Práctica Servidor virtual HTTPS en Linux

Realiza la siguiente configuración en el servidor Apache instalado en UbuntuServerXX.

- 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 raíiz /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.

CONFIGURACIÓN 1: Servidor seguro.daw01.net

1. Configura el servidor DNS de Windows2008ServerXX para que resuelva el nombre **seguro**. **dawXX.net.** La dirección IP asociada al nombre será la IP de UbuntuServerXX, es decir, 10.12.1.xx

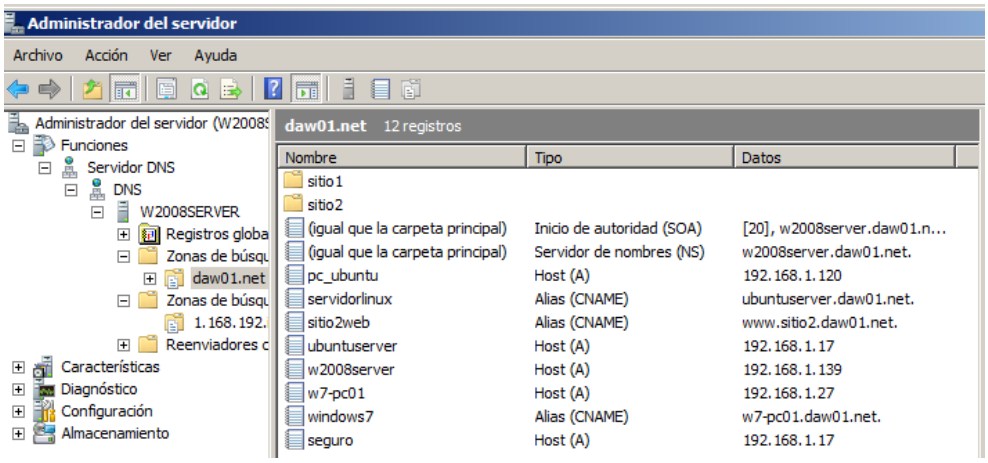


Figura 1: Configuración del servidor DNS en Windows2008ServerXX

Figura 2: Configuración de red del servidor windows2008

2. Asegurar que Windows7 utiliza el servidor DNS que has configurado.

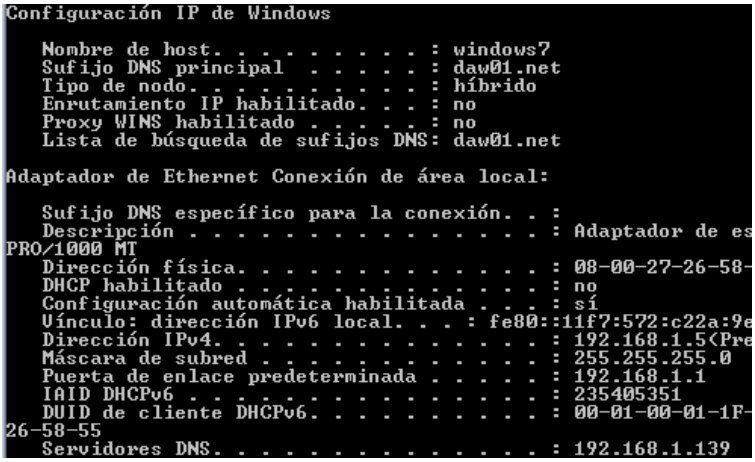


Figura 3: Configuración de red del cliente windows2007

3. Iniciar una sesión en UbuntuServerXX con un usuario con privilegios de administración.

4. Crear el directorio /var/www/html/seguro

```
sudo mkdir /var/www/html/seguro
```

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

```
sudo nano /var/www/html/seguro/index.html
```

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

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

```
alumno@ServidorLinux01:~$ openssl genrsa -out seguro.key 2048
Generating RSA private key, 2048 bit long modulus
..............................+++
.....................................................................................
.....................................................+++
e is 65537 (0x10001)
alumno@ServidorLinux01:~$
```

Figura 4: 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:

```
alumno@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]:Madrid
Locality Name (eg, city) []:Madrid
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 []:
An optional company name []:
alumno@ServidorLinux01:~$ _
```

Figura 5: Creación de la solicitud del certificado

Esta solicitud de certificado se podrá 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

```
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 6: 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:

```
<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin webmaster@localhost
                ServerName seguro.daw01.net
                DocumentRoot /var/www/html/seguro
                <Directory /var/www/html/seguro>
                Options Indexes
                AllowOverride None
                Require all granted
                </Directory>

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

                SSLEngine on

                SSLCertificateFile      /etc/ssl/certs/seguro.crt
                SSLCertificateKeyFile /etc/ssl/private/seguro.key

                <FilesMatch "\.(cgi|shtml|phtml|php)$">
                                SSLOptions +StdEnvVars
                </FilesMatch>
                <Directory /usr/lib/cgi-bin>
                                SSLOptions +StdEnvVars
                </Directory>

        </VirtualHost>
</IfModule>
```

Figura 7: 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.

