Een CSR voor certificaat en installatie van derden genereren op CMX 10.6 Configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u een certificaataanvraag (CSR) kunt genereren om een certificaat van derden te verkrijgen en hoe u een gekoppeld certificaat aan Cisco Connected Mobile Experiences (CMX) kunt downloaden.

Bijgedragen door Andres Silva en Ram Krishnamoorthy, Cisco TAC-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van Linux
- PKI-infrastructuur
- Digitale certificaten
- CMX

Gebruikte componenten

De informatie in dit document is gebaseerd op CMX versie 10.6.1-47

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de

mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Opmerking: Gebruik CMX 10.6.2-57 of hoger tijdens het werken met certificaten.

Configuraties

CSR genereren

Stap 1. Open de CMX-interface (CLI) van de opdrachtregel met behulp van SSH. Start de volgende opdracht om een CSR te genereren en bevestig de gevraagde informatie:

```
[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
```

De privétoets en de CSR worden opgeslagen in **/opt/cmx/srv/certs/**

> Opmerking: als u CMX 10.6.1 gebruikt, wordt het SAN-bestand automatisch aan de CSR toegevoegd. Als CA van derden niet in staat is om CSR te tekenen vanwege het SAN-veld, verwijdert u de SAN-string uit het openssl**.conf-**bestand in CMX. Raadpleeg CSCvp39346 voor meer informatie.

Stap 2. Ontvang de CSR door een certificeringsinstantie van derden.

Om het certificaat van CMX te krijgen en het naar de derde partij te verzenden, **voert** u de kat opdracht uit om de CSR te openen. U kunt de uitvoer naar een .txt-bestand kopiëren en plakken of de extensie wijzigen op basis van de vereisten van de derde.

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

Certificaten van certificeringsinstanties (CA) importeren naar CMX

> Opmerking: Om de certificaten op CMX te kunnen importeren en installeren is de installatie van root patch vereist op CMX 10.6.1 en 10.6.2 vanwege bug CSCvr27467.

Stap 1. Bundel particuliere sleutel met het ondertekende certificaat in een **.pem-**bestand. Kopieer en plak ze als volgt:

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

Stap 2. Bundel de CA-certificaten van middelgroot en wortel in een bestand crt. Kopieer en plak ze als volgt:

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

Stap 3. Breng beide bestanden van Stap 1 en 2 naar CMX over.

Stap 4. Toegang tot de CLI van CMX als root en maak de huidige certificaten vrij door de volgende opdracht uit te voeren:

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

Stap 5. Start de **cmxctl-configuratiesector certs belangrijke** opdracht om CA-certificaat te importeren. Voer een wachtwoord in en herhaal het voor alle andere wachtwoordaanwijzingen.

```
[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
```

Stap 6. Om servercertificaat en privé sleutel te importeren (gecombineerd in één bestand), voer het **cmxctl-configuratie certs importserver cert** opdracht uit. Selecteer een wachtwoord en herhaal het voor alle wachtwoordaanwijzingen.

```
[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.
```

Stap 7. Druk op **Voer** de Cisco CMX-services opnieuw in.

Certificaten installeren in hoge beschikbaarheid

- Certificaten moeten afzonderlijk op zowel de primaire als de secundaire servers worden geïnstalleerd.
- Als de servers al zijn gekoppeld, moet HA eerst worden uitgeschakeld voordat u doorgaat met het installeren van het certificaat.
- Om enige bestaande certificaten op het primaire te ontruimen, gebruik "cmxctl de beslist' van de beslist van de decor van de CLI
- Certificaten die zowel op de primaire als de secundaire dienst moeten worden geïnstalleerd, moeten van dezelfde certificeringsinstantie afkomstig zijn.
- Na de installatie van de certificaten moeten de CMX-diensten opnieuw worden gestart en daarna worden afgebouwd voor HA.

Verifiëren

Om te bevestigen dat het certificaat correct is geïnstalleerd, opent u de web interface van CMX en controleert u het in gebruik zijnde certificaat.

Problemen oplossen

Indien CMX het servercertificaat niet importeert vanwege de SAN-verificatie, is zoiets als dit geregistreerd:

```
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
```

Als het SAN-veld niet vereist is, kunt u de SAN-verificatie via CMX uitschakelen. Raadpleeg de procedure voor bug CSCvp39346