CMX 10.5 SSL-Zertifikatsinstallationsverfahren

Inhalt

Einführung

In diesem Artikel wird ein Beispiel für das Abrufen eines kostenlosen SSL-Zertifikats und dessen Installation auf CMX vorgestellt. Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Ein Domänenname, der extern aufgelöst werden kann.

- Grundlegende Linux-Kenntnisse

- Grundkenntnisse der PKI (Public Key Infrastructure)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- CMX 10.5

Vorbereitung und Backup

Das Webzertifikat befindet sich im folgenden Ordner:

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

Sichern Sie das alte Zertifikat und den alten Schlüssel:

```
[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
```

Falls Sie mit Linux nicht sehr vertraut sind, können die obigen Befehle folgendermaßen interpretiert werden:

```
[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
```

Konfigurieren

Erstellen eines privaten Schlüssels:

```
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
```

Erstellen Sie einen CSR (Certificate Sign Requests) mit dem privaten Schlüssel, der im vorherigen Schritt generiert wurde.

```
[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
```

CSR anzeigen:

```
[root@cmxtry ssl]# cat cmxtry.com.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIDZTCCAk0CAQAwgY0xCzAJBgNVBAYTAkJFMRMwEQYDVQQIDApTb211LVN0YXRl
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-----
```

Kopieren Sie den CSR (einschließlich Beginn der Zeile für die Zertifikatsanforderung und Ende der Zertifikatsanforderungszeile).

Im Fall meiner Übung habe ich das kostenlose Zertifikat von Comodo (https://www.instantssl.com/) verwendet.