Configuración Servicio Web en Windows 2012 Server r2

El servicio web es un programa que implementa el protocolo http (*hypertext transfer protocol*). Este programa se mantiene a la espera de peticiones por parte de clientes de tipo navegador web y responde a estas peticiones de forma adecuada en el navegador del cliente.

Las páginas web o los documentos servidor van en formato HTML (*hypertext markup language*). El servidor web implementa el protocolo HTTTP o HTTPS (*hypertext transfer protocol secure*), que es una variante segura del protocolo HTTP.

El HTTP define la sintaxis y la semántica que usan los elementos de programación de la arquitectura web para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema de petición-respuesta entre un cliente y un servidor.

Los puertos que habitualmente usa el servicio son los puertos 80/TCP para HTTP y 443/TCP para HTTPS.

Se sitúan fuera de la red interna, para ser visibles desde Internet. En la denominada red DMZ.

La organización de esta práctica se resume en los siguientes pasos:

1. Objetivos
2. Preparativos
3. Direccionamiento
4. Instalación
5. Configuración básica
6. Configuración avanzada
7. Configuración segura
8. Creación sitio web seguro
9. Consulta de registros

1. Objetivos

En esta práctica aprendemos a instalar un servidor web. Primero hacemos una configuración básica y comprobamos el funcionamiento. Después hacemos una configuración segura del tipo HTTPS en que se usa un certificado en el servidor para cifrar las comunicaciones con el protocolo SSL. Al final vemos como se realizan tareas de resolución de incidencias consultando los registros que genera la aplicación.

La nueva máquina tendrá de nombre WWW2012.

2. Preparativos

La nueva máquina tendrá de nombre WWW2012.

3. Direccionamiento

El paso siguiente es configurar la tarjeta de red del servidor.

NIC1:

Dirección IP:	10.XX.99.209
Máscara de Subred:	255.255.255.0
Puerta de Enlace:	10.XX.99.1

Servidor DNS Preferido: 158.42.250.65

Servidor DNS Alternativo: 158.43.250.195

NIC2:

Dirección IP: 10.XX.100.209

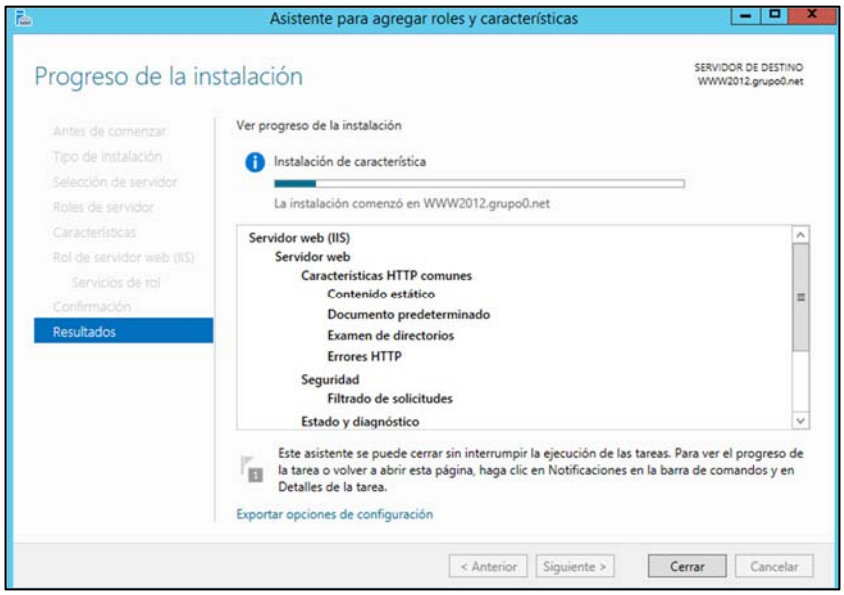
Máscara de Subred: 255.255.255.0

4. Instalación

El primer paso para la instalación del servicio http es instalar en servicio IIS. Proceda a su instalación.

Vaya pasando por las diferentes pantallas de la instalación del servicio con las opciones propuestas por defecto.

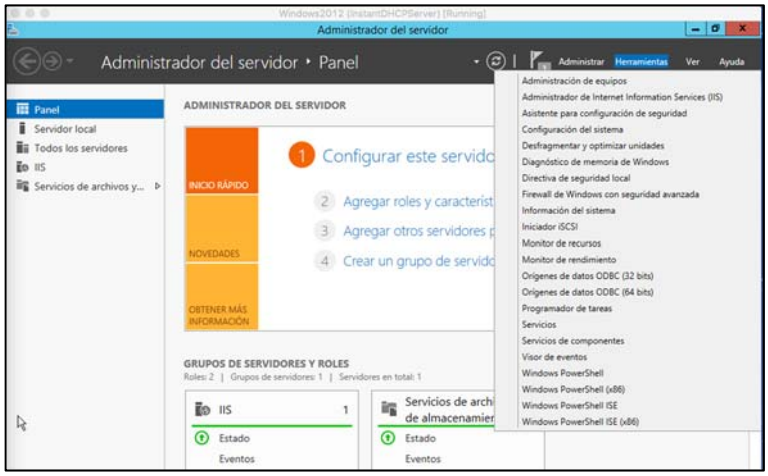
A continuación se muestra la última pantalla de la instalación del servicio IIS (conviene ir leyendo lo que nos va indicando cada pantalla en el proceso de la instalación).



5. Configuración básica

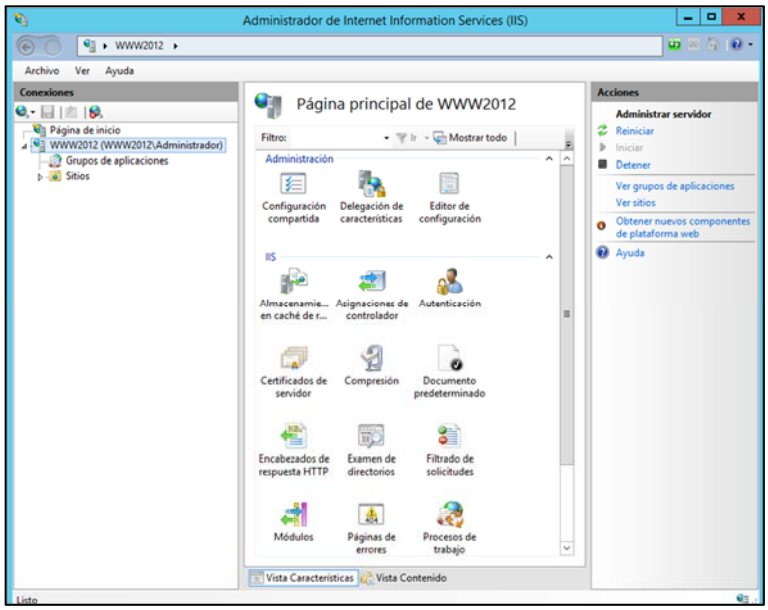
A continuación vamos a proceder a realizar una configuración básica y donde encontrar las herramientas para administrar el servidor.

Panel del Administrador del Servidor→Herramientas→Administrador de Internet Information Services (IIS).

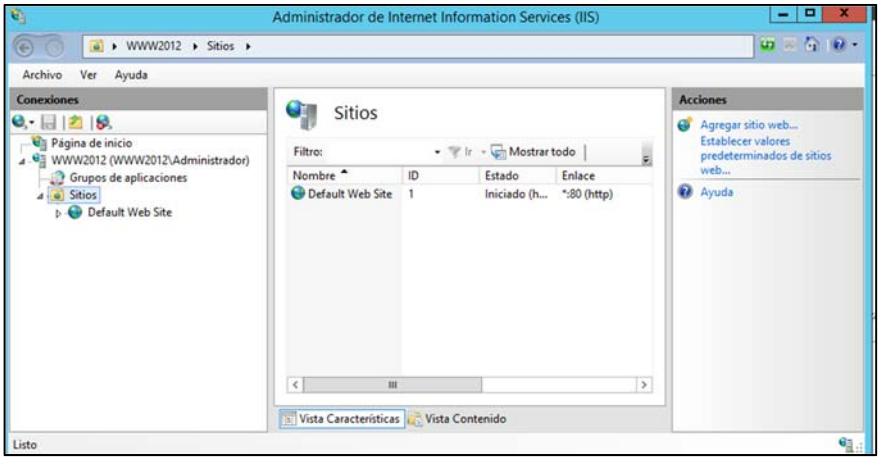


Nos aparecerá la siguiente pantalla:

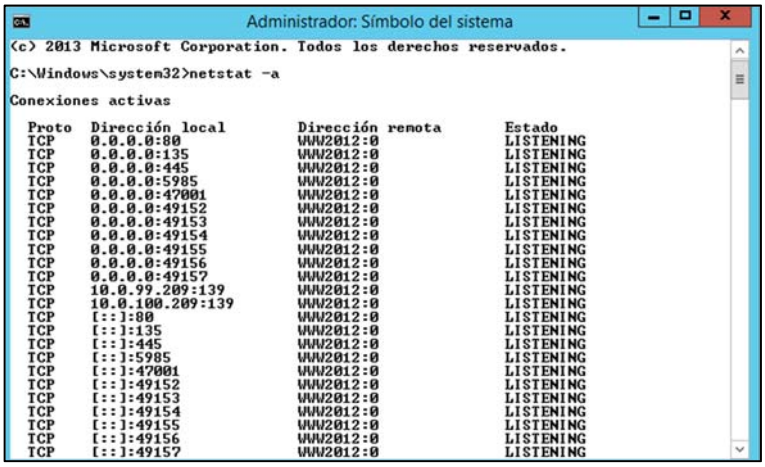
Hacemos clic en WWW2012(WWW2012\Administrador) (le indicamos no a la ventana emergente). Las opciones generales se encuentran en la parte central del Administrador:



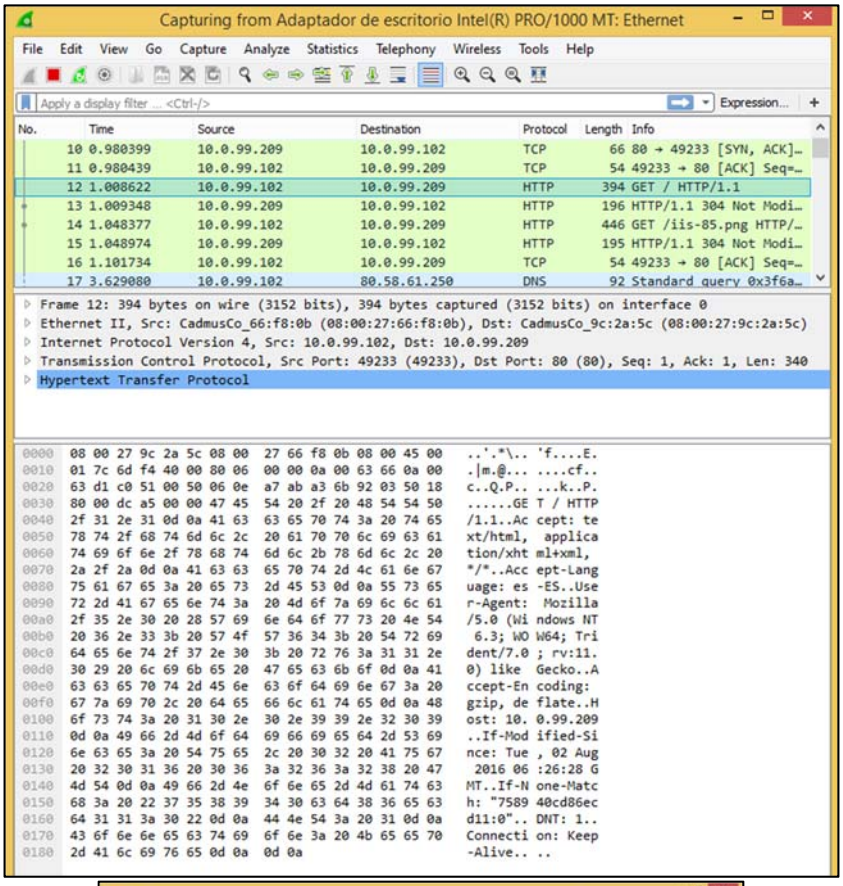
Un servidor web físico puede gestionar más de un servidor web virtual. Haciendo clic en ***Sitios*** aparecen los servidores virtuales o lugares web creados. En estos momentos sólo nos aparece uno, el creado por defecto, denominado ***Default Web Server.***

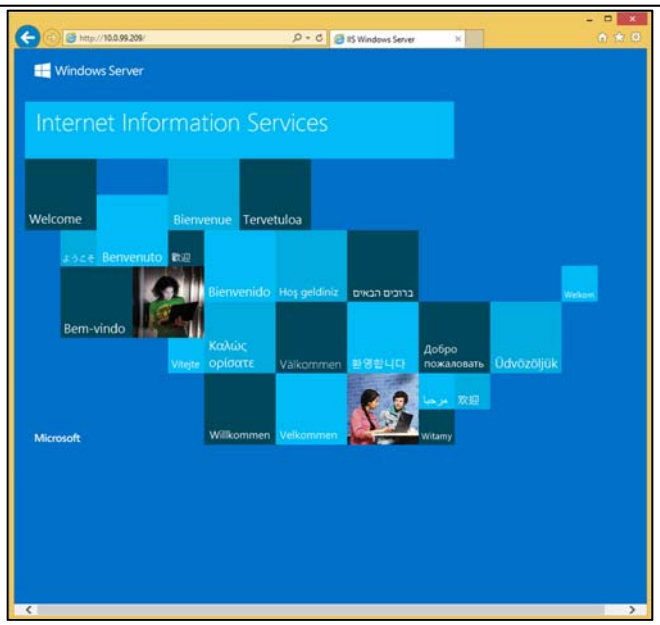


En esta figura aparecen las características del sitio creado y en qué estado se encuentra. Otra comprobación que podemos hacer es consultar cuales son los puertos que el servidor gestiona, con el comando ***netstat –a***. El puerto que utiliza HTTP por defecto es el 80.



A continuación comprobamos el funcionamiento con un cliente. Para ver el funcionamiento del protocolo hemos de iniciar al detector Wireshark en el cliente. Posteriormente hemos de poner en marcha el detector y capturar el tráfico hacia el servidor (*filter: host 10.0.99.209*)





6. Configuración avanzada

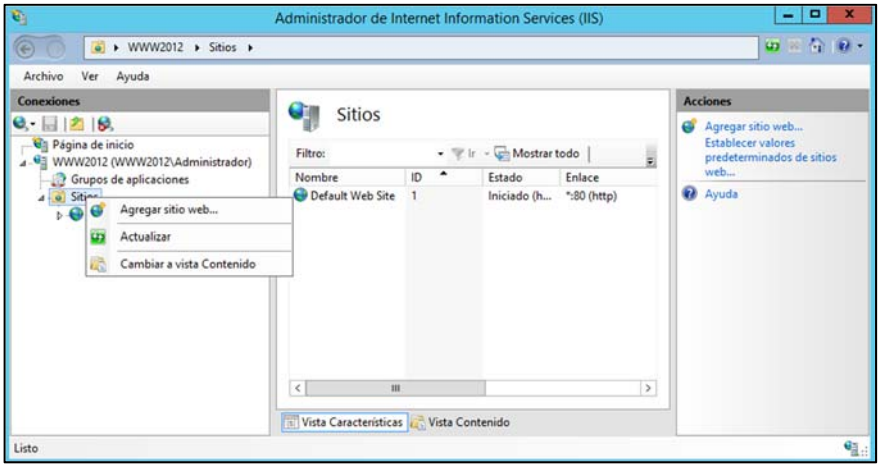
Un servidor web puede gestionar diversas web al mismo tiempo. En este punto se trata cómo tener más de un servicio web en un mismo servidor físico de forma simultánea. Este tipo de configuración se denomina lugares o webs virtuales.

