Installation des certificats d'administration Web sur les commutateurs Catalyst 9000

Table des matières

Introduction

Ce document décrit le processus de génération, de téléchargement et d'installation de certificats sur les commutateurs de la gamme Catalyst 9000.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration des commutateurs de la gamme Catalyst 9000
- Comment signer des certificats à l'aide de Microsoft Windows Server
- Infrastructure à clé publique (PKI) et certificats numériques

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Commutateur Cisco Catalyst 9300, Cisco IOS® XE version 17.12.4
- Microsoft Windows Server 2022

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Ce document fournit un guide étape par étape pour générer une demande de signature de certificat (CSR), la faire signer par une autorité de certification (CA) et installer le certificat résultant (avec le certificat CA) sur un commutateur Catalyst 9000.

L'objectif est d'activer l'administration Web sécurisée (HTTPS) du commutateur à l'aide d'un certificat approuvé, garantissant la compatibilité avec les navigateurs Web modernes et la conformité avec les stratégies de sécurité de l'entreprise.

Configurer

Cette section fournit un workflow détaillé pour la génération, la signature et l'installation d'un certificat d'administration Web sur un commutateur Catalyst 9000. Chaque étape comprend des commandes CLI pertinentes, des explications et des exemples de résultats.

Étape 1 : Définir une clé

Générez une paire de clés RSA à usage général et utilisez-la pour sécuriser le certificat. La clé doit être exportable et peut être dimensionnée en fonction des besoins de sécurité (1 024 à 4 096 bits).

<#root>

```
device(config)#
```

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

Exemple de résultat lorsque vous êtes invité à indiquer la taille du module :

<#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)
```

Étape 2 : Générer une demande de signature de certificat (CSR)

Configurez un point de confiance sur le commutateur pour le certificat d'administration Web, en spécifiant l'inscription via le terminal, en désactivant le contrôle de révocation et en fournissant des informations d'identification (nom du sujet, clé et autres noms du sujet).

<#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
```

Inscrivez le point de confiance pour générer le CSR. Vous devez être invité à saisir différentes options ; si nécessaire, indiquez « oui » ou « non ». La demande de certificat doit être affichée sur le terminal.

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

Exemple de rapport :

<#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

Paramètres disponibles pour la configuration du nom du sujet :

- C : Pays, deux lettres majuscules uniquement (États-Unis)
- ST : Nom du département ou de la province
- L : Nom du lieu (ville)
- O : Nom de l'organisation (société)
- OU : Nom de l'unité organisationnelle (département/section)
- CN : Nom commun (nom de domaine complet ou adresse IP à utiliser)

Étape 3 : Envoyer le CSR à l'autorité de certification (CA)

Copiez la chaîne CSR complète (y compris les lignes BEGIN et END) et soumettez-la à votre autorité de certification pour signature.

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

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

Si vous utilisez une autorité de certification Microsoft Windows Server, téléchargez le certificat signé au format Base64. Vous recevez généralement le certificat de périphérique signé et éventuellement un certificat d'autorité de certification racine.

Étape 4 : Authentifier le certificat racine CA Base64

Installez le certificat de l'autorité de certification (au format Base64) sur le commutateur pour établir la confiance dans l'autorité de certification qui a émis le certificat de votre périphérique.

<#root>

```
device(config)#
```

crypto pki authenticate webadmin-TP

Collez le certificat CA (y compris les lignes BEGIN et END) lorsque vous y êtes invité. Exemple :

<#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

Étape 5 : Authentifier le certificat Base64 du périphérique

Authentifiez le certificat signé du périphérique par rapport au certificat CA installé.

<#root>

```
device(config)#
```

crypto pki trustpoint webadmin-TP

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

chain-validation stop

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

crypto pki authenticate webadmin-TP

Lorsque vous y êtes invité, collez le certificat du périphérique :

<#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

Étape 6 : Importer le certificat signé par le périphérique sur le commutateur Catalyst 9000

Importez le certificat de périphérique signé Base64 dans le point de confiance.

<#root>

```
device(config)#
```

crypto pki import webadmin-TP certificate

Collez le certificat lorsque vous y êtes invité :

<#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

À ce stade, le certificat du périphérique est importé sur le commutateur avec toutes les autorités de certification pertinentes, et le certificat est prêt à être utilisé, y compris l'accès à l'interface utilisateur graphique (HTTPS).

Étape 7 : Utiliser le nouveau certificat

Associez le point de confiance au serveur sécurisé HTTP et activez l'accès HTTPS sur le commutateur.

<#root>

```
device(config)#
```

ip http secure-trustpoint webadmin-TP

<#root>

```
device(config)#
```

no ip http secure-server

<#root>

device(config)#

ip http secure-server

Étape 8 : Comment s'assurer que le certificat est approuvé par les navigateurs Web

- Le nom commun (CN) ou un autre nom de sujet (SAN) du certificat doit correspondre à l'URL à laquelle le navigateur accède.
- Le certificat doit être valable pendant sa période de validité.
- Le certificat doit être émis par une autorité de certification (ou chaîne d'autorités de certification) dont la racine est approuvée par le navigateur. Le commutateur doit fournir la chaîne de certificats complète (à l'exception de l'autorité de certification racine, qui est généralement déjà présente dans le magasin du navigateur).
- Si le certificat contient des listes de révocation, assurez-vous que le navigateur peut les télécharger et que le CN du certificat ne figure dans aucune liste de révocation.

Vérifier

Vous pouvez utiliser ces commandes pour vérifier la configuration du certificat et l'état actuel :

Affichez les certificats installés et leur état pour un point de confiance :

<#root>

device#

show crypto pki certificate webadmin-TP

Exemple de rapport :

<#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
```

Vérifiez l'état du serveur HTTPS et le point de confiance associé :

<#root>

```
device#
```

show ip http server secure status

Exemple de rapport :

<#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
```

Dépannage

Si vous rencontrez des problèmes lors du processus d'installation du certificat, utilisez ces commandes pour activer le débogage des transactions PKI. Cela est particulièrement utile pour diagnostiquer les échecs lors de l'importation ou de l'inscription de certificats.

<#root>

```
device#

debug crypto pki transactions
```

Exemple de résultat de débogage de scénario réussi :

<#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:
```

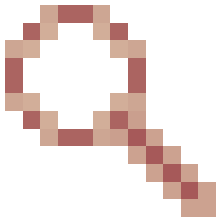
```
Added 1 certs to trusted chain.

*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
```

Remarques et limites

- Cisco IOS® XE ne prend pas en charge les certificats CA dont la validité dépasse 2099 (ID de bogue Cisco CSCvp64208)

.

- Cisco IOS® XE ne prend pas en charge les ensembles PKCS 12 de condensation de message SHA256 (les certificats SHA256 sont pris en charge, mais pas si l'ensemble



PKCS12 lui-même est signé avec SHA256) (ID de bogue Cisco CSCvz41428 . Ce problème est résolu dans la version 17.12.1.

Informations connexes

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.