CARLOS CHRISTIAN PÉREZ AZUAGA 2ºDAW24-25 15/11/2024

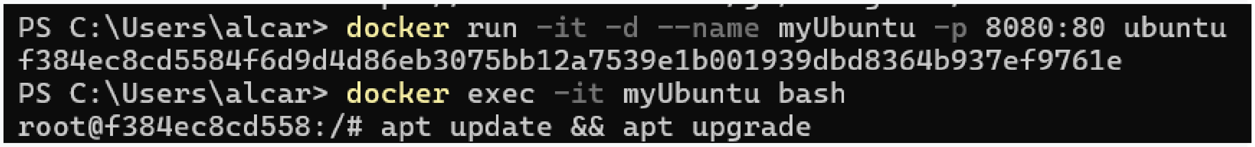
Crear un certificado auto-firmado

Objetivos

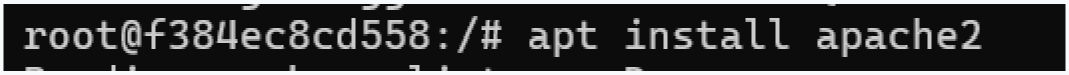
- Crear un certificado auto-firmado utilizando OpenSSL

Requisitos previos

- Instalar OpenSSL en Windows si es necesario desde slproweb.com.



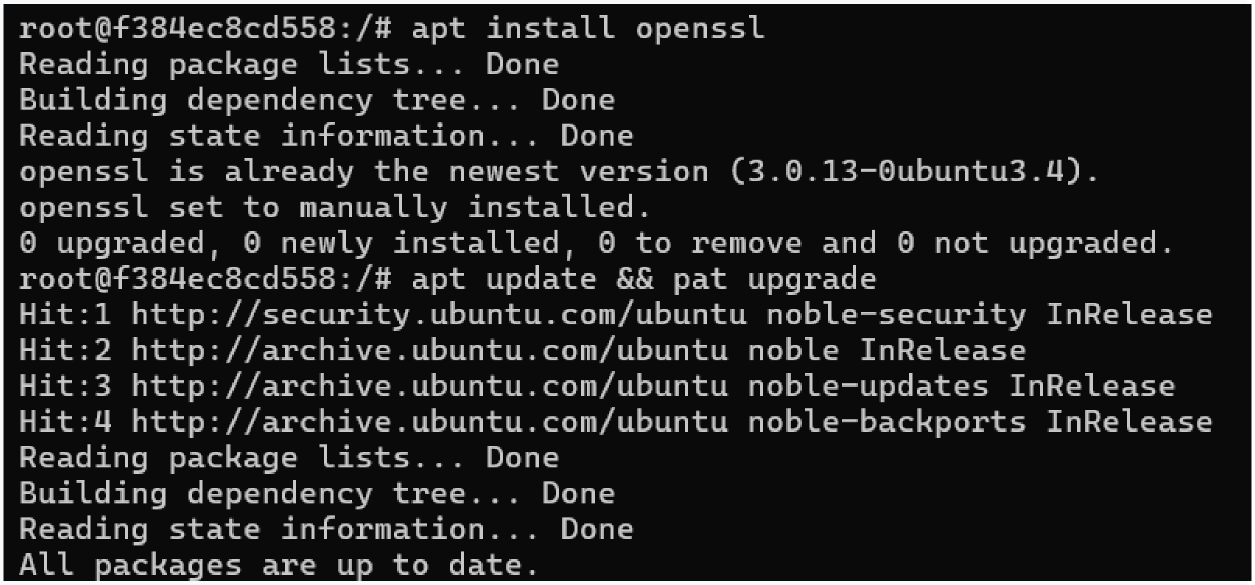
```
PS C:\Users\alcar> docker run -it -d --name myUbuntu -p 8080:80 ubuntu
f384ec8cd5584f6d9d4d86eb3075bb12a7539e1b001939dbd8364b937ef9761e
PS C:\Users\alcar> docker exec -it myUbuntu bash
root@f384ec8cd558:/# apt update && apt upgrade
```



```
root@f384ec8cd558:/# apt install apache2
```

Instalar OpenSSL en Linux (Ubuntu)

```
sudo apt update && sudo apt install openssl
```