- Podemos usar diferentes direcciones IP en caso de que el servidor tenga configuradas diversas direcciones en una misma tarjeta o disponga de diversas tarjetas de red.
- También es posible utilizar diversos puertos TCP. Cada web escucha un puerto diferente.

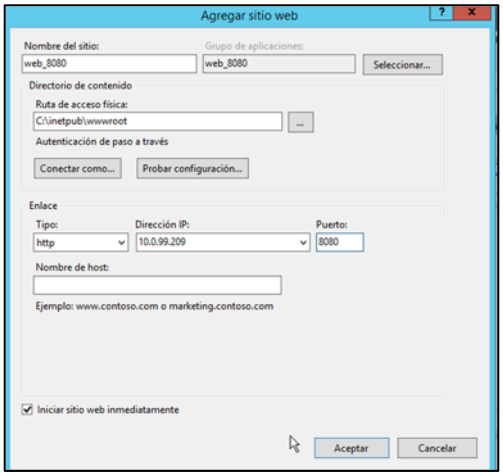
- Otra forma es diferenciar la cadena de entrada de la petición HTTP. Se trata de manera diferente, por ejemplo, una entrada del tipo http://www.grupoXX.net, que otra como http://www1.grupoXX.net, porque se consideran que son dos webs diferentes. Es posible que dos nombres de dominio (www.grupoXX.net y www1.grupo1.net) sean resueltos mediante la misma dirección IP utilizando alias en el servidor DNS.

Para poder crear estos lugares o webs virtuales en el servidor se ha de realizar lo siguiente:

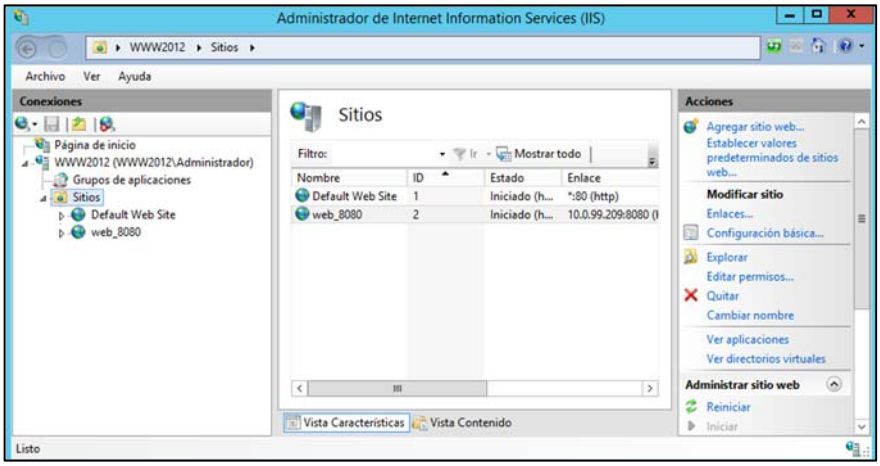
En primer lugar agregaremos un nuevo sitio web:



Aparece un formulario donde se puede indicar las opciones principales. Hemos de indicar el nombre, la ruta de acceso al directorio donde se encuentra la web, el tipo de protocolo, la dirección IP y el puerto. En este caso, se ha indicado el puerto 8080 para así comprobar que se puede tener otro sitio web en un puerto diferente:

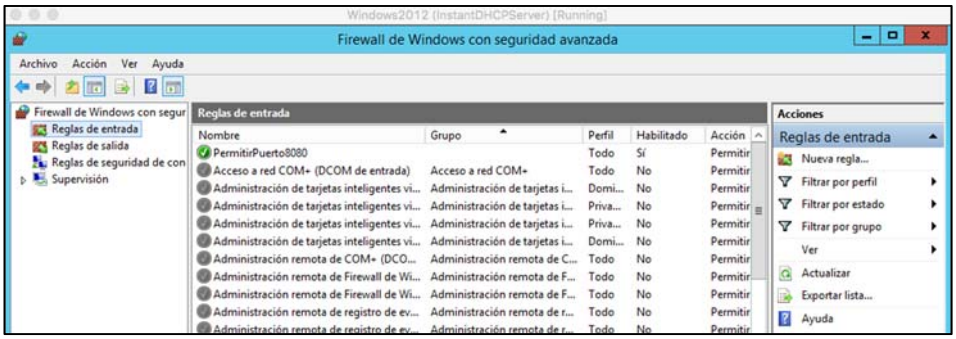


Tal como se muestra en el administrador, aparece un nuevo sitio con la configuración indicada.

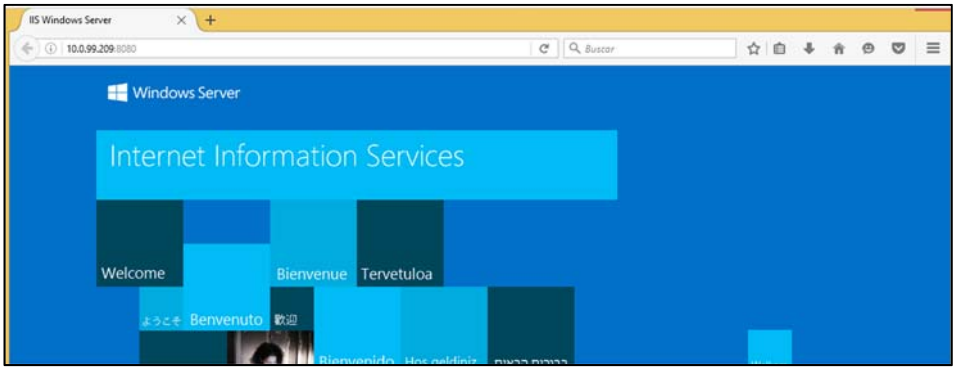


El siguiente paso es habilitar el puerto 8080 en el cortafuegos (*firewall*).

Para ello, y tal como hemos hecho en prácticas anteriores, crea una nueva regla de entrada denominada ***PermitirPuerto8080***, que habilite la conexión al puerto 8080. Actualice posteriormente el cortafuegos.

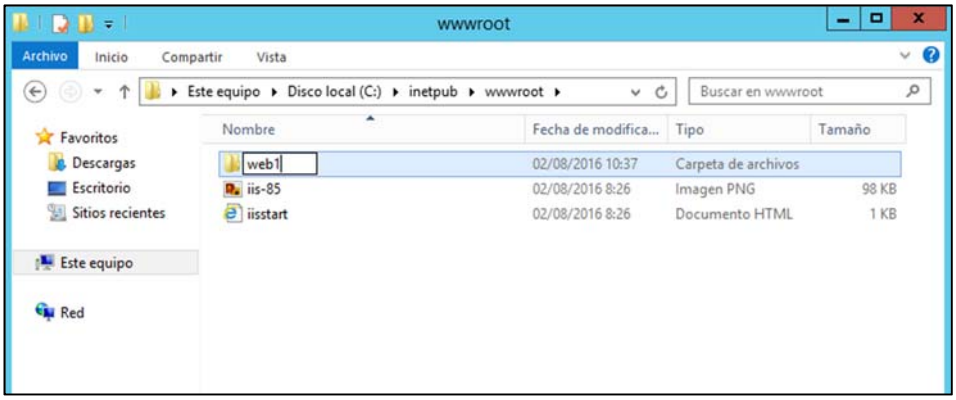


Verifique el funcionamiento accediendo desde el navegador del cliente a la dirección http://10.XX.99.209 :8080

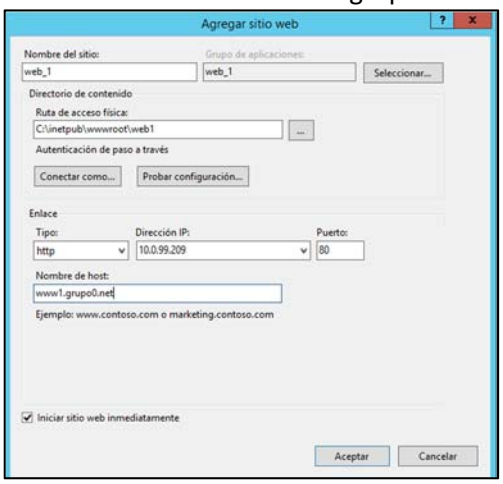


Tal como hemos dicho antes, los servidores web permiten poder tener más de un sitio web en el mismo servidor teniendo en cuenta la cadena de solicitud HTTP. Las configuraciones de este tipo se realizan de la siguiente forma.

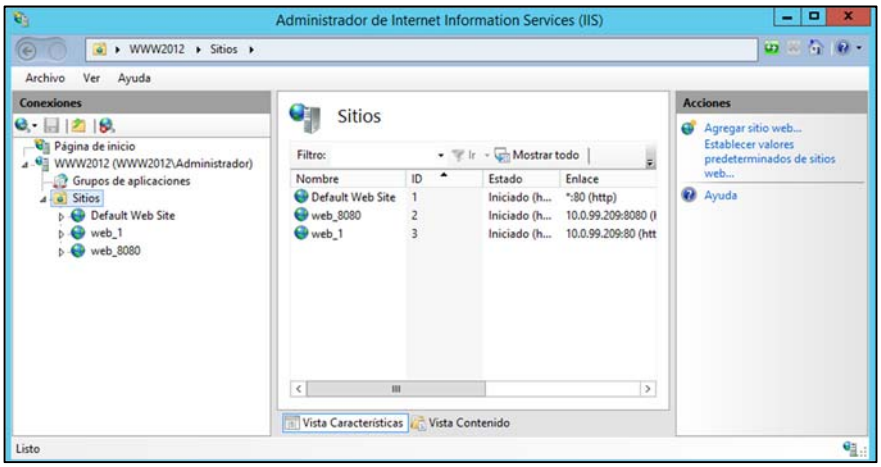
Agregamos un nuevo sitio web. Previamente dentro de la carpeta c:\inetpub\wwwroot vamos a crear la carpeta web1



Lo importante es colocar como nombre del host www1.grupoXX.net



Vemos que el sitio web se ha creado en el administrador IIS.



Para ello abrimos la instantánea donde tenemos configurado nuestro servidor DNS en Centos y añadimos las líneas indicadas en la siguiente figura al archivo named.grupo0.net. Haced lo mismo para el de resolución inversa.

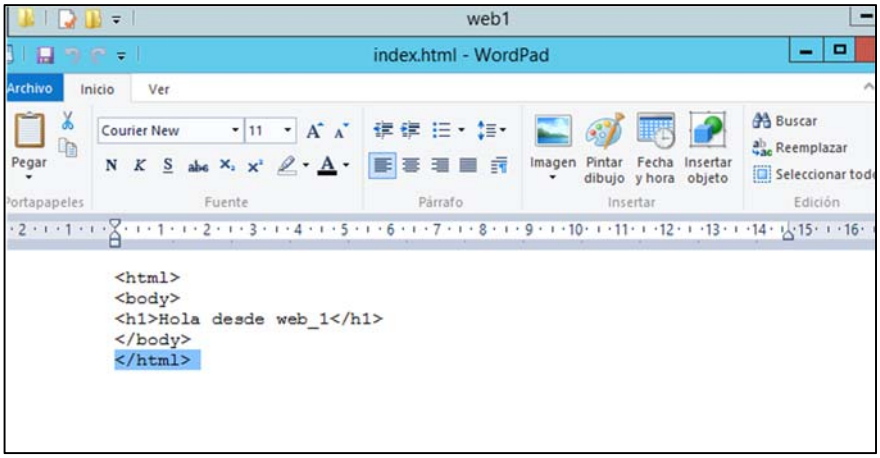
```
paubernabeu — root@dnsC:/var/named — ssh root@10.0.100.250 — 106×26
;Fichero named.grupo0.net
$TTL 1D
@       IN SOA  dnsc.grupo0.net. root.grupo0.net.    (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
;Servidor
        IN      NS              dnsc.grupo0.net.
        IN      NS              dnsW.grupo0.net.
        IN      MX 10           mail.grupo0.net.
        IN      NS              www.grupo0.net. ;Anadimos esta línea para servidor de nombres

;Hosts
dnsc            IN      A       10.0.99.250
dnsw            IN      A       10.0.99.249
mail            IN      A       10.0.99.230
www             IN      A       10.0.99.209  ; Le indicamos su IP
pop             IN      CNAME   mail
smtp            IN      CNAME   mail
www1            IN      CNAME   www ; le indicamos el alias www1
```

Reiniciamos el servicio DNS:

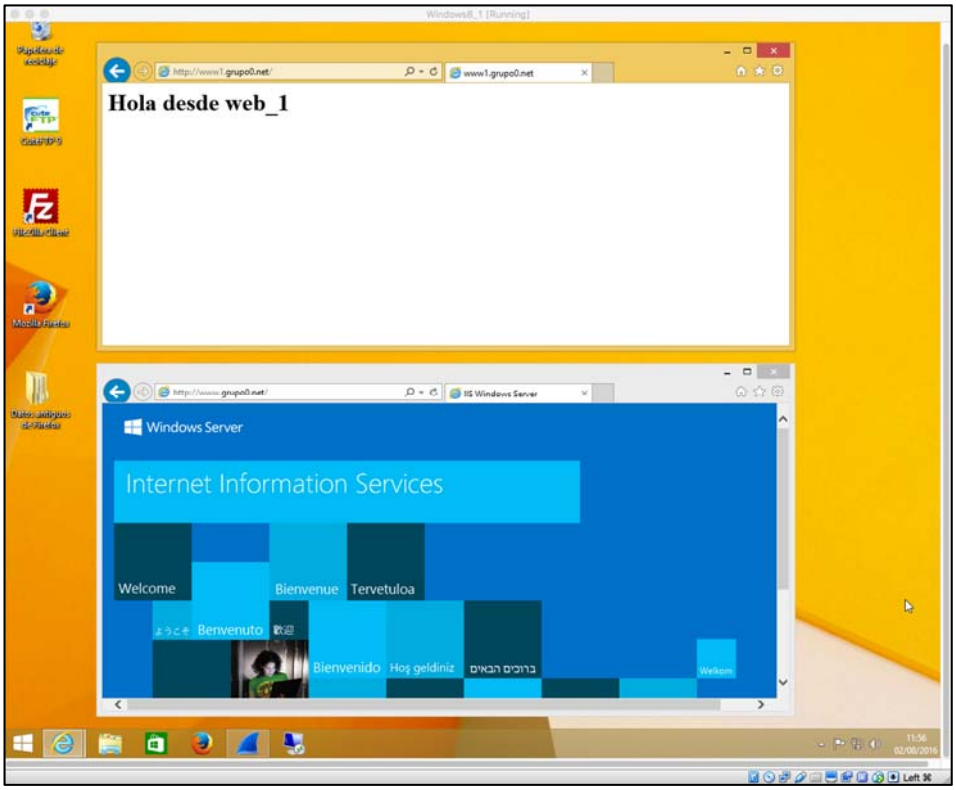
```
systemctl restart named
```

Vamos a las conexiones de red tanto del máquina WWW2012 como de la máquina cliente y cambiamos los DNS de la universidad por los DNS 10.0.99.250 y 10.0.99.249 (este no activo al ser el servidor Windows, pero no hay problema alguno)

En la carpeta web 1 creamos un nuevo fichero con el siguiente código HTML, ficheros que guardamos con el nombre index.html



Desde la máquina cliente, abrimos explorer y ejecutamos en una ventana http://www1.grupoXX.net y en otra ventana http://www.grupoXX.net. Observa cómo se abren webs distintas.



