Memoria de prácticas Servidor Web (https)

José Antonio Castillejo Lobato

Índice

1. Creación de Dockerfile

Creamos un Dockerfile donde indicamos con el from el contenedor y su versión y ponemos el archivo public-html en la ruta de htdocs

```
FROM httpd:2.4
COPY ./public-html/ /usr/local/apache2/htdocs/
```

Luego ejecutamos los comandos para ejecutar y compilar la imagen de docker dándole un nombre con –name y asignándole el puerto

```
$ docker build -t my-apache2 .
$ docker run -dit --name my-running-app -p 8080:80 my-apache2
```

2. Creación sin Dockerfile

Si queremos crear el Dockerfile solo debemos incluir el siguiente comando donde ejecutamos y compilamos la imagen de cocker dándole un nombre con –name y asignándole el puerto y la ruta del htdocs

```
$ docker run -dit --name my-apache-app -p 8080:80 -v "$PWD":/usr/local/apache2/htdocs/ httpd:2.4
```

3. Configuración

Para personalizar la configuración del servidor httpd, primero hay que obtener la configuración predeterminada del contenedor

```
$ docker run --rm httpd:2.4 cat /usr/local/apache2/conf/httpd.conf > my-httpd.conf
```

Y luego puedes poner la configuración creada en el paso de la creación de Dockerfile

```
FROM httpd:2.4
COPY ./my-httpd.conf /usr/local/apache2/conf/httpd.conf
```

4. SSL/HTTPS

Para ejecutar su tráfico web a través de SSL, la configuración más sencilla es COPIAR o montar un server.crt y server.key dentro de /usr/local/apache2/conf/ y luego personalizar el /usr/local/apache2/conf/httpd.conf eliminando el símbolo de comentario de las siguientes líneas

```
...
#LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
...
#LoadModule ssl_module modules/mod_ssl.so
...
#Include conf/extra/httpd-ssl.conf
```

El archivo de configuración conf/extra/httpd-ssl.conf usará los archivos de certificado agregados previamente y le indicará al demonio que también escuche en el puerto 443. Hay que asegurarse de agregar también algo como -p 443:443 a la ejecución de su ventana acoplable para reenviar el puerto https.

Esto se logra con una línea sed como a la siguiente:

```
RUN sed -i \
                -e 's/^#\(Include .*httpd-ssl.conf\)/\1/' \
                -e 's/^#\(LoadModule .*mod_ssl.so\)/\1/' \
                -e 's/^#\(LoadModule .*mod_socache_shmcb.so\)/\1/' \
                conf/httpd.conf
```

5. Creación del certificado SSL

1. Asegúrese de que OpenSSL esté instalado y en su PATH.
2. Cree una clave privada RSA para su servidor Apache

```
$ openssl genrsa -des3 -out server.key 2048
$ openssl rsa -noout -text -in server.key

$ openssl rsa -in server.key -out server.key.unsecure
```

3. Cree una solicitud de firma de certificado (CSR) con la clave privada RSA del servidor

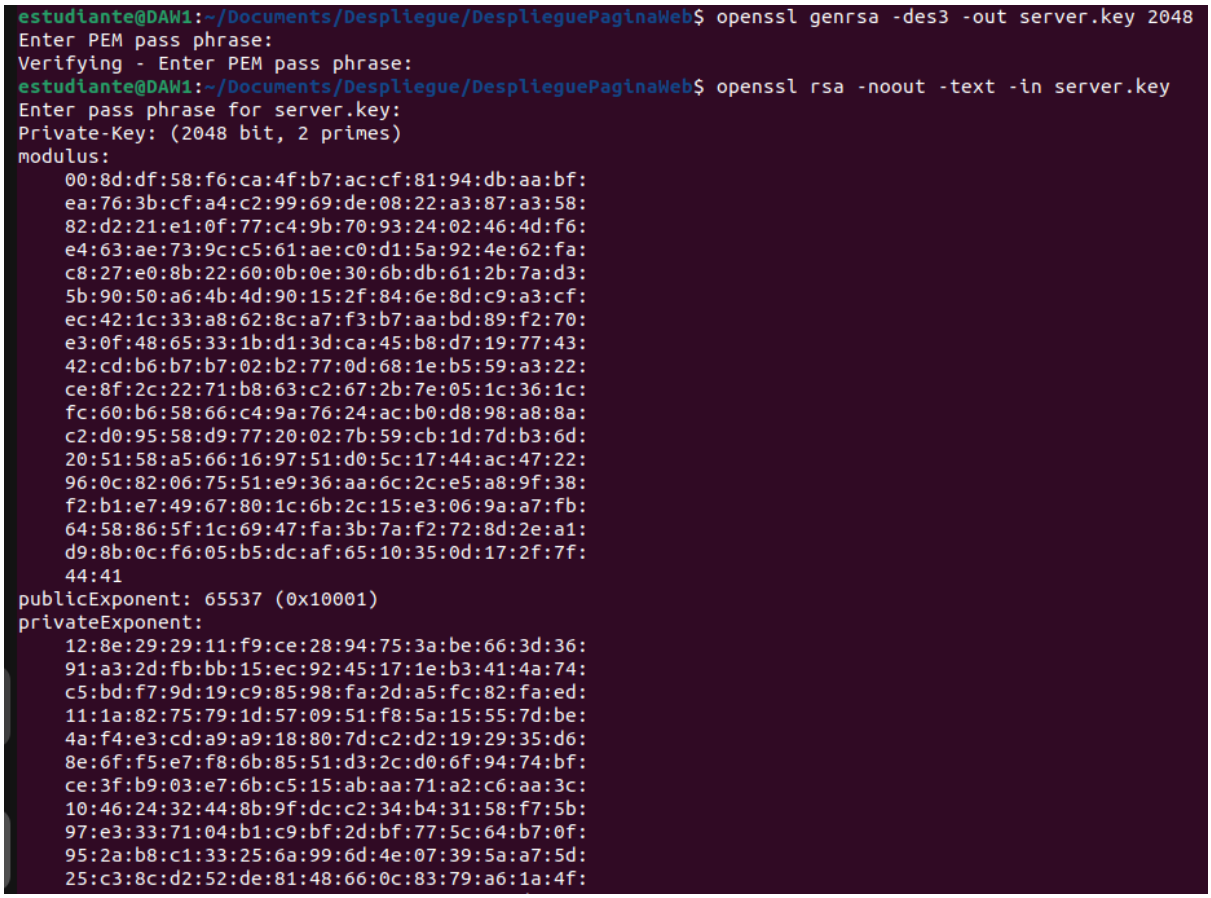
```
$ openssl req -new -key server.key -out server.csr

$ openssl req -noout -text -in server.csr
```