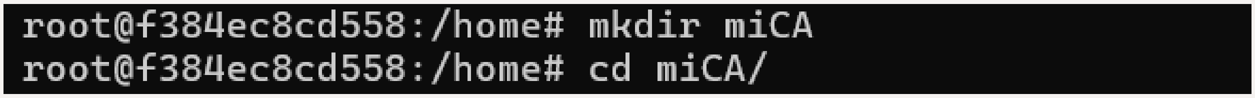


```
root@f384ec8cd558:/# apt install openssl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssl is already the newest version (3.0.13-0ubuntu3.4).
openssl set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@f384ec8cd558:/# apt update && pat upgrade
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://archive.ubuntu.com/ubuntu noble InRelease
Hit:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
```

Generar el certificado auto-firmado de la Entidad Certificadora (Certification Authority / CA)

Crear un directorio para los archivos de la CA:

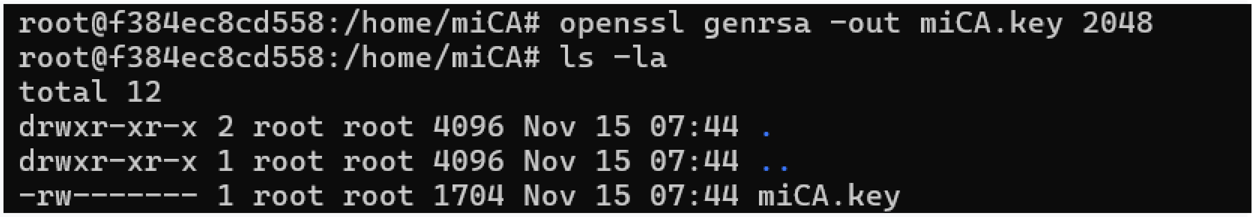
```
mkdir ~/miCA && cd ~/miCA
```



```
root@f384ec8cd558:/home# mkdir miCA
root@f384ec8cd558:/home# cd miCA/
```

Generar la clave privada de la CA:

`openssl genrsa -out miCA.key 2048`

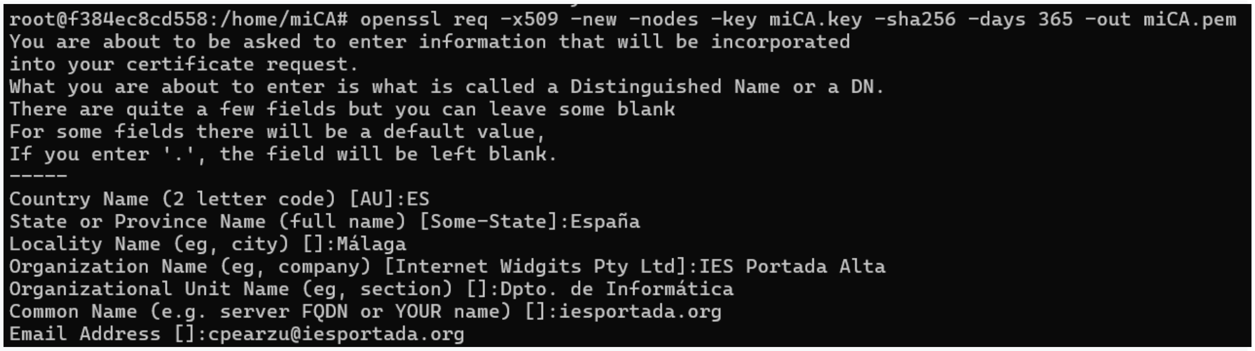


```
root@f384ec8cd558:/home/miCA# openssl genrsa -out miCA.key 2048
root@f384ec8cd558:/home/miCA# ls -la
total 12
drwxr-xr-x 2 root root 4096 Nov 15 07:44 .
drwxr-xr-x 1 root root 4096 Nov 15 07:44 ..
-rw------- 1 root root 1704 Nov 15 07:44 miCA.key
```

Crear el certificado autofirmado de la CA:

`openssl req -x509 -new -nodes -key miCA.key -sha256 -days 365 -out miCA.pem`

1. Completa la información del certificado (Nombre de la CA, país, etc.), puedes utilizar datos similares a estos:
   Country Name (2 letter code) [AU]:ES
   State or Province Name (full name) [Some-State]:España
   Locality Name (eg, city) []:Málaga
   Organization Name (eg, company) [Internet Widgits Pty Ltd]:IES Portada Alta
   Organizational Unit Name (eg, section) []:Dpto. de Informática
   Common Name (e.g. server FQDN or YOUR name) []:iesportada.org
   Email Address []:juanperez@iesportada.org

