI)和數位憑證

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Catalyst 9300交換機，Cisco IOS® XE版本17.12.4
- Microsoft Windows Server 2022

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文提供逐步指南，說明如何產生憑證簽署請求(CSR)、讓憑證授權單位(CA)簽署，以及如何在Catalyst 9000交換器上安裝產生的憑證（連同CA憑證）。

目標是使用受信任的證書啟用交換機的安全Web(HTTPS)管理，確保與現代Web瀏覽器相容並符合組織安全策略。

設定

本節提供在Catalyst 9000交換器上產生、簽署及安裝Web管理員憑證的詳細工作流程。每個步驟都包含相關的CLI命令、說明和示例輸出。

步驟 1:定義金鑰

生成一個通用RSA金鑰對，並使用該金鑰對保護證書。金鑰必須是可匯出的，並且可以根據安全需求（1024至4096位）調整大小。

<#root>

```
device(config)#
```

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

當提示輸入模數大小時，輸出示例：

<#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)
```

步驟 2:生成證書簽名請求(CSR)

在交換機上為Web管理員證書配置信任點，通過終端指定註冊，禁用撤銷檢查，並提供標識資訊（主題名稱、金鑰和主題替代名稱）。

<#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

註冊信任點以生成CSR。必須提示您輸入各種選項；根據需要提供「是」或「否」。證書請求必須在終端上顯示。

device(config)#crypto pki enroll webadmin-TP

輸出示例：

<#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

可用於使用者名稱配置的引數：

- 思:國家/地區，僅兩個大寫字母(US)
- ST:省或州名稱
- L:位置名稱（城市）
- O:組織名稱（公司）
- OU:組織單位名稱（部門/科）
- CN:公用名（要訪問的FQDN或IP地址）

步驟 3:將CSR提交給憑證授權單位(CA)

複製完整的CSR字串（包括BEGIN和END行），並將其提交給CA進行簽名。

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

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

如果使用Microsoft Windows Server CA，請以Base64格式下載已簽名的證書。您通常會收到已簽名的裝置證書，可能還會收到根CA證書。

步驟 4:驗證根CA Base64證書

將CA的證書（Base64格式）安裝到交換機上，以在頒發裝置證書的CA中建立信任。

<#root>

```
device(config)#

crypto pki authenticate webadmin-TP
```

出現提示時，貼上CA憑證（包括BEGIN和END行）。範例：

<#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
```

步驟 5:驗證裝置Base64證書

根據已安裝的CA證書驗證裝置的簽名證書。

<#root>

```
device(config)#

crypto pki trustpoint webadmin-TP

device(ca-trustpoint)#

chain-validation stop

device(ca-trustpoint)#

crypto pki authenticate webadmin-TP
```

出現提示時，請貼上到裝置證書中：

<#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
```

步驟 6:在Catalyst 9000交換器上匯入裝置簽名的憑證

將Base64簽名的裝置證書匯入信任點。

<#root>

```
device(config)#

crypto pki import webadmin-TP certificate
```

出現提示時貼上證書：

<#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
```

這時，裝置憑證會與所有相關的CA一起匯入交換器，且憑證準備使用，包括GUI(HTTPS)存取許可權。

步驟 7:使用新證書

將信任點與HTTP安全伺服器關聯並在交換機上啟用HTTPS訪問。

<#root>

```
device(config)#

ip http secure-trustpoint webadmin-TP
```

<#root>

```
device(config)#

no ip http secure-server
```

<#root>

```
device(config)#

ip http secure-server
```

步驟 8:如何確保Web瀏覽器信任證書

- 證書的公用名(CN)或使用者替代名稱(SAN)必須與瀏覽器訪問的URL匹配。
- 證書必須在有效期限內。
- 憑證必須由瀏覽器信任其根的CA（或CA鏈結）核發。交換器必須提供完整的憑證鏈結（除了根CA，通常已在瀏覽器的儲存區中）。
- 如果憑證包含撤銷清單，請確保瀏覽器可以下載這些清單，並確保在任何撤銷清單中都沒有列出憑證的CN。

驗證

您可以使用以下命令驗證憑證組態和目前狀態：

檢視信任點的已安裝證書及其狀態：

<#root>

device#

show crypto pki certificate webadmin-TP

輸出示例：

<#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
```

驗證HTTPS伺服器狀態和關聯的信任點：

```
<#root>

device#

show ip http server secure status
```

輸出示例：

```
<#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
```

疑難排解

如果在證書安裝過程中遇到問題，請使用此命令啟用PKI事務的調試。這對於在證書匯入或註冊期間診斷故障尤其有用。

```
<#root>

device#

debug crypto pki transactions
```

成功的方案調試輸出示例：

<#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.

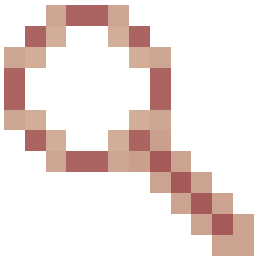
```
*Jun 12 05:20:32.097: CRYPTO_PKI: unlocked trustpoint webadmin-TP, refcount is 0
*Jun 12 05:21:50.789: CRYPTO_PKI:
```

using private key csr-key for enrollment

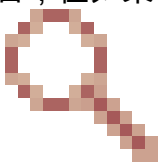
```
*Jun 12 05:22:12.947: CRYPTO_PKI:
```

make trustedCerts list for webadmin-TP

註釋和限制



- Cisco IOS® XE不支援有效期超過2099的CA證書(思科錯誤ID CSCvp64208)。
- Cisco IOS® XE不支援SHA256 message digest PKCS 12捆綁包（支援SHA256證書，但如果



PKCS12捆綁包本身使用SHA256進行簽名，則不支援）(思科錯誤ID CSCvz41428)。 此問題已在 17.12.1 中修正。

相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。