```
usuario@ubuntuserver01:/etc/apache2/sites-enabled$ ls -la
total 12
drwxr-xr-x 2 root root 4096 feb  6 12:12 .
drwxr-xr-x 9 root root 4096 ene 10 19:57 ..
lrwxrwxrwx 1 root root   35 ene 18 20:59 000-default.conf -> ../sites-available/000-default.conf
-rw-r--r-- 1 root root 1332 dic  9 20:04 000-default.conf.BAK
lrwxrwxrwx 1 root root   31 ene  8 18:48 daw.net.conf -> ../sites-available/daw.net.conf
lrwxrwxrwx 1 root root   34 ene 10 19:21 despliegue.conf -> ../sites-available/despliegue.conf
lrwxrwxrwx 1 root root   32 ene 11 18:34 entornos.conf -> ../sites-available/entornos.conf
lrwxrwxrwx 1 root root   30 feb  6 11:31 seguro.conf -> ../sites-available/seguro.conf
usuario@ubuntuserver01:/etc/apache2/sites-enabled$ _
```

Figura 8: Servidor seguro activo

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

sudo service apache2 restart/reload

sudo */etc/*init.d/apache2 stop y sudo */etc/*init.d/apache2 start

también:

```
usuario@ubuntuserver01:/etc/apache2/sites-enabled$ sudo systemctl reload apache2
usuario@ubuntuserver01:/etc/apache2/sites-enabled$ _
```

Figura 9: reinicio de apache

13. Desde Windows7XX abre el navegador y establece una conexión a https:\\seguro. dawXX.net.

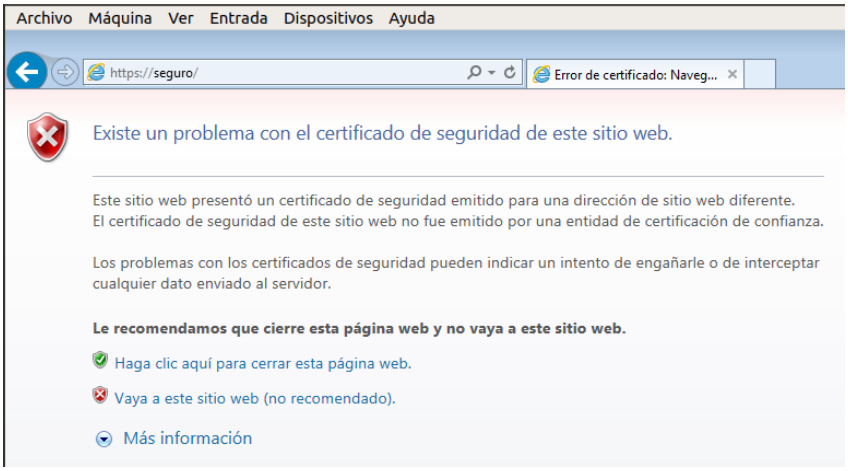


Figura 10: Conexión https desde Windows2007

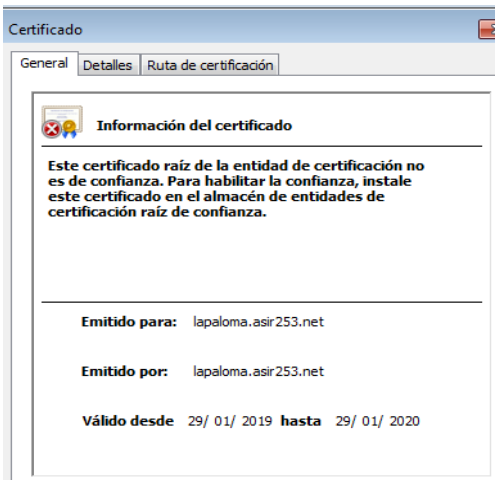


Figura 11: Certificado autofirmado

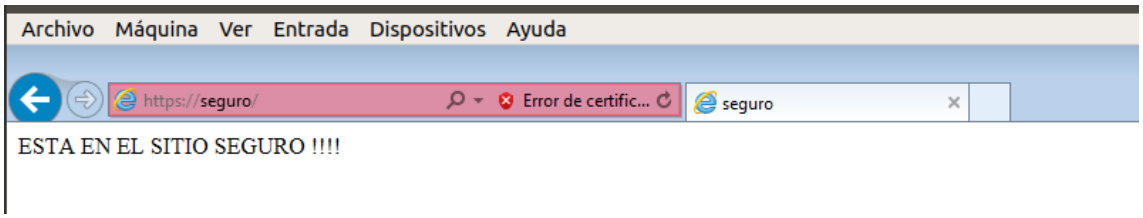
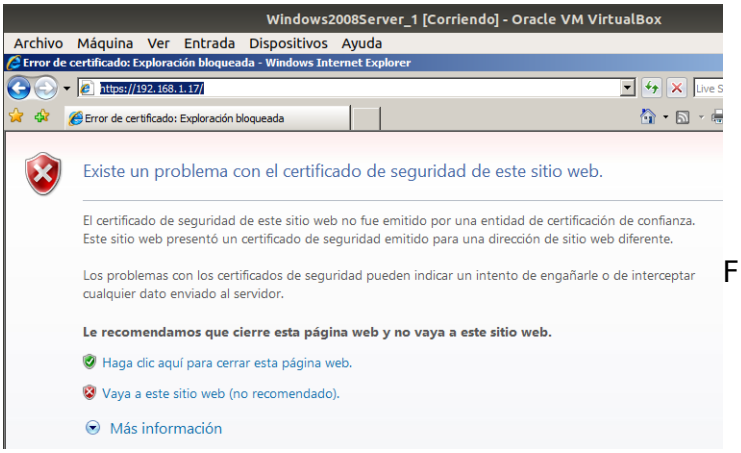


Figura 12: Aceptando los riesgos ...



F

Figura 13: Conexión https desde Windows2008

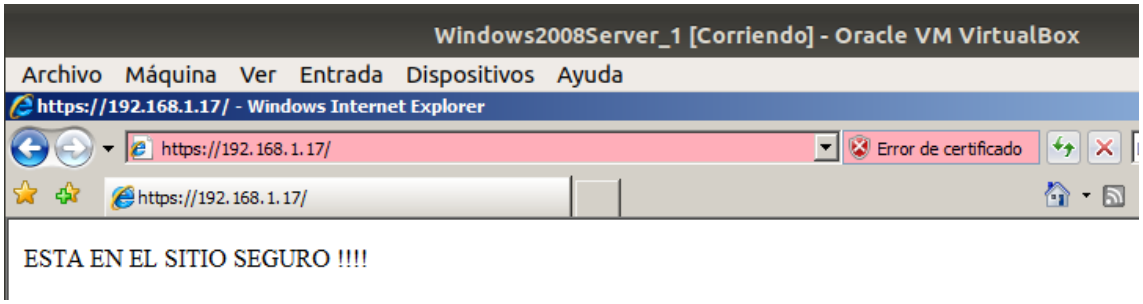


Figura 14: Conexión https desde Windows2008

CONFIGURACIÓN 2: Servidor seguroUbuntu.asir01.net

1. Configura el servidor DNS de UbunruServerXX para que resuelva el nombre **seguroUbuntu**. **asirXX.net.** La dirección IP asociada al nombre será la IP de UbuntuServerXX, es decir, 10.12.1.xx

```
 GNU nano 2.9.3                                  db.asir01.net

;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ubuntuserver01 root.ubuntuserver. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ubuntuserver01.asir01.net.
ubuntuserver01  IN      A       192.168.1.17
W2008Server.asir01.net. IN A 192.168.1.139
W7-PC01[redacted]IN A 192.168.1.27
windows IN      CNAME   W7-PC01
daw.net IN A 192.168.1.17
entornos        IN[redacted]A 192.168.1.17
seguroUbuntu            IN[redacted]A       192.168.1.17
```

Figura 2.1: Fichero de zona directa para el dominio asir01.net

```
 GNU nano 2.9.3                                  db.1.168.192

;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ubuntuserver01.asir01.net. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ubuntuserver01.asir01.net.
17      IN      PTR     ubuntuserver01
27[redacted]IN      PTR     W7-PC01
139     IN      PTR     W2008Server
17      IN[redacted]PTR     entornos
17      IN      PTR     seguroUbuntu
```

Figura 2.2: Fichero de zona inversa para el dominio 1.168.192.in-addr.arpa.

```
usuario@ubuntuserver01:/etc/bind$
usuario@ubuntuserver01:/etc/bind$ sudo service bind9 restart
```

Figura 2.3: Reinicio servidor DNS (bind9)

2. Configurar el cliente DNS de Windows7 para que utilice el servidor DNS que has configurado (modificar IP del DNS y sufijo de red).

Figura 2.4: Configuración cliente Windows2007

3.- Crear la carpeta seguroUbuntu dentro del DocumentRoot y un fichero a servir por defecto:

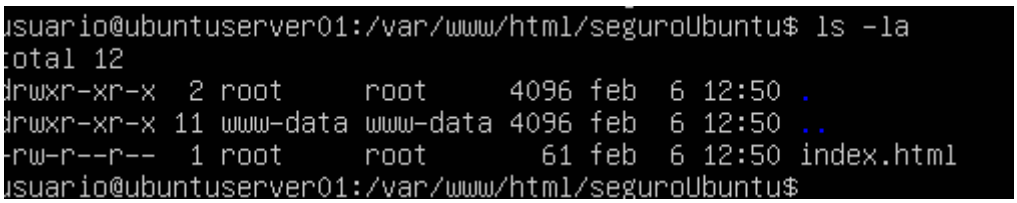
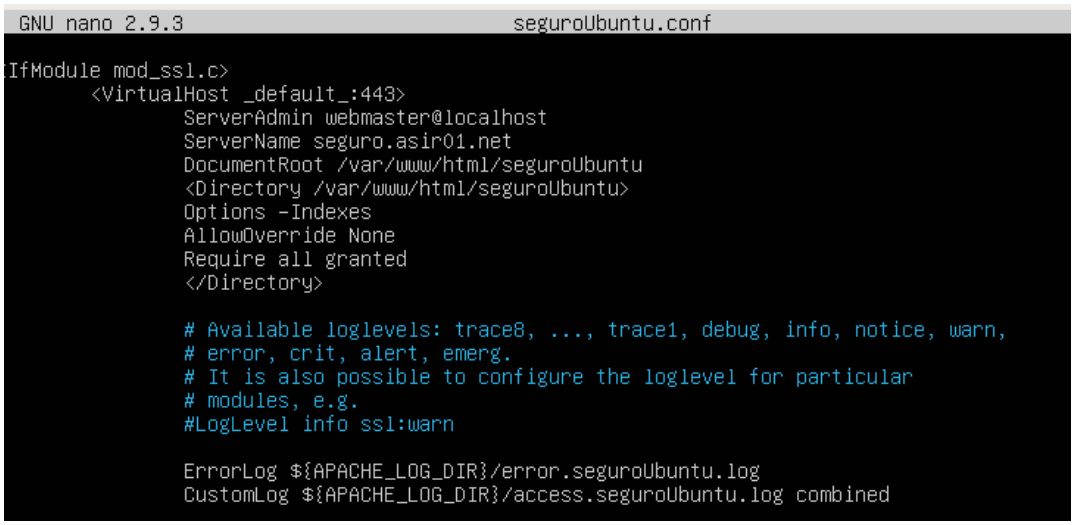


Figura 2.5: Configuración del DocumentRoot del nuevo sitio a servir.

4.- Crear el sitio seguroUbuntu.



Sugerencia: se puede copiar el fichero seguro.conf y modificar el nombre del sitio, el DocumentRoot, fichero de errores y accesos, etc.

Figura 2.6: Configuración del sitio seguroUbuntu

5.- Deshabilitar el sitio seguro, habilitar seguroUbuntu y recargar apache.

```
usuario@ubuntuserver01:/etc/apache2/sites-available$
usuario@ubuntuserver01:/etc/apache2/sites-available$
usuario@ubuntuserver01:/etc/apache2/sites-available$ sudo a2dissite seguro.conf
Site seguro disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
usuario@ubuntuserver01:/etc/apache2/sites-available$ sudo a2ensite seguroUbuntu.conf
Enabling site seguroUbuntu.
To activate the new configuration, you need to run:
  systemctl reload apache2
usuario@ubuntuserver01:/etc/apache2/sites-available$ sudo systemctl reload apache2
usuario@ubuntuserver01:/etc/apache2/sites-available$
```

Figura 2.7: Activación del sitio seguroUbuntu y de apache.

6.- Comprobación desde el cliente Windows 2007

Figura 2.8: Petición desde la máquina de Windows2007

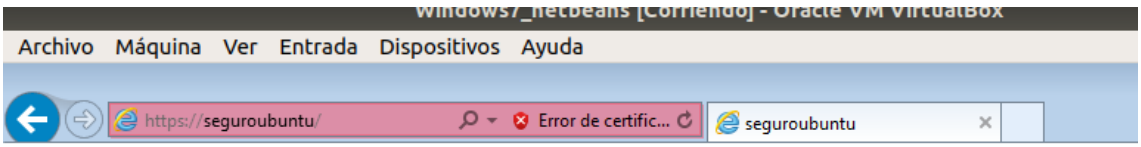


Figura 2.9: Petición desde la máquina de Windows2007

¿Qué operación se ha hecho en el servidor de ubuntu, para que muestre esta página?

Desde cualquier máquina que no sea la de Windows2007, ¿podremos acceder al servidor seguro que acabamos de configurar?. Indicar cómo.