**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**

o Se servirá el fichero **index**.**html** si no se indica ningún fichero en la URL.

o Se mostrará un listado del directorio raíz si no se solicita ningún fichero.

o 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.

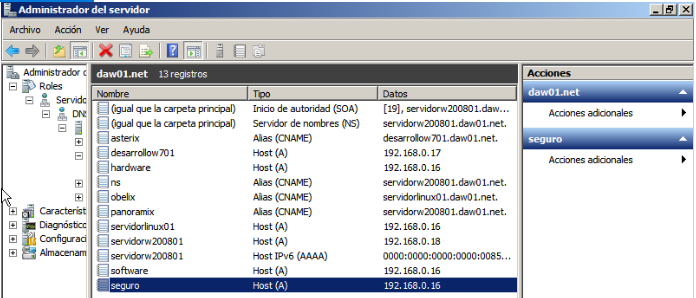


Figura 4.117: Configuración del servidor DNS en ServidorW2008XX

1. Asegúrate que **DesarrolloW7XX** utiliza el servidor DNS que has configurado.
2. Inicia una sesión en **ServidorLinuxXX** con un usuario con privilegios de administración.
3. Crea el directorio **/var/www/html/seguro**.
4. Crea el fichero de texto **/var/www/html/seguro/index.html** con el contenido que quieras.
5. Crea un certificado digital autofirmado usando openssl.
   1. Sitúate en el directorio **home** del usuario con el que has iniciado sesión.
   2. Crea una clave privada RSA de 2048 bit, Figura 4.118.

*openssl genrsa -out seguro.key 2048*

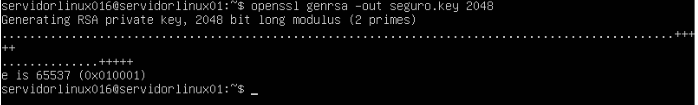
**

Figura 4.118: Creación de una clave privada

* 1. 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.al

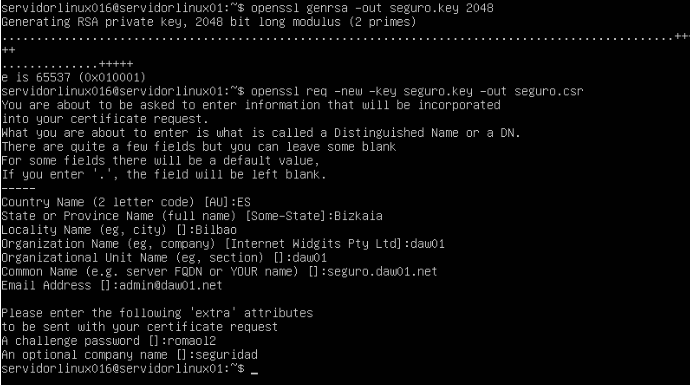


Figura 4.119: Creación de la solicitud del certificado

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.

de

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

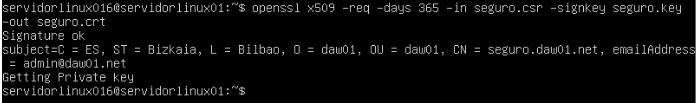


Figura 4.120: Creación del certificado digital autofirmado

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.

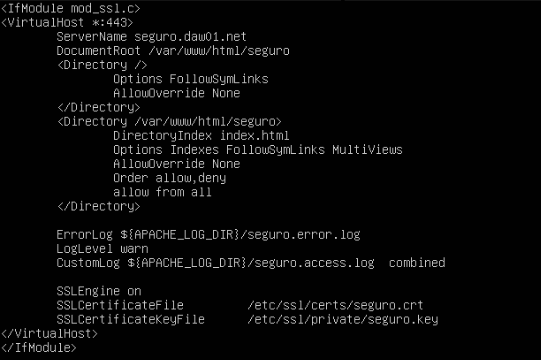


Figura 4.121**:** Fichero de configuración del servidor seguro

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.

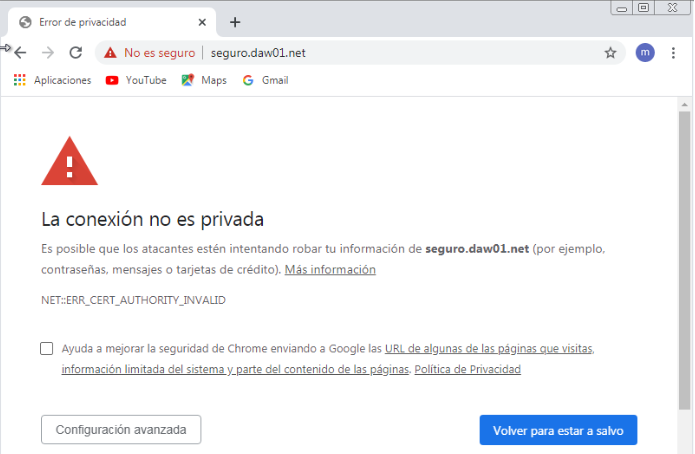
****

Figura 4.122: Conexión https

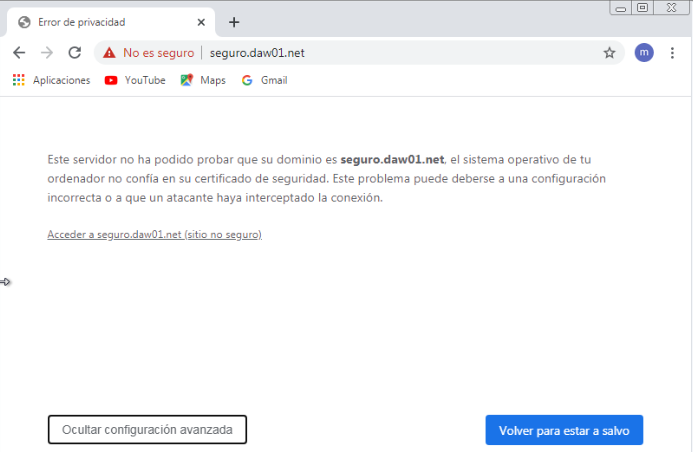


Figura 4.123: Conexión https

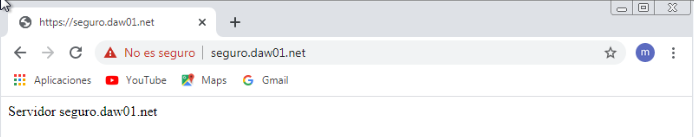


Figura 4.124: Conexión https