

Contenido

HTTPS.....	1
Autenticacion digest.....	2

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:

```
GNU nano 6.2                                daw201-ssl.conf
IfModule mod_ssl.c>
<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    ServerName daw201.josue.local
    DocumentRoot /var/www/daw201/public_html

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # 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}/daw201-ssl-error.log
    CustomLog ${APACHE_LOG_DIR}/daw201-ssl-access.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 example the
    # following line enables the CGI configuration for this host only
    # 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 installing
    #   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, only the
    #   SSLCertificateFile directive is needed.
    SSLCertificateFile      /etc/ssl/certs/daw201.crt
    SSLCertificateKeyFile   /etc/ssl/private/daw201.key
```

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
```