Ejemplo de Configuración de Generación de CSR para Certificado e Instalación de Terceros en CMX 10.6

Contenido

Introducción

Este documento describe cómo generar una solicitud de firma de certificado (CSR) para obtener un certificado de terceros y cómo descargar un certificado encadenado a Cisco Connected Mobile Experiences (CMX).

Colaborado por Andres Silva y Ram Krishnamoorthy, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de Linux
- Public Key Infrastructure (PKI)
- Certificados digitales
- CMX

Componentes Utilizados

La información en este documento se basa en la versión CMX 10.6.1-47

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Nota: Utilice CMX 10.6.2-57 o superior cuando trabaje con certificados.

Configuraciones

Generar CSR

Paso 1. Acceda a la interfaz de línea de comandos (CLI) de CMX mediante SSH, ejecute el siguiente comando para generar una CSR y completar la información solicitada:

```
[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 clave privada y el CSR se almacenan en **/opt/cmx/srv/certs/**

> **Nota:** si utiliza CMX 10.6.1, el archivo SAN se agrega automáticamente a la CSR. Si la CA de terceros no puede firmar el CSR debido al campo SAN, quite la cadena SAN del archivo openssl**.conf** en CMX. Refiérase al bug CSCvp39346 para obtener más información.

Paso 2. Consiga la CSR firmada por una Autoridad de Certificación de Terceros.

Para obtener el certificado de CMX y enviarlo a terceros, ejecute el comando **cat** para abrir la CSR. Puede copiar y pegar el resultado en un archivo .txt o cambiar la extensión según los

requisitos de terceros.

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

Importar certificados firmados y certificados de autoridad certificadora (CA) a CMX

> **Nota:** Para importar e instalar los certificados en CMX, se requiere la instalación del parche raíz en CMX 10.6.1 y 10.6.2 debido al error CSCvr27467.

Paso 1. Agrupe la clave privada con el certificado firmado en un archivo **.pem**. Copie y pegue los siguientes elementos:

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

Paso 2. Agrupe los certificados de CA intermedio y raíz en un archivo **.crt**. Copie y pegue los siguientes elementos:

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

Paso 3. Transferir ambos archivos desde el paso 1 y el 2 anteriores a CMX.

Paso 4. Acceda a la CLI de CMX como root y borre los certificados actuales ejecutando el siguiente comando:

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

Paso 5. Ejecute el comando **cmxctl config certs importcacert** para importar el certificado de CA. Introduzca una contraseña y repítela para el resto de avisos de contraseña.

```
[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
```

Paso 6. Para importar el certificado del servidor y la clave privada (combinadas en un solo archivo), ejecute el comando **cmxctl config certs importservercert**. Seleccione una contraseña y repítela para todas las indicaciones de contraseña.

```
[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.
```

Paso 7. Presione **Enter** para reiniciar los servicios de Cisco CMX.

Instalación de certificados en alta disponibilidad

- Los certificados deben instalarse por separado en los servidores primario y secundario.
- Si los servidores ya están emparejados, se debe inhabilitar HA primero antes de continuar con la instalación del certificado.
- Para borrar cualquier certificado existente en el primario, utilice el comando "cmxctl config certs clear" de la CLI
- Los certificados que se instalarán tanto en el primario como en el secundario deben provenir de la misma autoridad de certificación.
- Después de la instalación de los certificados, los servicios CMX deben reiniciarse y, a continuación, emparejarse para HA.

Verificación

Para confirmar que el certificado se ha instalado correctamente, abra la interfaz web de CMX y revise el certificado en uso.

Troubleshoot

En caso de que CMX no importe el certificado del servidor debido a la verificación de SAN, se registra algo así:

```
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 el campo SAN no es necesario, puede inhabilitar la verificación de SAN en CMX. Para hacerlo, consulte el procedimiento en el bug CSCvp39346