

Configuración Acceso Remoto en Windows 2012 Server r2

1. Direccionamiento (ya lo tenemos al usar la máquina ftpW)

El servicio de acceso remoto permite tener acceso a equipos de forma remota. Se trata de una herramienta útil para poder gestionar redes de servidores.

El acceso remoto de los sistemas Windows se basan en RDP (remote Desktop protocol), un protocolo de escritorio remoto. Este protocolo, además, permite diversas sesiones simultáneas y envío de datos multipunto. RDP está diseñado para admitir diferentes topologías de red, servicios de telefonía y diferentes protocolos como IPX, NetBios o TCP/IP

El puerto que trabaja, por defecto este servicio TCP es 3389.

En este capítulo se muestra como se activa un servicio de acceso remoto. Este acceso remoto puede ser activado en cualquier equipo. Para esta práctica se usa el mismo equipo de la práctica FTP.

2. Consideraciones previas.

Configure las direcciones de red, tal como se le indicaron, tanto para la VLAN de gestión para la VLAN de producción.

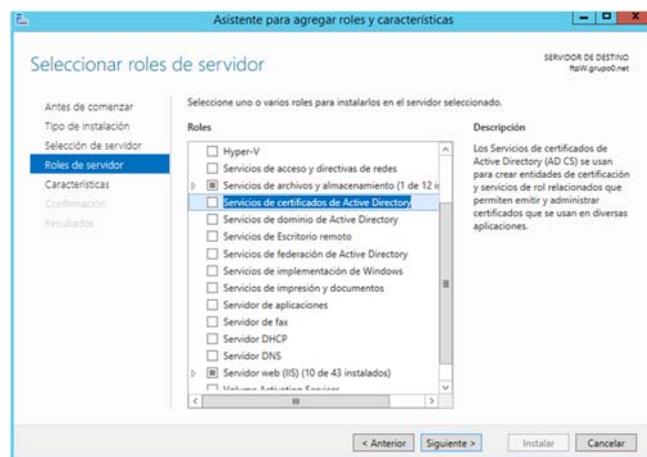
Nombre a la máquina con el nombre ftpW.

El acceso Remoto se realizará usando la VLAN de Gestión.

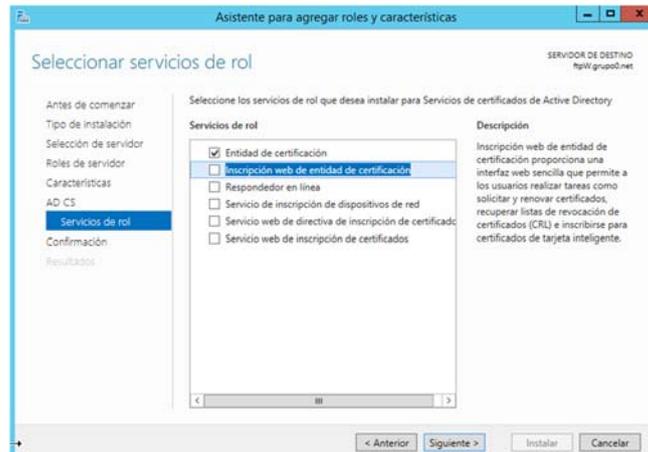
3. Instalación segura.

- **Paso Previo: Crear certificado autofirmado, para la instalación segura.**

Panel del Administrador del Servidor → Administrar → Agregar Roles y características, hacemos clic en siguiente hasta llegar Roles de servidor. Marcamos Servicios de certificados de Active Directory.



Agregamos las características y clicamos en siguiente hasta llegar a la pantalla Servicios de Rol y añadimos Inscripción web de entidad de certificación.

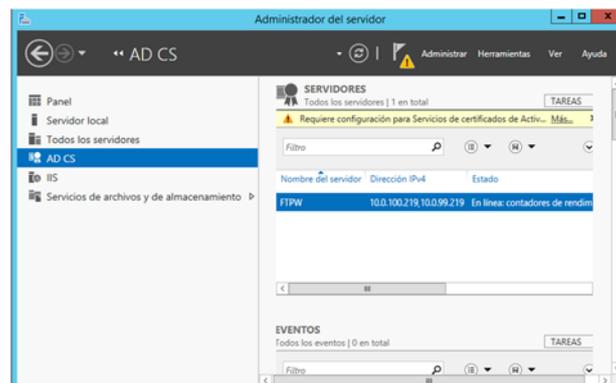


Agregamos las características, confirmamos indicando reinicie si es necesario e instalamos.

Una consideración importante, una vez instalado un Autoridad Certificadora, ya no podemos cambiar el nombre y el grupo de la máquina.

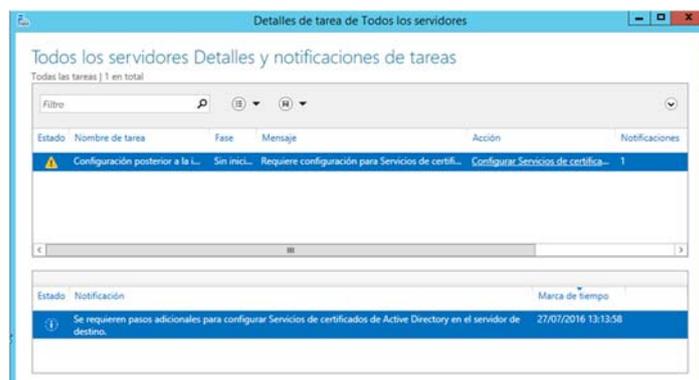
Ahora hay que configurar el servicio de certificados instalados: AD CS.

Clicamos en el panel en AD –CS

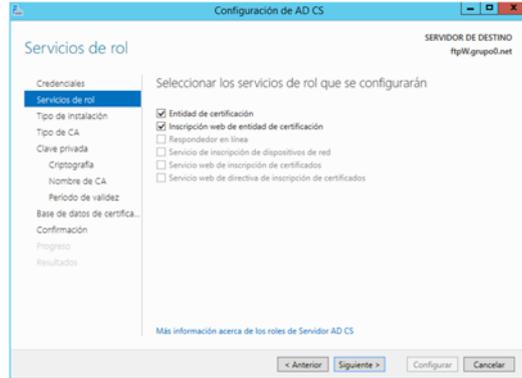


Se observa como aparece una línea de aviso (con fondo color amarillo) en la que se nos indica que “Requiere configuración para Servicios de certificados...), en esa línea aparece Más.. (clicamos sobre Más..). O bien directamente desde el icono bandera, tenemos un aviso y desde allí también podemos acceder a la configuración.

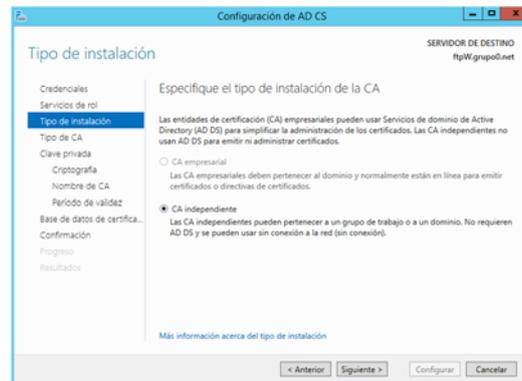
Se abre una ventana, donde clicaremos en Configurar Servicios de Certificación,



Ya estaremos pues en la ventana de Configuración de AD CS, clicamos en siguiente y seleccionamos Entidad de certificación e Inscripción web de entidad de certificación ...