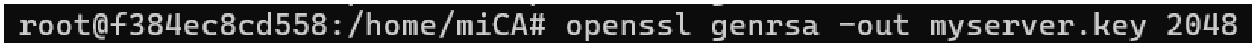


```
root@f384ec8cd558:/home/miCA# openssl req -x509 -new -nodes -key miCA.key -sha256 -days 365 -out miCA.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite 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]:ES
State or Province Name (full name) [Some-State]:España
Locality Name (eg, city) []:Málaga
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IES Portada Alta
Organizational Unit Name (eg, section) []:Dpto. de Informática
Common Name (e.g. server FQDN or YOUR name) []:iesportada.org
Email Address []:cpearzu@iesportada.org
```

Crear el certificado auto-firmado para el servidor

Crear una clave privada para el servidor:

`openssl genrsa -out myserver.key 2048`



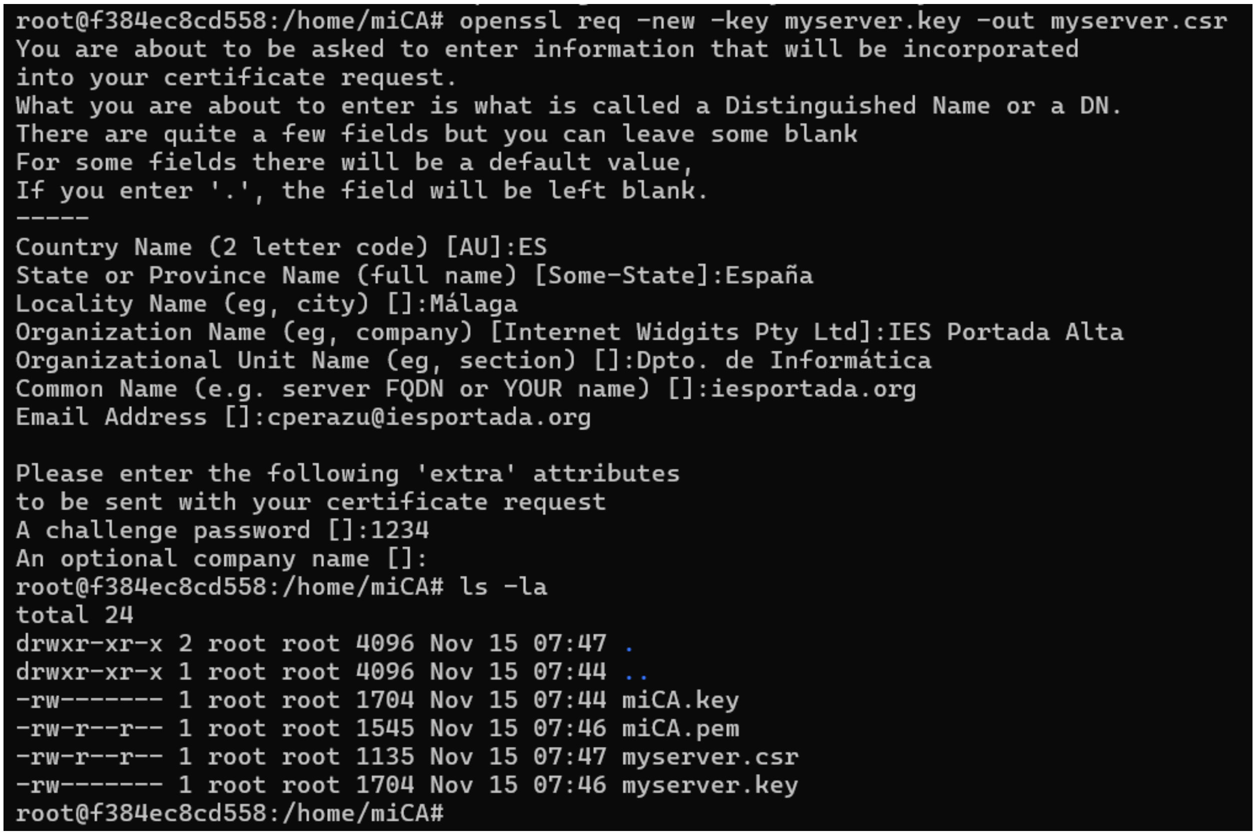
```
root@f384ec8cd558:/home/miCA# openssl genrsa -out myserver.key 2048
```

