在Catalyst 9000交换机上安装Web管理员证书

目录

简介

本文档介绍在Catalyst 9000系列交换机上生成、下载和安装证书的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 如何配置Catalyst 9000系列交换机
- 如何使用Microsoft Windows Server签署证书
- 公钥基础设施(PKI)和数字证书

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Catalyst 9300交换机，Cisco IOS® XE版本17.12.4
- Microsoft Windows Server 2022

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档提供了生成证书签名请求(CSR)、获得证书颁发机构(CA)的签名并在Catalyst 9000交换机上安装生成的证书（以及CA证书）的分步指南。

目标是使用可信证书对交换机进行安全Web(HTTPS)管理，确保与现代Web浏览器兼容并符合组织安全策略。

配置

本节提供在Catalyst 9000交换机上生成、签名和安装Web管理员证书的详细工作流程。每个步骤都包括相关的CLI命令、说明和示例输出。

步骤 1：定义密钥

生成通用RSA密钥对并使用它保护证书。密钥必须可导出，并可根据安全需求确定大小（1024至4096位）。

```
<#root>

device(config)#

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

当提示输入模数大小时，输出示例：

```
<#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)
```

步骤 2：生成证书签名请求(CSR)

在交换机上为Web管理员证书配置信任点，通过终端指定注册，禁用撤销检查，并提供标识信息（主题名称、密钥和主题备用名称）。

<#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
```

注册信任点以生成CSR。必须提示您输入各种选项；根据需要提供“是”或“否”。证书请求必须显示在终端上。

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

示例输出：

<#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
```

可用于主题名称配置的参数：

- C：国家/地区，仅两个大写字母(US)
- ST:省或州名称
- L:位置名称（城市）
- O:组织名称（公司）
- OU:组织单位名称（部门/部门）
- CN:公用名称（要访问的FQDN或IP地址）

步骤 3：向证书颁发机构(CA)提交CSR

复制完整的CSR字符串（包括BEGIN和END行），并将其提交给CA进行签名。

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

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

如果使用Microsoft Windows Server CA，请下载Base64格式的签名证书。您通常会收到已签名的设备证书，可能还会收到根CA证书。

步骤 4：验证根CA Base64证书

在交换机上安装CA证书（Base64格式），以在颁发设备证书的CA中建立信任。

<#root>

```
device(config)#

crypto pki authenticate webadmin-TP
```

出现提示时，粘贴CA证书（包括BEGIN和END行）。示例：

<#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
```

步骤 5：验证设备Base64证书

根据已安装的CA证书对设备的签名证书进行身份验证。

<#root>

device(config)#

crypto pki trustpoint webadmin-TP

device(ca-trustpoint)#

chain-validation stop

device(ca-trustpoint)#

crypto pki authenticate webadmin-TP

出现提示时，粘贴设备证书：

<#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

步骤 6：在Catalyst 9000交换机上导入设备签名证书

将Base64签名的设备证书导入信任点。

<#root>

device(config)#

crypto pki import webadmin-TP certificate

出现提示时粘贴证书：

<#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
```

此时，设备证书将与所有相关CA一起导入到交换机，并且证书已准备就绪，可以使用，包括GUI(HTTPS)访问。

步骤 7：使用新证书

将信任点与HTTP安全服务器关联并在交换机上启用HTTPS访问。

<#root>

```
device(config)#

ip http secure-trustpoint webadmin-TP
```

<#root>

```
device(config)#

no ip http secure-server
```

<#root>

```
device(config)#

ip http secure-server
```

步骤 8::如何确保Web浏览器信任证书

- 证书的公用名(CN)或主题备用名(SAN)必须与浏览器访问的URL匹配。
- 证书必须在其有效期内。
- 证书必须由浏览器信任其根的CA（或CA链）颁发。交换机必须提供完整的证书链（根CA除外，它通常已存在于浏览器的存储中）。
- 如果证书包含撤销列表，请确保浏览器可以下载这些列表，并且证书的CN未在任何撤销列表中列出。

验证

您可以使用以下命令验证证书配置和当前状态：

查看信任点的已安装证书及其状态：

<#root>

device#

show crypto pki certificate webadmin-TP

示例输出：

<#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
```

验证HTTPS服务器状态和关联的信任点：

```
<#root>

device#

show ip http server secure status
```

示例输出：

```
<#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
```

故障排除

如果在证书安装过程中遇到问题，请使用此命令启用PKI事务的调试。这对于在证书导入或注册期间诊断故障尤其有用。

```
<#root>

device#

debug crypto pki transactions
```

成功的场景调试输出示例：

<#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.

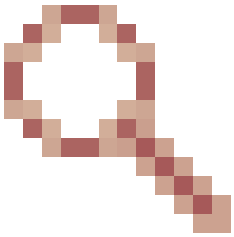
```
*Jun 12 05:20:32.097: CRYPTO_PKI: unlocked trustpoint webadmin-TP, refcount is 0
*Jun 12 05:21:50.789: CRYPTO_PKI:
```

using private key csr-key for enrollment

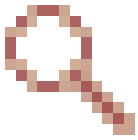
```
*Jun 12 05:22:12.947: CRYPTO_PKI:
```

make trustedCerts list for webadmin-TP

附注和限制



- Cisco IOS® XE不支持有效期超过2099的CA证书(Cisco bug ID CSCvp64208 影响。
- Cisco IOS® XE不支持SHA256消息摘要PKCS 12捆绑包（支持SHA256证书，但如果



PKCS12捆绑包本身使用SHA256进行签名，则不支持）(Cisco bug ID CSCvz41428 影响。 此漏洞已在 17.12.1 中修复。

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。