

Práctica 5.21: Servidor virtual HTTPS por defecto en *Windows*

Realiza la siguiente configuración en el servidor *Apache* instalado en **ServidorW2008XX**.

- Deshabilita los **servidores virtuales** creados en las prácticas anteriores.
- Habilita el modulo *mod_ssl*.
- Habilita el servidor virtual *ssl* por defecto

Prueba la configuración.

1. Inicia una sesión en **ServidorW2008XX** con un usuario con privilegios de administración.
2. Deshabilita los servidores virtuales creados en prácticas anteriores.
 - 2.1. Edita el fichero **C:\Program Files\Apache Software Foundation\Apache2.2\conf\httpd.conf** y comenta la directiva **Include** del fichero **conf/extra/httpd-vhost.conf**.
 - 2.2. Reinicia el servidor para que los cambios tengan efecto.
3. Edita el fichero **C:\Program Files\Apache Software Foundation\Apache2.2\conf\httpd.conf** y habilita el módulo **mod_ssl** eliminando el comentario de la directivas **LoadModule**, Figura 1.

```
#LoadModule mime_magic_module modules/mod_mime_magic.so
LoadModule negotiation_module modules/mod_negotiation.so
#LoadModule proxy_module modules/mod_proxy.so
#LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
#LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
#LoadModule proxy_connect_module modules/mod_proxy_connect.so
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
#LoadModule proxy_http_module modules/mod_proxy_http.so
#LoadModule proxy_scgi_module modules/mod_proxy_scgi.so
#LoadModule reqtimeout_module modules/mod_reqtimeout.so
#LoadModule rewrite_module modules/mod_rewrite.so
LoadModule setenvif_module modules/mod_setenvif.so
#LoadModule spelling_module modules/mod_spelling.so
LoadModule ssl_module modules/mod_ssl.so
#LoadModule status_module modules/mod_status.so
#LoadModule substitute_module modules/mod_substitute.so
#LoadModule unique_id_module modules/mod_unique_id.so
LoadModule userdir_module modules/mod_userdir.so
#LoadModule usertrack_module modules/mod_usertrack.so
#LoadModule version_module modules/mod_version.so
```

Figura 1: Habilitar el módulo *mod_ssl*

4. Habilita el servidor virtual *ssl* defecto (*default-ssl*) de *Apache*. Edita el fichero **C:\Program Files\Apache Software Foundation\Apache2.2\conf\httpd.conf** y eliminana el comentario de la directiva **Include** del fichero **conf/extra/httpd-ssl.conf**, Figura 2.

```
#Include conf/extra/httpd-vhosts.conf

# Local access to the Apache HTTP Server Manual
#include conf/extra/httpd-manual.conf

# Distributed authoring and versioning (WebDAV)
#include conf/extra/httpd-dav.conf

# Various default settings
#include conf/extra/httpd-default.conf

# Secure (SSL/TLS) connections
#include conf/extra/httpd-ssl.conf
#
# Note: The following must be present to support
#       starting without SSL on platforms with no /dev/random equivalent
#       but a statically compiled-in mod_ssl.
#
<IfModule ssl_module>
SSLRandomSeed startup builtin
```

Figura 2: Habilitar el servidor virtual https

5. Si observas en el fichero **C:\Program Files\Apache Software Foundation\Apache2.2\conf\extra\httpd-ssl.conf** existen dos directivas para definir el certificado digital y la clave privada del servidor (que debemos crear), Figura 3.

```
#SSLCipherSuite RC4-SHA:AES128-SHA:HIGH:MEDIUM:!aNULL:!MD5
#SSLHonorCipherOrder on

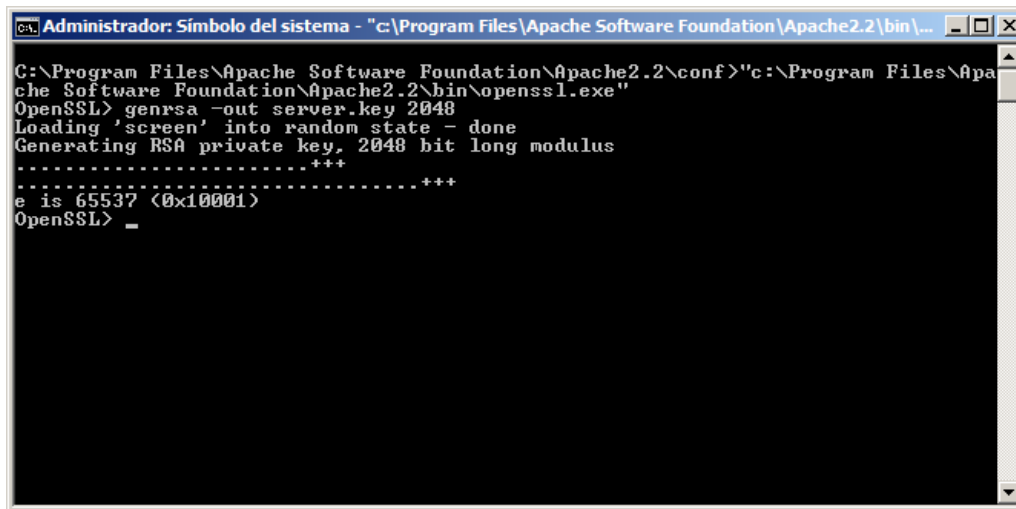
# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. Keep
# in mind that if you have both an RSA and a DSA certificate you
# can configure both in parallel (to also allow the use of DSA
# ciphers, etc.)
SSLCertificateFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/server.crt"
#SSLCertificateFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/server-dsa.crt"

# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/server.key"
#SSLCertificateKeyFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/server-dsa.key"
```

