Générer un CSR pour un certificat et une installation tiers sur CMX

Contenu

Introduction

Ce document décrit comment générer une demande de signature de certificat (CSR) afin d'obtenir un certificat tiers et comment télécharger un certificat chaîné vers Cisco Connected Mobile Experiences (CMX).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de Linux
- Infrastructure à clé publique (PKI)
- Certificats numériques

Components Used

Les informations de ce document sont basées sur la version 10.3 de CMX

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.

Configuration

Générer le CSR

Étape 1. Connectez-vous à la CLI de CMX, accédez en tant que root, accédez au répertoire de certificats et créez un dossier pour le CSR et le fichier de clé.

```
[cmxadmin@cmx]$ su -
```

```
Password:
[root@cmx]# cd /opt/haproxy/ssl/
[root@cmx]# mkdir newcert
[root@cmx]# cd newcert
```

Note: Le répertoire par défaut des certificats sur CMX est /opt/haproxy/ssl/.

Étape 2. Générez le fichier CSR et la clé.

```
[root@cmx newcert]# openssl req -nodes -days 365 -newkey rsa:2048 -keyout
/opt/haproxy/ssl/newcert/private.key -out /opt/haproxy/ssl/newcert/cert.crt
Generating a 2048 bit RSA private key
........+++
......................+++
writing new private key to '/opt/haproxy/ssl/newcert/private.key'
-----
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) [XX]:MX
State or Province Name (full name) []:Tlaxcala
Locality Name (eg, city) [Default City]:Tlaxcala
Organization Name (eg, company) [Default Company Ltd]:Cisco
Organizational Unit Name (eg, section) []:TAC
Common Name (eg, your name or your server's hostname) []:cmx.example.com
Email Address []:cmx@example.com
```

Étape 3. Obtenez la signature du CSR par le tiers.

Afin d'obtenir le certificat de CMX et de l'envoyer à un tiers, exécutez la commande **cat** pour ouvrir le CSR. Vous pouvez copier et coller la sortie dans un fichier .txt ou modifier l'extension en fonction des exigences du tiers. Voici un exemple.

```
[root@cmx newcert]# cat cert.crt
-----BEGIN CERTIFICATE REQUEST-----
MIIC0TCCAbkCAQAwgYsxCzAJBgNVBAYTAk1YMREwDwYDVQQIDAhUbGF4Y2FsYTER
MA8GA1UEBwwIVGxheGNhbGExDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANUQUMx
GDAWBgNVBAMMD2NteC5leGFtcGxlLmNvbTEeMBwGCSqGSIb3DQEJARYPY214QGV4
YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2YybDkDR
vRSwD19EVaJehsNjG9Cyo3vQPOPcAAdgjFBpUHMt8QNgn6YFdHYZdpKaRTJXhztm
fa/7Nevb1IP/pSBgYRxHXQEhl9Gj4DT0gT2T+AZ8j3J9KMSe8Bakj4qY8Ua7GCdC
A62NzVcDxDM83gUD92oGbxOF9VFE2hiRvCQc+d6gBRuTOXxtyLBAtcL3hkiOEQx7
sDA55CwZU7ysMdWHUBn4AglzI1gPyzlmT3dwR0gfOSYN4j5+H0nrYtrPBZSUbZaa
8pGXVu7sFtV8bahgtnYiCUtiz9J+k5V9DBjqpSzYzb3+KxeAA+g0iV3J1VzsLNt7
mVocT9oPaOEI8wIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAI6Q/A4zTfrWP2uS
xtN8X6p6aP8guU0bTWhGEMBEgBQd0bBWYdhxaItGt1a1tdNcIGLACeMPuk7WpsiH
rUs5kiIjlAc2/ANBao6/nlv56vhGUx0dOq0fk/glbrKL+a8Lx9ixtee77aPZ1xVD
A/n3FdNdSIidWH0M4q8JunxbT33vM9h8H6oqe/JI3BDnw4tRnkYaGWJsyWUlPCuO
TWPMagMkntv0JaEOHLg4/JZyVSdDiTnmb/U8cEH2RrcUP8iwjykDpb/V4tb4VtgM
7+9HKxQRQHq5Qji8/QyMG6ctoD+B7k6UpzXvi5FpvqGQWwXJNC52suAt0QeeZj1J
rpudLUs=
-----END CERTIFICATE REQUEST-----
[root@cmx newcert]#
```

Étape 4. Créez la chaîne de certificats à importer dans CMX.

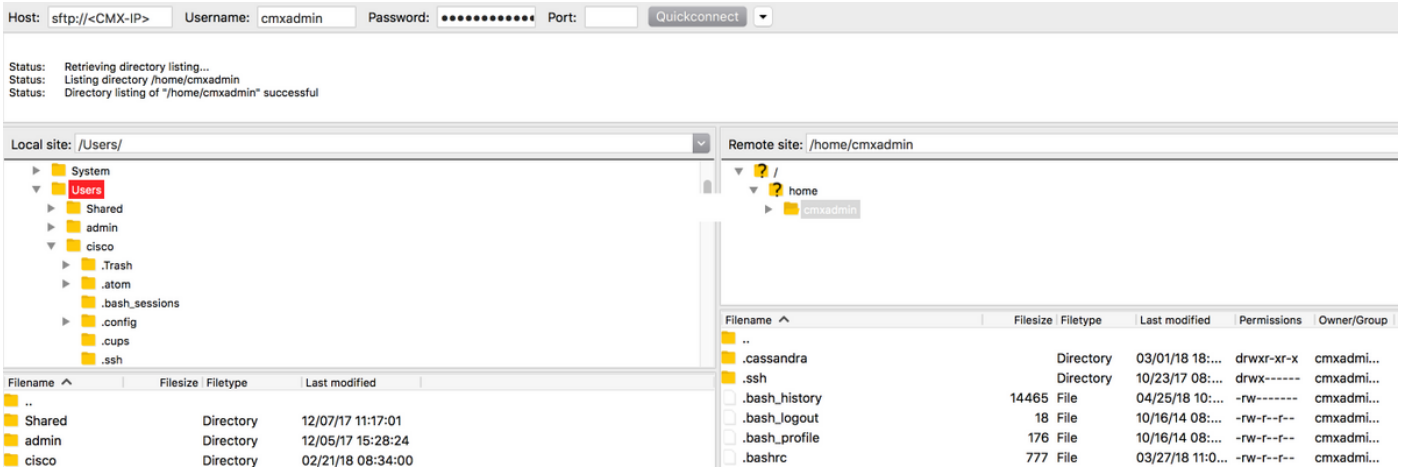
Afin de créer le certificat final, copiez et collez le certificat signé dans un fichier .txt avec la clé privée, le certificat intermédiaire et le certificat racine. Assurez-vous de l'enregistrer en tant que fichier **.pem**.

Cet exemple montre le format du certificat final.

```
-----BEGIN RSA PRIVATE KEY----- < Your Private Key
MIIEpAIBAAKCAQEA2gXgEo7ouyBfWwCktcYo8ABwFw3d0yG5rvZRHvS2b3FwFRw5
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE----- < Your CMX server signed certificate
MIIFEzCCAvugAwIBAgIBFzANBgkqhkiG9w0BAQsFADCBlDELMAkGA1UEBhMCVVMx
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < Your intermediate CA certificates
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < The root CA certificate that signed your certificate
MIIGqjCCBJKgAwIBAgIJAPj9p1QMdTgoMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYD
...
-----END CERTIFICATE-----
```

Étape 5. Transférez le certificat final dans CMX.

Afin de transférer le certificat final vers CMX à partir de votre ordinateur, ouvrez votre application SFTP et connectez-vous à CMX avec les informations d'identification de l'administrateur. Vous devez être en mesure d'afficher les dossiers de CMX comme indiqué dans l'image.



Ensuite, faites glisser et déposez le certificat chaîné dans le dossier /home/cmxadmin/.

> **Note**: Le répertoire par défaut lorsque vous ouvrez une connexion SFTP à CMX est /home/cmxadmin/.

Étape 6. Modifiez l'autorisation du certificat final et du propriétaire. Ensuite, déplacez-le vers le dossier qui contient la clé privée. Voici un exemple.

```
[root@cmx ~]# cd /home/cmxadmin/
[root@cmx cmxadmin]# chmod 775 final.pem
[root@cmx cmxadmin]# chown cmx:cmx final.pem
[root@cmx cmxadmin]# mv final.pem /opt/haproxy/ssl/newcert/
[root@cmx cmxadmin]# cd /opt/haproxy/ssl/newcert/
```

```
[root@cmx newcert]# ls -la
total 16
drwxr-xr-x 2 root root 4096 Apr 25 12:30 .
drwxr-xr-x 4 cmx  cmx  4096 Apr 25 09:25 ..
-rw-r--r-- 1 root root 1054 Apr 25 11:01 cert.crt
-rwxrwxr-x 1 cmx  cmx     0 Apr 25 12:29 final.pem
-rw-r--r-- 1 root root 1708 Apr 25 11:01 private.key
[root@cmx newcert]#
```

Étape 7. Assurez-vous que tout est correctement construit.

```
[root@cmx newcert]#openssl verify -CAfile /opt/haproxy/ssl/newcert/final.pem
/opt/haproxy/ssl/newcert/final.pem
/opt/haproxy/ssl/newcert/final.pem: OK
```

Vous devez obtenir un message OK.

Étape 8. Installez le certificat final et redémarrez CMX.

```
[root@cmx newcert]#cmxctl node sslmode enable --pem /opt/haproxy/ssl/newcert/final.pem
enabling ssl
ssl enabled

[root@cmx newcert]#reboot
```

Étape 9 (Facultatif) Si vous exécutez CMX 10.3.1 ou version ultérieure, vous pouvez être affecté par ce bogue :

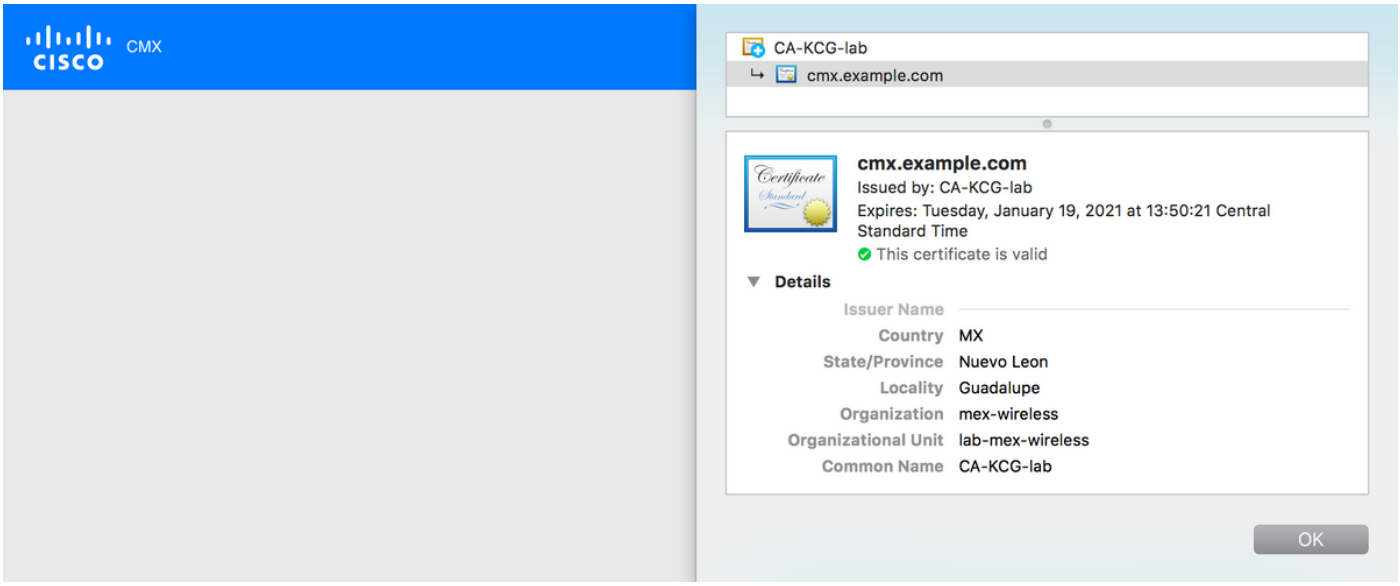
- CSCvh21464 :: CMX WEBUI n'utilise pas le certificat auto-signé ou tiers installé

