HTTPS

Generar clave privada:

```
admindwes@OLP-USED:~$ openssl genrsa 2048 > clave.key
```

Generar solicitud de la firma a partir de la clave generada:

```
e is 65537 (0x010001)
admindwes@OLP-USED:~$ openssl req -new -key clave.key > clave.csr
```

Pedirá información sobre el servidor:

```
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Zamora
Locality Name (eg, city) []:Benavente
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Sauces
Organizational Unit Name (eg, section) []:DAW
Common Name (e.g. server FQDN or YOUR name) []:www.oscar.local
Email Address []:oscar.llapar@educa.jcyl.es
```

El apartado de contraseña se puede dejar vacío:

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Generar el certificado con el siguiente comando:

```
admindwes@OLP-USED:~$ openssl x509 -req -days 365 -in clave.csr -signkey clave.k
ey > clave.crt
Signature ok
subject=C = ES, ST = Zamora, L = Benavente, O = Sauces, OU = DAW, CN = www.oscar
.local, emailAddress = oscar.llapar@educa.jcyl.es
Getting Private key
admindwes@OLP-USED:~$
```

Los tres ficheros "clave" estarían generados:

```
admindwes@OLP-USED:~$ ls
clave.crt  clave.key
clave.csr  DAWDespliegueAplicacionesWeb
```

Activar el módulo de Apache SSL:

```
admindwes@OLP-USED:~$ sudo a2enmod ssl
```

Tras activarlo, reiniciar servidor:

```
admindwes@OLP-USED:~$ sudo service apache2 restart
```

Comprobar que el puerto 443, que pertenece a https esté abierto:

```
admindwes@OLP-USED:~$ ss -punta
Netid State   Recv-Q  Send-Q   Local Address:Port    Peer Address:Port  Process
udp   UNCONN  0       0        127.0.0.53%lo:53           0.0.0.0:*
tcp   LISTEN  0       151            0.0.0.0:3306         0.0.0.0:*
tcp   LISTEN  0       4096     127.0.0.53%lo:53           0.0.0.0:*
tcp   LISTEN  0       128            0.0.0.0:22           0.0.0.0:*
tcp   ESTAB   0       0        192.168.3.114:22      192.168.3.14:62740
tcp   LISTEN  0       511               *:80                 *:*
tcp   LISTEN  0       100               *:8080               *:*
tcp   LISTEN  0       128            [::]:22              [::]:*
tcp   LISTEN  0       511               *:443                *:*
tcp   LISTEN  0       70                *:33060              *:*
admindwes@OLP-USED:~$ ss -puta
Netid State  Recv-Q Send-Q  Local Address:Port       Peer Address:Port  Process
udp   UNCONN 0      0       127.0.0.53%lo:domain          0.0.0.0:*
tcp   LISTEN 0      151           0.0.0.0:mysql           0.0.0.0:*
tcp   LISTEN 0      4096    127.0.0.53%lo:domain          0.0.0.0:*
tcp   LISTEN 0      128           0.0.0.0:ssh             0.0.0.0:*
tcp   ESTAB  0      64      192.168.3.114:ssh       192.168.3.14:62740
tcp   LISTEN 0      511              *:http                *:*
tcp   LISTEN 0      100              *:http-alt            *:*
tcp   LISTEN 0      128           [::]:ssh              [::]:*
tcp   LISTEN 0      511              *:https               *:*
tcp   LISTEN 0      70               *:33060               *:*
admindwes@OLP-USED:~$
```

Mover la clave privada (.key) a /etc/ssl/private:

```
admindwes@OLP-USED:~$ sudo mv clave.key /etc/ssl/private
admindwes@OLP-USED:~$ sudo ls -l /etc/ssl/private
total 8
-rw-rw-r-- 1 admindwes admindwes 1675 feb 23 11:31 clave.key
-rw-r----- 1 root      ssl-cert  1704 oct  5 10:50 ssl-cert-snakeoil.key
admindwes@OLP-USED:~$
```

