

Instalación del entorno Microsoft Windows Server 2012R2

MARZO 12, 2015 / FERNANDO SIERRA PAJUELO



En el presente artículo vamos a instalar los distintos componentes de una infraestructura **Microsoft Windows Server 2012R2** perfectamente diferenciada (*Controlador de Dominio y Active Directory, Equipo del Dominio, Servidor de Licencias (KMS) y Servidor de Licencias de Escritorio Remoto*). Un mismo equipo se puede configurar con diferentes roles, pero instalaremos cada uno por separado puesto que es la forma más eficiente a la hora de gestionar el sistema.

Elegir versión e instalar Microsoft Windows Server 2012R2

Lo primero que vamos a ver son las versiones de Microsoft Windows Server 2012R2 que existen e instalar la que mejor le convenga a nuestra infraestructura.



¿Qué versión elegir?

Esta vez Microsoft ha ido a lo fácil para no marear a sus clientes y las versiones disponibles para grandes empresas son tan solo dos: **Standard** y **Datacenter**. Ambas proporcionan el mismo conjunto de características y lo único que las diferencia son los derechos de virtualización. Una licencia de edición *Standard* nos da derecho a ejecutar hasta dos *Virtual Machines* (VMs) en hasta dos procesadores (sujeto a los derechos de uso de VM descritos en el documento de Derechos de uso de Microsoft, que suele ser variable). Por otra parte, una licencia de edición *Datacenter* le da derecho a ejecutar un número ilimitado de VMs en hasta dos procesadores. Cabe mencionar que para empresas pequeñas tenemos otros dos tipos de versiones:

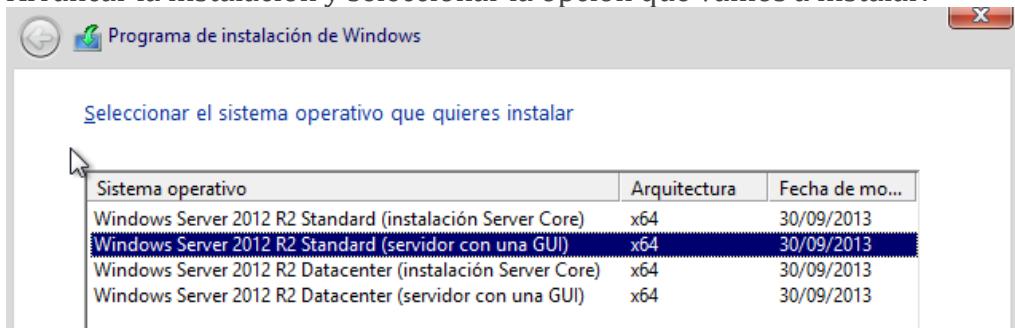
- **Essentials:** Para pequeñas empresas con hasta 25 usuarios, especialmente aquellas empresas que quieran implementar su primer servidor.

- **Foundation:** Para pequeñas empresas con hasta 15 usuarios (solo disponible a través de partners OEM directos).

En este caso instalaremos la versión Microsoft Windows Server 2012R2 Standard, puesto que es más que suficiente para lo que vamos a hacer y no tenemos pensado crear máquinas virtuales. Realizaremos la instalación con la ***Guest User Interface*** (GUI) para utilizar la administración de escritorio visual y no hacerlo todo mediante consola, lo cual será un alivio para muchos de nosotros.

Instalar

Arrancar la instalación y seleccionar la opción que vamos a instalar.



Una vez

cargados los archivos hay que seleccionar el tipo de instalación: **Personalizada**. De esta forma podremos seleccionar dónde vamos a instalar el

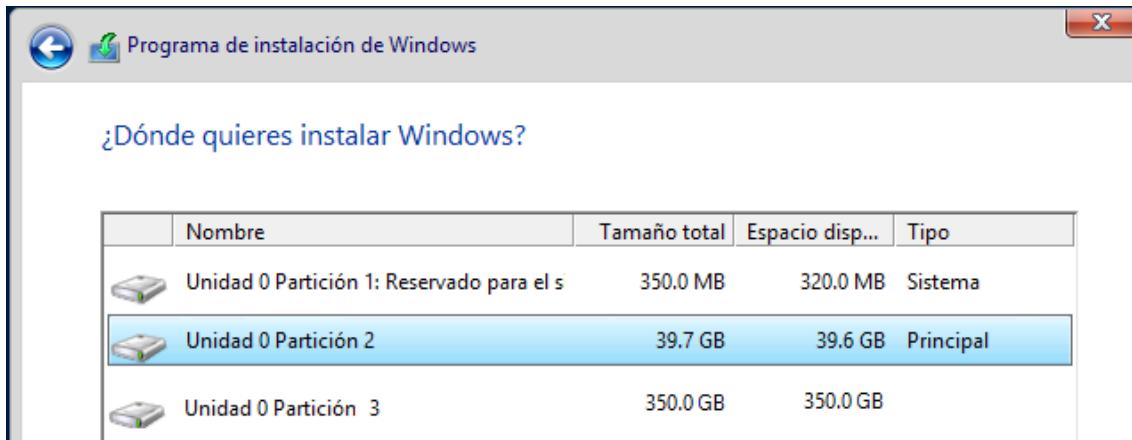


sistema.

El

último paso antes de instalar es elegir dónde hacerlo. Podemos utilizar todo el disco para la instalación o si lo deseamos, *esta es la opción que yo recomiendo*, hacer una partición para instalar Microsoft Windows y otra para los programas y

datos.



Terminada la instalación nos pedirá la contraseña de Administrador. Crear contraseña y finalizar la instalación. Microsoft Windows Server 2012R2 lleva la interfaz de usuario *metro*, para toda la gestión se utiliza el **Administrador del Servidor**.

Domain Controller & Active Directory

Una vez instalado Microsoft Windows Server 2012R2, procederemos a instalar el Controlador de Dominio. La forma más eficiente de aprovechar el potencial de los equipos con Microsoft Windows Server es mediante la creación de dominios. En los dominios se almacena de forma centralizada la información administrativa y de seguridad, facilitando así la labor del administrador. Para manejar los datos se crea el Directorio Activo, que guarda en una base de datos toda la información sobre los recursos de la red, permitiendo el acceso de los usuarios. Cuando se instala un **Active Directory** se convierte ese equipo en un **Domain Controller**, por lo que este rol irá unido.

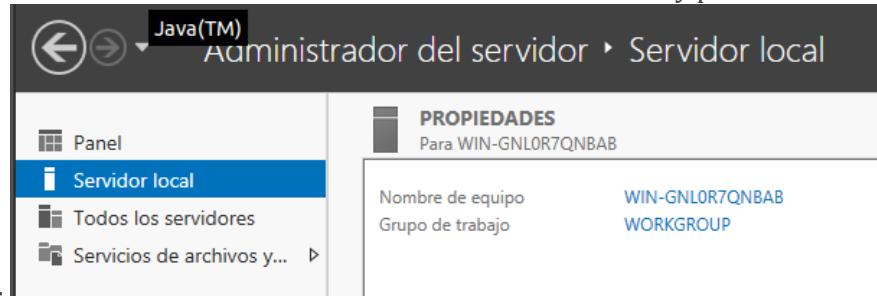
En resumen, la importancia de un controlador de dominio para una red corporativa radica en los siguientes aspectos:

- Se centralizan las contraseñas de usuarios en un solo punto físico.
- La información se puede proteger de una forma mucho más fácil al estar centralizada en un solo equipo.
- Perimetralmente, es más fácil evitar una intrusión en un ordenador que hacerlo en una red al completo.

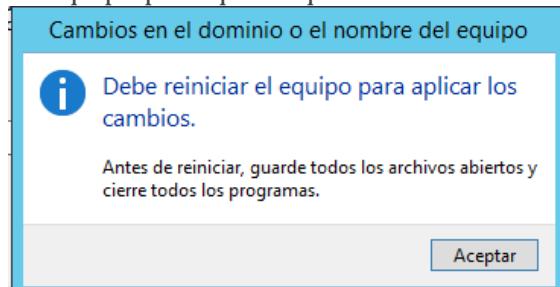
Cada dominio quedará identificado bajo un nombre de servidor por el **Domain Name System** (DNS), en español: Sistema de Nombres de Dominio, por lo que junto al Domain Controller se instalará un Server DNS.

Instalación del Domain Controller

1. Dentro de *Administrador del Servidor* seleccionar *Servidor local* y pulsar sobre **Nombre de Equipo:**

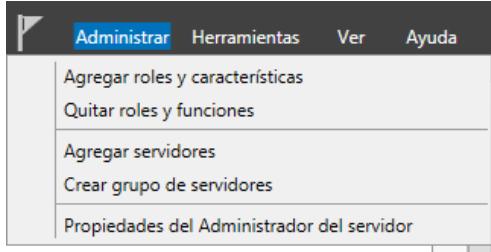


- Pulsar en *Cambiar* e introducir el nombre del equipo, en nuestro caso usaremos **domaincontroller**.
- Reiniciar el equipo para que adquiera su nuevo



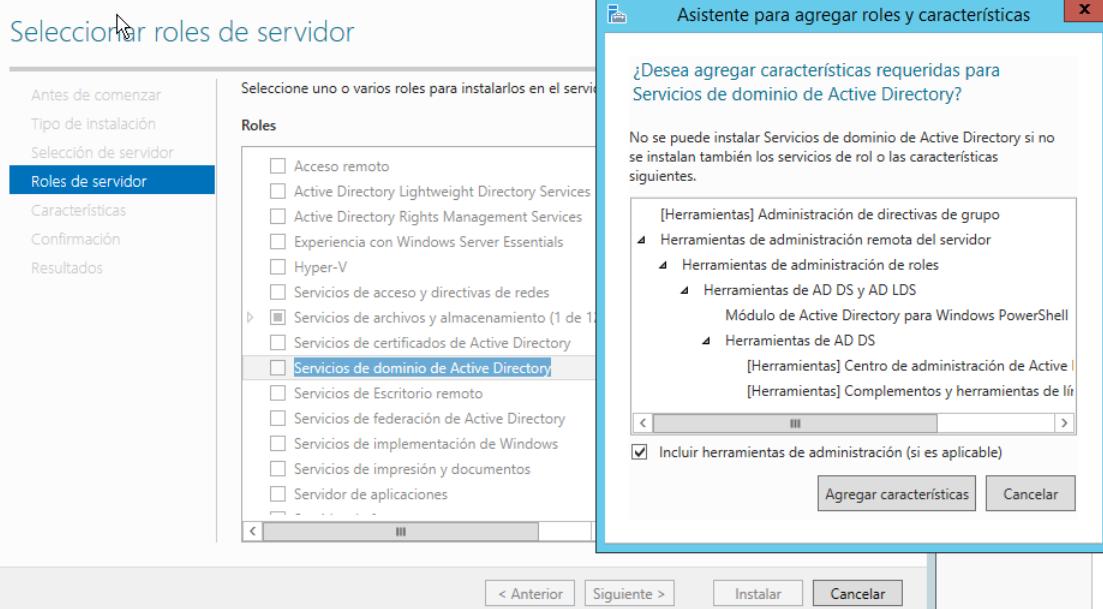
nombre.

2. Dentro de *Administrador del Servidor* seleccionar *Administrar* y pulsar sobre **Agregar roles y características:**

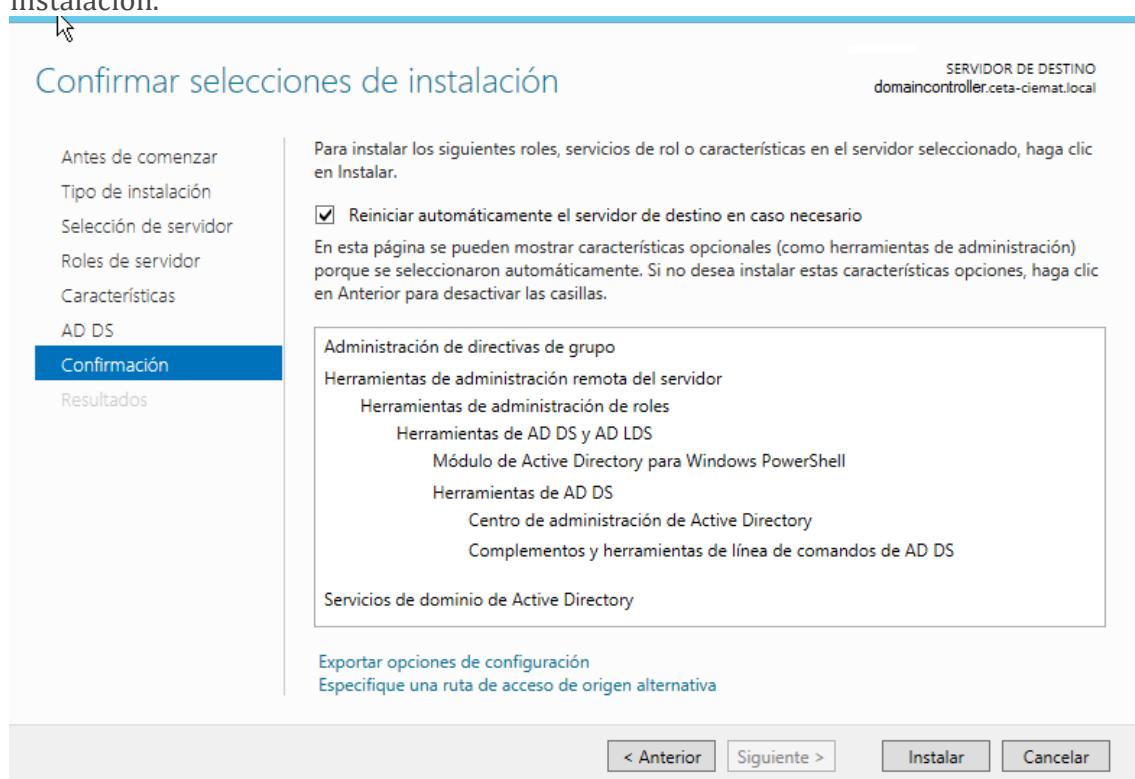


- En la primera ventana pulsar **siguiente >**. En la segunda, seleccionar **Instalación basada en características o en roles** y pulsar **siguiente >**. Seleccionar el servidor desde el que estamos realizando la instalación (domaincontroller) y pulsar **siguiente >**. Seleccionar **Servicios de dominio de Active Directory** y en el cuadro que aparecer *Agregar*

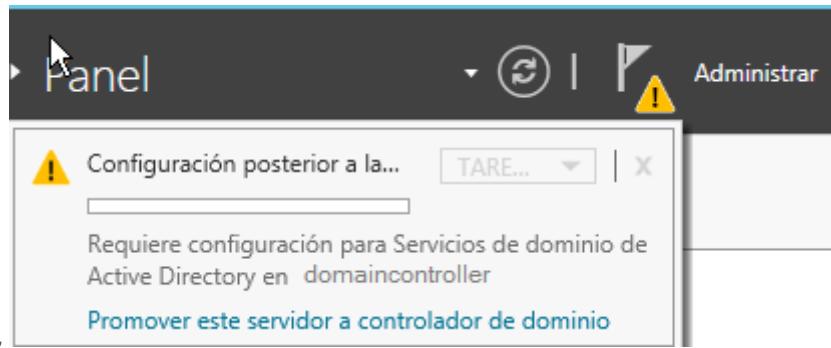
características.



- Pulsar **siguiente >** hasta que se confirme la instalación.



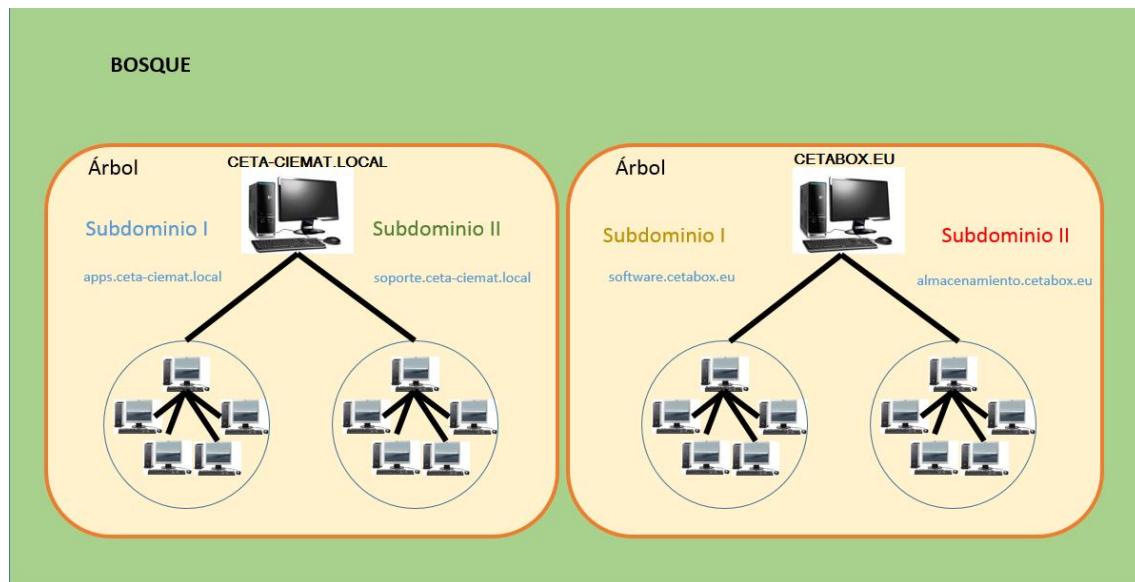
3. Una vez terminada la instalación, cerrar el cuadro de diálogo y en la bandera de *Notificaciones* seleccionar **Promover este servidor a controlador de dominio.**



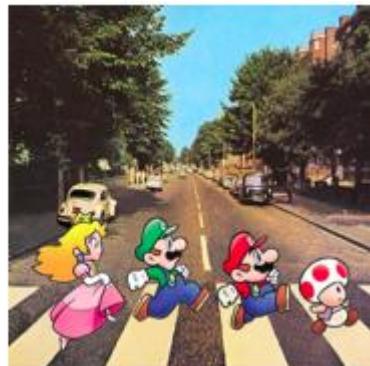
Antes de continuar vamos a comentar los términos más utilizados en este ámbito.

1. **Espacio de nombres:** Los nombres de dominio se forman por dos o más palabras separadas por puntos. Así se nombran los equipos del dominio: equipo.dominio.local.
2. **Server DNS:** permite realizar la resolución de nombres al convertir los nombres de hosts a direcciones IP y viceversa.
3. **Domain Controller:** Microsoft Windows Server con **Active Directory** instalado. En este equipo se realiza la gestión.
4. **Nombre de Dominio:** Son las denominaciones asignadas a los equipos de la red. En el caso de nuestra infraestructura es **ceta-ciemat.local**.
5. **Árbol de dominio:** es el conjunto de dominios formado por el nombre de dominio raíz y el resto de dominios.
6. **Bosque de árboles de dominios:** Es el conjunto de árboles de dominio.

Seguramente esto nos dice a algunos mucho y a otros nada, así que ahí va un esquema:



Seguimos!!



- Pulsar en **Agregar un nuevo bosque** y crear el dominio para nuestro AD. Después pulsar **Siguiente >**.

Configuración de implementación

Configuración de imple...

Opciones del controlador...

Opciones de DNS

Opciones adicionales

Rutas de acceso

Revisar opciones

Comprobación de requisi...

Instalación

Resultado

Seleccionar la operación de implementación

- Agregar un controlador de dominio a un dominio existente
 Agregar un nuevo dominio a un bosque existente
 Agregar un nuevo bosque

Especificación de dominio para esta operación

Nombre de dominio raíz:

[Más información acerca de configuraciones de implementación](#)

< Anterior

Siguiente >

- Seleccionar el nivel funcional del bosque y del dominio. Si se pretenden añadir servidores Microsoft Windows Server 2008R2 o 2012 es recomendable bajar el nivel predeterminado. Siempre se puede promocionar a un nivel superior pero jamás se puede descender a un nivel funcional inferior. Se debe seleccionar el server DNS y escribir una contraseña *Directory Services Restore Mode (DSRM)*. Una vez seleccionados todos los

campos que necesitamos, pulsar **Siguiente >**.

The screenshot shows the configuration of the new forest and domain root. It includes dropdown menus for selecting the forest functional level (Windows Server 2008 R2) and domain functional level (Windows Server 2008 R2). Below these are checkboxes for specifying domain controller capabilities: 'Servidor de Sistema de nombres de dominio (DNS)' (checked), 'Catálogo global (GC)' (checked), and 'Controlador de dominio de solo lectura (RODC)' (unchecked). There is also a section for entering a password for the directory service recovery mode, with fields for 'Contraseña:' and 'Confirmar contraseña:' both containing masked text.

- Comprobar los requisitos de la instalación y pulsar **Instalar**.