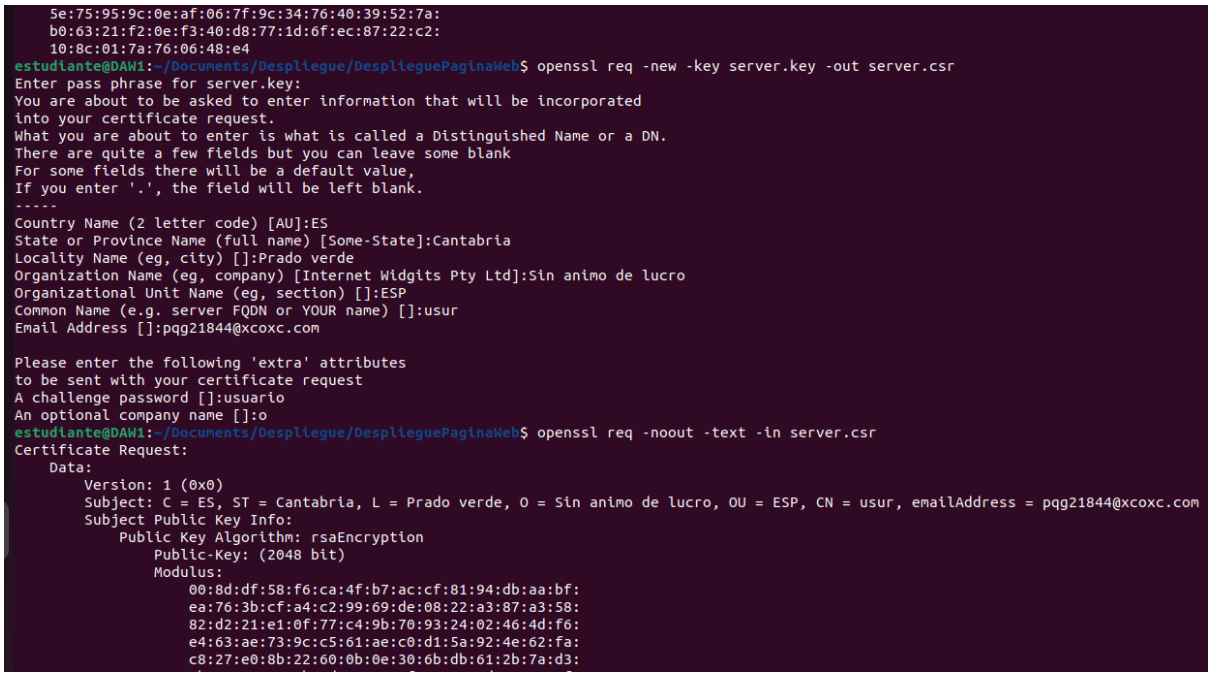
4. Ahora debe enviar esta Solicitud de firma de certificado (CSR) a una Autoridad de certificación (CA) para que la firme.

```
$ openssl x509 -noout -text -in server.crt
```

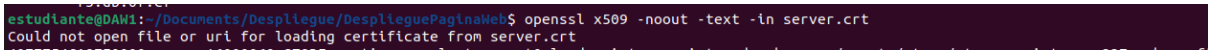
5. Ahora deberías tener dos archivos.

```
SSLCertificateFile    "/path/to/this/server.crt"
SSLCertificateKeyFile "/path/to/this/server.key"
```


estudiante@DAW1:~/Documents/Despliegue/DespliguePaginaWeb$ openssl genrsa -des3 -out server.key 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
estudiante@DAW1:~/Documents/Despliegue/DespliguePaginaWeb$ openssl rsa -noout -text -in server.key
Enter pass phrase for server.key:
Private-Key: (2048 bit, 2 primes)
modulus:
00:8d:df:58:f6:ca:4f:b7:ac:cf:81:94:db:aa:bf:
ea:76:3b:cf:a4:c2:99:69:de:08:22:a3:87:a3:58:
82:d2:21:e1:0f:77:c4:9b:70:93:24:02:46:4d:f6:
e4:63:ae:73:9c:c5:61:ae:c0:d1:5a:92:4e:62:fa:
c8:27:e0:8b:22:60:0b:0e:30:6b:db:61:2b:7a:d3:
5b:90:50:a6:4b:4d:90:15:2f:84:6e:8d:c9:a3:cf:
ec:42:1c:33:a8:62:8c:a7:f3:b7:aa:bd:89:f2:70:
e3:0f:48:65:33:1b:d1:3d:ca:45:b8:d7:19:77:43:
42:cd:b6:b7:b7:02:b2:77:0d:68:1e:b5:59:a3:22:
ce:8f:2c:22:71:b8:63:c2:67:2b:7e:05:1c:36:1c:
fc:60:b6:58:66:c4:9a:76:24:ac:b0:d8:98:a8:8a:
c2:d0:95:58:d9:77:20:02:7b:59:cb:1d:7d:b3:6d:
20:51:58:a5:66:16:97:51:d0:5c:17:44:ac:47:22:
96:0c:82:06:75:51:e9:36:aa:6c:2c:e5:a8:9f:38:
f2:b1:e7:49:67:80:1c:6b:2c:15:e3:06:9a:a7:fb:
64:58:86:5f:1c:69:47:fa:3b:7a:f2:72:8d:2e:a1:
d9:8b:0c:f6:05:b5:dc:af:65:10:35:0d:17:2f:7f:
44:41
publicExponent: 65537 (0x10001)
privateExponent:
12:8e:29:29:11:f9:ce:28:94:75:3a:be:66:3d:36:
91:a3:2d:fb:bb:15:ec:92:45:17:1e:b3:41:4a:74:
c5:bd:f7:9d:19:c9:85:98:fa:2d:a5:fc:82:fa:ed:
11:1a:82:75:79:1d:57:09:51:f8:5a:15:55:7d:be:
4a:f4:e3:cd:a9:a9:18:80:7d:c2:d2:19:29:35:d6:
8e:6f:f5:e7:f8:6b:85:51:d3:2c:d0:6f:94:74:bf:
ce:3f:b9:03:e7:6b:c5:15:ab:aa:71:a2:c6:aa:3c:
10:46:24:32:44:8b:9f:dc:c2:34:b4:31:58:f7:5b:
97:e3:33:71:04:b1:c9:bf:2d:bf:77:5c:64:b7:0f:
95:2a:b8:c1:33:25:6a:99:6d:4e:07:39:5a:a7:5d:
25:c3:8c:d2:52:de:81:48:66:0c:83:79:a6:1a:4f:


5e:75:95:9c:0e:af:06:7f:9c:34:76:40:39:52:7a:
b0:63:21:f2:0e:f3:40:d8:77:1d:6f:ec:87:22:c2:
10:8c:01:7a:76:06:48:e4
estudiante@DAW1:~/Documents/Despliegue/DespliguePaginaWeb$ openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:
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]:Cantabria
Locality Name (eg, city) []:Prado verde
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Sin animo de lucro
Organizational Unit Name (eg, section) []:ESP
Common Name (e.g. server FQDN or YOUR name) []:usur
Email Address []:pqg21844@xcoxc.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:usuario
An optional company name []:o
estudiante@DAW1:~/Documents/Despliegue/DespliguePaginaWeb$ openssl req -noout -text -in server.csr
Certificate Request:
Data:
Version: 1 (0x0)
Subject: C = ES, ST = Cantabria, L = Prado verde, O = Sin animo de lucro, OU = ESP, CN = usur, emailAddress = pqg21844@xcoxc.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:8d:df:58:f6:ca:4f:b7:ac:cf:81:94:db:aa:bf:
ea:76:3b:cf:a4:c2:99:69:de:08:22:a3:87:a3:58:
82:d2:21:e1:0f:77:c4:9b:70:93:24:02:46:4d:f6:
e4:63:ae:73:9c:c5:61:ae:c0:d1:5a:92:4e:62:fa:
c8:27:e0:8b:22:60:0b:0e:30:6b:db:61:2b:7a:d3:


estudiante@DAW1:~/Documents/Despliegue/DespliguePaginaWeb$ openssl x509 -noout -text -in server.crt
Could not open file or uri for loading certificate from server.crt

Damos permiso para que el navegador acceda