Práctica 5.20: Servidor virtual HTTPS en *Linux*

Realiza la siguiente configuración en el servidor *Apache* instalado en **ServidorLinuxXX**.

- Deshabilita el servidor virtual *ssl* por defecto (*default-ssl*).
- Crea un certificado digital autofirmado con *openssl* para el dominio `seguro.dawXX.net`.
- Crea y habilita un servidor virtual *https* para el dominio `seguro.dawXX.net`
  - Directorio raíz **/var/www/seguro/**.
    - Se servirá el fichero **index.html** si no se indica ningún fichero en la URL.
    - Se mostrará un listado del directorio raíz si no se solicita ningún fichero.
    - Podrán acceder todos los usuarios.
  - 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*.

Prueba la configuración.

1. Configura el servidor DNS de **ServidorWindowsXX** para que resuelva el nombre `seguro.dawXX.net`. La dirección IP asociada al nombre será la IP de **ServidoLinuxXX** es decir `192.168.1.X7`, Figura 1.

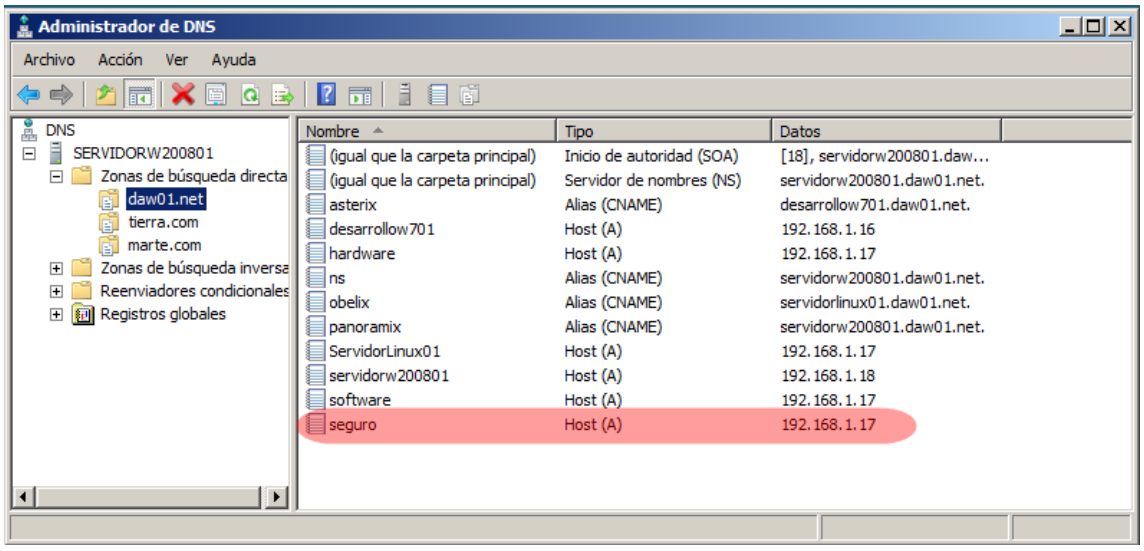

Figura 1: Configuración del servidor DNS en **ServidorWindowsXX**

2. Asegúrate que **DesarrolloW7XX** utiliza el servidor DNS que has configurado.
3. Inicia una sesión en **ServidorLinuxXX** con un usuario con privilegios de administración.
4. Crea el directorio **/var/www/seguro**.

5. Crea el fichero de texto **/var/www/seguro/index.html** con el contenido que quieras.
6. Crea un certificado digital autofirmado usando openssl.
   6.1. Sitúate en el directorio **home** del usuario con el que has iniciado sesión.
   6.2. Crea una clave privada RSA de 2048 bit, Figura 2.