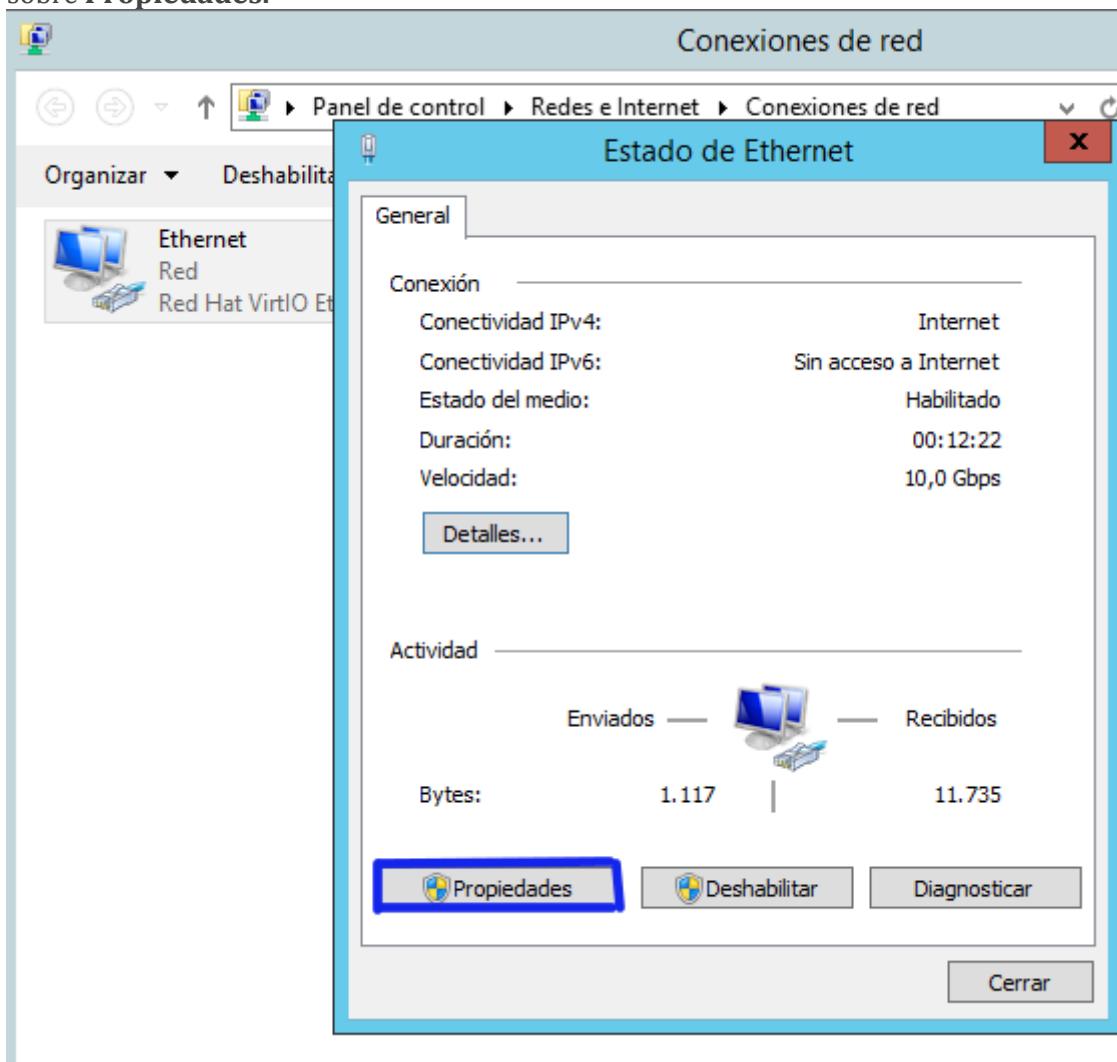
The screenshot shows the results of prerequisite checks. A green checkmark indicates that all previous checks were successful. It includes a link to 'Mostrar más' (Show more) and a summary message: 'Los requisitos previos deben validarse antes de instalar los servicios de dominio de Active Directory en el equipo'. Below this is a link to 'Volver a comprobar requisitos previos' (Check prerequisites again). A 'Ver resultados' (View results) button is expanded, showing two warning messages: one about the Windows NT 4.0 compatibility setting and another about network adapter IP address assignments. At the bottom, there is a note about automatic restart after installation and a link to 'Más información acerca de requisitos previos' (More information about prerequisites).

- Una vez terminada la instalación **Reiniciar** el equipo y quedará instalado nuestro server Active Directory / Domain Controller.
CONSEJO: Crear un segundo Domain Controller para el Active Directory. Para ello crear un equipo del dominio e instalar el rol de Domain Controller.

Equipo del Dominio

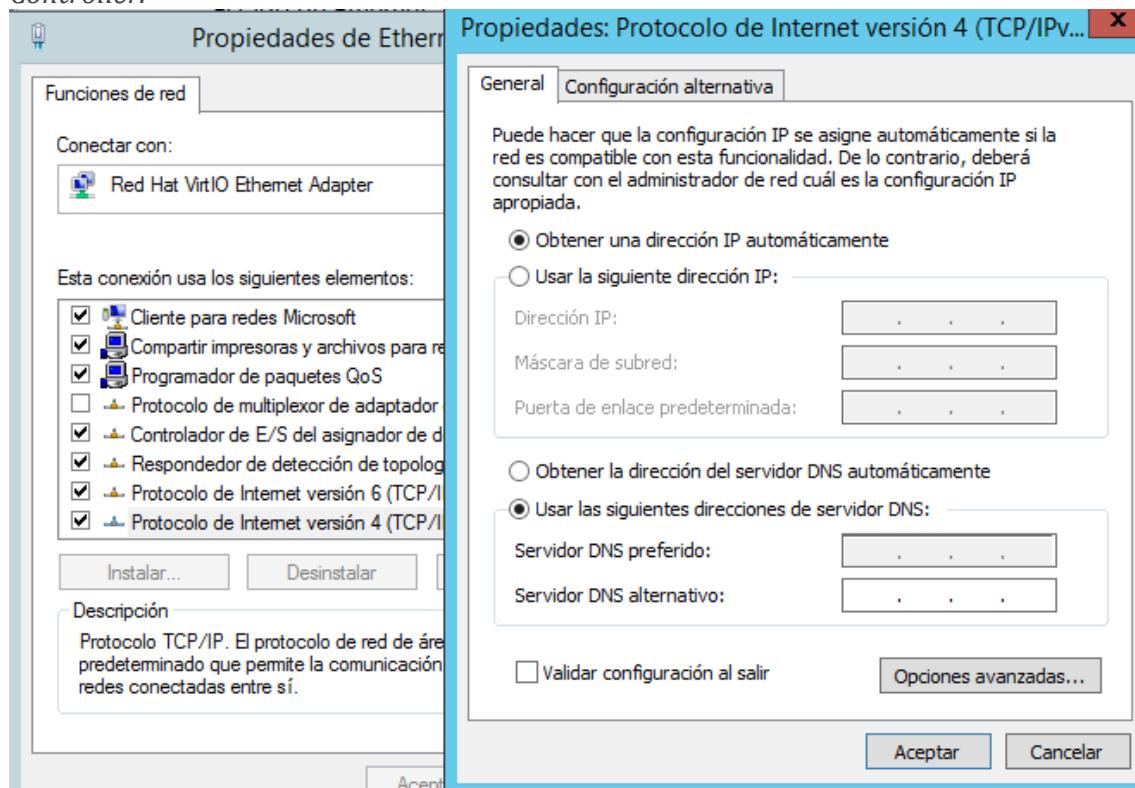
1. Cualquier equipo que tengamos se puede unir al dominio. Para ello hay que ir a la *configuración de Red* y pulsar

sobre **Propiedades**.

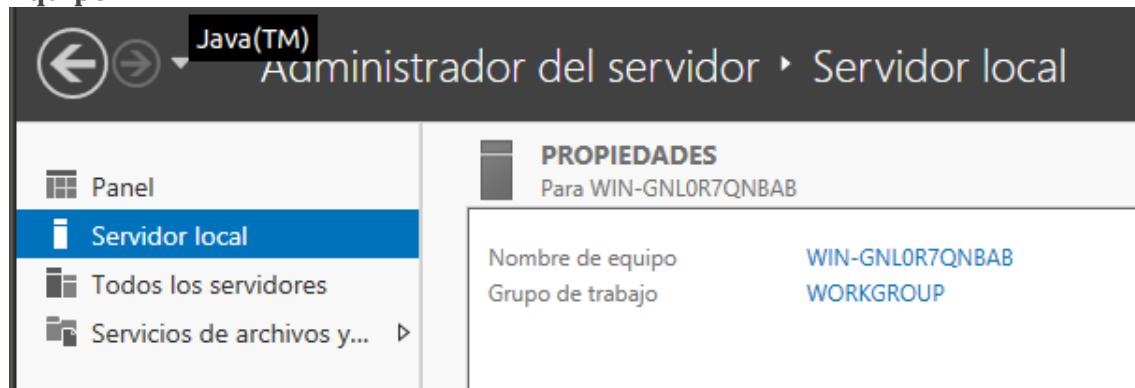


2. Seleccionar **Protocolo de Internet versión 4 (TCP/IPv4)** y poner la dirección del *Domain*

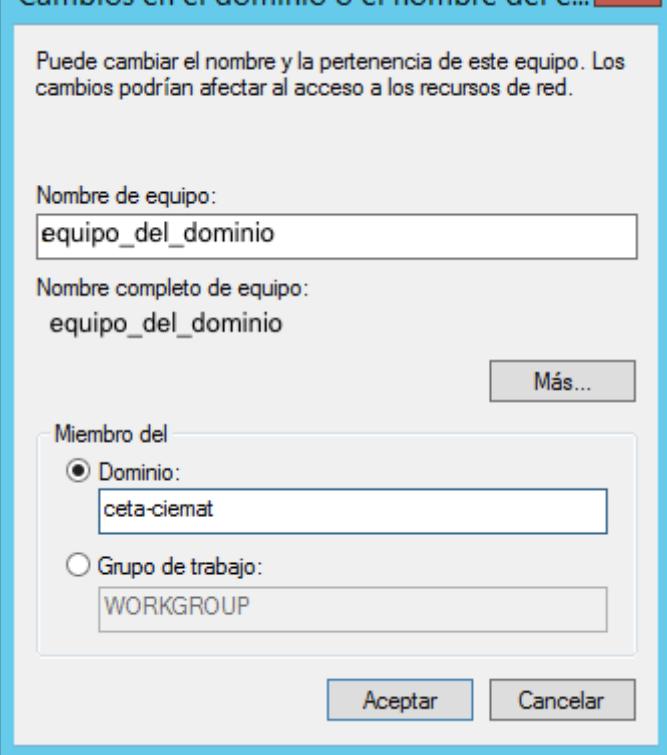
Controller.



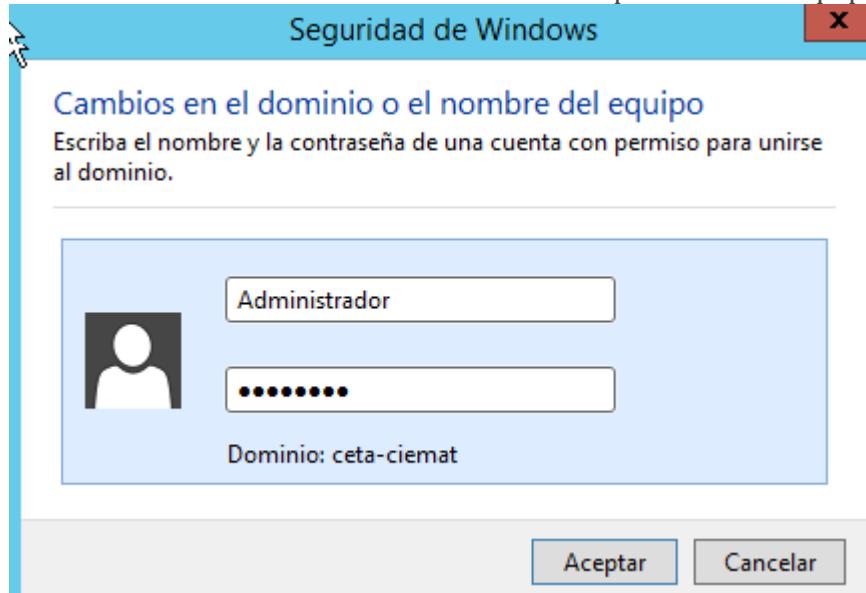
3. Dentro del **Administrador del servidor**, seleccionar *Servidor Local* y pulsar en **Nombre del Equipo**.



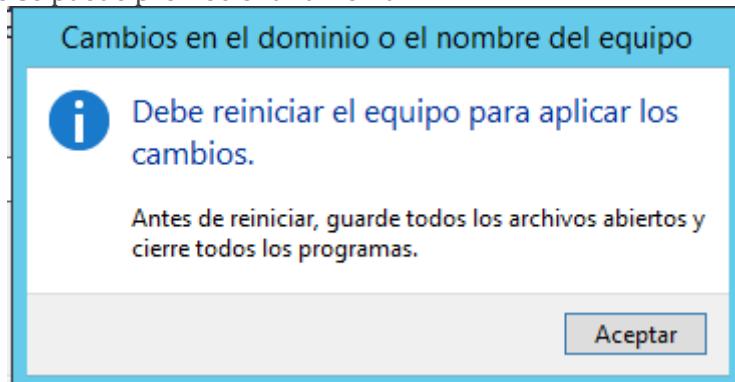
4. Pulsar en **Cambiar** e introducir el nombre del equipo y el dominio, en este caso, **ceta-ciemat**



5. Pulsar **Aceptar** e introducir la clave de *Administrador del Dominio* para añadir el equipo al Active Directory.



6. **Reiniciar** el equipo y quedará añadido al Dominio. Cualquier equipo que forma parte de un dominio se puede promocionar a Domain Controller.



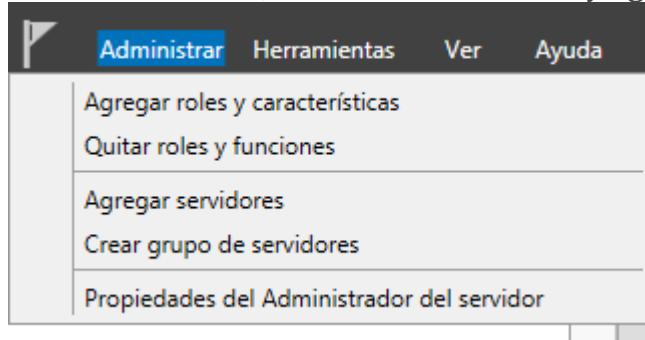
Servidor de Licencias KMS

Existen dos tipos de claves, **KMS** (*Key Management Service*) y **MAK** (*Multiple Activation Key*). Para crear un server de licencias *KMS* se debe alcanzar un **límite mínimo** de activaciones. El mínimo en Microsoft Windows Server 2012R2 es de cinco equipos licenciados y con windows 8.1 es de 25 equipos.

En nuestro caso creamos un server *KMS* para que veamos como se hace. Si no se espera alcanzar el mínimo de equipos licenciados se añade la licencia de tipo *MAK* y listo. Con las claves *KMS* el equipo que quiere licenciarse hace una solicitud al server DNS preguntando cual es su servidor *KMS* para licenciarse.

Las claves *MAK* se utilizan para la activación directa de cada server, cada una tiene un número predeterminado de activaciones permitidas que se basa en acuerdos de licencias por volumen. Al insertar la licencia *MAK* el equipo se conecta de manera independiente y es activado por *Microsoft*.

1. Dentro de *Administrador del servidor*, seleccionar *Administrar* y **Agregar roles y**

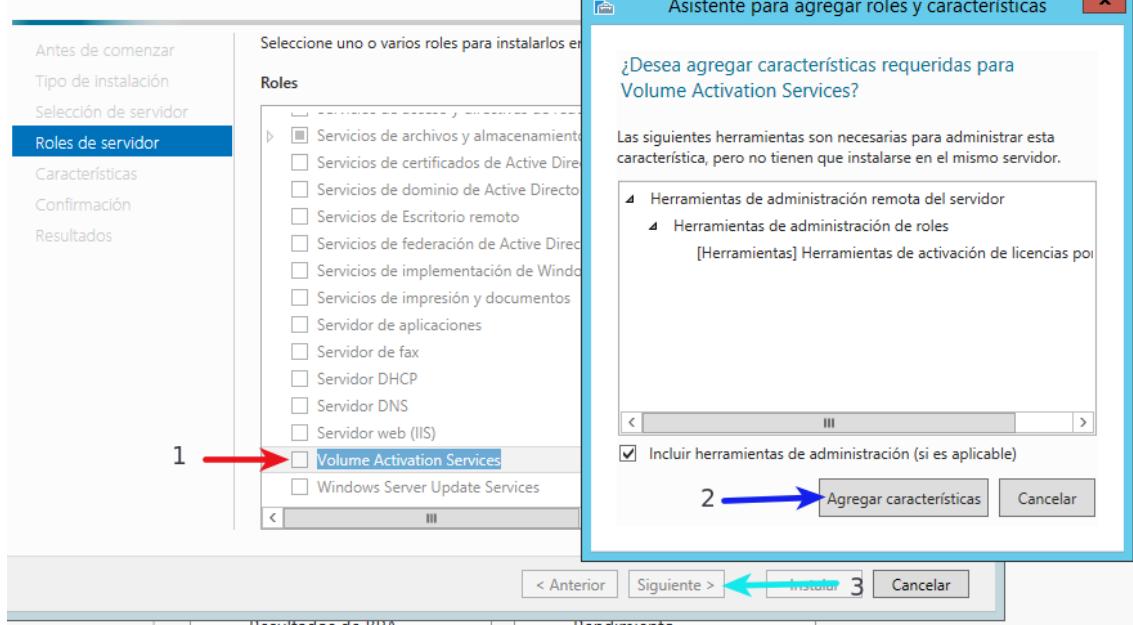


características.

- En la primera ventana pulsar **Siguiente >**. En la segunda seleccionar **Instalación basada en características o en roles** y pulsar **Siguiente >**. Seleccionar el servidor desde el que estamos realizando la instalación y pulsar **Siguiente >**. Seleccionar **Volume Activation Services** y **Agregar características** y

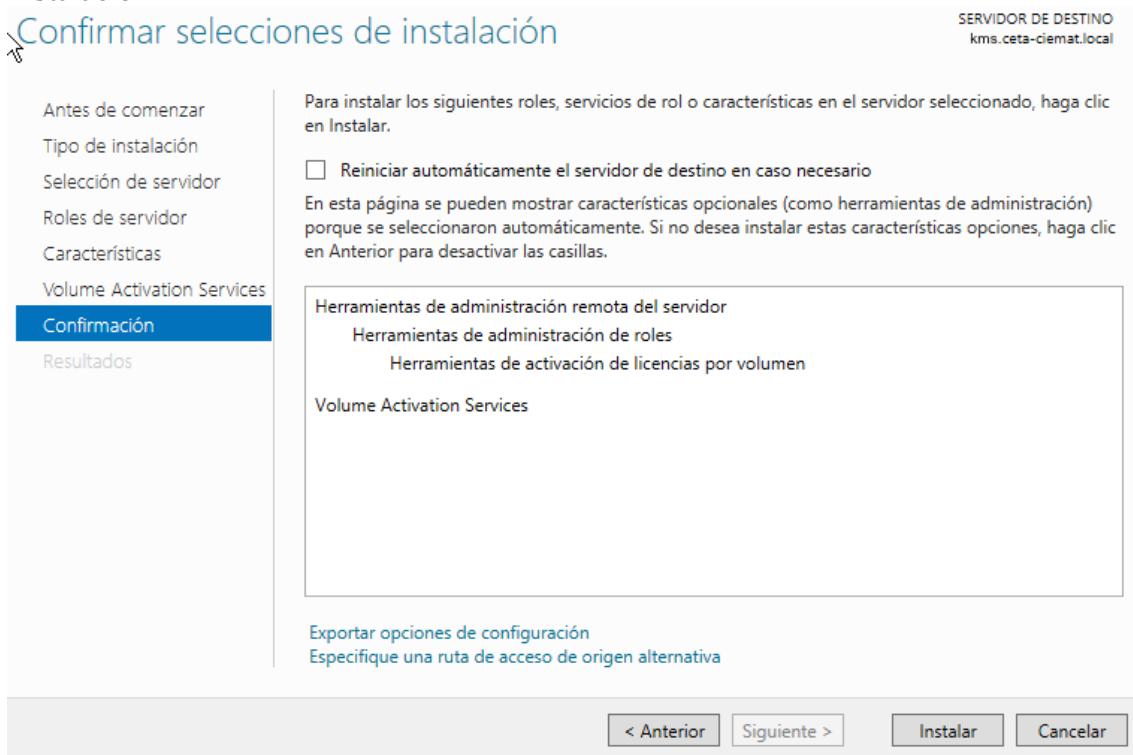
después **Siguiente >**.

Seleccionar roles de servidor

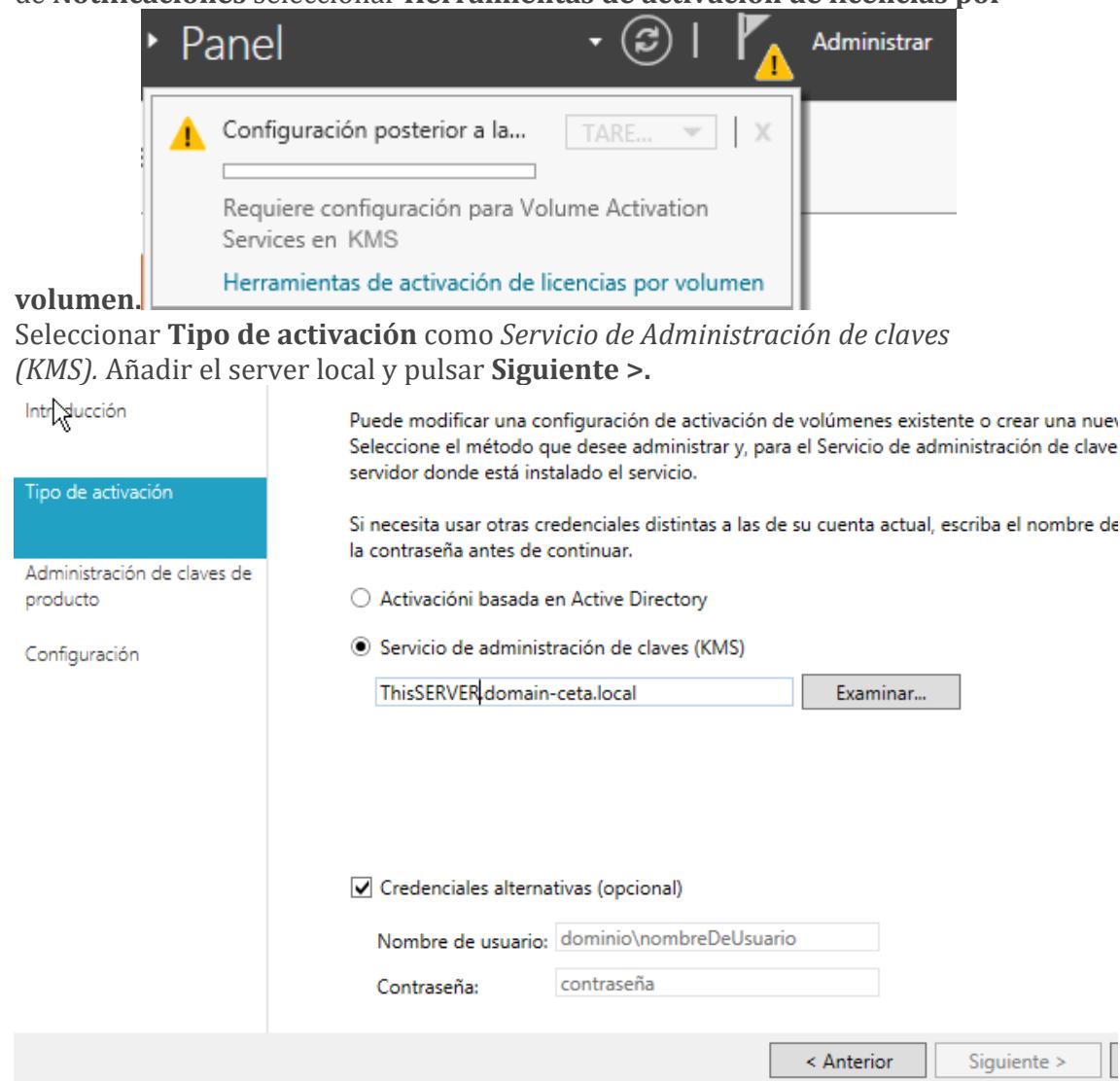


- Pulsar **Siguiente >** hasta la ventana de **Confirmación** y proceder con la instalación.

