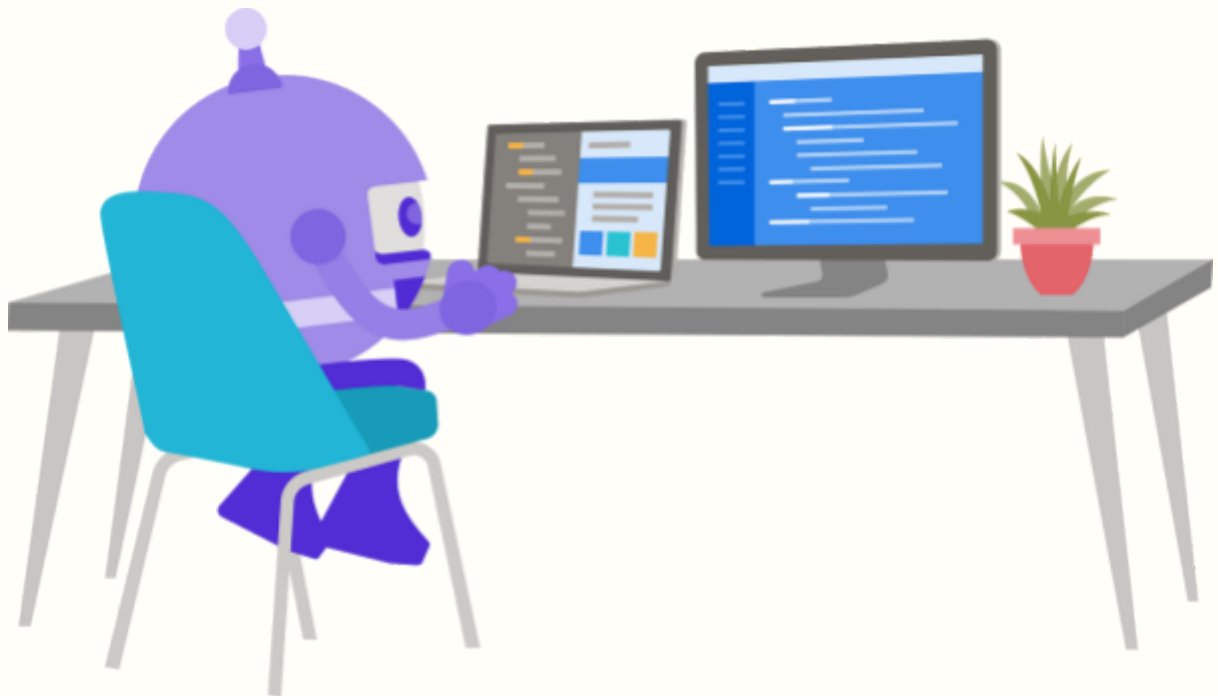


# *Seguridad Apache*



<b>Objetivos.....</b>	<b>3</b>
<b>Información básica / Preparación.....</b>	<b>3</b>
<b>Condiciones de entrega.....</b>	<b>3</b>
<b>Desarrollo.....</b>	<b>3</b>
Paso 1: Activar el módulo SSL.....	4
Paso 2: Puerto seguro.....	6
Paso 3: Crear host virtual.....	7
Paso 4: Instalar OpenSSL.....	11
Paso 5: Generar el certificado autofirmado y su clave.....	12
Paso 6: Modificar fichero de configuración de servidor seguro.....	16
Paso 7: Aplicar cambios.....	18
Paso 8: Comprobar funcionamiento.....	19
Paso 9: Comprobar que el certificado es el correcto.....	20

## Objetivos

- Instalar servidor HTTPs
- Configurar servidor HTTPs

## Información básica / Preparación

Este laboratorio se llevará a cabo individualmente con la ayuda de uno de tus compañeros en las partes que se te indique.

Se necesitan los siguientes recursos:

- Una computadora con Linux Ubuntu
- Al menos una computadora con Windows

## Condiciones de entrega

Debes entregar un documento dónde se indique los pasos dados para llevar a cabo la tarea expuesta.

## Desarrollo

## Paso 1: Activar el módulo SSL

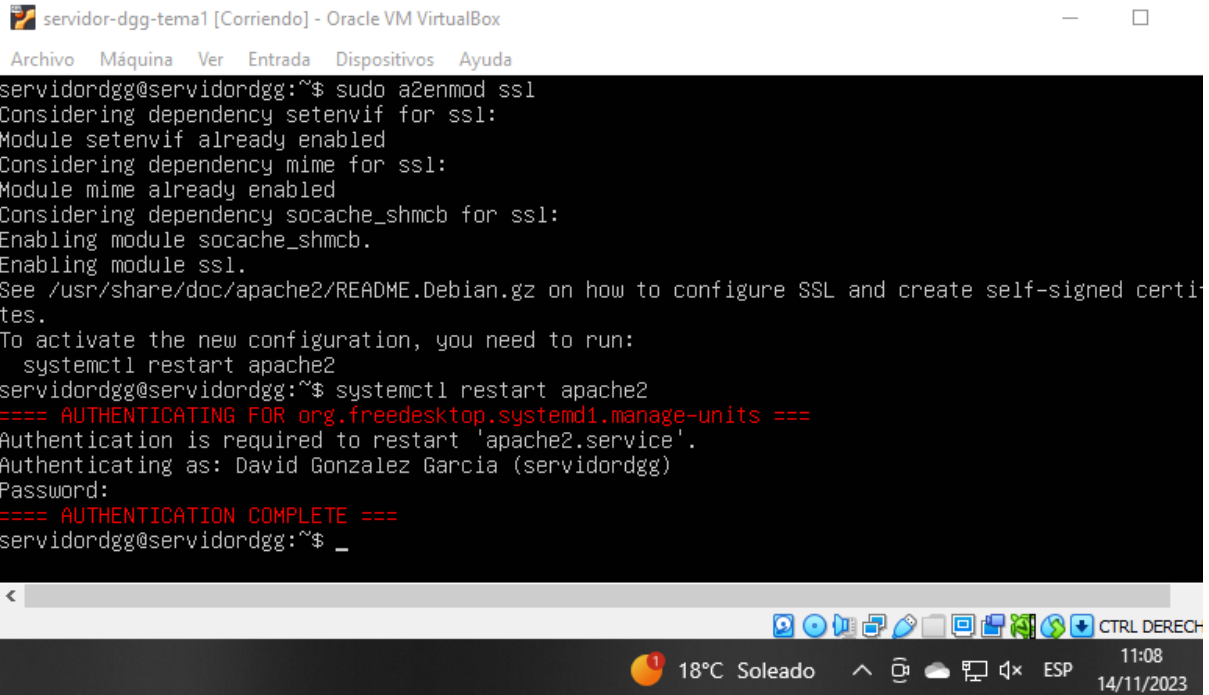
Activar el módulo SSL de Apache.

```
linuxserver@servidordaw: ~  
linuxserver@servidordaw:~$ sudo a2enmod ssl  
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 s  
elf-signed certificates.  
To activate the new configuration, you need to run:  
    systemctl restart apache2  
linuxserver@servidordaw:~$
```

Con Webmin, se podría activar el módulo en

The screenshot shows the Webmin interface for 'Servidor Web Apache' (Apache version 2.4.29). The left sidebar shows the 'Servidores' (Servers) menu with 'Servidor Web Apache' selected. The main panel shows the 'Configurar módulos de Apache' (Configure Apache modules) page. A red box highlights the 'Configurar módulos de Apache' icon in the top navigation bar. Below, a table lists various Apache modules and their status.

Module	Status
cache_socache	Discapacitado
cern_meta	Discapacitado
cgi	Discapacitado
cgid	Discapacitado
charset_lite	Discapacitado
data	Discapacitado
dav	Discapacitado
dav_fs	Discapacitado
dav_lock	Discapacitado
dbd	Discapacitado
deflate	Habilitado
dialup	Discapacitado
dir	Habilitado
dump_io	Discapacitado
echo	Discapacitado
env	Habilitado
expires	Discapacitado
ext_filter	Discapacitado
file_cache	Discapacitado
filter	Habilitado
headers	Discapacitado
heartbeat	Discapacitado
heartmonitor	Discapacitado
http2	Discapacitado
ident	Discapacitado
imagemap	Discapacitado
include	Discapacitado
info	Discapacitado
lbmethod_bybusyness	Discapacitado
proxy_wstunnel	Discapacitado
ratelimit	Discapacitado
reflector	Discapacitado
remoteip	Discapacitado
reqtimeout	Habilitado
request	Discapacitado
rewrite	Discapacitado
sed	Discapacitado
session	Discapacitado
session_cookie	Discapacitado
session_crypto	Discapacitado
session_dbd	Discapacitado
setenvif	Habilitado
slotmem_plain	Discapacitado
slotmem_shm	Discapacitado
socache_dbm	Discapacitado
socache_memcache	Discapacitado
socache_shmcb	Habilitado
speling	Discapacitado
ssl	Habilitado
status	Habilitado
substitute	Discapacitado
suexec	Discapacitado
unique_id	Discapacitado
userdir	Discapacitado
usertrack	Discapacitado
vhost_alias	Discapacitado
xml2enc	Discapacitado



```
servidordgg@servidordgg:~$ sudo a2enmod ssl
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
servidordgg@servidordgg:~$ systemctl restart apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'apache2.service'.
Authenticating as: David Gonzalez Garcia (servidordgg)
Password:
==== AUTHENTICATION COMPLETE ====
servidordgg@servidordgg:~$ _
```

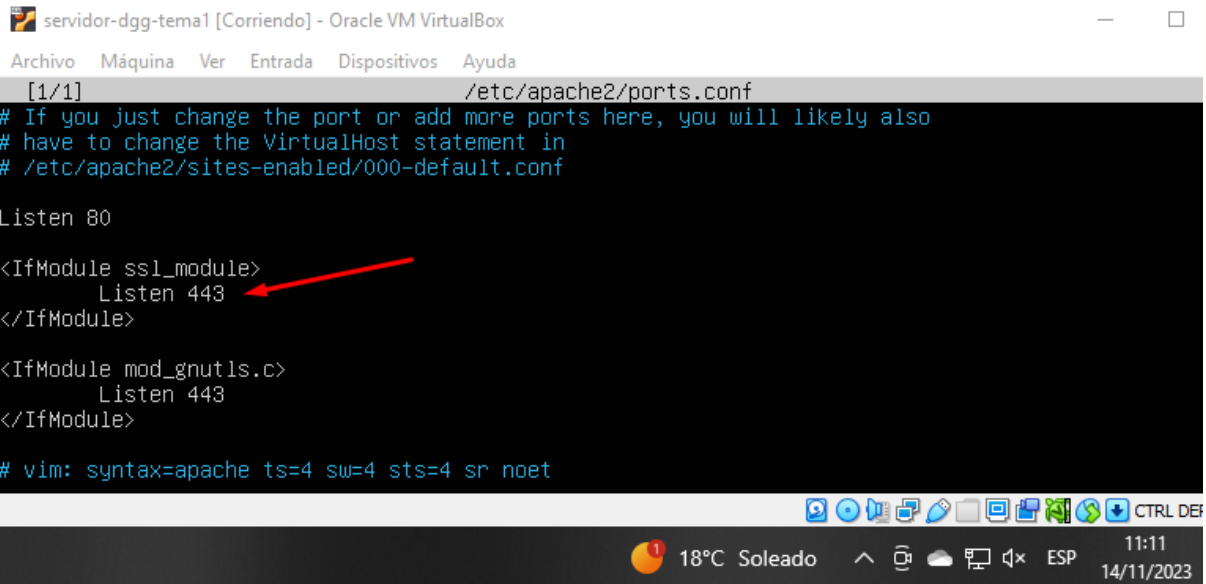
The screenshot shows a terminal window titled 'servidor-dgg-tema1 [Corriendo] - Oracle VM VirtualBox'. The terminal output shows the command 'sudo a2enmod ssl' being executed, which enables the SSL module and its dependencies (setenvif, mime, socache\_shmcb). It then prompts the user to restart the service with 'systemctl restart apache2'. The user enters the command, and the system prompts for authentication. The user's name 'David Gonzalez Garcia' is shown, and the authentication is successful. The terminal ends with a prompt character '\_'. The bottom of the window shows a taskbar with various icons, including a clock showing 11:08 and the date 14/11/2023.

## Paso 2: Puerto seguro

Comprobar que el archivo `/etc/apache2/ports.conf`, hay una directiva `<IfModule>` donde está incluida la escucha en el puerto 443, ya que el módulo SSL está activado.

Para ello usaremos el siguiente comando:

```
$ sudo nano /etc/apache2/ports.conf
```



```
servidor-dgg-tema1 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[1/1] /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

<IfModule ssl_module>
    Listen 443
</IfModule>

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

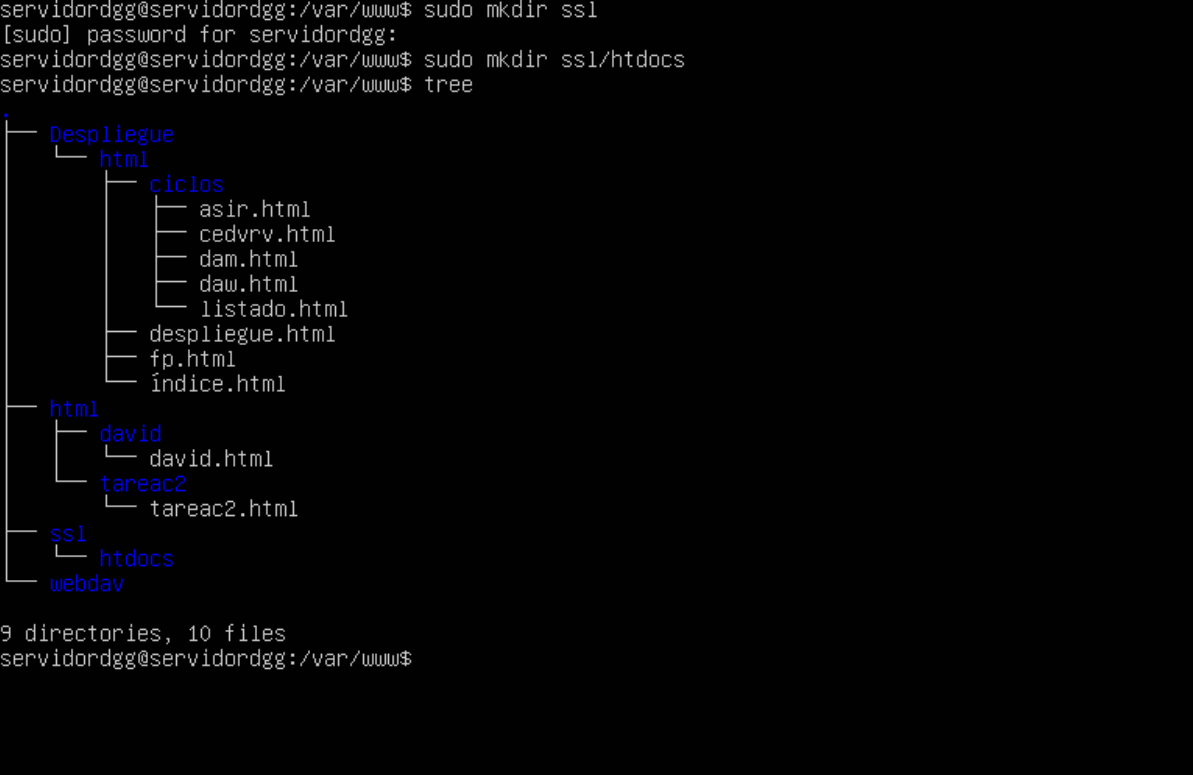
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

## Paso 3: Crear host virtual

Crear un hosts virtual basado en el hosts virtual por defecto (default-ssl.conf) y con directorio de inicio para documentos `/var/www/ssl/htdocs`. Crear dicho directorio previamente como usuario root. Crea también un archivo `index.html` preparado para la prueba de conexión.

```
servidordgg@servidordgg:/var/www$ sudo mkdir ssl
[sudo] password for servidordgg:
servidordgg@servidordgg:/var/www$ sudo mkdir ssl/htdocs
servidordgg@servidordgg:/var/www$ tree
.
├── Despliegue
│   └── html
│       ├── ciclos
│       │   ├── asir.html
│       │   ├── cedvrv.html
│       │   ├── dam.html
│       │   ├── daw.html
│       │   └── listado.html
│       ├── despliegue.html
│       ├── fp.html
│       └── índice.html
├── html
│   ├── david
│   │   └── david.html
│   └── tareac2
│       └── tareac2.html
├── ssl
│   └── htdocs
└── webdav

9 directories, 10 files
servidordgg@servidordgg:/var/www$
```



Observamos que es el archivo original, el que viene por defecto, e incluye las rutas para los certificados, siendo uno el certificado de seguridad y otro el archivo key para la clave privada.

```

GNU nano 2.9.3                                default-ssl.conf

# 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

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convinience.
#SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

# Certificate Authority (CA):

```

```

GNU nano 6.2                                /etc/apache2/sites-available/default-ssl.conf
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

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convinience.
#SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

# Certificate Authority (CA):
# Set the CA certificate verification path where to find CA

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify   ^_ Go To Line M-E Redo

CTRL DERECH
EUR/JPY -0.69% 12:30 17/11/2023

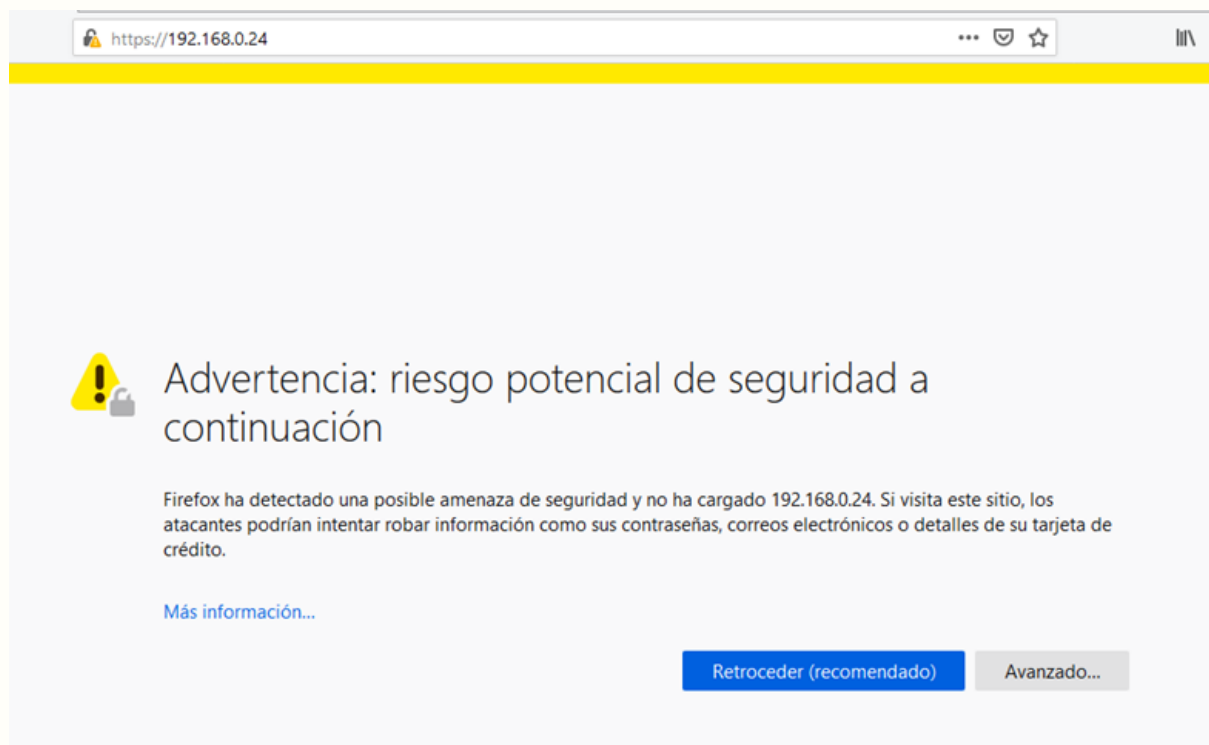
```

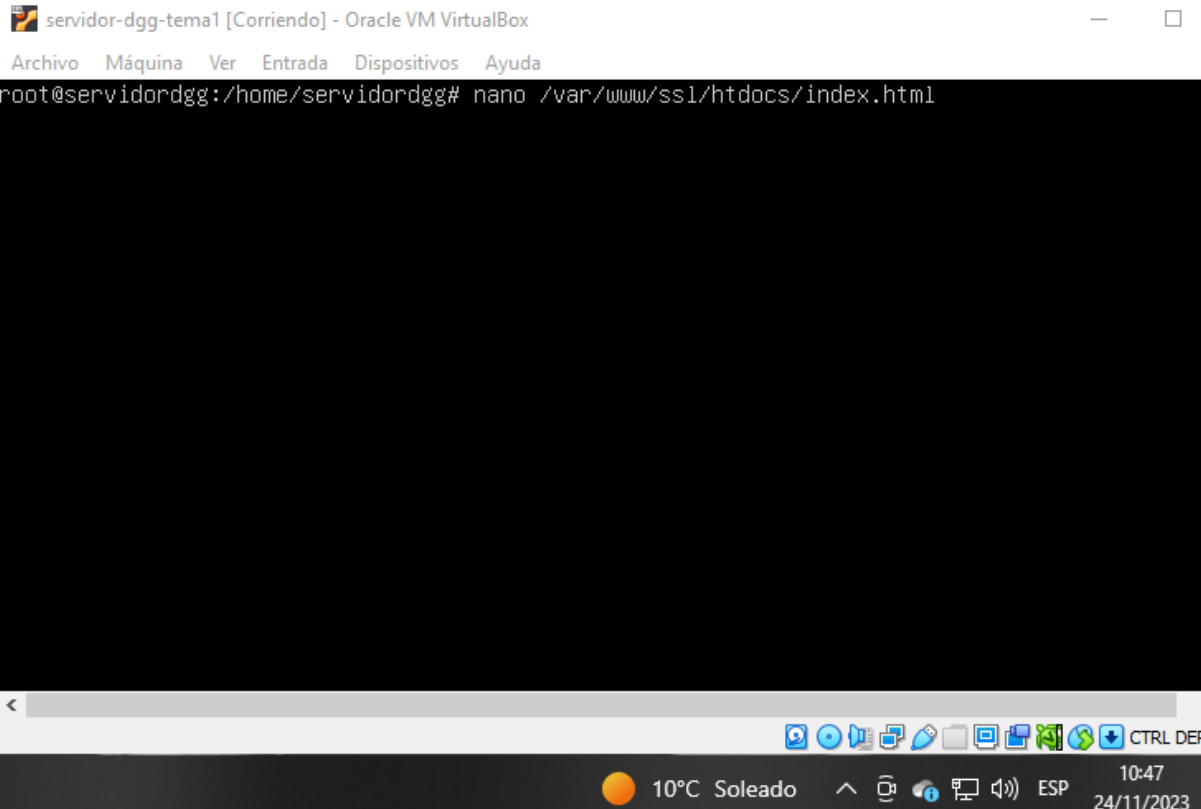


En sí, el sistema te crea dos claves: una privada y otra pública y se necesitan ambos archivos para poder crear el servidor seguro.

Una vez activado el módulo y comprobado que los certificados por defecto se encuentran en su ubicación, comprobamos que el navegador detecta un certificado que no es de ninguna entidad certificadora y nos tiene que avisar de ello. Primero habilitamos el servidor seguro con `a2ensite default-ssl.conf` y reiniciamos el servicio con `service apache2 restart`.

```
root@serverdaw:/etc/apache2/sites-available# a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@serverdaw:/etc/apache2/sites-available# service apache2 restart
root@serverdaw:/etc/apache2/sites-available# _
```



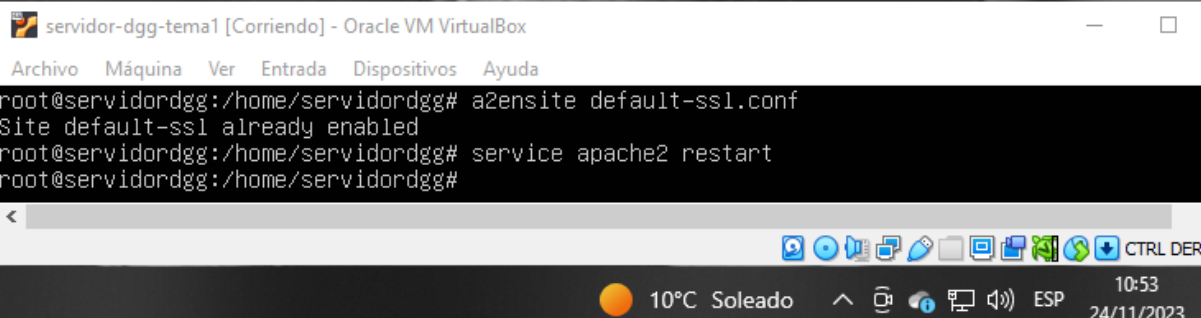


servidor-dgg-tema1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
root@servidordgg:/home/servidordgg# nano /var/www/ssl/htdocs/index.html
```

The terminal window shows the nano text editor open at the file `/var/www/ssl/htdocs/index.html`. The editor area is currently blank. The bottom status bar displays system information: 10°C, Soleado, and the date/time 10:47 24/11/2023.



servidor-dgg-tema1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
root@servidordgg:/home/servidordgg# a2ensite default-ssl.conf
Site default-ssl already enabled
root@servidordgg:/home/servidordgg# service apache2 restart
root@servidordgg:/home/servidordgg#
```

The terminal window shows the execution of the `a2ensite default-ssl.conf` command, which outputs "Site default-ssl already enabled". This is followed by the `service apache2 restart` command. The bottom status bar displays system information: 10°C, Soleado, and the date/time 10:53 24/11/2023.

## Paso 4: Instalar OpenSSL

Primero vamos a instalar openssl, escribimos:

```
$ sudo apt-get install openssl
```

Si vemos que ya está instalado, entonces lo ignoramos y seguimos.

```
root@serverdaw:/etc/apache2/sites-available# apt-get install openssl
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
openssl ya está en su versión más reciente (1.1.1-1ubuntu2.1~18.04.5).
fijado openssl como instalado manualmente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 9 no actualizados.
root@serverdaw:/etc/apache2/sites-available# _
```

 servidor-dgg-tema1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
root@servidordgg:/home/servidordgg# sudo apt-get install openssl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssl ya está en su versión más reciente (3.0.2-0ubuntu1.12).
fijado openssl como instalado manualmente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 50 no actualizados.
root@servidordgg:/home/servidordgg#
```

<

 CTRL DEF

 10°C Soleado  10:56  
24/11/2023

## Paso 5: Generar el certificado autofirmado y su clave

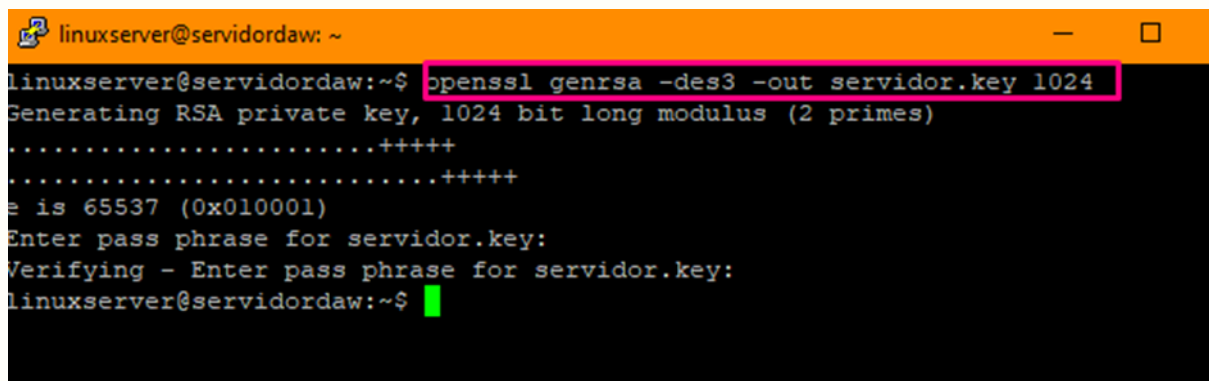
Una vez lo instalemos, debemos crear la clave privada de nuestro servidor que será de 1024 bit.

Sustituye servidor por: **servidornombre**. (Sustituye la palabra nombre por tu nombre de pila)

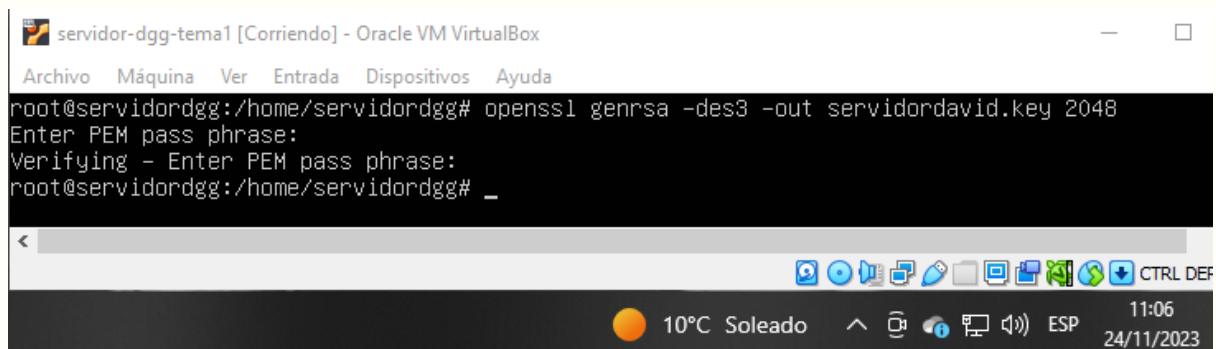
```
openssl genrsa -des3 -out servidor.key 1024
```

Si no funcionara con la línea anterior, sustituirla por la siguiente:

```
openssl genrsa -des3 -out servidor.key 1024
```



```
linuxserver@servidordaw: ~  
linuxserver@servidordaw:~$ openssl genrsa -des3 -out servidor.key 1024  
Generating RSA private key, 1024 bit long modulus (2 primes)  
.....+++++  
.....+++++  
e is 65537 (0x010001)  
Enter pass phrase for servidor.key:  
Verifying - Enter pass phrase for servidor.key:  
linuxserver@servidordaw:~$
```



```
servidor-dgg-tema1 [Corriendo] - Oracle VM VirtualBox  
Archivo Máquina Ver Entrada Dispositivos Ayuda  
root@servidordgg:/home/servidordgg# openssl genrsa -des3 -out servidordavid.key 2048  
Enter PEM pass phrase:  
Verifying - Enter PEM pass phrase:  
root@servidordgg:/home/servidordgg# _
```

**La frase que escribas recuérdala, te la pedirá en el proceso de configuración.**

Ya podemos crear los nuevos certificados. Rellenamos los datos y en Common Name ponemos la IP de nuestro servidor o el dominio.

Sustituye servidor por: **servidornombre**. (Sustituye la palabra nombre por tu nombre de pila)

```
$ openssl req -new -key servidor.key -out servidor.csr
```

req: este modificador especifica usar la administración de la solicitud de firma de certificados (CSR)

X.509, este es un estándar de claves públicas.

Nos aparecerá un asistente en la terminal que nos preguntará por diferentes datos que debemos rellenar:

- **Country Name:** corresponde a un código con las dos letras de nuestro país. Si vivimos en España, por ejemplo, escribimos ES.
- **State or Province Name:** escribimos el nombre de nuestra provincia o estado. Si eres español como yo, se refiere al nombre de tu comunidad autónoma. Por ejemplo, la mía es Andalucía. Por si acaso, para evitar problemas con las tildes y para aumentar la visibilidad, la escribimos en mayúsculas y sin tildes.
- **Locality Name:** escribimos el nombre de nuestra localidad en mayúsculas y sin tildes. SEVILLA
- **Organization Name:** se refiere al nombre de nuestra organización. nombreapellido1.
- **Organizational Unit Name:** se refiere al nombre del sector de nuestra organización. Poner IESVELAZQUEZ.
- **Common Name:** este campo es esencial, aquí debemos poner el nombre del dominio de la página web. En mi caso, aún no tenemos dominio así que la IP del servidor.
- **Email Address:** ponemos una dirección de correo personal, esto sirve por si nos tienen que enviar algún correo informativo o si necesitamos que nos contacten.

```
linuxserver@servidordaw: ~  
linuxserver@servidordaw:~$ openssl req -new -key servidor.key -out servidor.csr  
Enter pass phrase for servidor.key:  
Can't load /home/linuxserver/.rnd into RNG  
140655486263744:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:88:Filename=/home/linuxserver/.rnd  
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]:ANDALUCIA  
Locality Name (eg, city) []:SEVILLA  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:linuxserver  
Organizational Unit Name (eg, section) []:linuxserver  
Common Name (e.g. server FQDN or YOUR name) []:192.168.0.24  
Email Address []:linuxserver@servidordaw2.org  
  
Please enter the following 'extra' attributes  
to be sent with your certificate request  
A challenge password []:  
An optional company name []:  
linuxserver@servidordaw:~$
```

```
servidor-dgg-tema1 [Corriendo] - Oracle VM VirtualBox  
Archivo Máquina Ver Entrada Dispositivos Ayuda  
servidordgg@servidordgg:~$ sudo openssl req -new -key servidordavid.key -out servidordavid.csr  
[sudo] password for servidordgg:  
Enter pass phrase for servidordavid.key:  
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]:ANDALUCIA  
Locality Name (eg, city) []:SEVILLA  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:davidgonzalez  
Organizational Unit Name (eg, section) []:IESVELAZQUEZ  
Common Name (e.g. server FQDN or YOUR name) []:172.26.2.205  
Email Address []:dgongar3112@g.educaand.es  
  
Please enter the following 'extra' attributes  
to be sent with your certificate request  
A challenge password []:  
An optional company name []:  
servidordgg@servidordgg:~$
```

Le daremos una duración al certificado, en este caso 365 días.

```
linuxserver@servidordaw: ~  
linuxserver@servidordaw:~$ openssl x509 -req -days 365 -in servidor.csr -signkey servidor.key -out servidor.crt  
Signature ok  
subject=C = ES, ST = ANDALUCIA, L = SEVILLA, O = linuxserver, OU = linuxserver, CN = 192.168.0.24, emailAddress = lin  
uxserver@servidordaw2.org  
Getting Private key  
Enter pass phrase for servidor.key:  
linuxserver@servidordaw:~$
```

```
servidor-dgg-tema1 [Corriendo] - Oracle VM VirtualBox  
Archivo Máquina Ver Entrada Dispositivos Ayuda  
servidordgg@servidordgg:~$ sudo openssl x509 -req -days 365 -in servidordavid.csr -signkey servidord  
avid.key -out servidordavid.crt  
Enter pass phrase for servidordavid.key:  
Certificate request self-signature ok  
subject=C = ES, ST = ANDALUCIA, L = SEVILLA, O = davidgonzalez, OU = IESVELAZQUEZ, CN = 172.26.2.205  
, emailAddress = dgongar3112@g.educaand.es  
servidordgg@servidordgg:~$
```

Movemos los certificados a sus directorios correspondientes:

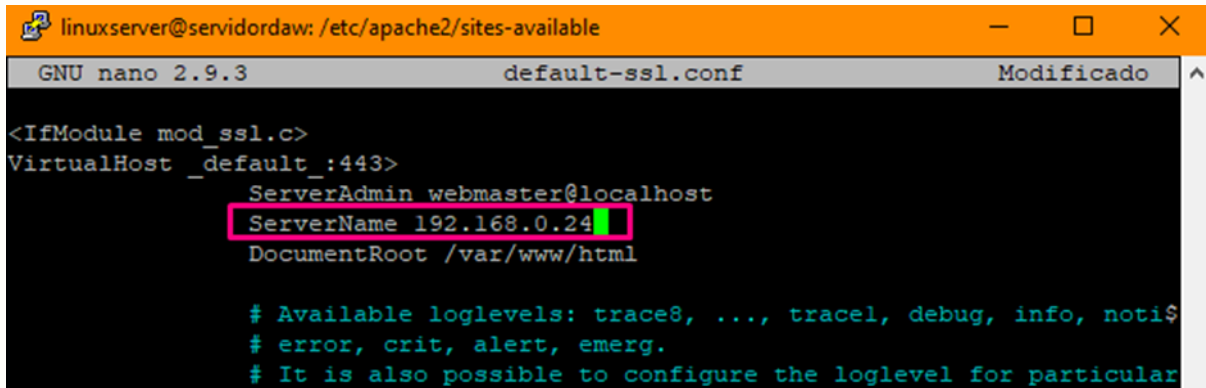
```
linuxserver@servidordaw:~$ sudo mv servidor.crt /etc/ssl/certs  
[sudo] contraseña para linuxserver:  
linuxserver@servidordaw:~$ sudo mv servidor.key /etc/ssl/private/  
linuxserver@servidordaw:~$
```

```
servidor-dgg-tema1 [Corriendo] - Oracle VM VirtualBox  
Archivo Máquina Ver Entrada Dispositivos Ayuda  
servidordgg@servidordgg:~$ sudo mv servidordavid.crt /etc/ssl/certs  
servidordgg@servidordgg:~$ sudo mv servidordavid.key /etc/ssl/private  
servidordgg@servidordgg:~$ _
```

## Paso 6: Modificar fichero de configuración de servidor seguro

Ir al archivo del servidor virtual seguro, en el directorio `/etc/apache2/sites-available`, editar el archivo del servidor virtual seguro e incluir las directivas siguientes:

**Si no funcionara con la clave de 1024, quitar la línea de `ServerName`**



```
linuxserver@servidordaw: /etc/apache2/sites-available
GNU nano 2.9.3 default-ssl.conf Modificado
<IfModule mod_ssl.c>
VirtualHost _default_:443>
    ServerAdmin webmaster@localhost
    ServerName 192.168.0.24
    DocumentRoot /var/www/html

    # Available loglevels: trace8, ..., trace1, debug, info, notice, error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
```

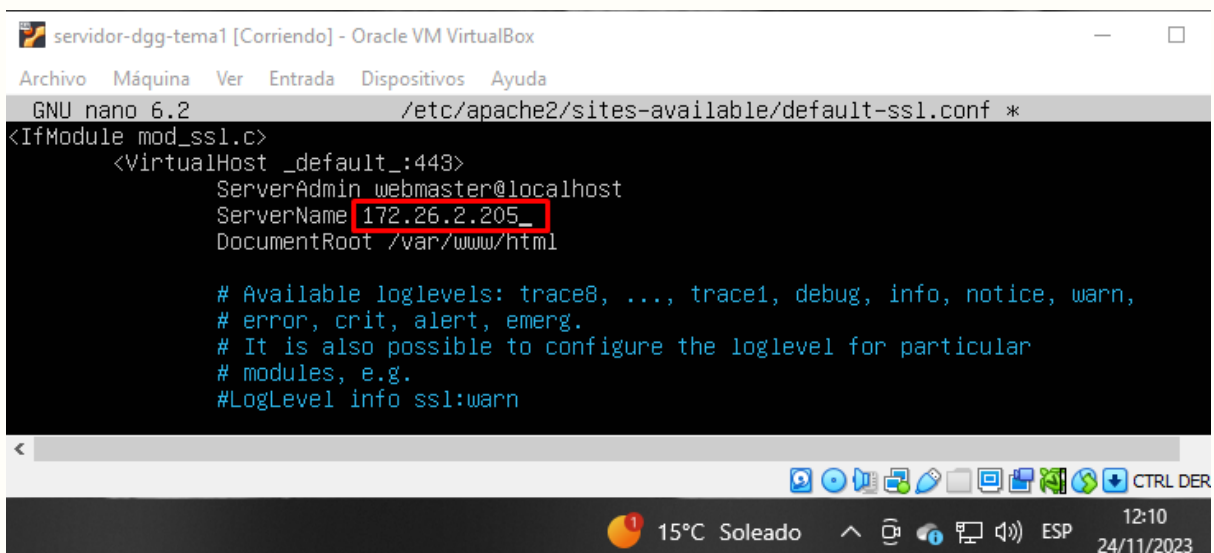
**SSL Engine on**

**SSLCertificateFile** `/etc/ssl/certs/servidor.crt`

**SSLCertificateKeyFile** `/etc/ssl/private/servidor.key`

Para poder editar el archivo usaremos el siguiente comando:

```
$ sudo nano /etc/apache2/sites-available/default-ssl.conf
```



```
servidor-dgg-tema1 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 6.2 /etc/apache2/sites-available/default-ssl.conf *
<IfModule mod_ssl.c>
    <VirtualHost _default_:443>
        ServerAdmin webmaster@localhost
        ServerName 172.26.2.205_
        DocumentRoot /var/www/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
```



```
GNU nano 2.9.3      default-ssl.conf      Modificado

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 ex$
# following line enables the CGI configuration for this host $
# 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 in$
#   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, $
#   SSLCertificateFile directive is needed.
SSLCertificateFile      /etc/ssl/certs/servidor.crt
SSLCertificateKeyFile   /etc/ssl/private/servidor.key

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
```

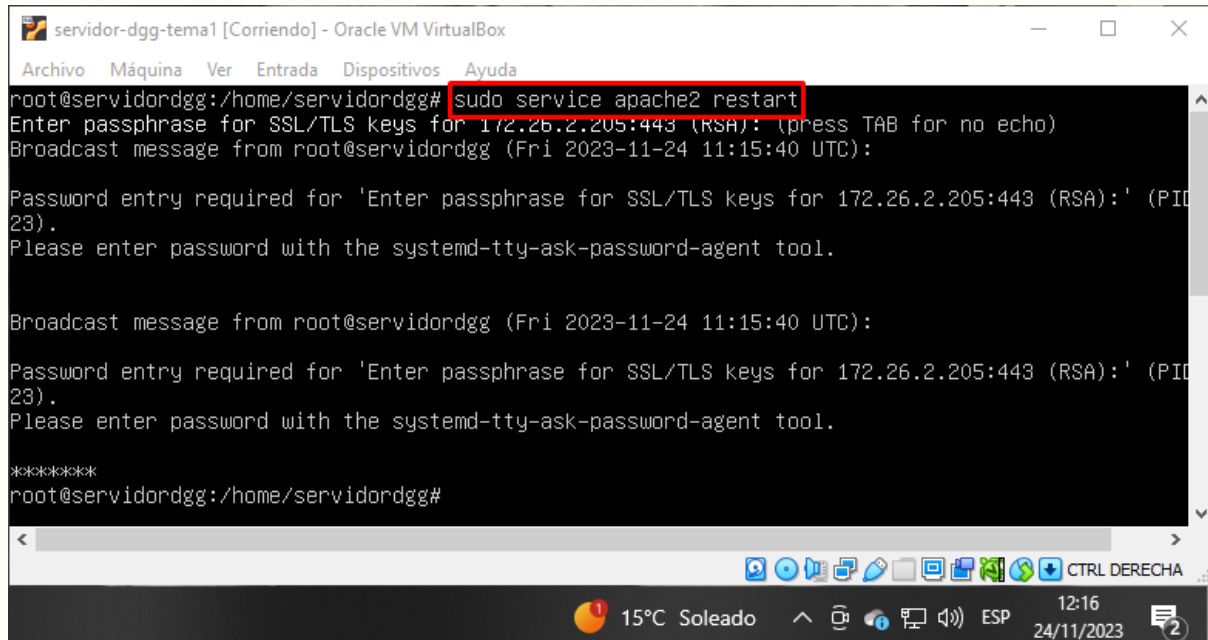
```
servidor-dgg-tema1 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 6.2      /etc/apache2/sites-available/default-ssl.conf *
SSLEngine on

#   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/servidordavid.crt
SSLCertificateKeyFile   /etc/ssl/private/servidordavid.key_

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
```

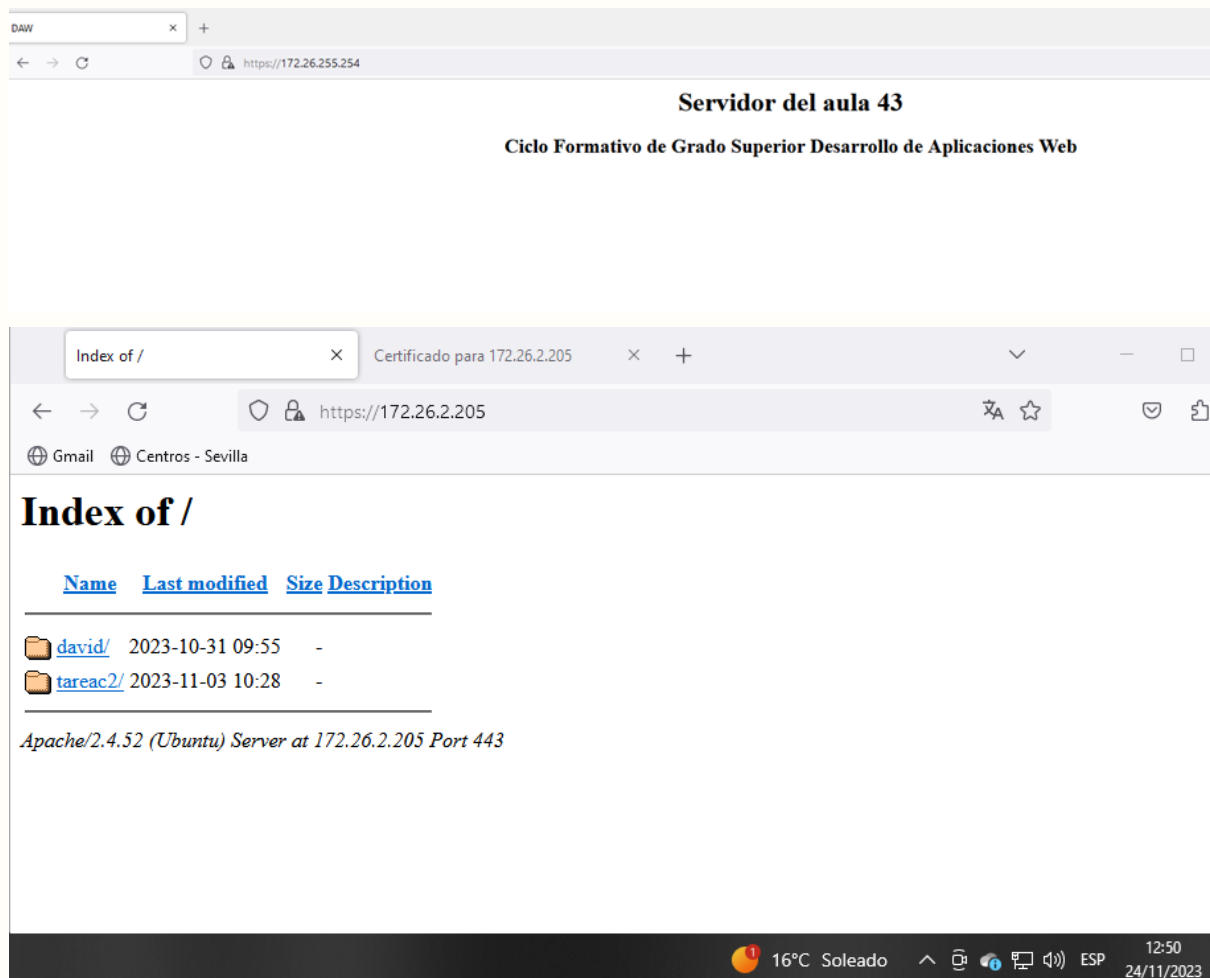
## Paso 7: Aplicar cambios

```
linuxserver@servidordaw:/etc/apache2/sites-available$ sudo service apache2 restart
Enter passphrase for SSL/TLS keys for 192.168.0.24:443 (RSA): *****
linuxserver@servidordaw:/etc/apache2/sites-available$
```



## Paso 8: Comprobar funcionamiento

Abrir el navegador de la máquina anfitriona y escribir `https://IP` en la barra de direcciones:



## Paso 9: Comprobar que el certificado es el correcto

Administrador de certificados

Sus certificados

Decisiones de autenticación

Personas

Servidores

Autoridades

Estas entradas identifican las excepciones de error del certificado del servidor

Servidor	Nombre del certificado	Vida útil
172.26.0.51:10000	*	Permanente
172.26.255.254:10000	*	Temporal
172.26.255.254:443	172.26.255.254	Temporal

Ver...

Exportar...

Eliminar...

Añadir excepción...

Aceptar

Certificado

192.168.1.254	
<b>Nombre del asunto</b>	
País	ES
Estado/Provincia	Andalucia
Localidad	Sevilla
Organización	linuxserver
Unidad organizativa	IESVelazquez
Nombre común	192.168.1.254
Dirección de correo electrónico	linuxserver@servidordaw2.org
<b>Nombre del emisor</b>	
País	ES
Estado/Provincia	Andalucia
Localidad	Sevilla
Organización	linuxserver
Unidad organizativa	IESVelazquez
Nombre común	192.168.1.254
Dirección de correo electrónico	linuxserver@servidordaw2.org
<b>Validez</b>	
No antes	Tue, 07 Nov 2023 09:54:35 GMT
No después	Wed, 06 Nov 2024 09:54:35 GMT
<b>Información de clave pública</b>	

Index of / × Certificado para 172.26.2.205 × +

← → ↻ Firefox about:certificate?cert=MIIDzzCCArcCFcRJNzGoGVleOrk8B3f%2Fot5fqaSz 60% ☆ 📧 📁

🌐 Gmail 🌐 Centros - Sevilla

### Certificado

172.26.2.205

<b>Nombre del asunto</b>	
País	ES
Estado/Provincia	ANDALUCIA
Localidad	SEVILLA
Organización	davidgonzalez
Unidad organizativa	IESVELAZQUEZ
Nombre común	172.26.2.205
Dirección de correo electrónico	dgongar3112@g.educaand.es

<b>Nombre del emisor</b>	
País	ES
Estado/Provincia	ANDALUCIA
Localidad	SEVILLA
Organización	davidgonzalez
Unidad organizativa	IESVELAZQUEZ
Nombre común	172.26.2.205
Dirección de correo electrónico	dgongar3112@g.educaand.es

<b>Validez</b>	
No antes	Fri, 24 Nov 2023 11:40:55 GMT
No después	Sat, 23 Nov 2024 11:40:55 GMT

<b>Información de clave pública</b>	
Algoritmo	RSA
Tamaño de la clave	2048
Exponente	65537
Módulo	BF:76:30:45:01:FA:87:F9:E5:F4:4D:D8:EF:AA:4C:FC:CE:E8:47:E0:2E:28:78:44:68:9...

<b>Misceláneo</b>	
Número de serie	24:49:37:31:A8:19:52:1E:3A:B9:3C:07:77:FF:A2:DE:5F:A9:A4:83
Algoritmo de firmas	SHA-256 with RSA Encryption
Versión	1
Descargar	<a href="#">PEM (.cert)</a> <a href="#">PEM (.cadena)</a>

<b>Huellas digitales</b>	
SHA-256	F8:27:7D:21:D2:A4:CD:48:E4:3F:52:CA:7D:0E:CE:8E:81:05:5C:C0:45:80:AED:8...
SHA-1	37:FA:A6:C6:AE:05:FE:7E:36:88:99:5F:81:85:8E:68:54:83:09:18

16°C Soleado 12:52 24/11/2023

<b>Nombre del emisor</b>	
País	ES
Estado/Provincia	Andalucía
Localidad	Sevilla
Organización	linuxserver
Unidad organizativa	IESVelazquez
Nombre común	192.168.1.254
Dirección de correo electrónico	linuxserver@servidordaw2.org
<b>Validez</b>	
No antes	Tue, 07 Nov 2023 09:54:35 GMT
No después	Wed, 06 Nov 2024 09:54:35 GMT
<b>Información de clave pública</b>	
Algoritmo	RSA
Tamaño de la clave	2048
Exponente	65537
Módulo	DF:01:69:D5:6E:73:32:0C:DC:65:54:F5:04:71:46:D3:9C:6A:2A:27:4C:40:63:2D:3A:FF:...
<b>Misceláneo</b>	
Número de serie	65:5C:D6:AC:2E:03:B8:67:01:03:0F:17:1F:1F:D5:D7:78:6B:03:0B
Algoritmo de firmas	SHA-256 with RSA Encryption
Versión	1
Descargar	<a href="#">PEM (cert)</a> <a href="#">PEM (cadena)</a>
<b>Huellas digitales</b>	
SHA-256	32:EF:24:6B:9C:28:4B:A3:EB:27:FE:E1:E0:F8:8A:7C:DA:59:0F:97:D1:18:48:36:9D:61:6...
SHA-1	D2:CC:FC:80:CC:DD:28:9D:D6:B2:D9:57:F3:23:8E:46:C7:51:91:09

**Validez**

No antes

Fri, 24 Nov 2023 11:40:55 GMT

No después

Sat, 23 Nov 2024 11:40:55 GMT

**Información de clave pública**

Algoritmo

RSA

Tamaño de la clave

2048

Exponente

65537

Módulo

BF:76:30:45:01:FA:B7:F9:E5:F4:4D:D8:EF:AA:4C:FC:CE:EB:47:E0:2E:28:78:44:6B:9F:...

**Misceláneo**

 16°C Soleado



ESP 12:53  
24/11/2023

También puedes conseguir la información del certificado en:

 <https://192.168.1.254>

Información del sitio para 192.168.1.254

 Conexión no segura

>

**Servidor Seguro del Aula 43**

Ciclo Formativo de Grado Superior en Desarrollo de Aplicaciones Web