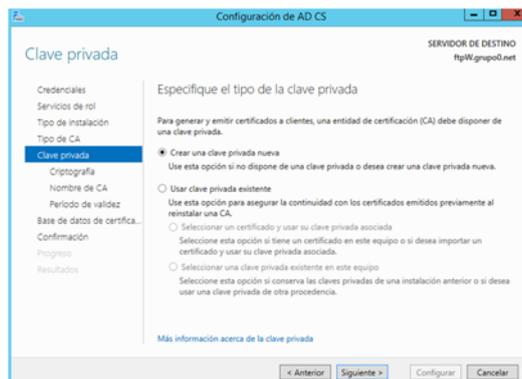
Clicamos en siguiente,



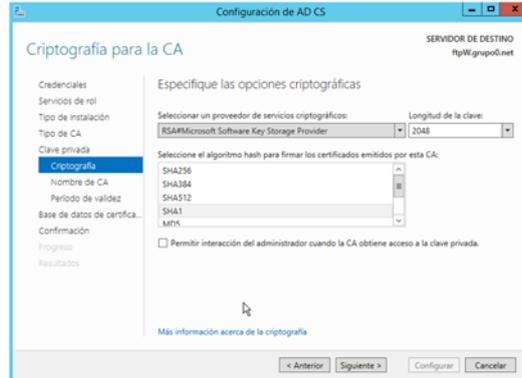
Clicamos en siguiente, Seleccionamos CA raíz,



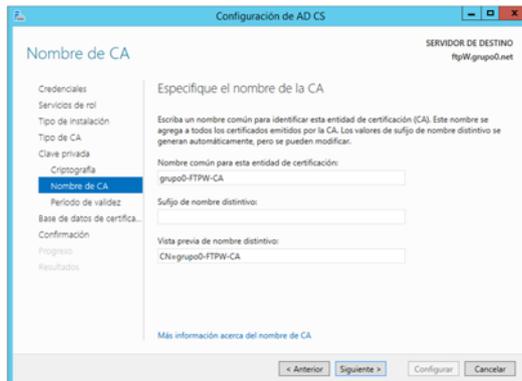
Siguiente, le indicamos "Crear una clave privada nueva",



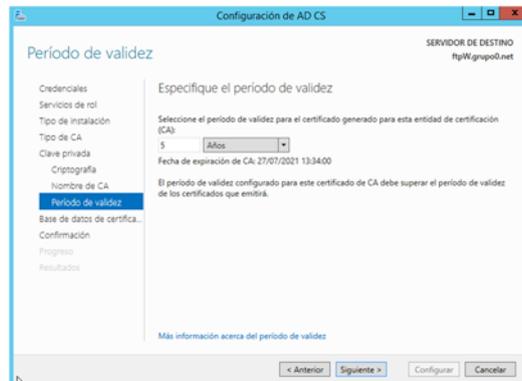
Dejamos las opciones por defecto, cifrado RSA, longitud de clave 2048 y algoritmo hash o resum SHA1:



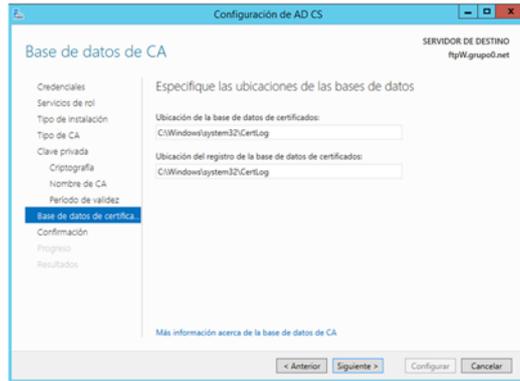
Clicamos en siguiente, y dejamos el nombre por defecto que ofrece el asistente, que ha de ser la asignada para la entidad de certificación creada:



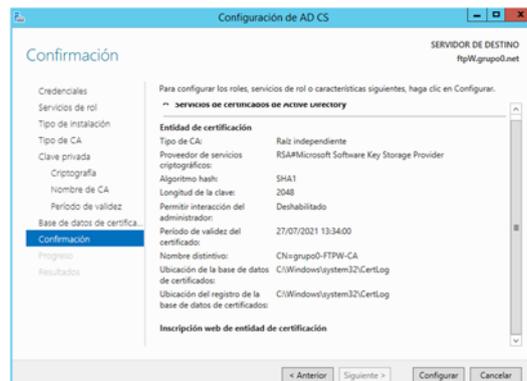
Dejamos período de validez de 5 años,



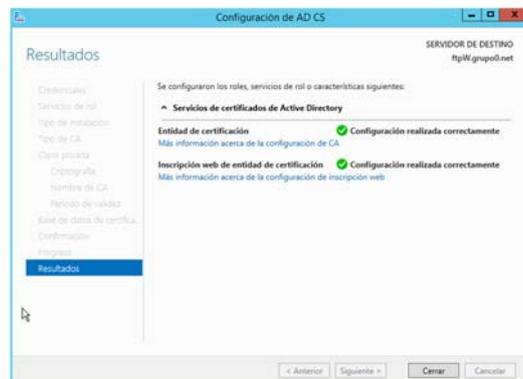
Clicamos en siguiente, aparece una pantalla donde instalará los registros de este servidor:



Clicamos en siguiente, donde tenemos que confirmar, clicando en Configurar.



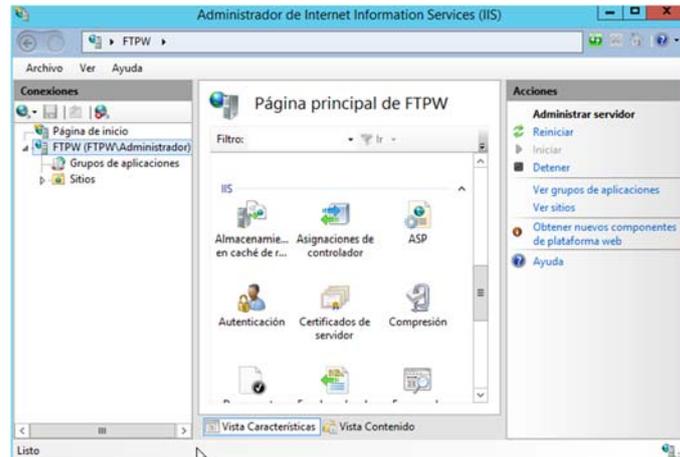
Si todo ha ido bien, nos aparece una pantalla que nos indica que la Configuración ha sido correcta.



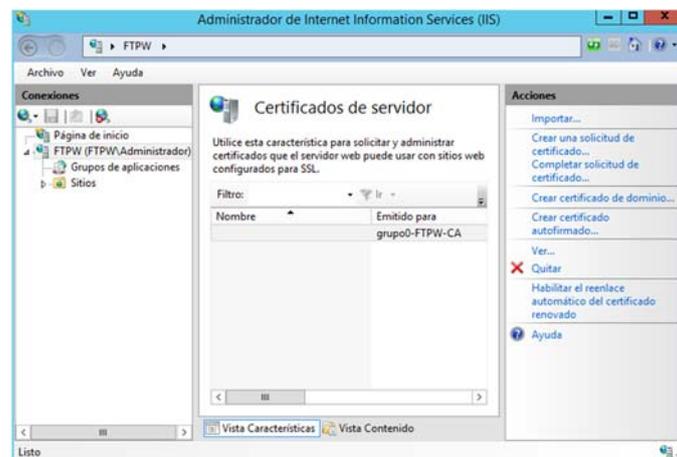
Clicamos en cerrar,

Una vez creada la entidad certificadora vamos a proceder a obtener un certificado del servidor.

