Erstellen eines CSR für Drittanbieterzertifikate und Installation auf CMX 10.6 - Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie eine Zertifikatsanforderung (Certificate Signing Request, CSR) für den Erhalt eines Zertifikats eines Drittanbieters generieren und ein verkettetes Zertifikat auf Cisco Connected Mobile Experiences (CMX) herunterladen.

Unterstützt von Andres Silva und Ram Krishnamoorthy, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse von Linux
- Public Key Infrastructure (PKI)
- Digitale Zertifikate
- CMX

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf CMX-Version 10.6.1-47.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Hinweis: Verwenden Sie beim Arbeiten mit Zertifikaten CMX 10.6.2-57 oder höher.

Konfigurationen

CSR erstellen

Schritt 1: Greifen Sie über SSH auf die Befehlszeilenschnittstelle (CLI) von CMX zu, führen Sie den folgenden Befehl aus, um einen CSR zu generieren, und füllen Sie die angeforderten Informationen aus:

```
[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
```

Der private Schlüssel und die CSR werden in **/opt/cmx/srv/certs/** gespeichert.

> **Hinweis**: Bei Verwendung von CMX 10.6.1 wird das SAN-Feld automatisch dem CSR hinzugefügt. Wenn eine CA eines Drittanbieters aufgrund des SAN-Felds die CSR-Datei nicht signieren kann, entfernen Sie die SAN-Zeichenfolge aus der Datei openssl**.conf** in CMX. Weitere Informationen finden Sie unter Fehler CSCvp39346.

Schritt 2: Lassen Sie sich den CSR von einer Zertifizierungsstelle eines Drittanbieters signieren.

Um das Zertifikat von CMX abzurufen und an Dritte zu senden, führen Sie den Befehl **cat** aus, um den CSR zu öffnen. Sie können die Ausgabe in eine TXT-Datei kopieren und einfügen oder die Erweiterung entsprechend den Anforderungen des Drittanbieters ändern.

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

Importieren signierter Zertifikate und Zertifikate der Zertifizierungsstelle (Certificate Authority, CA) in CMX

> **Hinweis**: Um die Zertifikate in CMX zu importieren und zu installieren, ist die Installation des Root-Patches auf CMX 10.6.1 und 10.6.2 aufgrund des Fehlers CSCvr27467 erforderlich.

Schritt 1: Binden Sie einen privaten Schlüssel mit dem signierten Zertifikat in eine **.pem-**Datei ein. Kopieren Sie die Dateien und fügen Sie sie wie folgt ein:

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

Schritt 2: Bundle die Zertifikate der Zwischen- und Stammzertifizierungsstelle in einer **.crt-**Datei. Kopieren Sie die Dateien und fügen Sie sie wie folgt ein:

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

Schritt 3: Übertragen Sie beide Dateien von Schritt 1 und 2 oben auf CMX.

Schritt 4: Greifen Sie auf die CLI von CMX als Root zu, und löschen Sie die aktuellen Zertifikate, indem Sie den folgenden Befehl ausführen:

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

Schritt 5: Führen Sie den Befehl **cmxctl config certs importcacert** aus, um das CA-Zertifikat zu importieren. Geben Sie ein Kennwort ein, und wiederholen Sie es für alle anderen Kennwortaufforderungen.

```
[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
```

Schritt 6: Um Serverzertifikat und privaten Schlüssel (kombiniert in einer Datei) zu importieren, führen Sie den Befehl **cmxctl config certs importservercert aus**. Wählen Sie ein Kennwort aus, und wiederholen Sie es für alle Kennwortaufforderungen.

```
[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.
```

Schritt 7: Drücken Sie **die Eingabetaste**, um die Cisco CMX-Services neu zu starten.

Installieren von Zertifikaten in hoher Verfügbarkeit

- Zertifikate müssen sowohl auf dem primären als auch auf dem sekundären Server separat installiert werden.
- Wenn die Server bereits gepaart sind, sollte HA zunächst deaktiviert werden, bevor mit der Zertifikatsinstallation fortgefahren wird.
- Um alle vorhandenen Zertifikate auf dem primären zu löschen, verwenden Sie den Befehl "cmxctl config certs clear" aus der CLI.
- Zertifikate, die sowohl auf der primären als auch auf der sekundären Ebene installiert werden sollen, sollten von derselben Zertifizierungsstelle stammen.
- Nach der Installation von Zertifikaten sollten CMX-Dienste neu gestartet und dann für HA gepaart werden.

Überprüfen

Um zu überprüfen, ob das Zertifikat korrekt installiert wurde, öffnen Sie die Webschnittstelle von CMX, und überprüfen Sie das verwendete Zertifikat.

Fehlerbehebung

Falls CMX das Serverzertifikat aufgrund der SAN-Überprüfung nicht importieren kann, wird so etwas protokolliert:

```
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
```

Wenn das SAN-Feld nicht erforderlich ist, können Sie die SAN-Überprüfung in CMX deaktivieren. Lesen Sie dazu das Verfahren zum Fehler CSCvp39346