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

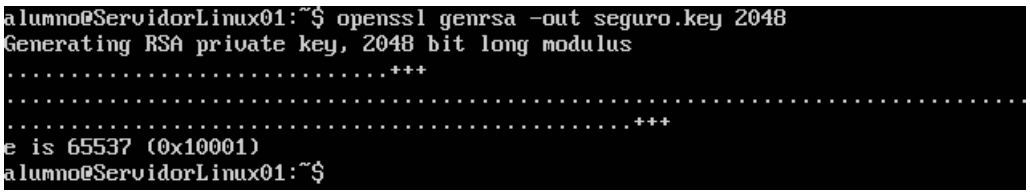

Figura 2: Creación de una clave privada

   6.3. Genera una solicitud de certificado (CSR, *Certificate Signing Request*).

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

Introduce los datos del certificado, Figura 3

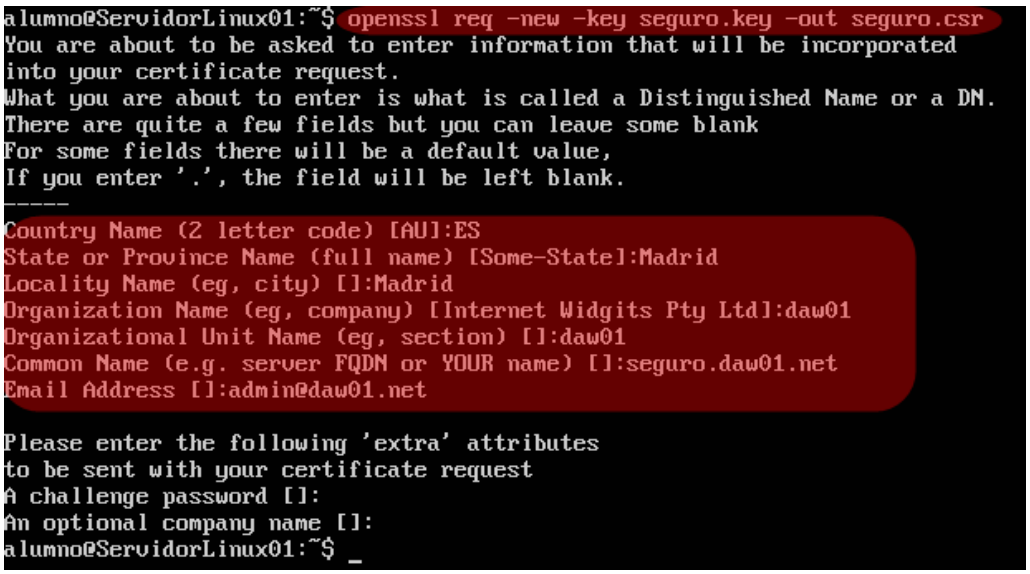

Figura 3: Creación de la solicitud del certificado

Esta solicitud de certificado se la podrías enviar a una autoridad de certificación para que generase el certificado (CRT). En este caso lo vamos a firmar nosotros, vamos a crear un certificado autofirmado.

   6.4. Crea el certificado digital autofirmado usando la clave privada, Figura 4.

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

```
alumno@ServidorLinux01:~$ openssl x509 -req -days 365 -in seguro.csr -signkey se
guro.key -out seguro.crt
Signature ok
subject=/C=ES/ST=Madrid/L=Madrid/O=daw01/OU=daw01/CN=seguro.daw01.net/emailAddre
ss=admin@daw01.net
Getting Private key
alumno@ServidorLinux01:~$ _
```

Figura 4: Creación del certificado digital autofirmado

7. 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/
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
```

8. Crea el fichero **/etc/apache/site-available/seguro** con las siguientes directivas, Figura5.

```
<IfModule mod_ssl.c>
<VirtualHost *:443>
        ServerName seguro.daw01.net
        DocumentRoot /var/www/seguro
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/seguro>
                DirectoryIndex index.html
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/seguro.error.log
        LogLevel warn
        CustomLog ${APACHE_LOG_DIR}/seguro.access.log combined

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

Figura 5: Fichero de configuración del servidor seguro

9. Deshabilita el servidor ssl por defecto.

```
sudo a2dissite default-ssl
```

10. Habilita el servidor virtual seguro.

    ```
    sudo a2ensite seguro
    ```

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

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

13. Desde **DesarrolloW7XX** abre el navegador y establece una conexión a `https:\\seguro.dawXX.net`, Figuras 6, 7, 8 y 9.

