CMX 10.6でのサードパーティ証明書用CSRの生成とインストールの設定例

内容

概要

このドキュメントでは、サードパーティの証明書を取得するために証明書署名要求(CSR)を生成する方法、およびチェーン証明書をCisco Connected Mobile Experiences(CMX)にダウンロードする方法について説明します。

著者：Cisco TACエンジニア、Andres SilvaおよびRam Krishnamoorthy

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Linuxの基礎知識
- 公開キー インフラストラクチャ（PKI）
- デジタル証明書
- CMX

使用するコンポーネント

このドキュメントの情報は、CMXバージョン10.6.1-47に基づくものです

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

_

注：証明書を操作する際は、CMX 10.6.2-57以降を使用してください。

設定

CSR の生成

ステップ1:SSHを使用してCMXのコマンドラインインターフェイス(CLI)にアクセスし、次のコマンドを実行してCSRを生成し、要求された情報を入力します。

```
[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
```

秘密キーとCSRは/opt/cmx/**srv/certs/に保存されます**

> **注**：cmx 10.6.1を使用している場合、SANフィールドは自動的にCSRに追加されます。SANフィールドが原因でサードパーティCAがCSRに署名できない場合は、CMXのopenssl.confファイルからSAN**文字列を削**除します。詳細は、バグCSCvp39346を参照してください。

ステップ2：サードパーティ認証局によって署名されたCSRを取得します。

CMXから証明書を取得してサードパーティに送信するには、**catコマンドを実行**してCSRを開き

ます。出力を.txtファイルにコピーアンドペーストするか、サードパーティの要件に基づいて拡張子を変更できます。

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

署名付き証明書および認証局(CA)証明書をCMXにインポートします

> **注**：CMXに証明書をインポートしてインストールするには、CMX 10.6.1および10.6.2にルートパッチのインストールが必要です。これは、バグCSCvr27467が原因で発生します。

ステップ1：署名済み証明書を含む秘密キーを.pemファイルに**バッジング**します。次のようにコピーして貼り付けます。

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

ステップ2：中間CA証明書とルートCA証明書を.crtファイルに**バッジング**します。次のようにコピーして貼り付けます。

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

ステップ3：上記のステップ1と2の両方のファイルをCMXに転送します。

ステップ4：ルートとしてCMXのCLIにアクセスし、次のコマンドを実行して現在の証明書をクリアします。

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

ステップ5:**cmxctl config certs importcacertコマンドを実行**して、CA証明書をインポートします。パスワードを入力し、他のすべてのパスワードプロンプトに対して同じパスワードを繰り返します。

```
[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
```

ステップ6：サーバ証明書と秘密キー（1つのファイルに結合）をインポートするには、**cmxctl**

config certs importservercertコマンドを実行します。パスワードを選択し、すべてのパスワードプロンプトに対してパスワードを繰り返します。

```
[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.
```

ステップ7:Enterキーを押してCisco CMXサービスを再起動します。

ハイアベイラビリティでの証明書のインストール

- 証明書は、プライマリサーバとセカンダリサーバの両方に個別にインストールする必要があります。
- サーバがすでにペアになっている場合は、証明書のインストールを続行する前に、まずHAを無効にする必要があります。
- プライマリの既存の証明書をクリアするには、CLIから「cmxctl config certs clear」コマンドを使用します
- プライマリとセカンダリの両方にインストールする証明書は、同じ認証局からのものである必要があります。
- 証明書をインストールした後、CMXサービスを再起動し、HAとペアリングする必要があります。

確認

証明書が正しくインストールされたことを確認するには、CMXのWebインターフェイスを開き、使用中の証明書を確認します。

トラブルシュート

SANの検証のためにCMXがサーバ証明書のインポートに失敗した場合、次のようなログが記録されます。

```
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
```

[SAN]フィールドが不要な場合は、CMXでSAN検証を無効にできます。これを行うには、バグCSCvp39346の手順を参照してくださ[い]