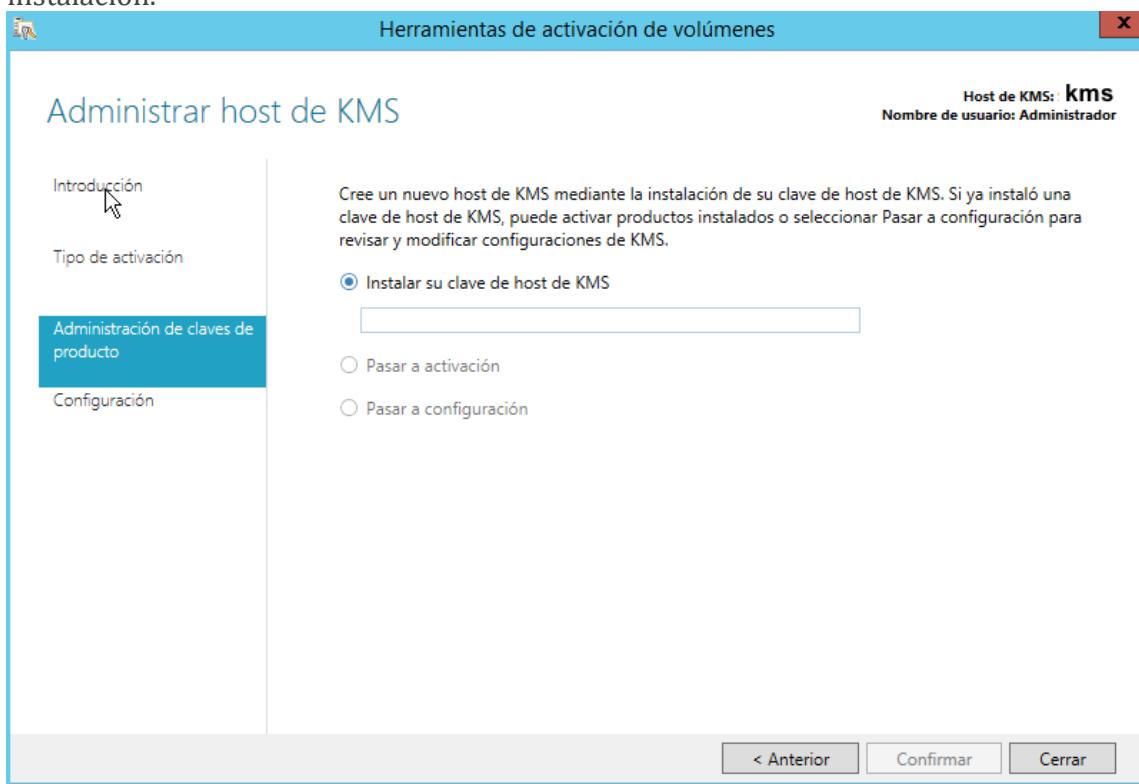
Confirmar selecciones de instalación



- Una vez terminada la instalación, cerrar el cuadro de diálogo y en la bandera de **Notificaciones** seleccionar **Herramientas de activación de licencias por volumen**.

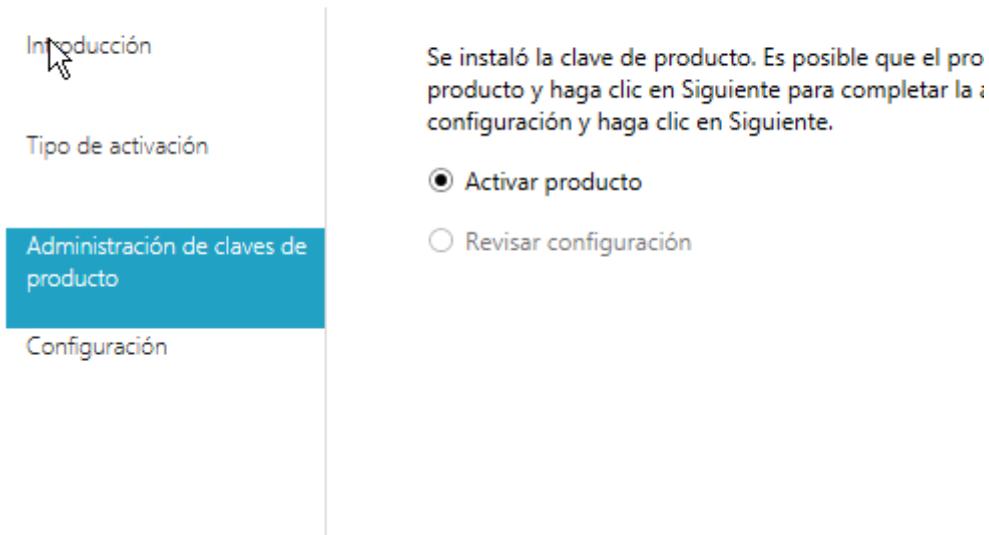


- Introducir la clave de host KMS y pulsar en confirmar para terminar la instalación.



- Pulsar en **Activar Producto** y **Siguiente >** para concluir la instalación.

La clave de producto se instaló correctamente



El rol está activado y el server KMS está en funcionamiento.

Servidor de Licencias de Escritorio Remoto

Los servicios de Escritorio Remoto (*Remote Desktop Services – RDS*) permiten a los usuarios conectarse a escritorios virtuales, escritorios basados en sesión y a programas tipo *RemoteApp*. Con *RDS* se puede administrar el servidor hasta con dos accesos simultáneos , además permite distintas implementaciones:



RDSH - Remote Desktop Session Host



RDWA - Remote Desktop Web Access



RDCB - Remote Desktop Connection Broker



RDGW - Remote Desktop Gateway



RDVH - Remote Desktop Virtualization Host



RDLI - Remote Desktop Licensing

Remote Desktop Session Host (RDSH)

Para este servicio los servidores son los que realmente alojan los procesos del usuario. Antiguamente conocido como “**Terminal Services**”, este término, se ha dejado de utilizar oficialmente. Cuando un usuario, se conecta a un equipo por Remote Desktop o ejecuta un programa en forma de *RemoteApp*, éstos se están ejecutando en el *Session Host*.

Remote Desktop Web Access (RDWA)

Este servicio brinda un sitio web con los recursos disponibles para usarlos a través de **RDS** y ofrece un feed RSS para ser consumido desde otras aplicaciones o dispositivos.

Remote Desktop Connection Broker (RDCB)

Este servicio asegura que todas las conexiones que los usuarios inicien contra los distintos **Session Hosts** se mantengan y también permite que el usuario tenga la experiencia de *inicio de sesión único* aunque acceda a aplicaciones en distintos hosts de sesión.

Remote Desktop Gateway (RDGW)

Es un Servicio Web que actúa como túnel de tráfico RDP sobre HTTPS para permitir a usuarios externos a nuestra infraestructura conectarse a un **RDS** interno de forma segura.

Remote Desktop Virtualization Host (RDVH)

Este servicio requiere un servidor físico con **Hyper-V** que lo alberge y se utiliza para implementar y administrar máquinas virtuales en una infraestructura virtual (**VDI**).

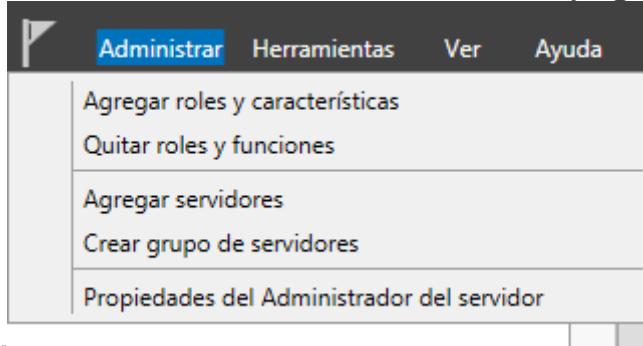
Remote Desktop Licensing (RDLI)

Este servicio concede las licencias necesarias de acceso al resto de los servidores **Session Host**. Para entornos en los que se conectan varios usuarios de manera concurrente, como **Citrix XenDesktop** ó **VMWare Horizon View**, es necesario que los usuarios adquieran licencias de este tipo.

Continuamos la instalación....



1. Abrir el *Administrador del Servidor*, seleccionar *Administrar* y **Agregar roles y**



características.

2. En la primera ventana pulsar **Siguiente >** y después seleccionar **Instalación basada en características o en roles** y pulsar *Siguiente >*. Seleccionar el server desde el que hacemos la instalación y *Siguiente >* otra vez. Marcar la opción **Servicios de Escritorio Remoto** y seleccionar **Administración de Licencias de Escritorio Remoto**.



Asistente para agregar roles y características

Seleccionar roles de servidor

Antes de comenzar

Tipo de instalación

Selección de servidor

Roles de servidor

Características

Confirmación

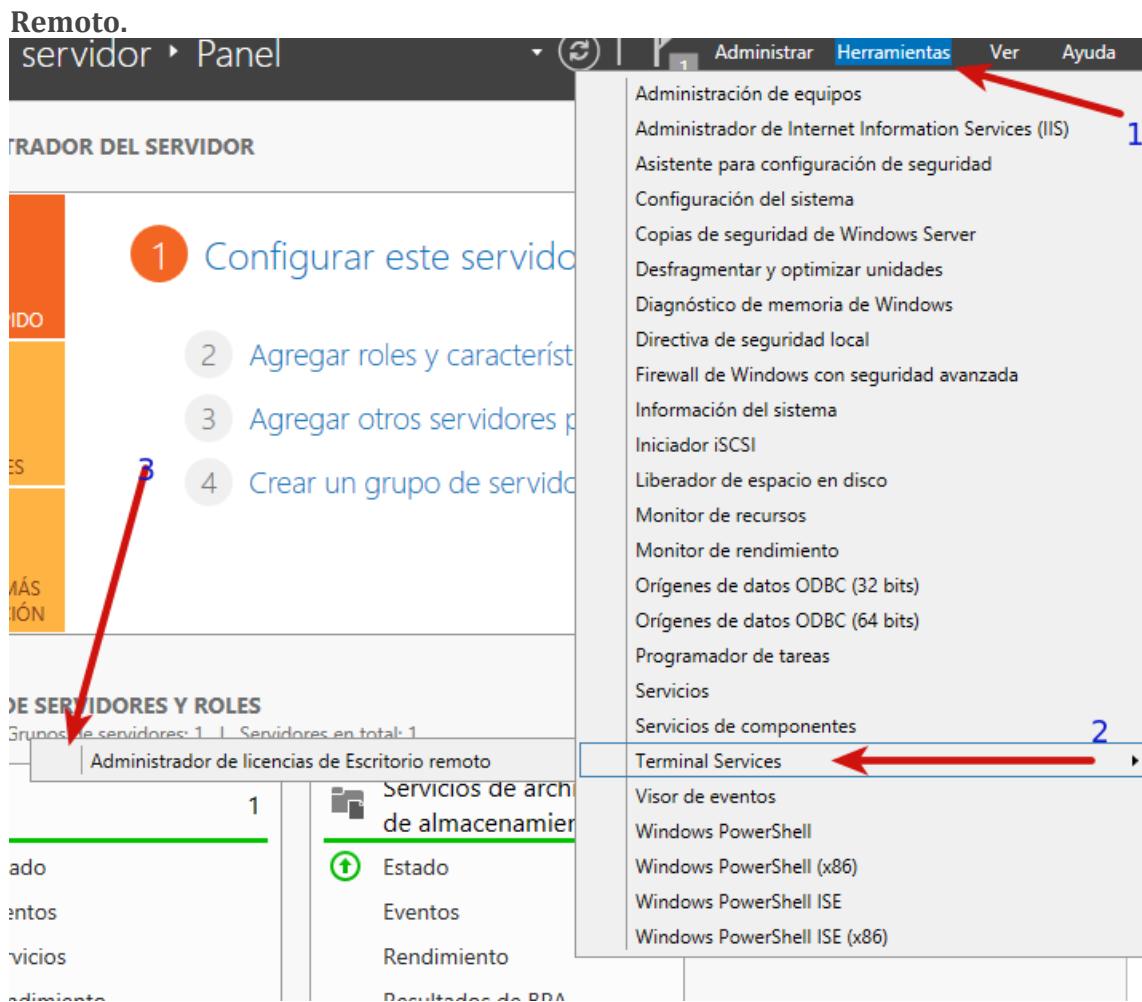
Resultados

Seleccione uno o varios roles para instalarlos en el servidor seleccionado.

Roles

- └ **ACTIVE DIRECTORY RIGHTS MANAGEMENT SERVICES**
 - Experiencia con Windows Server Essentials
 - Hyper-V
 - Servicios de acceso y directivas de redes
 - └ **Servicios de archivos y almacenamiento (1 de 12 instalados)**
 - Servicios de certificados de Active Directory
 - Servicios de dominio de Active Directory
 - └ **Servicios de Escritorio remoto (1 de 6 instalados)**
 - Acceso web a Escritorio remoto
 - Administración de licencias de Escritorio remoto**
 - Agente de conexión a Escritorio remoto
 - Host de sesión de Escritorio remoto (Instalado)

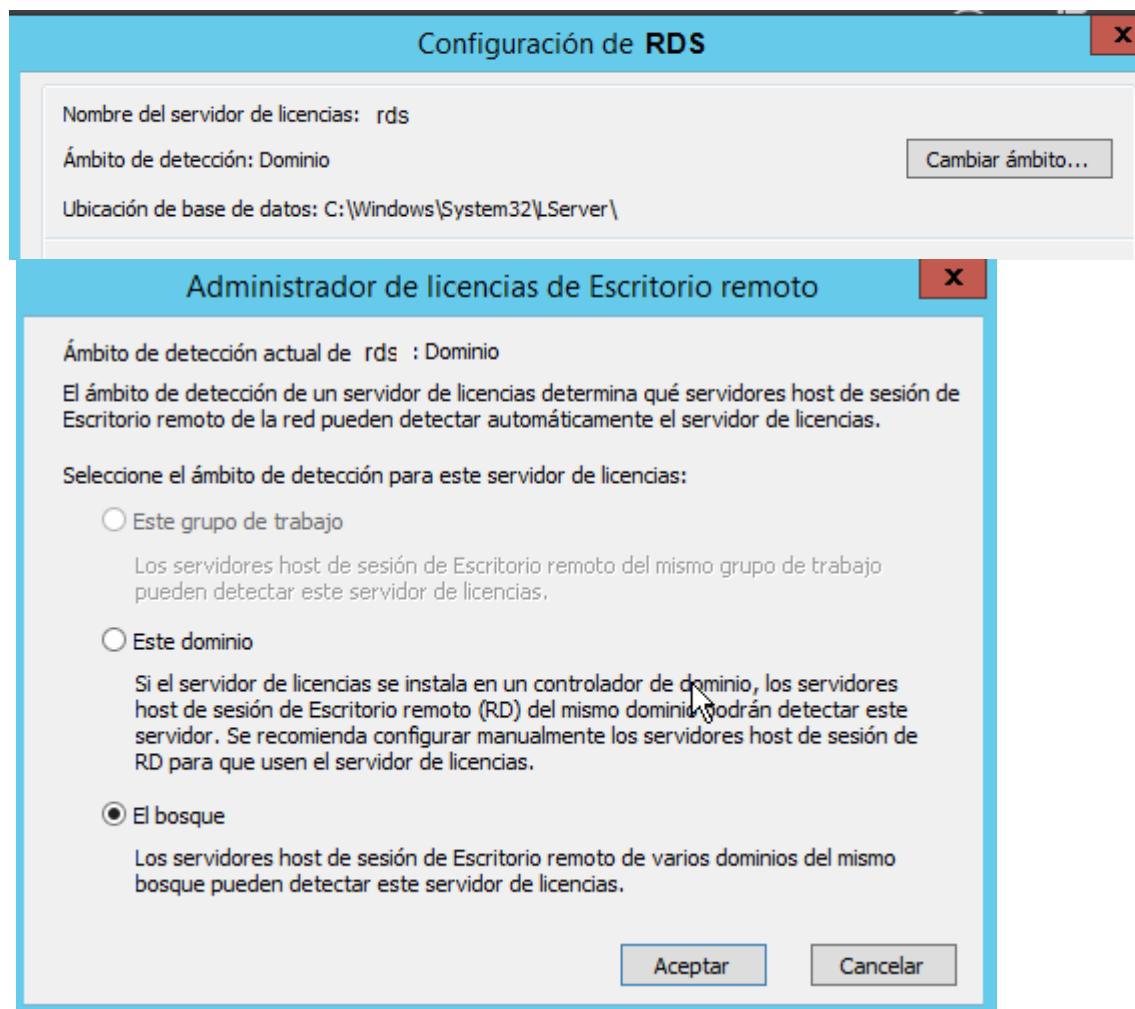
3. Pulsar **Siguiente >** y confirmar la instalación. Una vez instalado el rol hay que instalar las licencias. Para ello hay que abrir el *Administrador del Servidor* y pulsar en el menú **Herramientas -> Terminal Services y Administrador de Licencias de Escritorio**



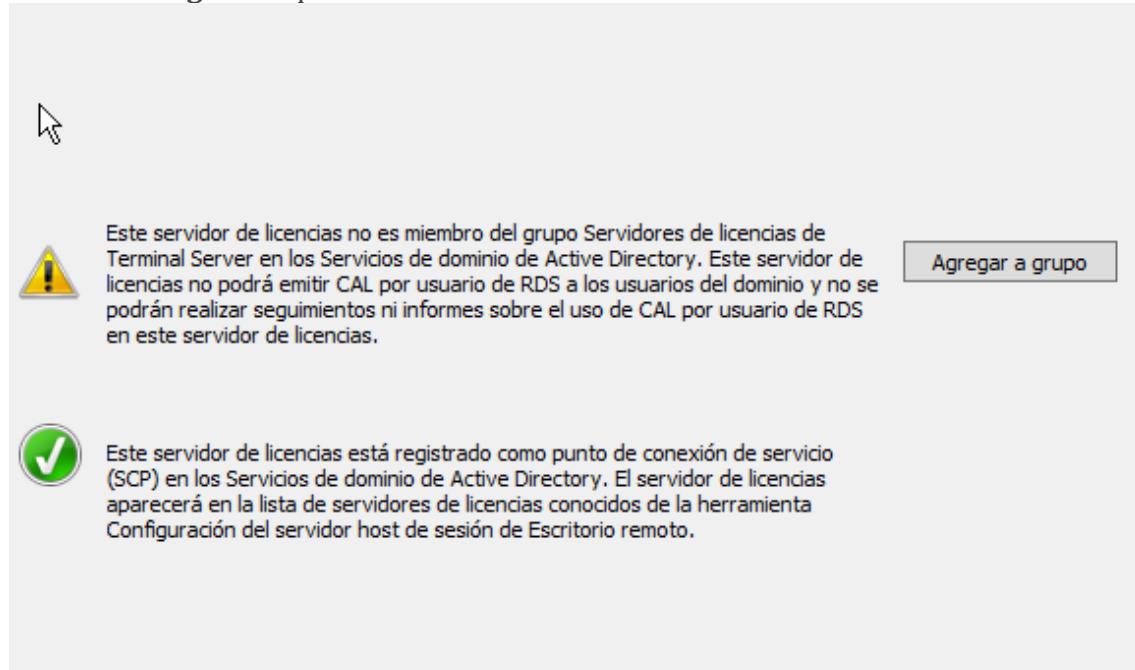
4. Seleccionamos el server, en nuestro caso **RDS** y pulsamos en **Revisar**.

Administrador de licencias de Escritorio remoto				
Acción	Ver	Ayuda		
Todos los servidores	RDS			
			Nombre	Estado de activación

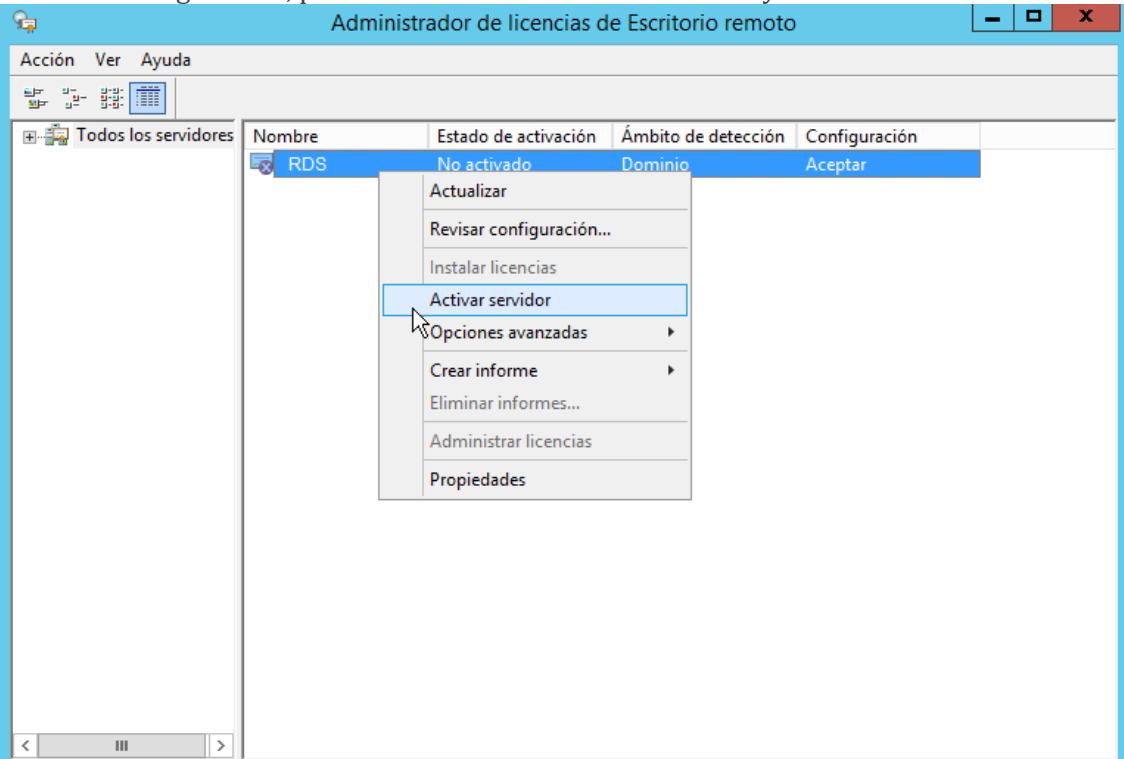
5. Se debe seleccionar el **ámbito** sobre el que actuará el server de licencias. En nuestro caso seleccionaremos el **Bosque** completo.



