Gerar um CSR para certificado e instalação de terceiros no exemplo de configuração do CMX 10.6

Contents

Introduction

Este documento descreve como gerar uma Solicitação de Assinatura de Certificado (CSR - Certificate Signing Request) para obter um certificado de terceiros e como fazer o download de um certificado em cadeia para o Cisco Connected Mobile Experiences (CMX).

Contribuído por Andres Silva e Ram Krishnamoorthy, engenheiros do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do Linux
- Public Key Infrastructure (PKI)
- Certificados digitais
- CMX

Componentes Utilizados

As informações neste documento são baseadas na versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Note: Use o CMX 10.6.2-57 ou superior ao trabalhar com certificados.

Configurações

Gerar CSR

Etapa1. Acesse a CLI (Command Line Interface, interface de linha de comando) do CMX usando SSH, execute o seguinte comando para gerar um CSR e completar as informações solicitadas:

```
[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
```

A chave privada e o CSR são armazenados em **/opt/cmx/srv/certs/**

> **Note**: se estiver usando o CMX 10.6.1, o campo da SAN será automaticamente adicionado ao CSR. Se a CA de terceiros não puder assinar o CSR devido ao campo SAN, remova a string SAN do arquivo openssl**.conf** no CMX. Consulte o bug CSCvp39346 para obter mais informações.

Etapa 2. Obtenha o CSR assinado por uma autoridade de certificado de terceiros.

Para obter o certificado do CMX e enviá-lo para terceiros, execute o comando **cat** para abrir o

CSR. Você pode copiar e colar a saída em um arquivo .txt ou alterar a extensão com base nos requisitos de terceiros.

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

Importar certificados assinados e certificados da autoridade de certificação (CA) para o CMX

> **Note**: Para importar e instalar os certificados no CMX, a instalação do patch raiz é necessária no CMX 10.6.1 e 10.6.2 devido ao bug CSCvr27467.

Etapa 1. Pacote de chave privada com o certificado assinado em um arquivo **.pem**. Copie e cole-os da seguinte maneira:

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

Etapa 2. Junte os certificados CA intermediário e raiz em um arquivo **.crt**. Copie e cole-os da seguinte maneira:

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

Etapa 3. Transfira ambos os arquivos das etapas 1 e 2 acima para o CMX.

Etapa 4. Acesse o CLI do CMX como raiz e limpe os certificados atuais executando o seguinte comando:

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

Etapa 5. Execute o comando **cmxctl config certs import** para importar o certificado CA. Digite uma senha e repita-a para todos os outros prompts de senha.

```
[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
```

Etapa 6. Para importar certificado do servidor e chave privada (combinados em um único arquivo), execute o comando **cmxctl config certs importservercert**. Selecione uma senha e repita-a

para todos os prompts de senha.

```
[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.
```

Passo 7. Pressione **Enter** para reiniciar os serviços do Cisco CMX.

Instalando certificados em alta disponibilidade

- Os certificados devem ser instalados separadamente nos servidores principal e secundário.
- Se os servidores já estiverem emparelhados, o HA deve ser desativado primeiro antes de continuar com a instalação do certificado.
- Para limpar todos os certificados existentes no principal, use o comando "cmxctl config certs clear" na CLI
- Os certificados a serem instalados no primário e no Secundário devem ser da mesma autoridade de certificado.
- Após a instalação dos certificados, os serviços CMX devem ser reiniciados e depois emparelhados para HA.

Verificar

Para confirmar se o certificado foi instalado corretamente, abra a interface da Web do CMX e reveja o certificado em uso.

Troubleshoot

Caso o CMX não importe o certificado do servidor devido à verificação da SAN, algo como isso é registrado:

```
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
```

Se o campo SAN não for necessário, você pode desativar a verificação de SAN no CMX. Para fazer isso, consulte o procedimento no bug CSCvp39346