TEMA 7: WINDOWS SERVER

WINDOWS SERVER.

Ya hemos visto en el tema anterior un sistema operativo cliente, vamos a estudiar ahora un sistema operativo servidor. En concreto vamos a tratar en este tema un sistema operativo servidor de la familia Windows, el Windows Server.

Windows Server es un sistema operativo de tipo servidor, preparado para gestionar una red de ordenadores mediante un sistema de dominios y un directorio activo que permite una administración centralizada. Antes de comenzar es interesante conocer algunos aspectos básicos sobre las técnicas de redes de ordenadores.

INTRODUCCIÓN A LAS TÉCNICAS DE RED.

Hemos visto en el tema sobre Windows cliente como estos clientes trabajan en una red entre iguales, usando los grupos de trabajo. Sin embargo este tipo de solución sólo es válida para redes simples.

En la actualidad hay un número creciente de redes que no son simples. Incorporan servidores múltiples (archivos, impresión, correo, web, etc.) y a menudo están distribuidos en diversas ubicaciones, y no es posible en este tipo de redes ir repitiendo cuentas de usuarios en distintos equipo y se hace necesario mayores posibilidades de Administración.

Asimismo, lo más frecuente en una red de este tipo es que los servidores almacenen muchos gigabytes de datos en distintos recursos. No es realista esperar que bajo estas circunstancias los usuarios sepan dónde están las cosas y sean capaces de manejarlas por ellos mismos recordando las direcciones IP o los nombres de cada máquina que comparte algo.

Es evidente además que en una red de este tipo necesitamos un sistema de control, ya que no todos los usuarios deben poder acceder a todos los recursos. Además, la administración de una red tan grande en un grupo de trabajo es realmente complicada.

Por ello, los diseñadores de redes han buscado la manera de simplificar el uso de este tipo de redes complejas y facilitar la ubicación de los recursos de cara a los usuarios. En este punto vamos a presentar varias técnicas que se usan para lograr esta simplificación, y vamos a profundizar en las especificaciones de Microsoft, basada en dominios y relaciones de confianza. Estos bloques de construcción permiten armar redes empresariales que resulten fáciles de manejar a los administradores y de utilizar para los usuarios.

Una LAN (Local Área Network, red de área local) puede ofrecer servicios de muy diversas maneras dependiendo del método empleado por la red. En esta sección haremos una revisión de las técnicas que han sido utilizadas para organizar los recursos en red:

- Servicios individuales.
- Grupos de trabajo.
- Servicios de directorio. (LDAP).

SERVICIOS INDIVIDUALES.

La gran mayoría de las primeras redes incorporaban un solo servidor, de manera que los usuarios tenían poca dificultad para ubicar archivos, impresoras u otros recursos compartidos. Todo estaba situado en el servidor central, y los equipos individuales no podían compartir absolutamente nada con el resto de la red.

NetWare ha sido el sistema operativo para redes dominantes en redes pequeñas. Estas redes incluyen sólo un servidor y 30 o menos estaciones de trabajo normalmente.

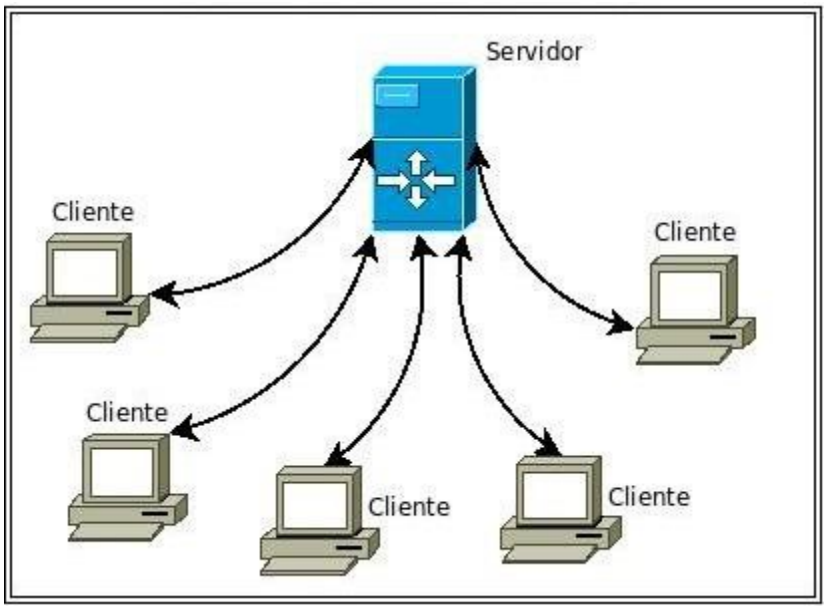
Con este sistema no se requiere un sofisticado servicio de administración de recursos, dado que todos los recursos que se comparten están conectados directamente al servidor.

Sin embargo, agregar un segundo servidor puede complicar las cosas de manera significativa. El problema surge porque cada servidor individual mantiene su propia lista de usuarios y recursos. Veamos un ejemplo:

El servidor A da alojamiento a aplicaciones como documentos de texto y hojas de cálculo; el servidor B aloja el correo electrónico de la compañía, las aplicaciones de contabilidad y la base de datos de ventas. Los usuarios que requieren acceso a la base de datos y utilizar las aplicaciones, necesitan una cuenta en ambos servidores, y deben cerrar e iniciar sesión cada vez que deseen cambiarse de servidor.

Los usuarios también tienen un problema con los diversos servidores individuales. Para usar una impresora, el usuario debe saber cuál servidor tiene la impresora. Para tener acceso a un archivo o programa, el usuario debe conocer cuál servidor lo aloja. A menos que el usuario obtenga herramientas amigables para ubicar los servicios, sería difícil tener acceso a muchas de las capacidades de la red.

Este tipo de redes siguen siendo muy adecuadas en situaciones simples, donde solo existe un servidor y tiene unas funciones muy delimitadas, aunque es una solución no válida para la mayoría de las situaciones actuales, lo que ha hecho que hayan quedado obsoletas.



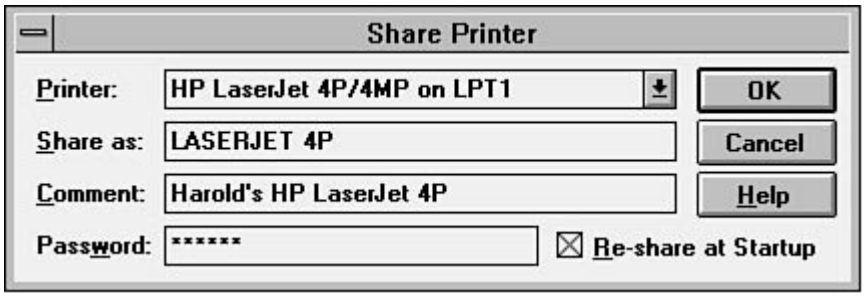
GRUPOS DE TRABAJO.

Los grupos de trabajo son conceptualmente opuestos a los servicios individuales. Los servicios individuales son formales y están administrados centralmente en un único servidor; los grupos de trabajo son informales y operados por los usuarios que comparten sus propios recursos locales y no cuentan con ningún servidor. Este tipo de redes se conocen como redes peer to peer, entre pares o entre iguales (y no punto a punto).

Las redes entre iguales se topan con dos problemas en las grandes organizaciones; hay tantos recursos disponibles que los usuarios pueden tener problemas para su localización y los usuarios no disponen de un método fácil para compartir los recursos sólo con un grupo limitado de compañeros.

Microsoft introdujo los grupos de trabajo con el producto Windows for Workgroups (WfW). WfW permite a los usuarios compartir los recursos de su estación de trabajo y los grupos de trabajo facilitan el establecimiento de grupos relacionados que pueden ver y compartir recursos entre ellos.

Después de que alguien se anexa a un grupo de trabajo, tiene acceso a todos los recursos compartidos en ese grupo. Podemos compartir una impresora local, simplemente indicando que queremos compartirla, y si acaso, poniendo una contraseña en dicho recurso compartido. La figura siguiente muestra la forma en que WfW utilizaba para compartir impresora.



Es importante notar que la ventana en la figura anterior permite al propietario de la impresora asignar una contraseña que puede ser utilizada para restringir el acceso a sólo ciertos individuos. Si no existiera la contraseña, cualquier miembro del grupo de trabajo podría utilizar la impresora. Esta es la única seguridad ofrecida por WfW.

Para localizar los recursos en una red, Microsoft utiliza el propio explorador de archivos.

Los grupos de trabajo hacen que el compartir recursos sea una operación muy simple, pero no organizan los servicios en ninguna lista o directorio. Tampoco facilitan la administración de los recursos compartidos de manera eficiente. Las contraseñas pueden ser utilizadas para restringir el acceso a los recursos, pero con una contraseña para cada recurso, éstas proliferan con rapidez. Para cambiar una contraseña debe notificarse a todos los que utilizan dicho recurso. Si cada recurso tiene una contraseña diferente, las cosas se vuelven realmente complicadas. Es difícil mantener un buen nivel de seguridad bajo tales circunstancias.

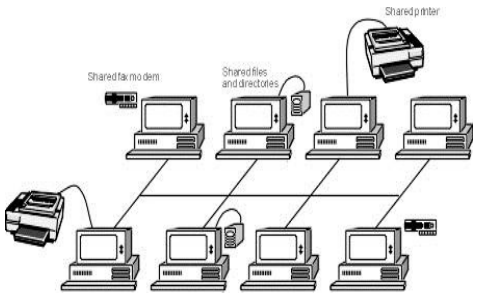
Cuando diferentes contraseñas son asignadas para usuarios individuales, la cantidad de contraseñas que un usuario debe recordar se multiplica con rapidez. Para facilitar las cosas, los usuarios tienden a elegir contraseñas fáciles de recordar, pero también tienden a ser fáciles de adivinar.

Para empeorar las cosas, imaginad que la red tiene la capacidad de que pueda accederse desde el exterior, mediante la línea telefónica por ejemplo o por una VPN (red privada virtual) a través de internet y un empleado acaba de irse a trabajar con la competencia. Habrá que cambiar todas las contraseñas de manera que el empleado no pueda llamar y obtener datos. Obviamente, cambiar todas esas contraseñas e informar a todos acerca del cambio será un enorme problema.

También podemos usar los grupos de trabajo, sin tener que establecer contraseñas a los recursos. En su lugar, podemos indicar por cada recurso que usuarios pueden acceder al mismo, pero tenemos el problema que sólo podremos escoger usuarios desde nuestra lista de usuarios locales. Esto implica que si queremos acceder desde la red a un recurso compartido en una maquina Windows cliente, tenemos que conocer (o usar) el nombre de usuario y la contraseña de un usuario local de dicha maquina.

También podemos usar acceso anónimo a los recursos, pero esto implicaría que todos en la empresa podrían acceder al recurso, cosa que habitualmente es indeseable.

Las organizaciones grandes o las que quieren más control sobre sus redes requieren algo más que grupos de trabajo. Por ello, Microsoft ha incorporado el concepto de dominio desde Windows NT Server.



Los grupos de trabajo de Windows utilizan SMB (Server Message Block) como software para la conexión en red. Este software SMB corre sobre otro software conocido como NetBIOS (Network Basic Input Output System), y a su vez NetBIOS estaba diseñado para funcionar sobre el protocolo NetBEUI (NetBIOS Extended User Interface) aunque también existen implementaciones de NetBIOS sobre IPX/SPX y sobre TCP/IP que es la más usada hoy en día. Este software NetBIOS al ser muy antiguo (1984) es un protocolo de red bastante inseguro y sobre todo, tremendamente ruidoso (utiliza mucho el broadcast en red).

Todo este “lio” viene provocado por que ni SMB, ni NETBIOS ni NETBEUI son verdaderos protocolos de red “completos”. Veamos cómo se distribuye este sistema entre las 7 capas ISO de red:

Capa	Descripción Capa	Protocolo
7	Nivel de Aplicación	Redirector (parte de SMB)
6	Nivel de Presentación	SMB
5	Nivel de Sesión	NetBIOS
4	Nivel de Transporte	NetBEUI
3	Nivel de Red	NetBEUI
2	Nivel de Enlace	NDIS + NIC driver
1	Nivel Físico	NIC (Network Interface Card)

SERVICIO DE DIRECTORIO.

Bajo este sistema, los recursos pueden estar situados en varios equipos, tanto servidores como no servidores, pero se recogen todos en una única lista o directorio. Los recursos pueden agruparse de manera lógica en este directorio para hacerlos más fáciles de ubicar. Los usuarios pueden buscar en el directorio la información que desean, ya sea buscando por tipos de impresoras, capacidades de volúmenes compartidos, etc.

Un servicio de directorio es una especie de guía telefónica exhaustiva que permite a usuarios, administradores y aplicaciones acceder a la información existente de todos y cada uno de los usuarios y sistemas de una red con tan sólo pulsar un botón o a través de programas muy simples.

Como servicios de directorios de red, podemos citar:

- Banyan ofrece el servicio de directorio StreetTalk como parte de su sistema operativo para redes VINES.
- X.500 es un estándar internacional para servicios de directorio, aunque su función se centra en la creación de directorios a nivel global y no en redes locales.
- NetWare Directory Services (NDS, Servicios de directorio NetWare) está incorporado dentro de la línea de productos Novell NetWare 4.x. NDS está basada en X.500, aunque no es totalmente compatible con el estándar.
- LDAP. Es el estándar basado en X.500, pero bastante mejorado y simplificado, y que está diseñado para trabajar sin problemas en TCP/IP.

El concepto de un servicio de directorio es atractivo. En lugar de conectarse a diversos servidores, el usuario se conecta a una red y tiene acceso a los recursos de la red a través del servicio de directorio, sin importar cuál servidor ofrezca el servicio. El usuario ve el directorio de la red de una forma lógica, puede acceder a los recursos sin preocuparse de quien comparte dichos recursos, del mismo modo, puede iniciar sesión una única vez en cualquier servidor, y será reconocido automáticamente por todos los servidores.

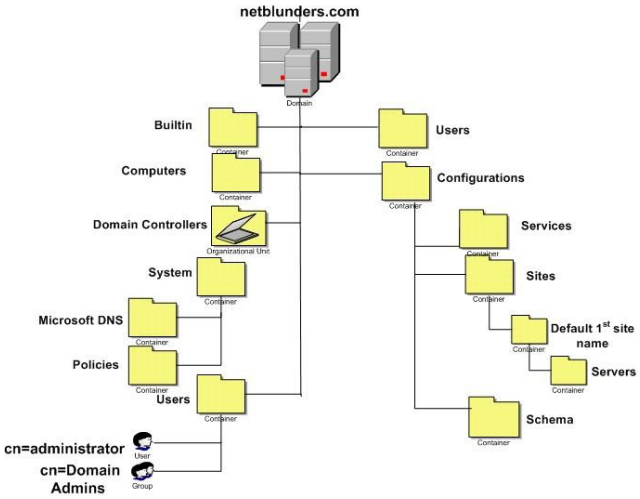
Por su importancia actual, veamos más en profundidad el servicio de directorio LDAP.

LDAP.

LDAP (Lightweight Directory Access Protocol, Protocolo Ligero de Acceso a Directorios) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP se considera muchas veces como una base de datos a la que pueden realizarse consultas, aunque en realidad no es una base de datos como tal.

Un directorio es un conjunto de objetos con atributos organizados en una manera lógica y jerárquica. El ejemplo más común es el directorio telefónico, que consiste en una serie de nombres (personas u organizaciones) que están ordenados alfabéticamente, con cada nombre teniendo una dirección y un número de teléfono adjuntos.

Los despliegues actuales de LDAP tienden a usar nombres de Sistema de Nombres de Dominio (DNS por sus siglas en inglés) para estructurar los niveles más altos de la jerarquía. Conforme se desciende en el directorio pueden aparecer entradas que representan personas, unidades organizacionales, impresoras, documentos, grupos de personas o cualquier cosa que representa una entrada dada en el árbol (o múltiples entradas).



Habitualmente almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc.). A manera de síntesis, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

Existen diversas implementaciones y aplicaciones reales del protocolo LDAP como pueden ser Active Directory (Directorio Activo), Novell Directory Services, IPLanet, OpenLDAP o Red Hat DS.

La implementación que vamos a estudiar en este tema es la de Active Directory, utilizada por Microsoft en sus versiones servidores.

ACTIVE DIRECTORY

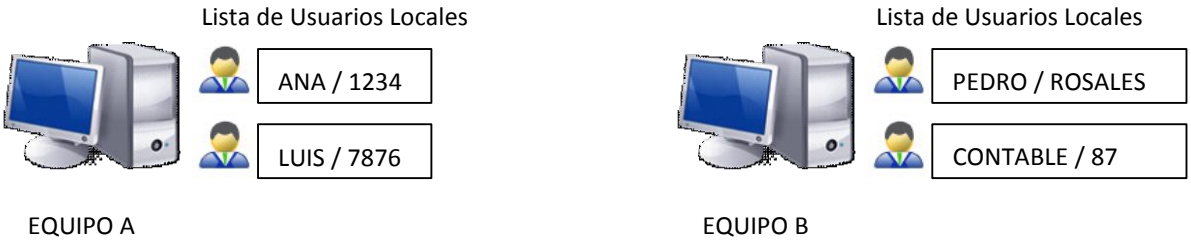
Active Directory es el nombre utilizado por Microsoft (desde Windows 2000) en su servicio de directorio.

Un Servicio de Directorio es un depósito estructurado de la información de los diversos objetos que contiene el Active Directory, en este caso podrían ser impresoras, usuarios, equipos, etc.

Bajo este nombre se encuentra realmente un esquema (definición de los campos que pueden ser consultados) LDAP versión 3, lo cual permite integrar otros sistemas que soporten el protocolo. En este LDAP se almacena información de usuarios, recursos de la red, políticas de seguridad, configuración, asignación de permisos, etc.

ROL DE SERVIDOR. DOMINIO.

Si estamos usando un grupo de trabajo, y compartimos un recurso, al acceder a la lista de usuarios de dicho recurso hemos visto cómo podemos añadir únicamente usuarios locales, de nuestro propio sistema. Esto quiere decir que no podemos compartir uno de nuestros recursos para un usuario que no sea local en nuestro sistema, a menos que dupliquemos la cuenta de usuario en los demás sistemas.

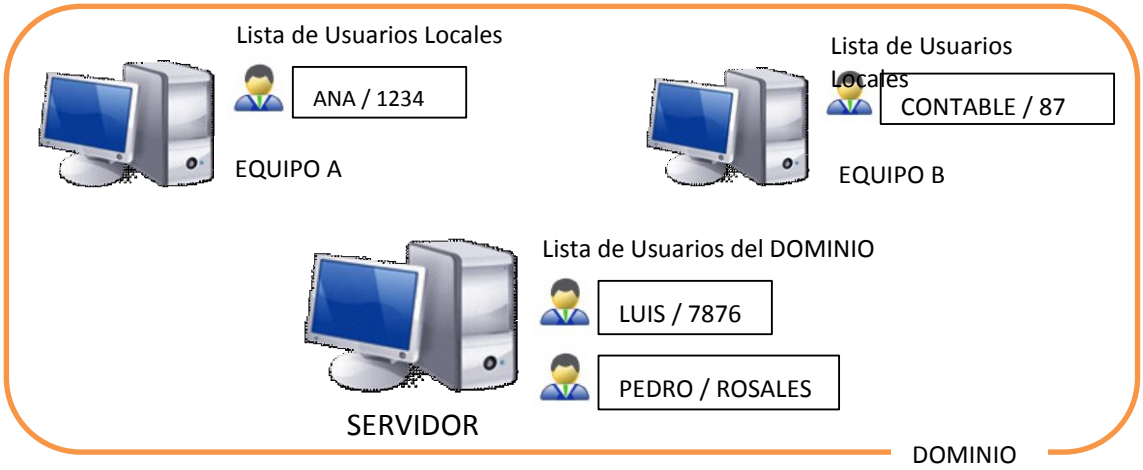


Así, si en el equipo A tenemos un recurso compartido, solo podremos indicar dentro de su ACL, que puede ser usado por ANA (con contraseña 1234) o por LUIS (con contraseña 7876). Si queremos que ese recurso compartido del equipo A sea usado por la cuenta PEDRO del equipo B, no tenemos más remedio que añadir esa cuenta de usuario en el equipo A, para que así PEDRO aparezca en la lista de usuarios locales del equipo A y pueda ser añadido a la lista de acceso del recurso. Obviamente podríamos establecer un acceso anónimo, pero esto no suele ser interesante en una empresa, ya que no es habitual que dejemos un recurso abierto a todo el mundo.

El grupo de trabajo se comporta así porque todas las cuentas de usuario son locales y son almacenadas en cada equipo individual, y al ser una red entre iguales, ningún equipo confía en los demás, por lo que no permite que entre en la maquina un usuario que no esté en su lista de usuarios locales.

Una solución para este problema es crear cuentas globales o comunes, es decir cuentas que no pertenezcan a una sola máquina, sino que sean reconocidas en todas las máquinas de la red.

Para hacer esto, necesitamos establecer un ordenador especial que va a ser el encargado de almacenar todas estas cuentas globales, mientras que las cuentas locales seguirán estando almacenadas en cada equipo normal. Este ordenador especial en el que todos los demás ordenadores confían pasa a ser un servidor y nuestro grupo de trabajo se convierte en un dominio, dado que se ha establecido una relación de dominio de un equipo sobre los demás.



Así conseguimos que la cuenta LUIS no se almacene localmente en el equipo A, sino que sea una cuenta del dominio creada y almacenada en el SERVIDOR del dominio. Ahora, tanto el equipo A como el equipo B cuando vayan a compartir un recurso verán en sus ACL a LUIS, ya que ambos confían en el servidor y por tanto dejan entrar a sus usuarios.

Fijaros como en el grafico anterior vemos que LUIS y PEDRO son usuarios del dominio mientras que los usuarios ANA y CONTABLE son usuarios locales que solo aparecen en las listas de sus propios equipos, y no pueden interactuar con el dominio.

Si queremos trabajar en un dominio, hay que indicar en todos los equipos que dejamos de trabajar en un grupo de trabajo, y queremos conectarnos a un dominio. Podemos decir que los equipos deben decidir dejar de ser “libres” para pasar a ser dominados por el servidor.

Los dominios toman conceptos de los grupos de trabajo y servicios de directorio. Al igual que los grupos de trabajo, los dominios pueden ser bastante informales y cada equipo puede decidir compartir sus propios recursos que estarán disponibles en red al igual que los recursos puestos por el servidor.

Un dominio organiza los recursos de diversos servidores en una estructura administrativa. Los usuarios reciben privilegios de conexión a un dominio más que a un servidor individual. Debido a que un dominio controla los recursos de varios servidores, es más fácil de administrar que una red con muchos servidores individuales.

Los servidores, dentro del dominio, anuncian sus servicios a los usuarios. Los usuarios que se conectan en un dominio obtienen acceso a todos los recursos del dominio para el cual han recibido autorización de acceso, sin importar desde que servidor se conectaron ni que servidor está prestando el recurso.

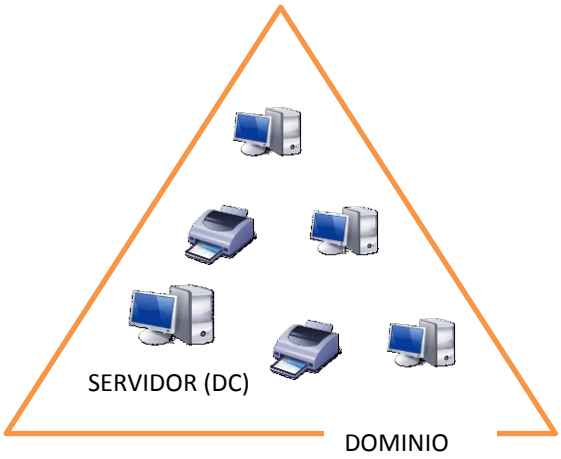
Cuando las redes se vuelven lo suficientemente amplias como para requerir varios dominios, los administradores pueden establecer relaciones de confianza (trust) entre los dominios. Estas relaciones simplifican la administración, ya que un usuario sólo requiere una cuenta en uno de los dominios. Los otros dominios que confían en el dominio de conexión del usuario pueden depender de que el dominio de conexión autentifique dicha conexión.

ACTIVE DIRECTORY (DIRECTORIO ACTIVO).

Active Directory (AD) es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos (como LDAP, DNS, DHCP, Kerberos, etc.). Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

Active Directory (AD) es usado por las versiones de Windows Server NT, Windows 2000 y Windows 2003. Windows 2008 utiliza una nueva versión de AD conocida como Active Directory Domain Servers (ADDS).

Active Directory se basa en el uso de dominios, cada dominio contiene una serie de máquinas clientes, unos recursos y al menos un servidor que domina a los equipos clientes, este servidor se conoce como Controlador de Dominio (Domain Controler, DC).



Podemos agrupar varios dominios formando estructuras de dominios, donde cada uno de estos dominios cuenta con su propio controlador de dominio. Esta agrupación de dominios se realiza de forma anidada, de la misma forma que anidamos carpetas en un volumen de datos. Cada dominio puede tener dominios padres y dominios hijos, y todos los dominios tienen un dominio padre menos el dominio raíz, que es el primero de todos.

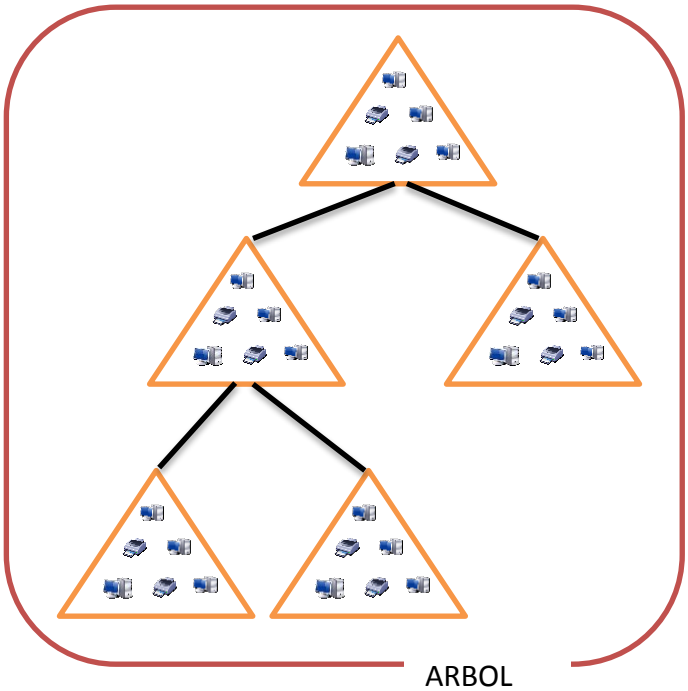
Esta estructura de dominios anidados se conoce como árbol.

En este ejemplo de la derecha, vemos un árbol creado con 5 dominios. Cada uno de estos dominios cuenta con un controlador de dominio (DC) como mínimo, sus equipos clientes, sus recursos locales, su infraestructura de red, etc.

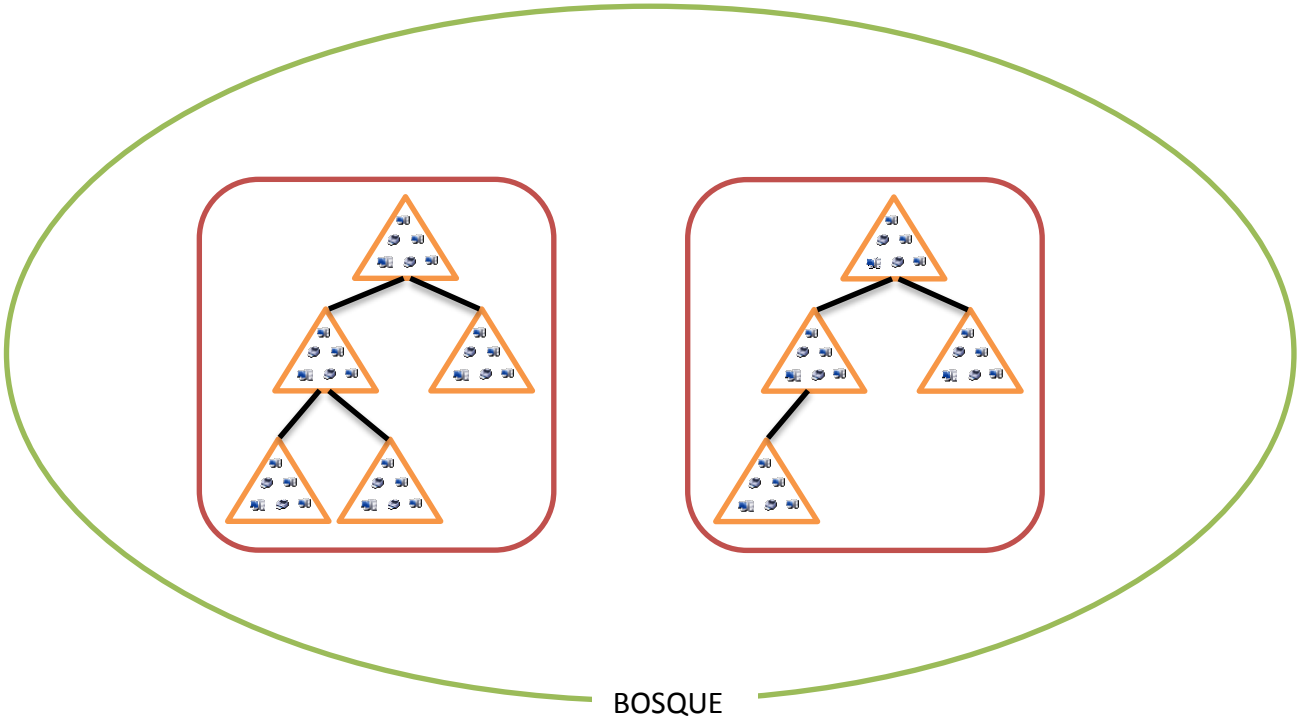
Vemos como el dominio raíz tiene dos dominios hijos, y uno de ellos tiene a su vez dos hijos más.

Al hablar de árbol, podemos decir que el dominio raíz tiene dos ramas, y una de esas ramas tiene a su vez dos ramas más.

Es posible crear una estructura que cuente con más de un árbol, estas estructuras de carácter superior al árbol se conocen como bosque. (Un bosque son varios árboles).

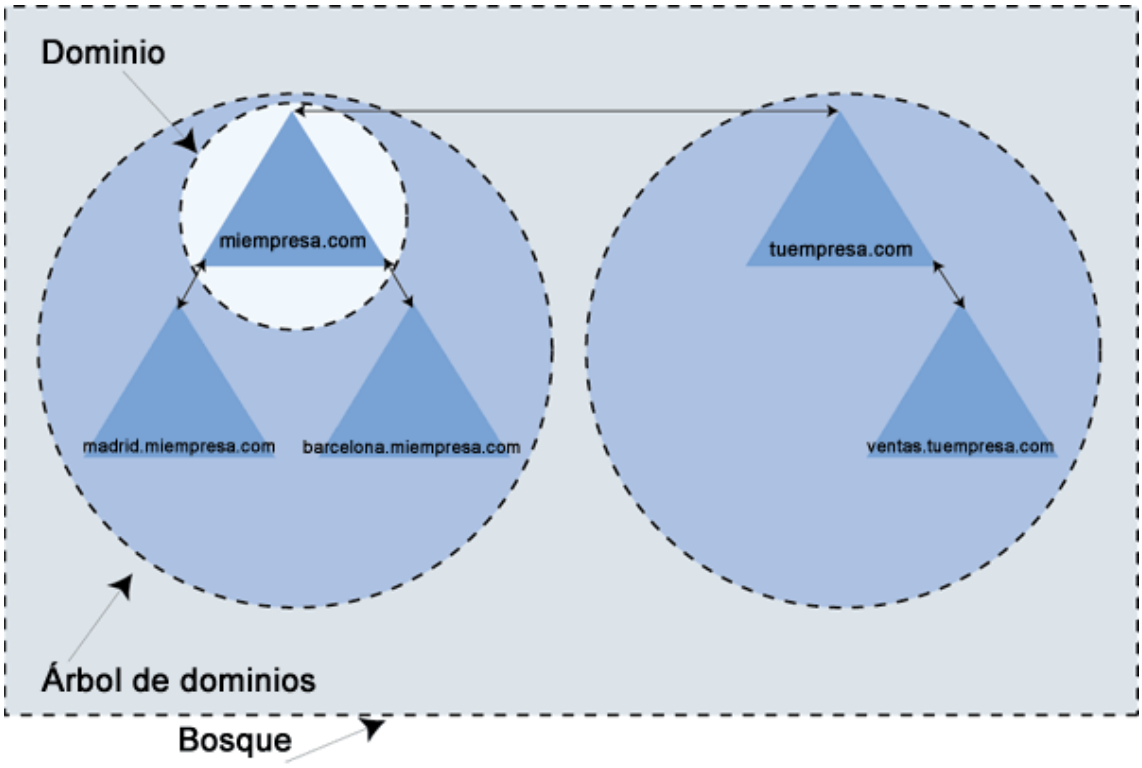


ARBOL



BOSQUE

En este ejemplo vemos un bosque formado por dos árboles, uno con 5 dominios y el otro con 4. Cada uno de estos dominios contará con al menos un DC, por lo que al menos en ese bosque existirán 9 Controladores de Dominio.

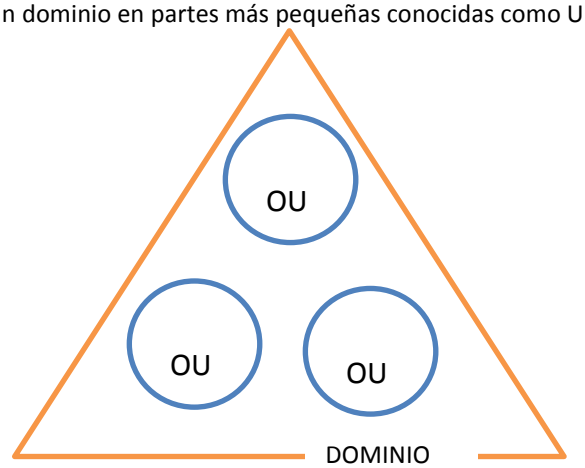


En este ejemplo vemos como hemos unido 5 dominios (miempresa.com, Madrid.miempresa.com, Barcelona.miempresa.com, tuempresa.com y ventas.tuempresa.com).

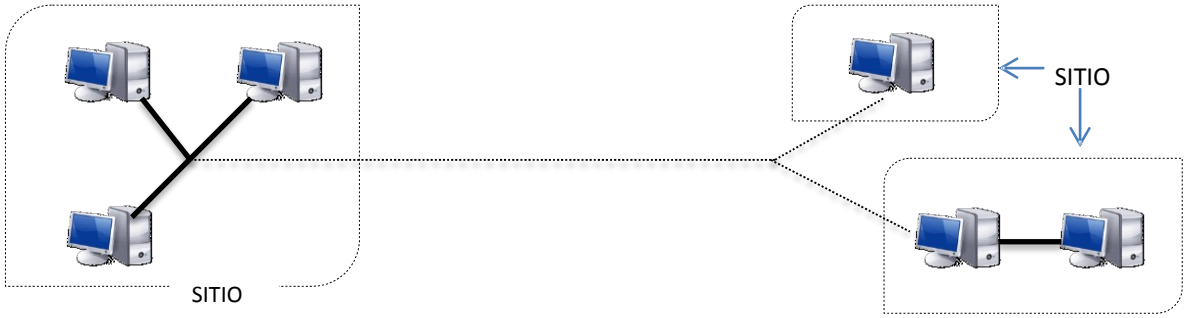
Cada uno de estos dominios contará como mínimo con un controlador de dominio Windows Server, y un gran número de máquinas clientes conectados. Para realizar esto en Windows Server sólo hemos tenido que crear miempresa.com (nombre de dominio) como dominio raíz de un árbol de dominios. Madrid.miempresa.com y Barcelona.miempresa.com se han montado como dominios que cuelgan de la raíz del árbol de dominios formado por miempresa.com.

Hemos creado otro dominio tuempresa.com que forma una raíz de árbol, y hemos colgado el dominio ventas.tuempresa.com de la raíz tuempresa.com.

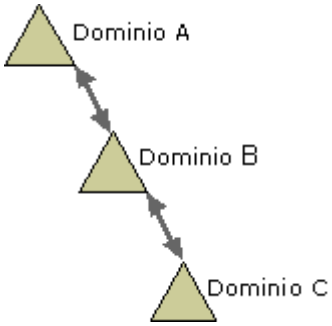
Hemos visto como la estructura que podemos crear usando Active Directory se forma con un bosque, que a su vez se divide en árboles, los cuales se dividen en dominios. Para facilitar la administración podemos a su vez dividir un dominio en partes más pequeñas conocidas como Unidades Organizativas (OU).



Estas divisiones que hemos visto hasta ahora son divisiones “lógicas”, es decir, no tienen en cuenta donde están situados los equipos físicamente. AD también nos permite crear estructuras de equipos “bien conectados”, es decir, equipos que tienen un gran ancho de banda entre ellos. Estas divisiones se conocen como sitios.

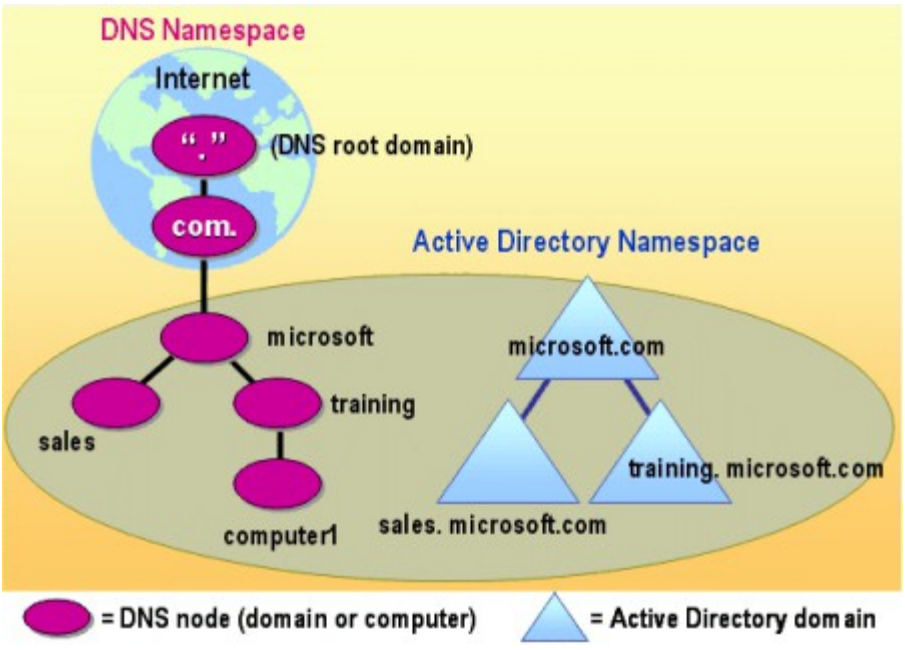


Hemos indicado anteriormente que todos los equipos de un dominio confían totalmente en el controlador de dominio o servidor de ese mismo dominio. Cuando montamos un árbol, tenemos varios dominios interactuando entre ellos, así que tenemos que indicar que dominios confían en que dominios, o lo que es lo mismo, establecer relaciones de confianza entre los dominios. Por defecto, en los Windows Server posteriores al Windows 2000 se establecen relaciones de confianza biunívocas entre todos los dominios, de modo que todos los DC confían en todos los demás DC. Estas relaciones de confianza pueden ser modificadas si nos interesan.



