1 Windows 2003

Windows 2003 es un sistema operativo de tipo servidor, preparado para gestionar una red de ordenadores mediante un sistema de dominios que permite una administración centralizada. Antes de comenzar es interesante conocer algunos aspectos básicos sobre las redes de ordenadores.

1.1 Introducción a las técnicas de red.

Hemos visto en el tema sobre Windows XP como trabajar en una red entre iguales, usando los grupos de trabajo. Sin embargo este tipo de solución sólo es valida para redes simples.

En la actualidad hay un número creciente de redes que no son simples. Incorporan servidores múltiples (archivos, impresión, fax, correo, 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 archivos. Obviamente, no es realista esperar que bajo estas circunstancias los usuarios sepan dónde están las cosas y sean capaces de manejarlas por ellos mismos.

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 tema 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 Area 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.
- Servicios de directorio.
- Grupos de trabajo.
- Dominios.

Hay que hacer constar que estas técnicas no son incompatibles entre si, y de hecho, muchas veces se usan varias en conjunción dentro de una misma red.

1.2 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 2.x y 3.x han sido los sistemas operativos para redes dominantes en redes pequeñas. Las estadísticas indican que las redes promedio Novell 2.x y 3.x incluyen sólo un servidor y 30 o menos estaciones de trabajo.

Con tal arreglo no se requiere un sofisticado servicio de administración de recursos. Los archivos pueden localizarse utilizando comandos como el DIR y las impresoras pueden seleccionarse fácilmente entre una lista. En la mayoría de los casos, los ambientes de usuarios LAN están completamente preconfigurados por el administrador. Los usuarios tienen acceso a ciertas impresoras, se predetermina el acceso a archivo y no requieren mucho conocimiento acerca de LAN para utilizarlo de manera efectiva.

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.

El servidor A da alojamiento a aplicaciones como WordPerfect y Lotus 1-2-3; el servidor B, al 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.

Cada una de esas cuentas de usuarios debe ser creada y mantenida de manera separada. Habrá que notar que algunos usuarios tienen cuenta en un solo servidor. Es fácil para los servidores perder sincronía cuando deben ser actualizados manualmente. La situación también se complica desde el punto de vista de usuario, pues debe conectarse y mantener una contraseña en cada uno de los servidores. Este proceso puede ser automatizado, pero suele generar errores. Los Administradores de este tipo de redes con varios servidores individuales están acostumbrados a recibir llamadas para volver a sincronizar las contraseñas del usuario entre los servidores.

Eliminado:

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 valida para la mayoría de las situaciones actuales.

1.3 Directorio de red.

Bajo este sistema, los recursos pueden estar situados en varios 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 esta 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 sin indicación de cuál servidor tiene la cuenta del usuario.

Un servicio de directorio es una manera extremadamente formal de organizar los recursos en red. La configuración de tal servicio implica una cuidadosa planeación que involucra a todos los departamentos de la organización. Los servicios de directorio funcionan mejor cuando una organización (como un departamento de sistemas) es responsable del mantenimiento del directorio. Algunos servicios de directorio permiten a los departamentos tener responsabilidad sobre ciertas porciones del directorio, pero un departamento deberá ser el responsable primario. En las organizaciones que no tienen un departamento de sistemas, podría ser difícil identificar un administrador primario del directorio.

Por su importancia, veamos un poco más en profundidad LDAP.

LDAP

LDAP (Lightweight Directory Access Protocol) es un protocolo de red que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP puede considerarse una base de datos (aunque su sistema de almacenamiento puede ser otro diferente) al que pueden realizarse consultas.

Habitualmente, almacena la información de login (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...).

En conclusión, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

Al ser LDAP un protocolo abierto, es usado por gran cantidad de compañías, e incluso existe un proyecto conocido como OpenLDAP, que se trata de una implementación libre del protocolo que soporta múltiples esquemas por lo que puede utilizarse para conectarse a cualquier otro LDAP. Así es posible usar LDAP en Linux, Unix, Windows, Mac, etc.

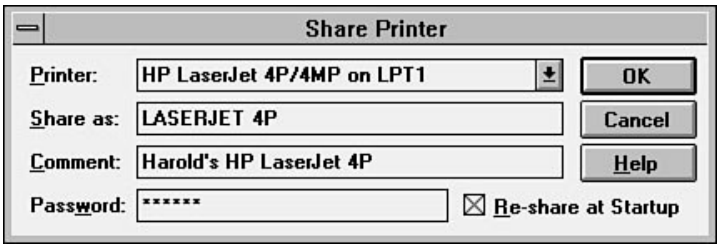
1.4 Grupos de trabajo.

Los grupos de trabajo son conceptualmente opuestos a los servicios de directorio. Los directorios son formales y están administrados centralmente; los grupos de trabajo son informales y operados por los usuarios que comparten sus propios recursos locales. Este tipo de redes se conocen como redes peer to peer, entre pares o entre iguales.

Las redes entre 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 que quieren compartir recursos a menudo necesiten 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 de Windows for Workgroups que se utiliza 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 Windows for Workgroups.

Para localizar los recursos en una red, Microsoft utiliza un servicio de explorador. En Windows NT o Windows 9x, el Entorno de Red o el Explorador de Windows puede ser utilizado para explorar la red e identificar los recursos para conectarse.

Los grupos de trabajo hacen que el compartir recursos sea una operación muy simple, pero no organizan los servicios en ningún 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 a la red desde el exterior, mediante la línea telefónica 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.

Si utilizamos Windows 2000, 2003 o Windows XP, 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 XP, tenemos que conocer (o usar) el nombre de usuario y la contraseña de un usuario local de dicha maquina XP.

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.

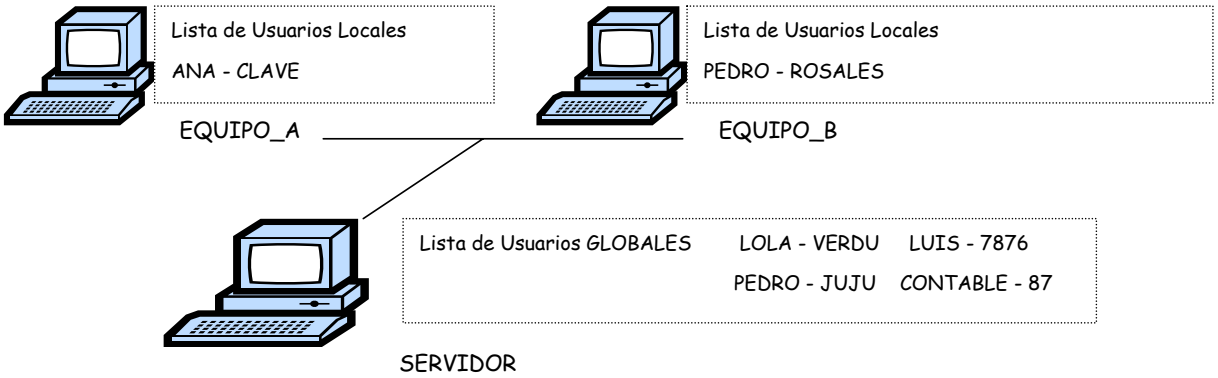
1.5 Dominios.

Si estamos usando un grupo de trabajo, y compartimos un recurso, al acceder a la lista de usuarios que pueden acceder a dicho recurso desde la red local podemos elegirlos de una lista donde aparecen todos los usuarios locales de nuestro sistema. Esto quiere decir que no podemos compartir uno de nuestros recursos para un usuario que no sea local en nuestro sistema.

Así, si en el equipo A tenemos un recurso compartido, solo podremos indicar dentro de su lista de acceso, que puede ser usado por por ANA o por LUIS cada uno de ellos con su correspondiente contraseña. 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 LOLA aparezca en la lista de usuarios 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.

Esto es así por que todas las cuentas de usuario son locales y son almacenadas en cada equipo individual. Una solución para este problema es que tengamos la opción de crear cuentas globales, es decir que podamos crear cuentas que no solo sean reconocidas en una maquina, sino que sean reconocidas en todas las maquinas 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 local. Este ordenador pasa a ser un servidor, y nuestro grupo de trabajo se convierte en un dominio.



Así conseguimos que la cuenta LUIS no se almacene localmente en el equipo B, sino que sea una cuenta global 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 su lista de usuarios a LUIS, que ahora es un usuario del dominio. Fijaros como en el grafico anterior vemos que LOLA, LUIS, PEDRO y CONTABLE son usuarios del dominio (es decir, globales en toda la red) mientras que los usuarios ANA y PEDRO son usuarios locales que solo aparecen en las listas de sus propios equipos.

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.

Los dominios toman conceptos de los grupos de trabajo y servicios de directorio. Al igual que los grupos de trabajo, los dominios son bastante informales y pueden ser administrados utilizando una mezcla de controles locales y centrales. Los dominios pueden desarrollarse con relativa facilidad y establecerse con menos complejidad que la requerida normalmente para un directorio.

Al igual que un directorio, 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.

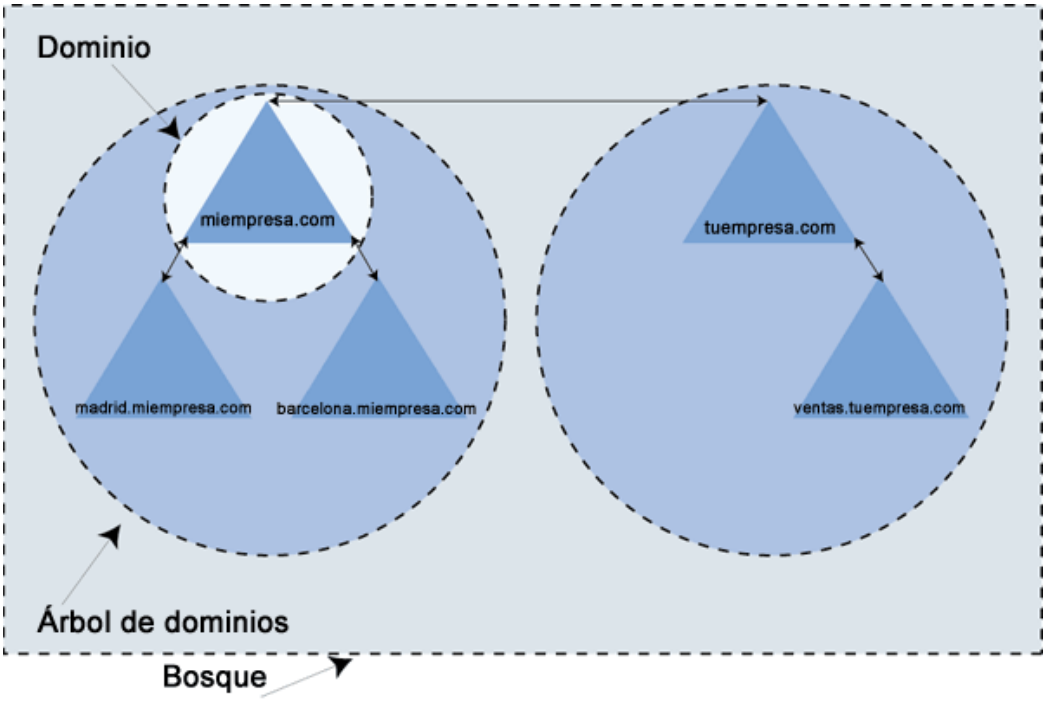
Los servidores, dentro del dominio, anuncian sus servicios a los usuarios. Los usuarios que se conectan en un dominio obtienen acceso a todos los recursos del dominio para el cual han recibido autorización de acceso. Pueden explorar los recursos en un dominio como lo harían en un grupo de trabajo, sin embargo, los dominios son alojados por servidores Windows NT y son más seguros que los grupos de trabajo.

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.

2 El Directorio Activo (Active Directory).

Windows 2003 utiliza LDAP y basa su estructura en dominios. El nombre bajo el que esta estructura se presenta es el de Directorio Activo (Active Directory).

Anteriormente, usando sistemas servidores Windows NT la estructura de dominios era bastante complicada, dado que en una red podemos establecer varios dominios, y había que establecer relaciones de confianza entre los dominios, controladores de dominio principal y de respaldo, etc. Sin embargo, en Windows 2003 toda esta estructura se ha simplificado mucho mediante el uso del Directorio Activo y la utilización de los servidores DNS.



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 2003, y un gran numero de maquinas clientes conectadas. Para realizar esto en Windows 2000 o 2003 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 un raíz de árbol, y hemos colgado el dominio ventas.tuempresa.com del raíz tuempresa.com.

Todas las relaciones de confianza que vemos en el dibujo (esas flechitas que unen dominios y que indican que dominios confían en que dominios) han sido creadas automáticamente por Windows 2003 (son relaciones de confianza implícitas) excepto la relación de confianza que une ambos árboles. Esta es la única relación de confianza que hemos tenido que indicar de forma explicita.

Sin embargo, todos los dominios son capaces de comunicarse entre si sin problemas, gracias a las propiedades de las relaciones de confianza de Windows 2000.

Al haber unido estos dos árboles de dominio, se dice que estamos formando un nuevo bosque.

Si esta misma organización se quisiera llevar a cabo con Windows NT, necesitaríamos 20 relaciones de confianza explicitas bajo el método de confianza total.

Podemos comprobar como el modelo de organización para la unión de dominios de Windows 2003 es mucho más lógico que el modelo usado por Windows NT (o por organizaciones mixtas, Windows 2003 y Windows NT). Sin embargo, para que este tipo de modelos puedan funcionar, se necesita que en los modelos de Windows 2003 se usen servidores DNS propios, cosa que no es necesaria en los modelos de Windows NT y todos estos conceptos se agrupan bajo el Directorio Activo, que es el protocolo de servicio de directorios usado por Windows 2003.

3 Instalación de Active Directory.

A diferencia de la versión 4 y anteriores de Microsoft Windows NT Server, Windows 2000 y 2003 Server no designa un sistema como controlador de dominio durante la instalación del sistema operativo. Cada servidor de Windows 2000/2003 (a partir de ahora simplemente indicaremos Windows 2000) se instala como un sistema independiente o un miembro de un dominio, cuando la instalación esta completa se puede promocionar al servidor al estado de controlador de dominio utilizando el Asistente para instalación de Active Directory de Windows 2000.

Esta herramienta proporciona una gran flexibilidad adicional a los administradores de Active Directory porque los servidores se pueden promover o degradar en cualquier momento, mientras que los servidores Windows NT 4 se designan irrevocablemente como controladores de dominio durante el proceso de instalación.

Algo que también ha desaparecido es la distinción entre controladores principales de dominio y controladores de dominio de reserva. Los controladores de dominio Windows 2000 son todos parejos en un sistema de réplica con múltiples maestros. Esto significa que los administradores pueden modificar los contenidos del árbol de Active Directory de cualquier servidor que funcione como controlador de dominio.

Esto es un avance muy importante desde el sistema de réplica de un solo maestro de Windows NT 4, en el cual un administrador sólo puede cambiar el controlador principal de dominio (PDC, Primary Domain Controller) para que después los cambios se repliquen a todos los controladores de dominio de reserva (BDC, Backup Domain Controller).

Otra ventaja de Windows 2000 es que se puede utilizar el Asistente para instalación de Active Directory para degradar un controlador de dominio de nuevo a un servidor independiente o miembro. En Windows NT 4, una vez que se instala un servidor como controlador de dominio, es posible degradarlo de PDC a BDC, pero no se puede eliminar su estado de controlador de dominio completamente, excepto reinstalando el sistema operativo.

La función básica del Asistente para instalación de Active Directory es configurar un servidor para que funcione como controlador de dominio, pero dependiendo del estado actual de Active Directory en la red, esta tarea puede tomar distintas formas.

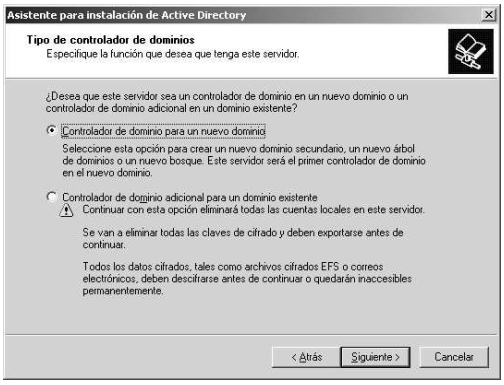
Si se instala el primer Windows 2000 Server de la red, antes de la promoción del sistema a controlador de dominio crea un Active Directory completamente nuevo con esa computadora alojando el primer dominio del primer árbol del primer bosque.

3.1 Instalación del primer controlador de Dominio.

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 2000 incorpora vínculos al asistente en la página de Active Directory de la página principal de Configurar el servidor de Windows 2000. Esta página se muestra en el explorador Microsoft Internet Explorer automáticamente después de la instalación del SO. Esta página Web local esta 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 minimas con Windows 2003, básicamente son inguales).

Para instalar el Primer controlador deberemos seguir los siguientes pasos:

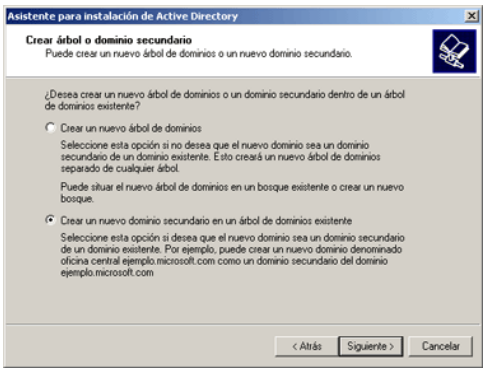


Iniciar la Herramienta Configuración del Servidor desde el menú de Herramientas Administrativas. También puede iniciar el asistente directamente ejecutando el archivo ejecutable Dcpromo.exe desde el cuadro de dialogo Ejecutar.

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.

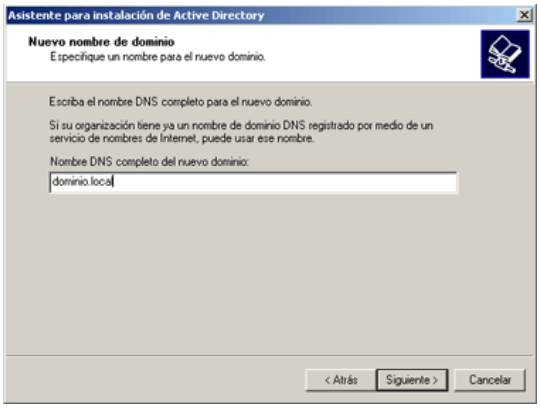
Crear un bosque o unirse a un bosque, que permite especificar una de las siguientes opciones:

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.

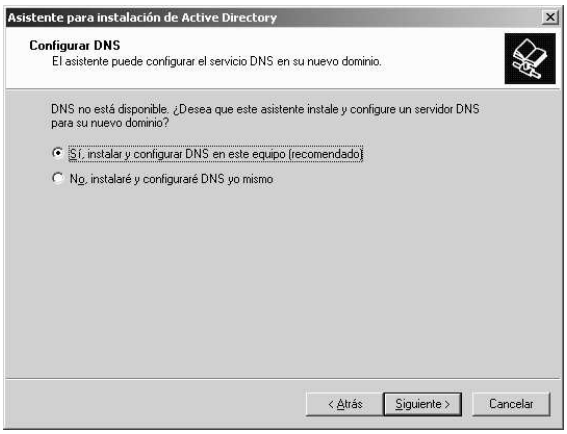
Los sistemas Windows 2000 todavía utilizan el espacio de nombres NetBIOS para sus nombres de equipo, pero Active Directory utiliza la nomenclatura DNS para los dominios. Windows NT 4 y los sistemas Microsoft Windows 9x utilizan nombres NetBIOS para todos los recursos de la red, incluyendo los dominios.

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 2000 y esta 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 2000, el asistente se ofrece a instalar Microsoft DNS Server y configurarlo para que funcione como servidor autorizado para el dominio.

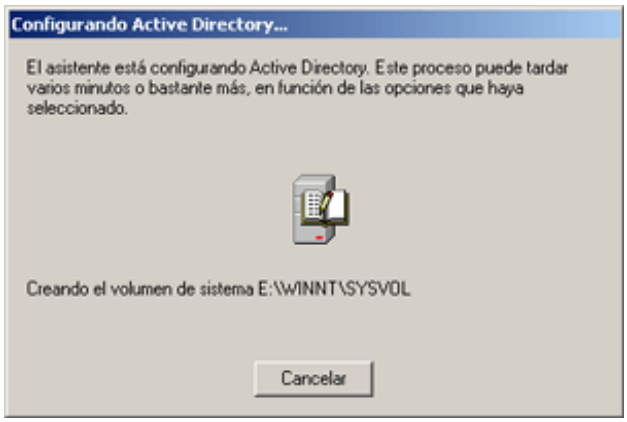
La pantalla Configurar DNS permite especificar si se desea instalar el servidor DNS o configurar uno personalmente. Si se opta por utilizar otra máquina para el servidor DNS, es preciso instalarlo y configurarlo antes de poder completar la instalación de Active Directory.

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 a Windows 2000.

Siempre que sea posible, escogeremos la opción de permisos compatibles sólo con servidores Windows 2000, ya que si no, no podremos trabajar correctamente con los bosques y árboles.

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.



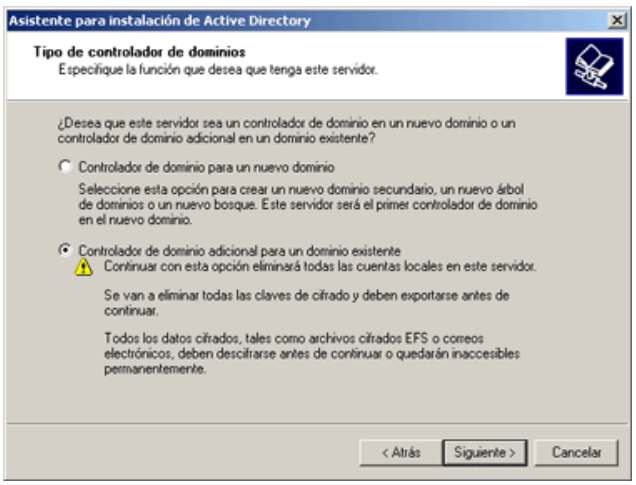
Finalización de la instalación de Active Directory: El asistente registra todas las actividades que se producen durante el proceso de instalación en dos archivos llamados Dcpromo.log y Dcpromoui.log, localizados en la carpeta %SystemRoot%\debug. La instalación puede durar varios minutos, después de lo cual hay que reiniciar el sistema para que tengan efecto los cambios.

3.2 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 2000 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 esta 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.

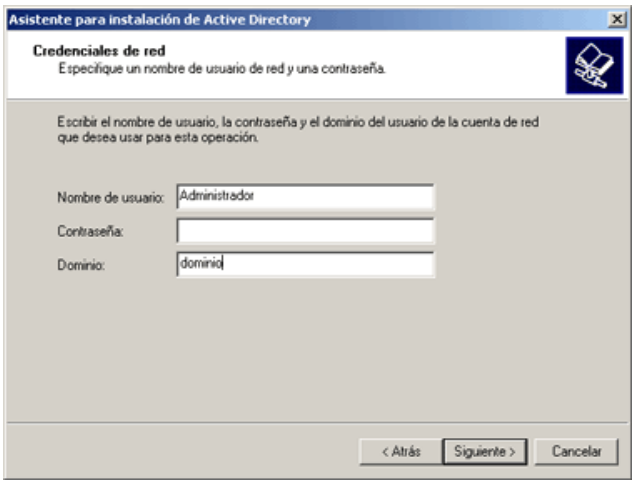
Cuando se crea una réplica, el Asistente para instalación de Active Directory configura automáticamente el proceso de réplica entre los controladores de dominio. Se puede personalizar el proceso de réplica utilizando Sitios y servicios de Active Directory.

3.3 Creación de un DC para un dominio secundario en un árbol existente

Cuando se crea el primer dominio Windows 2000 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.

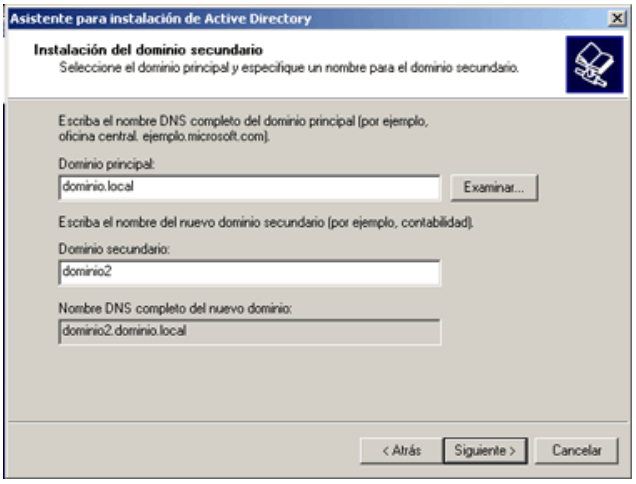
Por regla general, los dominios secundarios reflejan las divisiones geográficas, departamentales o políticas de una organización, pero se puede utilizar cualquier principio para el diseño del árbol que se desee. Un dominio principal puede tener cualquier número de secundarios, y la estructura del árbol 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 replica; 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.

3.4 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.

3.5 Degradación de controladores de dominios.

Una diferencia fundamental entre los controladores de dominio Windows 2000 y los controladores de dominio Windows NT es que se puede degradar un controlador de dominio Windows 2000 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 replica en la red, el servidor permanece como, miembro de ese dominio después de la degradación.

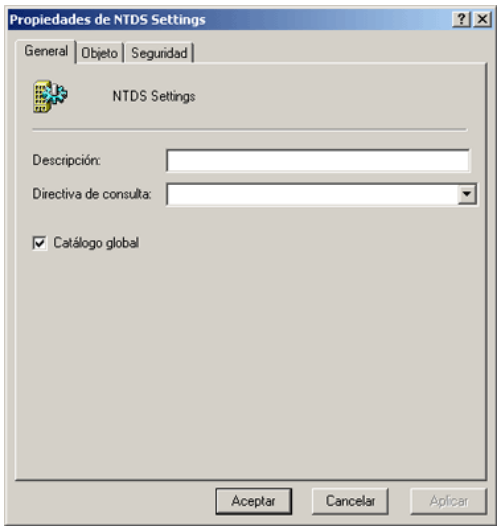
Si el servidor es el único controlador de dominio de un dominio particular, la degradación provoca que el dominio se elimine completamente de Active Directory, y que el sistema se convierta en un servidor independiente hasta que se una a otro dominio. Si el servidor es el único controlador del dominio 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:

- Abrir la herramienta Sistema del Panel de control y pulsar en la pestaña Identificación de red.
- Pulsar el botón Avanzada para abrir el cuadro de diálogo Cambios de identificación.

- 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, podriamos hacerlo también).
- 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 maquina. 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 maquina pueda volver a trabar en un dominio.

3.6 Establecimiento de un servidor de Catálogo Global

El primer controlador de dominio Windows 2000 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 replica 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:

- Escoger Sitios y servicios de Active Directory en el menú Herramientas administrativas.
- Abrir Sites y seleccionar el sitio correspondiente.
- Abrir Servers y seleccionar después el controlador de dominio que se desea convertir en servidor de Catalogo global.
- Seleccionar NTDS Settings en el panel derecho y escoger propiedades en el menú Acción.
- En la pestaña General, seleccionar la casilla de verificación Catalogo global.