




Práctica Servidor virtual HTTPS por defecto en Windows

Realiza la siguiente configuración en el servidor Apache instalado en Windows2008ServerXX.

-  Deshabilita los servidores virtuales creados en las practicas anteriores.
-  Habilita el modulo mod ssl.
-  Habilita el servidor virtual ssl por defecto

Prueba la configuración.

1. Inicia una sesión en Windows2008ServerXX con un usuario con privilegios de administración.
2. Deshabilita los servidores virtuales creados en prácticas anteriores.
 - 2.1. Edita el fichero C:\Apache2\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:\Apache2\conf\httpd.conf y habilita el modulo ssl eliminando el comentario de la directivas LoadModule.

```
#LoadModule unique_id_module modules/mod_unique_id.so
LoadModule userdir_module modules/mod_userdir.so
#LoadModule usertrack_module modules/mod_usertrack.so
#LoadModule vhost_alias_module modules/mod_vhost_alias.so
LoadModule ssl_module modules/mod_ssl.so
```

Figura 1: Habilitar el módulo mod ssl

4. Habilita el servidor virtual ssl defecto (default-ssl) de Apache. Edita el fichero C:\Apache2.2\conf\httpd.conf y elimina el comentario de la directiva Include del fichero conf/extra/httpd-ssl.conf.

```
#include conf/extra/httpd-ssl.conf
# virtual hosts
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
#
```

Figura 2: Habilitar el servidor virtual https

5. Si observas en el fichero C:\Apache2.2\conf\extra\httpd-ssl.conf existen dos directivas para definir el certificado digital y la clave privada del servidor (que debemos crear).

```
<VirtualHost _default_:443>
# General setup for the virtual host
DocumentRoot "C:/apache2/htdocs"
ServerName w2008Server.daw253.net:443
ServerAdmin admin@daw253.net
ErrorLog C:/apache2/logs/error_log
TransferLog C:/apache2/logs/access_log

SSLEngine on
SSLCertificateFile C:/apache2/conf/secreto.crt
SSLCertificateKeyFile C:/apache2/conf/secreto.key
<FilesMatch "\.(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
</FilesMatch>
<Directory "C:/apache2/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>

BrowserMatch ".MSIE.*" \
    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0

CustomLog C:/apache2/logs/ssl_request_log \
    "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"

</VirtualHost>
```

Figura 3: Fichero C:\Apache2\conf\extra\httpd-ssl.conf

6. Crea un certificado digital autofirmado usando openssl

6.1. Abre un terminal.

6.2. Accede al directorio C:\Apache2\conf.

6.3. Ejecuta el comando

C:\Apache2\bin>openssl.

6.4. Crea una clave privada RSA de 2048 bit.

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

```
c:\apache2\conf>openssl genrsa -out secreto.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
```

Figura 4: Creación de una clave privada

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

```
Openssl> req -config ../conf/openssl.cnf -new -key server.key -out server.csr
```

Introduce los datos del certificado, Figura 5

```
c:\apache2\conf>openssl req -config openssl.cnf -new -key secreto.key -out secreto.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]:daw253.net
Organizational Unit Name (eg, section) []:daw253
Common Name (eg, YOUR name) []:secreto
Email Address []:secreto@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:root
An optional company name []:
```

Figura 5: Creación de la solicitud del certificado

Esta solicitud de certificado se la podríamos 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.

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

```
c:\apache2\conf>openssl x509 -req -days 365 -in secreto.csr -signkey secreto.key
-out secreto.crt
Loading 'screen' into random state - done
Signature ok
subject=/C=es/ST=madrid/L=madrid/O=daw253.net/OU=daw253/CN=secreto/emailAddress=
secreto@gmail.com
Getting Private key
c:\apache2\conf>_
```