Crear una solicitud de firma de certificado (CSR) para el servidor:

`openssl req -new -key myserver.key -out myserver.csr`

1. Completa la información con datos similares a estos:
   - Country Name (2 letter code) [AU]:ES
     State or Province Name (full name) [Some-State]:España

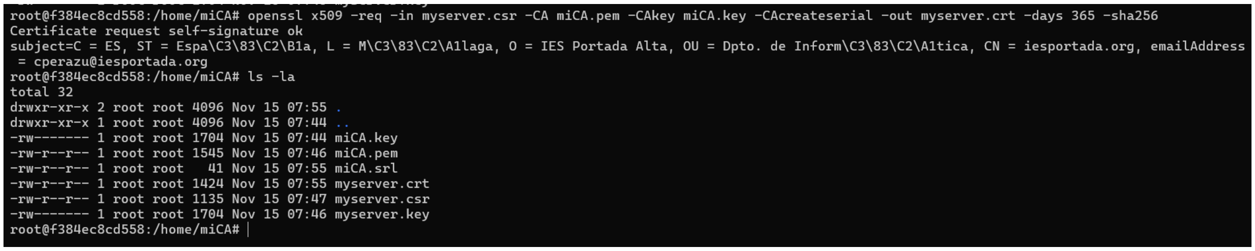
Locality Name (eg, city) []:Málaga
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IES Portada Alta
Organizational Unit Name (eg, section) []:Dpto. de Informática
Common Name (e.g. server FQDN or YOUR name) []:ejemplo.iesportada.org
Email Address []:juanperez@iesportada.org



```
root@f384ec8cd558:/home/miCA# openssl req -new -key myserver.key -out myserver.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]:ES
State or Province Name (full name) [Some-State]:España
Locality Name (eg, city) []:Málaga
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IES Portada Alta
Organizational Unit Name (eg, section) []:Dpto. de Informática
Common Name (e.g. server FQDN or YOUR name) []:iesportada.org
Email Address []:cperazu@iesportada.org

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:
root@f384ec8cd558:/home/miCA# ls -la
total 24
drwxr-xr-x 2 root root 4096 Nov 15 07:47 .
drwxr-xr-x 1 root root 4096 Nov 15 07:44 ..
-rw------- 1 root root 1704 Nov 15 07:44 miCA.key
-rw-r--r-- 1 root root 1545 Nov 15 07:46 miCA.pem
-rw-r--r-- 1 root root 1135 Nov 15 07:47 myserver.csr
-rw------- 1 root root 1704 Nov 15 07:46 myserver.key
root@f384ec8cd558:/home/miCA#
```

2. Firmar el CSR con la CA para generar el certificado:
   `openssl x509 -req -in myserver.csr -CA miCA.pem -CAkey miCA.key -CAcreateserial -out myserver.crt -days 365 -sha256`



```
root@f384ec8cd558:/home/miCA# openssl x509 -req -in myserver.csr -CA miCA.pem -CAkey miCA.key -CAcreateserial -out myserver.crt -days 365 -sha256
Certificate request self-signature ok
subject=C = ES, ST = Espa\C3\83\C2\B1a, L = M\C3\83\C2\A1laga, O = IES Portada Alta, OU = Dpto. de Inform\C3\83\C2\A1tica, CN = iesportada.org, emailAddress
 = cperazu@iesportada.org
root@f384ec8cd558:/home/miCA# ls -la
total 32
drwxr-xr-x 2 root root 4096 Nov 15 07:55 .
drwxr-xr-x 1 root root 4096 Nov 15 07:44 ..
-rw------- 1 root root 1704 Nov 15 07:44 miCA.key
-rw-r--r-- 1 root root 1545 Nov 15 07:46 miCA.pem
-rw-r--r-- 1 root root   41 Nov 15 07:55 miCA.srl
-rw-r--r-- 1 root root 1424 Nov 15 07:55 myserver.crt
-rw-r--r-- 1 root root 1135 Nov 15 07:47 myserver.csr
-rw------- 1 root root 1704 Nov 15 07:46 myserver.key
root@f384ec8cd558:/home/miCA#
```