Si queremos que los usuarios del dominio B puedan acceder a los recursos del dominio A, tendremos que hacer que el dominio A confié en el dominio B.

Active Directory está estrechamente relacionado con el protocolo DNS, de modo que cuando creamos un árbol AD estamos creando al mismo tiempo un árbol DNS. Esto es importante recordarlo ya que al mismo tiempo que configuramos AD estaremos configurando DNS.



INSTALACIÓN DE ACTIVE DIRECTORY EN WINDOWS 2008.

Para instalar Active Directory primero debemos configurar el Servicio de Dominios en el equipo servidor, y para ello debemos realizar los siguientes pasos:

1) En la ventana Administrador del Servidor hacemos clic en Agregar Funciones. También podemos es válida la opción Agregar Roles.
2) Seleccionamos el elemento Servicios de Dominio de Active Directory.

3) Hacemos clic en Siguiente.
4) Para confirmar que se desea instalar funciones, servicios o características hacemos clic en Siguiente.
5) Confirmamos los servicios seleccionados y hacemos clic en Instalar.
6) Se mostrará por pantalla el progreso de la instalación. Esperamos.
7) Una ventana nos indicará que el Servicio de Dominio de Active Directory se ha instalado correctamente, y que ahora podemos instalar un Controlador de Dominio. Hacemos clic en cerrar.

Con estos pasos no habremos creado ningún dominio, simplemente hemos preparado nuestro Windows Server 2008 para que a partir de ahora pueda empezar a trabajar con los dominios.

Este paso no era necesario en Windows Server 2003 y anteriores, dado que estos sistemas operativos traían instalado por defecto estos servicios de dominio de Active Directory.

INSTALAR EL PRIMER CONTROLADOR DE DOMINIO.

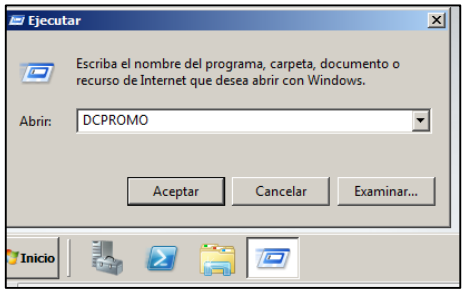
Una vez instalado los ADDS (Servicios de Dominio de Active Directory) podemos empezar a crear controladores de dominio. Para ello, debemos realizar una promoción de un equipo a Controlador de dominio utilizando el comando **DCPROMO**.

Antes de realizar esta promoción a CD, debemos revisar algunos requisitos previos:

1) Se debe iniciar sesión en el servidor con un usuario con privilegios de administrador.

2) Debemos tener claro que tipo de instalación vamos a realizar:
   a. un controlador de dominio para un dominio nuevo
   b. un controlador de dominio adicional que ayude al controlador de dominio principal ya creado.
   c. Vamos a crear un árbol nuevo o a colgar de un árbol ya existente
   d. Vamos a crear un bosque nuevo, o vamos a ser la raíz de un árbol en un bosque ya existente
3) Debemos tener configurados los dispositivos de red y comprobar que tenemos conexión.
4) Debemos contar una dirección IP estática, nunca debemos instalar un CD con una dirección IP dinámica.
5) Debemos tener suficiente espacio en el volumen de datos donde vayamos a instalar la base de datos del AD.
6) Debemos asegurarnos del nombre de nuestro equipo, usando un nombre corto siempre que sea posible.

Una vez comprobados todos estos puntos, estamos en disposición de realizar la promoción de nuestro Windows 2008 a Controlador de Dominio, para ello ejecutamos el comando CDPROMO y pulsamos

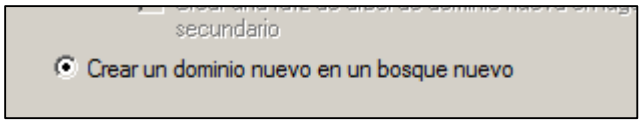


Intro.

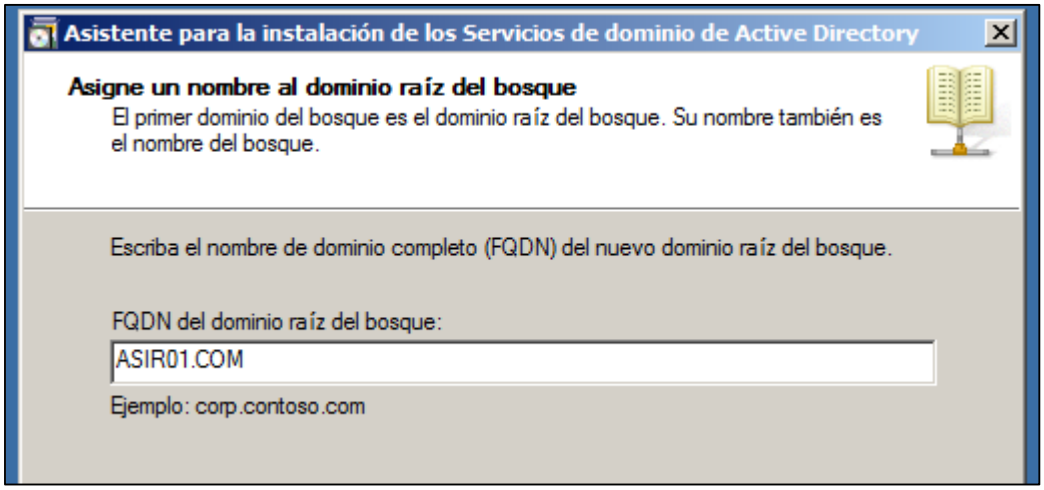
1) Se iniciará el asistente, debemos activar la casilla Usar la instalación en modo avanzado. Hacemos clic en siguiente.

2) Nos mostrará el sistema un aviso de Compatibilidad de sistema operativo, indicando que algunas aplicaciones y servicios puede que no funcionen adecuadamente. Hacemos clic en siguiente.

3) Seleccionamos crear un dominio nuevo en un bosque nuevo y hacemos clic en siguiente.

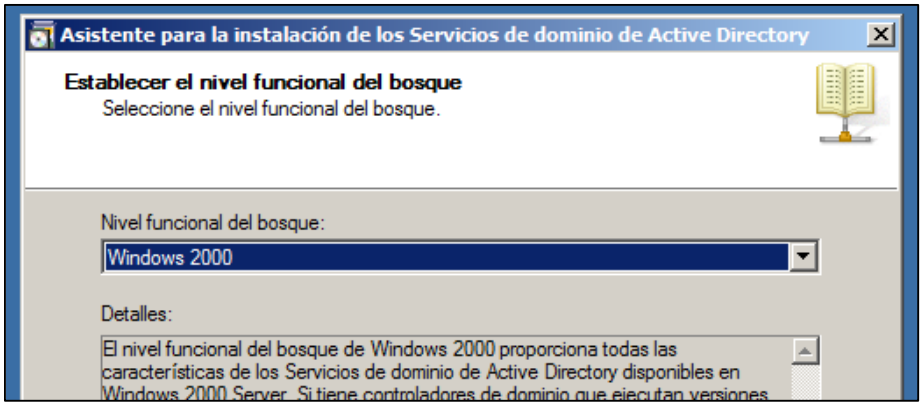


4) Definimos el nombre DNS para el dominio raíz del bosque, en nuestro caso asignaremos el ASIR01.COM (ASIR, el número del ordenador de clase con dos dígitos, y punto com al final). Hacemos clic en siguiente.



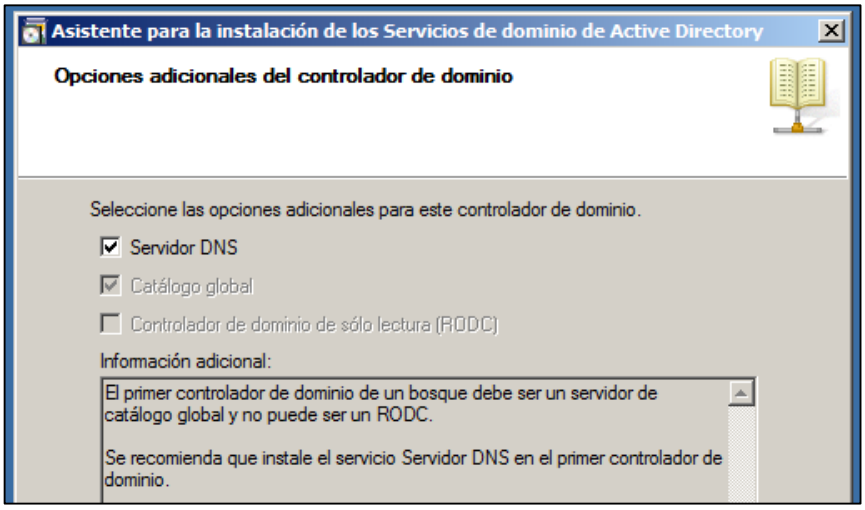
5) Asignamos el nombre NetBIOS que permitirá identificar al dominio en equipos con versiones anteriores de Windows, especialmente Windows 98 y Windows NT. Dejamos el que nos propone por defecto y pulsamos siguiente.

6) Seleccionamos el nivel de funcionamiento del bosque, el cual definirá la compatibilidad de nuestro AD. Seleccionamos Windows 2000.

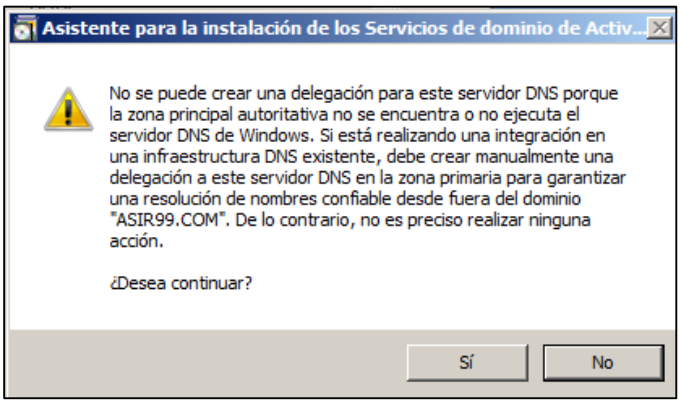


7) Seleccionamos el nivel de funcionamiento del dominio. Seleccionamos Windows 2000 nativo.

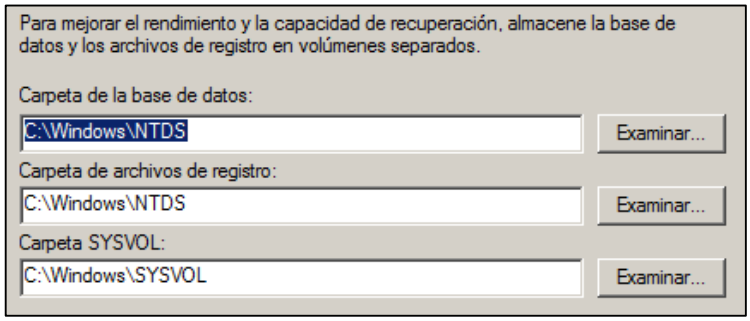
8) Uno de los requisitos para AD es que el Controlador de Dominio raíz del árbol también tenga instalado el servidor DNS que se va a utilizar en todo el árbol. Debemos indicar que deseamos instalarlo.



9) Debido a que aún no está instalado el servidor DNS, recibiremos un mensaje de advertencia. Hacemos clic en Sí.

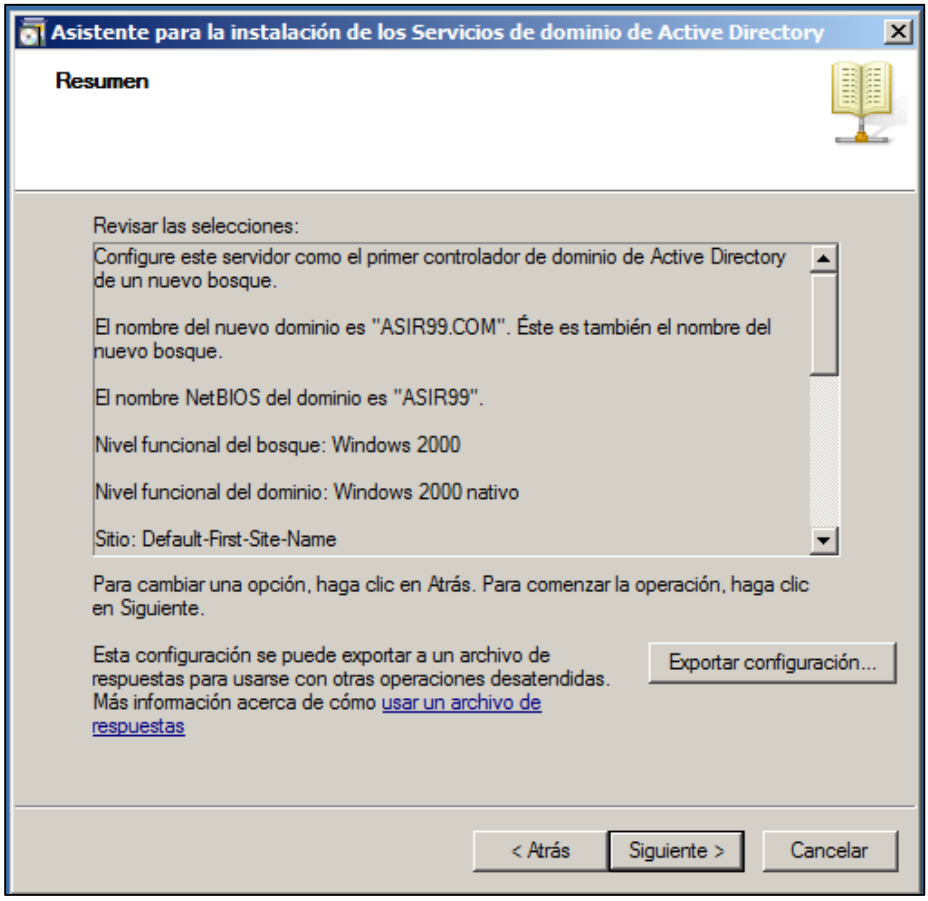


10) AD guarda su base de datos NTDS en una carpeta, y la carpeta pública SYSVOL donde se almacenarán todos los perfiles en otra. El sistema nos preguntará donde deseamos crear dichas carpetas. Lo ideal sería colocarlas en discos duros distintos, para que pudieran accederse a ellas más rápidamente. Nosotros dejamos las opciones por defecto.



11) Por si se produce un fallo en el Servicio de Directorio, Windows Server cuenta con un modo de acceso especial conocido como modo de restauración del servicio de directorio. El sistema procederá en este momento a pedirnos la contraseña que deseamos usar para tal restauración. Recomiendo utilizar la misma contraseña que le vamos a asignar al administrador del Dominio.

12) Ahora se nos presenta una pantalla de resumen. Aquí podemos exportar la configuración a un archivo para futuras instalaciones. Hacemos clic en siguiente.



13) El sistema procederá a copiar, instalar y configurar los archivos para que funcionen los servicios de DNS y AD. Esperamos (a veces, un rato largo).

14) Nos aparecerá un cuadro indicando que se ha finalizado el asistente. Reiniciamos el equipo para que los cambios surtan efecto, y nuestro servidor se haya transformado en un Controlador de Dominio. Es muy normal que este primer inicio del CD tarde algo de tiempo, ya que tiene que aplicar una gran cantidad de configuraciones y debe hacer un examen exhaustivo de la red local.

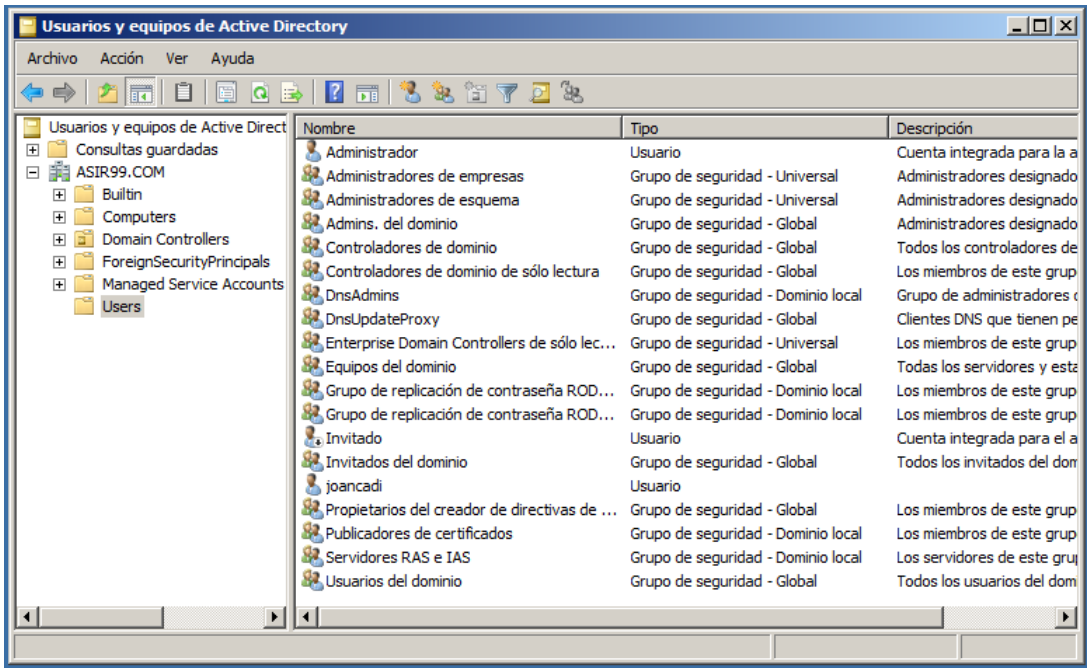
A partir de este momento, cada vez que abramos sesión en ese equipo, usaremos una cuenta de usuario del dominio. Vemos en la imagen de la derecha como el usuario que va a abrir sesión es el Administrador del Dominio ASIR99. Esto en Windows Server se representa como vemos con Nombre del Dominio, contra barra, nombre de la cuenta del usuario.

No podremos usar los usuarios que teníamos en el equipo Windows 2008 anteriormente (que eran cuentas locales). En un Controlador de Dominio, solo se pueden usar cuentas del dominio.

ACCESO A LAS HERRAMIENTAS PARA GESTIONAR EL ACTIVE DIRECTORY.

Una vez completado el punto anterior (DCPROMO) habremos promocionado nuestro servidor a Controlador de Dominio, y habremos creado nuestro bosque y nuestro árbol. Veamos ahora desde donde podemos administrar nuestro Active Directory.

1) Hacemos clic en Inicio, Todos los programas, Herramientas Administrativas.
2) Veremos que existen una gran cantidad de programas en estas Herramientas Administrativas. Cada uno de dichos programas es una consola de administración de AD.
3) Hacemos clic en la consola (MMC, Microsoft Management Console) Usuarios y Equipos de Active Directory.
4) Desde esta consola podemos agregar usuarios, equipos, etc. en el dominio.

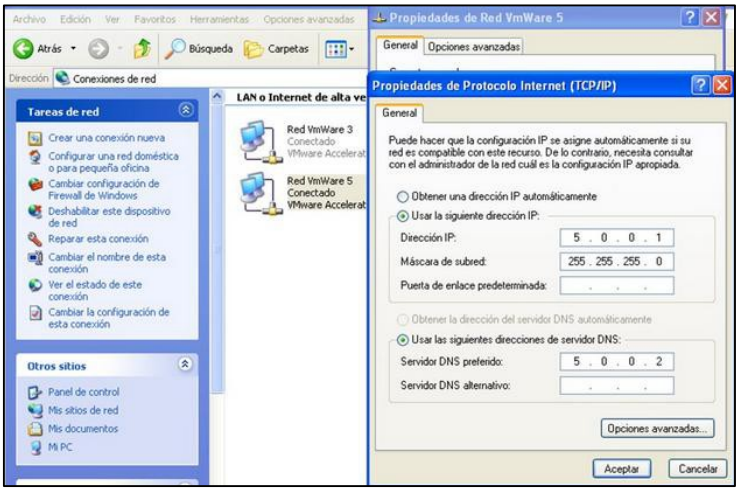


CONEXIÓN DE CLIENTES AL DOMINIO.

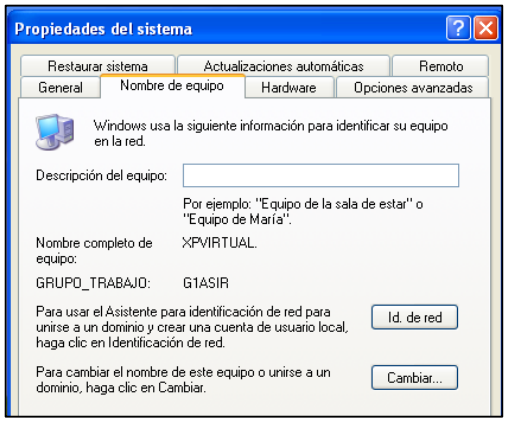
Para comprobar si nuestro recién estrenado dominio funciona correctamente, vamos a añadir a nuestro servidor algunos clientes. Para ello, debemos tener en red local algunos equipos con un sistema operativo que permita conexión a dominios (en la actualidad, prácticamente todos) e indicarles que pasen a trabajar dentro del dominio.

Veamos cómo hacerlo en un Windows XP:

1) En primer lugar tenemos que indicar a nuestro Windows XP que utilice el servidor DNS que ha montado nuestro dominio. En nuestro ejemplo, en las propiedades de Red de XP debemos indicar que use como servidor DNS único la dirección IP de nuestro Controlador de Dominio.

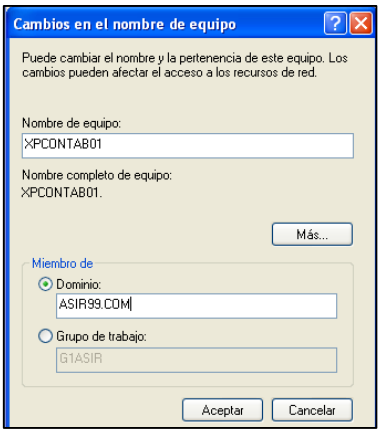


2) Accedemos propiedades del sistema (Windows + Pausa) y desde allí a la pestaña Nombre de equipo.

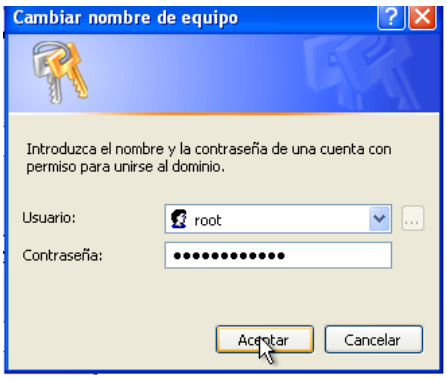


3) Vemos como nos indica la pantalla que para unirnos a un dominio hagamos clic en Cambiar.

4) Desde aquí ponemos un nombre al equipo adecuado y a continuación escribimos el nombre FQDN (nombre DNS) del dominio al que queremos conectarnos y le damos clic a Aceptar. (Si nos indica que no encuentra el dominio, revisar el paso 1).



5) XP nos pedirá un nombre de usuario y contraseña para unirnos al dominio. Este usuario debe ser usuario del dominio, creado desde el Controlador de Dominio mediante la consola de Usuarios y Equipos de Active Directory que vimos anteriormente.



6) Si todo funciona bien, recibiremos un mensaje de “Bienvenido al dominio” y nos pedirá que reiniciemos la máquina.

7) A partir de ese momento, podremos iniciar sesión en nuestro XP, tanto de forma individual (usaremos la maquina fuera del dominio con sus usuarios locales), como formando parte del dominio (usando la maquina dentro del dominio con sus usuarios de dominio).

La forma de conectarnos que hemos visto es la del Windows XP pero es prácticamente idéntica a la forma en que se conectan todos los sistemas operativos Windows. La forma de conexión de máquinas con sistemas operativos no Windows lo dejamos para más adelante.

Hemos visto como el equipo una vez conectado al dominio tiene la posibilidad de abrir sesión fuera del dominio, abriendo sesión en el propio equipo. Para evitar esto simplemente tenemos que eliminar todas las cuentas de usuario locales del equipo cliente y dejar únicamente la cuenta de administrador local, con una contraseña evidentemente que no conozcan los usuarios de ese equipo. De este modo, obligaremos a que los usuarios solo puedan abrir sesión usando su cuenta de dominio. Por regla general, una vez establecido el dominio todas las personas reciben una cuenta de usuario de dominio, y se evita el trabajar con cuentas locales.

Una de las acciones que se llevan a cabo automáticamente cuando conectamos un equipo a un dominio, es que se integra al grupo “Admins. Del dominio” como miembro del grupo local de la maquina “Administradores”, también se integra al grupo “Usuarios del dominio” como miembro del grupo local de la máquina “Usuarios”. Esto permite que cualquier usuario del dominio es automáticamente usuario de esa máquina, y que cualquier administrador del dominio es automáticamente administrador de esa máquina.

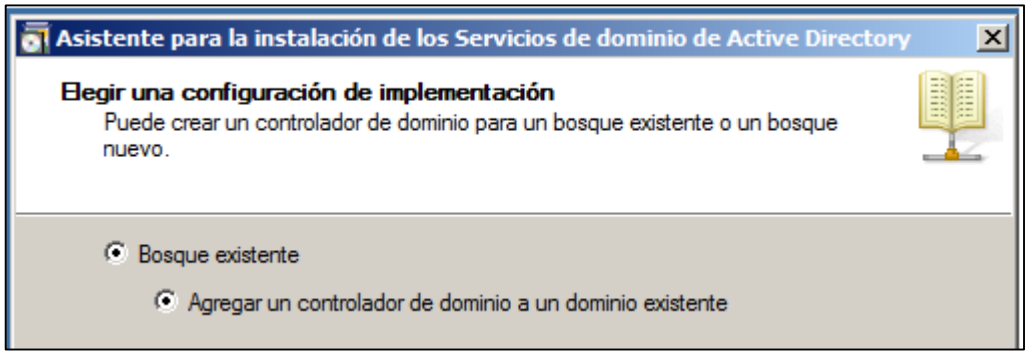
INSTALAR UN CONTROLADOR DE DOMINIO ADICIONAL.

Si tenemos un dominio de gran tamaño con cientos de máquinas conectadas al mismo, no es aconsejable que todo dependa de un único servidor. Un fallo en este equipo sería catastrófico para toda la infraestructura. En casos así, es aconsejable instalar varios servidores, es decir, contar con varios controladores de dominio en un único dominio.

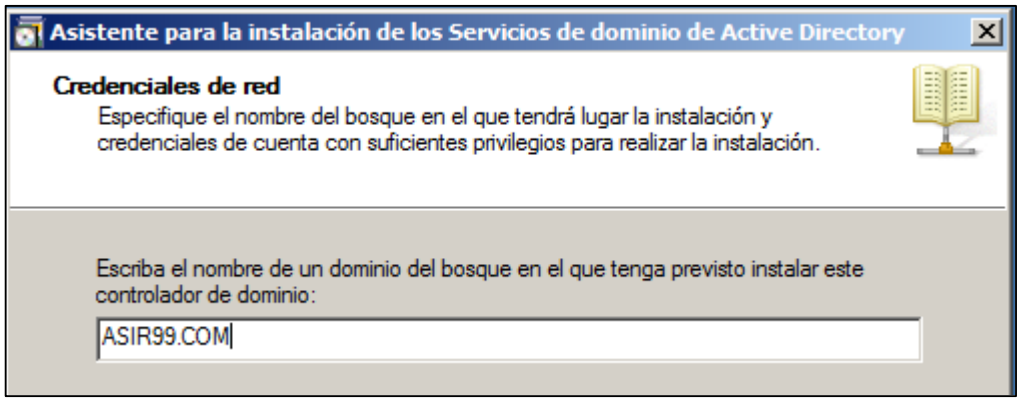
En versiones anteriores de Windows Server teníamos que establecer controladores de dominios principales y secundarios, pero desde Windows 2003 no es necesario hacer esta diferenciación. Todos los controladores funcionan al mismo nivel y trabajan entre sí de forma automática.

Vamos a realizar ahora la incorporación de un nuevo CD a nuestro dominio, para ello:

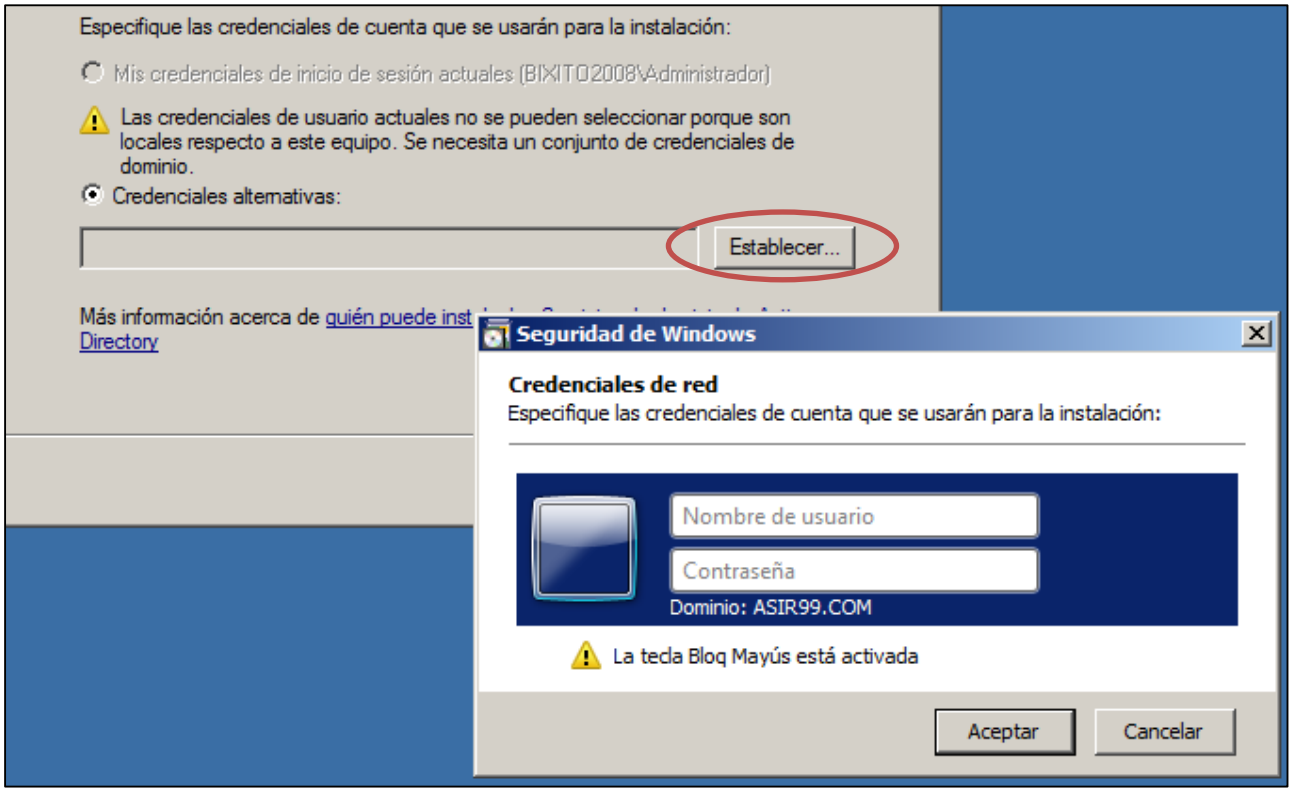
1) Debemos contar con un dominio ya creado y con un CD correctamente configurado.
2) En la nueva máquina con Windows Server, indicamos que queremos usar como servidor DNS la dirección del DNS del dominio. No hace falta añadir esta máquina como cliente del dominio.
3) Ejecutamos dcpromo en esta máquina (la promocionamos a servidor).
4) En este momento, dcpromo comenzará a hacernos preguntas para saber dónde queremos instalar nuestro CD. Tenemos que indicar que queremos trabajar en un bosque existente, y que queremos agregar un CD a un dominio existente.



5) A continuación el sistema nos pedirá que introduzcamos el nombre FQDN del dominio al que queremos conectarnos. (Nombre del dominio ya existente).



6) También tenemos que introducir unas credenciales, es decir, un nombre de usuario y contraseña del dominio donde queremos conectarnos. Obviamente ya que queremos instalar un Controlador de Dominio, la cuenta que usemos debe tener permisos de administrador.



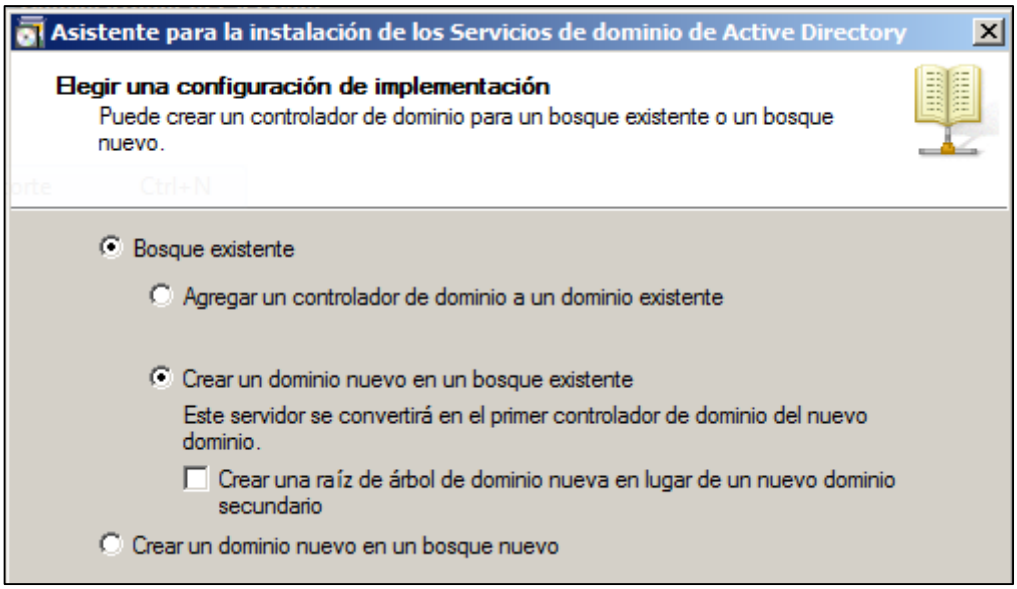
7) A continuación, y si la cuenta introducida es reconocida, continuará la instalación del CD tal como ya vimos. Es importante indicar que en este caso que estamos tratando el servidor DNS ya está instalado en la red, por lo que no tendremos que instalarlo junto con el CD.

Una vez terminado el proceso de instalación de nuestro CD y reiniciado el equipo, ya tendremos en nuestro dominio un CD adicional. Para probarlo, apagar el CD principal y comprobar como basta con tener el CD adicional encendido para que los clientes puedan seguir conectándose al dominio sin problemas.

INSTALAR UN NUEVO DOMINIO EN UN ARBOL YA EXISTENTE.

En este caso vamos a crear una “rama” de un árbol ya existente. Vamos a instalar un dominio nuevo pero que “cuelga” de un dominio ya existente.

Todos los pasos anteriores son válidos, la primera diferencia la encontraremos en el punto 4. En este caso debemos indicar igualmente que queremos crear un dominio en un bosque ya existente, pero no debemos indicar que queremos agregar un controlador de dominio adicional a un dominio ya existente.



Con esto conseguiremos instalar el dominio como rama de un árbol ya existente.

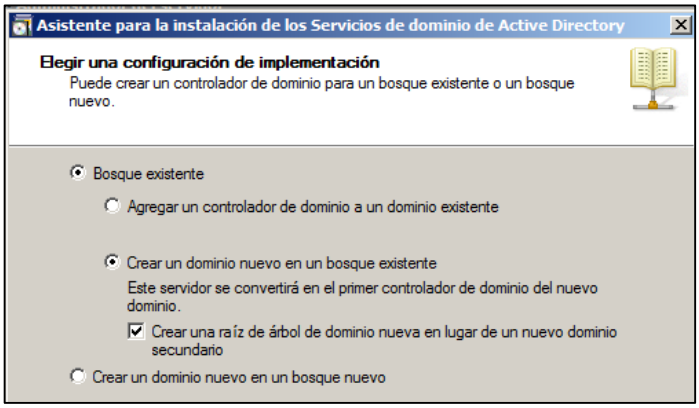
A continuación nos pedirá el sistema que introduzcamos el nombre del dominio del que queremos colgar y las credenciales necesarias de dicha dominio, exactamente igual que en el punto anterior.

Una novedad es que tras esto nos pedirá el nombre de nuestro nuevo dominio. Es importante fijarse que no nos pide el nombre FQDN, ya que dicho nombre aparece automáticamente. Es decir, si introducimos como nombre de dominio nuevo VENTAS veremos como el nombre completo se forma automáticamente y será VENTAS.ASIR99.COM por ejemplo.

Una vez reiniciado el servidor contaremos con 2 dominios en un árbol, cada uno será el único CD de su propio dominio.

INSTALAR UN NUEVO ARBOL EN UN BOSQUE YA EXISTENTE.

Es muy parecido al punto anterior, ya que también crearemos un nuevo CD, pero en este caso, en vez de crear una rama en un árbol ya existente, crearemos la raíz de un nuevo árbol en un bosque ya existente, es decir, en un bosque donde ya existe un CD que forma la raíz de otro árbol.



DEGRADAR UN CONTROLADOR DE DOMINIO.

Degradar un controlador de dominio consiste en retirarle la función de CD, lo contrario de promocionarlo. Para ello, podemos ejecutar dcpromo. Este comando si se ejecuta en un equipo cliente permite promocionarlo a CD, pero si se ejecuta en un CD permite degradarlo a equipo cliente.

La degradación de un controlador de dominio elimina la base de datos de Active Directory de la máquina, borra todas las referencias a ella del servidor DNS y devuelve las cuentas de seguridad del sistema a un estado local.

Si el servidor es el único controlador de dominio de un dominio particular, la degradación provoca que el dominio se elimine completamente. Si el servidor es el único controlador del dominio raíz de un bosque, hay que destruir el resto de dominios del bosque antes de que se pueda proceder con la degradación del controlador de dominio raíz. Una vez que se ha degradado un dominio (mediante el asistente por ejemplo), hay que asegurarse de que se cambia la identidad del equipo, para conseguir esto se realizan los siguientes pasos:

1) Abrir la herramienta Sistema del Panel de control y pulsar en la pestaña Identificación de red.

2) Pulsar el botón Avanzada para abrir el cuadro de diálogo Cambios de identificación.

3) Introducir el nuevo nombre para el equipo si es que se desea cambiar, y agregar el equipo a un grupo de trabajo cualquiera. (Si quisiéramos integrarlo como miembro de un dominio, podríamos hacerlo también).

4) Pulsar el botón Más y asegurarse de que se borra la casilla donde aparece el nombre de nuestro anterior dominio, que se usa como sufijo en el nombre de máquina. Mucho cuidado de no desactivar la casilla de verificación que indica que se debe usar el sufijo, ya que si lo hacemos será imposible que esa máquina pueda volver a trabar en un dominio.

Una pregunta que el sistema nos puede hacer en este punto, es si el dominio que queremos desinstalar posee el catalogo global.

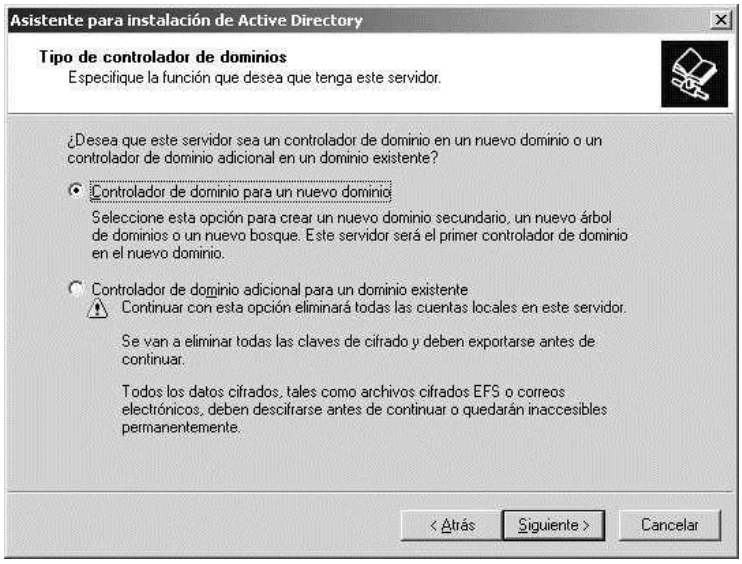
INSTALACIÓN DE ACTIVE DIRECTORY EN WINDOWS 2003.

Siguiendo el patrón de un asistente estándar, la instalación de Active Directory en un servidor es una cuestión de responder a las solicitudes en una secuencia de pantallas. Windows Server incorpora vínculos al asistente en la página de Active Directory de la página principal de Configurar el servidor de Windows Server. Esta página se muestra en el explorador Microsoft Internet Explorer automáticamente después de la instalación del SO. Esta página Web local está diseñada para guiar al administrador a través de los procesos necesarios para configurar un nuevo servidor mediante preguntas al estilo de los asistentes y vínculos a las herramientas apropiadas para cada tarea.

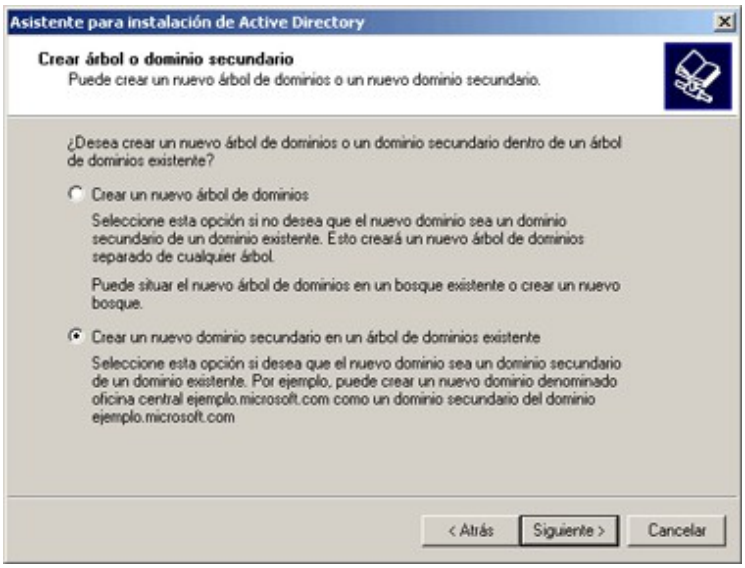
(Atención, en estos apuntes utilizamos imágenes procedentes de Windows 2000. Aunque hay algunas diferencias mínimas con Windows Server 2003, básicamente son iguales).

Para instalar el Primer controlador deberemos seguir los siguientes pasos:

Iniciar la Herramienta Configuración del Servidor desde el menú de Herramientas Administrativas. También puede iniciar el asistente directamente ejecutando el archivo ejecutable Dcpromo.exe desde el cuadro de dialogo Ejecutar.



Después de una pantalla de bienvenida, el Asistente para instalación pregunta sobre la acción que se va a realizar, basándose en el estado actual de Active Directory en el sistema. Si el servidor ya es un controlador de dominio, el asistente solo proporciona la opción de degradar el sistema de nuevo a servidor independiente o miembro. En un equipo que no es un controlador de dominio, el asistente muestra la pantalla Tipo de controlador de dominios, la cual pide que se seleccione una de las siguientes opciones:



- Controlador de dominio para un nuevo dominio: Instala Active Directory en el servidor y lo designa como el primer controlador de dominio de un nuevo dominio.
- Controlador de dominio adicional para un dominio existente: Instala Active Directory en el servidor y replica la información del directorio desde un dominio existente.

Para instalar el primer servidor Active Directory en la red, se selecciona la opción **Controlador de dominio para un nuevo dominio**. Esto hace que el asistente instale los archivos de soporte de Active Directory, cree el nuevo dominio y lo registre en el DNS

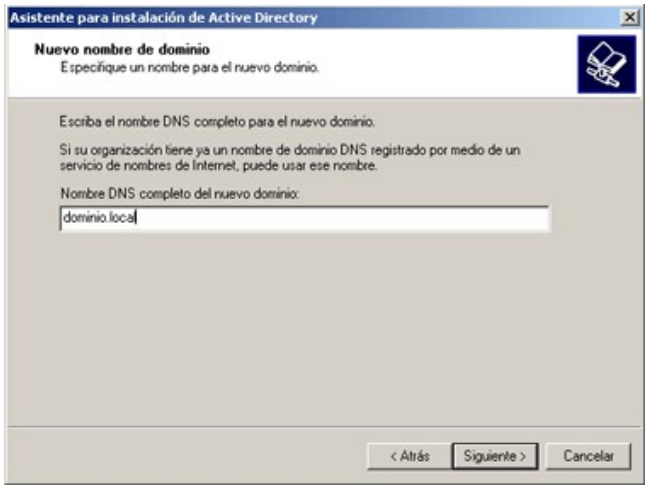
Crear un árbol o unirse a un árbol. Deberemos elegir el tipo de dominio que queremos configurar de las dos opciones que se presentan en el siguiente cuadro.

- Crear un nuevo árbol de dominios: Configura el nuevo controlador de dominio pare que aloje el primer dominio de un nuevo árbol. Esta es la opción que debemos escoger para instalar nuestro primer servidor.
- Crear un nuevo dominio secundario en un árbol de dominios existente: Configura el nuevo controlador de dominio para que aloje un hijo de un dominio de un árbol que ya existe.

Crear un bosque o unirse a un bosque, que permite especificar una de las siguientes opciones:

- Crear un nuevo bosque de árboles de dominios: Configura el controlador de dominio para que sea la raíz de un nuevo bosque de árboles.
- Situar este nuevo árbol de dominios en un bosque existente: Configura el controlador de dominio para que aloje el primer dominio de un nuevo árbol en un bosque que ya contiene uno o más árboles.

En este caso hay que seleccionar Crear un nuevo bosque de árboles de dominios, porque el primer controlador de dominio Windows 2000 de la red será siempre un nuevo dominio, en un nuevo árbol, en un nuevo bosque. A medida que se instalen controladores de dominio adicionales, se pueden utilizar estas mismas opciones para crear otros bosques nuevos o para poblar el bosque existente con árboles y dominios adicionales.



Nombre de nuevo Dominio: Para identificar el controlador de dominio en la red se debe especificar un nombre DNS valido para el dominio que se esta creando.

Este nombre no tiene por que ser el mismo que el del dominio que utiliza la empresa para su presencia en Internet (aunque puede serlo). El nombre tampoco tiene que estar registrado en el Centro de información de redes de Internet (InterNIC, Internet Network información), la organización responsable de mantener el registro de los nombres DNS en los dominios de nivel superior com, net, org y edu. Sin embargo, el uso de un nombre de dominio registrado es una buena idea si los usuarios de la red van a acceder a los recursos de Internet al mismo tiempo que a los recursos de red locales, o si los usuarios externos a la organización accederán a los recursos de red locales vía Internet.

Nombre de dominio NetBIOS. Después de introducir un nombre DNS para el dominio, el sistema solicita un equivalente NetBIOS para el nombre del dominio para que los utilicen los clientes antiguos que no soporten Active Directory.

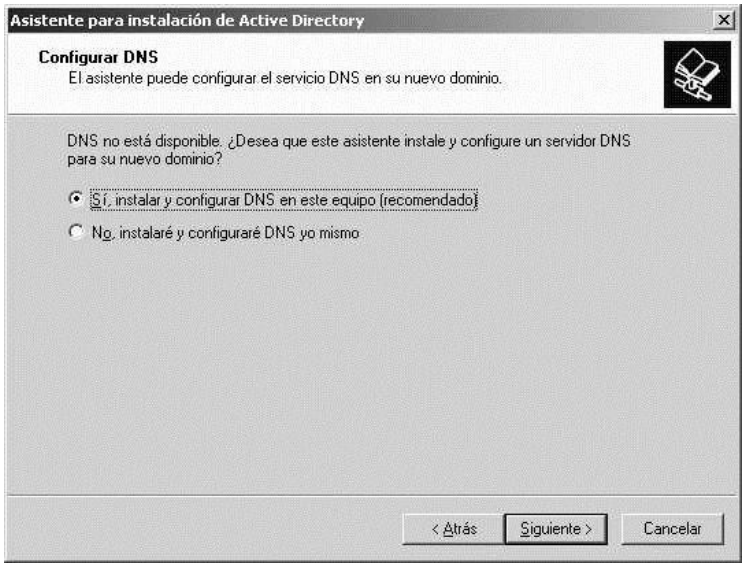
Los sistemas Windows Server todavía utilizan el espacio de nombres NetBIOS para sus nombres de equipo, pero Active Directory utiliza la nomenclatura DNS para los dominios. Windows NT 4 y los sistemas Microsoft Windows 9x utilizan nombres NetBIOS para todos los recursos de la red, incluyendo los dominios.

Si se dispone de clientes de nivel inferior en la red (esto es, Windows NT 4, Windows 9x, Microsoft Windows para Trabajo en grupo o Cliente de red Microsoft para sistemas MS-DOS), estos solo serán capaces de ver el nuevo dominio por medio del nombre NetBIOS. La pantalla Nombre de dominio NetBIOS contendrá una sugerencia para el nombre, basándose en el nombre DNS especificado, qua se puede utilizar o bien se puede reemplazar con un nombre qua se elija qua tenga 15 caracteres o menos.

Después de especificar los nombres de dominio, el asistente solicita las ubicaciones de la base de datos, los archivos de registro y el volumen del sistema de Active Directory. La base de datos de Active Directory contendrá los objetos Active Directory y sus propiedades, mientras qua los archivos de registro registran las actividades del servicio de directorio. Los directorios para estos archivos se especifican en la pantalla ubicación de la base de datos. La ubicación predeterminada tanto para la base de datos como para los registros es la carpeta %SystemRoot%\Ntds del volumen del sistema, pero se pueden modificar según nuestras necesidades siendo aconsejable que no residan en el mismo disco duro, para optimizar el rendimiento.

La pantalla Volumen del sistema compartido permite especificar la ubicación de lo qua se convertirá en el recurso compartido Sysvol del controlador de dominio. El volumen del sistema es un recurso compartido que contiene información del dominio que se replica al resto de controladores de dominio de la red. De forma predeterminada, el sistema crea este recurso compartido en la carpeta %SystemRoot%\Sysvol en la unidad de disco del sistema.

La base de datos, los registros y el volumen del sistema de Active Directory tiene que situarse en volúmenes que utilicen el sistema de archivos NTFS 5. Si el asistente detecta que alguno de los volúmenes escogidos no utiliza NTFS 5, habrá que convertirlos o seleccionar otro volumen antes de poder completar el proceso de instalación de Active Directory. También resulta aconsejable situarlo en otro disco distinto al del sistema operativo

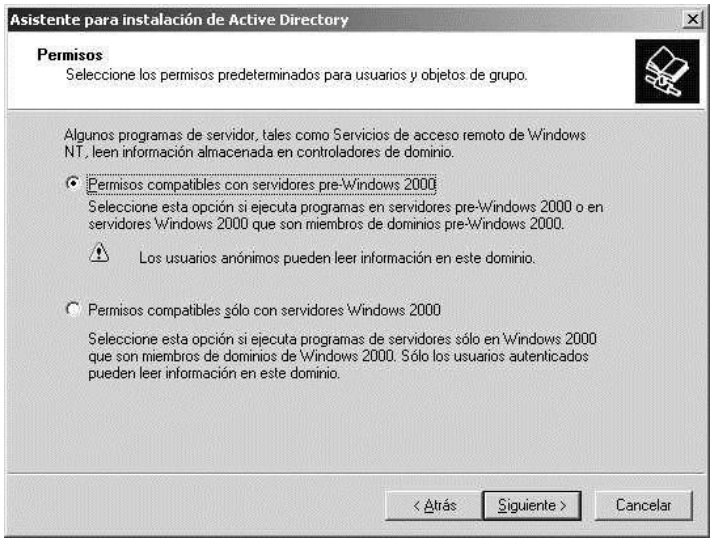


Instalación de DNS: En este punto, el Asistente para instalación de Active Directory tiene toda la información de configuración necesaria para instalar Active Directory y promover el servidor a controlador de dominio. El asistente determina ahora si el servidor DNS que se ha indicado en las

propiedades TCP/IP (si es que se ha indicado) es capaz de trabajar con el servidor Windows Server y está activo.

El asistente también determina si el servidor DNS que alojara el dominio soporta el protocolo de Actualización dinámica. Si el sistema no puede contactar con el servidor DNS especificado en la configuración TCP/IP cliente del equipo, o si el servidor DNS especificado no es capaz de dar soporte a un dominio Windows Server, el asistente se ofrece a instalar Microsoft DNS Server y configurarlo para que funcione como servidor autorizado para el dominio.

La pantalla Configurar DNS permite especificar si se desea instalar el servidor DNS o configurar uno personalmente. Si se opta por utilizar otra máquina para el servidor DNS, es preciso instalarlo y configurarlo antes de poder completar la instalación de Active Directory.



En nuestro caso, escogeremos la opción de **instalar y configurar DNS en este equipo**.

Ahora el asistente nos solicitará que escojamos entre trabajar en modo nativo o en modo mixto. En caso de que tengamos en nuestra red servidores NT y deseemos que estos servidores se conecten al dominio como servidores, tendremos que escoger permisos compatibles con servidores anteriores al Windows Server que se esté instalando.

Siempre que sea posible, escogeremos la opción de permisos compatibles sólo con servidores Windows Server actuales, ya que será la forma más cómoda de trabajar.

A continuación, el asistente nos solicitará una contraseña que tendremos que usar si queremos restaurar el sistema. Tenemos que tener en cuenta que al promocionar nuestro equipo desde servidor individual a servidor de dominio, creamos una cuenta especial; la de Administrador del Dominio, que tendrá la misma contraseña que tenia el Administrador del equipo donde instalamos el Active Directory. Como es obvio, esta contraseña no debe olvidarse bajo ningún concepto. Es muy recomendable usar la misma contraseña para el Administrador del servidor y el Administrador del dominio, así no nos equivocaremos cuando nos la pida el sistema luego.

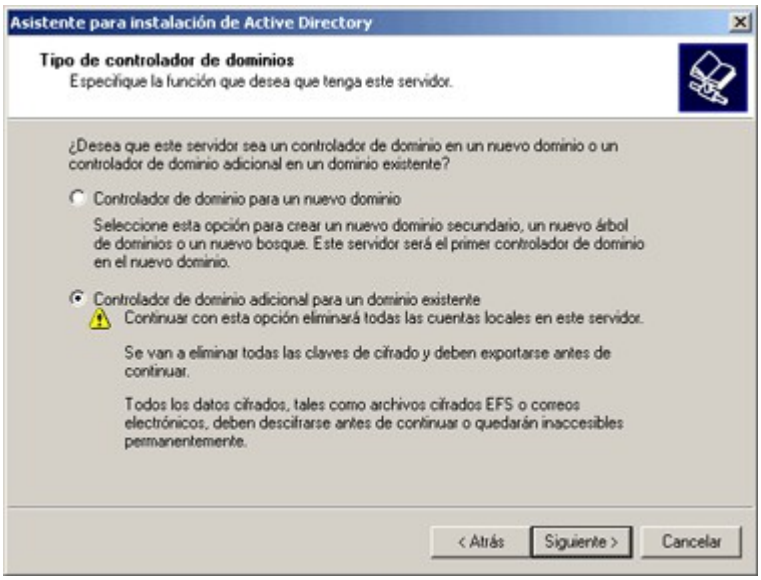
Finalización de la instalación de Active Directory: El asistente registra todas las actividades que se producen durante el proceso de instalación en dos archivos llamados Dcpromo.log y Dcpromoui.log, en la carpeta %SystemRoot%\debug.

La instalación puede durar varios minutos, después de lo cual hay que reiniciar el sistema para que tengan efecto los cambios.

INSTALACIÓN DE UN CONTROLADOR DE DOMINIO ADICIONAL.

Los servidores adicionales proporcionan tolerancia a fallos en un dominio Active Directory, y pueden reducir el tráfico entre redes permitiendo a los clientes de la red autenticarse utilizando un controlador de dominio en el segmento local.

Cuando un controlador de dominio no funciona correctamente o no esta disponible por algún motivo, sus réplicas asumen automáticamente sus funciones. Incluso un dominio pequeño necesita al menos dos controladores de dominio para mantener esta tolerancia a fallos.



Para crear una réplica de un dominio existente, hay que ejecutar el Asistente para instalación de Active Directory (dcpromo) en un Windows Server recién instalado después de unirse al dominio que se trata de replicar.

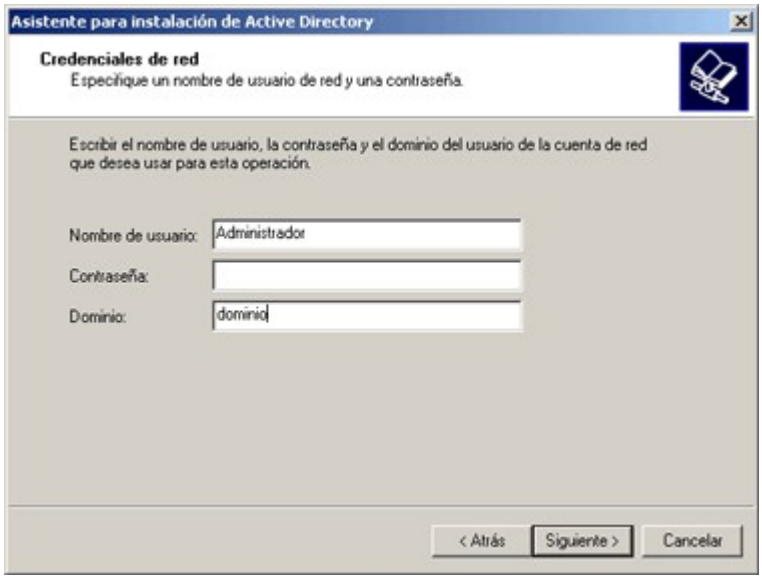
Cuando aparece la pantalla Tipo de controlador de dominios en el asistente, hay que seleccionar Controlador de dominio adicional para un dominio existente y especificar el nombre DNS del dominio que se va a replicar. Después hay que suministrar el nombre de usuario, la contraseña y el nombre de dominio de una cuenta con privilegios administrativos en el dominio.

El asistente instala Active Directory en el servidor, crea la base de datos, los registros y el volumen del sistema en las ubicaciones especificadas, registra el controlador de dominio en el servidor DNS y replica la información de un controlador de dominio para ese dominio existente.

Una vez que la réplica del controlador de dominio está en funcionamiento, no es distinguible del controlador de dominio existente, al menos en lo que concierne a la funcionalidad de los clientes. Las réplicas funcionan como iguales, a diferencia de los servidores Windows NT, que están designados como controladores de dominio principales o de reserva. Los administradores pueden modificar el contenido de Active Directory (tanto los objetos como el esquema) de cualquier controlador de dominio, y los cambios se replicarán al resto de controladores de dominio de ese dominio.

Cuando se crea una réplica, el Asistente para instalación de Active Directory configura automáticamente el proceso de réplica entre los controladores de dominio. Se puede personalizar el proceso de réplica utilizando Sitios y servicios de Active Directory.

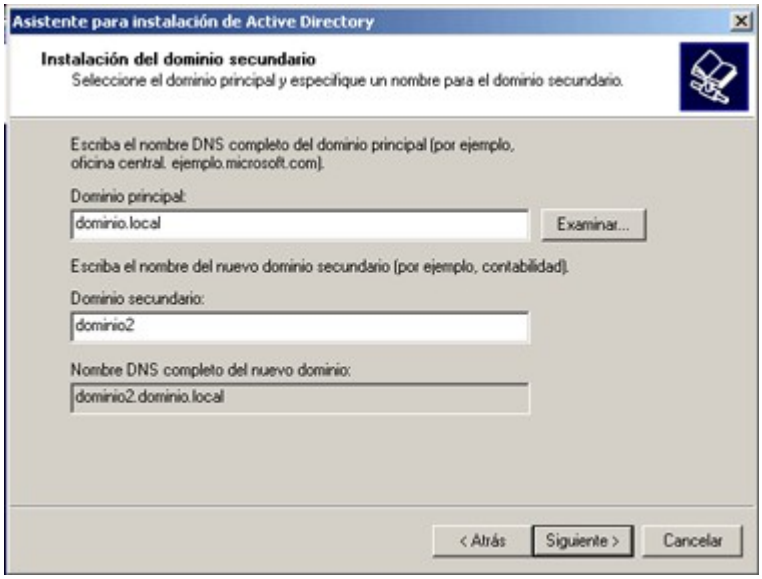
CREACIÓN DE UN DC PARA UN DOMINIO SECUNDARIO EN UN ÁRBOL EXISTENTE



Cuando se crea el primer dominio Windows Server de la red, también se esta creando el primer árbol del bosque. Se puede poblar el árbol a medida que se crean dominios adicionales haciéndolos secundarios de dominios existentes. Un dominio secundario es uno que utiliza el mismo espacio de nombres que un dominio principal. Este espacio de nombres se establece por el nombre DNS del dominio principal, al cual el secundario añade un nombre precedente para el nuevo dominio.

Por ejemplo, si se crea un dominio llamado SANA.COM, un dominio secundario de ese dominio podría llamarse algo así como INVESTIGACION.SANA.COM.

Por regla general, los dominios secundarios reflejan las divisiones geográficas, departamentales o políticas de una organización, pero se puede utilizar cualquier principio para el diseño del árbol que se desee. Un dominio principal puede tener cualquier número de secundarios, y la estructura del árbol puede extenderse a través de cualquier número de generaciones, lo que permite utilizar un único espacio de nombres para crear un árbol de dominios que refleje la estructura de toda la organización.



Para instalar Active Directory y crear un dominio secundario:

Unir el equipo en el que se desea crear el Dominio secundario al dominio principal suministrando las credenciales administrativas o creando manualmente un objeto equipo en el dominio por medio de Usuarios y equipos de Active Directory.

Iniciar sesión en el sistema utilizando la cuenta de administrador local

Ejecutar el Asistente para instalación de Active Directory desde la página Configurar el servidor o ejecutando Dcpromo.exe desde el cuadro de dialogo Ejecutar.

Un dominio secundario no es una réplica; es un dominio completamente independiente situado en el mismo árbol. Por lo tanto, cuando el asistente muestra la pantalla Tipo de controlador de dominios, hay

que seleccionar Controlador de dominio para un nuevo dominio. En el cuadro de diálogo Crear árbol o dominio secundario, hay que seleccionar Crear un nuevo dominio secundario en un árbol de dominios existente. El asistente solicita a continuación el nombre DNS del dominio que ha de ser el principal del secundario. Después de suministrar esto, hay que especificar el nombre corto para el dominio secundario. El nombre corto es el nombre que se añadirá al nombre DNS del dominio principal para formar el nombre completo del dominio secundario. Por ejemplo, para crear un dominio secundario llamado Investigacion.miempresa.com, se especifica Miempresa.com como nombre del dominio principal a investigación como nombre corto del secundario.

En la siguiente pantalla nos solicita un nombre NetBIOS para el nuevo dominio de no más de 15 caracteres.

CREACIÓN DE UN DC PARA UN NUEVO ÁRBOL EN UN BOSQUE YA EXISTENTE

La diferencia fundamental entre la creación de un nuevo árbol y la creación de un nuevo bosque es que los bosques tienen cada uno sus propios esquema y configuración individuales. El escenario más obvio en el que una red debería tener múltiples bosques es cuando dos empresas con instalaciones Active Directory existentes se fusionan, y las suficientes diferencias de esquema y configuración existentes entre las dos hacen que la unión de ambas en un solo bosque sea impracticable. El proceso de crear un nuevo bosque es el mismo que el de la creación del primer dominio de la red.

DEGRADACIÓN DE CONTROLADORES DE DOMINIOS.

Una diferencia fundamental entre los controladores de dominio Windows 200X y los controladores de dominio Windows NT es que se puede degradar un controlador de dominio Windows 200X a servidor independiente o miembro. Cuando se ejecuta el Asistente para instalación de Active Directory, el programa determina que el sistema ya esta funcionando como controlador de dominio y solo proporciona la opción de degradar el servidor. La pantalla Configurar el servidor también detecta el estado del sistema y proporciona una única opción.

La degradación de un controlador de dominio elimina la base de datos de Active Directory de la máquina, borra todas las referencias a ella del servidor DNS y devuelve las cuentas de seguridad del sistema a un estado idéntico al de un servidor Windows 2000 recién instalado. Si el dominio al que pertenece el sistema tiene controladores de dominio de réplica en la red, el servidor permanece como, miembro de ese dominio después de la degradación.

Si el servidor es el único controlador de dominio de un dominio particular, la degradación provoca que el dominio se elimine completamente de Active Directory, y que el sistema se convierta en un servidor independiente hasta que se una a otro dominio. Si el servidor es el único controlador del dominio raíz de un bosque, hay que destruir el resto de dominios del bosque antes de que se pueda proceder con la degradación del controlador de dominio raíz. Una vez que se ha degradado un dominio (mediante el asistente por ejemplo), hay que asegurarse de que se cambia la identidad del equipo, para conseguir esto se realizan los siguientes pasos:

5) Abrir la herramienta Sistema del Panel de control y pulsar en la pestaña Identificación de red.

6) Pulsar el botón Avanzada para abrir el cuadro de diálogo Cambios de identificación.

7) Introducir el nuevo nombre para el equipo si es que se desea cambiar, y agregar el equipo a un grupo de trabajo cualquiera. (Si quisiéramos integrarlo como miembro de un dominio, podríamos hacerlo también).

8) Pulsar el botón Más y asegurarse de que se borra la casilla donde aparece el nombre de nuestro anterior dominio, que se usa como sufijo en el nombre de máquina. Mucho cuidado de no desactivar la casilla de verificación que indica que se debe usar el sufijo, ya que si lo hacemos será imposible que esa máquina pueda volver a trabar en un dominio.

MAESTROS DE OPERACIONES.

Hemos comentado anteriormente como en el antiguo Windows NT los controladores de dominio se dividían en controladores principales (uno por dominio) y controladores secundarios. Desde Windows 2000 esto ya no es así, todos los controladores de dominio trabajan al mismo nivel.

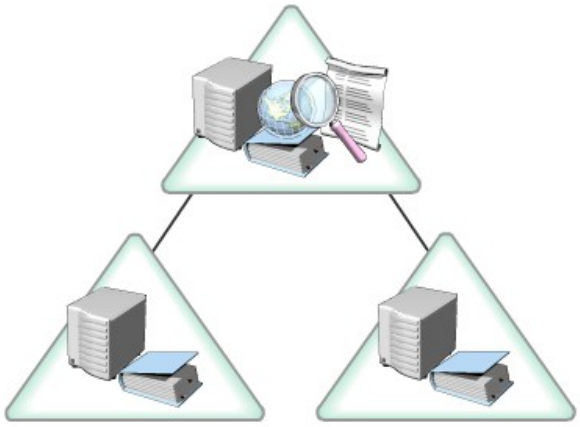
Sin embargo, hay controladores de dominio que realizan una serie de operaciones especiales y por lo tanto son más importantes que el resto, estos son los maestros de operaciones.

Las funciones de maestro de operaciones son funciones específicas en las que se organizan las operaciones que utilizan la replicación de maestro único. La replicación de maestro único designa un controlador de dominio como el único controlador de dominio en el que pueden realizarse ciertos cambios en el directorio activo. Esto se hace para evitar conflictos de replicación que pueden presentarse si dos controladores de dominio realizan actualizaciones al mismo tiempo en el mismo atributo de objeto (dos controladores que cambian el nombre de un usuario al mismo tiempo, por ejemplo). Active Directory utiliza la replicación de maestro único para cambios importantes, como la adición de un nuevo dominio o un cambio en el esquema de todo el bosque.

El controlador de dominio que es responsable de una función particular es el maestro de operaciones de esa función. Active Directory almacena la información acerca del controlador de dominio que tiene una función específica. Active Directory define cinco funciones de maestro de operaciones, con una ubicación predeterminada para cada una. Las funciones de maestro de operaciones abarcan todo el bosque o todo el dominio, hay dos funciones que abarcan todo el bosque y tres funciones que abarcan todo el dominio.

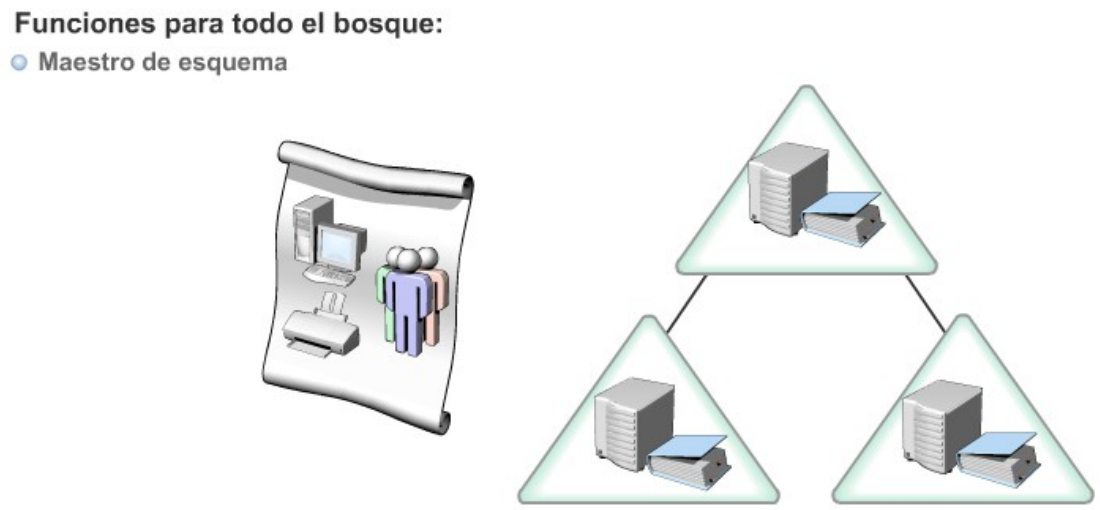
Funciones para todo el bosque
- Maestro de nombres de dominio
- Maestro de esquema

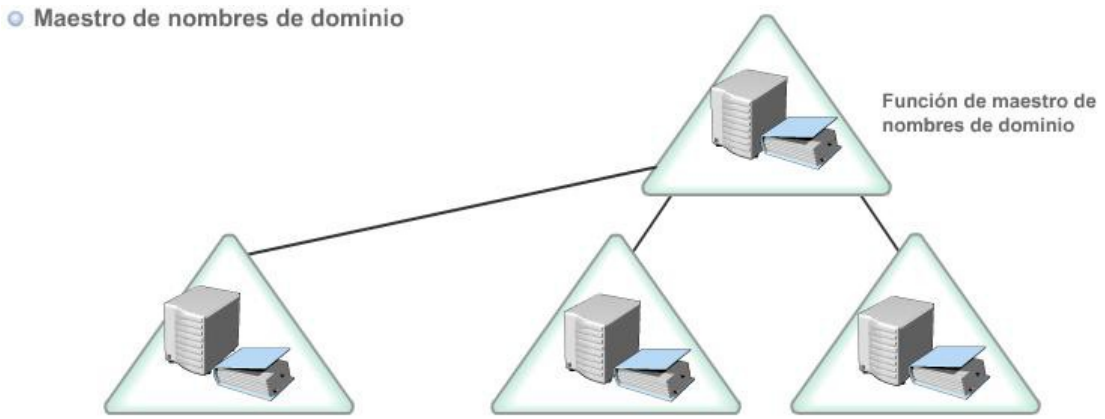
Funciones para todo el dominio:
- Emulador de PDC
- Maestro de RID
- Maestro de infraestructura



Las funciones que abarcan todo el bosque, incluyen el maestro de esquema que controla todas las actualizaciones del esquema. El esquema contiene una lista general de clases de objetos y atributos que se utilizan para crear todos los objetos de Active Directory como, por ejemplo, usuarios, equipos e impresoras.

La otra función que abarca todo el bosque, el maestro de nombres de dominio, controla la adición o eliminación de dominios en el bosque. Sólo el controlador de dominio que tiene la función de maestro de nombres de dominio puede agregar un nuevo dominio. Sólo existe un maestro de esquema y un maestro de nombres de dominio en todo el bosque.





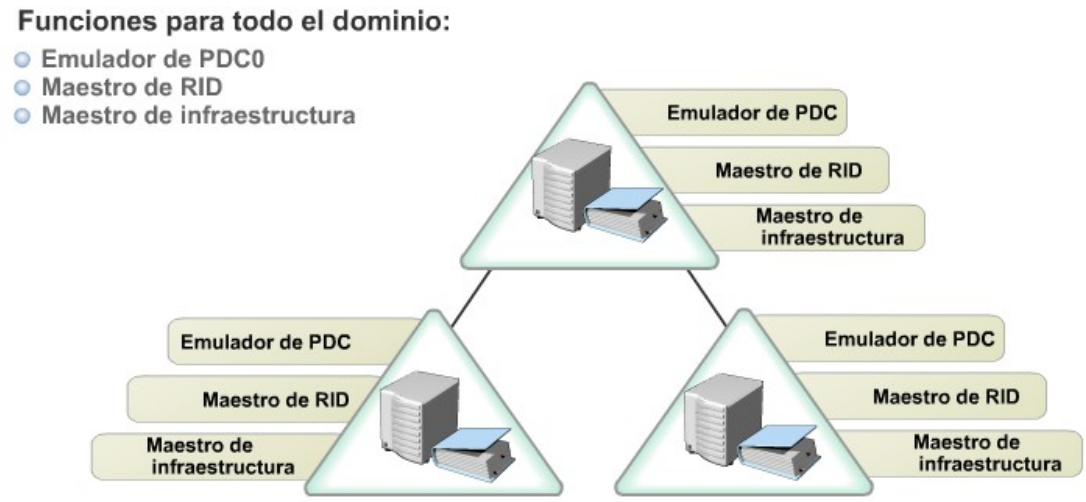
Las funciones para todo el dominio son exclusivas de cada dominio en un bosque. Las funciones que abarcan todo el dominio son el emulador del controlador principal de dominio (PDC), el maestro de identificadores relativos (RID) y el maestro de infraestructura. Cada dominio de un bosque tiene su propio emulador de PDC, maestro de RID y maestro de infraestructura.

El emulador de PDC, el primer controlador de dominio que se crea en un nuevo dominio, acepta los controladores de dominio de reserva (BDC) que ejecutan Microsoft Windows NT® dentro de un dominio de modo mixto. Este tipo de dominio tiene controladores de dominio que ejecutan Windows NT® 4.0.

El maestro de RID asigna bloques de identificadores relativos a cada controlador de dominio en el dominio.

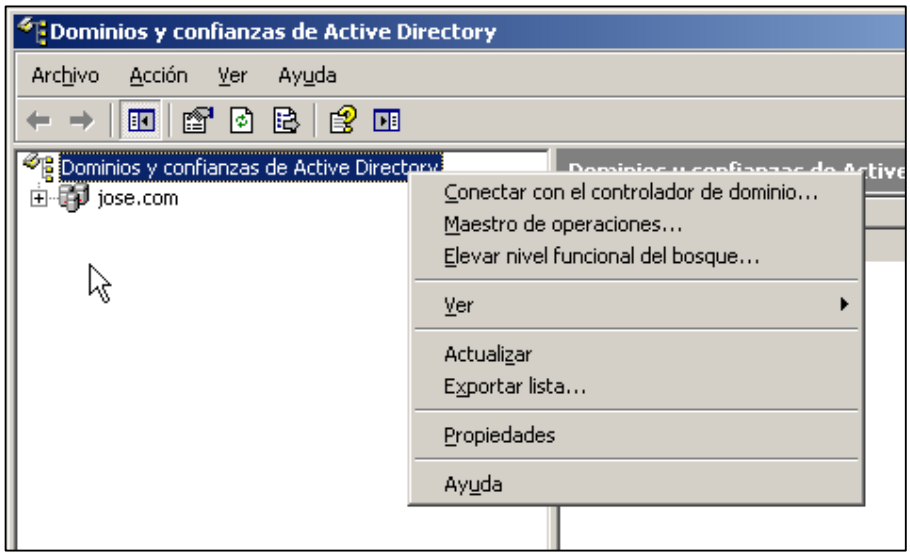
Cuando se mueven objetos de un dominio a otro, el maestro de infraestructura actualiza las referencias a objetos en su dominio que apuntan al objeto en el otro dominio. La referencia al objeto contiene el identificador único global (GUID) y un identificador de seguridad (SID). Active Directory actualiza

periódicamente el nombre completo y el SID en la referencia al objeto para que se reflejen los cambios realizados en el objeto propiamente dicho, como los movimientos dentro de los dominios y entre éstos y la eliminación del objeto.



CAMBIAR EL MAESTRO DE OPERACIONES PARA NOMBRES DE DOMINIO.

Windows Server irá asignando estas funciones de maestros de operaciones a los primeros controladores de dominio creados. Si queremos modificar estas asignaciones podemos hacerlo desde la consola MMC de Dominios y Confianzas de Active Directory. Para ello pulsamos con botón derecho sobre Dominios y confianzas de Active Directory y escogemos la opción Maestro de Operaciones, que nos permitirá cambiar el CD que realiza la función de maestro de nombres de dominio.

