Instalación de certificados de administrador web en switches Catalyst 9000

Contenido

Introducción

Este documento describe el proceso para generar, descargar e instalar certificados en los switches Catalyst de la serie 9000.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cómo configurar los switches Catalyst serie 9000
- Cómo firmar certificados mediante Microsoft Windows Server
- Infraestructura de clave pública (PKI) y certificados digitales

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento proporciona una guía paso a paso para generar una Solicitud de firma de certificado (CSR), obtener la firma de una Autoridad de certificación (CA) e instalar el certificado resultante (junto con el certificado de CA) en un switch Catalyst 9000.

El objetivo es habilitar la administración web segura (HTTPS) del switch mediante un certificado de confianza, lo que garantiza la compatibilidad con los navegadores web modernos y el cumplimiento de las políticas de seguridad de la organización.

Configurar

Esta sección proporciona un flujo de trabajo detallado para generar, firmar e instalar un certificado de administración web en un switch Catalyst 9000. Cada paso incluye comandos CLI relevantes, explicaciones y resultados de ejemplo.

Paso 1: Definir una clave

Genere un par de claves RSA de uso general y utilícelo para proteger el certificado. La clave debe ser exportable y el tamaño puede ajustarse a las necesidades de seguridad (de 1024 a 4096 bits).

<#root>

```
device(config)#
```

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

Ejemplo de salida cuando se le solicita el tamaño del 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)
```

Paso 2: Generar una solicitud de firma de certificado (CSR)

Configure un punto de confianza en el switch para el certificado de administración web, especificando la inscripción a través del terminal, deshabilitando la comprobación de revocación y proporcionando información de identificación (nombre del sujeto, clave y nombres alternativos del sujeto).

<#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
```

Inscriba el punto de confianza para generar el CSR. Se le deben solicitar varias opciones; proporcionar "sí" o "no" según sea necesario. La solicitud de certificado debe mostrarse en el terminal.

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

Ejemplo de salida:

<#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
```

Parámetros disponibles para la configuración del nombre del sujeto:

- C: País, sólo dos letras mayúsculas (EE.UU.)
- ST: Nombre de estado o provincia
- L: Nombre de la ubicación (ciudad)
- O: Nombre de la organización (empresa)
- OU: Nombre de la unidad organizativa (departamento/sección)
- NC: Nombre común (FQDN o dirección IP a la que se va a acceder)

Paso 3: Envíe el CSR a la autoridad de certificación (CA)

Copie la cadena CSR completa (incluidas las líneas BEGIN y END) y envíela a la CA para su firma.

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

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

Si utiliza una CA de Microsoft Windows Server, descargue el certificado firmado en formato Base64. Por lo general, recibirá el certificado de dispositivo firmado y posiblemente un certificado de CA raíz.

Paso 4: Autenticar certificado raíz CA Base64

Instale el certificado de la CA (en formato Base64) en el switch para establecer la confianza en la CA que emitió el certificado del dispositivo.

<#root>

```
device(config)#

crypto pki authenticate webadmin-TP
```

Pegue el certificado de la CA (incluidas las líneas BEGIN y END) cuando se le solicite. Ejemplo:

<#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

Paso 5: Certificado Authenticate Device Base64

Autenticar el certificado firmado del dispositivo con el certificado de CA instalado.

<#root>

```
device(config)#
```

crypto pki trustpoint webadmin-TP

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

chain-validation stop

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

crypto pki authenticate webadmin-TP

Cuando se le solicite, pegue el certificado 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

Paso 6: Importar certificado firmado de dispositivo en el switch Catalyst 9000

Importe el certificado de dispositivo firmado Base64 en el punto de confianza.

<#root>

```
device(config)#
```

crypto pki import webadmin-TP certificate

Pegue el certificado cuando se le solicite:

<#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

En este momento, el certificado del dispositivo se importa al switch junto con todas las CA relevantes y el certificado está listo para utilizarse, incluido el acceso mediante GUI (HTTPS).

Paso 7: Utilizar el nuevo certificado

Asocie el punto de confianza al servidor HTTP seguro y habilite el acceso HTTPS en el 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
```

Paso 8: Cómo garantizar que los exploradores web confían en el certificado

- El nombre común (CN) del certificado o un nombre alternativo del sujeto (SAN) deben coincidir con la dirección URL a la que accede el explorador.
- El certificado debe estar dentro de su período de validez.
- El certificado debe ser emitido por una CA (o cadena de CA) cuya raíz sea de confianza para el explorador. El switch debe proporcionar la cadena de certificados completa (excepto la CA raíz, que normalmente ya está presente en el almacén del explorador).
- Si el certificado contiene listas de revocación, asegúrese de que el explorador puede descargarlas y de que el CN del certificado no aparece en ninguna lista de revocación.

Verificación

Puede utilizar estos comandos para verificar la configuración del certificado y el estado actual:

Ver los certificados instalados y su estado para un punto de confianza:

```
<#root>
device#
show crypto pki certificate webadmin-TP
```

Ejemplo de salida:

```
<#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 el estado del servidor HTTPS y el punto de confianza asociado:

<#root>

```
device#

show ip http server secure status
```

Ejemplo de salida:

<#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
```

Troubleshoot

Si encuentra problemas durante el proceso de instalación del certificado, utilice estos comandos para habilitar la depuración de las transacciones PKI. Esto es especialmente útil para diagnosticar errores durante la importación o inscripción de certificados.

<#root>

```
device#

debug crypto pki transactions
```

Ejemplo de resultado de depuración de escenario exitoso:

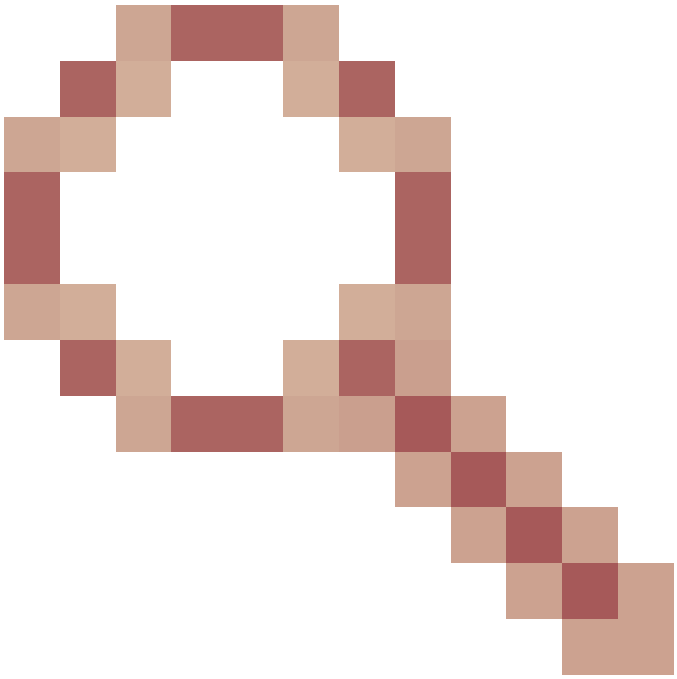
<#root>

```
*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 y limitaciones

- Cisco IOS® XE no admite certificados de CA con una validez superior a 2099 (Id. de error de Cisco CSCvp64208)
).
- Cisco IOS® XE no admite paquetes de mensajes de resumen SHA256 PKCS 12 (se admiten certificados SHA256, pero no si el paquete PKCS12 en sí está firmado con



SHA256) (Id. de error de Cisco CSCvz41428
). Esto se corrigió en 17.12.1.

Información Relacionada

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).