Universidad Politécnica de Valencia
Departamento de Sistemas Informáticos y Computación

Administración avanzada de Windows Server 2008 R2

por
Fernando Ferrer García
Andrés Terrasa Barrena

Curso Académico 2011/2012
Valencia, 2 de febrero de 2012

Administración avanzada de Windows Server 2008 R2

Indice

Lista de figuras

Lista de tablas

1

Despliegue y recuperación en entornos Windows

Indice

1.1. Introducción de la unidad

Con la llegada de Windows Vista y Windows Server 2008, el proceso estándar de instalación del Sistema Operativo ha cambiado. Actualmente se utiliza un sistema basado en imágenes de disco en fichero denominado Windows Imaging Format (WIM). Este formato no solo es válido para Windows Vista sino también para sistemas operativos anteriores como Windows XP o Windows Server 2003.

Este nuevo formato junto con las herramientas necesarias para su manipulación representa un marco de trabajo nuevo para conseguir el despliegue masivo de instalaciones de una forma sencilla.

1.2. Objetivos

1. Analizar el nuevo formato de imágenes WIM basado en fichero.
2. Conocer la nueva herramienta de manipulación de imágenes (ImageX) que proporciona Microsoft.
3. Descubrir el nuevo entorno de desarrollo Windows Automated Installation Kit (WAIK) que ayudará al administrador de sistemas a realizar el despliegue básico de laboratorios docentes.

1.3. Esquema

1. Introducción al formato WIM
2. ImageX y WAIK
3. Creación y despliegue de imágenes WIM.

1.4. Introducción al formato WIM

El formato de imágenes de Windows (WIM) es un formato de imagen de disco basado en fichero, lo cual quiere decir que la unidad más pequeña de información es el fichero, a diferencia de lo que ocurre con otros formatos basados en sectores de disco como pueden ser .ISO, .CUE .BIN, preferentemente utilizados para hacer imáge-

nes de CDs o DVDs. Básicamente, un fichero WIM contiene un conjunto de ficheros y los metadatos del sistema de ficheros en el que reside.

La principal ventaja de este formato es que la imagen será independiente del hardware, lo que supone que el administrador solo necesitará una imagen para implementar diferentes configuraciones de hardware. El formato WIM también permite almacenar varias imágenes dentro de un único fichero, las cuales serán referenciadas bien por un índice numérico o por un nombre único. Además, este formato de imagen permite compresión e instancias únicas, reduciendo el tamaño de la imagen significativamente.

También permite este formato, añadir o borrar componentes del sistema operativo, parches y nuevos drivers, sin tener que crear una nueva imagen, es decir, no hace falta arrancar el sistema operativo, aplicar el parche y realizar la nueva imagen. Esta característica se consigue debido a que las imágenes WIM pueden ser montadas en un directorio de la estructura del sistema de ficheros de la máquina sobre la que estamos trabajando. Microsoft ha publicado una API que permite manipular imágenes WIM, permitiendo a los desarroladores realizar sus propias utilidades de manipulación de imágenes. Por supuesto Microsoft tiene ya su propia utilidad que permite manipular dichas imágenes denomina ImageX.

Las imágenes WIM necesitan ser volcadas (desplegadas) a un volumen o partición existente, por lo tanto se necesita de alguna otra utilidad de bajo nivel que nos permita generar las particiones necesarias en nuestro disco duro y además formatearlas. Los sistemas operativos de Microsoft proporcionan una aplicación en línea de comandos denominada DiskPart que permite la creación de nuevos volúmenes (creación de la partición y del sistema de ficheros asociado).

Por tanto, con la inclusión del formato WIM y la herramienta ImageX, Microsoft, por fin posee un verdadero mecanismo de implantación de imágenes de Windows que serán de gran ayuda al administrador para poder realizar el despliegue de un número elevado de PCs.

Como conclusión podemos afirmar que una imagen WIM:

1. Es independiente del hardware, lo que significa que una misma imagen puede responder a diferentes configuraciones
2. Permite varias imágenes en un solo archivo
3. Un archivo base para todo el mundo (uno de 32 y otro de 64bits)
4. Comprime los archivos para ocupar menos espacio

5. Se puede ver la imagen sin conexión, incluso agregar y eliminar configuraciones, sin crear una imagen nueva

6. El formato de imagen WIM permite instalar una imagen de disco en particiones de cualquier tamaño, a diferencia de los formatos de imagen basados en sectores

7. Permite montar imágenes como carpetas

Hay que destacar que la instalación de Windows Vista, ya sea una actualización local o una instalación desde cero, es un proceso nuevo y basado por completo en imágenes. Tanto es así que el propio Windows Vista sólo se facilita en el formato de imagen WIM.

1.5. Entorno WAIK

La implementación o el despliegue de un sistema operativo en una organización consisten en su instalación masiva en todos los equipos. Las diferencias entre una implementación y una instalación sencilla son básicamente de escala. La implementación supone un gran esfuerzo ya que:

1. Se cuenta con una gran diversidad de sistemas

2. Hay que realizar numerosas pruebas

3. Hay que migrar datos y configuraciones de usuarios

Es recomendable hacer una implementación gestionada por los siguientes motivos:

1. Conseguir sistemas homogéneos con configuraciones limitadas

2. Reducir costes al centralizar y automatizar procedimientos

3. Conseguir mayor fiabilidad con sistemas fácilmente restituibles

Históricamente Microsoft ha proporcionado herramientas para ayudar en la implementación de sus operativos, como puede ser RIS, pero con Vista se han introducido muchos cambios y nuevas herramientas que son necesarias conocer.

Entre las nuevas características de la instalación de Windows Vista se incluyen las siguientes:

Tabla 1.1. Principales características de instalación de Windows Vista

Característica	Descripción
Windows Imaging (WIM)	Nuevo formato de archivo para imágenes.
ImageX.exe, Dism.exe	Comandos de manipulación de imágenes wim
Windows System Image Manager	Windows SIM es una herramienta gráfica para el mantenimiento de los archivos de imágenes de Windows (añadir paquetes y controladores) y creación de archivos de respuesta
Windows Preinstallation Environment (Windows PE)	Entorno de preinstalación de Windows. Es un mini sistema operativo que se puede arrancar desde CD, discos USB o por PXE y soporta todos los drivers de Vista, así como discos NTFS, redes, etc.
Windows Deployment Services (WDS)	Servicios de implementación de Windows que reemplazan a los servicios de instalación remota (RIS) en la implementación de Windows.
Unattend.xml	Nuevo formato de secuencia de comandos para todas las instalaciones basadas en imágenes de Windows Vista.
System Preparation (SysPrep)	Herramienta de preparación del sistema con un funcionamiento mejorado para operar con el diseño modular y la instalación basada en imágenes.

1.5.1. ImageX y Dism

Para crear y manejar los archivos de imágenes WIM, Microsoft proporciona una utilidad llamada ImageX. **ImageX** es una utilidad simple de línea de comandos que se ejecuta desde el símbolo del sistema o desde el entorno de preinstalación de Microsoft Windows (Windows Preinstallation Environment, Windows PE). En otras palabras, se interactúa con ImageX de la misma forma que con Xcopy. Las características principales de ImageX permiten capturar un volumen en un archivo WIM y aplicar un archivo WIM a un volumen.

Por ejemplo, para crear una imagen del disco C utilizaríamos el siguiente comando:

```
imagex /capture C: image.wim "Nombre"
```

Y para aplicarla a un volumen:

```
imagex /apply image.wim 1 C:
```

donde 1 indica a ImageX que debe aplicar desde un archivo image.wim la imagen que tenga el número de índice 1.

En WAIK para Windows 7 se ha introducido una nueva herramienta de linea de comandos que tambien permite manipular las imagenes wim, **Dism**. Su función básica es poder añadir nuevos paquetes y drivers a la imagen.

```
Dism /image:C:\winpe_x86\mount /Add-Package /PackagePath:"C:\Program \
Files\Windows AIK\Tools\PETools\x86\WinPE_FPs\winpe-wmi.cab"
DISM /image:c:\winpe_x86\mount /Add-Driver /driver:C:\INF_DRIVERS\ /recurse
```

1.5.2. Windows Automated Installation Kit (WAIK)

Windows Automated Instalation Kit, formalmente conocido como WAIK, es un entorno de desarrollo para la implantación y recuperación de sistemas Microsoft Windows. Con la puesta en el mercado de Windows Vista, Microsoft liberó su entorno de pre-instalación (WinPE) en el que se basan las instalaciones de Windows 7 y Windows Server 2008.

WinPE es una versión reducida de Windows XP, Windows Server 2003 o Windows Vista, utilizado por los fabricantes para el despliege masivo (deployment) de estaciones de trabajo o servidores.

Este kit de desarrollo que se puede descargar gratuitamente desde la siguiente URL
http://www.microsoft.com/downloads/details.aspx?FamilyID=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=en, permite a cualquier desarrollador o administrador de sistemas crearse un CD de arranque con todas las utilidades necesarias para poder implantar un nuevo sistema de Microsoft en una nueva maquina o para poder recuperar el sistema de un mal funcionamiento o por lo menos poder recuperar los datos importantes en algún recurso de red o soporte extraíble.

Actualmente existen tres versiones del kit de desarrollo WAIK. La última versión solo puede ser instalada sobre Windows Vista SP1 o Windows Server 2008, conocida también como WinPE 2.1.

WinPE 2.0 puede ser instalado tanto sobre el sistema operativo Windows XP o sobre Windows Server 2003.

1.5.3. Limitaciones de Windows PE

Windows PE es un subconjunto de Windows 7 y presenta algunas limitaciones.

Para reducir su tamaño, Windows PE sólo incluye un subconjunto de las API Win32 disponibles. Se incluyen las API Win32 de E/S (disco y red) y las principales.

Para evitar su uso como un sistema operativo, Windows PE detiene automáticamente la ejecución del shell y se reinicia tras 72 horas de uso continuo. Este período de tiempo no se puede configurar.

Windows PE no puede funcionar como un servidor de archivos o como un servidor de Terminal Server. (El escritorio remoto no es compatible).

La resolución de nombres del Sistema de archivos distribuido (DFS) sólo se permite para las raíces independientes. No se aceptan raíces de dominio.

Los métodos probados para lograr la conectividad de red a los servidores de archivos son TCP/IP y NetBIOS sobre TCP/IP. Otros métodos, como el protocolo de red IPX/SPX, no son compatibles.

Todos los cambios realizados en el Registro de Windows PE mientras se está ejecutando se pierden la próxima vez que se reinicia el equipo. Para que los cambios en el Registro sean permanentes, debe modificar el Registro sin conexión antes de iniciar Windows PE.

Las letras de unidad se asignan por orden consecutivo al crear las particiones en Windows PE; no obstante, las letras de unidad se restablecen al orden predeterminado al reiniciar Windows PE.

Windows PE no es compatible con Microsoft .NET Framework ni con Common Language Runtime (CLR).

Windows PE no incluye los subsistemas Windows on Windows 32 (WOW32), Windows on Windows 64 (WOW64), máquina DOS virtual (VDM), OS/2 o POSIX.

Para instalar una versión de 64 bits de Windows, debe usar una versión de 64 bits de Windows PE. Asimismo, para instalar una versión de 32 bits de Windows, debe usar una versión de 32 bits de Windows PE.

Windows PE se puede usar para configurar y crear particiones en los discos del equipo antes de iniciar el programa de instalación de Windows. Si alguno de los discos duros se convierte en un disco dinámico con Diskpart.exe antes de iniciar la instalación de Windows, esos discos duros se reconocerán como externos cuando se instale el sistema operativo y no se obtendrá acceso a ninguno de sus volúmenes.

Windows PE no es compatible con aplicaciones empaquetadas con Windows Installer (.msi).

1.5.4. Creación de un CD de arranque de WinPE

En esta guía se describe cómo crear un disco RAM de arranque de Windows PE en un CD-ROM con el script copype.cmd. La RAM de Windows PE permite iniciar un equipo con fines de implementación y recuperación. El CD de Windows PE arranca directamente en la memoria, lo que permite quitar el medio de Windows PE una vez que arranca el equipo.

Los pasos a seguir serían:

Paso 1: configurar un entorno Windows PE

1. Abrir la consola de WAIK, haciendo clic en Inicio, seleccione Todos los programas, AIK de Windows y, a continuación, haga clic en Símbolo del sistema de herramientas de Windows PE.

2. En el símbolo del sistema, ejecute el script copype.cmd. El script requiere dos argumentos: la arquitectura del hardware y la ubicación de destino.

```
copype.cmd <architecture> <destination>
<architecture> puede ser x86, amd64 o ia64
<destination> es una ruta de acceso al directorio local.
Por ejemplo: copype.cmd x86 c:\winpe_x8
```

3. El script crea la siguiente estructura de directorios y copia todos los archivos necesarios para dicha arquitectura.

```
\winpe_x86
\winpe_x86\ISO
\winpe_x86\mount
```

Paso 2: Personalizar el CD de arranque WinPE

Si queremos introducir cambios al CD de arranque WinPE, tenemos dos alternativas. Copiar el programa que deseemos en la carpeta c:\winpe_x86\iso el cual será incluido automáticamente en nuestro CD, pero nos obligará a mantenerlo siempre insertado, ya que no será uno de los programas residente en memoria.

Si necesitamos por alguna circunstancia que nuestro programa esté incluido en la imagen RAM del WinPE que se cargará en memoria, necesitamos montar esta imagen, copiar lo que necesitemos, desmontarla y volver a hacer el CD (la imagen iso):

```
imagex /mountrw c:\winpe_x86\winpe.wim 1 c:\winpe_x86\mount
copy “c:\WAIK\Tools\x86\imagex.exe” c:\winpe_x86\mount\Windows\System32
imagex /unmount c:\winpe_x86\mount /commit
```

Además de poder personalizar los contenidos de un CD de arranque WinPE, podemos alterar el proceso de arranque del mismo. Por defecto WinPE utiliza un script de arranque denominado startnet.cmd que llama a la utilidad winpeinit que se encarga de configurar el sistema (discos, red …). Por tanto, modificando dicho script, podemos introducir nuestras modificaciones para que automáticamente realice las tareas adecuadas.

Otra posibilidad es utilizar el script Winpeshl.ini el cual tiene el formato siguiente:

```
[LaunchApp]
AppPath = %SYSTEMDRIVE%\myshell.exe
[LaunchApps]
%SYSTEMDRIVE%\mydir\application1.exe, -option1 -option2application2.exe,
-option1 -option2
```

La variable AppPath define la shell por defecto. Este script tiene su interes cuando queremos personalizar nuestra imagen WinPE y que parezca un Windows de verdad.

Paso 3: Agregar paquetes adicionales

Con la herramienta Dism se instalan características de Windows. Las características de Windows se incluyen con la imagen base (Winpe.wim) pero no se instalan. También puede importar paquetes y agregar controladores y paquetes de idioma.

Agregue una característica de Windows a la imagen base con el comando peimg /install. Por ejemplo:

```
Dism /image:C:\winpe_x86\mount /Add-Package /PackagePath:"C:\Program \
Files\Windows AIK\Tools\PETools\x86\WinPE_FPs\winpe-wmi.cab"
```

Windows PE 2.1 incorpora las siguientes características de Windows conocidas como paquetes.

Tabla 1.2. Características de Windows incluídas en Windows PE 2.1

Característica	Descripción
WinPE-FONTSup-port-<región>-Packages	Compatibilidad con fuentes adicionales para ja-jp, ko-kr, zh-cn, zh-hk y zh-tw.
WinPE-HTA-Package	Compatibilidad con aplicaciones HTML
WinPE-MDAC-Package	Compatibilidad con Microsoft Data Access Components
WinPE-Scripting-Package	Compatibilidad con Windows Script Host
WinPE-SRT-Package	Componente Entorno de recuperación de Windows (disponible sólo en OPK de Windows)
WinPE-WMI-Packages	Compatibilidad con Instrumental de administración de Windows (WMI)
WinPE-XML-Package	Compatibilidad con Microsoft XML (MSMXL) Parser

Paso 4: Agregar drivers adicionales

El proceso que el administrador dispone para añadir nuevos drivers a la imagen WIM que estamos creando, es muy parecido al de agregar paquetes o características que vimos en el paso anterior.

En primer lugar montaremos la imagen en modo lectura/escritura para a continuación con el comando peimg, inyectar los drivers a esa imagen. Lo que hay que tener en cuenta, es que este procedimiento no funcionará con paquetes de drivers en formato .msi o .exe, estos deberán ser .inf

```
DISM /image:c:\winpe_x86\mount /Add-Driver
/driver:C:\YOUR_FOLDER_OF_INF_DRIVERS\
/recurse
```

Paso 5: Crear un CD-ROM de arranque

A continuación, habría que crear una imagen iso auto arrancable con el siguiente

comando:

```
oscdimg -n -bc:\winpe_x86\etfsboot.com \
c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso.
```

Arrancar la máquina de pruebas y comprobar que funciona la red, se detectan los diferentes discos etc.

1.6. Creación y despliegue de imágenes WIM

Paso 1: Creación de la instalación maestra

Podríamos definir a un ordenador maestro como una instalación de Windows personalizada que el administrador planea duplicarla a otros ordenadores.

Esa instalación maestra se puede generar automáticamente utilizando un fichero de respuesta y el DVD de Windows Vista.

El proceso básico para definir una instalación maestra se podría resumir en los siguientes pasos:

1. Ensamblar el hardware necesario.
2. Instalar Windows desde el DVD y ayudado por un fichero de respuestas. Instalación desatendida.
3. Personalizar y verificar la instalación.
4. Preparar la imagen y apagar el ordenador.

```
C:\Windows\System32\Sysprep\Sysprep.exe /oobe /generalize /shutdown
```

Paso 2: Creación de la imagen

El paso siguiente una vez construida la imagen maestra, sería capturar dicha imagen para poder aplicarla a diferentes PCs. Para conseguir dicho objetivo, los pasos básicos podrían ser:

1. Creación de un CD de arranque Windows PE.

2. Arrancar la instalación maestra con el CD de Windows PE.

3. Capturar la imagen de la instalación maestra utilizando la herramienta imagex:

```
imagex.exe /compress fast /capture C: C:\Myimage.wim \
"my Windows Install" /verify
```

4. Almacenar la imagen en un recurso de red:

```
net use y: \\server\sahre
copy c:\Myimage.wim y:
```

Paso 3: Despliegue de imágenes

1. En el ordenador destino, arrancaremos con el CD de Windows PE.

2. Una vez situados en la línea de comandos del Windows PE, deberemos formatear el disco para lo cual utilizaremos la herramienta de Microsoft Windows diskpart. Un ejemplo de creación de una partición primaria de 20GB sería el siguiente:

```
diskpart
select disk 0
clean
create partition primary size=20000
select partition 1
active
format
exit
```

3. A contiunuación copiaremos la imagen que habíamos capturado en el proceso de creación de imágenes a la unidad c.

```
net use Y: \\server\sahre
copy Y:\Myimage.wim c:
```

4. Por último quedaría la fase de implantación de la imagen en la partición recién creada del nuevo ordenador, gracias de nuevo a la herramienta imagex:

```
Imagex.exe /apply C:\Myimage.wim 1 c:
```

2

Administración de discos

Indice

2.1. Geometría de los discos duros

Los discos duros son el medio de almacenamiento masivo y permanente por excelencia en los ordenadores. Existen dos grandes grupos de discos en función de su interfaz con el ordenador, IDE y SCSI. En esencia, ambos grupos son equivalentes, salvo en aspectos de rendimiento, fiabilidad y precio. Difieren, eso sí, en laslimitaciones que el software de sistemas ha impuesto de formaartificial a los discos IDE en el mundo de los PCs.Un disco almacena su información en uno o más platos, disponiendo de una cabeza lectora para cada una de las dos caras del plato (aunque en algunas ocasiones una cara no es utilizada). Cada cara está dividida en varios anillos concéntricos, denominados pistas. Esta división es debida a que el plato gira sobre su eje, y la cabeza lectora se desplaza longitudinalmente hacia o desde el eje. A su vez, cada pista está subdividida en sectores, todos ellos de igual capacidad, 512 bytes en la gran mayoría de los casos. Todos los platos de un disco están unidos y también lo están entre si las cabezas lectoras. El conjunto de pistas que se encuentran bajo todas las cabezas lectoras recibe el nombre de cilindro. Resumiendo, la capacidad de un disco puede describirse indicando su número de cilindros, cabezales y sectores por pista. Por ejemplo, un disco con 4096 cilindros, 16 cabezales y 63 sectores por pista alberga un total de:

4096 x 16 x 63 = 4.128.768 sectores de 512 bytes

2.113.929.216 bytes

2.064.384 Kbytes

2.016 Mbytes =

1'96875 Gbytes.

Hay que tener en cuenta que el fabricante del disco dirá que su disco tiene 2^30 Gbytes. Los fabricantes de discos asumen que un Gbyte equivale a mil millones de bytes, no a 2^{30} bytes. Por cierto, los nuevos estándares dan la razón a los fabricantes, y nos indican que deberíamos utilizar los nuevos términos Kibytes, Mibytes, Gibytes para expresar las correspondientes potencias de 2. Sin embargo, en este documento no vamos a utilizar este estándar.

2.1.1. Límites a la geometría de los discos IDE

Existen diferentes límites a la geometría descrita que han sido impuestos (artificialmente) por el hardware o el software. Los tres más importantes se explican a continuación, seguidos de un apartado que comenta cómo se han superado hasta la fecha.

2.1.1.1. La especificación ATA

Según la especificación establecida por los fabricantes de discos duros, la forma de indicar al controlador del disco qué sector deseamos acceder es mediante su número de cilindro, de cabezal y de sector. La especificación también establece un número máximo de bits para cada valor, lo cual condiciona el número más grande de cilindros, cabezales y sectores que podemos direccionar. Este máximo número de bits es, para cada valor, el siguiente:

- Para el número de cilindro : 16 bits.
- Para el número de cabezal : 4 bits.
- Para el número de sector: 8 bits.

Por tanto, según la especificación ATA, un disco duro puede direccionar, como mucho:

65536 cilindros * 16 cabezales * 256 sectores por pista.

Si multiplicamos este número máximo de sectores por 512 bytes, el resultado es de 127'5 Gbytes, es decir, el tamaño teórico máximo de disco duro de la especificación ATA.

En el momento de escribir estas líneas, este límite está prácticamente a punto de alcanzarse, dado que ya se venden discos IDE de 100Gb de capacidad.

2.1.1.2. Las rutinas de disco clásicas de la BIOS

Algunos sistemas operativos antiguos para PC, como por ejemplo MSDOS, utilizan la BIOS como la forma natural de acceder a los discos, entre otros dispositivos. Es el mismo caso que muchos de los cargadores de los sistemas operativos actuales. En estos casos, el sistema operativo informa a la BIOS de qué número de sector desea acceder, y la BIOS traduce esta petición al controlador del disco, según la especificación ATA presentada anteriormente.

En este caso, la propia BIOS presenta al sistema operativo una interfaz de funciones en la que tiene también un número de bits reservados para direccionar el cilindro, cabezal y sector. La cantidad máxima de bits que las funciones ``clásicas'' de acceso reservaban para cada valor son las siguientes:

- Para el número de cilindro : 10 bits.

- Para el número de cabezal : 8 bits.
- Para el número de sector: 6 bits.

Por tanto, utilizando las rutinas tradicionales de la BIOS, un disco duro puede direccionar, como mucho:

1024 cilindros * 256 cabezales * 63 sectores por pista

El hecho de que el número de sectores por pista sea de 63 en vez de 64 proviene del hecho de que, según el mecanismo tradicional de direccionamiento de los discos (denominado CHS\footnote{Su nombre viene del acrónimo inglés *Cylinder-Head-Sector*, los sectores se numeran desde 1 en vez de numerarlos desde 0.

Multiplicando esta cantidad de sectores por 512 bytes, el valor resultante es de 7'84 Gbytes, que es el tamaño máximo de disco duro que reconocen esas BIOS tradicionales. Incluso en BIOS más modernas, que incorporan otras funciones de acceso, esa limitación sigue existiendo para el software que utiliza aquellas funciones clásicas para acceder al disco. Este es el caso, por ejemplo, del ancestral sistema DOS y, hasta hace poco tiempo, también de LILO, el cargador por excelencia del sistema operativo Linux.

2.1.1.3. La limitación conjunta de las dos anteriores

En un primer momento, la limitación real no fue la anterior, sino la limitación combinada de las dos anteriores. Es decir, puesto que los discos duros no pueden tener más de 16 cabezales (porque así lo han decidido los fabricantes), la limitación de la BIOS aún se restringía más, dando como resultado los siguientes números:

- Para el número de cilindro : 10 bits.
- Para el número de cabezal : 4 bits.
- Para el número de sector: 6 bits.

Es decir:

1024 cilindros * 16 cabezales * 63 sectores por pista.

Multiplicando por 512 bytes, esta cantidad de sectores permitía un total de \B{504 Mbytes}, una cantidad supuestamente inalcanzable en los años de los primeros sistemas para PC, pero que apenas 15 años después resultó claramente insuficiente.

2.1.1.4. Superando las limitaciones

La aparición de discos de más de 504 Mb, con más de 1024 cilindros, causó serios problemas, ya que millones de ordenadores con DOS instalado no podían utilizarlos directamente.

La forma de salvar esta primera limitación consistió en aprovechar que la BIOS permitía un número mayor de cabezales que la especificación ATA, aunque menos cilindros. Por tanto, el objetivo consistía en implementar a nivel de BIOS una traducción que, manteniendo inalterable el número máximo de sectores del disco, ofreciera al sistema operativo un número superior (ficticio) de cabezales (hasta 256) y un número proporcionalmente inferior de cilindros (hasta 1024). Internamente la BIOS realiza la traducción de ese número de sector virtual al número de sector real.

En este sentido, el modo de direccionamiento LBA (o Logical Block Addressing) resulta particularmente interesante. En este modo de direccionamiento, el controlador del disco ofrece a los niveles superiores la visión de que el disco está formado por un vector lineal de sectores. Por tanto, los tres valores que identifican un sector en el disco (cilindro, cabezal y sector) se especifican como un único número entre 0 y el número máximo de sector. A nivel de la especificación ATA, el número de sector sería un número de 28 bits (16 + 4 + 8). Al aparecer discos que permitían direccionamiento LBA, las BIOS fueron modificadas para utilizar también este modo y sus 24 bits de direccionamiento (10 + 8 + 6) se utilizaron para especificar un número lineal entre 0 y 2^24, que luego la BIOS pasa directamente al controlador del disco, permitiendo llegar naturalmente hasta el máximo de 7'84 Gb.

Finalmente, esa barrera de los 7'84 Gb se ha superado incluyendo nuevas funciones en las BIOS, con una especificación LBA que utiliza un número mayor de bits. De esta forma se puede llegar hasta el máximo de la especificación ATA.

2.1.2. Problemas causados por límites a la geometría IDE

Estas limitaciones en los discos típicos para PC han ocasionado limitaciones en algunos sistemas operativos. A continuación se revisan los sistemas más populares:

1. DOS, Windows 3.x, Windows 95, Windows NT 3.x. DOS utiliza las rutinas clásicas de la BIOS para acceder al disco. Por tanto, DOS no puede utilizar más de 1024 cilindros. El modo LBA es imprescindible y el tamaño máximo de disco soportado, tal como se ha explicado anteriormente, es de 7'84 Gbytes. Los sistemas Windows que aparecieron a continuación heredaron esta restricción de DOS por motivos de compatibilidad.

2. Windows 95 OSR2, Windows 98, Windows ME. No tienen ningún problema.

No utilizan las rutinas clásicas de la BIOS y por tanto pueden utilizar más de 1024 cilindros.

3. Windows NT 4.0. Este sistema tiene soporte para discos grandes desde su aparición. No obstante, el proceso de instalación de NT está basado en DOS, con lo cual, la partición donde reside NT debe estar antes de la barrera de los 1024 cilindros.

En resumen, en nuestros días apenas nos estamos librando de las restricciones que impuso el diseño original de la BIOS. Sólo en las últimas versiones de los sistemas operativos para PC, esas limitaciones no suponen un problema de instalación o de uso.

2.1.3. Particiones del disco

En el primer sector de un disco duro reside el denominado MBR (o Master Boot Record). En estos 512 bytes residen el código inicial de carga del sistema operativo, la tabla de particiones primarias y la firma del disco.

El código de carga más frecuente es el que define el sistema operativo DOS, el cual se encarga de buscar la partición de arranque, cargar en memoria el primer sector de dicha partición y cederle el control. Éste es el método utilizado por todos los sistemas operativos de Microsoft. Este código de carga puede recuperarse (reinstalarse) con el mandato DOS FDISK /MBR, el cual deja intacta la tabla de particiones.

Otros códigos de carga bastante utilizados son los cargadores que vienen con el sistema operativo Linux: LILO y GRUB. En realidad, el código que se ubica en el MBR es el correspondiente a la primera fase del proceso de arranque. Estos cargadores son más complejos y flexibles que el código de carga de DOS, y utilizan la información que reside en el directorio /boot de Linux para determinar qué sistema operativo debe cargarse.

El código de carga se utiliza tan sólo en el disco principal del sistema (es decir, el disco maestro del interfaz IDE primario). Hay BIOS que permiten arrancar de otros discos duros, pero generalmente aparecen numerosos problemas al utilizar esta opción.

La tabla de particiones está formada por cuatro entradas, donde cada una de ellas describe una potencial partición primaria. Los detalles de cada entrada son algo oscuros, y su utilización varía sensiblemente de un sistema operativo a otro. No obstante, simplificando un poco, cada entrada indica, para la partición que describe, la siguiente información:

1. El sector del disco donde comienza.
2. Su tamaño.
3. Si es una partición de arranque (activa).
4. Su tipo.

DOS, Windows 3.x y Windows 95 representan el inicio de la partición utilizando la tripleta <cilindro,cabezal,sector>, con lo cual el tamaño máximo de una partición es de 7'84 Gbytes (debido a la limitación de los 1024 cilindros). El resto de sistemas representan el inicio de la partición indicando cuál es el sector lógico donde comienza (viendo al disco como un vector de sectores lógicos). Estos sistemas utilizan una palabra de 32 bits, lo que permite 2^32 sectores, equivalente a 2 Tbytes (2 x 1024 Gbytes). En este caso, aún estamos algo lejos de disponer de discos de estas características.

El indicador de partición de arranque es utilizado tan sólo por el código de carga de DOS. Linux ignora por completo esta información.

Existen numerosos tipos de particiones, en función de su utilización o de su organización interna (establecida por el sistema operativo que la defina). Existe una convención que establece el identificador de cada tipo de partición como un número concreto en hexadecimal. La siguiente abla expone los tipos de particiones más habituales.

Tabla 2.1. Principales tipos de particiones

Tipo	Uso	Limitación
0	Partición vacía	
5	Partición extendida	1024 cilindros (7'84GB)
6	DOS FAT 16	2 GB
7	OS2 o NTFS	2TB
b	Windows 95 FAT 32	2TB
f	Extendida Windows 95	2TB
80	Old Minix	-
82	Linux Swap	-
83	Linux Native	2TB

Una partición extendida es un contenedor para otras particiones, a las cuales se les denomina particiones lógicas. Sólo una de las particiones primarias puede declararse como extendida. La representación de las unidades lógicas se realiza utilizando una lista enlazada que reside dentro de la partición extendida, por lo que no hay

límite en cuanto al número de particiones lógicas que se pueden crear. La partición extendida convencional ha tenido que ser cambiada por la nueva partición extendida Windows 95, ya que la primera no puede abarcar discos mayores de 7'84 Gbytes.

2.2. La consola de administración de discos

La herramienta típica para manejar discos y particiones en el entorno windows, siempre ha sido *FDISK*. Cuando el sistema posee múltiples discos, esta utilidad suele traer muchos quebraderos de cabeza al administrador.

En el proceso de instalación de un sistema windows 2008, se solicita la creación, borrado y formateado de particiones, como paso previo a la definición de un sistema de ficheros. La utilidad encargada de ello se denomina *DISKPART* (ver sección...).

Una vez arrancado el sistema la consola de administración de discos, será la principal utilidad para manejar los discos físicos y lógicos de nuestra máquina. La Consola de Administración de Discos puede ser utilizada por usuarios miembros del grupo Administradores. Esta herramienta se utiliza tanto para configurar nuevos discos, como para administrar la tolerancia a fallos de los mismos.

Para ejecutar la Consola de Administración de Discos, sigue los siguientes pasos:

1. En el menú Inicio, selecciona Programas.
2. En Programas, selecciona Herramientas Administrativas.
3. En Herramientas Administrativas, selecciona Administración de Equipo.

2.2.1. Configuración de la consola

La Consola es una herramienta altamente configurable. Muestra de una forma visual el tamaño y el tipo de las particiones para poder identificarlas fácilmente.

La Consola de Administración de Discos tiene dos paneles configurados por defecto para mostrar en el superior la lista de dispositivos extraíbles, discos, cd-rom, mientras que el inferior muestra una vista gráfica y coloreada de las particones, conjuntos espejo, seccionados etc ...

Para poder personalizar la Consola de Administración de Discos, sigue los siguientes pasos:

1. En el menú, seleccionar Ver.

2. Desde aquí se puede seleccionar lo que queremos ver, tanto en el panel superior como en el inferior. Las elecciones pueden ser las siguientes:

- Lista de discos: muestra todos los dispositivos en forma de lista.
- Lista de Volúmenes: es la vista por defecto en el panel superior.
- Vista Gráfica: vista por defecto en el panel inferior.

2.2.2. Discos básicos y dinámicos

En Windows 2008 disponemos de dos tipos de almacenamiento:

1. Básico:

   Discos orientados a particiones, que es el sistema tradicional del PC. El disco puede contener particiones primarias y extendidas, y dentro de estas últimas volúenes lógicos. Todos los sistemas anteriores a Windows 2008 pueden ver este tipo de disco.

2. Dinámico:

   Se trata de una novedad de Windows 2008 para dar soporte a sistemas tolerantes a fallos mediante el uso de varios discos. Los discos no se organizan en particiones sino en volúmenes, superando esta nueva organización las restricciones tradicionales del sistema de particiones del PC. Con el almacenamiento dinámico, los cambios en los discos surten efecto en el sistema sin necesidad de reiniciar el equipo. Por el contrario, no pueden contener particiones y por tanto no son accesibles desde versiones anteriores de Windows ni desde MS-DOS.

   Se administran con el servicio LDM (Logic Disk Manager) y el controlador dmio.sys.

   Todos los discos dinámicos forman parte del grupo de discos de la máquina. La información de los discos dinámicos se encuentra guardada en un espacio reservado en los propios discos, y no en el registro como en la versión anterior de Windows NT. De este modo, si se lleva el disco a otra máquina, la máquina destino sabe que ese disco estaba en otra máquina y podráa acceder a la información pues los metadatos están en el mismo disco. En la máquina origen, se reconoce la falta del disco pues en el resto de discos dinámicos se tiene la infor-

mación referente a este disco.

