Exemple de configuration de génération d'un CSR pour un certificat et une installation tiers sur CMX 10.6

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).

Contribué par Andres Silva et Ram Krishnamoorthy, ingénieurs du TAC Cisco.

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
- CMX

Components Used

Les informations de ce document sont basées sur la version 10.6.1-47 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

Note: Veuillez utiliser CMX 10.6.2-57 ou version ultérieure lors de l'utilisation de certificats.

Configurations

Générer CSR

Étape 1. Accédez à l'interface de ligne de commande (CLI) de CMX à l'aide de SSH, exécutez la commande suivante pour générer un CSR et complétez les informations demandées :

```
[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
```

La clé privée et la CSR sont stockées dans **/opt/cmx/srv/certs/**

> **Note**: si vous utilisez CMX 10.6.1, le champ SAN est automatiquement ajouté au CSR. Si une autorité de certification tierce n'est pas en mesure de signer le CSR en raison du champ SAN, supprimez la chaîne SAN du fichier openssl**.conf** sur CMX. Référez-vous au bogue CSCvp39346 pour plus d'informations.

Étape 2. Obtenez la signature du CSR par une autorité de certification tierce.

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.

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

Importer des certificats de certificat et d'autorité de certification signés vers CMX

> **Note**: Afin d'importer et d'installer les certificats sur CMX, l'installation du patch racine est requise sur CMX 10.6.1 et 10.6.2 en raison du bogue CSCvr27467.

Étape 1. Associez la clé privée avec le certificat signé dans un fichier **.pem**. Copiez-les et collez-les comme suit :

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

Étape 2. Associez les certificats de l'autorité de certification intermédiaire et racine dans un fichier **.crt**. Copiez-les et collez-les comme suit :

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

Étape 3. Transférez les deux fichiers des étapes 1 et 2 ci-dessus vers CMX.

Étape 4. Accédez à la CLI de CMX en tant que racine et effacez les certificats actuels en exécutant la commande suivante :

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

Étape 5. Exécutez la commande **cmxctl config certs importcacert** pour importer le certificat CA. Saisissez un mot de passe et répétez-le pour toutes les autres invites de mot de passe.

```
[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
```

Étape 6. Pour importer un certificat de serveur et une clé privée (combinés dans un fichier unique), exécutez la commande **cmxctl config certs importservercert**. Sélectionnez un mot de

passe et répétez-le pour toutes les invites de mot de passe.

```
[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.
```

Étape 7. Appuyez sur **Entrée** pour redémarrer les services Cisco CMX.

Installation de certificats en haute disponibilité

- Les certificats doivent être installés séparément sur les serveurs principal et secondaire.
- Si les serveurs sont déjà jumelés, la HA doit être désactivée avant de poursuivre l'installation du certificat.
- Pour effacer les certificats existants sur le serveur principal, utilisez la commande « cmxctl config certs clear » de l'interface de ligne de commande
- Les certificats à installer sur le principal et le secondaire doivent provenir de la même autorité de certification.
- Après l'installation des certificats, les services CMX doivent être redémarrés, puis appariés pour HA.

Vérification

Pour confirmer que le certificat a été installé correctement, ouvrez l'interface Web de CMX et vérifiez le certificat utilisé.

Dépannage

Si CMX ne parvient pas à importer le certificat du serveur en raison de la vérification SAN, un élément comme celui-ci est consigné :

```
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
```

Si le champ SAN n'est pas requis, vous pouvez désactiver la vérification SAN sur CMX. Pour ce faire, référez-vous à la procédure du bogue CSCvp39346