Figura 6: Creación del certificado digital autofirmado

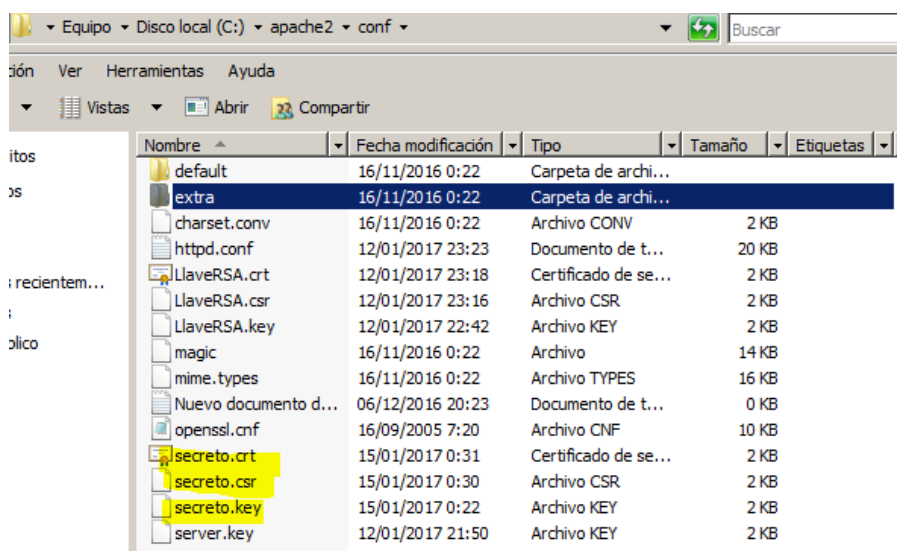


Figura 7: Ficheros creados

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

`httpd -k start` o desde el monitor  o desde el panel de control/servicios

8. Verifica que el servidor escucha en los puertos 80/TCP y 443/TCP.

`netstat -a -p TCP -n`

9. Desde el propio servidor Windows2008 abre el navegador y establece una conexión a `https://10.12.2.XX` o `https://localhost`

Creamos un directorio seguro dentro del DocumentRoot y en él un `index.html`:

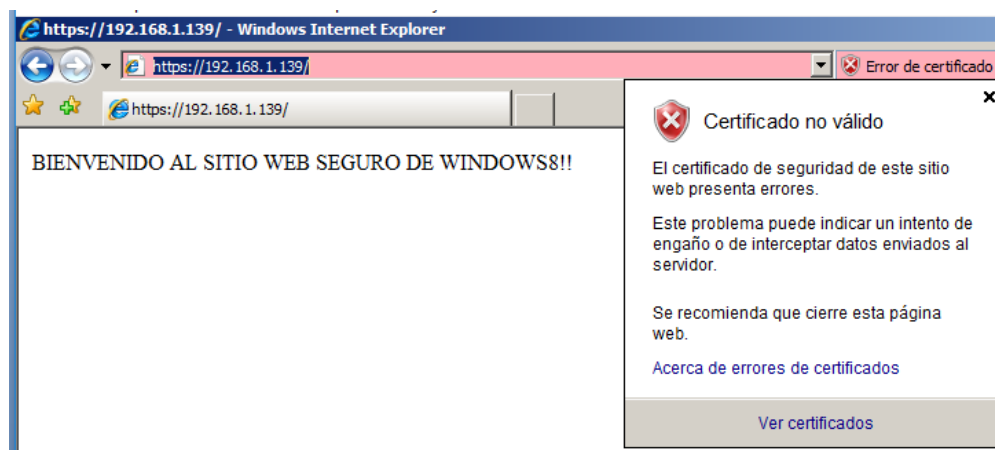


Figura 8: Conexión https

Desde el propio W2008:



Si quisiéramos darle a ese directorio un comportamiento determinado, lo haríamos dentro de un contenedor <Directory C:/apache2/htdocs/seguo>

El fichero de configuración C:/apache2/conf/extra/httpd_ssl.conf contiene:

```
Listen 443
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl .crl

<VirtualHost _default_:443>
```