No obstante, Windows 2008 es compatible con los conjuntos de volúenes de Windows NT. Dispone del controlador FTDISK de modo que reconoce los conjuntos de volúmenes que NT creaba sobre particiones en discos básicos.

Visto lo anterior, cuando se quiera destinar un nuevo disco en el sistema para crear particiones y unidades lógicas se utilizará en modo básico. Si se desea crear un sistema tolerante a fallos, se inicializará el disco en modo dinámico.

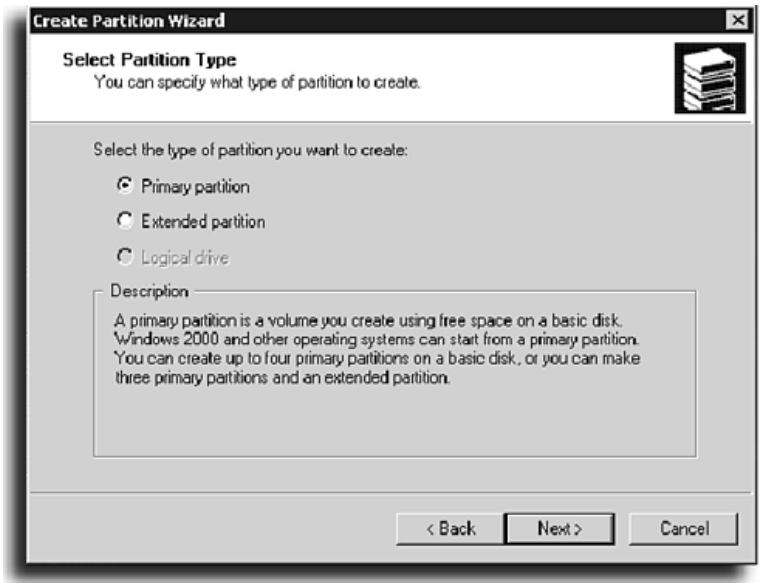
Un disco puede pasar de dinámico a básico y viceversa, pero cuando el disco contiene datos, se deben tener en cuenta ciertas restricciones que se detallan en el apartado Actualización de discos básicos a dinámicos, más adelante en este capítulo.

2.2.3. Creación de particiones

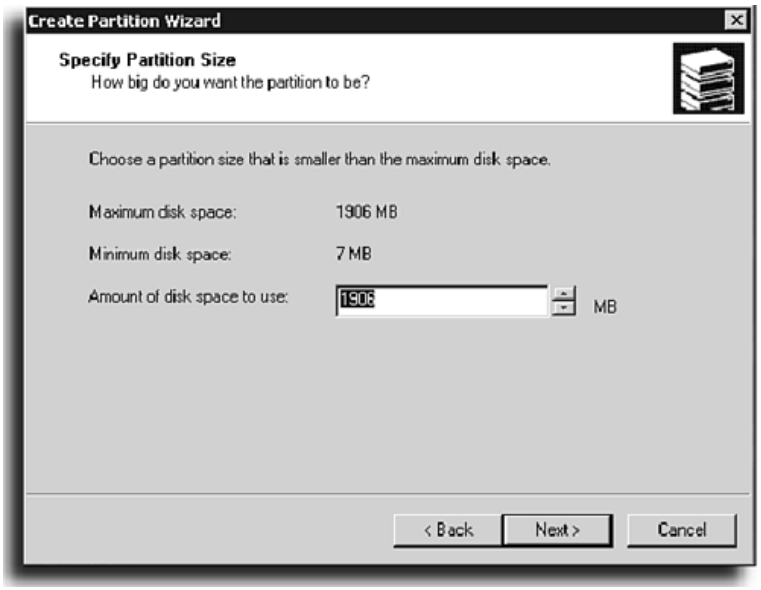
Antes de crear una partición se necesita saber que tipo de partición queremos: primaria, extendida o lógica. Los pasos necesarios para poder crear una partición se detallan a continuación:

1. Abrir la Consola de Administración de Discos.
2. Selecciona el disco sobre el que crear la partición y que dispone de espacio libre.
3. Con el botón derecho del ratón, selecciona Crear Partición.

4. En el cuadro de dialogo que aparece, selecciona el tipo de partición (primaria,extendida,lógica). Si es sobre un espacio libre las únicas opciones que nos aparecerán son primaria y extendida. Si es sobre una partición extendida, solo aparecerá tipo de partición lógica.



5. A continuación se selecciona el tamaño de la partición.



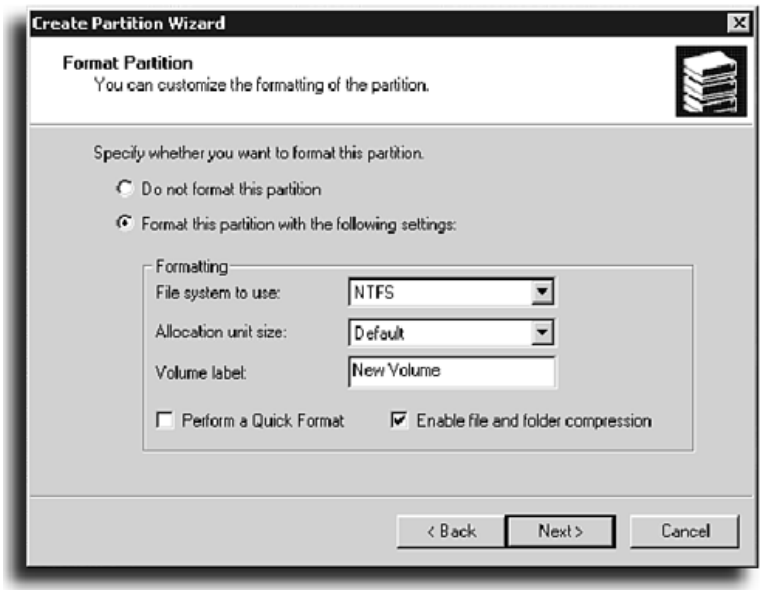
6. El siguiente paso sería asignar a la partición un punto de montaje (letra de unidad o Path). Windows 2008 trata a los volúmenes como unidades de almacenamiento que pueden o no encontrarse en el espacio de nombres del almacenamiento del sistema. Para que los volúmenes sean accesibles, se han de montar en el espacio de nombres. Los puntos de montaje son estáticos, es decir, una vez asignado, el volumen mantiene su ruta de acceso.

   Una letra de unidad hace accesible la partición al modo tradicional de MS-

DOS. Todos los datos del volúmen se encuentran accesibles partiendo de la letra que se ha asignado. Windows 2008 permite asignar 26 letras, de las que la A y la B están reservadas para unidades de disquete, y de la C a Z al resto. Las letras de las particiones del sistema o de arranque no pueden ser modificadas. Además, solo puede asignarse una letra.

Asignando al volumen un punto de montaje en una carpeta vacía de otro volúmen ya montado, el volúmen se hace accesible a partir de esa carpeta. Los volúmenes pueden montarse en cualquier carpeta de un volúmen formateado con NTFS de Windows 2008, de un disco tanto básico como dinámico. La unidad montada puede estar formateada con cualquier sistema de archivos soportado por Windows 2008.

7. El último paso consistirá en decidir que sistema de ficheros (formato) queremos asignar a la partición a crear. También está la posibilidad de no formatearla en este instante.



Este proceso al final mostrará un sumario de las acciones que se van a llevar a cabo. Hacer notar que si se decide formatear la partición, este proceso se realizará en un segundo plano.

2.2.4. Creación de volúmenes

Los volúmenes aparecen en Windows 2003 gracias a la nueva gestión de los discos. Solo están disponibles en discos dinámicos, y dan posibilidad de disponer de tolerancia a fallos. Un volúmen de disco es una porción de disco duro que funciona como si se tratase de un disco físico independiente. El volúmen puede estar formado por una sola porción de un disco duro o por varias porciones del mismo disco o varias porciones de varios discos duros.

Los volúmenes de Windows 2008 pueden ser de varios tipos:

- Simple: Unico tipo posible si solo disponemos de un disco en modo dinámico.
- Distribuido
- Seccionado.
- De espejo.
- RAID-5

2.2.4.1. Volumen simple

Se trata de un volúmen formado por una o varias porciones del mismo disco. Solo pueden crearse en discos dinámicos y se pueden reflejar, aunque no soportan más opciones de tolerancia a fallos. Los volúmenes simples son lo mas parecido a las particiones en los discos básicos.

Los volúmenes simples pueden extenderse añdiendo porciones del mismo disco o de otros discos, pero no se puede reducir su tamaño una vez extendido ni eliminar porciones que se añadieron, sólo se podrá eliminar el volúmen completo. Un volúmen simple puede extenderse por otros discos hasta ocupar un máximo de 32 discos dinámicos.

2.2.4.2. Volumen distribuido

Se trata de un volúmen formado por varias porciones de varios discos. Sólo pueden crearse en discos dinámicos y no soportan opciones de tolerancia a fallos.

Los volúmenes distribuidos se pueden extender añadiendo porciones del mismo disco. Al extender un volúmen distribuido, ocurrirá igual que en los simples, que no se podrá desasignar espacio. Se corresponden con los conjuntos de volúmenes de Windows NT.

2.2.4.3. Volumen seccionado

Volumen que esta formado por un conjunto de porciones o bandas de igual tamaño (64 Kbytes) de varios discos, hasta un máximo de 32 discos. La información se reparte entre las bandas de los distintos discos. El reparto de información es equitativo y alternativo, ocupando de este modo todas las bandas o porciones de los discos integrantes. Como resultado, el rendimiento de E/S es mas alto.

Los discos no tienen por qué ser del mismo tamaño, pues lo que es igual son las bandas que se crean en los discos. Además, no pueden variar de tamaño una vez creados.

Estos volúmenes sólo pueden crearse en discos dinámicos y no ofrecen tolerancia a errores si no todo lo contrario. Si uno de los discos, o una banda, tuviese errores, el volúmen completo falla y la información se pierde. Se corresponde con lo que en Windows NT se conocía como conjunto de bandas (RAID 0). La fiabilidad de este sistema es siempre menor que la fiabilidad del disco menos fiable.

Los volúmenes seccionados son el sistema de almacenamiento que ofrece el mejor rendimiento de todos los tipos de volúmenes de Windows 2008, tanto en escritu-

ra como lectura, por lo que se puede escoger por su rendimiento.

2.2.4.4. Volumen reflejado

Volúmen tolerante a fallos que utiliza un segundo espacio de almacenamiento físico de igual tamaño donde duplica toda la información del volumen. Aunque el tamaño utilizado en los dos discos es el mismo, los discos no tienen porqué tener el mismo tamaño físico, ni en número de cilindros, etc...

Las dos copias siempre deben encontrarse en dos discos distintos, y preferentemente en controladoras de disco distintas, a este mecanismo se le denomina duplexación. Si uno de los discos fallase, el sistema se repondrá utilizando la copia. Esto es recomendable, por ejemplo, para el volumen del sistema. Además, desde el disco de reparación de emergencia, se puede arrancar de una copia en espejo. Como inconveniente, el espacio útil de disco se reduce en un 50%.

Sólo pueden crearse en discos dinámicos. Se corresponde con lo que en Windows NT era el conjunto de espejos (RAID-1). Son más lentos a la hora de escribir, puesto que se han de realizar las escrituras por duplicado. Esto puede mitigarse con la duplexación.

Para reflejar el volúmen, es necesario que en el sistema exista al menos otro disco en modo dinámico, además del que queremos reflejar. En ese momento, pulsando con el botón derecho sobre el volúmen, el sistema ofrece la posibilidad de reflejarlo utilizando espacio no asignado de alguno de los discos.

Para eliminar un volumen reflejado tenemos dos opciones:

- Romper el espejo: Esta opción descompone el volúmen reflejado dividiéndola en dos volúmenes independientes. Como resultado tenemos dos volúmenes idénticos en tamaño y con la misma información en ambos, pero ya no están reflejados.
- Quitar un espejo: Esta opción libera una de las dos copias integrantes del espejo, dejando el espacio que ocupaba tal copia como no asignado. La otra copia sigue funcionando, pero ahora no está reflejada.

2.2.4.5. Volumen RAID-5

Volúmen formado por bandas o porciones de tres o más discos duros, hasta 32 discos. En estos volúmenes, a los datos se les añade un información de paridad que servirá de código de detección y corrección de posibles errores. Los datos y la paridad se escribe de forma alterna entre el conjunto de bandas del volúmen.

La banda de paridad se calcula utilizando una función OREX del resto de bandas de datos.

Los volúmenes de RAID5 son tolerantes a fallos. Si un disco o una banda contiene errores, Windows 2008 puede reconstruir la información perdida a partir de los datos que quedan en las otras bandas junto con la paridad. El sistema puede por tanto soportar la perdida de un disco sin perdida de datos, ya que el volumen continua en línea.. No obstante, a partir del momento de la recuperación, el sistema es propenso a fallos hasta que se cambia el disco averiado o se rompe el RAID. En una operación de lectura, solo se lee la banda donde se encuentran los datos. Solo es necesario leer una banda para saber si existe o no error. Si el sistema detecta un error en la banda que ha leído o un error en el disco, leerá el resto de bandas de datos y la banda de paridad, con lo que podrá reconstruir la banda dañada. Si el error se produce en la banda de la paridad no es necesaria la reconstrucción.

No toda la capacidad de un volúmen RAID5 esta disponible para guardar datos, puesto que siempre una de las bandas se destina a guardar los datos de paridad. El tamaño disponible dependerá del número de discos que componen el RAID5, como siempre se destina una banda a la paridad, al incrementar el número de discos del RAID5 aumenta el espacio de almacenamiento útil disponible. En la figura se puede observar una configuración RAID5 con 3 discos. En cada disco, se utilizan porciones del mismo tamaño (20 Mbytes) . El tamaño total del volumen es de 40 Mbytes, y no 60 Mbytes, pues una de las bandas se destina a paridad.

Si el volúmen estuviese formado por 4 discos y también con 20Mbytes por banda, el tamaño de disco disponible hubiese aumentado hasta 60Mbytes, pues se seguirán ocupando 20Mbytes para la paridad. Los volúmenes RAID5 sólo pueden crearse en discos dinámicos y no pueden reflejarse ni extenderse. Además, no se puede instalar el sistema en un volumen RAID5.

Los volúmenes RAID5 consumen mas memoria del sistema. Su uso es para información importante que en la medida de lo posible no sea muy cambiante, pues el rendimiento en escrituras es peor.

2.3. Utilidades

2.3.1. Diskpart

Diskpart es una utilidad que proporciona Microsoft para realizar la gestión de discos desde la línea de comandos. Soporta, mediante comandos o mediante el paso de un script de comandos, operaciones sobre los discos del sistema.

```
diskpart [ /s script]
```

2.3.1. Diskpart

Los comandos de diskpart funcionan sobre: un disco, una partición,un volúmen

Los comandos emitidos se realizan sobre el foco , que es un objeto de uno de los tipos anteriores seleccionado mediante el comando Select. Por tanto, este es el primer comando que se debe utilizar para determinar donde se realizaran los comandos siguientes.

La sintáxis de Select es la siguiente:

```
Select [ volume | partition | disk ] [ = numero]
```

Todos los comandos requieren la selección del foco, a excepción de:

- List [disk | volume | partition] :Lista los discos, volúmenes y particiones.
- Help: Visualiza la ayuda de la herramienta.
- Rem: Introducir comentarios en los scripts de diskpart.
- Exit: Salir de la consola.
- Rescan: Fuerza a volver a buscar discos en el sistema.

El resto de comandos que admite diskpart es siempre sobre el foco, de entre ellos podemos destacar:

- Active: Hacer activa la partición foco.
- Assign [letter=letra | mount=ruta] [noerr]: Asignarle un punto de montaje.
- Remove [letter=letra | mount=ruta | all] [noerr]: Eliminarle un punto de montaje.
- Create: Crear una partición en el disco foco.
- Delete: Eliminar la partición foco.
- Extend [size=n] [noerr]: Extender el volumen foco.
- Add: Agregar un espejo al volumen simple foco.
- Break: Dividir o Romper el espejo del volumen foco.
- Convert: Para pasar de modo dinámico a básico.

Los códigos de error que puede dar diskpart son:

- 0: "Sin errores. Toda la secuencia de comandos se ejecutó sin errores."
- 1: "Excepción fatal. Puede haber un problema grave."
- 2: "Argumentos incorrectos especificados en una línea de comandos de Diskpart."
- 3: "DiskPart no pudo abrir la secuencia de comandos o el archivo de salida especificados."
- 4: "Uno de los servicios que utiliza DiskPart ha devuelto un error."
- 5: "Error en la sintaxis de un comando. Error en la secuencia de comandos porque un objeto se seleccionó incorrectamente o su uso no era válido en dicho comando."

2.4. Sistemas de ficheros

Cuando apareció Windows NT 3.1 en 1993, Microsoft utilizó las capacidades avanzadas del sistema de ficheros HPFS (High Performance File System) previamente utilizado en Microsoft/IBM OS/2, para crear el sistema de ficheros NTFS. La parte principal del modelo de seguridad que ofrece W2008 está basada en NTFS. Aunque los recursos compartidos se pueden configurar en W2008 sin tener en cuenta el sistema de ficheros subyacente, solo con NTFS se pueden asignar permisos a ficheros individuales.

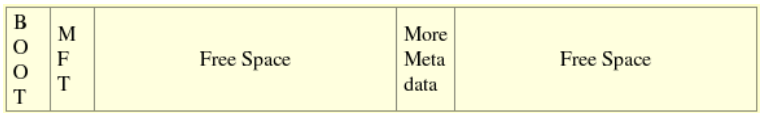
Aunque W2008 soporta varios sistemas de ficheros (FAT,FAT16,FAT32,NTFS), NTFS es el sistema preferido ya que permite utilizar todas las características de seguridad avanzadas.

Aviso

W2008 no utiliza NTFS para formatear un floppy disk, debido a la cantidad de información necesaria para crear el sistema de ficheros y que excedería la capacidad de un disquete

Un volúmen NTFS almacena la información sobre descriptores de ficheros en una tabla de ficheros maestra (MFT), la cual es asu vez un fichero. A parte de varios registros que contienen información sobre la propia MFT, esta contiene un registro por cada fichero y directorio del sistema La MFT también contiene un fichero de log. Se mantiene en el propio sistema de ficheros una copia de la MFT. Enlaces a la MFT

y su copia están almacenados en el sector de inicio del disco. Una copia del sector de inicio se almacena en el centro del disco. Al mantener tanta información replicada, la recuperación de los datos de un sistema de ficheros NTFS es mucho más fácil. La estructura de un sistema NTFS se puede apreciar en la siguiente imagen:

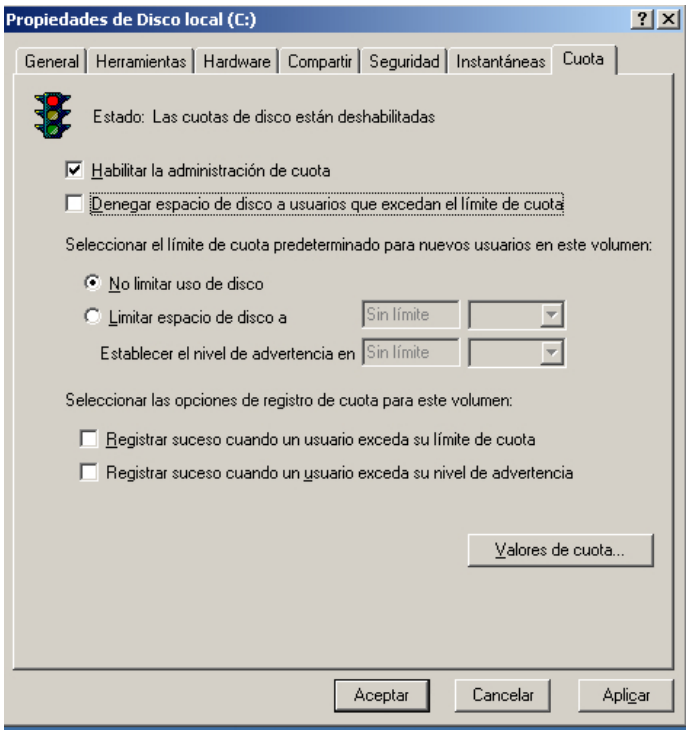


2.5. Cuotas de disco

Cuando se trabaja con cuotas de disco, se puede empezar definiendo una cuota por defecto para cada volúmen y luego ir ajustando individualmente las cuotas de usuario según se necesiten. Definiendo una pequeña cuota por defecto y luego ajustaándola según las necesidades es la forma más eficiente de abordar el problema de las cuotas.

2.5.1. Habilitar cuotas

Para empezar a trabajar con cuotas de disco en Windows Server 2008 hay que habilitar el soporte de cuotas sobre un volúmen. Si presionamos el botón derecho del ratón sobre el volúmen y accedemos a Propiedades, la lengüeta Cuotas nos permitirá definir todas las opciones posibles.



Seleccionaremos **Denegar espacio de disco a usuarios ...** si queremos prevenir que el usuario pueda escribir en el disco cuando alcance su cuota. En caso contrario, los usuarios serán advertidos de que llegan al límite de la cuota.

El administrador puede definir dos valores para las cuotas:

1. **Limitar espacio de disco a**:

   Define la cantidad de espacio en disco que un usario tiene permitido utilizar.

2. **Establecer el nivel de advertencia en**:

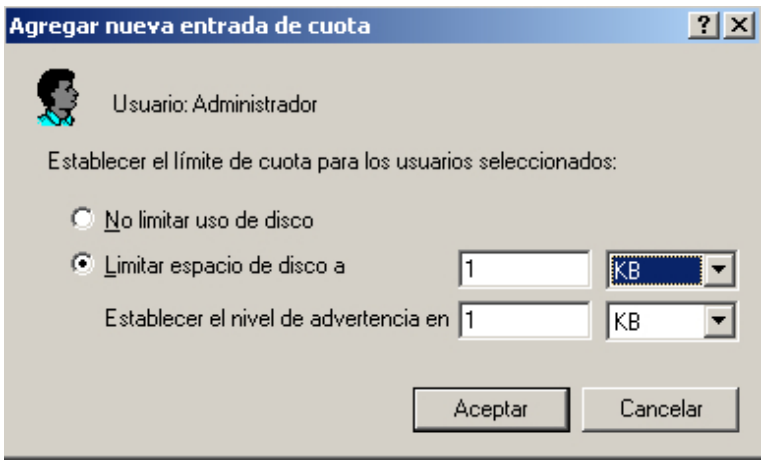
   Cuando se alcance este límite, el sistema avisará al usuario de que está cerca de alcanzar la cuota de disco asignada.

Estas dos opciones permiten introducir un número y la unidad de medida asociada a las cuotas. Estas unidades de medida que se muestran en el desplegable, se generan dinámicamente segun la capacidad del volúmen.

En esta misma pestaña, tenemos la posibilidad de registrar eventos de cuotas, bien cuando se alcanza la cuota o cuando se produce la advertencia.

2.5.2. Definición de cuotas individuales

Tenemos la capacidad de definir cuotas por usuario, habilitandole para que exceda el límite por defecto definido para el volúmen. También podemos definir usuarios que no tengan ningún límite de cuotas.



2.6. Copias de seguridad

La herramienta de copia de seguridad que viene instalada en la familia de servidores Windows 2008 proporciona al administrador las utilidades necesarias para copiar todos los datos importantes del sistema o el sistema entero. Con esta nueva versión, el administrador puede respaldar su sistema en un fichero en otro disco, en un recurso de red y por supuesto en cinta. La herramienta es fácil de usar y configurable, proporcionando wizards que guiarán al administrador en la complicada tarea de respaldar el sistema.

Algunas de las características de ntbackup son más útiles bajo windows 2008 Server, ya que permite copiar partes del Directorio Activo, por ejemplo. O también es posible habilitar el Servicio de almacenamiento remoto que permite planficar las copias de seguridad de una pequeña red de area local. Entre las funciones básicas de ntbackup están:

- Creación del disco de reparación de emergencia
- Hacer copias del estado del sistema: registro, ficheros de arranque y bases de datos del Servicio de Certificados.

Como pasa con la mayoría de herramientas de Windows 2008, el usuario debe de tener los privilegios necesarios para usarla. Para poder copiar y restaurar cualquier fichero o carpeta del sistema local el usuario debe pertenecer al grupo Administradores o al grupo Operadores de Copia de Seguridad. Si no eres miembro de uno de estos grupos.

Puede utilizar Windows Server Backup de seguridad para proteger el sistema operativo, el estado del sistema, los volúmenes, archivos y datos de aplicación. Las copias de seguridad se pueden guardar en discos únicos o múltiples, en volúmenes individuales o múltiples, DVDs, medios removibles, o carpetas compartidas. Pueden ser programados para ejecutarse de forma automática o manualmente.

Puede crear una copia de seguridad utilizando el Asistente para copia de seguridad de la Lista de copias de seguridad para permitir que se ejecute en un horario regular o utilizando el Asistente para copia de seguridad que ejecute una copia de seguridad de una sola vez. Puede acceder a estos dos *wizars* a través del complemento Windows Server de Microsoft Management Console (MMC). También puede crear copias de seguridad periódicas utilizando el comando **Wbadmin** o Windows PowerShell cmdlets de Windows Server Backup.

Windows Server Backup crea copias de seguridad completas que le permiten rea-

lizar la recuperación de su ordenador sin necesidad de hacer referencia a otra copia de seguridad. Sin embargo, estas copias de seguridad se han optimizado para comportarse como copias de seguridad incrementales, para aumentar el rendimiento de copia de seguridad y ahorrar espacio. Además, si utiliza un disco o volumen para almacenar copias de seguridad, Windows Server Backup elimina automáticamente copias de seguridad antiguas a medida que el almacenamiento se llene.

Además de la copia de seguridad, esta carpeta incluye archivos de catálogo que contiene información sobre todas las copias de seguridad en ese lugar hasta la copia de seguridad actual, y un archivo, *Mediaid*, que contiene el identificador de la ubicación de almacenamiento de copia de seguridad. Esta información es necesaria para llevar a cabo una recuperación.

2.6.1. Qué copiar

Como parte de la creación de una copia de seguridad, tendrá que especificar los archivos, carpetas o volúmenes que desea incluir. Los elementos que seleccione en una copia de seguridad, tendrán un impacto en lo que puede recuperarse.

No se puede utilizar Windows Server Backup para copias de seguridad de archivos y carpetas en los volúmenes que requieren más de 2040 GB (o 2 TB). Sin embargo, siempre y cuando el tamaño de los datos es menor de 2 TB, puede realizar copias de seguridad de un archivo o carpeta. Por ejemplo, usted puede hacer copias de seguridad de 1,5 TB de datos desde un volumen de 3-TB. Pero, un servidor completo o la recuperación de volúmenes utilizando la copia de seguridad volverá a crear un volumen de 2 TB en lugar de un volumen de 3-TB.

Disponemos de las siguientes opciones:

1. **Servidor Completo**:

   Realiza una copia de todos los volúmenes si desea ser capaz de recuperar el servidor completo. Puede utilizar una copia de seguridad completa del servidor para realizar todo tipo de recuperaciones, incluyendo el estado del sistema y recuperación de *baremetal*. Le recomendamos esta opción.

2. **Volúmenes críticos**:

   Elija crear una copia de seguridad para la recuperación de *baremetal* si desea realizar una copia de los elementos necesarios para recuperar el sistema operativo (volúmenes críticos solamente). Esta opción es un subconjunto de una copia de seguridad completa del servidor.

3. **Estado del Sistema**:

   Elija una copia de seguridad del estado del sistema si desea realizar una copia de los elementos necesarios para realizar una recuperación del estado del sistema. Esta opción es un subconjunto de una copia de seguridad completa del servidor.

4. **Volúmenes individuales**:

   Copias de seguridad de volúmenes individuales sólo si desea ser capaz de recuperar archivos, aplicaciones o datos de los volúmenes

5. **Carpetas o ficheros**:

   Copias de seguridad de carpetas o archivos individuales sólo si desea ser capaz de recuperar esos elementos.

2.6.2. Lugar de Almacenamiento

También tendrá que especificar una ubicación para almacenar las copias de seguridad que crea. El tipo de ubicación de almacenamiento que usted elija tendrá un impacto en lo que puede recuperarse.

El tamaño de la ubicación para almacenar copias de seguridad debe ser como mínimo 1,5 veces el tamaño de copia de seguridad que le permiten almacenar un par de versiones de copia de seguridad.

No se puede utilizar unidades de cinta como ubicación de almacenamiento de copia de seguridad para Windows Server Backup. Sin embargo, los *drivers* de almacenamiento en cinta todavía están incluidos en Windows Server 2008 y Windows Server 2008 R2.

No se puede almacenar copias de seguridad en discos con formato FAT32, los discos deben presentar el formato NTFS porque Windows Server Backup utiliza instantáneas para mantener versiones de copia de seguridad. Usted puede utilizar el comando *Format* para formatear el disco o el comando *Convert* para cambiar el formato.

No puede almacenar copias de seguridad en las unidades flash USB o pen drives.

Los diferentes medios de almacenamiento de las copias de seguridad se detallan a continuación:

1. **Recurso compartido:**

   Se pueden almacenar copias de seguridad únicas y copias de seguridad programadas en carpetas compartidas. (La capacidad para almacenar copias de seguridad programadas en carpetas compartidas es una característica nueva en Windows Server 2008 R2.) Por tanto, puede utilizar copias de seguridad almacenadas en carpetas compartidas para recuperar archivos, carpetas, estado de sistema, aplicaciones y volúmenes completos-o para realizar recuperación de *baremetal*.

   Si guarda la copia de seguridad en una carpeta compartida remota, la copia de seguridad se sobrescribirá cada vez que cree una nueva copia de seguridad. No seleccione esta opción si desea almacenar varias copias de seguridad. Además, si crea una copia de seguridad en una carpeta compartida que ya contiene una copia de seguridad, si el proceso de copia de seguridad falla, usted puede ser que se queden sin las copias de seguridad.

2. **DVD o medios removibles:**

   Puede almacenar copias de seguridad únicas (no copias de seguridad programadas) en medios ópticos o removibles. A continuación, puede utilizar copias de seguridad almacenadas en soportes ópticos o removible para llevar a cabo una recuperación de un volumen o baremetal.

   No se pueden recuperar las aplicaciones, archivos individuales, o el estado del sistema de copias de seguridad almacenadas en soportes ópticos o removibles. Las copias de seguridad almacenadas en discos DVD se comprimen y ocupan menos espacio que las copias de seguridad guardados en el disco duro.

3. **Disco duro interno:**

   Puede almacenar copias de seguridad programadas en un disco con formato NTFS o una tabla de particiones GUID (GPT). Sin embargo, si almacena copias de seguridad programadas en un disco interno, tiene la opción de dedicar ese disco para el almacenamiento de backup. Pir tanto, el disco que elija será dedicado para almacenar sus copias de seguridad programadas y no será visible en el Explorador de Windows.

   Puede utilizar las copias de seguridad almacenadas en discos internos para recuperar los archivos, carpetas, aplicaciones y volúmenes, realizar la recuperación desde cer, realizar la recuperación del estado del sistema si la copia de seguridad utilizada contiene el estado del sistema.

4. **Disco duro externo:**

Se puede guardar la copia de seguridad en el disco duro externo con formato NTFS o GPT. Podemos recuperar los archivos, carpetas, aplicaciones y volúmenes. Recuperar el estado del sistema y el sistema operativo (baremetal), si la copia de seguridad utilizada contiene los elementos necesarios. Sin embargo, como con los discos internos, tiene la opción de dedicar el disco de almacenamiento de manera que no aparecerá en el Explorador de Windows.

3

Protección local en Windows Server 2008

Indice

3.1. Concepto de usuario

Como muchos otros sistemas operativos, Windows Server 2008 permite tener un riguroso control de las personas que pueden entrar en el sistema y de las acciones que dichas personas están autorizadas a ejecutar.

Windows Server 2008 denomina *usuario* a cada persona que puede entrar en el sistema. Para poder controlar la entrada y las acciones de cada usuario utiliza básicamente el concepto de *cuenta de usuario* (*user account*). Una cuenta de usuario almacena toda la información que el sistema guarda acerca de cada usuario. De entre los numerosos datos que Windows Server 2008 almacena en cada cuenta de usuario, los más importantes son los siguientes:

- **Nombre de usuario**. Es el nombre mediante el cual el usuario *se identifica* en el sistema. Cada usuario ha de tener un nombre de usuario distinto para que la identificación sea unívoca.
- **Nombre completo**. Es el nombre completo del usuario.
- **Contraseña**. Palabra cifrada que permite *autenticar* el nombre de usuario. En Windows Server 2008 la contraseña distingue entre mayúsculas y minúsculas. Sólo los usuarios que se identifican y autentican positivamente pueden ser *autorizados* a conectarse al sistema.
- **Directorio de conexión**. Es el lugar donde (en principio) residirán los archivos personales del usuario. El directorio de conexión de cada usuario es privado: ningún otro usuario puede entrar en él, a menos que su propietario conceda los permisos adecuados.
- **Horas de conexión**. Se puede controlar a qué horas un usuario puede conectarse para trabajar en el sistema. Inclusive se puede especificar un horario distinto para cada día de la semana.
- **Activada**. Esta característica permite inhabilitar temporalmente una cuenta. Una cuenta desactivada sigue existiendo, pero no puede ser utilizada para acceder al sistema, ni siquiera conociendo su contraseña.

Existe un dato especial que se asocia a cada cuenta, pero que a diferencia de todos los expuestos arriba, no puede ser especificado manualmente cuando se da de alta la cuenta. Se trata del **identificador seguro** (*Secure Identifier*, o SID). Este identificador es interno y el sistema lo genera automáticamente cuando se crea una nueva cuenta. Además, los SIDs se generan de tal forma que se asegura que no pueden

existir dos iguales en todas las instalaciones de Windows Server 2008 del mundo (son identificadores únicos). Windows Server 2008 utiliza siempre el SID (y no el nombre de usuario) para controlar si un usuario tiene o no permisos suficientes para llevar a cabo cualquiera de sus acciones. La ventaja de este modelo es que el SID es un dato completamente interno del sistema operativo, es decir, ningún usuario puede establecerlo en ningún sitio (ni siquiera el administrador del sistema). Por tanto, nadie puede obtener un mayor grado de privilegio intentando *suplantar* la identidad de otro usuario.

Cuando en un equipo se instala Windows Server 2008, existen de entrada las cuentas de dos usuarios integrados (*built-in users*): el Administrador y el Invitado. El primero es un usuario especial, el único que en principio posee lo que se denominan derechos administrativos en el sistema. Es decir, tiene la potestad de administrar el sistema en todos aquellos aspectos en que éste es configurable: usuarios, grupos de usuarios, contraseñas, recursos, derechos, etc. La cuenta de Administrador no puede ser borrada ni desactivada. Por su parte, la cuenta de Invitado es la que utilizan normalmente aquellas personas que no tienen un usuario propio para acceder al sistema. Habitualmente esta cuenta no tiene contraseña asignada, puesto que se supone que el nivel de privilegios asociado a ella es mínimo. En cualquier caso, el Administrador puede desactivarla si lo considera oportuno.