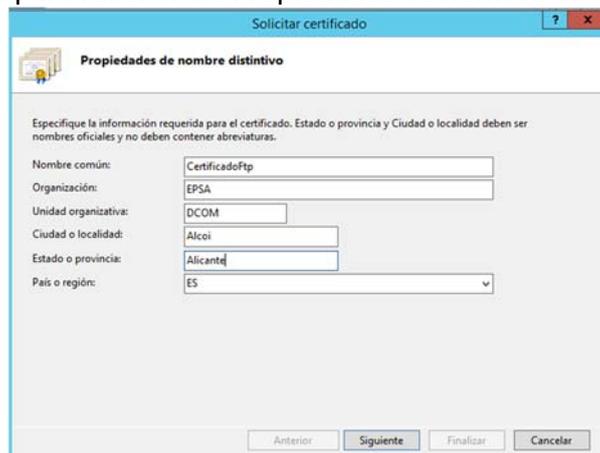
En primer lugar Panel Administrador del servidor → Herramientas → Administrador de Internet Information Services (IIS) , nos desplazamos por la barra hasta encontrar Certificados de Servidor



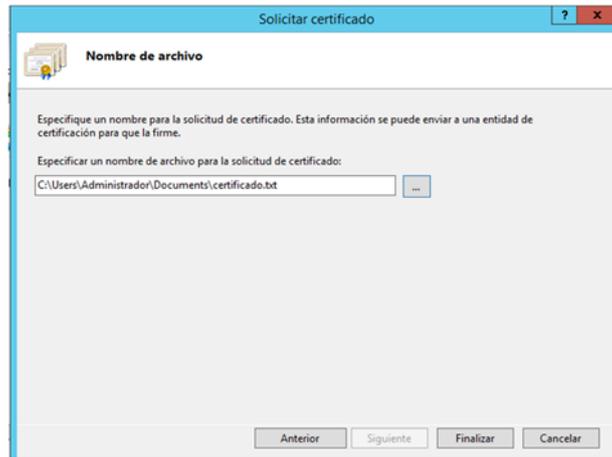
El proceso que vamos hacer es crear una solicitud de certificado que más adelante completaremos.



en la barra Acciones (menú izquierda), clicamos en “Crear una solicitud de certificado”, se abre una pantalla para rellenar las Propiedades de nombre distintivo.

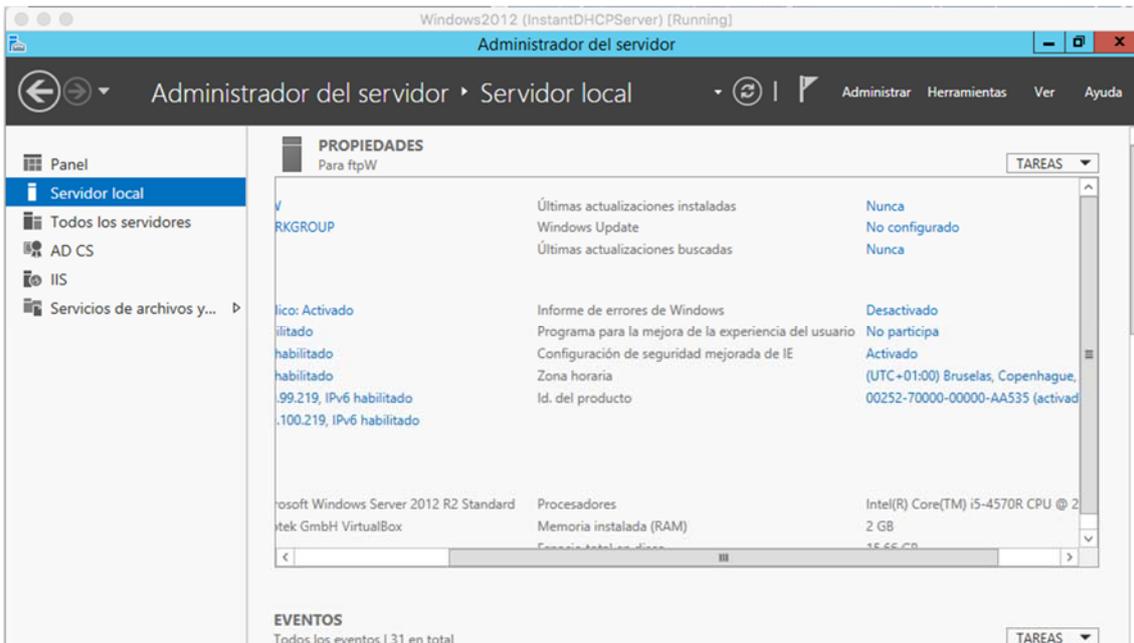


Clicamos en siguiente, aceptamos la longitud y el proveedor nos da por defecto, clic siguiente y especificamos un nombre para la solicitud

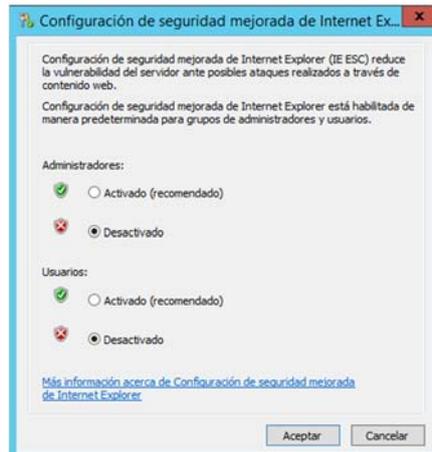


Clicamos en finalizar.

Vamos a abrir internet explorer, pero antes de ello, vamos a desactivar la seguridad para poder crear adecuadamente el certificado: Panel del Administrador del servidor → Servidor local (menú izquierda)



Leemos que configuración de seguridad mejorad de IE está Activado, hemos de desactivarlo. Doble clic sobre Activado

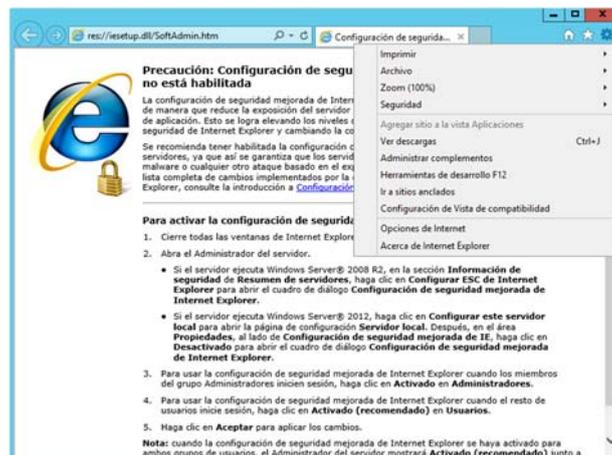


Y marcamos las opciones desactivado, clic Aceptar,

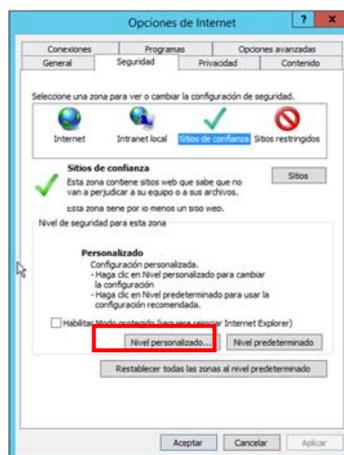
Ahora abrimos internet explorer del servidor

Para ello, en primer lugar, tenemos que permitir a Internet Explorer ADMITIR controles ActiveX. Para ello,

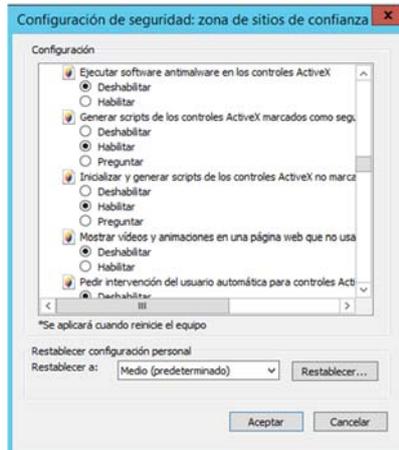
Abrimos Internet Explorer en el servidor, y seleccionamos Opciones de Internet,



Clicamos en la pestaña seguridad y luego clic en Sitios de Confianza, posteriormente clicamos en Nivel Personalizado.



Nos desplazamos por la barra para buscar la opción "Inicializar y generar scripts de los controles ActiveX no marcados como seguros para scripts". La habilitaremos.



Damos a aceptar,

A continuación, introducimos en el navegador la ruta: <http://10.XX.99.219/certsrv/>



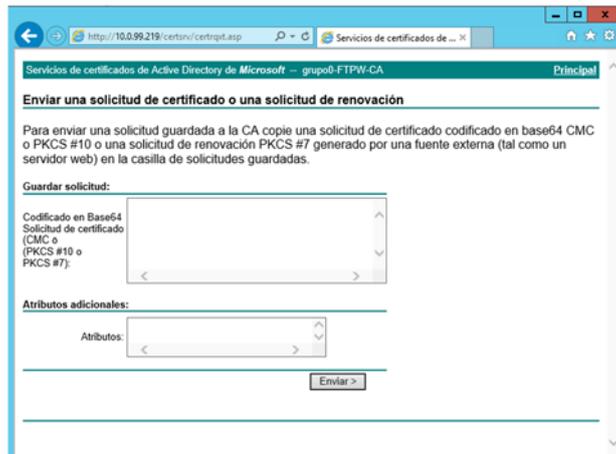
Clicamos en solicitar un certificado,



Clicamos en: "O bien envíe una solicitud avanzada de certificado"



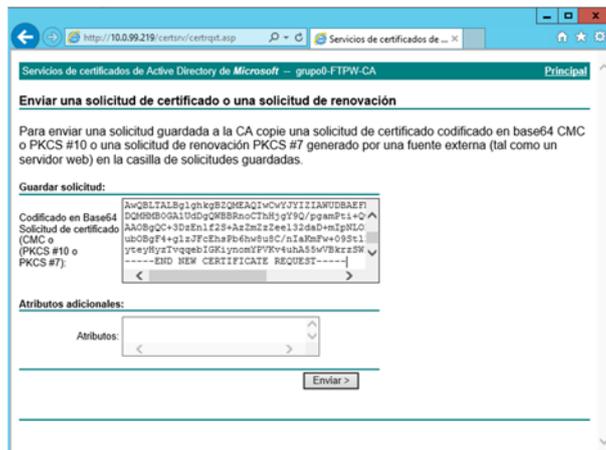
Y seleccionamos la segunda opción, vemos que se nos abre la siguiente pantalla.



Vamos a la carpeta donde hemos guardado certificado.txt y la abrimos



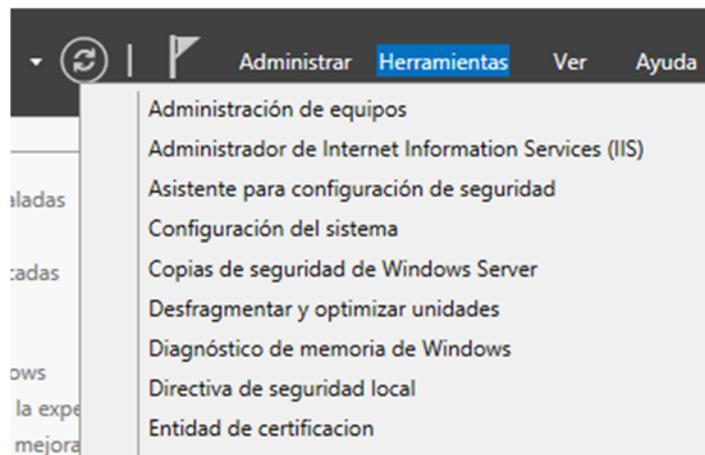
Copiamos el contenido, y lo pegamos en la ventana de solicitud del certificado,



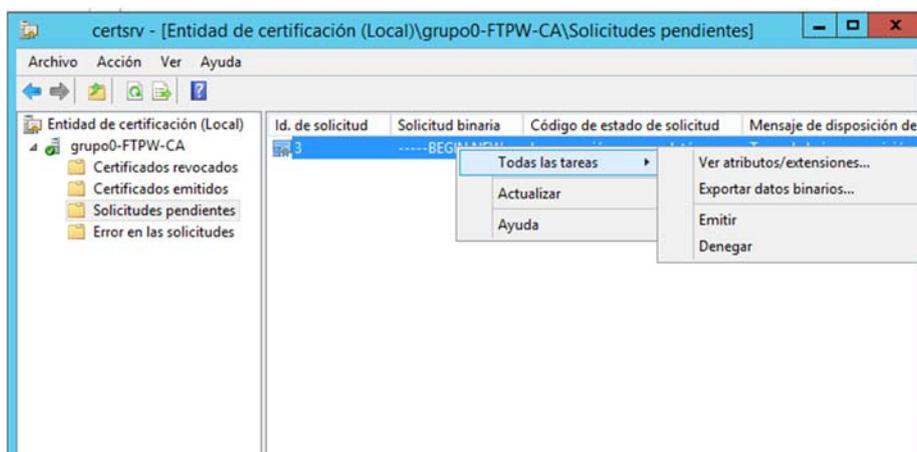
Clicamos en enviar,



Ahora vamos a crear el certificado para cifrar nuestra conexión ftp, para ello, primero vamos a Panel Administrador Servidor → Herramientas → Entidad de certificación.



En la entidad de certificación local, clicamos en la carpeta solicitudes pendientes, clicamos botón derecho sobre nuestra solicitud → Todas las Tareas → Emitir

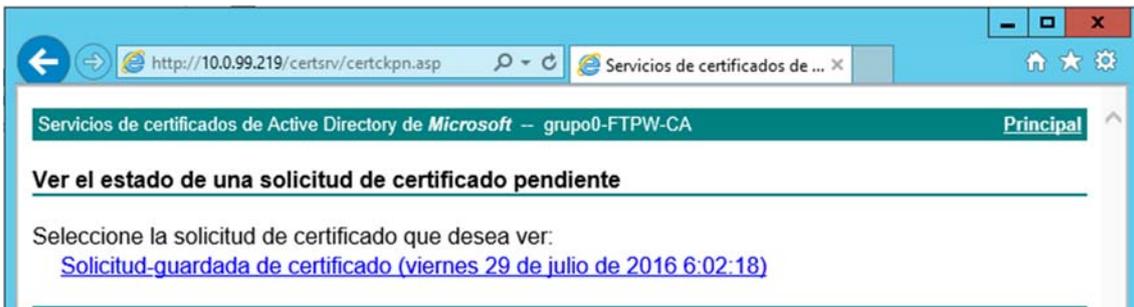


Posteriormente, veremos que aparece en la carpeta certificado emitidos.

Ahora volvemos al navegador, <http://10.XX.99.219/certsrv>



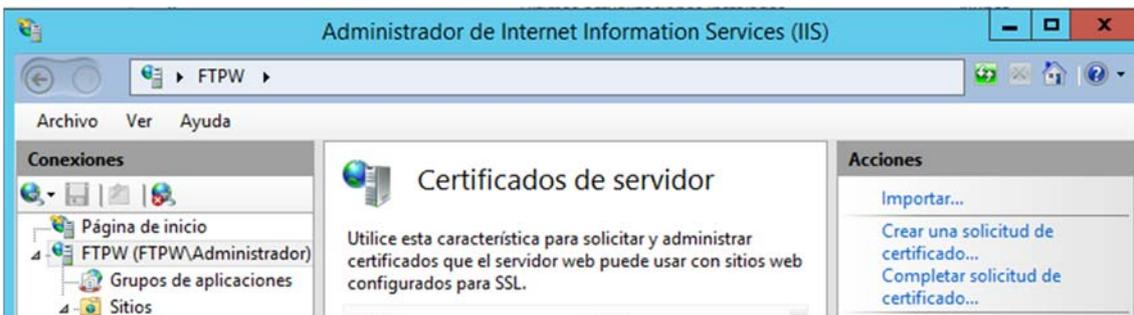
Y clicamos en ver el estado de una solicitud de certificado pendiente. No aparece,



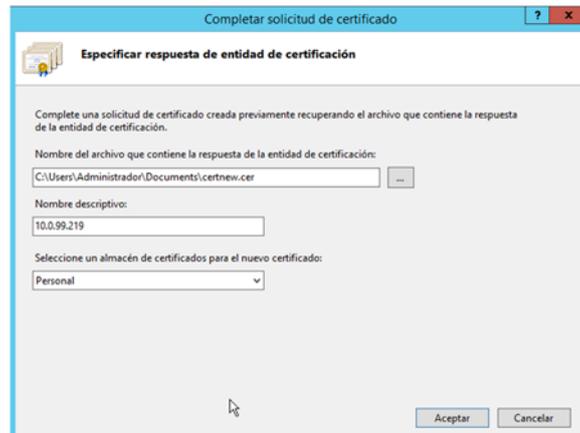
Clicamos en la solicitud y descargamos el certificado, observamos se ha generado el fichero certnew.cer



Si recordamos, aún nos quedaba completar la solicitud del certificado para nuestro servidor



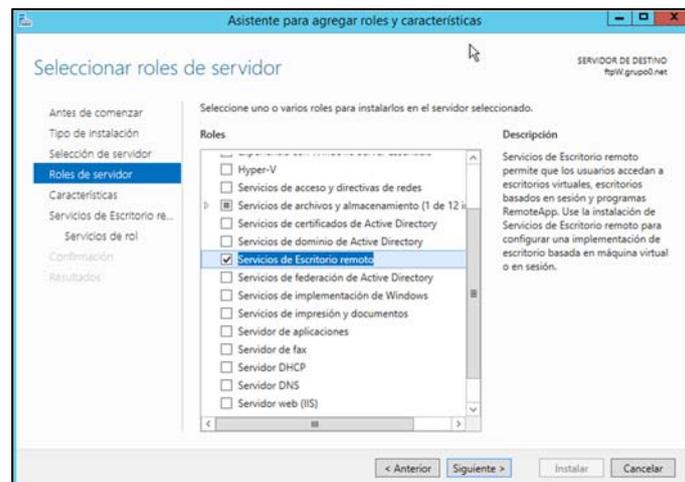
Clicamos en completar solicitud: Buscamos el certificado descargado y como nombre descriptivo ponemos el nombre de servidor, si tuviésemos DNS, habrá que poner ftpW.grupo0.net, en nuestro caso hemos de poner la IP (10.0.99.219)



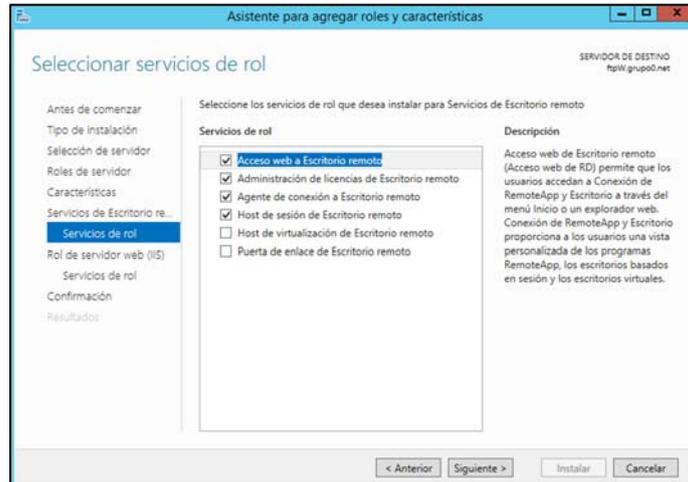
Damos a aceptar,

- **Activación rol de servicio remoto**

Para la activación del servicio de acceso remoto hemos de agregar en el Rol Servicios de Escritorio Remoto.



Clic en siguiente hasta llegar a la pantalla de Servicios de Rol donde seleccionamos las opciones se indican en la siguiente figura:



Clicamos en siguiente hasta llegar a Confirmación: Indicamos se reinicie si es necesario y clicamos en instalar.

En este caso se reinicia el servidor.

Como observamos ahora podemos iniciar con otros usuarios (aún no creados), usuarios que podrán tendrán acceso escritorio remoto. Pero el objetivo de esta configuración es la de gestionar al servidor, por lo que sólo tendrá como usuario el Administrador y el acceso se realizará sólo a través de la VLAN de Gestión. Colocamos como usuario Administrador y la contraseña

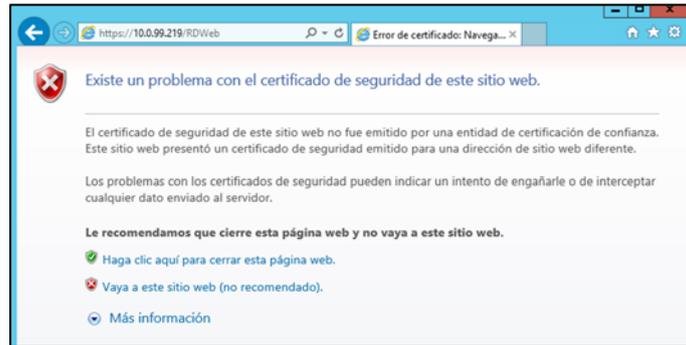
Podemos comprobar que está instalado realizando las siguientes pruebas:

En primer lugar, ver si está instalado el acceso web al escritorio remoto. Como se ejecutan Jscript de Java, lo más rápido será desactivar "Configuración de seguridad mejorada de IE". Panel administrador del servidor → Servidor Local

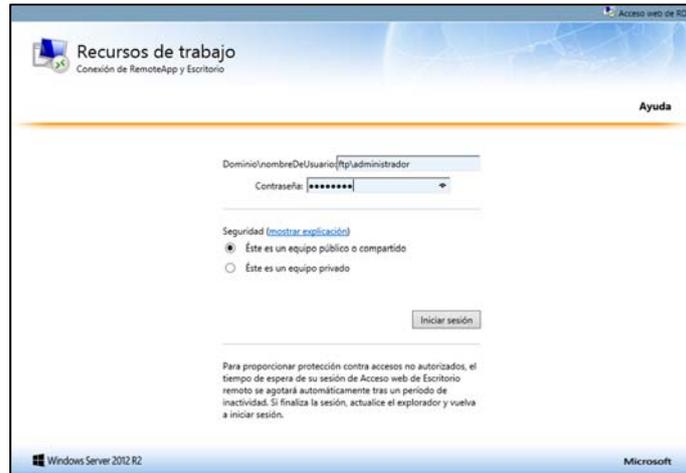


Colocamos <http://nombreServidor/RDWeb>, en caso de no tener activado DNS por nombreServidor colocamos la IP del Servidor.

Al no tener el certificado del sitio web emitido por una entidad de certificación, no sale previamente la página de que existe un problema con el certificado de seguridad. Clicamos en "Vaya a este sitio web (no recomendado)".



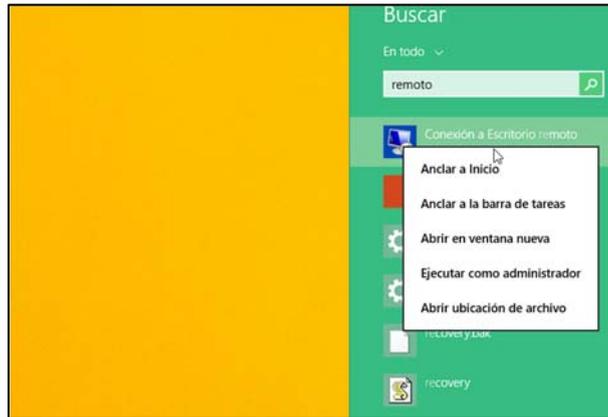
Con lo que nos abre la pantalla para el acceso a Recursos del trabajo:



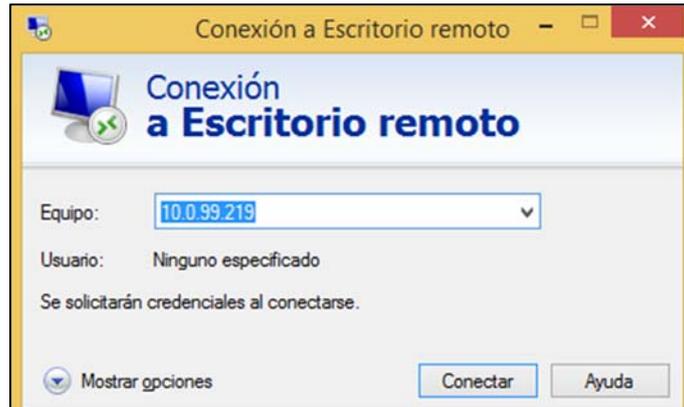
Introducimos ftpWadministrador y la contraseña. Clic iniciar sesión y si todo está bien entraremos en su carpeta, de momento vacía, ya que no hemos añadido ninguna aplicación a la colección.



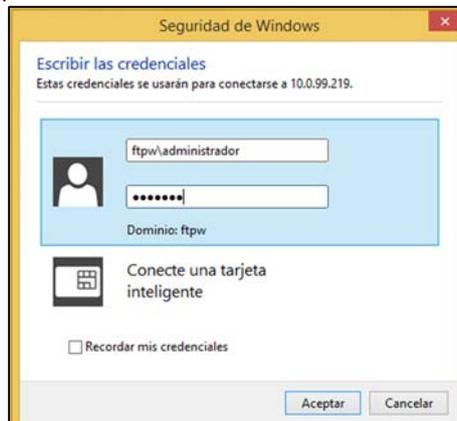
Ahora podemos probarlo desde cualquier máquina cliente. Abrimos Windows 8.1. Buscamos la conexión a Escritorio Remoto. Vamos al vértice inferior izquierdo de nuestra ventana de Windows 8.1 → buscar, escribimos remoto, y aprovecharemos para anclar a la barra de tareas, por ejemplo.



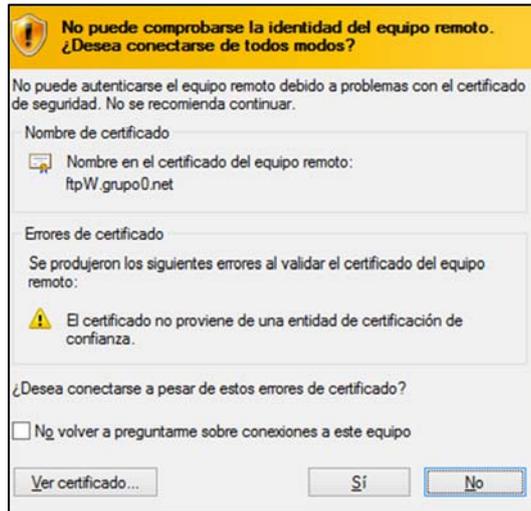
Clicamos en el icono creado en la barra de tareas,



Colocamos la IP de la máquina o ftpW.grupoX.net, si hay activo servicio DNS, y clic en conectar, Como nombre de usuario: ftpw\administrador



Damos a aceptar, nos indica que no puede comprobar la identidad del equipo. De momento no es problema y clicamos en Si:



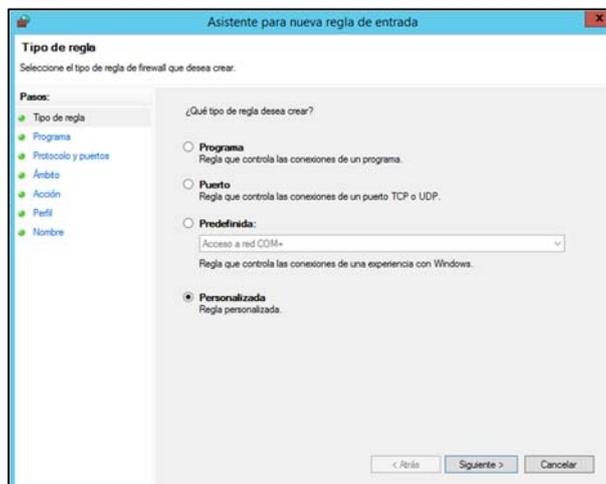
Y ya estamos dentro del servidor para gestionarlo remotamente. A partir de ahora trabajaremos desde nuestra conexión remota

Si todo ha ido bien, estamos en situación de seguir adelante.

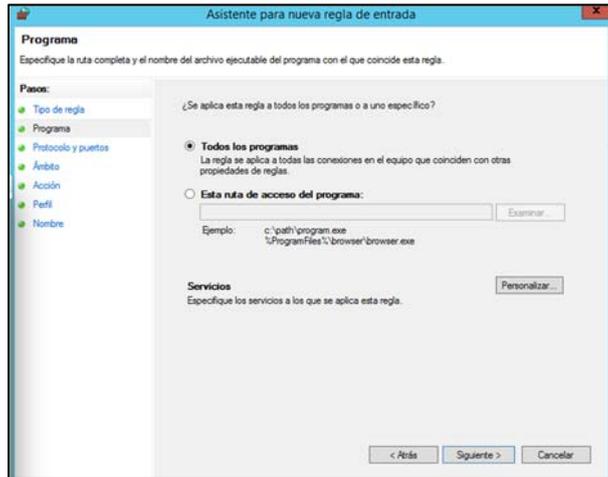
Como observamos hemos entrado por la VLAN de producción, lo cual no es correcto.

En Windows no podemos decirle que escuche por una dirección IP, como si podemos hacer en Centos.

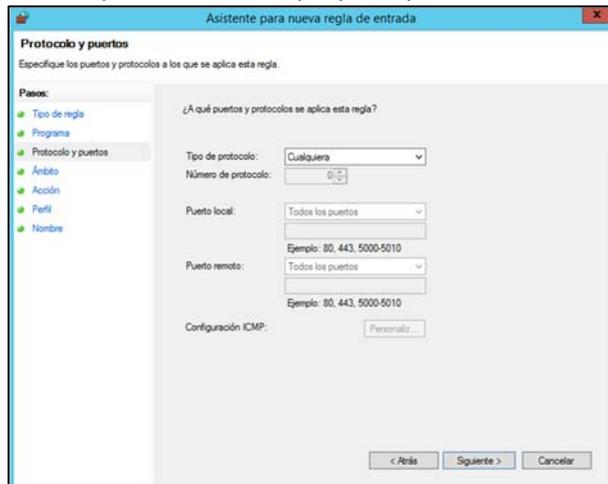
Una de las formas para indicarle que porque IP debe acceder es usando el Firewall, para ello, id a Firewall de Windows con seguridad avanzada. Añadimos una nueva regla de entrada. El tipo de regla es Personalizada.



Clicamos en siguiente, seleccionamos todos los programas,

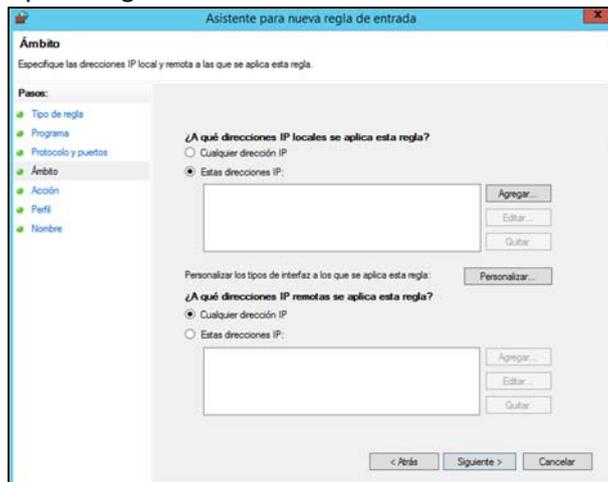


Clic en siguiente, dejamos los parámetros nos propone por defecto.

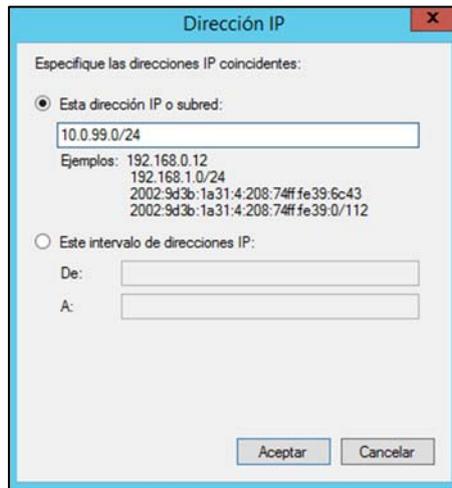


Clic en siguiente,

Y le indicamos que aplique la regla a las direcciones locales clicando en “Estas direcciones”

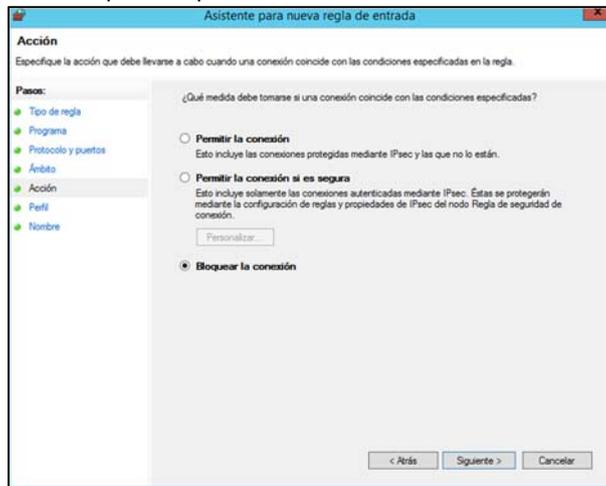


Clicamos en agregar, e indicamos la red de VLAN de producción (10.XX.99.0/24)



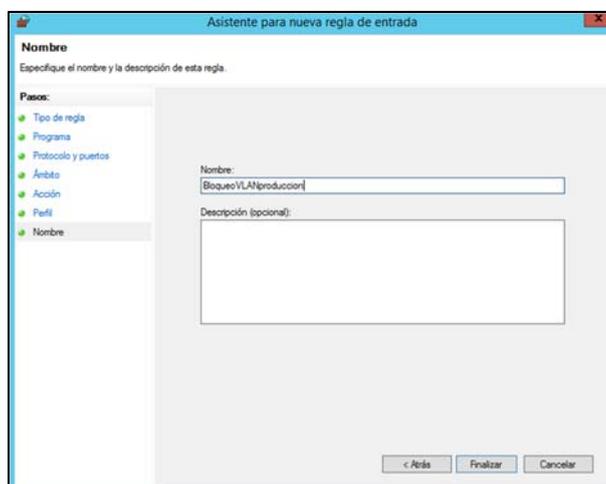
Clicamos en aceptar y en siguiente.

En esta pantalla le indicamos que Bloquee la conexión a escritorio remoto.



Clic en siguiente, le indicamos aplique la regla a Dominio, Privado y Público y nuevamente clicamos en siguiente.

Ponemos nombre a la regla:



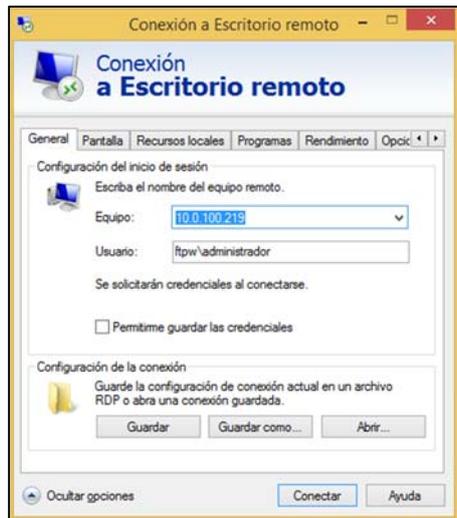
Clicamos en Finalizar.

Ahora deberemos comprobar se aplica la regla.

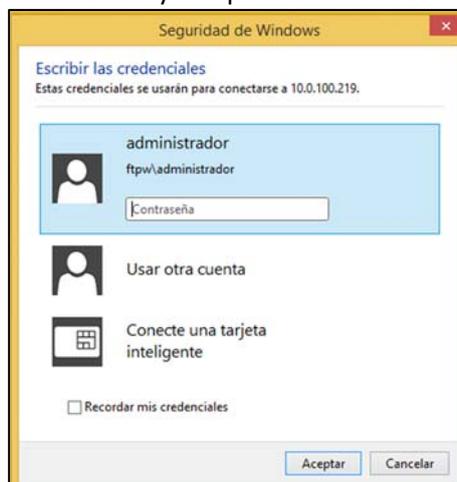
Vamos a nuestra máquina cliente y abrimos el escritorio remoto. Tras un cierto período de tiempo, nos indica que:



Veamos que sucede si nos conectamos por la VLAN de gestión 10.XX.100.219



Rápidamente ha establecido la conexión y nos pide la contraseña:



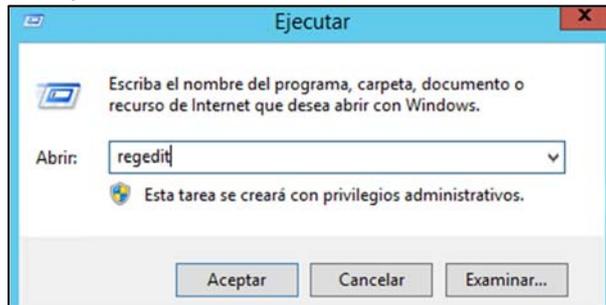
Damos a aceptar, aceptamos las credenciales y ya estamos conectados para administras el servidor.

4. Configuración avanzada

En la configuración siguiente se indica cómo cambiar el puerto donde se encuentre funcionando el acceso remoto. Esta opción se utiliza para dar mayor seguridad al servicio.

El primer paso es acceder al editor de registro (vamos a trabajar desde nuestra máquina cliente en remoto).

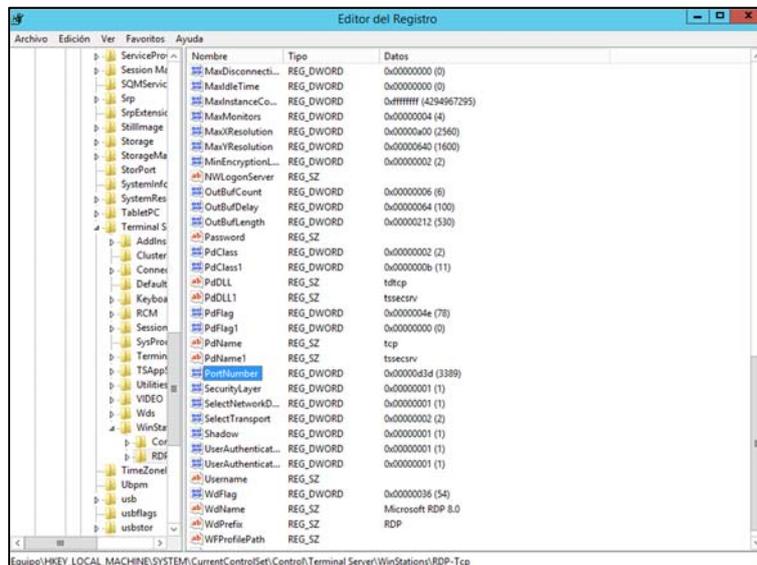
Botón derecho en Inicio → Ejecutar



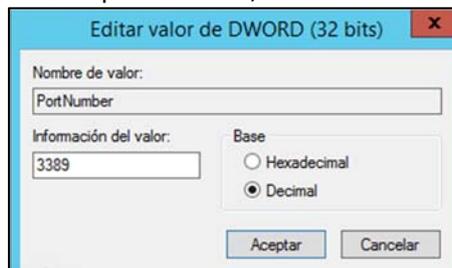
Damos a aceptar, dentro del editor de registro hemos de buscar la ruta siguiente:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-tcp`

Buscamos PortNumber:

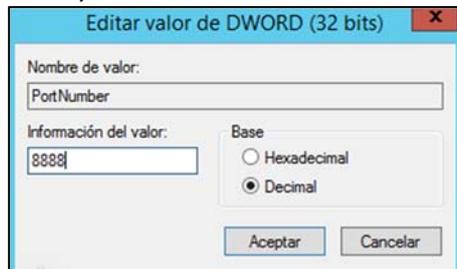


Hacemos doble clic en el parámetro portNumber, clicamos en decimal:



Cambiaremos el puerto a un valor que nosotros deseemos y que sólo sabrá el administrador. Por ejemplo, 8888.

Clicamos en Información de Valor y le damos el valor 8888.

