4. Administración de Apache

4.20. 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.conf).*
- 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/html/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 **ServidorW2008XX** para que resuelva el nombre **seguro.dawXX.*net***. La dirección IP asociada al nombre será la IP de **ServidorLinuxXX** es decir 172.16.10.XX6. Recuerda crea un nuevo registro llamado "seguro" de tipo Host A en la zona de búsqueda directa "dawXX.net" asociándole la IP 172.16.10.XX6, Figura 4.117.

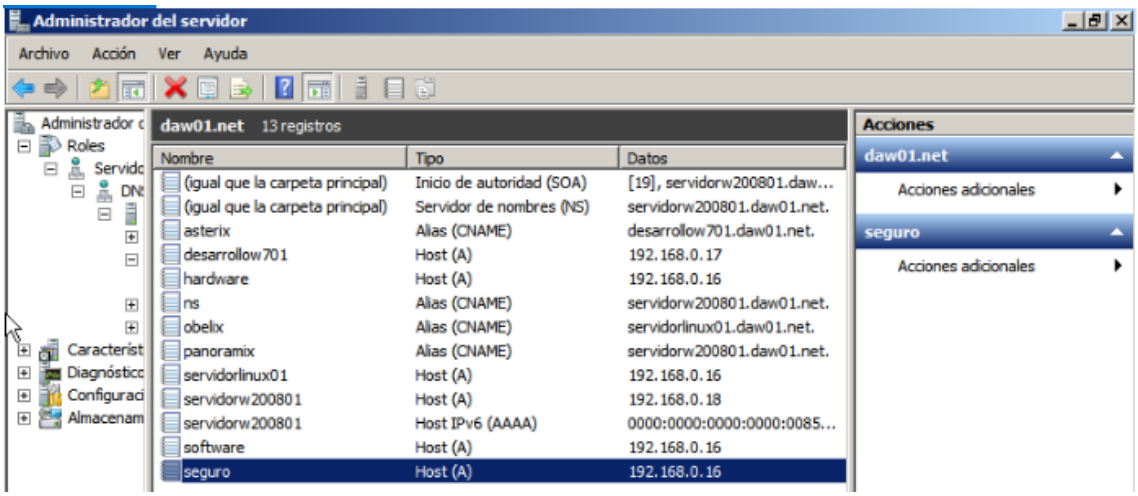

Figura 4.117: Configuración del servidor DNS en ServidorW2008XX

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/html/seguro**.
5. Crea el fichero de texto **/var/www/html/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 4.118.

openssl genrsa -out seguro.key 2048

```
servidorlinux016@servidorlinux01:~$ openssl genrsa -out seguro.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................................................+++
++
.............+++++
e is 65537 (0x010001)
servidorlinux016@servidorlinux01:~$ _
```

Figura 4.118: 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 4.119.

```
servidorlinux016@servidorlinux01:~$ openssl genrsa -out seguro.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................................................++
++
.............+++++
e is 65537 (0x010001)
servidorlinux016@servidorlinux01:~$ 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]:ES
State or Province Name (full name) [Some-State]:Bizkaia
Locality Name (eg, city) []:Bilbao
Organization Name (eg, company) [Internet Widgits Pty Ltd]:daw01
Organizational Unit Name (eg, section) []:daw01
Common Name (e.g. server FQDN or YOUR name) []:seguro.daw01.net
Email Address []:admin@daw01.net

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:romao12
An optional company name []:seguridad
servidorlinux016@servidorlinux01:~$ _
```

Figura 4.119: 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 4.120.

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

```
servidorlinux016@servidorlinux01:~$ openssl x509 -req -days 365 -in seguro.csr -signkey seguro.key
-out seguro.crt
Signature ok
subject=C = ES, ST = Bizkaia, L = Bilbao, O = daw01, OU = daw01, CN = seguro.daw01.net, emailAddress
 = admin@daw01.net
Getting Private key
servidorlinux016@servidorlinux01:~$
```