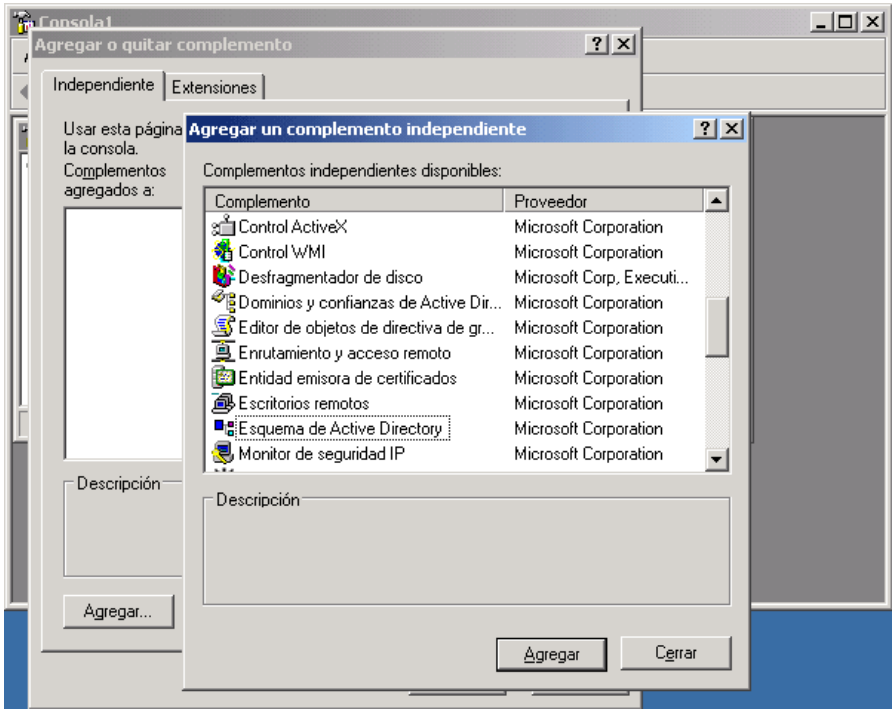


La función de maestro de nombres de dominio recordemos que es la encargada de añadir y eliminar dominios de nuestro árbol, por lo que es muy importante tener controlado que CD realiza esta función, ya que si dicho CD está apagado, no se podrán añadir ni eliminar ramas a nuestro árbol, o arboles a nuestro bosque.

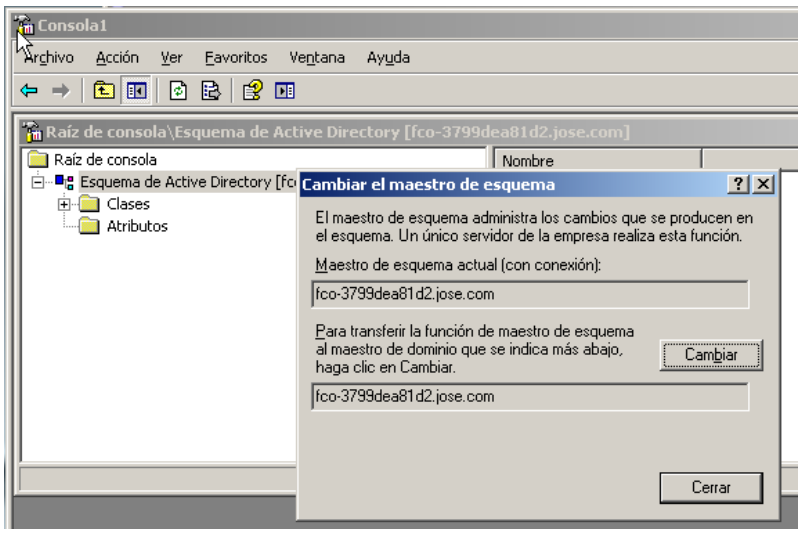
Para llevar a cabo este procedimiento, debemos ser miembros del grupo Administradores de dominio o del grupo Administradores de organización de Active Directory.

CAMBIAR EL MAESTRO DE OPERACIONES PARA MAESTRO DE ESQUEMA.

Se realiza dicho cambio desde la MMC de Esquema de Active Directory. Recordamos que dicha MMC no se instala por defecto, ya explicamos anteriormente como instalarla, ejecutando en una terminal el comando *regsvr32 schmmgmt.dll*. Una vez hecho nos aparecerá un mensaje de éxito en pantalla, volveremos a Inicio -> Ejecutar y una vez allí ejecutaremos "mmc" lo que nos abrirá una consola vacía, navegamos a Archivo -> Agregar o quitar complemento.. y seleccionar Esquema de Active Directory.

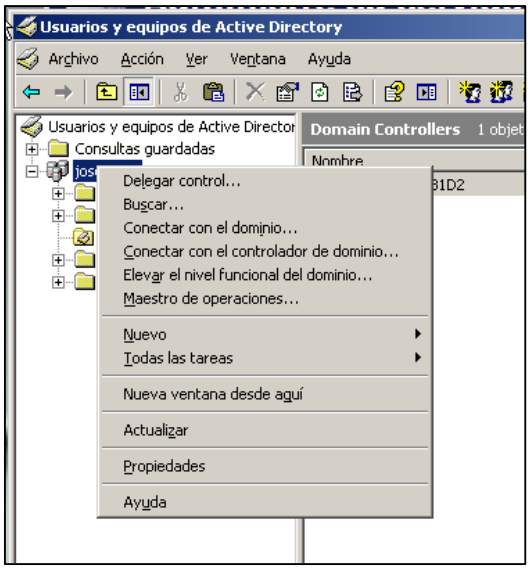


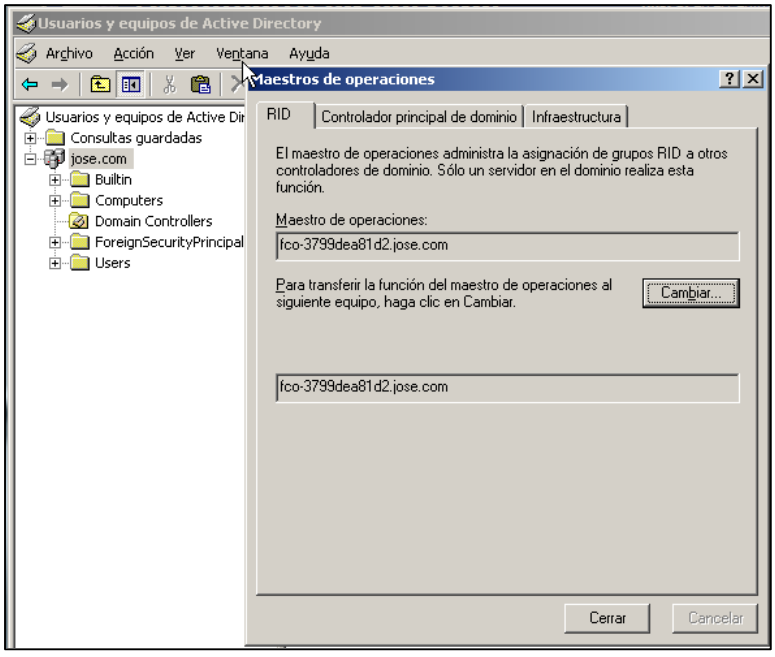
Una vez hecho esto, pulsamos botón derecho sobre Esquema de Active Directory y escogemos como siempre, la opción de cambiar el maestro de operaciones.



CAMBIAR EL MAESTRO DE OPERACIONES PARA EMULADOR DE PDC, MAESTRO DE RID Y MAESTRO DE INFRAESTRUCTURA.

Para cambiar estas funciones que trabajan a nivel de dominio, tenemos que ejecutar la consola Usuarios y Equipos de Active Directory. Pulsamos con botón derecho sobre el nombre de nuestro dominio y escogemos la opción maestro de operaciones.





Veremos cómo nos aparece un formulario que nos permita cambiar el maestro de RID, el Controlador principal de dominio que realiza las funciones de emulador de PDC y el maestro de infraestructura.

CATALOGO GLOBAL.

El primer controlador de dominio Windows Server de un bosque es automáticamente un servidor de Catálogo global. El Catálogo global (CG) contiene una réplica completa de todos los objetos de directorio del dominio en que se aloja además de una réplica parcial de todos los objetos de directorio de cada dominio del bosque. El objetivo de un CG es proporcionar autenticación a los inicios de sesión. Además, como un CG contiene información sobre todos los objetos de todos los dominios del bosque, la búsqueda de información en el directorio no requiere consultas innecesarias a los dominios. Una única consulta al CG produce la información sobre donde se puede encontrar el objeto.

De forma predeterminada, habrá un CG, pero cualquier controlador de dominio se puede configurar como servidor de Catalogo global. Si se necesitan servicios de inicio de sesión y búsqueda adicionales, se pueden tener múltiples servidores de Catalogo global en el dominio.

Para convertir un controlador de dominio en un servidor de Catalogo global, hay que seguir estos pasos:

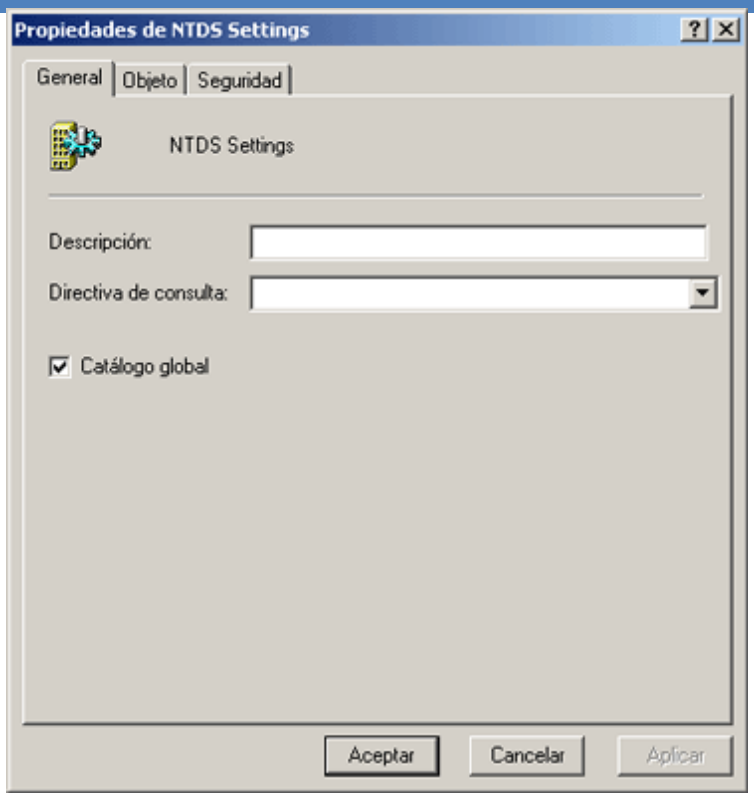
1) Escoger Sitios y servicios de Active Directory en el menú Herramientas administrativas.

2) Abrir Sites y seleccionar el sitio correspondiente. (normalmente el de por defecto).

3) Abrir Servers y seleccionar después el controlador de dominio que se desea convertir en servidor de Catalogo global.

4) Seleccionar NTDS Settings en el panel derecho y escoger propiedades en el menú Acción.

5) En la pestaña General, seleccionar la casilla de verificación Catalogo global.

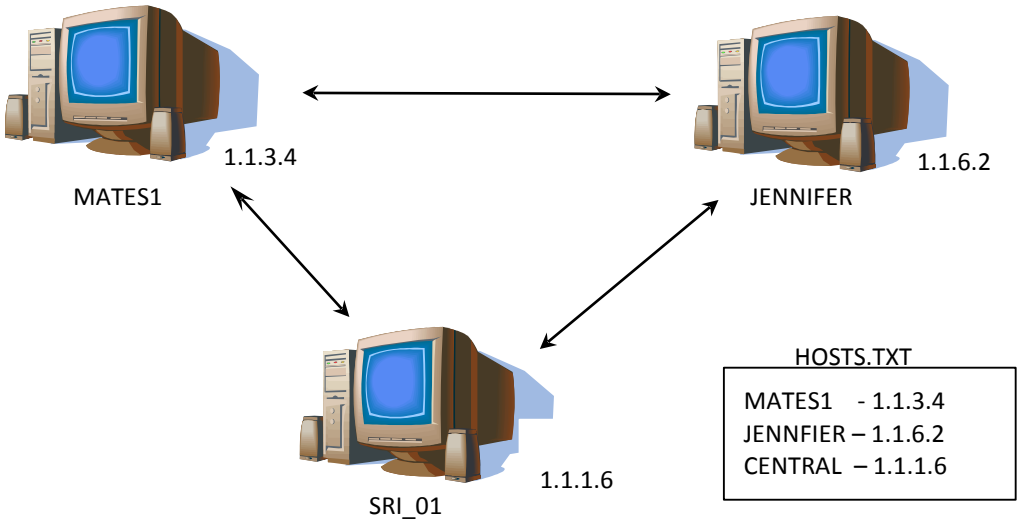


SERVIDORES DNS Y DHCP EN WINDOWS SERVER.

SERVIDOR DNS.

Todos los hosts con TCP/IP tienen una dirección de IP única que se utiliza para la comunicación con otros equipos de la red. Un equipo trabaja fácilmente con direcciones IP, pero estas direcciones son muy difíciles de usar para las personas, ya que los usuarios suelen identificar los sistemas por un nombre. Para facilitar una comunicación efectiva y eficiente, los usuarios deben poder referirse a los equipos por un nombre y permitir que su equipo use su dirección de IP transparentemente.

En los primeros días de ARPANET, el antecesor de la Internet actual, sólo existía un pequeño número de equipos conectados a la red. El Centro de Información de Red (NIC), ubicado en el Instituto de Investigaciones de Stanford, SRI (Stanford Research Institute), era el responsable de compilar en un único archivo, HOSTS.TXT, los nombres y direcciones de todos los equipos. Los administradores debían mandar un mensaje al SRI, quien actualizaba el archivo HOSTS.TXT. A continuación, los usuarios de ARPANET debían descargar la nueva versión del archivo HOSTS.TXT mediante el Protocolo de transferencia de archivos (FTP).



Con el crecimiento de ARPANET, resultaba obvio que este método no era práctico, ya que:

- El ancho de banda consumido para transmitir las versiones actualizadas de un archivo de host de ARPANET sería proporcional al cuadrado del número de hosts en la ARPANET. Con un número de hosts creciendo exponencialmente, el impacto a largo plazo probablemente sería de una sobrecarga que ningún host podría mantener. (Para 4 hosts, había que mandar un archivo de 4 KB a 4 equipos lo que ocuparía un ancho de banda de 16 KB, con 100 hosts había que mandar un archivo de 100 KB a 100 equipos, lo que ocuparía un ancho de banda de 10.000 KB).
- El archivo de host plano y estático significaría que no podría haber dos equipos en la ARPANET con la misma dirección. Al crecer el número de hosts, crece el riesgo de añadir nombres duplicados, así como la dificultad de intentar un control centralizado.

- La naturaleza de la red subyacente estaba cambiando, los grandes equipos de tiempo compartido con que se había construido ARPANET se estaban viendo desplazados por miles de estaciones de trabajo y cada una necesitaba un nombre de host único. Empezaba a ser imposible controlar todos estos nombres centralizadamente desde un único equipo.

Con el crecimiento de ARPANET, resultaba más claro que se necesitaba una solución mejor. Se generaron varias propuestas según el concepto de servicio de nombres distribuido, que se basaban en un espacio de nombres jerárquico. Nacieron las RFC 882 y 883, donde se describe el diseño de un sistema de nombres de dominio, basado en una base de datos distribuida que contiene información generalizada de recursos. Este diseño evolucionó, y las RFC 1034 y 1035 describen el servicio del Sistema de nombres de dominio (DNS) que se usa hoy en Internet.

DESCRIPCIÓN GENERAL DE DNS EN MICROSOFT WINDOWS SERVER.

Para facilitar las comunicaciones entre equipos se les puede dar un nombre en un espacio de nombres. El espacio de nombres concreto define las reglas para dar nombre a un equipo y cómo se resuelve un nombre en una dirección de IP. Cuando un equipo se comunica con otro debe resolver, o convertir, un nombre de equipo en una dirección de IP según las reglas del espacio de nombres utilizado. Esta resolución se puede realizar mediante un servicio de resolución de nombres.

Existen dos espacios de nombres principales y métodos de resolución de nombres que se usan en Windows Server: NetBIOS, implementado por el Servicio de Nombres de Internet de Windows (WINS) y DNS. WINS es tan inefectivo que es obligatorio montar y usar DNS, aunque se permite usar también WINS por motivos de compatibilidad, pero siempre y cuando DNS ya esté en funcionamiento.

TÉRMINOS CLAVE DNS.

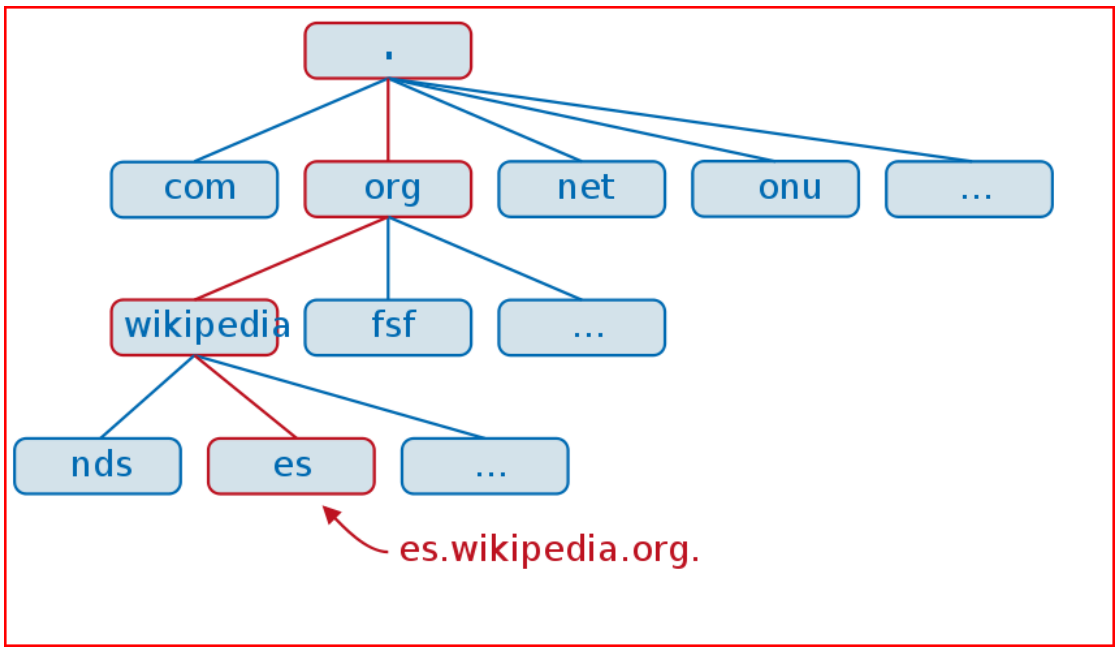
DNS es un servicio de nombres estándar. El servicio de DNS permite que un equipo cliente de la red registre y resuelva nombres de dominio de DNS. Estos nombres se utilizan para encontrar y acceder a recursos de otros equipos de la red o de otras redes como Internet. Los tres componentes principales de DNS son los siguientes:

- Los Clientes DNS: Un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS (Por ejemplo: ¿Qué dirección IP corresponde al nombre www.eufrasia.com ?).

- Los Servidores DNS: Que contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada. (Así, el servidor DNS respondería al ejemplo anterior: El nombre www.eufrasia.com tiene registrada la IP 10.1.2.15).

- Zonas de autoridad, que son porciones del espacio de nombres de dominio que almacenan los datos. Cada zona de autoridad abarca al menos un dominio y posiblemente sus subdominios, si estos últimos no son delegados a otras zonas de autoridad.

El espacio de nombres de dominio está estructurado de manera jerárquica en un árbol que empieza en una raíz sin nombre para todas las operaciones de DNS. En el espacio de nombres de DNS cada nodo y cada hoja en el árbol del espacio de nombres de dominio representan un dominio con nombre. Cada dominio puede tener dominios hijos adicionales.



NOMBRE DE DOMINIO.

Cada nodo en el árbol de DNS tiene un nombre distinto, llamado etiqueta que puede tener entre 1 y 63 caracteres. El dominio raíz no tiene caracteres (.).

Un nombre de dominio concreto es la lista de etiquetas en la ruta desde el nodo nombrado hasta la raíz del árbol de DNS. La convención de DNS es que las etiquetas que componen un nombre de dominio se leen de izquierda a derecha, desde lo más concreto hasta la raíz, por ejemplo, ventas.europa.cocacola.com. Este nombre completo también se denomina nombre de dominio completo o FQDN (Fully Qualified Domain Name).

Los nombres de dominio se pueden almacenar en mayúsculas o en minúsculas indistintamente, ya que todas las comparaciones y funciones de dominios se definen como insensibles a mayúsculas y minúsculas. Por tanto, www.midominio.com es idéntico a WWW.MIDOMINIO.COM para las operaciones DNS.

Un nombre de dominio usualmente consiste en dos o más etiquetas, separadas por puntos cuando se las escribe en forma de texto. Por ejemplo, www.theoatmeal.com o es.Wikipedia.org

Como vemos en el gráfico anterior, el raíz del árbol es el punto (.) que es la primera parte del nombre DNS (los nombres DNS se “escriben” de derecha a izquierda). Este punto normalmente nunca se representa ni se escribe para simplificar los nombres.

A la etiqueta ubicada más a la derecha (sin contar el punto) se le llama dominio de nivel superior (Top Level Domain). Como **com** en www.theoatmeal.**com** o **es** en www.Wikipedia.**es**

Cada etiqueta a la izquierda especifica una subdivisión o subdominio. (No hay que confundir los "dominios y subdominios" DNS con los dominios y subdominios de Windows). En teoría, esta subdivisión puede tener hasta 127 niveles, y cada etiqueta contener hasta 63 caracteres, pero restringido a que la longitud total del nombre del dominio no exceda los 255 caracteres, aunque en la práctica los dominios son casi siempre mucho más cortos.

Finalmente, la parte más a la izquierda del dominio suele expresar el nombre de la máquina (hostname). Más a la izquierda aún se puede colocar un prefijo como www, ftp, etc. Estos prefijos no forman parte real del nombre DNS y solo se utilizan para indicar que tipo de protocolo se va a usar para la conexión, no tienen ninguna utilidad adicional.

DOMINIOS SUPERIORES.

Un dominio superior es un dominio de DNS directamente debajo de la raíz (el punto final de cualquier host DNS aunque normalmente no se representa). Resulta difícil crear nombres adicionales, al menos en Internet. Las tres categorías de dominios superiores son las siguientes:

- <ARPA>. Es un dominio especial, se usa en la actualidad para búsqueda inversa de nombres.
- Dominios de 3 letras. Existen siete dominios superiores de 3 caracteres. (en la actualidad, estos nombres se han incrementado con algunos más).
- Nombres de 2 letras para los países. Estos dominios con código de país se basan en los nombres de país de la Organización Internacional de Normalización (ISO) y se usan, principalmente, por compañías y organizaciones fuera de los EE.UU.

REGISTROS DE RECURSOS DE DNS.

Un registro de recurso es un registro que contiene información relacionada con un dominio que puede contener la base de datos de DNS y que puede solicitar y usar un cliente de DNS. Por ejemplo, el RR de host de un dominio concreto mantiene la dirección de IP de tal dominio (host); un cliente de DNS podrá utilizar este RR para conseguir la dirección de IP para el dominio.

Cada servidor de DNS contiene los RR relacionados con aquellas porciones del espacio de nombre de DNS para el que es autoridad, o para el que puede responder las solicitadas por un host.

Cuando un servidor de DNS es autorizado para una porción del espacio de nombres de DNS, dicho servidor es el responsable de asegurar que la información sobre esa porción del espacio de nombres de DNS es correcta. Para aumentar la eficiencia, un servidor de DNS dado puede hacer caché de los RR relativos a un dominio de cualquier parte del árbol de dominios.

Cada RR contendrá un conjunto de información común, como la siguiente:

- Propietario. Indica el dominio de DNS en el que se encuentra el registro de recurso.

- TTL. Tiempo que utilizan otros servidores de DNS para determinar durante cuánto tiempo se hace caché de la información de un registro antes de descartarla. Para la mayoría de los RR, este campo es opcional. El valor de TTL se mide en segundos, con un valor de 0 que indica que el RR contiene datos volátiles que no se deben guardar en caché. Por ejemplo, los registros SOA tienen un valor de TTL predeterminado de 1 hora. De esta forma se evita que otros servidores mantengan en caché estos registros durante largos períodos de tiempo, lo que podría retrasar la propagación de cambios.

- Clase. Para la mayoría de los RR, este campo es opcional. Cuando se utiliza, contiene un texto mnemónico que indica la clase de un RR. Por ejemplo, una clase con IN indica que el registro pertenece a la clase Internet (IN). Alguna vez existieron muchas clases, como CH para Chaos Net, pero en la actualidad sólo se usa la clase IN.

- Tipo. Este campo es requerido y mantiene un texto que indica el tipo del RR. Por ejemplo, la letra A indica que el RR guarda la información de dirección (Address) del host.

- Datos específicos del registro. Es un campo de tamaño variable que contiene información que describe el recurso. Este formato de información varía de acuerdo con el tipo y clase del RR.

Los archivos de zona de DNS estándar contienen el conjunto de RR de dicha zona en un archivo de texto. En este archivo de texto, cada RR se encuentra en una línea separada y contiene todos los elementos de datos anteriores, como un conjunto de campos de texto separados por espacios en blanco.

```
$TTL 86400 ; 1 day
$ORIGIN example.com.
@                IN       SOA      linux01.example.com.       hostmaster.example.com.
@                IN       NS       linux01.example.com.
@                IN       NS       linux02.example.com.
;-------
;  Hosts in the Primary Data Centre - 192.168.1.0/24
;-------
router01 IN      A        192.168.1.1
linux01 IN       A        192.168.1.10
router02 IN      A        192.168.2.1
linux02 IN       A        192.168.2.10
router03 IN      A        192.168.3.1
router03 IN      A        192.168.4.1
linux03 IN       A        192.168.4.10
```

REGISTROS DE RECURSOS QUE ADMITE WINDOWS SERVER.

Existen numerosos tipos de RR definidos. La mayoría de los tipos de RR ya no se necesitan ni se usan, aunque todos esos están disponibles en Windows Server. Los RR usados más habitualmente, son:

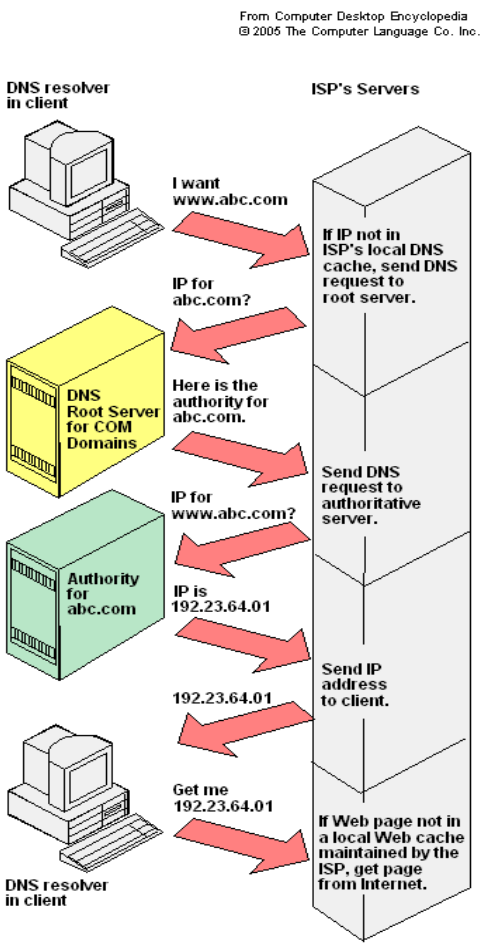
- Dirección de host (A) Address 32 bits. Este RR contiene la dirección de host que hace corresponder un nombre de dominio de DNS con una dirección de IPv4 de 32 bits.

    - Ejemplo: `LINUX03 IN A 192.168.4.10`

- Dirección de host (AAAA) Address de 128 bits. Este RR contiene la dirección de host que hace corresponder un nombre de dominio DNS con una dirección de IPV6 de 128 bits.
  - Ejemplo: `LINUX03 IN A 4321:0:1:2:3:4:567:89ab`
- Nombre canónico (CNAME) canonical name. El RR nombre canónico (CNAME) permite crear alias (sobrenombres) para un host.
  - Ejemplo: `SERVIDOR3 CNAME LINUX03`
- Puntero (PTR) Pointer reverse. Este RR se usa para los mensajes de búsqueda inversa de nombre, es decir, en vez de buscarse un nombre y devolver su dirección IP, se busca una dirección IP y se devuelve el nombre. Normalmente, se usa el árbol de dominio in-addr.arpa para la búsqueda inversa de la correspondencia dirección-nombre.
  - Ejemplo: `192.168.4.10 IN PTR LINUX03`
- Localizador de servicio (SRV) [Server] El RR SRV (Service Locator) permite a un equipo localizar un host que disponga de un cierto servicio, como el Controlador de dominio del Active Directory de Windows Server.
- Servidores de Nombre (NS). El RR NS permite a un equipo localizar a los servidores de nombre, es decir, a los propios servidores DNS.

Especial atención debemos prestar cuando usemos Windows Server a los RR PTR dado que estos registros deben estar en una zona de búsqueda inversa, y dicha búsqueda no se crea automáticamente en Windows Server, tendremos que crearla manualmente cada vez que instalemos un servidor DNS que funcione en una zona integrada de Active Directory.

OPERACIÓN DE SOLICITUD DE DNS



Como vemos en el gráfico de la derecha, nuestra maquina necesita resolver un nombre de dominio (por ejemplo www.bekkoame.co.jp). Para conocer su dirección IP, le enviará una petición de un registro de recurso (RR) de tipo A a nuestro servidor DNS (el que tengamos configurado en las propiedades de red).

Si nuestro servidor DNS tiene un RR de tipo A de nuestra petición nos enviará directamente el RR, con lo que sabremos que su dirección ip es 202.11.252.20.

Pero es bastante habitual que nuestro servidor DNS no tenga ningún registro sobre ese nombre (sería imposible e indeseable que en un solo servidor estuvieran almacenados todos los RR de todos los nombres de todas las máquinas de internet).

En estos casos, nuestro servidor DNS manda una petición de ayuda a un servidor root de Internet (hay 13 root-servers principales en internet). El servidor root normalmente no devuelve la dirección IP de nuestra petición, sino que busca la dirección IP del servidor DNS que tiene autoridad (SOA, Start of Autority) sobre nuestra petición. En nuestro caso, y como nuestra petición www.bekkoame.co.jp pertenece a Japón (jp) nos devolvería la dirección a un servidor con autoridad sobre Japón.

Ahora solicitamos al nuevo servidor DNS de Japón un RR de tipo A sobre www.bekkoame.co.jp y normalmente nos responderá sin problemas. Si este servidor tampoco es capaz de encontrar el host, obtendríamos el mensaje de host inexistente.

SOLICITUD INVERSA

Una solicitud inversa es aquella en la que se solicita a un servidor de DNS el nombre de dominio de DNS de un host con una determinada dirección de IP. Los mensajes de Solicitud de búsqueda inversa son, realmente, solicitudes estándar, pero relacionadas con las zonas de búsqueda inversa.

Las zonas de búsqueda inversa se basan en el nombre de dominio in-addr.arpa y mantiene, principalmente, los RR de PTR.

En este tipo de solicitudes lo que se manda al servidor DNS no es un nombre de host del que queremos saber su IP, sino lo inverso o contrario, le mandamos una IP y queremos que nos devuelva el nombre.

CLASES DE SOLICITUDES DE DNS

Las solicitudes de DNS pueden ser de dos clases: recursivas o iterativas.

Una solicitud **recursiva** es una solicitud de DNS que se envía a un servidor de DNS en la que el host solicitante pregunta al servidor de DNS para que le proporcione una respuesta completa a la solicitud, aunque ello signifique que tenga que ponerse en contacto con otros servidores para obtener la respuesta.

Una solicitud **iterativa** es una solicitud de DNS que se envía a un servidor de DNS en el que el host solicitante pide que se devuelva la mejor respuesta que el servidor de DNS pueda proporcionar sin buscar ayuda adicional de otros servidores de DNS.

En general, los equipos envían solicitudes recursivas. Los equipos suponen que el servidor de DNS conoce la respuesta a la solicitud, o puede encontrarla.

Por otra parte, un servidor de DNS normalmente enviará solicitudes iterativas a otros servidores de DNS si no puede responder a la solicitud con la información de que dispone.

OPERACIÓN DE ACTUALIZACIÓN DE DNS

Una operación de actualización de DNS la envía un cliente a un servidor de DNS para actualizar, añadir o eliminar algunos o todos los RR de información relacionada con un determinado dominio, por ejemplo, para actualizar el registro de host del equipo con nombre kona.midominio.com para que apunte a 10.10.1.100. La operación de actualización también se denomina actualización dinámica.

RESOLUCIÓN DE NOMBRES: RESOLUTOR DE DNS

En Windows, el resolutor de DNS es un componente del sistema que realiza solicitudes de DNS a otro u otros servidores de DNS. La pila de TCP/IP de Windows se configura, normalmente, con la dirección de IP de al menos un servidor de DNS al que el resolutor envía una o más solicitudes de información de DNS.

En Windows, el resolutor forma parte del servicio Cliente de DNS. Este servicio se instala automáticamente cuando se instala TCP/IP y se ejecuta como parte del proceso Services.Exe.

CACHÉ DEL RESOLUTOR DE DNS

Un host de IP podría necesitar ponerse en contacto periódicamente con otro host y por tanto necesitaría resolver un nombre concreto de DNS muchas veces, como por ejemplo el nombre del servidor de correo electrónico.

Para evitar tener que enviar solicitudes a un servidor de DNS cada vez que el host quiere resolver el nombre, Windows Server implementa una caché especial de información de DNS.

```
G:\>IPCONFIG /DISPLAYDNS

Configuración IP de Windows 2000

    localhost.
    ----------------------------------------
      Nombre de registro. . : localhost
      Tipo de registro . . .: 1
      Tiempo de vida  . . . : 31532890
      Longitud de los datos : 4
      Sección . . . . . . . : Answer
      Un registro (Host). . :
                         127.0.0.1


    1.0.0.127.in-addr.arpa.
    ----------------------------------------
      Nombre de registro. . : 1.0.0.127.in-addr.arpa
      Tipo de registro . . .: 12
      Tiempo de vida  . . . : 31532890
      Longitud de los datos : 4
      Sección . . . . . . . : Answer
      Registro PTR. . . . . :
                         localhost
```

El servicio Cliente de DNS hace caché de los RR recibidos en las respuestas a las solicitudes de DNS. La información se mantiene durante un Período de vida, TTL (Time To Live), y se puede utilizar para responder solicitudes posteriores. De forma predeterminada, la caché utiliza el valor de TTL recibido en la respuesta de solicitud de DNS. Cuando se resuelve una solicitud, el servidor autoridad de DNS en el dominio resuelto define el TTL para un RR dado.

Puede utilizar el comando IPCONFIG con la opción /DISPLAYDNS para mostrar el contenido actual de la caché del resolutor.

CACHÉ NEGATIVA

El servicio Cliente de DNS también utiliza una caché negativa. La caché negativa ocurre cuando no existe un RR de un nombre de dominio solicitado o cuando el propio nombre de dominio no existe, en cuyo caso se guarda la falta de resolución. La caché negativa evita repetir solicitudes adicionales de RR o dominios que no existen.

Si se realiza una solicitud a un servidor de DNS y la respuesta es negativa, las siguientes solicitudes al mismo nombre de dominio se responden negativamente durante un tiempo predeterminado de 300 segundos.

Para evitar guardar en la caché información negativa anticuada, cualquier información de solicitud respondida negativamente se mantiene durante un período de tiempo inferior al que se utiliza para las respuestas positivas. Con la caché negativa se reduce la carga en los servidores de DNS, pero estarán disponibles los RR relevantes, y se podrán enviar solicitudes posteriores para obtener la información.

Si se realiza una solicitud a todos los servidores de DNS y no está disponible ninguno durante un tiempo predeterminado de 30 segundos, las solicitudes posteriores por nombre fallarán inmediatamente en lugar de esperar los plazos. De esta forma se puede ahorrar tiempo en servicios que utilizan DNS durante el proceso de arranque, sobre todo cuando se arranca de la red.

La orden IPCONFIG puede ser usada con el parámetro /FLUSHDNS para vaciar la caché del resolutor, con lo que también eliminamos la caché negativa.

DELEGACIÓN DE ZONA

DNS es una base de datos distribuida de información diseñada específicamente para superar las limitaciones de la resolución de nombres anterior con el archivo HOSTS.TXT.

La función que permite a DNS manejar grandes espacios de nombres/redes, como Internet, es su capacidad para delegar la administración de dominios. Se produce una delegación de zona cuando la responsabilidad de los RR de un subdominio se traslada del propietario del dominio principal al propietario del subdominio.

En el núcleo de Internet existen 13 servidores raíz, denominados de A.ROOTSERVERS.NET a M.ROOT-SERVERS.NET. Los servidores raíz están extensamente distribuidos. Mantienen datos de todos los dominios de nivel superior, como los .com, .org y .net, así como para los dominios geográficos como .uk y .jp. Estos servidores raíz permiten a los hosts de Internet tener un acceso a toda la base de datos de DNS. Por debajo de los dominios raíz y superior están los dominios y subdominios de las organizaciones individuales. En algunos dominios superiores existen niveles jerárquicos adicionales. Por ejemplo, en el domino .uk existe un subdominio co.uk para las compañías de UK (por ejemplo, psp.co.uk) y ac.uk para las instituciones académicas (por ejemplo, ic.ac.uk para el Imperial Collage).

La delegación ocurre como una división del DNS en las responsabilidades para los dominios debajo de la división que se delega del dominio superior. En el dominio midominio.com está el subdominio jh.midominio.com. La responsabilidad para el dominio subordinado se ha delegado a un servidor diferente.

Para implantar la delegación, la zona superior debe tener tanto un RR A como un registro de Servicio de nombre (NS), ambos apuntando a la nueva raíz de dominio delegado.

CLIENTE DE ACTUALIZACIÓN DINÁMICA DE DNS

En grandes redes, conseguir toda la información de RR necesaria en el DNS y mantenerla actualizada puede ser una tarea agotadora. El mantenimiento de los registros de hosts, en algunos entornos, puede ser un trabajo a tiempo completo para una o más personas. Para simplificar esta tares, Windows Server incluye la actualización dinámica de DNS.

Mediante el DNS dinámico, los clientes envían un mensaje de registro de DNS al servidor de DNS, indicándole que actualice el registro (A) para el host. Además, si el cliente es también cliente de DHCP, cada vez que ocurre un suceso de dirección, por ejemplo, una concesión de una nueva dirección o una renovación de dirección, como parte del proceso de administración de las concesiones de DHCP, el cliente de DHCP envía la Opción 81 al servidor de DHCP junto con su nombre completo. La Opción 81 indica al servidor de DHCP que registre el RR PTR por él.

Este mecanismo, donde el cliente actualice el registro (A) y el servidor de DHCP actualice el registro PTR, es el elegido porque sólo el cliente conoce qué direcciones de IP en el host se corresponden con el nombre del host. El servidor de DHCP puede que no sea capaz de realizar correctamente el registro del RR (A) debido a un conocimiento parcial. Si resulta apropiado también se puede configurar el servidor de DHCP para registrar ambos registros en el DNS.

INSTALACIÓN Y CONFIGURACIÓN DE UN SERVIDOR DNS.

Los servidores DNS son una parte esencial de una red basada en TCP/IP además de una parte esencial del Active Directory. Microsoft recomienda la instalación de DNS en cada controlador de dominio cuando se utilice Active Directory.

Esta solución permite al servidor DNS dinámico de Windows Server utilizar Active Directory para almacenar información de la zona, permitiendo de este modo la réplica con múltiples maestros completa de la zona por medio de Active Directory, simplificando la tarea de conseguir la tolerancia a fallos y haciendo menos difícil la administración del DNS.

Es fundamental instalar DNS en el controlador primario que forme la raíz del árbol en un bosque nuevo.

