Active Directory

¿Qué es?

Active Directory es uno de los tantos componentes que vienen dentro de Windows Server 2008 R2 y que nos hará de base para armar nuestra red lógica empresarial. Desde el AD (Active Directory) podremos centralizar todos los recursos tales como usuarios, computadoras, impresoras, grupos de distribución, grupos de seguridad entre otros pero principalmente tendremos Identidad y Acceso a nuestra red.

Si se realiza una traducción literal Active Directory no es ni más ni menos que Directorio Activo, pero esta traducción no nos dice gran cosa. Lo primero que tenemos que especificar es qué entendemos por directorio. Un directorio es una guía donde podemos encontrar distinta información clasificada según un determinado criterio. El concepto de directorio no es único de la informática, ya que a lo largo de la historia se han utilizado multitud de directorios, como por ejemplo las paginas amarillas.

Pero el Directorio Activo no solo contiene la información, si no que también presta los servicios necesarios para poder realizar la administración de esta información desde un único punto.

Así pues, podemos ver el directorio activo como un único catalogo global, que guarda información acerca de los recursos (impresoras, dispositivos de almacenamiento de información,...) existentes en un dominio, de los servicios dados de alta en el dominio (servicio web, servicio de impresión,...), de los usuarios, las operaciones que pueden realizar sobre los recursos y los servicios que pueden utilizar.

Terminología y conceptos de Directorio Activo

- **Dominio**

  El dominio es la estructura fundamental del directorio Activo. Permite agrupar todos los objetos que se administran de forma estructurada y jerárquica.

- **Unidad Organizativa**

  Es la unidad jerárquica inferior del dominio, que puede estar compuesta por una serie de objetos y/o por otras unidades organizativas.

- **Espacios de nombres y resolución de nombres**

  Un espacio de nombres es un área en la que un nombre se puede resolver. Por ejemplo, un sistema de archivos informático constituye un espacio de nombres en el cual se puede relacionar un nombre de archivo con el propio archivo.

Directorio Activo constituye un espacio de nombres en el cual se puede relacionar el nombre del directorio con el propio objeto. La resolución de nombres es el proceso de relacionar un nombre con un objeto o información que representa dicho nombre.

- **Atributo**

  Cada fragmento de información que describe algún aspecto de una entrada se denomina atributo. Un atributo está formado por un tipo del atributo y uno o más valores del atributo. Un ejemplo de un atributo podría ser "numero de teléfono", y un ejemplo del valor del atributo "numero de teléfono" podría ser: "555322552".

- **Objeto**

  Un objeto es un conjunto determinado de atributos que representa algo en concreto, como un usuario, una impresora o una aplicación. Los atributos contienen la información que describe lo que se identifica por medio del objeto del directorio. Entre los atributos de un usuario podrían incluirse el nombre, los apellidos, y la dirección de correo electrónico, por ejemplo. Cada objeto en Directorio Activo tiene una identidad única. Los objetos se pueden mover o renombrar, pero su identidad nunca cambia.

  Los objetos se conocen internamente por su identidad, no por su nombre actual. La identidad de un objeto es un identificador único global (GUID, Globally Unique Identifier), asignado por el Agente del sistema de directorios (DSA, Dierctory System Agent) cuando se crea el objeto. El GUID se almacena en un atributo que forma parte de todo objeto (objectGUID) y no se puede ni modificar ni borrar.

- **Contenedor**

  Un contenedor se parece a un objeto en que posee atributos, y forma parte del espacio de nombres, sin embargo, a diferencia de un objeto, un contenedor no representa algo en concreto, es un almacén de objetos y otros contenedores.

- **Arbol y subárbol**

  Un árbol en directorio Activo es simplemente una extensión de la idea de árbol de directorios. Es una jerarquía de objetos y contenedores que muestra cómo se relacionan los objetos, o el camino desde un objeto a otro, Un subárbol es cualquier camino sin interrupciones del árbol, incluyendo todos los miembros de cada contenedor de dicho camino.

- **Esquema**

  Esquema es un término utilizado generalmente en el trabajo con bases de datos. En el contexto de Directorio Activo, el esquema son todos los fragmentos que componen un Directorio Activo: los objetos, atributos, contenedores, entre otros.

Directorio Activo posee un esquema predeterminado que define la mayoría de las clases de objetos habituales, como usuarios, grupos, computadoras, departamentos, políticas de seguridad y dominios. Pero que tenga definidos estas clases de objetos no significa que los usuarios que tengan los permisos adecuados, no puedan definir nuevas clases de objetos y nuevos tipos de atributos.

Estructura Lógica de un Dominio

Antes de realizar la instalación del Directorio Activo es necesario realizar la planificación de la estructura de dominio que se desea tener. La estructura del Directorio Activo es de tipo jerárquico, en la que cada rama puede ser un dominio o una Unidad Organizativa. En el caso más sencillo en el que un único dominio cumple las necesidades bastaría con un único árbol que contenga el dominio. Para construir un árbol hay que comenzar por crear el primer dominio en la estructura.

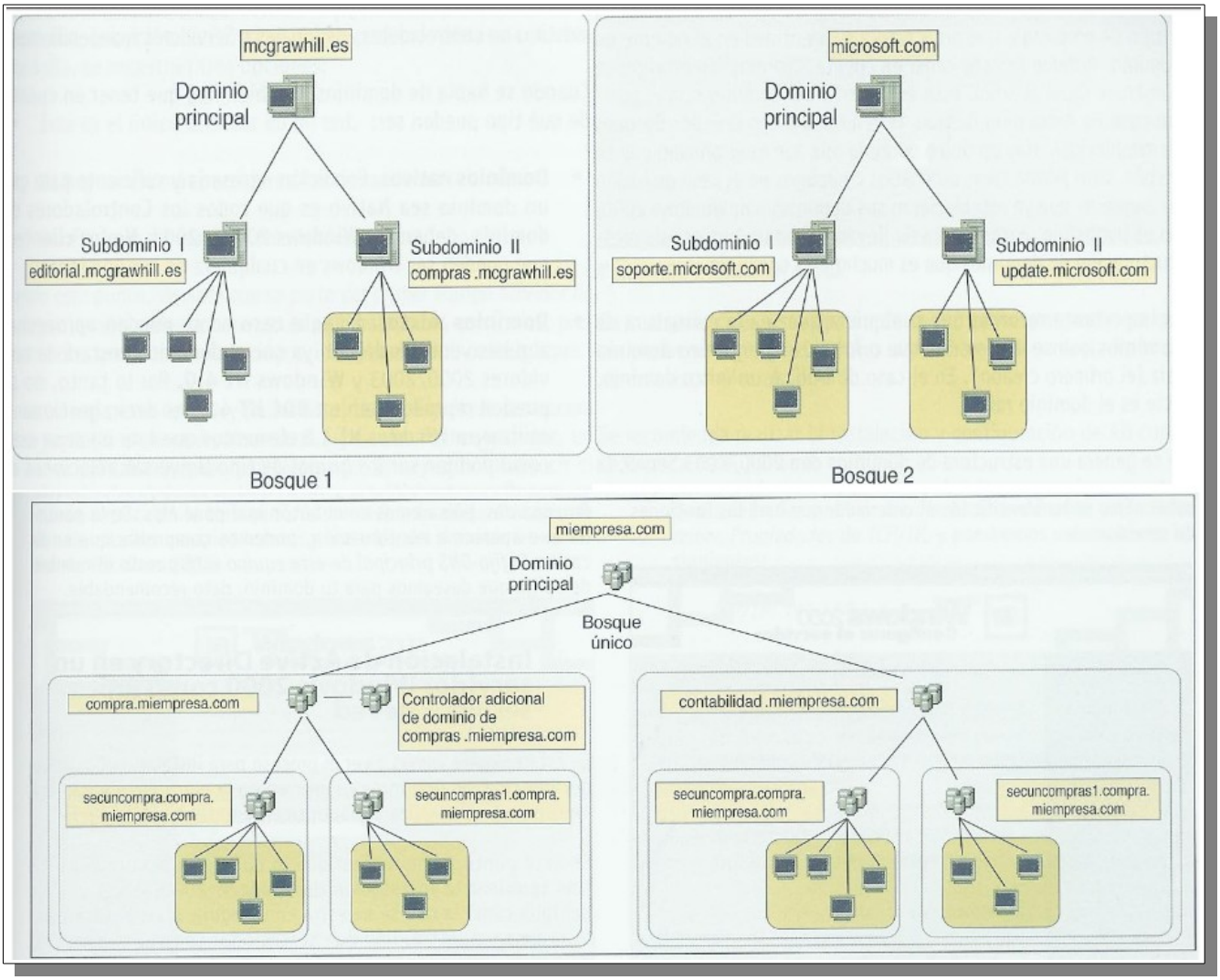
El primer controlador de dominio, si se parte de cero, se considerará el dominio principal o dominio maestro. Dependiendo de las necesidades de la organización, se puede partir de la base de dos premisas diferentes:

Necesitamos un solo dominio: En este caso tendremos un ordenador principal que controle todo el sistema. El dominio principal siempre tendrá un nombre similar a dominio principal.com, por ejemplo, y el resto de dominios hijos que dependen de él tendrán denominaciones similares a subdominio1.dominioprincipal.com , subdominio2.dominioprincipal.com , etc.

Necesitamos más de un dominio: Este caso es similar al anterior, con la única diferencia de que contaremos con dos controladores principales de dominio, tales como dominioprincipal1.com, dominioprincipal12.com. En este caso surge la necesidad de que ambos dominios principales estén integrados en una única unidad de control centralizada. Aparece el concepto de bosque.

El bosque se define como una estructura principal capaz de aglutinar a varios controladores principales de dominio. De esta forma, el bosque será la estructura principal, y cada controlador de dominio una estructura delegada dentro del mismo.

En las siguientes figuras podemos ver la estructura de dos árboles de dominios y un bosque con ambos integrados:



Árboles

Es posible dar una definición más precisa de un árbol de dominio : conjunto jerárquico de dominios que comparten relaciones de confianza y espacio contiguo de nombres:

- **Relaciones de confianza**

  Creadas automáticamente con el dominio superior, de tipo bidireccional (A -> B y B -> A) y transitivo (A -> B, B -> C ; por lo tanto, A -> C)

- **Espacio contiguo de nombres**

  Cada subdominio debe incluir el nombre del dominio del cual cuelga, salvo el primero. No hay un límite teórico en cuanto a la cantidad de subdominios que puede tener cada uno, ni en cuanto

a los niveles de hijos de cada uno.

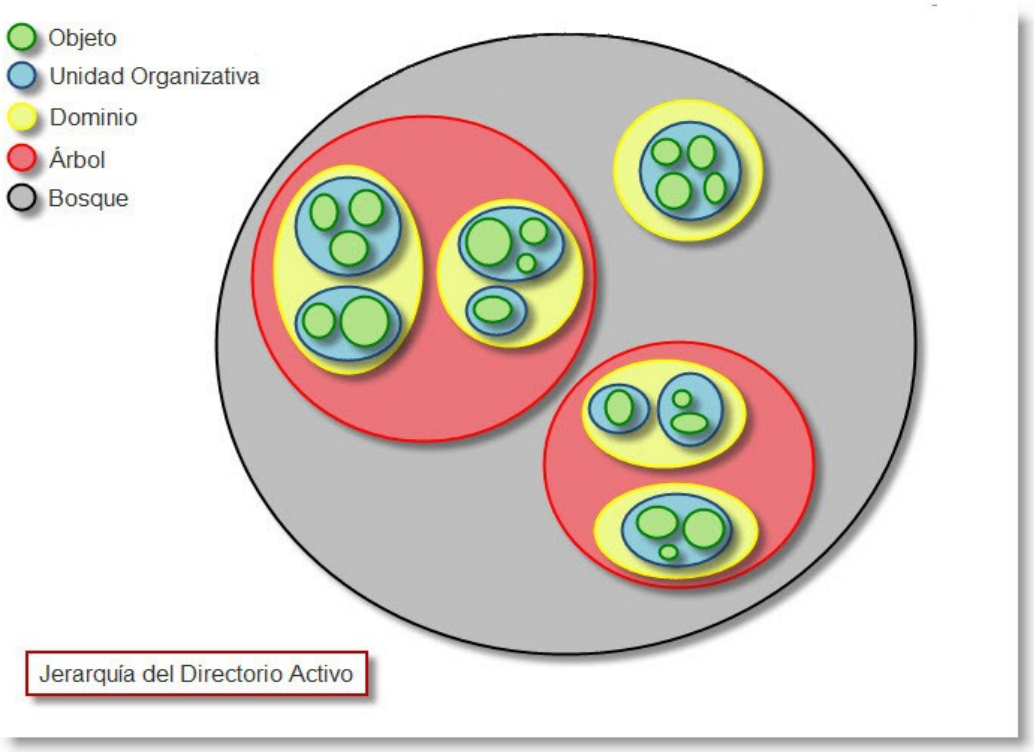
- Comparten la configuración y el esquema.
- Comparten la información en el Catálogo Global

La configuración es una sección del Directorio Activo donde está almacenada la configuración común de todos los dominios, como pueden ser los nombres y la ubicación de cada uno de ellos, relaciones de confianza, etc.

El esquema es la definición formal de los atributos y clases de objetos que forman el directorio. Una de las novedades más importantes de Windows 2000 es la posibilidad de crear nuevas clases de objetos o modificar clases existentes para adaptarlo a necesidades propias de la empresa.

El catalogo global aglutina el conjunto de todos los objetos del directorio. Es posible realizar copias del catalogo global bajo otros controladores de dominio en cada uno de los cuales se realizará una replica de los objetos. El catalogo global se utiliza durante el inicio de sesión y cuando se hacen búsquedas de objetos en todo el directorio.

Es importante destacar que la estructura se ha de crear de arriba abajo, es decir, se debe crear el dominio raíz del árbol, a partir del cual se pueden crear los que cuelgan del mismo. Además, el dominio raíz tiene características particulares que no tiene ningún otro dominio; entre otras, tiene el grupo con privilegios para modificar el esquema, y es el único que tiene un grupo capaz de efectuar configuraciones que afecten a todo el directorio.



Instalación del Directorio Activo

Para realizar la instalación de un directorio activo necesitamos al menos una máquina con W2000 Server o W2003 Server instalado sobre una partición formateada en NTFS.

Esta máquina se convertirá en el controlador del dominio principal de nuestra organización, seguirá teniendo el S.O. instalado y funcionando, la diferencia con un W2000 o W2003 Server "normal" es que dispondremos de un mayor número de servicios y mejorará notablemente el control sobre todos y cada uno de los recursos dados de alta en el dominio.

Para convertir nuestra máquina al controlador de dominio tenemos que ejecutar la aplicación "dcpromo" (Inicio -> Ejecutar - > dcpromo). De la misma forma, si queremos realizar el paso contrario, "degradar" la máquina controlador de dominio a un servidor normal, también utilizamos el "dcpromo".

Para poder poner en marcha nuestro primer AD, precisamos contar con al menos un servidor con Windows Server 2008 R2 instalado, en nuestro caso con Service Pack 1 ya instalado como también todos sus updates.

Check List Esencial

Antes de empezar con la instalación y configuración de nuestro AD, debemos cumplir con un check list esencial:

- **Nombre del host**

  Nuestro servidor debe tener el nombre adecuado que queramos, ya que lo recomendado es que una vez configurado nuestro AD, el nombre de host no se cambie.

- **IP**

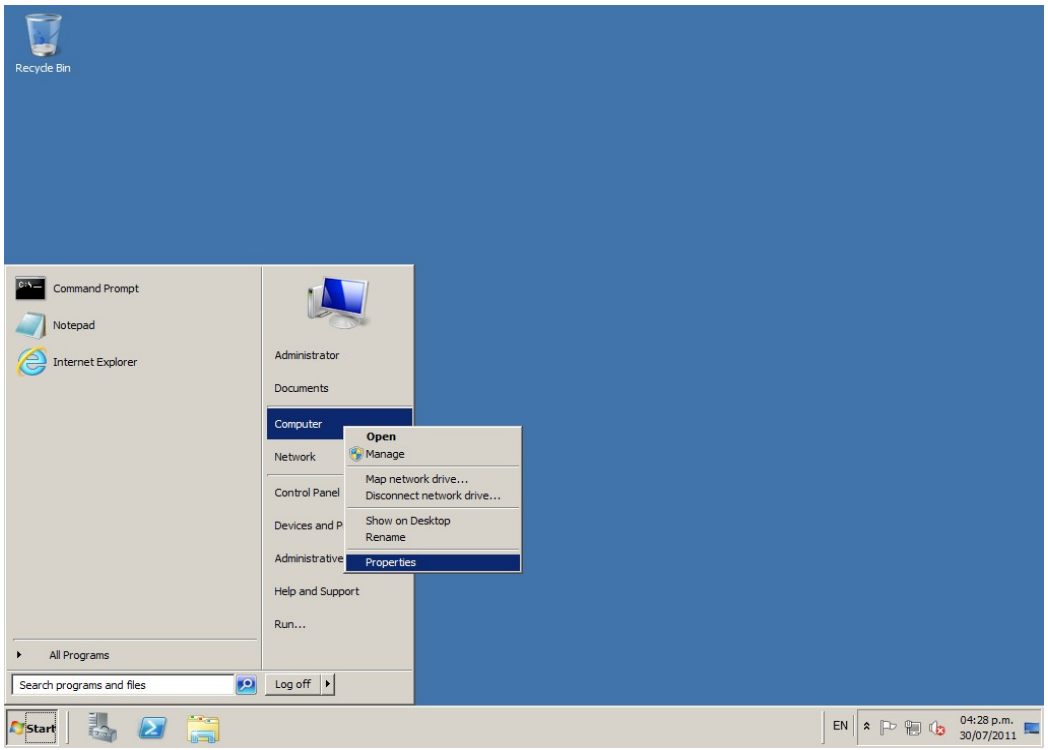
  Adicionalmente al nombre de host, el servidor debe contar con una IP fija, la cual debemos establecerla según la red que estemos armando.

- **Nombre de dominio**

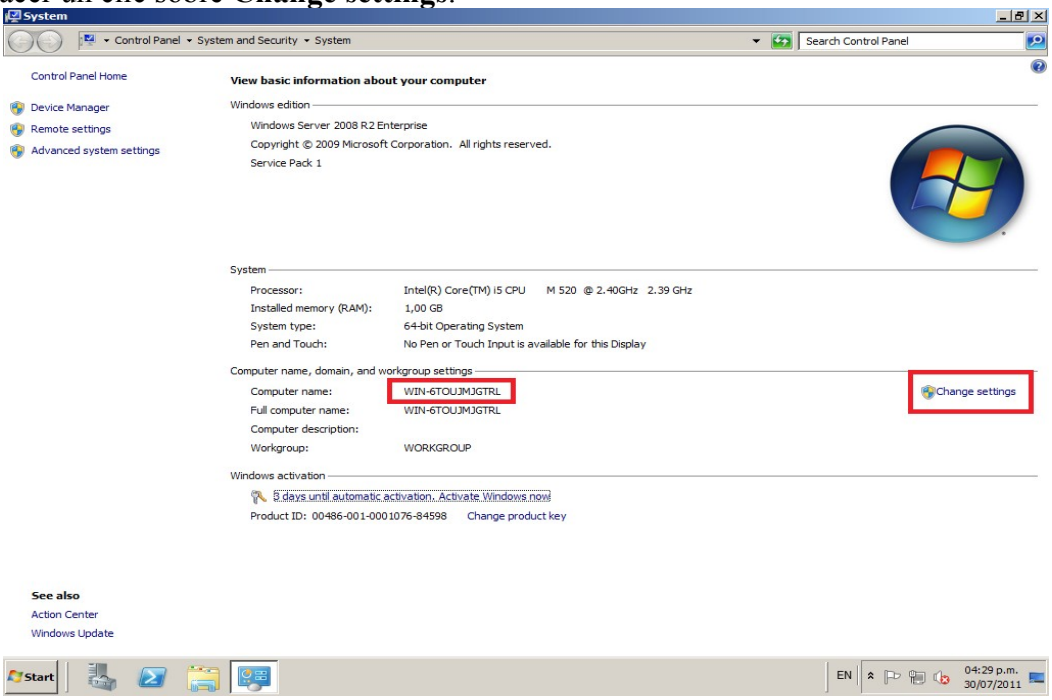
  Este punto es muy importante dado que representa en la mayoría de los casos a la organización o compañía. Si bien podemos elegir como dominio, uno propio que ya dispongamos en Internet, se recomienda que éste sea de uso exclusivo de uso interno de nuestra red. Si nuestro dominio en Internet es mswin.org, lo ideal para nuestro AD sería mswin.local o mswin.corp o similares.

1) Cambiando el nombre de host a nuestro servidor:

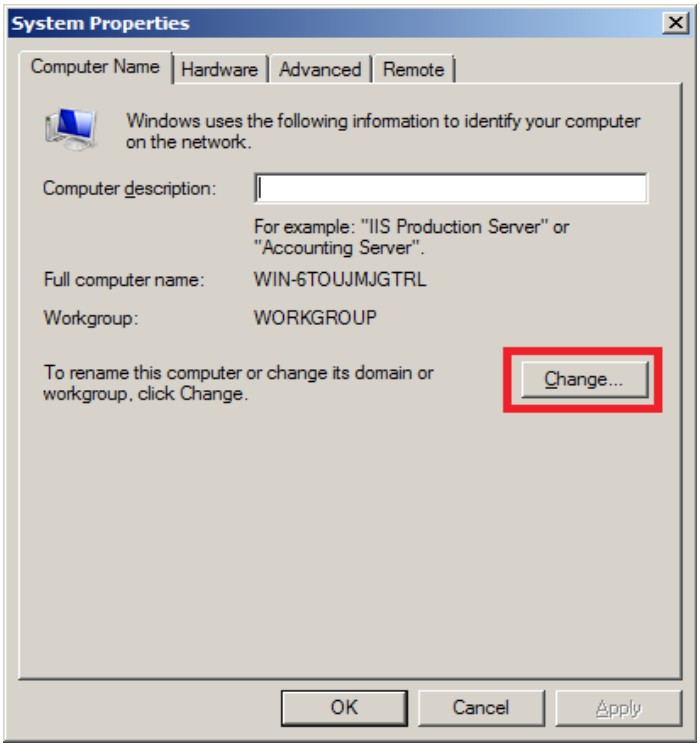
1.1) Vamos a Start y hacemos clic con el botón derecho del mouse sobre Computer y elegimos Properties



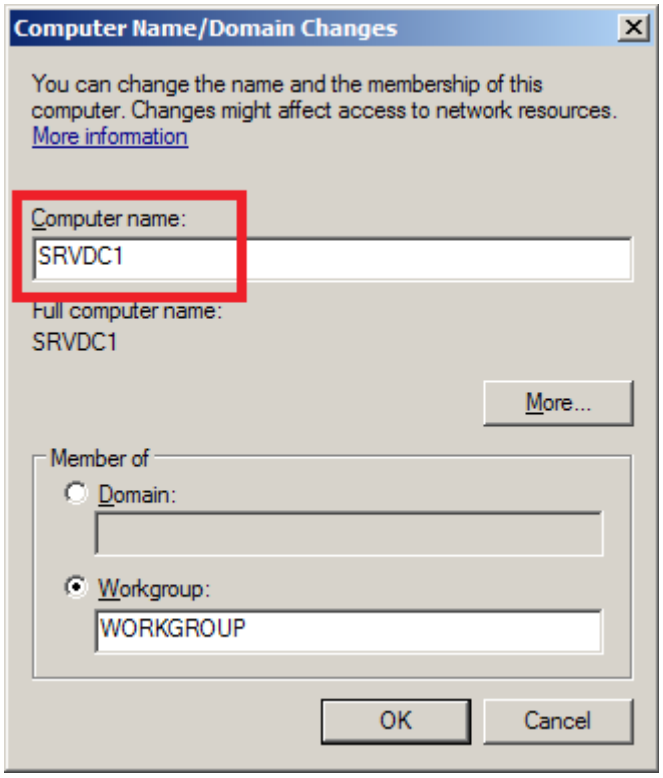
1.2) Luego en la ventana de **System**, veremos el actual nombre de nuestro servidor y para cambiarlo debemos hacer un clic sobre **Change settings**.



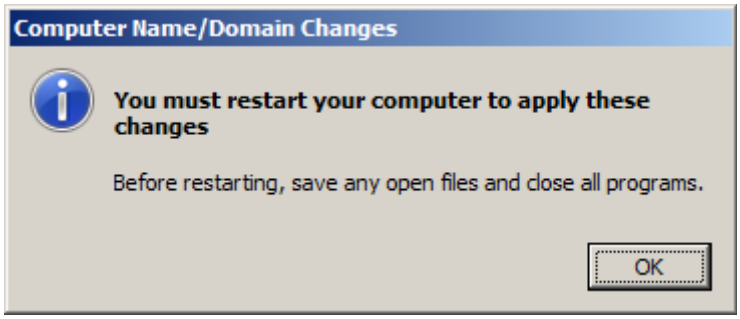
1.3) Ahora hacemos un clic en **Change**



1.4) En este paso debemos darle el nombre que queramos y luego hacer un clic en **Ok**.

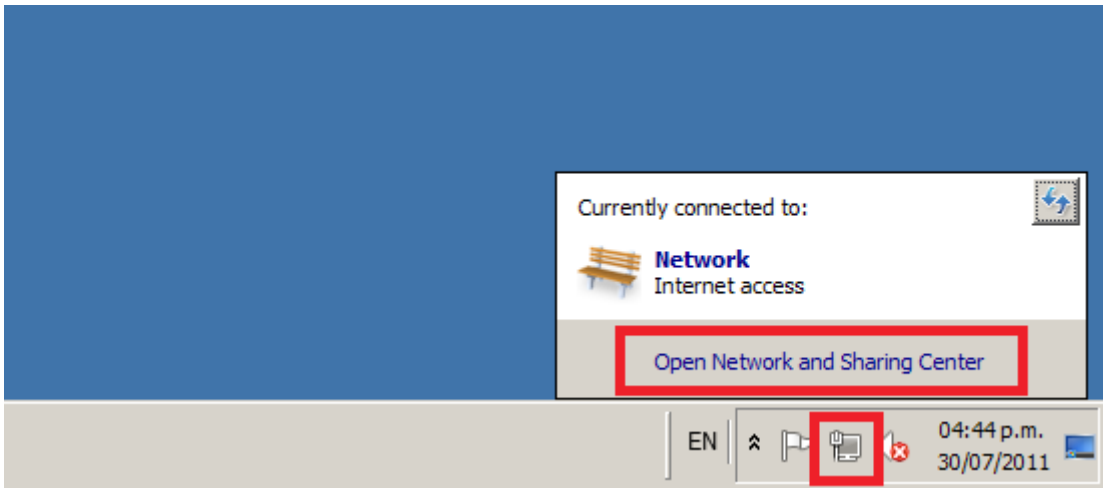


1.5) Debido a que cambiamos el nombre de nuestro servidor, el sistema nos pedirá un reinicio para que aplique los cambios, lo cual aceptamos y luego lo reiniciamos.

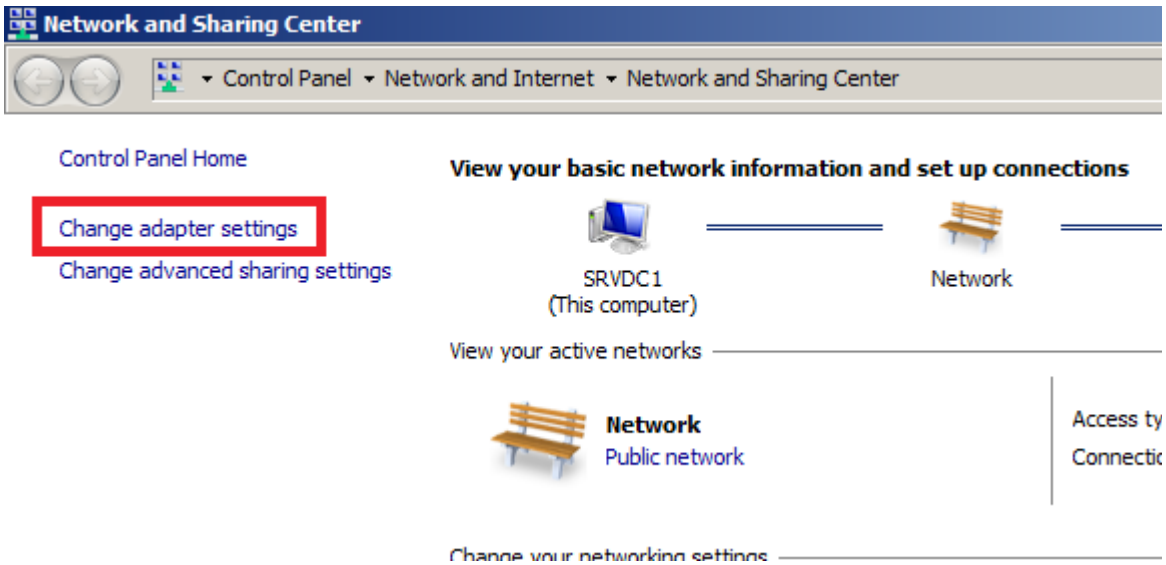


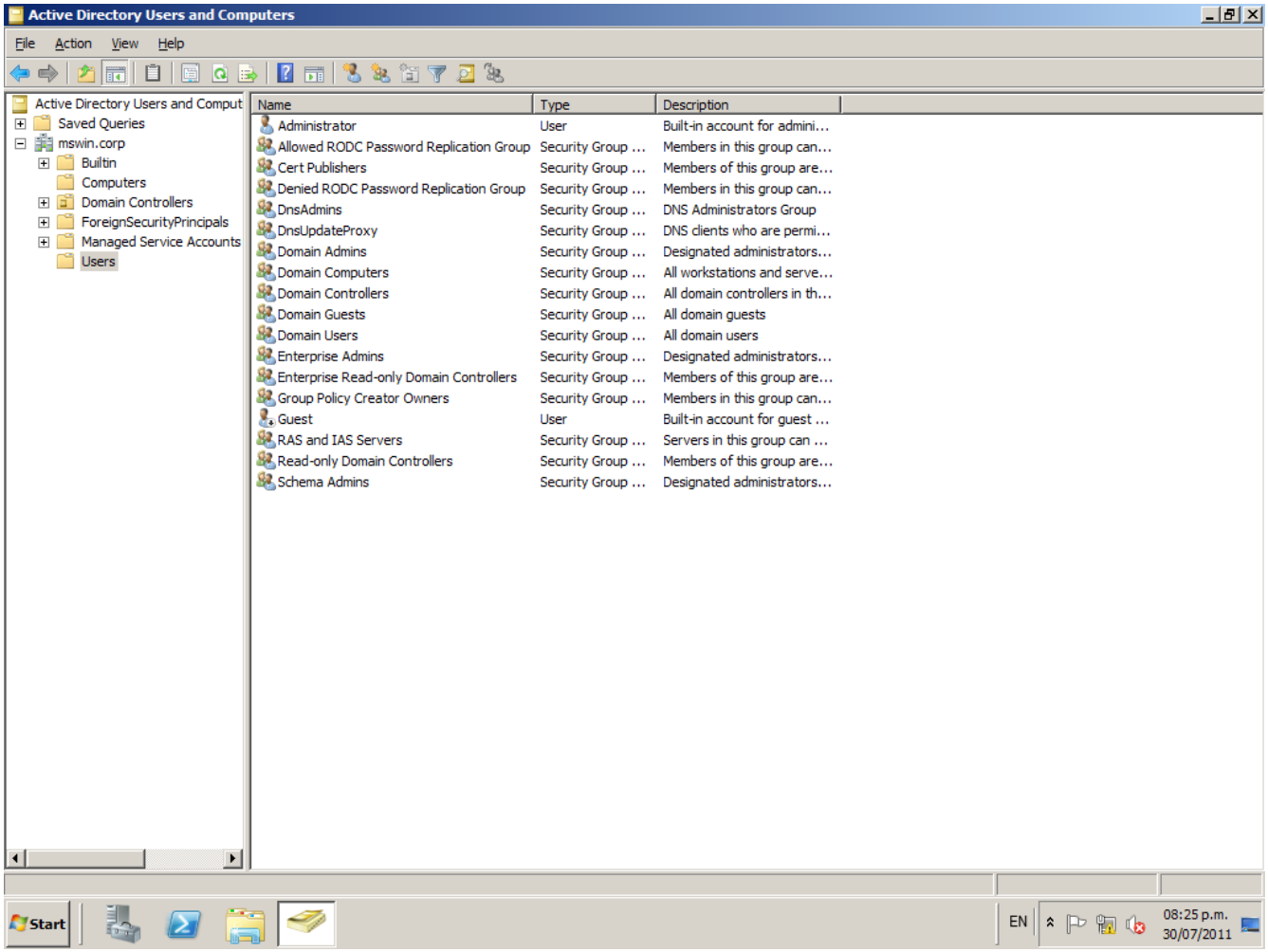
2) Cambiando la IP de nuestro servidor

2.1) Para cambiar la IP de nuestro servidor, debemos acceder a las propiedades del adaptador de red. Para ello, hacemos un clic en el icono de red tal como se muestra en la siguiente imagen, y seleccionamos "Open Network and Sharing Center"



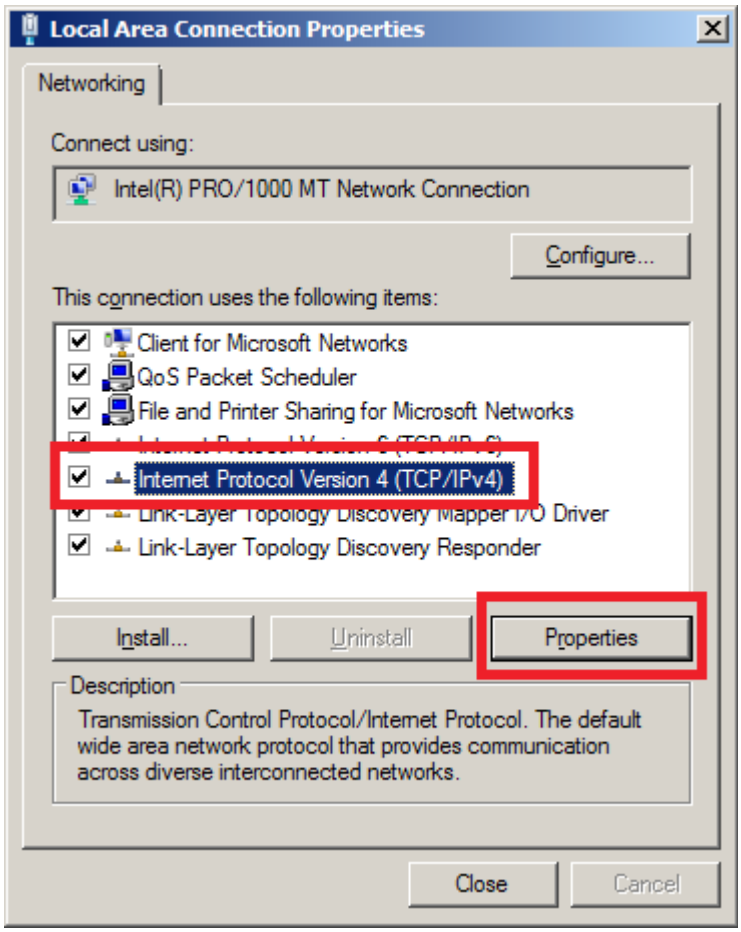
2.2) Luego en la ventana de **Network and Sharing Center**, seleccionamos "**Change adapter settings**"



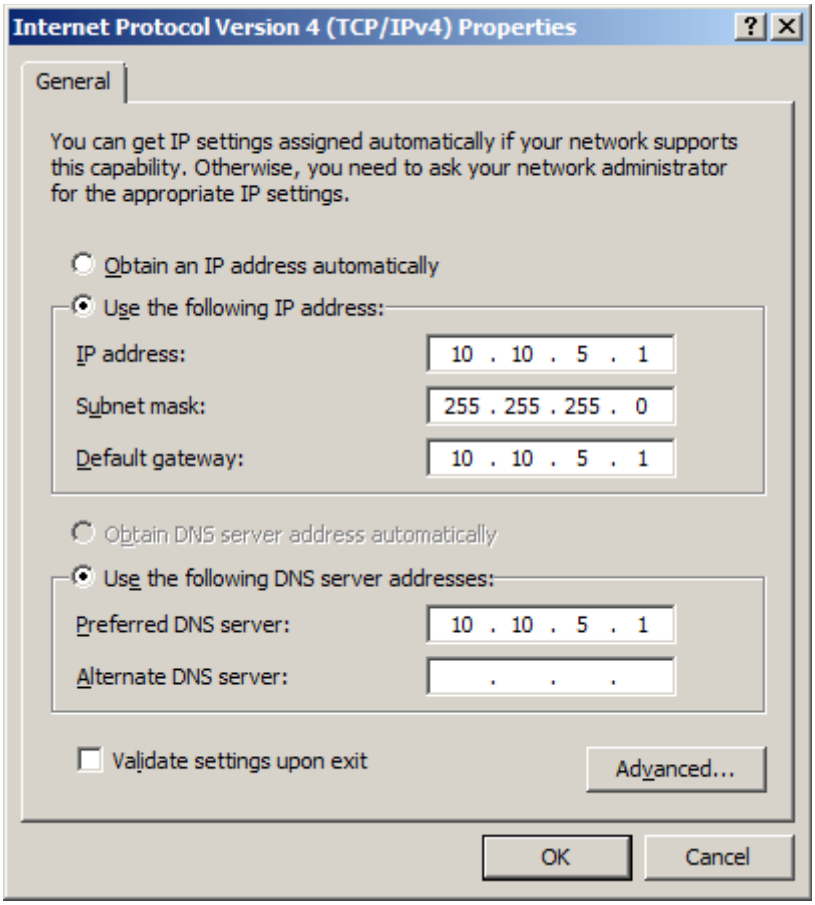


2.3) En este paso, debemos seleccionar el protocolo "**Internet Protocol Version 4 (TCP/IPv4)**" y apretar en el boton de **Properties.**

2.4)

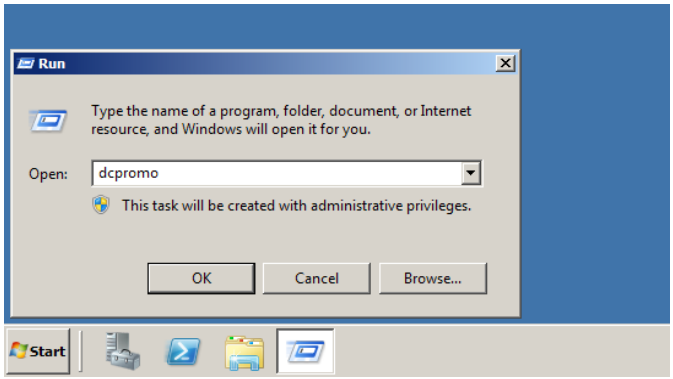


2.4) Ahora debemos ingresar la IP correspondiente para nuestro servidor como así también la Subnet Mask, el Default Gateway y el DNS Primario. Estos últimos dos ítems, llevan la misma IP que nuestro servidor. En el caso del DNS es debido a que nuestro primer servidor de AD también será nuestro primer DNS, servicio básico para que Active Directory funcione.

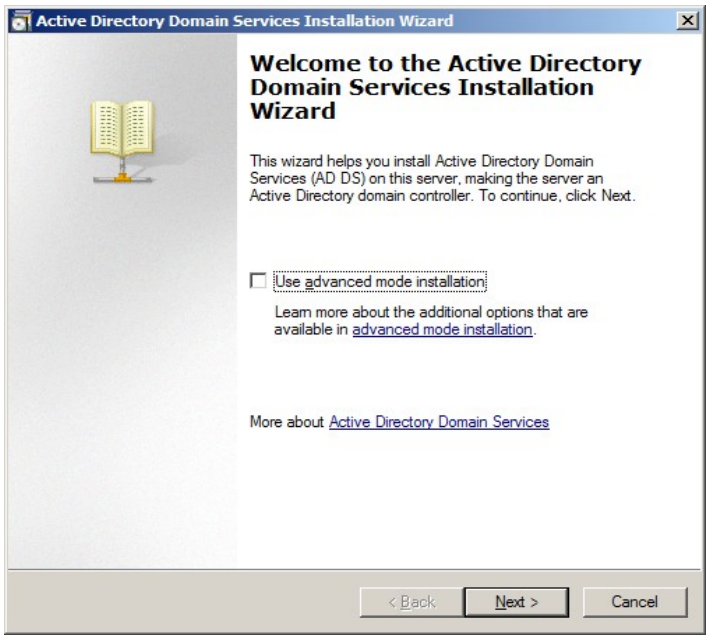


3) Instalando y Configurando Active Directory Domain Services (AD DS) Role

3.1) Una vez que tenemos listo los pasos anteriores, estaremos preparados para iniciar la instalación de nuestro primer Domain Controller. Existen varias formas para poder instalar el rol de AD DS, pero en este caso utilizaremos el comando dcpromo.exe para iniciar el proceso.
Vamos a Start – Run y en Open escribimos dcpromo y luego hacemos un clic en Ok.
Luego debemos esperar a que se instalen los archivos necesarios para poder comenzar con el proceso.



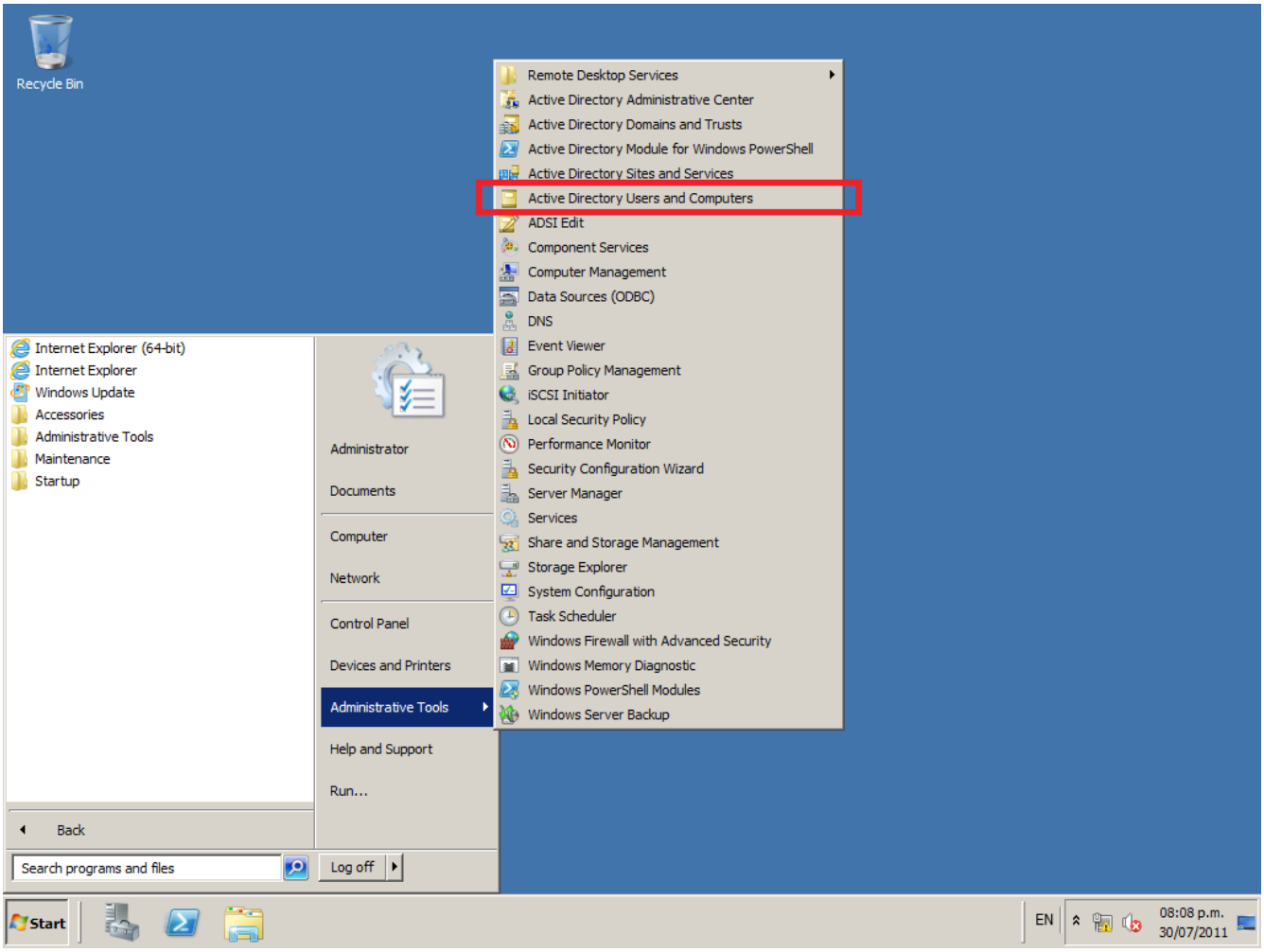
3.2) Ahora veremos que se abre el "Active Directory Domain Services Installation Wizard", donde nos dará la opción de usar el modo avanzado de instalación el cual no utilizaremos en este caso. Para avanzar tan solo apretamos en Next.

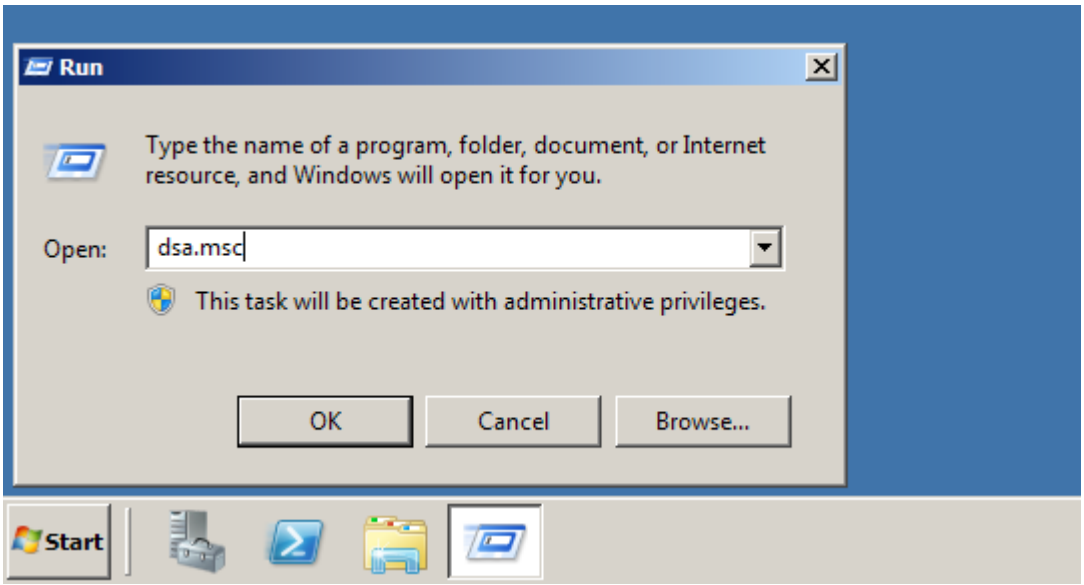


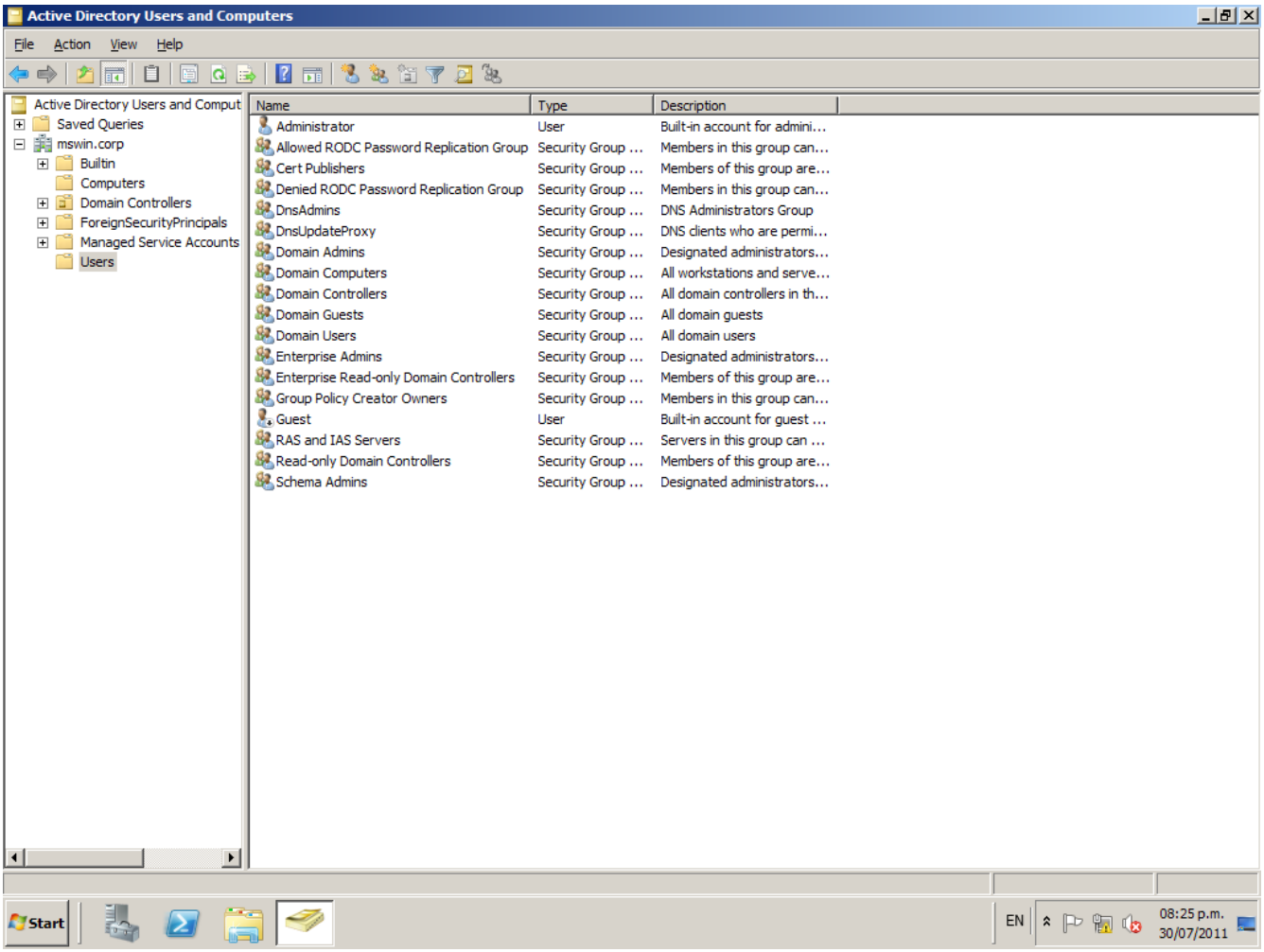
4) Tareas posteriores a la instalación del rol AD DS

4.1) Lo primero que debemos hacer luego del reinicio es iniciar sesión en el dominio y revisar en el Event Viewer los eventos y chequear que éstos no tengan relevancia alguna. En caso de tener eventos importantes debemos proceder con la solución de los mismos.

4.2) Otra de las cosas que podemos hacer es iniciar la consola de Active Directory Users and Computers desde donde administraremos los objetos tales como Usuarios, Grupos y equipos entre otros. Para iniciar dicha consola podremos hacerlo desde Start – Administrative Tools y allí seleccionamos Active Directory Users and Computers. Otra forma de hacerlo mas rápidamente es desde Start – Run y allí escribimos dsa.msc y le damos Enter.


Recycle Bin
Remote Desktop Services
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Data Sources (ODBC)
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy
Performance Monitor
Security Configuration Wizard
Server Manager
Services
Share and Storage Management
Storage Explorer
System Configuration
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell Modules
Windows Server Backup
Internet Explorer (64-bit)
Internet Explorer
Windows Update
Accessories
Administrative Tools
Maintenance
Startup
Administrator
Documents
Computer
Network
Control Panel
Devices and Printers
Administrative Tools
Help and Support
Run...
Back
Search programs and files
Log off
Start
EN
08:08 p.m.
30/07/2011


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
dsa.msc
This task will be created with administrative privileges.
OK
Cancel
Browse...
Start


Active Directory Users and Computers
File Action View Help
Active Directory Users and Comput
Saved Queries
mswin.corp
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Name Type Description
Administrator User Built-in account for admini...
Allowed RODC Password Replication Group Security Group ... Members in this group can...
Cert Publishers Security Group ... Members of this group are...
Denied RODC Password Replication Group Security Group ... Members in this group can...
DnsAdmins Security Group ... DNS Administrators Group
DnsUpdateProxy Security Group ... DNS clients who are permi...
Domain Admins Security Group ... Designated administrators...
Domain Computers Security Group ... All workstations and serve...
Domain Controllers Security Group ... All domain controllers in th...
Domain Guests Security Group ... All domain guests
Domain Users Security Group ... All domain users
Enterprise Admins Security Group ... Designated administrators...
Enterprise Read-only Domain Controllers Security Group ... Members of this group are...
Group Policy Creator Owners Security Group ... Members in this group can...
Guest User Built-in account for guest ...
RAS and IAS Servers Security Group ... Servers in this group can ...
Read-only Domain Controllers Security Group ... Members of this group are...
Schema Admins Security Group ... Designated administrators...
Start
EN
08:25 p.m.
30/07/2011