

SWAP: Asegurar la granja web

David Cabezas Berrido

dxabezas@correo.ugr.es

27 de abril de 2021

Índice

1. Instalar un certificado SSL autofirmado para configurar el acceso por HTTPS

2

1. Instalar un certificado SSL autofirmado para configurar el acceso por HTTPS

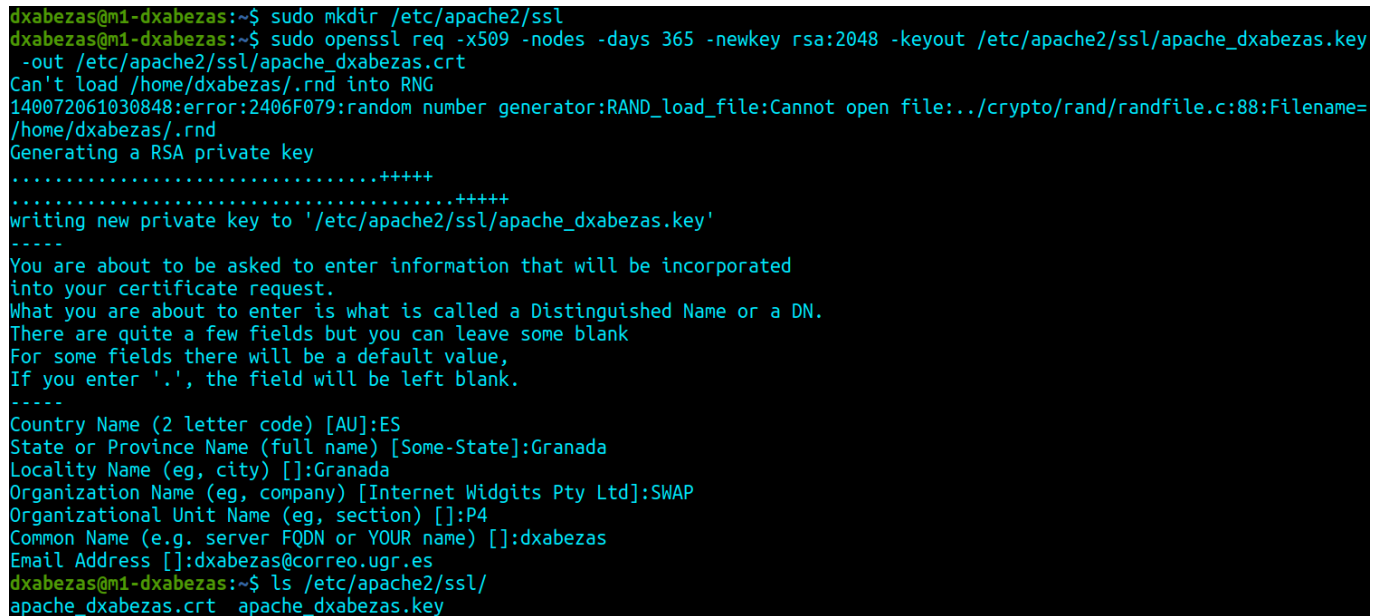
Para habilitar el módulo SSL de Apache2, ejecutamos la siguiente línea.

```
sudo a2enmod ssl
```

Habilita el módulo y sus dependencias. Salida:

```
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
systemctl restart apache2
```

Restauramos el servicio con `sudo systemctl restart apache2`. Ahora creamos una carpeta para los certificados de Apache, y creamos un par de clave y certificado. Le ponemos longitud de clave 2048 bits y 365 de validez.



```
dxabezas@n1-dxabezas:~$ sudo mkdir /etc/apache2/ssl
dxabezas@n1-dxabezas:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache_dxabezas.key -out /etc/apache2/ssl/apache_dxabezas.crt
Can't load /home/dxabezas/.rnd into RNG
140072061030848:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:88:Filename=
/home/dxabezas/.rnd
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/apache2/ssl/apache_dxabezas.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]:Granada
Locality Name (eg, city) []:Granada
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SWAP
Organizational Unit Name (eg, section) []:P4
Common Name (e.g. server FQDN or YOUR name) []:dxabezas
Email Address []:dxabezas@correo.ugr.es
dxabezas@n1-dxabezas:~$ ls /etc/apache2/ssl/
apache_dxabezas.crt  apache_dxabezas.key
```

Figura 1: Rellenamos los datos del certificado como se indica en el guión. Comprobamos que se ha creado el par correctamente.

Como opciones avanzadas comentamos que `-x509` auto-firma el certificado, se obtendría una solicitud de certificado si no usásemos esta opción. Además, la opción

`-subj /C=TheCountry/CN=theCommonName/ST=theState/O=theOrganization/...` permite especificar los datos desde la orden, pueden consultarse las abreviaturas en [este post](#) se encuentran los distintos atributos y sus abreviaturas.

Ahora modificamos el fichero de configuración `/etc/apache2/sites-available/default-ssl.conf`, tenemos que tener el siguiente bloque (`SSLEngine` on ya estaba puesto).

```
# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on
```

```
SSLCertificateFile /etc/apache2/ssl/apache_dxabezas.crt
SSLCertificateKeyFile /etc/apache2/ssl/apache_dxabezas.key
```

También tenemos que comentar las líneas que sobrescriben estas directivas más abajo. Guardamos los cambios y ejecutamos

```
a2ensite default-ssl
service apache2 reload
```

Cuando accedemos a la página, nos avisa de que es insegura porque el certificado es auto-firmado. Debemos permitir la excepción en el navegador o añadir `-k` con `curl`. Si le damos al candado junto a la dirección y a **More Information**, podemos visualizar el certificado que hemos creado.

Certificate	
dxabezas	
Subject Name	
Country	ES
State/Province	Granada
Locality	Granada
Organization	SWAP
Organizational Unit	P4
Common Name	dxabezas
Email Address	dxabezas@correo.ugr.es
Issuer Name	
Country	ES
State/Province	Granada
Locality	Granada
Organization	SWAP
Organizational Unit	P4
Common Name	dxabezas
Email Address	dxabezas@correo.ugr.es

Figura 2: Certificado con los datos que hemos creado.

Como opciones avanzadas, mostramos como obtener el certificado sin ayuda del navegador, con `openssl`:

```
openssl s_client -connect 192.168.56.101:443 -showcerts
```

También hay varias opciones adicionales en la configuración de Apache2 SSL. Se activan con

```
SSLOptions +opcion1 +opcion2
```

Por ejemplo, cuando se trabaja con autenticación y se requiere que los clientes también tengan certificados, la opción `FakeBasicAuth` requiere que los clientes pongan el campo Subject the su certificado como usuario, la contraseña siempre es la misma: “xxj31ZMTZzkVA” (que es una encriptación por DES de la palabra “password”), por ello el nombre de Fake.