

Procedimiento de instalación del certificado SSL CMX 10.5

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Preparación y copia de seguridad](#)

[Configurar](#)

[Verificar los certificados](#)

[Instale los certificados en CMX](#)

[Troubleshoot](#)

Introducción

En este artículo se proporciona un ejemplo sobre cómo obtener un certificado SSL gratuito y cómo instalarlo en 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.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Un nombre de dominio que se puede resolver externamente
- Técnicas básicas de Linux
- Conocimiento básico de PKI (Infraestructura de clave pública)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CMX 10.5

Preparación y copia de seguridad

El certificado Web se encuentra en la carpeta siguiente:

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

Copia de seguridad del certificado y la clave antiguos:

```
[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
```

En caso de que no esté familiarizado con Linux, los comandos anteriores pueden interpretarse de la siguiente manera:

```
[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
```

Configurar

Generar una clave privada:

```
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
```

Genere una CSR (solicitudes de firma de certificado) utilizando la clave privada que ha generado en el paso anterior.

```
[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
```

Mostrar la CSR:

```
[root@cmxtry ssl]# cat cmxtry.com.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIDZTCCAk0CAQAwY0xCzAJBgNVBAYTAKJFMRMwEQYDVQQIDApTb211LVN0YXR1
MQ8wDQYDVQQHDAZESUVVHRU0xDzANBgNVBAoMBkNNWFERSWTEPMA0GA1UECwwGQ01Y
VFJZMRMwEQYDVQQDDApjbXh0cnkuY29tMSEwHwYJKoZIhvcNAQkBFhJhdml0b3Np
bkBjaXNjby5jb20wggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCkEIg0
AxV/3HxAxUu7UI/LxkTP+DZJvuuu1WgyQ+tLD4r1+k1Wv1eINcJqywg1CKt9vVg
aiYp4JAKL28TV7rtSKqNFnWDMtTKoYRkYWI3L48r9Mu9Tt3zDCG09ygnQFi6SnmX
VmKx7Ct/wIkkBXfkq1nq4vqosCry8SToS1PThX/KSuwIF6w2akj1Fbrw3eW4XJxc
5hoQFrSsquqmbi5IZWgH/zMZUZTdWYvFc/h50PCBJsAa9HTY0sgUe/nyjHdt+v/l
alNSh41jsrulhWiPzqbaPW/Fej9/5gtPG5LReWuS20ulAnso4tdcST1vV1etoXJw
F58S8AqeVrcOV9SnAgMBAAGggZEwFQYJKoZIhvcNAQkCMQgMBkNNWFERSWTAXBgkq
hkiG9w0BCQcxCGwIQ21zY28xMjMwXwYJKoZIhvcNAQkOMVIwUDAJBgNVHRMEAjAA
MBCGA1UdEQQQMA6CDF9fSE9TVE5BTUVfXzAdBgNVHSUEFjAUBgggrBgEFBQcDAQYI
KwYBBQUHAWIwCwYDVR0PBAQDAGoOMA0GCSqGSIb3DQEBCwUAA4IBAQCBS1fRzbiw
WBBBN74aWm6Ywk00Yexpr2yCrQhcOosxWTu jPVvzNP9WadNxlrw6o3iZclGi6D61
qFsKtchQhnc1vOj7rNI8TInaxIorR2zMy0lF2vtJmvY4YQFso9qzmuaxkmttEMFU
Fj0bxKh6Spvxeph6+BDcwt+kQExK5aF3Q6cRIMyKBS2+I5J5eddJ0cdIqTfwZOGD
5dMDWqHGd7IZyrend8AMPZvNKm3Sbx11Uq+A/fa7f9JZE002Q9h3sl3hj3QIPU6s
w1Pyd66/OX04yYIvMyjJ8xpJGigNwBOvQ+GLvK0ce441h2u2oIoPe60sDOYldL+X
JsnSbefiJ4Fe
-----END CERTIFICATE REQUEST-----
```

Copie el CSR (incluya el comienzo de la línea de solicitud de certificado y la línea de solicitud de fin de certificado).

En el caso de mi laboratorio, estaba usando el certificado gratuito de Comodo

(<https://www.instantssl.com/>)

[OBJ]