7. Configuración segura

En este punto se configura un servidor web seguro que permita cifrar los datos enviados entre el servidor y el cliente. El puerto a escuchar es 443.

Para activar el servidor web seguro con el protocolo HTTPS, el primer paso es añadir un certificado en el servidor que permita cifrar las comunicaciones.

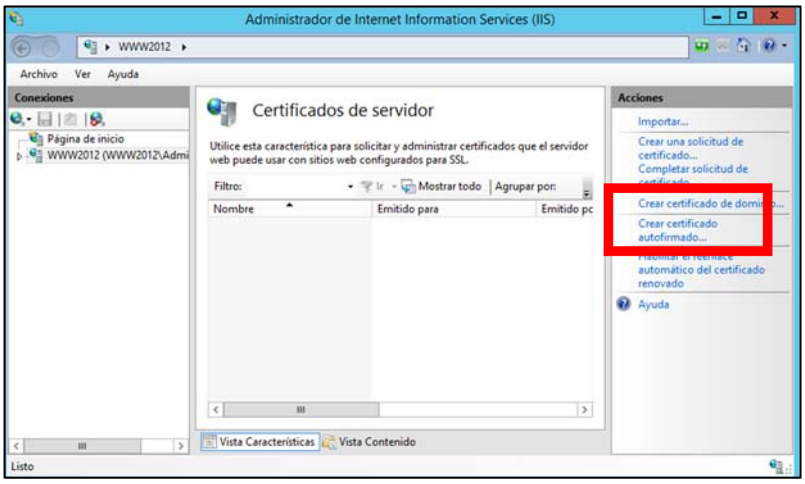
Para ello debemos tener una autoridad certificadora. Instalaremos pues dicho servicio en nuestro servidor web (lo correcto es que fuese una entidad validada al respecto).

Si recordamos de la práctica de FTP accedíamos mediante http://IP_address/certsrv. Lo correcto y para tener mayor funcionalidad es acceder a dicha dirección pero de forma segura, es decir, https://IP_address/certsrv (con HTTPS).

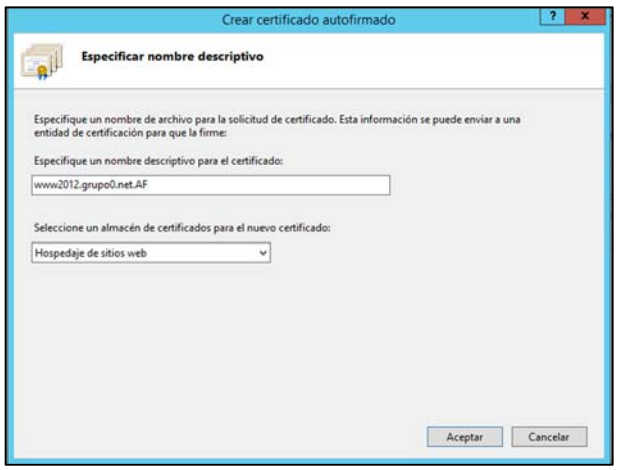
Por tanto hemos de crear un certificado previo de uso propio para poder habilitar el servidor de autoridad certificadora de forma segura.

En el Administrador de Internet Information Server (IIS) hacemos clic en el árbol WWW2012(WWW2012\Administrador)

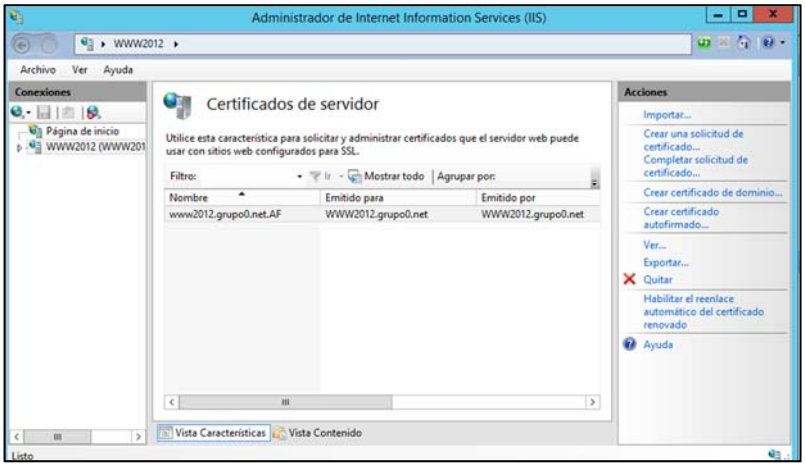
Y doble clic en Certificados de Servidor, crearemos de momento un certificado autofirmado:



Le ponemos de nombre www2012.grupo0.net.AF (para saber es el autofirmado) y lo guardamos en Hospedaje de Sitios Web

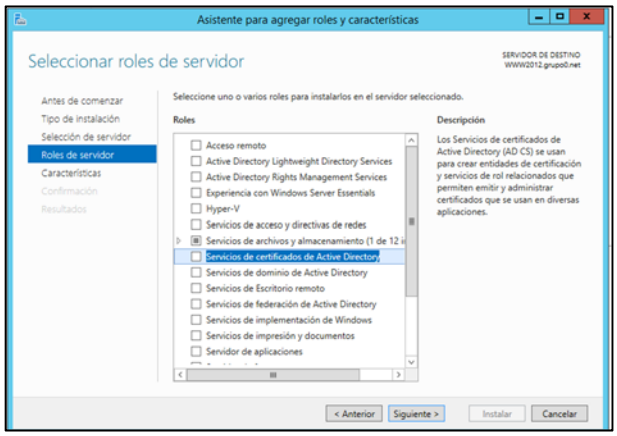


Vemos que nos aparece ya el certificado creado:

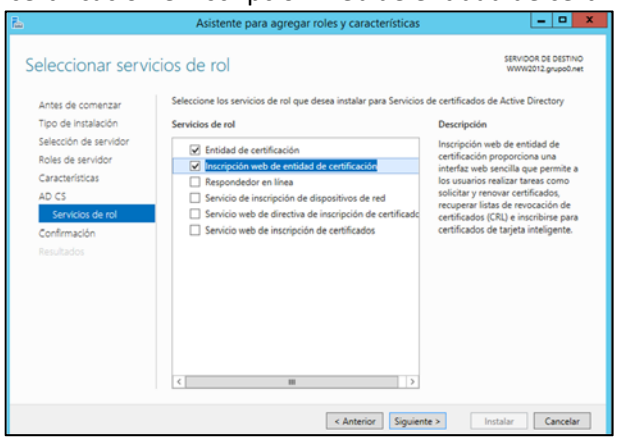


La realidad nos ha de llevar a una entidad certificadora para obtener un certificado básico. En este caso, vamos a que nuestro servidor dé el servicio de autoridad certificadora.

Agregar roles y características→Servicios de certificados de Active Directory, tal como hicimos en la práctica FTP.

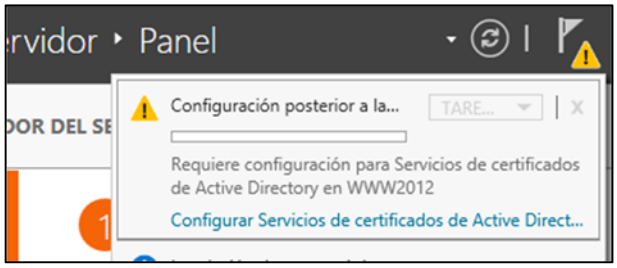


Marcamos Entidad de certificación e Inscripción web de entidad de certificación:

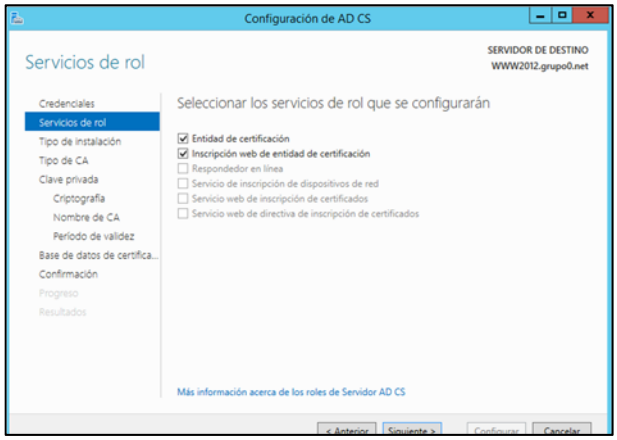


Procedemos a la instalación.

Una vez instalado, vamos al icono “bandera” donde nos indica hemos de realizar tareas de configuración del servicio AD CS.

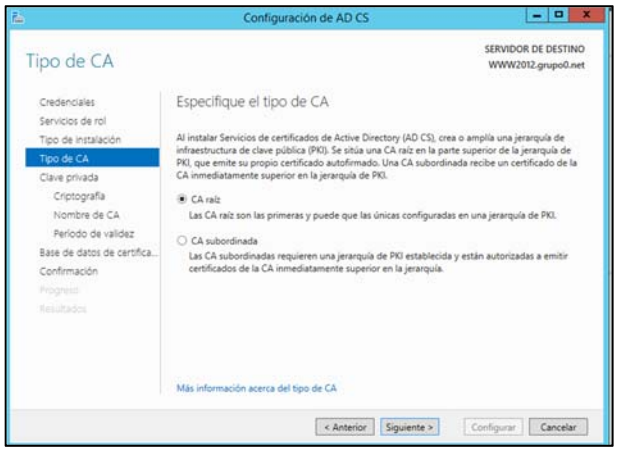


Clicamos en Configurar, damos a siguiente y en la pantalla de la figura marcamos las dos casillas indicadas:

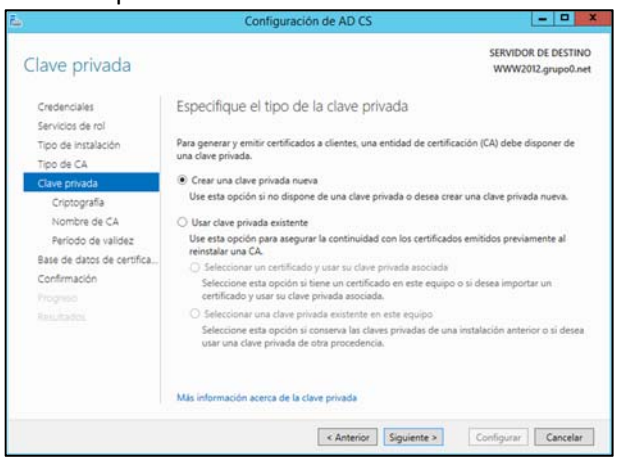


Elegimos CA independiente:

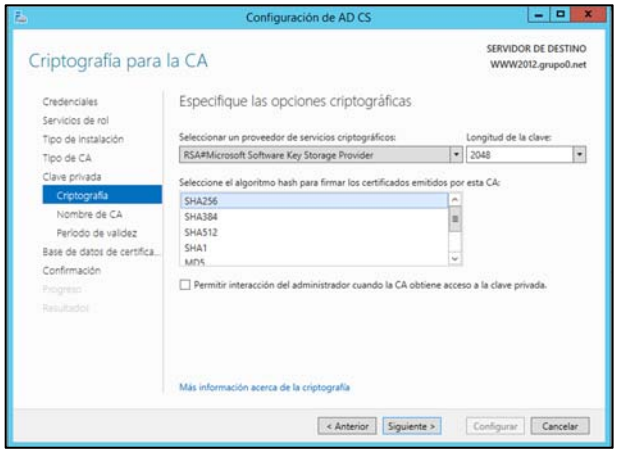
Seleccionamos CA raíz:



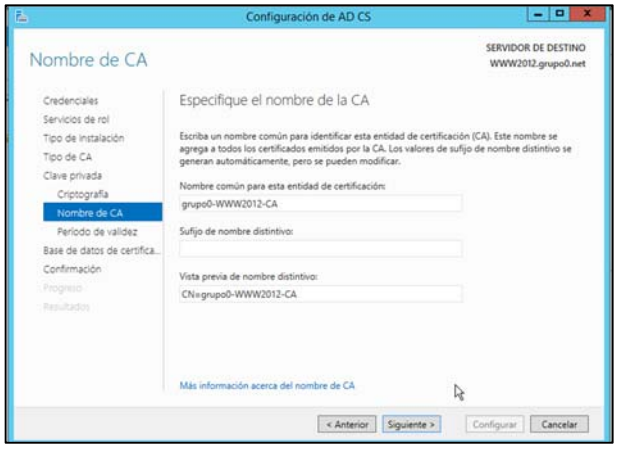
Seleccionamos Crear una clave privada nueva:



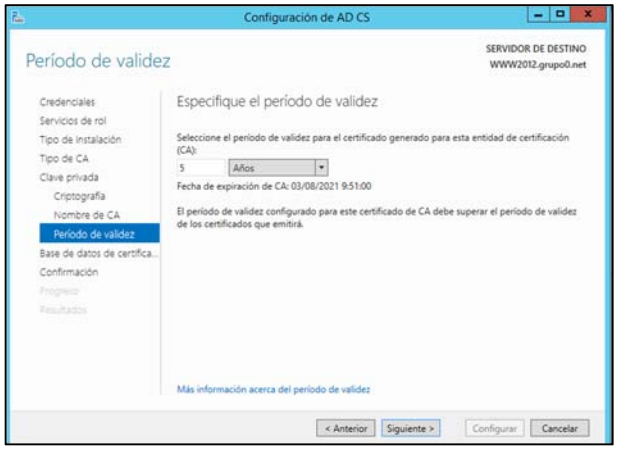
Seleccionamos SHA256, por ejemplo:



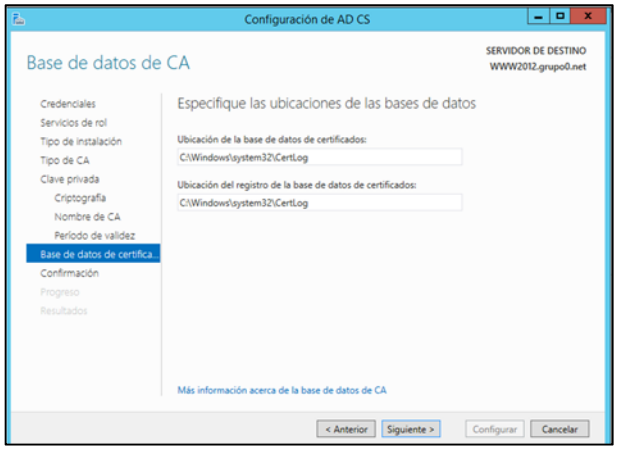
Aceptamos el nombre nos propone (no debemos cambiarlo):



