在CMX 10.6上生成第三方證書和安裝的CSR配置示例

目錄

簡介

本文說明如何產生憑證簽署請求(CSR)，以便取得第三方憑證，以及如何將鏈結憑證下載到思科連線行動體驗(CMX)。

作者：Andres Silva和Ram Krishnamoorthy，Cisco TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- Linux基礎知識
- 公開金鑰基礎架構 (PKI)
- 數位憑證
- CMX

採用元件

本檔案中的資訊是根據CMX版本10.6.1-47

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

附註：使用證書時，請使用CMX 10.6.2-57或更高版本。

組態

產生CSR

步驟1.使用SSH訪問CMX的命令列介面(CLI)，運行以下命令生成CSR並完成請求的資訊：

```
[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
```

私鑰和CSR儲存在**/opt/cmx/srv/certs/**中

> **附註**：如果使用CMX 10.6.1，則SAN欄位會自動新增到CSR。如果第三方CA由於SAN欄位原因無法簽署CSR，請從CMX上的openssl.conf檔案中**移除**SAN字串。如需詳細資訊，請參閱錯誤CSCvp39346。

步驟2.讓第三方憑證授權機構簽署CSR。

若要從CMX取得憑證並將其傳送至第三方，請執行**cat** 命令以開啟CSR。您可以將輸出複製並貼上到.txt檔案中，也可以根據第三方的要求更改副檔名。

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

將簽名的證書和證書頒發機構(CA)證書匯入到CMX

附註：為了在CMX上匯入和安裝證書，由於CSCvr27467錯誤，必須在CMX 10.6.1和10.6.2上安裝根修補程式。

步驟1.將具有簽名證書的私鑰捆綁到.pem文件中。按如下方式複製並貼上它們：

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

步驟2.將中間和根CA證書捆綁到.crt文件。按如下方式複製並貼上它們：

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

步驟3.將以上步驟1和2中的兩個檔案傳輸到CMX。

步驟4.以超級使用者身份訪問CMX的CLI，並通過運行以下命令清除當前證書：

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

步驟5.運行cmxctl config certs importcacert命令以匯入CA證書。輸入密碼，然後對所有其它密碼提示重複該密碼。

```
[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
```

步驟6.要匯入伺服器證書和私鑰（合併到單個檔案中），請運行cmxctl config certs importservercert命令。選擇一個口令，然後對所有口令提示重複該口令。

```
[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.
```

步驟7.按**Enter**鍵重新啟動Cisco CMX服務。

在高可用性中安裝證書

- 證書必須分別安裝在主伺服器和輔助伺服器上。
- 如果伺服器已配對，應先停用HA，然後再繼續憑證安裝。
- 要清除主上的任何現有證書，請使用CLI中的「cmxctl config certs clear」命令
- 要同時安裝在主要和輔助上的證書應該來自同一證書頒發機構。
- 安裝證書後，應重新啟動CMX服務，然後針對HA配對。

驗證

要確認證書是否正確安裝，請開啟CMX的Web介面並檢視正在使用的證書。

疑難排解

如果CMX由於SAN驗證而無法匯入伺服器證書，則會記錄類似以下內容：

```
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
```

如果不需要SAN欄位，您可以在CMX上禁用SAN驗證。如需瞭解相關資訊，請參閱錯誤CSCvp[上的程式39346]