3.2. Grupos de Usuarios

La información de seguridad almacenada en una cuenta de usuario es suficiente para establecer el grado libertad (o de otro modo, las restricciones) que cada usuario debe poseer en el sistema. Sin embargo, resultaría muchas veces tedioso para el administrador determinar dichas restricciones usuario por usuario, especialmente en sistemas con un elevado número de ellos. El concepto de *grupo de usuarios* permite agrupar de forma lógica a los usuarios de un sistema, y establecer permisos y restricciones a todo el grupo de una vez. De forma análoga a las cuentas de usuario, una cuenta de grupo posee un nombre y un identificador interno o SID, además de una lista de los usuarios que pertenecen a dicho grupo.

La administración de la protección del sistema mediante grupos de usuarios es mucho más flexible y potente que el establecimiento de permisos en base a usuarios individuales, ya que un usuario puede pertenecer a tantos grupos como sea necesario, obteniendo implícitamente la *suma* de los permisos asignados a todos ellos. Considérese, por ejemplo, que en una empresa un sistema es utilizado por empleados de distinto rango, y que cada rango posee un distinto nivel de privilegios. Supongamos que se desea cambiar de rango a un empleado, debido a un ascenso, por ejemplo. Si la seguridad estuviera basada en usuarios individuales, cambiar los privilegios de este usuario adecuadamente supondría modificar sus privilegios en cada lugar del sistema en que estos debieran cambiar (con el consiguiente trabajo, y el riesgo de olvidar alguno). Por el contrario, con la administración de seguridad basada en gru-

pos, esta operación sería tan sencilla como cambiar al usuario de un grupo a otro. Por ello, en Windows Server 2008 se recomienda que los permisos se asignen en base a *grupos*, y no en base a usuarios individuales.

Al igual que existen usuarios integrados, en todo sistema Server 2008 existen una serie de grupos integrados (*built-in groups*): Administradores, Operadores de Copia, Usuarios Avanzados, Usuarios, e Invitados. El grupo Administradores recoge a todos aquellos usuarios que deban poseer derechos administrativos completos. Inicialmente posee un solo usuario, el Administrador. De igual forma, el grupo Invitados posee al Invitado como único miembro. Los otros tres grupos están vacíos inicialmente. Su uso es el siguiente:

- **Usuarios**. Son los usuarios normales del sistema. Tienen permisos para conectarse al sistema interactivamente y a través de la red.
- **Operadores de copia**. Estos usuarios pueden hacer (y restaurar) una copia de todo el sistema.
- **Usuarios avanzados**. Son usuarios con una cierta capacidad administrativa. Se les permite cambiar la hora del sistema, crear cuentas de usuario y grupos, compartir ficheros e impresoras, etc.

El Administrador, al ir creando las cuentas de los usuarios, puede hacer que cada una pertenezca al grupo (o grupos) que estime conveniente. Asimismo, puede crear nuevos grupos que refinen esta estructura inicial, conforme a las necesidades particulares de la organización donde se ubique el sistema.

Finalmente, Windows Server 2008 define una serie de grupos especiales, cuyos (usuarios) miembros no se establecen de forma manual, sino que son determinados de forma dinámica y automática por el sistema. Estos grupos se denominan genéricamente identidades especiales (*special identities*) y se utilizan normalmente para facilitar la labor de establecer la protección del sistema. De entre estos grupos, destacan:

- **Usuarios Interactivos** (*Interactive*). Este grupo representa a todos aquellos usuarios que tienen el derecho de iniciar una sesión local en la máquina.
- **Usuarios de Red** (*Network*). Bajo este nombre se agrupa a todos aquellos usuarios que tienen el derecho de acceder al equipo desde la red.
- **Todos** (*Everyone*). Agrupa a todos los usuarios que el sistema conoce. Puede agrupar a usuarios existentes localmente y de otros sistemas (conectados a través de la red). A partir de Windows Server 2003, este grupo no incluye las conexio-

nes anónimas (sin aportar usuario y contraseña).

- **Usuarios autentificados** (*Authenticated Users*). Agrupa a todos los usuarios que poseen una cuenta propia para conectarse al sistema. Por tanto, aquellos usuarios que se hayan conectado al sistema utilizando la cuenta de "invitado" pertenecen a "Todos" pero no a "Usuarios autentificados".

3.3. El modelo de protección

El modelo de protección de Windows Server establece la forma en que el sistema lleva a cabo el *control de acceso* de cada usuario y grupo de usuarios. En otras palabras, es el modelo que sigue el sistema para establecer las acciones que un usuario (o grupo) está autorizado a llevar a cabo. Este modelo está basado en la definición y contrastación de ciertos *atributos de protección* que se asignan a los procesos de usuario por un lado, y al sistema y sus recursos por otro. En el caso del sistema y sus recursos, Windows Server 2008 define dos conceptos distintos y complementarios: el concepto de *derecho* y el concepto de *permiso*, respectivamente.

Un *derecho* o *privilegio* de usuario (*user right*) es un atributo de un usuario (o grupo) que le permite realizar una accion que afecta al sistema en su conjunto (y no a un objeto o recurso en concreto). Existe un conjunto fijo y predefinido de derechos en Windows Server 2008. Para determinar qué usuarios poseen qué derechos, cada derecho posee una lista donde se especifican los grupos/usuarios que tienen concedido este derecho.

Un *permiso* (*permission*) es una característica de cada *recurso* (carpeta, archivo, impresora, etc.) del sistema, que concede o deniega el acceso al mismo a un usuario/grupo concreto. Cada recurso del sistema posee una lista en la que se establece qué usuarios/grupos pueden acceder a dicho recurso, y también qué tipo de acceso puede hacer cada uno (lectura, modificación, ejecución, borrado, etc.).

En los apartados siguientes se detallan los atributos de protección de los procesos de usuario (Sección 3.4, “Atributos de protección de los procesos”), los derechos que pueden establecerse en el sistema (Sección 3.5, “Derechos de usuario”) y los atributos de protección que poseen los recursos (Sección 3.6, “Atributos de protección de los recursos”). La Sección 3.7, “Reglas de protección” establece las reglas concretas que definen el control de acceso de los procesos a los recursos.

3.4. Atributos de protección de los procesos

Cuando un usuario es autorizado a conectarse interactivamente a un sistema Windows Server 2008, el sistema construye para él una acreditación denominada *Secu-*

rity Access Token o SAT. Esta acreditación contiene la información de protección del usuario, y Windows Server 2008 la incluye en los procesos que crea para dicho usuario. De esta forma, los *atributos de protección* del usuario están presentes en cada proceso del usuario, y se utilizan para controlar los accesos que el proceso realiza a los recursos del sistema en nombre de dicho usuario.

En concreto, el SAT contiene los siguientes atributos de protección:

1. **SID**. El identificador único del usuario.
2. **SIDs de sus grupos**. Lista de los SIDs de los grupos a los que pertenece el usuario.
3. **Derechos**. Lista de derechos del usuario. Esta lista se construye mediante la inclusión de todos los derechos que el usuario tiene otorgados por sí mismo o por los grupos a los que pertenece (ver Sección 3.5, "Derechos de usuario").

Esta forma de construir la acreditación introduce ya una de las máximas de la protección de Windows Server 2008: el nivel de acceso de un usuario incluye implícitamente los niveles de los grupos a los que pertenece.

3.5. Derechos de usuario

Un *derecho* es un atributo de un usuario o grupo de usuarios que le confiere la posibilidad de realizar una acción concreta sobre el sistema en conjunto (no sobre un recurso concreto). Como hemos visto, la lista de derechos de cada usuario se añade explícitamente a la acreditación (SAT) que el sistema construye cuando el usuario se conecta al sistema. Esta lista incluye los derechos que el usuario tiene concedidos a título individual más los que tienen concedidos todos los grupos a los que el usuario pertenece.

Windows Server 2008 distingue entre dos tipos de derechos: los *derechos de conexión* (*logon rights*) y los *privilegios* (*privileges*). Los primeros establecen las diferentes formas en que un usuario puede conectarse al sistema (de forma interactiva, a través de la red, etc.), mientras que los segundos hacen referencia a ciertas acciones predefinidas que el usuario puede realizar una vez conectado al sistema. La Tabla 3.1, "Principales derechos de usuario en Windows Server 2008" presenta los derechos más destacados de cada tipo, junto con su descripción.

Es importante hacer notar lo siguiente: cuando existe un conflicto entre lo que concede o deniega un permiso y lo que concede o deniega un derecho, este último tiene prioridad. Por ejemplo: los miembros del grupo Operadores de Copia poseen el derecho de realizar una copia de seguridad de todos los archivos del sistema. Es

posible (y muy probable) que existan archivos sobre los que no tengan ningún tipo de permiso. Sin embargo, al ser el derecho más prioritario, podrán realizar la copia sin problemas. De igual forma, el administrador tiene el derecho de tomar posesión de cualquier archivo, inclusive de aquellos archivos sobre los que no tenga ningún permiso. Es decir, como regla general, los derechos y privilegios siempre prevalecen ante los permisos particulares de un objeto, en caso de que haya conflicto.

Tabla 3.1. Principales derechos de usuario en Windows Server 2008

DERECHOS DE CONEXIÓN	
Nombre	**Significado**
Acceder a este equipo desde la red	Permite/impide al usuario conectar con el ordenador desde otro ordenador a través de la red.
Inicio de sesión local	Permite/impide al usuario iniciar una sesión local en el ordenador, desde el teclado del mismo.
PRIVILEGIOS	
Nombre	**Significado**
Añadir estaciones al dominio	Permite al usuario añadir ordenadores al dominio actual.
Hacer copias de seguridad	Permite al usuario hacer copias de seguridad de archivos y carpetas.
Restaurar copias de seguridad	Permite al usuario restaurar copias de seguridad de archivos y carpetas.
Atravesar carpetas	Permite al usuario acceder a archivos a los que tiene permisos a través de una ruta de directorios en los que puede no tener ningún permiso.
Cambiar la hora del sistema	Permite al usuario modificar la hora interna del ordenador.
Instalar manejadores de dispositivo	Permite al usuario instalar y desinstalar manejadores de dispositivos *Plug and Play*.
Apagar el sistema	Permite al usuario apagar el ordenador local.
Tomar posesión de archivos y otros objetos	Permite al usuario tomar posesión (hacerse propietario) de cualquier objeto con atributos de seguridad del sistema (archivos, carpetas, objetos del Directorio Activo, etc.).

3.5.1. Otras directivas de seguridad

En Windows Server 2008, los derechos son un tipo de *directivas de seguridad*. En este sentido, Windows Server 2008 ha agrupado un conjunto de reglas de seguridad que en versiones anteriores de NT estaban dispersas en distintas herramientas administrativas, y las ha incorporado a una consola de administración única denominada *directivas de seguridad local*).

Dentro de esta herramienta de administración podemos establecer, entre otras, los siguientes tipos de reglas de seguridad para el equipo local:

1. **Cuentas**. En este apartado podemos establecer cuál es la *política de cuentas* o de contraseñas que sigue el equipo para sus usuarios locales. Dentro de este apartado se pueden distinguir reglas en tres epígrafes: *Contraseñas*, *Bloqueo* y *Kerberos*. Entre ellas, las dos primeras hacen referencia a cómo deben ser las contraseñas en el equipo (longitud mínima, vigencia máxima, historial, etc.) y cómo se debe bloquear una cuenta que haya alcanzado un cierto máximo de intentos fallidos de conexión local.

2. **Directiva local**. Dentro de este apartado se encuentra, por una parte, la *Auditoría* del equipo, que permite registrar en el visor de sucesos ciertos eventos que sean interesantes, a criterio del administrador (por ejemplo, inicios de sesión local). Por otra parte, este apartado incluye los *derechos y privilegios* que acabamos de explicar.

3. **Claves públicas**. Este apartado permite administrar las opciones de seguridad de las claves públicas emitidas por el equipo.

3.6. Atributos de protección de los recursos

En un sistema de archivos NTFS de Windows Server 2008, cada carpeta o archivo posee los siguientes atributos de protección:

1. **SID del propietario**. Inicialmente, el propietario es siempre el usuario que ha creado el archivo o carpeta, aunque este atributo puede ser luego modificado (esto se explica más adelante).

2. **Lista de control de acceso de protección**. Esta lista incluye los *permisos* que los usuarios tienen sobre el archivo o carpeta. La lista puede contener un número indefinido de entradas, de forma que cada una de ellas concede o deniega un conjunto concreto de permisos a un usuario o grupo conocido por el sistema. Por tanto, Windows Server 2008 permite definir multitud de niveles de acceso a cada objeto del sistema de archivos, cada uno de los cuales puede ser *positivo* (se otorga un permiso) o *negativo* (se deniega un permiso).

3. **Lista de control de acceso de seguridad**. Esta segunda lista se utiliza para definir qué acciones sobre un archivo o carpeta tiene que *auditar* el sistema. El proceso de auditoría supone la anotación en el *registro del sistema* de las acciones que los usuarios realizan sobre archivos o carpetas (las entradas de este regis-

tro, denominado registro de seguridad, pueden consultarse más tarde mediante la herramienta administrativa Visor de Sucesos). El sistema sólo audita las acciones especificadas (de los usuarios o grupos especificados) en la lista de seguridad de cada archivo o carpeta. Esta lista está inicialmente vacía en todos los objetos del sistema de archivos.

La lista de control de acceso de protección se divide realmente en dos listas, cada una de ellas denominada *Discretionary Access Control List* (lista de control de acceso discrecional) o DACL. Cada elemento de una DACL se denomina *Access Control Entry* (entrada de control de acceso) o ACE. Cada entrada liga a un SID de usuario o grupo con la concesión o denegación de un permiso concreto (o conjunto de permisos), tal como se ha descrito arriba. Los diferentes permisos que se pueden asignar a usuarios o grupos en Windows Server 2008 se explican en la Sección 3.6.2, "Permisos estándar e individuales".

El hecho de que cada archivo o carpeta tenga dos DACL en vez de una tiene que ver con el mecanismo de la *herencia de permisos* que incorpora Windows Server 2008: cada archivo o carpeta puede heredar implícitamente los permisos establecidos para la carpeta que lo contiene y puede además definir permisos propios (denominados explícitos en la jerga de Windows Server). Es decir, que cada archivo o carpeta puede poseer potencialmente una *DACL heredada* y una *DACL explícita* (aunque no está obligado a ello, como veremos). De esta forma, si una cierta carpeta define permisos explícitos, éstos (junto con sus permisos heredados) serán a su vez los permisos heredados de sus subcarpetas y archivos (y así sucesivamente). El mecanismo de herencia de permisos es dinámico, queriendo decir que la modificación un permiso explícito de una carpeta se refleja en el correspondiente permiso heredado de sus subcarpetas y archivos.

3.6.1. Asociación de permisos a recursos

La asociación de permisos a archivos y carpetas sigue una serie de reglas:

- Cuando se crea un **nuevo** archivo o carpeta, éste no posee ningún permiso explícito y adquiere como permisos heredados los permisos heredados y explícitos de su carpeta padre.
- Si se desea añadir permisos sobre un archivo o carpeta, éstos se añaden siempre a la lista de permisos explícitos. De igual forma, sólo se puede modificar o eliminar *individualmente* un permiso si éste es explícito.
- El control sobre la **herencia** de permisos (i.e., qué recursos heredan y qué permisos se heredan) se puede realizar a dos niveles de forma independiente:

1. Cada carpeta o archivo tiene la potestad de decidir si desea o no heredar los permisos de su carpeta padre (herencia *"desde arriba"*). Es decir, en cada recurso se puede *desactivar* la herencia, con lo que los permisos definidos por encima del recurso en la jerarquía de archivos no se le aplican. Desactivar la herencia no es una acción irreversible: la herencia puede volver a activarse más tarde si se desea, sin que ello modifique los permisos explícitos que pueda tener el recurso.
2. Cada permiso lleva asociada una regla que indica qué recursos van a poder heredarlo (herencia *"hacia abajo"*). Esta regla sólo interviene cuando se asocia un permiso a una carpeta, puesto que sólo las carpetas poseen recursos dentro de ellas (subcarpetas y archivos) que puedan heredar el permiso. Por tanto, cuando en una carpeta se define un permiso explícito, su regla de la herencia puede utilizarse para restringir qué recursos por debajo de dicha carpeta van a poder heredarlo.

   Concretamente, la regla permite establecer que el permiso sea aplicable: (a) sólo en la propia carpeta, (b) sólo en las subcarpetas, (c) sólo en los archivos, o cualquier combinación entre estas tres opciones. La regla por defecto al crear un nuevo permiso explícito es que dicho permiso sea heredable por la carpeta y todas sus subcarpetas y archivos.

- **Copiar** un archivo o carpeta a otra ubicación se considera una creación, y por tanto el archivo copiado recibe una lista de permisos explícitos vacía y se activa la herencia de la carpeta padre correspondiente a la nueva ubicación.

- **Mover** un archivo distingue dos casos: si movemos una carpeta o archivo a otra ubicación dentro del mismo volúmen (partición) NTFS, se desactiva la herencia y se mantienen los permisos que tuviera como explíticos en la nueva ubicación. Si el volúmen destino es distinto, entonces se actúa como en una copia (sólo se tienen los permisos heredados de la carpeta padre correspondiente a la nueva ubicación).

3.6.2. Permisos estándar e individuales

Windows Server 2008 distingue entre los *permisos estándar* de carpetas y los de archivos. Como ocurría en versiones previas de Windows NT, los permisos estándar son combinaciones predefinidas de *permisos individuales*, que son aquellos que controlan cada una de las acciones individuales que se pueden realizar sobre carpetas y archivos. La existencia de estas combinaciones predefinidas es el resultado de una agrupación "lógica" de los permisos individuales para facilitar la labor del administrador (y de cada usuario cuando administra los permisos de sus archivos). Por este motivo, los permisos estándar se conocen también como "plantillas de permisos".

En la Tabla 3.2, "Permisos estándar sobre carpetas y archivos en Windows Server 2008" se muestran los permisos estándar de carpetas y archivos junto con su significado cualitativo. La descripción de las tablas hacen referencia a las acciones que cada permiso concede, pero no olvidemos que en Windows Server 2008 cada permiso puede ser positivo o negativo, es decir, que realmente cada permiso *permite* o *deniega* la acción correspondiente. Como puede verse en ambas tablas, muchos de los permisos estándar se definen de forma *incremental*, de forma que unos incluyen y ofrece un nivel de acceso superior que los anteriores. La herencia de permisos se establece de forma natural: las carpetas heredan directamente los permisos estándar establecidos en la carpeta padre, mientras que los archivos heredan cualquier permiso excepto el de `Listar` (sólo definido para carpetas).

Tabla 3.2. Permisos estándar sobre carpetas y archivos en Windows Server 2008

CARPETAS	
Nombre	**Significado**
`Listar`	Permite listar la carpeta: ver los archivos y subcarpetas que contiene.
`Leer`	Permite ver el contenido de los archivos y subcarpetas, así como su propietario, permisos y atributos (sistema, sólo lectura, oculto, etc.).
`Escribir`	Permite crear nuevos archivos y subcarpetas. Permite modificar los atributos de la propia carpeta, así como ver su propietario, permisos y atributos.
`Leer y Ejecutar`	Permite moverse por la jerarquía de subcarpetas a partir de la carpeta, incluso si no se tienen permisos sobre ellas. Además, incluye todos los permisos de `Leer` y de `Listar`.
`Modificar`	Permite eliminar la carpeta más todos los permisos de `Escribir` y de `Leer y Ejecutar`.
`Control Total`	Permite cambiar permisos, tomar posesión y eliminar subcarpetas y archivos (aun no teniendo permisos sobre ellos), así como todos los permisos anteriores.
ARCHIVOS	
Nombre	**Significado**
`Leer`	Permite ver el contenido del archivo, así como su propietario, permisos y atributos (sistema, sólo lectura, oculto, etc.).
`Escribir`	Permite sobreescribir el archivo, modificar sus atributos y ver su propietario, permisos y atributos.
`Leer y Ejecutar`	Permite ejecutar el archivo más todos los permisos de `Leer`.
`Modificar`	Permite modificar y eliminar el archivo más todos los permisos de `Escribir` y de `Leer y Ejecutar`.
`Control Total`	Permite cambiar permisos y tomar posesión del archivo, más todos los permisos anteriores.

Cuando la asignación de permisos que queremos realizar no se ajusta al comportamiento de ninguno de los permisos estándar, debemos entonces ir directamente a asignar permisos individuales. La Tabla 3.3, "Permisos individuales en Windows

Server 2008" muestra cuáles son los permisos individuales en Windows Server 2008, junto con su significado concreto. También en este caso debe entenderse que cada permiso puede ser concedido de forma positiva o negativa.

Tabla 3.3. Permisos individuales en Windows Server 2008

Nombre	Significado
`Atravesar carpeta/ejecutar archivo`	Aplicado a una carpeta, permite moverse por subcarpetas en las que puede que no se tenga permiso de acceso. Aplicado a un archivo, permite su ejecución.
`Leer carpeta/Leer datos`	Aplicado a una carpeta, permite ver los nombres de sus ficheros y subcarpetas. Aplicado a un archivo, permite leer su contenido.
`Leer atributos`	Permite ver los atributos del fichero/carpeta, tales como `oculto` o `sólo lectura`, definidos en NTFS.
`Leer atributos extendidos`	Permite ver los atributos extendidos del archivo o carpeta. (Estos atributos están definidos por los programas y pueden variar).
`Crear ficheros/escribir datos`	Aplicado a una carpetas, permite crear archivo en ella. Aplicado a un archivo, permite modificar y sobreescribir su contenido.
`Crear carpetas/anexar datos`	Aplicado a una carpeta, permite crear subcarpetas en ella. Aplicado a un archivo, permite añadir datos al mismo.
`Escribir atributos`	Permite modificar los atributos de un archivo o carpeta.
`Escribir atributos extendidos`	Permite modificar los atributos extendidos de un archivo o carpeta.
`Borrar subcarpetas y archivos`	Sólo se puede aplicar a una carpeta, y permite borrar archivos o subcarpetas de la misma, aun no teniendo permiso de borrado en dichos objetos.
`Borrar`	Permite eliminar la carpeta o archivo.
`Leer permisos`	Permite leer los permisos de la carpeta o archivo.
`Cambiar permisos`	Permite modificar los permisos de la carpeta o archivo.
`Tomar posesión`	Permite tomar posesión de la carpeta o archivo.

Finalmente, la Tabla 3.4, "Correspondencia entre permisos estándar e individuales en Windows Server 2008" pone de manifiesto el subconjunto de los permisos individuales forman cada uno de los permisos estándar mencionados anteriormente. Como curiosidad, puede verse que los permisos individuales correspondientes a `Listar` y `Leer y Ejecutar` son los mismos. En realidad, lo que les distingue es cómo se heredan: el primero sólo es heredado por carpetas, mientras que el segundo es heredado por carpetas y archivos.

Tabla 3.4. Correspondencia entre permisos estándar e individuales en Windows Server 2008

Permiso	C.Total	Modif.	L.y Ej.	Listar	Leer	Escribir
Atravesar carpeta/ejecutar archivo	+	+	+	+		
Leer carpeta/Leer datos	+	+	+	+	+	
Leer atributos	+	+	+	+	+	
Leer atributos extendidos	+	+	+	+	+	
Crear ficheros/escribir datos	+	+				+
Crear carpetas/anexar datos	+	+				+
Escribir atributos	+	+				+
Escribir atributos extendidos	+	+				+
Borrar subcarpetas y archivos	+					
Borrar	+	+				
Leer permisos	+	+	+	+	+	+
Cambiar permisos	+					
Tomar posesión	+					

3.6.3. Modificación de atributos de protección

Las reglas que plantea Windows Server 2008 para controlar quién puede modificar los atributos de protección de un recurso están completamente integradas en su modelo de protección, basado en los *permisos* y los *derechos* del usuario implicado en la modificación. Este modelo es diferente del que plantean los sistemas UNIX, cuyas reglas en este sentido son independientes de los permisos que posea el propio recurso.

En concreto, las reglas que dictan quién puede modificar los diferentes atributos de protección de los recursos (archivos y carpetas) son:

1. **Propietario**. Cualquier usuario que posea el permiso individual `Tomar posesión`(incluido dentro de `Control Total`) sobre un recurso concreto, puede pasar a ser su nuevo propietario.

   Asimismo, cualquier usuario que tenga concedido el derecho `Tomar posesión de archivos y otros objetos` puede convertirse en propietario de

cualquier recurso del sistema. Por defecto, este derecho solamente lo tiene concedido el grupo `Administradores`.

Finalmente, Windows Server 2008 ha introducido otra posibilidad: el derecho de usuario `Restaurar archivos y carpetas` lleva asociado la posibilidad de *asignar* la posesión de cualquier archivo y carpeta del sistema a cualquier usuario, sin tener que tomar posesión en nombre propio. Por defecto, sólo los grupos `Administradores` y `Operadores de copia` tienen este derecho concedido.

2. **Lista de control de acceso de protección**. Cualquier usuario que posea el permiso individual `Cambiar Permisos` (incluido dentro de `Control Total`) sobre un recurso concreto, puede modificar sus permisos. De forma independiente, el *propietario* de un recurso siempre puede cambiar los permisos del mismo.

   Las acciones concretas que se incluyen en el cambio de permisos sobre un recurso son: (a) la activación/desctivación de la herencia de permisos y (b) la edición (creación, modificación y eliminación) de permisos explícitos.

3. **Lista de control de acceso de seguridad**. Se aplican las mismas reglas que en el caso anterior.

Después de haber visto el modelo de protección y de cambio de atributos, es interesante analizar la diferencia de los modelos de Windows Server y UNIX respecto a la figura del `Administrador`/`root`. En el mundo UNIX, `root` no tiene ninguna restricción en sus acciones en el sistema. En Windows Server, por el contrario, al `Administrador` se le aplican las mismas reglas que al resto de usuarios: si dicho usuario no posee permisos sobre un recurso, no podrá acceder al mismo. Si podrá, no obstante, tomar posesión del recurso (gracias al *derecho* que tiene concedido) y, una vez sea su propietario, añadirse permisos que le permitan cualquier acceso. El modelo de Windows Server se basa, por tanto, en definir la protección como un conjunto de reglas (permisos, derechos) y conceder a cada usuario aquellas necesarias para que desempeñe su función. El Administrador tiene concedidas más reglas que el resto de usuarios, pero aún así el sistema sigue verificándolas para cada acción que realiza en el sistema. Se recomienda al lector reflexionar sobre este hecho y su repercusión en el modelo de protección.

3.7. Reglas de protección

Las principales reglas que controlan la comprobación de permisos a carpetas y archivos son las siguientes:

- Una única acción de un proceso puede involucrar varias acciones individuales sobre varios archivos y/o carpetas. En ese caso, el sistema verifica si el proceso tiene o no permisos para todas ellas. Si le falta algún permiso, la acción se rechaza con un mensaje de error genérico de falta de permisos.

- Los permisos en Windows Server 2008 son acumulativos: un proceso de usuario posee implícitamente todos los permisos correspondientes a los SIDs de su acreditación (ver Sección 3.4, "Atributos de protección de los procesos"), es decir, los permisos del usuario y de todos los grupos a los que pertenece.

- La ausencia un cierto permiso sobre un objeto supone implícitamente la imposibilidad de realizar la acción correspondiente sobre el objeto.

- Si se produce un conflicto en la comprobación de los permisos, los permisos negativos tienen prioridad sobre los positivos, y los permisos explícitos tienen prioridad sobre los heredados.

Estas reglas son más fáciles de recordar si se conoce el algoritmo que sigue Windows Server 2008 para conceder o denegar una acción concreta sobre un archivo o directorio concreto. Para ello, el sistema explora secuencialmente las entradas de las DACLs de protección de dicho objeto hasta que se cumple alguna de las condiciones siguientes:

1. Cada permiso involucrado en la acción solicitada está concedido explícitamente al SID del usuario o de algún grupo al que el usuario pertenece. En ese caso, se permite la acción.

2. Alguno de los permisos involucrados está explícitamente denegado para el SID del usuario o para alguno de sus grupos. En este caso, se deniega la acción.

3. La lista (DACL) ha sido explorada completamente y no se ha encontrado una entrada (ni positiva ni negativa) correspondiente a alguno de los permisos involucrados en la acción para el SID del usuario o sus grupos. En este caso, se deniega la acción.

Este algoritmo realmente produce el comportamiento descrito por las reglas anteriores debido al orden en que Windows Server 2008 establece las entradas de las DACLs de cada objeto. Este orden es siempre el siguiente: permisos negativos explícitos, permisos positivos explícitos, permisos negativos heredados y permisos positivos heredados.

4

Administración de dominios Windows Server 2008

Indice

4.1. Introducción

Este capítulo introduce los conceptos fundamentales sobre dominios Windows Server 2008, que permiten unificar y centralizar la administración de conjuntos de sistemas Windows servidores y clientes en organizaciones de cualquier tamaño.

En concreto, se explicarán los denominados Servicios de Dominio del Directorio Activo (*Active Directory Domain Services*), que en conjunto permiten implantar dominios en una organizción, así como la administración de los mismos, incluyendo los principales objetos que pueden definirse en el dominio, la compartición de recursos entre sistemas de la organización y la delegación de tareas administrativas dentro de un dominio.

4.2. El Directorio Activo

4.2.1. Servicios de Dominio del Directorio Activo

Hoy en día, los ordenadores existentes en cualquier organización se encuentran formando parte de redes de ordenadores, de forma que pueden intercambiar información. Desde el punto de vista de la administración de sistemas, la mejor forma de aprovechar esta característica es la creación de un *dominio* de sistemas, en donde la información administrativa y de seguridad se encuentra *centralizada* en uno o varios servidores, facilitando así la labor del administrador. Windows Server 2008 utiliza el concepto de **directorio** para implementar dominios de sistemas Windows, que pueden incluir sistemas servidores (como Windows 2000, Windows Server 2003 o Windows Server 2008) y clientes (como Windows XP, Windows Vista o Windows 7).

En el ámbito de las redes de ordenadores, el concepto de *directorio* (o almacén de datos) se define como una estructura jerárquica que almacena información sobre objetos existentes en la red (o más ampliamente, en la organización). Normalmente, un directorio se implementa mediante una base de datos optimizada para operaciones de lectura, que soporta búsquedas de grandes volúmenes de información y con capacidades de exploración. Existen varios estándares de la industria que especifican cómo debe definirse un servicio de directorio, destacando entre ellos el *Directory Access Protocol*, así como una versión simplificada y más utilizada del mismo, denominada *Lightweight Directory Access Protocol*, o LDAP.

Active Directory Domain Services (AD DS), o Servicios de Dominio del Directorio Activo, es el nombre que recibe el conjunto de elementos que globalmente constituyen el servicio directorio en dominios Windows Server 2008 (por simplificar, en adelante nos referiremos a este servicio como Directorio Activo, tal como se le denominaba en versiones previas de Windows Server). En esencia, este servicio almacena

información acerca de los recursos disponibles en el dominio y permite el acceso controlado de los usuarios y aplicaciones a dichos recursos, de forma que se convierte en un medio de organizar, controlar y *administrar* centralizadamente el acceso a los recursos de la red.

Como veremos, al instalar el Directorio Activo en sistemas Windows Server 2008 de nuestra red, convertimos a dichos sistemas en los servidores del dominio, o más correctamente, en los denominados *Controladores de Dominio* (*Domain Controllers*, o "DCs"). El resto de los equipos de la red pueden convertirse entonces en los clientes de dicho servicio de directorio, también denominados *miembros* del dominio, con lo que pueden consultar toda la información almacenada en los DCs. Como veremos, esta información incluye elementos típicamente centralizados en dominios de muchos tipos de sistemas, como cuentas de usuario, grupo, ordenador, etc., así como otras características propias de sistemas Windows Server, como directivas de usuario o equipo, relaciones de confianza, aspectos sobre la replicación de datos entre servidores, etc. De esta forma, el Directorio Activo se convierte en una herramienta fundamental de administración de toda la organización.

Una de las ventajas fundamentales del Directorio Activo a la hora de administrar dominios es que conceptualmente separa la estructura *lógica* de la organización (dominios) de su estructura *física* (topología de red). Ello permite, por una parte, independizar la estructuración de dominios de la organización de la topología de la red o redes que interconectan los sistemas; y, por otra parte, permite administrar la estructura física explícitamente cuando es necesario, de forma independiente de la administración de los dominios. Más adelante en este capítulo se exponen ambas estructuras detalladamente.

4.2.2. Estándares relacionados

A partir de la versión Windows 2000, Windows Server ha basado la implementación del Directorio Activo, una serie de protocolos y estándares existentes, lo cual ha permitido obtener un servicio de directorio no sólo robusto y escalable, sino también interoperable con otros servicios de directorio. Entre estos estándares, podemos destacar los siguientes:

- DHCP (*Dynamic Host Configuration Protocol*). Protocolo de configuración dinámica de ordenadores, que permite la administración desatendida de características de red.
- DNS (*Domain Name System*). Servicio de nombres de dominio que permite la administración de los nombres de ordenadores. Este servicio constituye el mecanismo de asignación y resolución de nombres (traducción de nombres simbólicos a direcciones IP) en Internet.

- SNTP (*Simple Network Time Protocol*). Protocolo simple de tiempo de red, que permite disponer de un servicio de sincronización de tiempo entre sistemas conectados por red.
- LDAP (*Lightweight Directory Access Protocol*). Protocolo ligero (o compacto) de acceso a directorio. Este es el protocolo mediante el cual las aplicaciones acceden para leer o modificar la información existente en la base de datos del directorio.
- Kerberos V5. Protocolo utilizado para la autenticación de usuarios y máquinas..
- Certificados X.509. Estándar que permite distribuir información a través de la red de una forma segura.

De entre todos ellos, es imprescindible que el administrador conozca en detalle la relación entre el Directorio Activo y DNS. A continuación se exponen los aspectos fundamentales de esta relación.

4.2.3. El Directorio Activo y DNS

Tanto el Directorio Activo como DNS establecen espacios de nombres. Podemos entender un espacio de nombres como un área delimitada en la cual un nombre puede ser resuelto. La resolución de nombres es el proceso de traducción de un nombre en un objeto o información que lo representa. Por ejemplo, el sistema de ficheros NTFS puede ser considerado un espacio de nombres en cual un nombre de fichero puede ser resuelto en el fichero propiamente dicho.

DNS es el sistema de nombres de facto para redes basadas en el protocolo TCP/IP y además, es el servicio de nombres que se usa para localizar ordenadores en Internet. Inclusive sin considerar dominios, Windows Server 2008 utiliza principalmente DNS para localizar a otros ordenadores en la red. A continuación se expone la relación que existe entre DNS y los dominios Windows Server 2008.

Cada dominio Windows Server 2008 se identifica unívocamente mediante un nombre de dominio DNS (por ejemplo, `miempresa.com`). Por otro lado, cada ordenador basado en Windows Server que forma parte de un dominio tiene un nombre DNS cuyo sufijo es precisamente el nombre DNS de dicho dominio (siguiendo con el ejemplo, un ordendor de dicho dominio podría denominarse `pc0100.miempresa.com`). De esta forma, los dominios y ordenadores que se representan como objetos en Active Directory, són también nodos en DNS. Por tanto resulta fácil confundir ambos espacios de nombres, ya que comparten idénticos nombres de dominio. La diferencia es que aunque comparten la misma estructura, almacenan información diferente: DNS almacena zonas y registros de recursos y el Directorio Activo almacena dominios y objetos de dominio.

Como conclusión diremos que Directorio Activo *utiliza* DNS para tres funciones principales:

1. **Resolución de nombres**: DNS es el mecanismo por defecto de resolución de nombres en dominios Windows Server 2008, permitiendo localizar por nombre a los ordenadores de la red (al traducir nombres a direcciones IP).

2. **Definición del espacio de nombres**: el Directorio Activo utiliza las convenciones de nomenclatura de DNS para asignar nombres a los dominios. Es decir, los dominios Windows Server 2008 se nombran necesariamente mediante nombres de dominio DNS.

3. **Búsqueda de los componentes físicos de AD**: para iniciar una sesión de red o realizar consultas al Directorio Activo, los sistemas Windows miembros de un dominio deben encontrar primero a alguno de los DCs del dominio, y para ello realizan consultas DNS. Por tanto, debe existir un servidor DNS disponible que incluya la información necesaria para responder estas consultas. En particular, esta información se almacena en DNS mediante registros de recursos SRV que especifican el servidor (o servidores) del dominio que proporcionan los servicios de directorio correspondientes (LDAP, Kerberos, catálogo global, etc.).

4.2.4. Estructura lógica

La estructura lógica del Directorio Activo se centra en la administración de los *recursos* de la organización, independientemente de la ubicación física de dichos recursos, y de la topología de las redes subyacentes. Como veremos, la estructura lógica de la organización se basa en el concepto de *dominio*, o unidad mínima de directorio, que internamente contiene información sobre los recursos (usuarios, grupos, ordenadores, directivas, etc.) existentes en dicho dominio. Dentro de un dominio es posible subdividir lógicamente el directorio mediante el uso de *unidades organizativas*, que permiten una administración independiente sin la necesidad de crear múltiples dominios. Sin embargo, si la organización necesita estructurarse en varios dominios, también puede hacerlo, mediante los conceptos de *árbol* y *bosque*; ambos son jerarquías de dominios a distintos niveles, en función de si los dominios comparten o no un espacio de nombres común. A continuación se presentan todos estos conceptos de forma más detallada.

4.2.4.1. Dominios

La unidad principal de la estructura lógica del Directorio Activo es el dominio. Un dominio es un conjunto de ordenadores, o equipos, que comparten una base de datos de directorio común. En un dominio tiene que existir uno o varios sistemas Win-

dows Server 2008 que actúen como DCs (es decir, con el rol AD DS instalado), y pueden existir además un número indeterminado de sistemas clientes o miembros del dominio. Como hemos visto, cada dominio se identifica unívocamente por un nombre de dominio DNS, que debe ser el sufijo DNS principal de todos los ordenadores miembros del dominio, incluyendo el o los controladores.

El uso de dominios permite conseguir los siguientes objetivos:

- **Delimitar la seguridad**. Un dominio Windows Server 2008 define un límite de seguridad. Las directivas de seguridad, los derechos administrativos y las listas de control de acceso (*Access Control Lists*, ACLs) no se comparten por defecto entre dominios. Es decir, aunque en una organización pueden existir múltiples dominios interrelacionados, cada uno presenta una configuración de seguridad independiente.

- **Replicar información**. Como veremos más adelante, la información sobre los objetos que existen en un dominio se almacena en una de las *particiones* que contiene la base de datos del directorio (en particular, la denominada partición del dominio). Cada partición constituye lo que se conoce como una unidad de replicación, o conjunto concreto de equipos (DCs) que mantienen una copia idéntica de la partición mediante replicación. Active Directory utiliza un modelo de replicación multimaestro, lo cual significa que cualquier DC admite cambios en la información de su partición, y es capaz de replicarlos luego al resto de DCs que constituyen su unidad de replicación. En particular, la unidad de replicación de la partición de dominio de un dominio concreto está constituida por los DCs de dicho dominio, pero no de otros.

- **Aplicar Políticas (o Directivas) de Grupo**. Un dominio define un posible ámbito para las políticas. Al aplicar un objeto de política de grupo (GPO) en un dominio, este establece comportamientos específicos a los ordenadores (equipos) y usuarios del dominio bajo su ámbito. Por defecto, estas políticas se aplican siempre dentro de un mismo dominio y no entre dominios.

- **Delegar permisos administrativos**. En dominios Windows Server 2008 se puede realizar una delegación personalizada de los derechos administrativos a usuarios o grupos concretos dentro del Directorio Activo, tanto a nivel del dominio completo como de unidades organizativas (OUs) individuales. Esto reduce la necesidad de tener varios administradores con amplios permisos administrativos. Ya que un dominio representa un límite de seguridad, los permisos administrativos delegados también se limitan al dominio.

4.2.4.2. Múltiples dominios en la misma organización

Existen muchos casos, especialmente en organizaciones grandes, en los que es interesante que una misma organización disponga de varios dominios (por ejemplo, para reflejar una distribución geográfica o departamental, distintas empresas, etc.). El Directorio Activo permite almacenar y organizar la información de directorio de varios dominios de forma que, aunque la administración de cada uno sea independiente, dicha información esté disponible para todos los dominios. Como se explica a continuación, el conjunto de dominios de una organización pertenece a una estructura lógica denominada bosque, que puede estar formado por uno o varios dominios, distribuidos en uno o varios árboles de dominios.

La estructura de dominios de una organización se basa en los nombres de sus dominios. Puesto que en Windows Server, estos nombres se basan en el estándar DNS, los dominios se crean en una estructura de arbol invertida, con la raíz en la parte superior. Sin embargo, aunque la estructura se basa en los nombres, la vinculación entre dominios se establece explícitamente mediante las denominadas relaciones de confianza, que se describen más adelante.

Cuando se instala el primer controlador de dominio en la organización se crea lo que se denomina el *dominio raíz* del bosque, el cual contiene la configuración y el esquema del bosque (compartidos por todos los dominios de la organización). Más adelante, podemos agregar dominios como subdominios de dicha raíz (**árbol de dominios**) o bien crear otros dominios "hermanos" del dominio inicial (es decir, ampliando el número de árboles del **bosque de dominios**), debajo del cual podemos crear subdominios, y así sucesivamente.

Arbol Un árbol es un conjunto de uno o más dominios dentro de un bosque que comparten un espacio de nombres contiguo, es decir, comparten un sufijo de DNS común. Como hemos dicho, si en una organización existe más de un dominio, estos se disponen en una o varias estructuras de árbol jerárquicas.

El primer dominio que se crea en una organización es el dominio raíz del bosque, y crea el propio bosque y el primer árbol del mismo. Cuando se agrega un dominio a un árbol existente, éste pasa a ser un dominio secundario (o hijo) de alguno de los dominios existentes, que pasa a ser su dominio padre. Los dominios secundarios pueden representar entidades geográficas (valencia, madrid, barcelona), entidades administrativas dentro de la organización (departamento de ventas, departamento de desarrollo ...), u otras delimitaciones específicas de una organización, según sus necesidades.

Los dominios que forman un árbol se vinculan mediante relaciones de confianza bidireccionales y transitivas. La relación padre-hijo entre dominios en un árbol de dominio es simplemente una relación de confianza. Sin embargo, los dominios siguen siendo independientes entre sí: los administradores de un dominio padre no son automáticamente administradores del dominio hijo y el conjunto de políticas de un dominio padre no se aplican automáticamente a los dominios hijo.

Por ejemplo, en la Universidad Politécnica de Valencia cuyo dominio actual de Active Directory es `upv.es` se crean dos nuevos departamentos: DSIC y DISCA. Con el fin de permitir la administración de los dominios por parte de los técnicos de los respectivos departamentos, se decide agregar dos nuevos dominios a su árbol de dominios existente en lugar de crear dos unidades organizativas en el dominio principal. Los dominios resultantes, `dsic.upv.es` y `disca.upv.es` forman un espacio de nombres contiguo, cuya raíz es `upv.es`. El administrador del dominio padre (`upv.es`) puede conceder permisos para recursos a cuentas de cualquiera de los tres dominios del árbol, pero por defecto no los puede administrar.

Bosque Un bosque se define como un grupo de árboles que no comparten un espacio de nombres contiguo, y que se conectan mediante relaciones de confianza bidireccionales y transitivas. A efectos prácticos, se debe recordar que sea cual sea la cantidad y estructuración de dominios de una organización, todos ellos constituyen un único bosque. Por lo tanto, aunque en la organización exista un único domnio, o varios dominios en un único árbol, dicho dominio o dicho árbol constituyen por sí mismos el bosque de la organización. En un bosque, todos los dominios comparten la misma configuración, el mismo esquema de directorio, y el mismo catálogo global (que se describe más adelante).

Añadir nuevos dominios a un bosque es fácil. Sin embargo, existen ciertas limitaciones que hemos de tener en cuenta al respecto:

- No se pueden mover dominios de Active Directory entre bosques.
- Sólo se puede eliminar un dominio de un bosque si este no tiene dominios hijo.
- Después de haber creado el dominio raíz de un árbol, no se pueden añadir al bosque dominios con un nombre de dominio de nivel superior.
- No se puede crear un dominio padre de un dominio existente.

En general, la estructuración de los dominios de una organización mediante un bosque con uno o varios árboles permite mantener convenciones de nombres de dominio tanto contiguos como discontiguos, lo cual puede ser útil en organizaciones con divisiones independendientes que quieren mantener sus propios nombres DNS.

Finalmente, debemos relacionar estos conceptos con el procedimiento para **crear un dominio**. Esto se hace mediante la ejecución de un asistente denominado **dcpromo.exe** en el sistema Windows Server 2008 que queramos *promocionar* a controlador de dominio. En concreto, este asistente nos permite elegir entre las siguientes opciones de instalación:

1. DC adicional de un dominio existente o DC para un dominio nuevo (creación de un dominio).

2. En el segundo caso, el dominio (nuevo) puede ser un dominio secundario de otro dominio existente (es decir, un subdominio en un árbol de dominios ya creado), o bien el dominio principal (raíz) de un nuevo árbol de dominios.

3. En este segundo caso, el dominio raíz puede ser de un bosque existente (agregamos una raíz nueva a un bosque) o de un nuevo bosque (creación del bosque). Por tanto, el primer dominio que creemos en una organización siempre será un dominio nuevo de un árbol nuevo de un bosque nuevo.

4.2.4.3. Niveles funcionales

A lo largo del tiempo, los sistemas Windows Server (y sus dominios) han evolucionado respecto a la funcionalidad que ofrecen. Esta evolución se refleja en los denominados *niveles funcionales*. Un nivel funcional, que puede estar definido a nivel de dominio o de bosque, establece simultáneamente una serie de características o funcionalidades disponibles en el dominio/bosque y la posibilidad de ser compatible con una versión previa de Windows Server a nivel de servidor (DC). Es decir, cuando situamos el nivel funcional del dominio/bosque en un valor determinado, podemos tener en dicho dominio DCs de cualquier versión de Windows Server que admita dicho nivel simultáneamente. Si elevamos el nivel funcional, ampliamos las posibilidades del dominio/bosque, pero a costa de no poder tener DCs de versiones previas de Windows que no sean compatibles con dicho nivel funcional. Una vez elevado el nivel funcional de un dominio/bosque, no puede volver a ponerse en el nivel previo.

A efectos prácticos, podemos entender los niveles funcionales como una forma

razonable de actualizar los servidores (DCs) de los dominios de una organización a una versión superior de Windows Server. Lo habitual es instalar un DC con la versión nueva (o actualizar alguno de los existentes), y durante un tiempo de transición mantenerlo junto con el resto de los DCs que aún mantienen la versión previa de Windows Server. Durante la transición, el dominio se mantiene en el nivel funcional que marca la vesión previa, para mantener la compatibilidad entre ambas versiones. Una vez todos los DCs han sido actualizados a la nueva versión, la transición se culmina elevando el nivel funcional, para aprovechar las nuevas características que sólo están disponibles en dicha versión.

Hasta Windows Server 2003, se ofrecía compatibilidad hacia atrás con sistemas Windows NT4. A partir de Windows Server 2008 se ha eliminado esta posibilidad, así como los niveles funcionales de dominio/bosque que la permitían.

En concreto, Windows Server 2008 R2 soporta cuatro niveles funcionales *de dominio* y tres niveles funcionales *de bosque*, explicados a continuación.

Un *dominio* Windows Server 2008 R2 puede estar en cuatro niveles funcionales:

1. **Windows 2000 nativo**. En este nivel funcional, los DCs de Windows Server 2008 son compatibles dentro del mismo dominio con DCs que ejecuten versiones previas a partir de Windows 2000 (se excluye Windows NT4). Se tiene una funcionalidad completa del Directorio Activo a nivel de Windows 2000, incluyendo por ejemplo el anidamiento de grupos, los grupos universales o la conversión entre grupos de seguridad y de distribución.

2. **Windows Server 2003**. En este nivel funcional, los DCs de Windows Server 2008 son compatibles dentro del mismo dominio con Dcs que ejecuten versiones previas a partir de Windows Server 2003. Este nivel ofrece la funcionalidad previa, más características nuevas como por ejemplo el cambio de nombre de un DC (sin despromoción previa), la inclusión de un atributo de usuario que almacena la hora del último inicio de sesión en el dominio, o la posiblidad de redirigir los contenedores por defecto para nuevos usuarios y equipos.

3. **Windows Server 2008**. En este nivel funcional, los DCs de Windows Server 2008 son compatibles dentro del mismo dominio con Dcs que ejecuten versiones previas a partir de Windows Server 2008. Este nivel ofrece la funcionalidad previa, más características nuevas como por ejemplo las políticas de contraseñas específicas para usuarios/grupos dentro del dominio, mayor seguridad de cifrado en el protocolo Kerberos, o un nuevo sistema de replicación para el recurso SYSVOL (compartido por todos los DCs).

4. **Windows Server 2008 R2**. En este nivel funcional, los DCs de Windows Server 2008 R2 son compatibles dentro del mismo dominio sólo con otros Dcs que eje-

cuten esta versión de Windows Server. Este nivel ofrece la funcionalidad previa, más alguna característica nueva relacionada con el inicio de sesión en dominios que incorporan un entorno de identidades federadas (que queda fuera del ámbito de este texto).

Por otro lado, un *bosque de dominios* Windows Server 2008 R2 puede estar en tres niveles funcionales:

- **Windows 2000**. En este nivel funcional, los DCs de Windows Server 2008 son compatibles dentro del bosque con DCs que ejecuten versiones previas de Windows a partir de Windows 2000. Se tiene una funcionalidad completa del bosque a nivel de Windows 2000.
- **Windows Server 2003**. En este nivel funcional, los DCs de Windows Server 2008 son compatibles dentro del bosque con Dcs que ejecuten versiones previas a partir de Windows Server 2003. Este nivel ofrece la funcionalidad previa, más características como por ejemplo: cambio de nombre de un dominio, confianza entre bosques, replicación mejorada del atributo que define la pertencia de un grupo, DCs de sólo lectura, desactivación y nueva definición de atributos y clases en el esquema, etc.
- **Windows Server 2008**. En este nivel funcional, los DCs de Windows Server 2008 son compatibles dentro del bosque con Dcs que ejecuten versiones previas a partir de Windows Server 2008. Este nivel ofrece la funcionalidad previa, pero no incorpora nuevas características.
- **Windows Server 2008 R2**. En este nivel funcional, los DCs de Windows Server 2008 R2 son compatibles dentro del mismo bosque sólo con otros Dcs que ejecuten esta versión de Windows Server. Este nivel ofrece la funcionalidad previa, más la existencia de la papelera de reciclaje del Directorio Activo, que permite restaurar objetos del directorio previamente eliminados.

Como se comentaba arriba, la transición entre niveles funcionales tanto a nivel de dominio como de bosque sólo es posible *elevando* el nivel actual, es decir, pasando a un nivel con mayor funcionalidad. La elevación de nivel funcional es, por tanto, un paso irreversible, y sólo debe hacerse cuando se está seguro de que en el futuro no van a añadirse sistemas anteriores como DCs al dominio, o al bosque.

A diferencia de versiones previas de Windows Server, durante el proceso de promoción del primer DC de un dominio/bosque se puede elegir el nivel funcional en el que se situará dicho dominio/bosque. Si posteriormente se desea elevar el nivel elegido, esta acción se realiza desde la herramienta administrativa "Dominios y Con-

fianzas de Active Directory".

4.2.4.4. Relaciones de confianza

Una relación de confianza es una relación establecida entre dos dominios de forma que permite a los usuarios de un dominio ser reconocidos por los DCs de otro dominio. Estas relaciones permiten a los usuarios acceder a los recursos de otro dominio y a los administradores definir los permisos y derechos de usuario para los usuarios del otro dominio.

Windows Server 2008 soporta varios tipos de relaciones de confianza, que veremos posteriormente. Al margen de su uso, los diferentes tipos de relaciones se diferencian en función de tres rasgos característicos:

- **Método de creación**: algunos tipos de relaciones de confianza se crean de forma automática (implícita) y otros de forma manual (explícita).
- **Dirección**: algunos tipos de relaciones son unidireccionales y otros bidireccionales. Si la relación es unidireccional, los usuarios del dominio A (de confianza) pueden utilizar los recursos del dominio B (que confía), pero no al revés. En una relación bidireccional, ambas acciones son posibles.
- **Transitividad**: algunos tipos de relaciones son transitivas y otras no. Una relación de confianza transitiva es aquella que permite que si un dominio A confía en otro B, y éste confía en un tercero C, entonces de forma automática, A confía en C. En las relaciones no transitivas, la confianza entre A y C tendría que añadirse explícitamente.

Después de ver las características de las relaciones de confianza, se explican a continuación los tipos de relaciones de confianza válidos en dominios y bosques Windows Server 2008:

- **Confianza raíz de árbol**. Esta relación se establece de forma automática entre los dominios raíz del mismo bosque. Es bidireccional y transitiva.
- **Confianza principal-secundario**. Esta relación se establece de forma automática entre un dominio dado y cada uno de sus subdominios (o dominios secundarios). Es bidireccional y transitiva.
- **Confianza de acceso directo**. Este tipo de relación debe establecerse de forma manual, y tiene como objetivo mejorar la eficiencia en los inicios de sesión remotos. Si los usuarios de un dominio A necesitan acceder frecuentemente a los re-

cursos de un dominio B, y ambos dominios se encuentran "lejos" entre sí (con muchos dominios intermedios), la confianza permite una relación directa que acorta el tiempo necesario para la autentificación de los usuarios. Es transitiva y unidireccional (si se necesita en ambos sentidos, deben crearse dos relaciones de confianza).

- **Confianza externa** . Este tipo de relación se crea manualmente y permite a usuarios de un dominio Windows 2003 acceder a recursos ubicados en dominios de otro bosque, o bien dominios Windows NT4. Es unidireccional e intransitiva.

- **Confianza de bosque** . Este tipo de relación debe crearse de forma manual entre los dominios raíz de dos bosques distintos, y permite a los usuarios de cualquier dominio de un bosque acceder a los recursos de cualquier dominio del otro bosque. Es unidireccional y sólo es transitiva entre dos bosques. Este tipo de relaciones sólo están disponibles si ambos bosques se sitúan como mínimo en el nivel funcional "Windows Server 2003".

- **Confianza de territorio** . Este tipo de relación debe crearse de forma manual entre un dominio Windows Server 2008 y un territorio (*realm*) Kerberos (versión 5) que no sea Windows, y permite interoperabilidad entre ambos. Es unidireccional y puede ser transitiva o no.

Por tanto, las relaciones de confianza automáticas (implícitas) se crean por defecto al ir añadiendo dominios al bosque, y mantienen relacionados todos esos dominios de forma bidireccional y transitiva. El efecto de estas relaciones es que de forma automática, los usuarios de cualquier dominio del bosque son conocidos (y pueden acceder a los recursos) en todos los dominios de dicho bosque. Las relaciones de confianza manuales (explícitas) están reservadas para casos en donde se busca mejorar la eficiencia o permitir interactuar con otros bosques o con dominios que no son Windows.

4.2.4.5. Unidades Organizativas

Una Unidad Organizativa (*Organizational Unit*, OU) es un objeto del Directorio Activo que puede contener a otros objetos del directorio. Es decir, es un *contenedor* de otros objetos, de forma análoga a una carpeta o directorio en un sistema de archivos tradicional. En concreto, dentro de una unidad de este tipo pueden crearse cuentas de usuario, de grupo, de equipo, de recurso compartido, de impresora compartida, etc., además de *otras* unidades organizativas. Es decir, mediante unidades organizativas podemos crear una *jerarquía* de objetos en el directorio (lo cual se asemeja otra vez a un sistema de archivos típico de Windows). Los objetos ubicados dentro de una unidad organizativa pueden moverse más tarde a otra, si fuera necesario. Sin embargo, un objeto no puede *copiarse*, ya que su nombre distinguido (que incluye la

secuencia invertida de contenedores donde se ubica hasta alcanzar el contenedor que representa el dominio) es su clave primaria en la base de datos del directorio, y por tanto debe ser único.

Por tanto, el objetivo de las unidades organizativas es *estructurar* u organizar el conjunto de los objetos del directorio, agrupándolos de foma coherente. En el Directorio Activo, las unidades organizativas permiten:

1. **Delegar la administración**. Cada unidad organizativa puede administrarse de forma independiente. En concreto, se puede otorgar la administración total o parcial de una unidad organizativa a un usuario o grupo de usuarios cualquiera. Esto permite *delegar* la administración de subconjuntos estancos del dominio a ciertos usuarios que posean el nivel de responsabilidad adecuada.

2. **Establecer de forma centralizada comportamientos distintos a usuarios y equipos**. A cada unidad organizativa pueden vincularse objetos de políticas o directivas de grupo, que aplican comportamientos a los usuarios y equipos cuyas cuentas se ubican en dicha unidad. De esta forma, podemos aplicar políticas distintas a subconjuntos de usuarios y equipos del dominio, en función exclusivamente de la unidad organizativa donde se ubican. De esta manera podríamos, por ejemplo, limitar a los usuarios del departamento (OU) de contabilidad para que sólo pudieran utilizar ciertas aplicaciones, o que no pudieran modificar el aspecto de su escritorio, pero que esto no se aplicara a los usuarios del departamento (OU) de informática.

   En este sentido, es importante conocer que en el Directorio Activo existen contenedores que no son en realidad unidades organizativas (por ejemplo, "Users" o "Computers"), y que en estos contenedores no es posible definir directivas.

En muchos sentidos, el concepto de unidad organizativa se puede utilizar en Windows 2003 de la misma forma que se entendía el concepto de dominio en versiones anteriores de Windows NT, es decir, conjunto de usuarios, equipos y recursos administrados independientemente. En realidad, en Windows Server 2008 el concepto de dominio viene más bien asociado a la implementación de DNS que exista (o quiera crearse) en la empresa.

De este modo, en muchas organizaciones de pequeño o medio tamaño resulta más adecuado implementar un modelo de dominio único con múltiples unidades organizativas que un modelo de múltiples dominios. Si es necesario, cada unidad puede administrarse independientemente, con uno o varios administradores delegados y comportamientos (políticas) diferentes.

4.2.5. Estructura física

En Active Directory, la estructura lógica está separada de la estructura física. La estructura lógica se utiliza para organizar los recursos de la organización mientras que la estructura física se utiliza fundamentalmente para configurar y administrar el tráfico de red. En concreto, la estructura física de Active Directory se compone de sitios y controladores de dominio.

La estructura física de Active Directory controla dónde y cuándo se producen el tráfico de replicación y de inicio de sesión, con lo que una buena comprensión de los componentes físicos de Active Directory permite optimizar el tráfico de red y el proceso de inicio de sesión, así como solventar problemas de replicación.

4.2.5.1. Sitios

Un sitio es una combinación de una o varias subredes IP que están conectadas por un vínculo de alta velocidad. Definir sitios permite configurar la topología de replicación y el acceso a Active Directory de forma que los sistemas Windows Server 2008 utilicen los vínculos y programas más efectivos para el tráfico de inicio de sesión y replicación.

Normalmente los sitios se crean por dos razones principalmente:

- Para optimizar el tráfico de replicación.
- Para permitir que los usuarios se conecten a un controlador de dominio concreto mediante una conexión confiable de alta velocidad.

Es decir, los sitios definen la estructura física de la red, mientras que los dominios definen la estructura lógica de la organización.

4.2.5.2. Controladores de dominio

Un controlador de dominio (*Domain Controller*, DC) es un equipo donde se ejecuta Windows Server 2008 (o una versión previa) y que almacena una replica del directorio. Los controladores de dominio ofrecen autenticación de usuarios mediante el protocolo Kerberos y consulta de información del directorio mediante el protocolo LDAP.

La información almacenada en cada controlador de dominio se divide en cuatro categorías o particiones (también denominadas contextos de nombrado): dominio, esquema, configuración y aplicación. Estas particiones del directorio constituyen las unidades de replicación:

1. **Partición del directorio de esquema**: contiene la definición de los tipos de objetos y atributos que pueden ser creados en Active Directory. Estos datos debem ser comunes a todos los dominios en el bosque, y por tanto los datos del esquema se replican a todos los controladores de dominio del bosque. Sólo existe un DC en cada bosque donde puede modificarse el esquema, y por lo tanto en el resto de DCs esta partición es de sólo lectura.

2. **Partición de directorio de configuración**: contiene la estructura de los dominios y la topología de replicación. Estos datos son comunes a todos los dominios en el bosque, y por tanto se replican a todos los controladores de dominio en el bosque. Cualquier DC del bosque puede modificar esta partición, en cuyo caso las modificaciones deben replicarse al resto de DCs del bosque.

3. **Partición de directorio de dominio**: contiene todos los objetos del directorio para este dominio (usuarios, grupos, ordenadores, etc.). Dichos datos se replican a todos los controladores de ese dominio, pero no a otros dominios.

4. **Particiones de directorio de aplicaciones**: contienen datos específicos de aplicación. Estos datos pueden ser de cualquier tipo excepto *principales de seguridad* (es decir, cuentas de usuarios, grupos y equipos). En este caso, se tiene un control fino sobre el ámbito de la replicación y la ubicación de las réplicas. Este tipo de partición está disponible a partir de Windows Server 2003. Si al instalar el primer DC del bosque se elige integrar la configuración de DNS en Active Directory (opción por defecto), el servidor DNS utiliza dos de estas particiones (`ForestDNSZones` y `DomainDNSZones`).

Además de estas cuatro particiones de directorio, existe una quinta categoría de información que puede almacenarse en un controlador de dominio: el catálogo global, que se describe en la siguiente sección.

4.2.5.3. Funciones de los controladores de dominio

En los orígenes de Windows NT Server, un dominio podía incorporar múltiples controladores de dominio pero sólo se permitía que uno de ellos actualizase la base de datos del directorio. Este esquema de funcionamiento, denominado "de maestro único", exigía que todos los cambios se replicasen desde el controlador de dominio principal (*Primary Domain Controller*, PDC) a los controladores de dominio secundarios o de reserva (*Backup Domain Controllers*, BDCs).

A partir de Windows 2000, todos los controladores de dominio admiten cambios, y estos cambios se replican al resto de los controladores de dominio, mediante lo que se denomina replicación multi-maestro. Las acciones habituales de administración de usuarios, grupos, equipos, etc., son operaciones típicas de múltiples maes-

tros (y por tanto pueden realizarse en cualquiera de los controladores del dominio).

Sin embargo, en algunos casos concretos, no resulta práctico que algunos cambios se permitan en múltiples maestros, debido a un excesivo tráfico de replicación y a posibles conflictos de operaciones muy básicas y/o muy poco frecuentes. Por estos motivos, existen una serie de funciones especiales, como la de catálogo global, o las denominadas de maestro único, que se asignan sólo a determinados controladores dentro de un dominio, o inclusive en todo el bosque. A continuación veremos estas funciones.

4.2.5.4. Servidor de catálogo global

El *catálogo global* una partición de sólo lectura que almacena una copia parcial de las particiones de dominio de todos los dominios del bosque. La copia es parcial porque, aunque incorpora todos los objetos de cada dominio, de cada uno sólo almacena un subconjunto reducido de atributos. En particular, se guardan aquellos que se utilizan más frecuentemente para las consultas (esto puede configurarse en el esquema). Por otro lado, el catálogo global incorpora la información necesaria para determinar la ubicación de cualquier objeto del directorio.

Un servidor de catálogo global es un controlador de dominio que almacena una copia del catálogo y procesa las consultas al mismo. En cada bosque debe existir al menos un DC configurado como servidor de catálogo global, y esta función puede incorporarse a cualquier otro DC del bosque que se desee. Por defecto, el primer controlador de dominio que se crea en el bosque se configura automáticamente como un servidor de catálogo global. En función de la cantidad de dominios y de la topología de la red, puede ser conveniente definir otros servidores de catálogo global, con el fin de equilibrar el tráfico de autenticación de inicios de sesión y la transferencia de consultas.

El catálogo global cumple dos funciones importantes en el directorio:

- Permite que un usuario inicie una sesión en la red mediante el suministro de la información de pertenencia a grupos universales a un controlador de dominio durante el proceso de inicio de sesión. La pertenencia de los grupos universales se almacena sólo en los catálogos globales.
- Permite que un usuario busque información de directorio en todo el bosque, independiente de la ubicación de los datos.

4.2.5.5. Operaciones de maestro único

Un maestro de operaciones es un controlador de dominio al que se le ha asignado una o varias funciones de maestro único en un dominio o bosque de Active Directory. Los controladores de dominio a los que se les asignan estas funciones realizan operaciones que no pueden ocurrir simultáneamente en otros controladores de dominio de la red. La propiedad de estas operaciones de maestro único puede ser transferida a otros controladores de dominio.

Todos los bosques de Active Directory deben tener controladores de dominio que incorporen las dos siguientes operaciones de maestro único (por defecto, estas funciones las posee el primer controlador que se instala en el bosque):

- **Maestro de esquema**. El controlador de dominio maestro de esquema controla todas las actualizaciones y modificaciones del esquema. La partición de esquema se replica a todos los controladores del bosque, pero sólo en uno de ellos (el maestro de esquema), dicha partición es de lectura/escritura.

- **Maestro de nombres de dominio**. El controlador de dominio maestro de nombres de dominio controla las operaciones de agregar, quitar y renombrar dominios del bosque, asegurando que los nombres de dominio sean únicos en el bosque. Asimismo, este controlador debe autorizar la creación o eliminación de particiones de aplicación en cualquier dominio del bosque.

Todos los dominios de Active Directory deben tener controladores de dominio que cumplan las siguientes tres operaciones de maestro único (por defecto, estas funciones las posee el primer controlador que se instala en el dominio):

- **Maestro de identificadores relativos (RID)**. El controlador de dominio maestro de RID asigna secuencias de identificadores relativos a cada uno de los distintos controladores de su dominio. Con eso se garantiza que dos controladores de dominio no pueden asignar el mismo SID a dos objetos principales de seguridad (usuarios, grupos o equipos).

  Cuando un controlador de dominio crea un objeto de usuario, grupo o equipo, asigna al objeto un identificador de seguridad único (SID). Este identificador está formado por un identificador de seguridad de dominio, que es el mismo para todos los que se crean en el dominio, y un identificador relativo que es único para cada identificador de seguridad que se crea en ese dominio.

- **Emulador de controlador de dominio principal (PDC)**. Aunque la compatibilidad a nivel de servidor con sistemas Windows NT4 se ha eliminado en Windows Server 2008, el emulador de PDC aún es necesario para dos funciones. En primer lugar, para autenticar usuarios que inicien sesión en miembros del dominio pre-

vios a Windows 2000. Y en segundo lugar, siempre que se cambia la contraseña de un usuario en un DC concreto, se realiza una replicación de urgencia de dicho cambio en el emulador de PDC del dominio. En este sentido, si un inicio de sesión falla por contraseña incorrecta, se reintenta el inicio en el emulador de PDC, por si hubiera habido un cambio reciente de contraseña y éste no hubiera llegado aún a todos los DCs.

- **Maestro de infraestructuras**. Cuando un objeto se mueve de unidad organizativa (es decir, cambia de nombre) o se borra, es necesario actualizar la pertenencia de grupos de otros dominios que pudieran contener a dicho objeto. El maestro de infraestructuras es el responsable de actualizar los identificadores de seguridad y nombres completos en las referencias de objetos entre dominios.

4.3. Objetos que administra un dominio

El Directorio Activo, tal como se ha visto en secciones anteriores, es en realidad una base de datos jerárquica de *objetos*, que representan las entidades que pueden administrarse en una red de ordenadores, o, más correctamente en nuestro caso, en un *dominio* de sistemas Windows Server 2008. Esta base de datos de objetos de administración es compartida, para consulta, por todos los ordenadores miembros del dominio y, para modificación, por todos los controladores del dominio (o DCs, *Domain Controllers*).

Por tanto, en Windows Server 2008, la gestión de un dominio puede realizarse de forma centralizada, administrando únicamente el Directorio Activo. En el contexto particular de este capítulo, "administrar" significa crear y configurar adecuadamente los objetos de directorio que representan a las entidades o *recursos* que existen en el dominio (recursos como usuarios, grupos, equipos, directivas, etc.).

Este apartado expone en detalle los tipos de objetos más relevantes que pueden crearse en el Directorio Activo de Windows Server 2008, planteando en cada caso sus opciones de configuración principales y su utilidad dentro de la administración del dominio.

4.3.1. Usuarios globales

En la administración de sistemas Windows independientes, o administración *local*, se pueden crear en cada sistema cuentas de usuario y de grupo, que sirven para:

1. identificar y autenticar a las personas (usuarios) que deben poder acceder al sistema, y

2. administrar los permisos y derechos que permitirán aplicar el control de acceso adecuado a dichos usuarios en el sistema.

Por lo tanto, en el contexto de la protección local, si una persona debe trabajar en varios ordenadores de la organización, necesita poseer una cuenta de usuario en cada uno de ellos. Como veremos a continuación, al disponer de un dominio, esto no es necesario.

En un dominio Windows Server 2008, cualquier servidor que actúa como DC puede crear cuentas de usuario global, también denominadas cuentas de *usuario del dominio*. Las cuentas de usuario del dominio se almacenan en el Directorio Activo y por tanto son conocidas por todos los ordenadores del dominio; en realidad, por sus definición en el esquema, las cuentas de usuario son visibles en todos los ordenadores del *bosque*, es decir, de toda la organización. Un usuario puede utilizar su cuenta del dominio para acceder a recursos situados en cualquier dominio del bosque, es decir, a dicha cuenta se le pueden asignar individualmente permisos y derechos en cualquier recurso y ordendor de la organización. Para ello, resulta necesario poder distinguir unívocamente entre cualquier usuario de cualquier dominio del bosque a efectos de asignación y protección de recursos. Por ello, cada cuenta de usuario tiene un SID único en el bosque. Internamente, este SID consta de dos partes: un prefijo común a todas las cuentas del mismo dominio, y un identificador relativo (RID), que es único para las cuentas dentro de dicho dominio. En un dominio Windows Server 2008 existen otros tipos de cuentas que poseen este atributo, como por ejemplo grupos y equipos (ordenadores). Por ello, estos tipos de cuentas se conocen como "principales de seguridad".

Cuando una persona inicia sesión en cualquier ordenador del bosque utilizando para ello su cuenta de usuario del dominio, el ordenador en cuestión realiza una consulta al Directorio Activo (en particular, a alguno de los DCs del dominio donde se creó la cuenta), para que se validen las credenciales del usuario. El resultado de la validación es enviado al ordenador donde se está iniciando la sesión, concediendo o rechazando la conexión.

Los ordenadores miembros de un dominio que no sean DCs, además de reconocer a los usuarios del dominio, pueden crear también sus propios usuarios *locales*. En este caso, estos usuarios son únicamente visibles en el ordenador en el que han sido creados. Cuando una persona inicia sesión en un sistema Windows miembro del dominio utilizando una cuenta local, dicha cuenta se valida contra la base de datos local de ese ordenador. Además, es importante resaltar que a dicho usuario local no se le pueden asignar permisos sobre recursos que residan en otro sistema del dominio/bosque, puesto que allí no existe. Para evitar confusiones, en lo sucesivo nos referiremos a las cuentas de usuario creadas en el Directorio Activo simplemente como "usuarios", y como "usuarios locales" a las cuentas creadas localmente en sistemas

independientes o miembros del dominio.

Al crear una cuenta de usuario en el Directorio Activo, en la ficha de creación correspondiente aparecen varios nombres distintos: "nombre de pila", "nombre para mostrar", "nombre completo", "nombre de inicio de sesión de usuario" y "nombre de inicio de sesión (anterior a Windows 2000)". Entre ellos, sólo los dos últimos se pueden utilizar para identificar a los usuarios en los procesos de inicio de sesión (los otros nombres almacenan la información sobre la "persona" que hay detrás de cada cuenta de usuario). Entre los dos últimos nombres existen diferencias significativas:

- **Nombre de inicio de sesión**. Este es el identificador nativo en Windows Server 2008 para iniciar sesión en sistemas Windows de cualquier dominio del bosque. Posee dos partes: un identificador de usuario, seguido del símbolo "@" y un nombre de dominio (por ejemplo, "pepito@admon.lab"). Este nombre también se conoce como nombre principal del usuario (*User Principal Name*, o UPN). La ventaja de el UPN es que el nombre del dominio añadido al identificador del usuario no tiene porqué coincidir con el dominio donde se ha creado la cuenta. Por lo tanto, el UPN de cada usuario debe ser único en el *bosque*. La ventaja de los UPNs es que el nombrado de los usuarios es independiente de los dominios de origen, y puede coincidir, por ejemplo, con la dirección de correo electrónico del usuario, para mayor comodidad.

- **Nombre de inicio de sesión (anterior a Windows 2000)**. Este es el identificador que se mantiene para permitir inicios de sesión en sistemas previos a Windows 2000. Posee dos partes: el nombre NetBios del dominio donde se crea la cuenta, seguido del símbolo "\" y el nombre de inicio de sesión del usuario (siguiendo con el ejemplo anterior, "ADMON\pepito"). En este caso, puesto que el nombre siempre incluye el identificador del dominio de origen de la cuenta, el nombre de inicio de sesión del usuario debe ser único en el dominio donde se crea.

Al crear un dominio, se crea por defecto una cuenta denominada "Administrador", que es quien posee capacidades administrativas completas en el dominio, es decir, tanto en la base de datos del Directorio Activo como en cada ordenador miembro del dominio, al mismo nivel que su administrador local. Esta cuenta no puede borrarse ni bloquearse, pero sí renombrarse, por motivos de seguridad.

4.3.2. Grupos

De forma análoga a los usuarios, existen *grupos* que son almacenados en el Directorio Activo y que por tanto son visibles desde todos los ordenadores del dominio (y, en algunos casos, también de otros dominios del bosque). En el directorio pueden crearse dos tipos de grupos: grupos de distribución y grupos de seguridad. Los primeros se utilizan exclusivamente para crear listas de distribución de correo electró-

nico, mientras que los segundos son principales de seguridad, y por tanto son los que se utilizan con fines administrativos. Por este motivo, a partir de ahora nos referiremos exclusivamente a los grupos de seguridad.

En concreto, en dominios Windows Server los grupos de seguridad pueden definirse en tres *ámbitos* distintos: Grupos locales de dominio, grupos globales y grupos universales. A continuación se explican las diferencias entre ellos:

1. **Grupos locales de dominio**. Pueden contener cuentas de usuario de cualquier dominio del bosque, así como cuentas de grupos globales o universales de cualquier dominio del bosque, y otros grupos locales de dominio del mismo dominio (anidamiento). Sólo son visibles en el dominio en que se crean, y suelen utilizarse para administrar recursos (mediante la concesión de permisos y derechos) situados en cualquiera de los ordenadores del dominio.

2. **Grupos globales**. Pueden contener usuarios del mismo dominio, así como otros grupos globales de dicho dominio (anidamiento). Son visibles en todos los dominios del bosque, y suelen utilizarse para agrupar a los usuarios de manera amplia, en función de las labores que realizan o los roles que juegan en el dominio.

3. **Grupos universales**. Pueden contener cuentas de usuario y grupos globales, así como otros grupos universales (anidamiento), de cualquier dominio del bosque. Son visibles en todo el bosque, y suelen utilizarse para administrar recursos (mediante la concesión de permisos y derechos) situados en ordenadores de varios dominios del bosque.

En un ordenador miembro de un dominio también se pueden definir grupos locales. Los grupos locales pueden estar formados por cuentas de usuario locales y usuarios y grupos globales y universales de cualquier dominio del bosque. Los grupos locales no admiten anidamiento, es decir, un grupo local no puede ser miembro de otro grupo local. Los grupos locales pueden utilizarse para administrar recursos en el equipo en que son creados. Sin embargo, ei el ordenador es un miembro del dominio, se recomienda administrar sus recursos mediante grupos locales del dominio, por dos motivos: primero, porque se consigue una centralización de todas las cuentas en el dominio (los ordenadores miembros son liberados de esta tarea), y segundo, porque las cuentas almacenadas en el Directorio Activo son replicadas entre los DCs del dominio, y por tanto se incrementa la tolerancia a fallos ante una catástrofe.

En particular, la regla que se recomienda a la hora de utilizar los grupos en dominios Windows Server 2008 es la siguiente:

1. Asignar usuarios a grupos globales, según las labores que desempeñen en la organización.

2. Incluir (usuarios y/o) grupos globales en grupos locales del dominio según el nivel de acceso que vayan a tener en los recursos del dominio.

3. Asignar permisos y derechos únicamente a estos grupos locales del dominio en dichos recursos.

La utilización de grupos universales está recomendada en casos en los que un mismo conjunto de usuarios (y/o grupos) pertenecientes a varios dominios deben recibir acceso a recursos situados en dominios distintos. Desde el punto de vista de su formación y de su visibilidad, los grupos universales son los más flexibles que pueden crearse en el Directorio Activo, pero esta flexibilidad tiene un coste asociado, que incluye dos aspectos. En primer lugar, la lista completa de miembros de un grupo universal se debe replicar al catálogo global, a diferencia de los grupos locales de dominio o globales, para los que la lista de miembros sólo se almacena en el dominio donde se crea el grupo. Por tanto, siempre que se modifica la lista de miembros de un grupo universal, el cambio hay que replicarlo en todos los DCs que sean catálogos globales en el bosque. Y en segundo lugar, la pertenencia de los usuarios a grupos universales puede afectar su habilidad de iniciar sesión. Cada vez que un usuario inician sesión en un sistema de cualquier dominio del bosque, el DC del dominio donde se autentica la cuenta del usuario debe contactar con un servidor de catálogo global para que éste le informe de posibles grupos universales a los que pertenece. Si en ese momento el servidor de catálogo global no está disponible, el inicio de sesión puede fallar.

Ambos problemas, detectados desde la aparición de grupos univresales en Windows 2000, han sido suavizados con la aparición de versiones más modernas de Windows Server. En particular, el problema del alto tráfico de replicación al cambiar la lista de miembros se debía a que en Windows 2000, la replicación de cualquier cambio en la lista de miembros incluía necesariamente la lista completa, ya que se trata de un solo atributo del objeto grupo. Si elevamos el nivel funcional del dominio al menos a "Windows Server 2003", la estrategia de replicación de atributos multivaludos utiliza un esquema de valores enlazados, que permite replicar sólo los valores (miembros del grupo) que han cambiado, disminuyendo mucho el tráfico de replicación. Respecto al problema de inicio de sesión cuando el servidor de catálogo global no está disponible, a partir de Windows Server 2003 se ha incorporado la posibilidad de que cuando un DC consulta la pertenencia de un usuario a grupos globales en el catálogo global, guarde dicha pertencia en una caché, y luego la actualice periódicamente; de esta manera, mientras esa información siga actulizada en la caché, no es necesario volver a contactar con el catálogo global cuando dicho usuario inicie sesión en el dominio.

Existen numerosos grupos creados por defecto en Active Directory, tanto en el contenedor "Builtin" como en el contenedor "Users". En el primer caso, los grupos son los equivalentes a los que encontramos como grupos locales por defecto en cualquier sistema Windows independiente o miembro del domino: básicamente, los grupos que tienen concedidos ciertos accesos predeterminado en el propio sistema, tales como "Administradores", "Usuarios", "Operadores de Copia", etc. En el segundo caso, los grupos son propios del Directorio Activo, y su uso tiene relación con ciertas niveles de acceso preasignados en el directorio, aunque en la mayoría de casos, estos grupos están inicialmente vacíos. Entre estos grupos encontramos los siguientes:

- **Admins. del domino**. Tienen derechos administrativos sobre toda la base de datos del Directorio Activo del dominio, así como localmente en cada DC y cada miembro del dominio.
- **Usuarios del domino**. Los miembros de este grupo se consideran usuarios convencionales en el dominio. Cada vez que se añade un usuario al dominio, su cuenta se hace miembro de este grupo automáticamente.
- **Administradores de empresas**. Tienen derechos administrativos sobre toda la base de datos del Directorio Activo del bosque.
- **Propietarios del creador de directivas de grupo (*Group Policy Creator Owners*)**. Pueden crear nuevos objetos de directiva o política de grupo (GPO) en el dominio.

En relación con esto, es importante saber que cuando un sistema Windows pasa a ser miembro de un dominio, el grupo global `Admins. del dominio` se incluye automáticamente en el grupo local `Administradores` de dicho sistema. De igual forma, el grupo global `Usuarios del dominio` se incluye dentro del grupo local `Usuarios`. De esta forma, los administradores y usuarios normales del dominio tienen en cada miembro los mismos derechos y permisos que los que tengan ya definidos los administradores y usuarios locales, respectivamente.

4.3.3. Equipos

Como hemos visto, en el Directorio Activo de un dominio se conserva toda la información relativa a cuentas de usuarios y grupos globales. Esta misma base de datos de directoio recoge también una *cuenta de equipo* por cada uno de los ordenadores del dominio, tanto de los DCs como de los sistemas miembro. En particular, las cuentas de los DCs se ubican en la unidad organizativa denominada "DomainControllers", mientras que las del resto de ordenadores se ubican por defecto en el contenedor "Computers" (ambos contenedores se sitúan justo debajo del contenedor

que representa el dominio).

Entre otros datos, la cuenta de equipo que cada ordenador posee en el dominio incluye los siguientes atributos:

- **Nombre del equipo**. Coincide con el nombre que el equipo tiene, sin contar con su sufijo DNS.
- **Contraseña**. Cada equipo posee una contraseña que el ordenador utiliza para acreditarse en el dominio, de forma análoga a los usuarios cuando inician sesión. Esta contraseña se genera automáticamente cuando se agrega el equipo al dominio, y se cambia automáticamente cada 30 días.
- **SID**. Cada equipo posee un SID, igual que ocurre con las cuentas de usuario y de grupo (por ello, los tres tipos de cuentas se denominan genéricamente "principales de seguridad"). El hecho de que posea un SID permite a una cuenta de usuario el que se le concedan permisos y derechos sobre recursos del dominio, bien directamente, o bien mediante la pertenencia a un grupo que a su vez tenga permisos sobre los recursos.

  Por ejemplo, la aplicación de una objeto de directiva de grupo (GPO) sobre un equipo del dominio requiere que, además de que el equipo esté situado bajo el ámbito del GPO, el equipo tenga concedidos los permisos "Leer" y "Aplicar directiva" del objeto GPO. En caso contrario, las políticas definidas en el GPO no se aplicarían sobre el equipo.

Windows Server 2008 incorpora dos protocolos que implementan la autenticación de sistemas y usuarios en el proceso de acceso a los recursos en el dominio. Estos protocolos son on NTLM y Kerberos V5. NTLM era el protocolo de autenticación nativo en dominios Windows NT4, y se mantiene básicamente por compatibilidad hacia atrás con estos sistemas. Con el tiempo se han ido generado versiones más modernas de NTLM que mejoran aspectos de seguridad (por ejemplo, la última versión, NTLMv2, incorpora un protocolo de cifrado de 128 bits). Sin embargo, si todos los sistemas del dominio incorporan las versiones Windows 2000, Windows XP o versiones más modernas, la autenticación por defecto en el dominio utiliza el protocolo Kerberos. Entre otros, hay tres motivos motivos fundamentales por los que Kerberos es preferible sobre NTLM:

1. En NTLM, el servidor autentifica al cliente. En Kerberos, la autentificación es *mutua*, con lo que en la interacción entre servidor y cliente, cada uno autentica al otro, y se garantiza que ninguno de ambos han sido suplantados.
2. En NTLM, cada vez que un usuario del dominio intenta acceder a un recurso si-

tuado en un servidor, dicho servidor tiene que contactar con un DC para autenticar al usuario. En Kerberos, el ordenador cliente (donde está trabajando el usuario) obtiene un tiquet del DC con el que puede acceder a múltiples servidores del dominio, sin que dichos servidores tengan que volver a contactar con el DC.

3. Las confianzas en NTLM son manuales, unidireccionales y no transitivas. En el caso de Kerberos, las confianzas son bidireccionales y transitivas, y se configuran automáticamente conforme se añaden dominios al bosque. Además, Kerberos admite confianzas entre bosques y entre dominios Kerberos que no sean Windows.

4.3.4. Unidades Organizativas

Como hemos visto en Sección 4.2.4.5, "Unidades Organizativas", las Unidades Organizativas (*Organizational Units*) o UOs, son objetos del directorio que a su vez, pueden contener otros objetos. El uso fundamental de las UOs es delegar la administración de sus objetos a otros usuarios del dominio distintos del Administrador, así como personalizar el comportamiento de los usuarios y/o equipos mediante la aplicación de directivas de grupo (GPOs) específicas a la unidad.

4.4. Compartición de recursos

Cuando un sistema Windows Server 2008 participa en una red (grupo de trabajo o dominio), puede compartir sus recursos con el resto de ordenadores de la red. En este contexto, sólo vamos a considerar como recursos a compartir las *carpetas* que existen en los sistemas Windows del dominio. La compartición de otros recursos (tales como impresoras, por ejemplo) queda fuera del ámbito de este texto.

4.4.1. Permisos y derechos

Cualquier sistema Windows Server 2008 puede compartir carpetas, tanto si es un servidor como si es una estación de trabajo, tanto si se encuentra formando parte de un dominio como si se trata de un sistema independiente. Para poder compartir una carpeta basta con desplegar su menú contextual desde una ventana o desde el explorador de archivos, y seleccionar `Compartir...`. En la ventana asociada a esta opción se determina el nombre que tendrá el recurso (que puede ser distinto del nombre de la propia carpeta), así como la lista de permisos que controlará qué usuarios y grupos van a poder acceder al mismo. En este sentido, existe una gran diferencia entre que la carpeta resida en una partición FAT y que lo haga en una de tipo NTFS, como se presenta a continuación.

Si la carpeta reside en una partición FAT, este filtro de acceso es el único que determinará qué usuarios y grupos van a poder acceder al contenido de la carpeta, puesto que este tipo de sistema de archivos no incorpora la posibilidad de definir permisos sobre las carpetas y los ficheros almacenados en el. Es decir, en este caso los permisos *del recurso* constituyen el único filtro que controlará el acceso al mismo y a todo su contenido. Si un usuario tiene permisos suficientes para conectarse a un recurso, tendrá ese mismo acceso sobre todos los archivos y subcarpetas del recurso. A este nivel, existen sólo tres permisos distintos que pueden concederse a cada usuario/grupo: `Lectura`, `Escritura` y `Control Total`.

Por el contrario, si la carpeta que vamos a compartir se encuentra en una partición NTFS, la propia carpeta y cada uno de sus subcarpetas y archivos tendrá unos permisos establecidos, siguiendo con el modelo de permisos de NTFS, al margen de que se comparta o no. En este caso también es posible establecer permisos al propio recurso desde la ventana de `Compartir...`, pero entonces sólo los usuarios que puedan pasar *ambos* filtros podrán acceder a la carpeta compartida y a su contenido. En este caso se recomienda dejar `Control Total` sobre `Todos` en los permisos asociados al recurso (opción por defecto), y controlar quién y cómo puede acceder al recurso y a su contenido mediante los permisos asociados a dicha carpeta y a sus archivos y subcarpetas. En Windows Server 2008 esta es la opción por defecto, aunque no lo era en Windows Server 2003, que sólo concedía inicialmente el permiso de lectura al grupo `Todos` al compartir una carpeta.

Esta recomendación es muy útil, si tenemos en cuenta que de esta forma para cada carpeta del sistema no utilizamos dos grupos de permisos sino uno solo, independientemente de que la carpeta sea o no compartida. Este forma de trabajar obliga al administrador a asociar los permisos correctos a cada objeto del sistema (aunque no esté compartido), pero por otra parte se unifica la visión de la seguridad de los archivos y carpetas, con lo que a la larga resulta más segura y más sencilla.

Cuando compartimos recursos a otros usuarios en la red, especialmente cuando se trata de un dominio/bosque, hay que tener en cuenta no sólo los permisos del recurso y de la propia carpeta, sino también los *derechos* del ordenador que comparte el recurso. En concreto, si un usuario desea acceder a una carpeta compartido por un determinado ordenador, además de tener suficientes permisos (sobre el recurso y sobre la propia carpeta y su contenido) necesita tener concedido en dicho ordenador el derecho denominado "Tener acceso a este equipo desde la red". Normalmente, este filtro se encuentra abierto para todos los usuuarios, ya que la opción por defecto en todos los sistemas Windows es que este derecho esté concedido al grupo "Todos". El Administrador puede, si lo desea, restringir este derecho, limitando quiénes pueden acceder a recursos en dicho ordenador a través de la red. Sin embargo, hay que advertir que esta acción es muy delicada, y debe probarse de manera exhaustiva para evitar que produzca fallos en otros servicios de red proporcionados por el orde-

nador.

4.4.2. Compartición dentro de un dominio

Cuando la compartición de recursos la realizan equipos que forman parte de un dominio Windows, existen consideraciones que el administración debe conocer.

Primero, una vez se ha compartido físicamente una carpeta en la red (según el procedimiento descrito arriba), el Administrador del dominio puede además *publicar* este recurso en el directorio. Para ello debe crear un nuevo objeto, en la unidad organizativa adecuada, de tipo `Recurso compartido`. A este objeto se le debe asociar un nombre simbólico y el nombre de recurso de red que representa (de la forma `\\equipo\recurso`). Es importante tener en cuenta que cuando se publica el recurso de esta forma, no se comprueba si realmente existe o no, por lo que es responsabilidad del administrador el haberlo compartido y que su nombre coincida con el de la publicación. Una vez publicado, el recurso puede localizarse mediante búsquedas en el Directorio Activo, como el resto de objetos del mismo, tanto por nombre como por palabras clave (descripción).

Y segundo, cuando un sistema Windows Server (Windows 2000, Windows Server 2003, etc.) se agrega a un dominio, los siguientes recursos se comparten de forma automática y por defecto (estas comparticiones no deben modificarse ni prohibirse):

- `letra_de_unidad$`. Por cada partición existente en el sistema Windows Server (`C:`, `D:`, etc.) se crea un recurso compartido denominado `C$`, `D$`, etc. Los administradores del dominio, así como los operadores de copia del domino, pueden conectarse por defecto a estas unidades. Esto permite acceso centralizado a los sistemas de archivos locales de cada sistema miembro del dominio.

- `ADMIN$`. Es un recurso utilizado por el propio sistema durante la administración remota de un ordenador Windows Server.

- `IPC$`. Recurso que agrupa los tubos (colas de mensajes) utilizados por los programas para comunicarse entre ellos. Se utiliza internamente durante la administración remota de un ordenador Windows Server, y cuando se observa los recursos que comparte.

- `NETLOGON`. Recurso que exporta un DC para proporcionar a los ordenadores miembros del dominio el servicio de validación de cuentas globales a través de la red (*Net Logon service*), que se mantiene por compatibilidad hacia atrás con sistemas Windows anteriores a Windows 2000 o Windows XP.

- `SYSVOL`. Recurso que exporta cada DC de un dominio. Contiene ciertos datos

asociados del Directorio Activo distintos de la base de datos del directorio (por ejemplo, de directivas de grupo) que deben replicarse en todo los DCs del dominio.

En relación con los nombres de estos recursos, es interesante saber que añadir el carácter "$" al final de cualquier nombre de recurso tiene un efecto específico: cuando exploramos los recursos compartidos por un sistema en la red, aquellos que acaban en este símbolo no se visualizan. Es decir, el recurso no es visible desde otros sistemas Windows de la red, y por tanto un usuario remoto sólo podrá conectarse al mismo si conoce su nombre de antemano (y tiene suficientes permisos, obviamente).

4.4.3. Mandatos Windows Server para compartir recursos

La compartición de recursos en Windows Server puede realizarse en línea de órdenes utilizando los mandatos **net share** y **net use**. La sintaxis de ambos mandatos es la siguiente:

1. Mandato **net share**: Crea, elimina o muestra recursos compartidos.

```
net share
net share recurso_compartido
net share recurso_compartido=unidad:ruta_de_acceso
          [/users:número | /unlimited] [/remark:"texto"]
net share recurso_compartido [/users:número | unlimited]
          [/remark:"texto"]
net share {recurso_compartido | unidad:ruta_de_acceso} /delete
```

2. Mandato **net use**: Conecta o desconecta un equipo de un recurso compartido o muestra información acerca de las conexiones del equipo. También controla las conexiones de red persistentes.

```
net use  [nombre_dispositivo]
         [\\nombre_equipo\recurso_compartido[\volumen]]
         [contraseña | *]] [/user:[nombre_dominio\]nombre_usuario]
         [[/delete] | [/persistent:{yes | no}]]
net use nombre_dispositivo [/home[contraseña | *]]
         [/delete:{yes | no}]
net use  [/persistent:{yes | no}]
```

4.5. Delegación de la administración

Para delegar, total o parcialmente, la administración de una unidad organizativa

existe un asistente (o *wizard*) que aparece cuando se selecciona la acción `Delegar control...` en el menú contextual de la unidad organizativa. Este asistente pregunta básicamente los dos aspectos propios de la delegación: *a quién* se delega y *qué* se delega. La primera pregunta se contesta o bien con un usuario o con un grupo (se recomienda un grupo). Para responder a la segunda pregunta, se puede elegir una tarea *predefinida* a delegar (de entre una lista de tareas frecuentes), o bien podemos optar por construir una tarea personalizada. En este último caso, tenemos que especificar la tarea mediante un conjunto de permisos sobre un cierto tipo de objetos del directorio. Esto se explica a continuación.

Internamente, los derechos de administración (o control) sobre los objetos de un dominio o unidad organizativa funcionan de forma muy similar a los permisos sobre una carpeta NTFS: existe una DACL propia y otra heredada, que contienen como entradas aquellos usuarios/grupos que tienen concedida (o denegada) una cierta acción sobre la unidad organizativa o sobre su contenido. En este caso, las acciones son las propias de la administración de objetos en el directorio (control total, creación de objetos, modificación de objetos, consulta de objetos, etc.), donde los "objetos" son las entidades que pueden ser creados dentro de la unidad: usuarios, grupos, unidades organizativas, recursos, impresoras, etc.

En resumen, la delegación de control sobre una unidad organizativa puede hacerse de forma completa (ofreciendo el *Control Total* sobre la unidad) o de forma parcial (permitiendo la lectura, modificación y/o borrado de los objetos de la misma). Hay que tener en cuenta que en el caso de la delegación parcial, el número de posibilidades es inmenso: por una parte, se incluye la posibilidad de establecer el permiso sobre cada *atributo* de cada tipo de objeto posible; por otra parte, se puede establecer a qué unidades se va a aplicar la regla (sólo en esa unidad organizativa, en todas las que se sitúan por debajo, en parte de ellas, etc.). Por tanto, para una delegación parcial se recomienda el uso del asistente, ya que su lista de delegación de tareas más frecuentes (como por ejemplo "Crear, borrar y administrar cuentas de usuario" o "Restablecer contraseñas en cuentas de usuario") resulta muy útil. Sin embargo, cuando la delegación que buscamos no se encuentra en la lista, tendremos que diseñar una a medida, asignando los permisos oportunos sobre los objetos del directorio que sean necesarios.

5

Administración de Políticas de Grupo

Indice

5.1. Introducción

Este capítulo introduce una de las herramientas que incluye Windows Server 2008 para centralizar la administración y configuración de usuarios y equipos en un dominio: las *Políticas o Directivas de Grupo* (*Group Policies*). Las políticas de grupo permiten establecer de forma centralizada múltiples aspectos de la configuración que reciben los equipos cuando arrancan, así como los usuarios cuando inician sesión en dichos equipos del dominio. Estos aspectos incluyen, entre otros, configuraciones del registro, políticas de seguridad, instalación automática de software, ejecución de *scripts*, redirección de carpetas locales a recursos de red, etc.

5.2. Objeto de Política de Grupo (GPO)

En cada sistema Windows Server, forme parte o no de un dominio, existe una *política local* que el administrador puede editar según su criterio para ajustar el comportamiento de dicho equipo, y de los usuarios que inicien sesión en él. A este respecto, los sistemas Windows Server 2008 incorporan la posibilidad de definir varias políticas locales en cada equipo; esta posibilidad es útil en entornos en donde los sistemas forman parte de grupos de trabajo en lugar de dominios, pero como vamos a centrarnos en la definición de políticas en un dominio, esta posibilidad queda fuera del ámbito de este texto.

En cualquier caso, haya una única política local por equipo o varias, cuando un administrador debe configurar múltiples equipos, resulta incómodo tener que establecer sus configuraciones y comportamientos uno por uno, especialmente si se da el caso que varios de ellos deben compartir parte o toda la configuración. Por este motivo, las políticas de grupo se han integrado dentro de la administración del Directorio Activo como una utilidad de configuración centralizada en dominios Windows Server. Para ello, se incorpora una herramienta denominada "Administración de directivas de grupo", cuya interfaz se muestra en la Figura 5.1, “Herramienta Adminstración de directivas de grupo en Windows 2008”.

En concreto, las políticas se especifican mediante objetos del Directorio Activo denominados *Objetos de Directiva de Grupo* (*Group Policy Objects*), o simplemente GPOs. Un GPO es un objeto que incluye como atributos cada una de las directivas o políticas que pueden aplicarse centralizadamente a equipos y a usuarios en sistemas Windows (tanto servidores como Windows Server 2003 o Windows Server 2008, como clientes, como Windows XP, Windows Vista o Windows 7). En ocasiones, las políticas disponibles dependen de la versión concreta que ejecutan los DCs y los miembros del dominio. Desde el punto de vista de los DCs, los GPOs de Windows Server 2008 incluyen todas las políticas soportadas tanto por esta versión de Windows como por todas las versiones previas (a partir de Windows 2000). Desde el punto de

vista de un equipo miembro, si en algún caso su versión de Windows no soporta una política que se le aplica desde un GPO, simplemente ignora dicha política.

La forma de utilizar GPOs es la siguiente: en primer lugar, creamos el GPO. Esto genera una plantilla que incorpora todas las posibles políticas que el GPO puede incluir (cuyo número es fijo), pero inicialmente todas se encuentran en estado *no configurado*. Es decir, si queremos que cualquiera de ellas se aplique, primero debemos configurarla adecuadamente. En algunas ocasiones, es simplemente un valor binario, y en otras hay que incluir más opciones de configuración (por ejemplo, en el caso de un script de inicio de sesión, hay que proporcionar el propio script). Una vez creado y configurado, el GPO se *vincula* a algún *contenedor* del Directorio Activo. No todos los contenedores admiten esta vinculación, sólo los sitios, los dominios y las unidades organizativas.

El efecto de vincular un GPO a uno de esos contendores del Directorio Activo es que los usuarios y equipos cuyas cuentas se ubiquen dentro de dicho contenedor recibirán de manera automática las políticas que se hayan configurado en dicho GPO. De esta forma, y utilizando sólo el Directorio Activo, cada equipo y cada usuario del dominio puede recibir una configuración apropiada al tipo de tarea que debe desempeñar.

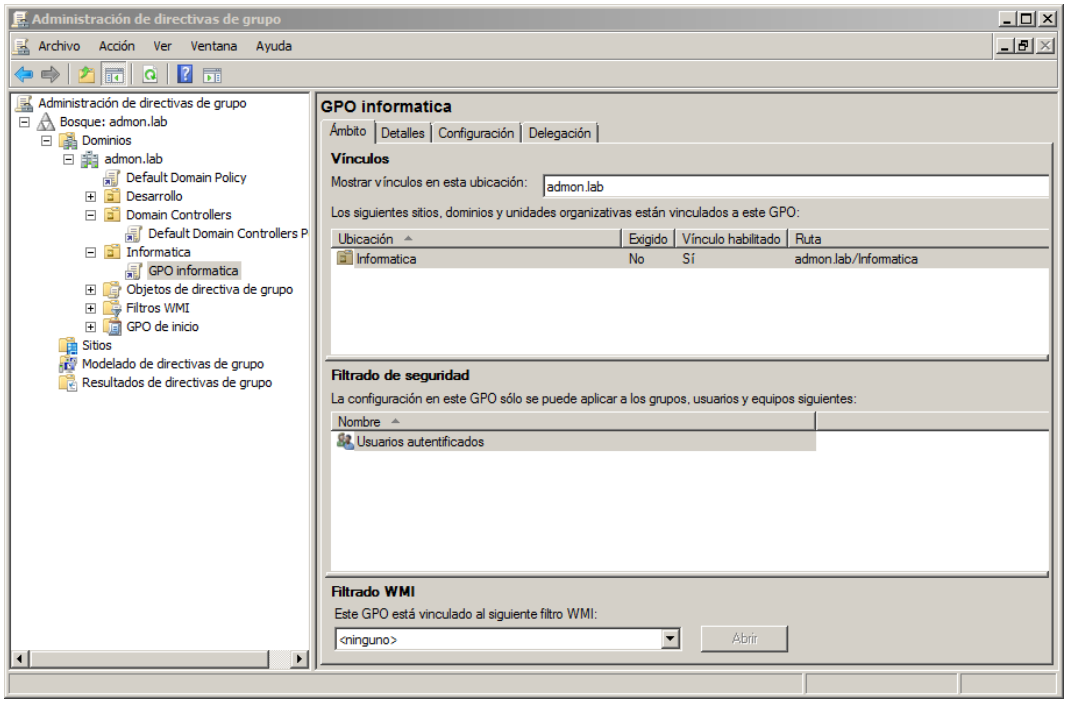


Figura 5.1. Herramienta Adminstración de directivas de grupo en Windows 2008

De entre los contenedores que existen por defecto al crear un dominio, el que representa al dominio y la unidad organizativa "Domain Controllers" ya tienen crea-

dos y vinculados sendos GPOs que incorporan un conjunto mínimo de configuraciones necesarias para el buen funcionamiento del dominio. Estos GPOs se denominan "Default Domain Policy" y "Default Domain Controllers Policy", respectivamente. El resto de contenedores que existen inicialmente en el dominio ("Builtin", "Computers", y "Users", más algunos otros ocultos) no son en realidad unidades organizativas, y por este motivo no se les pueden asociar GPOs. Por lo tanto, para poder implementar un esquema de GPOs en un dominio es necesario crear primero una estructura adecuada de unidades organizativas, y distribuir en ellas los objetos usuario/equipo.

Dentro de cada GPO, las políticas se organizan jerárquicamente en un *árbol temático* que permite una distribución lógica de las mismas, tal como muestra la Figura 5.2, "Arbol de políticas contenido en un GPO en Windows Server 2008".

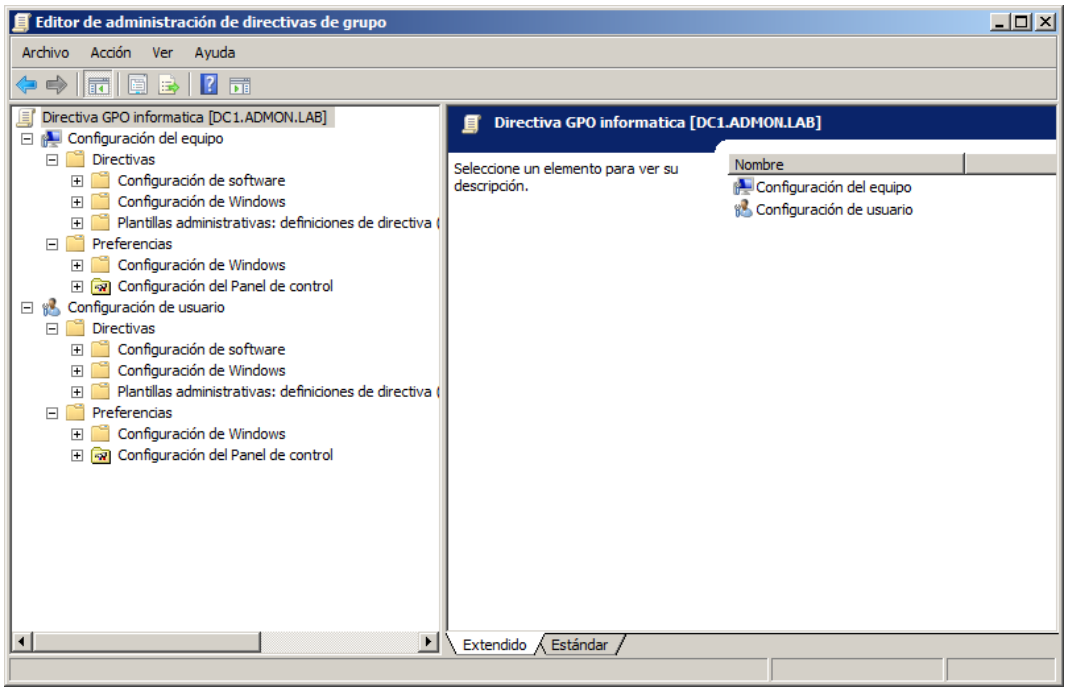


Figura 5.2. Arbol de políticas contenido en un GPO en Windows Server 2008

En este árbol de políticas, justo debajo del nodo raíz, existen dos *nodos principales* que separan las configuraciones para equipos y para usuarios:

1. La **configuración del equipo** agrupa todas las políticas, o parámetros de configuración, que pueden establecerse a nivel de equipo. Cuando un GPO afecta a un equipo, todas aquellas políticas de equipo del GPO que el administrador haya configurado se aplicarán al equipo cada vez que éste se inicie.

2. La **configuración de usuario** agrupa todas las políticas, o parámetros de configuración, que pueden establecerse a nivel de usuario. Cuando un GPO afecta a un usuario, todas aquellas políticas de usuario del GPO que el administrador haya configurado se aplicarán cuando dicho usuario inicie una sesión (en cualquier equipo del bosqe).

Además de esa aplicación inicial de las políticas (en el inicio de los equipos y en el inicio de sesión de los usuarios), éstas se reevalúan automáticamente de forma periódica. Por defecto, la reevaluación periódica se produce en los sistemas miembros del dominio cada 90 minutos (con un retraso aleatorio de hasta 30 minutos), y en los DCs cada 5 minutos. El administrador también puede forzar la aplicación inmediata de un GPO en un equipo ejecutando la orden Gpupdate. Sin embargo, hay que tener en cuenta que algunas políticas, por sus características, sólo se pueden aplicar cuando el equipo reinicia o el usuario reinicia sesión. Por ejemplo, este es el caso de la instalación de software, o la redirección de carpetas.

Por último, es interesante saber que en cada GPO se pueden *deshabilitar* selectivamente las políticas de equipo y/o las de usuario. Cuando deshabilitamos uno de ambos subárboles de un GPO, sus políticas dejan de aplicarse a partir de ese momento. Esta característica resulta útil cuando en un GPO sólo se configuran políticas de un tipo, bien de usuario o bien de equipo, ya que el administrador puede deshabilitar el subárbol que no contiene ninguna política configurada. El objetivo de ello es evitar que el sistema pierda tiempo procesando un subárbol (al iniciar el ordenador si es de equipo, o al iniciar sesión el usuario, si es de usuario) en el que todas sus políticas se encuentran no configuradas.

5.3. Aplicación de Políticas de Grupo

El apartado anterior ha introducido las generalidades sobre los GPOs. Partiendo de esa base, a continuación se explica con más detalle el comportamiento de los GPOs respecto a su aplicación en el dominio:

- Un mismo GPO puede contener indistintamente parámetros (o políticas) de configuración que deben aplicarse a equipos y a usuarios.
- Cada GPO se vincula a un contenedor del directorio activo (un sitio, un dominio o una unidad organizativa), afectando implícitamente a todos los objetos que residen en él:
    - Los equipos se verán afectados por las políticas de equipo del GPO.
    - Los usuarios se verán afectados por las política de usuario del GPO.
    - Los sub-contenedores *heredarán* el GPO completo.

Es decir, los GPOs vinculados a un *sitio* son heredados por su *dominio*. Estos GPOs, más los vinculados al dominio, son heredados por las *unidades organizativas* de primer nivel establecidas en el dominio. Todos ellos, más los vinculados a estas unidades organizativas, son heredados por las unidades de segundo nivel ubicadas dentro de aquellas, y así sucesivamente.

- Existe una relación "muchos a muchos" entre contenedores y GPOs: un mismo GPO puede vincularse a múltiples contenedores y un contenedor puede tener vinculados múltiples GPOs simultáneamente.

En resumen, las políticas de grupo son *heredables* y *acumulativas*. Eso quiere decir que, desde el punto de vista de un equipo o de un usuario concretos, la lista de GPOs que les afecta depende de su ubicación en Directorio Activo: esta lista incluye *todos* los GPOs vinculados a los contenedores por los que hay que pasar para llegar desde el sitio (y dominio) hasta la unidad organizativa concreta donde ese equipo o usuario se ubica.

Puesto que cada GPO incorpora exactamente el mismo árbol de políticas, es posible que se produzcan conflictos entre los distintos GPOs que afectan a un usuario/equipo, si varios de esos GPOs han configurado una *misma política* con valores distintos. Resulta por tanto necesario que exista un orden de aplicación concreto y conocido, de forma que se sepa finalmente qué politica(s) afectarán a cada usuario y equipo, sin ambigüedades. Este orden es el siguiente:

1. Se aplica la política de grupo local del equipo (denominada *Local Group Policy Object*, o LGPO).
2. Se aplican los GPOs vinculados a sitios.
3. Se aplican los GPOs vinculados a dominios.
4. Se aplican los GPOs vinculados a unidades organizativas de primer nivel. En su caso, posteriormente se aplicarían GPOs vinculados a unidades de segundo nivel, de tercer nivel, etc.

Este orden de aplicación decide la *prioridad* entre los GPOs, puesto que una política que se aplica más tarde prevalece sobre otras establecidas anteriormente (las *sobreescribe*). De forma análoga a lo establecido para permisos en el sistema de archivos NTFS, podríamos decir que las políticas explícitas de un contenedor tienen prioridad (se aplican más tarde) sobre las políticas heredadas de contenedores superiores. Precisamente para que siempre haya un orden explícito, en el caso de que haya más de un GPO vinculado a un mismo contenedor, siempre hay establecido un or-

den entre ellos, que el administrador puede cambiar si lo desea.

Por último, el comportamiento respecto a la herencia y prioridad entre GPOs en contenedores anidados puede ser refinado mediante los siguientes dos parámetros de configuración:

1. **Exigido** (*Enforced*). Este parámetro puede activarse independientemente a cada *vínculo* de un GPO. En particular, si el vínculo de un GPO a un contenedor tiene este parámetro activado, sus políticas no pueden ser sobrescritas por GPOs que se apliquen posteriormente (a subcontenedores de dicho contenedor).

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

El comportamiento que se acaba de describir afecta a todos los equipos y a todos los usuarios del dominio en función, exclusivamente, de su ubicación dentro del Directorio Activo. En el caso de las políticas de usuario, este comportamiento y la propia administración de los GPOs puede refinarse aún más utilizando grupos de seguridad.

5.4. Políticas de Grupo y grupos de seguridad

Como todos los objetos del Directorio Activo, los GPOs poseen listas de control de acceso (o DACLs). En general, estas DACLs establecen qué usuarios y grupos pueden leer, escribir, administrar, etc., dichos objetos. En el caso concreto de los GPOs, esta asociación de permisos a *grupos de seguridad* permite tanto filtrar el ámbito de aplicación de un GPO como delegar su administración. Ambas posibilidades se exponen a continuación.

5.4.1. Filtrar el ámbito de aplicación de un GPO

Uno de los permisos de cada GPO es "Aplicar directiva de grupos" (o, simplemente, *Aplicar*). Por defecto, este permiso lo tienen concedido el grupo *Usuarios autentificados*, que incluye en la práctica a todos los usuarios y todos los equipos del dominio. Por tanto, la política afecta a todos los usuarios y equipos cuyas cuentas se ubiquen dentro del contenedor al que se vincula el GPO.

Si este comportamiento no es el que se desea, se puede eliminar este permiso y concederlo a otro(s) grupo(s) más restringidos, o bien mantener este permiso y añadir permisos negativos a otros grupos. Hay que tener en cuenta varias cosas a este

respecto:

- Si denegamos el permiso *Aplicar* a un grupo, impediremos que sus políticas afecten a cualquiera de sus miembros (usuarios/equipos), aunque pertenezca a otros grupos que tengan este permiso concedido. Por tanto, esta opción debe utilizarse con especial cuidado.

- El permiso *Aplicar* debe asignarse conjuntamente con el permiso *Leer*, ya que si no, el equipo/usuario correspondiente no puede siquiera procesar el GPO. Si asignamos *Aplicar* a grupos más restringidos que el de Usuarios Autentificados, es recomendable que hagamos lo mismo con el permiso *Leer*, puesto que el GPO se *procesa* para todos los usuarios/equipos que poseen este permiso, aunque sólo se *aplica* a los que poseen, además, el permiso *Aplicar*.

- Existe un caso en el que no se debe seguir esta recomendación: si la política no debe aplicarse al grupo de administradores, éstos no deben tener concedido el permiso *Aplicar*. Sin embargo, no es posible eliminar el permiso *Leer* a estos usuarios porque entonces no podrían administrar el GPO.

5.4.2. Delegar la administración de un GPO

Cualquier usuario o grupo que tenga concedido el permiso de Control Total sobre un GPO puede administrarlo. Por defecto, en todos los GPOs que se crean en el dominio, este caso se encuentran:

- el grupo Administadores de Empresas,
- el grupo Admins. del Dominio,
- el creador del GPO (*Creator Owner*),
- y el propio sistema (*SYSTEM*).

A pesar de que estos grupos no tienen concedido el permiso "Aplicar a", si los administradores se encuentran bajo el ámbito del GPO entonces recibirán sus políticas, puesto que forman parte de "Usuarios Autentificados".

Es posible delegar la administración de GPOs a otros usuarios y grupos. En realidad, la administración de un GPO consta de dos actividades distintas y complementarias, que pueden delegarse independientemente:

1. **Creación de un GPO**. La creación de un GPO es una actividad previa (e independiente) a su vinculación a un contenedor del directorio. Unicamente los administradores de empresa y dominio y aquellos usuarios o grupos miembros del grupo *Group Policy Creator Owners* pueden crear nuevos objetos de este tipo. Por tanto, el administrador puede delegar esta acción haciendo que un cierto usuario o grupo pertenezca a este grupo de creadores de GPOs.

2. **Vinculación de un GPO a un contenedor**. Esta acción se controla mediante permisos específicos del *contenedor* (sitio, dominio o unidad organizativa), y puede delegarse mediante una de las tareas de delegación predefinidas denominada *Manage Group Policy links*. El procedimiento para realizar este tipo de delegaciones se encuentra en la Sección 4.5, “Delegación de la administración”.

5.5. Principales políticas incluidas en un GPO

Como se ha visto en previamente, cada GPO consta de un árbol de políticas, subdividido en su nivel más alto en dos subárboles denominados *Configuración de equipo* y *Configuración de usuario*. Internamente, cada uno de esos subárboles se subdivide de manera análoga, en dos nodos denominados "Directivas" y "Preferencias", que se resumen a continuación:

1. **Directivas**. Tanto en el caso de equipos como de usuarios, esta subárbol incluye a su vez tres nodos:

   - **Configuración de software**. Contiene opciones de instalación automática de software.
   - **Configuraciones de Windows**, incluyendo entre otros aspectos de seguridad, ejecución de scripts y redirección de carpetas (para usuarios).
   - **Plantillas Administrativas**, que incluyen aquellas políticas basadas en la modificación de valores del registro de Windows.

2. **Preferencias**. Este subárbol incluye numerosos aspectos de configuración que típicamente se realizaban mediante la ejecución de scripts en versiones previas de Windows. Tanto en el caso de equipos como en el de usuarios, este subárbol contiene a su vez dos nodos:

   - **Configuración de Windows**. Incluye opciones de configuración como por ejemplo creación de variables de entorno, creación de accesos directos, mapeo de unidades de red, etc.
   - **Configuración del Panel de Control**. Incluye opciones de configuración como por ejemplo la instalación de dispositivos y de impresoras, la configura-

ción de opciones de energía, de tareas programadas, de servicios, etc.

Es decir, en muchos casos, la misma política existe en ambos subárboles (equipo y usuario), aunque generalmente en cada caso con significados y parámetros distintos. Por ejemplo, bajo *Configuración del Equipo--Directivas--Configuración de Windows--Scripts* podemos encontrar los *scripts* que deben ejecutarse cada vez que el equipo se inicia o detiene, mientras que bajo *Configuración de Usuario--Directivas--Configuración de Windows--Scripts* se encuentran los *scripts* que deben ejecutarse cada vez que el usuario inicia o finaliza una sesión local.

A continuación se exponen los grupos de políticas más importantes que pueden configurarse mediante un GPO, independientemente de su ubicación concreta dentro de la jerarquía.

5.5.1. Plantillas administrativas

Este grupo contiene todas las configuraciones de políticas basadas en el registro de Windows Server 2008, incluyendo aquellas que controlan el funcionamiento y apariencia del escritorio, de los componentes de Windows Server 2003 y de algunas aplicaciones que utilizan estas políticas. El cambio principal que Windows Server 2008 ha incorporado en estas políticas respecto a versiones previas de Windows Server es que se ha rediseñado el formato de los ficheros que las definen internamente, estando ahora basado en el estándar XML. Entre otras ventajas, este cambio favorece la definición textual de estas plantillas en diferentes idiomas.

5.5.2. Configuraciones de seguridad

En este apartado se encuentra la configuración de muchos de los aspectos de seguridad que pueden establecerse en un sistema Windows Server 2008.

En concreto, y centrándonos en los aspectos de seguridad a nivel de equipo, podemos destacar los siguientes (de entre muchos más):

1. **Políticas de Cuentas**. Se pueden configurar todos los aspectos sobre el plan de cuentas que se vieron en la Sección 3.5.1, “Otras directivas de seguridad”, tales como caducidad de contraseñas, bloqueo de cuentas, configuración de Kerberos, etc.

2. **Políticas Locales**. Bajo este apartado se encuentran las configuraciones que corresponden a la denominada "Directiva local" de la Sección 3.5.1, “Otras directivas de seguridad”, es decir, la configuración de la auditoría, la asignación de

derechos y privilegios de usuario y las opciones de seguridad.

3. **Registro de Eventos**. Aquí se controla el registro de eventos en los registros de aplicación, seguridad y sistema, que posteriormente pueden visualizarse con la herramienta Visor de Sucesos.

5.5.3. Instalación de software

Mediante este apartado se puede *asignar* y/o *publicar* aplicaciones a equipos o a usuarios en el dominio:

1. **Asignar** una aplicación significa que los usuarios que la necesitan la tienen disponible en su escritorio sin necesidad de que un administrador la instale. Cuando se asigna una aplicación a un usuario o equipo, se crea una entrada para ella en el menú de inicio y se configura el registro adecuadamente. La primera vez que el usuario ejecuta la aplicación, ésta es automáticamente instalada en el equipo cliente.

2. **Publicar** una aplicación a un equipo o usuario le da la oportunidad al usuario de instalar dicha aplicación bajo demanda (a voluntad), pero no se realiza ninguna acción automática en el equipo (no se modifica el menú de inicio ni el registro). La lista de aplicaciones publicadas para un usuario aparecen en el Panel de Control, bajo la herramienta de *Añadir/Eliminar Programas*, desde donde pueden ser instaladas.

5.5.4. Guiones o *Scripts*

Bajo este apartado, se pueden asignar *scripts* a equipos o usuarios. En concreto, existen cuatro tipos de *scripts* principales:

1. **Inicio** (equipo). Se ejecuta cada vez que el equipo arranca.

2. **Apagado** (equipo). Se ejecuta cada vez que el equipo va a detenerse.

3. **Inicio de sesión** (usuario). Se ejecuta cada vez que el usuario inicia una sesión interactiva (local) en un equipo.

4. **Cierre de sesión** (usuario). Se ejecuta cada vez que el usuario se finaliza una sesión interactiva en un equipo.

En todos esos casos, los *scripts* pueden implementarse en cualquiera de los lenguajes que entiende el soporte de *scripts* independiente del lenguaje de Windows Server 2008, o *Windows Scripting Host*, el nuevo lenguaje de scripts propio de Windows Server 2008 denominado PowerShell, así como los tradicionales archivos por lotes heredados de MS-DOS.

El comportamiento de los *scripts* puede perfilarse mediante algunas políticas que se sitúan en el apartado de Plantillas Administrativas. En la tabla a continuación se muestran algunas que resulta útil conocer.

Tabla 5.1. Principales políticas que afectan el comportamiento de los *scritps*

Config. del Equipo--Directivas--Plantillas Administrativas--Sistema--Scripts	
Política	**Significado**
Ejecutar secuencia de comandos de inicio de sesión de forma síncrona.	Si esta política está activada, Windows 2000 espera a que se hayan procesado los *scripts* de inicio antes de iniciar el escritorio. Esta opción también existe para el usuario, pero la establecida aquí tiene preferencia.
Ejecutar archivos de comandos de inicio de forma asíncrona.	Por defecto, los *scripts* de inicio de equipo se ejecutan ocultos y de forma síncrona (el sistema operativo no termina de arrancar hasta que se han procesado completamente). Esta política permite cambiar este comportamiento por defecto.
Ejecutar archivos de comandos de inicio visibles.	Si está habilitada, los *scripts* de inicio del sistema se ejecutan visibles en una ventana de órdenes.
Ejecutar archivos de comandos de apagado visibles.	Esta es la política equivalente a la anterior para los *scritps* de detención del equipo.
Tiempo de espera máximo para secuencias de comandos de directivas de grupo.	El tiempo máximo de espera para los *scripts* (en el caso de que se queden suspendidos, por ejemplo) es de 600 segundos. Mediante esta política se puede cambiar este intervalo, hasta un máximo de 32000 segundos.

Config. de Usuario--Directivas--Plantillas Administrativas--Sistema--Scripts	
Política	**Significado**
Ejecutar secuencia de comandos de inicio de sesión de forma síncrona.	Si esta política está activada, Windows Server espera a que se hayan procesado los *scripts* de inicio antes de iniciar el escritorio.
Ejecutar archivos de comandos de inicio de sesión visibles.	Si está habilitada, los *scripts* de inicio de se sesión del usuario se ejecutan visibles en una ventana de órdenes.
Ejecutar archivos de comandos de cierre de sesión visibles	Esta es la política equivalente a la anterior para los *scritps* de fin de sesión del usuario.

5.5.5. Redirección de carpetas

Este grupo de políticas permite redirigir la ubicación local predefinida de ciertas carpetas particulares de cada usuario (como "Mis Documentos" o el menú de inicio)

a otra ubicación, bien sea en la misma máquina o en una unidad de red.

Un ejemplo útil de redirección sería que la carpeta "Mis documentos" apuntara a un directorio personal de cada usuario en la red, como por ejemplo el recurso `\\servidor\home\%username%`. Esta aproximación resulta más últil que conectarle a dicho usuario ese recurso a una unidad de red, puesto que muchas aplicaciones abren automáticamente la carpeta "Mis documentos" para buscar los archivos personales de ese usuario. Para que dicha redirección funcione correctamente, es necesario que el usuario que recibe la redirección sea el propietario de la carpeta compartida.

5.6. Recomendaciones de uso

Todo administrador debería tener en cuenta una serie de reglas básicas que permiten simplificar el diseño y la administración de las Políticas de Grupo. A continuación se exponen las más relevantes:

- **Administración de GPOs**. Un adecuado diseño de la administración y delegación de GPOs es crucial en empresas medianas y grandes, en las que generalmente los dominios se encuentran muy jerarquizados en unidades organizativas. Este diseño debe realizarse en función de la organización y el reparto de labores administrativas que exista en la empresa.

- **Separar usuarios y equipos en unidades organizativas diferentes**. Esta decisión de diseño simplifica la aplicación de GPOs, ya que al diseñarlas sólo hay que tener en cuenta la configuración de usuarios o de equipos. Por otra parte, este diseño facilita que las labores de administrar equipos y administrar usuarios puedan repartirse entre grupos de administradores distintos. Finalmente, también es beneficioso respecto al tiempo dedicado a procesar las políticas de grupo, puesto que pueden deshabilitarse las políticas (de equipo o de usuario) que no se hayan configurado.

- **Organización homogénea de unidades organizativas**. La organización de las unidades organizativas (primero geográfica y luego funcional, o al revés) debe partir de la organización de la empresa y debe ser consistente con ella. Si se sobrediseña esta estructura, resultará más difícil aplicar correctamente las políticas de grupo a equipos y usuarios.

- **Miniminzar los GPOs asociados a usuarios o equipos**. El tiempo de inicio de un equipo y el tiempo de inicio de sesión de un usuario se incrementan conforme más GPOs se aplican a dicho equipo o usuario. Resulta por tanto más interesante intentar conseguir las configuraciones adecuadas con el menor número posible de GPOs.

- **Minimizar el uso de "No reemplazar" y de "Bloquear la herencia"**. Estas dos propiedades de un GPO resultan interesantes en ciertos escenarios, aunque su abuso puede complicar mucho la comprensión por parte del administrador de qué políticas están afectando realmente a equipos y usuarios. Lógicamente, esto dificulta la capacidad del administrador de resolver situaciones en las que el efecto de las políticas no es el desado.

- **Evitar asignaciones de GPOs entre dominios**. Aunque es técnicamente posible vincular a un contenedor de un dominio un GPO creado en *otro* dominio, esta práctica está desaconsejada. El motivo es que los GPOs están almacenados en sus dominios respectivos y al utilizarlos desde otros dominios, el tiempo para su proceso se incrementa.

- **Utilizar el proceso *Loopback* sólo cuando sea necesario**. Aunque esta opción queda fuera de los objetivos de este capítulo, se explicará brevemente a continuación. En algunas ocasiones muy concretas, puede resultar conveniente para ciertos equipos en un dominio que sólo se apliquen las políticas de equipo que les afecten. En otras palabras, conseguir que *nunca* se apliquen las políticas de usuario, independientemente del usuario que inicie una sesión local en dichos equipos. Esto puede conseguirse mediante la denominada Política de Grupo "de bucle inverso" o *Loopback*, que puede configurarse en la política `Configuración del Equipo--Plantillas Administrativas--Sistema--Directivas de Grupo--Modo de procesamiento de bucle invertido de la directiva de grupo de usuario`.. Puesto que esta opción se aleja bastante del funcionamiento normal de los GPOs, se recomienda limitarlo a las ocasiones en que sea estrictamente necesario.

6

Servicios del sistema

Indice

6.1. Introducción

Un servicio es un programa que está ejecutándose indefinidamente para atender a peticiones de otros programas o del usuario. Como ocurría con Windows NT, Windows 2008 también utiliza los servicios. Por defecto W2008, ejecuta automáticamente muchos servicios (necesarios o no) que consumen más memoria que la necesaria para las funciones que está desempeñando el sistema. Si nunca vas a utilizar el Servicio de Fax o el Programador de Tareas, por qué tienen que estar ejecutándose y consumiendo memoria.

6.2. Servicios

Para poder acceder a todos los servicios disponibles en un sistema Windows 2008, se debe de iniciar sesión como administrador. Para ejecutar la utilidad Servicios, hay que seleccionar *Inicio->Programas->Herramientas Administrativas->Servicios*.

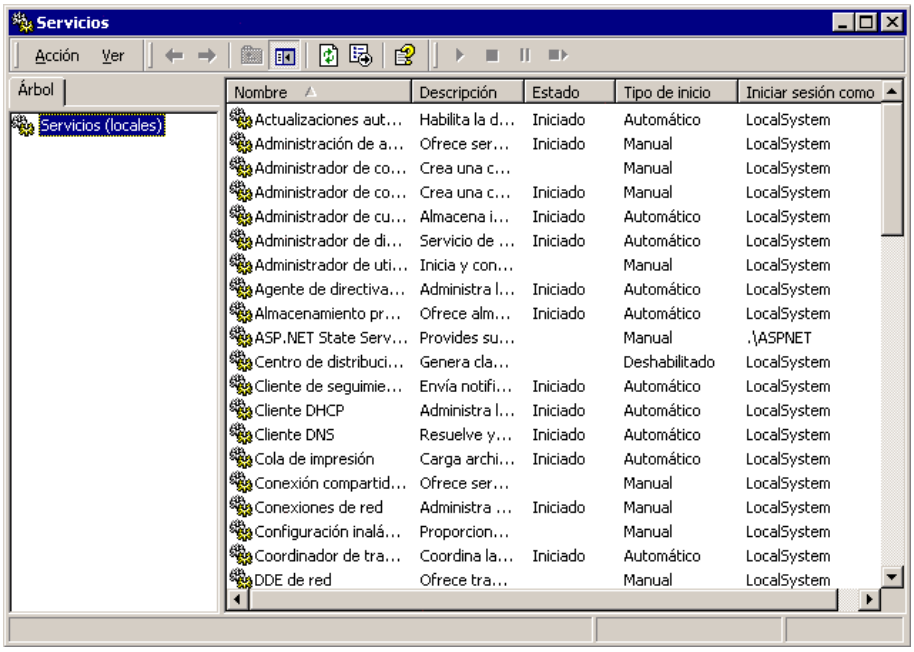


Figura 6.1. Utilidad Servicios de Windows 2008

Esta utilidad muestra todos los serevicios disponibles en el sistema. Sobre todo hay que fiharse en la columna **Tipo de Inicio**, ya que este atributo define cuando se arrancará el servicio. Existen tres opciones a la hora de arrancar un servicio, que serán vistas más adelante en este capítulo.

6.2.1. Tipo de inicio de un servicio

Existen tres opciones a la hora de elegir el tipo de inicio de un servicio que esté disponible en el sistema:

1. **Automático**: el servicio se inicia automáticamente mientras se carga el sistema operativo (Windows 2008). Esta opción puede incrementar el tiempo de inicio del sistema, así como el consumo de recursos, mientras que el servicio igual no es necesario.

2. **Manual**: el servicio no se inicia de forma predeterminada trás la carga del sistema operativo, en cambio pude ser iniciado - manulamente - en cualquier instante.

3. **Deshabilitado**: esta opción en el tipo de inicio de un servicio, obliga al administrador a tener que habilitarlo antes de poder ejecutarlo.

Para poder cambiar el tipo de inicio de un servicio hay que editar las *Propiedades* de servicio respectivo. Para hacer esto, basta con apretar el botón derecho de nuestro ratón sobre el servicio en cuestión y seleccionar Propiedades.

Una vista de la ficha propiedades se muestra a continuación:

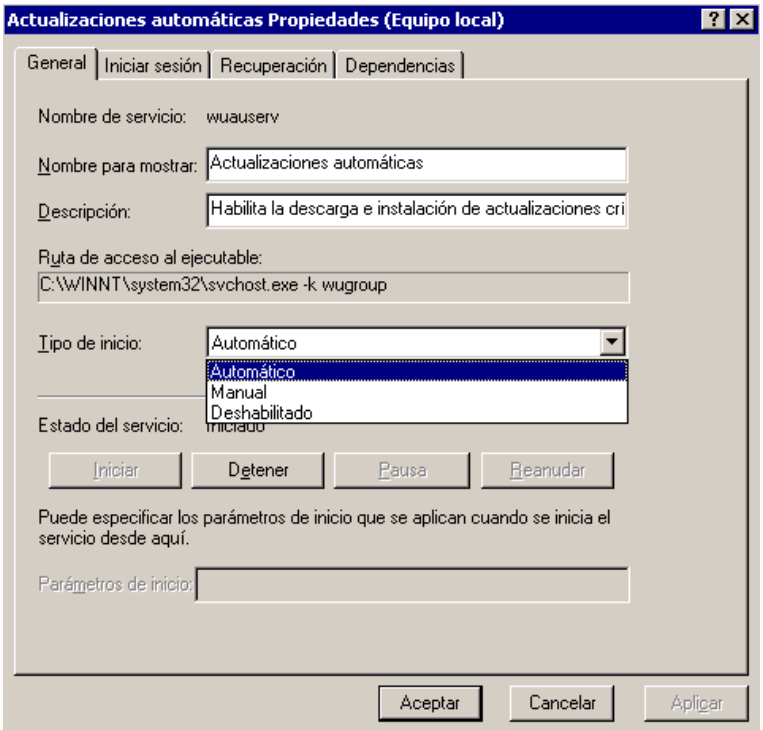


Figura 6.2. Ficha Propiedades de un servicio

En el menú desplegable Tipo de Inicio, se elige como se ha de iniciar el servicio en el arranque: *Automático, Manual o Deshabilitado*. Una vez elegido el tipo de inicio, seleccionamos *Aplicar* para que los cambios surtan efecto. A veces es preferible dejar un servicio con un tipo de inicio *Manual* que deshabilitarlo.

6.2.2. Dependencias entre servicios

Las relaciones de dependencia entre los servicios implican que a la hora de parar servicios, todos aquellos que dependan de el se verán afectados también y así sucesivamente, corriendo el peligro de dejar el sistema en un estado no utilizable.

Para saber que servicios dependen de que otros, en la ficha de *Propiedades* del servicio, elige la lengüeta *Dependencias*.

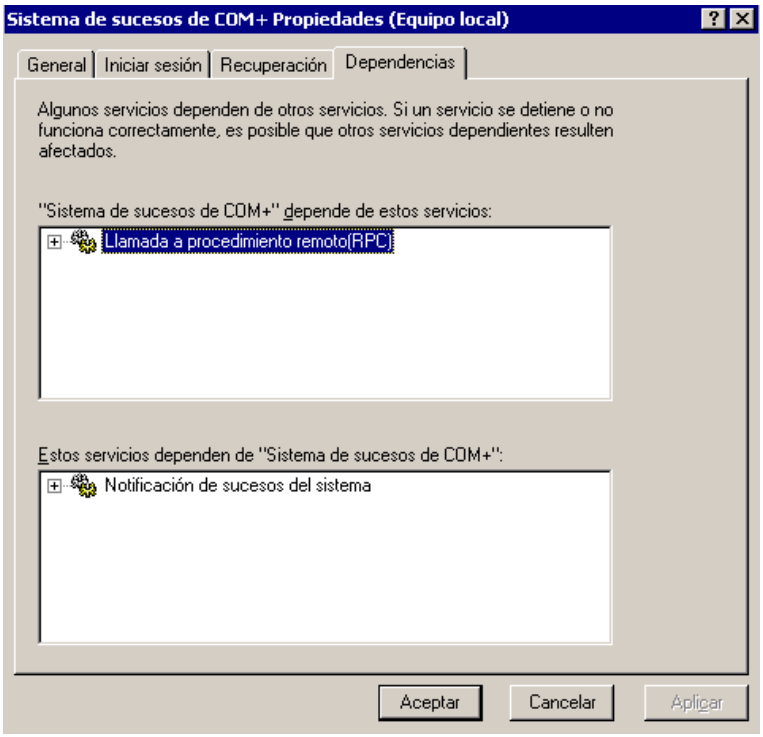


Figura 6.3. Interdepencias de servicios

Esta vista muestra en el panel superior los servicios de los que depende el servicio seleccionado, y en el panel inferior se muestran los servicios dependientes de él.

6.2.3. Recuperación de un servicio

También se pueden personalizar las opciones de **Recuperación** de un servicio ante

un fallo o parada del servicio. En otras palabras, que hacer cuando falla un servicio.

De nuevo en la ficha *Propiedades* eligiendo la lengüeta *Recuperación* podemos definir dicho comportamiento.

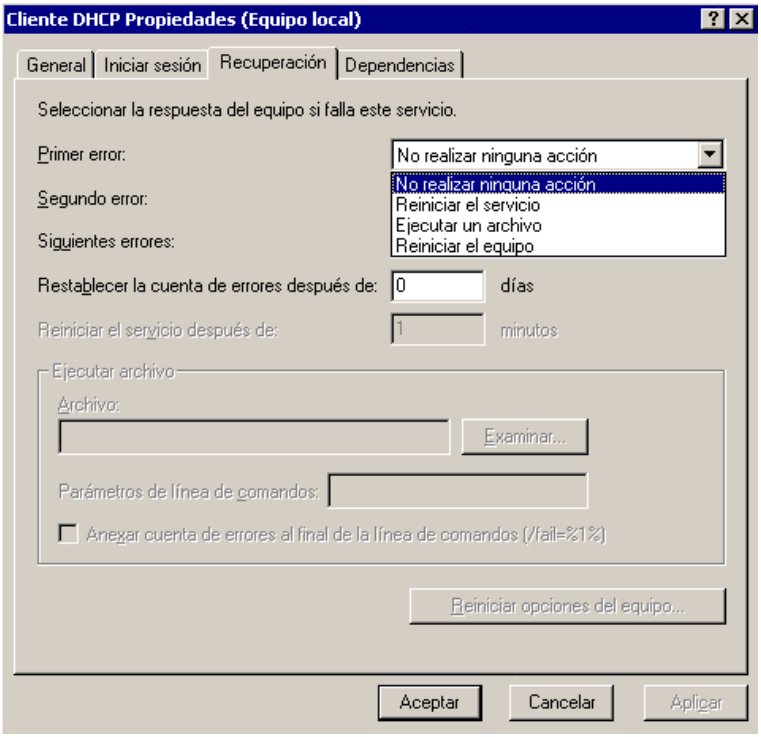


Figura 6.4. Acciones de recuperación de un servicio

Las acciones posibles a tomar son:

- **No realizar ninguna acción**
- **Reiniciar el servicio**: el sistema intentará reinicar el servicio si este falló. Se puede definir el periodo de tiempo en minutos en que lo volverá a intentar
- **Ejecutar un archivo**: tenemos la posibilidad de ejecutar un archivo de comandos para tomar de una forma más granular las acciones adecuadas.
- **Reiniciar el equipo**: si es un servicio importante y no hay forma de levantarlo, ya se sabe, botonazo ;-)

6.3. Solucionando problemas

Puede suceder que al haber deshabilitado un servicio que era necesario para la carga del sistema operativo Windows 2008 o para el buen funcionamiento del sistema, nos encontremos con la desagradable situación de que la utilidad de Servicios no nos permite devolver el estado a un servicio concreto. Una opción para arreglar esto es editar la subclave del registro *HKLM\SYSTEM\CurrentControlSet\Services*

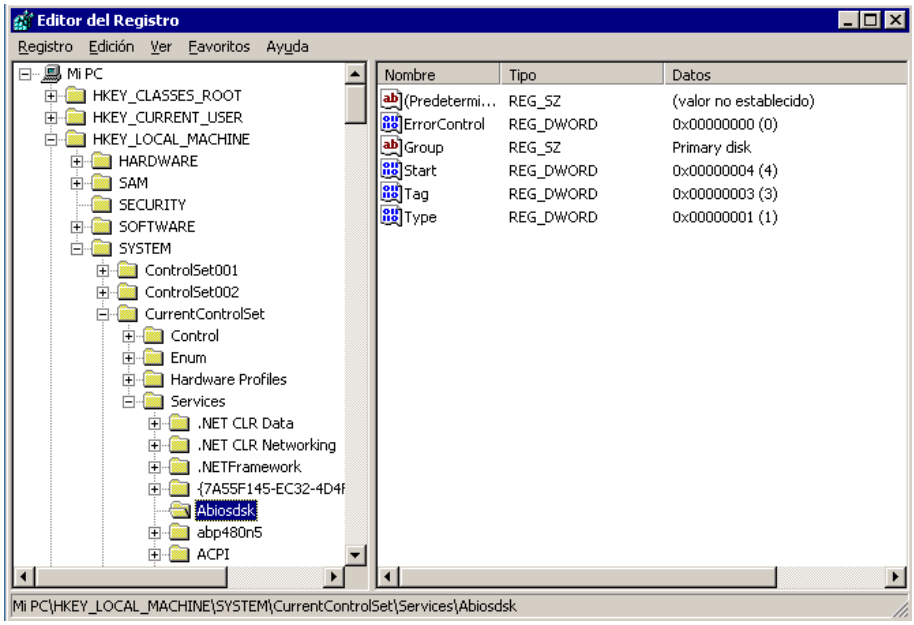


Figura 6.5. HKLM\SYSTEM\CurrentControlSet\Services

Es aquí donde se almacena el valor de tipo de inicio para cada servicio. Lo que hay que hacere es seleccionar el servicio apropiado y en el panel de la derecha cambiar el valor de la clave Start de tipo. Un valor DWORD hexadecimal o decimal determina el tipo de inicio del servicio. Los valores posibles de esta clave son:

1. Un valor **2** significa un tipo de inicio *Automático*
2. Un valor **3** significa un tipo de inicio *Manual*.
3. Un valor **4** significa que el servicio está *deshabilitado*.

7

El servicio DHCP en Windows 2008

Indice

7.1. El protocolo DCHP

DHCP (*Dynamic Host Configuration Protocol*) o Protocolo Dinámico de Configuración de Equipos no es un protocolo específico de Windows 2008, sino que se trata de un estándar para cualquier tipo de sistema conectado a una red TCP/IP.

La función básica de este protocolo es evitar que el administrador tenga que configurar manualmente las características propias del protocolo TCP/IP en cada equipo. Para ello, existe en la red un sistema especial, denominado *servidor DHCP*, que es capaz de asignar la configuración TCP/IP al resto de máquinas presentes en la red, o *clientes DHCP*, cuando estos arrancan.

Entre los datos que más habitualmente proporciona el servidor a los clientes se incluyen:

- Una dirección IP por cada tarjeta de red o NIC (*Network Interface Card*) que posea el cliente.
- La máscara de subred.
- La puerta de enlace o *gateway*.
- Otros parámetros adicionales, como el sufijo del dominio DNS, o la dirección IP del servidor DNS.

En una red pueden convivir equipos que sean clientes DHCP con otros cuya configuración se haya establecido manualmente. Aquellos que estén configurados como clientes DHCP necesitarán encontrar en la red local un servidor DHCP para que les proporciones los parámetros TCP/IP.

Cuando un cliente arranca por primera vez, lanza por la red un mensaje de difusión (*broadcast*, solicitando una dirección IP. Si en la red existe un solo servidor DHCP, cuando este reciba el mensaje contestará al cliente asociándole una dirección IP junto con el resto de parámetros de configuración. En concreto, el servidor DHCP puede estar configurado para asignar al cliente una dirección IP cualquiera de las que tenga disponibles, o bien para asignarle una dirección en concreto (o dirección reservada), en función de la dirección física de la tarjeta ethernet del cliente. En ambos casos, una vez el cliente recibe el mensaje del servidor, ya tiene una configuración IP con la que poder acceder a la red de forma normal.

Si en la red hay más de un servidor DHCP, es posible que dos o más servidores escuchen la petición y la contesten. Entonces, el primer mensaje que recibe el cliente es aceptado y el resto son rechazados. Es muy importante resaltar que cuando hay

varios servidores DHCP en una misma red local, estos no se comunican entre ellos para saber qué direcciones IP debe asignar cada uno. Es responsabilidad de los administradores que sus configuraciones sean independientes y consistentes.

En otras palabras, cuando en una misma red TCP/IP existe más de un servidor DHCP, es imprescindible que estén configurados de manera que no puedan asignar la misma dirección IP a dos ordenadores distintos. Para ello basta que los rangos de direcciones IP que puedan proporcionar no tengan direcciones comunes, o, si las tienen, que estas sean direcciones reservadas.

En cualquiera de los casos anteriores, desde el punto de vista del cliente los parámetros que ha recibido se consideran una *concesión*, es decir, son válidos durante un cierto tiempo. Cada vez que el cliente arranca, o bien cuando se alcanza el límite de la concesión (*lease time*) el cliente tiene que solicitar su renovación.

El protocolo DHCP es especialmente útil cuando el parque de equipos de una organización se distribuye en varias subredes físicas, y además los equipos cambian de ubicación (de subred) con cierta frecuencia. En este caso, cambiar el equipo de sitio no supone nunca reconfigurar manualmente sus parámetros de red, sino simplemente conectarlo a la nueva red e iniciarlo.

7.2. Concesión y renovación

Un cliente DHCP obtiene una concesión para una dirección IP de un servidor DHCP. Antes que se acabe el tiempo de la concesión, el servidor DHCP debe renovar la concesión al cliente o bien este deberá obtener una nueva concesión. Las concesiones se guardan en la base de datos del servidor DHCP aproximadamente un día después de que se agote su tiempo. Este periodo de gracia protege la concesión del cliente en caso de que este y el servidor se encuentren en diferentes zonas horarias, de que sus relojes internos no estén sincronizados o en caso de que el cliente esté fuera de la red cuando caduca el tiempo de la concesión.

La primera vez que se inicia un cliente DHCP e intenta unirse a una red, se realiza automáticamente un proceso de inicialización para obtener una concesión de un servidor DHCP:

1. El cliente DHCP solicita una dirección IP difundiendo un mensaje `DHCP Discover`.
2. El servidor responde con un mensaje `DCHP Offer` proporcionando una dirección al cliente.
3. El cliente acepta la oferta respondiendo con un mensaje `DHCP Request`.

4. El servidor envía un mensaje `DHCP Ack` indicando que aprueba la concesión.

5. Cuando el cliente recibe la confirmación entonces configura sus propiedades TCP/IP usando la información de la respuesta DHCP.

Si ningún servidor DHCP responde a la solicitud del cliente (`DHCP Discover`), entonces el cliente autoconfigura una dirección IP para su interfaz. En raras ocasiones un servidor DHCP puede devolver una confirmación negativa al cliente. Esto suele ocurrir si el cliente solicita una dirección no válida o duplicada. Si un cliente recibe una confirmación negativa (`DHCP Nack`), entonces deberá comenzar el proceso de concesión.

Cuando se inicia un cliente que ya tenía concedida una dirección IP previamente, este debe comprobar si dicha dirección sigue siendo válida. Para ello, difunde un mensaje `DHCP Request` en vez de un mensaje `DHCP Discover`. El mensaje `DHCP Request` contiene una petición para la dirección IP que se le asignó previamente. Si el cliente puede usar la dirección IP solicitada, el servidor responde con un mensaje `DHCP Ack`. Si el cliente no pudiera utilizarla porque ya no es válida, porque la esté usando otro cliente o porque el cliente se ha desplazado físicamente a otra subred, entonces el servidor responde con un mensaje `DHCP Nack`, obligando al cliente a reiniciar el proceso de concesión. Si el cliente no consigue localizar un servidor DHCP durante el proceso de renovación, entonces éste intenta hacer un `ping` al *gateway* predeterminado que se lista en la concesión actual, procediendo de la siguiente forma:

- Si tiene éxito, el cliente DHCP supone que todavía se encuentra en la red en la que obtuvo la concesión actual y la seguirá usando. En segundo plano, el cliente intentará renovar la concesión actual cuando se agote el 50% del tiempo de la concesión asignada.

- Si falló el `ping`, el cliente supone que se desplazó a otra red y autoconfigura su dirección IP, intentando cada 5 minutos localizar un servidor DHCP y obtener una concesión.

La información de TCP/IP que se concede al cliente, deberá ser renovada por éste de forma predeterminada cuando se haya agotado el 50% del tiempo de concesión. Para renovar su concesión, un cliente DHCP envía un mensaje `DHCP Request` al servidor del cual se obtuvo la concesión. El servidor renueva automáticamente la concesión respondiendo con un mensaje `DHCP Ack`. Este mensaje contiene la nueva concesión, así como cualquier parámetro de opción DHCP. Esto asegura que el cliente DHCP puede actualizar su configuración TCP/IP si el administrador de la red actualiza cualquier configuración en el servidor DHCP.

7.3. Concepto de ámbito

En el contexto de DHCP, un *ámbito* (*scope*) se define como una agrupación administrativa de direcciones IP que posee una serie de parámetros de configuración comunes y que se utiliza para asignar direcciones IP a clientes DHCP situados en una misma red física.

Es decir, para que un servidor DHCP pueda asignar direcciones IP a sus potenciales clientes, es necesario que defina al menos un ámbito en cada red física en la que haya clientes que atender. El administrador debe establecer para dicho ámbito sus parámetros de configuración, tales como el rango de direcciones IP que puede asignar, las direcciones excluidas, la máscara de red, el límite de tiempo que los equipos pueden disfrutar de la concesión, etc.

En cualquier caso, para que un servidor DHCP pueda atender varias redes físicas distintas interconectadas, es necesario que esté conectado a dichas redes, o bien que los encaminadores utilizados tengan la capacidad de encaminar los mensajes del protocolo DHCP entre dichas redes. De no ser así, es necesario utilizar un servidor DHCP distinto en cada red, o bien instalar el servicio de reenvío de DHCP en algún host el cual está configurado para escuchar los mensajes de difusión utilizados por el protocolo DHCP y redirigirlos a un servidor DHCP específico. De esta manera se evita la necesidad de tener que instalar dos servidores DHCP en cada segmento de red.

En cada ámbito sólo se admite un rango consecutivo de direcciones IP. Si todas las direcciones de dicho rango no deben de ser asignadas, es posible definir subrangos (o direcciones individuales) que deban ser excluidos.

7.3.1. Administración de ámbitos

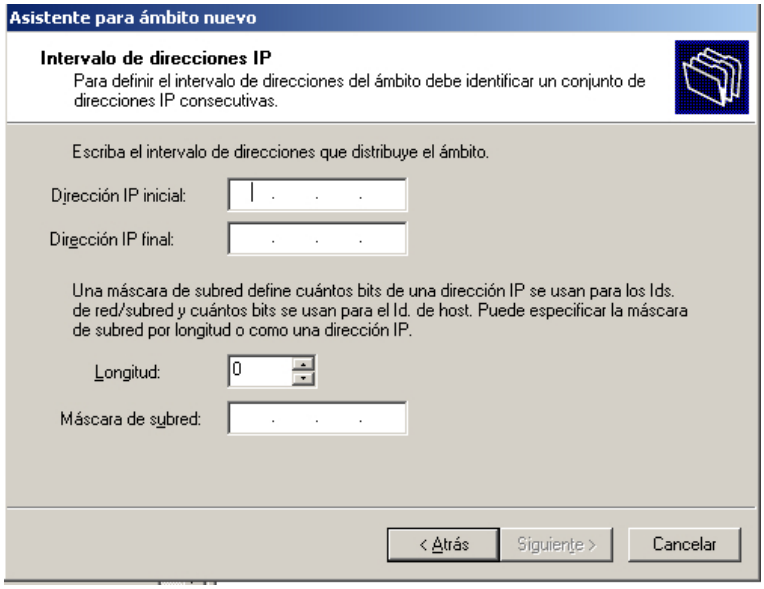
Es necesario definir y activar al menos un ámbito en el servidor para que los clientes DHCP puedan recibir la configuración dinámica de TCP/IP. Como hemos definido, un ámbito es una colección administrativa de direcciones IP y de parámetros de configuración TCP/IP que se encuentran disponibles para la concesión a los clientes DHCP.

Un ámbito tiene las siguientes propiedades:

- Un nombre de ámbito.
- Rango de direcciones IP a ofertar.
- Máscara de subred (única para todo el ámbito).
- Valores de duración de concesión.

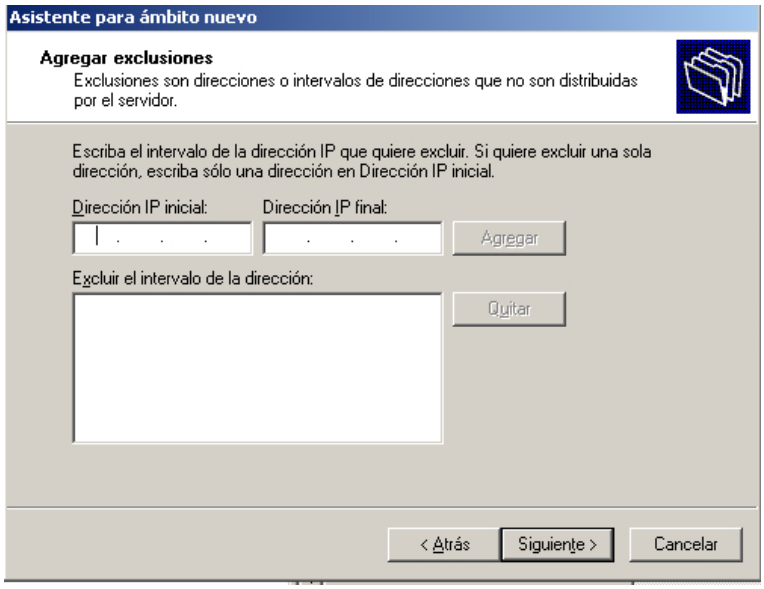
- Opcionalmente, otros datos de TCP/IP comunes para el ámbito, tales como sufijo DNS, servidor(es) DNS, etc. Estos se denominan genéricamente "opciones DHCP".

Cada subred puede tener un único ámbito DHCP con un solo intervalo continuo de direcciones IP. Si se desea ofrecer varios grupos de direcciones en el mismo ámbito (o en una sola subred), es necesario definir primero el ámbito y luego establecer intervalo(s) de exclusión.



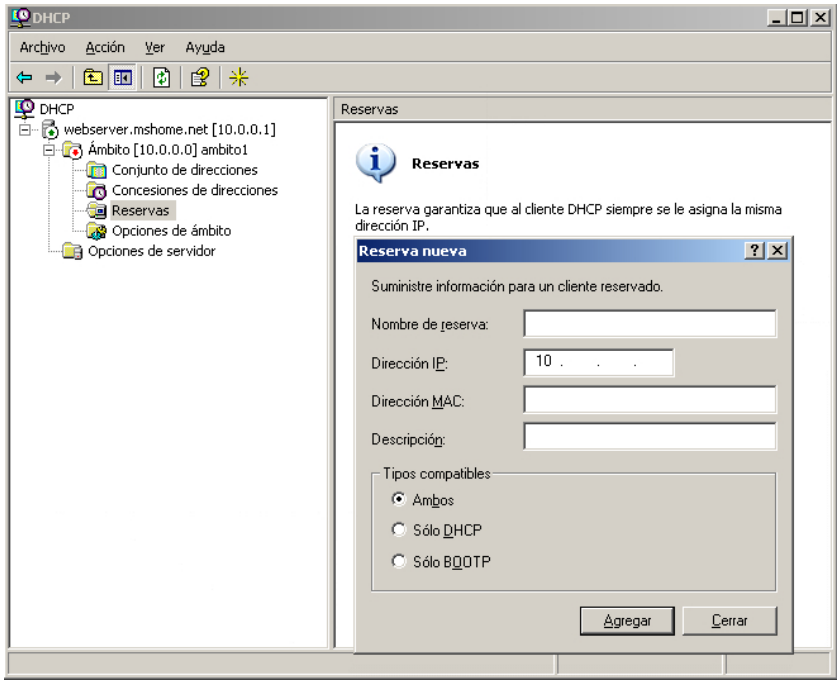
7.3.2. Intervalos de exclusión

Cuando se crea un nuevo ámbito, deberían excluirse del intervalo las direcciones de equipos configurados estáticamente, de forma que esas direcciones no puedan ofrecerse a los clientes. Como Windows 2008 Server necesita que el equipo que ejecuta el servicio DHCP tenga configurada estáticamente su dirección IP, hay que asegurarse que la dirección IP del equipo servidor esté excluida de las posibles ofertadas (y, lógicamente, que éste no sea cliente DHCP).



7.3.3. Reservas

Un administrador de red puede reservar direcciones IP para la asignación de concesiones permanentes a equipos y dispositivos específicos de la red. Las reservas se encargan de asegurar que un dispositivo hardware específico siempre pueda usar la misma dirección IP. Se recomienda hacer reservas para clientes DHCP que funciones como servidores de impresión, servidores web o encaminadores (*routers*).



7.3.4. Eliminación de concesiones

Hay ocasiones en las que es necesario modificar un ámbito para eliminar la concesión de un cliente DHCP, normalmente porque ésta entra en conflicto con un intervalo de exclusión de una dirección IP o una dirección reservada.

La acción de eliminar una concesión tiene el mismo efecto que si se agotara el tiempo de concesión del cliente, es decir, la próxima vez que se inicie el sistema del cliente éste deberá repetir el proceso de solicitud de concesión. Sin embargo, no existe ninguna forma de evitar que el cliente obtenga una nueva concesión para la misma dirección IP. Para evitar esto se debe conseguir que la dirección deje de estar disponible antes de que el cliente pueda solicitar otra concesión, quitándola del ámbito mediante una reserva o una exclusión.

7.4. Administración de opciones DHCP

Las opciones DHCP que el servidor proporciona a los clientes junto con el resto de propiedades TCP/IP (dirección, máscara, etc.) pueden configurarse en el servidor a diferentes niveles. En concreto, existen cuatro niveles donde dichas opciones se pueden configurar:

a. **Opciones globales predeterminadas**: las opciones configuradas a este nivel se aplican globalmente a todos los ámbitos, clases y clientes. Las opciones globales activas se aplican siempre, a menos que sean ignoradas o modificadas por un ámbito, clase o cliente en concreto.

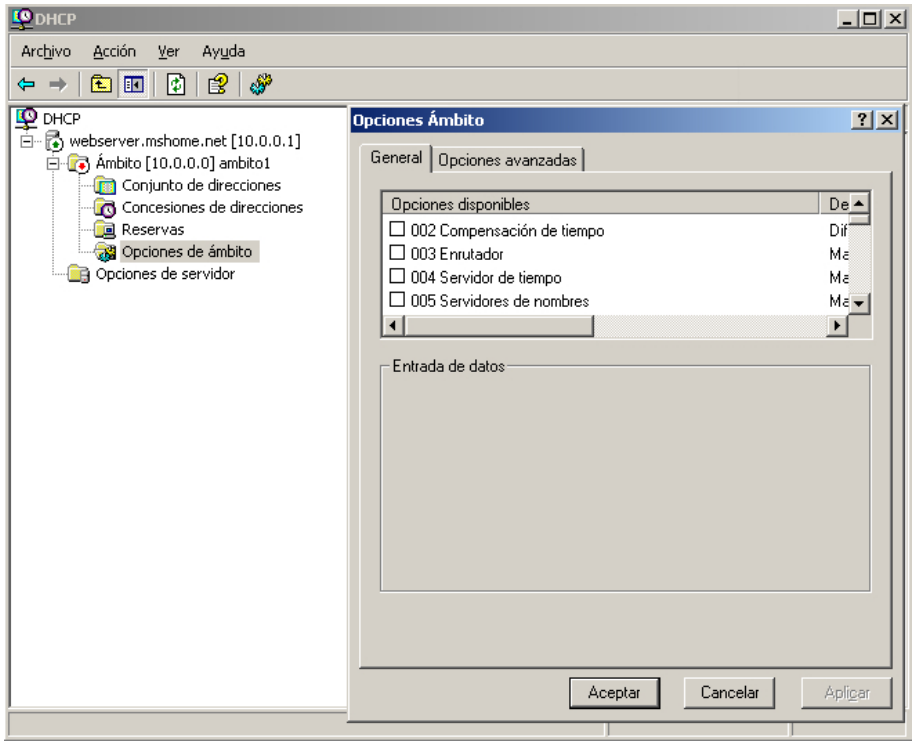
b. **Opciones de ámbito**: las opciones configuradas para un ámbito se aplican a cualquier cliente que obtenga una concesión en dicho ámbito, siempre y cuando no sean ignoradas o modificadas por opciones de clase o específicas de cliente.

c. **Opciones de clase**: se aplican a cualquier cliente que especifique el valor concreto de identificador de clase DHCP cuando obtiene una concesión de ámbito. Los tipos de opción de clase activa se aplican siempre a todos los equipos que se configuran como miembros en una opción de clase DHCP especificada, a menos que las ignore o modifique la configuración específica de cliente reservada.

d. **Opciones de cliente reservado**: se aplican a cualquier equipo que tenga una reserva en el ámbito para su dirección IP. Cuando los tipos de opción de cliente reservado sean activos, las configuraciones para estos tipos de opciones ignorarán el resto de los posibles valores predeterminados.

De la explicación anterior se deduce que, en caso de que se produzca un conflicto entre los valores especificados para una opción DHCP en distintos niveles, el valor

del nivel más específico siempre tiene preferencia sobre el menos específico.

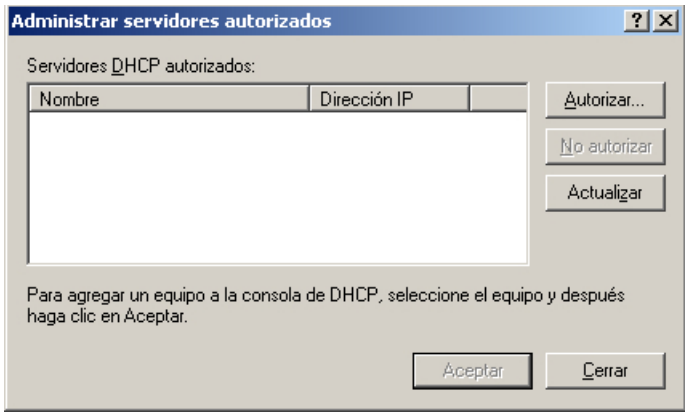


7.5. Autorización de un servidor DHCP

En las implementaciones anteriores de DHCP (de Microsoft), cualquier usuario podía crear un servidor DHCP en la red, lo que podía ocasionar conflictos en las asignaciones de direcciones IP. En Windows 2008, Active Directory debe autorizar a un servidor DHCP para que dicho servidor pueda emitir concesiones para los clientes DHCP. Como resultado, los administradores de redes tienen mayor control sobre las asignaciones de concesiones IP en una red de Windows 2008.

Cuando un servidor DHCP se inicia, entra en contacto con Active Directory para determinar si se encuentra en la lista de los servidores que están actualmente autorizados para operar en la red. Si el servidor DHCP está autorizado, se iniciará correctamente el servicio, si no lo está, el servidor DHCP anotará un error en el registro del sistema y no responderá a los clientes.

La autorización de un servidor DHCP se realiza en la acción "Autorización de Servidores" de la consola de admininistración DHCP. Sólo los miembros del grupo "Administración de Empresas" (perteneciente al dominio raíz del bosque) tienen permisos suficientes para realizar esta acción.



7.6. DHCP y DNS

De manera predeterminada, la implementación de DHCP de Windows 2008 está configurada para permitir la actualización dinámica de los servidores de nombres DNS que sean compatibles con el protocolo de actualización dinámica. Por tanto, DHCP actualiza automáticamente los registros PTR con las direcciones IP asignadas a los equipos cliente. Esta característica reduce considerablemente el trabajo administrativo necesario para mantener los servidores DNS.

La configuración de DHCP para permitir la actualización dinámica de los servidores DNS se realiza en la ficha DNS del cuadro de diálogo Propiedades del servidor DHCP. Están disponibles las siguientes opciones:

- Actualizar automáticamente la información del cliente DHCP en DNS.
- Descartar las búsquedas directas al caducar la concesión.
- Habilitar actualizaciones para clientes DNS que no sean compatibles con actualizaciones dinámicas.

Sin embargo, cuando se utiliza un servidor DHCP de Microsoft Windows NT 4.0 con clientes Windows 2008, es el cliente DHCP de Windows 2008 quien tiene que actualizar los registros A y PTR en el servidor DNS. Exactamente igual ocurre cuando un cliente configurado de forma estática actualiza dinámicamente los registros A y PTR cada vez que se inicia, o cuando se modifica su dirección IP o su nombre de dominio.

8

El Sistema de Nombres de Dominio (DNS)

Indice

8.1. Funcionamiento de DNS

El *Domain Name System* (DNS) o Sistema de Nombres de Dominio permite a los usuarios de una red TCP/IP utilizar nombres jerárquicos y descriptivos para localizar fácilmente ordenadores (*hosts*) y otros recursos en dicha red, evitando de esta manera tener que recordar la dirección IP de cada ordenador al que se desea acceder. En esencia, DNS es una base de datos distribuida que contiene asociaciones de nombres simbólicos (de hosts) a direcciones IP. El hecho de que sea distribuida permite delegar el control sobre diferentes segmentos de la base de datos a distintas organizaciones, pero siempre de forma que los datos de cada segmento están disponibles en toda la red, a través de un esquema cliente-servidor.

Los programas denominados servidores de nombres (*name servers*) constituyen la parte servidora del esquema cliente-servidor. Los servidores de nombres contienen información sobre algunos segmentos de la base de datos y los ponen a disposición de los clientes, llamados solucionadores o *resolvers*.

8.1.1. El espacio de nombres de dominio

La base de datos distribuida de DNS está indexada por nombres de dominio. Cada nombre de dominio es esencialmente una trayectoria en un árbol invertido denominado *espacio de nombres de dominio*. La estructura jerárquica del árbol es similar a la estructura del sistema de ficheros UNIX. El árbol tiene una única raíz en el nivel superior llamada raíz (*root*). Cada nodo del árbol puede ramificarse en cualquier número de nodos de nivel inferior. La profundidad del árbol está limitada a 127 niveles.

Cada nodo en el árbol se identifica mediante una etiqueta no nula que puede contener hasta 63 caracteres, excepto el nodo raíz, identificado mediante una etiqueta nula. El nombre de dominio completo de cualquier nodo está formado por la secuencia de etiquetas que forman la trayectoria desde dicho nodo hasta la raíz, separando cada etiqueta de la siguiente mediante un punto. De esta forma, el nombre del nodo especifica de forma unívoca su localización en la jerarquía. A este nombre de dominio completo o absoluto se le conoce como *nombre de dominio completamente cualificado* o *Fully Qualified Domain Name* (FQDN). Al ser nula la etiqueta que identifica el nodo raíz, el FQDN de cualquier nodo del árbol siempre acaba con un punto. La única restricción que se impone en el árbol de nombres es que los nodos hijos del mismo padre tengan etiquetas diferentes.

En el esquema jerárquico de nombres DNS, se denomina *dominio* a cualquier subárbol del espacio de nombres de dominio. De esta forma, cada dominio puede contener, a su vez, otros dominios. Generalmente, los hosts están representados por las hojas del árbol, aunque es posible nombrar a un host con una etiqueta correspon-

diente a un nodo intermedio del árbol (en este caso, tendríamos un dominio y un nodo que se llaman igual).

La información sobre los nombres de dominio DNS se guarda mediante los denominados *registros de recursos* en los servidores DNS de la red. Concretamente, cada servidor DNS contiene los registros de recursos necesarios para responder a las consultas sobre la parte del espacio de nombres en la que tiene autoridad.

8.1.2. El espacio de nombres de dominio en Internet

El estándar DNS no impone muchas reglas sobre las etiquetas de los nombres de dominio, ni tampoco asocia un significado determinado a las etiquetas de un determinado nivel del espacio de nombres. Cuando manejamos una parte de este espacio, podemos decidir el significado y la sintaxis de nuestros nombres de dominio. Sin embargo, en el espacio de nombres Internet existente, se ha impuesto una estructura de nombres bien definida, especialmente en los dominios de primer nivel.

Los dominios originales de primer nivel dividían originalmente el espacio de nombres de Internet en siete dominios: `com`, `edu`, `gov`, `mil`, `net`, `org`, e `int`. Posteriormente, para acomodar el crecimiento y la internacionalización de Internet, se reservaron nuevos dominios de primer nivel que hacían referencia a países individuales.

Actualmente, los dominios originales se denominan *dominios de primer nivel genéricos* y han surgido nuevos nombres que se ajustan a los tiempos que corren.

8.1.3. Delegación

Es importante resaltar que el objetivo principal del diseño del sistema de nombres de dominio fue su administración descentralizada. Este objetivo se consigue a través de la *delegación*. La delegación de dominios funciona de forma parecida a la delegación de tareas en una organización. Un responsable de proyecto divide el proyecto en pequeñas tareas y asigna (delega) la responsabilidad de las mismas a diferentes empleados.

De la misma forma, una organización que administra un dominio puede dividirla en subdominios. Cada subdominio puede ser delegado a diferentes organizaciones, lo cual implica que esa organización será responsable de mantener los datos (registros de recursos) de ese subdominio. Esa organización puede libremente cambiar los datos e incluso volver a dividir el dominio delegado en subdominios y delegarlos. El dominio padre solamente contiene enlaces a los responsables del subdominio delegado, de forma que pueda hacer referencia a ellos cuando se le planteen consultas sobre nombres en dicho subdominio delegado.

Realmente, la subdivisión de un dominio en subdominios y la delegación de dichos subdominios son cosas distintas. En primer lugar, un dominio que tenga capacidad de autogestión (autoridad), siempre puede decidir subdividirse en diferentes subdominios, manteniendo él en principio la autoridad sobre todos ellos. Posteriormente, la organización que gestiona el dominio puede decidir además delegar la autoridad de algunos (o todos) sus subdominios en otras organizaciones. La delegación es una acción que siempre decide el dominio padre, y éste puede revocarla cuando desee, volviendo a retomar la autoridad sobre el subdominio que había delegado.

8.1.4. Servidores de nombres y zonas

Como se ha dicho anteriormente, los programas que almacenan información sobre el espacio de nombres de dominio se denominan servidores de nombres. En virtud de la delegación mencionada anteriormente, cada servidor de nombres posee generalmente información completa sobre una *parte contigua* del espacio de nombres (generalmente un dominio, potencialmente dividido en subdominios). Dicha parte del espacio se denomina *zona*, y se dice que el servidor de nombres tiene *autoridad* sobre ella. En realidad, un mismo servidor de nombres puede tener autoridad sobre múltiples zonas, y obtiene la información que describe la zona (los registros de recursos) o bien de un fichero local o bien de otro servidor de nombres.

Entender la diferencia entre una zona y un dominio es importante. Todos los dominios de primer nivel, y la mayoría de dominios de segundo nivel, se dividen en unidades más pequeñas y manejables gracias a la delegación. Estas unidades se denominan zonas y contienen una serie de registros almacenados en un servidor. Sin embargo, las zonas no son dominios. Un dominio es un subárbol del espacio de nombres, mientras que una zona es una parte del espacio de nombres DNS que se almacena generalmente en un fichero y que puede contener informació sobre múltiples dominios.

DNS define dos tipos de servidores de nombres que mantienen informacion sobre el espacio de nombres: primarios (*maestros*) y secundarios (*esclavos*). Un servidor de nombres primario para una zona lee los datos de la zona desde un fichero que él mantiene. Un servidor de nombres secundario para una zona obtiene los datos de la zona desde otro servidor de nombres que es autoritario para la zona, llamado servidor maestro. Normalmente el servidor maestro es el servidor primario de la zona, pero esto no es un requisito ya que un servidor secundario puede cargar los datos desde otro secundario.

Cuando un servidor de nombres secundario se inicia, éste se pone en contacto con su servidor maestro y, si es necesario, inicia una transferencia de zona, es decir, una actualización de su información sobre la zona (ver Sección 8.2.4, “Transferencias

de zona"). Además, periódicamente el servidor secundario contacta con el servidor maestro para ver si los datos de zona han cambiado. Tanto el servidor primario como el secundario poseen autoridad sobre la zona. Definir servidores secundarios proporciona tolerancia a errores y reduce la carga en el servidor primario de la zona.

8.1.5. Resolución de nombres

Los clientes DNS utilizan bibliotecas llamadas "solucionadores" (*resolvers*) que efectúan las consultas DNS a los servidores en nombre del cliente.

Los servidores de nombres son los expertos en obtener información del espacio de nombres de dominio. Es decir, no solamente responden los datos referentes a las zonas sobre los que tienen autoridad, sino que pueden también buscar información a través del espacio de nombres de dominio para encontrar datos sobre los que no son autoritarios. A este proceso se le denomina *resolución de nombres*. Por ese motivo, existen servidores de nombres que no mantienen información sobre ninguna zona, y únicamente sirven para responder consultas de los clientes (*resolvers*) sobre cualquier dominio. Este tipo de servidores DNS se denomina *cache only*.

Ya que el espacio de nombres está estructurado como un árbol invertido, un servidor de nombres necesita únicamente los nombres de dominio y las direcciones de los servidores de nombres raíz para encontrar cualquier punto en el árbol. Los servidores raíz conocen dónde se encuentran los servidores de nombres con autoridad para los dominios de primer nivel. De hecho, la mayoría de servidores raíz son autoritarios para los dominios de primer nivel genéricos.

Cuando se solicita una consulta a cualquier nombre de dominio, los servidores raíz pueden al menos proporcionar los nombres y direcciones de los servidores de nombres autoritarios para el dominio de primer nivel al que pertenece el nombre de dominio buscado. Y los servidores de nombres de primer nivel pueden proporcionar la lista de servidores de nombres autoritarios para el dominio de segundo nivel al que pertenece el nombre de dominio buscado. De esta forma, cada servidor de nombres consultado va proporcionando la información más próxima a la respuesta buscada, o proporciona la propia respuesta.

Como conclusión hay que resaltar la importancia que tienen los servidores de nombres raíz en el proceso de resolución. Por esta razón, el sistema de nombres de dominio proporciona mecanismos de caché para ayudar a reducir la carga que supondría el proceso de resolución sobre los servidores raíz. Si todos los servidores raíz de Internet fallaran por un largo período de tiempo, toda la resolución en Internet fallaría. Para protegerse, Internet posee 13 servidores de nombres raíz repartidos por diferentes partes de la Red.

8.2. Configuración de DNS

Los estándares de DNS no especifican la estructura de datos interna en que deben almacenarse los registros de recursos (registros de la base de datos DNS), y por tanto existen varias implementaciones que son diferentes en este sentido. Por regla general, los servidores guardan la información sobre las zonas en ficheros en texto plano sin formato. Los nombres de los archivos son arbitrarios y se especifican en la configuración del servidor DNS.

Por ejemplo, en la implementación habitual de DNS en el mundo UNIX, denominada BIND (*Berkeley Intenet Name Domain*), se utiliza los nombres de archivo siguientes para almacenar los registros de cada zona:

- `Db.nombre_de_zona`: zona de resolución directa.
- `Db.identificador_de_red`: zona de resolución inversa.
- `Db.cache`: sugerencias de servidores raíz.
- `Db.127.0.0.1`: resolución inversa de bucle cerrado.

Sin embargo, la configuración predeterminada del servidor DNS de Microsoft Windows 2000 no utiliza los mismos nombres de archivo que BIND, sino que usa la nomenclatura `nombre_zona.dns`. Por otra parte, Windows 2000 permite que la base de datos DNS se integre en la base de datos del Directorio Activo, en cuyo caso dicha información participa de los mismos mecanismos de almacenamiento y replicación que el resto de información contenida en dicho servicio de directorio.

8.2.1. Registros de Recursos (RR)

Para resolver nombres, los servidores consultan sus zonas. Las zonas contienen *registros de recursos* que constituyen la información de recursos asociada al dominio DNS. Por ejemplo, ciertos registros de recursos asignan nombres descriptivos a direcciones IP, otros establecen quienes son los servidores de nombres de la zona, etc.

El formato de cada registro de recursos es el siguiente:

```
Propietario     TTL     Clase     Tipo     RDATA
```

donde:

- **Propietario**: nombre de *host* (ordenador) o del dominio DNS al que pertenece este recurso. Puede contener:

1. un nombre de host o de dominio, completamente cualificados o no (cualquier nombre que no acaba en un punto se considera *relativo* a la zona que se está describiendo),
2. el símbolo "@" (que representa el nombre de la zona que se está describiendo), o
3. una cadena vacía (en cuyo caso equivale al propietario del registro de recursos inmediatamente anterior).

- **TTL**(*Time To Live*): Tiempo de vida, generalmente expresado en segundos, que un servidor DNS o un resolver debe guardar en caché esta entrada antes de descartarla. Este campo es opcional. También se puede expresar mediante letras indicando días (d), horas (h), minutos (m) y segundos (s). Por ejemplo: "2h30m".

- **Clase**: define la familia de protocolos en uso. Suele ser siempre "`IN`", que representa Internet.

- **Tipo**: identifica el tipo de registro.

- **RDATA** : los datos del registro de recursos.

Las siguientes secciones describen los principales tipos de registros de recursos: SOA, NS, A, PTR, CNAME, MX y SRV.

8.2.1.1. Registro de Recurso SOA

Cada zona contiene un registro de recursos denominado Inicio de Autoridad o SOA (*Start Of Authority*) al comienzo de la zona. Los registros SOA incluyen los siguientes campos (sólo se incluyen los que poseen un significado específico para el tipo de registro):

- **Propietario**: nombre de dominio de la zona.

- **Persona responsable**: contiene la dirección de correo electrónico del responsable de la zona. En esta dirección de correo, se utiliza un punto en el lugar del habitual símbolo "@".

- **Número de serie**: muestra el número de versión de la zona, es decir, un número que sirve de referencia a los servidores secundarios de la zona para saber cuándo deben proceder a una actualización de su base de datos de la zona (o *transferencia de zona*). Cuando el número de serie del servidor secundario sea *menor* que el número del maestro, esto significa que el maestro ha cambiado la zona, y por tanto el secundario debe solicitar al maestro una transferencia de zona. Por tanto, este

número debe ser incrementado (manualmente) por el administrador de la zona cada vez que realiza un cambio en algún registro de la zona (en el servidor maestro).

- **Actualización**: muestra cada cuánto tiempo un servidor secundario debe ponerse en contacto con el maestro para comprobar si ha habido cambios en la zona.

- **Reintentos**: define el tiempo que el servidor secundario, después de enviar una solicitud de transferencia de zona, espera para obtener una respuesta del servidor maestro antes de volverlo a intentar.

- **Caducidad**: define el tiempo que el servidor secundario de la zona, después de la transferencia de zona anterior, responderá a las consultas de la zona antes de descartar la suya propia como no válida.

- **TTL mínimo**: este campo especifica el tiempo de validez (o de vida) de las respuestas "negativas" que realiza el servidor. Una respuesta negativa significa que el servidor contesta que un registro no existe en la zona.

  Hasta la versión 8.2 de BIND, este campo establecía el tiempo de vida por defecto de todos los registros de la zona que no tuvieran un campo TTL específico. A partir de esta versión, esto último se consigue con una *directiva* que debe situarse al principio del fichero de la zona. Esta directiva se especifica así:

```
$TTL tiempo
```

  Por ejemplo, un tiempo de vida por defecto de 30 minutos se establecería así:

```
$TTL 30m
```

Un ejemplo de registro SOA sería el siguiente:

```
admon.com.  IN  SOA pc0100.admon.com  hostmaster.admon.com.
                (
                  1      ; número de serie
                  3600   ; actualización 1 hora
                  600    ; reintentar 10 minutos
                  86400  ; caducar 1 día
                  60     ; TTL (negativo) 1 minuto
                )
```

8.2.1.2. Registro de Recurso NS

El registro de recursos NS (*Name Server*) indica los servidores de nombres autoriza-

dos para la zona. Cada zona debe contener registros indicando tanto los servidores principales como los secundarios. Por tanto, cada zona debe contener, como mínimo, un registro NS.

Por otra parte, estos registros también se utilizan para indicar quiénes son los servidores de nombres con autoridad en subdominios delegados, por lo que la zona contendrá al menos un registro NS por cada subdominio que haya delegado.

Ejemplos de registros NS serían los siguientes:

```
admon.com.           IN   NS    pc0100.admon.com.
valencia.admon.com.  IN   NS    pc0102.valencia.admon.com.
```

8.2.1.3. Registro de Recurso A

El tipo de registro de recursos A (*Address*) asigna un nombre de dominio completamente cualificado (FQDN) a una dirección IP, para que los clientes puedan solicitar la dirección IP de un nombre de host dado.

Un ejemplo de registro A que asignaría la dirección IP 158.42.178.1 al nombre de dominio `pc0101.valencia.admon.com.`, sería el siguiente:

```
pc0101.valencia.admon.com.    IN   A       158.42.178.1
```

8.2.1.4. Registro de Recurso PTR

El registro de recursos PTR (*PoinTeR*) o puntero, realiza la acción contraria al registro de tipo A, es decir, asigna un nombre de dominio completamente cualificado a una dirección IP. Este tipo de recursos se utilizan en la denominada *resolución inversa*, descrita en Sección 8.1.4, "Servidores de nombres y zonas".

Un ejemplo de registro PTR que asignaría el nombre `pc0101.valencia.admon.com.` a la dirección IP 158.42.178.1 sería el siguiente:

```
1.178.42.158.in-addr.arpa.  IN   PTR  pc0101.admon.valencia.com.
```

8.2.1.5. Registro de Recurso CNAME

El registro de nombre canónico (CNAME, *Canonical NAME*) crea un alias (un sinónimo) para el nombre de dominio especificado.

Un ejemplo de registro CNAME que asignaría el alias `controlador` al nombre de dominio `pc0102.valencia.admon.com`, sería el siguiente:

```
controlador.valencia.admon.com.
                    IN      CNAME   pc0101.valencia.admon.com.
```

8.2.1.6. Registro de Recurso MX

El registro de recurso de intercambio de correo (MX, *Mail eXchange*) especifica un servidor de intercambio de correo para un nombre de dominio. Puesto que un mismo dominio puede contener diferentes servidores de correo, el registro MX puede indicar un valor numérico que permite especificar el orden en que los clientes deben intentar contactar con dichos servidores de correo.

Un ejemplo de registro de recurso MX que define al servidor `pc0100` como el servidor de correo del dominio `admon.com`, sería el siguiente:

```
admon.com.     IN     MX     0      pc0100.admon.com.
```

8.2.1.7. Registro de Recurso SRV

Con registros MX se puede especificar varios servidores de correo en un dominio DNS. De esta forma, cuando un proveedor de servicio de envío de correo necesite enviar correo electrónico a un host en el dominio, podrá encontrar la ubicación de un servidor de intercambio de correo. Sin embargo, esta no es la forma de resolver los servidores que proporcionan otros servicios de red como WWW o FTP.

Los registros de recurso de servicio (SRV, *SeRVice*) permiten especificar de forma genérica la ubicación de los servidores para un servicio, protocolo y dominio DNS determinados.

El formato de un registro SRV es el siguiente:

```
servicio.protocolo.nombre  TTL  clase  SRV
                           prioridad  peso  puerto  destino
```

donde:

- **Servicio**: especifica el nombre de servicio: http, telnet, etc.
- **Protocolo**: especifica el protocolo utilizado: TCP o UDP.
- **Nombre**: define el nombre de dominio al que hace referencia el registro de recurso SRV.

- **TTL** y **clase** ha sido definidos anteriormente.
- **Prioridad**: especifica el orden en que los clientes se pondrán en contacto con los servidores: los clientes intentarán ponerse en contacto primero con el host que tenga el valor de prioridad más bajo, luego con el siguiente y así sucesivamente.
- **Peso**: es un mecanismo de equilibrio de carga.
- **Puerto**: muestra el puerto del servicio en el host.
- **Destino**: muestra el nombre de dominio completo para la máquina compatible con ese servicio.

Un ejemplo de registros SRV para los servidores Web del dominio `admon.com.`, sería:

```
http.tcp.admon.com.  IN  SRV   0  0  80  www1.admon.com.
http.tcp.admon.com.  IN  SRV  10  0  80  www2.admon.com.
```

8.2.2. Definición de la delegación

Para que una zona especifique que uno de sus subdominios está delegado en una zona diferente, es necesario agregar un *registro de delegación* y, generalmente, el denominado "registro de pegado" (*glue record*). El registro de delegación es un registro NS en la zona principal (padre) que define el servidor de nombres autorizado para la zona delegada. El registro de pegado es un registro tipo A para el servidor de nombres autorizado para la zona delegada, y es necesario cuando el servidor de nombres autorizado para la zona delegada también es un miembro de ese dominio (delegado).

Por ejemplo, si la zona `admon.com` deseara delegar la autoridad a su subdominio `valencia.admon.com`, se deberían agregar los siguientes registros al archivo de configuración correspondiente de la zona `admon.com`:

```
valencia.admon.com.         IN  NS  pc0102.valencia.admon.com.
pc0102.valencia.admon.com.  IN  A   158.42.178.2
```

8.2.3. Tipos de zonas

Aunque distintas implementaciones de DNS difieren en cómo configurar las zonas, generalmente existe un fichero que indica sobre qué zonas tiene autoridad el servidor, indicando para cada una el fichero que contiene la información de dicha zona

(si el servidor es primario para la zona), o la dirección del servidor maestro a quien preguntar por ella (si es secundario).

En general, existen tres tipos distintos de zonas: zonas de búsqueda directa, zonas de búsqueda inversa y zonas de "sugerencia raíz". Un servidor DNS puede tener autoridad sobre varias zonas directas e inversas, y necesita poseer información sobre las "sugerencias raíz" si desea responder a sus clientes sobre registros de zonas sobre las que no posee autoridad. A continuacion se describe cada tipo brevemente.

8.2.3.1. Zona de búsqueda directa

Las zonas de búsqueda directa contienen la información necesaria para resolver nombres en el dominio DNS. Deben incluir, al menos, registros SOA y NS, y pueden incluir cualquier otro tipo de registros de recurso, excepto el registro de recursos PTR.

8.2.3.2. Zona de búsqueda inversa

Las zonas de búsqueda inversa contienen información necesaria para realizar las búsquedas inversas. La mayor parte de las consultas proporcionan un nombre y solicitan la dirección IP que corresponde a ese nombre. Este tipo de consulta es el descrito en la zona de resolución directa.

Pero existen ocasiones en que un cliente ya tiene la dirección IP de un equipo y desea determinar el nombre DNS de ese equipo. Esto es importante para los programas que implementan la seguridad basándose en el FQDN que se conecta y también se utiliza para la solución de problemas de red TCP/IP.

Si el único medio de resolver una búsqueda inversa es realizar una búsqueda detallada de todos los dominios en el espacio de nombres DNS, la búsqueda de consulta inversa sería demasiado exhaustiva como para realizarla de forma práctica.

Para solucionar este problema se creó un dominio DNS especial para realizar búsquedas "inversas", denominado `in-addr.arpa.`. Este dominio utiliza un orden inverso de números en la notación decimal de las direcciones IP. Con esta disposición se puede delegar la autoridad de miembros inferiores del dominio `in-addr.arpa.` a las distintas organizaciones, a medida que se les asigna identificadores de red de clase A, B o C.

8.2.3.3. Sugerencias de los servidores del Dominio Raíz

El archivo de "sugerencias raíz" (*root hint*), denominado también archivo de sugerencias de caché, contiene la información de host necesaria para resolver nombres fuera

de los dominios en los que el servidor posee autoridad. En concreto, este archivo contiene los nombres y las direcciones IP de los servidores DNS del dominio punto (`.`) o raíz.

8.2.4. Transferencias de zona

En aquellas zonas en las que existen diferentes servidores de nombres con autoridad (uno principal o maestro y uno o varios secundarios o esclavos), cada vez que se realizan cambios en la zona del servidor maestro, estos cambios deben replicarse a todos los servidores secundarios de esa zona. Esta acción se lleva a cabo mediante un mecanismo denominado transferencia de zona. Existen dos tipos de transferencia de zonas: completa e incremental.

8.2.4.1. Transferencia completa de zona

En una transferencia completa de zona, el servidor maestro para una zona transmite toda la base de datos de zona al servidor secundario para esa zona.

Los servidores secundarios siguen los siguientes pasos a la hora de realizar una transferencia de zona:

1. El servidor secundario para la zona espera el tiempo especificado en el campo Actualizar del registro SOA y luego le pregunta al servidor maestro por su registro SOA.
2. El servidor maestro responde con su registro SOA.
3. El servidor secundario para la zona compara el número de serie devuelto con su propio número y si este es mayor que el suyo, solicita una transferencia de zona completa.
4. El servidor maestro envía la base de datos de la zona completa al servidor secundario.

Si el servidor maestro no responde, el servidor secundario lo seguirá intentando después del intervalo especificado en el campo Reintentos del registro SOA. Si todavía no hay respuesta después del intervalo que se especifica en el campo `Caduca` desde la última transferencia de zona, este descarta su zona.

8.2.4.2. Transferencia incremental de zona

Las transferencias completas de zona pueden consumir gran ancho de banda de la red. Para poder solucionar este problema se define la transferencia incremental de

zona, en la cual sólo debe transferirse la parte modificada de una zona.

La transferencia incremental de zona funciona de forma muy similar a la transferencia completa. En este caso, el servidor secundario para la zona comprueba el número de serie del registro SOA del maestro con el suyo, para determinar si debe iniciar una transferencia de zona, la cual en este caso sería incremental (sólo de los cambios realizados).

8.2.4.3. Notificación DNS

Con este proceso se pretende que el servidor maestro para la zona notifique los cambios a ciertos servidores secundarios y de esta manera los secundarios podrán comprobar si necesitan iniciar una transferencia de zona. De esta forma se mejora la coherencia de los datos mantenida por todos los servidores secundarios.

8.2.5. Actualizaciones dinámicas

Originalmente, DNS se diseñó para que solamente admitiera cambios estáticos. De esta forma, sólo el administrador del sistema DNS podía agregar, quitar o modificar los registros de recursos, realizando cambios manuales sobre los ficheros de configuración correspondientes.

El sistema de actualizaciones dinámicas, permite que el servidor principal para la zona pueda configurarse de forma que acepte actualizaciones de recursos enviadas desde otros equipos (habitualmente, sus clientes DNS). Este es el sistema preferido en el caso de Windows 2000, aunque muchos administradores de DNS lo desaconsejan por razones de seguridad.

Por ejemplo, el servidor maestro puede admitir (e incluir en su configuración) actualizaciones de registros A y PTR de las estaciones de trabajo de su dominio, que le envían esa información cuando arrancan. También sería posible recibir estas actualizaciones de un servidor DHCP, una vez ha proporcionado la configuración IP a un cliente.

9

El servicio DFS

Indice

9.1. Introducción

El Sistema de archivos distribuidos o DFS (*Distributed File System*) es un componente de red del servidor que facilita la forma de encontrar y manejar datos en la red. DFS agrupa ficheros que están en diferentes ordenadores en un espacio de nombres único.

DFS facilita la construcción de una única vista jerárquica de múltiples servidores de archivos. En vez de ver una red física compuesta por decenas de servidores de ficheros, cada uno con una estructura de directorios separada, los usuarios verán unos pocos directorios lógicos que incluyen todos los servidores y carpetas compartidas. Cada carpeta compartida aparecerá en el lugar lógico que le corresponde en el directorio, sin importar en que servidor se encuentra.

DFS es, para los servidores y las carpetas compartidas, lo que los sistemas de ficheros es para los discos duros. Los sistemas de ficheros proporcionan un acceso nominado uniforme al conjunto de sectores del disco; DFS proporciona una convención de nominación uniforme para los servidores , carpetas compartidas y ficheros. De esta forma, DFS hace posible organizar los servidores de archivos y sus recursos compartidos en una estructura jerárquica, haciendo más fácil para una gran organización administrar y usar sus recursos de información.

Históricamente, con la convención de nombres universal (*Universal Name Convention*, UNC), un usuario o aplicación debía de especificar el servidor y el recurso compartido, seguido de la ruta a partir del recurso hasta llegar al fichero, para poder acceder a dicho fichero. Es decir, un UNC tiene la forma siguiente:

```
\\servidor\recurso_compartido\ruta\...\archivo
```

Aunque en general los nombres UNC se pueden utilizar directamente, la forma más habitual de acceder a ficheros compartidos por otros equipos es realizar como paso previo la asignación del recurso (carpeta) compartida a una letra de unidad local (que queda redireccionada a dicho recurso `\\servidor\recurso_compartido`). Posteriormente, el usuario se desplaza a partir de dicha unidad redireccionada a los datos a los que desea tener acceso. Por ejemplo:

```
net use x: \\servidor\carpeta_compartida
copy x:\ruta\....\archivo   directorio
```

Mientras las redes continúan creciendo en tamaño y las organizaciones empiezan a usar el almacenamiento del que disponen, tanto interna como externamente, para

tales fines como son las intranets, la asignación de una única letra de unidad a medios de red compartidos resulta eficaz. Además, a pesar de poder usar directamente nombres UNC, los usuarios pueden verse desbordados por el número creciente de lugares de donde deben obtener datos.

DFS soluciona estos problemas vinculando servidores de archivos y recursos compartidos a un espacio de nombres sencillo y descriptivo. Dado que DFS asigna el almacenamiento físico como una representación lógica, la ventaja es que la ubicación física de los datos se hace transparente para los usuarios y las aplicaciones.

9.2. Tipos y características de DFS

Como hemos visto, en un entorno de red, los usuarios pueden tener dificultades para mantenerse al corriente de las ubicaciones físicas de los recursos compartidos. Cuando se utiliza DFS, sin embargo, las estructuras de la red y del sistema de archivos se hacen transparentes para los usuarios. Esto permite al administrador centralizar y optimizar el acceso a los recursos en función de una estructura con un único árbol. DFS proporciona una estructura de árbol lógico para los recursos del sistema de archivos que pueden estar en cualquier lugar de la red. Como el árbol de DFS es un punto de referencia único, los usuario pueden tener acceso fácilmente a los recursos de la red cualquiera que sea su ubicación real. DFS también permite a los administradores administrar varias carpetas compartidas desde una única ubicación.

Se pueden configurar dos tipos de DFS:

A. **DFS independiente**. Almacena la topología de DFS en el registro del equipo local donde se crea. Este tipo de DFS no proporciona tolerancia a errores si se produce un error en el equipo donde se almacenan las carpetas compartidas o la topología DFS, puesto que se almacena en una sola máquina. Cada equipo puede alojar solo un árbol DFS como máximo.

B. **DFS de dominio**. Almacena la topología de DFS en Active Directory. Este tipo de DFS señala a varias carpetas compartidas idénticas, lo que proporciona tolerancia a errores. Además, admite el Sistema de nombres de dominio, varios niveles y la replicación de archivos.

Como conclusión, podemos decir que para compartir los recursos de archivo en toda la red, DFS:

- **Organiza los recursos en una estructura de árbol**. Un recursos compartido de DFS utiliza una estructura de árbol que contiene un nodo raíz y vínculos. Para

crear un recurso compartido DFS, primero debe crear una raíz DFS. Cada raíz DFS puede tener varios vínculos por debajo, cada uno de los cuales señala a una carpeta compartida. Los vínculos de el espacio de nombres DFS representan carpetas compartidas que pueden encontrarse físicamente en diferentes servidores.

- **Facilita la exploración de la red**. Un usuario que recorre un árbol administrado por DFS no necesita conocer el nombre del servidor donde está compartida la carpeta. Esto simplifica el acceso a la red, ya que los usuarios no necesitan encontrar el servidor donde se encuentra un determinado recurso de red. Tras conectar con el espacio de nombres DFS, los usuarios podrán buscar y tener acceso a todos los recursos situados por debajo del espacio de nombres, con independencia de la ubicación o el nombre del servidor.

- **Facilita la administración de la red**. DFS de dominio también simplifica la administración de la red. Si se produce un error en un servidor, un administrador puede mover un vínculo de un servidor a otro sin que los usuarios se den cuentan del cambio. Para mover un vínculo basta con modificar la carpeta DFS para que haga referencia a la ubicación de las carpetas compartidas en el nuevo servidor. Los usuarios siguen utilizando la misma ruta DFS que señala el vínculo.

- **Conserva los permisos de red**. Un usuario puede tener acceso a una carpeta compartida a través de DFS, siempre y cuando tenga el permiso necesario de acceso a la carpeta compartida.

Sólo los equipos cliente con software de cliente DFS pueden tener acceso a los recursos de DFS. Los equipos que corren bajo Windows 98, Windows NT 4.0 o Windows 2008 incluyen software de cliente DFS. Debe descargar e instalar este software en los equipos que ejecuten Microsoft Windows 95.

9.3. Funcionamiento de DFS

Un recurso compartido de DFS utiliza una estructura de árbol. Para crear un recurso compartido DFS, primero debe crear una raíz DFS. el espacio de nombres en sí es un recurso compartido que se encuentra en lo mas alto del árbol DFS y que sirve de punto de inicio para alojar:

- **Carpetas compartidas**.

- **Vínculos a recursos compartido**, que se trata de una referencia a una carpeta compartida SMB, NetWare, NFS , NCP u otra raíz DFS. Se componen de una etiqueta, que es el nombre visible en el árbol DFS y la referencia al recurso de red vinculado.

Dentro de un árbol DFS, el administrador organiza los recursos compartidos, vínculos a recursos compartidos en los distintos servidores y vínculos a vínculos en otros árboles DFS. Por tanto, podemos crear estructuras más complejas que nos permitirá organizar todos nuestros recursos en un único espacio de nombres uniforme, independizando la forma de acceder a los recursos de la forma en que hemos distribuido éstos entre los servidores.

Toda la información de recursos definida a partir del espacio de nombres de un sistema DFS comparten el espacio de nombres DFS, que es lo que verán los usuarios. Este espacio de nombres tiene una limitación en el tamaño de ruta hacia cualquier archivo en 260 caracteres y otra en el número máximo de carpetas compartidas y vínculos DFS que se pueden crear por raíz, que es de 1000.

Cuando el árbol DFS es de dominio, puede tener varias réplicas del espacio de nombres, aunque en un servidor sólo puede haber una réplica de la misma raíz. Windows 2008 acepta hasta 256 miembros de una replica del árbol DFS. El conjunto de raíces del árbol DFS contienen la misma información, pero dotan al sistema de tolerancia a fallos y de reparto de carga equilibrado entre los servidores integrantes. Toda la información de la topología se almacena en el directorio y los mecanismos de replicación de éste se encargan de mantener replicada la topología en todos los servidores raíz de DFS.

Los cambios en la topología son visibles en el momento de aplicar sin necesidad de detener el servicio.

9.3.1. Acceso a los recursos de un DFS

El acceso a una archivo o carpeta dentro del espacio de nombres de DFS se realiza del mismo modo que a un recurso UNC. Por tanto, los clientes NT 4.0 y Windows 9x pueden acceder a él de la forma:

```
\\servidor\recurso
```

siendo `recurso` el nombre del recurso compartido raíz del árbol DFS y `servidor` el nombre del ordenador que ofrece tal recurso.

Desde clientes Windows 2008 o Windows anteriores actualizados con el software de acceso a DFS, se puede también acceder a los árboles DFS de dominio mediante el UNC:

```
\\nombre_del_dominio\raiz_DFS
```

De este modo, el usuario no necesita recordar los nombres de los servidores don-

de están alojados realmente los recursos compartidos. Si creamos una raíz DFS de dominio, el usuario podrá localizar los recuros simplemente con el nombre del dominio y un nombre significativo a el espacio de nombres DFS.

Además, desde Windows 2008 y NT 4.0, se puede utilizar:

- **net use** "**profundo**", que consiste en poder asignar letra de unidad a una ruta dentro del espacio de nombres del árbol DFS.
- **Vínculos a volúmenes** NetWare, NFS o NCP. Desde el resto de clientes, estos vínculos aparecen como carpetas vacías.

Internamente, cuando el usuario necesita acceso a los recursos del DFS, el cliente DFS hace una consulta a los servidores para obtener una estructura de datos que almacena la topología del DFS y que se denomina PKT (*Partition Knowledge Table*). Esta tabla almacena información sobre los recursos del DFS del tipo:

- Ruta DFS de recurso. Por ejemplo, el siguiente:

```
\\upv.es\raiz_dfs\ms\aplicaciones
```

- UNC o UNCs del recurso. Como, por ejemplo:

```
\\izar2\aplicaciones    e    \\izar3\aplicaciones
```

- Sistema operativo de la máquina servidora.
- Tiempo de vida de la entrada PKT.

Con esta información y la dirección IP del cliente, el software cliente DFS de Windows 2008 escogerá el recurso al cual debe conectarse para dar acceso al usuario. Windows 2008 garantiza que se realiza equilibrio de la carga si un recurso se encuentra replicado en varios servidores y que el acceso se realizará sobre la réplica más accesible, desde el punto de vista de la configuración de sitios del directorio.

Para acelerar el acceso, los clientes almacenan en caché las partes de la PKT a medida que el usuario va recorriendo la estructura del espacio DFS. Por este motivo, se introduce un campo de validez de la PKT.

9.3.2. Replicación de DFS basado en dominio

La replicación de DFS consta de dos partes:

a. **Replicación de la topología DFS.** La información de la topología se encuentra en el directorio activo y por tanto esta sujeta a la replicación de éste. Esto implica que durante un tiempo, diferentes controladores pueden ver una topología distinta hasta que los cambios realizados en algún controlador leguen a replicarse en él.

   El tiempo de replicación puede ser considerable debido a que cada vínculo ocupa alrededor de 400 bytes en la PKT. Dependiendo del árbol en concreto, esto puede traducirse en varias decenas de kilo-bytes a replicar.

b. **Replicación del contenido DFS.** Pueden configurarse múltiples copias de una carpeta compartida con, o sin, replicación de contenido. Se puede encargar al servicio de replicación de archivos, en adelante FRS (*File Replication Service*) la sincronización de las copias o bien realizar copias manuales. Si el recurso no se actualiza a menudo puede considerarse realizar a mano la sincronización.

9.3.3. Seguridad de DFS

Al espacio de nombres de DFS no se pueden aplicar ACLs. Cuando un usuario accede a un vínculo en concreto del DFS, se aplicarán las ACLs definidas para ese recurso en el servidor. Cuando un usuario intenta acceder a una carpeta intermedia donde no tenga permisos, ésta aparecerá vacía para él. Esto implica que el resto de la jerarquía no será visible aunque en niveles inferiores si tuviese permisos.

Si se realiza a mano la sincronización de réplicas de los vínculos, se ha de asegurar que el almacenamiento destino tenga los mismos permisos. Si la replicación es por FRS, las ACLs también se copian en las réplicas.

Por lo que respecta a la administración, el administrador del dominio puede administrar la topología del DFS, pero la administración de las ACLs de los recursos a los que se vincula queda condicionada a los permisos de administración que pueda tener en dichos recursos.

9.4. Espacio de Nombres DFS

Un espacio de nombres DFS es básicamente un lugar donde usted tendrá todos los enlaces a sus recursos compartidos de archivos. Desde el punto de vista del admi-

nistrador, usted debe pensar en ello como una estructura de carpetas en las que guarda la lista de recursos compartidos de archivos de destino. Los usuarios lo verán como una sola acción con muchas carpetas y no tendrán idea de que están navegando a través de un conjunto de servidores para llegar a las subcarpetas y archivos

Cuando se procede a la configuración de DFS, se tiene la opción de usar un **espacio de nombres basado en dominio o independiente**. Si ya dispone de Active Directory implementado, debe considerar el uso de un espacio de nombres basado en dominios. Si no está utilizando Active Directory, su única opción es un *stand-alone* uno.

La principal ventaja de los espacios de nombres basados en dominios es que su configuración se almacena en Active Directory y usted no tendrá que depender de un solo servidor para proporcionar la información de espacio de nombres a sus clientes. La ruta de acceso que los usuarios utilizan, será el nombre del dominio y no tendrá que cambiar porque el nombre del servidor de espacio de nombres ha cambiado (sólo si usted cambia su nombre de dominio).

Con un DFS independiente, el nombre de servidor se convierte en parte del camino principal al espacio de nombres.

También hay dos **modos** de DFS basado en dominio:

1. Windows Server 2008: requiere Windows Server 2003 nivel funcional de bosque, Windows Server 2008 nivel funcional de dominio y Windows Server 2008 se ejecuta en todos los servidores de espacio de nombres.
2. Windows Server 2000

El primer paso para configurar un recurso compartido de DFS es crear una raíz DFS. Las raíces DFS se pueden crear sobre particiones FAT o NTFS. Como siempre, hay que tener en cuenta que el sistema de archivos FAT no ofrece las ventajas de seguridad (permisos) del sistema NTFS.

Cuando se crea una raíz DFS, se tiene la opción de establecer una raíz independiente o una raíz de dominio. A continuación se explican ambas.

9.4.1. Configuración de espacio de noombres independiente

Una raíz independiente se encuentra físicamente en el servidor al que los usuarios se conectan inicialmente. Para crear una raíz DFS independiente, en Herramientas

administrativas abra la consola del Sistema de archivos distribuido e inicie el Asistente para crear nueva raíz DFS. Las opciones del asistente son las siguientes:

- Seleccionar el tipo de raíz DFS: en este caso, independiente.
- Especificar el servidor huésped para el espacio de nombres DFS: el punto de conexión inicial, o el servidor *host*, para todos los recursos contenidos en el árbol DFS. Se puede crear una raíz DFS en cualquier equipo que corra bajo Windows 2008 Server.
- Especificar el recurso compartido de raíz DFS: una carpeta compartida para albergar el espacio de nombres DFS.
- Nombre del espacio de nombres DFS: un nombre descriptivo para el espacio de nombres DFS.

9.4.2. Configuración de un espacio de nombres DFS de dominio

Una raíz DFS de dominio debe estar alojada en un servidor miembro del dominio. Active Directory almacena la topología de cada árbol DFS y replica la topología en todos los servidores raíz DFS participantes. Como los cambios realizados en un árbol DFS se sincronizan automáticamente con Active Directory, siempre puede restaurar la topología de un árbol DFS si el espacio de nombres DFS está fuera de conexión por cualquier motivo.

Se puede implementar la tolerancia a fallos los archivos contenidos en el árbol DFS mediante la asignación de réplicas a un vínculo DFS. Un conjunto de recursos replicados puede atender a cualquier nodo del árbol DFS. Si por cualquier motivo se produce un error en la conexión de un cliente a una réplica, el cliente DFS intentará automáticamente conectarse a otra réplica. El cliente DFS recorre todas las réplicas hasta que encuentra una disponible.

Para crear una raíz DFS de dominio, utilice la consola del Sistema de archivos distribuido y desde ahí, inicie el Asistente para crear nueva raíz DFS. A continuación se describen las opciones que se pueden configurar:

- Selección del tipo de raíz DFS: en este caso, raíz DFS de dominio.
- Selección del dominio huésped para el espacio de nombres DFS: el dominio *host* del árbol DFS. Un dominio puede alojar varias raíces DFS.
- Especificar el servidor huésped para el espacio de nombres DFS: el punto de co-

nexión inicial, o el servidor *host*, para todos los recursos contenidos en el árbol DFS.

- Especificar el recurso compartido de raíz DFS: una carpeta compartida para albergar el espacio de nombres DFS. Puede elegirse una carpeta compartida existente o crearse una nueva.
- Nombre del espacio de nombres DFS: un nombre descriptivo para el espacio de nombres DFS.

Para crear una segunda raíz DFS de dominio, hay que abrir la consola del Sistema de archivos distribuidos, hacer clic con el botón secundario del ratón en el dominio y después hacer clic en "Nuevo miembro duplicado de raíz". Las únicas opciones que hay para crear una segunda raíz son "Especifique el servidor para albergar DFS" y "Seleccione el recurso compartido para el volumen del espacio de nombres DFS".

9.5. Configuración de los vínculos DFS

Se pueden agregar recursos compartidos DFS en el espacio de nombres o en cualquier otro nodo de rama del árbol. Si el recurso en cuestión no es de Windows 2008, el recurso compartido se agregará como una hoja, que no puede tener un vínculo por debajo de ella.

Una vez que haya creado una raíz DFS, puede crear vínculos DFS que señalen a las carpetas compartidas. Para crear un vínculo DFS, deben seguirse los pasos citados a continuación:

1. En la consola Sistema de archivos distribuido, hacer clic en el espacio de nombres DFS a la que agregará un vínculo.
2. En el menú Acción, hacer clic en Nuevo vínculo DFS.
3. En el cuadro de diálogo Crear un nuevo vínculo DFS, se pueden configurar las opciones:

    - Nombre de vínculo: el nombre que los usuarios verán cuando se conecten a DFS.
    - Enviar el usuario a esta carpeta compartida: el nombre UNC de la ubicación real de la carpeta compartida a la que se refiere el vínculo.
    - Comentario.

- Los clientes mantienen en caché esta referencia durante x segundos: es el intervalo de tiempo durante el que los clientes mantendrán en caché una referencia a un vínculo DFS. Una vez caducada la referencia, el cliente tienen que volver a consultar al servidor DFS para conocer la ubicación del vínculo.

Una vez creado el vínculo, este aparecerá bajo el volumen del espacio de nombres DFS en la consola del Sistema de archivos distribuidos.

9.6. Sistema de Replicación de Archivos

Llegados a este punto, se plantea la pregunta: ¿Cómo se copian los datos entre varios servidores? Bueno, Windows Server 2008 incluye un componente para replicar datos entre servidores de archivos. Se llama **DFS-R** (*Distributed File System Replication*).

DFS-R se introdujo con Windows Server 2003 R2 (en sustitución del antiguo FRS con muchas ventajas). DFS-R se puede utilizar para ambos DFS basados en dominios e independientes. Para replicar archivos entre dos (o más) recursos compartidos, es necesario crear un grupo de replicación y especificar algunas cosas como los servidores que replican (miembros) y lo que van a replicar (replicado las carpetas).

DFS-R conoce la topología de sitio. También tiene opciones para controlar la programación y el uso de ancho de banda (*estrangulamiento*). DFS-R utiliza la compresión diferencial remota (RDC), lo que significa que sólo los cambios son enviados por la red entre los distintos servidores miembros y no el fichero entero.

El sistema dispone un calendario configurable para marcar el momento de replicar la información de una carpeta ubicada en varias máquinas, permitiendo la copia del archivo, su información, atributos y ACLs.

A

Nota Legal