6. En la ventana de *configuración* comprobar el estado del servidor. Si alguno está marcado como **warning** habrá que activarlo.

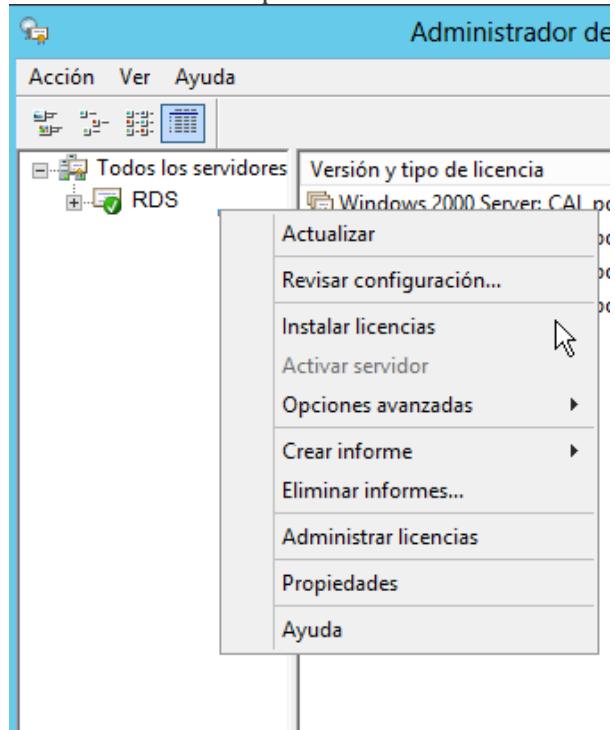


7. Verificar configuración, pulsar botón derecho sobre servidor y **Activar servidor**.



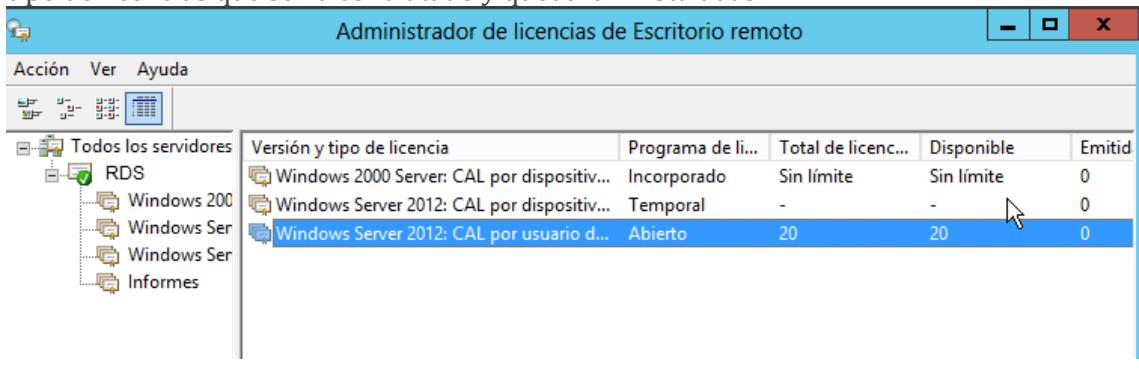
Hay que seguir los pasos de instalación con los datos de licencia proporcionados por *Microsoft* y el server quedará activado.

Ahora procedemos a instalar las licencias: Para ello pulsar con el botón derecho



sobre el server y **Instalar Licencias**.

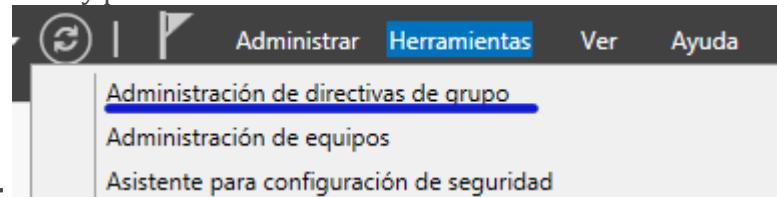
- Se iniciará el asistente de instalación de licencias. Seleccionar los datos que vengan en el tipo de licencias que se ha contratado y quedarán instaladas.



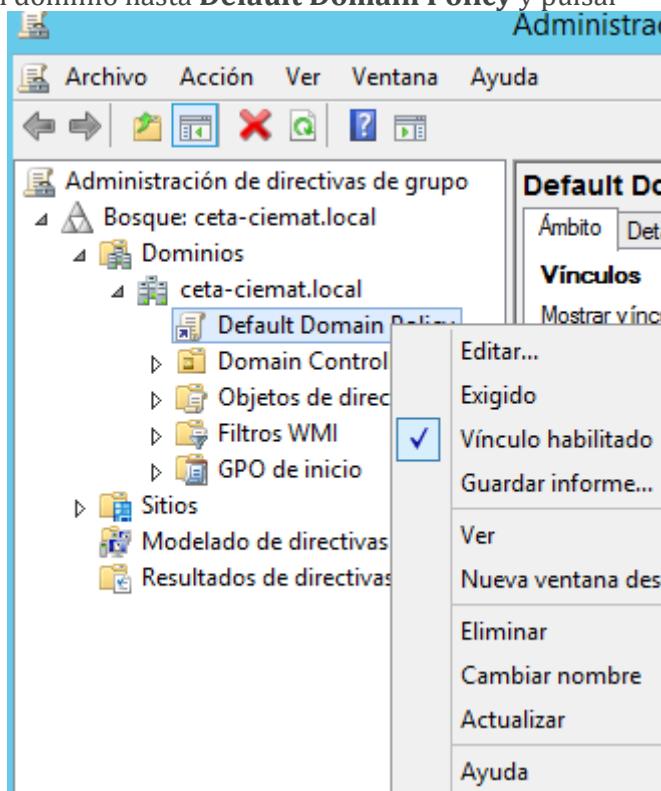
Establecer tipo de licencia de Escritorio Remoto

La configuración del tipo de licencia se cambiará en el *Domain Controller* y después la toman como GPO ([ver artículo sobre GPOs](#)) los equipos del dominio. Para establecer el tipo de licencia:

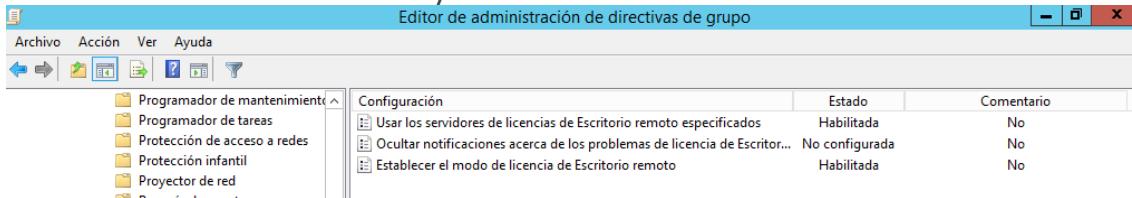
- Ir a *Administrador del servidor* y pulsar en el menú **Herramientas -> Administración**



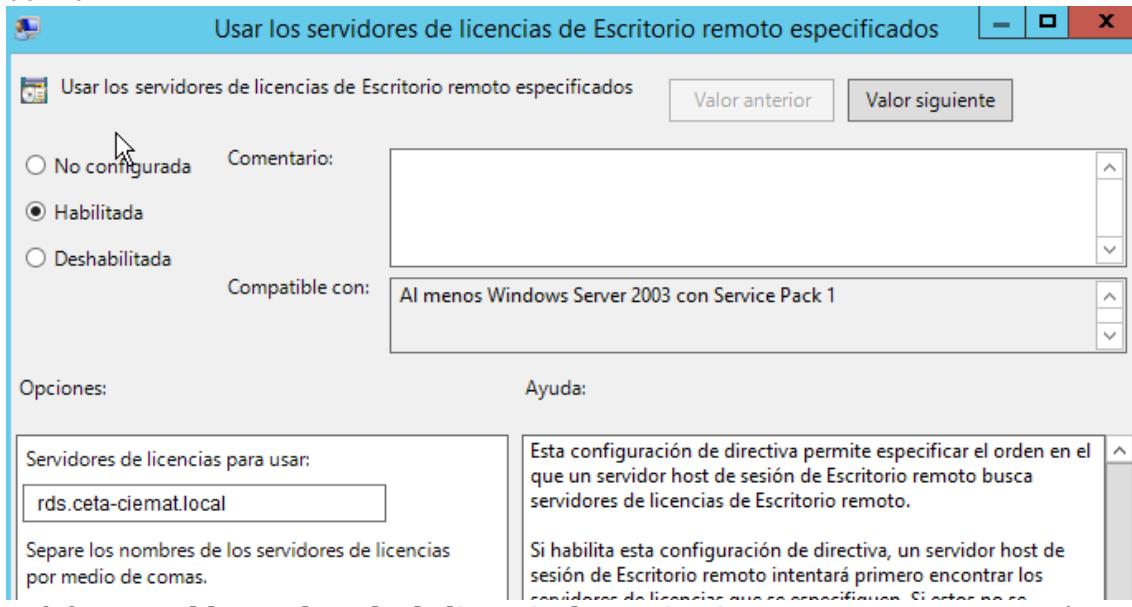
- Navegar en el dominio hasta **Default Domain Policy** y pulsar **Editar...** sobre **Editar**.



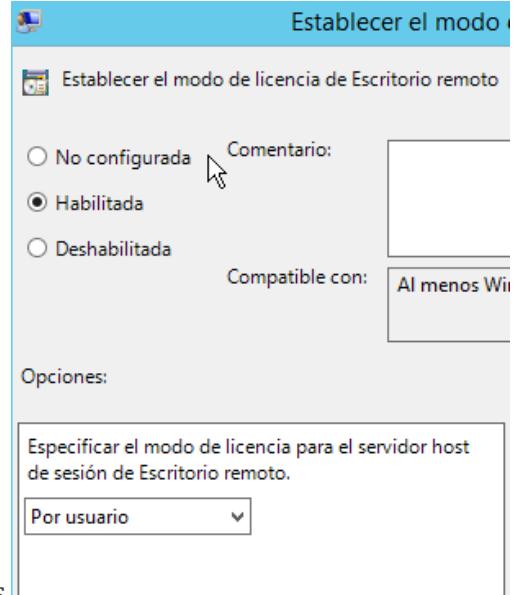
3. Navegar hasta **Configuración del equipo/directivas/plantillas administrativas/componentes de windows/servicios de escritorio remoto/host de sesión de escritorio remoto/licencias**:



- Establecer dentro de **Usar los servidores de licencias de Escritorio remoto especificados** el server de licencias de escritorio remoto que debemos utilizar.



- Habilitar **Establecer el modo de licencia de Escritorio remoto** en *Por Usuario* ó *Por*



Equipo, según la licencia que tengamos.

Con esto quedaría configurado el tipo de licencias. Es recomendable siempre en estos cambios lanzar desde el PowerShell: **gpupdate /force**

Configurar Equipo del dominio contra Server de Licencias RDS

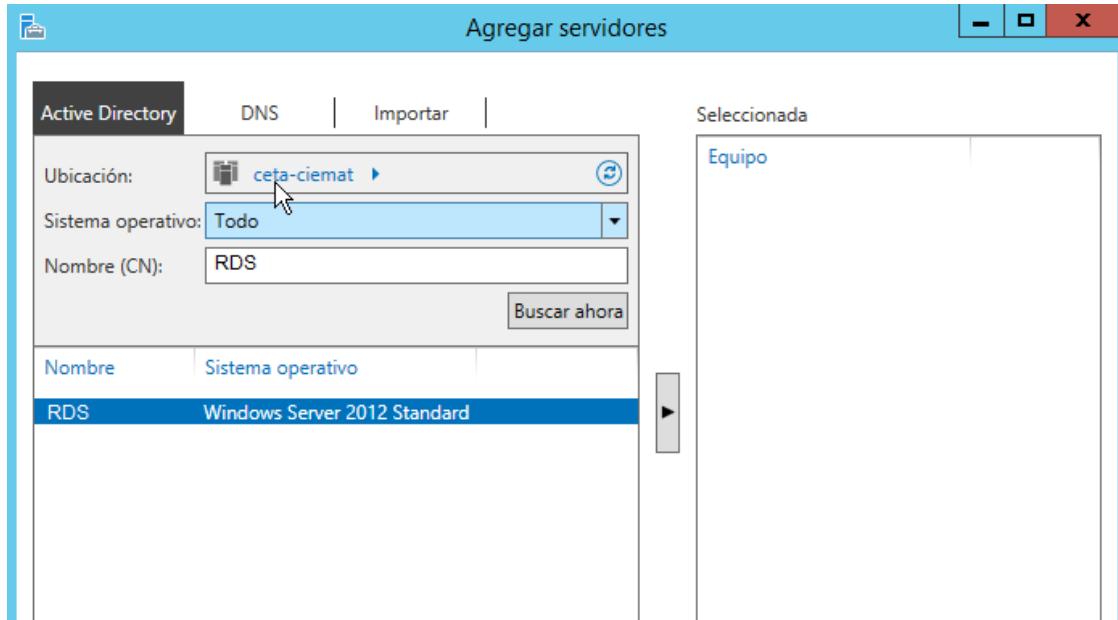
El equipo del dominio establecerá su server de licencias, para ello hay que seguir dos pasos.

1. INSTALAR SERVER DE LICENCIAS

- Vamos a *Administrador del Servidor* y **Agregar otros servidores para administrar**



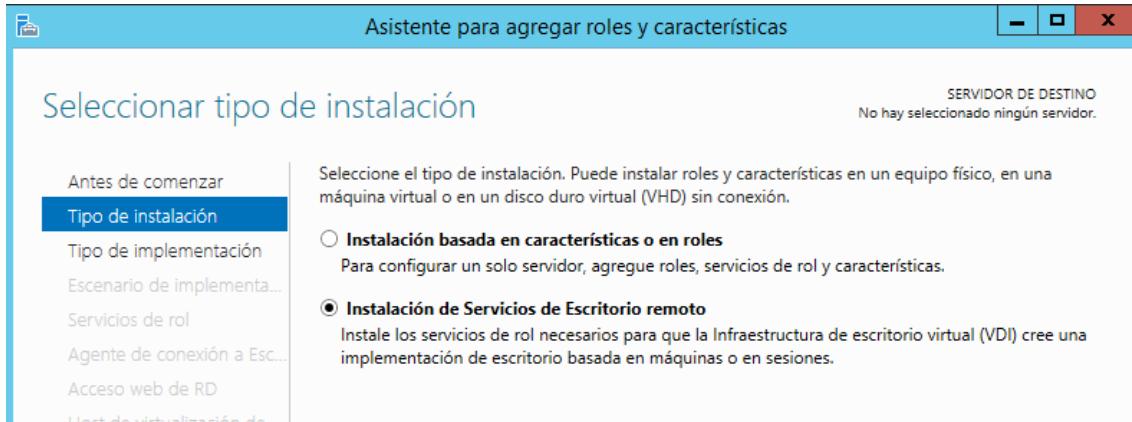
- Buscar dentro del *Active Directory* el server **RDS** y añadirlo.



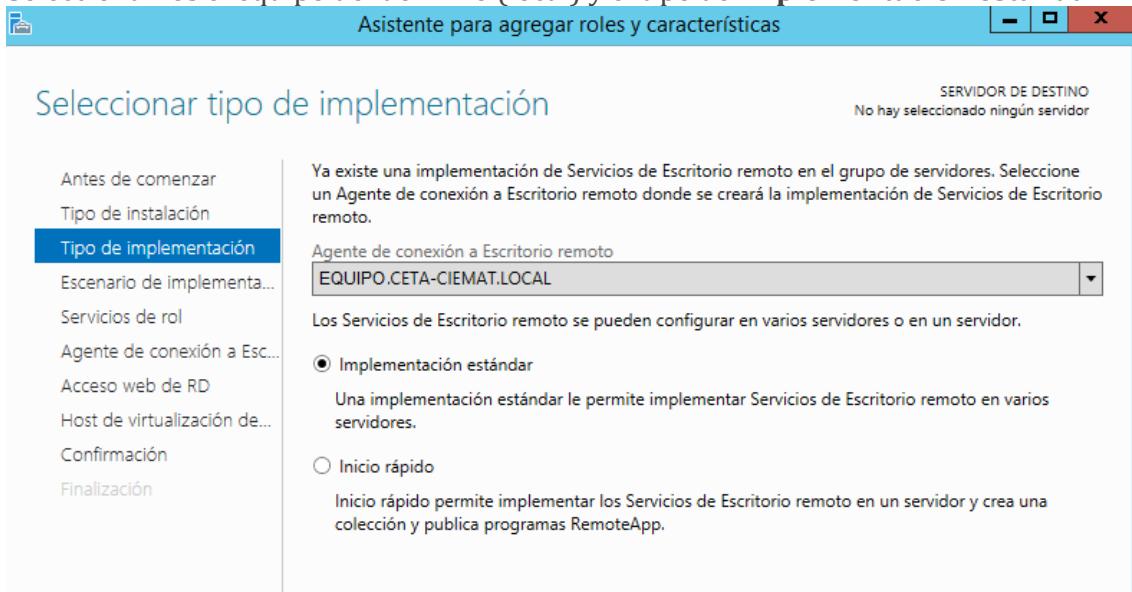
2. AUTENTICAR EQUIPO DEL DOMINIO

- Vamos a *Administrador del servidor*, y seleccionar **Agregar roles y características**. Esta vez seleccionamos la segunda opción, **Instalación de Servicios de Escritorio**

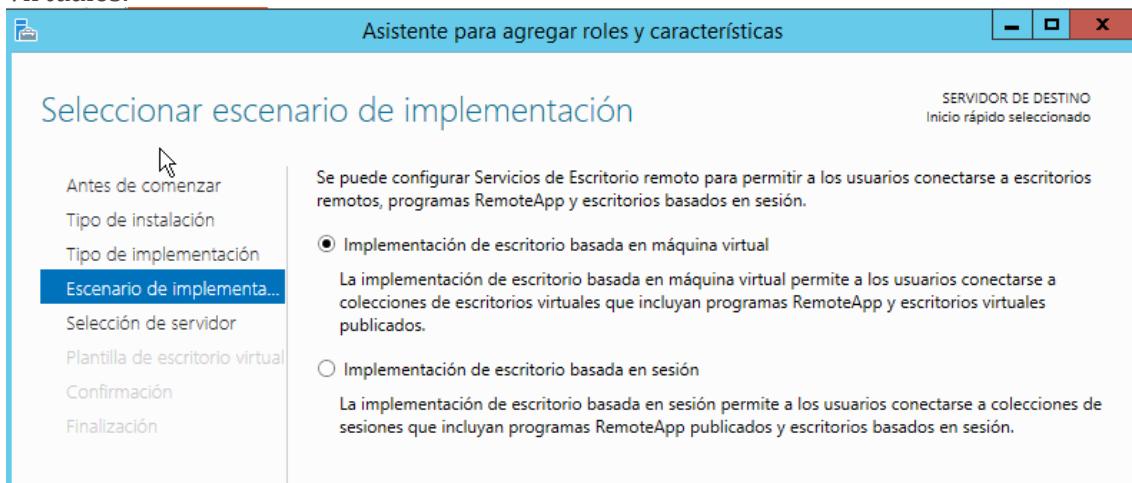
Remoto.



- Seleccionamos el equipo del dominio (local) y el tipo de **Implementación estándar**.

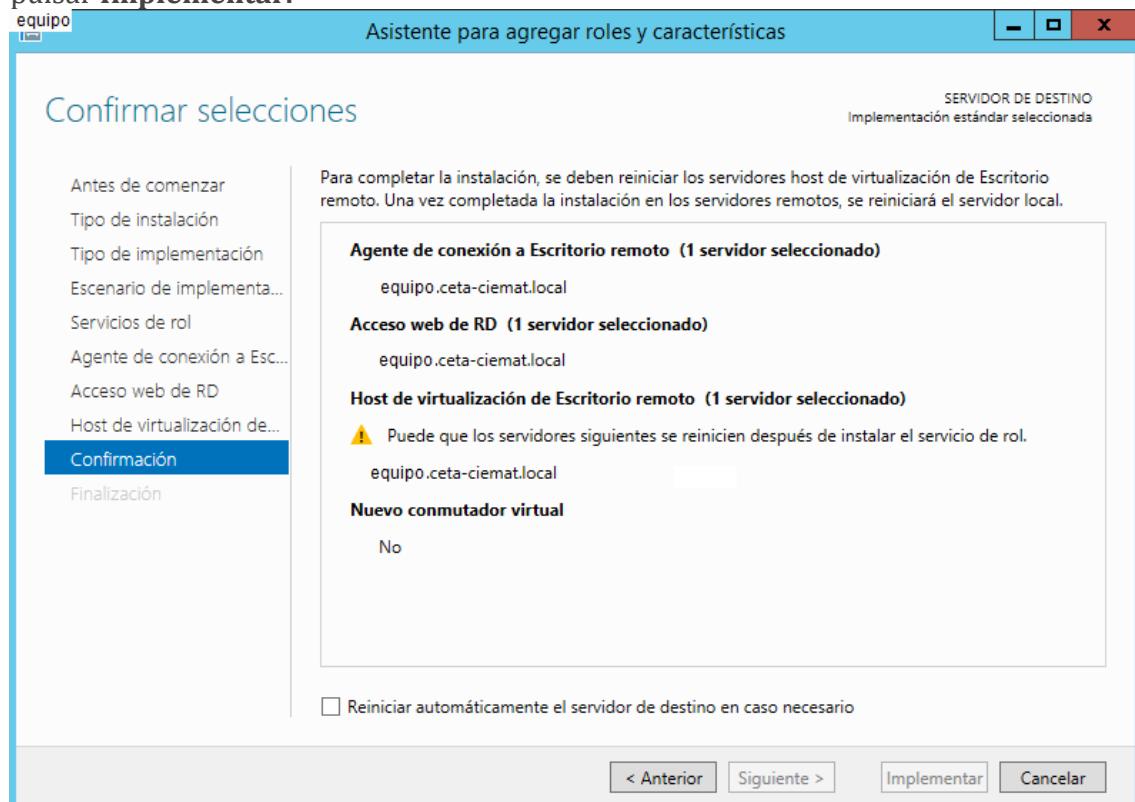


- Marcar *Implementación de escritorio basada en máquina virtual* para que los usuarios se conecten a la plataforma y así poder usar escritorios virtuales.