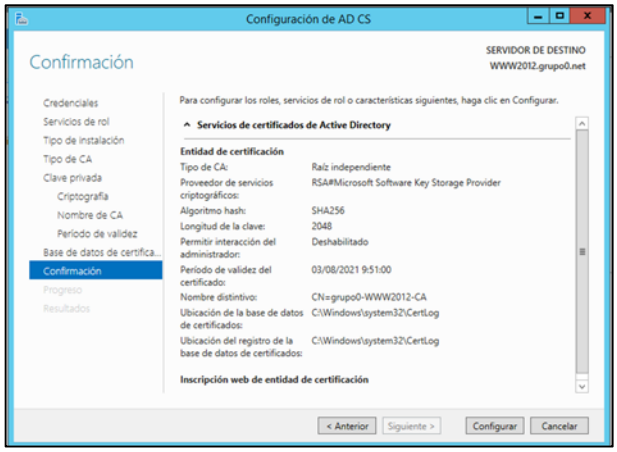
Aceptamos período de validez 5 años:



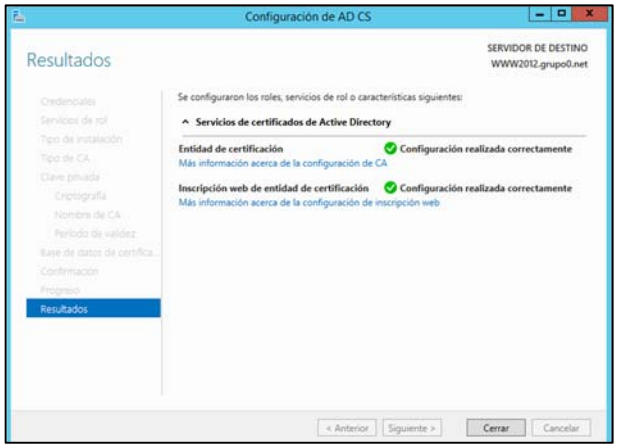
Dejamos las ubicaciones por defecto:



Nos muestra cómo queda la configuración de nuestra autoridad certificadora:

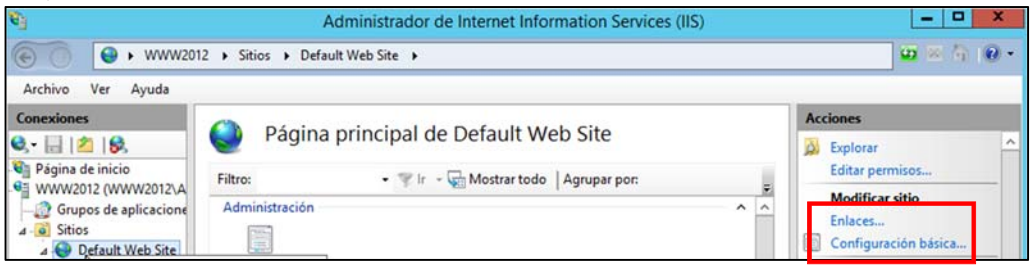


Clicamos en configurar y, si todo ha ido bien, nos indicará, que la configuración ha sido realizada con éxito.

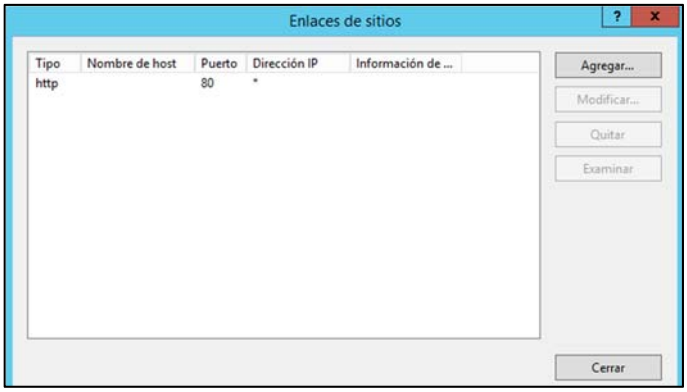


Ahora debemos configurar la web de la entidad certificadora como segura (https).

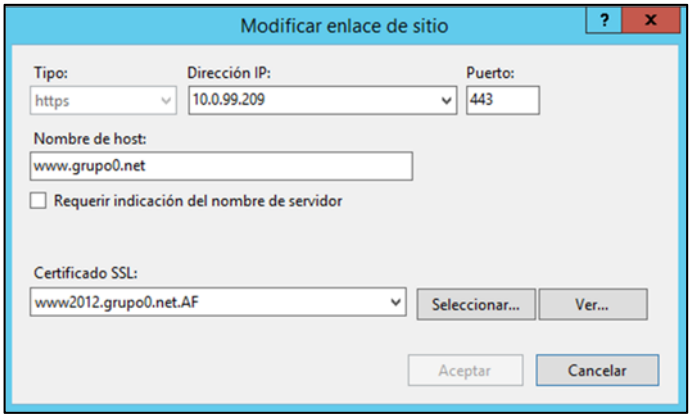
Para ello el Administrador IIS clic en sitios y posteriormente en Default Web Server, barra de la derecha, clic en Enlaces...



Vamos a darle permiso HTTPS:

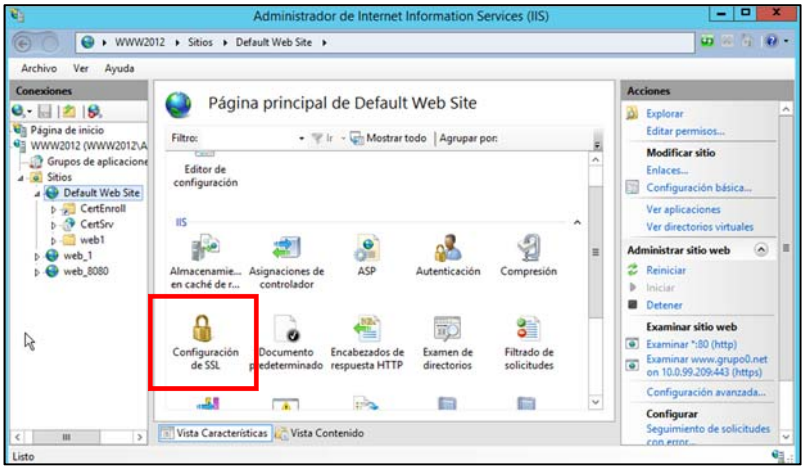


Clicamos en agregar y rellenad los datos se indican en la figura:

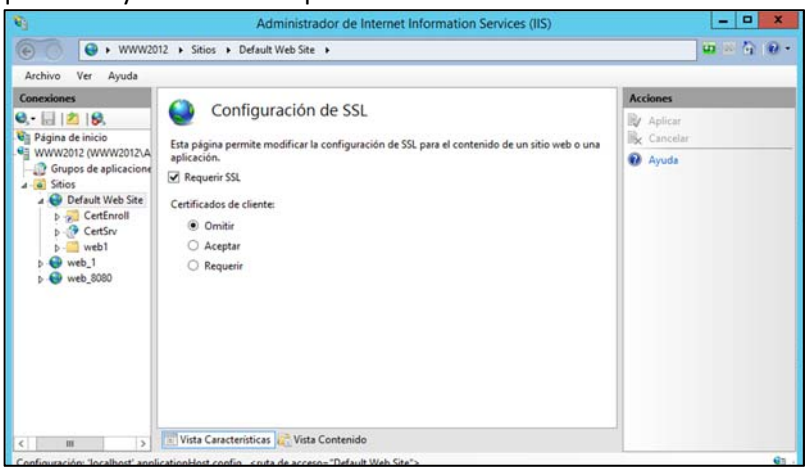


Damos a aceptar.

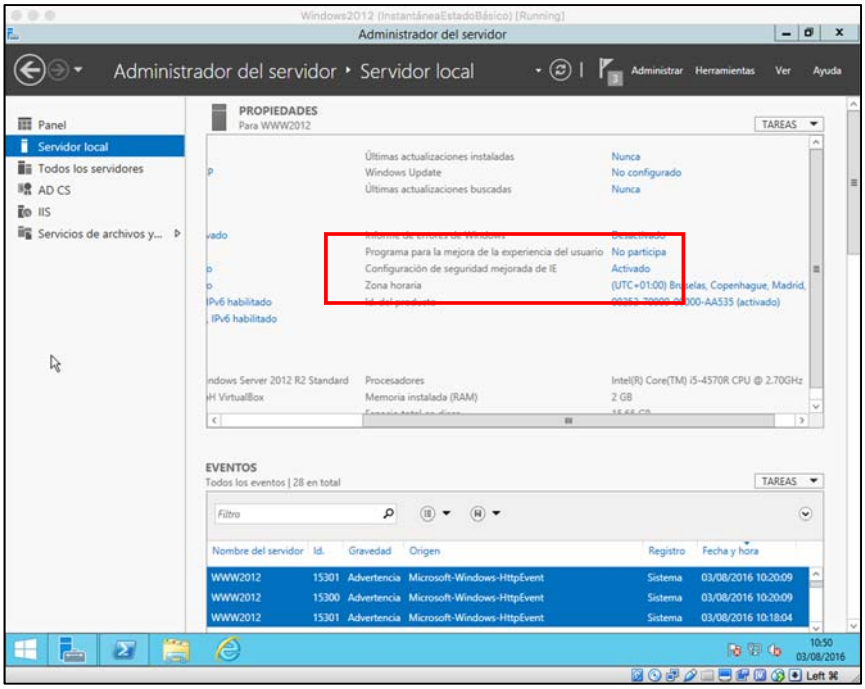
Clic en Default Web Site y clic en el icono Configuración SSL.



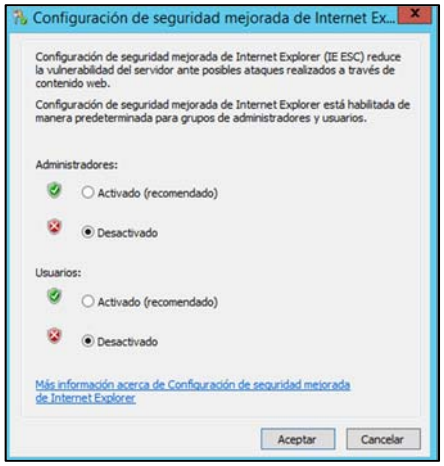
Indicamos Requerir SSL y clicamos en Aplicar:



Deshabilitamos la seguridad del navegador web: Panel de Administrador del Servidor→Servidor Local (panel izquierdo)→Configuración de seguridad mejorad de IE



Clicamos en Activado, nos abre una ventana y clicamos en Desactivado:

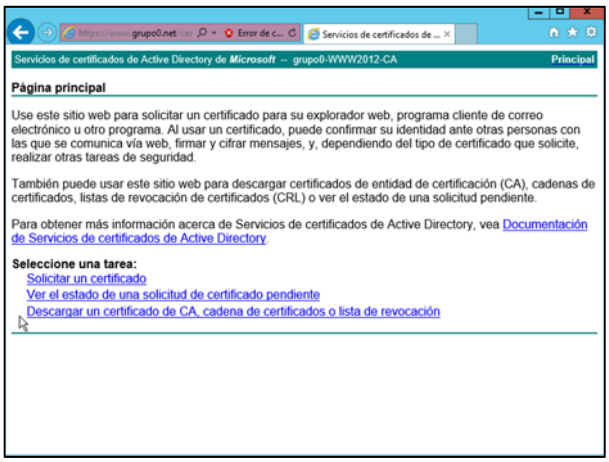


Nos aparecerá que la "Configuración de seguridad mejorada IE," está desactivada

Abrimos el navegador del servidor. (Internet Explorer), dirección URL: https://www.grupoXX.net/certsrv

Nos aconseja no ir al ser un certificado que no es de confianza, pero clicamos "Vaya a sitio web":

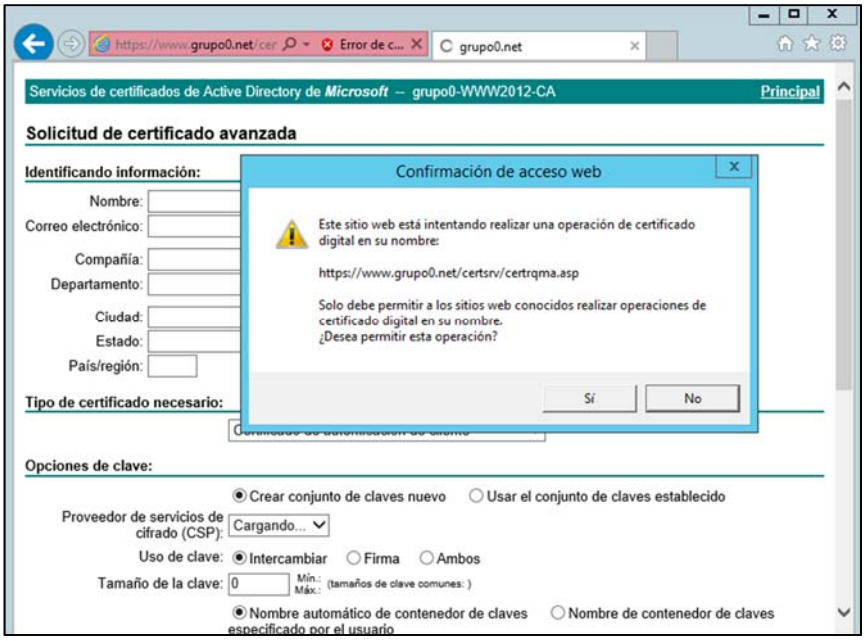
Nos abrirá la web de los servicios de certificado de Active Directory de Microsoft:



Solicitamos certificado haciendo clic en solicitar certificado.

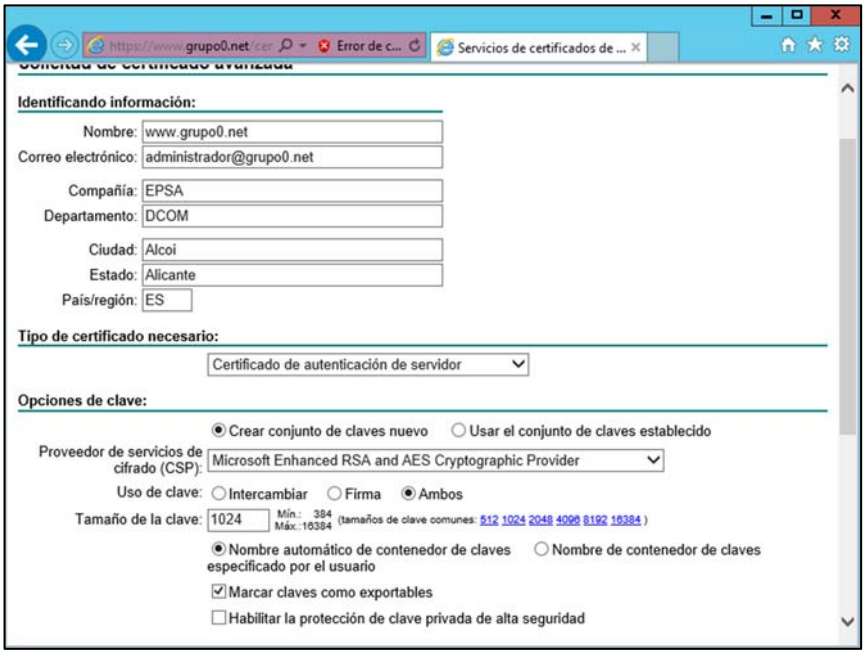
Clic en solicitud avanzada de certificado:

Clic en crear y enviar una solicitud a esta CA. Nos abre una ventana, donde nos solicita la opción de permitir la operación. Respondemos que sí.