Figura 3: Fichero **C:\Program Files\Apache Software Foundation\Apache2.2\conf\extra\httpd-ssl.conf**

6. Crea un certificado digital autofirmado usando *openssl*.
 - 6.1. Abre un terminal.
 - 6.2. Accede al directorio **C:\Program Files\Apache Software Foundation\Apache2.2\conf**.
 - 6.3. Ejecuta el comando **C:\Program Files\Apache Software Foundation\Apache2.2\bin\openssl**.
 - 6.4. Crea una clave privada RSA de 2048 bit, Figura 4.

```
Openssl> genrsa -out server.key 2048
```



```

C:\Program Files\Apache Software Foundation\Apache2.2\bin>"c:\Program Files\Apache Software Foundation\Apache2.2\bin\openssl.exe"
OpenSSL> genrsa -out server.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
e is 65537 (0x10001)
OpenSSL> _

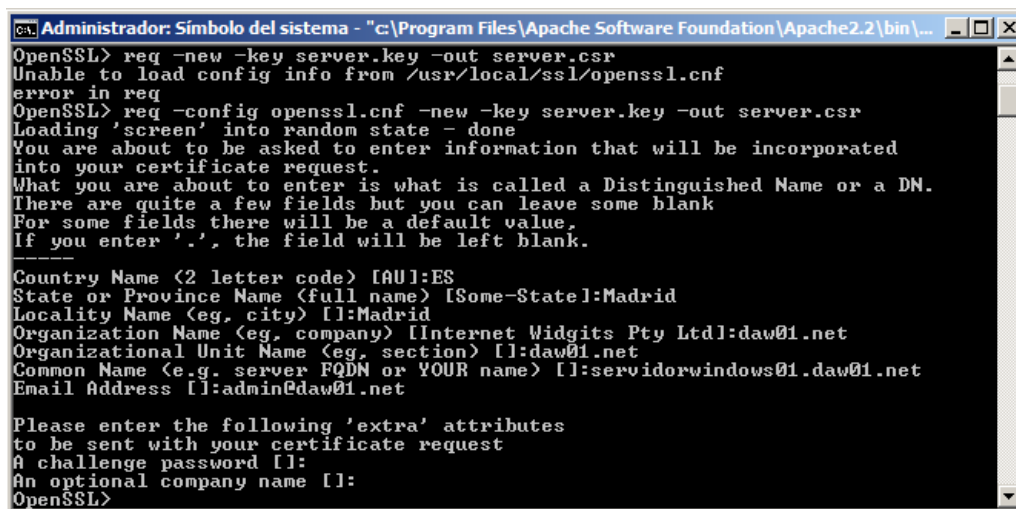
```

Figura 4: Creación de una clave privada

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

```
OpenSSL> req -config openssl.cnf -new -key server.key -out server.csr
```

Introduce los datos del certificado, Figura 5



```

OpenSSL> req -new -key server.key -out server.csr
Unable to load config info from /usr/local/ssl/openssl.cnf
error in req
OpenSSL> req -config openssl.cnf -new -key server.key -out server.csr
Loading 'screen' into random state - done
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-Statel:Madrid
Locality Name (eg, city) []:Madrid
Organization Name (eg, company) [Internet Widgits Pty Ltd]:daw01.net
Organizational Unit Name (eg, section) []:daw01.net
Common Name (e.g. server FQDN or YOUR name) []:servidorwindows01.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 []:
OpenSSL>

```

Figura 5: 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.