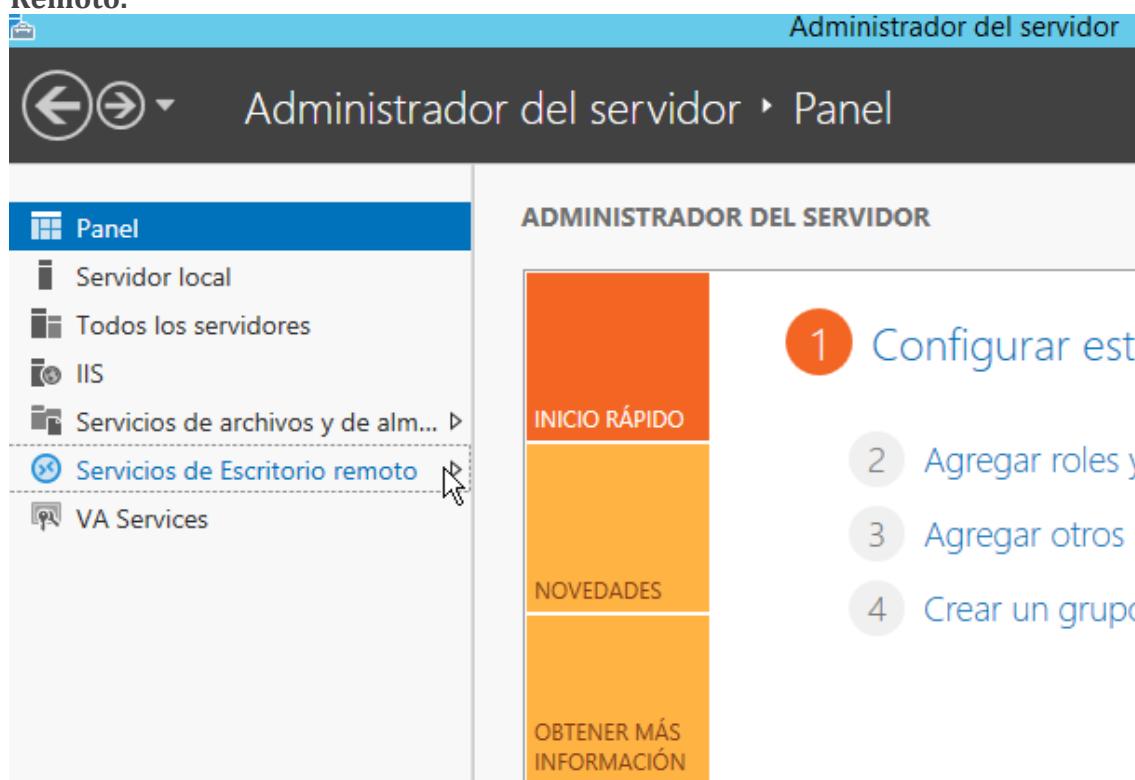
- Seguir hasta *Agente de conexión* y seleccionar en todos los casos la máquina local. Confirmar los servicios de rol y

pulsar **Implementar**.

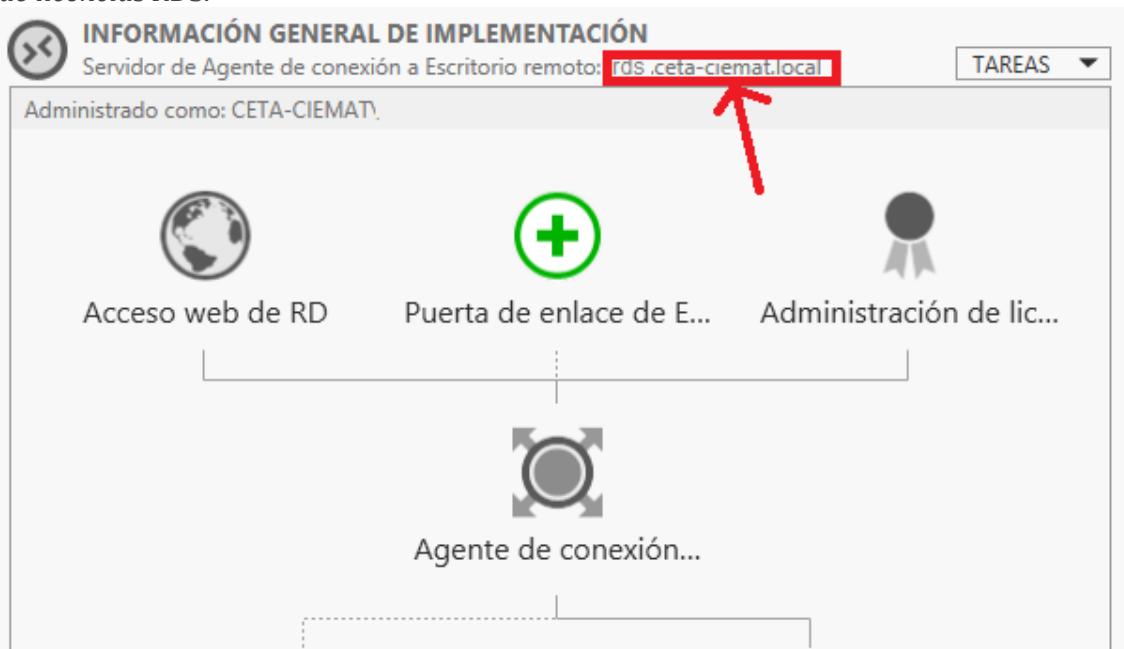


Con esto queda instalado el server **RDS**. Pasamos a realizar un diagnóstico para comprobar que todo está correctamente instalado.

1. Ir a *Administrador del servidor* y en el panel izquierdo pulsar sobre **Servicios de Escritorio Remoto**.



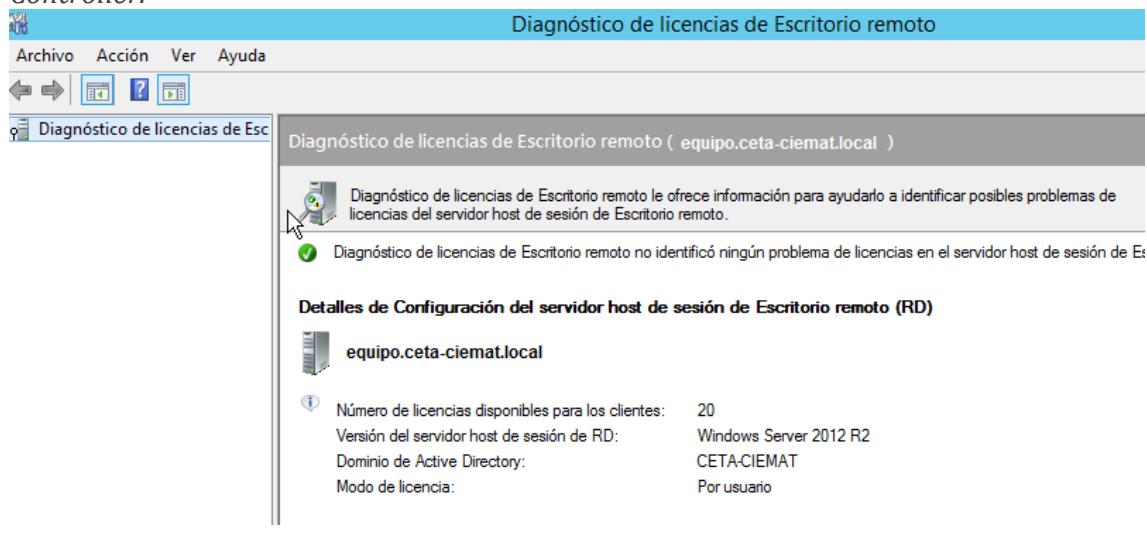
2. Comprobar que la administración de licencias esta **OK**, en caso contrario *agregar servidor de licencias RDS*.



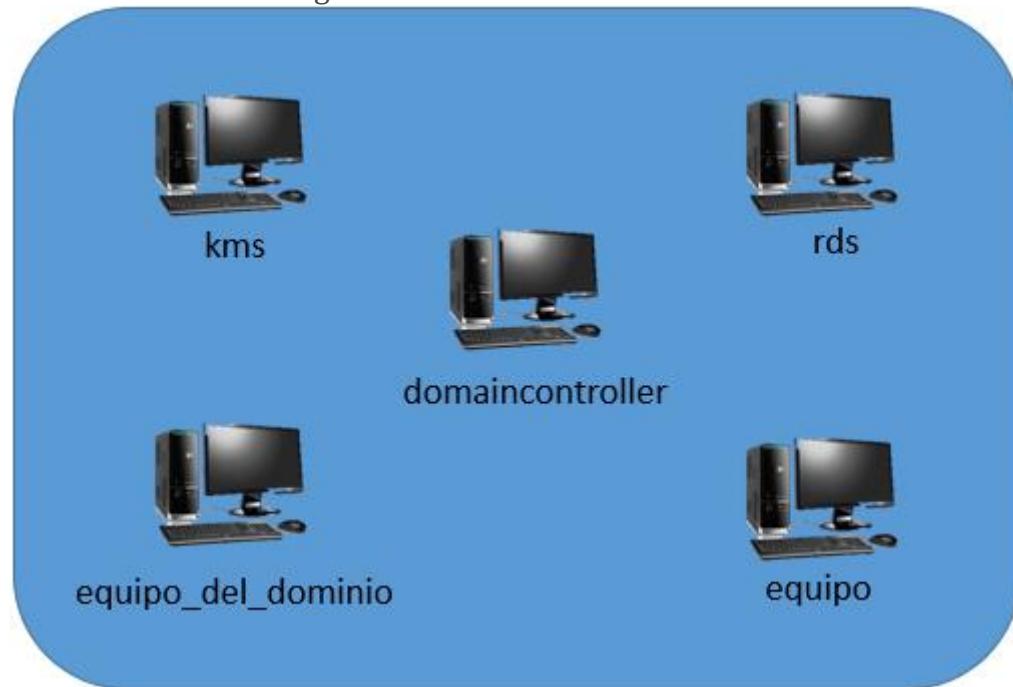
3. Ir a **Servidores** y pulsar con el botón derecho sobre el equipo local. Pulsar **Diagnóstico de licencias de Escritorio Remoto**.

The screenshot shows the 'SERVIDORES' (Servers) screen in the Windows Server Management Console. The left sidebar has tabs for 'Información general', 'Servidores' (which is selected and highlighted in blue), 'Colecciones', and 'QuickSessionCollection'. The main area is titled 'SERVIDORES' and shows 'Todos los servidores | 2 en total'. A table lists two servers: 'RDS' and 'CETA-CIEMAT'. The 'RDS' row has a context menu open, listing options like 'Agregar roles y características', 'Cerrar servidor local', 'Administración de equipos', 'Conexión a Escritorio remoto', 'Windows PowerShell', 'Configurar formación de equipos de NIC', 'Configurar comentarios automáticos de Windows', 'Diagnóstico de licencias de Escritorio remoto' (which is highlighted with a green box), 'Administrar como...', 'Iniciar contadores de rendimiento', 'Actualizar', and 'Copiar'. The 'EVENTOS' section below shows 'Todos los eventos | 3' and a 'Filtro' button.

4. Debe estar **Activo** y con el tipo de licencias que se especificó en el *Domain Controller*.



Hemos instalado los siguientes elementos:



Capítulo 8: Usuarios, grupos y equipos en Windows Server

Publicado por [P. Ruiz](#) en 26 agosto, 2014

 [Volver al índice](#)

8.1. Conceptos básicos



Uno de los elementos fundamentales en la administración de una red, es el control de los usuarios, grupos y equipos. Por ello, debemos aprender cómo crearlos, modificarlos, organizarlos y, si llega el caso, eliminarlos. Además, deberemos asignar privilegios para cada uno de ellos, de modo que podamos establecer en qué medida y bajo qué condiciones podrán beneficiarse de los recursos de la red. Este objetivo lo cubriremos, en parte durante el presente capítulo, pero seguiremos completándolo en el siguiente.

Cuenta de usuario

Como ya comentábamos en el capítulo anterior, una de las primeras ideas que deben quedar claras cuando hablamos de cuentas de usuario es que no siempre representan a personas concretas, sino que también pueden ser utilizadas como mecanismos de acceso para determinados servicios o aplicaciones de la máquina local o, incluso, de un equipo remoto.

Las cuentas de usuario también suelen identificarse como **entidades de seguridad**.

En definitiva, una cuenta de usuario es un objeto que posibilita el acceso a los recursos del dominio de dos modos diferentes:

- Permite **autenticar la identidad** de un usuario, porque sólo podrán iniciar una sesión aquellos usuarios que dispongan de una cuenta en el sistema asociada a una determinada contraseña.

- Permite **autorizar, o denegar**, el acceso a los recursos del dominio, porque, una vez que el usuario haya iniciado su sesión sólo tendrá acceso a los recursos para los que haya recibido los permisos correspondientes.

Cada cuenta de usuario dispone de un identificador de seguridad (*SID, Security Identifier*) que es único en el dominio.

Por razones de seguridad, debes evitar que varios usuarios utilicen la misma cuenta para iniciar sesión en el dominio.

Cuentas integradas

Cuando se crea el dominio, se crean también dos nuevas cuentas: *Administrador* e *Invitado*. Posteriormente, cuando es necesario, se crea también la cuenta *Asistente de ayuda*. Estas son las denominadas *cuentas integradas* y disponen de una serie de derechos y permisos predefinidos:

- **Administrador:** Tiene control total sobre el dominio y no se podrá eliminar ni retirar del grupo *Administradores* (aunque sí podemos cambiarle el nombre o deshabilitarla).
- **Invitado:** Está deshabilitada de forma predeterminada y, aunque no se recomienda, puede habilitarse, por ejemplo, para permitir el acceso a los usuarios que aún no tienen cuenta en el sistema o que la tienen deshabilitada. De forma predeterminada no requiere contraseña, aunque esta característica, como cualquier otra, puede ser modificada por el administrador.
- **Asistente de ayuda:** se utiliza para iniciar sesiones de *Asistencia remota* y tiene acceso limitado al equipo. Se crea automáticamente cuando se solicita una sesión de asistencia remota y se elimina cuando dejan de existir solicitudes de asistencia pendientes de satisfacer.

Por último, debemos tener en cuenta que, aunque la cuenta *Administrador* esté deshabilitada, podrá seguir usándose para acceder al controlador de dominio en *modo seguro*.

Desde el punto de vista de la seguridad, puede ser interesante cambiar el nombre de la cuenta *Administrador*.

Cuenta de equipo

Como ocurría con las cuentas de usuario, una cuenta de equipo sirve para autenticar a los diferentes equipos que se conectan al dominio,

permitiendo o denegando su acceso a los diferentes recursos del dominio.

Del mismo modo que con las cuentas de usuario, las cuentas de equipo deben ser únicas en el dominio. Aunque una cuenta de equipo se puede crear de forma manual (como veremos más adelante), también se puede crear en el momento en el que el equipo se une al dominio.

Los sistemas de escritorio Windows que sean anteriores a XP no pueden disponer de cuentas de equipo. El motivo es que estos sistemas carecen de características de seguridad avanzadas.

Cuenta de grupo

Un grupo es un conjunto de objetos del dominio que pueden administrarse como un todo. Puede estar formado por cuentas de usuario, cuentas de equipo, contactos y otros grupos.

Cuando una cuenta de usuario o de equipo está incluida en un grupo se dice que es *miembro del grupo*.

Podemos utilizar los grupos para facilitar algunas tareas, como:

- *Simplificar la administración*: Podemos asignar permisos al grupo y éstos afectarán a todos sus miembros.
- *Delegar la administración*: Podemos utilizar la directiva de grupo para asignar derechos de usuario una sola vez y, más tarde, agregar los usuarios a los que queramos delegar esos derechos.
- *Crear listas de distribución de correo electrónico*: Sólo se utilizan con los grupos de distribución que comentaremos más abajo.

El *Directorio Activo* proporciona un conjunto de grupos predefinidos que pueden utilizarse tanto para facilitar el control de acceso a los recursos como para delegar determinados roles administrativos. Por ejemplo, el grupo *Operadores de copia de seguridad* permite a sus miembros realizar copias de seguridad de todos los controladores de dominio, en el dominio al que pertenecen.

Ámbito de los grupos

El ámbito de un grupo establece su alcance, es decir, en qué partes de la red puede utilizarse, y el tipo de cuentas que pueden formar parte de él. En ese sentido, pueden pertenecer a una de las siguientes categorías:

- **Ámbito local:** Entre sus miembros pueden encontrarse uno o varios de los siguientes tipos de objetos:

- Cuentas de usuario o equipo.
- Otros grupos de ámbito local.
- Grupos de ámbito global.
- Grupos de ámbito universal.

Las cuentas o grupos contenidos tendrán necesidades de acceso similares dentro del propio dominio. Por ejemplo, los que necesiten acceder a una determinada impresora.

- **Ámbito global:** Sólo pueden incluir otros grupos y cuentas que pertenezcan al dominio en el que esté definido el propio grupo. Los miembros de este tipo de grupos pueden tener permisos sobre los recursos de cualquier dominio dentro del bosque. Sin embargo, estos grupos no se replican fuera de su propio dominio, de modo que, la asignación de derechos y permisos que alberguen, no serán válidas en otros dominios del bosque.

Los grupos de ámbito global son perfectos para contener objetos que se modifique con frecuencia, debido a que, como no se replican fuera del dominio, no generan tráfico en la red para la actualización del catálogo global.

- **Ámbito universal:** Entre sus miembros pueden encontrarse cuentas o grupos de cualquier dominio del bosque, a los que se les pueden asignar permisos sobre los recursos de cualquier dominio del bosque.

Tipos de grupos

Existen dos tipos de grupos en *Active Directory*:

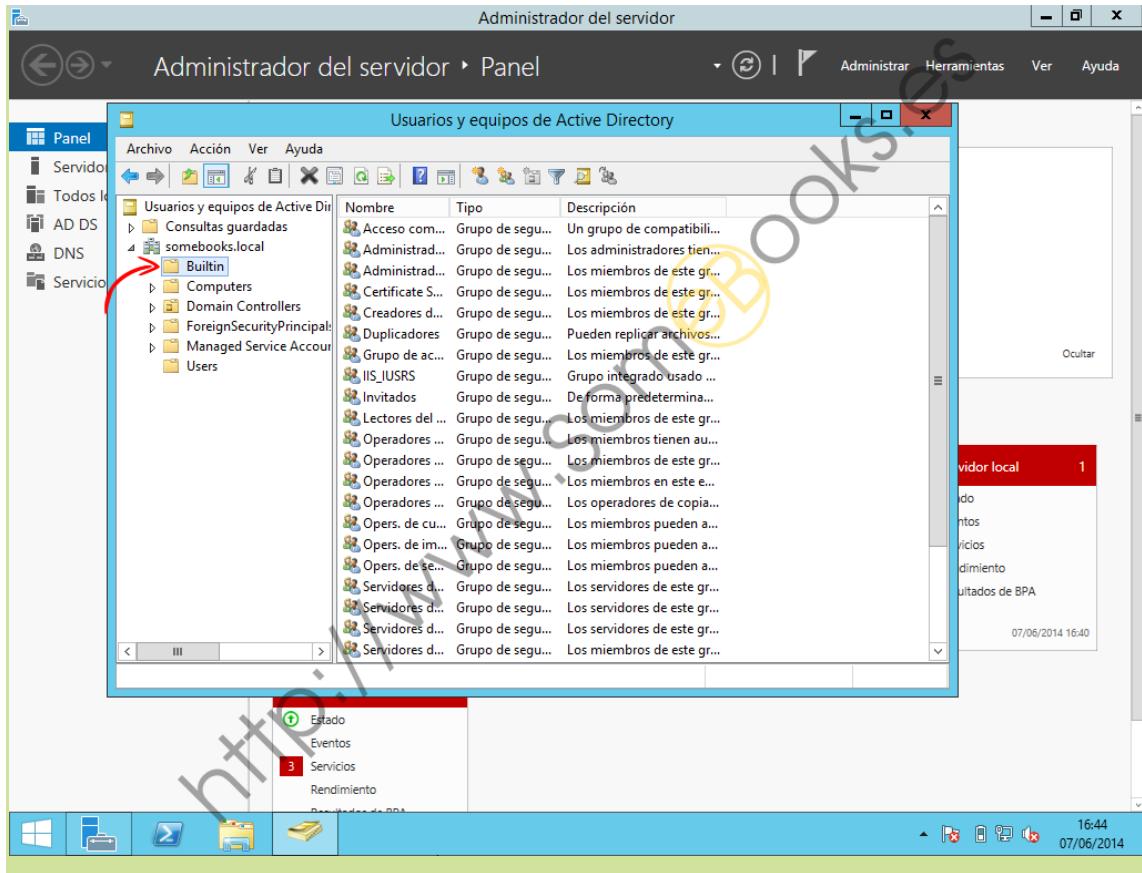
- **Grupos de distribución:** Se utilizan en combinación con programas como *Microsoft Exchange Server*, para crear listas de distribución de correo electrónico. Estos grupos no disponen de características de seguridad, por lo que no pueden aparecer en las listas de control de acceso discrecional (*DACL, Discretionary Access Control Lists*).
- **Grupos de seguridad:** Permiten asignar permisos a las cuentas de usuario, de equipo y grupos sobre los recursos compartidos. Con los grupos de seguridad podemos:

- *Asignar derechos de usuario* a los grupos de seguridad del Directorio Activo. De esta forma, podemos establecer qué acciones pueden llevar a cabo sus miembros dentro del dominio (o del bosque). Como veremos después, durante la instalación del Directorio Activo, se crean grupos de seguridad predeterminados que facilitan al administrador la delegación de ciertos aspectos de la administración (como, por ejemplo, las copias de seguridad) en otros usuarios del sistema.
- *Asignar permisos para recursos* a los grupos de seguridad. Lo que nos permite definir quién accede a cada recurso y bajo qué condiciones (control total, sólo lectura, etc.) También se establecen permisos de forma predeterminada sobre diferentes objetos del dominio para ofrecer distintos niveles de acceso.

Grupos integrados

Como hemos mencionado antes, durante la instalación del *Directorio Activo* se crean una serie de grupos que podremos utilizar para simplificar la asignación de derechos y permisos a otras cuentas o grupos. Como veremos más abajo, los grupos se administran con el complemento *Usuarios y equipos de Active Directory*. Cuando ejecutemos esta herramienta, encontraremos los grupos predeterminados en dos contenedores:

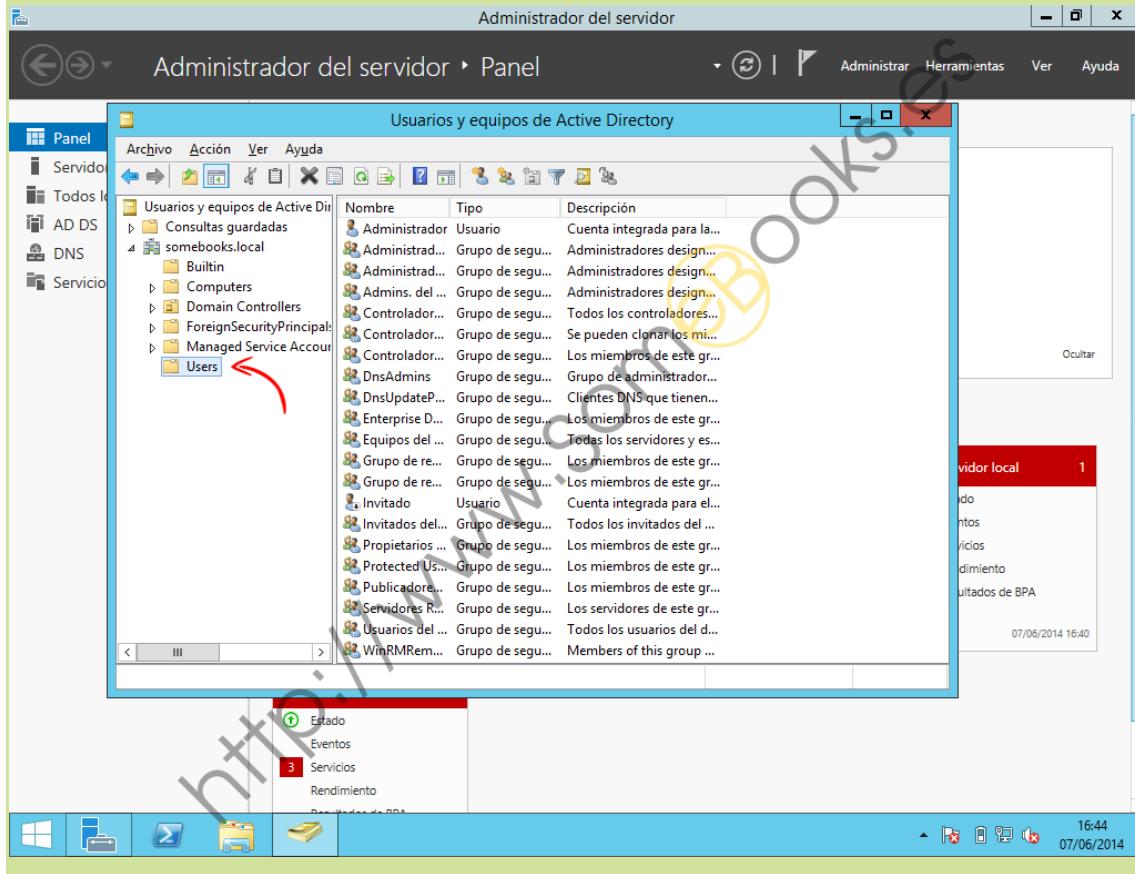
Los grupos predeterminados incluidos en el contenedor *Builtin* tienen un ámbito local.



Puedes ver un pequeño resumen de todos ellos en la siguiente tabla:

Grupos del contenedor Built-in		
Grupo	Descripción	Derechos de sus miembros
Operadores de cuentas	Sus miembros pueden crear, modificar y eliminar grupos y cuentas de usuario y equipo dentro del contenedor contoso salvo en la unidad organizativa Controladores de dominio. Tampoco pueden modificar los grupos de administradores o Administradores del dominio (ni sus miembros). Sus miembros pueden iniciar y cerrar sesión de forma local en el controlador del dominio.	Permitir el inicio de sesión local Apagar el sistema
Administradores	Sus miembros tienen un control total sobre los controladores del dominio. Lógicamente, la cuenta Administrador es miembro predeterminado de este grupo. Un usuario que sea miembro de este grupo podrá asignarse cualquier privilegio que no ostentara de forma predeterminada.	Acceder al equipo desde la red Ajustar cuotas de memoria a los procesos. Realizar backups. Eliminar comprobación de recorrido. Modificar la hora del sistema Crear un archivo de paginación Depurar programas Habilitar la delegación de control para cuentas de usuario y grupos. Forzar cierre desde un sistema remoto. Aumentar prioridad de planificación. Cargar y descargar controladores de dispositivo. Permitir el inicio de sesión local Administrar registros de seguridad y auditoría. Modificar valores de entorno del firmware. Analizar un solo proceso Analizar el rendimiento del sistema Eliminar el estado de conexión de un equipo. Restaurar archivos y directorios Apagar el sistema Tomar posesión de archivos y otros objetos
Operadores de copia de seguridad	Sus miembros pueden hacer backups de todos los datos de los controladores del dominio y restaurarlos, aunque no tengan permisos de lectura o escritura sobre ellos. También pueden iniciar sesión en los controladores de dominio y apagárslos.	Hacer backups de archivos y directorios, y restaurarlos Permitir el inicio de sesión local Apagar el sistema
Invitados	Por defecto, el grupo Invitados del dominio es miembro de este grupo. También lo es la cuenta Invitado (deshabilitada de forma predeterminada).	No tiene derechos de usuario predeterminados.
Creadores de confianza de bosque de entrada (solo aparece en el dominio raíz del bosque)	Sus miembros pueden crear relaciones de confianza a nivel del bosque, siempre que sean unidireccionales al dominio raíz del bosque. Es decir, si nos encontramos en el bosque A, los miembros de este grupo pueden crear una relación de confianza para el bosque B que permita a los usuarios del bosque A acceder a los recursos del bosque B.	No tiene derechos de usuario predeterminados.
Operadores de configuración de red	Sus miembros pueden cambiar la configuración de red, añadir o liberar direcciones TCP/IP en los controladores del dominio. De forma predeterminada, no tiene ningún miembro.	No tiene derechos de usuario predeterminados.
Usuarios del monitor de sistema	Sus miembros pueden comprobar los valores de rendimiento de los controladores del dominio. Pueden usarse en modo local o desde un cliente.	No tiene derechos de usuario predeterminados.
Usuarios del registro de rendimiento	Sus miembros pueden administrar cambios en el rendimiento, reajustarlo y efectuarlo en los controladores del dominio. Pueden usarse en modo local o desde un cliente.	No tiene derechos de usuario predeterminados.
Acceso compatible con versiones anteriores a Windows 2000	Sus miembros tienen acceso de lectura a todos los usuarios y grupos del dominio. Ofrece compatibilidad con equipos que ejecutan Windows NT 4.0 o anterior. Por defecto, la identidad Todos es miembro de este grupo.	Tener acceso a este equipo desde la red Omitir comprobación de recorrido
Operadores de impresión	Sus miembros pueden administrar, crear, compartir e eliminar impresoras conectadas a los controladores del dominio. También puede instalar y desinstalar controladores de dispositivo en los controladores del dispositivo. No tiene miembros predeterminados.	Permitir el inicio de sesión local Apagar el sistema
Usuarios de escritorio remoto	Sus miembros pueden iniciar una sesión remota en los controladores del dominio. No tiene miembros predeterminados.	No tiene derechos de usuario predeterminados.
Replicador	Alberga funciones de replicación de directorio. El Servicio de replicación de archivos lo utiliza en los controladores del dominio. No tiene miembros predeterminados y no debe asignarse ninguno.	No tiene derechos de usuario predeterminados.
Operadores de servidores	Sus miembros pueden iniciar sesión de forma interactiva, crear y eliminar recursos compartidos. Iniciar y parar ciertos servicios, realizar backups y recuperarlos, formatear el disco duro y apagar el equipo. No tiene miembros predeterminados.	Hacer backups de archivos y directorios, y restaurarlos Modificar la hora del sistema Realizar backups y recuperarlos Forzar el cierre desde un equipo remoto Permitir el inicio de sesión local Apagar el sistema
Usuarios	Sus miembros pueden realizar las tareas más simples: ejecutar programas, utilizar impresoras (locales o de red), etc. Por defecto, los grupos Usuarios de dominio, Usuarios autenticados e Interactivos son miembros de este grupo. Los cambios de usuario que se crean en el dominio son miembros de este grupo.	No tiene derechos de usuario predeterminados.

En el contenedor *Users* podemos encontrar grupos predeterminados que tienen tanto ámbito local como global.



También en este caso tienes una tabla con un resumen de sus grupos:

Grupos del contenedor Users		
Grupo	Descripción	Derechos de sus miembros
Publicadores de certificados	Sus miembros pueden publicar certificados relativos a usuarios y equipos. No tiene miembros predeterminados.	No tiene derechos de usuario predeterminados.
DnsAdmins (Se instala con el servicio DNS)	Sus miembros pueden administrar el servicio DNS. No tiene miembros predeterminados.	No tiene derechos de usuario predeterminados.
NsUpdateProxy (Se instala con DNS)	Sus miembros son clientes DNS que pueden hacer actualizaciones para hacerse cargo de otros clientes (p. ej., un servidor DHCP). No tiene miembros predeterminados.	No tiene derechos de usuario predeterminados.
Administradores del dominio	Sus miembros tienen todo el control del dominio. Por defecto, este grupo forma parte del grupo Administradores en los controladores del dominio, las estaciones de trabajo del dominio y los servidores miembros del dominio, cuando éstos se unieron al dominio. Lógicamente, la cuenta Administrador es miembro predeterminado de este grupo.	Acceder al equipo desde la red Ajustar cuotas de memoria a los procesos Realizar backups y restaurarlos Eliminar comprobación de recorrido Modificar la hora del sistema Crear un archivo de paginación Depurar programas Habilitar la delegación de confianza para cuentas de usuario y equipo. Forzar cierre desde un sistema remoto Aumentar prioridad de planificación Cargar y descargar controladores de dispositivo Permitir el inicio de sesión local Administrar registro de seguridad y auditoría Modificar valores de entorno del firmware Analizar un solo proceso Analizar el rendimiento del sistema Eliminar el estado de conexión de un equipo. Apagar el sistema Tomar posesión de archivos y otros objetos
Equipos del dominio	Contiene todas las estaciones de trabajo y servidores que se han unido al dominio. Por defecto, al crear una cuenta de equipo, se hace miembro de este grupo automáticamente.	No tiene derechos de usuario predeterminados.
Controladores de dominio	Contiene todos los controladores del dominio.	No tiene derechos de usuario predeterminados.
Invitados del dominio	Contiene todos los invitados del dominio.	No tiene derechos de usuario predeterminados.
Usuarios del dominio	Contiene a los usuarios del dominio. Por defecto, las cuentas de usuario pasan a formar parte de este grupo cuando se crean. Así, para asignar permisos sobre un recurso a todos los usuarios (p. ej., una impresora), usaremos este grupo.	No tiene derechos de usuario predeterminados.
Administradores de organización (Solo aparece en el dominio raíz del bosque)	Sus miembros controlan todos los dominios del bosque. Por defecto, este grupo forma parte del grupo Administradores en todos los controladores del bosque. La cuenta Administrador es miembro predeterminado de este grupo.	Acceder al equipo desde la red Ajustar cuotas de memoria a los procesos Realizar backups y restaurarlos Eliminar comprobación de recorrido Modificar la hora del sistema Crear un archivo de paginación Depurar programas Habilitar la delegación de confianza para cuentas de usuario y equipo. Forzar cierre desde un sistema remoto Aumentar prioridad de planificación Cargar y descargar controladores de dispositivo Permitir el inicio de sesión local Administrar registro de seguridad y auditoría Modificar valores de entorno del firmware Analizar un solo proceso Analizar el rendimiento del sistema Eliminar el estado de conexión de un equipo. Apagar el sistema Tomar posesión de archivos y otros objetos
Propietarios del creador de directivas de grupo	Sus miembros pueden cambiar la directiva de grupo del dominio. Por defecto, la cuenta Administrador es miembro de este grupo.	No tiene derechos de usuario predeterminados.
IIS_WPG (Se instala con IIS)	Este grupo de trabajo para Internet Information Services (IIS) 6.0. IIS tiene procesos que ofrecen servicio a ciertos espacios de nombres (p. ej., www.microsoft.com)	No tiene derechos de usuario predeterminados.
Servidores RAS e IAS	Los servidores incluidos en el grupo pueden acceder a las propiedades de acceso remoto de los usuarios.	No tiene derechos de usuario predeterminados.
Administradores de esquema (aparece únicamente en el dominio raíz del bosque)	Sus miembros pueden modificar el esquema de Active Directory. Por defecto, la cuenta Administrador es miembro de este grupo.	No tiene derechos de usuario predeterminados.

Tanto los grupos del contenedor *Builtin* como los del contenedor *Users* pueden cambiarse libremente de contenedor, siempre que se mantengan dentro del mismo dominio. Los grupos ubicados en estos contenedores se pueden mover a otros grupos o unidades organizativas (OU) del dominio, pero no se pueden mover a otros dominios.

Debemos conocer los privilegios y derechos que ofrece cada grupo predeterminado a sus miembros antes de asignarle una cuenta de usuario o equipo. Lógicamente, la precaución será mayor cuanto más elevadas sean las capacidades del grupo en cuestión.

 [Volver al índice](#)

Directivas de Grupo (GPO) en Windows Server 2012

DICIEMBRE 10, 2014 / FERNANDO SIERRA PAJUELO



Las **Directivas de Grupo** (en adelante *GPO*) permiten implementar configuraciones específicas para uno o varios usuarios y/o equipos. Nos centraremos en cómo se debe hacer la gestión correcta de GPO en *Active Directory* de Microsoft Windows.

Para la configuración de GPO que sólo afecten a un usuario o equipo local se puede utilizar el editor de directivas locales ***gpedit.msc***. En nuestro caso accederemos en el entorno de Servicios de Dominio de Active Directory, con la consola de administración ***gpmc.msc***.

Las GPO permiten administrar objetos de usuarios y equipos, aplicando la más restrictiva en caso de existir más de una política. Se puede usar una GPO para casi cualquier cosa, como indicar qué usuario o grupo tiene acceso a una unidad de disco, o limitar el tamaño máximo que puede tener un archivo .

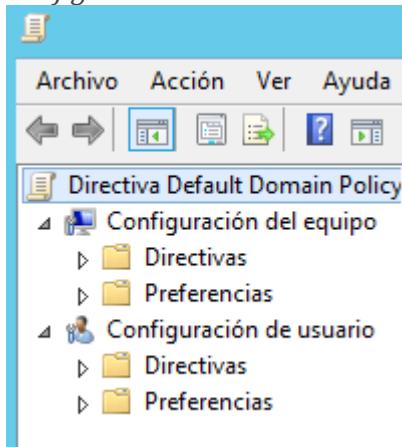
Las GPO se pueden diferenciar dependiendo del objeto al que configuran y se pueden entender en distintos niveles:

- **Equipo Local:** tan solo se aplican en el equipo que las tiene asignadas independientemente del dominio al que pertenezca.
- **Sitio:** se aplican a los equipos y/o usuarios de un sitio, independientemente del dominio.

- **Dominio:** se aplican a todos los equipos y/o usuarios de un dominio.
- **Unidad Organizativa (OU):** se aplican únicamente a los equipos y/o usuarios que pertenecen a la OU.

Dentro de la configuración de directiva se puede acceder a lo siguiente:

- *Configuración de equipo*
- *Configuración de usuario*

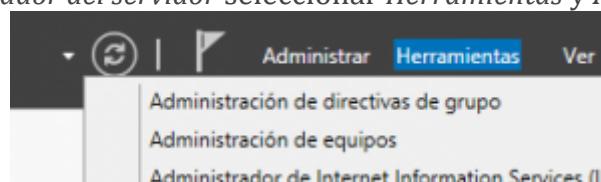


Ambos elementos se dividen en los mismos submenús, pero las políticas son distintas.

Vamos a ver un ejemplo de creación de GPO para que los usuarios monten una unidad de red al iniciar sesión.

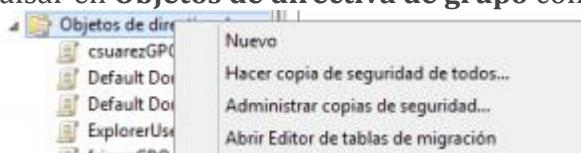
Creación de una GPO

1. Dentro de *Administrador del servidor* seleccionar **Herramientas y Administración de**



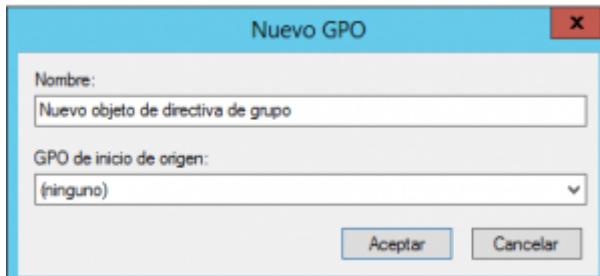
directivas de grupo:

2. Aparecen las GPO del dominio.
3. Para crear una nueva GPO desde cero, pulsar en **Objetos de directiva de grupo** con el botón derecho y seleccionar **Nuevo**:

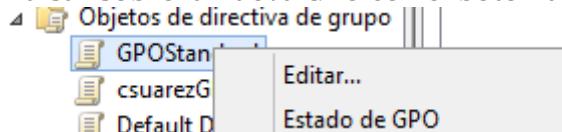


el botón derecho y seleccionar **Nuevo**:

4. No seleccionar ninguna GPO de origen. Pulsar **Aceptar**:

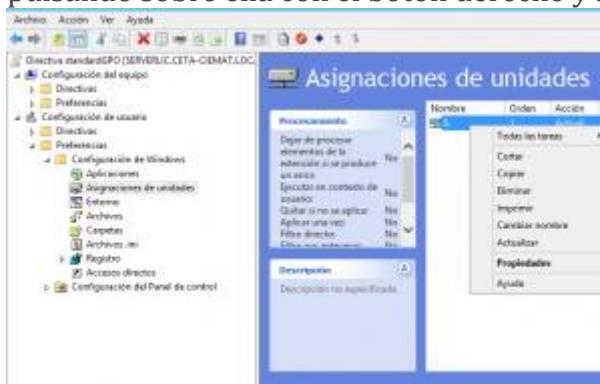


5. Pulsar sobre la nueva GPO con el botón derecho y seleccionar **Editar...**



Una vez dentro de la edición de la GPO hay que asignar la unidad de red que los usuarios deben montar, siguiendo las políticas adecuadas.

1. Navegar a **Configuración del usuario->Preferencias->Configuración de Windows->Asignaciones de Unidades** y editar la unidad que viene asignada en la GPO pulsando sobre ella con el botón derecho y seleccionar **Propiedades**:



2. Seleccionar la ubicación, el nombre con el que se quiere mostrar la unidad, la letra que se le asignará y el usuario que se conectará:



Activar una GPO

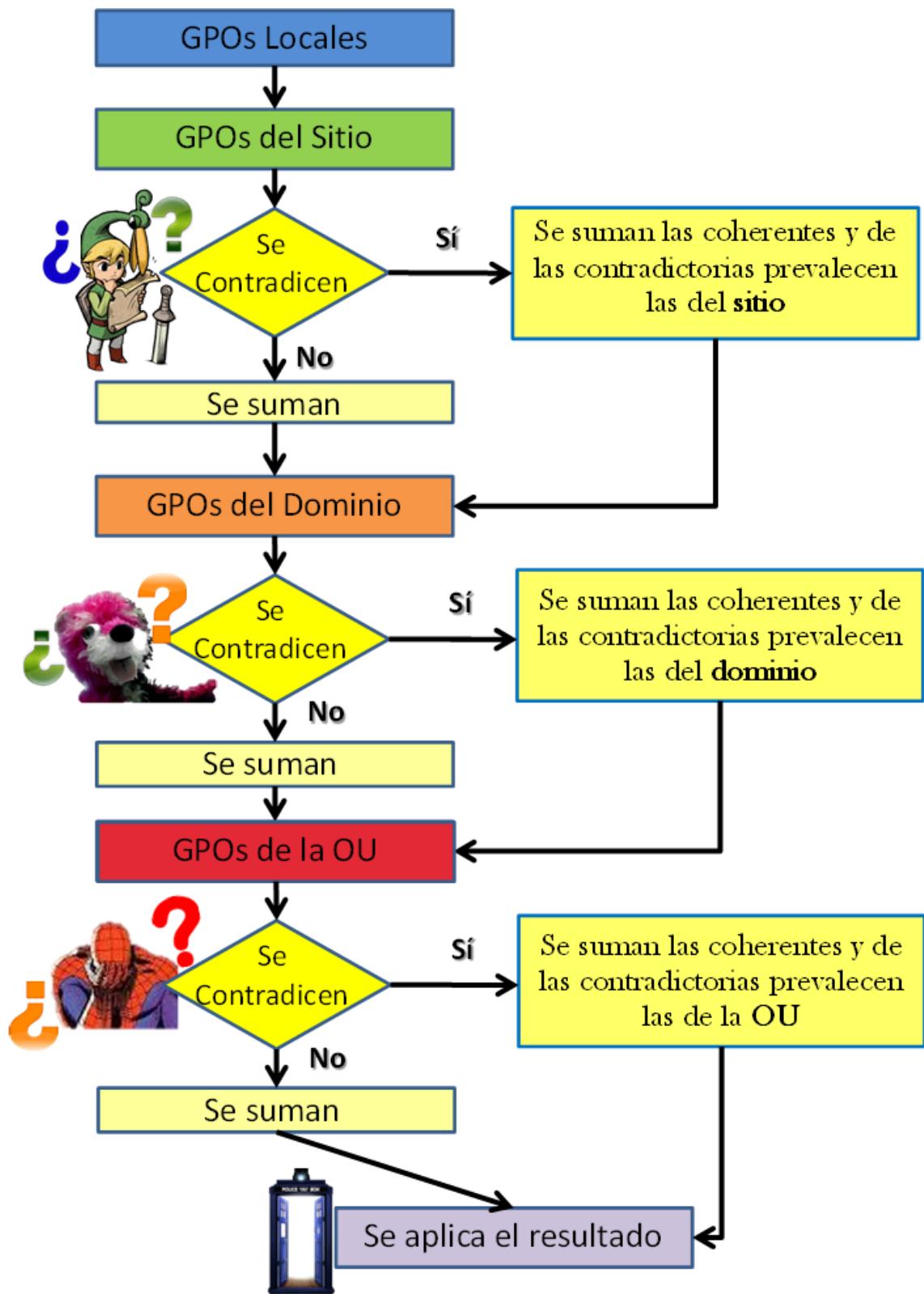
Para activar una GPO se debe seleccionar la OU, dominio, sitio o equipo local donde se quiere activar la GPO.

Un usuario, estará en un equipo local que a su vez se ubica en un sitio, y este sitio pertenecerá a un dominio que será miembro de una OU. Se puede dar la situación en la que en un equipo local se aplique una GPO, en el sitio otra, y en el dominio y la OU otras, respectivamente. Cuando se den casos así, las políticas se aplicarán según unas prioridades que atienden a una serie de reglas que se describen a continuación.

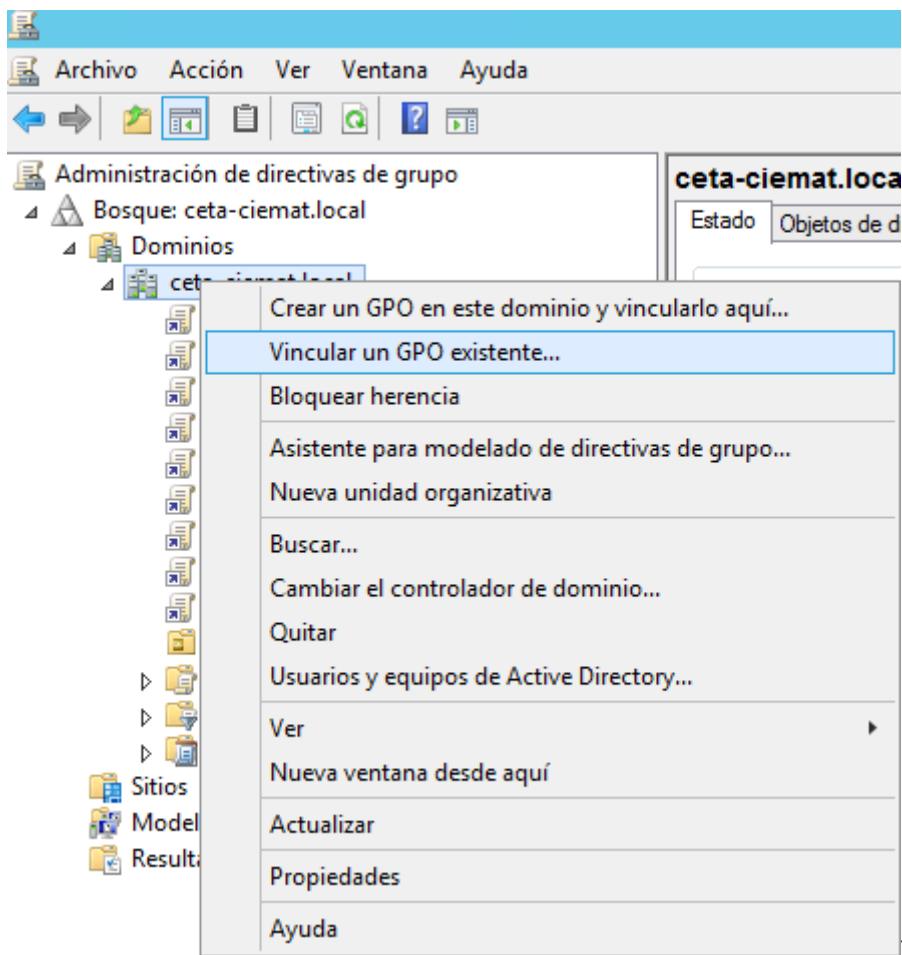
En las GPO, las políticas asignadas a una OU prevalecen sobre las del dominio, que a su vez prevalecen sobre las del sitio y estas, sobre las del equipo local. Esto no quiere decir que las políticas se anulen unas a otras, sino que siempre se suman y tan solo se anulan en caso de contradecirse entre ellas.



Se aplica el siguiente diagrama de flujo para leer las GPO y se comprueba si se contradicen o no, sumando las coherencias y prevaleciendo las más restrictivas.



Cada organización debe crear las GPO que más se acerquen a sus necesidades. Para añadir la GPO, por ejemplo al dominio, hacer click con el botón derecho y seleccionar **Vincular GPO existente....**



Y por ultimo

personalizar a que usuarios o grupos se aplicará la política.

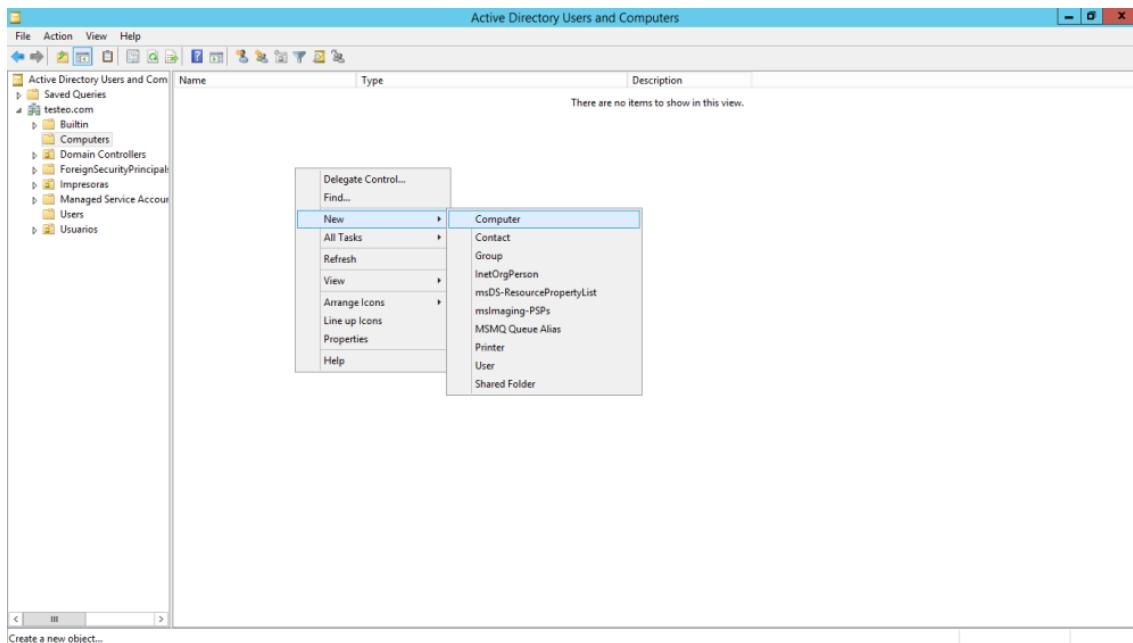
Con esto quedaría dada de alta la GPO y creada a nuestro antojo. Actualmente existen 3667 políticas disponibles para configurar y se pueden descargar de la web de [Microsoft](#).

Añadir equipos y hacer restricciones de horario a los usuarios de Active Directory

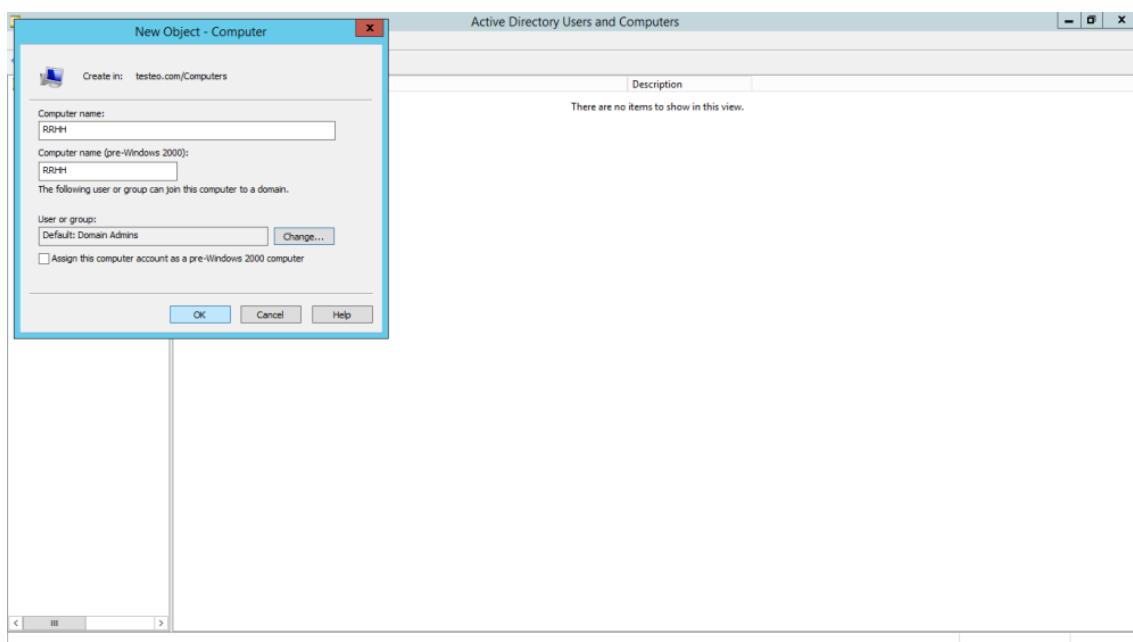
Posted on marzo 1, 2015 by [josearmnt](#)

¿Qué tal amigos? El día de hoy aprenderemos a añadir equipos a nuestro dominio de Active Directory y hacer restricciones de horario para los usuarios en Windows Server 2012 R2. Comencemos:

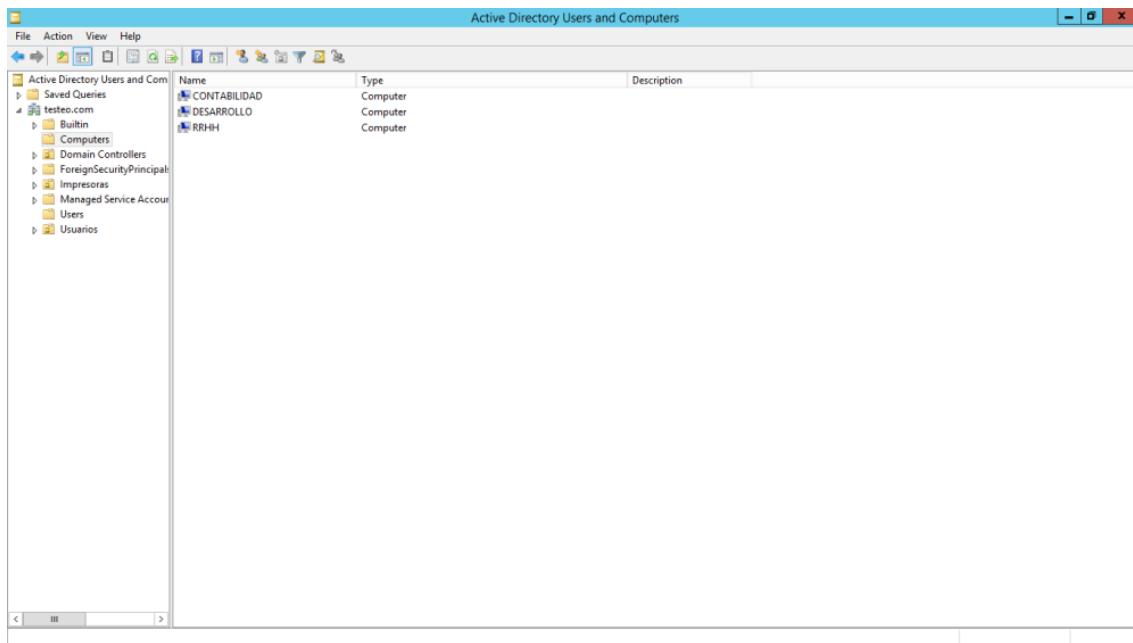
Primero vamos a crear 3 equipos:



El primer paso es ir a nuestro Server Manager, y a continuación en el administrador de Usuarios y equipos de Active Directory, en el menú de navegación de la izquierda hacemos clic en Computers y nos hacemos clic derecho > New > Computer

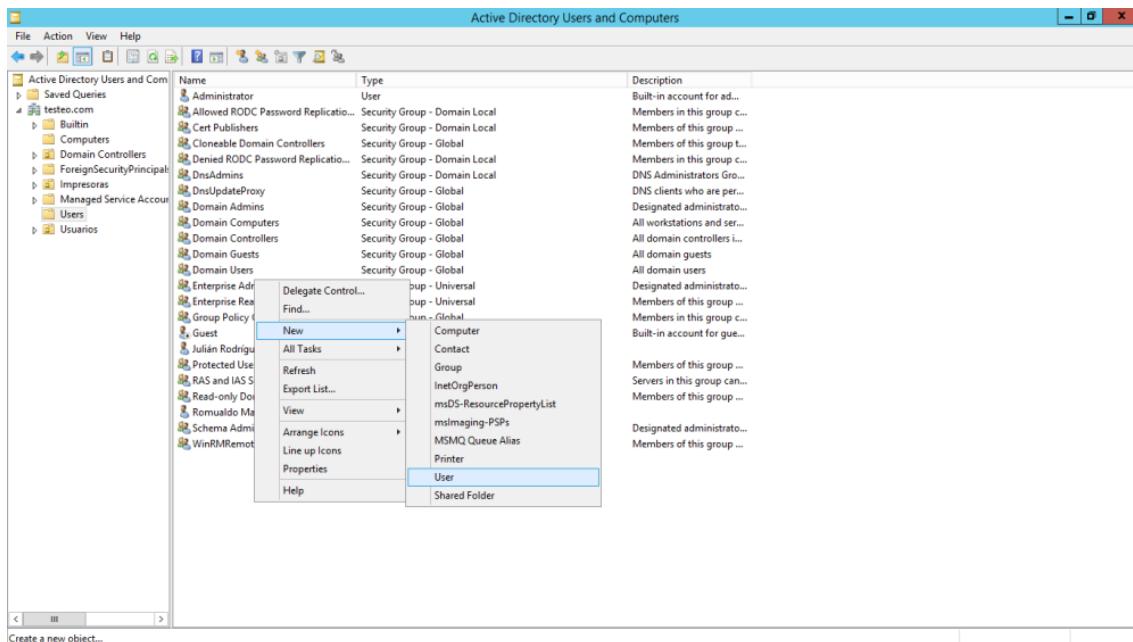


Le daremos un nombre a nuestro nuevo equipo y damos clic en Aceptar, en este caso yo haré 3, "RRHH", "CONTABILIDAD" y "DESARROLLO"

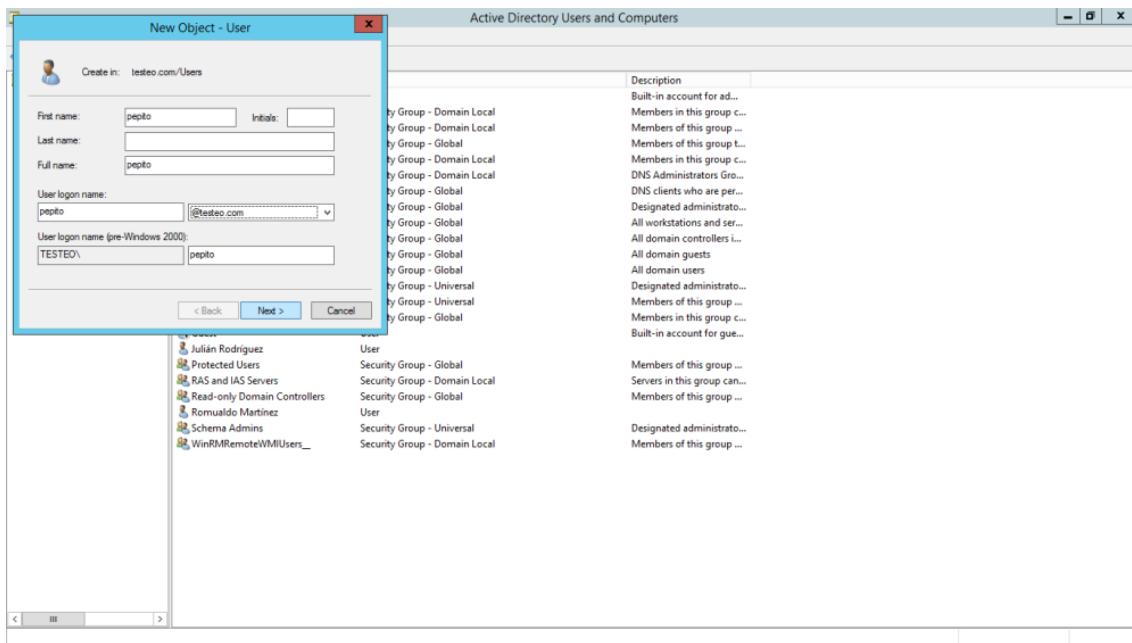


Así se verá una vez que creamos los 3 equipos

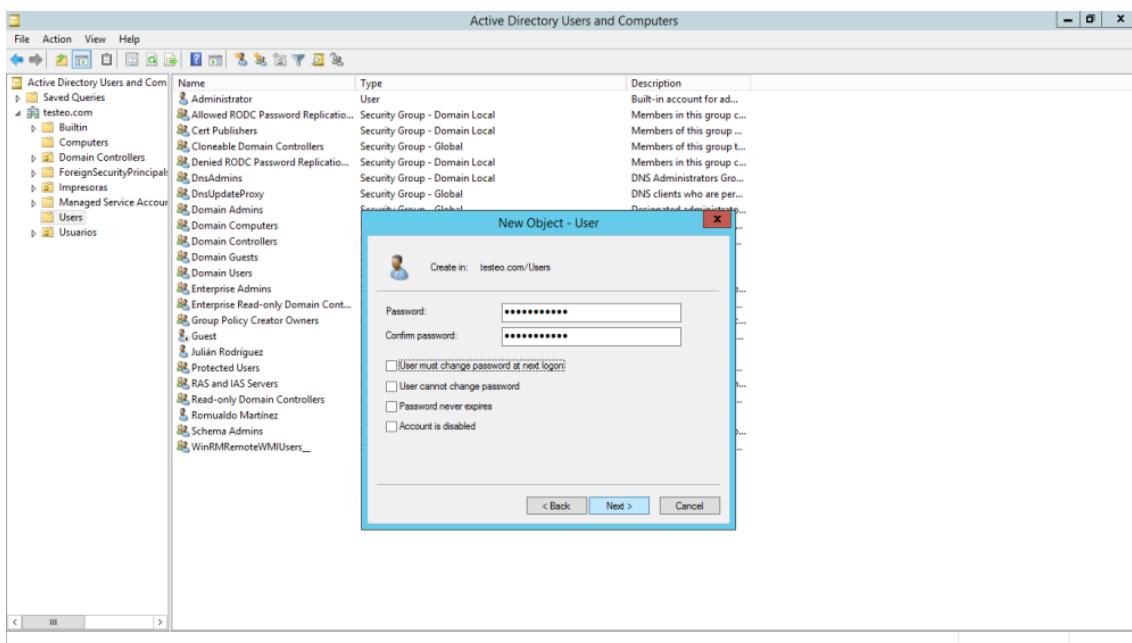
Ahora vamos a crear un usuario, al que le asignaremos un horario definido y equipos en los que puede iniciar sesión:



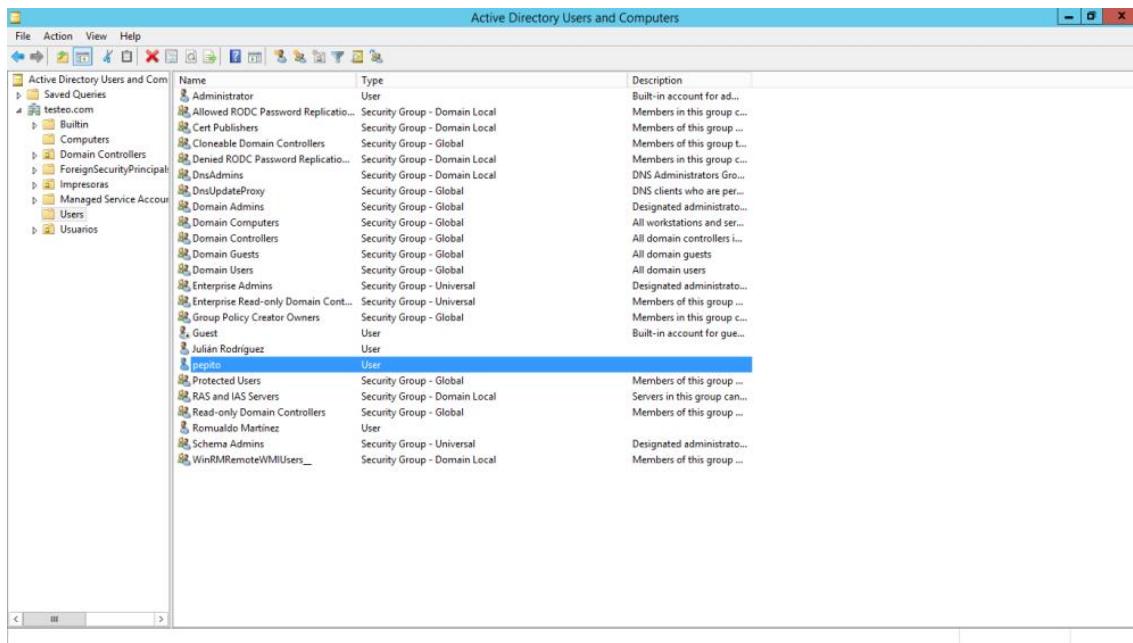
En la misma ventana del administrador de usuarios y equipos, vamos a la parte de usuarios, y damos clic derecho > New > User