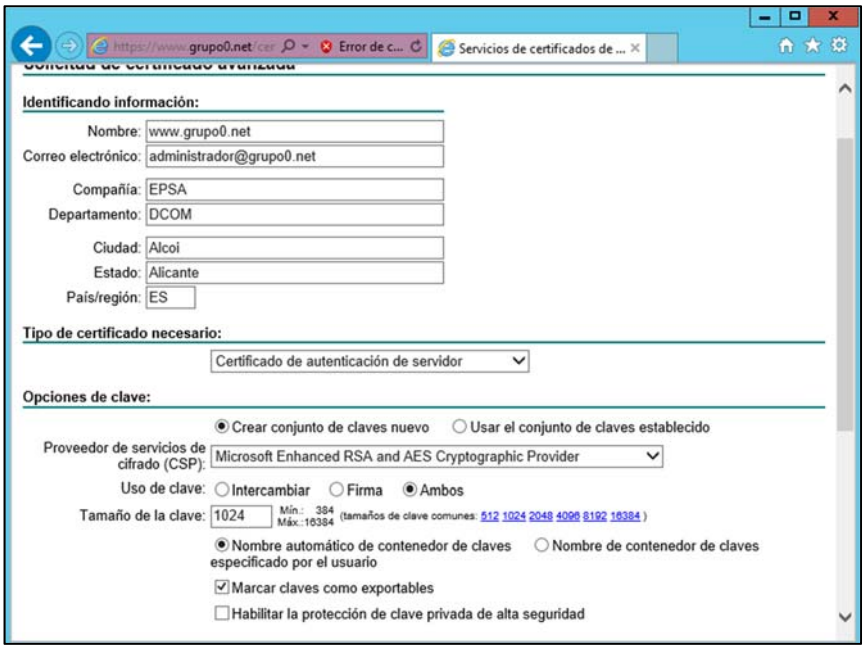


Completamos los nombres se nos indica. Poned como nombre: www.grupoXX.net. Correo electrónico: administrador@grupoXX.net

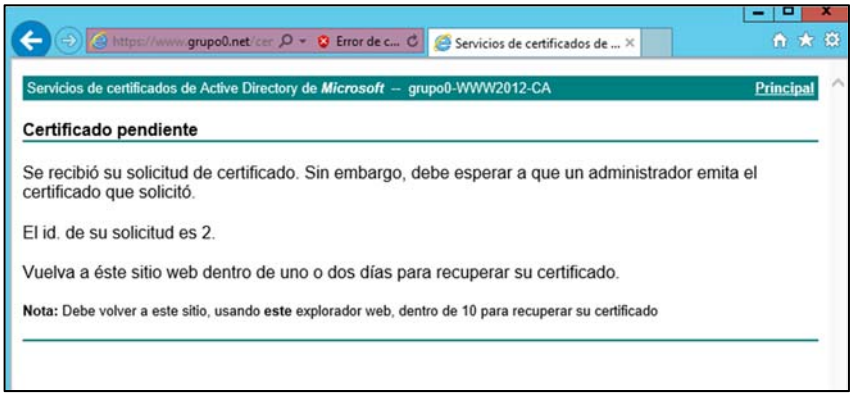
Completáis el resto de datos, tal como se indica en la siguiente figura. Como tipo de certificado necesario, seleccionáis “Certificado de autentificación de servidor” y seleccionamos “Marcar claves como exportables”.



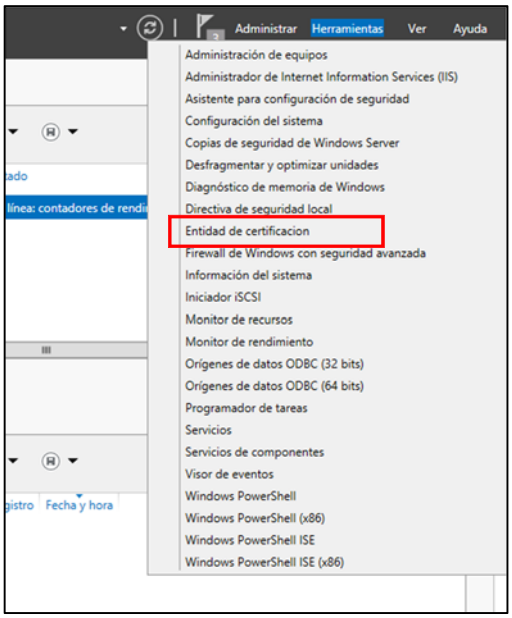
Como algoritmo SHA, seleccionamos SHA256. Dejamos el resto de valores los indicados por defecto.



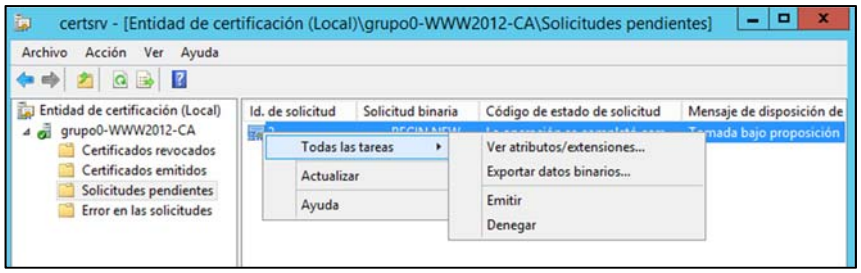
Clicamos en enviar. Nos indica que se ha creado y que está pendiente de validar.



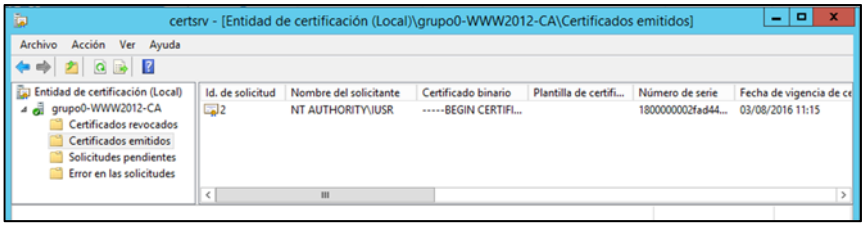
Para validar el certificado, vamos a Panel del Administrador del servidor→Herramientas→Entidad de certificación.



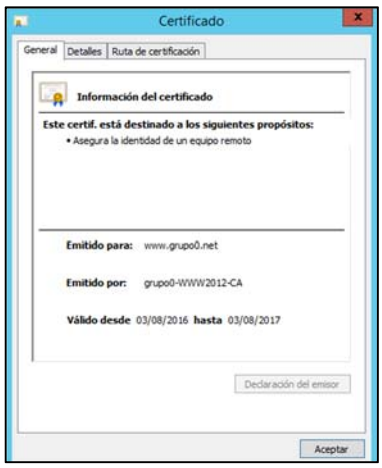
Desplegamos y clicamos en la carpeta solicitudes pendientes, sobre el certificado pendiente, botón derecho→Todas las tareas→Emitir



De esta forma pasa a la carpeta de Certificados emitidos:



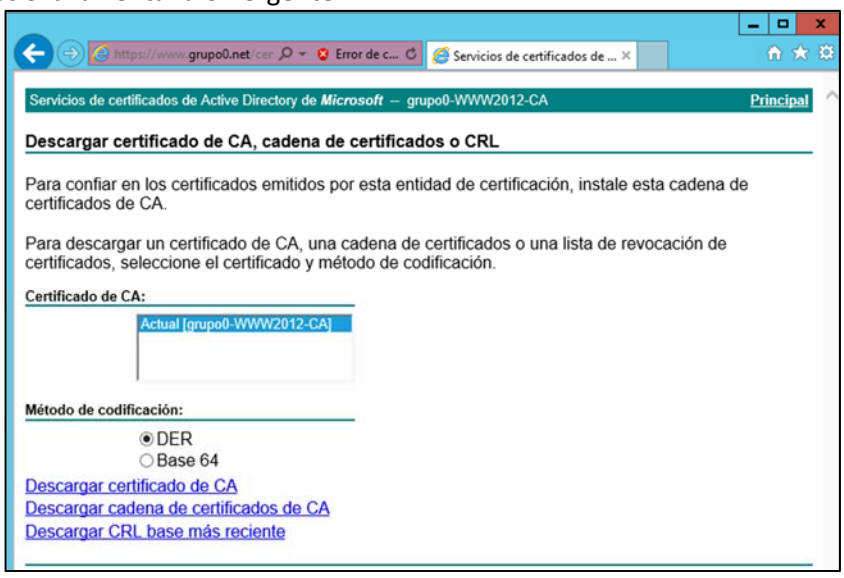
Haciendo doble clic en el certificado emitido podemos observar su contenido.



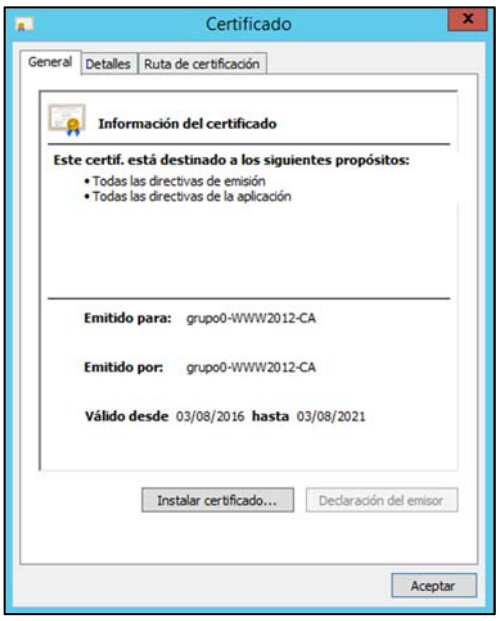
En este momento, el servidor WWW ya puede obtener el certificado. Accedemos nuevamente al servidor de certificados https://www.grupoXX.net/Certsrv.

En primer lugar vamos a instalar el certificado de la entidad de certificación.

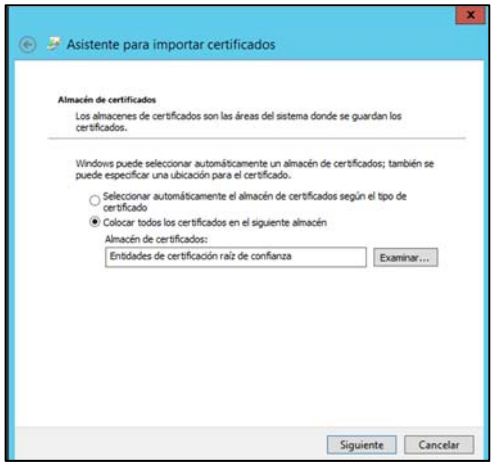
Clicamos en “Descargar un certificado de CA, cadena de certificados o lista de revocación”, respondemos Sí a la ventana emergente.



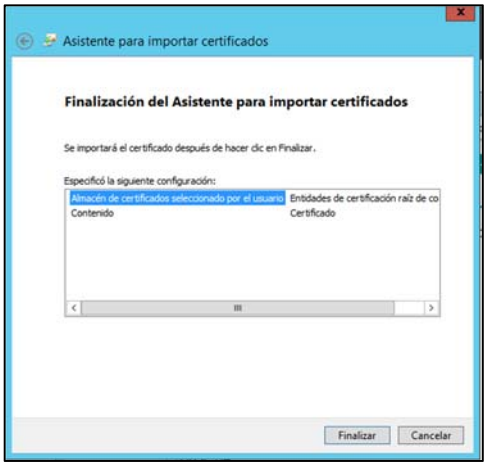
Clicamos en “Descargar certificado de CA”, clicamos en Abrir:



Clicamos en Instalar certificado, abre el Asistente para importar certificado , e indicamos Usuario Local, clic en siguiente. Le indicamos:



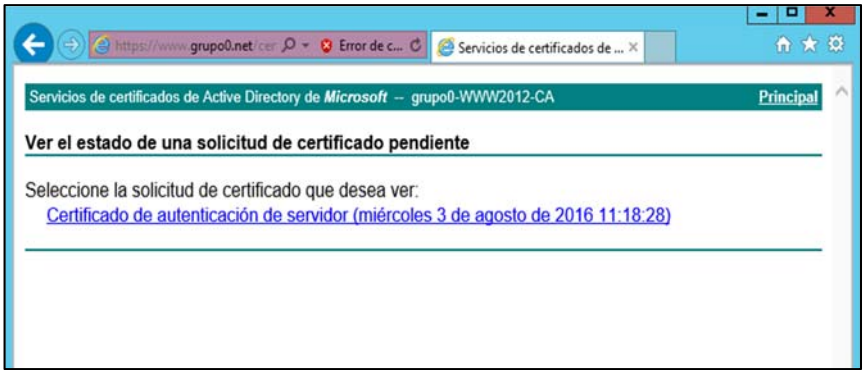
Clicamos en siguiente,



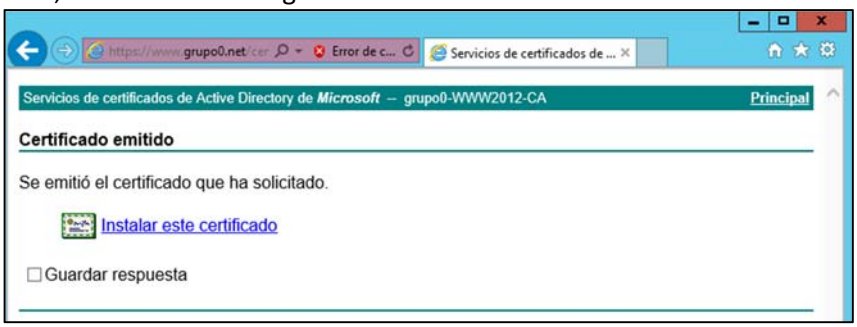
Clicamos en Finalizar y nos indica la importación se completó con éxito.

Volvemos a la página inicial del servicio de certificados,

Clicamos en "Ver el estado de una solicitud de certificado pendiente", nos aparecerán todas la solicitudes emitidas que hay accediendo a través del navegador:

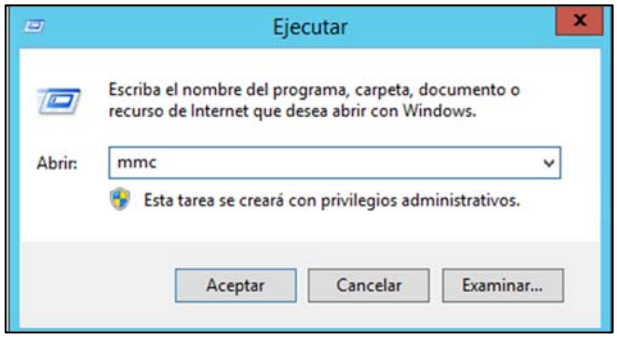


Respondemos sí, a la ventana emergente. Aún haremos clic en instalar este certificado.