6.6. Crea el certificado digital autofirmado usando la clave privada, Figura 6.

```
OpenSSL> x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

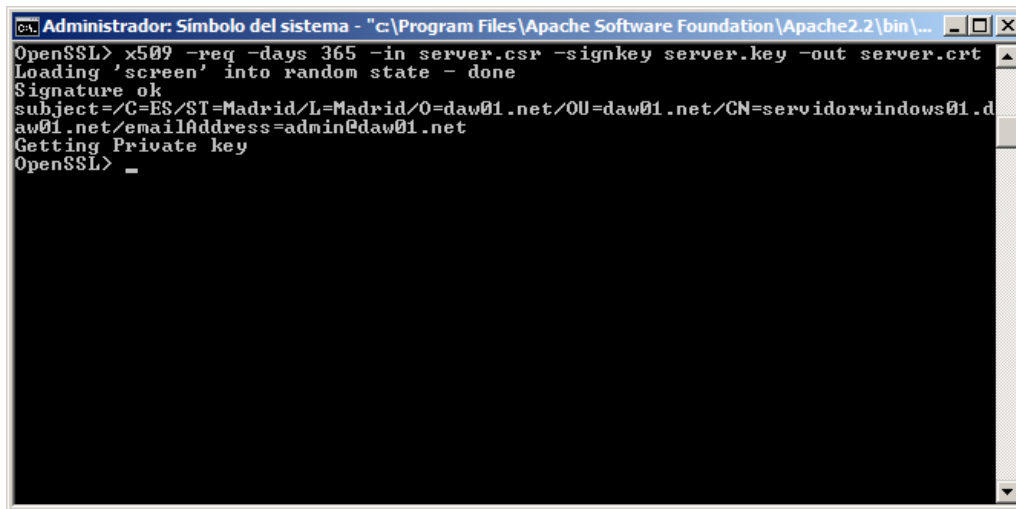


Figura 6: Creación del certificado digital autofirmado

7. Reinicia el servidor para que los cambios tengan efecto.
8. Verifica que el servidor escucha en los puertos 80/TCP y 443/TCP.

```
netstat -a -p TCP -n
```

9. Desde **DesarrolloW7XX** abre el navegador y establece una conexión a `http://192.168.1.18`, Figura 7.

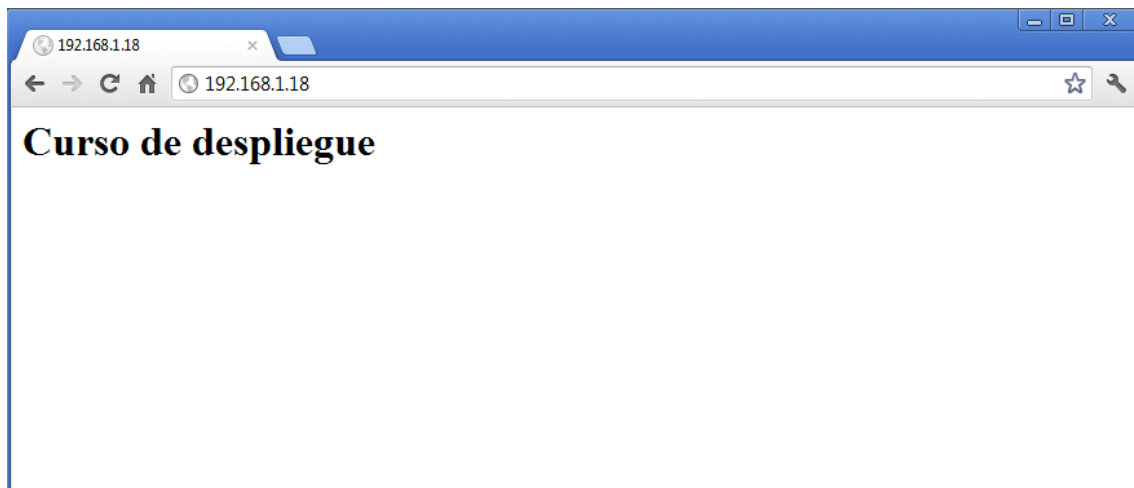


Figura 7: Conexión http

10. Desde **DesarrolloW7XX** abre el navegador y establece una conexión a `https://192.168.1.18`, Figuras 8 y 9.

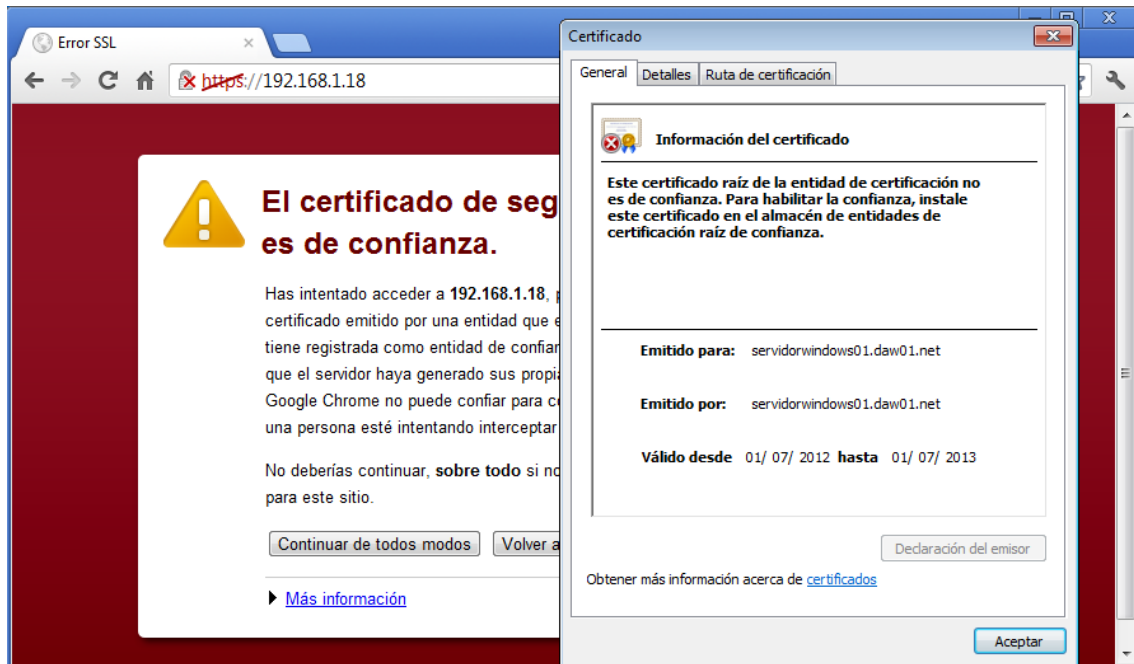


Figura 8: Conexión https

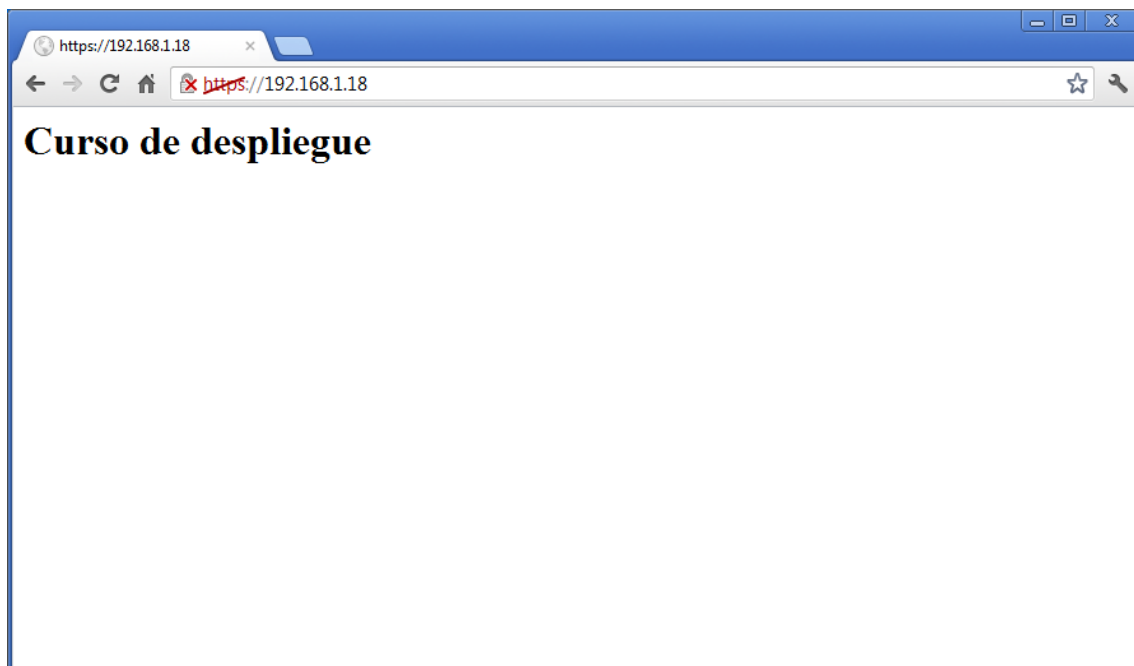


Figura 9: Conexión https