Figura 4.120: 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/sites-available/seguro** con las siguientes directivas, Figura 4.121.

```
<IfModule mod_ssl.c>
<VirtualHost *:443>
        ServerName seguro.daw01.net
        DocumentRoot /var/www/html/seguro
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/html/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 4.121**:** Fichero de configuración del servidor seguro

9. Deshabilita el servidor ssl por defecto.

sudo a2dissite default-ssl.conf

10. Habilita el servidor virtual seguro

sudo a2ensite seguro.conf

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***, Figura 4.122, 4.123 y 4.124.

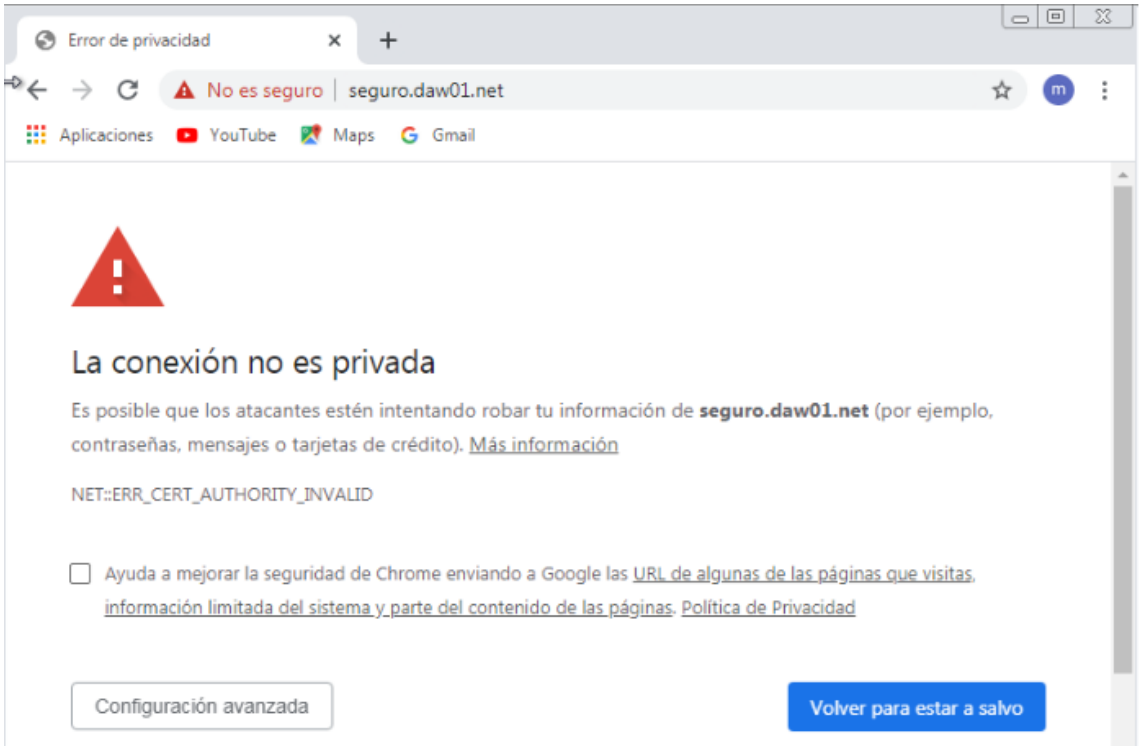

Figura 4.122: Conexión https

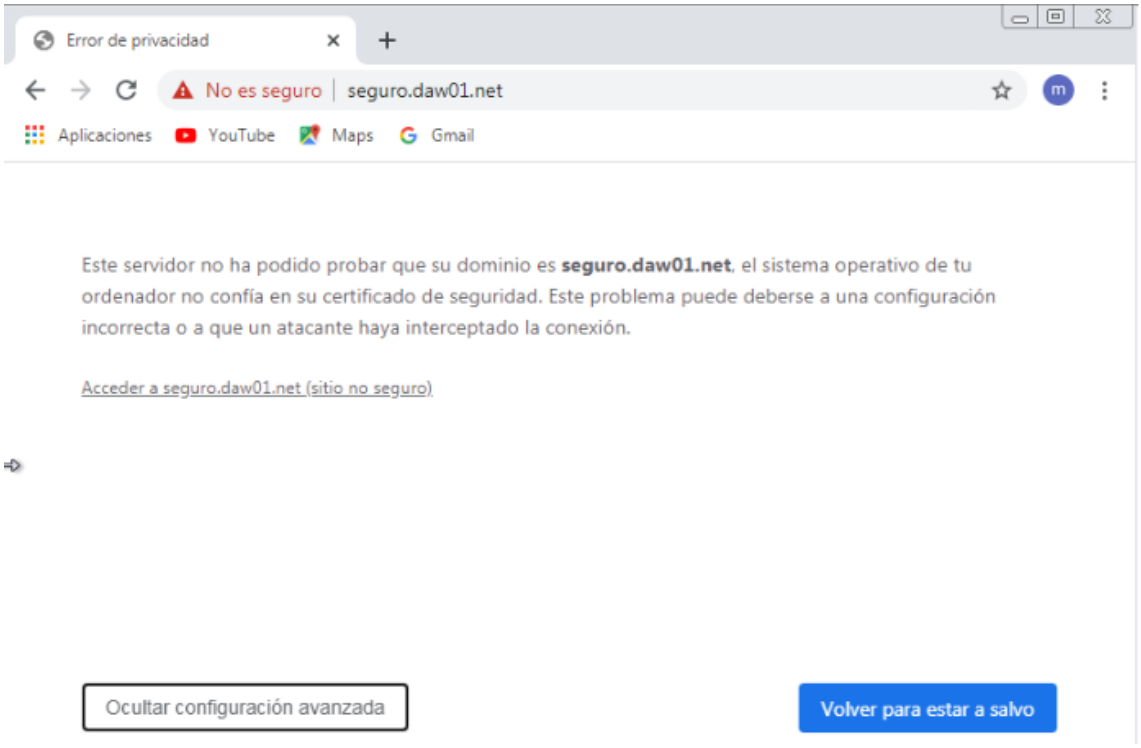

Figura 4.123: Conexión https

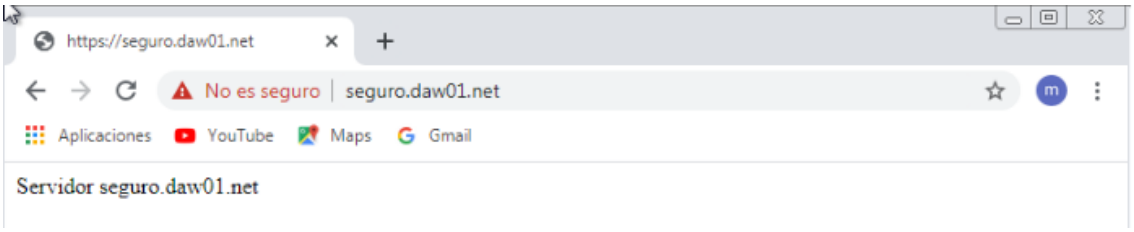

Figura 4.124: Conexión https