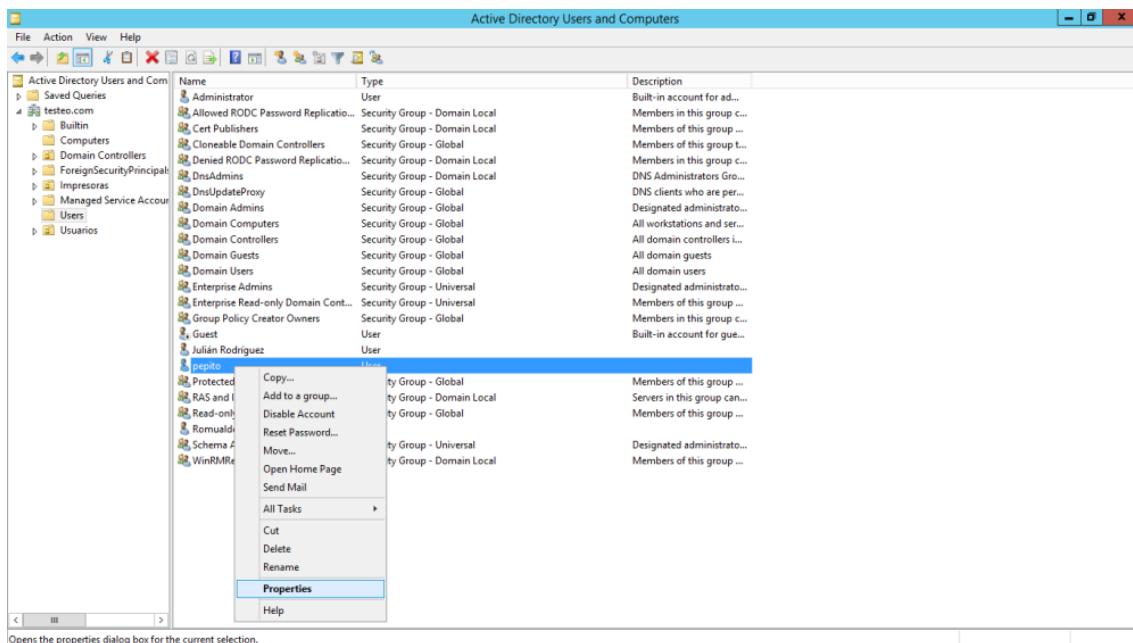
Le damos un nombre, en el ejemplo hacemos al usuario “pepito” y damos clic a siguiente



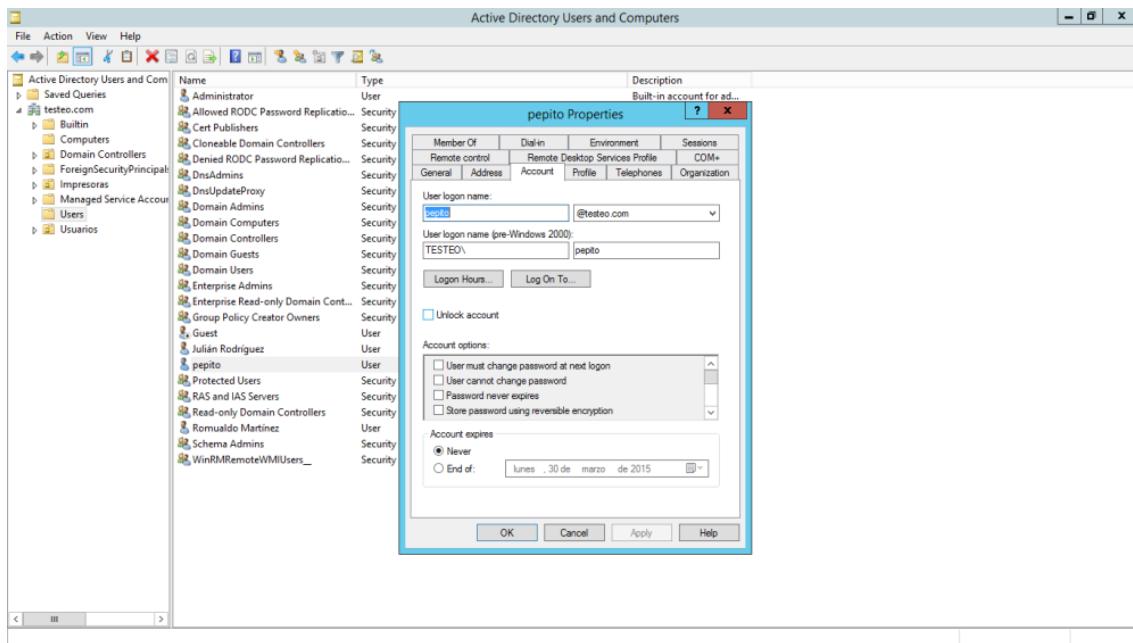
Le asignamos una contraseña a ese usuario y los criterios de esa contraseña, en mi caso le estoy diciendo que el usuario no va a cambiar la contraseña asignada, damos clic a siguiente



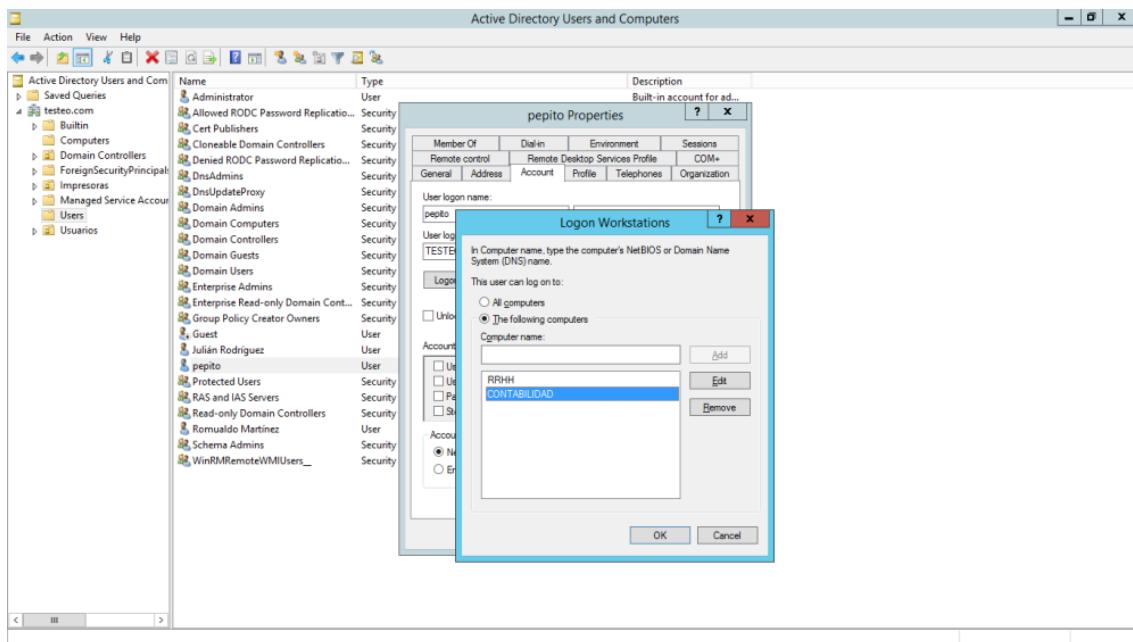
Aquí nos aparece nuestro nuevo usuario junto al resto de usuarios de AD



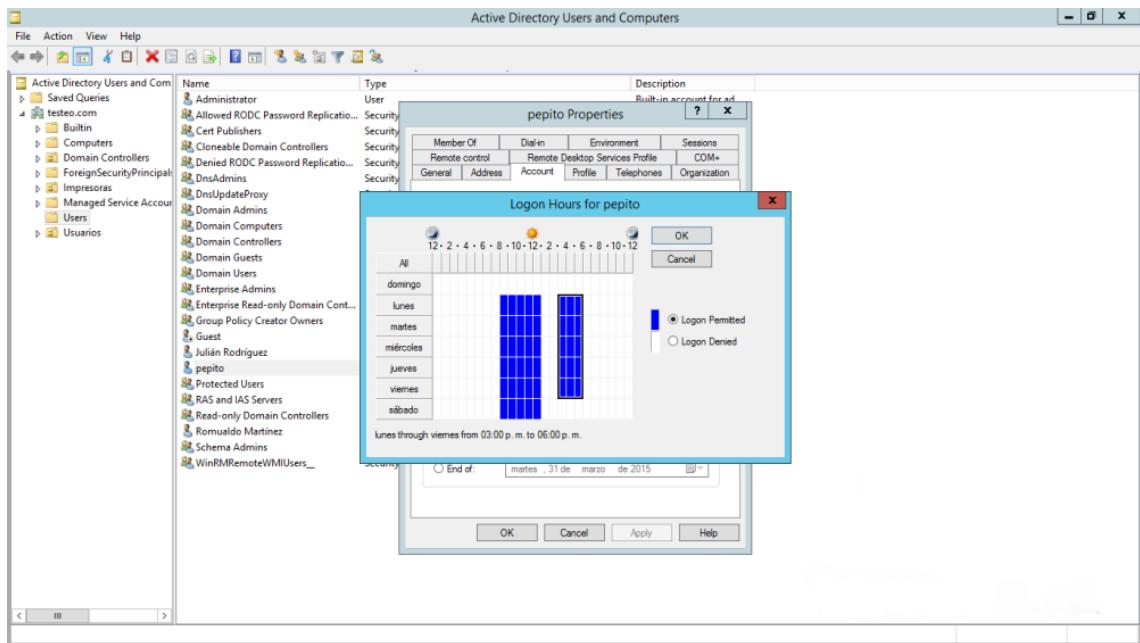
Ahora aplicaremos los criterios de inicio de sesión para esa cuenta, vamos al usuario y hacemos clic derecho en el, y a continuación en propiedades



Nos dirigimos a la pestaña “Account” y hacemos clic en “Log On To...”, esto es para indicarle desde qué equipos puede iniciar sesión “pepito”



Hacemos clic a la opción “The Following Computers” y le indicamos los nombres de los equipos desde los que se puede conectar este usuario, para el ejemplo, vamos a dejar que pepito se conecte desde “RRHH” y “CONTABILIDAD”, damos clic en aceptar

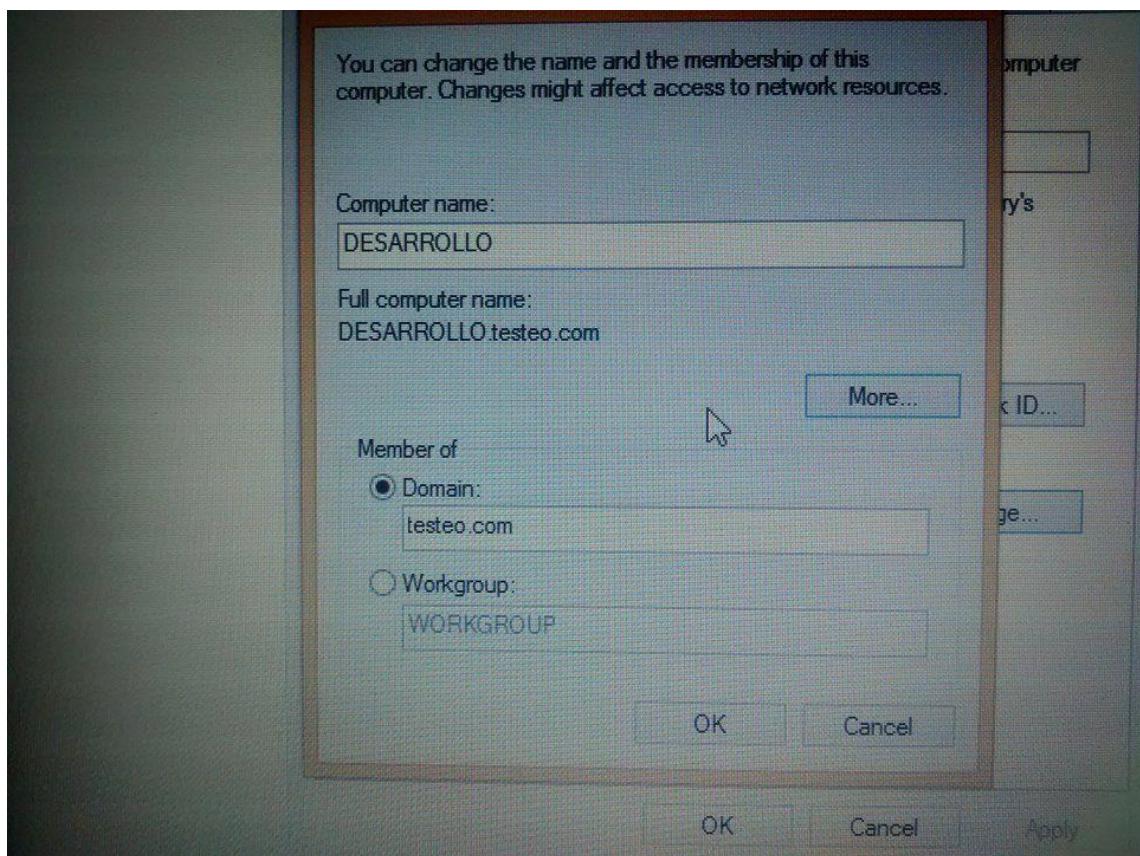


Ahora nos vamos a “Logon Hours...” para indicarle los días y horas en los que puede iniciar sesión pepito, lo marcado en azul es los horarios en los que está permitido su acceso, y lo blanco es donde el acceso estará denegado. Para el ejemplo, pepito se puede conectar de Lunes a Viernes de 8 AM a 1 PM y de 3 PM a 6 PM, y los sábados de 8 AM a 1 PM

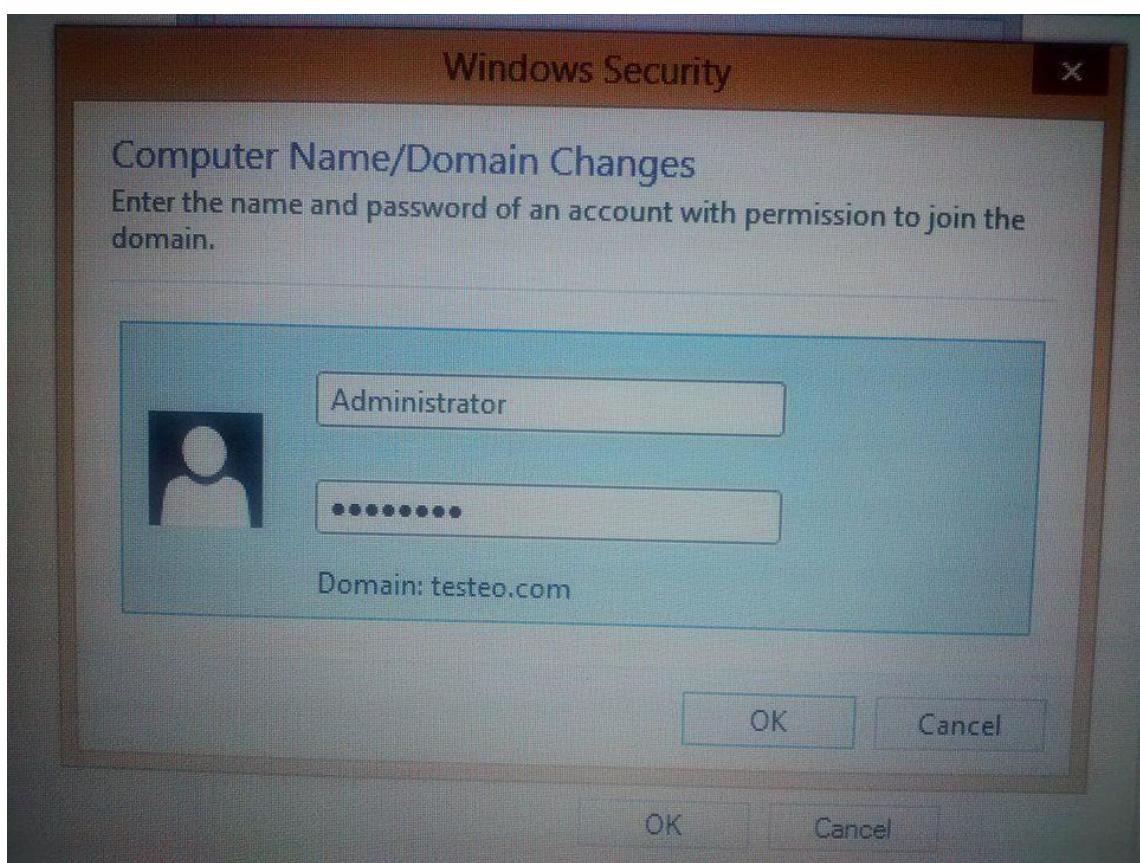
Listo, con estos pasos podemos crear equipos y añadir restricciones de horarios a los usuarios que tengamos en nuestro dominio de Active Directory.

Ahora veremos ejemplos de cómo el sistema indica al usuario las restricciones de tiempo y equipos:

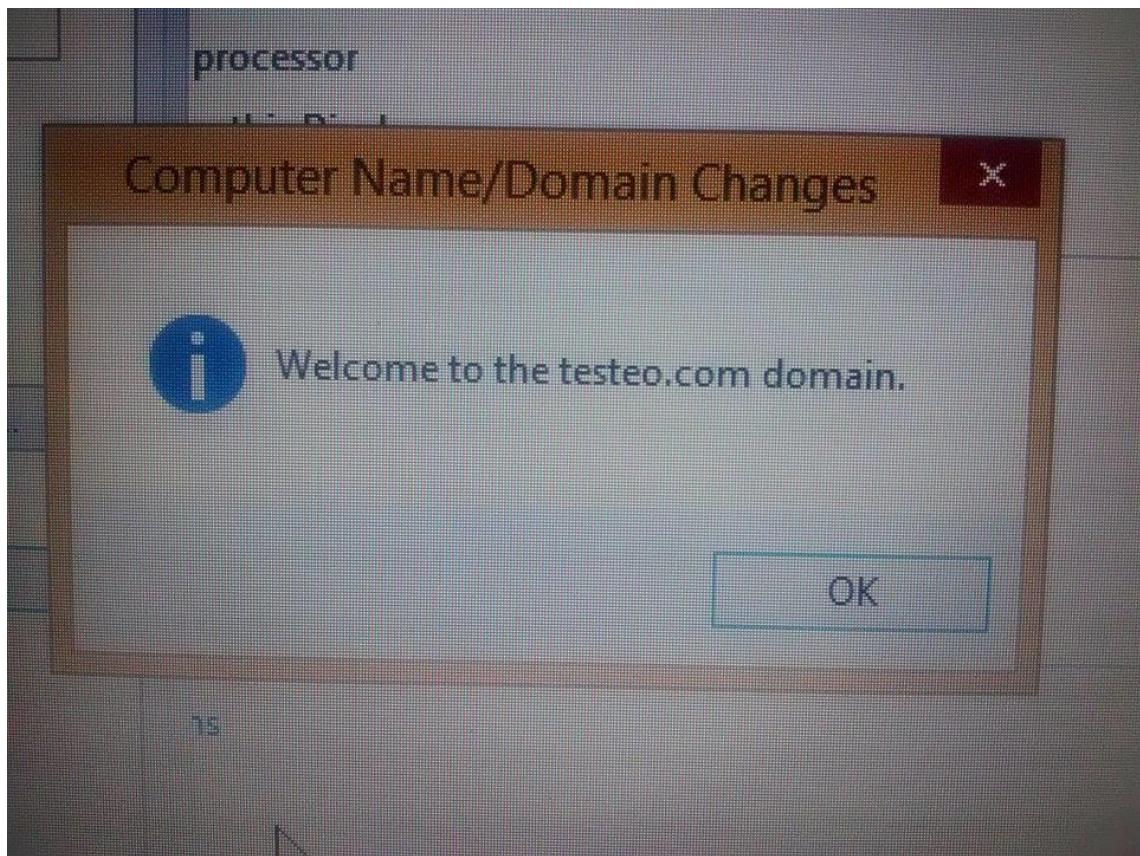
Añadiremos un equipo llamado DESARROLLO al dominio, y a continuación intentaremos iniciar sesión como “pepito”



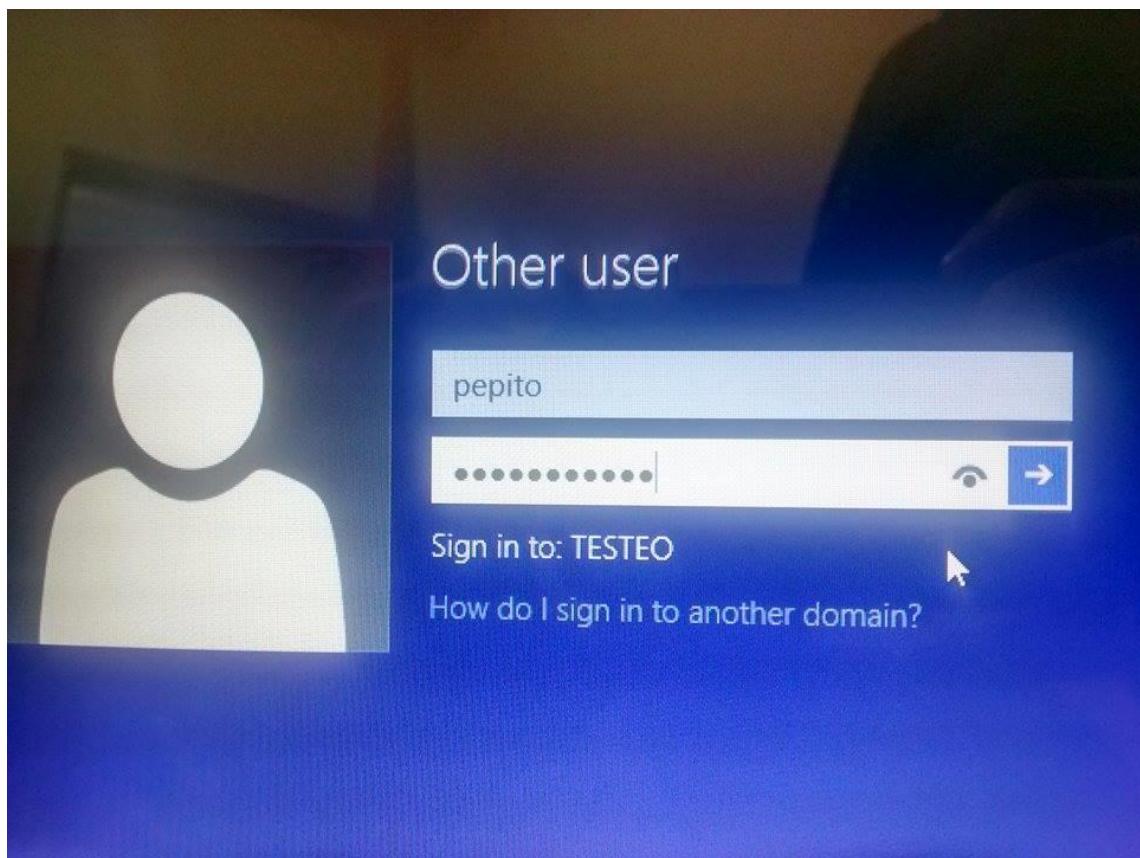
Agregamos al dominio el nuevo equipo



Ingresamos nuestra cuenta de Administrador del servidor



Nos hemos unido correctamente al dominio



Ingresamos nuestras credenciales de "pepito"



El sistema nos muestra la notificación de que este “pepito” no puede iniciar sesión desde el equipo de DESARROLLO

En la siguiente imagen, tratamos de iniciar sesión esta vez desde “CONTABILIDAD”, un equipo en el que “pepito” si tiene permiso de iniciar sesión, sin embargo, la hora a la que trata de entrar no es la permitida por el servidor:

