Procédure d'installation du certificat SSL CMX 10.5

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Préparation et sauvegarde](#)
[Configuration](#)
[Vérifier les certificats](#)
[Installer les certificats sur CMX](#)
[Dépannage](#)

Introduction

Cet article donne un exemple sur comment obtenir un certificat SSL gratuit et comment l'installer sur CMX. The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Nom de domaine pouvant être résolu en externe

- Compétences de base en linux

- Connaissances de base de l'ICP (infrastructure à clé publique)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CMX 10,5

Préparation et sauvegarde

Le certificat Web se trouve dans le dossier suivant :

```
[root@cmxtry ssl]# pwd
/opt/haproxy/ssl
```

Sauvegarder l'ancien certificat et la clé :

```
[cmxadmin@cmxtry ssl]$cd /opt/haproxy/ssl/

[cmxadmin@cmxtry ssl]$su root
Password: (enter root password)

[root@cmxtry ssl]# mkdir ./oldcert
[root@cmxtry ssl]# mv host.* ./oldcert/

[root@cmxtry ssl]# ls ./oldcert/
host.key  host.pem
```

Si vous n'êtes pas familier avec Linux, les commandes ci-dessus peuvent être interprétées de la manière suivante :

```
[cmxadmin@cmxtry ssl]$cd /opt/haproxy/ssl/

[cmxadmin@cmxtry ssl]$su root
Password: (enter root password)

[root@cmxtry ssl]# mkdir /opt/haproxy/ssl/oldcert
[root@cmxtry ssl]# mv host.pem /opt/haproxy/ssl/oldcert/
[root@cmxtry ssl]# mv host.key /opt/haproxy/ssl/oldcert/

[root@cmxtry ssl]# ls /opt/haproxy/ssl/oldcert/
host.key  host.pem
```

Configuration

Générer une clé privée :

```
openssl genrsa -out cmxtry.com.key 2048

[root@cmxtry ssl]# openssl genrsa -out cmxtry.com.key 2048
Generating RSA private key, 2048 bit long modulus
.............
...............
e is 65537 (0x10001)

[root@cmxtry ssl]# ls
cmxtry.com.key  oldcert
```

Générez un CSR (demandes de signature de certificat) à l'aide de la clé privée que vous avez générée à l'étape précédente.

```
[root@cmxtry ssl]# openssl req -new -sha256 -key cmxtry.com.key -out cmxtry.com.csr

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]:BE
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:DIEGEM
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CMXTRY
Organizational Unit Name (eg, section) []:CMXTRY
Common Name (e.g. server FQDN or YOUR name) []:cmxtry.com
Email Address []:avitosin@cisco.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Cisco123
An optional company name []:CMXTRY


[root@cmxtry ssl]# ls
cmxtry.com.csr  cmxtry.com.key  oldcert
```

Afficher le CSR :

```
[root@cmxtry ssl]# cat cmxtry.com.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIDZTCCAk0CAQAwgY0xCzAJBgNVBAYTAkJFMRMwEQYDVQQIDApTb21lLVN0YXRl
MQ8wDQYDVQQHDAZESUVHRU0xDzANBgNVBAoMBkNNWFRSWTEPMA0GA1UECwwGQ01Y
VFJZMRMwEQYDVQQDDApjbXh0cnkuY29tMSEwHwYJKoZIhvcNAQkBFhJhdml0b3Np
bkBjaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCkEIg0
AxV/3HxAxUu7UI/LxkTP+DZJvvuua1WgyQ+tlD4r1+k1Wv1eINCJqywglCKt9vVg
aiYp4JAKL28TV7rtSKqNFnWDMtTKoYRkYWI3L48r9Mu9Tt3zDCG09ygnQFi6SnmX
VmKx7Ct/wIkkBXfkq1nq4vqosCry8SToS1PThX/KSuwIF6w2aKj1Fbrw3eW4XJxc
5hoQFrSsquqmbi5IZWgH/zMZUZTdWYvFc/h50PCBJsAa9HTY0sgUe/nyjHdt+V/l
alNSh41jsrulhWiPzqbaPW/Fej9/5gtPG5LReWuS20ulAnso4tdcST1vVletoXJw
F58S8AqeVrcOV9SnAgMBAAGggZEwFQYJKoZIhvcNAQkCMQgMBkNNWFRSWTAXBgkq
hkiG9w0BCQcxCgwIQ2lzY28xMjMwXwYJKoZIhvcNAQkOMVIwUDAJBgNVHRMEAjAA
MBcGA1UdEQQQMA6CDF9fSE9TVE5BTUVfXzAdBgNVHSUEFjAUBggrBgEFBQcDAQYI
KwYBBQUHAwIwCwYDVR0PBAQDAgOoMA0GCSqGSIb3DQEBCwUAA4IBAQCBslfRzbiw
WBBBN74aWm6YwkO0YexpR2yCrQhcOsxWTujPVvzNP9WaDNxu1rw6o3iZclGi6D61
qFsKtchQhnclvOj7rNI8TInaxIorR2zMy0lF2vtJmvY4YQFso9qzmuaxkmttEMFU
Fj0bxKh6SpvxePh6+BDcwt+kQExK5aF3Q6cRIMyKBS2+I5J5eddJ0cdIqTfwZOGD
5dMDWqHGd7IZyrend8AMPZvNKm3Sbx11Uq+A/fa7f9JZE0O2Q9h3sl3hj3QIPU6s
w1Pyd66/OX04yYIvMyjJ8xpJGigNWBOvQ+GLvK0ce441h2u2oIoPe60sDOYldL+X
JsnSbefiJ4Fe
-----END CERTIFICATE REQUEST-----
```

Copier le CSR (inclure le début de la ligne de demande de certificat et la fin de la ligne de demande de certificat).

Dans le cas de mon laboratoire, j'utilisais le certificat gratuit de Comodo (https://www.instantssl.com/)

OBJ