为第三方证书生成CSR并在CMX 10.6上安装配置示例

目录

简介

本文档介绍如何生成证书签名请求(CSR)以获取第三方证书，以及如何将链接证书下载到思科互联移动体验(CMX)。

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

先决条件

要求

Cisco 建议您了解以下主题：

- Linux基础知识
- 公用密钥基础结构 (PKI)
- 数字证书
- CMX

使用的组件

本文档中的信息基于CMX版本10.6.1-47

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

注意：使用证书时，请使用CMX 10.6.2-57或更高版本。

配置

生成 CSR

步骤1.使用SSH访问CMX的命令行界面(CLI)，运行以下命令以生成CSR并完成请求的信息：

```
[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
```

私钥和CSR存储在/opt/cmx/srv/certs/

> **注意：**如果使用CMX 10.6.1,SAN字段会自动添加到CSR。如果第三方CA由于SAN字段而无法对CSR进行签名，请从CMX上的openssl.conf文件中删除SAN字符串。有关详细信息，请参阅Bug CSCvp39346。

步骤2.获取由第三方证书颁发机构签署的CSR。

要从CMX获取证书并将其发送到第三方，请运行**cat** 命令以打开CSR。您可以将输出复制并粘贴到.txt文件中，或根据第三方的要求更改扩展名。

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

将签名证书和证书颁发机构(CA)证书导入CMX

注意：要在CMX上导入和安装证书，由于CSCvr27467的缺陷，需要在CMX 10.6.1和10.6.2上安装根补丁。

步骤1.将带签名证书的私钥捆绑到.pem文件中。复制并粘贴如下：

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

步骤2.将中间和根CA证书捆绑到.crt文件中。复制并粘贴如下：

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

步骤3.将上述步骤1和步骤2中的两个文件传输到CMX。

步骤4.以根用户身份访问CMX的CLI，并通过运行以下命令清除当前证书：

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

步骤5.运行cmxctl config certs importcacert命令以导入CA证书。输入密码，并对所有其他密码提示重复该密码。

```
[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
```

步骤6.要导入服务器证书和私钥（合并到单个文件中），请运行cmxctl config certs importservercert命令。选择密码，并对所有密码提示重复该操作。

```
[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.
```

步骤7.按**Enter**重新启动Cisco CMX服务。

在高可用性中安装证书

- 证书必须分别安装在主服务器和辅助服务器上。
- 如果服务器已成对，则应先禁用HA，然后再继续安装证书。
- 要清除主上的任何现有证书，请在CLI中使用“cmxctl config certs clear”命令
- 要同时安装在主证书和辅助证书上的证书应来自同一证书颁发机构。
- 在安装证书后，应重新启动CMX服务，然后配对HA。

验证

要确认证书已正确安装，请打开CMX的Web界面并查看使用中的证书。

故障排除

如果CMX由于SAN验证而无法导入服务器证书，则会记录以下内容：

```
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字段，您可以在CMX上禁用SAN验证。为此，请参阅Bug CSCvp39346上的步骤