Catalyst 9000 스위치에 웹 관리자 인증서 설치

목차

소개

이 문서에서는 Catalyst 9000 Series 스위치에 인증서를 생성, 다운로드 및 설치하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Catalyst 9000 Series 스위치 구성 방법
- Microsoft Windows Server를 사용하여 인증서를 서명하는 방법
- PKI(Public Key Infrastructure) 및 디지털 인증서

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 CSR(Certificate Signing Request)을 생성하고 CA(Certificate Authority)에서 서명을 받고 Catalyst 9000 스위치에 결과 인증서(CA 인증서와 함께)를 설치하는 방법에 대한 단계별 가이드를 제공합니다.

목표는 신뢰할 수 있는 인증서를 사용하여 스위치의 보안 웹(HTTPS) 관리를 활성화하여 최신 웹 브라우저와의 호환성 및 조직의 보안 정책 준수를 보장하는 것입니다.

구성

이 섹션에서는 Catalyst 9000 스위치에 웹 관리자 인증서를 생성, 서명 및 설치하기 위한 자세한 워크플로를 제공합니다. 각 단계에는 관련 CLI 명령, 설명 및 출력 예가 포함됩니다.

1단계: 키 정의

범용 RSA 키 쌍을 생성하여 인증서를 보호하는 데 사용합니다. 키는 내보낼 수 있어야 하며 보안 요구 사항(1024~4096비트)에 따라 크기를 조정할 수 있습니다.

```
<#root>

device(config)#

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

모듈러스 크기를 입력하라는 프롬프트가 표시될 때의 출력 예:

```
<#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)
```

2단계: CSR(Certificate Signing Request) 생성

터미널을 통한 등록을 지정하고, 폐기 검사를 비활성화하고, 식별 정보(주체 이름, 키 및 주체 대체 이름)를 제공하여 웹 관리자 인증서에 대한 스위치의 신뢰 지점을 구성합니다.

<#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
```

신뢰 지점을 등록하여 CSR을 생성합니다. 다양한 옵션을 입력하라는 메시지가 표시되어야 합니다. 필요에 따라 "예" 또는 "아니요"를 제공합니다. 인증서 요청이 터미널에 표시되어야 합니다.

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

출력 예:

<#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

주체 이름 구성에 사용할 수 있는 매개 변수:

- C: 국가, 대문자 2자만(US)
- ST: 시/도 이름
- L: 위치 이름(구/군/시)
- O: 조직 이름(회사)
- OU: 조직 단위 이름(부서/섹션)
- CN: 일반 이름(액세스할 FQDN 또는 IP 주소)

3단계: CSR을 CA(Certification Authority)에 제출

전체 CSR 문자열(BEGIN 및 END 줄 포함)을 복사하고 서명을 위해 CA에 제출합니다.

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

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

Microsoft Windows Server CA를 사용하는 경우 서명된 인증서를 Base64 형식으로 다운로드합니다. 일반적으로 서명된 디바이스 인증서를 받으며, 루트 CA 인증서일 수도 있습니다.

4단계: 루트 CA Base64 인증서 인증

스위치에 CA 인증서(Base64 형식)를 설치하여 디바이스 인증서를 발급한 CA에 신뢰를 설정합니다.

<#root>

```
device(config)#

crypto pki authenticate webadmin-TP
```

프롬프트가 표시되면 CA 인증서(BEGIN 및 END 행 포함)를 붙여넣습니다. 예:

<#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

5단계: 디바이스 Base64 인증서 인증

설치된 CA 인증서에 대해 디바이스의 서명된 인증서를 인증합니다.

<#root>

```
device(config)#
```

crypto pki trustpoint webadmin-TP

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

chain-validation stop

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

crypto pki authenticate webadmin-TP

프롬프트가 표시되면 디바이스 인증서에 붙여넣습니다.

<#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

6단계: Catalyst 9000 스위치에서 디바이스 서명 인증서 가져오기

Base64 서명 디바이스 인증서를 신뢰 지점으로 가져옵니다.

<#root>

```
device(config)#
```

crypto pki import webadmin-TP certificate

프롬프트가 표시되면 인증서를 붙여넣습니다.

<#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
```

이때 디바이스 인증서가 모든 관련 CA와 함께 스위치로 가져오며, GUI(HTTPS) 액세스를 포함하여 인증서를 사용할 준비가 된 것입니다.

7단계: 새 인증서 사용

신뢰 지점을 HTTP 보안 서버와 연결하고 스위치에서 HTTPS 액세스를 활성화합니다.

<#root>

```
device(config)#

ip http secure-trustpoint webadmin-TP
```

<#root>

```
device(config)#

no ip http secure-server
```

<#root>

```
device(config)#

ip http secure-server
```

8단계: 웹 브라우저에서 인증서를 신뢰할 수 있는지 확인하는 방법

- 인증서의 CN(Common Name) 또는 SAN(Subject Alternative Name)은 브라우저에서 액세스하는 URL과 일치해야 합니다.
- 인증서는 유효 기간 내에 있어야 합니다.
- 인증서는 브라우저에서 루트를 신뢰하는 CA(또는 CA 체인)에서 발급해야 합니다. 스위치는

전체 인증서 체인을 제공해야 합니다(일반적으로 브라우저의 저장소에 이미 있는 루트 CA 제외).
- 인증서에 해지 목록이 포함되어 있는 경우 브라우저에서 이를 다운로드할 수 있으며 인증서의 CN이 해지 목록에 나열되어 있지 않은지 확인합니다.

다음을 확인합니다.

다음 명령을 사용하여 인증서 컨피그레이션 및 현재 상태를 확인할 수 있습니다.

신뢰 지점에 대해 설치된 인증서 및 해당 상태를 확인합니다.

<#root>

device#

show crypto pki certificate webadmin-TP

출력 예:

<#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
```

HTTPS 서버 상태 및 관련 신뢰 지점을 확인합니다.

