Sitio web seguro

David Aparicio Sir

Despliegue de Aplicaciones Web

Generamos la Clave privada

```
miadmin@das-used:~$ openssl genrsa 2048 > david.key
```

Generamos el certificado

```
miadmin@das-used:~$ openssl req -new -key david.key > david.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]:Zamora
Locality Name (eg, city) []:Benavente
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IES Los Sauces
Organizational Unit Name (eg, section) []:Departamento de Informatica
Common Name (e.g. server FQDN or YOUR name) []:das-used.david.local
Email Address []:

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

```
miadmin@das-used:~$ ls -l
total 8
-rw-rw-r-- 1 miadmin miadmin 1119 ene 22 19:04 david.csr
-rw-rw-r-- 1 miadmin miadmin 1704 ene 22 19:02 david.key
```

Crear certificado autofirmado

```
miadmin@das-used:~$ openssl x509 -req -days 365 -in david.csr -signkey david.key > david.crt
Certificate request self-signature ok
subject=C = ES, ST = Zamora, L = Benavente, O = IES Los Sauces, OU = Departamento de Informatica, CN = das-used.david
.local
miadmin@das-used:~$ ls -l
total 12
-rw-rw-r-- 1 miadmin miadmin 1330 ene 22 19:12 david.crt
-rw-rw-r-- 1 miadmin miadmin 1119 ene 22 19:04 david.csr
-rw-rw-r-- 1 miadmin miadmin 1704 ene 22 19:02 david.key
```

Activamos el modulo ssl del servicio apache

```
miadmin@das-used:~$ sudo a2enmod ssl
[sudo] password for miadmin:
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
```

Movemos el fichero archivo.key al directorio /etc/ssl/private

```
miadmin@das-used:~$ sudo mv david.key /etc/ssl/private/david.key
```

Damos permisos 640 y propietario a root:ssl-cert

```
miadmin@das-used:~$ sudo chmod 640 /etc/ssl/private/david.key
miadmin@das-used:~$ sudo chown root:ssl-cert /etc/ssl/private/david.key
```

```
miadmin@das-used:~$ sudo ls -l /etc/ssl/private/ |grep david
-rw-r----- 1 root ssl-cert 1704 ene 22 19:02 david.key
```

Movemos el certificado al directorio /etc/ssl/certs

```
miadmin@das-used:~$ sudo mv david.crt /etc/ssl/certs/david.crt
```

Cambiamos el propietario del archivo a root

```
miadmin@das-used:~$ sudo chown root /etc/ssl/certs/david.crt
```

```
miadmin@das-used:~$ sudo ls -l /etc/ssl/certs/ |grep david
-rw-rw-r-- 1 root miadmin   1330 ene 22 19:12 david.crt
```

Copiamos el archivo /etc/apache2/sites-available/default-ssl.con y creamos un fichero llamado david.conf

```
miadmin@das-used:/etc/apache2/sites-available$ sudo cp default-ssl.conf david-ssl.conf
[sudo] password for miadmin:
```

Establecemos la direccion de la clave y de los certificados y donde redirigir el log de errores y de accesos

```
 GNU nano 6.2                                david-ssl.conf
                # It is also possible to configure the loglevel for particular
                # modules, e.g.
                #LogLevel info ssl:warn

                ErrorLog ${APACHE_LOG_DIR}/ssl-error.log
                CustomLog ${APACHE_LOG_DIR}/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/david.crt
                SSLCertificateKeyFile /etc/ssl/private/david.key
```

Configuramos el sitio

```
  GNU nano 6.2                                          david-ssl.conf *
<IfModule mod_ssl.c>
        <VirtualHost *:443>
                ServerAdmin webmaster@localhost

                DocumentRoot /var/www/html
```

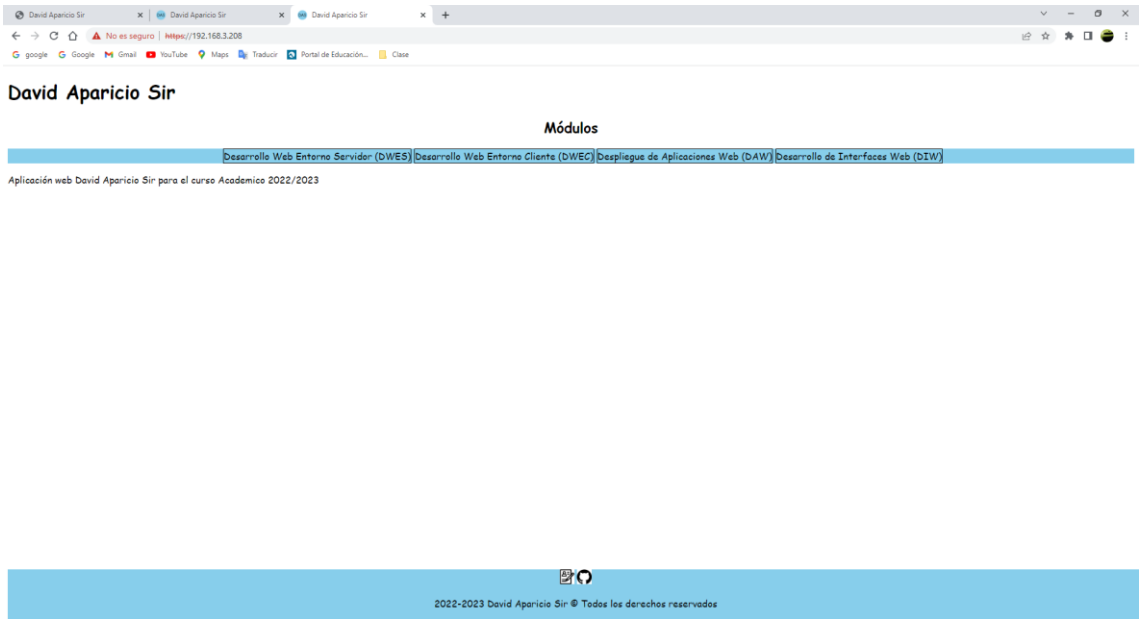
Activamos el sitio virtual

```
miadmin@das-used:/etc/apache2/sites-available$ sudo a2ensite david-ssl.conf
[sudo] password for miadmin:
Enabling site david-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

Reiniciamos el servicio apache2

```
miadmin@das-used:/etc/apache2/sites-available$ sudo service apache2 restart
miadmin@das-used:/etc/apache2/sites-available$ sudo apache2ctl -S
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'Se
rverName' directive globally to suppress this message
VirtualHost configuration:
*:443                  127.0.1.1 (/etc/apache2/sites-enabled/david-ssl.conf:2)
*:80                   is a NameVirtualHost
        default server 127.0.1.1 (/etc/apache2/sites-enabled/000-default.conf:1)
        port 80 namevhost 127.0.1.1 (/etc/apache2/sites-enabled/000-default.conf:1)
        port 80 namevhost daw201.david.local (/etc/apache2/sites-enabled/daw201.conf:1)
ServerRoot: "/etc/apache2"
Main DocumentRoot: "/var/www/html"
Main ErrorLog: "/var/log/apache2/error.log"
Mutex mpm-accept: using_defaults
Mutex watchdog-callback: using_defaults
Mutex ssl-stapling-refresh: using_defaults
Mutex ssl-stapling: using_defaults
Mutex ssl-cache: using_defaults
Mutex default: dir="/var/run/apache2/" mechanism=default
PidFile: "/var/run/apache2/apache2.pid"
Define: DUMP_VHOSTS
Define: DUMP_RUN_CFG
User: name="www-data" id=33
Group: name="www-data" id=33
```

Comprobamos



Hacer que siempre se utilice https

Activar el modulo rewrite

```
miadmin@das-used:/etc/apache2/sites-available$ sudo a2enmod rewrite
[sudo] password for miadmin:
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
miadmin@das-used:/etc/apache2/sites-available$ systemctl restart apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to restart 'apache2.service'.
Authenticating as: david (miadmin)
Password:
==== AUTHENTICATION COMPLETE ===
```

Desde el usuario operadorweb creamos el fichero .htaccess

```
miadmin@das-used:/var/www/html$ ls -l
total 48
drwxr-sr-x  6 operadorweb www-data 4096 dic 14 20:09 201DAWProyectoDAW
drwxr-sr-x 13 operadorweb www-data 4096 ene 21 13:45 201DWESLoginLogoff
drwxr-sr-x  5 operadorweb www-data 4096 ene 11 18:10 201DWESProyectoDWES
drwxr-sr-x  8 operadorweb www-data 4096 nov 30 16:15 201DWESProyectoLoginLogoffTema5
drwxr-sr-x  8 operadorweb www-data 4096 nov 22 17:15 201DWESProyectoTema3
drwxr-sr-x 10 operadorweb www-data 4096 dic  4 23:06 201DWESProyectoTema4
drwxr-sr-x  9 operadorweb www-data 4096 dic  4 23:05 201DWESProyectoTema5
drwxr-sr-x  3 operadorweb www-data 4096 nov  4 16:30 doc
drwxr-sr-x 11 operadorweb www-data 4096 oct 10 19:25 DWEC
-rw-r--r--  1 operadorweb www-data 1631 dic 14 19:05 index.html
drwxr-sr-x  2 operadorweb www-data 4096 nov  4 16:30 prueba
drwxr-sr-x  3 operadorweb www-data 4096 oct 10 17:24 webroot
miadmin@das-used:/var/www/html$ cat .htaccess
RewriteEngine On
RewriteCond %{SERVER_PORT} 80
RewriteRule^(.*)$
https://david.com/$1 [R,L]miadmin@das-used:/var/www/html$
```