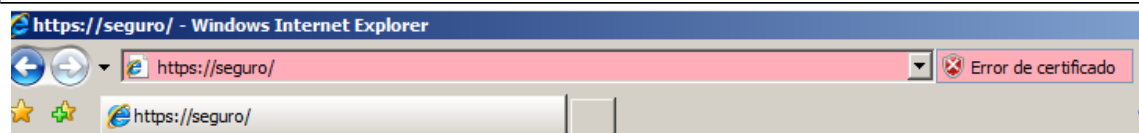
```

DocumentRoot "C:/apache2/htdocs/seguro"
ServerName seguro.daw253.net:443
ServerAdmin admin@daw253.net
ErrorLog C:/apache2/logs/error_log
TransferLog C:/apache2/logs/access_log

SSLEngine on
SSLCertificateFile C:/apache2/conf/secreto.crt
SSLCertificateKeyFile C:/apache2/conf/secreto.key

</VirtualHost>

```

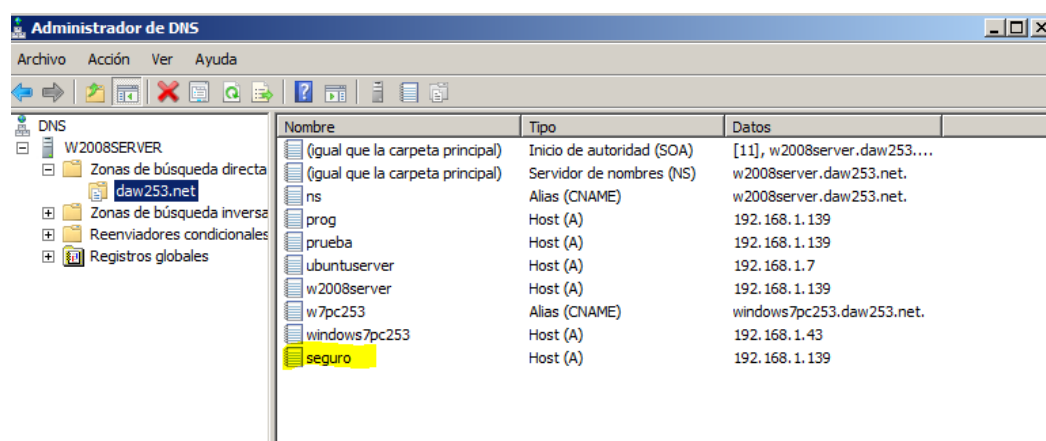


BIENVENIDO AL SITIO WEB SEGURO DE WINDOWS8!!

10. Desde DesarrolloW7XX abre el navegador y establece una conexión https a la IP del servidor Windows2008 : https\\10.12.3.XX.

11. Desde DesarrolloW7XX abre el navegador y establece una conexión https al servidor seguro configurado en el servidor Windows2008 : https\\seguro.daw253.net y https\\seguro. Explica todos los pasos necesarios.

Para poder acceder al sitio virtual seguro, se añadirá un registro A en el servidor de Windows 2008 al fichero de zona directa:



En la M.V de Windows 7 se modificará el cliente DNS para que tenga la dirección del servidor Windows 2008.

Nota: Hay que desactivar el firewall o activar reglas de entradas y salida que permitan la conexión en el servidor windows2008.

```

:\Users\alumno>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : windows7
Sufijo DNS principal . . . . : daw253.net
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . : no
Lista de búsqueda de sufijos DNS: daw253.net

Adaptador de Ethernet Conexión de área local:

Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Adaptador de escritorio Intel(R)
PRO/1000 MT
Dirección física. . . . . : 08-00-27-26-58-55
DHCP habilitado . . . . . : no
Configuración automática habilitada . . : sí
Vínculo: dirección IPv6 local. . . : fe80::11f7:572:c22a:9e5b%11(Preferido)
Dirección IPv4. . . . . : 192.168.1.120(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . : 192.168.1.1
IAD DHCPv6 . . . . . : 235405351
DUID de cliente DHCPv6. . . . . : 00-01-00-01-1F-78-31-9F-08-00-27-
6-58-55
Servidores DNS. . . . . : 192.168.1.139
8.8.4.4
NetBIOS sobre TCP/IP . . . . . : habilitado

```

