Procedura di installazione del certificato SSL CMX 10.5

Sommario

Introduzione

In questo articolo verrà fornito un esempio su come ottenere un certificato SSL gratuito e su come installarlo in CMX. Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Nome di dominio risolvibile esternamente

- Conoscenze base di Linux

- Conoscenze base di PKI (Public Key Infrastructure)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CMX 10.5

Preparazione e backup

Il certificato Web si trova nella cartella seguente:

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

Esegui backup del certificato e della chiave precedenti:

```
[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
```

Se non si ha molta familiarità con Linux, i comandi di cui sopra possono essere interpretati nel modo seguente:

```
[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
```

Configurazione

Genera una chiave privata:

```
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
```

Generare un CSR (Certificate Sign Requests) utilizzando la chiave privata generata nel passaggio precedente.

```
[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
```

Visualizzare il 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-----
```

Copiare il CSR (includere l'inizio della riga di richiesta certificato e la fine della riga di richiesta certificato).

Nel caso del mio laboratorio, stavo usando il certificato gratuito di Comodo (https://www.instantssl.com/)

OBJ