

PRÁCTICA HTTPS



Http



Https

Miguel Ángel de la Rosa Leva

2 DAW 🌑

Índice

-PASO 1:.....	3
-PASO 2:.....	4
-PASO 3:.....	5
-PASO 4:.....	6
-PASO 5:.....	8
-PASO 6:.....	8
-PASO 7:.....	9

-PASO 1:

Instalación del módulo “SSL” (realizar previamente un “apt update& upgrade”)

```
root@ServerMroslev:~# apt install openssl
```

Activación del módulo “SSL”

```
root@ServerMroslev:~# a2enmod ssl
```

Reiniciamos Apache

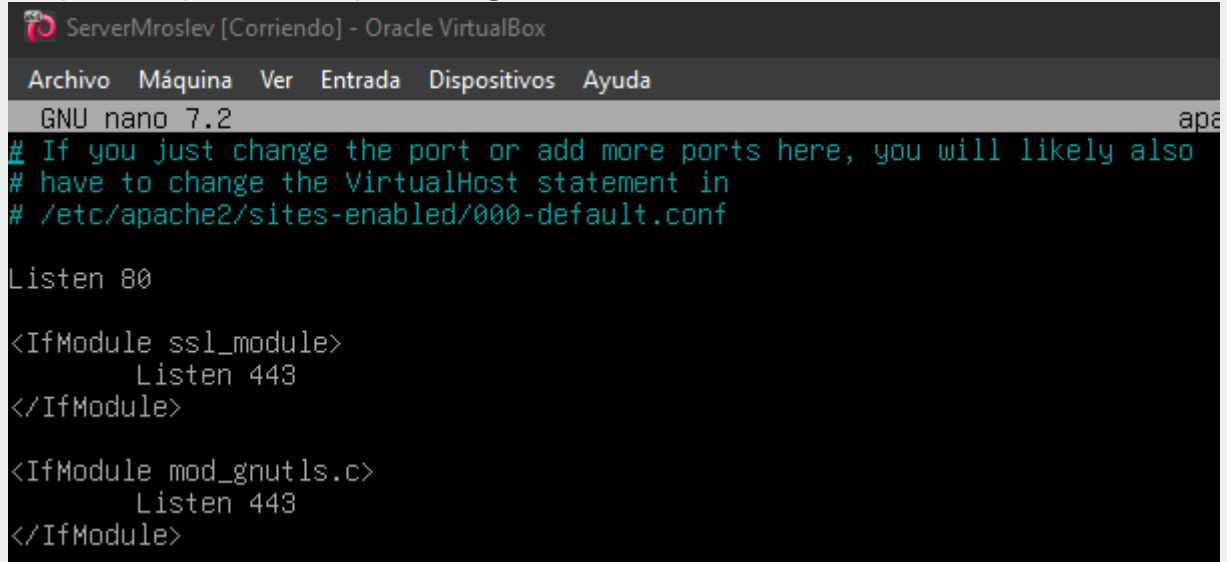
```
root@ServerMroslev:~# systemctl reload apache2
```

Ver módulos activados: (apache2ctl - M --> Listado de módulos activos)

```
root@ServerMroslev:~# apache2ctl -M
AH00557: apache2: apr_sockaddr_info_get() failed for ServerMroslev
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this message
Loaded Modules:
  core_module (static)
  so_module (static)
  watchdog_module (static)
  http_module (static)
  log_config_module (static)
  logio_module (static)
  version_module (static)
  unixd_module (static)
  access_compat_module (shared)
  alias_module (shared)
  auth_basic_module (shared)
  authn_core_module (shared)
  authn_file_module (shared)
  authz_core_module (shared)
  authz_groupfile_module (shared)
  authz_host_module (shared)
  authz_user_module (shared)
  autoindex_module (shared)
  deflate_module (shared)
  dir_module (shared)
  env_module (shared)
  filter_module (shared)
  mime_module (shared)
  mpm_event_module (shared)
  negotiation_module (shared)
  reqtimeout_module (shared)
  setenvif_module (shared)
  socache_shmcb_module (shared)
  ssl_module (shared)
  status_module (shared)
```


-PASO 3:

El puerto 433 debe estar activo a la escucha. Consultar el archivo /etc/apache2/ports.conf para asegurarnos.



```
ServerMroslev [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 7.2
# 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

<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>
```

Como podemos ver el puerto 433 esta activo a la escucha en el archivo de ports.conf.

-PASO 4:

Usaremos como plantilla el host virtual para https por defecto que trae apache

Haremos copia de /etc/apache2/sites-available/default-ssl.conf

```
root@ServerMroslev:/etc/apache2/sites-available# cp default-ssl.conf websegura.conf
```

En este ejemplo hemos creado un archivo llamado websegura.conf que debe quedar mas o menos así (sólo se han modificado las líneas resaltadas).

```
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
ServerAdmin webmaster@websegura.com
ServerName www.websegura.com

DocumentRoot /var/www/websegura
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
SSLEngine on
# SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
# SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
SSLCertificateFile /ruta/certificado.crt
SSLCertificateKeyFile /ruta/clave.key

<FilesMatch "\.(cgi|shtml|phtml|php)$">
SSLOptions +StdEnvVars
</FilesMatch>

<Directory /usr/lib/cgi-bin>
SSLOptions +StdEnvVars
</Directory>

BrowserMatch "MSIE [2-6]" \
nokeepalive ssl-unclean-shutdown \
downgrade-1.0 force-response-1.0
BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown

</VirtualHost>
</IfModule>
```

```
ServerMroslev [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 7.2 websegura.conf
<VirtualHost *:443>
    ServerAdmin webmaster@websegura.com
    ServerName www.websegura.com

    DocumentRoot /var/www/websegura

    # 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}/error.log
    CustomLog ${APACHE_LOG_DIR}/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/ssl-cert-snakeoil.pem
    SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
```

-PASO 5:

En la carpeta definida en el parámetro DocumentRoot

```
root@ServerMroslev:/var/www/html# mkdir websegura
root@ServerMroslev:/var/www/html# cd websegura/
root@ServerMroslev:/var/www/html/websegura# nano index.html_
```

-PASO 6:

sudo a2ensite websegura.conf

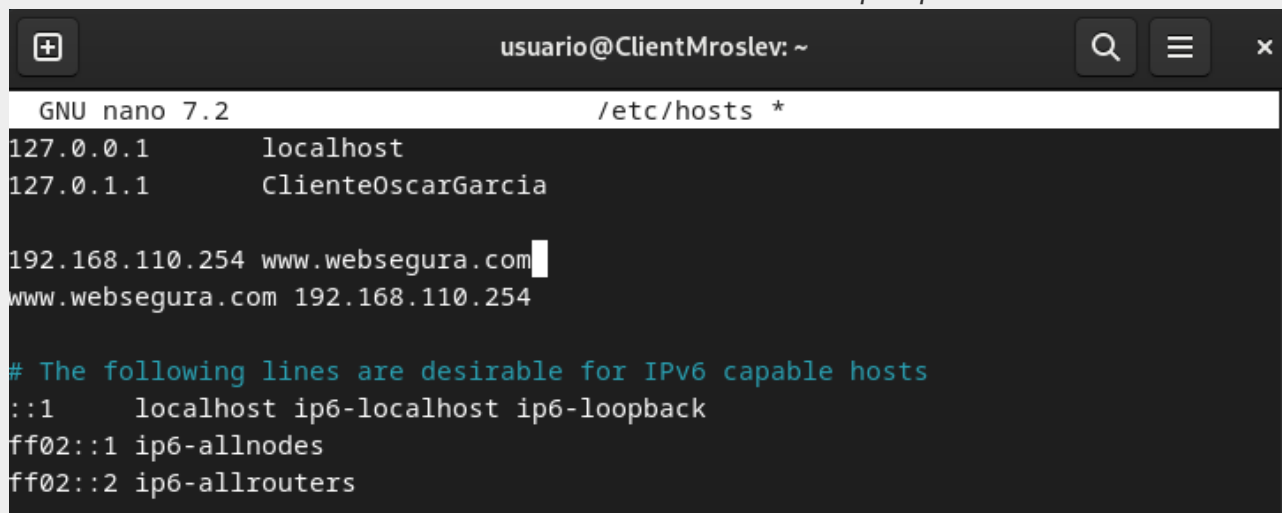
```
root@ServerMroslev:/etc/apache2/sites-available# a2ensite websegura.conf
Enabling site websegura.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

sudo service apache2 restart (reload)

```
root@ServerMroslev:/etc/apache2/sites-available# systemctl reload apache2
```


-PASO 7:

Introducir las resoluciones DNS directas necesarias en /etc/hosts



```
GNU nano 7.2 /etc/hosts *
127.0.0.1    localhost
127.0.1.1    ClienteOscarGarcia

192.168.110.254 www.websegura.com
www.websegura.com 192.168.110.254

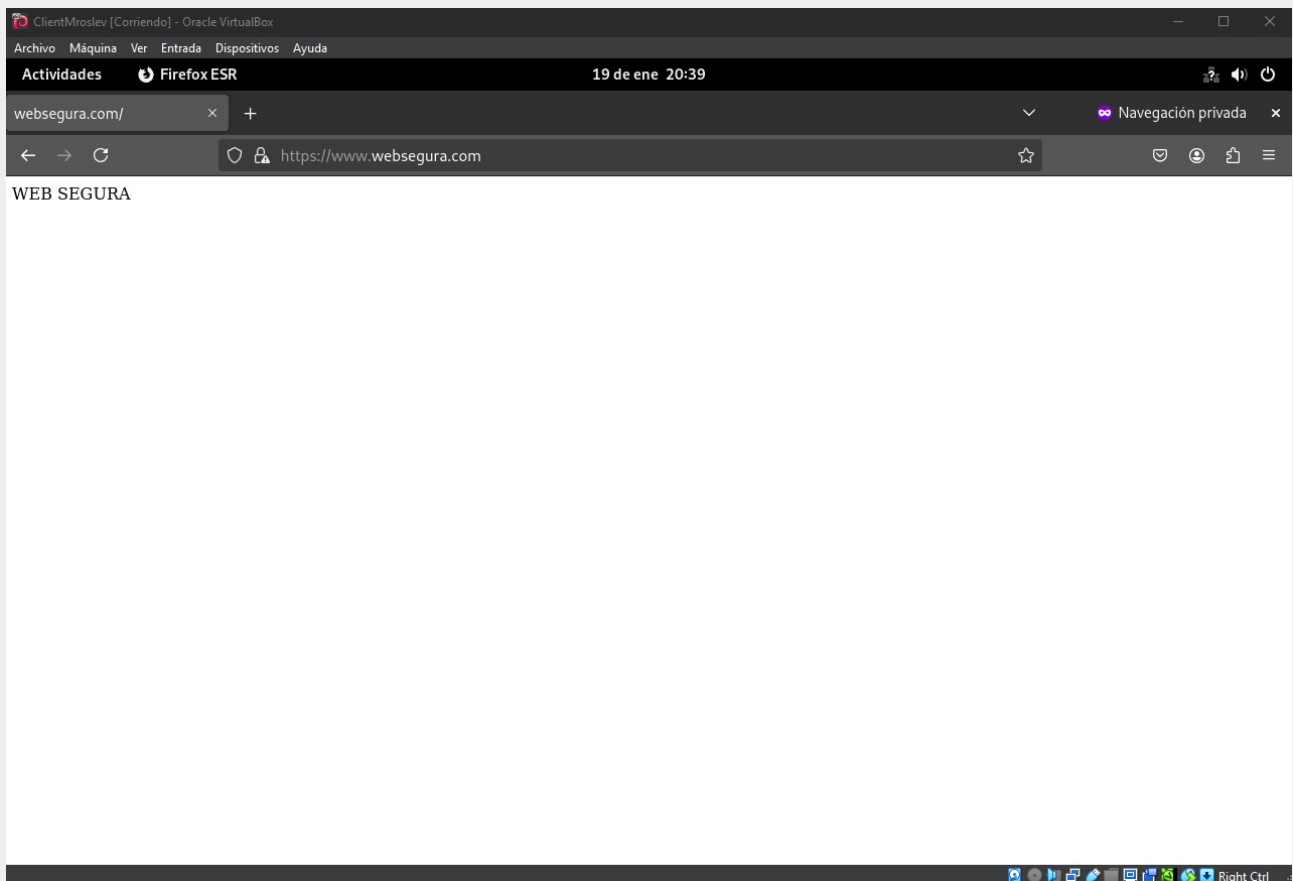
# The following lines are desirable for IPv6 capable hosts
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
```

Usar el navegador con el protocolo seguro <https://www.websegura.com>

Debe pedirnos aceptación del certificado la primera vez.

Esto se debe a que es un certificado auto-firmado creado por nosotros y las autoridades de certificación no lo tienen en su base de datos

Como medida de seguridad el navegador nos indica que aceptemos nosotros por nuestra cuenta y riesgo la validez del certificado.



Como podemos ver después de aceptar el certificado como seguro, nos redirige correctamente a la web, pero con este mensaje de seguridad