Figura 6: Conexión https

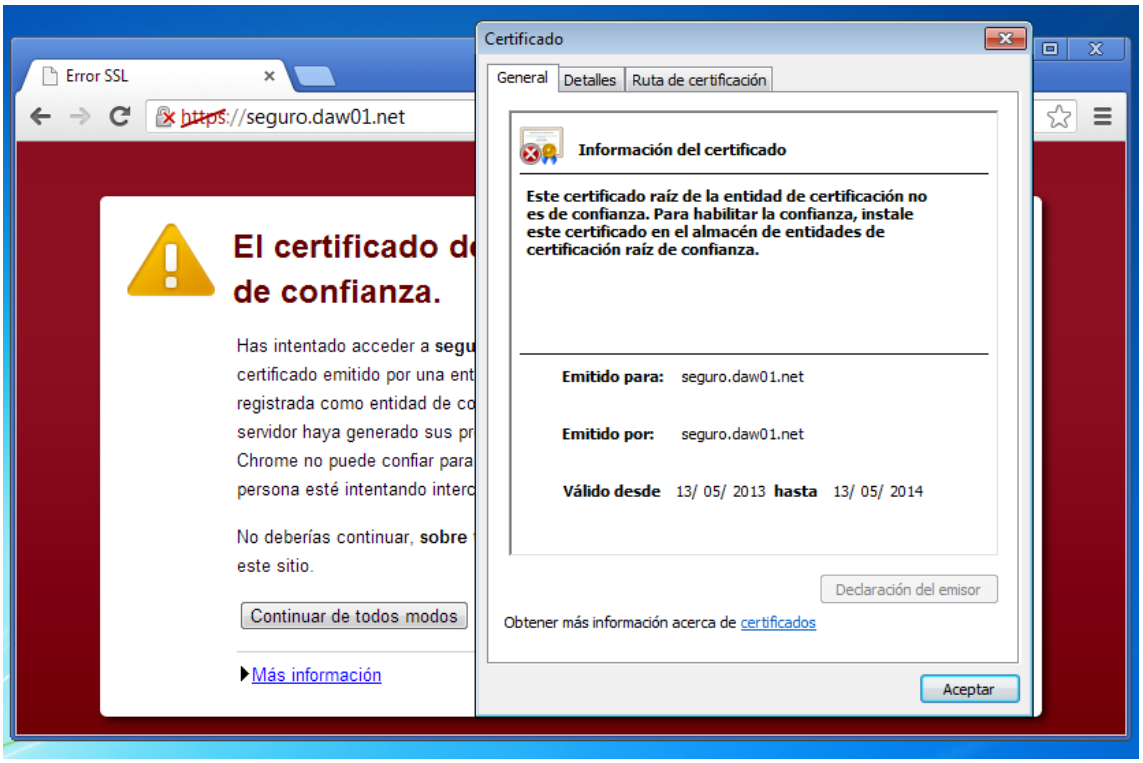

Figura 7: Conexión https

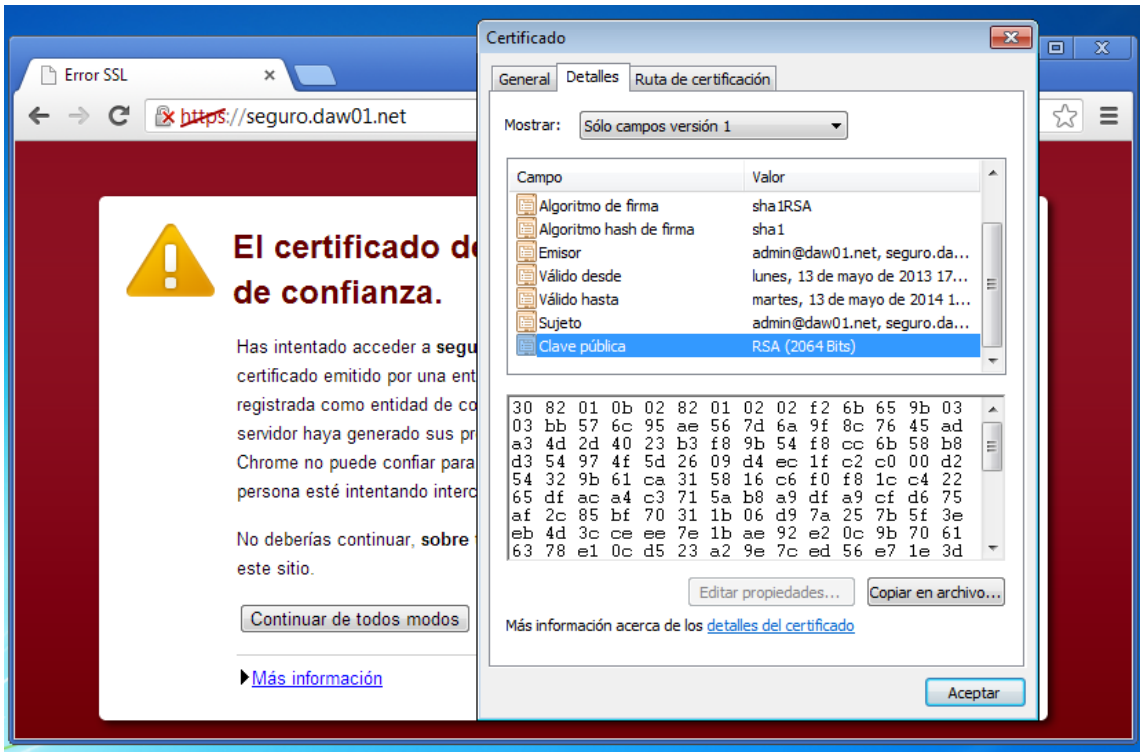

Figura 8: Conexión https

Figura 9: Conexión https

◇