

Servidor Web seguro



Índice


Generar clave privada.....	3
Datos de registro.....	3
Auto-firmado certificado.....	4
Activación módulo SSL de Apache.....	4
Edición ports.conf.....	5
Apertura de puertos y comprobación de status.....	5
Reinicio módulo apache2.....	6
Instalación certificado en el sitio virtual por defecto.....	6
Copia de los certificados en su directorio.....	7
Comprobación.....	7
Configuración del sitio virtual seguro.....	7
Copia de archivo default-ssl.conf.....	7
Edición de la copia daw201-ssl.conf.....	7
Activación del sitio virtual.....	8

SSL – Servidor Web seguro

Generar clave privada

La siguiente imagen muestra en primer lugar el comando necesario para generar la clave privada y en segundo lugar, un listado de directorios en el que se puede ver que efectivamente este archivo ha sido creado.

```
miadmin@RST-USED:~$ openssl genrsa 2048 > daw201.key
miadmin@RST-USED:~$ ll
total 56
drwxr-x--- 4 miadmin miadmin 4096 ene 12 09:41 ./
drwxr-xr-x 3 root    root    4096 sep 27 11:29 ../
-rw----- 1 miadmin miadmin 14945 ene 10 12:54 .bash_history
-rw-r--r-- 1 miadmin miadmin  220 ene  6 2022 .bash_logout
-rw-r--r-- 1 miadmin miadmin 3771 ene  6 2022 .bashrc
drwx----- 2 miadmin miadmin 4096 sep 27 11:29 .cache/
-rw-rw-r-- 1 miadmin miadmin 1704 ene 12 09:41 daw201.key
-rw----- 1 miadmin miadmin  20 ene 10 11:39 .lessht
-rw-rw-r-- 1 miadmin miadmin  0 dic  1 10:47 nslookup
-rw-r--r-- 1 miadmin miadmin  807 ene  6 2022 .profile
drwx----- 2 miadmin miadmin 4096 oct 27 10:21 .ssh/
-rw-r--r-- 1 miadmin miadmin 3439 oct 27 10:21 sshd_config
-rw-r--r-- 1 miadmin miadmin  0 sep 27 11:34 .sudo_as_admin_successful
```



Datos de registro

A continuación documento la solicitud de certificado y los datos que el sistema CSR solicita para concederlo.

En primer lugar hay que ejecutar la instrucción que aparece en la imagen.

```
miadmin@RST-USED:~$ openssl req -new -key daw201.key > daw201.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]:
```

Y continua el registro con el relleno de datos que queremos certificar.

En primer lugar introduciremos dos letras para especificar el país donde está ubicado el recurso a certificar. En segundo lugar se especifica la provincia, en tercero la ciudad, a continuación el nombre de la organización seguido por la sección dentro de esta, en sexto lugar el nombre común y por último una dirección de Email; se pueden añadir atributos 'extra' como un password y un nombre de compañía.

```

-----
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]:Instituto Educacion Secundaria Los Sauces
Organizational Unit Name (eg, section) []:Informatica y comunicaciones
Common Name (e.g. server FQDN or YOUR name) []:daw201.ricardo.local
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
miadmin@RST-USED:~$

```

Auto-firmado certificado

Como en este ejemplo no vamos a mandar nuestro registro a una entidad certificadora para que (valga la redundancia) nos lo certifique, voy a optar por auto-firmar el certificado con la siguiente instrucción. En esta instrucción se le indica el periodo de validez del certificado, así como los archivos con los datos del registro y de la clave.

```

miadmin@RST-USED:~$ openssl x509 -req -days 365 -in daw201.csr -signkey daw201.key -out daw201.crt
Certificate request self-signature ok
subject=C = ES, ST = Zamora, L = Benavente, O = Instituto Educacion Secundaria Los Sauces, OU = Informatica y comunicaciones, CN = daw201.ricardo.local

```

Repito operación para usuario daw202, quedando así registrados daw201 y daw202.

```

miadmin@RST-USED:~$ openssl x509 -req -days 365 -in daw201.csr -signkey daw202.key -out daw202.crt
Certificate request self-signature ok
subject=C = ES, ST = Zamora, L = Benavente, O = Instituto Educacion Secundaria Los Sauces, OU = Informatica y comunicaciones, CN = daw201.ricardo.local

```

Activación módulo SSL de Apache

```

miadmin@RST-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

```

El módulo SSL es quien permite cifrar la información entre navegador y servidor web proporcionando SSL v2/v3 y TLS v1 para Apache HTTP; se basa en OpenSSL para proporcionar la criptografía.

Edición ports.conf

En el siguiente archivo indicaremos los puertos a la escucha para el módulo SSL.

```
miadmin@RST-USED: ~  
GNU nano 6.2 /etc/apache2/ports.conf  
# If you just change the port or add more ports here, you will likely also  
# have to change the VirtualHost statement in  
# /etc/apache2/sites-enabled/000-default.conf  
  
Listen 80  
Listen 81  
<IfModule ssl_module>  
    Listen 443  
</IfModule>  
  
<IfModule mod_gnutls.c>  
    Listen 443  
</IfModule>  
  
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Apertura de puertos y comprobación de status.

```
miadmin@RST-USED:~$ sudo ufw allow 443  
Rule added  
Rule added (v6)  
miadmin@RST-USED:~$ sudo ufw status  
Status: active
```

To	Action	From
--	-----	----
22/tcp	ALLOW	Anywhere
80	ALLOW	Anywhere
9003	ALLOW	Anywhere
8080/tcp	ALLOW	Anywhere
81	ALLOW	Anywhere
53	ALLOW	Anywhere
443	ALLOW	Anywhere
22/tcp (v6)	ALLOW	Anywhere (v6)
80 (v6)	ALLOW	Anywhere (v6)
9003 (v6)	ALLOW	Anywhere (v6)
8080/tcp (v6)	ALLOW	Anywhere (v6)
81 (v6)	ALLOW	Anywhere (v6)
53 (v6)	ALLOW	Anywhere (v6)
443 (v6)	ALLOW	Anywhere (v6)

Reinicio módulo apache2

```
miadmin@RST-USED:~$ sudo systemctl restart apache2
```

Y comprobación de estado de apache2.

```
miadmin@RST-USED:~$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2023-01-12 09:59:14 UTC; 15s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 1519 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 1524 (apache2)
    Tasks: 6 (limit: 2238)
   Memory: 10.8M
      CPU: 48ms
   CGroup: /system.slice/apache2.service
           └─1524 /usr/sbin/apache2 -k start
             └─1525 /usr/sbin/apache2 -k start
               └─1526 /usr/sbin/apache2 -k start
                 └─1527 /usr/sbin/apache2 -k start
                   └─1528 /usr/sbin/apache2 -k start
                     └─1529 /usr/sbin/apache2 -k start
```

Instalación certificado en el sitio virtual por defecto.

Copiando ficheros por seguridad.

```
miadmin@RST-USED:~$ sudo cp *.key /etc/ssl/private
[sudo] password for miadmin:
```

Propietario será root y grupo ssl-cert.

```
miadmin@RST-USED:~$ sudo chown root:ssl-cert /etc/ssl/private/daw201.key
miadmin@RST-USED:~$ sudo chown root:ssl-cert /etc/ssl/private/daw202.key
```

En la siguiente imagen muestro los permisos originales, el cambio a permisos 640 y compruebo si se ha realizado correctamente.

```
miadmin@RST-USED:~$ sudo ls -l /etc/ssl/private
total 12
-rw-r--r-- 1 root ssl-cert 1704 ene 12 10:30 daw201.key
-rw-r--r-- 1 root ssl-cert 1704 ene 12 10:30 daw202.key
-rw-r----- 1 root ssl-cert 1704 oct 3 08:49 ssl-cert-snakeoil.key
miadmin@RST-USED:~$ sudo chmod 640 /etc/ssl/private/daw201.key
miadmin@RST-USED:~$ sudo chmod 640 /etc/ssl/private/daw202.key
miadmin@RST-USED:~$ sudo ls -l /etc/ssl/private
total 12
-rw-r----- 1 root ssl-cert 1704 ene 12 10:30 daw201.key
-rw-r----- 1 root ssl-cert 1704 ene 12 10:30 daw202.key
-rw-r----- 1 root ssl-cert 1704 oct 3 08:49 ssl-cert-snakeoil.key
miadmin@RST-USED:~$
```

Copia de los certificados en su directorio

```
sudo cp daw201.crt /etc/ssl/certs
sudo cp daw202.crt /etc/ssl/certs
```

Comprobación

```
miadmin@RST-USED:~$ ls -l /etc/ssl/certs | grep daw
-rw-r--r-- 1 root root 1407 ene 12 10:40 daw201.crt
-rw-r--r-- 1 root root 1407 ene 12 10:40 daw202.crt
```

Configuración del sitio virtual seguro.

Copia de archivo default-ssl.conf.

Situado en la siguiente ruta /etc/apache2/sites-available listo los archivos presentes y a continuación realizo una copia del archivo default-ssl.conf en el archivo daw201-ssl.conf.

Incluyo nuevo listado para comprobar si se ha realizado la copia.

```
miadmin@RST-USED:~$ cd /etc/apache2/sites-available
miadmin@RST-USED:/etc/apache2/sites-available$ ls -l
total 20
-rw-r--r-- 1 root root 1332 oct 25 11:24 000-default.conf
-rw-r--r-- 1 root root 1364 ene 10 11:48 daw201.conf
-rw-r--r-- 1 root root 1361 ene 10 11:49 daw202.conf
-rw-r--r-- 1 root root 6338 mar 23 2022 default-ssl.conf
miadmin@RST-USED:/etc/apache2/sites-available$ cp default-ssl.conf daw201-ssl.conf
cp: cannot create regular file 'daw201-ssl.conf': Permission denied
miadmin@RST-USED:/etc/apache2/sites-available$ sudo cp default-ssl.conf daw201-ssl.conf
miadmin@RST-USED:/etc/apache2/sites-available$ ls -l
total 28
-rw-r--r-- 1 root root 1332 oct 25 11:24 000-default.conf
-rw-r--r-- 1 root root 1364 ene 10 11:48 daw201.conf
-rw-r--r-- 1 root root 6338 ene 12 10:47 daw201-ssl.conf
-rw-r--r-- 1 root root 1361 ene 10 11:49 daw202.conf
-rw-r--r-- 1 root root 6338 mar 23 2022 default-ssl.conf
```

Edición de la copia daw201-ssl.conf

En la imagen señalo en rojo las líneas a ser editadas según se nos indica en el manual proporcionado como guía para esta instalación.

Serán las siguientes:

SSL Engine on

SSLCertificateFile /etc/ssl/certs/_____.crt

SSLCertificateKeyFile /etc/ssl/private/_____.key.

En ellas, hay que sustituir lo subrayado por los nombres de nuestros archivos .crt y .key

También subrayo en amarillo las líneas que contendrán otros datos que en caso de no coincidir con los deseados por nosotros, habremos de modificar.


```

GNU nano 0.2 daw201-ssl.conf
<IfModule mod_ssl.c>
    <VirtualHost *:443>
        ServerAdmin webmaster@localhost
        ServerName daw201.ricardo.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

```

Activación del sitio virtual.

Activación.

```

miadmin@RST-USED:/etc/apache2/sites-available$ sudo a2ensite daw201-ssl.conf
Enabling site daw201-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2

```

Recarga apache2. Nos pedirá autenticación y password, si los datos introducidos son correctos, nos lo anunciará con un "AUTHENTICATION COMPLETE".

```

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

```


Siguiente paso. Editar fichero /etc/apache2/sites-enabled/____-ssl.conf.

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo nano ../sites-enabled/daw201-ssl.conf
```

AÑADIR IMAGEN DE FICHERO /etc/apache2/sites-enabled/daw201-ssl.conf.
Buscar en qué máquina está.

Para forzar su habilitación y des-habilitación hay que introducir los siguientes comandos.
Deshabilitar daw201-ssl.conf y reiniciar apache2 para guardar cambios.

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo a2dissite daw201-ssl.conf
Site daw201-ssl disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
miadmin@RST-USED:/etc/apache2/sites-available$ systemctl reload apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to reload 'apache2.service'.
Authenticating as: rstuslimpia (miadmin)
Password:
==== AUTHENTICATION COMPLETE ====
```

Habilitar daw201-ssl.conf y reiniciar apache2 para guardar cambios.

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo a2ensite daw201-ssl.conf
Enabling site daw201-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
miadmin@RST-USED:/etc/apache2/sites-available$ systemctl reload apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to reload 'apache2.service'.
Authenticating as: rstuslimpia (miadmin)
Password:
==== AUTHENTICATION COMPLETE ====
```

A continuación, para comprobar su correcto funcionamiento, escribiremos una ruta en el navegador al sitio que hemos configurado para poder ser visitado como seguro encabezándola con HTTPS.
En mi caso <https://daw201.ricardo.local/>

AÑADIR IMAGEN DE CONSULTA A NAVEGADOR AQUÍ.

Secuencia completa de habilitación y reinicio de ficheros .conf.
Este paso se realizará por cada uno de los sitios que queramos habilitar.

```
miadmin@RST-USED:/etc/apache2/sites-available$ sudo a2ensite daw201-ssl.conf
Enabling site daw201-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2
miadmin@RST-USED:/etc/apache2/sites-available$ systemctl reload apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to reload 'apache2.service'.
Authenticating as: rstuslimpia (miadmin)
Password:
==== AUTHENTICATION COMPLETE ====
miadmin@RST-USED:/etc/apache2/sites-available$ sudo nano daw202.conf
miadmin@RST-USED:/etc/apache2/sites-available$ systemctl reload apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to reload 'apache2.service'.
Authenticating as: rstuslimpia (miadmin)
Password:
==== AUTHENTICATION COMPLETE ====
miadmin@RST-USED:/etc/apache2/sites-available$ sudo nano sites-enabled/daw201-ssl.conf
miadmin@RST-USED:/etc/apache2/sites-available$ sudo nano sites-enabled
/daw201-ssl.conf
miadmin@RST-USED:/etc/apache2/sites-available$ sudo nano ../sites-enabled/daw201-ssl.conf
miadmin@RST-USED:/etc/apache2/sites-available$ sudo a2dissite daw201-ssl.conf
Site daw201-ssl disabled.
To activate the new configuration, you need to run:
    systemctl reload apache2
miadmin@RST-USED:/etc/apache2/sites-available$ systemctl reload apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to reload 'apache2.service'.
Authenticating as: rstuslimpia (miadmin)
Password:
==== AUTHENTICATION COMPLETE ====
miadmin@RST-USED:/etc/apache2/sites-available$ sudo a2ensite daw201-ssl.conf
Enabling site daw201-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2
miadmin@RST-USED:/etc/apache2/sites-available$ systemctl reload apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to reload 'apache2.service'.
Authenticating as: rstuslimpia (miadmin)
Password:
==== AUTHENTICATION COMPLETE ====
miadmin@RST-USED:/etc/apache2/sites-available$
```

Este documento aún está en fase de edición. Cuando la versión sea definitiva, este mensaje no aparecerá.