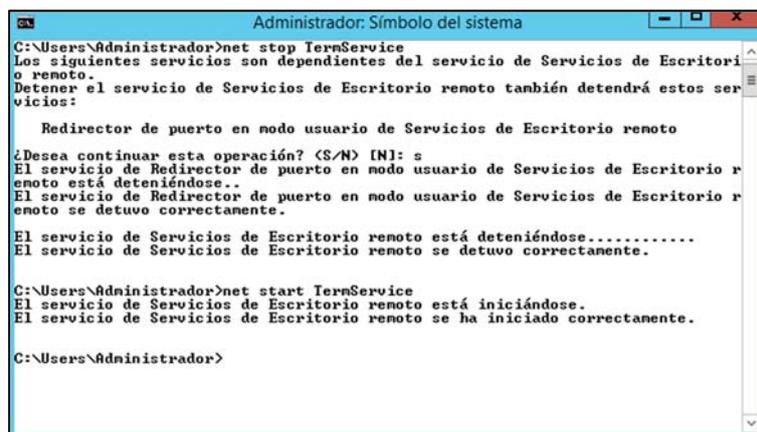


Clicamos en aceptar.

Para que los cambios se apliquen debemos reiniciar el servicio. Para ello tenemos dos formas (vamos a la máquina servidor, no desde la remota).

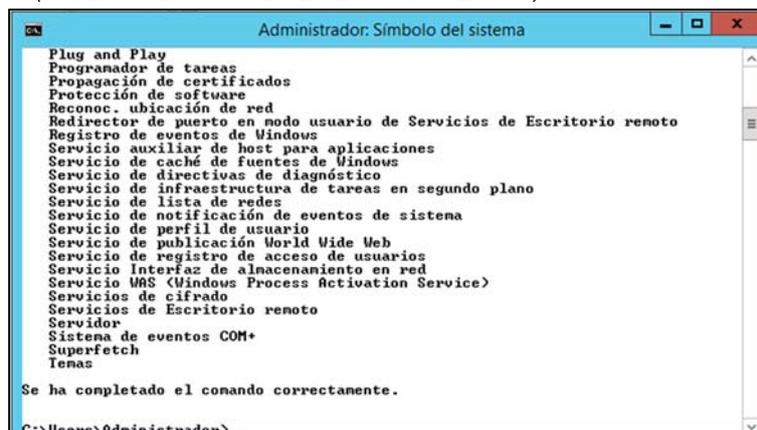
Desde símbolo de sistema:

```
>>net stop TermService
>>net start TermService
```



O bien con

```
>>net start (vemos los servicios activos)
```



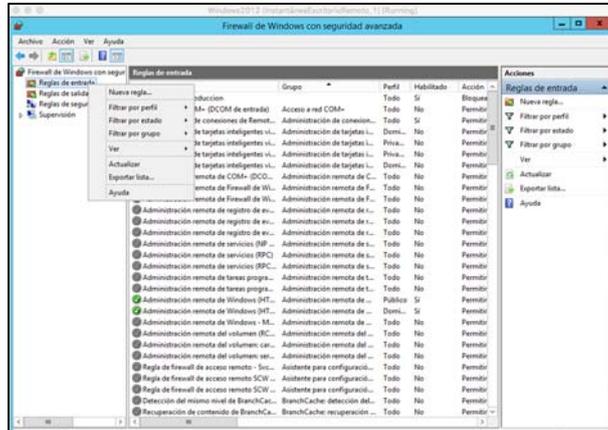
Vemos que está activo “Servicios de Escritorio Remoto”

Y debemos ejecutar:

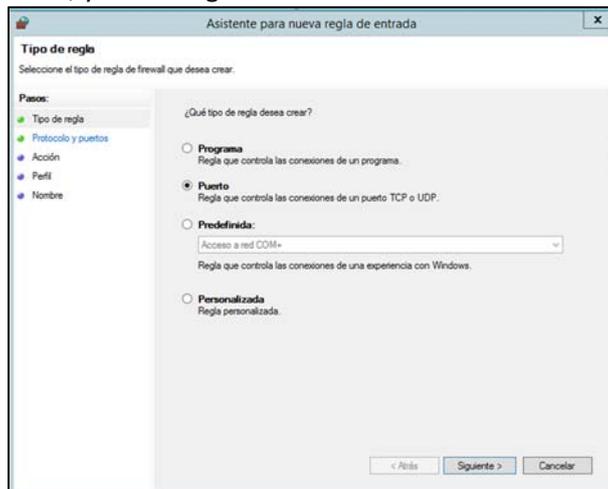
```
>>net stop "Servicios de Escritorio Remoto"
>>net start "Servicios de Escritorio Remoto"
```

Finalmente hemos de indicar en el cortafuegos que permita el tráfico hacía ese puerto.

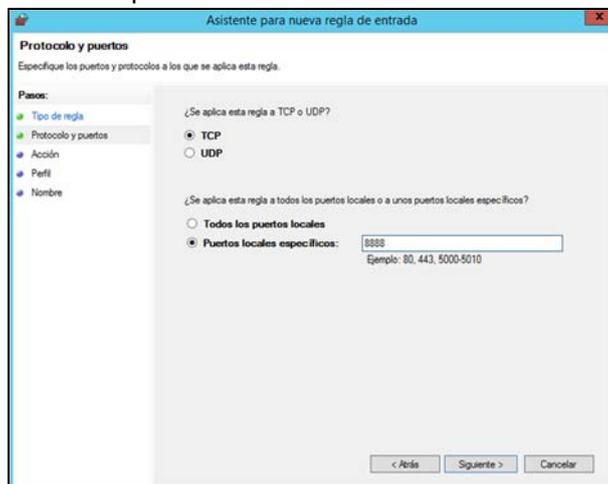
Añadimos nueva regla. Vamos a Firewall de Windows con Seguridad Avanzada, añadimos nueva regla de entrada.



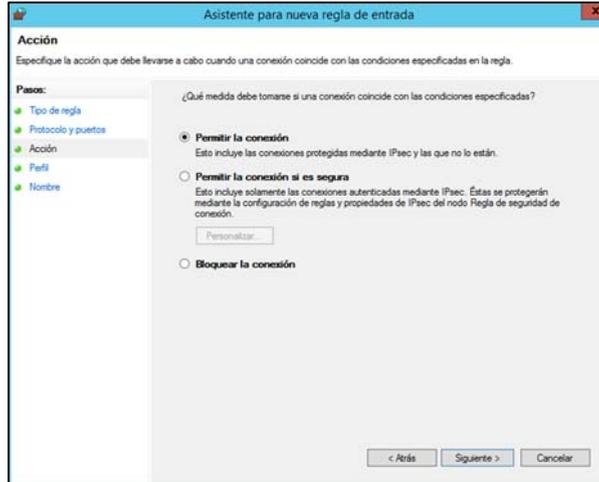
Indicamos la opción puerto, y clic en Siguiete:



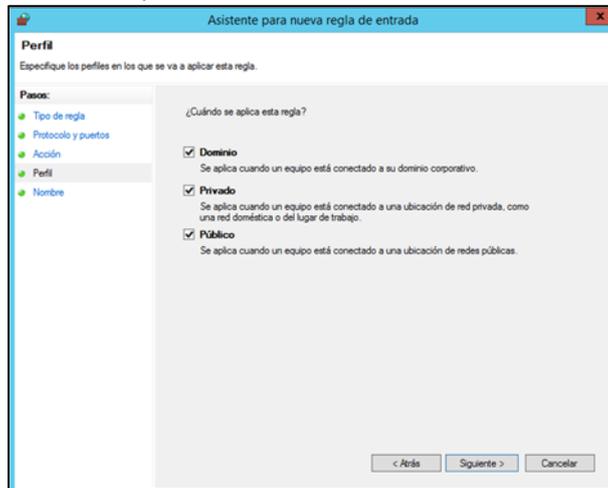
Seleccionamos TCP y marcamos puerto 8888:



Le indicamos Permitir la conexión:



Siguiente y permitimos todos los perfiles:



Clic en siguiente y le ponemos de nombre Acceso Remoto, por ejemplo.

Damos a Finalizar,

Actualizamos el Firewall.

Comprobación en máquina cliente,

Observamos si clic en conectar a 10.XX.100.219 que no se conecta, el motivo, si no le indicamos el puerto, lo hace por el de defecto y éste no está activado.

Le debemos pues indicar el puerto,



Damos a conectar y se inicia el proceso para introducir la contraseña.

5. Análisis de paquetes (WireShark)

Abra la aplicación WireShark y conéctese a Escritorio Remoto, analice las tramas enviadas y recibidas por el servidor.