Contenido

HTTPS

Abrir el puerto 443:

Sudo ufw allow 443

openssl genrsa 2048 >daw201.key

openssl req -new -key daw201.key > daw201.csr

openssl x509 -req -days 365 -in daw201.csr -signkey daw201.key -out daw201.crt

copiar la clave privada a /etc/ssl/private

sudo cp daw201.key /etc/ssl/private

permisos 640

chmod 640 /etc/ssl/private/daw201.key

propietario root:ssl-cert

chown root:ssl-cert /etc/ssl/private/daw201.key

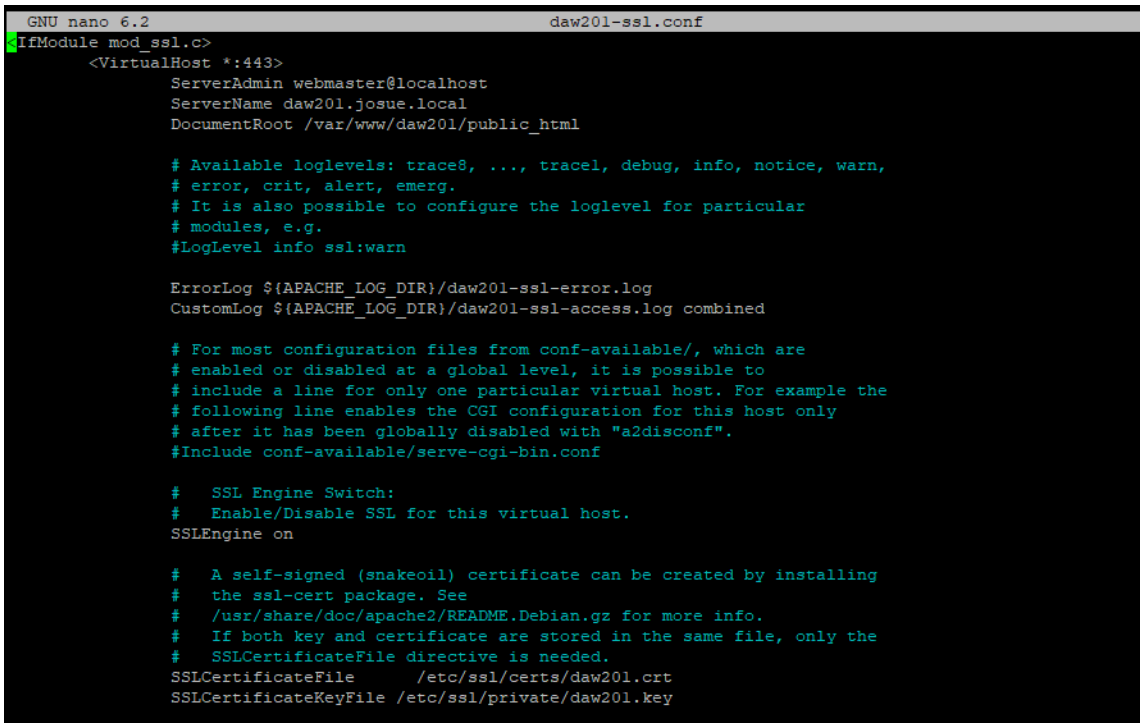
copiar el certificado a /etc/ssl/certs

sudo cp daw201.crt /etc/ssl/certs

copiar el archivo default-ssl.conf

sudo cp default-ssl.conf daw201-ssl.conf

editar el archivo:



Habilitar sitio y reiniciar apache.

Para redirigir de HTTP a HTTPS:

Habilitar el modulo REWRITE:

Sudo a2enmod rewrite

En el fichero apache2.conf para var/www cambiar la directiva AllowOverride de none a All

En el fichero .htaccess añadir las siguientes lineas:

RewriteEngine On

RewriteCond %{SERVER_PORT} 80

RewriteRule ^(.*)$ https://daw201.josue.local/$1 [R,L]

Autenticacion digest

Habilitar el modulo:

A2enmod auth_digest

Reiniciar apache…

Crear una carpeta en /var/www/daw201 llamada data

Sudo mkdir /var/www/daw201/data

Cambiar el propietario:

sudo chown -R daw201:www-data /var/www/daw201/data

Crear los usuarios con la web y guardarlos dentro de data en un archivo .usuarios

Crear un directorio nttdata dentro de pulic html (Con el usuario daw201):

Crear un archivo .htaccess dentro de nttdata

```
Options Indexes FollowSymLinks
AuthType Digest
AuthName "ntt" -> Grupo
AuthDigestProvider file
AuthUserFile /var/www/daw201/data/.usuarios -> Fichero
Require valid-user -> Cualquiera que este en el fichero
```

Creando grupos:

Crear un archivo .grupos al mismo nivel de .usuarios:

Dentro del fichero pegar:

jefeproyectos: jero

recursos: israel imelda

Dentro de .htaccess:

Require group jefeproyectos

AuthGroupFile /var/www/daw201/data/.grupos

Habilitar modulo:

Sudo a2enmod authz_groupfile