Cambio de permisos de la clave privada (propiedad de root:ssl-cert):

```
admindwes@OLP-USED:~$ sudo chown root:ssl-cert /etc/ssl/private/clave.key
admindwes@OLP-USED:~$ sudo chmod 640 /etc/ssl/private/clave.key
admindwes@OLP-USED:~$ sudo ls -l /etc/ssl/private
total 8
-rw-r----- 1 root ssl-cert 1675 feb 23 11:31 clave.key
-rw-r----- 1 root ssl-cert 1704 oct  5 10:50 ssl-cert-snakeoil.key
admindwes@OLP-USED:~$
```

Mover el certificado a /etc/ssl/certs:

```
admindwes@OLP-USED:~$ sudo mv clave.crt /etc/ssl/certs
admindwes@OLP-USED:~$ sudo ls -l /etc/ssl/certs | grep clave
-rw-rw-r-- 1 admindwes admindwes   1346 feb 23 11:37 clave.crt
admindwes@OLP-USED:~$
```

Cambiar propietario del certificado a root:

```
admindwes@OLP-USED:~$ sudo chown root:root /etc/ssl/certs/clave.crt
admindwes@OLP-USED:~$
```

En /etc/apache2/sites-available, crear un nuevo sitio ssl copiando el archivo default-ssl.conf y poniendo el nombre del sitio seguido de –ssl:

```
admindwes@OLP-USED:/etc/apache2/sites-available$ sudo cp default-ssl.conf
daw202-ssl.conf
```

Contenido del fichero creado:

```
<IfModule mod_ssl.c>
        <VirtualHost *:443>
                ServerName daw202.oscar.local
                ServerAlias www.daw202.oscar.local
                ServerAdmin daw202@oscar.local
                DocumentRoot /var/www/daw202/public_html

                # Available loglevels: trace8, ..., trace1, debug, info, notice,
                # error, crit, alert, emerg.
                # It is also possible to configure the loglevel for particular
                # modules, e.g.
                #LogLevel info ssl:warn

                ErrorLog ${APACHE_LOG_DIR}/error-daw202-ssl.log
                CustomLog ${APACHE_LOG_DIR}/access-daw202-ssl.log combined

                # For most configuration files from conf-available/, which are
                # enabled or disabled at a global level, it is possible to
                # include a line for only one particular virtual host. For examp
                # following line enables the CGI configuration for this host onl
                # after it has been globally disabled with "a2disconf".
                #Include conf-available/serve-cgi-bin.conf

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

                #   A self-signed (snakeoil) certificate can be created by insta
                #   the ssl-cert package. See
                #   /usr/share/doc/apache2/README.Debian.gz for more info.
                #   If both key and certificate are stored in the same file, onl
                #   SSLCertificateFile directive is needed.
                SSLCertificateFile      /etc/ssl/certs/clave.crt
                SSLCertificateKeyFile /etc/ssl/private/clave.key

                #   Server Certificate Chain:
                #   Point SSLCertificateChainFile at a file containing the
                #   concatenation of PEM encoded CA certificates which form the
                #   certificate chain for the server certificate. Alternatively
                #   the referenced file can be the same as SSLCertificateFile
                #   when the CA certificates are directly appended to the server
                #   certificate for convinience.
                #SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt
```

Activar el sitio ssl:

```
admindwes@OLP-USED:/etc/apache2/sites-available$ sudo a2ensite daw202-ssl.conf
Enabling site daw202-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
admindwes@OLP-USED:/etc/apache2/sites-available$
```

Reiniciar Apache:

```
admindwes@OLP-USED:/etc/apache2/sites-available$ systemctl reload apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to reload 'apache2.service'.
Authenticating as: admin (admindwes)
Password:
==== AUTHENTICATION COMPLETE ===
admindwes@OLP-USED:/etc/apache2/sites-available$
```

Entrada a la dirección por el navegador: