

1. Configura el servidor DNS para que resuelva el nombre seguro.africalinux.org. La dirección IP asociada al nombre será la IP del Servidor Linux.

```
GNU nano 4.8 db.enrique.org
;
; BIND data file for local loopback interface
;
$ORIGIN enrique.org.
$TTL 2D
@ IN SOA enrique-server1 root (
    2020121401 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
enrique.org. IN NS enrique-server1
enrique-server1 IN A 192.168.1.200
www IN CNAME enrique-server1
web IN CNAME enrique-server1
seguro IN CNAME enrique-server1
```

```
Enrique-Server-Apache 2 Actualizacion [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 4.8 db.192.168.1
;
; BIND data file for local loopback interface
;
$ORIGIN 192.168.1. in-addr.arpa.
$TTL 2D
@ IN SOA enrique-server1 root (
    2020121401 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS enrique-server1.enrique.org.
200 IN PTR enrique-server1.enrique.org.
200 IN PTR www.enrique.org.
200 IN PTR web.enrique.org.
200 IN PTR seguro.enrique.org_

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos ^M
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line ^
```

2. Reiniciar el servidor para guardar cambios.

`sudo service bind9 restart`

```
Enrique-Server-Apache 2 Actualizacion [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
enrique@enrique:/etc/bind$ sudo service bind9 restart
enrique@enrique:/etc/bind$
```

3. Crea el directorio /var/www/html/seguro

Este directorio será el directorio raíz

```
Enrique-Server-Apache 2 Actualizacion [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
enrique@enrique:/var/www/html$ sudo mkdir seguro
enrique@enrique:/var/www/html$ ll
total 56
drwxr-xr-x 8 root root 4096 Feb 22 19:30 ./
drwxr-xr-x 4 root root 4096 Feb 18 15:30 ../
-rw-r--r-- 1 root root 173 Feb 1 21:54 404.html
drwxr-xr-x 2 root root 4096 Feb 11 15:19 carpetaprivada/
drwxr-xr-x 2 root root 4096 Feb 1 20:13 ciclos/
-rw-r--r-- 1 root root 125 Feb 1 20:15 despliegue.html
-rw-r--r-- 1 root root 112 Feb 1 19:57 fp.html
drwxr-xr-x 2 root root 4096 Feb 22 19:29 html/
-rw-r--r-- 1 root root 10918 Jan 18 11:56 indice.html
drwxr-xr-x 2 root root 4096 Feb 6 18:10 profesor/
drwxr-xr-x 2 root root 4096 Feb 22 19:30 seguro/
drwxr-xr-x 2 root root 4096 Feb 18 15:41 webalizer/
enrique@enrique:/var/www/html$ _
```

4. Crea el fichero de texto /var/www/html/seguro/index.html con el contenido que quieras.

```
Enrique-Server-Apache 2 Actualizacion [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 4.8                                index.html
<html>
<body>
Venga que ya queda poco para terminar
</body>
</html>
```

5. Crea un certificado digital autofirmado usando openssl

5.1 Sitúate en el directorio home del usuario con que has iniciado sesión.

5.2 Crea una clave privada RSA de 2048 bit.

```
openssl genrsa -out seguro.key 2048
```

```
Enrique-Server-Apache 2 Actualizacion [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
enrique@enrique:~$ openssl genrsa -out seguro.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
enrique@enrique:~$ _
```

5.3 Genera una solicitud de certificado (CSR)

```
openssl req -new -key seguro.key -out seguro.csr
```

```
Enrique-Server-Apache 2 Actualizacion [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
enrique@enrique:~$ openssl req -new -key seguro.key -out seguro.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]:SP
State or Province Name (full name) [Some-State]:Cadiz
Locality Name (eg, city) []:Sanlucar de Barrameda
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:Enrique
Email Address []:enrique.cuevas@iesdonana.org

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

A continuación, introduce los datos del certificado.

Esta solicitud de certificado se la podrías enviar a una autoridad de certificación para que generase el certificado

(CTR). En este caso lo vamos a firmar nosotros, vamos a crear un certificado autofirmado.

5.4 Crea el certificado digital autofirmado usando la clave privada.

```
openssl x509 -req -days 365 -in seguro.csr -signkey seguro.key -out seguro.crt
```

```
enrique@enrique:~$ openssl x509 -req -days 365 -in seguro.csr -signkey seguro.key -out seguro.crt
Signature ok
subject=C = SP, ST = Cadiz, L = Sanlucar de Barrameda, O = Internet Widgits Pty Ltd, CN = Enrique, e
mailAddress = enrique.cuevas@iesdonana.org
Getting Private key
enrique@enrique:~$
```

6. Copia la clave y el certificado en los directorios que utiliza por defecto Apache y configura los permisos adecuados.

```
sudo mv seguro.key /etc/ssl/private
```

```
sudo mv seguro.crt /etc/ssl/certs
```

```
enrique@enrique:~$ sudo mv seguro.key /etc/ssl/private/
enrique@enrique:~$ sudo mv seguro.crt /etc/ssl/certs
enrique@enrique:~$ _
```

```
sudo chown root:ssl-cert /etc/ssl/private/seguro.key
```

```
sudo chmod 640 /etc/ssl/private/seguro.key
```

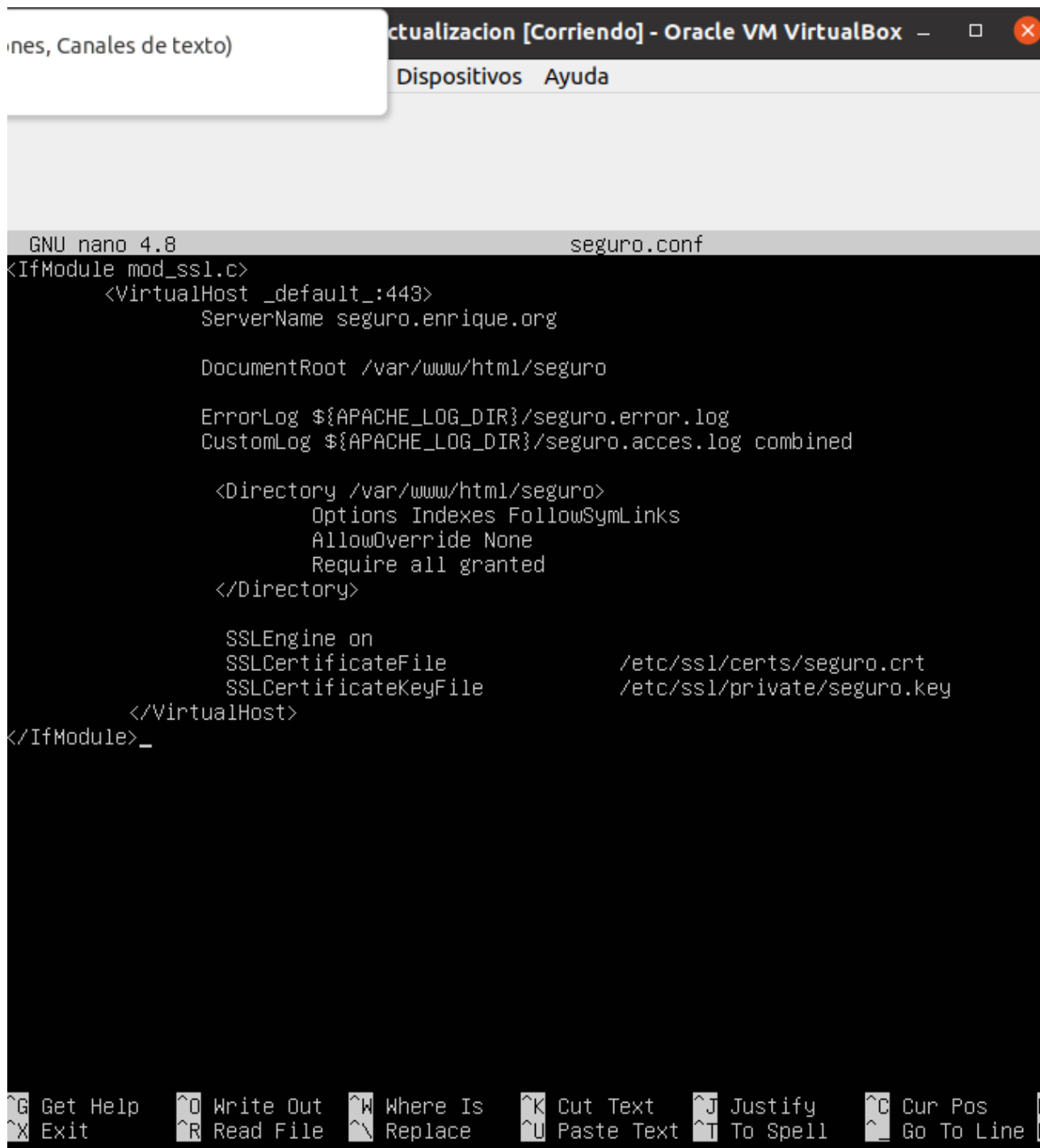
```
sudo chown root:root /etc/ssl/certs/seguro.crt
```

```
enrique@enrique:~$ sudo chown root:ssl-cert /etc/ssl/private/seguro.key
enrique@enrique:~$ sudo chmod 640 /etc/ssl/private/seguro.key
enrique@enrique:~$ sudo chown root:root /etc/ssl/certs/seguro.crt
enrique@enrique:~$ _
```

7. Crea el fichero `/etc/apache/sites-available/seguro.conf` con las siguientes directivas

El log de errores será `/var/log/apache2/seguro.error.log`

El log de accesos será `/var/log/apache2/seguro.access.log`, con formato `combined`



The screenshot shows a terminal window titled "Actualización [Corriendo] - Oracle VM VirtualBox". Inside the terminal, the GNU nano 4.8 editor is open, editing the file `seguro.conf`. The configuration content is as follows:

```
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerName seguro.enrique.org

    DocumentRoot /var/www/html/seguro

    ErrorLog ${APACHE_LOG_DIR}/seguro.error.log
    CustomLog ${APACHE_LOG_DIR}/seguro.acces.log combined

    <Directory /var/www/html/seguro>
      Options Indexes FollowSymLinks
      AllowOverride None
      Require all granted
    </Directory>

    SSLEngine on
    SSLCertificateFile      /etc/ssl/certs/seguro.crt
    SSLCertificateKeyFile   /etc/ssl/private/seguro.key
  </VirtualHost>
</IfModule>_
```

At the bottom of the terminal, there is a status bar with various keyboard shortcuts: `^G Get Help`, `^O Write Out`, `^W Where Is`, `^K Cut Text`, `^J Justify`, `^C Cur Pos`, `^X Exit`, `^R Read File`, `^N Replace`, `^U Paste Text`, `^T To Spell`, and `^_ Go To Line`.

8. Deshabilita el servidor ssl por defecto

sudo a2dissite default-ssl

```
enrique@enrique:~$ sudo a2dissite default-ssl
[sudo] password for enrique:
Site default-ssl disabled.
To activate the new configuration, you need to run:
    systemctl reload apache2
enrique@enrique:~$ systemctl reload apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to reload 'apache2.service'.
Authenticating as: enrique
Password:
==== AUTHENTICATION COMPLETE ====
enrique@enrique:~$
```

9. Habilita el servidor virtual seguro.

sudo a2ensite seguro

```
enrique@enrique:~$ sudo a2ensite seguro
Enabling site seguro.
To activate the new configuration, you need to run:
    systemctl reload apache2
enrique@enrique:~$ systemctl reload apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to reload 'apache2.service'.
Authenticating as: enrique
Password:
==== AUTHENTICATION COMPLETE ====
enrique@enrique:~$ _
```

10. Verifica que dentro del directorio /etc/apache2/sites-enabled se ha creado el enlace seguro.conf

```
enrique@enrique:~$ cd /etc/apache2/sites-enabled/
enrique@enrique:/etc/apache2/sites-enabled$ ll
total 8
drwxr-xr-x 2 root root 4096 Feb 22 20:04 ./
drwxr-xr-x 8 root root 4096 Feb 18 14:47 ../
lrwxrwxrwx 1 root root   35 Jan 18 11:56 000-default.conf -> ../sites-available/000-default.conf
lrwxrwxrwx 1 root root   30 Feb 22 20:04 seguro.conf -> ../sites-available/seguro.conf
enrique@enrique:/etc/apache2/sites-enabled$ _
```

11. Reinicia el servidor para que los cambios tengan efecto.

```
enrique@enrique:/etc/apache2/sites-enabled$ sudo systemctl restart apache2
enrique@enrique:/etc/apache2/sites-enabled$ _
```

12. Desde el cliente abre el navegador y establece una conexión a <https://seguro.africalinux.org>