Si no se instaló DNS en el controlador de dominio durante la instalación de Windows Server, será necesario usar uno que ya esté instalado en la empresa y habrá que configurarlo para que trabaje con nuestro dominio. También es posible instalar el servidor DNS en nuestro servidor después de instalar nuestro dominio, pero es una operación complicada y engorrosa.

CONFIGURACIÓN DEL SERVICIO DNS

Las zonas son los cerebros del DNS; por lo tanto, el servidor DNS es inútil hasta que se configuren las zonas del dominio. Las zonas permiten almacenar porciones del espacio de nombres del DNS de forma que un único servidor DNS pueda servir una porción del espacio de nombres. Así, si creamos un dominio INSTITUTO.LOCAL tendremos que crear una zona INSTITUTO.LOCAL en un servidor DNS.

Cuando se configuran los dominios, hay que comenzar por el dominio de nivel más alto. Después hay que crear los subdominios y delegar el control de los dominios a otros servidores DNS si fuese necesario. Podemos elegir si INFORMATICA.INSTITUTO.LOCAL es una zona DNS dentro del mismo servidor DNS que ya tenemos instalado, o bien instalar un nuevo servidor DNS que tendrá delegada la zona INFORMATICA y dependerá del servidor DNS de la zona principal INSTITUTO.LOCAL.

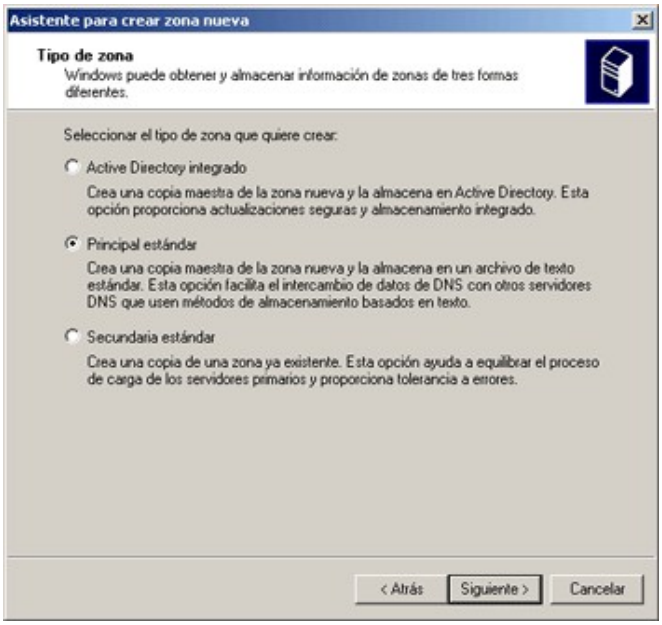
Los dos tipos de zonas que es necesario tomar en consideración son las zonas de búsqueda directa y las zonas de búsqueda inversa.

- Las zonas de búsqueda directa son los tipos de zonas que se asocian normalmente con servidores DNS; ellas devuelven una dirección IP cuando se les proporciona un nombre DNS. Estas zonas se suelen crear automáticamente cuando instalamos el Active Directory, de modo que no tendremos que crearlas a mano. Sin embargo, su creación no es inmediata, y suelen necesitar que exista cierta actividad dentro del dominio antes de que se creen correctamente.
- Las búsquedas inversas se utilizan menos a menudo, aun siendo importantes de todos modos. Proporcionan la capacidad de asignar un nombre DNS a una dirección IP, algo que los Servicios de Internet Information Server (IIS) también utilizan para sus archivos de registro y herramientas de solución de problemas como Nslookup. Es importante destacar que estas zonas de búsqueda inversa no se crean automáticamente, y tendremos que crearlas siempre a mano. Si no creamos dichas zonas, será imposible realizar ciertas funciones en Active Directory.

CREACIÓN DE UNA NUEVA ZONA

Para crear una nueva zona de búsqueda directa en el servidor DNS para que los clientes puedan obtener la dirección IP de un nombre DNS, hay que seleccionar DNS en la carpeta Herramientas administrativas, Seleccionar el servidor DNS en el árbol de la consola.

Escoger entonces Crear una zona nueva en el menú Acción para iniciar el Asistente para crear zona nueva. Hay que pulsar Siguiente para comenzar a utilizar el asistente.

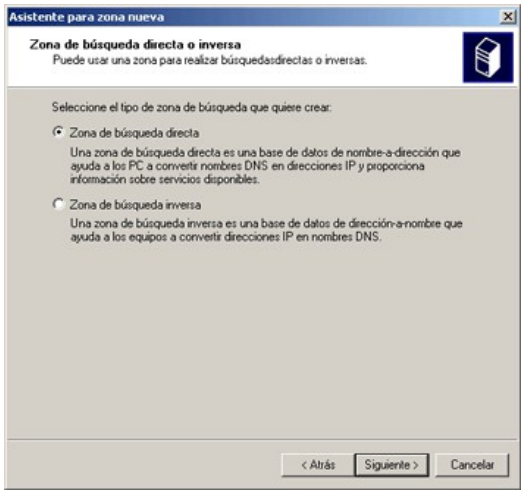


Tipo de Zona: En esta ventana hay que escoger una de las siguientes opciones y pulsar entonces Siguiente para continuar:

Active Directory integrado: Se debe utilizar si todos los controladores de dominio ejecutan Windows Server. Esta opción también se puede utilizar en una red mixta si los servidores UNIX son compatibles con el DNS de Microsoft.

Principal estándar: Se debe utilizar si el servidor DNS ejecuta Windows Server pero no es un controlador de dominio.

Secundaria estándar: Se debe utilizar si el servidor DNS está alojado en servidores UNIX. También se debe utilizar si este servidor va a tener privilegios de sólo lectura en la zona para toda la información obtenida del servidor DNS principal.

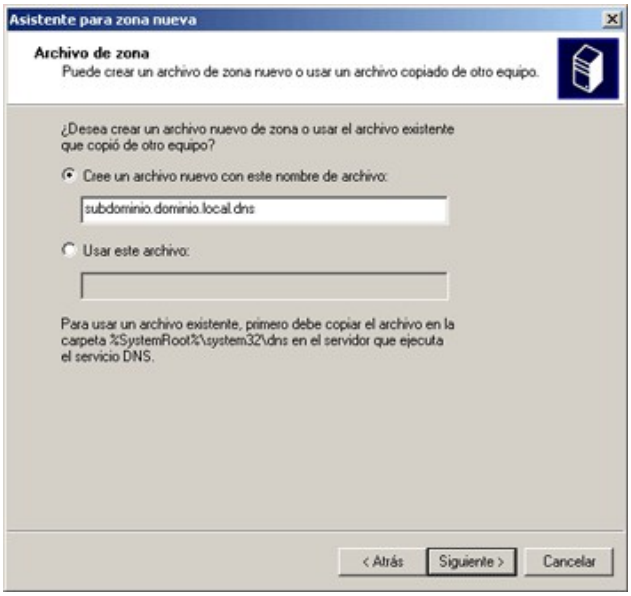


Zona de búsqueda directa o inversa. Esta ventana nos permite escoger el tipo de zona que queremos crear.

Zona de búsqueda directa: Es la que permite a los clientes buscar los equipos de la red a través de los nombres, convirtiendo los nombres DNS a direcciones IP.

Zona de búsqueda inversa: Las zonas de búsqueda inversa permiten a los clientes obtener el nombre DNS de un host a partir de una dirección IP, lo que resulta útil para herramientas de solución de problemas como Nslookup. Y realizar una búsqueda inversa junto con los archivos de registro de IIS permite el registro de un nombre DNS en lugar de una dirección IP. Para crear una zona de búsqueda inversa tenemos que indicar la parte fija de las direcciones IP de nuestra red. Normalmente en nuestro caso siempre creamos la zona de búsqueda inversa como 192.168.x.x.

Nombre de Zona: Introducir el nombre DNS para la zona en el cuadro de texto Nombre y pulsar Siguiente



Si se ha escogido la instalación de una Zona Active Directory Integrada, se creará ahora. Si se está creando una Zona principal estándar, seguirá el proceso de instalación. Para una Zona secundaria estándar se abre la ventana Servidores maestros DNS. Hay que introducir las direcciones IP de los servidores maestros de los cuales se desea copiar la información de zona, pulsando Agregar después de introducir cada una. Se puede utilizar el botón Examinar para buscar servidores. Se pueden utilizar los botones Arriba y Abajo para organizar las direcciones IP en el orden en el que se deseen contactar. Hay que pulsar Siguiente cuando se haya terminado y pulsar después Finalizar para completar la configuración de la zona secundaria.

Archivo de Zona: Nos permitirá elegir el archivo que queremos utilizar para la Zona DNS que estamos creando.

Cree un archivo nuevo con este nombre de archivo: introducir el nombre que se le quiere dar al archivo de zona o utilizar el que se proporciona.

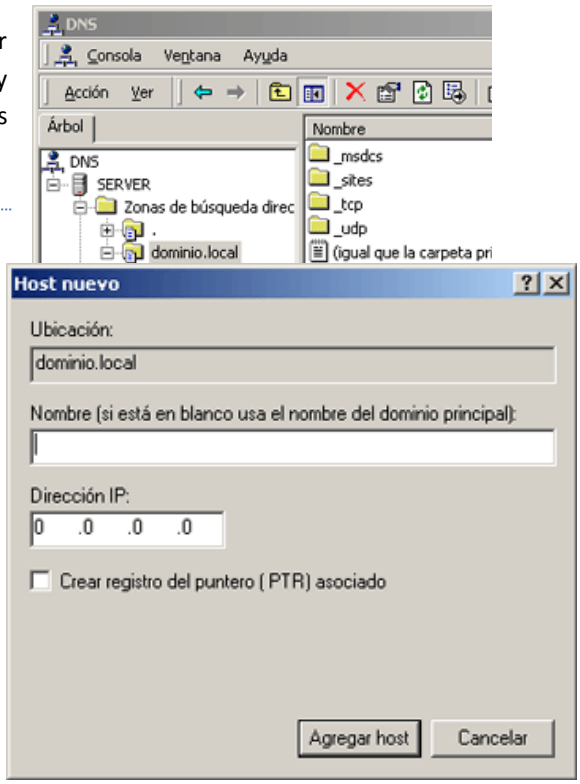
Usar este archivo: Para utilizar un archivo de zona existente para almacenar la información de la zona, hay que copiar el archivo a la carpeta %SystemRoot%\System32\DNS. Esta es la opción a elegir si estamos importando una Zona DNS desde otro sistema.

CREACIÓN DE SUBDOMINIOS Y DELEGACIÓN DE AUTORIDAD

En muchos entornos de red grandes es necesario crear subdominios y delegar su administración a otras zonas DNS que estén alojadas en otros servidores DNS. Este paso elimina la situación de tener un enorme espacio de nombres alojado en una única zona de un único servidor. Por lo tanto, se debería tener una zona que contuviera el dominio raíz dominio.com además del subdominio marketing.dominio.com; sin embargo, se debería tener el subdominio subdominio.dominio.com y sus subdominios delegados a una zona separada administrada por otro servidor DNS.

Hay que asegurarse de que se tiene un registro de host creado para el servidor DNS en la Zona de búsqueda directa y un registro del puntero para el servidor DNS en la Zona de búsqueda inversa. Puede que el DNS no los cree automáticamente (especialmente el registro del puntero), por lo que conviene verificar ambos; en otro caso el servidor podría no funcionar.

Conviene observar que las zonas deben tener un espacio de nombres contiguo, por lo que no es posible combinar subdominios de diferentes ramas del espacio de nombres y situarlos en una única zona: sería necesario crear zonas separadas para cada parte no contigua del dominio.



AGREGACIÓN DE REGISTROS DE RECURSOS DEL HOST

Después de crear las zonas y los subdominios se deberían añadir registros de recursos (RR) para el servidor del dominio y cualquier otro servidor con direcciones IP estáticas o reservas de IP (servidores DHCP, servidores WINS, enrutadores, etc.). El servidor DNS no funcionará adecuadamente sin un registro de host y un registro del puntero, este último no se creará de forma automática.

- Seleccionar la zona y dominio o subdominio al cual pertenece el host y escoger entonces Host nuevo en el menú Acción. Escoger el tipo de RR que queremos crear. (En este caso Tipo A).
- Introducir el nombre del host o dejar el cuadro Nombre en blanco para utilizar el nombre del dominio principal. Hay que introducir la dirección IP del host.
- Seleccionar Crear registro del puntero (PTR) asociado para crear un RR para el host en la zona de búsqueda inversa.
- Pulsar Agregar host y rellenar después los campos para cualquier registro de host adicional que se quiera crear o pulsar Realizado.

Cuando instalamos el DNS por primera vez, veremos cómo aparecen algunos hosts del tipo A con nombre de host y que sin embargo no están creados en la zona de búsqueda inversa. Estos host hay que borrarlos de la zona directa y volver a crearlos de la forma que se ha explicado, marcando la casilla Crear registro del puntero PTR asociado.

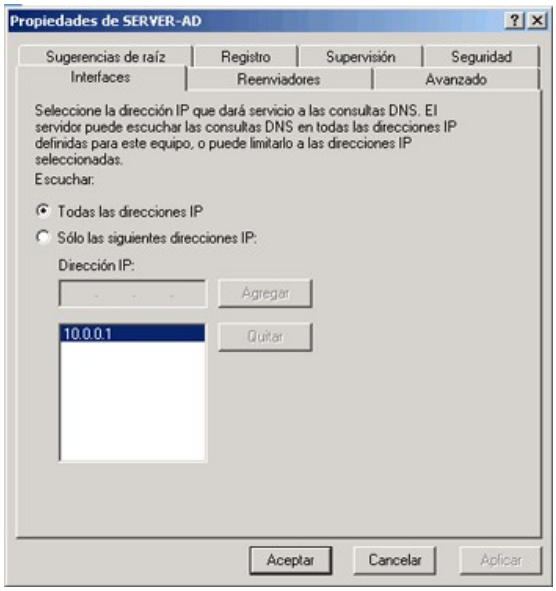
Para actualizar manualmente el archivo de zona, hay que seleccionar la zona que se desea actualizar y escoger entonces Actualizar archivo de datos del servidor en el menú acción.

INTEROPERACIÓN CON OTROS SERVIDORES DNS

De forma predeterminada, el servidor DNS de Windows Server realiza transferencias de zona rápidas con compresión de datos y envío de múltiples registros de recursos en cada mensaje. Este método de transferencia de zona funciona con todos los servidores DNS de Windows y servidores DNS BIND versión 4.9.4 o posterior. Si se necesita realizar transferencias de zona con servidores BIND anteriores a la versión 4.9.4, será necesario desactivar este método de transferencia de zona rápida. Hay que seleccionar el servidor DNS en el árbol de la consola y escoger propiedades en el menú Acción. Después hay que pulsar la pestaña Avanzado y desactivar la casilla de verificación Enlazar secundarios.

ADMINISTRACIÓN DEL SERVIDOR DNS.

PESTAÑA INTERFACES.



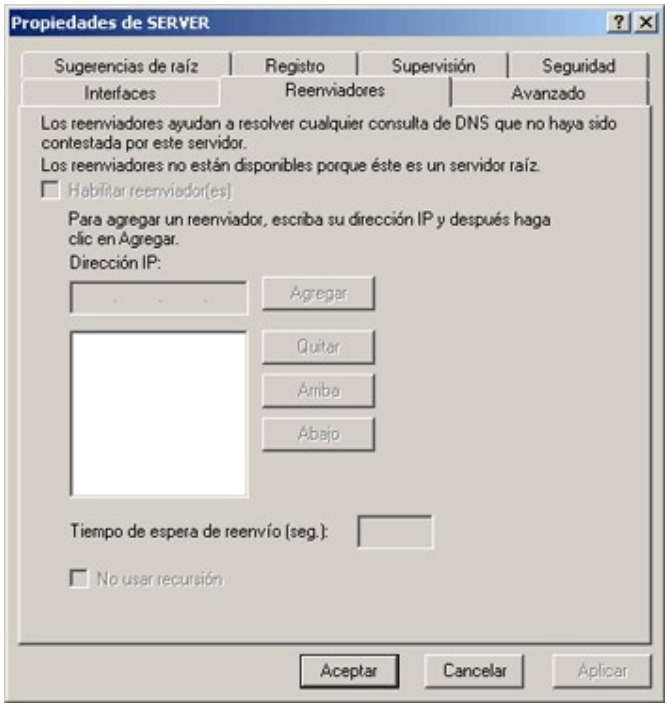
En el caso de los servidores DNS multitarjeta (que funcionan en ordenadores con varias tarjetas de red), puede configurar el servicio DNS para habilitar de forma selectiva y enlazar sólo con las direcciones IP que especifique con la consola DNS. De forma predeterminada, el servicio DNS enlaza con todas las interfaces IP configuradas para el equipo. Esto puede incluir:

Cualquier dirección IP adicional configurada para una conexión de red única.

Direcciones IP individuales configuradas para cada conexión diferente donde haya instaladas más de una conexión de red en el equipo servidor.

En el caso de los servidores DNS multitarjeta, puede restringir el servicio DNS para las direcciones IP seleccionadas. Cuando se utilice esta característica, el servicio DNS sólo atenderá y responderá a las peticiones DNS que se envíen a las direcciones IP especificadas en la ficha Interfaz de las Propiedades del servidor.

PESTAÑA REENVIADORES



Ningún servidor de nombres será capaz de responder a las consultas de todos los clientes; algunas veces los clientes solicitarán un nombre DNS que no se encuentra en ninguna de las zonas administradas por el servidor DNS. En estos casos, se puede configurar un servidor DNS para que reenvíe la petición a otro servidor DNS con más probabilidad de tener el registro en su zona o archivo caché. Esta capacidad se necesita más frecuentemente para resolver nombres externos a la red en la que residen los clientes.

Cuando un cliente quiere resolver un nombre fuera de la red interna, se puede configurar un servidor DNS interno para que reenvíe la consulta a un servidor DNS externo a la red, quizás al otro lado de un cortafuego. Este servidor de nombres externo puede entonces realizar consultas más a fondo fuera de la red si es necesario y devolver los resultados al servidor DNS reenviador. Para configurar el servidor DNS de forma que reenvíe las consultas no resueltas a otro servidor DNS, hay que seguir estos pasos:

(Por razones de seguridad, un único servidor DNS reenviará por regla general las peticiones de la red interna a un servidor DNS al otro lado de un cortafuego. El resto de los servidores DNS internos reenvían sus consultas al reenviador designado para que sean pasadas al servidor de nombres externo (o resueltas a partir del archivo caché del reenviador).

1. En el árbol de la consola, hay que seleccionar el servidor DNS sobre el que se desea activar el reenvío, y escoger después propiedades en el menú Acción.
2. Escoger la ficha Reenviadores y seleccionar la casilla de verificación Habilitar reenviador(es).
3. Introducir las direcciones IP del servidor o servidores DNS a los cuales se desea reenviar las consultas no resueltas, pulsando el botón Agregar tras introducir cada una.

Antes de avanzar al siguiente servidor de la lista de servidores a los que reenviar consultas, hay que introducir la cantidad de tiempo que se desea emplear en contactar con un servidor DNS.

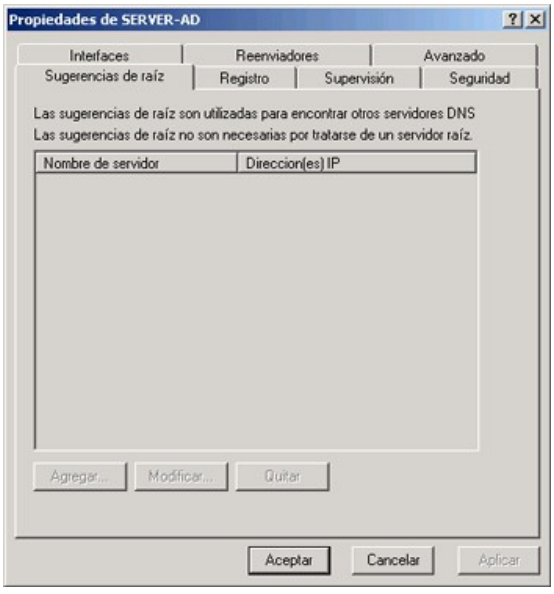
Para configurar el servidor DNS como un servidor esclavo -un servidor que no trata de resolver ninguna consulta a partir de sus propios archivos de zona o caché- hay que seleccionar la casilla de verificación No usar recursión

PESTAÑA AVANZADAS

Cuando se inicia el servicio, los servidores DNS de Windows Server utilizan los valores de configuración del servidor obtenidos de los parámetros establecidos en el archivo de información de inicio, en el Registro de Windows Server o en los valores predeterminados que proporciona la integración de Active Directory.

En la mayoría de las situaciones, los valores predeterminados de la instalación son aceptables y no deberían necesitar modificaciones. Sin embargo, cuando sea necesario puede utilizar la consola DNS para ajustar los siguientes parámetros avanzados, que permiten adaptarse a las situaciones y necesidades especiales de distribución.

PESTAÑA SUGERENCIAS DE RAÍZ



Las sugerencias de raíz se utilizan para preparar los servidores autoritativos para zonas que no sean de raíz, a fin de que puedan aprender y descubrir servidores autoritativos que administran dominios de un nivel superior o de otros subárboles del espacio de nombres del dominio DNS. Estas sugerencias son esenciales para los servidores autoritativos de niveles inferiores del espacio de nombres cuando localicen y busquen servidores en estas condiciones.

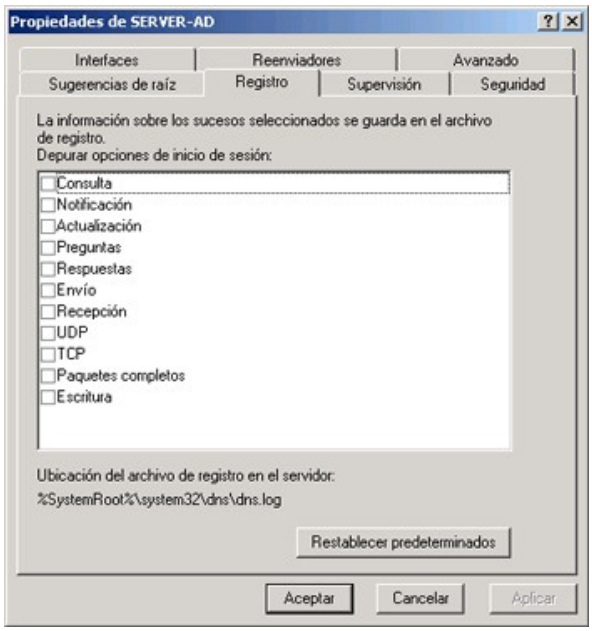
Por ejemplo, suponga que un servidor DNS (Servidor A) tiene una zona llamada sub.ejemplo.microsoft.com. En el proceso de respuesta a una consulta de un dominio de nivel superior, como

el dominio microsoft.com, el Servidor A necesita ayuda para ubicar un servidor autoritativo (como el Servidor B) de este dominio.

Para que el Servidor A encuentre al Servidor B o cualquier otro servidor autoritativo para el dominio microsoft.com, es necesario que pueda consultar a los servidores raíz del espacio de nombres DNS.

Los servidores raíz pueden remitir el Servidor A a los servidores autoritativos del dominio com. A su vez, los servidores del dominio com pueden ofrecer referencia al Servidor B u otros servidores autoritativos para el dominio microsoft.com.

Las sugerencias de raíz utilizadas por el Servidor A deben tener sugerencias útiles para los servidores raíz a fin de que este proceso localice al Servidor B (u otro servidor autoritativo), como se pretende.



PESTAÑA REGISTROS

Para los servidores DNS de Windows Server se pueden utilizar las siguientes opciones de registro de depuración:

- Consulta: Registra consultas recibidas por el servicio del Servidor DNS desde los clientes.
- Notificar: Registra mensajes de notificación recibidos por el servicio del Servidor DNS desde otros servidores.
- Actualización: Registra actualizaciones dinámicas recibidas por el servicio del Servidor DNS desde otros equipos.
- Preguntas: Registra el contenido de la sección de preguntas de cada mensaje de consulta DNS procesado por el servicio del Servidor DNS.
- Respuestas: Registra el contenido de la sección de respuestas de cada mensaje de consulta DNS procesado por el servicio del Servidor DNS.
- Envío: Registra los distintos mensajes de consulta DNS enviados por el servicio del Servidor DNS.
- Recepción: Registra los distintos mensajes de consulta DNS recibidos por el servicio del Servidor DNS.
- UDP: Registra las distintas solicitudes DNS recibidas por el servicio del Servidor DNS a través de un puerto UDP.
- TCP: Registra las distintas solicitudes DNS recibidas por el servicio del Servidor DNS a través de un puerto TCP.

- Paquetes completos: Registra los distintos paquetes completos escritos y enviados por el servicio del Servidor DNS.
- Escritura: Registra los distintos paquetes escritos completamente por el servicio del Servidor DNS y devueltos a la zona.

De forma predeterminada, todas las opciones de inicio de registro de depuración están deshabilitadas. Cuando se habilitan de forma selectiva, el servicio del Servidor DNS puede realizar un registro adicional a nivel de seguimiento de tipos seleccionados de sucesos o mensajes para solucionar problemas generales y depurar el servidor.

El registro de depuración puede emplear muchos recursos; esto afectará al rendimiento global del servidor y consumirá espacio en disco. Por lo tanto, sólo debe utilizarse temporalmente cuando se necesite información más detallada acerca del rendimiento del servidor.

Dns.log contiene actividad de registro de depuración. Se encuentra en la carpeta windir\System32\Dns.

FICHA INICIO DE AUTORIDAD (SOA) Y FICHA SERVIDORES DE NOMBRES

Las zonas se basan en el concepto de autoridad de servidor. Cuando se configura un servidor DNS para cargar una zona, utiliza dos tipos de registros de recursos para determinar las propiedades autorizadas de la zona.

Primero, el registro de recursos de inicio de autoridad (SOA) indica el nombre de origen de la zona y contiene el nombre del servidor que es el origen principal de información acerca de la zona. También indica otras propiedades básicas de la zona.

Muestra los servidores de nombres (NS) configurados para el servidor o la zona de la manera siguiente:

Cuando esta lista se muestra en la ficha Sugerencias de raíz, que se encuentra en las propiedades de servidor DNS correspondientes, presenta sugerencias de raíz que contienen los servidores raíz que el servidor debe utilizar y a los que debe hacer referencia para resolver nombres. En los servidores raíz, este campo debe estar en blanco.

Cuando esta lista se muestra en la ficha Servidores de nombres, que se encuentra en las Propiedades de zona correspondientes, presenta los servidores DNS configurados actualmente como autoridades para la zona. En la mayor parte de los casos, esto incluye todos los demás servidores que están configurados como secundarios de la zona.

FICHA WINS

El Servicio de nombres Internet de Windows (WINS) se puede usar para buscar nombres DNS que no se pueden resolver mediante la consulta del espacio de nombres de dominio DNS. Para ejecutar la búsqueda WINS, se utilizan dos tipos de registros de recursos específicos que se pueden habilitar para cualquier zona cargada mediante el servicio DNS:

El registro de recursos WINS, que se puede habilitar para integrar la búsqueda WINS en las zonas de búsqueda directa

El registro de recursos WINS-R, que se puede habilitar para integrar la búsqueda inversa WINS en las zonas de búsqueda inversa

Los servicios WINS y DNS se utilizan para proporcionar la resolución de nombres para el espacio de nombres NetBIOS y el espacio de nombres de dominio DNS, respectivamente. Aunque DNS y WINS pueden proporcionar un servicio de nombres útil e independiente a los clientes, WINS se necesita, principalmente, para proporcionar compatibilidad con los clientes y programas antiguos que requieren compatibilidad con los nombres NetBIOS.

Sin embargo, el servicio DNS puede funcionar con WINS para proporcionar búsquedas de nombres combinados en los dos espacios de nombres cuando en una información de zona no se encuentra la resolución de un nombre de dominio DNS. Para proporcionar esta interoperabilidad, se ha definido un nuevo registro (el registro WINS) como parte del archivo de base de datos de zonas.

El registro de recursos WINS es específico para Windows Server y versiones anteriores de Windows NT Server, y se puede conectar sólo al dominio de origen de una zona. La presencia de un registro de recursos WINS puede indicar al servicio DNS que utilice WINS para buscar las consultas directas de nombres de host o nombres que no se encuentran en la base de datos de zonas. Esta funcionalidad es especialmente útil en la resolución de nombres que requieren los clientes que no admiten WINS (por ejemplo, UNIX) para los nombres de los equipos que no se registraron con DNS, como los equipos con Windows 95 o Windows 98.

Usar búsqueda directa WINS: Para impedir que el registro WINS sea replicado a cualquier servidor secundario por motivos de compatibilidad (los servidores DNS no Microsoft no soportan registros WINS-R), hay que seleccionar la casilla de verificación No replicar este registro.

Dirección IP: Introducir la dirección IP de cada servidor WINS que se quiera consultar, pulsando Agregar tras introducir cada una.

SERVIDOR DHCP.

Para que un host con TCP/IP se comunique correctamente con otro, ambos deben estar configurados apropiadamente. Requieren una dirección de IP válida y única, una máscara de subred y una dirección de pasarela predeterminada, aunque se puede omitir si el host sólo se va a comunicar en la subred local. Para redes mayores se necesita configurar otros elementos, como la dirección de IP de un servidor de DNS, la dirección de IP de un servidor WINS y los tipos de nodo NetBIOS.

En grandes redes, asegurar que todos los hosts se han configurado correctamente puede ser una tarea de administración y gestión importante, especialmente en redes dinámicas con usuarios móviles con ordenadores portátiles. La configuración manual o la reconfiguración de un gran número de equipos es una tarea que lleva mucho tiempo y un error en la configuración de un host puede hacer que sea imposible que se comunique con el resto de la red.

DHCP es un protocolo cliente-servidor que simplifica la administración de la configuración de los clientes de IP y la asignación de los datos de configuración de IP. Mediante DHCP, el administrador define todos los parámetros de configuración necesarios en un servidor central, quien proporciona a los hosts toda la información de configuración de IP.

DHCP proporciona tres ventajas clave en la planificación, diseño y mantenimiento de una red de IP:

- Administración centralizada de las configuraciones de IP. El administrador de DHCP puede administrar de manera centralizada toda la información de configuración de IP. De esta forma se elimina la necesidad de configurar manualmente los hosts individualmente cuando se implanta por primera vez TCP/IP o cuando se necesitan cambios en la infraestructura de IP.
- Sencillez en la configuración de IP de host. Mediante DHCP se asegura que los clientes de DHCP obtienen parámetros de configuración de IP precisos y en tiempo, sin intervención del usuario. Como la configuración es automática se elimina gran parte de los problemas.
- Flexibilidad. Utilizando DHCP, el administrador aumenta su flexibilidad para el cambio de la información de configuración de IP, lo que permite que el administrador cambie la configuración de IP de manera sencilla cuando se necesitan los cambios.

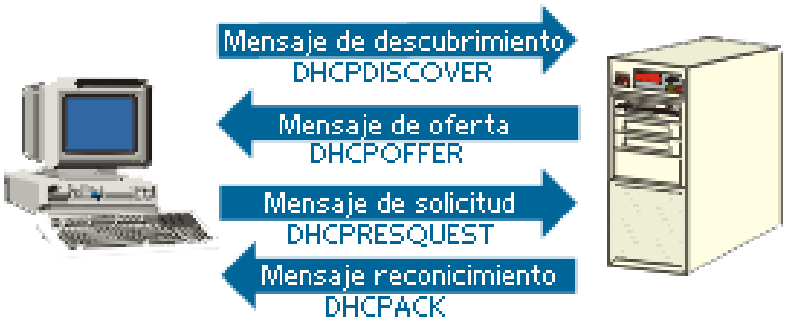
Todos los Windows Server (incluyendo 2000,2003 y 2008) incluyen el servicio Servidor de DHCP, que se instala como opcional. Todos los clientes de Microsoft Windows instalan automáticamente el servicio cliente de DHCP como parte de TCP/IP.

FUNCIONAMIENTO DE DHCP.

Los hosts utilizan el protocolo DHCP para obtener una concesión inicial, renovar una existente y detectar servidores de DHCP no autorizados.

OBTENCIÓN DE UNA CONCESIÓN INICIAL.

La adquisición de una concesión inicial ocurre la primera vez que un cliente de DHCP arranca.



1. El cliente de DHCP difunde, en primer lugar, el mensaje DHCPDISCOVER para buscar un servidor de DHCP. Como el host no tiene dirección de IP, se comunica con el servidor de DHCP mediante un mensaje de difusión en el área local.

2. Si hay más de un servidor de DHCP que puede proporcionar al cliente de DHCP una dirección de IP válida, es posible que el cliente reciba una o más respuestas DHCPOFFER. Si ocurre esto, el cliente elige la «mejor» de ellas, que en Windows Server será la primera recibida. Para ayudar al cliente a decidir cuál es la mejor oferta, el mensaje DHCPOFFER contiene valores para las opciones que el cliente había solicitado y que se configuran en el servidor de DHCP que la entrega. Cualquier servidor de DHCP que recibe un mensaje DHCPDISCOVER y puede asignar al cliente de DHCP una concesión, enviará un mensaje DHCPOFFER con la dirección de IP ofrecida y valores de opción.

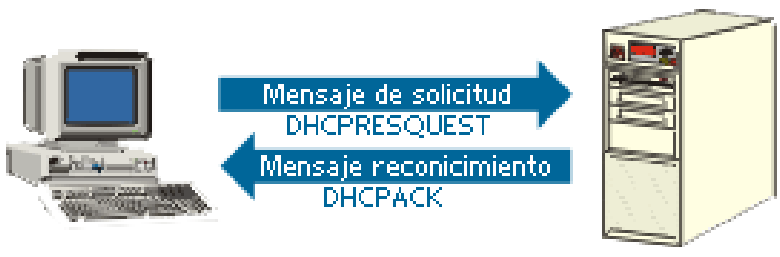
3. Si el cliente puede aceptar esta concesión, envía una DHCPREQUEST al servidor de DHCP, solicitando la dirección de IP ofrecida. Esta solicitud también contendrá todas las opciones de configuración que el cliente de DHCP desea obtener.

4. El mensaje final, DHCPACK, se envía desde el servidor de DHCP hasta el cliente de DHCP para confirmar que el cliente tiene la dirección de IP y los valores de las opciones solicitadas que especificó el administrador de DHCP en el servidor.

RENOVACIÓN DE UNA CONCESIÓN

Los clientes de DHCP intentarán renovar la concesión tras cada reinicio o a intervalos regulares después del inicio del cliente de DHCP.

La renovación de una concesión supone sólo dos mensajes de DHCP, DHCPREQUEST y DHCPACK.



Si el cliente de DHCP renueva una concesión mientras se reinicia, se usan paquetes de IP de difusión para enviar estos mensajes. Si la renovación de la concesión se realiza mientras se está ejecutando el cliente de DHCP, el cliente y el servidor de DHCP se comunican mediante dirección IP unicast.

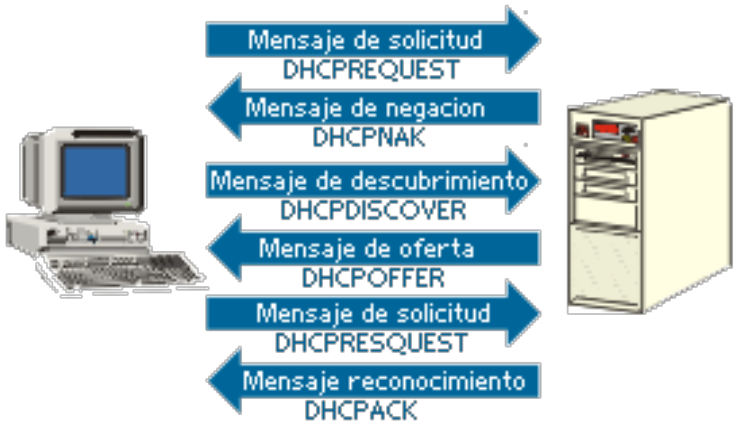
Cuando un cliente obtiene una concesión, DHCP proporciona los valores para las opciones de configuración solicitadas por el cliente.

Reduciendo el tiempo de concesión, el administrador fuerza a los clientes a solicitar periódicamente una renovación de la concesión y obtener detalles actualizados de configuración. Puede ser útil cuando el administrador desea cambiar la configuración de IP de una subred.

Un cliente de DHCP intenta en primer lugar volver a conseguir su concesión a la mitad del tiempo de concesión, conocido como T1. Si falla el cliente intentará de nuevo una nueva renovación de la concesión al 87,5 por 100 del tiempo de concesión, conocido como T2. Si no se consigue obtener la concesión antes de que expire (por ejemplo, si el servidor de DHCP no está accesible), en cuanto expira la concesión el cliente libera la dirección de IP e intenta conseguir una nueva concesión.

CAMBIOS EN SUBREDES Y SERVIDORES.

Si el cliente de DHCP solicita una conexión mediante un mensaje DHCPREQUEST y el servidor de DHCP no puede cumplir (por ejemplo, cuando se traslada un portátil a una subred distinta), el servidor de DHCP envía un mensaje DHCPNAK al cliente. El cliente conseguirá una nueva concesión usando el proceso de adquisición de concesión inicial.



Cuando arranca un cliente de DHCP difunde un mensaje DHCPREQUEST para renovar su concesión. Ello le asegura que la solicitud de renovación de DHCP se envía al servidor de DHCP que proporciona direcciones de DHCP para la subred en la que se encuentra ahora el cliente, que puede ser distinta de la del servidor de DHCP que proporcionó la concesión inicial. Cuando el servidor de DHCP recibe la difusión, compara la dirección del cliente de DHCP solicitante con el ámbito configurado en el servidor. Si es imposible satisfacer la solicitud del cliente, el servidor de DHCP envía un DHCPACK y el cliente consigue una nueva concesión.

Si el cliente de DHCP no es capaz de localizar ningún servidor de DHCP cuando se reinicia, para renovar su concesión envía una difusión de ARP (Address Resolución Protocol, Protocolo de Resolución de Direcciones) para la pasarela predeterminada que se obtuvo anteriormente, si la hubo. Si la dirección de IP de la pasarela predeterminada se resuelve correctamente, el cliente de DHCP supone que se encuentra situado en la misma red donde obtuvo su concesión actual que continúa usando.

Si la difusión de ARP del cliente enviada para la pasarela predeterminada no recibe respuesta, el cliente supone que el cliente se ha trasladado a una red que no dispone actualmente de servicios de DHCP, como la red de casa, y se auto configura él mismo mediante APIPA (Automatic Prívate IP Addressing, Dirección privada IP automática (169.254.x.x)). Una vez auto configurado a sí mismo, el cliente de DHCP intentará, cada 5 minutos, localizar un servidor de DHCP.

DETECCIÓN DE SERVIDORES DE DHCP NO AUTORIZADOS

Como parte de la inicialización del servicio de DHCP, todos los servidores de DHCP realizan una detección de servicios rogue. Si el servidor no está autorizado en el Active Directory, se apaga.

La detección de servidor rogue comienza con la inicialización del servidor de DHCP enviando una solicitud DHCPINFORM para determinar si existen otros servidores de DHCP inicializados en cualquier red conectada. Si es así, estos servidores responden con un mensaje DHCPACK que contiene el nombre del dominio en el que tienen autorización.

Si se encuentran otro servidor de DHCP, el servicio de DHCP de Windows Server que está arrancando se conecta con el Active Directory y envía una serie de llamadas LDAP para descubrir si está autorizado o no. Si el servidor no está autorizado, el servicio termina. Esta detección se lleva a cabo una vez cada hora por el servidor de DHCP para detectar nuevos servidores no autorizados.

Si está activado el registro de sucesos de DHCP, se escribe un mensaje en el registro de sucesos de DHCP.

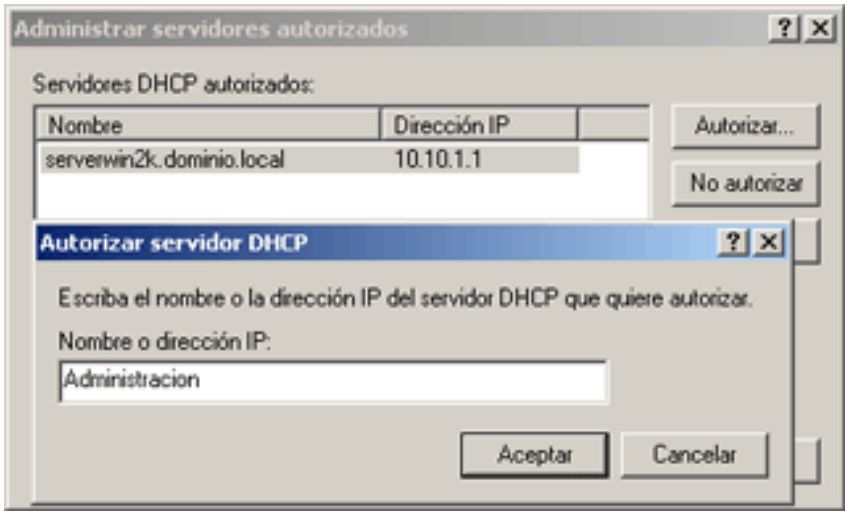
CONFIGURANDO UN SERVIDOR DHCP.

El servidor DHCP reduce enormemente la tarea administrativa de configurar estaciones de trabajo con una dirección IP y la configuración TCP/IP apropiada para la red. Antes de instalar el servidor DHCP hay que determinar el esquema de direcciones IP. También se deben completar estos pasos adicionales antes de instalar DHCP:

1. Determinar el intervalo de direcciones IP libres y únicas que manejará el servidor DHCP además de cualquier dirección IP que sea necesario excluir para soportar hosts con direcciones IP estáticas.
2. Hacer una lista de los servidores para los que se desea reservar una IP (como servidores DNS y WINS).
3. Si el servidor DHCP utilizará direcciones IP registradas en Internet, hay que registrar las direcciones IP con el ISP
4. Actualizar todos los controladores de dominio Windows NT 4 a Windows 2000,2003,2008.
5. Determinar los requisitos de hardware y de almacenamiento del servidor DHCP
6. Configurar manualmente las direcciones estáticas en el equipo donde se instalará el servicio DHCP

Para instalar el servidor DHCP, hay que seguir estos pasos:

1. Si se desea instalar el servicio DHCP en un servidor que no sea controlador de dominio, será necesario comunicárselo a Active Directory. Después de la instalación hay que abrir DHCP desde el menú Herramientas administrativas. Hay que resaltar DHCP en el árbol de la consola y escoger después Examinar servidores autorizados en el menú Acción. Hay que pulsar Agregar y escribir después el nombre o la dirección IP del servidor DHCP a autorizar.



Si se piensa utilizar múltiples servidores DHCP en una subred para realizar equilibrio de carga y tener redundancia, hay que configurar un superámbito en cada servidor DHCP que contenga todos los ámbitos válidos de la subred como ámbitos miembro. Hay que configurar entonces el ámbito miembro en cada servidor para que tenga excluidas las direcciones de los otros servidores de forma que no aparezcan direcciones en ninguna de las colas de direcciones de los servidores. Una buena división consiste en darle el 80 por 100 de las direcciones al servidor DHCP principal y el 20 por 100 al servidor secundario.

CREACIÓN DE UN NUEVO ÁMBITO.

Ahora ya se puede ejecutar el Administrador DHCP y crear un nuevo ámbito de direcciones IP para que las gestione el servidor DHCP. Pero antes de hacer esto, hay que asegurarse de que se conoce el intervalo de direcciones IP aprobado, qué direcciones IP son necesarias excluir para los sistemas con direcciones IP estáticas y qué direcciones son necesarias reservar para servidores DNS o WINS. Para abrir el Administrador DHCP y crear el nuevo ámbito, hay que seguir los siguientes pasos:

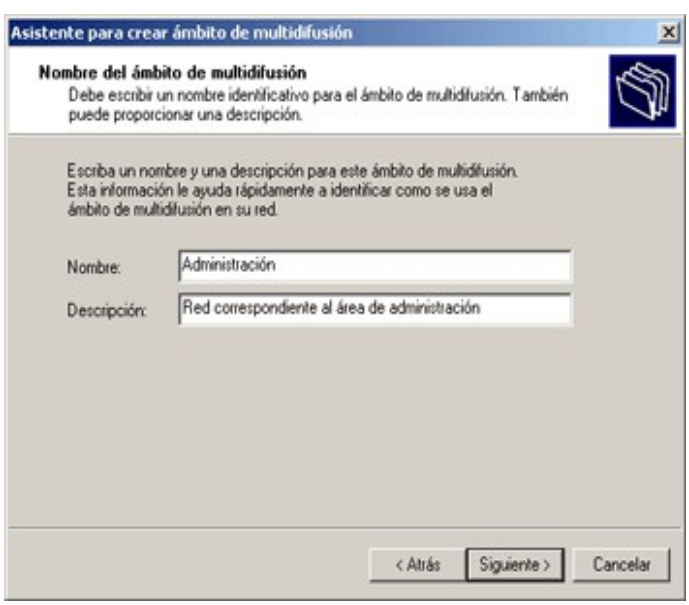
1. Escoger DHCP del menú Herramientas administrativas.

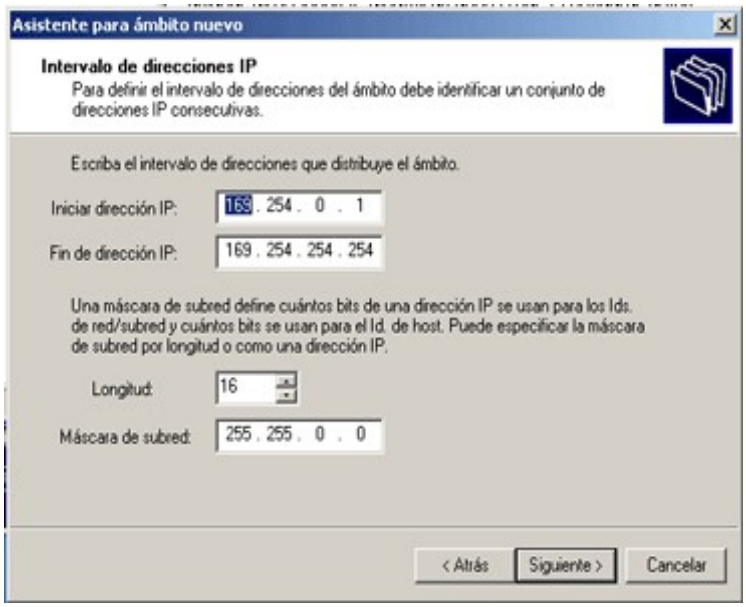
2. Seleccionar el servidor DHCP en el árbol de la consola. Seleccionar el menú Acción y escoger Ámbito nuevo para ejecutar el Asistente para ámbito nuevo.

3. Pulsar Siguiente e introducir el nombre y la descripción del ámbito que servirán para distinguir este ámbito de otros. Pulsar Siguiente.

4. Introducir la dirección IP por la que se desea que comience el ámbito en el campo Iniciar, e introducir la dirección IP por la que se desea qué finalice el ámbito en el campo Fin.

5. Introducir la máscara de subred de la red en el cuadro Máscara de subred, o utilizar el cuadro Longitud para ajustar la longitud de la máscara de subred. Después, pulsar Siguiente.





6. Para excluir un intervalo de direcciones del ámbito, en el cuadro Iniciar dirección IP, hay que introducir la dirección IP de comienzo para el intervalo de exclusión; en el cuadro Fin de dirección IP hay que introducir la dirección IP final del intervalo de exclusión. Después hay que pulsar Agregar. Hay que añadir las exclusiones que sean necesarias y pulsar Siguiente cuando se haya terminado.

7. Especificar la duración de la concesión a los clientes y pulsar Siguiente. Conviene utilizar concesiones más largas en redes sin servidores DHCP redundantes para permitir más tiempo de recuperación de un servidor DHCP sin conexión antes de que los clientes pierdan sus concesiones, o para minimizar el tráfico de red a expensas de una renovación de direcciones menos frecuente. También se pueden utilizar concesiones más largas si las direcciones del ámbito son abundantes (al menos un 20 por ciento disponible), la red es estable y los equipos rara vez se mueven. Por el contrario, los ámbitos que soportan clientes que acceden telefónicamente pueden tener concesiones más cortas y, por lo tanto, funcionar bien con menos direcciones.

8. Para configurar las opciones de DHCP, hay que pulsar Configurar estas opciones ahora; en otro caso, hay que pulsar Configuraré estas opciones más tarde. Si se selecciona Configuraré estas opciones más tarde hay que pulsar Finalizar para completar la instalación del ámbito.

9. Si se decide especificar las opciones de DHCP, hay que introducir las puertas de enlace (enrutadores) que se desea que utilicen los clientes en el cuadro Dirección IP, pulsando el botón Agregar después de introducir cada uno. Cuando se haya terminado de introducir puertas de enlace hay que pulsar Siguiente.

10. Introducir el nombre de dominio del dominio en el cuadro Dominio primario, y añadir las direcciones IP de los servidores DNS en el cuadro Dirección IP, pulsando Agregar tras introducir cada una. Hay que pulsar Siguiente cuando se haya terminado.

11. En el cuadro Dirección IP de Servidores WINS, hay que introducir las direcciones de todos los servidores WINS que se hayan configurado en la red para asignar direcciones IP a los nombres NetBIOS de los clientes de nivel inferior. Pulsar Siguiente.

12. Para activar el ámbito inmediatamente, hay que pulsar Activar este ámbito ahora; en caso contrario, hay que pulsar Activaré este ámbito más tarde. Hay que pulsar Siguiente y pulsar después Finalizar para completar la configuración del ámbito.

AUTORIZACIÓN DEL SERVIDOR DHCP Y ACTIVACIÓN DE LOS ÁMBITOS.

Después de configurar el servidor DHCP y crear los ámbitos, es necesario activar los ámbitos antes de que cualquier cliente pueda utilizar el servidor para obtener direcciones IP Antes de que se puedan activar los ámbitos, el servidor tiene que ser autorizado a realizar concesiones, a menos que se haya instalado DHCP en un controlador de dominio, en cuyo caso el servidor DHCP será autorizado automáticamente la primera vez que se añada el servidor a la consola Administrador DHCP.

La autorización de un servidor DHCP es una opción importante que proporciona Windows Server para reducir la capacidad de los hackers de configurar servidores DHCP corrompidos: servidores no autorizados configurados para proporcionar direcciones IP falsas a los clientes. Para autorizar el servidor DHCP después de instalar el servicio, hay que seguir los siguientes pasos:

1. En el Administrador DHCP hay que seleccionar DHCP en la raíz del árbol de la consola.

2. Escoger Administrar servidores autorizados en el menú Acción.

3. Seleccionar Autorizar en el cuadro de diálogo Administrar servidores autorizados.

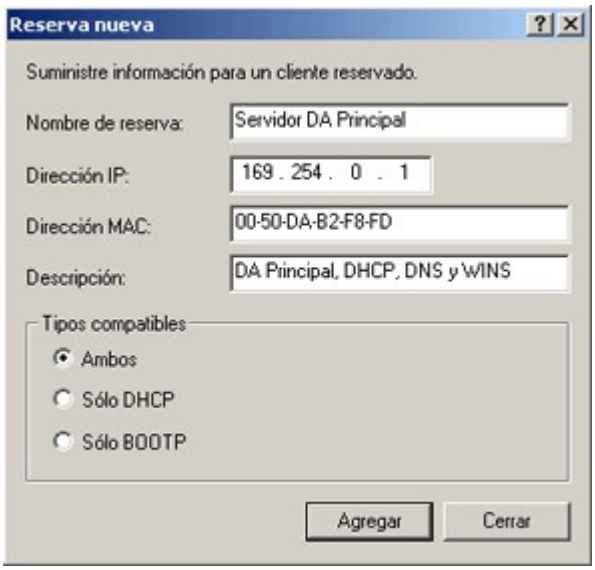
4. Introducir el nombre o la dirección IP del servidor en el cuadro de texto proporcionado y pulsar Aceptar.

5. Verificar que la información es correcta en el cuadro de diálogo que se muestra y entonces pulsar Sí. Hay que pulsar Aceptar para cerrar el cuadro de diálogo Administrar servidores autorizados.

6. Para activar un ámbito hay que seleccionarlo en el árbol de la consola y escoger después Activar en el menú Acción.

No se debe activar un ámbito hasta que se hayan terminado de seleccionar todas las opciones deseadas. Una vez activado un ámbito, el comando Activar del menú cambia a Desactivar. No se debe desactivar un ámbito a no ser que vaya a ser retirado permanentemente de la red.

RESERVANDO DIRECCIONES.



Las reservas son elementos prácticos que se pueden utilizar en lugar de las direcciones IP estáticas (que requieren exclusiones) para todos los servidores (excepto servidores DHCP) que necesiten mantener una dirección IP específica, como servidores DNS y WINS. Al utilizar reservas en lugar de direcciones estáticas se garantiza que un servidor tendrá una dirección IP consistente proporcionando al mismo tiempo la capacidad de recuperar la dirección IP en el futuro si el servidor es retirado de la circulación o movido. Se debería crear la reserva en todos los servidores DHCP que podrían servir potencialmente al cliente reservado.

Para añadir una reserva de dirección a un ámbito:

1. Pulsar con el botón derecho del ratón en la carpeta Reservas bajo el ámbito deseado y escoger Reserva nueva en el menú contextual.
2. Introducir el nombre de la reserva en el cuadro Nombre de reserva.
3. Introducir la dirección IP para el cliente en el cuadro Dirección IP e introducir la dirección MAC del cliente en el cuadro Dirección MAC.
4. Introducir una descripción para la reserva en el cuadro Descripción.
5. Determinar a qué tipo de cliente se desea permitir que utilice la reserva seleccionando Sólo DHCP, Sólo BOOTP o Ambos. A continuación, pulsar Agregar.

Para obtenerla dirección MAC hay que ir al equipo cliente y escribir ipcongif /all en el símbolo del sistema. La dirección MAC se muestra como dirección física.

Activación de las actualizaciones dinámicas de un servidor DNS

Los servidores DHCP y DNS de Windows Server soportan ahora actualizaciones dinámicas con un servidor DNS, una característica que cualquier administrador que haya tenido que gestionar un servidor DNS de Windows NT 4 estático (o similar) apreciará. Los clientes Windows Server pueden actualizar dinámicamente sus registros de búsquedas directas ellos mismos con el servidor DNS después de obtener una nueva dirección IP de un servidor DHCP

Además, el servidor DHCP de Windows Server soporta también actualización dinámica de registros DNS para clientes anteriores a Windows Server que no lo puedan hacer ellos mismos. Esta característica sólo funciona actualmente con los servidores DHCP y DNS de Windows Server.

Para permitir que un servidor DHCP actualice dinámicamente los registros DNS de sus clientes, hay que seguir los siguientes pasos:

1. Seleccionar el ámbito o el servidor DHCP en el cual se desea permitir actualizaciones dinámicas.
2. En el menú Acción, escoger Propiedades y pulsar después la pestaña DNS.

3. Seleccionar la casilla de verificación Actualizar automáticamente la información del cliente DHCP en DNS.

4. Para actualizar los registros DNS de un cliente basándose en el tipo de petición DHCP que hace el cliente y sólo cuando sea solicitado, hay que seleccionar la opción Actualizar DNS sólo a la petición del cliente DHCP

5. Para actualizar siempre los registros de búsqueda directa e inversa de un cliente, hay que seleccionar la opción Actualizar siempre DNS.

6. Seleccionar la casilla de verificación Descartar las búsquedas directas al caducar la concesión para permitir que el servidor DHCP borre el registro de recurso Host de un cliente cuando su concesión DHCP caduque y no sea renovada.

7. Seleccionar la casilla de verificación Habilitar actualizaciones para clientes DNS que no sean compatibles con actualizaciones dinámicas para permitir que el servidor DHCP actualice los registros de búsqueda directa e inversa de los clientes que no pueden actualizar sus propios registros de búsqueda directa. Si no se selecciona esta casilla de verificación, el servidor DHCP no actualizará dinámicamente los registros DNS de los clientes que no sean Windows Server.

Si se tienen servidores DNS estáticos como los de Windows NT 4, estos servidores no podrán interactuar dinámicamente cuando las configuraciones de los clientes DHCP cambien. Esta incompatibilidad puede provocar búsquedas fallidas en los clientes DHCP Para evitar este problema, hay que actualizar los servidores DNS estáticos con un DNS que soporte DNS dinámico (Windows Server). Es decir, vuelvo a desaconsejar fervientemente que se monten redes mixtas con servidores NT y 200X trabajando en el mismo entorno.

USO DE IPCONFIG PARA LIBERAR, RENOVAR O VERIFICAR UNA CONCESIÓN

En un equipo que ejecuta Windows con DHCP activado se puede ejecutar una utilidad de línea de comandos para liberar, renovar o verificar la concesión de dirección del cliente. En el símbolo del sistema (o en la ventana Ejecutar) hay que utilizar alguno de los siguientes comandos:

Para liberar una concesión de un cliente, hay que escribir ipconfig/release.

Para renovar una concesión, hay que escribir ipconfig/renew.

Para verificar la concesión del cliente, hay que escribir ipconfig /all.

Con clientes Windows 95/98 hay que utilizar Winipcfg con los mismos parámetros. El programa ipconfig es útil a la hora de solucionar problemas porque muestra cada detalle de la configuración TCP/IP actual.

CUENTAS DE USUARIO Y GRUPO EN WINDOWS SERVER.

TIPOS DE CUENTAS.

Podemos crear tres tipos de cuenta en Active Directory: cuentas de usuario, cuentas de grupo y cuentas de equipo. Las cuentas de usuario y equipo de Active Directory representan una entidad física, como un equipo o una persona. Las cuentas de grupo sirven como contenedores de los otros 2 tipos de cuenta.

CUENTAS DE USUARIO.

Cada persona que quiera acceder al dominio necesita que se le cree una cuenta de usuario del dominio. Una cuenta de usuario hace posible lo siguiente:

- Autentificar la identidad de la persona que se conecta a la red.
- Controlar el acceso a los recursos del dominio.
- Auditar las acciones realizadas utilizando la cuenta.

Windows Server sólo crea dos cuentas de usuario predefinidas: la cuenta **Administrador**, que otorga al usuario todos los derechos y permisos, y la cuenta **Invitado**, que tiene derechos limitados. El resto de las cuentas las crea un administrador y son cuentas de dominio (validas a lo largo de todo el dominio de forma predeterminada). Un controlador de dominio no puede crear cuentas locales, como se puede comprobar si intentamos ejecutar lusrmgr.msc (gestión de usuarios locales) en un controlador de dominio.

NOMBRE PRINCIPAL DE USUARIO (UPN).

Un nombre principal de usuario es un nombre de inicio de sesión que se utiliza para conectarse a una red de Windows Server. Este nombre también se denomina nombre de inicio de sesión de usuario. Un nombre principal de usuario tiene dos partes separadas por el signo @ (como si fuera una cuenta de correo electrónico). Ejemplos de nombres UPN son godofredo@iesromerovargas.local o floripondio@dominio.com.

De forma predeterminada, el nombre del usuario lo otorga un administrador al crear la cuenta de usuario, mientras que el sufijo principal (lo que va detrás de la arroba) es el nombre del dominio que se ha creado en nuestro controlador de dominio.

ESTRATEGIAS PARA NOMBRAR CUENTAS.

Crear nombres de cuentas de usuario parece una tarea trivial, y efectivamente lo es cuando tenemos que crear un par de usuarios, pero se transforma en una tarea mucho más complicada cuando queremos crear cientos, o incluso miles de cuentas de usuario.

Pongamos por ejemplo que queremos crear una cuenta de usuario para cada alumno del instituto Francisco Romero Vargas, que cuenta con unos 900 alumnos. Evidentemente no podemos usar el nombre (sin apellidos) como nombre de cuenta, o acabaremos con cuentas como Jennifer32, dado que habrá muchos usuarios con el mismo nombre.

Es importante crear una estrategia de denominación de cuentas para nuestros bosques y dominios, creando unas convenciones para nombrar cuentas. Ejemplos validos de estrategias podrían ser por ejemplo:

- Usar los 2 primeros caracteres del nombre, los 2 caracteres primeros del 1º apellido y los 2 caracteres primeros del 2º apellido.
- Usar 3 caracteres para indicar el curso del alumno, los 3 caracteres primeros del nombre y los 2 caracteres primeros del 1º apellido.
- Usar los 4 caracteres primeros del nombre del alumno, la inicial del 1º apellido, la inicial del 2º apellido y los 2 últimos números del DNI del alumno.

Fijaros como la 2ª estrategia tiene la ventaja de que la simple cuenta de usuario nos da información sobre el curso del alumno, por lo que tenemos más control que en los otros dos casos.

Aparte de facilitar la creación de las cuentas de usuario, estas estrategias tienen la gran ventaja de que nos permiten crear programas para crear automáticamente cuentas de usuario. Así, podemos llegar a una empresa que cuenta con 200 empleados a los que tenemos que crear una cuenta de usuario. Podemos crear un script o programa que leyendo una lista de los nombres de los usuarios nos cree directamente las cuentas, usando nuestra estrategia definida para nombrar las cuentas.

CONTRASEÑAS.

Todos los usuarios deberían tener contraseñas bien escogidas y se les debería requerir que las cambiaran periódicamente. Las cuentas deberían establecerse de forma que se bloquearan cuando se introdujeran contraseñas incorrectas. (Se pueden permitir tres intentos, para dejar margen a errores tipográficos.)Una buena contraseña tiene las siguientes características:

- No es una rotación de los caracteres del nombre de inicio de sesión.
- Contiene al menos un carácter alfabético en mayúsculas, uno en minúsculas y uno numérico.
- Tiene una longitud de al menos seis caracteres.
- No es el nombre o las iníciales del usuario, las iníciales de sus hijos, u otro dato significativo o cualquiera de esos elementos combinado con otra información personal comúnmente disponible como la fecha de nacimiento, el número de teléfono o el nombre del cónyuge.

Entre las mejores contraseñas se encuentran los acrónimos alfanuméricos de frases que tienen un significado para el usuario pero que no es probable que conozcan otros. Esto hace que la contraseña sea fácil de recordar para el usuario, mientras que al mismo tiempo sea difícil de adivinar por una persona de fuera. Por ejemplo, usamos la frase “hasta luego Lucas” y de ella sacamos la contraseña H4st4luegoluc4S (sustituimos las a por el número 4 y ponemos en mayúsculas la primera y última letra).

En Windows Server está activo por defecto la opción de seguridad que obliga a que todas las contraseñas cumplan los requisitos de complejidad. Podemos desactivarla si es necesario desde la consola de políticas de seguridad como ya vimos en temas anteriores.

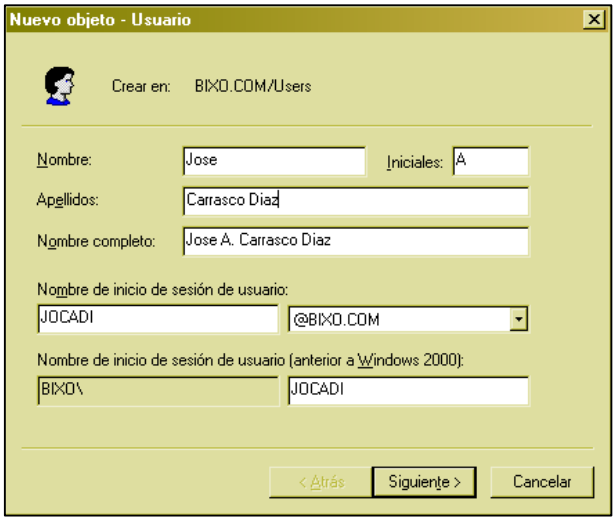
Conviene educar a los usuarios sobre las contraseñas y su privacidad, pero, sobre todo, merece la pena hacer caso de los propios consejos: hay que asegurarse de que la contraseña seleccionada para administración es una buena contraseña y cambiarla frecuentemente. Hacer esto ayudara a evitar las consecuencias de que alguien se introduzca en el sistema y cause estragos. Si los usuarios se conectaran telefónicamente a la red desde casa a otros sitios remotos, debería incluirse más seguridad que la autorización por contraseña de nivel de dominio.

Los administradores deberían tener dos cuentas en el sistema: una cuenta administrativa y una cuenta de usuario normal. Se debería utilizar la cuenta de usuario normal a menos que se estén realizando tareas administrativas.

CREACIÓN DE CUENTAS DE USUARIO DEL DOMINIO MEDIANTE LA CONSOLA "USUARIOS Y EQUIPOS DE ACTIVE DIRECTORY".

Para añadir una cuenta de usuario del dominio hay que abrir la consola MMC Usuarios y equipos de Active Directory desde el menú Herramientas administrativas.

Las cuentas de usuario del dominio se pueden crear en la carpeta USER o en algún otro contenedor creado para almacenar cuentas de usuario del dominio. Hay que seleccionar dicho contenedor y en el menú Acción, escoger Nuevo y escoger después Usuario.
Nos aparecerá en pantalla el asistente para la creación de cuentas de usuario, como podemos ver en la siguiente figura.

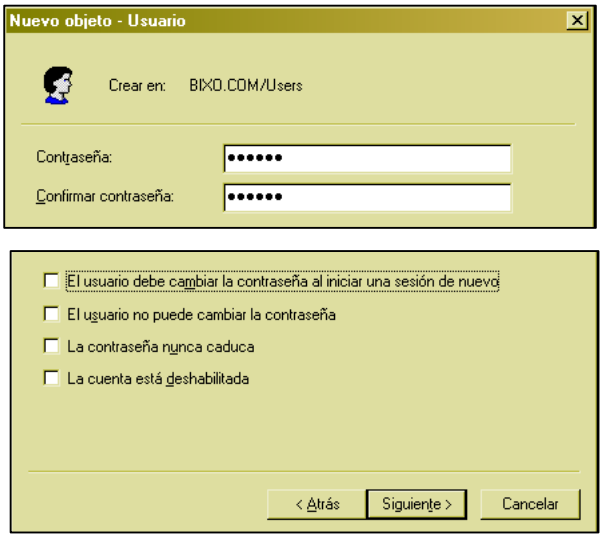


- Nombre, Iníciales y Apellidos: Un nombre de usuario no puede coincidir con otro nombre de usuario o de grupo en el equipo que está administrando. Puede contener hasta 20 caracteres, en mayúsculas o minúsculas, y no puede contener caracteres especiales.

- Nombre completo: se rellena automáticamente. El nombre completo debe ser único en la OU (carpeta) donde se crea el usuario.

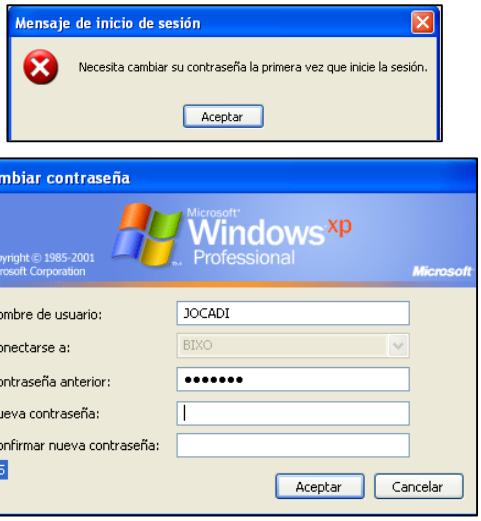
- Nombre de inicio de sesión de usuario: Hay que proporcionar el nombre de inicio de sesión de usuario basado en un convenio de denominación que previamente se ha tenido que establecer. Este nombre principal de usuario (UPN) debe ser único en el Active Directory. El nombre de inicio de sesión anterior a Windows 2000 se rellena automáticamente.

Al pulsar siguiente pasamos a la 2ª parte del asistente para crear usuarios, donde nos pedirá la contraseña y también nos pedirá que repitamos la contraseña para evitar posibles errores. La contraseña no se muestra por pantalla, en su lugar veremos asteriscos como medida de seguridad. La longitud máxima de una contraseña es de 127 caracteres.



Las opciones que vemos aquí son las siguientes:

- El usuario debe cambiar la contraseña en el siguiente inicio de sesión: Normalmente se selecciona para que el usuario controle la contraseña y no la conozca el administrador que le ha dado de alta. En cuento que el usuario abra sesión por primera vez introduciendo la contraseña que le acabamos de indicar en este formulario, el sistema le pedirá que se cambie la contraseña por una nueva que se invente el mismo. Mientras no se cambie la contraseña el sistema no dejará que haga ninguna otra acción.



- El usuario no puede cambiar la contraseña: Cuando por necesidades de seguridad la contraseña debe ser asignada por el administrador y no queremos que el usuario pueda cambiarla.

- La contraseña nunca caduca: Si seleccionamos esta casilla, no se aplicarán las restricciones de caducidad de contraseña a esta cuenta, así que la contraseña nunca caducará. Por defecto, la contraseña del administrador nunca caduca.

- Cuenta deshabilitada: Deshabilita cuentas que momentáneamente no se necesitan en la red. También puede seleccionarse automáticamente debido a las restricciones de seguridad impuestas por el Administrador, como por ejemplo que se bloquee la cuenta por excesivos intentos de acceder con una mala contraseña.

CREACIÓN DE CUENTAS USANDO EL SÍMBOLO DEL SISTEMA.

También podemos crear una cuenta de usuario desde el símbolo del sistema, para ello usamos el comando **dsadd user**. Para obtener ayuda sobre este comando podemos escribir en el símbolo del sistema de Windows Server el comando dsadd user /?

Para crear un usuario escribimos:

dsadd user "nombre distinguido del usuario" –pwd "contraseña"

El nombre distinguido (dn) del usuario se forma escribiendo su nombre común, el nombre de la UO o carpeta en la que lo queremos crear, el nombre del dominio y la "extensión del dominio". Así, si queremos crear un usuario con nombre MARGARITA en la carpeta USERS dentro del dominio BIXO.COM, escribimos la siguiente orden:

```
C:\>DSADD USER "CN=MARGARITA, CN=USERS, DC=BIXO, DC=COM" -PWD Abcd1234
dsadd correcto:CN=MARGARITA,CN=USERS,DC=BIXO,DC=COM
```

Así, para crear el usuario Margarita dentro de la unidad organizativa Users en el dominio Bixo.Com, utilizaríamos el siguiente nombre distinguido:

- CN (Nombre común) del usuario: Margarita
- CN (Nombre común) de la unidad organizativa dentro de la cual se crea el usuario: Users
- DC (Componente de dominio) Bixo
- DC (Componente de dominio) Com

Este nombre distinguido del usuario se utiliza mucho en Windows Server, aunque trabajaremos más con él en 2º curso.

CREACIÓN DE CUENTAS MÚLTIPLE.

Existen varios comandos en Windows Server que nos permiten crear cuentas de usuario en lotes, no de una en una. Estos comandos son CSVDE y LDIFDE.

CSVDE utiliza un fichero separado por comas .CSV en el cual podemos escribir los nombres de muchas cuentas. Con el parámetro –f podemos hacer que CSVDE genere un archivo separado por comas con toda la configuración de nuestro Active Directory.

Para ello, ejecutad el comando:

CSVDE –F EXPORTADO.CSV

Veremos cómo este comando nos crea un fichero exportado.csv. Si editamos dicho fichero, podremos entender el formato de estos ficheros CSV. Igualmente que podemos usar CSVDE para exportar cuentas y configuraciones, podemos usarlo para importar y crear dichos datos. Para realizar esta importación debemos usar el comando de la siguiente forma:

CSVDE –I –F EXPORTADO.CSV

El otro comando, LDIFDE, es muy parecido a CSVDE pero mucho más potente. Por ejemplo, con CSVDE no podemos exportar ni importar contraseñas, pero con LDIFDE sí. Este comando también funciona mediante ficheros de texto, pero en este caso no es un fichero separado por comas (CSV) sino que es un fichero con un formato especial.

Para exportar la configuración con LDIFDE, ejecutad el comando

LDIFDE –F EXPORTACION.LDF

Comprobad el fichero creado EXPORTACION.LDF y daros cuenta de la diferencia con el anterior fichero creado por CSVDE.

Para importar con LDIFDE usamos el comando de la siguiente forma:

LDIFDE -I –F EXPORTACION.LDF

ADMINISTRACIÓN DE CUENTAS DE USUARIO MEDIANTE LA CONSOLA.

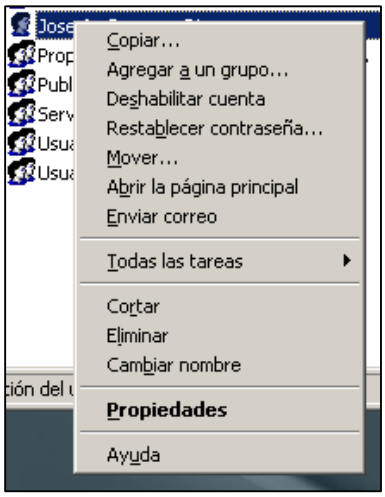
Especialmente en una red grande, la gestión de las cuentas de usuario es un proceso continuo de añadir, eliminar y realizar cambios.

Aunque estas tareas no son difíciles, pueden consumir tiempo y es necesario gestionarlas con cuidado. Vamos a ver como realizamos esta administración desde la consola (MMC) Usuarios y Equipos de Active Directory.

- Abrimos Usuarios y equipos de Active Directory desde el menú Herramientas administrativas.
- Abrimos el contenedor que almacena la cuenta de usuario (por defecto, USERS).
- Seleccionamos el usuario que queremos administrar y nos vamos al menú Acción (o pulsamos botón derecho sobre el usuario).

Aparecerán las siguientes opciones:

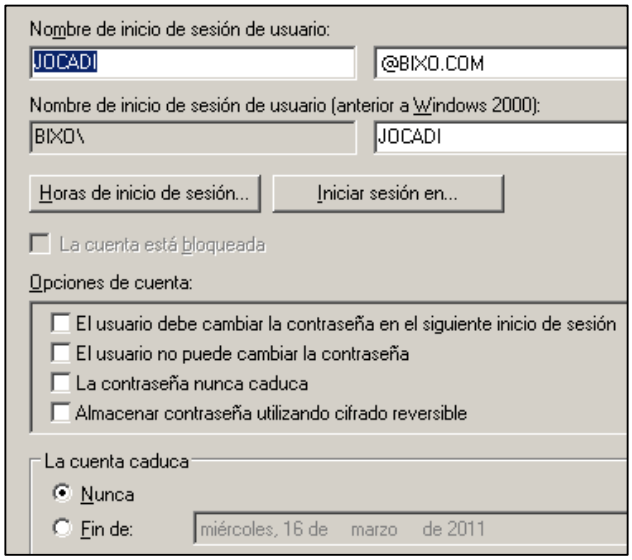
- Copiar.
    - Esto nos permite crear una cuenta de usuario nuevo, pero con la diferencia de que el nuevo usuario heredará las configuraciones del usuario que se copia.



- Agregar miembros a un grupo
  - Nos permite introducir al usuario en uno o varios grupos.
- Deshabilitar cuenta
  - Deshabilita la cuenta. Si la cuenta ya está deshabilitada, aparecerá la opción de habilitar cuenta.
- Restablecer contraseña.
  - Nos permite poner una contraseña nueva al usuario. No permite conocer cuál es la contraseña actual del usuario.
- Mover.
  - Nos permite mover el usuario entre contenedores o unidades organizativas. También es posible moverlo arrastrándolo con el ratón.
- Abrir la página principal.
  - Si hemos configurado una página web para el usuario.
- Enviar mensaje de correo.
  - Si hemos configurado una dirección de correo para el usuario.
- Cortar.
  - Corta el usuario, para permitir pegarlo en algún otro contenedor.
- Eliminar.
  - Elimina definitivamente la cuenta del usuario. En situaciones reales, no suele ser aconsejable eliminar cuentas, es mucho mejor deshabilitarlas.
- Cambiar nombre.
  - Nos permite cambiar el nombre del usuario. Hay que tener en cuenta que no permite cambiar el nombre de inicio de sesión del usuario o UPN, sino simplemente el nombre descriptivo del usuario.
- Propiedades.
  - Accedemos a las propiedades avanzadas del usuario. Es lo mismo que conseguimos si realizamos doble clic sobre el usuario.

Propiedades de cuentas de usuario del dominio.

- Pestaña General
  - Desde aquí podemos gestionar los atributos sobre el nombre, la descripción la ubicación de la oficina, el número de teléfono, la dirección de correo electrónico y la dirección de la página Web del usuario.
- Pestaña Dirección
  - Documenta la dirección física del usuario.
- Pestaña Cuenta
  - Podemos cambiar el nombre de inicio de sesión del usuario.
  - Podemos establecer unas horas de inicio de sesión para el usuario, de modo que no se le dejara abrir sesión fuera de este horario.
  - Podemos indicar el nombre de los equipos desde los que queremos que este usuario abra sesión, de modo que el sistema impedirá su acceso si intenta acceder desde un equipo cuyo nombre no esté en esta lista.
  - Podemos indicar varias opciones sobre la contraseña.
  - Podemos establecer una fecha en la cual la cuenta caducará automáticamente y pasará a deshabilitarse automáticamente.



- Pestaña Perfil
  - Muestra la ruta de acceso al perfil del usuario, la ruta de acceso de cualquier archivo de comandos que se ejecuta en el inicio de sesión, la ruta de acceso al directorio principal y cualquier conexión automática de unidades. Estas opciones las estudiaremos en el tema dedicado a perfiles de usuario en Active Directory.
- Pestaña Teléfonos
  - Enumera números de teléfono adicionales como el teléfono de un localizador, de un móvil, etc.
- Pestaña Organización
  - Documenta el título, el departamento, la organización, el administrador y las supervisiones directas del usuario.
- Pestaña Miembro de
  - Enumera las pertenencias a grupos del usuario.

- Pestaña Marcado
  - Podemos permitir que los usuarios se conecten a nuestro dominio a distancia, usando directamente la línea telefónica y un modem. Desde aquí podemos indicar opciones sobre dicho tipo de llamadas.
- Resto de pestañas.
  - El resto de pestañas de las propiedades del usuario se utilizan para configurar las opciones de Terminal Server. Estas opciones permiten que el usuario abra sesión a distancia en nuestro dominio usando terminales, y también permite que varias personas abran sesión en la misma máquina. Tal vez se vean estas opciones en un tema posterior.

ADMINISTRACIÓN DE CUENTAS DE USUARIO USANDO EL SÍMBOLO DEL SISTEMA.

Ya vimos anteriormente como mediante el comando dsadd podíamos crear cuentas de usuario. Pues conjuntamente con este comando, también podemos usar los siguientes comandos para la administración de usuarios:

- Dsadd. Añade usuarios.
- Dsmod. Modifica usuarios.
- Dsrm. Elimina usuarios.
- Dsmove. Mueve usuarios.
- Dsget. Muestra información sobre los usuarios.

Si escribimos dsmod user /? desde la línea de comandos nos aparecerá una ayuda sobre las opciones de dsmod. De igual modo podemos hacerlo con las restantes órdenes.

Veamos algunos ejemplos de uso de estos comandos:

- Restablecer la contraseña de un usuario. El formato de la orden sería:

  dsmod user "nombre distinguido del usuario" –pwd "nueva contraseña"

  Ya vimos cuando tratamos el dsadd en que consiste el nombre distinguido del usuario.

- Indicar al usuario que debe cambiar la contraseña la próxima vez que inicie sesión:

  dsmod user "nombre distinguido del usuario" –mustchpwd yes

- Deshabilitar una cuenta de usuario.

  dsmod user "nombre distinguido del usuario" –disabled yes

- Eliminar una cuenta de usuario.

  dsrm "nombre distinguido del usuario"

- Obtener la lista de grupos a la que pertenece un usuario.

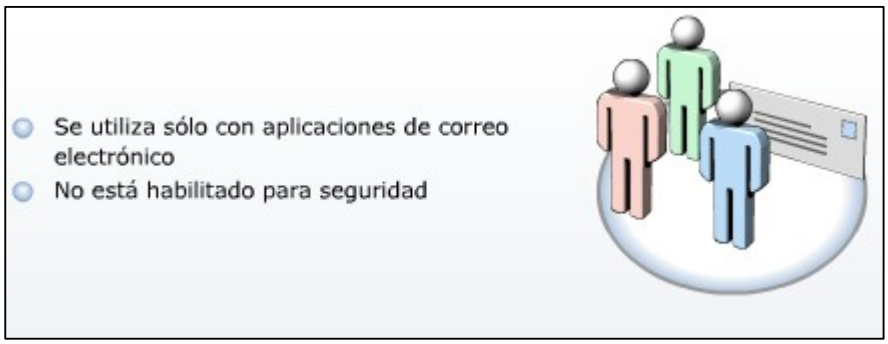
  dsget user "nombre distinguido del usuario" –memberof

CUENTAS DE GRUPO.

Los grupos son contenedores que nos facilitan la administración de los sistemas informáticos. Normalmente es recomendable no asignar permisos a usuarios individuales, sino agregar estos usuarios como miembros de un grupo, y asignar permisos al grupo.

Hay dos tipos de grupo en Active Directory: grupos de distribución y grupos de seguridad.

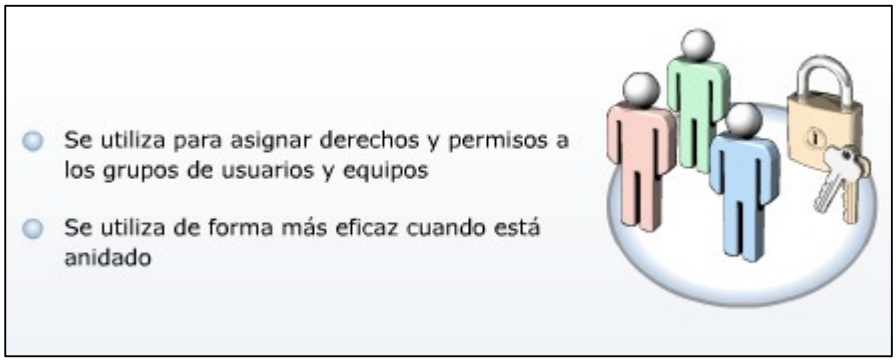
GRUPOS DE DISTRIBUCIÓN.



Estos grupos no cuentan con SID (identificador de seguridad) propio, de modo que no pueden ser introducidos en las ACL (listas de control de acceso a los recursos).

Estos grupos solo se suelen utilizar cuando queremos crear un grupo para realizar envíos de correo a varios usuarios habitualmente.

GRUPOS DE SEGURIDAD.



Estos grupos si cuentan con SID, de modo que pueden ser utilizados para ser introducidos en las ACL. Por regla general siempre que creemos un grupo lo crearemos de este tipo, de seguridad.

ÁMBITO DE LOS GRUPOS.

Todos los grupos tienen un atributo de ámbito que determina dónde se puede utilizar dicho grupo en una red. Así, nos encontramos con los siguientes tipos de grupos:

- Grupos **locales** de dominio.
  - Su **ámbito es local**, es decir, los grupos locales no son visibles fuera del dominio donde se crean.
- Grupos **globales** de dominio.
  - Su **ámbito es global**, es decir, los grupos globales son visibles en todos los dominios que formen parte de nuestro bosque.
- Grupos universales.
  - Su ámbito es global, al igual que en los grupos globales.

INTEGRANTES DE LOS GRUPOS.

Mientras que el ámbito de los grupos es independiente del nivel funcional de dominio (que establece la compatibilidad de Windows Server), la membresía de los grupos depende directamente de dicho nivel funcional.

Así, dependiendo del nivel funcional de nuestro dominio podremos o no introducir miembros determinados dentro de cada tipo de grupo.

Las siguientes reglas se aplican si el **nivel funcional** de dominio es al menos **Windows 2003**.

- Grupos **locales** de dominio.
  - Un grupo local de dominio **puede contener grupos globales** y universales de cualquier dominio del bosque. También **puede contener cuentas de usuario** y equipos **de cualquier dominio** del bosque. También puede contener otros grupos locales pero únicamente del mismo dominio donde se ha creado.
  - Un grupo local de dominio **no puede contener** otros grupos locales de fuera de su propio dominio. (Esto es evidente, ya que un grupo local no puede ser visible fuera de su propio dominio).
- Grupos globales de dominio.
  - Un grupo global **puede contener** otros **grupos globales del mismo dominio** donde se crea el grupo global. También **puede contener cuentas de usuario** y equipos del **mismo dominio** donde se crea el grupo global.
  - Un grupo global **no puede contener** grupos universales ni **grupos locales**. Tampoco puede contener grupos globales ni cuentas de usuario ni cuentas de equipo de fuera de su propio dominio.

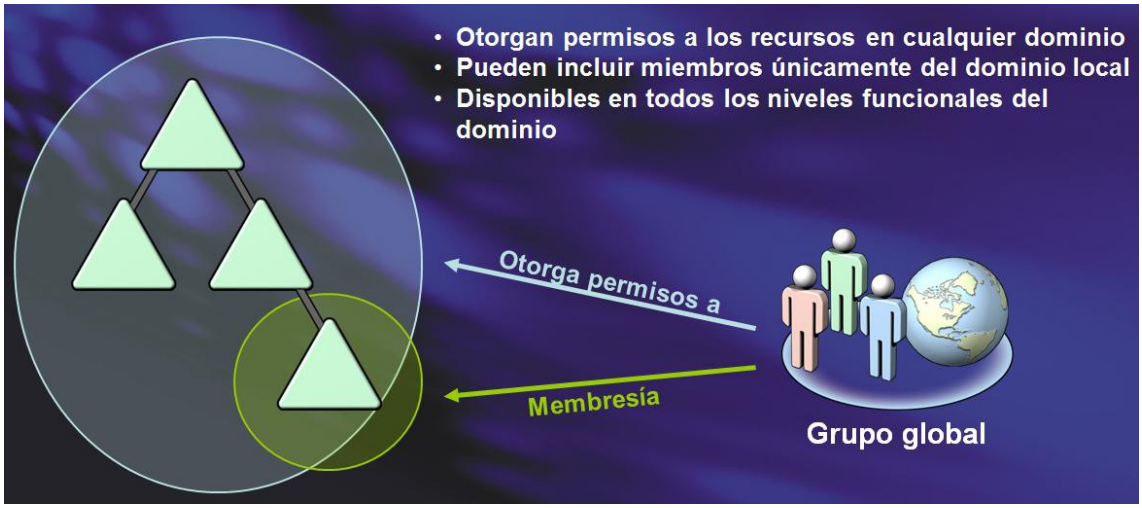
- Grupos universales.
  - Un grupo universal **puede contener** grupos universales, grupos globales, cuentas de usuario y cuentas de equipo de cualquier dominio del bosque.
  - Un grupo universal **no puede contener** grupos locales.

TIPOS DE GRUPOS EN WINDOWS SERVER.

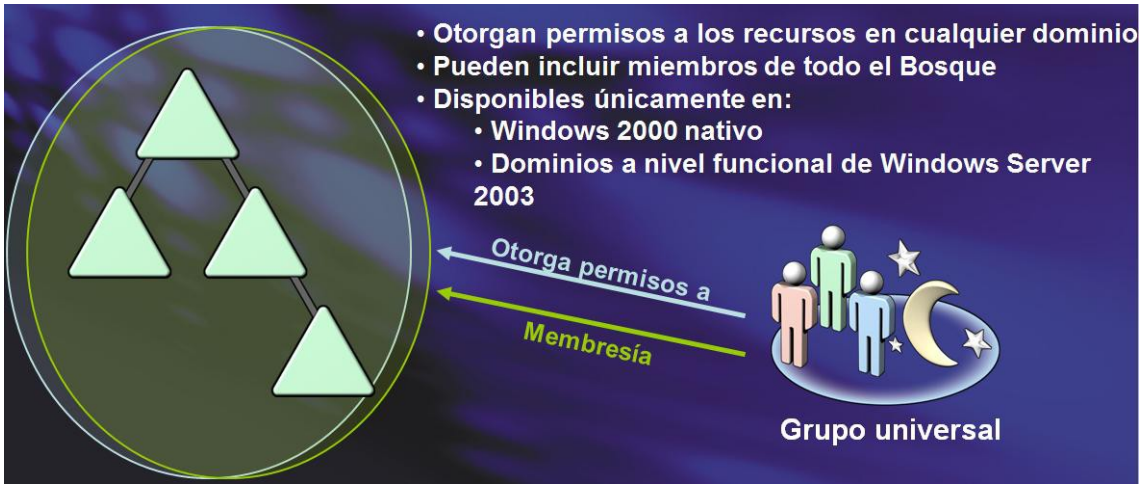
Un **grupo de dominio local** es un grupo de seguridad o distribución que puede contener grupos universales, grupos globales, otros grupos locales de dominio de su propio dominio y cuentas de cualquier dominio del bosque.

En los grupos de seguridad local, solamente puede otorgar derechos y permisos sobre los recursos que residen en el dominio en el que está ubicado el grupo local de dominio.

Un **grupo global** es un grupo de seguridad o distribución que puede contener usuarios, equipo y grupos globales de su propio dominio. Puede conceder derechos y permisos a los grupos de seguridad global para los recursos de cualquier dominio del bosque.



Un **grupo universal** es un grupo de seguridad o distribución que puede contener usuarios, equipos, grupos universales y grupos globales de cualquier dominio del bosque. Se pueden conceder derechos y permisos a los grupos de seguridad universales sobre los recursos de cualquier dominio del bosque.



ANIDAMIENTO DE GRUPOS.

Hay que tener mucho cuidado al anidar grupos (incluir grupos como miembros de grupos) si tenemos el nivel funcional del dominio elevado a Windows 2003 o superior, ya que el sistema permitirá anidar recursivamente, es decir, podemos llegar a formar un bucle infinito de membresías.

Así por ejemplo, imaginad que tenemos el grupo local LOCAL1, e indicamos que un miembro de dicho grupo es LOCAL2, y a su vez indicamos que un miembro de LOCAL2 es LOCAL1.

Para evitar esto, aunque el nivel funcional de AD sea el de Windows 2003, no se recomienda introducir dentro de un grupo local otro grupo local, del mismo modo que no se recomienda utilizar grupos universales.

CUANDO UTILIZAR CADA TIPO DE GRUPO.

Los grupos con ámbito local de dominio nos ayudan a definir y administrar el acceso a los recursos en un solo dominio. Por ejemplo, para conceder a cinco usuarios acceso a una impresora determinada, podemos agregar las cinco cuentas de usuario a la lista de permisos de la impresora. Sin embargo, si más tarde deseamos dar a esos cinco usuarios acceso a una nueva impresora, debemos especificar nuevamente las cinco cuentas en la lista de permisos de la nueva impresora.

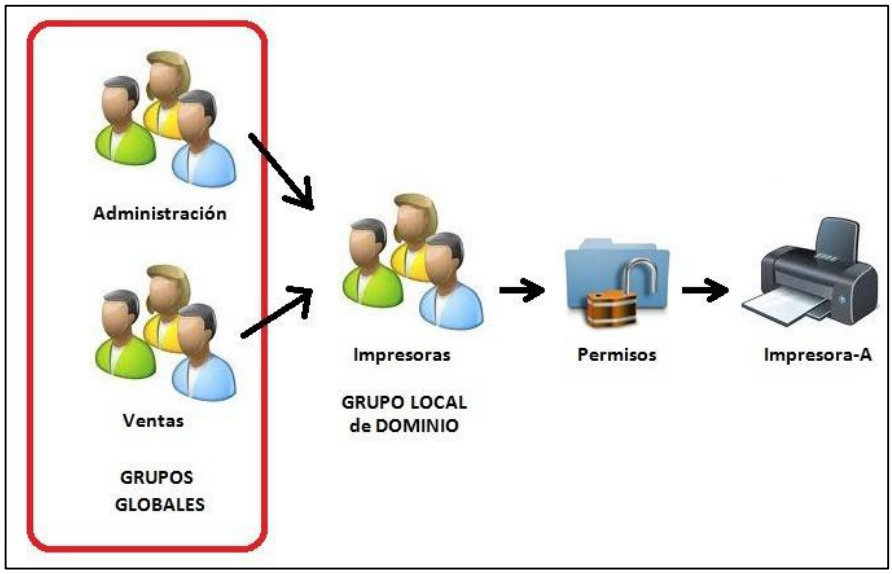
Si planeamos antes los grupos, podemos simplificar esta tarea administrativa rutinaria. Para hacerlo, deberemos crear un grupo de seguridad con ámbito local de dominio y asignarle los permisos necesarios para tener acceso a la impresora. Ahora añadimos a los 5 usuarios como miembros del nuevo grupo con lo cual podrán acceder a la impresora.

Si ahora deseamos dar a esos 5 usuarios acceso a una nueva impresora, basta con añadir a la lista de permisos de esa impresora el grupo local anteriormente creado (1 operación) y no añadir manualmente a los 5 usuarios (5 operaciones).

Además, si queremos que un usuario deje de poder usar las impresoras, bastará con sacar a dicho usuario del grupo, con lo que habremos conseguido que no pueda usar dichos recursos. Si no usamos grupos, no nos quedaría más remedio que ir impresora por impresora e ir quitándole los permisos al usuario por cada una de ellas.

Pero, ¿y si de necesitamos que estos 5 usuarios impriman en una impresora situada en otro domino del bosque?

Para ello, en lugar de añadir los usuarios a un grupo local de dominio, lo conveniente es colocar las cinco cuentas de usuario en un grupo con ámbito global y agregar este grupo global como miembro del grupo local de dominio que da permisos sobre las impresoras. De este modo, conseguiremos que a nuestros usuarios se les pueda asignar permisos en cualquier dominio del bosque.



No hemos nombrado aquí a los grupos universales, esto es así ya que personalmente recomiendo no usar dicho tipo de grupos, dado que no funcionan en los modos de Windows 2000 mixto, y además afectan al rendimiento del AD más que los grupos locales y globales.

En todos estos apuntes hasta ahora hemos tratado el tema de los grupos desde el nivel funcional de Windows Server 2003 o superior. Si cambiamos dicho nivel funcional a 2000 nativo o 2000 mixto veremos que cambian las reglas principalmente de anidamiento. Puesto que los servidores Windows 2000 son difíciles de encontrar en la actualidad, nos seguiremos centrando en este nivel funcional de dominio.

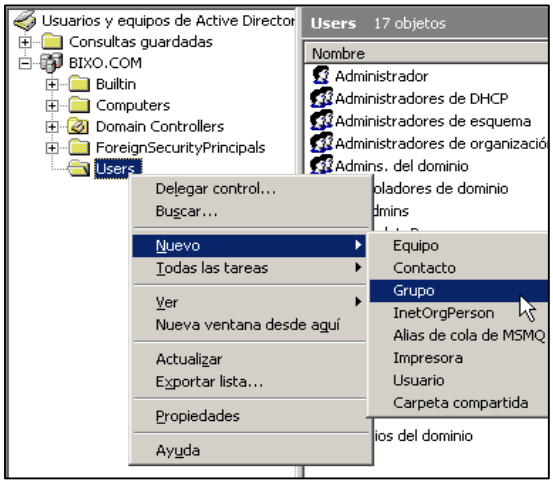
ADMINISTRACIÓN DE GRUPOS USANDO LA CONSOLA.

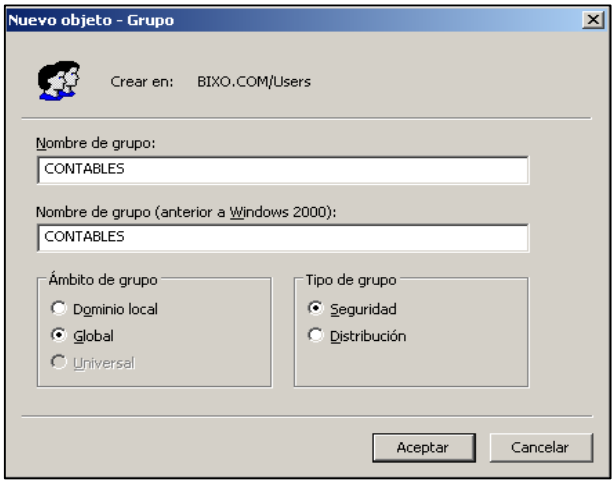
Podemos administrar las cuentas de grupo del mismo modo que administramos las cuentas de usuario, desde la MMC Usuarios y Equipos de Active Directory.

Al igual que hacíamos para las cuentas de usuario, podemos seleccionar la unidad organizativa deseada (en nuestro caso Users) y, o bien, pulsar botón derecho – Nuevo – Grupo o bien seleccionar del menú la opción Acción.

Una vez indicado que queremos crear un nuevo grupo, veremos en pantalla el siguiente formulario:

Como vemos, desde este formulario podemos indicar el nombre del grupo, indicar el ámbito (Local, global o universal) e indicar el tipo de grupo (seguridad o distribución).

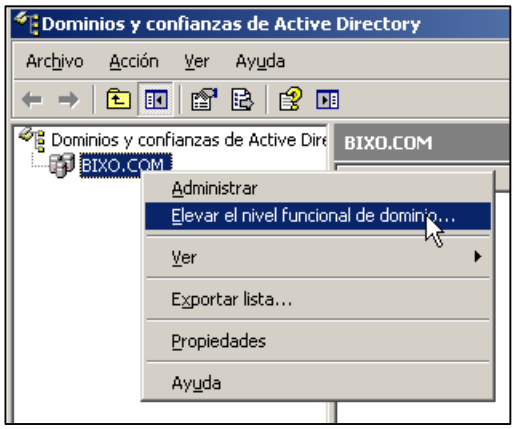




Si nos fijamos en el formulario anterior veremos cómo la opción Universal esta desactivada. Esto ocurre porque el servidor que se usó para capturar esa pantalla estaba usando un nivel funcional de dominio Windows 2000.

Si nos ocurriera algo como esto y quisiéramos elevar el nivel funcional de dominio lo podemos hacer desde la consola "Dominios y confianzas de Active Directory".

Una vez abierta la consola, pulsamos botón derecho sobre el nombre del dominio y escogemos la opción "Elevar el nivel funcional del dominio" como se muestra en la imagen.



El sistema nos preguntará si queremos elevar el nivel funcional del dominio. Si queremos trabajar con grupos universales tendremos que elevarlo a nivel de Windows 2003 como mínimo. Esta operación no tiene marcha atrás, e implicará que no podremos usar Windows 2000 en ningún controlador del dominio a partir del momento en que elevemos dicho nivel funcional.

Como prueba de todo lo que hemos hablado sobre grupos de dominio, crear un grupo de cada uno de los 6 tipos posibles (seguridad local, distribución local, seguridad global, distribución global, seguridad universal, distribución universal). Una vez creados, eliminad dichos grupos usando la consola.

Para añadir miembros a un grupo, simplemente tenemos que acceder a las propiedades de dicho grupo desde la consola. Desde allí escogemos la pestaña Miembros, y mediante el botón agregar podemos ir añadiendo miembros al grupo.

También podemos escoger la pestaña "Miembro de" e introducir al grupo como miembro de otro grupo.

Evidentemente, tanto para introducir miembros, como para introducirse como miembro de otro grupo, tendremos que respetar las reglas de ámbito y contenido que vimos para los grupos.

Como práctica, cread tres usuarios con nombres Pata, Peta y Pita. Cread un grupo local con nombre Grupito e introducir a los 3 usuarios como miembros.

ADMINISTRACIÓN DE GRUPOS DESDE EL SÍMBOLO DEL SISTEMA.

Podemos gestionar las cuentas de grupos desde el símbolo del sistema con los mismos comandos que usamos para gestionar las cuentas de usuario. Así, para crear una cuenta de grupo usamos el comando

dsadd group "nombre distinguido del grupo" opciones

Ya vimos en qué consistía un nombre distinguido, así por ejemplo, para crear un grupo con nombre VIKINGOS usamos el siguiente comando:

dsadd group "CN=VIKINGOS, CN=USERS, DC=BIXO, DC=COM"

Comprobad desde Usuarios y Equipos de Active Directory que efectivamente el grupo se ha creado correctamente.

Algunas de las opciones que podemos usar con este comando son:

Secgrp [yes | no] Indica si el grupo es de seguridad (yes) o de distribución (no).

Scope [L | G | U] Indica si el ámbito es Local (L), Global (G) o Universal (U).

Para borrar un grupo, usamos el comando dsrm.

dsrm "nombre distinguido del grupo"

Así, para borrar el grupo VIKINGOS anteriormente creado ejecutaríamos el comando:

dsrm "CN=VIKINGOS, CN=USERS, DC=BIXO, DC=COM"

Si queremos añadir un usuario a un grupo mediante línea de comandos lo podemos hacer con la orden dsmod.

dsmod group "nombre distinguido del grupo" –addmbr "nombre distinguido del usuario" "nombre distinguido del usuario" "nombre distinguido del usuario" ….

Vemos cómo podemos añadir varios miembros a la vez a un grupo, eso sí, siempre usando su nombre distinguido.

Como ejercicio, cread 4 usuarios cualesquiera en USERS, luego crear un grupo llamado NUEVO e introducid como miembros de dicho grupo a los 4 usuarios creados. Todo ello hay que realizarlo desde el símbolo de comandos. Para comprobar que dicho grupo cuenta con los usuarios una vez realizado el ejercicio, podéis acceder a la consola para comprobarlo más cómodamente.

Otro comando interesante nos permite eliminar la pertenencia de un usuario a un grupo. Esto se consigue con el comando:

dsmod group "nombre distinguido del grupo" –rmmbr "nombre distinguido del usuario" "nombre distinguido del usuario" "nombre distinguido del usuario" ….

Como ejercicio, eliminar del grupo NUEVO a dos usuarios de los que se han introducido anteriormente. Fijaros como simplemente sacamos a los usuarios del grupo, en ningún caso borramos las cuentas de los usuarios.

Para ver los miembros de un grupo sin tener que acceder a la consola, podemos usar el comando:

dsget group "nombre distinguido del grupo" –members

Ejercicio sobre grupos.

Crear un bosque formado por dos dominios:

- JESITEL.COM
  - AGUA.JESITEL.COM

Crear en el CD de jesitel.com una carpeta compartida con nombre RAIZ y en el CD de agua.jesitel.com una carpeta compartida con nombre RAMA.

Conectar una maquina con un Windows cliente al dominio jesitel.com como miembro del mismo.

Crear en jesitel.com dos cuentas de usuario; JOSE y JUANA.

Crear en agua.jesitel.com dos cuentas de usuario; ALBERTO y ANAMARIA.

Queremos que los 4 usuarios creados sean capaces de escribir tanto en la carpeta RAIZ como en la carpeta RAMA a través de la red. Queremos además que ellos 4 sean los únicos usuarios que puedan hacerlo, mientras que todos los demás usuarios solo podrán leer dichas carpetas, pero no escribir. Esto hay que comprobarlo, por lo que tendremos que crear algún otro usuario de prueba.

Queremos conseguir que si quiero que un usuario de esos 4 deje de poder escribir en las carpetas, me baste con realizar una acción. Es decir, que con una sola operación conseguiré que el usuario deje de poder escribir en ambas carpetas.

PERFILES DE USUARIO EN WINDOWS SERVER.

En Windows, un perfil de usuario consiste en un espacio de almacenamiento donde se guardan los documentos del usuario, distintas preferencias, la organización de su escritorio, los favoritos del navegador web, las configuraciones del registro de sistema de dicho usuario, etc.

Cuando trabajamos con un sistema operativo cliente, este perfil se almacena localmente, es decir, en la maquina donde trabajemos, y en una carpeta determinada:

- Documents and Settings\Nombre del usuario en Windows XP
- Users\Nombre del usuario en Vista y Windows 7.

Una de las ventajas de montar un dominio, es que podemos utilizar perfiles que no se almacenen localmente. En un dominio podemos utilizar:

- Perfiles de usuario locales
- Perfiles de usuario móviles
- Perfiles de usuario obligatorios

PERFILES DE USUARIO LOCALES.

Estos perfiles son los habituales, cada usuario guarda su perfil en un directorio de la maquina local donde inicia sesión. Es un tipo de perfil que precisa que los usuarios siempre usen el mismo ordenador si quieren poder acceder a sus documentos. Si en nuestro dominio los usuarios suelen cambiarse de ordenador, vamos a tener problemas con los perfiles de usuario locales.

Imaginemos que el usuario JOCADI abre sesión un lunes en el EQUIPO13, trabaja en un documento y cierra sesión al finalizar el día. Si este mismo usuario abre sesión el martes en un equipo distinto, pongamos EQUIPO28, no podrá acceder obviamente al perfil que dejó grabado en el EQUIPO13, y se creará un nuevo perfil local sin ningún contenido en el EQUIPO28.

Obviamente los usuarios pueden ir almacenando sus documentos en memorias USB e irlos pasando de un ordenador a otro, pero esto no quita que sea una fuente de errores importante. Además, un perfil guarda mucha más información aparte de los documentos.

Otro problema con los perfiles de usuario locales, es la perdida de datos por avería o cualquier otro motivo. Puesto que el perfil está grabado en el ordenador local, si este se estropea o tiene que ser cambiado, el usuario se encontrará con que ha perdido sus datos si no los tenía almacenados en algún otro sitio de respaldo.

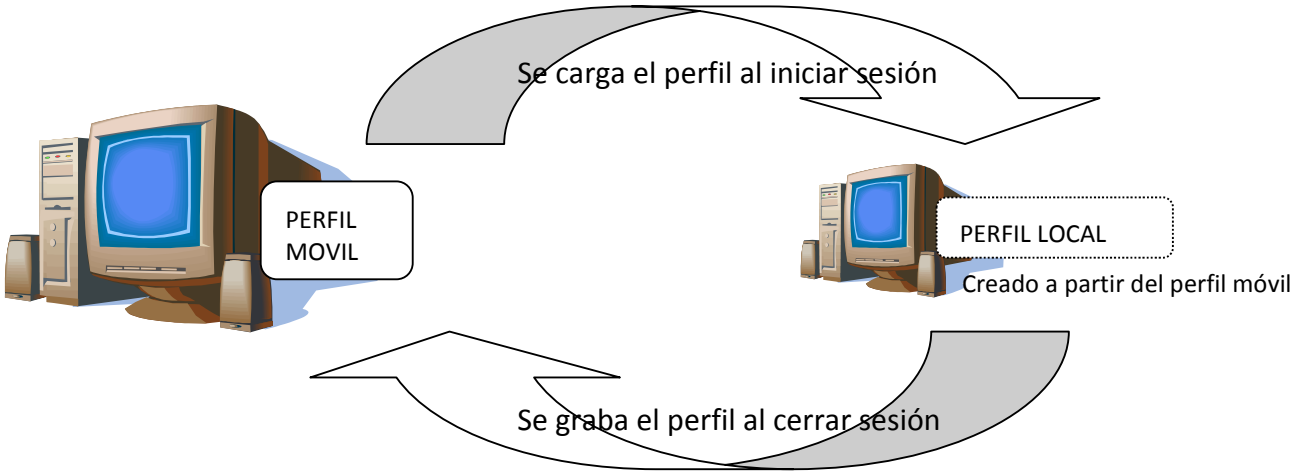
Las copias de seguridad de la empresa, también se ven muy afectadas por los perfiles de usuario locales. Cada vez que queramos hacer una copia de seguridad de todo, tendremos que ir ordenador por ordenador copiando sus perfiles, y nos encontraremos con muchas versiones de un mismo fichero.

Para utilizar perfiles de usuario locales no hay que hacer nada. Es la opción por defecto del dominio y si no lo configuramos, es la opción que utilizaremos.

PERFILES DE USUARIO MÓVILES.

En un perfil de usuario móvil, el perfil no se almacena en la maquina local donde se conecta el usuario, sino que se queda almacenado en una carpeta de red, normalmente ubicada en el mismo controlador de dominio.

Siguiendo el ejemplo anterior, el usuario JOCADI abre sesión un lunes en el EQUIPO13, trabaja en un documento y cierra sesión. Su perfil no queda grabado en el EQUIPO13, sino que queda almacenado en el controlador de dominio. Si este usuario llega el martes y abre sesión en el EQUIPO28, comprobará que puede seguir trabajando en el documento del lunes. Da la impresión de que el perfil se "mueve" entre los ordenadores siguiendo al usuario, es por ello que se le da el nombre de perfil móvil.



Como vemos en el gráfico anterior, cuando un usuario abre sesión en una maquina cliente de nuestro dominio, se carga el perfil móvil de dicho usuario desde nuestro servidor, y se guarda una copia en la maquina cliente.

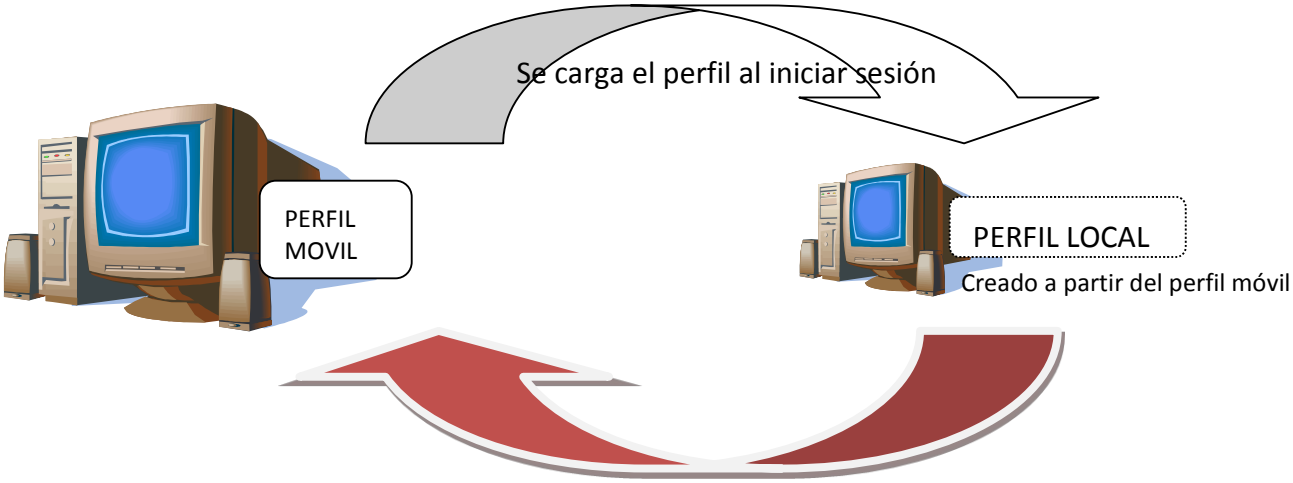
El usuario trabaja en la maquina cliente, y trabaja sobre ese perfil que se ha cargado desde el servidor, por lo que en realidad se comporta como si fuera un perfil local, es decir, cuando guarda un documento lo guarda localmente, no en el servidor.

Esto es así para no sobrecargar la red ni el dominio, si el usuario trabajara sobre el perfil móvil del servidor directamente, habría que estar continuamente enviando información entre la máquina y el servidor y sería muy lento desde el punto de vista del usuario. Otro motivo para trabajar con el perfil local, es que esto nos permite trabajar aunque el servidor deje de estar operativo momentáneamente.

Una vez que el usuario cierra sesión, el perfil local se sincroniza con el perfil que está almacenado en el servidor, añadiendo todos los nuevos documentos y configuraciones, cambiando los que se hayan modificado, etc.

Por lo tanto, en la maquina donde el cliente ha estado trabajando, se queda grabado un perfil local, que es (supuestamente) una copia del perfil móvil que está almacenado en el servidor.

¿Porque decimos lo de supuestamente?



SERVIDOR FUERA DE LINEA

Como vemos en este gráfico, se puede dar el caso de que se inicie sesión en el dominio, se cargue el perfil móvil a la maquina local, el usuario trabaje y modifique dicho perfil, pero cuando llega el momento de cerrar sesión y actualizar los datos del perfil en el servidor, el servidor no está operativo y sea imposible actualizar el perfil móvil almacenado en el servidor.

Como es lógico, esto hará que tengamos dos perfiles distintos para un mismo usuario, uno en el servidor (más antiguo) y otro en la maquina local (más reciente). ¿Qué ocurrirá la próxima vez que el usuario abra sesión en esa máquina, estando ya el servidor operativo?

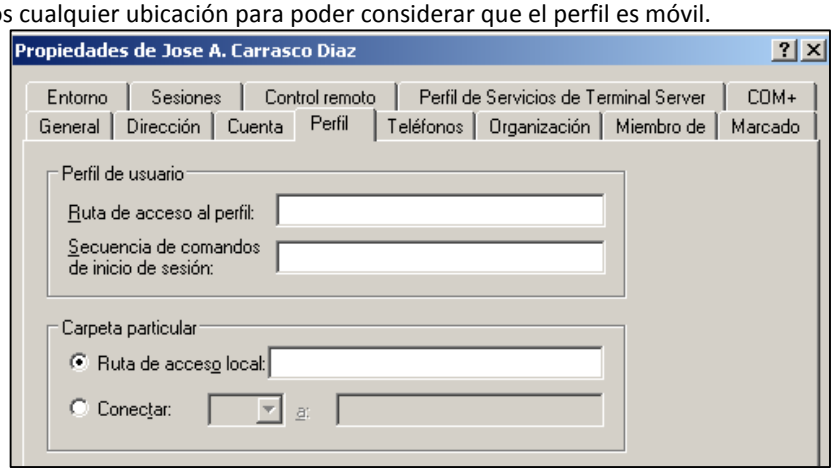
Lo que ocurre es que cada vez que un usuario inicia sesión, Windows Server no se limita a copiar el perfil móvil en el perfil local, machacando todo lo que hubiera en el equipo cliente, sino que realiza una combinación o **sincronización** de ambos perfiles, machacando los archivos y documentos siempre con el que tenga una fecha posterior, y combinando los archivos únicos de ambos perfiles.

Esto puede conllevar varios comportamientos “extraños” en los perfiles, sobre todo si existen varios usuarios que usen una misma cuenta de usuario, y esta se configura con perfil móvil. Por ello, hay que intentar siempre conceder perfiles móviles únicamente a las cuentas que sepamos que son usadas por una única persona. Si no lo hacemos así, tendremos problemas con los perfiles de esos usuarios compartidos.

Veamos ahora cómo podemos crear un perfil móvil para un usuario.

Accedemos a las propiedades del usuario al que queremos crearle un perfil móvil, usando la consola de Usuarios y Equipos de Active Directory. Desde esta hoja de propiedades accedemos a la pestaña Perfil.

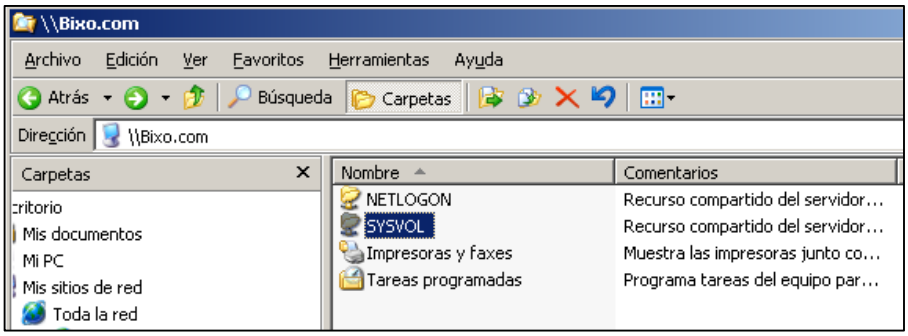
En las propiedades de un usuario del dominio, tenemos que indicar simplemente una ruta en “Ruta de acceso al perfil” que indicará en que sitio se tiene que almacenar el perfil de dicho usuario. Si no ponemos nada, el perfil se creará en la máquina del usuario, por lo que será un perfil local. Basta con que pongamos cualquier ubicación para poder considerar que el perfil es móvil.



Evidentemente, el usuario debe poder acceder a esta ruta desde una maquina cliente, por lo que debe ser una ruta de red, no tendría sentido grabar el perfil en una ubicación local.

Así, si ponemos como ruta “C:\PERFILES\PEDRO” el usuario guardara su perfil en el disco duro local C: es decir, el disco duro de la maquina cliente donde esté sentado, no en el disco duro del servidor. Lo mismo ocurre si utilizamos la ip 127.0.0.1 por ejemplo.

Si en un explorador de archivos, escribimos \\nombre_completo_del_servidor veremos como aparece una carpeta que directamente esta compartida por nuestro servidor en la red, SYSVOL.



Esta carpeta, que localmente esta almacenada en el controlador de dominio en el directorio %WinDir%\SYSVOL\SYSVOL es una carpeta que ya está preparada para ser compartida en red, para almacenar perfiles, scripts, etc. Tiene establecidos todos los permisos adecuados para que todos los usuarios puedan acceder a ella desde la red.

Dentro de esta carpeta sysvol veremos una carpeta con el nombre de nuestro dominio, dentro de esta carpeta crearemos una carpeta para almacenar los perfiles, a la que denominaremos por ejemplo PERFILES. Ahora, dentro de esta carpeta habrá que ir creando una carpeta para cada uno de los usuarios a los que queremos darle un perfil móvil, retocando los permisos tanto de compartición de la carpeta como de seguridad de la misma para asegurarnos que solo el usuario puede acceder a dicha carpeta desde la red.

Como esto es un engorro, hay un pequeño pero cómodo truco que podemos utilizar, y es indicar al sistema que cree una carpeta con nombre igual a su nombre de usuario automáticamente cuando el usuario inicie sesión por primera vez en el dominio, para ello usaremos la variable de sistema %username% que es la que almacena el nombre del usuario que ha abierto sesión.

De esta forma conseguimos que cada usuario automáticamente cree su propia carpeta, con lo que se establecerán los permisos justamente como nos interesa.

La ruta completa en la imagen anterior sería \\Bixo.com\SYSVOL\BIXO.COM\Perfiles\%username%

De esta manera, cuando el usuario abra sesión por primera vez en el dominio, el sistema creará una carpeta en la ubicación de red indicada. Esta carpeta, como es creada por el propio usuario automáticamente tendrá los permisos establecidos de modo que él será la única persona que podrá acceder a dicha carpeta y su contenido desde la red, que es precisamente lo que andamos buscando.

Evidentemente nadie nos obliga a crear los perfiles en sysvol, podemos usar cualquier otra carpeta compartida que deseemos, tanto en el controlador de dominio como en cualquier otro punto de la red. Igualmente no tenemos por qué usar la variable username, y podemos dar cualquier nombre a la carpeta donde se almacenará el perfil del usuario.

POSIBLES ERRORES EN UN PERFIL MÓVIL.

Si el sistema nos indica al abrir sesión con un usuario que cuenta con perfil móvil que **no encuentra el perfil**, normalmente es debido a que la carpeta que hemos introducido como ruta de perfil, o bien no existe o bien no puede ser accedida por el usuario, debido a permisos mal establecidos. Una forma rápida de comprobarlo, es abrir un explorador de archivos una vez que el usuario abra sesión y escribir la dirección exacta que hemos puesto en la ruta del perfil. Normalmente comprobaremos como recibimos un error al acceder a dicha carpeta, error que habrá que corregir.

Si el sistema nos indica al abrir sesión con un usuario que cuenta con perfil móvil que le resulta **imposible leer el perfil**, es normalmente debido a que el usuario no tiene permisos de lectura sobre la carpeta que hemos introducido como ruta de perfil. Lo comprobamos de la misma forma que en el punto anterior.

Si el sistema nos indica al **cerrar sesión** con un usuario que cuenta con perfil móvil que le resulta **imposible grabar el perfil**, es debido a que el usuario no tiene permisos de escritura sobre la carpeta que hemos introducido como ruta de perfil, o bien a que la carpeta ha dejado de estar compartida por alguna razón.

Como vemos, es muy importante leer la información del error en pantalla. Ya sabéis, hay que intentar resistir la extraña fuerza que os impulsa a cerrar los mensajes de error inmediatamente sin leerlos antes.

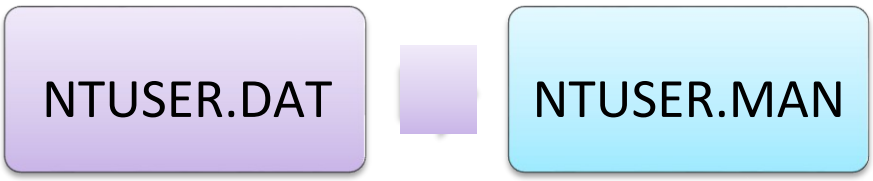
PERFILES DE USUARIO OBLIGATORIOS.

Un perfil de usuario obligatorio es en realidad un perfil móvil que asignamos a los usuarios, pero sin darles permiso para que graben el perfil en el servidor al terminar la sesión. Además es un perfil que no se combina con el perfil local al cargarse desde el servidor.

Al no permitir que el usuario sincronice el perfil en el servidor al cerrar sesión, conseguimos que el usuario use un perfil de "solo lectura". No importa lo que haga con el perfil de usuario, cuando cierre y vuelva a abrir sesión el perfil volverá siempre al mismo estado.

Es un perfil que se usa mucho en bibliotecas, cibercafés, y en general en cualquier situación donde queremos que un usuario pueda abrir sesión en nuestro dominio, pero no queremos que modifique nada o deje grabado nada en las máquinas.

Para conseguir que un perfil se transforme en obligatorio, simplemente hay que ir a la carpeta donde se almacena su perfil y buscar un archivo que se denomina NTUSER.DAT que es el archivo donde se almacenan todas las modificaciones del usuario en el registro del sistema. Basta con modificar la extensión de este fichero, de .DAT a .MAN, es decir, renombrar el fichero NTUSER.DAT a NTUSER.MAN. Con esto conseguiremos que dicho perfil sea obligatorio y que el usuario no lo pueda modificar.



Para poder modificar este fichero, necesitamos acceder al perfil del usuario como usuario administrador, el problema es que dicha cuenta no puede acceder a los perfiles del usuario. Para conseguir este acceso, tenemos que hacer al **grupo Administradores** propietario de la carpeta del perfil del usuario (recordando activar la herencia para subcontenedores) y posteriormente modificar la seguridad del perfil para que pueda ser accedido tanto por el usuario para el que se creó el perfil inicialmente como por el grupo administradores. Es importante no asignar la propiedad del perfil a nadie que no sea el grupo administradores, ya que de lo contrario el perfil se corrompería.

Una vez que tengamos un perfil obligatorio bien realizado debemos comprobar que realmente el perfil es obligatorio (de solo lectura). Podemos comprobarlo de la siguiente manera:

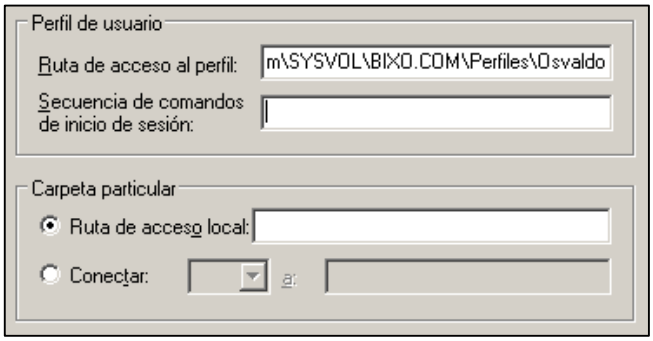
1. Abrimos sesión
2. Modificamos el perfil (poniendo accesos directos en el escritorio por ejemplo)
3. Cerramos sesión
4. Abrimos sesión y comprobamos que los cambios no se han grabado.

PERFILES DE USUARIO SUPER OBLIGATORIOS.

No entra de momento en este curso.

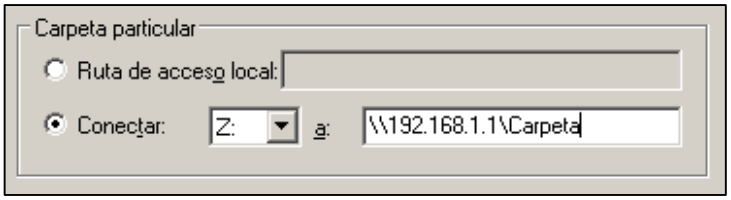
CARPETA PARTICULAR DEL USUARIO.

Como podemos comprobar, en la pestaña Perfil de las propiedades del usuario en la consola Usuarios y Equipos de Active Directory aparecen 3 opciones más aparte de la ruta del perfil.



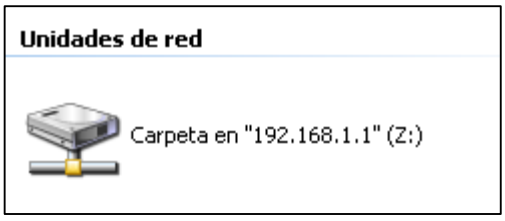
La opción de **Secuencia de comandos de inicio de sesión** nos permite indicar el nombre de un script (pequeño programa) que se ejecutará cada vez que el usuario inicie sesión localmente. Esta opción no suele ser utilizada y su función se realiza mediante el uso de una GPO como veremos en temas posteriores.

Las opciones de Carpeta particular si vamos a verlas con detenimiento. Estas opciones nos permiten montar una unidad de red en el equipo local donde el usuario abra sesión, e incluso asignarle una letra con la opción Conectar. Veamos un ejemplo.



Con estas opciones, le estamos indicando al sistema que cada vez que el usuario inicie sesión en una máquina del dominio automáticamente acceda a la carpeta compartida en red con nombre CARPETA y situada en el equipo 192.168.1.1 y la monte en el equipo local del usuario como un volumen de datos con la letra Z.

Si abrimos ahora sesión con dicho usuario en una maquina cliente, y abrimos el explorador de archivos, comprobaremos como efectivamente aparece una letra Z que es un volumen de datos montado sobre la carpeta compartida.



Como vemos, en el ejemplo anterior hemos usado un recurso compartido directamente en un equipo, normalmente lo más frecuente es crear un directorio dentro de nuestro SYSVOL y allí ir creando las carpetas para los usuarios que necesiten carpetas particulares. Ahora vamos a crear una carpeta en SYSVOL con el nombre de Particulares, y dentro iremos colocando carpetas para algunos usuarios.

En conectar pondremos en cada usuario dentro de la consola usuarios y equipos de Active directory la siguiente ruta: \\Bixo.com\SYSVOL\BIXO.COM\Personales\%username%

Evidentemente la carpeta Personales la hemos creado con anterioridad, y hemos dado control total sobre ella a todos los usuarios autentificados. Fijaros como usamos de nuevo el "truco" de usar la variable %username% para que de esta forma el sistema cree automáticamente la carpeta con el nombre del usuario cuando este abra sesión, de modo que no tenemos que preocuparnos de crear dicha carpeta a mano ni de ajustar sus permisos directamente.

Cuando el usuario Osvaldo abra sesión en cualquier equipo cliente de nuestro dominio, desde su explorador de archivos veremos la unidad Z: como si fuera un volumen de datos de su propia máquina.

En todas estas pruebas hemos utilizado la opción de conectar, no la de ruta de acceso local. Ambas opciones son excluyentes entre sí y realizan exactamente la misma función. La única diferencia es que si escribimos la ruta en Ruta de acceso local en lugar de en conectar, no se le asignará una letra al volumen de datos montado en el cliente.

Ejercicio sobre perfiles.

En un dominio crear 5 cuentas de usuario, con nombre PIPA, PIPE, PIPI, PIPO y PIPU.

Preparar PIPA y PIPE para que tengan perfil móvil.

Preparar PIPI y PIPO para que tengan perfil obligatorio (cada uno distinto). Queremos que en su escritorio tengan accesos directos al block de notas y a la calculadora.

Preparar PIPU para que tenga perfil local.

Conectar 2 máquinas clientes (XP, Vista, 7, etc.) a nuestro dominio, y comprobad como PIPA y PIPE pueden abrir sesión en cualquier ordenador sin perder su perfil.

Comprobad como PIPI y PIPO no pueden realizar cambios en su perfil y aunque borren los accesos directos al block de notas y a la calculadora, cuando abren sesión de nuevo vuelven a aparecer.

Comprobad como PIPU puede abrir sesión en cualquier ordenador, pero su perfil es distinto en cada máquina.

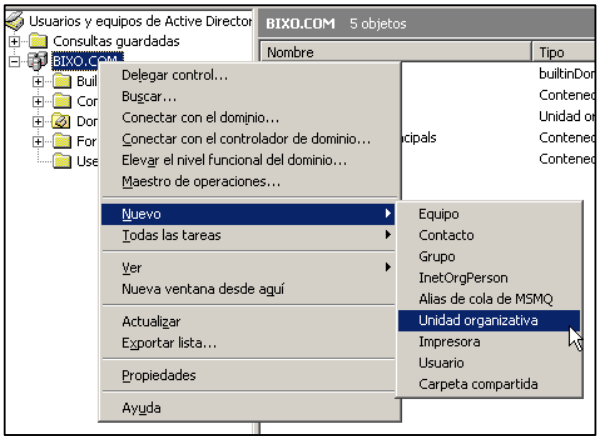
Queremos que PIPA tenga en su equipo un volumen con letra J que en realidad será una carpeta compartida en el controlador principal del dominio. Queremos que tenga control total sobre dicho volumen J.

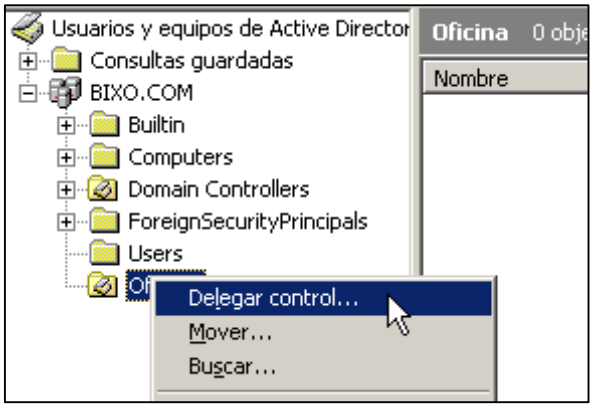
Queremos que PIPE, PIPI y PIPO cuenten en sus equipos con un volumen con letra V que en realidad será una carpeta compartida en el controlador principal del dominio. La carpeta es común para los 3, de modo que todos pueden leer y escribir en ella.

UNIDADES ORGANIZATIVAS. DELEGACIÓN.

En ocasiones, nos es útil delegar algunas tareas de administración en usuarios normales, sin tener que convertir a estos usuarios en miembros del grupo administradores. Algunas delegaciones podemos conseguirlas mediante el uso de los grupos de usuarios ya definidos en Windows Server; así por ejemplo si hacemos a un usuario miembro del grupo Operadores de Copia, conseguimos que dicho usuario pueda realizar copias del sistema, si hacemos a un usuario miembro del grupo Impresión, conseguimos que dicho usuario pueda administrar las impresoras, etc.

Si lo que queremos es que el usuario tenga algunos poderes de administración sobre los usuarios y equipos del Active Directory tendremos que utilizar las opciones de delegación incluidas en la consola Administrar usuarios y equipos en Active Directory. Para ello, basta con crear una nueva Unidad Organizativa y pulsar botón derecho del ratón en el nombre de dicha unidad. La primera opción que veremos es la Delegar control.





En el asistente que nos aparece, debemos agregar al usuario al que queremos darles poderes sobre dicha U.O. Luego podremos decidir que tareas queremos asignarle.

Si escogemos delegar tareas comunes, veremos cómo podemos permitir que dicho usuario restablezca las contraseñas de los usuarios incluidos en la U.O, gestionar grupos incluidos en la U.O, etc.

Normalmente no es necesario utilizar tareas personalizadas, ya que con las tareas comunes solemos tener más que suficiente.

Cuando tengamos que eliminar una delegación sobre una unidad organizativa, o modificarla de algún modo, veremos cómo no tenemos ninguna opción "a la vista" que nos permita eliminar las delegaciones, ni tan siquiera consultarlas.

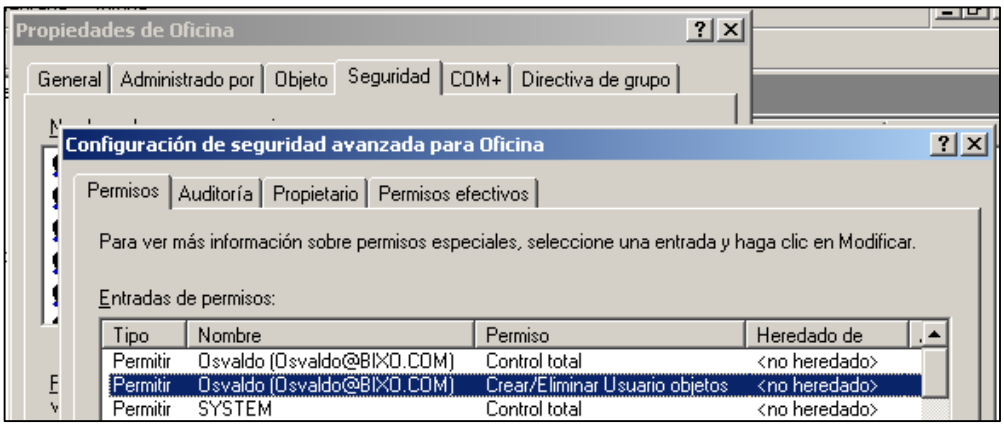
Para poder consultar, modificar o eliminar una delegación, tendremos que realizar los siguientes pasos:

1) En el menú Ver de la consola "Usuarios y Equipos de Active Directory" habrá que activar la opción de "Ver características avanzadas"

2) Dando botón derecho a la U.O. de la que queremos eliminar la delegación, escogeremos las opciones Propiedades – Seguridad – Opciones avanzadas.

Veremos cómo en Permisos, dentro la Configuración de seguridad avanzada para la U.O. tendremos al usuario al que hemos delegado tareas, normalmente ocupando varias líneas. Basta con quitar esas líneas para eliminar la delegación.

De la misma forma, podríamos añadir desde aquí nuevas delegaciones, modificar algunas de las delegaciones ya establecidas, etc.



Como ejercicio:

1) Cread una unidad organizativa con nombre CARNAVAL.

2) Cread tres usuarios con nombre SELU, LOBE y VERA en la unidad organizativa USERS y luego moverlos a la unidad organizativa CARNAVAL.

3) Queremos delegar el control de la UO CARNAVAL en el usuario LOBE, de modo que pueda crear y eliminar cuentas de usuario en dicha UO, restablecer las contraseñas y ver toda la información de las cuentas de usuario de dicha UO.

4) Abrid sesión en un Windows Cliente conectado al dominio con la cuenta LOBE.

5) Ejecutar en dicha sesión la consola de Usuarios y Equipos de Active Directory, comprobad como podemos eliminar a SELU por ejemplo, y cómo podemos restablecer la contraseña de VERA.

HERRAMIENTAS ADMINISTRATIVAS DE WINDOWS 7.

No entra de momento en este curso.

POLITICAS DE GRUPO.

Windows Server permite centralizar la administración y configuración de usuarios y equipos en un dominio mediante el uso de las Políticas o Directivas de Grupo (Group Policies). Las políticas de grupo nos permiten administrar y configurar usuarios y equipos de una forma centralizada, estas políticas nos permiten administrar cosas como configuraciones del registro, políticas de seguridad, instalación automática de software, ejecución de scripts, redirección de carpetas locales a recursos de red, etc.

OBJETO DE POLÍTICA DE GRUPO.

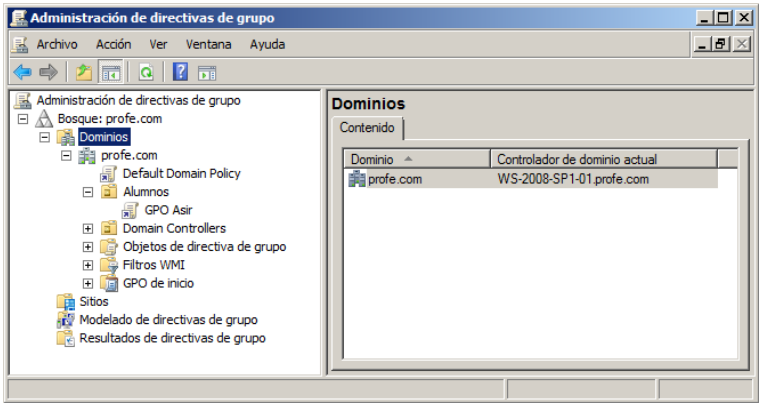
En temas anteriores vimos como podíamos configurar Windows con la orden gpedit.msc. Esta orden permite configurar las políticas de grupo (Group Policy EDIT) locales. En Windows server tenemos la opción de editar también estas mismas políticas de grupo pero no ya solo de forma local, sino que podemos establecer políticas de grupo que afectarán a todo el bosque, a un árbol en concreto, a un dominio completo, a uno o varios grupos o a uno o varios usuarios.

Las políticas de grupo se especifican mediante objetos de directiva de grupo (Group Policy Objects o GPO). Una GPO es un objeto que incluye una serie de directivas o políticas que pueden aplicarse centralizadamente a equipos y usuarios, viene a ser como un fichero que podemos crear en cualquier momento, que puede estar activo o no, y que puede usarse para controlar la configuración de usuarios y equipos.

La forma de utilizar una GPO es la siguiente: en primer lugar creamos el GPO, que incluye una plantilla que incorpora todas las posibles políticas o configuraciones que se pueden aplicar. Configuramos las políticas que nos interesen (por ejemplo, obligando a que se ejecute un script cada vez que un usuario inicie sesión, o impidiendo que en un equipo se pueda ejecutar el símbolo de comandos) y una vez configuradas las políticas tal como queremos, se graba dicha GPO. Esta GPO no estará activa, es decir, no servirá para nada mientras no la vinculemos.

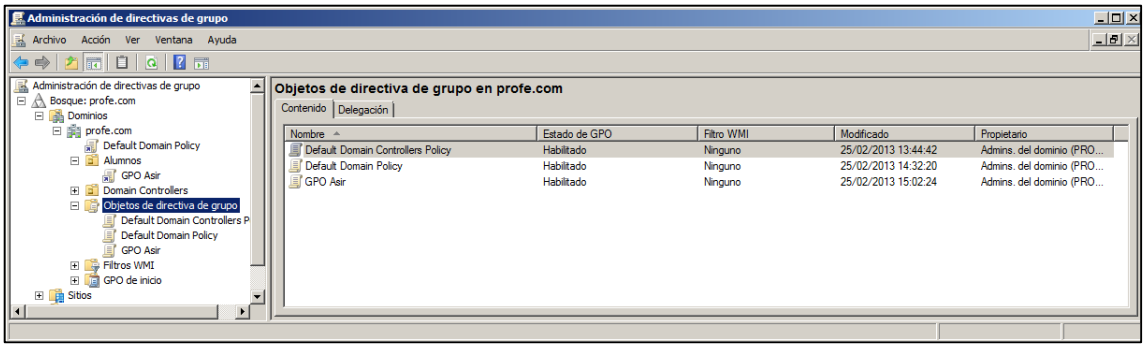
Las GPO se vinculan a nuestra estructura de árbol al nivel al que deseemos configurar. Así, por ejemplo, si vinculamos una GPO en el nombre de nuestro árbol, esta GPO afectara a todo el árbol. Si por el contrario vinculamos nuestra GPO en un nombre de domino, esta GPO solo afectará a dicho dominio. Las GPO se pueden vincular en sititos, dominios y unidades organizativas.

Vemos aquí el ejemplo de un GPO (GPO Asir) vinculado a una unidad organizativa (Alumnos) dentro del dominio profe.com.



Para obtener la anterior consola, tenemos que seleccionar “Administración de directivas de grupo” dentro del menú “Herramientas Administrativas”.

En esta consola veremos nuestro bosque con sus distintos subniveles. Existe un contenedor especial denominado objetos de directiva de grupo, donde se almacenan todos objetos GPO.

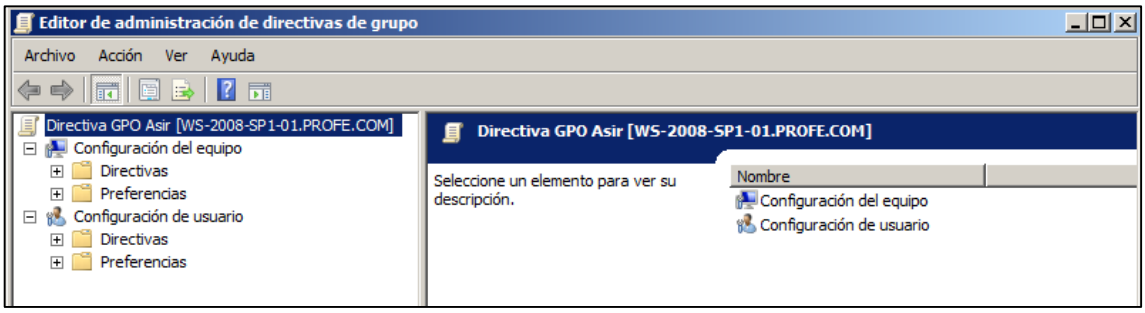


Que veamos un GPO en este contenedor Objetos de directiva de grupo no significa que dicho GPO este activo en nuestro Active Directory. Estos GPO una vez creados deben ser vinculados a la altura que deseemos en nuestro AD como hemos visto en el apartado anterior.

Para editar un GPO simplemente tenemos que pulsar botón derecho en el mismo, y escoger la opción editar.

Al crear un dominio por defecto también se crean dos GPO vinculadas al dominio y a la unidad organizativa “Controladores de Dominio”. Estas dos GPO incorporan un conjunto mínimo de configuraciones necesarias para el funcionamiento adecuado del dominio. Estos GPO se denominan “Default Domain Policy” y “Default Domain Controller Policy” respectivamente.

Dentro de cada GPO las políticas se organizan en un árbol que permite una distribución lógica de las mismas.



En este árbol de políticas existen dos ramas principales que separan las configuraciones para equipos y para usuarios.

La **configuración del equipo** agrupa todas las políticas o configuraciones que pueden establecerse a nivel del equipo. Así una política como activar un rastreador que nos permita conocer las circunstancias en las que se apaga un equipo, es una política que evidentemente pertenece a esta rama.

La **configuración del usuario** agrupa todas las políticas o configuraciones que pueden establecerse a nivel del usuario. Así una política como configurar la longitud de las contraseñas, es una política que evidentemente pertenece a esta rama.

Estas políticas se aplican cuando el equipo se inicia en el caso de las políticas de equipos o cuando el usuario inicia sesión en el caso de las políticas de usuario, pero posteriormente se van reaplicando automáticamente de forma periódica. Por defecto, la reevaluación se produce en cada usuario y cada equipo cada 90 minutos (con un retraso aleatorio de hasta 30 minutos) y en el caso de los servidores de dominio cada 5 minutos. El administrador puede forzar la aplicación inmediata de un GPO en el equipo ejecutando la orden **gpupdate** desde el símbolo de sistema.

APLICACIÓN DE POLÍTICAS DE GRUPO.

Hemos visto cómo podemos vincular un GPO en distintos niveles del árbol. A partir de ese nivel, todos los contenedores que estén incluidos en el, quedarán automáticamente bajo el ámbito del GPO vinculado.

Esto quiere decir que desde el punto de visto de un usuario o equipo, la lista de GPO que les afecta depende de su ubicación en el Directorio Activo: esta lista incluye todos los GPO vinculados a los contenedores por los que hay que pasar para llegar hasta llegar al contenedor donde ese equipo o usuario se ubica.

Puesto que cada GPO incorpora exactamente el mismo árbol de políticas, es posible que se produzcan conflictos entre los distintos GPO que afectan a un usuario o equipo.

Si varios GPO han configurado una misma política con valores distintos, el usuario o equipo recibirá configuraciones contradictorias. Resulta por tanto necesario que exista un orden de aplicación concreto y conocido, de forma que se sepa finalmente qué políticas afectan a cada usuario y equipo, sin ambigüedades. Este orden es el siguiente:

1) Se aplica la política del grupo local del equipo.
2) Se aplican los GPO vinculados a sitios.
3) Se aplican los GPO vinculados a dominios.
4) Se aplican los GPO vinculados a unidades organizativas (primero de 1º nivel, luego de 2º nivel, etc.).

Este orden de aplicación decide la prioridad entre los GPO puesto que una política que se aplica más tarde prevalece sobre otras establecidas anteriormente. Podemos decir que se van machacando o sobrescribiendo las configuraciones unas a otras. Si en un mismo contenedor o unidad organizativa existen varios GPO vinculados, estos deben de llevar un orden de aplicación.

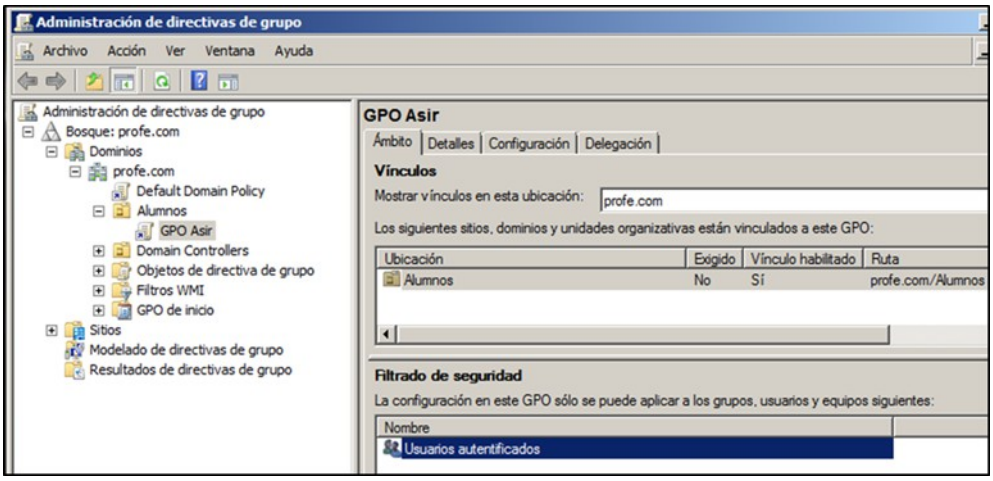
El comportamiento respecto a la herencia y prioridad entre GPO en contenedores anidados puede ser refinado mediante los siguientes dos parámetros de configuración:

1) Exigido (enforced). Este parámetro puede activarse independientemente a cada vínculo de un GPO. Si un vínculo de un GPO a un contenedor tiene este parámetro activado, sus políticas no pueden ser sobrescritas por GPO que se apliquen posteriormente.

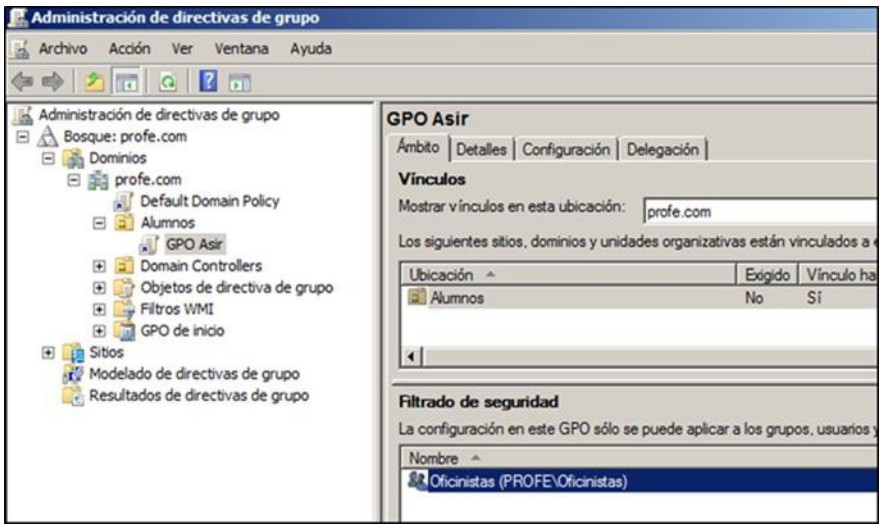
2) Bloquear herencia (de directivas) (Block Policy inheritance). Este parámetro pertenece a los contenedores del Directorio Activo. En particular, si un contenedor tiene este parámetro activado, se desactiva la herencia de las políticas establecidas en contenedores superiores, excepto aquellas que corresponden a GPO vinculados con el parámetro Exigido.

FILTRAR EL ÁMBITO DE APLICACIÓN DE UN GPO

Por defecto, a todos los usuarios y equipos incluidos en el contenedor donde vinculemos un GPO se les aplicarán todas las configuraciones o políticas que establezcamos en dicho GPO. Sin embargo, habrá ocasiones en que deseemos que a un usuario en concreto no se le aplique dicho GPO aunque sea miembro de dicho contenedor. En estos casos lo tenemos que hacer es configurar la opción de filtrado de seguridad.

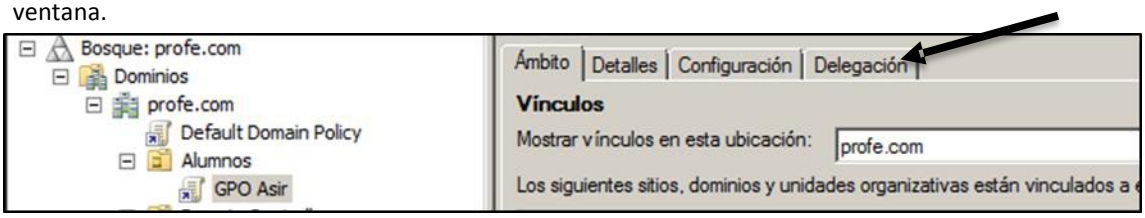


Como vemos, en esta opción por defecto se coloca el grupo de “Usuarios autentificados” al que pertenecen todos los usuarios y equipos de nuestro AD, y además es un grupo especial en el cual no podemos añadir ni quitar miembros manualmente. Lo que si podemos hacer, es borrar dicho grupo del filtrado de seguridad de nuestro GPO.



Vemos aquí como hemos reconfigurado el filtrado de seguridad para que en lugar de aplicarse a los miembros de nuestra OU alumnos que sean además miembros de usuarios autentificados (todos) se aplicará a los miembros de nuestra OU que además sean miembros del grupo Oficinistas. Si existen miembros en la OU alumnos que no sean miembros de dicho grupo Oficinistas no se les aplicará la GPO.

Esta forma de trabajar es normalmente cómoda, pero nos presenta mucho trabajo cuando simplemente queremos evitar que a un usuario en concreto no se le aplique la GPO, pues tendremos que crear un grupo nuevo y añadir a todos los usuarios de la OU menos al usuario al que queremos "salvar" de la GPO. Para estos casos es mucho mejor tocar la ACL (lista de control de acceso) de la GPO a mano. Para ello, seleccionamos la GPO en cuestión y seleccionamos Delegación en la parte superior derecha de la ventana.



Una vez en delegación, pulsamos el botón Opciones avanzadas que encontraremos en la parte inferior, y pasaremos a editar el ACL del GPO directamente.

Los permisos importantes que podemos configurar en esta ACL son los de leer y aplicar. Si a un usuario le denegamos el permiso de aplicar, quedará liberado de la GPO. Si le denegamos el permiso de leer ocurrirá exactamente lo mismo, ya que no se puede aplicar un GPO si no se puede leer. Hay que tener cuidado en el caso de que queramos que aun usuario administrador no se le aplique un GPO, ya que si le denegamos el permiso de leer, no podrá editar siquiera el GPO.

Una cosa que nos puede liar un poco, es que cualquier cambio que realicemos en el ACL directamente, no se verá reflejado en el filtrado de seguridad de la pantalla principal. Siempre que sea posible, se recomienda no tocar directamente el ACL del GPO y trabajar directamente con los filtros.

PRINCIPALES POLÍTICAS DE UN GPO.

Como hemos visto, cada GPO consta de un árbol de políticas que se dividen en dos ramas principales denominadas configuración de equipos y configuración de usuario. Cada una de estas ramas a su vez de dividen en dos ramas: Directivas y

Preferencias.

1) Directivas. Esta rama incluye tres apartados:
    a. Configuración de software. Opciones para la instalación automática de software.
    b. Configuración de Windows. Encontramos opciones de seguridad, ejecución de scripts y redirección de carpetas.
    c. Plantillas Administrativas. Políticas basadas en la modificación de valores del registro de Windows.
2) Preferencias. Esta rama incluye dos apartados:
    a. Configuración de Windows. Opciones de configuración como por ejemplo creación de variables de entorno, creación de accesos directos, mapeo de unidades de red, etc.

b. Configuración de Panel de Control. Opciones de configuración como por ejemplo instalación de dispositivos, configuración de opciones de energía, tareas programadas, servicios, etc.

En muchas ocasiones una política existe tanto en la rama de configuración de equipos como en la rama de configuración de usuarios, y dependiendo donde la encontremos tiene un significado distinto. Así, por ejemplo, si indicamos que se ejecute un script en configuración de equipos, dicho script se ejecutará cuando el equipo se encienda, sin embargo si indicamos que se ejecute un script en configuración de usuario, dicho script se pondrá en marcha cuando el usuario inicie sesión.

PLANTILLAS ADMINISTRATIVAS.

Este grupo contiene todas las configuraciones de política basadas en el registro de Windows, incluyendo aquellas que controlan el funcionamiento y apariencia del escritorio, de los componentes de Windows y de algunas aplicaciones que utilizan estas políticas, como por ejemplo la mayoría de las aplicaciones de la propia Microsoft.

Desde estas plantillas podemos configurar cosas como la longitud de las contraseñas de todos los usuarios del bosque, de un dominio o de una UO. Podemos configurar que un usuario no pueda ejecutar el símbolo de comandos, podemos configurar que se desactive el rastreador de sucesos de apagado, etc.

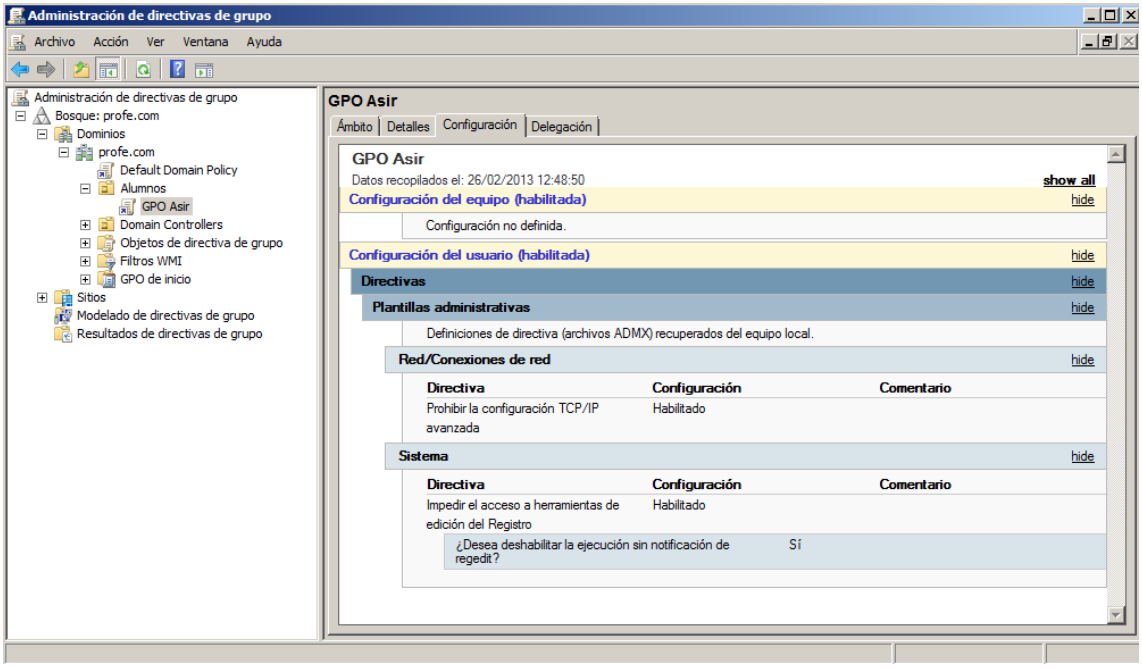
Para comprobar rápidamente que configuraciones se han realizado en un GPO podemos acceder a la pestaña configuración del GPO y desde allí se generará un informe. Dicho informe se genera utilizando el navegador de internet del equipo, y si este es Internet Explorer la primera vez que generemos un informe recibiremos un mensaje de error ya que por seguridad esa opción esta desactivada. Basta con agregar la excepción al IE para que pueda generarse el informe.

Como ejercicio, cread un GPO a nivel de dominio principal denominada GPO Ejemplo 1 y en ella indicad las siguientes configuraciones:

1) Queremos que las contraseñas no tengan que ser complicadas.
2) Queremos que las contraseñas puedan tener 3 caracteres como mínimo.
3) Las cuentas se bloquearan si se equivoca el usuario 5 veces a la hora de introducir la contraseña.
4) Se desactivará el rastreador de sucesos de apagado.
5) Se impedirá que los usuarios puedan abrir el símbolo de comandos.

Vemos aquí un ejemplo de un GPO donde se ha indicado lo siguiente:

- Se impide que los usuarios accedan a la herramienta de edición del registro (regedit).
- Se impide que el usuario pueda cambiar la configuración de TCP/IP ya que hacemos que desaparezca el botón de configuración avanzada dentro de los controladores de red.



AUDITORIAS DE SISTEMA.

No entra de momento en este curso.

VISOR DE EVENTOS.

No entra de momento en este curso.