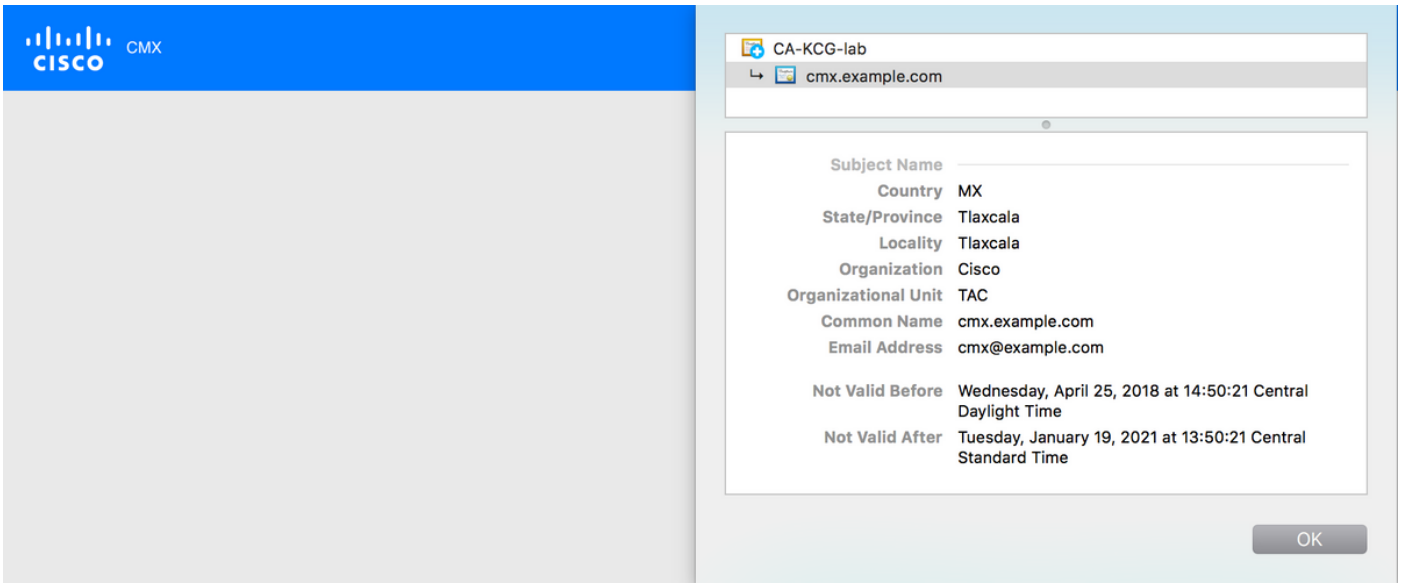
Ce bogue empêche CMX de mettre à jour le chemin du certificat. La solution de contournement pour résoudre ce problème consiste à créer deux liens logiciels pour pointer vers le nouveau certificat et la nouvelle clé privée, et recharger CMX. Voici un exemple :

```
[root@cmx ~]# cd /opt/haproxy/ssl/
[root@cmx ssl]# mkdir backup
[root@cmx ssl]# mv host.pem backup/
[root@cmx ssl]# mv host.key backup/
[root@cmx ssl]# ln -s /opt/haproxy/ssl/newcert/final.pem host.pem
[root@cmx ssl]# ln -s /opt/haproxy/ssl/newcert/private.key host.key
[root@cmx ssl]#
[root@cmx ssl]# ls -la
total 16
drwxr-xr-x 4 cmx  cmx  4096 Apr 25 12:59 .
drwxr-xr-x 6 cmx  cmx  4096 Mar 31  2017 ..
lrwxrwxrwx 1 root root   36 Mar 26 09:58 host.key -> /opt/haproxy/ssl/newcert/private.key
lrwxrwxrwx 1 root root   38 Mar 26 09:58 host.pem -> /opt/haproxy/ssl/newcert/final.pem
drwxr-xr-x 2 root root 4096 Apr 25 12:30 newcert
[root@cmx ssl]#
[root@cmx ssl]# reboot
```

Vérification

Ouvrez l'interface utilisateur graphique de CMX, dans ce cas Google Chrome est utilisé. Ouvrez le certificat en cliquant sur l'onglet **Secure** qui se trouve en regard de l'URL et vérifiez les détails comme indiqué dans l'image.


CMX
CA-KCG-lab
cmx.example.com
cmx.example.com
Issued by: CA-KCG-lab
Expires: Tuesday, January 19, 2021 at 13:50:21 Central Standard Time
This certificate is valid
Details
Issuer Name
Country MX
State/Province Nuevo Leon
Locality Guadalupe
Organization mex-wireless
Organizational Unit lab-mex-wireless
Common Name CA-KCG-lab
OK


CMX
CA-KCG-lab
cmx.example.com
Subject Name
Country MX
State/Province Tlaxcala
Locality Tlaxcala
Organization Cisco
Organizational Unit TAC
Common Name cmx.example.com
Email Address cmx@example.com
Not Valid Before Wednesday, April 25, 2018 at 14:50:21 Central Daylight Time
Not Valid After Tuesday, January 19, 2021 at 13:50:21 Central Standard Time
OK