CMX 10.6에서 타사 인증서 및 설치를 위한 CSR 생성 컨피그레이션 예

목차

소개

이 문서에서는 서드파티 인증서를 얻기 위해 CSR(Certificate Signing Request)을 생성하는 방법과 CMX(Cisco Connected Mobile Experiences)에 체인으로 연결된 인증서를 다운로드하는 방법에 대해 설명합니다.

기고자: Cisco TAC 엔지니어, Andres Silva 및 Ram Krishnmodohy.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Linux에 대한 기본 지식
- PKI(Public Key Infrastructure)
- 디지털 인증서
- CMX

사용되는 구성 요소

이 문서의 정보는 CMX 버전 10.6.1-47을 기반으로 합니다.

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

구성

참고:인증서 작업 시 CMX 10.6.2-57 이상을 사용하십시오.

구성

CSR 생성

1단계. SSH를 사용하여 CMX의 CLI(Command Line Interface)에 액세스하고 다음 명령을 실행하여 CSR을 생성하고 요청된 정보를 완료합니다.

```
[cmxadmin@cmx-andressi]$ cmxctl config certs createcsr
Keytype is RSA, so generating RSA key with length 4096
Generating RSA private key, 4096 bit long modulus
.............
...
e is 65537 (0x10001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:MX
State or Province Name (full name) [Some-State]:Tlaxcala
Locality Name (eg, city) []:Tlaxcala
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:cmx-andressi
Email Address []:cmx@cisco.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Cisco123
An optional company name []:Cisco
The CSR is stored in : /opt/cmx/srv/certs/cmxservercsr.pem
The Private key is stored in: /opt/cmx/srv/certs/cmxserverkey.pem
```

개인 키 및 CSR은 **/opt/cmx/srv/certs/**

> **참고:**CMX 10.6.1을 사용하는 경우 SAN 필드가 CSR에 자동으로 추가됩니다.SAN 필드 때문에 서드파티 CA가 CSR에 서명할 수 없는 경우 CMX의 openssl.conf 파일에서 SAN 문자열을 제거합니다.자세한 내용은 버그 CSCvp39346을 참조하십시오.

2단계. 서드파티 인증 기관에서 서명한 CSR을 가져옵니다.

CMX에서 인증서를 가져와 서드파티에 보내려면 **cat** 명령을 실행하여 CSR을 엽니다.출력을 복사하여 .txt 파일에 붙여넣거나 서드파티 요구 사항에 따라 확장자를 변경할 수 있습니다.

```
[cmxadmin@cmx-andressi]$ cat /opt/cmx/srv/certs/cmxservercsr.pem
```

서명된 인증서 및 CA(Certificate Authority) 인증서를 CMX로 가져오기

> **참고:**CMX에 인증서를 가져오고 설치하려면 버그 CSCvr27467로 인해 CMX 10.6.1 및 10.6.2에 루트 패치를 설치해야 합니다.

1단계. 서명된 인증서와 개인 키를 **.pem** 파일로 번들합니다.다음과 같이 복사하여 붙여넣습니다.

```
-----BEGIN RSA PRIVATE KEY----- < Private Key
MIIEpAIBAAKCAQEA2gXgEo7ouyBfWwCktcYo8ABwFw3d0yG5rvZRHvS2b3FwFRw5
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE----- <  Signed certificate
MIIFEzCCAvugAwIBAgIBFzANBgkqhkiG9w0BAQsFADCBlDELMAkGA1UEBhMCVVMx
```

2단계. 중간 및 루트 CA 인증서를 **.crt** 파일로 번들합니다.다음과 같이 복사하여 붙여넣습니다.

```
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < Intermediate CA certificates
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < The root CA certificate
MIIGqjCCBJKgAwIBAgIJAPj9p1QMdTgoMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYD
...
-----END CERTIFICATE-----
```

3단계. 위의 1단계와 2단계에서 CMX로 두 파일을 모두 전송합니다.

4단계. 다음 명령을 실행하여 CMX의 CLI를 루트로 액세스하고 현재 인증서를 지웁니다.

```
[cmxadmin@cmx-andressi]$ cmxctl config certs clear
```

5단계. cmxctl config certs importcacert 명령**을 실행하여** CA 인증서를 가져옵니다.비밀번호를 입력하고 다른 모든 비밀번호 프롬프트에 대해 반복합니다.

```
[cmxadmin@cmx-andressi]# cmxctl config certs importcacert ca.crt
Importing CA certificate.....

Enter Export Password:
Verifying - Enter Export Password:
Enter Import Password:

No CRL URI found. Skipping CRL download.
Import CA Certificate successful
```

6단계. 서버 인증서 및 개인 키(단일 파일로 결합)를 가져오려면 cmxctl config certs importservercert 명령**을** 실행합니다.비밀번호를 선택하고 모든 비밀번호 프롬프트에 대해 반복합니다.

```
[cmxadmin@cmx-andressi]# cmxctl config certs importservercert key-cert.pem

Importing Server certificate.....
Successfully transferred the file
```

```
Enter Export Password: password
Verifying - Enter Export Password: password
Enter Import Password: password
Private key present in the file: /home/cmxadmin/key-cert.pem
Enter Import Password: password

No CRL URI found. Skipping CRL download.
Validation of server certificate is successful
Import Server Certificate successful
Restart CMX services for the changes to take effect.
Server certificate imported successfully.

To apply these certificate changes, CMX Services will be restarted now.
Please press Enter to continue.
```

7단계. **Enter**를 눌러 Cisco CMX 서비스를 다시 시작합니다.

고가용성에 인증서 설치

- 인증서는 기본 서버와 보조 서버 모두에 별도로 설치해야 합니다.
- 서버가 이미 페어링된 경우 인증서 설치를 진행하기 전에 먼저 HA를 비활성화해야 합니다.
- 기본 인증서의 기존 인증서를 지우려면 CLI에서 "cmxctl config certs clear" 명령을 사용합니다
- 기본 및 보조 모두에 설치할 인증서는 동일한 인증 기관에서 가져와야 합니다.
- 인증서 설치 후 CMX 서비스를 다시 시작한 다음 HA에 대해 페어링해야 합니다.

다음을 확인합니다.

인증서가 올바르게 설치되었는지 확인하려면 CMX의 웹 인터페이스를 열고 사용 중인 인증서를 검토하십시오.

문제 해결

SAN 확인 때문에 CMX에서 서버 인증서를 가져오지 못할 경우 다음과 같은 내용이 기록됩니다.

```
Importing Server certificate.....

CRL successfully downloaded from http://
This is new CRL. Adding to the CRL collection.
ERROR:Check for subjectAltName(SAN) failed for Server Certificate
ERROR: Validation is unsuccessful (err code = 3)
ERROR: Import Server Certificate unsuccessful
```

SAN 필드가 필요하지 않으면 CMX에서 SAN 확인을 비활성화할 수 있습니다.이렇게 하려면 버그 CSCvp39346의 절차를 참조하십시오