Tema 4

Windows NT

Nociones sobre discos duros

MBR, particiones, volúmenes, formatos, son conceptos que tendremos que tener claro si pretendemos gestionar adecuadamente nuestros discos duros bajo Windows NT. Un disco duro es básicamente un conjunto de platos recubiertos con un material sensible a alteraciones magnéticas que giran a gran velocidad (cuya misión es la de almacenar los datos) y unos cabezales móviles de gran precisión (los encargados de leer y escribir en los platos magnéticos). Los dos estándares más utilizados son IDE y SCSI.

La secuencia de inicio

Una vez que la ROM ha detectado el disco duro principal lee el primer registro que se encuentra en éste, dicho registro es el **Master Boot Record** (**MBR**, literalmente registro maestro de arranque), que contiene un programa ejecutable y una tabla donde están definidas las particiones del disco. El ejecutable del MBR llama a su vez a otro programa contenido en el primer sector de la partición primaria activa que es el encargado de cargar el sistema operativo en memoria.

Particiones primarias y extendidas

Antes de comenzar a trabajar con un disco duro creamos en él una serie de particiones (de una a cuatro con NT) que contendrán los datos. Existen dos tipos de particiones: la **partición primaria** y la **partición extendida**. En NT podemos definir por cada disco hasta cuatro particiones primarias pero sólo una puede estar activa. Gracias a esto podrían convivir en nuestro equipo cuatro sistemas operativos distintos.

La partición extendida no puede usarse como partición de arranque de un sistema operativo, pero tiene la ventaja de poder dividirse en varios volúmenes y asignarle una letra distinta a cada uno de ellos. El usuario nunca trabaja directamente sobre las particiones de un disco duro, ni notará ninguna diferencia por trabajar en una primaria o en una extendida. Para trabajar con los datos se define el concepto de volumen, cada volumen lleva asignada una letra de unidad que la identifica para poder trabajar con ella.

Aunque se hayan definido las particiones en las que se va a estructurar el disco, todavía éstas no son accesibles al sistema operativo. Para ello tenemos que formatear cada una de las particiones con un formato reconocible por el sistema operativo que vayamos a instalar. Una vez formateadas podemos definir el concepto de volumen.

El fichero BOOT.INI

La partición primaria es la única desde la que puede arrancar el sistema operativo, aquí es donde el MBR buscará el programa que controla el arranque (**boot manager**), que en NT se configura con el archivo **BOOT.INI**.

```
[boot loader]
timeout=10
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT

[operating systems]
multi(0)disk(0)rdisk(0)partition(3)\WINNT="Windows NT Server versión 4.00"
multi(0)disk(0)rdisk(0)partition(3)\WINNT="Windows NT Server 4.00 [modo VGA]" /basevideo /sos
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT Workstation versión 4.00"
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT Workstation 4.00[modo VGA]" /basevideo /sos
```

En la primera parte del mismo ([boot loader]) se indica el tiempo para seleccionar dentro del menú y el sistema operativo que arrancará por defecto. En la segunda sección ([operating system]) se indica el menú que se mostrará por pantalla con la lista de todos los SOs instalados y las particiones donde se encuentran. Por cada sistema operativo se incluyen dos líneas: la primera para arrancarlo con la configuración de vídeo establecida y la segunda con una configuración de vídeo VGA, para evitar que una mala configuración nos impida volver a arrancar ese sistema operativo.

Nombres ARC

Los nombres ARC (**Advanced RISC Computing**) son la forma que tienen los equipos NT para nombrar a los discos duros y a sus particiones. Microsoft diseño estos nombres para que su tratamiento fuera independiente de la plataforma. Es decir, se emplea tanto en equipos RISC como en equipos x86. El nombre describe el tipo de adaptador y su número, el número del disco, el número del rdisk y el número de la partición.

<tipoadaptador>(x)disk(y)rdisk(z)partition(n)

donde el *tipoadaptador* puede ser *scsi* o *multi*. El *multi* se emplea en todos los adaptadores no-SCSI y para aquellos adaptadores SCSI que no empleen BIOS, que son casi todos los que se utilizan con procesadores x86. La *x* es el número del adaptador, comenzando por 0. El valor de *y* es el número del disco *scsi* en el adaptador SCSI y en *multi* siempre 0. El valor *z* es siempre 0 para *scsi* y ordinal del disco en *multi*, comenzando por 0. Finalmente el valor *n* es el número de la partición empezando en 1 (el 0 se reserva para el espacio no empleado).

Volúmenes

Los volúmenes o unidades lógicas son porciones de uno o varios discos duros que el sistema operativo trata como si fueran una sola unidad física, como si dijéramos un disco duro virtual. De manera que podemos escribir y leer datos en ellas, formatearlas, buscar errores, etc. Un volumen puede abarcar:

- Una partición primaria completa, la partición primaria sólo puede albergar un volumen, de hecho el administrador de discos de NT identifica este tipo de volumen como "partición primaria".
- Un fragmento de una partición extendida. En una partición extendida podemos incluir tantos volúmenes cómo queramos ;-) , este tipo de volumen recibe el nombre de "unidad lógica" en el administrador de disco de NT.
- Distintos fragmentos de particiones primarias o extendidas en discos duros diferentes, el administrador de disco marcará este tipo de volumen como "conjunto de volúmenes".

El Administrador de discos de NT nos permite jugar con todas estas variables a nuestro antojo.

¿Por qué de hacen particiones en un disco duro?

El hacer particiones en un disco duro puede representar interesantes ventajas:

- **Flexibilidad:** si tenemos en nuestro sistema sólo un disco con una sola partición primaria no podremos acceder a las interesantes opciones que nos permite el administrador de discos, ya que esta partición albergará el sistema y no puede ser modificada. Si tenemos uno o varios discos con unas cuantas particiones podremos crear nuevos volúmenes, ampliar el espacio en las unidades existentes, crear discos espejo, etc.
- **Organización:** es adecuado tener separados los grandes bloques de datos en distintas particiones de manera que nuestro árbol de directorios sea menos complicado y más intuitivo.
- **Seguridad:** para implementar niveles de seguridad RAID tendremos que disponer de diversas particiones y discos en nuestro sistema
- **Rendimiento:** en discos duros de gran tamaño formateados con FAT ganaremos espacio si hacemos un adecuado número de particiones.

Por otro lado no recomiendo a nadie tener una sola unidad de disco duro en un servidor, es más aconsejable tener dos o tres dispositivos, si sólo tenemos un disco de gran capacidad os animo a crear varias particiones. Tener más de un dispositivo puede ayudarnos en el momento en que uno de ellos decida fallar, perderemos menos información y siempre podremos mover esta a otro disco antes de un desastre total. En sistemas críticos podremos implementar el nivel adecuado de RAID. Por lo que respecta a las visitas indeseadas, el tener varias unidades (físicas o lógicas) dificultará el movimiento del posible intruso, pues una vez que acceda a una unidad podrá moverse por esta con relativa facilidad, sin embargo el salto de una unidad a otra es algo más complicado.

Una vez creadas las particiones y asignados los volúmenes, queda aún un importante trabajo que tocaremos en una próxima sección: decidir el sistema o los sistemas de archivos a utilizar y formatear cada volumen. Para ir abriendo boca diremos que NT sólo maneja dos sistemas de archivos: FAT y NTFS, aunque también entiende HPFS (OS/2) y CDFS (el de los cdroms). Desgraciadamente la versión 4.0 de NT no es capaz aún de leer FAT32, el sistema de archivos usado por Windows 95 en su versión OSR2.

La secuencia de arranque y el Registro

El arranque de NT depende y es controlado por el Registro. Conocer como se produce ese arranque nos puede ayudar a resolver ciertos problemas cuando NT no arranque correctamente. En el proceso de arranque intervienen cuatro elementos fundamentales:

- **NTLDR.** Es el fichero encargado de cargar NT en memoria y controlar el proceso de arranque del sistema operativo. En el caso de las plataformas RISC, la secuencia de arranque está controlada por OSLOADER.EXE.
- **NTDETECT.COM.** Programa encargado de detectar el hardware instalado en el equipo. En las plataformas RISC está función la realiza el proceso POST (Power on Self-Test).
- **NTOSKRNL.EXE.** El núcleo del sistema operativo.

Para las plataformas Intel, el proceso de arranque lo inicia el módulo NTLDR encargado de cargar el sistema operativo. En primer lugar se ejecuta el programa NTDETECT.COM que detectará el hardware del equipo. A partir de ese momento, se transfiere el control al núcleo, el NTOSKRNL.EXE, que será el responsable de culminar el resto de tareas hasta completar el proceso de arranque. Si bien las fases iniciales son diferentes en las plataformas Intel y RISC, sobre todo en cuanto a los responsable o ficheros encargados de realizar cada tarea, después de que el control se transfiere al programa NTOSKRNL.EXE se producen las mismas fases:

Carga del núcleo o kernel. Comienza cuando se transfiere el control a NTOSKRNL.EXE. En primer lugar se carga el componente HAL (Hardware Abstraction Layer) que contiene los aspectos relacionados con el hardware. A continuación se carga el hive file (system) del Registro que contiene los drivers y servicios que se deben iniciar. Esa lista se encuentra dentro de HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ServiceGruopOrder. Esta fase del arranque se produce cuando aparecen puntos (...) en la pantalla. Los drivers se cargan pero no se inicializan. Si se quiere ver los drives que se cargan hay que añadir el parámetro /SOS dentro del BOOT.INI.

multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows NT Server 4.0" /SOS

Inicialización del núcleo. En esta fase, se inicializa el núcleo y los drivers que se instalaron en la fase anterior. Es decir, se ejecutan las rutinas de inicialización del los drivers, que se encargan de inicializar el hardware que controlan. La clave HARDWARE perteneciente a HKEY_LOCAL_MACHINE se rellena con los componentes hardware que detectó el programa NTDETEC.COM. Se salvan el CurrentControlSet y se crea e inicializa el Clone. Si un driver falla en la inicialización, la acción que se realiza depende del valor de ErrorControl que se encuentra en HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DriverName, DriverName representa el nombre del Driver que falló. Los posibles valores son:

- **0x3** Error crítico. El sistema se debe reiniciar con el último LastKnownGood. Si se ha empleado el propio LastKnownGood aparecerá el consiguiente mensaje de error.
- **0x2** Error severo. El sistema se debe reiniciar con el último LastKnownGood. Si se ha empleado el propio LastKnownGood, se ignora el error y se continua con el arranque del sistema

- **0x1** Error normal. La secuencia de arranque muestra el error y continua.
- **0x0** Error ignorado. La secuencia arranque continua sin mostrar ningún mensaje de error.

Fase de carga de servicios. Esta fase se encarga de iniciar el programa Manager de Sesión (SMSS.EXE). Este programa ejecuta todos los programas contenidos en el BootExecute que se encuentra en HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager. Esa entrada del registro es de tipo REG_MULTI_SZ por lo que puede contener varios programas. Entre esos programas que se ejecutan en el inicio es frecuente incluir el AUTOCHK.EXE que es una versión del CHKDSK.EXE adaptada para ejecutarse en el arranque. Ese programa se encarga de chequear nuestro disco y buscar los posibles errores que contenga. Después de ejecutar esos programas, se crean los ficheros necesarios para habilitar la memoria virtual cuya configuración se encuentra en HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management, donde se encuentra, entre otras cosas, la localización, el nombre y el tamaño del fichero que se va a utilizar, generalmente c:\pagefile.sys. Por último, se cargan los subsistemas necesarios y cuya lista está en HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Subsystems.

Inicio del Subsistema Windows. El Manager de Sesión arranca el subsistema Win32. Cuando el subsistema Win32 se inicia se arranca el programa WINLOGON.EXE que muestra la ventana de entrada Ctrl+Alt+Del. También se inicial el programa encargado de autentificar las entradas al sistema de los usuarios, LSSA.EXE (Local Security Authority subsystem). Después de eso, sólo queda iniciar todos aquellos servicios que deban arrancarse automáticamente, como por ejemplos los servicios de Workstation y Server, imprescindibles para que NT funcione a través de la red. La secuencia de arranque se considera exitosa cuando un usuario entra en el sistema. En ese momento, si todo funciona bien, el Clone se copia dentro del LastKnownGood control set.

FAT vs NTFS

NT 4 soporta dos sistemas de archivos: FAT (DOS) y su propio sistema de archivos NTFS (**New Technology File System**). En versiones anteriores se soportaba HPFS (High Performance File System) pero a partir de la versión 4 ya no es posible instalar NT en una partición HPFS. Habrá que formatearla como FAT o NTFS antes de instalar NT.

Una de las tareas del administrador será seleccionar el sistema de archivos más apropiado. Como ya conocemos las características de FAT vamos a estudiar un poco las características de NTFS.

Características de NTFS

- Nombres de ficheros hasta 255 caracteres, permitiéndose espacios y múltiples extensiones.
- Genera automáticamente nombres compatibles MS-DOS.
- No crea cluster grandes aunque las particiones sean grandes. El tamaño del cluster es configurable.
- Permite especificar permisos a nivel de directorios y ficheros. Los ficheros mantienen sus permisos incluso cuando se mueven.
- No se puede acceder a una partición NTFS desde MS-DOS, arrancando desde disquete. Esto aumenta la seguridad de los datos que contiene.
- La fragmentación no es un problema en NTFS. Las particiones NTFS se fragmentan mucho menos que las particiones FAT ya que el sistema siempre busca almacenar los ficheros en bloques contiguos.

En general siempre deben emplearse particiones NTFS en los servidores. Los dos únicos casos en los que se emplean particiones FAT son:

- En los procesadores RISC para el arranque del sistema (basta con una partición de 10Mb, es resto se puede emplear para particiones NTFS).

- También se suele tener una pequeña partición FAT para guardar utilidades hardware o controladores de dispositivos. Si el sistema fallara podríamos acceder a esos datos arrancando desde disquete.

Aunque sólo el S.O. NT tiene acceso directo a los ficheros NTFS. Los usuarios de red podrán acceder a ellos incluso si usan MS-DOS, OS/2, UNIX o cualquier otra versión de Windows (3.x o 95).

En las siguientes tablas se comparan las características principales de los dos sistemas de archivos que podemos emplear, con sus ventajas e inconvenientes.

Característica	**FAT**	**NTFS**
Nombre	8.3	255 caracteres de 16 bits (unicode)
Path Máximo	64	Sin límite
Tamaño del fichero	2^{32}	2^{64}
Partición	2^{32}	2^{64}
Directorios	Sin ordenar	árboles B
Atributo	Unos pocos flags	Toda la información, incluidos los propios datos
Seguridad	Ninguna	SI
Diseño	Simple	Acceso rápido con aspectos de seguridad y recuperabilidad

Tabla 1 Características de FAT y NTFS

Ventajas e inconvenientes

Resumamos antes de finalizar las ventajas y desventajas de cada sistema.

Ventajas	**Desventajas**
Soporta nombres de ficheros largos	NTFS es accesible sólo desde NT. Si tienen instalados distintos SOs en el mismo equipo, las particiones NTFS no serán visibles desde el resto de SOs
	Genera automáticamente nombres cortos compatibles con DOS
	Ficheros transaccionales

Tabla 2 Ventajas y desventajas de NTFS

Ventajas	**Desventajas**
Ficheros pueden ser accedidos desde otros SOs	No tienen implementadas medidas de seguridad para ficheros y directorios
Muy empleado en PCs	No soportan nombres de ficheros largos
	Menos robusto que NTFS

Tabla 3 Ventajas y desventajas de FAT

Convertir particiones FAT en NTFS

Se puede formatear cualquier disco duro como FAT o NTFS, pero se pueden formatear los diskettes como NTFS. Existe una utilidad, CONVERT, que permite convertir una partición NTFS en FAT. No se puede convertir la partición de la unidad que se está empleando. En ese caso, la utilidad CONVERT nos ofrece realizar la conversión la próxima vez que se inicie el sistema.

CONVERT [drive:] /fs:ntfs [/v] [/nametable:filename]

drive especifica la unidad que se va a convertir

/fs:ntfs indica que se va a convertir en ntfs

/v vebose mode, es decir, se indican por pantalla los detalles de la conversión

/nametable:filename se utiliza para traducir nombres de fichero que pueden ser problemáticos

No se puede realizar la conversión contraria, de NTFS a FAT. La forma de hacerlo es hacer un backup, reformatear la partición y recuperar la copia de seguridad. Evidentemente perderemos toda la información de seguridad y permisos que contenía la partición NTFS.

Sistema de Archivos NTFS

Como se ha explicado con anterioridad el sistema de archivos NTFS proporciona muchas ventajas frente a los sistemas FAT. Por ello **es el sistema de archivos que se debe emplear en equipos NT**, sobre todo por los aspectos de seguridad que nos proporciona, como la asignación de permisos a ficheros y directorios.

En NTFS, los ficheros son tratados como objetos que tienen definidos atributos para los usuarios y para el propio sistema. Esos atributos se almacenan en el propio fichero, es decir, la información del sistema de ficheros, como el nombre del archivo, su tamaño, su descriptor de seguridad... , se guarda dentro del propio fichero.

Cada volumen NTFS tiene su **Master File Table** (MTF). La MTF almacena la información necesaria para poder trabajar con los ficheros que contiene el volumen. El primer registro de la MTF se denomina MTF **descriptor record** y sirve para describir la propia MTF. El segundo, llamado **mirror record**, es una copia exacta del primero, y se emplea como redundancia antes posibles fallos en el registro descriptor. La localización de estos dos primeros registros se guarda en el sector de arranque. El tercer registro de la MTF es el **Log File Record**, que se utiliza para recuperar los ficheros del volumen. Después de los 16 primeros registros, se sitúan los registros que describen los ficheros y directorios propiamente.

Nombre del fichero de sistema	Descripción
$	Nombre del fichero índice de la raíz. Es decir, directorio raíz.
$AttrDef	Definición de atributos. Contiene nombres de atributos, número y descriptores
$BadClus	Fichero con los clusters defectuosos.
$Bitmap	Mapa de clusters. Lista de clusters que se pueden usar en el volumen
$Boot	Fichero de arranque. Contiene el programa de arranque para las particiones desde las que se puede arrancar
$LogFile	Fichero de transacciones, empleado para la recuperación de errores.
$MTF	La Master File Table que lista los contenidos del volumen
$MTFMirr	Mirror de la MTF, para propósitos de redundancia
$Volume	Contiene la información relacionada con el volumen y la versión

Tabla 4 Ficheros del Sistema

Si un fichero o directorio es lo bastante pequeño (menos de 1500 bytes) se guarda directamente en la MTF. Si el fichero es más largo, se guarda el principio en el registro correspondiente de la MTF y el resto en extensiones de datos enlazadas con ese primer registro del fichero. Las extensiones son clusters externos del propio volumen y que se enlazan entre sí mediante punteros.

Del funcionamiento descrito se deduce que el acceso a los ficheros pequeños es rápido ya que sólo hay que hacer una búsqueda en la MTF. Los directorios se representan de una manera similar, excepto porque contienen índices para localizar los ficheros que contienen. Como pasa con los ficheros, si el directorio es lo bastante pequeño se guarda enteramente

en la MFT. Si es demasiado grande se emplean extensiones organizadas como árboles B. Toda la información que contiene el fichero, incluidos los propios datos, reciben el nombre de atributos. Cuando los atributos de un fichero o un directorio están enteramente en la MTF se dicen que son atributos residentes. Si mantienen en extensiones se dice que son no residentes.

NTFS usa ficheros especiales que están ocultos y que guardan los metadatos del propio volumen. Se crean cuando el volumen se formatea (véase Tabla 4).

Espacio de nombres

Todos los ficheros NTFS consideran toda la información como si de atributos se trataran y se denomina así. Los principales atributos de NTFS son:

- **Información estándar.** Atributos del fichero en sentido clásico (solo lectura, archivo, del sistema, oculto...); fecha y hora de la última modificación y número de links (número de entradas en directorios que apunta al fichero).
- **Lista de atributos.** Lista de atributos que componen el fichero; la referencia de la MTF donde el fichero está guardado. Este atributo se emplea cuando el fichero necesita más de un registro de la MFT.
- **Nombre del fichero.** Nombre del archivo empleando caracteres unicode. Pueden contener cualquier carácter excepto wild-card (? y *), delimitadores (\,/,:, y ;) y símbolos de redirección o tuberías (<, > y |). Se pueden usar varios . y espacios.
- **Descriptor de seguridad.** El propietario/creador del fichero y la lista de control de acceso (ACL) que define quién puede acceder al fichero y cómo puede hacerlo.
- **Datos.** El contenido propiamente dicho del fichero. Un fichero puede contener múltiples atributos de datos o streams.

Los ficheros NTFS pueden tener 255 caracteres y pueden ocupar 16 exabytes, es decir, se emplean offsets de 64 bits.

Ficheros como objetos

Internamente NT trata todos los recursos del sistema como objetos, incluidos los ficheros. La creación y manipulación de cualquier objeto tiene que contar con la aprobación del Security Reference Monitor. Este módulo del kernel es el encargado de comprobar que el usuario puede realizar una cierta acción. Si por ejemplo, un usuario quisiera crear un fichero en un directorio, el SRM cotejaría el **Security Access Token** (SAT) del usuario con la lista de control de acceso del directorio (ACL). El SAT contiene el SID del usuario y los SIDs de todos los grupos de los que ese usuario es miembro. El SRM comprueba la ACL y mira si alguno de los SIDs de la SAT tienen permiso para crear un archivo en el directorio. El SRM es, por tanto, el punto central donde se implementa la seguridad sobre los objetos del sistema.

Conversión a nombres DOS

Para soportar el acceso desde DOS, los nombres largos NTFS se convierten al formato tradicional 8.3. Cada vez que se asigna a un fichero un nombre largo (LFN Long File Name) se crea automáticamente el nombre corto correspondiente (SFN Short File Name). Las reglas para esa conversión son las siguientes (emplearemos para el ejemplo ESTE ES UN NOMBRE.[LARGO].DE FICHERO.DATA):

1. Se borran los espacios en blanco.

   ESTEESUNNOMBRE.[LARGO].DEFICHERO.DATA

2. Los caracteres no válidos en DOS se sustituyen por subrayado.

   ESTEESUNNOMBRE._LARGO_.DEFICHERO.DATA

3. Se borran todos los puntos excepto el último.

   ESTEESUNNOMBRE_LARGO_DEFICHERO.DATA

4. Se trunca el nombre a partir del sexto carácter y se añade ~n donde n es el número de nombres de ficheros dentro del directorio que coinciden en esas primeras seis letras.

ESTEES~1.DATA

5. Se trunca la extensión del fichero a tres letras.

   ESTEES~1.DAT

Distinción entre mayúsculas y minúsculas

Dado que NT soporta POSIX y este sistema necesita que los nombres de ficheros distingan entre mayúsculas, NTFS es un sistema de archivos case-sensitive, es decir, en NTFS se pueden crear varios ficheros con el mismo nombre y que sólo se diferencien en letras mayúsculas y minúsculas. Por ejemplo: Fichero1.txt, ficHero1.txt y fichero1.txt son tres ficheros distintos. Sin embargo los subsistemas DOS, WIN16, OS/2 Y WIN32 no distinguen entre mayúsculas y minúsculas, es decir que nos encontraremos con problemas en un ejemplo como el anterior.

Links simbólicos y letras de unidad

NT usa letras de unidad para referirse a discos duros y particiones. Esos objetos se implementan mediante lo que se denominan enlaces simbólicos. Por ejemplo la letra C: suele ser un enlace simbólico a \Device\HardDisk0. Es decir, que cuando nosotros queramos abrir el fichero C:\temp\prueba.txt el sistema remplazará la letra de unidad por su verdadero nombre: \Device\HardDisk0\temp\prueba.txt.

Implementación de seguridad en sistemas de archivos NTFS

Cuando se comparte un directorio en NT, se asignan excesivos permisos para acceder a ese recurso. Cualquiera puede acceder a ese directorio a través de la red ya que tiene acceso total (Control Total al grupo Todos). Aunque este funcionamiento simplifica el compartir recursos en redes igual a igual, ya que no se precisa ningún conocimiento para compartir un recurso, supone un agujero de seguridad en cualquier red donde ese aspecto sea importante. Para implementar un sistema de seguridad apropiado, es necesario limitar el acceso a los recursos compartidos, otorgando los permisos adecuados a los usuarios que lo necesiten.

Estructuras de datos para implementar permisos en ficheros

Como se ha indicado anteriormente, cualquier recurso se representa en NT como objetos. Y todo recurso u objeto en NT, como son los ficheros, tienen un propietario. El propietario es un usuario o grupo que tiene un control completo sobre el recurso, esto es, pueden decidir los usuarios que pueden acceder al recurso y las operaciones que pueden realizar. En principio el propietario de un objeto es el creador del mismo, aunque durante la vida del objeto puede ocurrir que otro usuario se convierta en propietario del recurso, aunque para que eso suceda debe tener un permiso que le habilite para hacerlo (O).

La seguridad de un fichero, o de un objeto, está implementado en una estructura llamada **Descriptor de Seguridad** (SD). Dentro de esa estructura, el propietario y los usuarios y grupos que tienen acceso al directorio compartido se identifican por su SIDs (Security Identifier) y las operaciones que pueden realizar están reflejadas en la lista de control de acceso (ACL), también conocida como lista de permisos y que forma parte del SD. Los elementos que componen el Descriptor de Seguridad son los siguientes:

SID del propietario. El propietario del objeto puede ser un usuario o un grupo. El propietario puede obtener un control total sobre el recurso y asignar los permisos que desee.

SID del grupo primario del propietario. El grupo primario del propietario se asigna a través de la definición de la cuenta del propietario. No tiene utilidad en NT, salvo para la implementación de POSIX.

Discretionary ACL. Identifica los SIDs de los usuarios que tiene acceso al objeto y el tipo de acceso que tienen.

System ACL. Indica las operaciones que el sistema va a auditar.

Security Descriptor de Prueba.txt en el Directorio: c:\temp

SID Propietario: Pepe (S-1-.....)

SID Grupo primario Propietario: Alumnos ASO ....

DACL: Deny (All) Juan

Grant (RW) Maria

Grant (R) Ana

SACL: Audit: (R) Everyone

Dentro de las dos listas de control de acceso (DACL y SACL) se otorgan tres tipos de entradas:

- **Permitir acceso** (Grant). Permite representar los permisos que se otorgan explícitamente a los usuarios y grupos. (DACL)
- **Denegar acceso** (Deny). Se indican los permisos que se deniegan explícitamente a los usuarios y grupos. (DACL)
- **Auditar (Audit).** Esta entrada la usa el Sistema de Seguridad para auditar los eventos de seguridad en función de los accesos que realicen los usuarios.

La DACL se implementa mediante punteros y existe una gran diferencia según esté vacía o esté directamente sin asignar. Si está vacía quiere decir que ningún usuario tiene acceso al recurso. Si está sin asignar, indica que el objeto no tiene ninguna protección, por lo que cualquier usuario tendrá acceso.

Permisos

La seguridad de un sistema de archivos NTFS se implementa mediante **permisos**. Los permisos se establecen a través del Explorador de NT y existen dos tipos de permisos: especiales y estándar, aunque en realidad los segundos son combinación de los primeros.

Permisos especiales

Los permisos especiales, también llamados individuales, se emplean cuando los permisos estándar no se adaptan a nuestras necesidades. Son seis:

R. Leer. Si se aplica a un fichero, indica que se puede ver el propietario y los permisos sobre el fichero, ver su contenido, sus atributos y permite cambiar los datos del fichero y añadir datos al mismo. Si se aplica a un directorio, indica que se puede ver el propietario y los permisos, ver los ficheros que contiene el directorio y mostrar los atributos del mismo.

W. Escribir. Si se aplica a un fichero, indica que se puede ver el propietario y los permisos sobre el fichero, cambiar sus atributos y permite cambiar los datos del fichero y añadir datos al mismo. Si se aplica a un directorio, indica que se puede ver el propietario y los permisos, añadir ficheros y subdirectorios y cambiar los atributos del directorio.

X. Ejecutar. Si se aplica a un fichero, indica que se puede ver el propietario y los permisos sobre el fichero, ver sus atributos y permite ejecutar el fichero si es un ejecutable. Si se aplica a un directorio, indica que se puede ver el propietario y los permisos, ver los atributos del directorio y cambiar a un subdirectorio.

D. Borrar. Tanto si se aplica a un fichero o un directorio, indica que se puede borrar el objeto.

P. Cambiar permisos. Permite cambiar los permisos sobre el fichero o el directorio.

O. Tomar posesión. Si se asigna este permiso a un usuario o grupo, ese usuario o grupo puede convertirse en propietario del objeto.

Permisos estándar

Aunque es posible emplear permisos especiales para controlar el acceso a ficheros y directorios, es más sencillo utilizar los permisos estándar. Los permisos estándar son combinaciones predefinidas de los permisos especiales y se suelen utilizar ya que estas combinaciones son las que suelen emplear normalmente cuando queremos asignar permisos. Es decir, son las combinaciones más habituales, aunque siempre es posible que no cubran todas las necesidades.

Los permisos estándar son distintos según se aplican a ficheros o directorios. Para ficheros, los permisos estándar son:

- **Sin Acceso ().** Los usuarios no tiene ningún acceso al fichero, incluso si el usuario es miembro de un grupo que si tenga algún permiso.
- **Lectura (RX).** Los usuarios pueden leer y ejecutar los ficheros.
- **Cambio (RWXD).** Los usuarios pueden leer, modificar, ejecutar y borrar el fichero.
- **Control Total (RWXDPO).** Todos los permisos, incluidos cambiar permisos y tomar posesión de un archivo.

Para los directorios, los permisos estándar no sólo incluyen las acciones que se pueden realizar sobre el propio directorio, sino también sobre los ficheros contenidos en él. El formato que representaremos para estos dos permisos será el siguiente:

(permisos del directorio) (permisos heredados por los ficheros del directorio)

Los permisos estándar definidos para los directorios son los siguientes:

- **Sin Acceso () ().** Los usuarios no tienen acceso ni al directorio ni a los ficheros contenidos en él. Esa restricción se mantiene aunque el usuario pertenezca a un grupo que tenga algún tipo de acceso sobre el directorio o los ficheros.
- **Listado (RX) ().** Los usuarios pueden listar el contenido del directorio y cambiar a uno de sus subdirectorios. Por contra, no pueden realizar ninguna operación sobre los ficheros.
- **Lectura (RX) (RX).** Los usuarios pueden listar el contenido del directorio y cambiar a uno de sus subdirectorios, además pueden ver el contenido de sus ficheros y ejecutar las aplicaciones que contenga.
- **Agregar (WX) (Sin especificar).** El usuario podrá añadir ficheros al directorio, y cambiar de directorio. Sobre los ficheros del directorio no se especifica el tipo de acceso permitido, es decir, mantiene los que tengan asignados individualmente.
- **Agregar y Leer (RWX) (RX).** El usuario puede ver el contenido del directorio, añadir nuevos ficheros y cambiar de directorios. Sobre los ficheros puede leerlos y ejecutar aquellos ejecutables.
- **Cambio (RWXD) (RWXD).** Los usuarios podrán ver el contenido del directorio, borrarlo, añadir ficheros y cambiar a un subdirectorio. Además sobre los ficheros pueden leerlos, modificarlos, ejecutarlos y borrarlos.
- **Control Total (RWXDPO) (RWXDPO).** Se tiene un control absoluto, es decir, se pueden realizar todas las operaciones posibles tanto sobre los ficheros como sobre el directorio.

Como se ve, los permisos que se aplican a un directorio afectan tanto al directorio como a los ficheros en él contenidos. Además, los nuevos ficheros que se crean en el directorio, heredan los permisos asignados a los ficheros del directorio en función del permiso estándar del directorio.

Trabajando con los permisos de ficheros

Cuando se asignan los permisos sobre los directorios y ficheros de nuestro sistema hay que tener en cuenta las siguientes consideraciones:

- Para impedir que un usuario acceda a un fichero o un directorio, no es necesario darle el permiso Sin Acceso. Es decir, no hay que asignar el permiso Sin Acceso a todos aquellos

usuarios que no deseemos que accedan al fichero o directorio; si no se da ningún permiso a un usuario o grupo se entiende que tiene el permiso Sin Acceso.

- Los permisos son acumulativos. Esto significa que si un usuario tiene permisos propios y de alguno de sus grupos, los permisos definitivos que tendrán será la combinación de todos ellos. La única excepción es el permiso Sin Acceso ya que este permiso elimina todos los anteriores.

  Sin Acceso + Cambio = Sin Acceso

- El permiso Sin Acceso se emplea precisamente para establecer excepciones sobre un miembro de un determinado grupo. Si por ejemplo queremos dar permiso Cambiar a un grupo de usuario pero queremos negárselo a uno de sus miembros, solamente tendremos que dar permiso Cambiar al grupo y darle a ese usuario el permiso Sin Acceso.
- Por defecto, los nuevos ficheros o subdirectorios heredan los permisos del directorio en el que se crean.

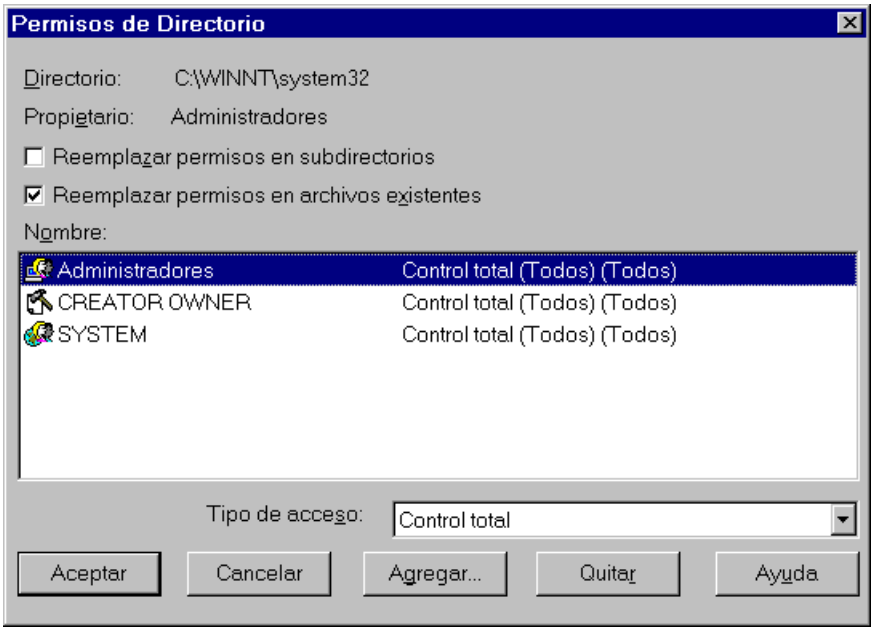

Figura 1 Permisos del directorio Winnt\System32

Asignación de permisos

Los permisos se asignan mediante el Explorador de NT, con el botón derecho del ratón se ejecuta el comando *Propiedades* y dentro de las propiedades se escoge la pestaña *Seguridad* y se hace click en el botón *Permisos*. En la Figura 1 se pueden ver los permisos que podría tener un directorio llamado Winnt. Como se puede apreciar, tiene asignado el permiso Control Total para el grupo Todos.

Supongamos que queremos cambiar los permisos de ese directorio para permitir el acceso de un nuevo usuario. Para ello deberemos pulsar el botón *Agregar*. Nos aparecerá la ventana *Agregar usuarios y grupos* (Figura 2) donde tendremos que seleccionar el usuario que vamos a añadir y el tipo de acceso que le vamos a otorgar. Por defecto la ventana muestra los grupos de nuestro dominio. Si queremos asignar permisos a un usuario concreto, tendremos que hacer que nos los muestre con el botón *Mostrar Usuarios*. En el ejemplo de la figura se ha seleccionado el usuario de nombre 10865934. Como se puede en el cuadro *Agregar Nombres*, delante del nombre se antepone el del dominio. Esto es debido a que podemos elegir usuarios y grupos de dominios en los que confiemos (lista *Mostrar Nombres en*) y podría ocurrir que existieran dos cuentas con el mismo nombre en dominios distintos. En la parte inferior podremos elegir el tipo de acceso que el usuario va a tener. En el ejemplo se le otorga el permiso Agregar y Leer. Una vez asignado y tras pulsar el botón Aceptar volveríamos a la ventana de la Figura 1.

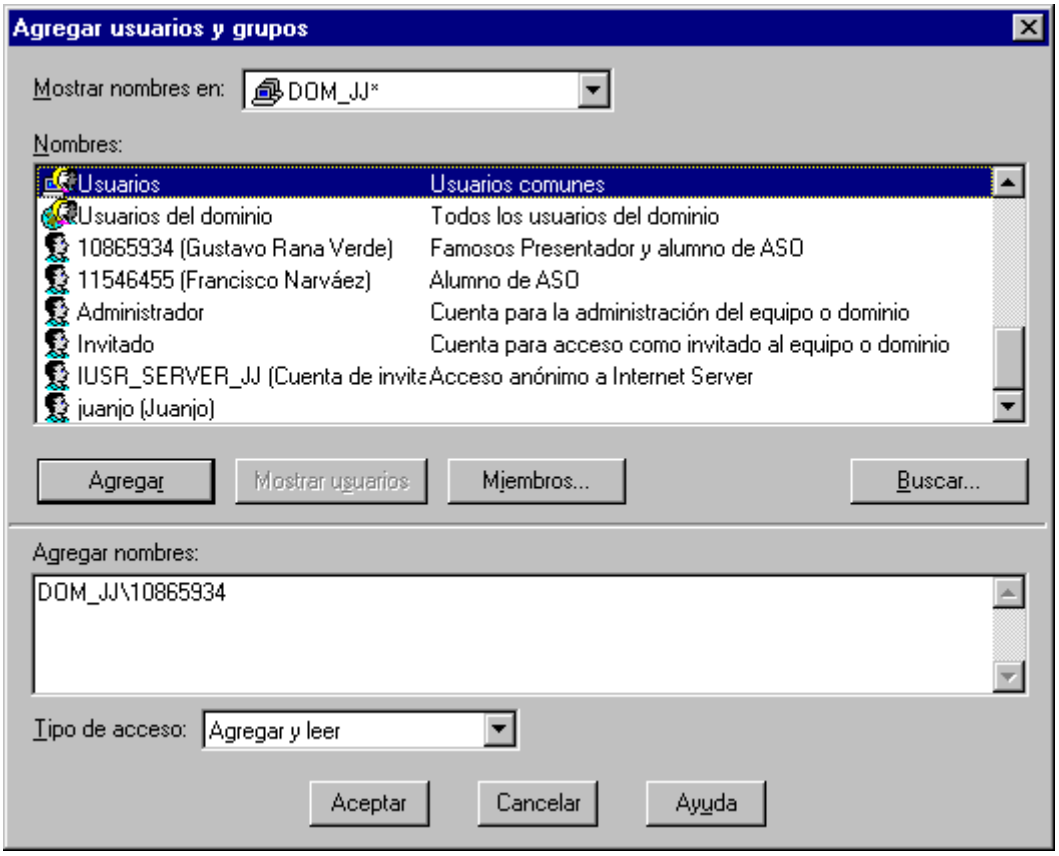

Figura 2 Agregar usuarios y grupos

Siempre que se cambia los permisos de un directorio, como es el caso, el Explorador nos permite seleccionar entre dos opciones (véase Figura 1):

- Reemplazar los permisos de sus subdirectorios
- Reemplazar los permisos de sus ficheros

Estas opciones sirven para cambiar los permisos de los ficheros y subdirectorios que cuelgan del directorio en el que hemos cambiado los permisos. Lo normal es reemplazar sólo los permisos de sus ficheros y mantener los de los subdirectorios (opción por defecto, véase Figura 1). Por ejemplo, si sobre un directorio le damos Control Total al usuario Pepe y decidimos que eso se extienda a los ficheros del directorio, eso implicará que tendrá Control Total sobre todos los ficheros del directorio. S

C:\Apps	*Juan Cambio*
C:\Apps\Subdirectorio	*María Lectura*
C:\Apps\Fichero viejo	*Pepe Cambio*

Si sobre el directorio C:\Apps damos Control Total a Ana y queremos que se extienda a los ficheros del propio directorio, el esquema de permisos que tendremos será:

C:\Apps	*Juan Cambio*
	Ana Control Total
C:\Apps\Subdirectorio	*María Lectura*
C:\Apps\Fichero viejo	*Pepe Cambio*
	Ana Control Total

El usuario que crea un fichero o un directorio se convierte en su propietario. El propietario puede controlar el acceso sobre el fichero o directorio y decidir qué usuarios y de qué forma podrán acceder a él.

Asignación de permisos con CACLS

Ocasionalmente también se puede emplear el comando en línea CACLS (Change ACLs) para dar y quitar permisos.

CACLS fichero [/G:user:perm] [/R user ...] [/P user:perm ...] [/D user ...]

fichero nombre del fichero al que se van a asignar permisos. Si se indica sólo el nombre del fichero, se muestra la ACL del mismo.

/G user:perm asigna los permisos al usuario. perm puede ser R (Lectura), C (Cambio) o F (Control Total)

/R user revoca los permisos que tenga ese usuario

/P user:perm reemplaza los permisos del usuario. perm puede ser R (Lectura), C (Cambio), F (Control Total) o N (Sin Acceso)

/D user deniega el acceso (como N)

Se pueden asignar permisos a los siguientes usuarios o grupos:

- Usuarios del dominios
- Usuarios de dominios en los que se confía
- Grupos locales del dominio
- Grupos globales del dominio
- Grupos globales de dominios en los que se confía
- Grupos especiales: Red, Interactivo, Sistema[1], Todos y Creador/Propietario

Cuando se asignan permisos al grupo Creador/Propietario en un directorio hay que tener en cuenta que esos permisos los heredarán los ficheros y subdirectorios que se creen en él, de forma que el creador de un nuevo fichero tendrá los permisos que se den al grupo Creador/Propietario.

C:\Apps

Creador/Propietario Cambio (RWXD) (RWXD)

Todos Lectura (RX) (RX)

Si Juan crea el fichero Texto1.Doc los permisos que tendrá el fichero serán

Juan Cambio (RWXD)

Todos Lectura (RX)

Si Pepe crea el fichero Texto2.Doc los permisos que tendrá el fichero serán

Pepe Cambio (RWXD)

Todos Lectura (RX)

Lo normal es que se asignen permisos a los grupos locales. Debe considerarse como excepcional el hecho de darle permisos a un usuario concreto. Los permisos que se suelen asignar son los permisos estándar. Es bastante raro que ninguno de ellos se ajuste a lo que necesitamos. Si fuera así, podemos componer el grupo de permisos que deseemos empleando los permisos especiales individuales. En el caso de los permisos para los ficheros, además de poder asignar los seis permisos especiales (R, W, X, D, P, O), se puede indicar que no asignan permisos específicos. Esa opción hace que el fichero indicado no herede los permisos que le otorga el directorio en el que se encuentra.

Cuando se crea un nuevo directorio, por defecto se le da al grupo Todos el permiso Cambiar (RWXD) (RWXD). Este permiso puede ser excesivo en determinadas ocasiones. Por defecto se da control total al Creador/Propietario.

---

[1] El grupo especial Sistema representa al propio Sistema Operativo. En la instalación, se asignan permisos a ese grupo sobre ciertos directorios. Por norma, no es necesario asignar permisos a este grupo sobre otros directorios, y hay que evitar eliminar los permisos que tiene por defecto ya que puede ocasionar que alguno de los servicios deje de funcionar.

Permisos de los ficheros copiados o movidos

Cuando se copia un fichero, el fichero destino hereda los permisos del directorio en el que se crea. Esto es así, ya que al copiar un fichero, lo que se está haciendo es crear un fichero en un determinado directorio y como siempre que se crea un nuevo fichero, éste hereda los permisos que tenga asignado el directorio en el que se crea. El usuario que copia el fichero se convierte en su propietario. Si se trata de un miembro del grupo Administradores, el propietario será todo el grupo.

Si en cambio lo que se hace es mover un fichero de un directorio a otro, el fichero mantiene los permisos originales. Para moverlo precisamos el permiso necesario para crear ficheros en el directorio destino y el permiso para borrar ficheros en el directorio origen.

Tomar posesión

El permiso de tomar posesión (P) sobre un objeto da al usuario que lo tiene la capacidad de cambiar los permisos de ese objeto. El propietario de un fichero o un directorio tiene la capacidad para cambiar sus permisos. Cuando un usuario toma posesión de un objeto adquiere automáticamente esa capacidad.

El Administrador puede tomar posesión de cualquier fichero o directorio. La posesión siempre se obtiene mediante una operación explícita. Es decir, no se puede transferir la posesión a un tercero, solamente puedes tomar la posesión para ti mismo. Para poder tomar posesión de un objeto se debe cumplir una de estas tres circunstancias:

- Tener Control Total
- Tener el permiso especial Tomar Posesión (P)
- Ser miembro del grupo Administradores

El acto de tomar posesión puede (y en muchas ocasiones, debe) ser auditado incluso para el Administrador. Esta situación garantiza a los usuarios que el Administrador no abuse de sus privilegios.

Cuando se toma posesión de un objeto en un dominio puedes tardar un tiempo hasta que ese cambio de posesión te permita cambiar los permisos de ese objeto. Eso se debe a que no se ha producido aún la sincronización de los controladores del dominio. En ese caso, puede ser necesario realizar una sincronización manual.

Para tomar posesión de un directorio se emplea el Explorador de NT, con el botón derecho del ratón se ejecuta el comando *Propiedades* y dentro de las propiedades se escoge la pestaña *Seguridad* y se hace click en el botón *Propietario*. En la Figura 3 se pueden ver la ventana que nos aparece. En este caso simplemente hay que pulsar el botón *Toma de posesión*. En ese momento, el usuario que lo realice será el propietario del objeto y podrá asignar y quitar permisos.

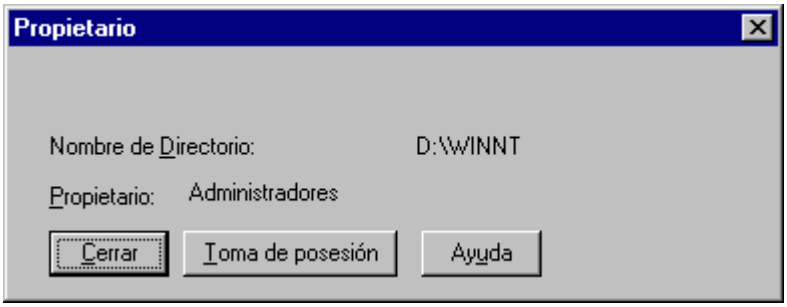

Figura 3 Tomar posesión

Atributos de los ficheros

NT soporta los siguientes atributos DOS para ficheros y directorios:

- **Oculto.** El fichero no es visible cuando se hace un listado normal (dir).
- **Del sistema.** Los ficheros propios del sistema operativo se marcan con este flag.

- **Archivo.** Ficheros que se han modificado desde el último backup. De está forma las utilidades para hacer copias de seguridad saben los ficheros que tienen que guardar.
- **Solo lectura.** Estos ficheros no pueden ser modificados ni borrados.

Además de estos atributos existe uno más que indica si el fichero está comprimido o no. Si asignamos el atributo de comprimido a un directorio, NT nos preguntará si deseamos comprimir los archivos que contiene. Los nuevos ficheros que añadamos a ese directorio serán comprimidos. NT, automáticamente y de forma transparente para el usuario, realizará la comprensión y descompresión de los ficheros.

File Delete Child

El permiso estándar Control Total incluye un permiso adicional. Ese permiso permite que los usuarios que tienen Control Total puedan borrar ficheros independientemente de los atributos de los mismos. Este permiso especial se llama File Delete Child (FDC). El File Delete Child está creado para mantener la compatibilidad POSIX en el que se basan los sistemas Unix. En Unix, un directorio o un fichero pueden tener tres permisos: lectura (r), escritura (w) y ejecución (x). Existen tres grupos de esos tres permisos por cada fichero: uno para el propietario, otro para el grupo primario y otro para el resto de usuarios. El Unix, el permiso w permite borrar ficheros de un directorio.

En el caso de NT, el File Delete Child se emplea para implementar el permiso w de Unix. En NT, el permiso W no permite borrar ficheros y no incluye el File Delete Child. En cambio el permiso estándar Control Total si lo incluye.

Compartir directorios

Lo normal, cuando trabajamos en una red de ordenadores, es que los usuarios compartan sus datos. Para hacerlo simplemente tienen que indicar aquellos directorios que quieres compartir y cómo quieres compartilos. Veamos como se realizan estas dos cosas.

Nombres para compartir

A cualquier recurso que pretendamos compartir en NT hay que darle un nombre que será el nombre con el que se conocerá a ese recurso (**share name**). El nombre para compartir puede tener hasta 12 caracteres. Por ejemplo, el nombre con el que se comparte el recurso %SYSTEMROOT%\system32\Repl\Import\Scripts es **NETLOGON**. Los recursos compartidos por una estación NT pueden ser accedidos simultáneamente por 10 usuarios. Para los servidores NT, el límite máximo viene dado por el número de licencias disponibles.

Se puede hacer que un mismo recurso esté compartido con distintos nombres. Esta particularidad puede ser útil si queremos dar un conjunto de permisos distintos a diferentes grupos de usuarios (aunque lo mismo se puede hacer con un solo nombre). Lo que si hay que cumplir siempre es que no se emplee dos veces el mismo nombre para compartir recursos de un mismo equipo. Dos equipos pueden usar el mismo nombre para un recurso compartido, ya que a ese nombre siempre se añade el nombre del equipo. Por ejemplo, si en la Estacion1 y la Estacion2 creamos un recurso compartido que se llame APPS, el nombre final de esos dos recursos compartidos será: \\Estacion1\APPS y \\Estacion2\APPS, que obviamente son distintos.

Uniform Naming Convention

Como se puede observar los nombres completos de los recursos compartidos siguen la **Uniform Naming Convention** (UNC). Esta norma permite fijar los nombres de los equipos y de los recursos dentro de ellos. Empieza por un delimitador \\ que indica que comienza un nombre UNC. Después viene el nombre de la máquina, seguido del nombre del recurso compartido y, por último, y opcionalmente el nombre de los subdirectorio (siempre que sea una carpeta compartida). Los elementos se separan entre sí mediante el separador \.

*computer_name**share_name[**subdirectorios]*

¿Cómo se comparte un directorio?

Para compartir (y dejar de compartir) un directorio podemos hacerlo de dos formas: mediante el Explorador de NT de forma gráfica o mediante el comando NET SHARE. Para compartir un directorio desde el Explorador simplemente hay que seleccionarlo y con el botón derecho del ratón seleccionar la opción *Compartir*. Las opciones que se pueden configurar son las siguientes (las mismas que con el comando NET SHARE):

- **Nombre del recurso compartido.** Una vez que se asigna el nombre al recurso compartido no se puede cambiar. Para cambiarlo hay que dejar de compartir el recurso y volver a compartirlo con el nuevo nombre. Los nombres que terminan con $ son recurso empleados por el Administrador y no aparecen cuando se ven los elementos compartidos del equipo a través del Entorno de Red.
- **Comentario.** Texto descriptivo sobre el recurso.
- **Límite de usuarios.** Número máximo de usuarios que pueden acceder simultáneamente al recurso compartido. Se puede escoger entre el máximo permitido por el propio sistema (10 en estaciones y el número de licencias en servidores) o fijar uno nosotros mismos.
- **Permisos.** Sirve para fijar los permisos con los que vamos a compartir el recurso.

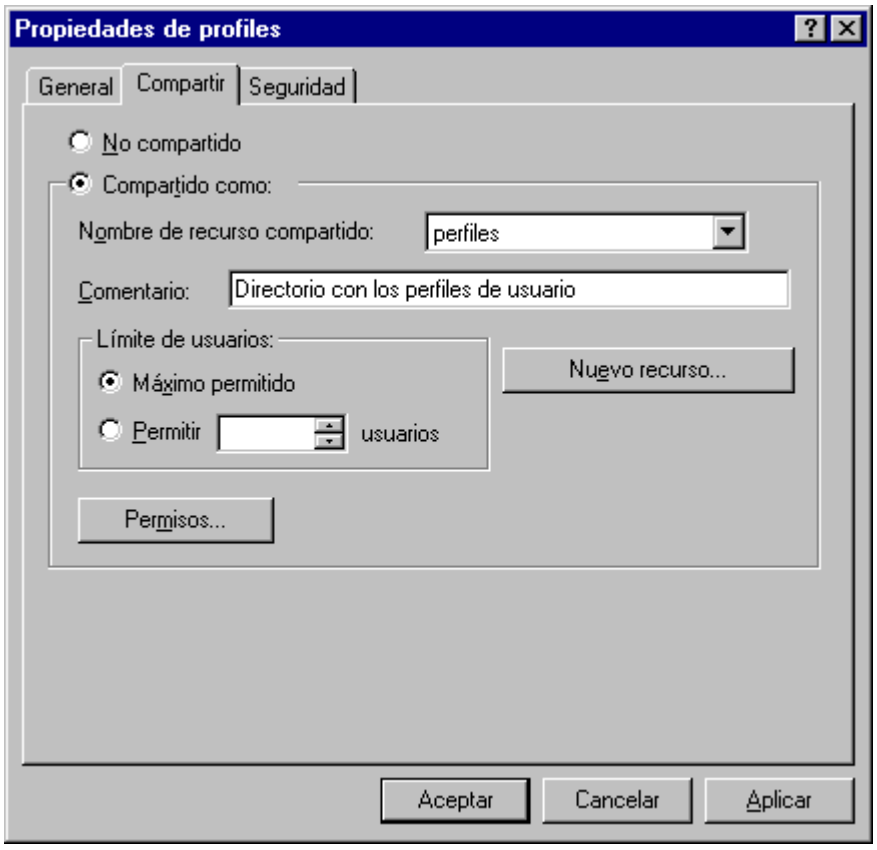

Figura 4 Compartir el directorio profiles

Para dejar de compartir el recurso desde el Explorador hay que escoger con el botón derecho del ratón de nuevo el comando C*ompartir* y marcar el recurso como *No Compartido*.

En la ventana de la Figura 4 está el ejemplo de cómo se comparte un directorio de nombre *profiles*. Como se ve, el recurso compartido se llama perfiles y se le asignado como límite de usuarios el máximo permitido. Para fijar los permisos con los que se comparte el directorio se utiliza el botón *Permisos*. Nos saldrá la misma ventana que cuando fijamos los permisos locales (Figura 5). Por defecto se comparten con Control Total para el grupo Todos. Si deseamos cambiar esa configuración tendremos que emplear el botón *Agregar* y asignar/desasignar los permisos oportunos.

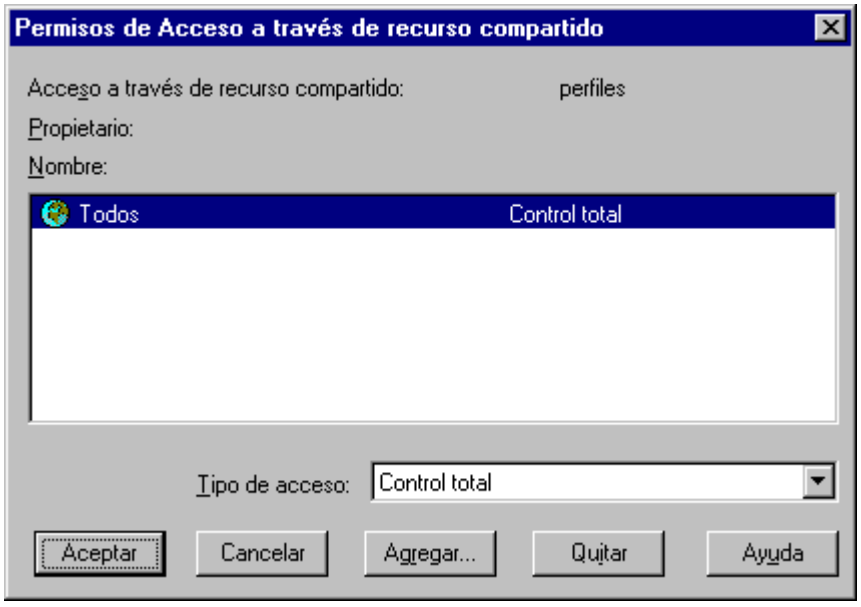

Figura 5 Permisos para compartir

Compartir con NET SHARE

También se puede compartir un directorio con el comando NET SHARE. Su sintaxis es:

NET SHARE sharename

sharename=drive:path [/USERS:number | /UNLIMITED] [/REMARK:text]

{sharename | devicename | drive:path} /DELETE

donde

sharename Nombre del recurso compartido

drive:path especifica el path absoluto donde está el recurso compartido

/USERS:number Número máximo de usuarios que pueden acceder simultáneamente al recurso compartido

/UNLIMITED indica que pueden acceder simultáneamente al recurso todos los usuarios que deseen

/REMARK:text descripción del recurso compartido

devicename nombre del dispositivo, generalmente un puerto (pe. LPT1)

/DELETE para dejar de compartir el recurso

NET SHARE APPS=C:\APLICACIONES

NET SHARE APPS \DELETE

NET SHARE

La primera instrucción comparte el directorio C:\APLICACIONES con el nombre APPS, la segunda deja de compartir ese mismo recurso y la última nos muestra por pantalla una lista con los recursos compartidos.

Ver y mapear recursos compartidos

Para ver los recursos compartidos tenemos también dos opciones. La primera con el comando NET VIEW.

NET VIEW [\\computername | DOMAIN[:domainname]]

computername. Nombre del equipo del que queremos ver los recursos compartidos.

/DOMAIN:domainname. Se emplea para ver los equipos que forman parte de un dominio. Si se omite el nombre del dominio, nos muestra los nombres de los dominios que hay en nuestra red local.

La otra forma de ver los recursos compartidos es a través del Entorno de Red. Simplemente tendremos que elegir el equipo del que queremos ver sus recursos y hacer doble click.

Para mapear un recurso compartido a un directorio se puede emplear el comando NET USE (véase la sección Login Scripts) o utilizar el Explorador y uno de los comandos que proporciona a través de la barra de herramientas. Las mismas dos opciones tenemos si queremos desconectar una unidad de red.

Permisos sobre directorios compartidos

Como se ha explicado en los apartados anteriores, sobre los ficheros y directorios de particiones NTFS podemos asignar permisos que limiten el tipo de acceso que los usuarios de nuestro sistema pueden realizar sobre nuestros ficheros y directorios. Pero además de fijar ese tipo de permisos, también se pueden fijar los permisos con los que vamos a compartir ciertos directorios.

Hasta que un directorio no se comparte, **nadie podrá acceder a él a través de la red**. Obviamente siempre se puede acceder a un fichero o directorio localmente, siempre y cuando tengamos permiso para ello. Pero si queremos que los usuarios accedan a un directorio y sus ficheros a través de la red es necesario compartirlo. Al compartir un directorio se le asignan tres cosas:

- Primero e imprescindible, el nombre con el que se va a compartir. Este nombre no tiene porque coincidir con el nombre del directorio y será el nombre que los usuarios verán a través del Entorno de Red y el que necesitarán conocer para conectarse al recurso.
- Segundo, al compartir un directorio también se asignan los permisos con los que se va a compartir.
- Tercero, el número de usuarios que podrán acceder simultáneamente al directorio.

Podemos compartir un directorio con dos nombres distintos. Esto hace que existan dos recursos compartidos, aunque en el fondo apunten al mismo directorio. Esto se suele hacer cuando se quieren dar distintos tipos de accesos a dos grupos de usuarios.

Podemos compartir directorios tanto de particiones NTFS como FAT. Por tanto, **compartir un directorio FAT es la única forma de asignarle permisos, permisos que sólo funcionarán a través de la red, no localmente**. En NTFS tendremos dos niveles de permisos: los que se fijan a la hora de compartir el directorio y los que se tengan asignados en la propia partición NTFS. Los primeros sólo entrarán en funcionamiento cuando se acceda al directorio a través de la red y los segundos tanto en accesos a través de la red, como en los accesos locales. En particiones FAT sólo hay un nivel de permisos, los permisos con los que se comparte y que sólo influyen para accesos a través de la red, localmente todos los usuarios tendrán acceso total.

Permisos para Compartir

Los permisos con los que se pueden compartir un directorio son los mismos que se pueden establecer localmente. Es decir, podemos asignar los siguientes permisos:

- **Sin Acceso () ().** Los usuarios no tienen acceso ni al directorio ni a los ficheros contenidos en él. Esa restricción se mantiene aunque el usuario pertenezca a un grupo que tenga algún tipo de acceso sobre el directorio o los ficheros.
- **Lectura (RX) (RX).** Los usuarios pueden listar el contenido del directorio y cambiar a uno de sus subdirectorios, además pueden ver el contenido de sus ficheros y ejecutar las aplicaciones que contenga.
- **Cambio (RWXD) (RWXD).** Los usuarios podrán ver el contenido del directorio, borrarlo, añadir ficheros y cambiar a un subdirectorio. Además sobre los ficheros pueden leerlos, modificarlos, ejecutarlos y borrarlos.
- **Control Total (RWXDPO) (RWXDPO).** Se tiene un control absoluto, es decir, se pueden realizar todas las operaciones posibles tanto sobre los ficheros como sobre el directorio.

Los permisos con los que se comparten operan en conjunción con los permisos propios NTFS. Los permisos efectivos serán los más restrictivos. Si un usuario tiene permiso de Lectura asignados en el recurso compartido y permiso local de Cambio, el permiso que prevalece cuando acceda por la red es el más restrictivo de los dos, es decir, el de Lectura. Obviamente, de forma local seguirá teniendo permiso de Cambio.

Por defecto los únicos usuarios que pueden fijar los permisos de un directorio compartido de un controlador primario son los Administradores y los Operadores de Servidores. En el caso de estaciones o servidores miembro también lo pueden hacer los Usuarios Avanzados.

Recursos compartidos administrativos

Dentro de la lista de recursos compartidos, se pueden ver algunos de ellos que tienen al final de su nombre el carácter dólar ($). Estos recursos compartidos tienen como objetivo facilitar la administración del sistema y se crean durante la instalación del SO. No se deben modificar ni borrar. Dependiendo de la configuración del equipo, alguno o todos los recursos compartidos administrativos pueden o no estar presentes. Son los siguientes:

- **ADMIN$.** Se usa durante la administración remota del equipo. Este recurso compartido apunta al directorio donde esté instalado el SO. Sólo los grupos Administradores, Operadores de Copia y los Operadores del Servidor pueden conectarse a este recurso. (Figura 6)

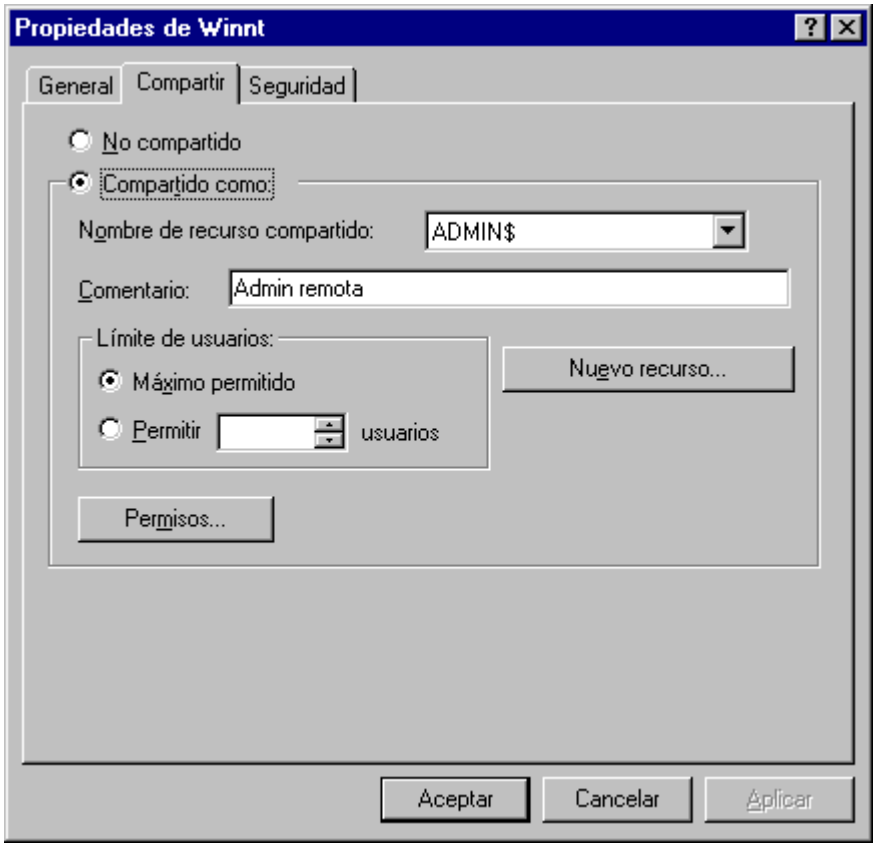

Figura 6 Recurso compartido ADMIN$

- **letraunidad$.** Comparten los directorios raíz de las unidades del sistema. Sólo los grupos Administradores, Operadores de Copia y los Operadores del Servidor pueden conectarse a este recurso.
- **IPC$.** También se emplea en la administración remota y cuando se ven los recursos compartidos. Es esencial para la comunicación en red.
- **NETLOGON.** Lo usa el servicio Net Logon de NT encargado de las entradas de los usuarios. Este recurso sólo lo comparten los servidores NT, no las estaciones.
- **PRINT$.** Usado para compartir impresoras.