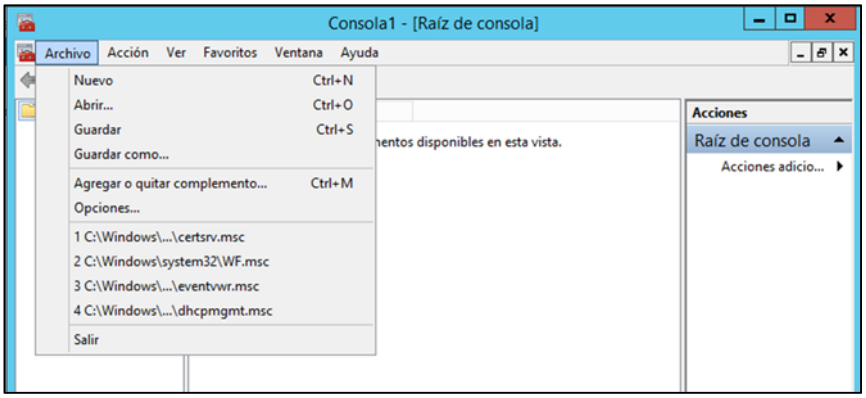


Nos indica que el certificado nuevo se instaló correctamente.

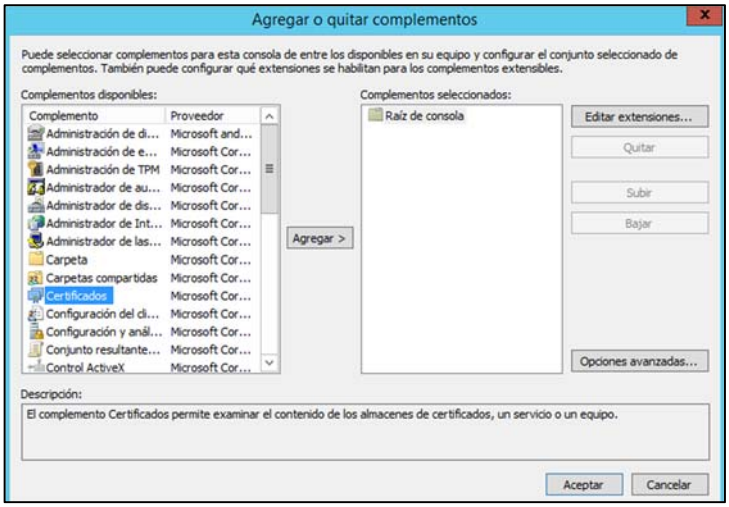
A continuación hemos de exportar el certificado para importarlo a la aplicación en que queremos configurar SSL (en este caso, el servidor web). Haremos clic en Inicio→Ejecutar e introducir mmc para ejecutar la consola.



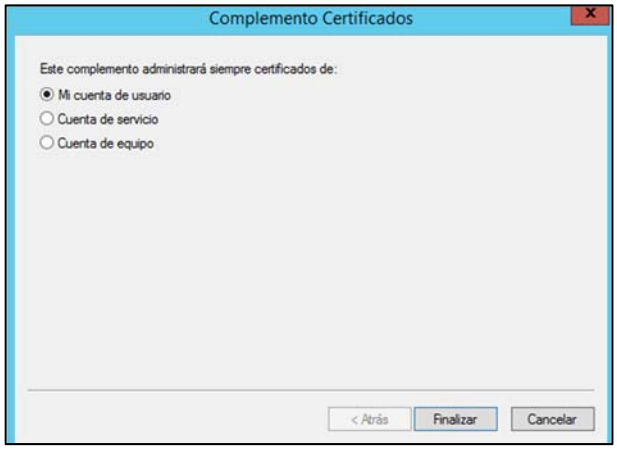
Hacemos clic en Archivo→Agregar o quitar complementos:



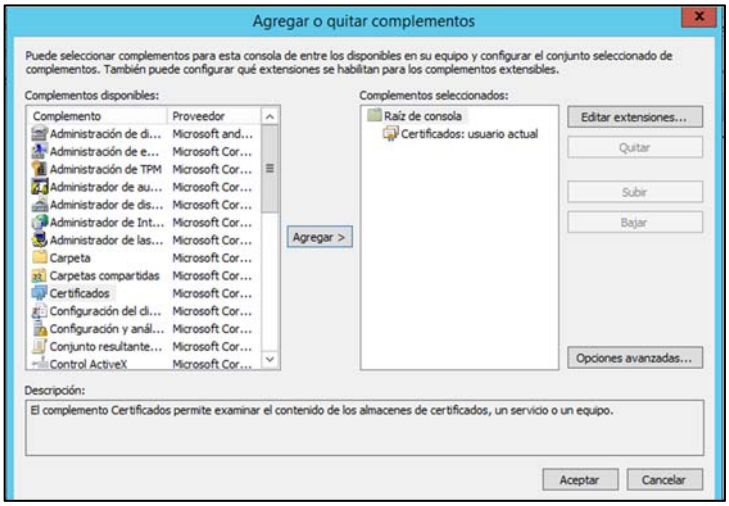
Hemos de poner en marcha el complemento de Certificados marcando *Certificados*, en la parte izquierda, y haciendo clic en el botón agregar.



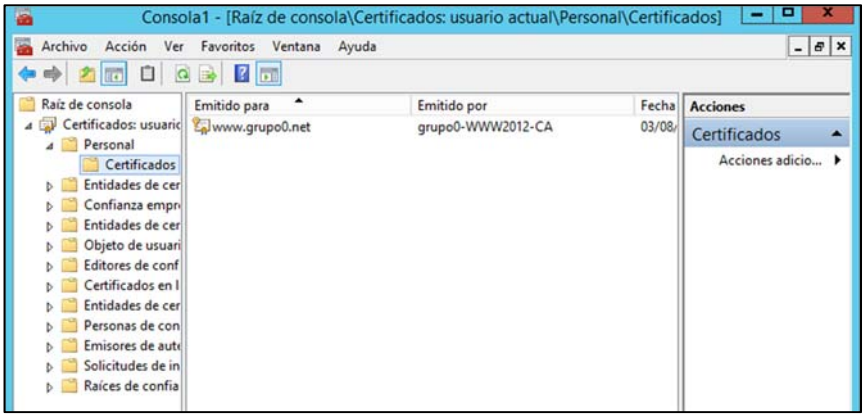
Aparece la siguiente pantalla que indica que tipo de complemento de certificados se desea abrir. Marcaremos **Mi cuenta de Usuario,** que es donde se almacenan los certificados importados a través del navegador de Internet.



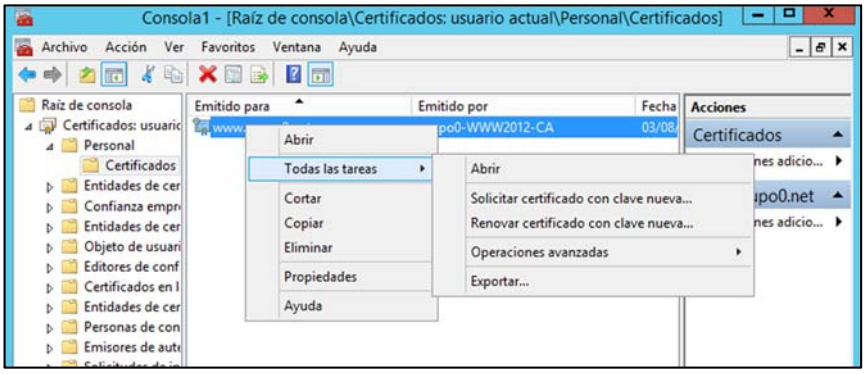
Clicamos en Finalizar. Tras ello aparece la siguiente pantalla donde clicamos en Aceptar.



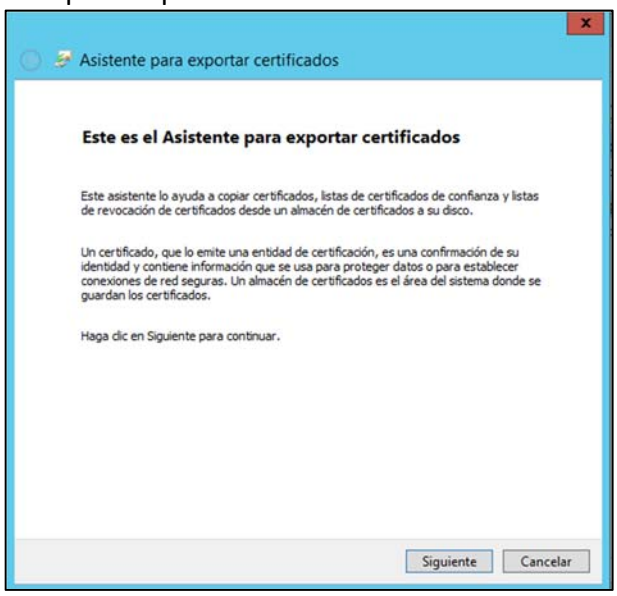
Ahora, clicamos en Certificados de usuario, luego en la carpeta personal y posteriormente en la carpeta Certificados.



Sobre el certificado, botón derecho→Todas las Tareas→Exportar.

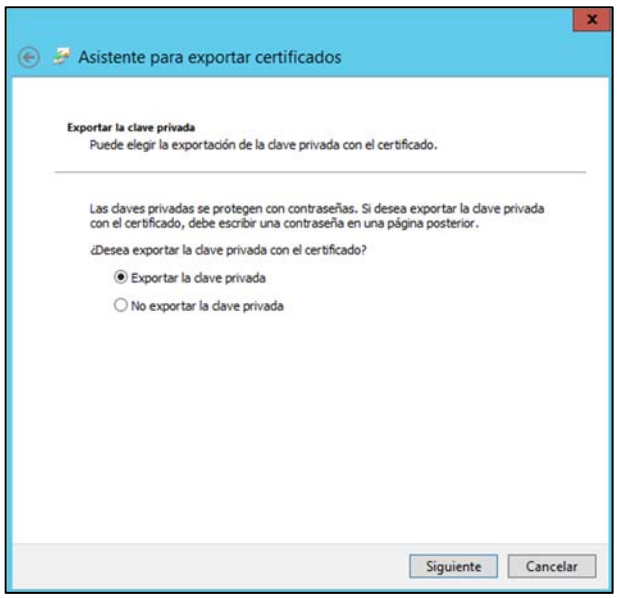


Lo cual abre el Asistente para exportar certificados:

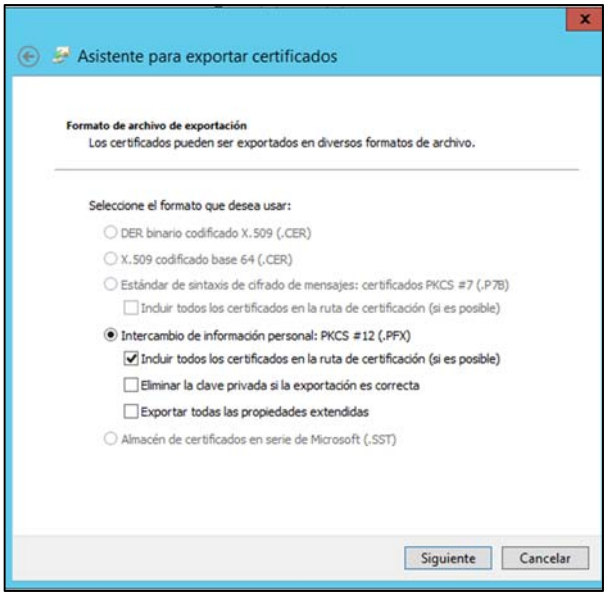


Clic en siguiente,

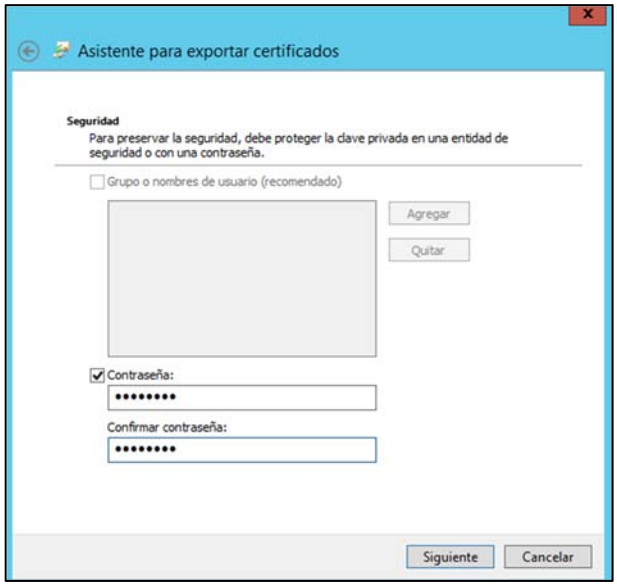
Le indicamos “Exportar la clave privada”:



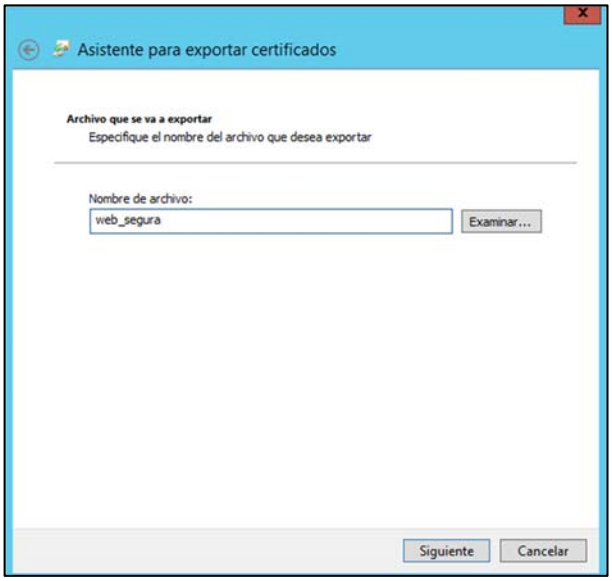
Clic en siguiente. Marcamos la opción “Incluir todos los certificados en la ruta de certificación (si es posible)”



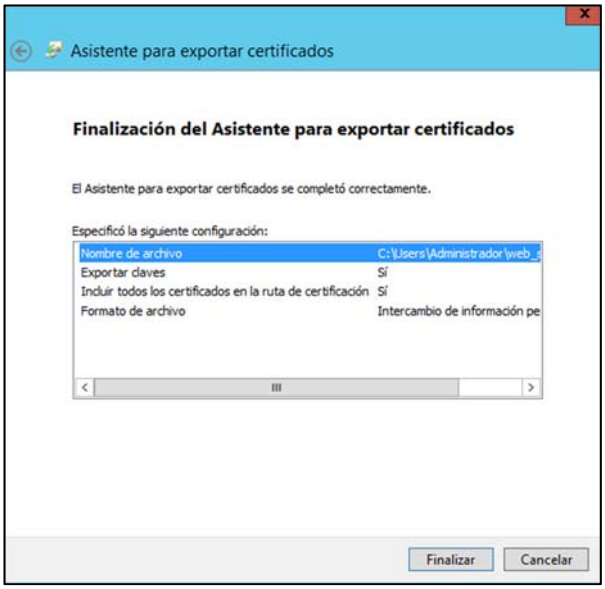
Clic en siguiente, introducimos una contraseña (no olvidar) y la confirmarnos.

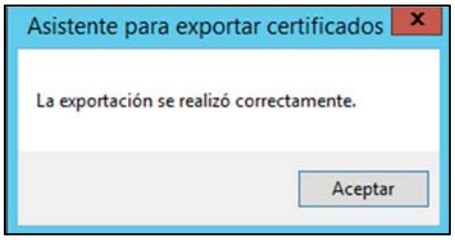


Clic en siguiente, le ponemos por nombre web_segura

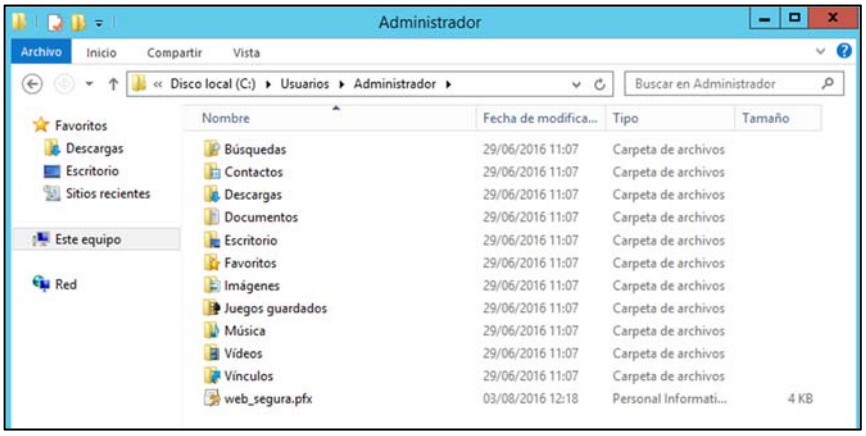


Clic en siguiente, clic en Finalizar y noes indica que la exportación se realizó correctamente.





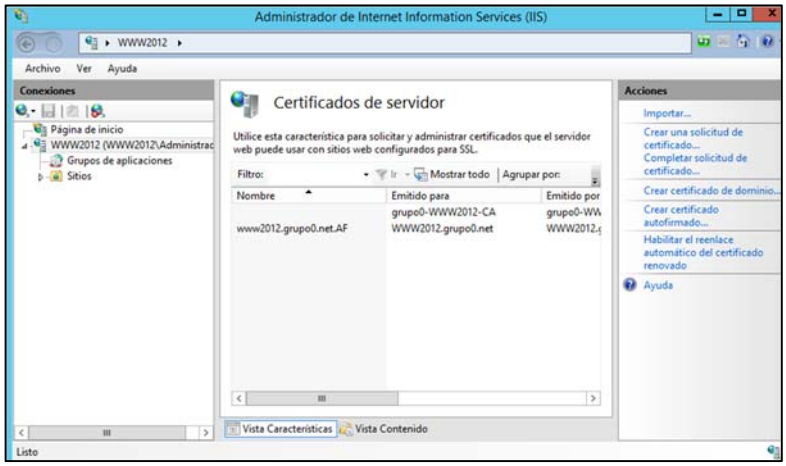
El fichero contiene el certificado queda guardado en c:\usuarios\Administrador.



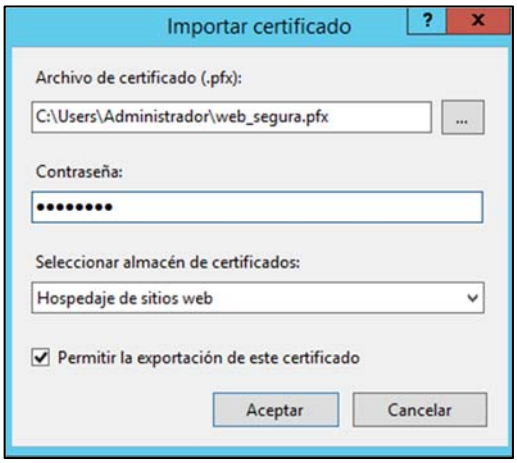
En estos momentos disponemos de un fichero que contiene el certificado y la clave privada asociada a éste. Este fichero ha de ser importado para la aplicación donde queremos configurar el protocolo SSL.

Importamos el certificado al Administrador de IIS.

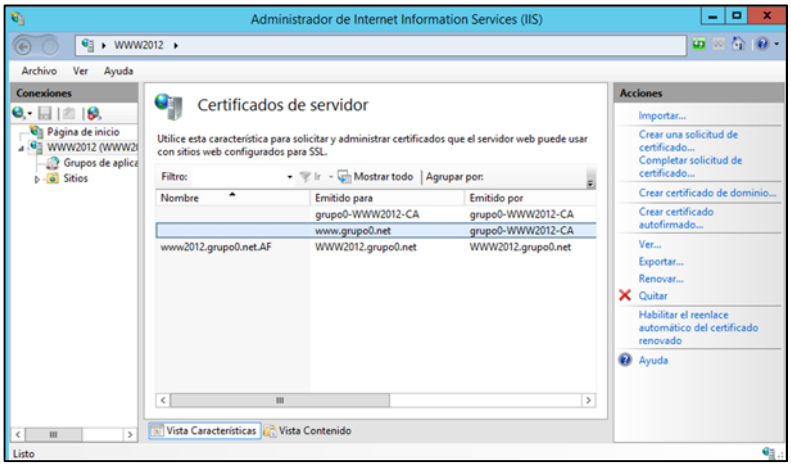
Clicamos en WWW2012\Administrador→Doble clic icono Certificados de Servidor:



Clicamos en importar (barra lateral derecha), introducimos la contraseña del certificado.

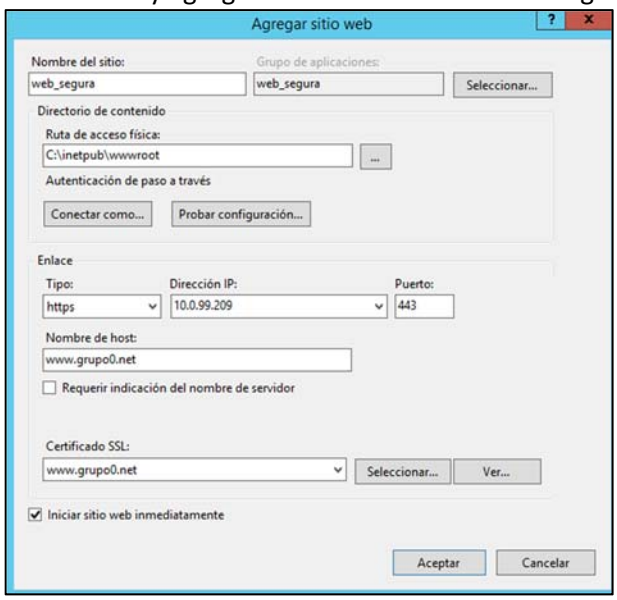


Clic Aceptar, nos aparee el certificado www.grupo0.net.



8. Creación sitio web seguro

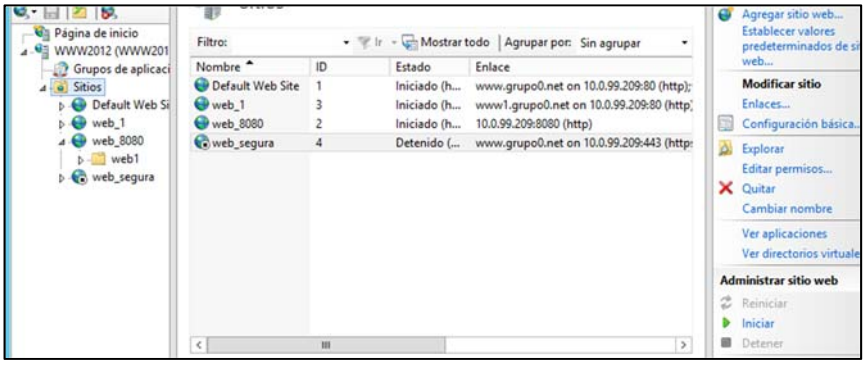
En este punto estamos pues en condiciones de crear sitios web seguros. Vamos a crear un nuevo sitio web. Completamos los datos y agregando el certificado SSL www.grupo0.net



Clicamos sí, a la ventana emergente.

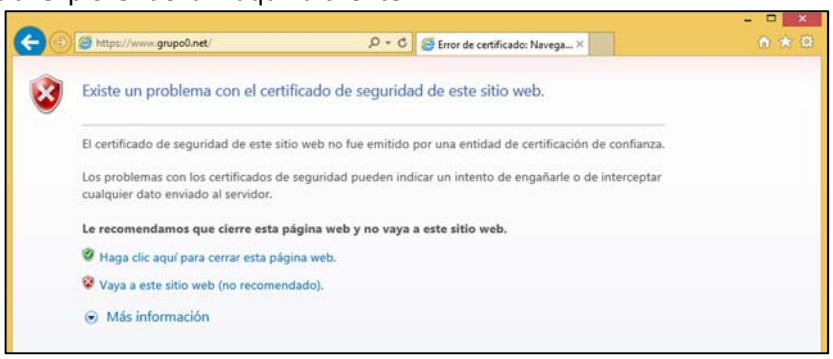
Para poder funcionar adecuadamente, debemos de tener activo o Default Web Site o Web segura ya que en ambos, hemos indicado el protocolo htttps. Ya nos lo indica la ventana emergente la crear la web segura.

Si observamos la web creada está detenida.



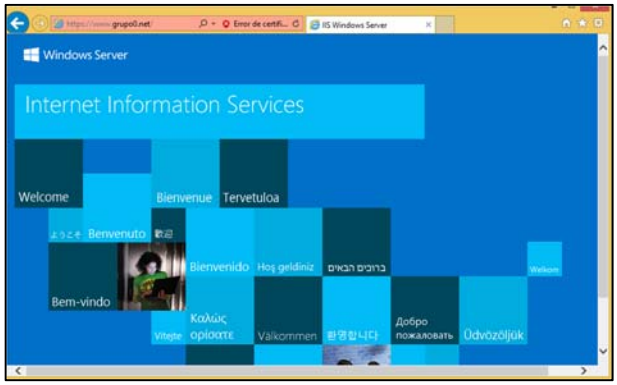
Detenemos Default Web Site (servidor certificados) e iniciamos web_segura.

Ahora vamos al explorer de la máquina cliente:

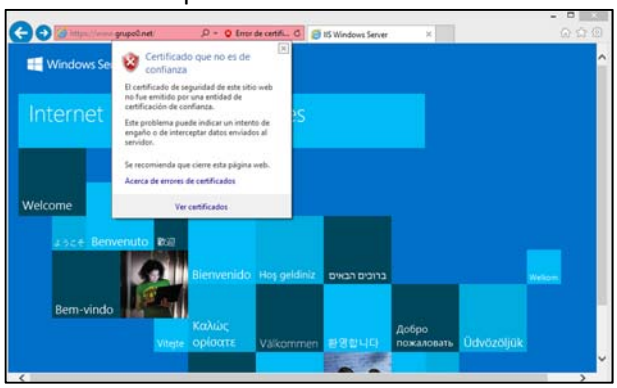


Como observamos el navegador indica que tenemos problemas con el certificado. Nos indica que el certificado no ha sido emitido por una entidad de certificación de confianza.

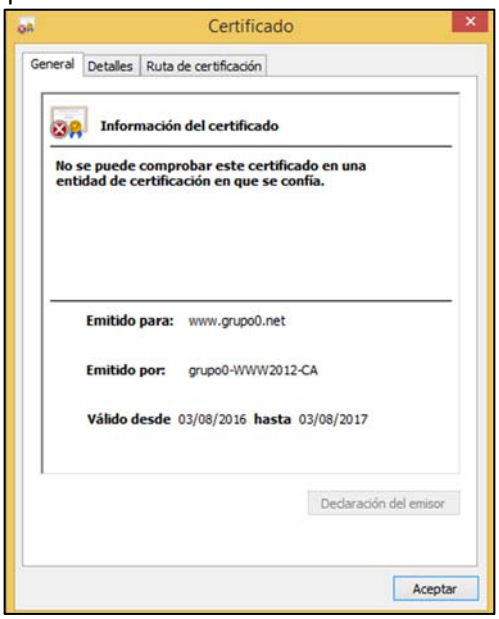
Hacemos clic en Vaya a Sitio Web (no recomendado) y se nos permite acceder:



Haciendo clic en Error de Certificado podemos ver información adicional del mismo:



Observando detenidamente la información del certificado, se puede ver que indica que este certificado ha sido emitido por una entidad certificadora en la cual no se confía.

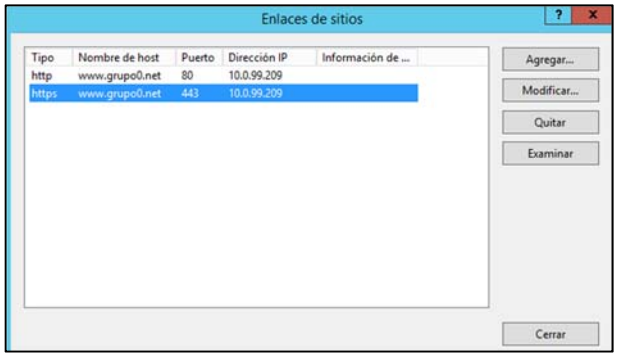


Para resolver que la entidad de certificación es de confianza hemos de conectarnos con la entidad de certificación, descargar el certificado e instalarlo en el cliente.

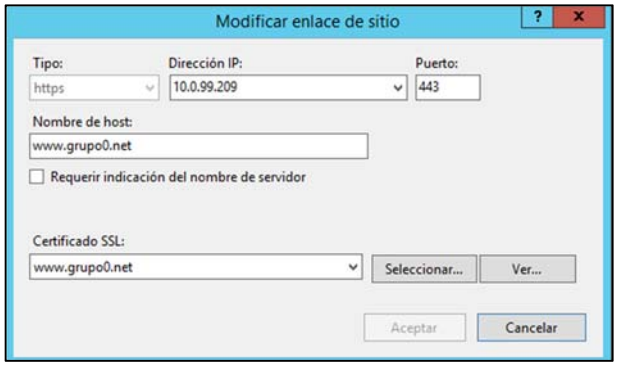
Acciones previas:

- Parar el sitio web_segura.
- Iniciar el sitio Default (entidad certificadora).
- Comprobar que el certificado es www.grupo0.net

Para verificar la tercera, clic en Default Web Site, y clic en Enlaces... (barra de la derecha)

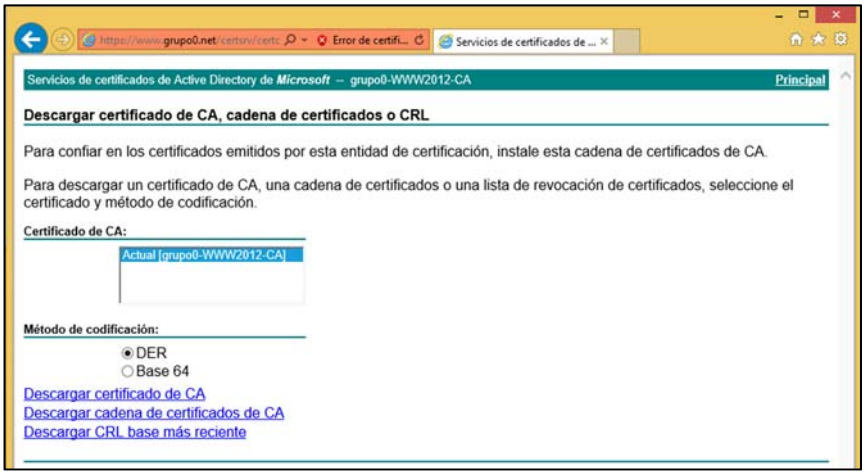


Clicamos en modificar, y verificamos que el Certificado SSL es el adecuado:



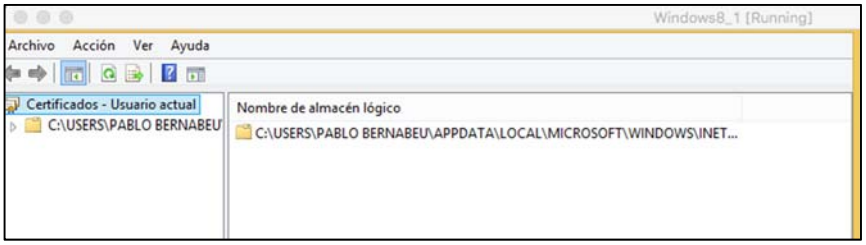
Vamos a nuestra máquina cliente y accedemos a la entidad certificadora https://www.grupoXX.net/Certsrv

Clicamos en Descargar un certificado de CA, cadena de certificación o lista de revocación.



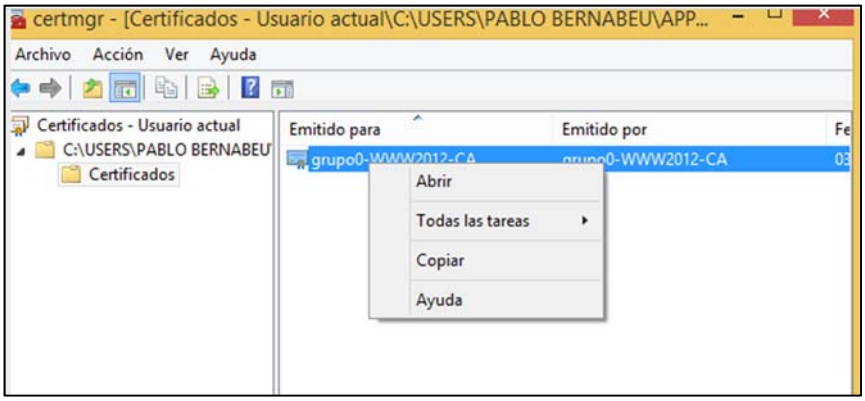
Hacemos clic en descargar cadena de certificados de CA. En este caso, se trata de una entidad de certificación independiente. Podría tratarse de una intermedia y, por tanto, deberíamos descargar toda la cadena:

Indicamos que abra la descarga y nos aparece la siguiente pantalla:

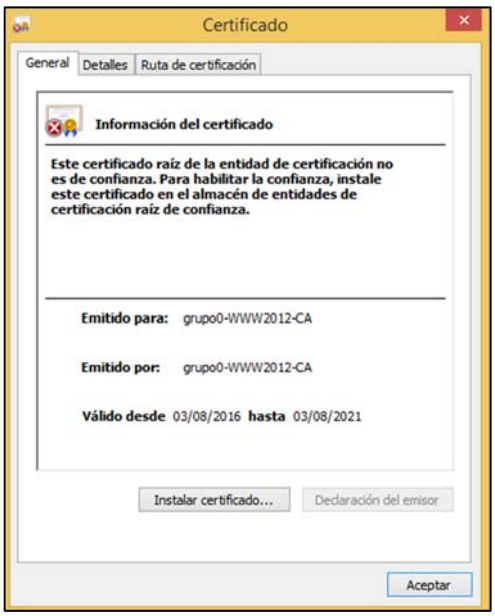


Abrimos el árbol, clicamos en la carpeta certificados y sobre el certificado botón derecho.

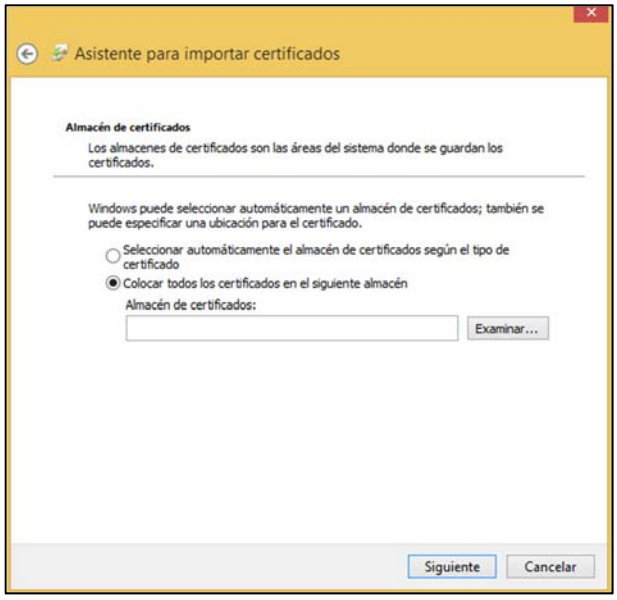
Clic en abrir.



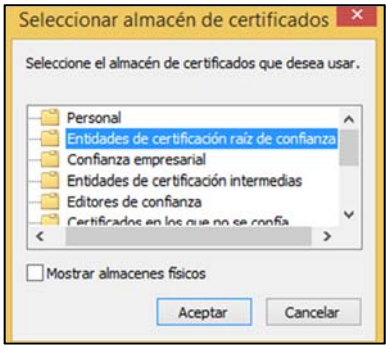
A continuación aparece el certificado raíz de la entidad de certificación. Cabe instalarlo haciendo clic en el botón Instalar certificado…



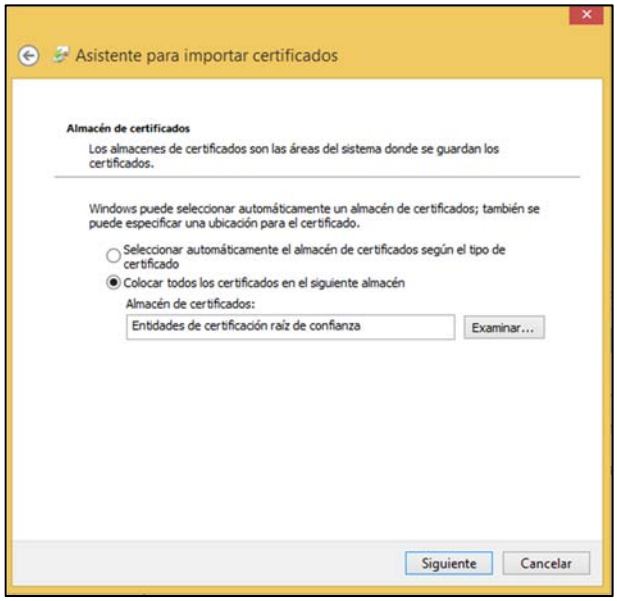
Se abre el asistente para la instalación de certificados, seleccionamos Usuario Local y clic en siguiente.



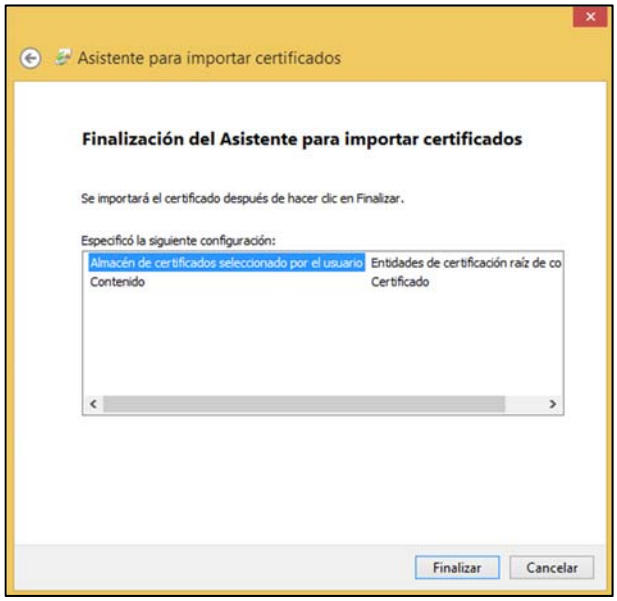
Clicamos en Colocar todos los certificados… y clic en Examinar. Hemos de seleccionar “Entidades de Certificación de confianza” y aceptar.



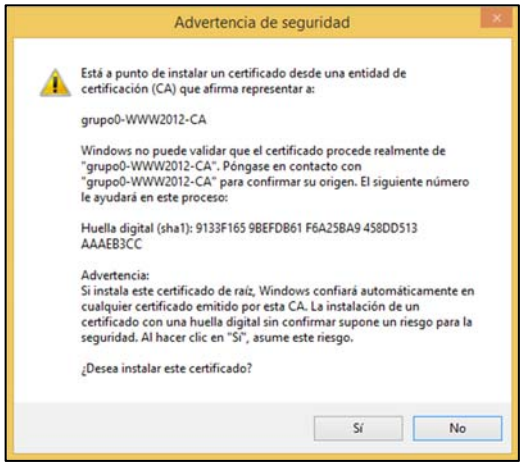
Aceptamos,



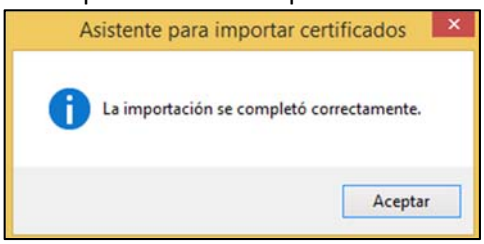
Clic en siguiente para continuar la importación,



Y clic en Finalizar. Aparece una última advertencia antes de instalar definitivamente el certificado, que se ha de aceptar.



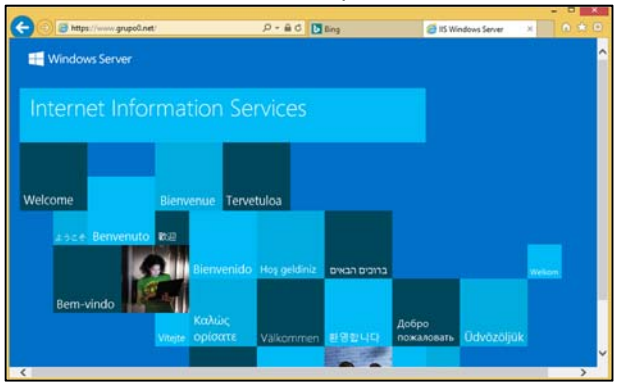
Finalmente, nos informa que la importación se completó correctamente.



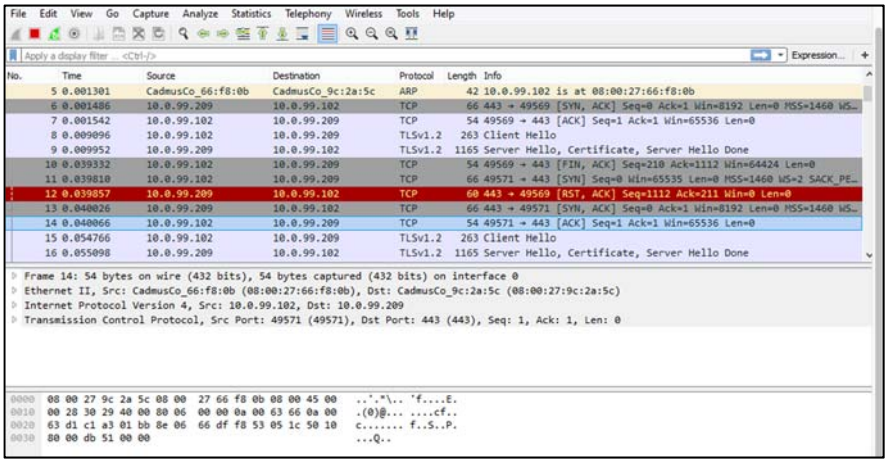
Una vez el cliente confía en la entidad de certificación, cuando se accede a la web no indicará ninguna advertencia de seguridad, directamente entra en la web de forma segura.

Para verificarlo, para la web por Defecto e inicia web_segura.

Observamos entra directamente sin indicar existe problema con el certificado.

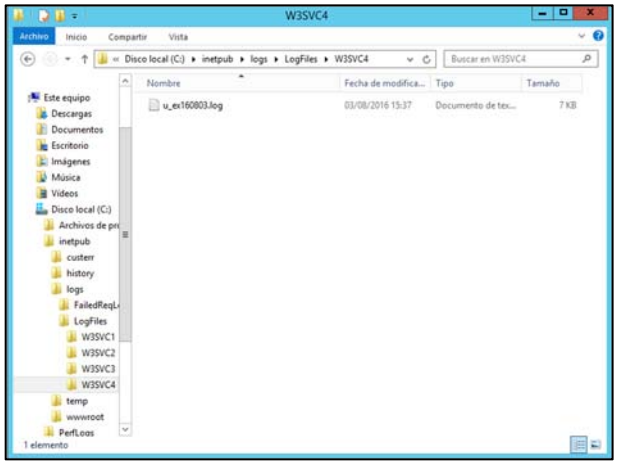


A continuación se consultan los registros que ha capturado el detector donde se pueden ver que las comunicaciones han sido cifradas con el protocolo SSL:

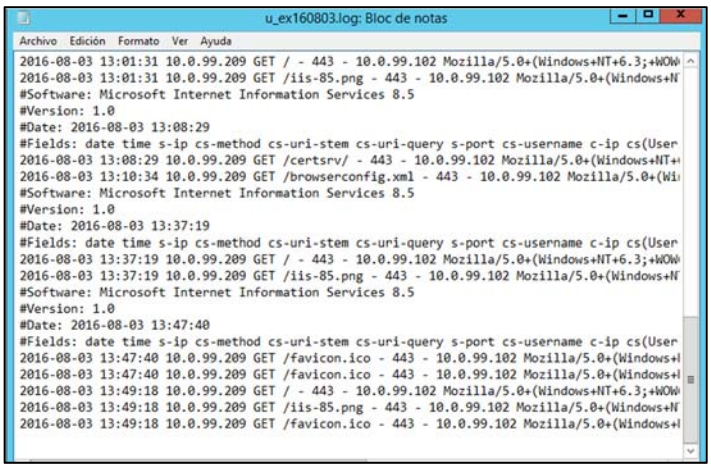


9. Consulta de registros

A fin de tener el máximo control de los servidores, conviene saber dónde se encuentran los ficheros de registros. Cualquiera problema que tenga el servidor web se alamacena en estos registros. En el directorio C:\inetpub\logs\LogFiles\ se encuentran las diferentes carpetas que corresponden a los servidores creados.



Dentro de estas carpetas, el servidor crea unos ficheros donde se encuentran los registros de cada petición web servida:



Si se quieren consultar los registros de aplicación de servidor web hay que acceder al Visor de Eventos. Accede al visor de eventos: