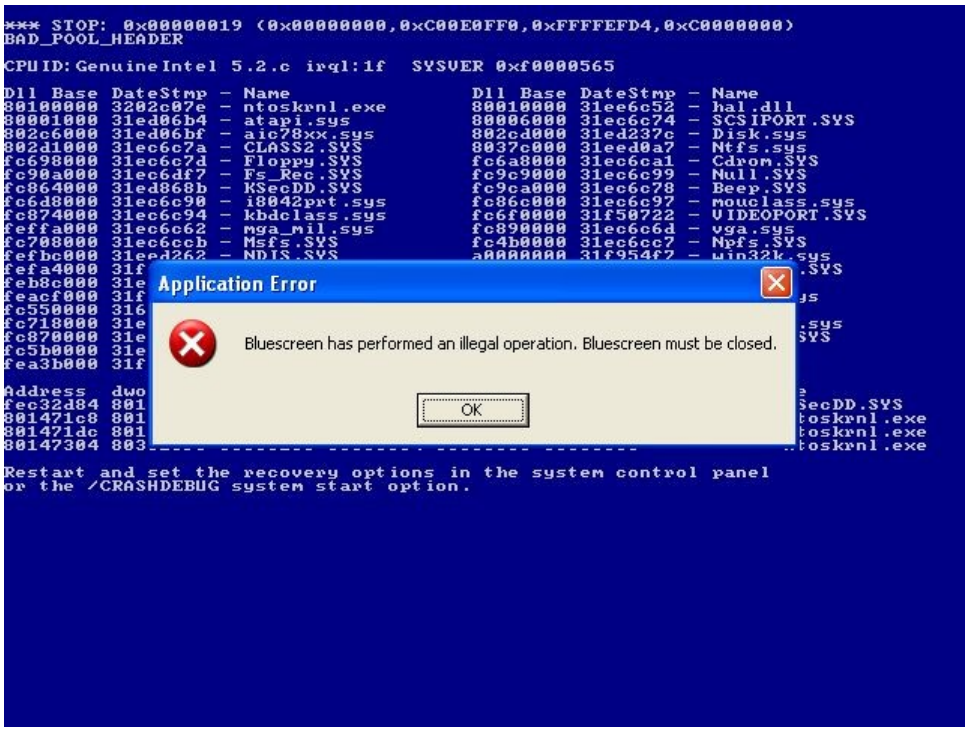
Servidores Windows

Última modificación 2009/04



“In a world without walls and fences,
who needs windows and gates?”

Basado en apuntes de Fernando Ferrer (http://fferrer.dsic.upv.es/), información de Microsoft y trabajo propio.

Servidores Windows

Índice de contenido

ADMINISTRACIÓN DE WINDOWS....3
TRABAJO COMO USUARIO NO PRIVILEGIADO.3
LA CONSOLA DE GESTIÓN: MMC....3
SERVICIOS DEL SISTEMA....3
Tipo de inicio de un servicio....3
Dependencias....3
Recuperación de un servicio....3
ARRANQUE DEL SISTEMA....4
Solución de errores en el arranque....4
La consola de recuperación....5
SISTEMA DE COPIA DE RESPALDO (NTBACKUP)....6
Ejemplos....6
SISTEMA DE FICHEROS NTFS....6
VOLÚMENES LÓGICOS....6
TRABAJO EN MODO GRUPO....7
SERVICIO DE TERMINAL (TS: Terminal Service)..7
MODELO DE PROTECCIÓN DE WINDOWS....8
EQUIPOS, USUARIOS Y GRUPOS (Security Principals)....8
PERMISOS Y DERECHOS....8
LISTAS DE CONTROL DE ACCESO....9
OTRAS DIRECTIVAS DE SEGURIDAD....10
COMPARTICIÓN DE RECURSOS....10
Comparticiones automáticas....10
DIRECTIVAS DE SEGURIDAD DE IP / IPSec....11
ISAKMP y Directivas de Seguridad....11
Asignación de Directivas de Seguridad....11
Reglas....12
SERVIDOR ENRUTAMIENTO Y ACCESO REMOTO 12
INTRODUCCIÓN AL DIRECTORIO ACTIVO (AD)...13
EL SERVICIO DNS EN AD....14
OBJETOS DEL DIRECTORIO ACTIVO....14
ORGANIZACIÓN DEL AD....15
ESTRUCTURA FÍSICA....15
ESTRUCTURA LÓGICA....15
NIVELES FUNCIONALES....15
RELACIONES DE CONFIANZA....16
Tipos de confianza....16
MAESTRO ÚNICO....16
HERRAMIENTAS DE ADMINISTRACIÓN DEL AD....17
Uso de ntdsutil....17
Asignar maestrías....17
Dar de baja un servidor que no está disponible o que ha fallado su “de-promoción”....17
Consultar maestrías de un servidor....18
OBJETOS DE POLÍTICAS DE GRUPO (GPOs)....19
MODIFICACIONES EN LA APLICACIÓN DE DIRECTIVAS....20
ADMINISTRACIÓN DE GPOS....20
CONFIGURACION DE DIRECTORIO ACTIVO (AD o ACTIVE DIRECTORY) EN WINDOWS 2003....21
CONFIGURACIÓN DE UN DC (Domain Controller) 21
HERRAMIENTAS DE SOPORTE....24
ASISTENTE PARA CONFIGURACIÓN DE SEGURIDAD....25
SISTEMA DE ARCHIVOS DISTRIBUIDO (DFS)....26
PERMISOS EN EL ESPACIO DE NOMBRE DFS. .28
INCLUIR OTROS SERVIDORES EN LA RAÍZ DFS 28
HERRAMIENTAS ACTUALIZADAS....29
EMPEZANDO DE NUEVO CON LAS HERRAMIENTAS ACTUALIZADAS....31
ANEXO I: COMANDOS DE ADMINISTRACIÓN....38
ANEXO II: ATAJOS DE TECLADO....39

ADMINISTRACIÓN DE WINDOWS

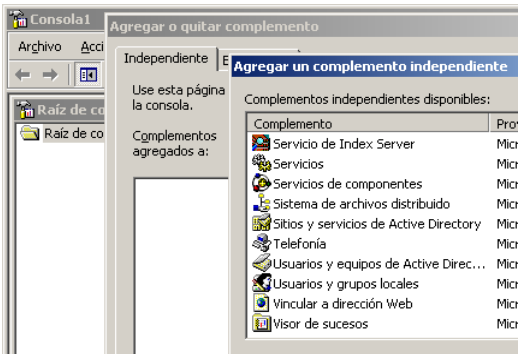
TRABAJO COMO USUARIO NO PRIVILEGIADO

Microsoft recomienda que no se trabaje con un usuario administrador a no ser que sea estrictamente necesario. Por ello la mayoría de los programas de gestión pueden lanzarse utilizando la opción "Ejecutar como" del menú secundario.
Desde línea de comandos se puede utilizar "`runas`". Por ejemplo:

```
> runas /noprofile /env /user:mi_dominio\guimi "mmc %windir%\system32\dsa.msc"
```

LA CONSOLA DE GESTIÓN: MMC

Windows dispone de una herramienta básica de gestión llamada MMC (*Microsoft Management Console*) o consola de gestión que permite gestionar gráficamente casi todos los aspectos del sistema mediante complementos.
Las herramientas administrativas son consolas MMC con un complemento determinado: visor de sucesos, usuarios y equipos de AD, servicios, desfragmentador, administrador de dispositivos...



SERVICIOS DEL SISTEMA

Un servicio es un programa que está ejecutándose indefinidamente para atender a peticiones de otros programas o del usuario. Por defecto W2003, ejecuta automáticamente varios servicios que no son necesarios y consumen más memoria de la necesaria.

Los servicios pueden consultarse y gestionarse utilizando una consola de gestión ("`mmc`") o la línea de comandos ("`sc`" o "`net [stop | start] servicio`").
Habitualmente se abre la consola de servicios desde:

Mi PC ->Administrar o desde Herramientas administrativas ->Servicios.

La información de los servicios en el registro reside en la clave "`HKLM\SYSTEM\CurrentControlSet\Services`".

Tipo de inicio de un servicio

El tipo de inicio puede marcarse como:

- **Automático**: El servicio arranca al iniciarse el sistema.
- **Manual**: El servicio se arranca manualmente.
- **Deshabilitado**: El servicio no puede arrancarse. (Evita que se arranque desde algún script, por ejemplo).

Dependencias

Se pueden indicar dependencias entre servicios, lo que obliga a que antes de parar / arrancar un servicio se paren o arranquen otros servicios.

Recuperación de un servicio

Las acciones posibles a tomar en caso de que ocurra algún error con el servicio son:

- **No realizar ninguna acción**: La opción por omisión.
- **Reiniciar el servicio**: Intentar reiniciar el servicio tras una pausa.
- **Ejecutar un archivo**: Lo que nos permite indicar un script que registre datos y haga comprobaciones antes de intentar reiniciar el servicio (con "`net start`" o "`sc`").
- **Reiniciar el equipo**: Si el servicio no arranca nunca el equipo se reiniciará continuamente hasta que lo arreglemos.

ARRANQUE DEL SISTEMA

Cuando un equipo arranca primero realiza una comprobación del sistema llamada POST, tras lo cual carga en memoria el sector maestro de arranque (MBR: *Master Boot Record*) del dispositivo indicado (en BIOS o por opción del usuario). En este MBR debe residir un pequeño programa cuya función es localizar el sector de arranque de la partición de arranque (PBR: *Partition Boot Record*), cargarlo en memoria y cederle el control.
Este segundo programa busca en la raíz de la partición de sistema el fichero `NtLdr` que comienza la carga del sistema operativo propiamente dicho. La secuencia de arranque se encarga ahora de obtener información sobre el equipamiento (*hardware*) del sistema, así como los controladores (*drivers*) asociados a los dispositivos.

El programa `NtLdr` (*NT Loader*) cambia el procesador del modo real al modo de 32 bits, ya que `NtLdr` es una aplicación de 32 bits. Una vez en modo 32 bits, la primera tarea que realiza el programa `NtLdr` consiste en cargar el minicontrolador del sistema de archivos. Este paso es necesario para la localización y la carga del sistema Windows.
A continuación lee el fichero "`Boot.ini`", mostrando los diferentes sistemas operativos con los que se puede arrancar. Una de las opciones ofrecidas es utilizar el sector de arranque anterior a la instalación de Windows, en cuyo caso NTLDR carga "`BootSec.dos`", cediéndole el control y finalizando por tanto el proceso de arranque de Windows 2003. En caso contrario el programa NTLDR ejecuta "`NtDetect.exe`", encargado de buscar el equipamiento del equipo, devolviendo una lista con el equipamiento encontrado a NTLDR para que sea incluido en el registro.
Por último NTLDR carga "`NtOSKrnl.exe`", "`Hal.dll`" y la clave "`System`" del Registro que permite a NTLDR cargar los controladores configurados para ser iniciados en el proceso de arranque. Tras ello, NTLDR cede el control al núcleo del sistema, NTOSKRNL, terminando el proceso de arranque para comenzar la carga del sistema operativo.

POST → MBR → PBR → NTLDR ← `Boot.ini`
a) `BootSec.dos`
b) `NtDetect.exe → NtOSKrnl.exe + Hal.dll + HKLM\System → NtOSKrnl.exe`

`Boot.ini` y `NtDetect.exe` también deben residir en la raíz del sistema (`C:\`).

Solución de errores en el arranque

Windows 2003 incorpora diversos medios para corregir los posibles errores en el proceso de arranque. Entre las soluciones a estos problemas vamos a destacar los siguientes:

1. Reparación de una instalación con los discos de instalación de Windows 2003. Estos ofrecen la posibilidad de realizar una instalación o reparar una existente, en cuyo caso nos ofrecerá recuperar los ficheros de sistema o la base de datos del usuario.
2. Creación de un disquete de arranque. Una vez formateado el disco, deben copiarse en el mismo los ficheros necesarios para el arranque como son `NtLdr`, `NtDetect` y `Boot.ini`; resulta necesario además `NtBootd` si tenemos dispositivos SCSI y `BootSec.dos` para utilizar el sector de arranque anterior a la instalación.
3. El menú de opciones avanzado. Se obtiene pulsando F8 en el arranque.
   - Modo Seguro. Carga solamente los ficheros y drivers necesarios para levantar y ejecutar el sistema operativo.
   - Modo Seguro con funciones de Red. Igual pero con red.
   - Modo Seguro con símbolo de sistema. Sin entorno gráfico (`explorer`).
   - Habilitar el registro de inicio. (Genera el registro de inicio `%SystemRoot%\NtBtLog.txt`)
   - Habilitar modo VGA. Arranca utilizando el driver básico de VGA (el usado en el modo seguro).
   - Ultima Configuración buena Conocida. El registro almacena bajo `HKLM\SYSTEM` conjuntos de configuraciones denominados `ControlSetxxx`.
   - [Solo para DCs] Modo de Restauración de SD (Servicio de Directorio).
   - Modo de Depuración.
   - Iniciar Windows Normalmente.
   - Reiniciar.
   - Regresar al menú de opciones del SO. Esta opción permite enviar información de depuración a otro ordenador a través de un cable serie.
4. La consola de recuperación.

La consola de recuperación

La Consola de recuperación es un intérprete de comandos que permite iniciar los equipos para acceder a todas las particiones de disco FAT16, FAT32 y NTFS del sistema, así como a un conjunto básico de mandatos y utilidades para la realización de tareas de recuperación.

Para instalar la consola hay que ejecutar el programa de instalación de W2003 (`winnt32.exe`) con el parámetro "`/cmdcons`". La consola, que normalmente ocupa unos 6 MB, se instala en una carpeta oculta denominada "`cmdcons`" (`C:\cmdcons`). Una vez instalada la consola el menú del cargador de sistemas operativos de W2003 incluirá la opción «Microsoft Windows 2003 Recovery Console» (Consola de recuperación de Microsoft Windows 2003).

Una limitación bastante importante es la de que no se puede instalar en un volumen espejo (RAID1) por *software*. Este problema se puede sortear eliminando el espejo, instalando la Consola de recuperación y volviendo a restablecer el espejo.

Cuando se selecciona la consola de recuperación, durante un breve espacio de tiempo se puede pulsar F6 para cargar un controlador RAID o SCSI. A continuación, el sistema pasa a modo texto y solicita al administrador que especifique la instalación de W2003 en la que desea iniciar una sesión. Esta característica permite utilizar la Consola de recuperación para recuperar las distintas instalaciones de sistema operativo de un sistema multi-inicio.
Una vez que se haya seleccionado la instalación a la que se desee acceder, el sistema pedirá al usuario que suministre la contraseña de administrador local para dicha instalación.

En caso de no haber instalado la consola, ésta se puede iniciar arrancando con el disco de instalación de Windows y usando la opción de "reparación" del programa de instalación.

Una lista con las causas más frecuentes de los fallos de inicio de W2003 y NT debidos a problemas con el software, se detalla a continuación:

- Se ha dañado o eliminado un archivo esencial del sistema (por ejemplo, los archivos de secciones del Registro o los archivos `NtOsKrnl.exe`, `NtDetect.com`, `HAL.dll` o `Boot.ini`).
- Se ha instalado un servicio o controlador incompatible o defectuoso, o se ha dañado o eliminado un servicio o controlador esencial.
- Se han producido daños en el disco o en el sistema de archivos, incluidos los daños en las estructuras de directorios, el MBR y el sector de inicio de W2003 o NT.
- El Registro contiene datos no válidos (es decir, el Registro se encuentra físicamente intacto pero contiene datos erróneos desde el punto de vista lógico, como un valor fuera de rango para un servicio o controlador).
- Son incorrectos o excesivamente restrictivos los permisos de la carpeta `%systemroot%` (`C:\winnt`).

Algunos de los comandos más útiles de la consola son:

- **`ChkDsk:`** comprueba el estado de un disco o partición.
- **`FixMBR`**: sustituye el MBR del disco principal del sistema por una copia en buen estado.
- **`Fixboot`**: sustituye el PBR de la partición principal del sistema por una copia en buen estado.
- **`DiskPart`**: permite la creación y eliminación de particiones.
- **`ListSvc`**, **`Enable`** y **`Disable`**: permiten generar una lista de los servicios y controladores del sistema, activarlos y desactivarlos, respectivamente.
- **`RegEdit`**: Permite modificar el registro del sistema.

SISTEMA DE COPIA DE RESPALDO (NTBACKUP)

Windows dispone de una herramienta gráfica de copias de seguridad llamada "NtBackup" que permite hacer copias de ficheros, carpetas y "datos del estado del sistema" en unidades locales o de red y en cinta. Se puede utilizar en modo comando para hacer copias, pero no para restaurar datos.
En el caso de los servidores de directorio activo (DCs) permite hacer copias del directorio (SD: Servicio de Directorio).
Los trabajos de copia pueden programarse para que se realicen diariamente, semanalmente, mensualmente, en el inicio del sistema, en el inicio de sesión o cada vez que el sistema esté inactivo.
Permite hacer copias en modo: normal (completa), copia (completa sin marcar copiado), diferencial (no marca copiado), incremental (marca copiado) o diaria (cambios del día sin marcar copiado).

Ejemplos

```
ntbackup backup d:\ /f "h:\copia.bkf"
ntbackup backup d:\ /t "Cinta_1" [/n "Nuevo_nombre_cinta"]
ntbackup backup d:\ /p "Grupo_de_cintas_1" [/n "Nuevo_nombre_cinta"]
```

Copia el contenido de "`d:\`" en el fichero, la cinta o el grupo de cintas especificado.

```
/j "Titulo_copia" /d "Descripcion_copia" /v:yes /r:no /l:s /hc:on
```

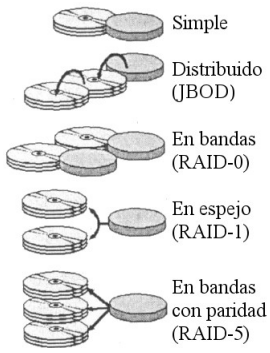
Con estas opciones indicamos indicamos: un título (`/j`), una descripción (`/d`), que se verifique la copia (`/v:yes`), que no se restrinja el acceso a la cinta al propietario (`/r:no`), que haga un registro resumen (`/l:s`) y que utilice compresión por *hardware* (`/hc:on`).

SISTEMA DE FICHEROS NTFS

El sistema de ficheros NTFS v5 utilizado desde Windows 2000 soporta compresión[1], cifrado, cuotas por volúmenes, hilos (*threads*)[2], montaje de particiones[3] y enlaces simbólicos (*junction*) a directorios[4].
Para gestionar las cuotas se puede indicar si el sistema debe denegar nuevo espacio de disco una vez superada la cuota, se puede establecer un nivel de advertencia y un nivel de cuota general, se puede definir niveles personalizados (incluso "sin límite") y se puede registrar sucesos de cuotas -registrar cuando un usuario sobrepasa un nivel de advertencia y/o de límite de cuota-.

VOLÚMENES LÓGICOS

Los volúmenes aparecen en Windows 2000 gracias a la nueva gestión de los discos. Solo están disponibles en discos configurados como "dinámicos", y dan posibilidad de disponer de tolerancia a fallos.
Los volúmenes de Windows 2003 pueden ser de varios tipos:



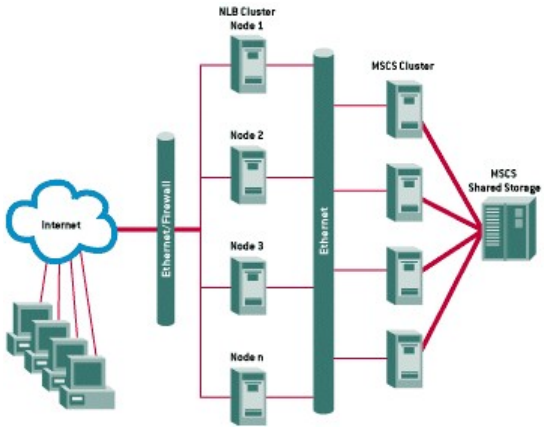
- **Simple**: Único tipo posible si solo disponemos de un disco en modo dinámico. Los volúmenes simples son como las particiones, pero se pueden ampliar sin necesidad de reiniciar el sistema (excepto la partición de arranque).
- **Distribuido**: Un volumen distribuido es igual que uno simple pero utiliza porciones concatenadas de distintos discos[5].
- **En bandas (RAID-0)**: Utiliza porciones de tamaño fijo (64 KB) en varios discos -hasta 32-.
- **En espejo (RAID-1)**.
- **En bandas con paridad (RAID-5)**.

1 Con un tamaño máximo de "cluster" de 4 KiB.
2 Un archivo puede tener varios hilos con diferente contenido (http://guimi.net/index.php?pag_id=tec-docs/recetas/win_hilos_ntfs.html).
3 Asignar una partición a una carpeta en vez de a una letra "X:". Permite sobrepasar el límite de 26 particiones.
4 Hay que instalar "`linkd.exe`" -Windows Resource Kit- o "`junction.exe`" (http://technet.microsoft.com/en-us/sysinternals/bb896768.aspx). Vista dispone del comando "`mklink`".

TRABAJO EN MODO GRUPO

El balanceo de carga (NLB: *Network Load Balancing*) permite repartir un servicio de red (cortafuegos, web, correo-e) entre varios nodos que trabajan por separado y no comparten componentes físicos. Si se necesita replicar los datos debe hacerse independientemente.
En un "*cluster*" (MSCS: *MS Cluster Server*) los nodos trabajan juntos, conectados (por ejemplo compartiendo discos duros) y coordinados comportándose de cara al resto de equipos como uno solo.

Aunque Windows no soporta que un servidor configure ambos servicios a la vez (NLB y MSCS), éstos pueden combinarse mediante capas de servidores. Por ejemplo un servicio web podría estar atendido por varios nodos balanceados que accediesen a un grupo ("*cluster*") con una base de datos donde residiría dicha web.



- Balanceo de carga (NLB: *Network Load Balancing*).
  - Distribuye la carga de un servicio entre los nodos del grupo, mejorando la escalabilidad y disponibilidad.

- Servicios de grupo (MSCS: *MS Cluster Server*).
  - Un servicio de grupo permite que la caída de un servidor del grupo no interrumpa dicho servicio.
  - Un recurso de *quorum* reside en un disco compartido por los nodos, y guarda la configuración del grupo.
  - Un grupo de recursos puede pertenecer a varios nodos y en un momento dado estar funcionando solo en uno de ellos.
  - Un servidor virtual es un grupo de recursos que se ofrecen con su propia IP y su propio nombre NetBIOS.

SERVICIO DE TERMINAL (*TS: Terminal Service*)

Los servicios de terminal aportan a los servidores Windows capacidades gráficas multiusuario, permitiendo ejecutar sesiones diferenciadas concurrentes basándose en el protocolo de escritorio remoto (RDP[6]: *Remote Desktop Protocol*).

Podemos distinguir dos tipos de instalación:

- **Servidor de Aplicaciones**: permite a múltiples clientes remotos acceder simultáneamente a las aplicaciones Windows que se ejecutan en el servidor. Este es el modo de empleo tradicional del Servicio de Terminal y requiere de licencias bien por dispositivo o bien por usuario.
  Las aplicaciones deben instalarse de forma específica y no todas lo permiten.
- **Administración Remota**: proporciona acceso remoto a los servidores por parte de los administradores. Soporta, además de la sesión de consola, dos sesiones más, sin tener que pagar ninguna licencia extra. Dos administradores remotos pueden compartir una sesión con propósitos de colaboración.

5 Es lo que se conoce como JBOD ("*Just a Bunch Of Drives*") cuando se implementa por *hardware*.
6 Puerto TCP 3389

MODELO DE PROTECCIÓN DE WINDOWS

EQUIPOS, USUARIOS Y GRUPOS (*Security Principals*)

Los equipos, usuarios y grupos de un dominio disponen de un SID (*Secure IDentifier*), un dato interno del sistema compuesto por la unión del ID del dominio y un RID que actúa de identificador estadísticamente único[7].
Estos elementos se conocen como "*security principals*" ya que los permisos y derechos se asignan a los SID.

Las cuentas de equipo se corresponden con equipos físicos o virtuales del dominio. Las cuentas de usuarios globales[8] se corresponde con accesos al sistema. Cada cuenta suele identificar a una persona pero una misma persona puede usar distintos usuarios según la función que vaya a realizar y existen usuarios utilizados únicamente por el sistema.
Los grupos son agrupaciones lógicas de usuarios que permiten establecer de forma cómoda permisos y restricciones. El sistema crea inicialmente una serie de grupos llamados "*built-in groups*", entre ellos: Administradores, Operadores de copia, Usuarios Avanzados, Usuarios, Invitados...
Además el sistema reconoce grupos dinámicos de usuarios conocidos como identidades especiales (*special identities*) que se basan en el estado de los usuarios: Usuarios interactivos, Usuarios de Red, Usuarios autenticados, Todos...

Cada usuario puede incluirse en múltiples grupos de seguridad[9], ya sean grupos creados por los administradores o del sistema (*built-in groups*: grupos de seguridad locales) y además el sistema lo considerará en una o varias identidades según su contexto.

Los grupos pertenecen a distintos ámbitos que se diferencian por las cuentas y grupos que pueden incluir y los dominios donde se les pueden aplicar permisos. Existen tres ámbitos de grupo:

	Pueden incluir	**De aplicación en**
Grupos Locales de Dominio	Cuentas, grupos globales y grupos universales(*) de cualquier dominio, así como grupos locales(*) del mismo dominio.	El mismo dominio.
Grupos Globales	Grupos globales(*) y cuentas del mismo dominio del grupo.	Cualquier dominio del bosque.
Grupos Universales (*)	Cuentas, grupos globales y grupos universales de cualquier dominio del bosque.	Cualquier dominio del bosque.

(*) Solo en dominios de nivel funcional W2000 nativo o W2003.

Habitualmente se crean cuentas de usuario, que se incluyen en grupos globales, que después forman parte de los grupos locales del dominio. Sobre estos grupos locales se aplican los permisos (no sobre usuarios).

PERMISOS Y DERECHOS

Cada recurso del sistema presenta una serie de *permisos* denegados o concedidos a algunos usuarios o grupos del sistema. Por otra parte el sistema puede garantizar *derechos* de realizar acciones a determinados usuarios o grupos, que tienen prevalencia sobre los permisos.
Entre los derechos podemos distinguir entre *derechos de conexión* y *privilegios*.

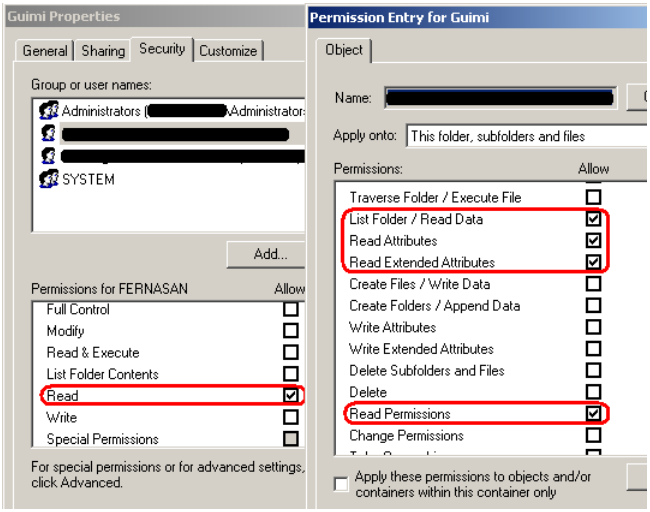
Ejemplos: el Administrador puede arrogarse la propiedad de un recurso sobre el cual no tiene permisos; un usuario puede tener permisos sobre un recurso pero no tener derecho de "Acceso al equipo desde la red" o "Inicio de sesión local"; un "Operador de copia" puede copiar y restaurar ficheros sobre los que no tiene permisos...

7 Los SID de equipos, usuarios y grupos están compuestos de un identificador de dominio y un RID. Algunos RID están predeterminados, como el del Administrador (500) o algunos grupos: Administradores del dominio (512), Usuarios del dominio (513), Invitados del dominio (514)...
8 Usuario "global" del dominio, por contraposición a usuario local en un único equipo.
9 Además de los grupos de seguridad existen los grupos de distribución (locales, globales o universales) que son objetos de grupo habilitados únicamente para correo utilizando Exchange. En este documento solo hablaremos de grupos de seguridad.

Para llevar a cabo el modelo de protección, a cada usuario se le adjudica en el momento de la conexión un SAT (*Security Acces Token*) que contiene el SID del usuario, los SID's de sus grupos y la lista de derechos del usuario. El SAT asegura que los atributos de protección del usuario están presentes en cada proceso del usuario.

Para facilitar la administración existen agrupaciones de permisos, conocidas como permisos "estándar". Así por ejemplo el permiso estándar "Leer" incluye los permisos de lectura del contenido y de lectura de los permisos y atributos.
Una entrada de la lista de permisos puede marcarse para que no se herede.

Los permisos estándar de las carpetas son: "Control total", "Modificar", "Leer y Ejecutar", "Listar contenidos" (solo para carpetas), "Leer" y "Escribir".



LISTAS DE CONTROL DE ACCESO

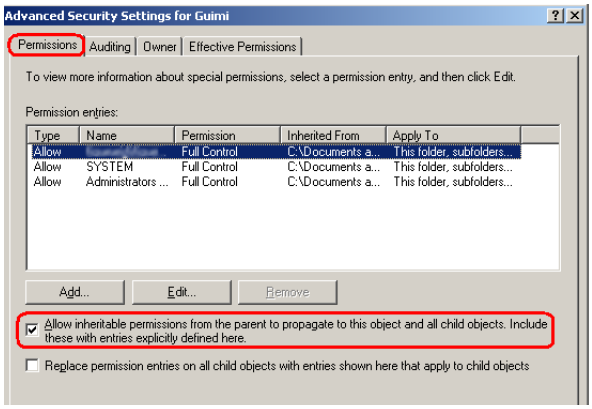
Un descriptor de seguridad de un recurso contiene el SID del propietario[10] y varias listas de control de acceso. Una ACL (ACL: *Access Control List*) es una lista de entradas de control (ACEs: *Access Control Entries*), cada una de las cuales identifica un fiado y unos permisos permitidos o denegados (ver imagen superior).
Las ACLs pueden ser de dos tipos: DACL (*Discretionary ACL*) o SACL (*System ACL*). Las DACL especifican permisos de acceso -permitidos o denegados- que el propietario del recurso especifica discrecionalmente[11]. Las SACL especifican las acciones del fiado que el sistema debe auditar (intentos fallidos o exitosos de acceso según su tipo).

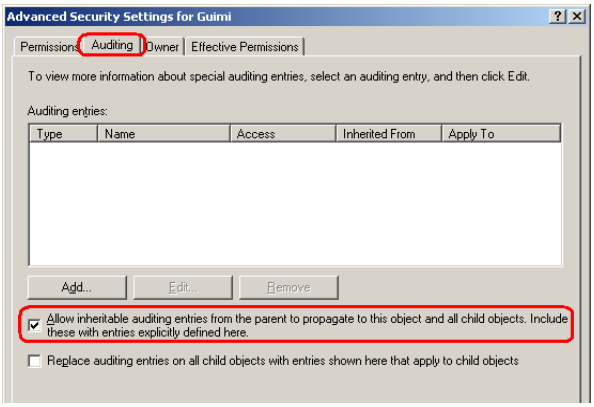
Cada recurso, además de poder incluir sus propias ACLs (ACLs explícitas), puede marcarse para que herede las ACLs de sus recursos antecesores (se indica separadamente para DACL y SACL).

Para determinar si debe concederse un permiso a un fiado el sistema primero ordena las ACEs de las distintas listas. Después las evalúa una a una y cuando encuentra una que se corresponde ya no evalúa el resto.
Si un recurso no tiene DACLs se concede el permiso. Si tiene DACL pero no tiene ACEs se deniega el permiso.

Para ordenar las ACEs el algoritmo tiene en cuenta lo siguiente:

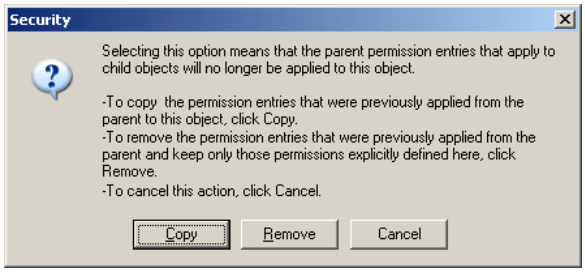
- Dentro de una lista, las ACEs que deniegan tienen prioridad sobre las que permiten.
- Las ACLs explícitas tienen prioridad sobre las heredadas.
- Las ACLs de los padres tienen prioridad sobre las de los abuelos.





10 El propietario de un recurso es en principio su creador, aunque existe el privilegio de tomar o asignar la posesión de un recurso. Los privilegiados son básicamente los administradores y los restauradores de copias.
11 También pueden cambiar las DACLs quienes tengan el permiso "Cambiar permisos", como los Administradores.

Al anular la herencia el sistema nos permite elegir entre quitar todos los permisos heredados o copiarlos como explícitos.
Cuando se crea un nuevo recurso éste hereda todos los permisos (todas las ACLs) de su padre (tanto heredados como explícitos).
Al copiar un recurso (o moverlo a otro volumen) creamos un nuevo recurso.
Al mover un recurso dentro de un volumen se mantienen los permisos.



El comando "`cacls`" permite modificar los permisos estándar de las ACLs. Sus principales modificadores son "`/T`" (aplicar a subdirectorios), "`/E`" modificar en vez de reemplazar y "`/[G|R|P] usuario:[R|W|C|F]`" que respectivamente concede, quita o modifica permisos de lectura, escritura, cambio o control total.

OTRAS DIRECTIVAS DE SEGURIDAD

Además de los permisos y los derechos (derechos de conexión y privilegios), existen las llamadas "Directivas de seguridad local" que se administran desde una consola de gestión única que permite establecer, entre otras cosas:

- **Política de cuentas**: Establece políticas sobre contraseñas, bloqueos y Kerberos.
- **Directivas locales**: Define los derechos y la auditoría del sistema.
- **Claves públicas**: Opciones sobre las claves públicas del equipo.

COMPARTICIÓN DE RECURSOS

Los equipos de un dominio pueden compartir carpetas con un nombre que no tiene porqué coincidir con el nombre original. Si el nombre del recurso compartido termina por '$' se comparte de manera oculta, es decir, es accesible pero no se muestra en una búsqueda.
Al compartir una carpeta se establecen unos permisos básicos de acceso desde la red (Lectura, Escritura, Control Total) que establecen un filtro antes de los permisos propios del recurso. Si la carpeta reside en un sistema NTFS, con gestión de ACLs, puede indicarse de forma segura en la compartición Lectura y Escritura, ya que serán las ACLs quienes filtren los permisos.
Hay que notar que si un usuario no tiene concedido el derecho de conexión "Acceder a este equipo desde la red" no podrá acceder al recurso independientemente de los permisos que tenga sobre él.
Un recurso compartido puede además publicarse en el directorio, para ello desde "Usuarios y equipos de AD" crearemos un nuevo "Recurso compartido" dentro de una OU.

Para compartir una carpeta puede usarse el explorador (botón secundario -> Compartir...) o el comando "`net share`".
Para conectar una unidad del sistema a un recurso compartido ("unidad de red") puede utilizarse el explorador ("Herramientas" -> "Conectar a unidad de red") o el comando "`net use`".
Para acceder a una carpeta compartida sin conectarla puede llamarse a `\\equipo\recurso` tanto desde "Ejecutar", como desde el explorador.

Comparticiones automáticas

Los equipos con Windows comparten los siguientes recursos:

- **letra_de_unidad$**: ('c$', 'd$'...)
- **ADMIN$**: directorio del sistema (normalmente C:\WINDOWS o C:\WINNT)
- **IPC$**: agrupa las tuberías de comunicación entre procesos

Además los DCs comparten los siguientes recursos:

- **NETLOGON**: Necesario para la validación de usuarios
- **SYSVOL**: Información del Directorio Activo

DIRECTIVAS DE SEGURIDAD DE IP / IPSec

Las directivas de IPSec se pueden configurar de acuerdo con los requisitos de seguridad de un usuario, grupo, aplicación, dominio, sitio o empresa global. Windows 2003 permite crear y administrar directivas de IPSec localmente o a través de la consola "Directiva de grupo". Windows proporciona directivas predefinidas (predeterminadas) para configuraciones de seguridad de grupo y locales. Se pueden modificar para cumplir requisitos específicos. Una vez definida una directiva, tiene que asignarse para que se aplique. No hay directivas asignadas de forma predeterminada.

ISAKMP y Directivas de Seguridad

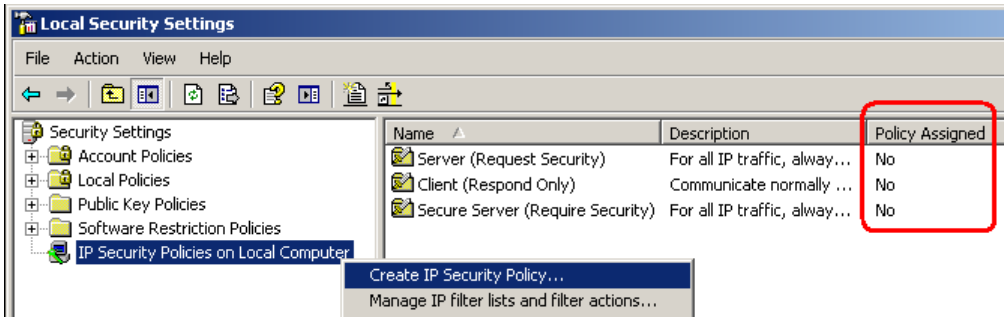
Durante la configuración de IPSec, se crea una directiva en la interfaz. Sin embargo, IPSec crea las dos siguientes directivas de negociación de seguridad en segundo plano:

- **Directiva de negociación**: La primera negociación incluye autenticación de identidad de usuario para los dos equipos que se van a comunicar y el intercambio de las claves de la sesión para proteger los datos. ISAKMP administra esta primera negociación.
- **Directiva de seguridad**: La segunda negociación sigue al intercambio de las claves. Los dos equipos tienen que acordar la configuración de seguridad que van a utilizar para proteger su comunicación sobre IP, mediante unas reglas.

Asignación de Directivas de Seguridad

Las directivas de IPSec locales se crean y configuran mediante Directiva de seguridad local. Se pueden definir varias directivas, pero sólo una se asigna a un equipo al mismo tiempo.
Una directiva de grupo presenta tres entradas de directiva predefinidas:

- **Cliente (sólo responder)**: permite comunicaciones sin IPSec, pero responderá a solicitudes de IPSec e intentará negociar la seguridad si se efectúa una solicitud de seguridad.
- **Servidor (seguridad de petición)**: permite recibir tráfico IPSec y tráfico no IPSec desde los clientes. Cada vez que se inicia una conexión intenta negociar seguridad mediante IPSec. Además para todas las peticiones que realiza solicita utilizar IPSec, pero permite realizar comunicaciones no IPSec si el otro equipo no lo admite. En resumen, esta directiva permite la comunicación sin IPSec pero siempre intenta utilizar IPSec.
- **Servidor seguro (requiere seguridad)**: requiere utilizar IPSec para todo el tráfico entrante y saliente. Por tanto siempre requiere que los equipos de destino sean de confianza y utilicen IPSec.



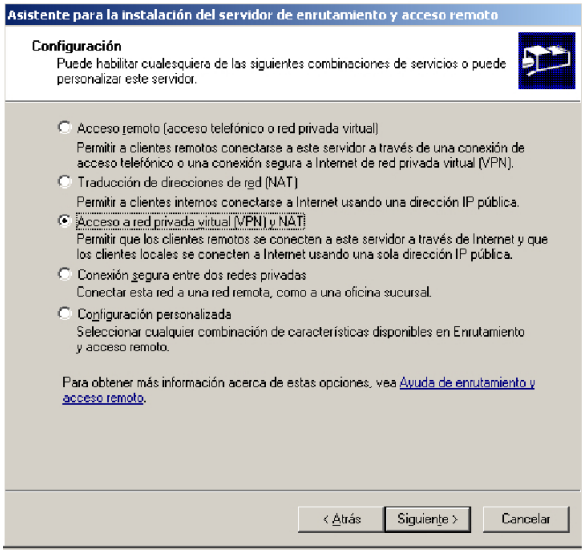
Cada directiva de IPSec puede contener una o varias reglas; una o todas ellas pueden estar activas de forma simultánea. Se proporcionan reglas predeterminadas que se adaptan a una amplia gama de comunicaciones entre cliente y servidor.

Reglas

Una regla se compone de 6 elementos:

1. **Lista de filtros IP**. Define qué tráfico se va a proteger con esta regla. Puede utilizar los filtros predeterminados o crear filtros específicos de directiva para ciertos tipos de tráfico IP o para subredes específicas.
2. **Acciones de filtrado**. Enumera las acciones de seguridad que se tomarán cuando el tráfico cumpla los criterios de un filtro. La acción especifica si el tráfico se bloquea, se permite o si se negocia la seguridad de la conexión. Se pueden especificar una o varias acciones de filtrado en una lista ordenada por preferencia. Si dicha acción de filtrado no se puede negociar, se intenta la acción de filtrado siguiente.
3. **Métodos de seguridad**. Especifica cómo los equipos que se comunican tienen que proteger el intercambio de datos. Puede utilizar los métodos predefinidos Medio y Alto, o definir métodos de seguridad personalizados.
4. **Configuración de túneles**. En algunas situaciones, como entre encaminadores que sólo están conectados por Internet, es interesante utilizar el modo de túnel en IPSec. Para definir un túnel IPSec tiene que haber dos reglas, una para cada sentido.
5. **Métodos de autenticación**. Los métodos de autenticación definen cómo cada usuario se va a asegurar de que el otro equipo o el otro usuario son realmente quienes dicen ser. Cada regla puede estar configurada con uno o varios Métodos de autenticación en una lista ordenada por preferencia. Si el primer método no se puede usar, se intenta el siguiente. Windows 2003 acepta tres Métodos de autenticación:
   - **Kerberos**. El protocolo de seguridad Kerberos V5 es la tecnología de autenticación predeterminada. Este método se puede usar en cualquier cliente que ejecute el protocolo Kerberos V5 (sean o no clientes de Windows) que sean miembros de un dominio de confianza.
   - **Certificados**. Este método requiere que se haya configurado al menos una entidad emisora de certificados (CA: *Certificate Authority*). Windows 2003 acepta certificados X.509 versión 3, incluidos los generados por entidades emisoras de certificados comerciales.
   - **Clave previamente compartida (PSK)**. Es una clave secreta, compartida, que dos usuarios acuerdan de antemano y que configuran manualmente antes de usarla.
6. **Tipos de conexión**. Permite que el administrador de la red elija si la regla se aplica a todas las conexiones de la red, a la red de área local o a las conexiones de acceso remoto.

SERVIDOR ENRUTAMIENTO Y ACCESO REMOTO



El “Asistente para la instalación de un servidor de enrutamiento y acceso remoto” permite:

- instalar un acceso remoto telefónico (Servidor RAS)
- hacer las veces de traductor NAT
- instalar un servidor VPN de acceso remoto
- configurar un túnel VPN entre redes
- realizar una configuración personalizada.

INTRODUCCIÓN AL DIRECTORIO ACTIVO (AD)

El Directorio Activo o AD (*Active Directory*) es una estructura jerárquica que almacena información sobre objetos en red. Para implementarlo Microsoft ha creado su propia versión del protocolo LDAP (*Lightweight Directory Access Protocol*), proveniente de otros entornos, mezclado con Kerberos, DNS y el servicio de dominio propio de Windows. Así Microsoft abandona otros protocolos propios como WINS o NTLM (aunque pueden seguir usándose) para implementar protocolos estándares como DHCP, SNTP, X.509 y los ya nombrados DNS y LDAP (versiones 2 y 3). Los protocolos imprescindibles para el funcionamiento de AD son DNS, LDAP y KRB (Kerberos).

En AD desaparecen los antiguos PDCs (*Primary Domain Controller*) y BDCs (*Backup Domain Controller*), pasando todos los servidores de dominio a ser simplemente DCs (*Domain Controllers*). Ahora los dominios son multimaestros, con toda la información y los servicios replicados. Todos los DCs permiten realizar cambios del AD y todo se replica automáticamente entre DCs. El catálogo global es una excepción ya que solo se replica entre los servidores que se indique[12] en un proceso llamado KCC (*Knowledge Consistency Checker* - Comprobador de coherencia de conocimiento).

Elementos principales:

- **Directorio Activo (AD)**: Servicio de directorio de Windows 2003. Es una implementación del protocolo LDAP utilizando además DNS y Kerberos.
- **Controlador de Dominio (DC)**: Servidor encargado de implementar el AD.
- **Controlador de Dominio Primario (PDC)**: si bien ya no existen PDCs y BDCs, un DC por cada dominio simula ser un PDC para mantener la compatibilidad con sistemas antiguos.
- **Catálogo global**: Subconjunto de atributos de todos los objetos del AD utilizado para acelerar el acceso a los mismos. Permite que un usuario inicie sesión en la red y que busque información en el directorio.
- **Esquema del Directorio**: Definición de tipos de datos, clases y atributos.

El principal protocolo de comunicaciones seguras en Windows 2003 es Kerberos v5, que se utiliza siempre que se intercambia información relativa a aspectos de seguridad y, en concreto, para autenticar usuarios en el AD. Presenta numerosas ventajas sobre NTLM, utilizado anteriormente, pero sólo es viable en la práctica si todas las máquinas del dominio son Windows 2000 o superior. Además Windows 2003 todavía utiliza NTLM en los siguientes casos:

- Si el cliente se autentica usando una dirección IP.
- Si el cliente se autentica en un servidor de otro bosque del directorio activo o no pertenece a ningún dominio o no existe ningún dominio.
- Si un cortafuegos corta los puertos necesarios para usar Kerberos.

Los cortafuegos de los servidores pueden bloquear el dominio; basta que bloqueen el DNS para que no funcione.
Los principales puertos que deben estar abiertos, tanto para TCP como para UDP, son:

- LDAP 389
- DNS 53
- Kerberos 88 (otros puertos interesantes de KRB -utiliza muchos- son 749-750)
- LDAPS 636 (*)
- RPC 135
- Directory Services 445
- Global Catalog 3268, 3269 (*)

(*) Solo utilizan TCP.

12 Para indicar que un servidor debe replicar el catálogo global hay que ir a la herramienta “Sitios y servicios de AD”, desplegar el sitio y seleccionar el servidor. Con el botón secundario lanzamos “Propiedades de NTDS” y seleccionamos “Catálogo global”.

EL SERVICIO DNS EN AD

El directorio activo y DNS son espacios de nombres: áreas delimitadas donde un nombre puede ser resuelto. Cada dominio se identifica unívocamente mediante un nombre DNS, que será el sufijo DNS de los clientes.
AD se encarga de mantener una asimilación entre zonas de DNS y árboles y dominios de LDAP y entre nodos de DNS y equipos de LDAP. Para ello el servidor de DNS ha de ser dinámico.

AD utiliza DNS para:
- resolución de direcciones IPs de los equipos
- definir el espacio de nombres (AD utiliza las convenciones de DNS para asignar nombres a los dominios)
- buscar los componentes físicos de AD. Cuando un cliente inicia sesión, es el servidor DNS quién indica qué equipos almacenan las funciones de controlador de dominio o servidor del catálogo global, identificados con registros DNS tipo SRV.

OBJETOS DEL DIRECTORIO ACTIVO

El AD almacena información sobre recursos y servicios de red. Los recursos como cuentas de usuario, impresoras, recursos compartidos, directivas, etc. constituyen objetos. Cada objeto posee una serie de atributos y tiene un nombre jerárquico que lo representa, por ejemplo: **`CN=guimi, OU=Administradores, DC=guimi, DC=net`**[13].

Los objetos se organizan en clases que son agrupaciones lógicas de objetos del mismo tipo, como usuarios o equipos, y que comparten los mismos atributos.

La definición de las clases y sus atributos se guarda en el esquema del directorio, que es único para todo el bosque.

13 CN=*Common Name*; OU=*Organization Unit*; DC=*Domain Component*.

ORGANIZACIÓN DEL AD

El servicio de directorio es una estructura jerárquica (o de árbol invertido) que almacena información sobre objetos en la red. Se organiza entorno a una estructura lógica y en torno a una estructura física (topología de red).

ESTRUCTURA FÍSICA

La estructura física se utiliza para configurar y administrar el tráfico de red. Define dónde y cuando se produce el tráfico de replicación y de inicio de sesión. Se compone de "Sitios" y "Controladores de dominio" (DCs):

- **Sitio**: Una o varias subredes IP conectadas por vínculos de alta velocidad. Cada subred pertenece a un sitio.
  - Asimilable a una sede física
- **Controlador de dominio (DC)**: Equipo que permite administrar el directorio y contiene una réplica del mismo dividido en las siguientes "unidades de replicación" o "particiones del directorio":
  - **Esquema**: contiene los tipo de objetos y atributos permitidos en el directorio. Se replica en todo el bosque.
  - **Configuración**: contiene la estructura de los dominios y la topología de replicación. Se replica en todo el bosque.
  - **Dominio**: contiene los objetos de un dominio. Se replica en un dominio.
  - **Aplicaciones**: (opcional) contiene datos de aplicaciones. Se indica manualmente sus réplicas.

ESTRUCTURA LÓGICA

La estructura lógica permite administrar los recursos con independencia de su ubicación física y se organiza jerárquicamente en base a bosques, árboles y dominios por medio de contenedores y unidades organizativas (OUs) sobre los que se aplican directivas y políticas:

- **Unidad Organizativa (OU)**: Organizadores jerárquicos de elementos.
  - Permiten aplicar políticas sobre OUs.
  - Permiten delegar la administración[14].
  - No confundir las OUs con los contenedores (*builtin*, *users*, *computers*...) que son organizadores NO jerárquicos que no permiten aplicar directivas ni delegar la administración.
- **Dominio**: Conjunto de elementos con un directorio común.
  - La información del directorio se replica entre todos los DCs del dominio.
  - **Es un límite de seguridad, sus políticas no se extienden ni hacia arriba ni hacia abajo (subdominios).**
  - Permite aplicar directivas de grupo (o políticas).
  - Permite delegar parcialmente la administración mediante OUs.
- **Árbol**: Conjunto de dominios que comparte un espacio de nombres común.
  - **En un árbol los dominios se enlazan por relaciones de confianza bidireccionales y transitivas.**
- **Bosque**: Conjunto de árboles que NO comparten un espacio de nombres.
  - Los árboles de un bosque se basan en diferentes nombres de dominio raíz de DNS.
  - **Los dominios de un mismo bosque comparten esquema, configuración y catálogo global.**
  - El dominio raíz de un bosque es el primer dominio creado en el bosque.

NIVELES FUNCIONALES

Hay 4 niveles funcionales de dominios:
- W2000 mixto (NT4, W2000, W2003) ***(Predef.)**
- W2000 nativo (W2000, W2003)
- W2003 provisional (NT4, W2003) para migraciones
- W2003 (W2003)

Hay 3 niveles funcionales de bosque:
- W2000 (NT4, W2000, W2003) ***(Predef.)**
- W2003 provisional (NT4, W2003)
- W2003 (W2003)

No se puede elevar el nivel del bosque si no se ha elevado primero el nivel de los dominios.

14 En "Usuarios y equipos de AD" botón secundario sobre la OU -> "Delegar administración...". Permite que usuarios no administradores den de alta o de baja objetos en la OU, por ejemplo.

RELACIONES DE CONFIANZA

Cada relación de confianza se establece **siempre entre dos dominios** y permite que los usuarios del dominio en que se confía puedan acceder al dominio que confía en ellos. Si el dominio A confía en el dominio B, los usuarios del dominio B pueden acceder a recursos del dominio A.
Son totalmente independientes de las políticas de seguridad.

La relación puede ser:

- ✔ explícita o implícita - (creada por el sistema o manualmente)
- ✔ unidireccional o bidireccional - (si A confía en B, ¿debe confiar B en A?)
- ✔ transitiva o no transitiva - (si A confía en B, y B confía en C, ¿debe confiar A en C?)

Tipos de confianza

- **Raíz de árbol**: implícita, bidireccional, transitiva
  Se crea al añadir un árbol al bosque, entre las dos raíces de árbol (que comparten la raíz del bosque)
- **Principal-Secundario**: implícita, bidireccional, transitiva
  Se crea al crear un dominio hijo (también llamado subdominio o dominio secundario)
- **Acceso directo**: explícita, unidireccional, transitiva
  Es un acceso directo o atajo entre dominios que ya tienen confianza a través de otras relaciones transitivas. Se utiliza para acelerar la autenticación.
- **Externa**: explícita, unidireccional, intransitiva
  Entre dominios de distinto bosque. Un dominio confía en otro dominio externo al bosque.
- **De bosque**: explícita, unidireccional, transitiva
  Entre dominios raíces de bosque. Es como la anterior pero transitiva y debe realizarse obligatoriamente entre los dominios raíces de bosque.
- **De territorio**: explícita, unidireccional, transitiva o intransitiva
  Entre un dominio windows y un territorio no windows, como un territorio Kerberos (p.e. máquinas Linux).

Al configurar una relación de confianza es bueno incluir en la configuración de red del servidor los sufijos DNS del otro dominio para que resuelva nombres "incompletos" como '`serv1`' sin necesidad de poner '`serv1.otrodominio.local`'.

MAESTRO ÚNICO

Existen 5 operaciones, 2 de bosque y 3 de dominios, que para evitar inconsistencias solo puede hacer un maestro de operaciones (maestro único), también llamado FSMO (*Flexible Single Master Operation*). Sin embargo cualquier DC puede autoerigirse en maestro único. Inicialmente el primer servidor del bosque es el maestro único de las 5 operaciones, por lo que es conveniente repartir las funciones.

- **BOSQUE**
  - **Maestro de esquema**. Permite modificar el esquema del directorio.
    Modificable en la consola de gestión con el complemento de esquema.
  - **Maestro de nombres de dominios**. Asegura que los nombres de dominio sean únicos en el bosque.
    Modificable en “Dominios y confianzas de AD”
- **DOMINIO** (Modificables en “Usuarios y equipos de AD”)
  - **Servidor de RIDs**. Sirve ID relativos (nombres únicos).
  - **Emulador de PDC**. Mantiene compatibilidad con servidores NT que funcionen como BDC.
  - **Maestro de infraestructura**. Actualiza los IDs de seguridad cuando un objeto se mueve o elimina.

Se puede consultar fácilmente los maestros con el comando “`netdom query [/domain:dominio] fsmo`”.

HERRAMIENTAS DE ADMINISTRACIÓN DEL AD

- Consola "**Dominios y confianzas de AD**". Permite:
  - Gestionar relaciones de confianza.
  - Cambiar el nivel funcional de los dominios y del bosque.
  - Modificar el maestro de nombres de dominios.
- Consola "**Sitios y Servicios de AD**". Permite:
  - Gestionar subredes y sitios.
  - Establecer la réplica del "Catálogo global"
  - Definir la topología de réplica.
- Consola "**Usuarios y Equipos de AD**". Permite:
  - Gestionar, usuarios, grupos, equipos y recursos.
  - Gestionar OUs y GPOs.
  - Modificar los maestros de RID, PDC e Infraestructura.
- **Complemento de Esquema para Consola**. Permite:
  - Modificar el maestro de esquema.
  - Gestionar el esquema.

  Para registrar el complemento de esquema hay que usar "**`regsvr32 schmmgmt.dll`**". Una vez registrado el complemento, lanzando directamente la consola ("**`mmc`**") se puede agregar el complemento de esquema.
- **Comandos en línea**: **`adsiedit`**, **`cacls`**, **`movetree`**, **`netdom`**, **`nltest`**, **`replmon`**, **`ntdsutil`**.

Uso de ntdsutil

La herramienta '**`ntdsutil`**' permite gestionar muchas características de los servidores de AD. Entre otras cosas permite cambiar los maestros y, de hecho, es la única herramienta que permite asumir la maestría cuando el maestro anterior no está disponible. También se utiliza para eliminar del dominio un servidor que no puede de-promocionarse por malfuncionamiento o indisponibilidad.

Asignar maestrías

Existen dos modos básicos de transferencia de maestrías. "**`Seize`**"[15] se utiliza para tomar una maestría aunque el maestro actual no esté disponible. "**`Transfer`**" se utiliza para transferir la maestría avisando al maestro actual. Es preferible usar "**`transfer`**" siempre que sea posible.

```
C:\> ntdsutil.exe
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server miServidor
...
server connections: quit
fsmo maintenance: {transfer | seize} {domain naming master | infrastructure master | pdc | rid
master | schema master}
...
fsmo maintenance: quit
ntdsutil: quit
```

15 "*Seize*", en inglés incautar o confiscar.

Dar de baja un servidor que no está disponible o que ha fallado su "de-promoción"

```
C:\> ntdsutil.exe
ntdsutil: metadata cleanup
metadata cleanup: connections
server connections: connect to server miServidor
...
server connections: quit
metadata cleanup: select operation target
select operation target: list domains
...
select operation target: select domain x
select operation target: list servers in site x
...
select operation target: select server x
...
select operation target: quit
metadata cleanup: remove selected server
metadata cleanup: quit
ntdsutil: quit
```

Consultar maestrías de un servidor

```
C:\> ntdsutil.exe
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server miServidor
...
server connections: quit
fsmo maintenance: select operation target
select operation target: list roles for connected server
...
```

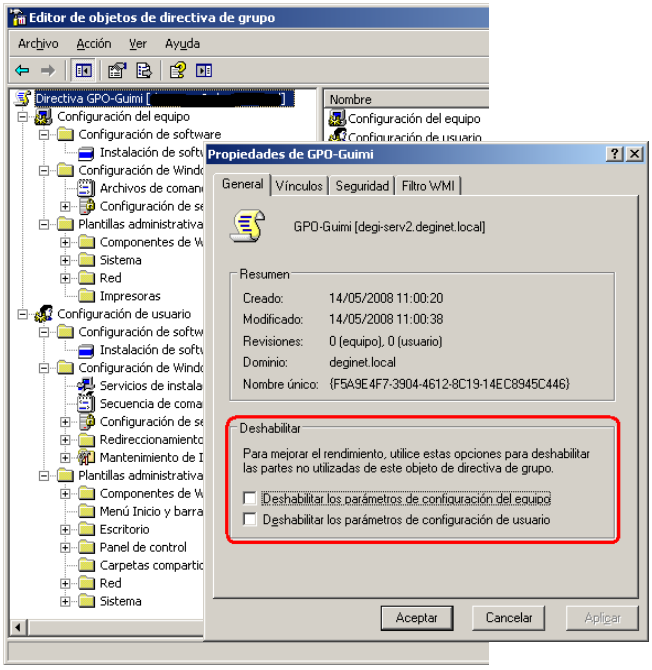
OBJETOS DE POLÍTICAS DE GRUPO (GPOs)

Los GPOs (*Group Policy Object*) son objetos del directorio activo que permiten establecer de forma centralizada la configuración de grupos de usuarios y equipos. Estos GPOs se vinculan a uno o varios sitios, dominios u OUs del directorio (no a contenedores *built-in*) y son heredados por las "sub-OUs"[16].
Cada OU puede tener vinculados múltiples GPOs cuyas directivas son acumulativas.

Dentro de cada GPO, las directivas se organizan jerárquicamente en un árbol temático cuyo primer nivel distingue entre "Configuración del equipo" -que aplica solo a equipos- y "Configuración de usuario" -que aplica solo a usuarios y grupos-. Cuando un usuario inicia sesión en un equipo, se procesan los apartados "Configuración del equipo" de los GPOs aplicables al equipo y los apartados "Configuración de usuario" de los GPOs aplicables al usuario y sus grupos.

Se recomienda que los equipos residan en OUs diferentes de los grupos y usuarios, para aplicar diferentes GPOs sobre ellas. En este caso podemos mejorar el rendimiento del procesamiento de directivas deshabilitando una de las dos partes principales del GPO (equipo / usuario) que de todas formas no se va a aplicar.

En el segundo nivel las políticas se agrupan en "Configuración de software" (sobre instalación automática de software), "Configuración de Windows" y "Plantillas administrativas" (políticas que se guardan en el registro de Windows).
Las políticas de "Plantillas Administrativas" en Windows 2003 se guardan en un apartado específico del registro y dejan de aplicarse si el GPO deja de estar en uso, por lo que se les llama "políticas verdaderas" ("*true policies*") en contraposición a las llamadas "preferencias" ("*GP preferences*") que se usaban anteriormente para las "Plantillas Administrativas" y escribían permanentemente el registro.



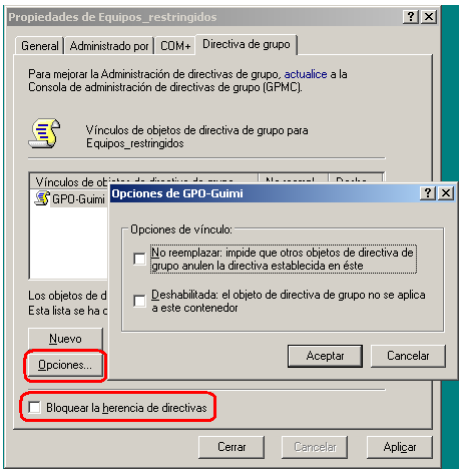
El orden de aplicación de las directivas o políticas es[17]:
- Directivas locales (llamadas a veces LGPO)
- GPOs vinculadas a sitios
- GPOs vinculadas a dominios
- GPOs vinculadas a OUs de primer nivel
- GPOs vinculadas a OUs de segundo nivel
- ...

En cada nivel puede haber varios GPOs que se aplican por el orden indicado en la OU (de arriba a abajo en la ventana).
Las últimas directivas aplicadas prevalecen sobre las anteriores.

Las políticas se aplican automáticamente en el inicio del equipo, en el inicio de sesión de usuario y periódicamente cada 90 minutos +[0-30]. Además el administrador puede forzar la recarga manualmente con el comando "`gpupdate`".
Un usuario puede consultar toda la información sobre las políticas que se aplican sobre él en ese equipo con el comando "`gpresult`".

16 Existe una GPO predefinida llamada "*Default Domain Controllers Policy*" vinculada a la OU -también predefinida- "*Domain Controllers*".
17 Hay que recordar que aunque en los dominios -estructura lógica- se heredan las políticas de los sitios -estructura física-, los dominios son límites de seguridad y sus políticas no se aplican en ningún otro dominio ascendente o descendente (dominios padres e hijos).

MODIFICACIONES EN LA APLICACIÓN DE DIRECTIVAS

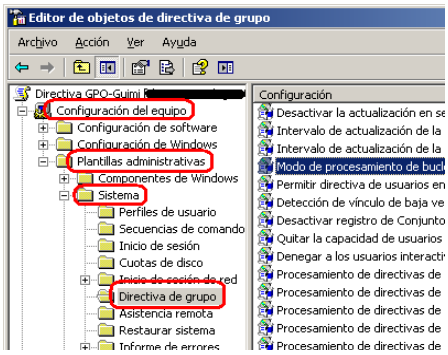


Se puede indicar al sistema que en una OU concreta se bloquee la herencia de directivas, para que en esa OU no se apliquen los GPOs heredados.

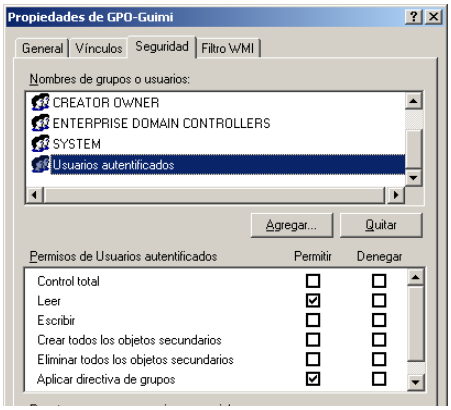
Se puede indicar que lo especificado en este GPO no pueda ser reemplazado por ningún GPO aplicado posteriormente ("No reemplazar" o "*Enforced*"), lo que se aplicará en todas las OUs en que esté vinculado el GPO.
También se puede indicar que se deshabilite el GPO. La explicación en castellano que muestra el sistema es errónea. Al deshabilitar una GPO lo que hacemos no es que no se aplique (para eso basta con no vincular el GPO a la OU) sino que revierta lo indicado en la GPO, es decir que deshabilite las políticas habilitadas en el GPO.

En un GPO aplicado sobre un equipo, se puede activar el "Modo de procesamiento de bucle inverso" (*loopback*) -ver imagen de la derecha-. Esto hace que se procesen los apartados "Configuración de usuario" de los distintos GPOs aplicables al equipo, lo que permite aplicar configuraciones referentes a usuario en función del equipo en que se inicia sesión. Esto es útil en kioscos y aulas:

- En el modo "reemplazar" solo se procesan los GPOs aplicables al equipo, mientras que los GPOs aplicables al usuario no llegan a procesarse.
- En el modo "combinar" la lista de GPOs del equipo se agrega al final de los GPOs correspondientes al usuario. Esto hace que las configuraciones de usuario de los GPOs aplicables al equipo tengan mayor prioridad que las configuraciones de usuario de los GPOs aplicables al usuario.



ADMINISTRACIÓN DE GPOS



Los GPOs, como el resto de objetos del AD, poseen DACLs que permiten establecer qué usuarios y grupos pueden leer o administrarlos y sobre qué usuarios y grupos de la OU se aplicará la GPO.

Lo habitual es que a todos los usuarios autenticados se les aplique -y que la puedan leer- y que el grupo de Administradores pueda administrar el GPO, que por omisión se les aplica por ser usuarios autenticados (podría denegarse para ellos el permiso 'Aplicar directiva de grupos') .

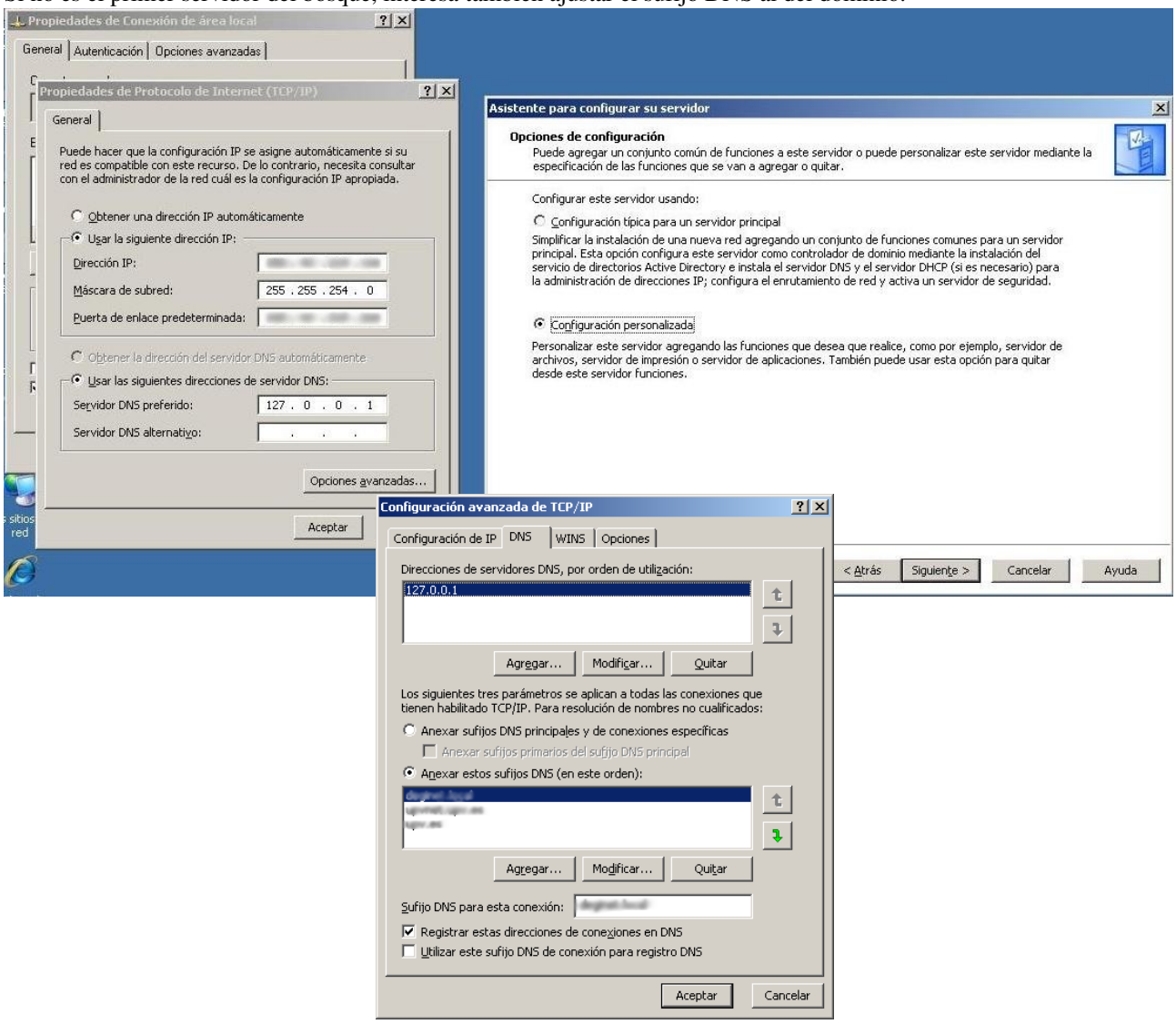
Las DACLs permiten por tanto filtrar el ámbito de aplicación y delegar la administración de las políticas (no confundir con la administración de una OU).

CONFIGURACION DE AD EN WINDOWS 2003

CONFIGURACIÓN DE UN DC (*Domain Controller*)

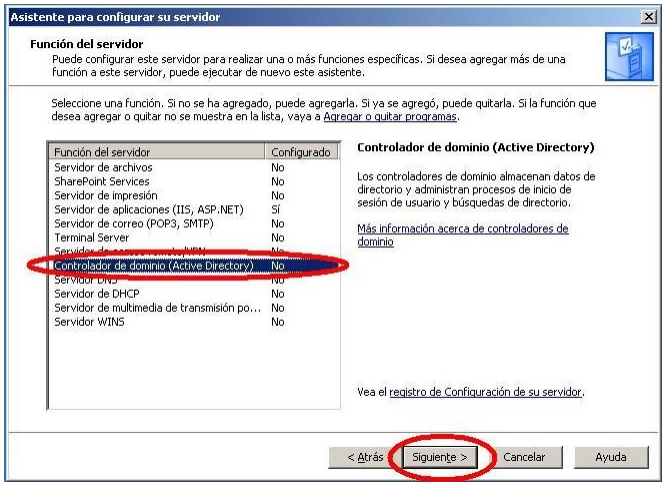
La IP del servidor no puede ser dinámica. El servidor DNS es la propia máquina y solo la propia máquina (sin DNS secundario). Después en el servicio DNS definimos *forwarders*.

Si no es el primer servidor del bosque, interesa también ajustar el sufijo DNS al del dominio.

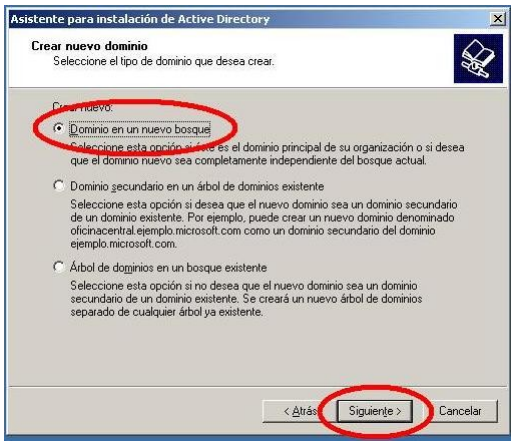


Agregamos la función de controlador de dominio (Active Directory). Podemos lanzarlo con el comando DCPromo o desde el asistente "Administre su servidor".

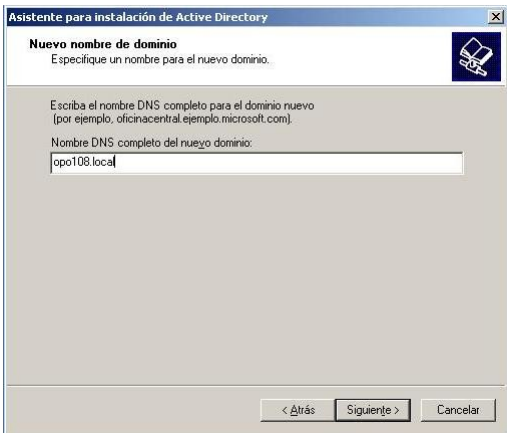
Lanzamos DCPromo desde “Administre su servidor”.

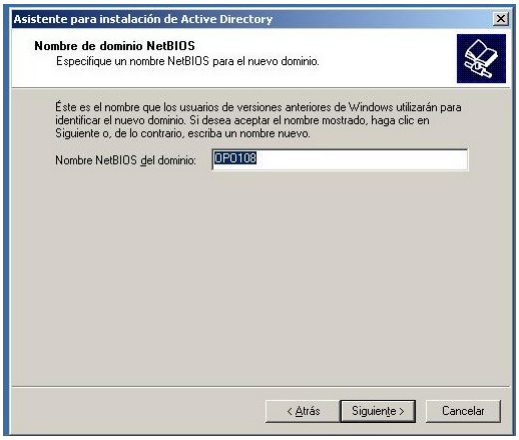


Para el primer servidor del dominio elegimos “Controlador de dominio de un dominio nuevo” y “Dominio en un nuevo bosque”. Para un segundo servidor elegiremos “Controlador de dominio adicional...”

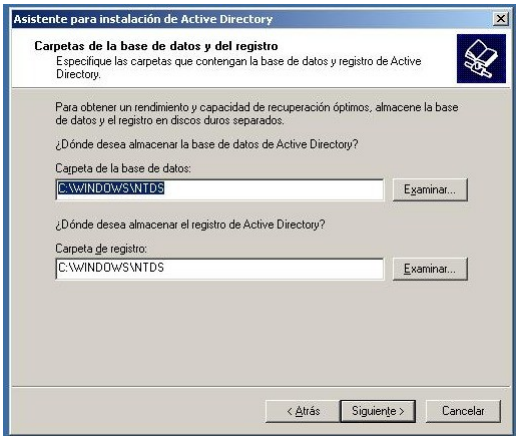


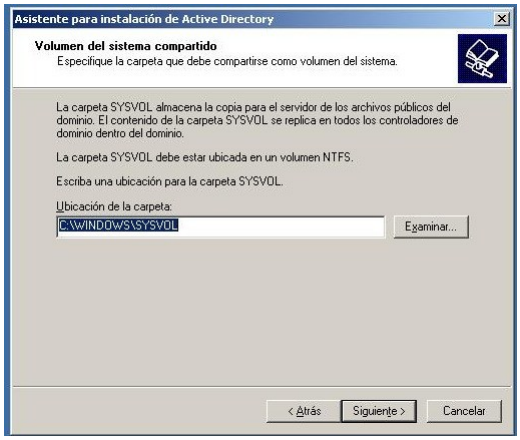
Se indica un nombre DNS completo. Si la máquina no va a servir un dominio en internet, podemos crear el dominio con la estructura <dominio>.local. Después le asignamos un nombre NetBIOS (como los dominios de NT).





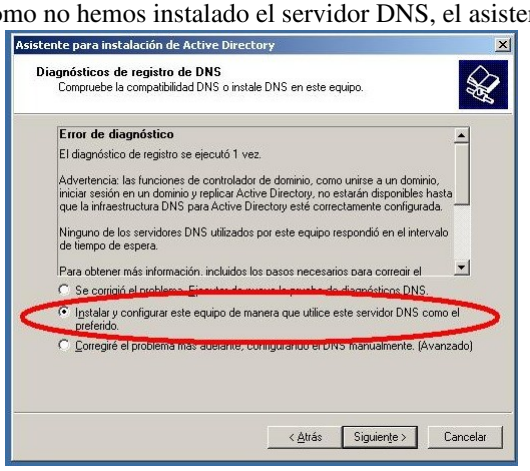
Indicamos las carpetas que usará el sistema.

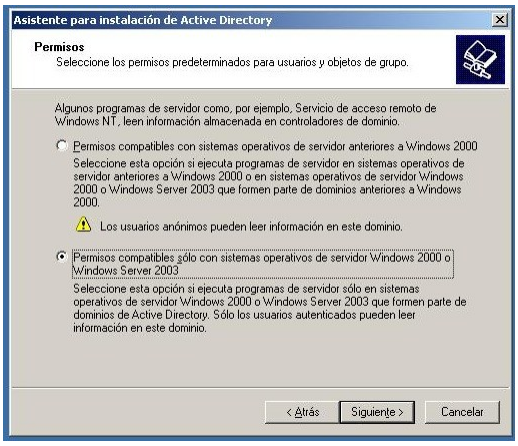




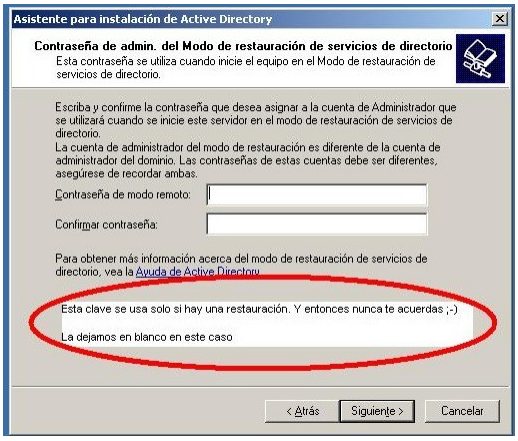
Como se ve, en NTDS se guarda la B.DD. del AD y el archivo del registro; mientras que en SYSVOL se guarda copia de los archivos públicos del dominio.

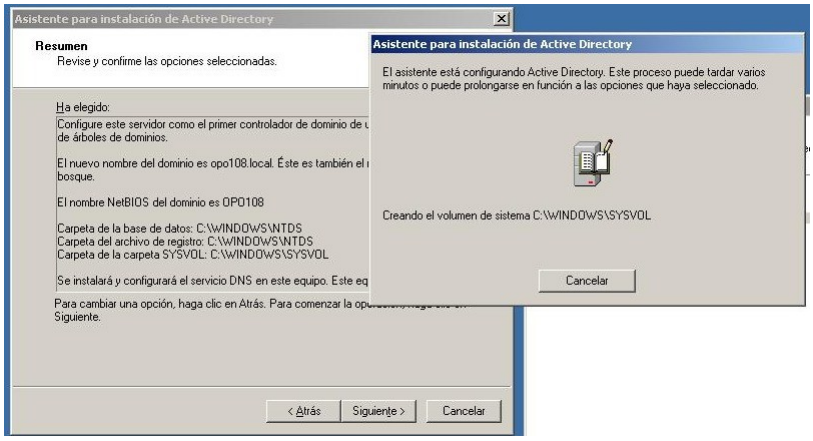
El servidor de AD depende de un servidor DNS, que suele estar en la misma máquina.
Como no hemos instalado el servidor DNS, el asistente de AD lo instalará.



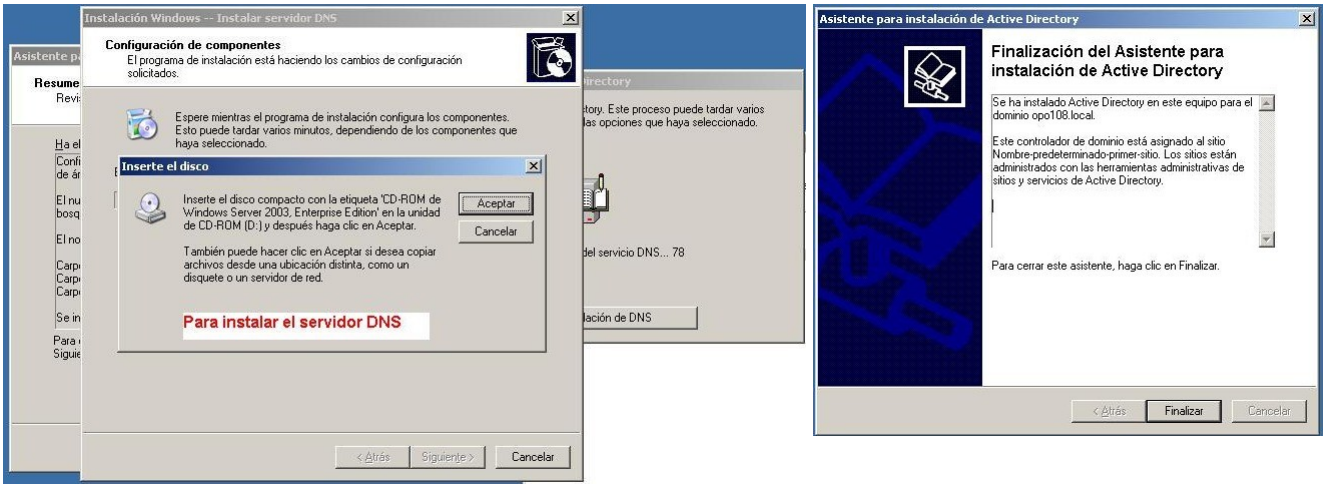


La clave de restauración solo se usa desde la consola de recuperación en caso de necesidad. Al no usarse casi nunca se suele olvidar. Dado que la recuperación se hace con acceso físico a la máquina puede dejarse en blanco en muchos casos.

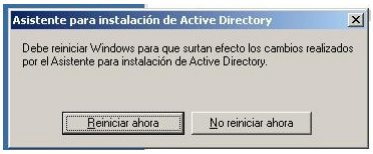




Nos solicita los CDs de W2003 para instalar el servidor DNS y termina.

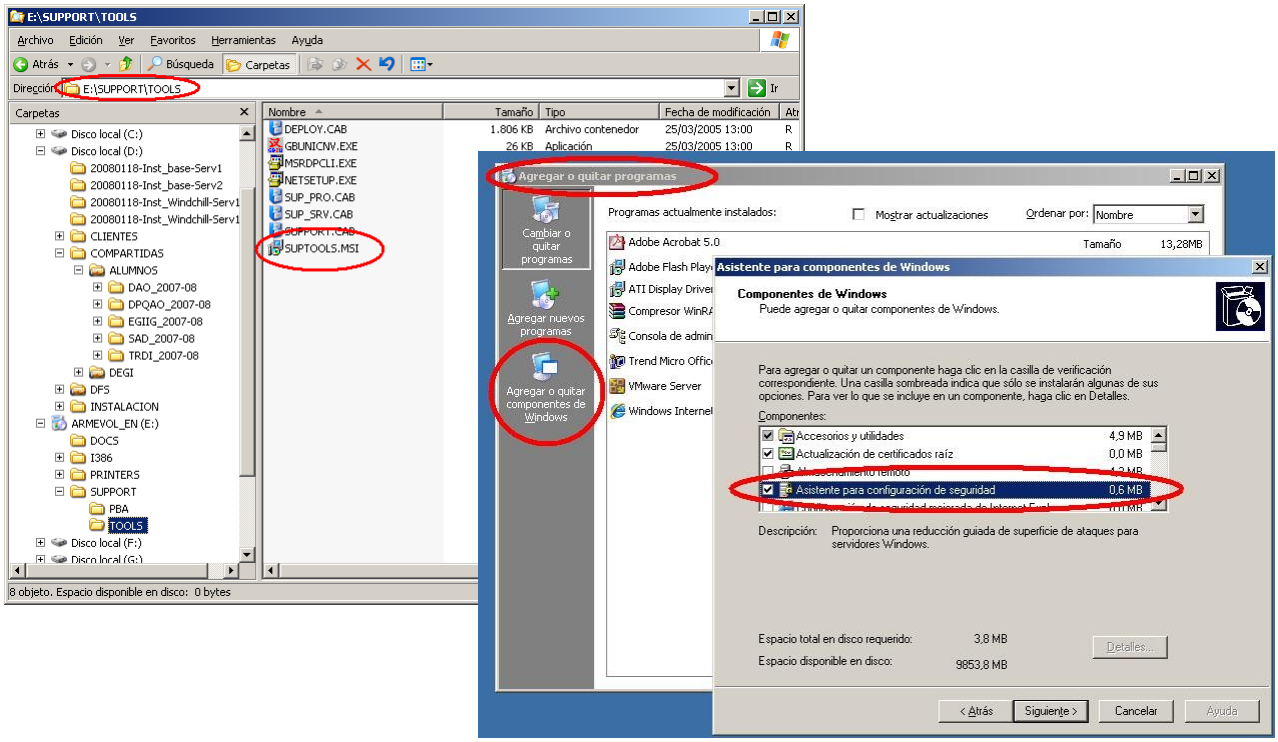


Por supuesto, solicita reiniciar y ya hemos configurado el equipo como DC (*Domain Controller*).



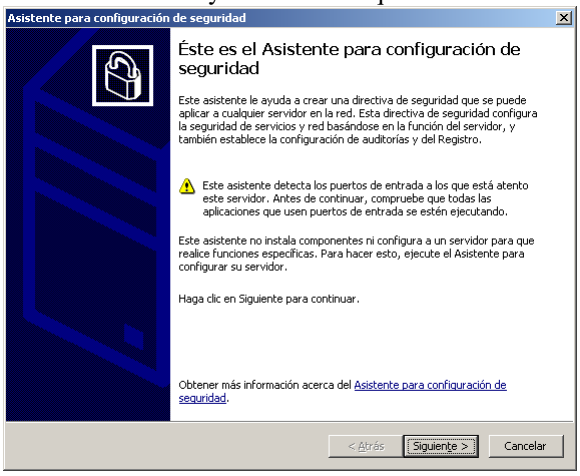
HERRAMIENTAS DE SOPORTE

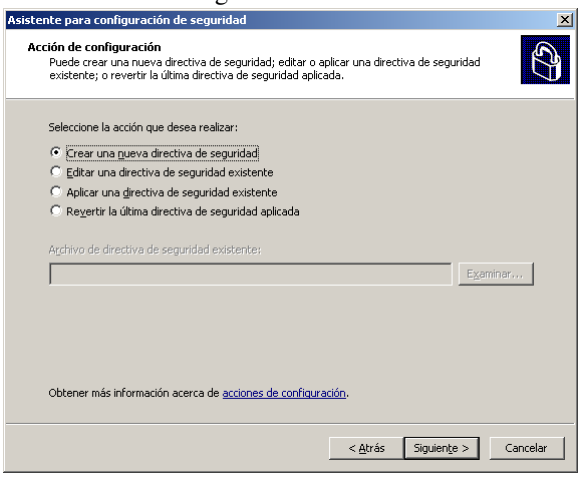
Tras instalar el DC es bueno instalar la herramienta de diagnóstico de red (netdiag) -incluido en las "*support tools*"- y el asistente para configuración de seguridad.



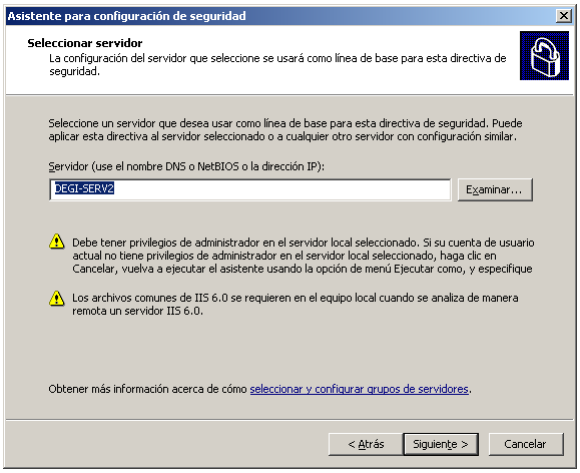
ASISTENTE PARA CONFIGURACIÓN DE SEGURIDAD

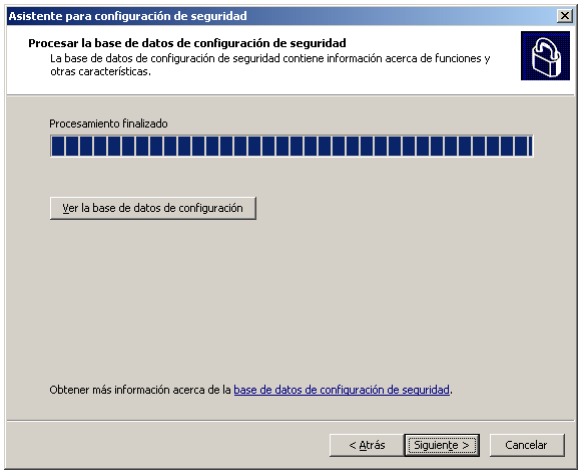
Lanzamos el asistente y le indicamos que vamos a crear una nueva directiva de seguridad.



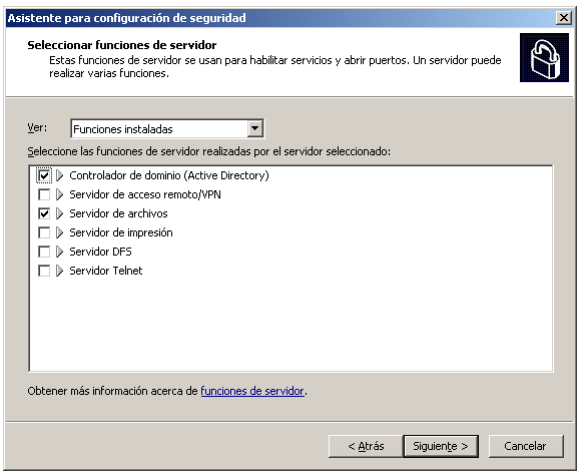


Seleccionamos un servidor que el asistente utilizará como base para crear la directiva.



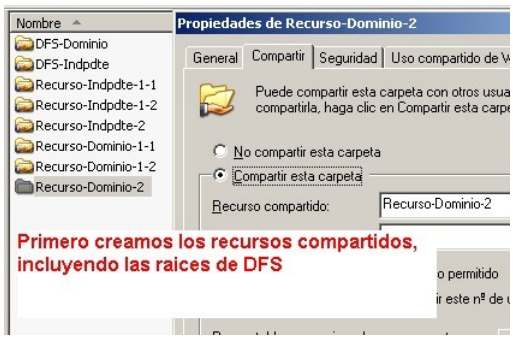


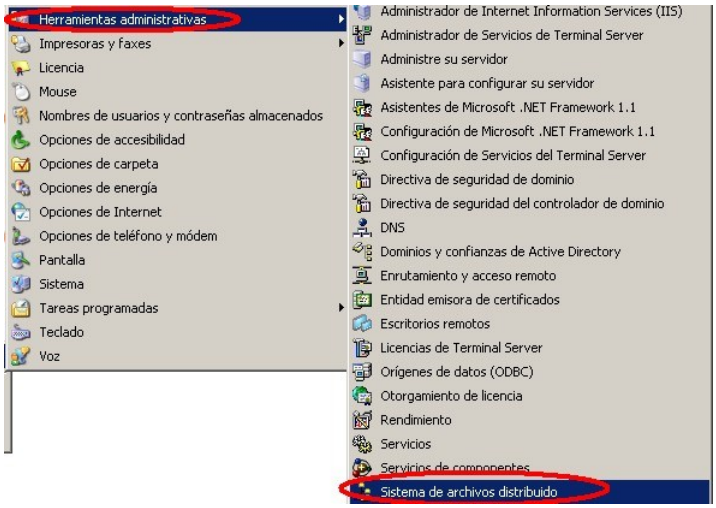
Seleccionamos las funciones del servidor. La directiva generada bloqueará el resto de funciones.



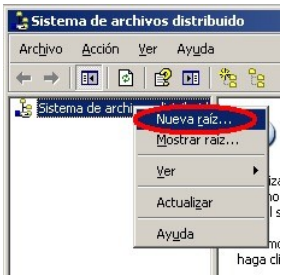
SISTEMA DE ARCHIVOS DISTRIBUIDO (DFS)

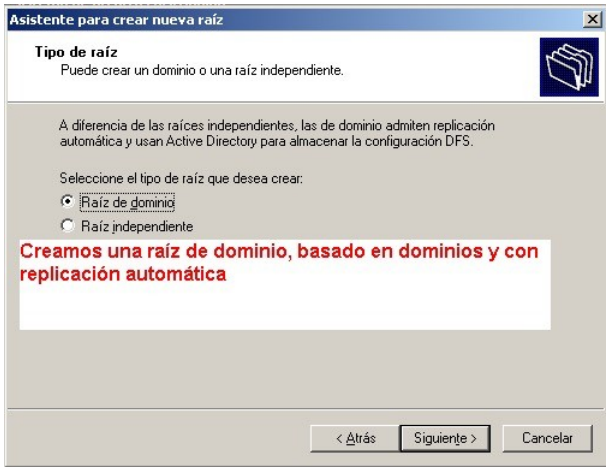
El sistema de archivos distribuido facilita a los clientes el acceso a diferentes recursos que pueden encontrarse en diferentes máquinas, agrupándolos bajo un solo nombre de recurso (punto de acceso único). Además un recurso puede estar replicado en diferentes máquinas, con las ventajas de reparto de carga y tolerancia a fallos que ello conlleva.
Primero creamos los recursos y los compartimos normalmente (preferentemente ocultándolos con un símbolo '$' al final del nombre de recurso compartido). Debemos crear y compartir al menos una carpeta para la propia raíz DFS y otra para cada recurso compartido. Después accedemos la herramienta de gestión "Sistema de archivos distribuido".



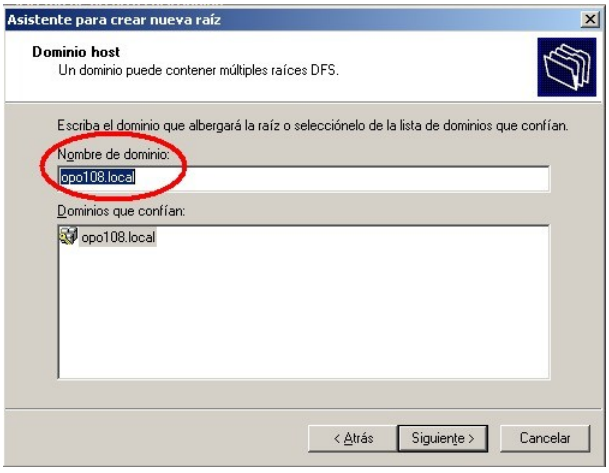


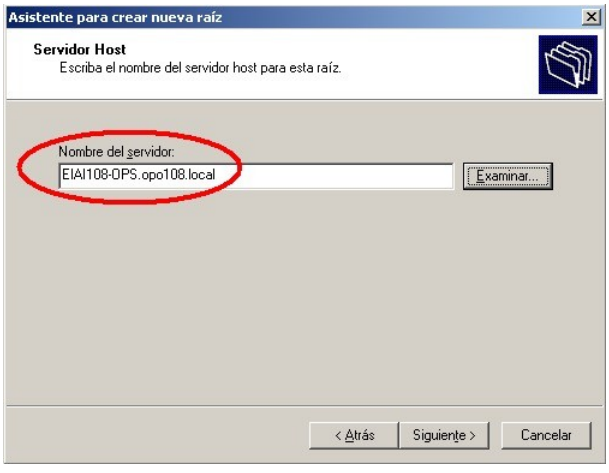
Creamos una nueva raíz. Esta raíz puede ser de dominio (basadas en AD y con replicación automática) o independiente (se pueden replicar recursos manualmente).
Una raíz basada en dominio no puede accederse desde fuera del mismo.



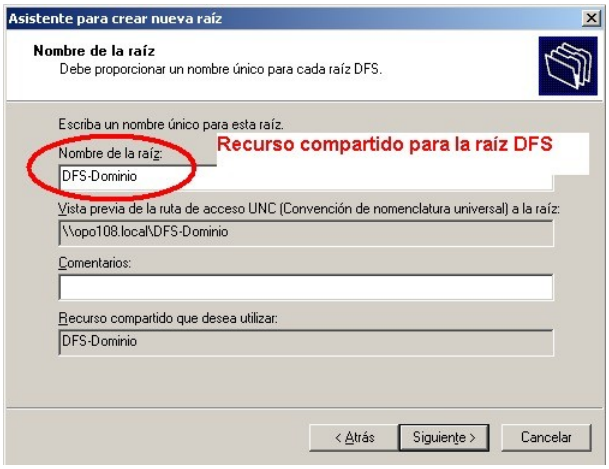


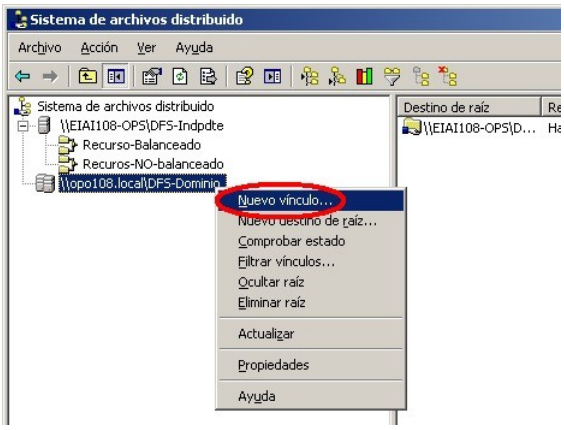
Vamos a crear una raíz de dominio. Indicamos el dominio y el servidor principal (*host*) de la raíz.



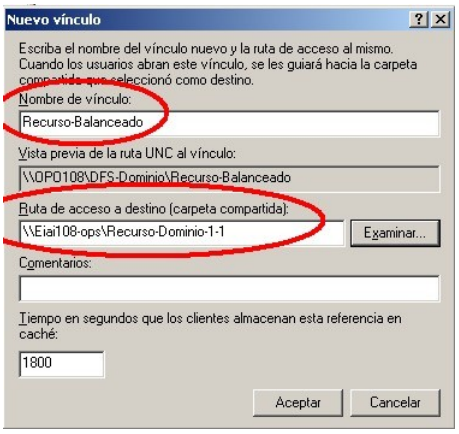


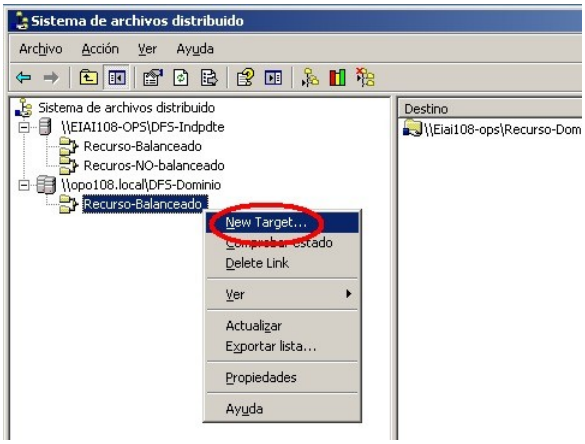
El nombre de la raíz es el recurso que se compartirá en el dominio. En este ejemplo los clientes accederán al recurso `\\<nombre_de_dominio>\DFS-Dominio`. Al ser una raíz de dominio el recurso no depende del servidor sino del propio dominio. Si fuese una raíz independiente se accedería con `\\<servidor>\DFS`. Una vez creada la raíz creamos un nuevo vínculo dentro de ella.



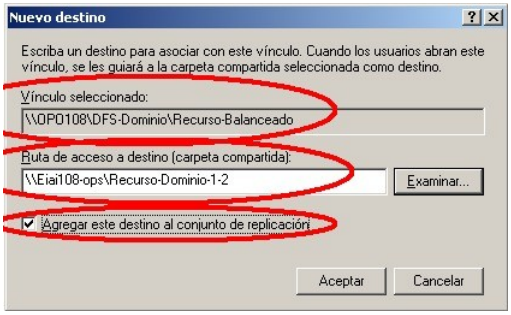


Recordemos que los recursos ya existen y están compartidos (preferentemente de manera oculta). En el sistema DFS gestionamos **vínculos**. Para ello creamos un vínculo y le asignamos "destinos".

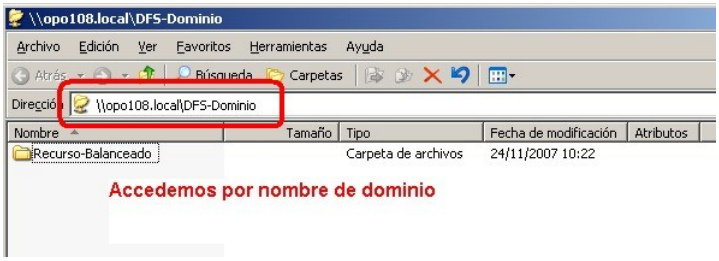




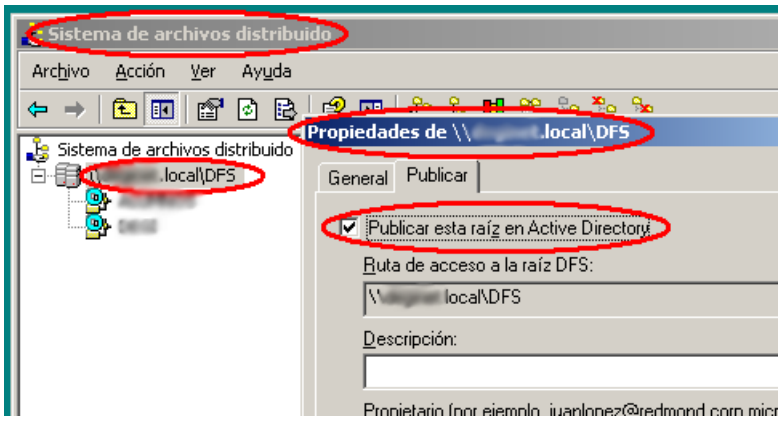
Normalmente asignaremos dos o más recursos de distintas máquinas y los replicaremos (para repartir carga y obtener tolerancia a fallos). Para ello al incluir recursos como destinos del vínculo los unimos al conjunto de replicación.



El resultado final es un recurso del dominio que realmente accede a distintos destinos, en distintas máquinas, que se mantienen automáticamente replicados.



Podemos publicar la raíz del DFS en el directorio. De este modo aparecerá el recurso al explorar “Mis sitios de red” y desplegar la raíz del dominio.

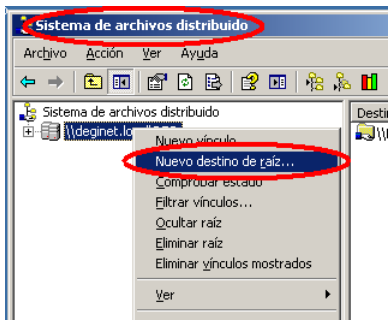


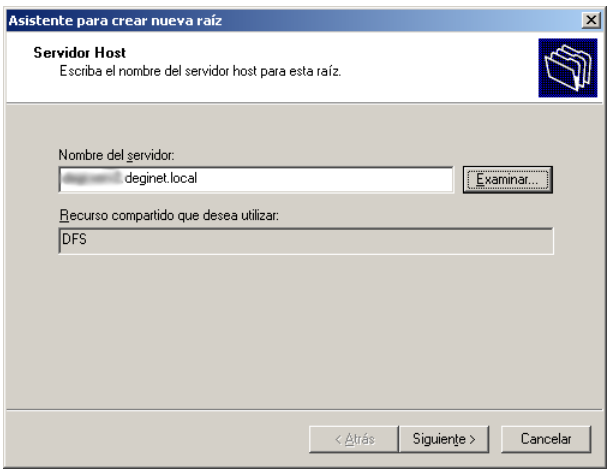
PERMISOS EN EL ESPACIO DE NOMBRE DFS

No se pueden aplicar ACLs específicas en el espacio de nombres DFS, sino que aplican los permisos de los recursos publicados.

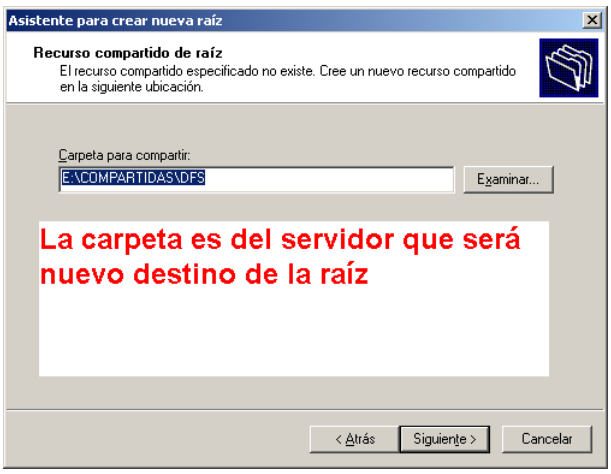
INCLUIR OTROS SERVIDORES EN LA RAÍZ DFS

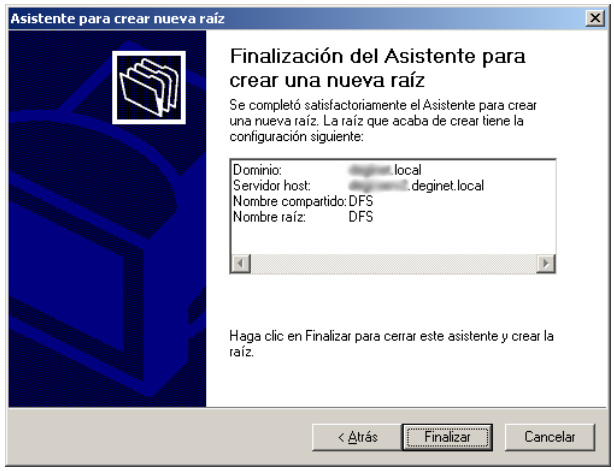
Lo que hemos visto hasta ahora permite que un vínculo DFS tenga como destino distintos recursos en distintas máquinas. Esto permite repartir la carga entre máquinas, sin embargo en caso de que el servidor que tiene la raíz DFS no esté disponible el sistema no será accesible. Para permitir tolerancia a fallos necesitamos incluir otro -u otros- servidor en la raíz del DFS.
Para ello seleccionamos la raíz e indicamos “Nuevo destino de raíz”.





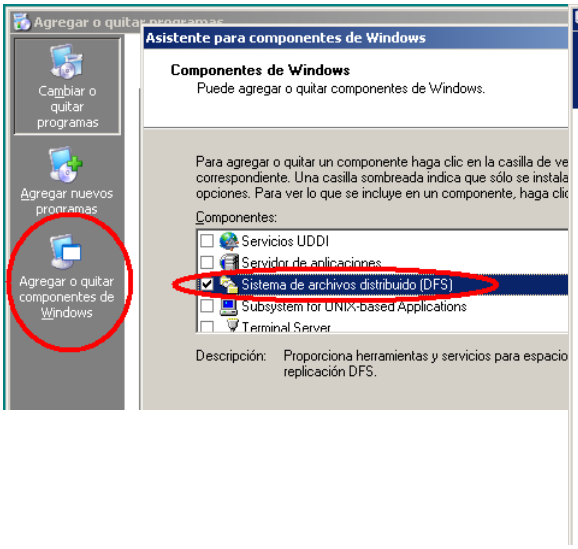
Si no hemos creado la carpeta para el recurso compartido de la raíz, la creamos en este momento.

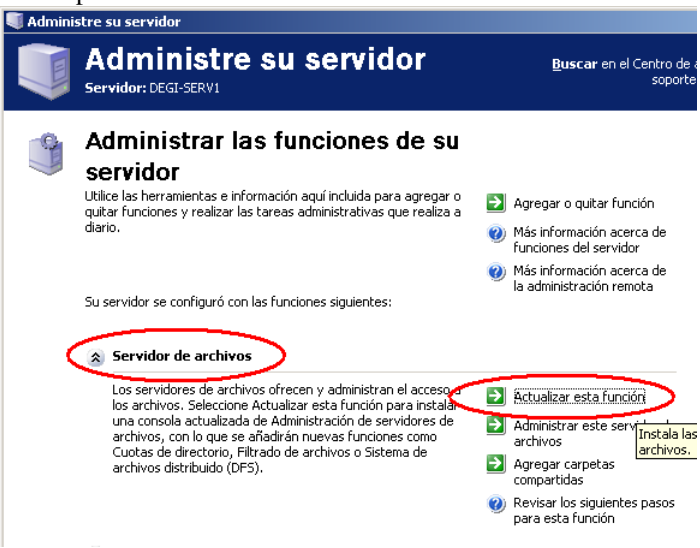


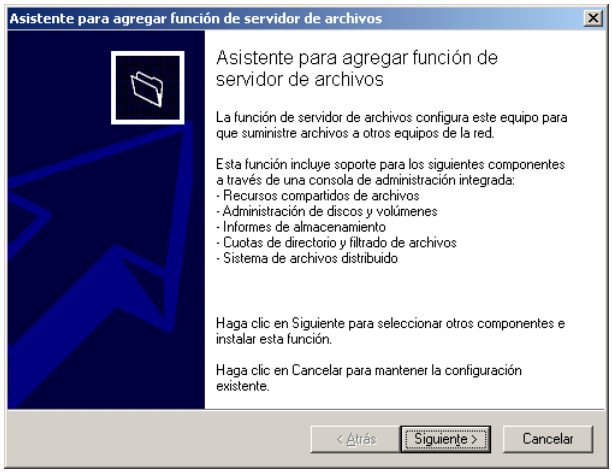


HERRAMIENTAS ACTUALIZADAS

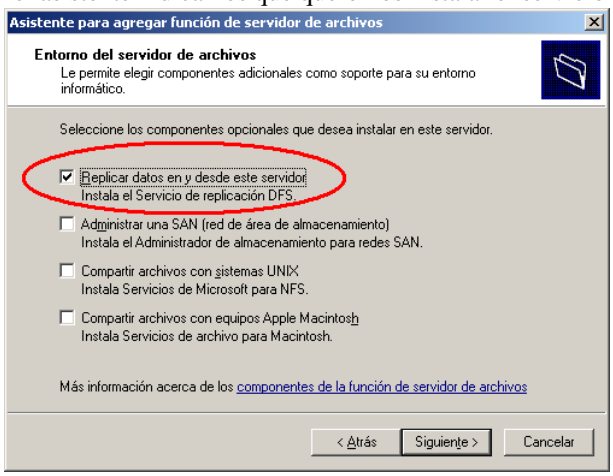
Microsoft incluye como componente de Windows una herramienta de gestión de DFS que sustituye a la que se instala inicialmente en el sistema, cuyo funcionamiento es bastante similar pero que presenta mucha más información en cada pantalla. Otro modo de instalar las herramientas de DFS es a partir del asistente "Administre su servidor".

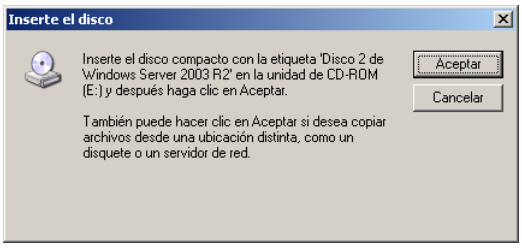


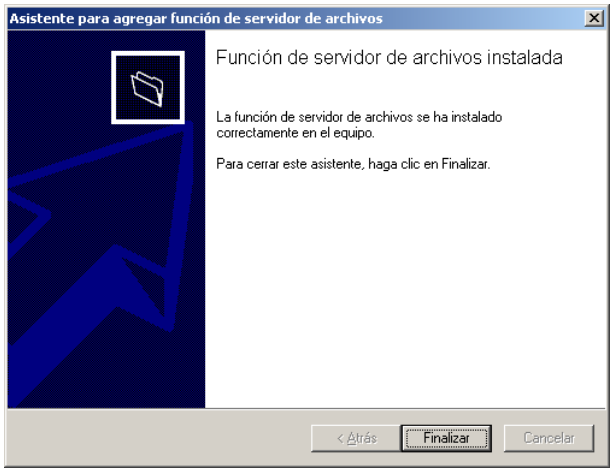




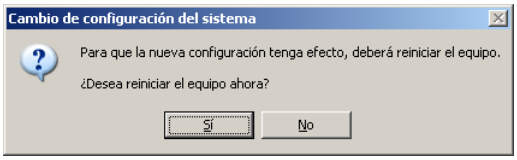
En el asistente indicamos que queremos instalar el servicio de DFS y nos solicita el disco de Windows.

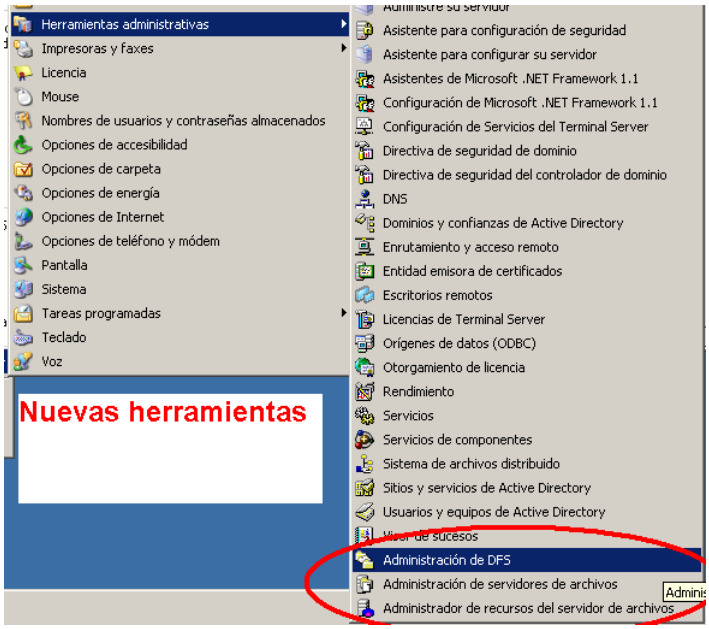






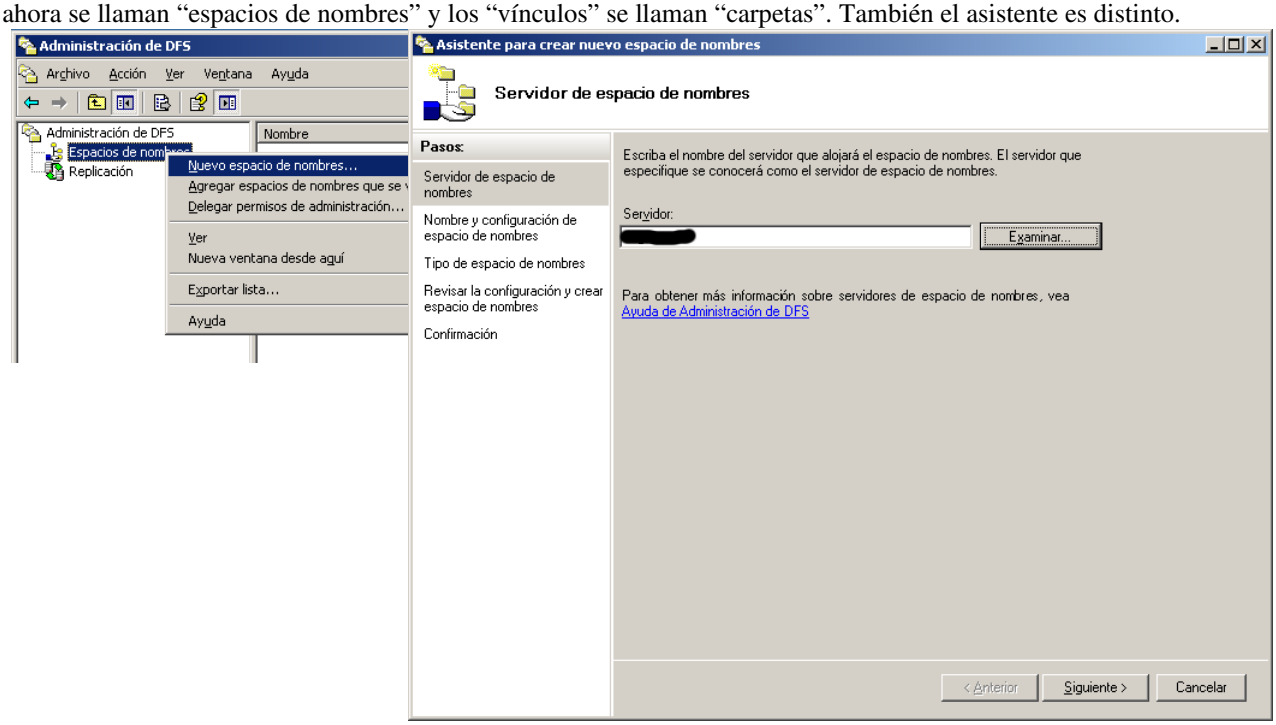
Por supuesto, pide reiniciar.



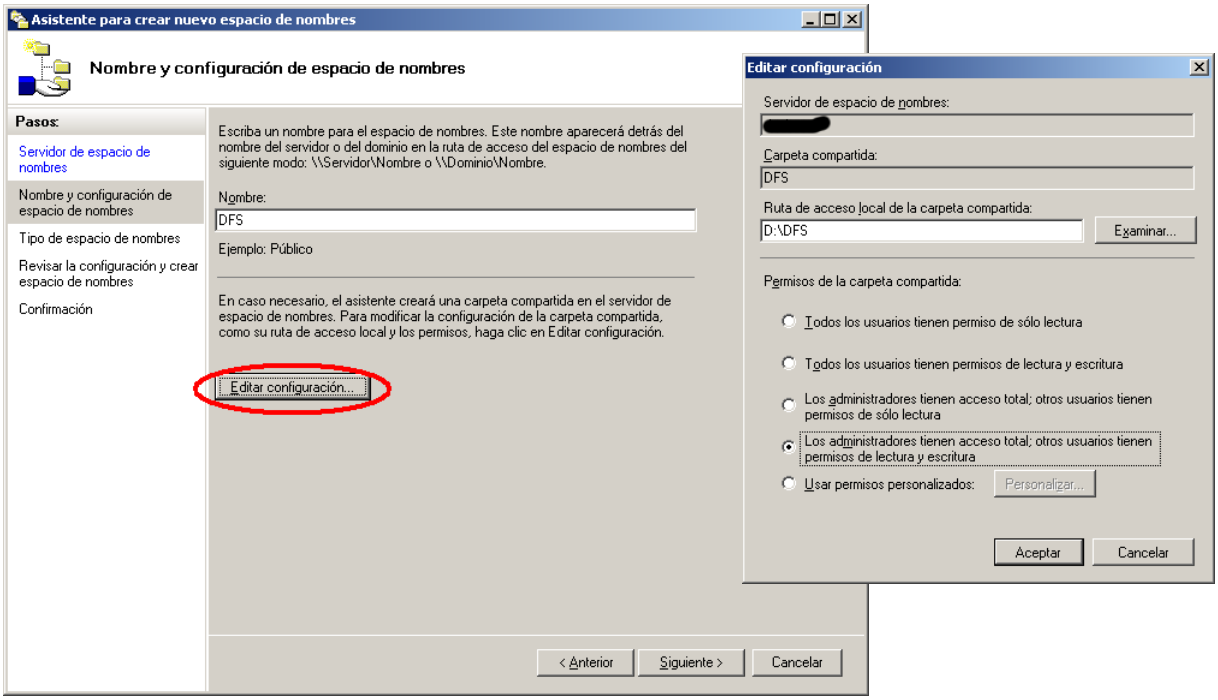


EMPEZANDO DE NUEVO CON LAS HERRAMIENTAS ACTUALIZADAS

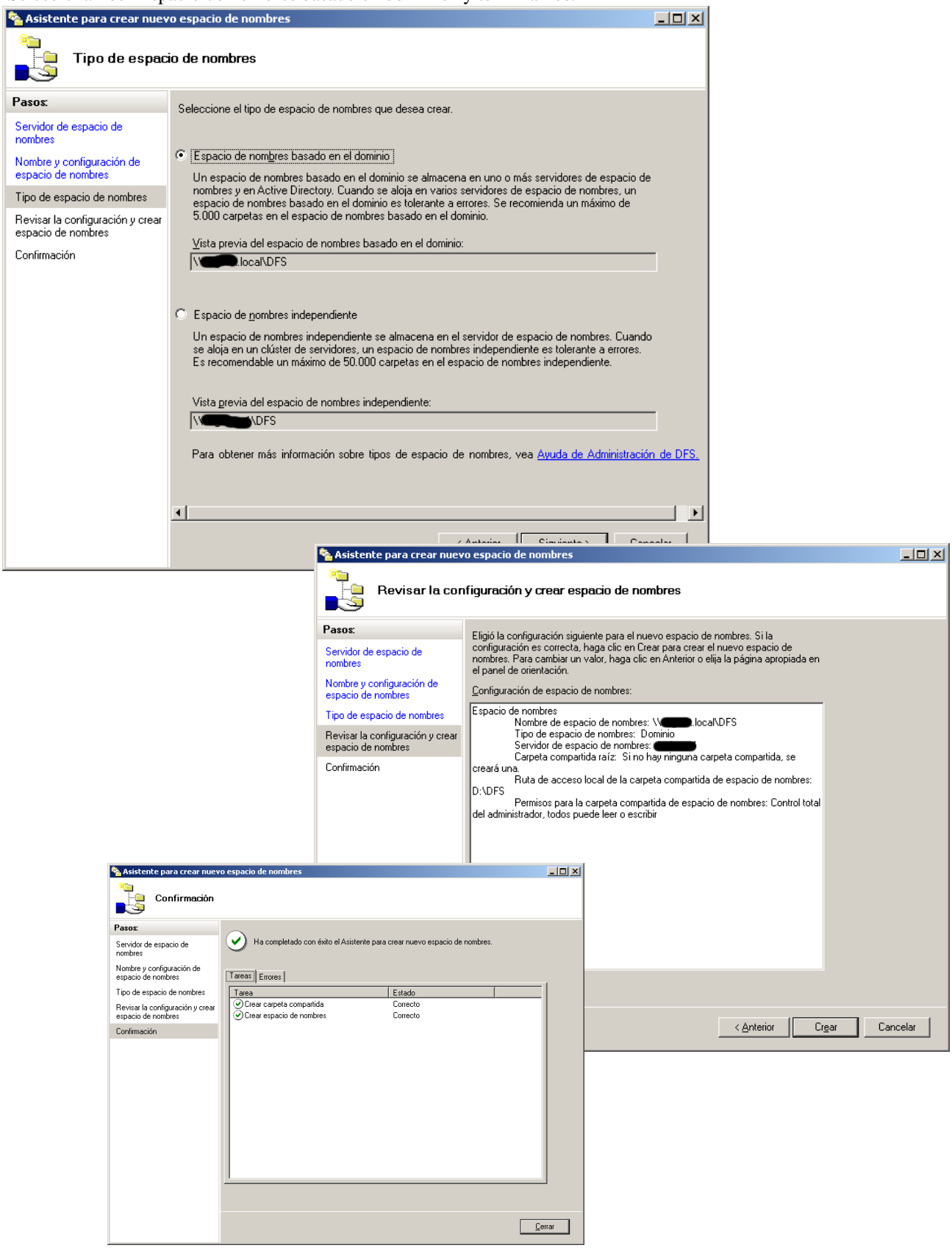
A modo de resumen vamos a realizar de nuevo una implantación de DFS, pero utilizando las nuevas herramientas instaladas. Nótese que ya no utilizamos "Sistema de archivos distribuidos" sino "Administración de DFS". Las "raíces" ahora se llaman "espacios de nombres" y los "vínculos" se llaman "carpetas". También el asistente es distinto.



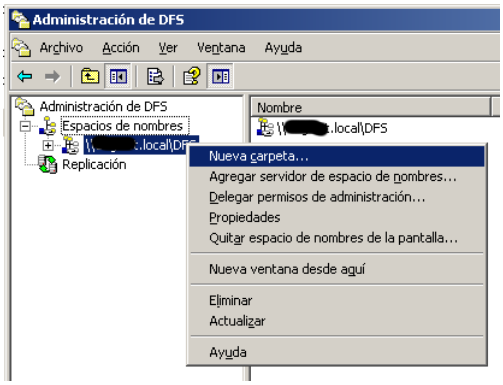
Indicamos el nombre de la raíz DFS y podemos editar la configuración (muy recomendable).

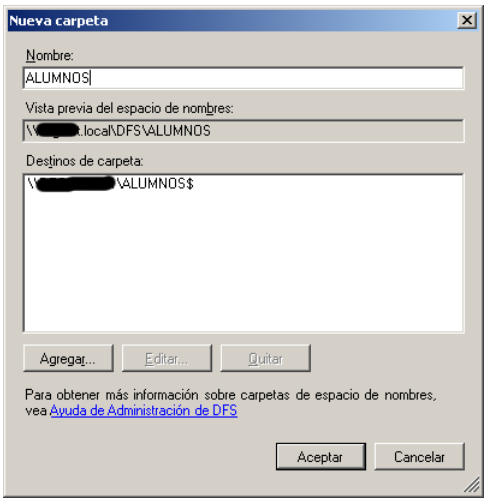


Seleccionamos “Espacio de nombres basado en dominio” y terminamos.

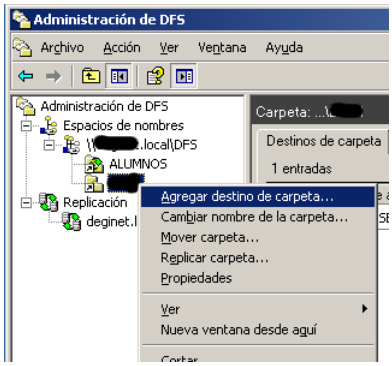


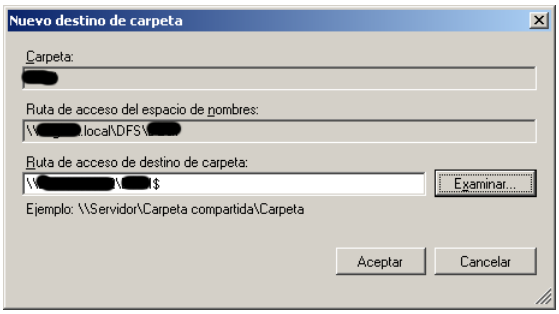
Creamos una nueva “carpeta” en el espacio de nombres y le adjuntamos “destinos”, es decir, carpetas compartidas del sistema.



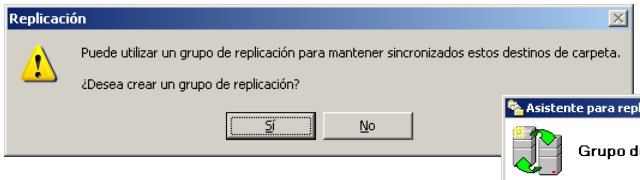


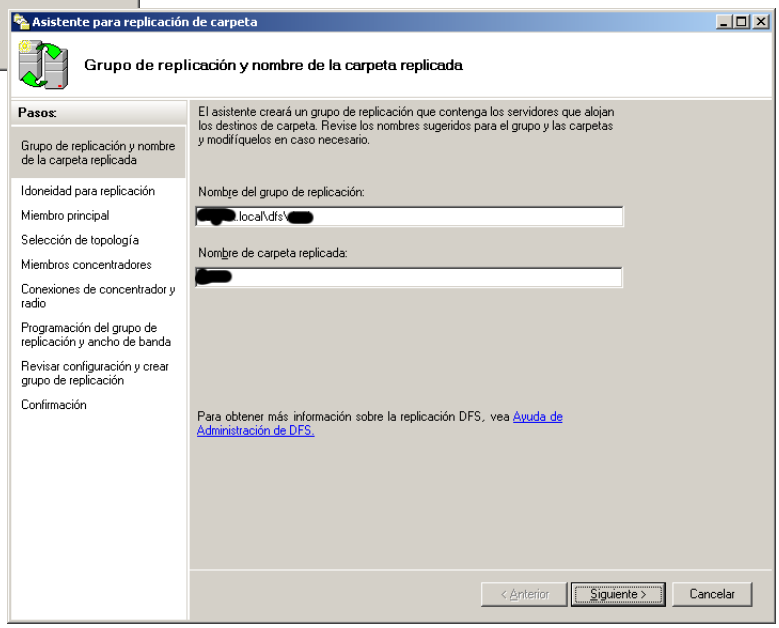
Agregamos nuevos destinos a las carpetas, para permitir el reparto de carga. Recordemos que los nuevos destinos son siempre carpetas que ya existen y están compartidas.



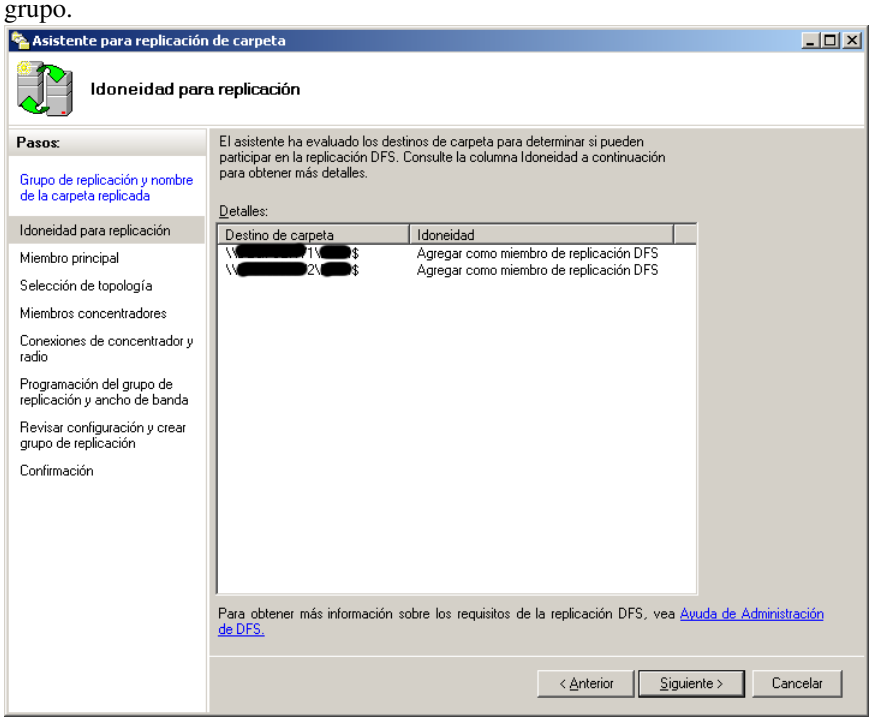


Al agregar nuevos destinos nos ofrece la posibilidad de crear un grupo de replicación automática.

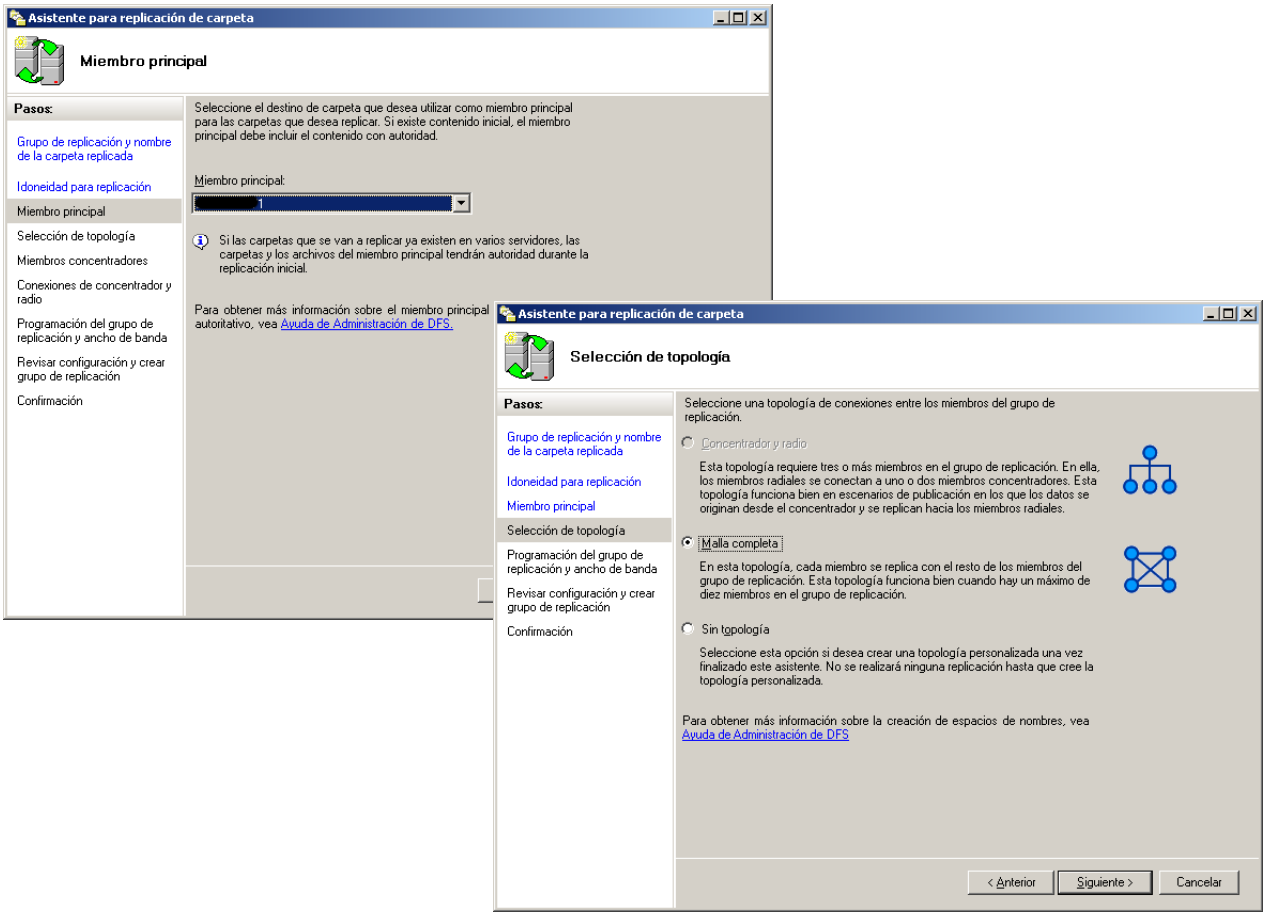




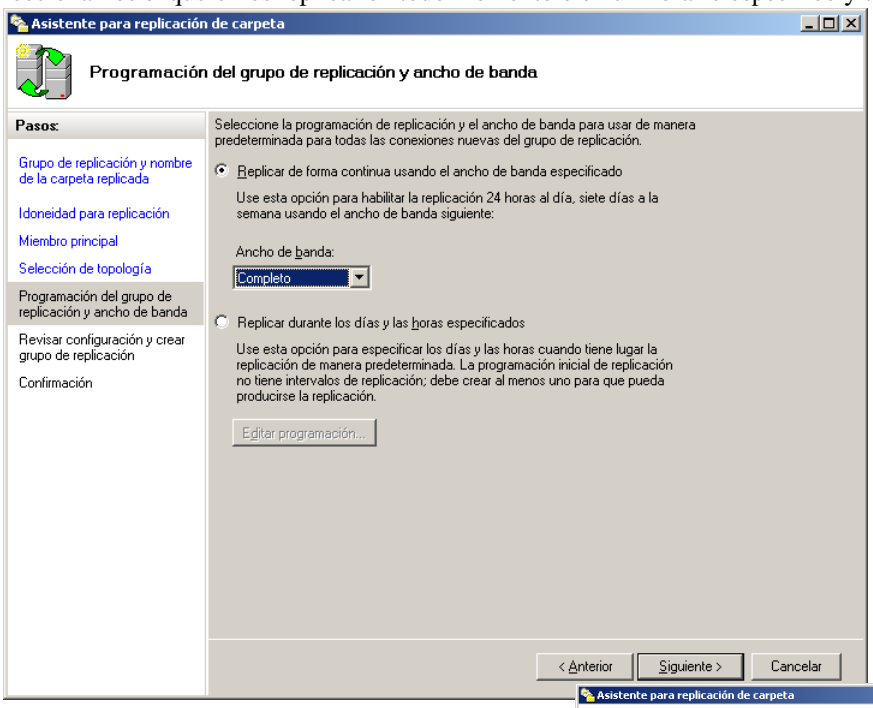
El asistente nos ofrece agregar al grupo de replicación los recursos que son “destino” de la “carpeta” para la que estamos creando el grupo.

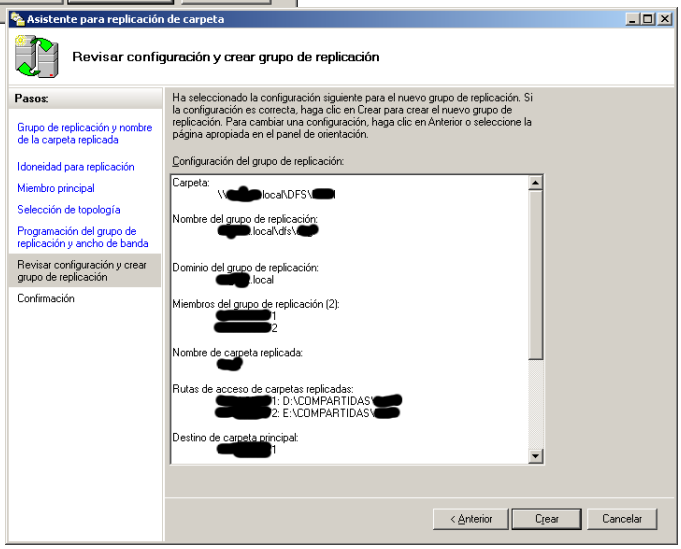


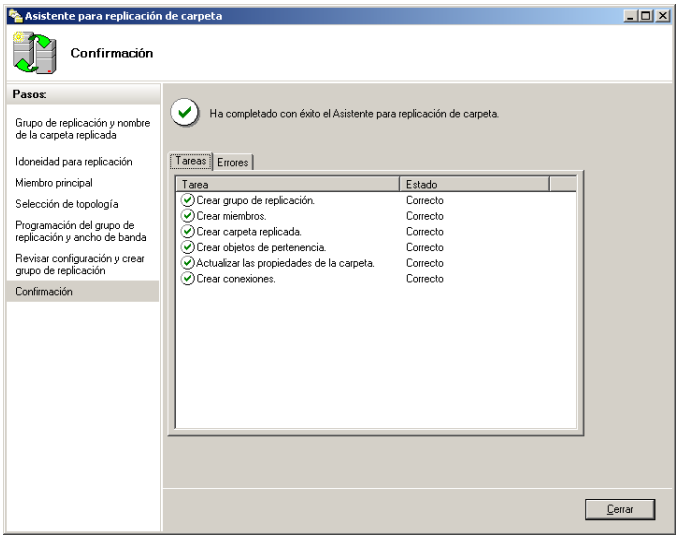
Seleccionamos uno de los servidores como “principal” para los algoritmos de replicación y el algoritmo de replicación que utilizaremos.



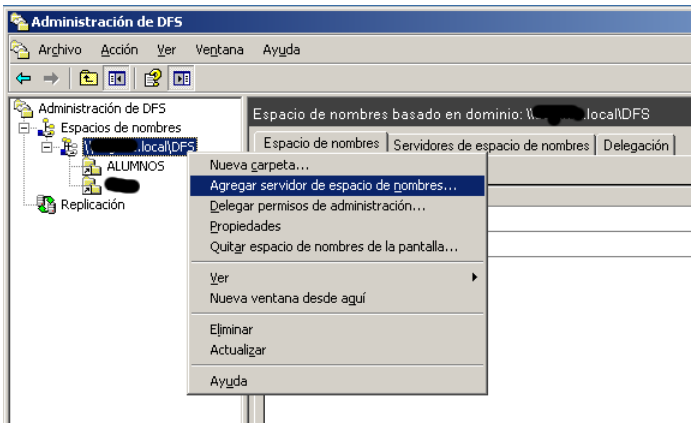
Seleccionamos si queremos replicar en todo momento o en un horario específico y terminamos.

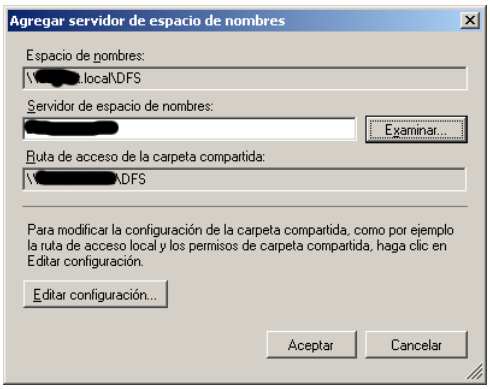




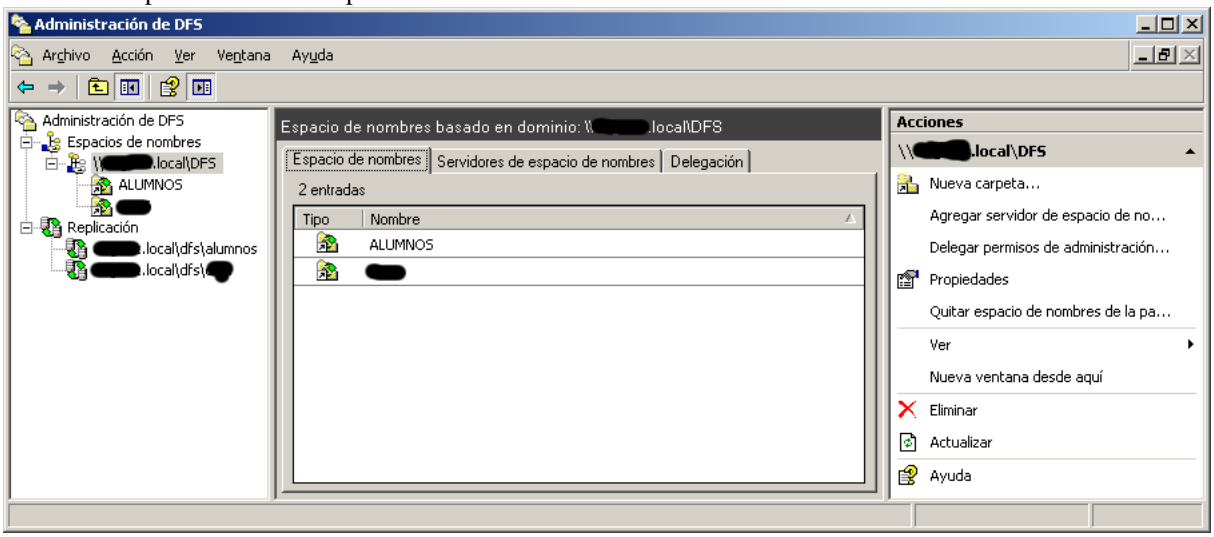


Para permitir la tolerancia a errores agregamos un servidor al espacio de nombres, lo que antes se llamaba “destino de raíz”.

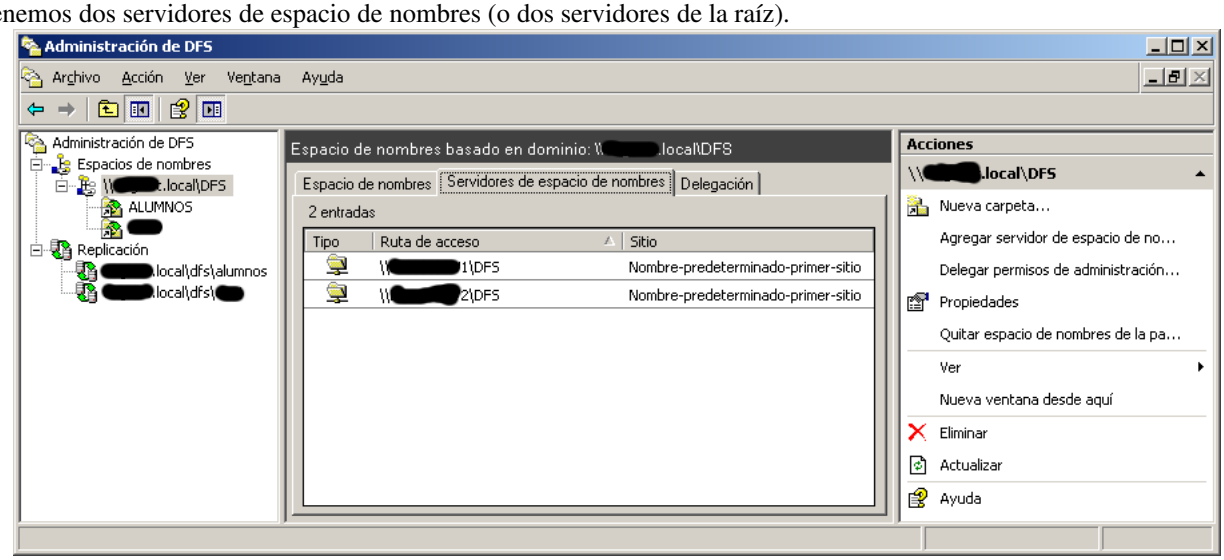




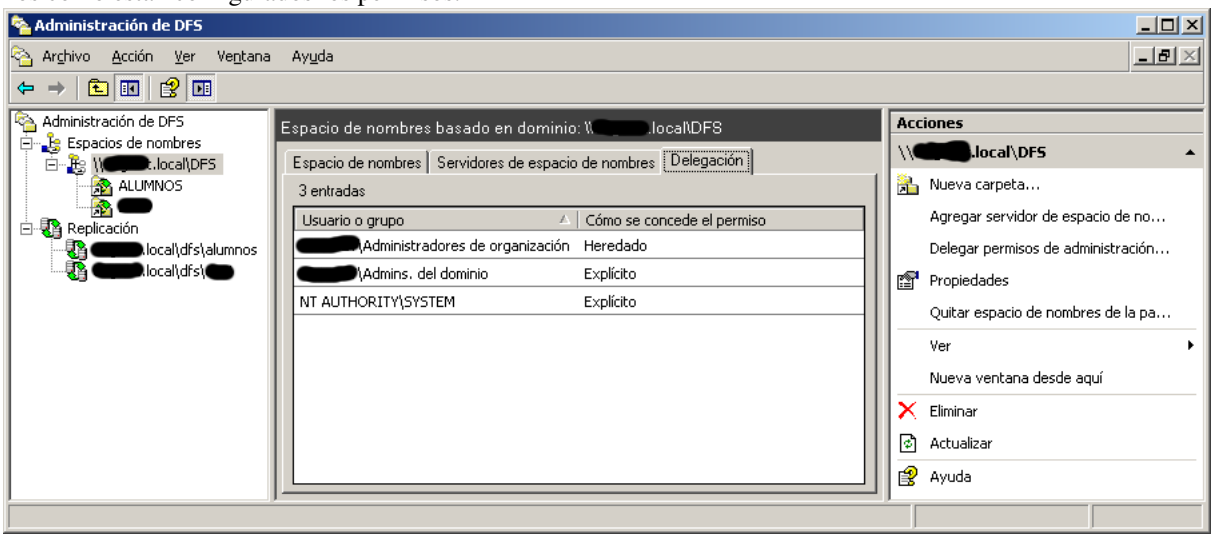
Revisamos la instalación con la nueva herramienta.
Tenemos dos carpetas en nuestro espacio de nombres \\<dominio>\DFS.



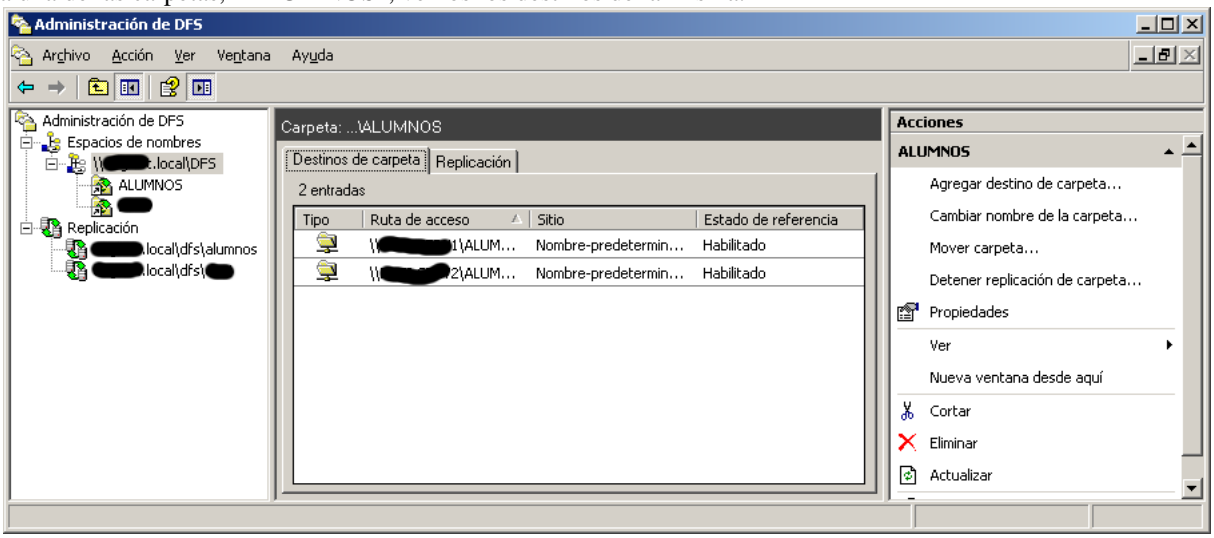
Tenemos dos servidores de espacio de nombres (o dos servidores de la raíz).



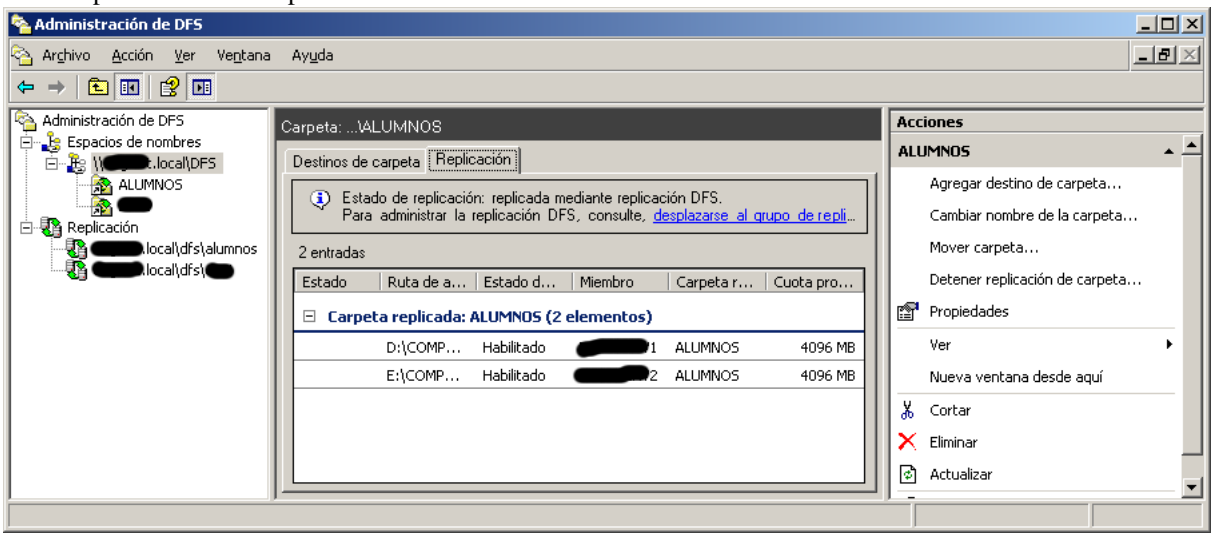
Vemos como están configurados los permisos.



Para una de las carpetas, “ALUMNOS”, vemos los destinos de la misma.



Vemos la replicación de la carpeta.



ANEXO I: COMANDOS DE ADMINISTRACIÓN

Microsoft ofrece una serie de comandos que pueden ser útiles para administrar un sistema Windows. Entre ellos:

- **`bootcfg`**: Configuración de arranque, incluyendo sistema por defecto.
- **`cacls`** (*Change ACLs*): Gestión de ACLs (ver `/T /E /{G|R|P} /{R|W|C|F}`).
- **`comp`**: Comparación de ficheros. Similar al comando diff de POSIX.
- **`control`**: Permite lanzar ventanas de control -las que aparecen al pulsar "Propiedades" y algunos asistentes (*wizards*)-. Hay que indicar el control a lanzar (ficheros *.cpl de la carpeta del sistema).
- **`driverquery`**: Lista información sobre los controladores del sistema.
- **`findstr`**: Similar al comando grep de POSIX.
- **`fsutil`**: Gestión de los sistemas de ficheros. Cuotas, sectores estropeados, archivo disperso...
- **`getmac`**: Muestra las MACs de los dispositivos de red del sistema.
- **`gpresult`**: Muestra información sobre las politicas que se están aplicando al usuario y equipo.
- **`gpupdate`**: Fuerza a recargar las políticas del usuario y equipo.
- **`ipconfig`**: Info. y mínima gestión de los dispositivos de red (ver `/all`, `/renew`, `/release` y `/flushdns`).
- **`mmc`** (*Microsoft Management Console* - consola de gestión): Herramienta base de la administración gráfica de Windows. Las herramientas administrativas son consolas MMC con un complemento determinado.
- **`net`**: Comando complejo que agrupa 22 comandos (net share, net use, net start, net view...).
- **`netdiag`** (*Resource kit*): Permite realizar pruebas (*tests*) de aspectos de la configuración de red.
- **`netsh`**: Configurador de red local o remota en modo comando.
- **`netstat`**: Información sobre protocolo y conexiones TCP. Ejemplo: `netstat -ano`.
- **`nslookup`**: Herramienta de resolución DNS.
- **`pathping`**: Muestra estadísticas de ping entre los nodos de una conexión. Mezcla de `tracert` y `ping`.
- **`ping`**: Comprueba la conexión con una máquina destino mediante paquetes ICMP.
- **`recover`**: Permite recuperar información de una unidad dañada.
- **`reg`**: Comando para gestionar el registro de Windows.
- **`runas`**: Permite lanzar un comando con privilegios de otro usuario.
- **`sc`** (*Service Controller*). Gestión de servicios. Permite no solo pararlos o iniciarlos sino incluso crearlos.
- **`secedit`**: Permite modificar las políticas de seguridad de un equipo en procesos por lotes.
- **`sfc`** (*System File Checker*) Comprueba archivos importantes del sistema y si es necesario los reemplaza por las versiones correctas.
- **`shutdown`**: Permite apagar o reiniciar un equipo.
- **`systeminfo`**: Muestra información variada sobre el sistema (nombre, memoria, tarjetas de red, sistema...).
- **`tasklist`** / **`taskkill`**: Gestor de tareas en línea de comandos.
- **`tracert`**: Muestra la ruta de los paquetes IP hasta su destino.

ANEXO II: ATAJOS DE TECLADO

Siempre que se utilice TAB, se puede usar May+TAB para recorrer en la otra dirección.

- F1: Ayuda.
- F2: Renombrar.
- F3: Buscar.
- F5: Recargar / Refrescar.
- F10: Activa el menú de la ventana.

- Esc: Cancela / Sale.
- Ins: Alterna entre los modos insertar y sobreescribir.
- Supr: Borra.
- May+Supr: Elimina (Borrar sin pasar por la papelera de reciclaje).
- ImprPant: Captura la pantalla (la guarda en el portapapeles).
- Alt+ImprPant: Captura la ventana activa (la guarda en el portapapeles).
- Inicio / Ctrl+Inicio: Va al inicio.
- Fin / Ctrl+Fin: Va al fin.
- RePag / AvPag: Retrocede o avanza páginas.
- Bloq.May. / Bloq.Num: Bloquea las mayúsculas o los numeros.
- Espacio: Activa el control seleccionado.

- Alt: Activa el menú de la ventana. (Igual que F3).
- Alt+Espacio: Menú contextual de la ventana (igual que botón secundario en el título).
- Alt+(letra subrayada): Activa la opción indicada.
- Alt+TAB / Alt+May+TAB: Alterna entre aplicaciones.
- Alt+Intro: Abre la ventana de propiedades del elemento seleccionado.
- Alt-F4: Cierra la aplicación activa (incluido Windows).

- Ctrl+F4: Cierra una subventana.
- Ctrl+TAB / Ctrl+May+TAB: Alterna entre pestañas.
- Ctrl+X / May+Supr: Cortar.
- Ctrl+C: Copiar.
- Ctrl+V / May+Ins: Pegar.
- Ctrl+Z: Deshacer.
- Ctrl+Y: Rehacer.
- Ctrl+Izq / Ctrl+Der: Desplazamiento por palabras.

- CTRL+Shift+ESC: Abre el administrador de tareas.
- CTRL+Esc: Abre el menú de inicio (Igual que W).

- W+M: Minimiza las ventanas.
- W+May+M: Restaura las ventanas.
- W+D: Alterna entre minimizar todas las ventanas (*Desktop*) o restaurarlas.
- W+E: Abre el explorador.
- W+F: Buscar ficheros (*Find*) (Igual que F3).
- W+Ctrl+F: Buscar Equipos.
- W+R: Diálogo “Ejecutar...” (*Run*).
- W+L: Bloquea el escritorio (*Lock*).
- W+Pause: Abre la ventana de propiedades del sistema (Mi PC).
- W+Tab / W+May+TAB: Alterna entre los botones de la barra de tareas.

- May: Altera comportamientos.
  - Al introducir un CD evita la autoejecución.
  - Al mostrar el menú contextual añade opciones (“Abrir con..”)
  - Al abrir un archivo mdb evita que se lance la macro “Autoexec” (en algunas versiones).
  - Junto con Ctrl y arrastrar y soltar permite copiar o mover o enlazar.
  - Marca mientras se desplaza el cursor.
  - Marca desde la selección anterior hasta la actual.
  - ...