Generazione di un CSR per il certificato di terze parti e installazione su CMX 10.6 Esempio di configurazione

Sommario

Introduzione

In questo documento viene descritto come generare una richiesta di firma di certificato (CSR) per ottenere un certificato di terze parti e come scaricare un certificato concatenato in Cisco Connected Mobile Experience (CMX).

Contributo di Andres Silva e Ram Krishnamoorthy, tecnici Cisco TAC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di Linux
- PKI (Public Key Infrastructure)
- Certificati digitali
- CMX

Componenti usati

Il riferimento delle informazioni contenute in questo documento è CMX versione 10.6.1-47

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Configurazione

Nota: Utilizzare CMX 10.6.2-57 o versione successiva quando si utilizzano i certificati.

Configurazioni

Genera CSR

Passaggio 1. Accedere all'interfaccia della riga di comando (CLI) di CMX utilizzando SSH, eseguire il comando seguente per generare un CSR e completare le informazioni richieste:

```
[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 chiave privata e il CSR sono memorizzati in **/opt/cmx/srv/certs/**

> **Nota:** se si utilizza CMX 10.6.1, il file SAN viene aggiunto automaticamente al CSR. Se l'autorità di certificazione di terze parti non è in grado di firmare il CSR a causa del campo SAN, rimuovere la stringa SAN dal file openssl**.conf** su CMX. per ulteriori informazioni, fare riferimento al bug CSCvp39346.

Passaggio 2. Firmare il CSR da un'autorità di certificazione di terze parti.

Per ottenere il certificato da CMX e inviarlo a terze parti, eseguire il comando **cat** per aprire il CSR. È possibile copiare e incollare l'output in un file txt o modificare l'estensione in base ai requisiti di terze parti.

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

Importa certificati firmati e certificati CA in CMX

> **Nota:** Per importare e installare i certificati su CMX, è necessario installare la patch radice su CMX 10.6.1 e 10.6.2 a causa del bug CSCvr27467.

Passaggio 1. Raggruppare la chiave privata con il certificato firmato in un file **.pem**. Copiarli e incollarli come segue:

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

Passaggio 2. Raggruppare i certificati CA intermedio e radice in un file **.crt**. Copiarli e incollarli come segue:

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

Passaggio 3. Trasferire entrambi i file dal passaggio 1 e 2 sopra a CMX.

Passaggio 4. Accedere alla CLI di CMX come root e cancellare i certificati correnti eseguendo il seguente comando:

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

Passaggio 5. Eseguire il comando **cmxctl config certs importcacert** per importare il certificato CA. Immettere una password e ripeterla per tutte le altre richieste.

```
[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
```

Passaggio 6. Per importare il certificato del server e la chiave privata (combinati in un unico file),

eseguire il comando **cmxctl config certs importservercert**. Selezionare una password e ripeterla per tutte le richieste.

```
[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.
```

Passaggio 7. Premere **Invio** per riavviare i servizi Cisco CMX.

Installazione dei certificati in alta disponibilità

- I certificati devono essere installati separatamente sui server principale e secondario.
- Se i server sono già accoppiati, prima di procedere con l'installazione del certificato è necessario disabilitare HA.
- Per cancellare i certificati esistenti sul server primario, usare il comando "cmxctl config certs clear" dalla CLI
- I certificati da installare sia nel database primario che in quello secondario devono provenire dalla stessa autorità di certificazione.
- Dopo l'installazione dei certificati, è necessario riavviare i servizi CMX e quindi accoppiarli per HA.

Verifica

Per verificare che il certificato sia stato installato correttamente, aprire l'interfaccia Web di CMX ed esaminare il certificato in uso.

Risoluzione dei problemi

Nel caso in cui CMX non riesca a importare il certificato del server a causa della verifica della SAN, viene registrato qualcosa di simile al seguente:

```
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 il campo SAN non è obbligatorio, è possibile disabilitare la verifica SAN su CMX. A tale scopo, consultare la procedura sul bug CSCvp39346