<#root>

```
device#
```

show ip http server secure status

출력 예:

<#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
```

문제 해결

인증서 설치 프로세스 중에 문제가 발생하면 이 명령을 사용하여 PKI 트랜잭션의 디버깅을 활성화합니다. 이는 인증서 가져오기 또는 등록 중에 실패를 진단하는 데 특히 유용합니다.

<#root>

device#

debug crypto pki transactions

성공적인 시나리오 디버그 출력의 예:

<#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

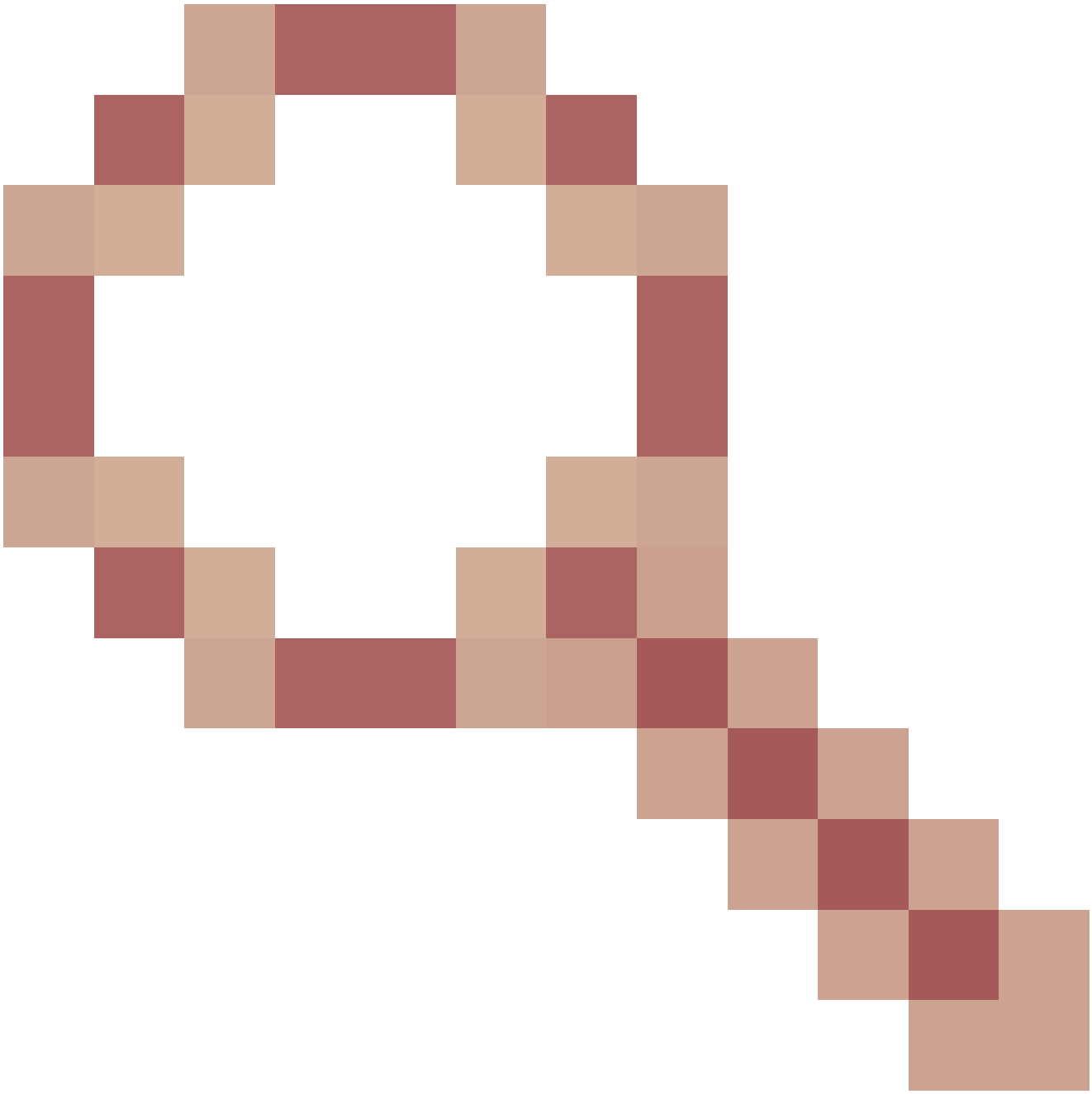
```
*Jun 12 05:20:25.735: CRYPTO_PKI: crypto_pki_authenticate_tp_cert()
*Jun 12 05:20:25.735: CRYPTO_PKI: trustpoint webadmin-TP authentication status = 0
*Jun 12 05:20:32.094: PKI: Cert key-usage: Digital-Signature , Certificate-Signing , CRL-Signing
*Jun 12 05:20:32.096: CRYPTO_PKI:
```

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
```

참고 및 제한 사항

- Cisco IOS® XE는 2099년 이후의 CA 인증서를 지원하지 않습니다(Cisco 버그 ID CSCvp64208).
- Cisco IOS® XE는 SHA256 메시지 다이제스트 PKCS 12 번들을 지원하지 않습니다(SHA256 인증서가 지원되지만 PKCS12 번들 자체가 SHA256으로 서명된 경우에는 지원되지 않음)(Cisco 버그 ID CSCvz41428



). 이는 17.12.1에서 수정됩니다.

관련 정보

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.