Actividad Apache. SSL y conexiones seguras

1. A partir de la documentación de la guía online UsuarioDebian: Servidor web Apache2 + SSL Auto-firmado (https), se pide crear un certificado SSL “auto firmado” (es decir, nosotros mismos establecemos la validez del certificado sin necesidad de que lo haga un organismo externo)

   NOTA: en la creación del fichero server.csr (solicitud o pedido de certificación) con el comando openssl, deben completarse los valores del certificado con datos del país, provincia, organización, nombre completo del servidor (como www.dominio.org), etc.., que podamos reconocer posteriormente cuando veamos el certificado en el navegador web

2. Una vez creados los ficheros server.key y server.crt deben copiarse respectivamente en las carpetas /etc/ssl/private y /etc/ssl/certs

3. A continuación deben activarse en Apache el modulo “ssl” y activarse también el host virtual seguro “default-ssl”. Tras ello, reiniciaremos apache

4. Deben indicarse en el host virtual default-ssl de Apache las rutas de los ficheros del certificado que copiamos en el apartado 2. Se muestra captura:

```
SSLCertificateFile      /etc/ssl/certs/server.crt
SSLCertificateKeyFile /etc/ssl/private/server.key
```

5. Finalmente debe verificarse el certificado accediendo a https://www.dominio.org y mostrar también el contenido del certificado

Resolver

Los 3 pasos en teoría

-Activar el módulo de certificación SSL

-Activar un sitio que se llama “defaultssl”

Las conexiones SSL pasan por el puerto 443

Configurar un certificado (guía en Web)

usar una directiva de redirección para dirigir el trafico de http a https

```
alumno@debian11:~$ su -
Contraseña:
root@debian11:~# cd /etc/apache2
root@debian11:/etc/apache2# ls
apache2.conf    conf-enabled  grupos  mods-available  passwords   sites-available
conf-available  envvars       magic   mods-enabled    ports.conf  sites-enabled
root@debian11:/etc/apache2# a2enmodssl
-bash: a2enmodssl: orden no encontrada
root@debian11:/etc/apache2# a2enmod ssl
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
root@debian11:/etc/apache2# S
```

Uso a2enmod para habilitar importante reiniciar después con service apache2 restart

```
1]+  Detenido                service apache2 status
oot@debian11:/etc/apache2# cd sites-available
oot@debian11:/etc/apache2/sites-available# nano default-ssl.conf


se «fg» para volver a nano.

2]+  Detenido                nano default-ssl.conf
oot@debian11:/etc/apache2/sites-available# S
```

No ha hace falta Modificar este archivo porque este el que tiene el puerto de la conexión segura, solo hay que activarlo

```
root@debian11:/etc/apache2/sites-available# a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@debian11:/etc/apache2/sites-available# S
```

Como esta en la carpeta de sitios le haces un a2ensite available importante reiniciar

```
root@debian11:/etc/apache2/sites-available# apt-get install openssl ca-certificates
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
ca-certificates ya está en su versión más reciente (20210119).
Se actualizarán los siguientes paquetes:
  openssl
1 actualizados, 0 nuevos se instalarán, 0 para eliminar y 352 no actualizados.
Se necesita descargar 0 B/859 kB de archivos.
Se utilizarán 6.144 B de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
Leyendo lista de cambios... Hecho.
(Leyendo la base de datos ... 163488 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../openssl_1.1.1w-0+deb11u4_amd64.deb ...
Desempaquetando openssl (1.1.1w-0+deb11u4) sobre (1.1.1n-0+deb11u3) ...
Configurando openssl (1.1.1w-0+deb11u4) ...
Procesando disparadores para man-db (2.9.4-2) ...
root@debian11:/etc/apache2/sites-available#
```

Sigue la guía (link del princicipio) en el paso 4 para instalar el comando openssl no confundir con modulo ssl

Luego creo y entro a la carpeta de certs

```
root@debian11:/etc/apache2/sites-available# mkdir certs
root@debian11:/etc/apache2/sites-available# cd certs
root@debian11:/etc/apache2/sites-available/certs#
```

```
root@debian11:/etc/apache2/sites-available/certs# openssl genrsa -out server.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
....+++++
e is 65537 (0x010001)
root@debian11:/etc/apache2/sites-available/certs#
```

Genero la clave virtual en la carpeta de certs

```
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
....+++++
e is 65537 (0x010001)
root@debian11:/etc/apache2/sites-available/certs# chmod 600 server.key
```

Le damos permisos a la server key para que sea accesible por el usuario

```
root@debian11:/etc/apache2/sites-available/certs# openssl req -new -key server.key -out server.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]:Oviedo
Locality Name (eg, city) []:Oviedo
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Naranco
Organizational Unit Name (eg, section) []:DAW
Common Name (e.g. server FQDN or YOUR name) []:128.0.0.1
Email Address []:
```

```
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]:Oviedo
Locality Name (eg, city) []:Oviedo
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Naranco
Organizational Unit Name (eg, section) []:DAW
Common Name (e.g. server FQDN or YOUR name) []:128.0.0.1
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@debian11:/etc/apache2/sites-available/certs# LS -L
-bash: LS: orden no encontrada
root@debian11:/etc/apache2/sites-available/certs# ls
server.csr  server.key
root@debian11:/etc/apache2/sites-available/certs# S
```

Relleno con los datos pedidos

```
root@debian11:/etc/apache2/sites-available/certs# openssl x509 -req -days 365 -in server.csr -signkey serv
er.key -out server.crt
Signature ok
subject=C = ES, ST = Oviedo, L = Oviedo, O = Naranco, OU = DAW, CN = 128.0.0.1
Getting Private key
root@debian11:/etc/apache2/sites-available/certs# S
```

Le doy un firmado por duración de 365 dias

```
root@debian11:/etc/apache2/sites-available/certs# cp server.key /etc/ssl/private
```

Aquí copio el archivo de key para la carpeta de /etc/ssl/private

```
root@debian11:/etc/apache2/sites-available/certs# cp server.crt /etc/ssl/certs
```

Aquí copio el archivo de certificado para /etc/ssl/certs

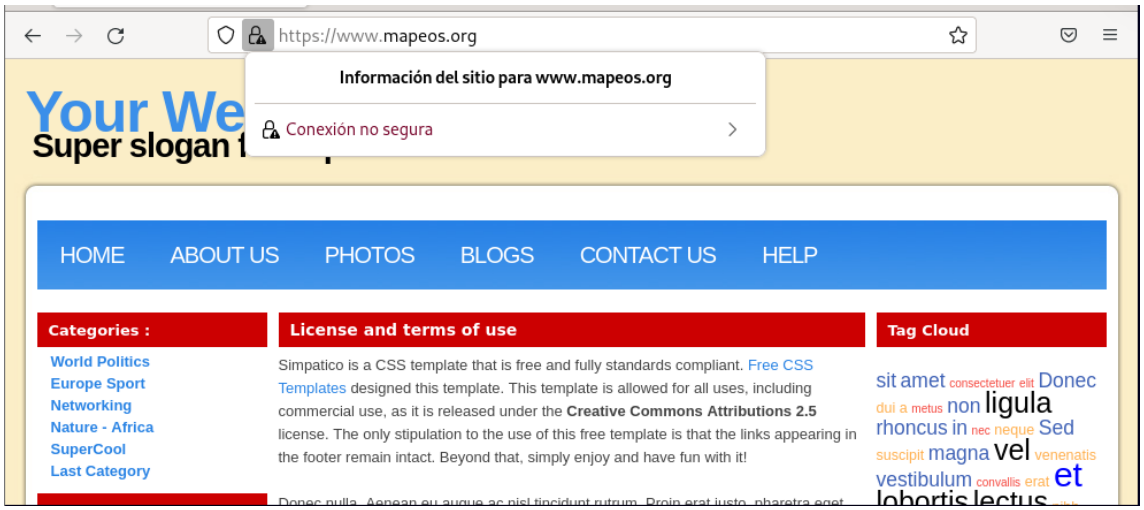
Como ya he copiado la crt y la key ingreso su nueva direccion

```
#   SSLCertificateFile directive is needed.
SSLCertificateFile      /etc/ssl/certs/server.crt
SSLCertificateKeyFile /etc/ssl/private/server.key
```

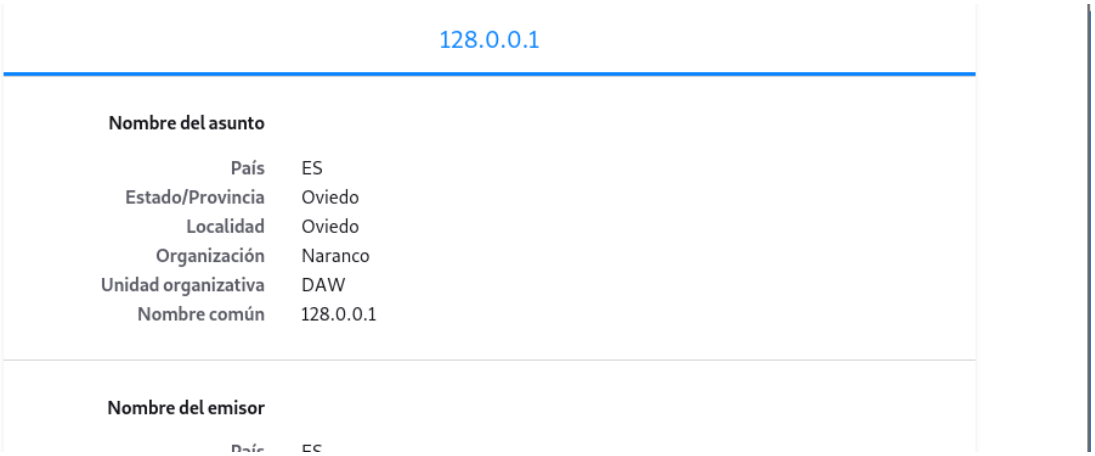
Finalmente reinicio el servidor

```
root@debian11:/etc/apache2/sites-available# service apache2 restart
```

Ahora Ya Funciona la dirección https en el servidor



Si entras a mas información te muestra el certificado



redirección automática

Con esa linea del redirect Permanent y reiniciar ya seria suficiente para que cuando escribamos el http a ese sitio redirija a https