- **REPL$.** Se crea en los servidores exportador para facilitar el servicio de duplicación o replicación.

El Administrador de Discos

En este apartado veremos las posibilidades del Administrador de disco, una herramienta fácil de usar y altamente intuitiva que nos ofrece múltiples opciones.

Posibilidades que ofrece

El Administrador de disco es la herramienta gráfica que emplea NT para la gestión de discos duros, con dicha herramienta podemos:

- Gestionar particiones de disco y unidades lógicas.
- Dar formato a volúmenes y asignarles nombres.
- Leer la información del estado de los discos.
- Leer la información del estado de los volúmenes, la etiqueta y la letra del volumen, el sistema de archivos y su tamaño.
- Crear y modificar las asignaciones de letras.
- Ampliar un volumen o un conjunto de volúmenes.
- Crear y eliminar conjuntos de volúmenes.
- Crear o eliminar conjuntos de bandas con o sin paridad (RAID 0 y RAID 5)
- Regenerar un miembro no encontrado de un conjunto de bandas.
- Establecer o romper conjuntos de espejos.(RAID 1).

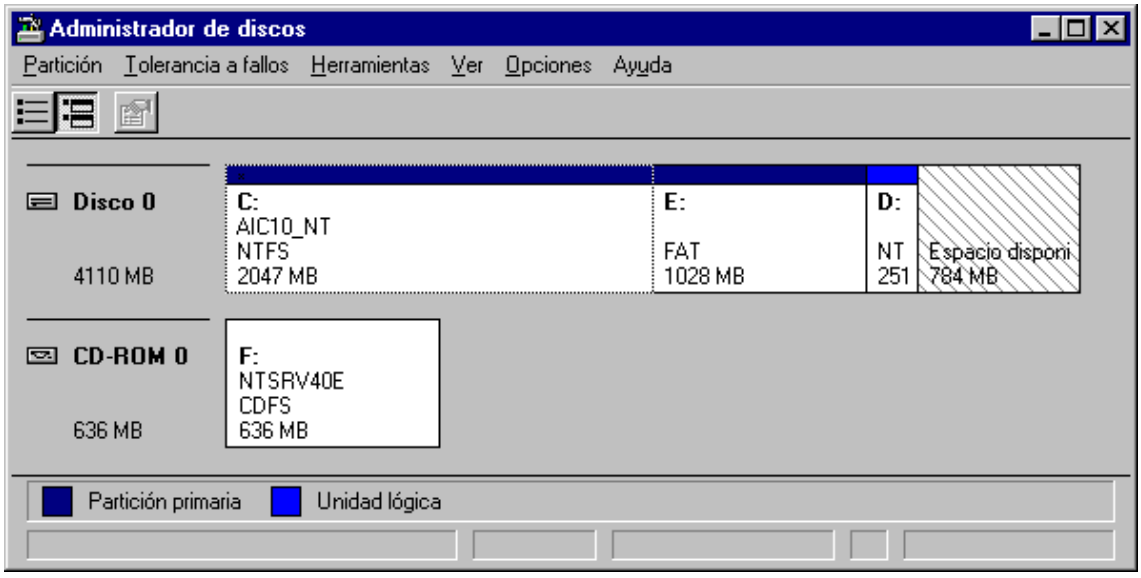

Figura 7 Administrador de discos I

Un vistazo rápido

Antes de comenzar un par de advertencias: el administrador de discos no permite trabajar sobre la partición de sistema (normalmente C:), ya que contiene los archivos necesarios para que NT se ejecute, el resto de las particiones son totalmente moldeables pero tendrás que tener cuidado con lo que haces en aquellas que contengan datos, ya que podrías perderlos.

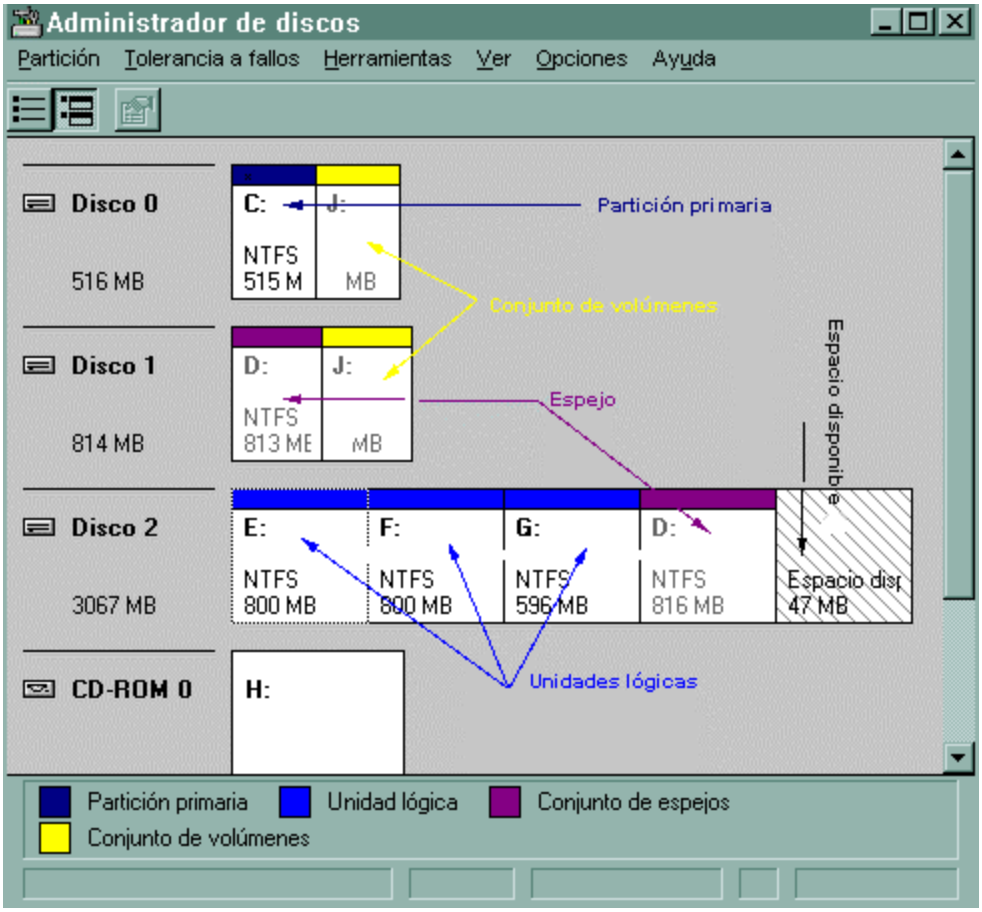

Figura 8 Administrador de discos II

En la Figura 8 puedes ver al Administrador de discos trabajando sobre un sistema con tres discos físicos (0,1 y 2) y un lector de cdrom, aquí puedes apreciar:

- Una partición primaria y activa de 515 MB que contiene la unidad lógica C: en el disco duro 0.
- Un conjunto de espejos para integridad de datos (unidad D:) en el disco duro 1.
- Una unidad lógica repartida en dos particiones de dos discos distintos, el 0 y el 1,(conjunto de volúmenes J:). fíjate en que aún está sin formatear.
- Un disco duro con cinco particiones: tres de unidades lógicas E:, F:, G: y un espejo de la unidad D: del disco 1.
- Espacio disponible sin particionar en el disco 2.

Con esta configuración hemos conseguido:

- Realizar un espejo (o sea una copia exacta) de un volumen (D:) que contiene los datos más importantes almacenados en este servidor, si mañana me falla uno de los discos duros puedo romper el espejo en el que ha quedado funcionando y seguir trabajando como si nada, incluso podré hacer un nuevo espejo con un tercer disco duro que siga en funcionamiento.
- Hemos aprovechado el espacio sobrante en dos discos duros para crear un solo volumen (J:) de mayor capacidad.
- También existe una zona sin asignar de 47 MB que podemos utilizar con total libertad para ampliar cualquiera de los volúmenes que se nos quede pequeño.

Todo esto se ha realizado usando solamente el Administrador de discos y una cierta planificación a la hora de adquirir los discos duros para el equipo (mejor dos o tres más pequeños que uno sólo más grande). También es muy importante saber como particionar correctamente un disco duro antes o durante la instalación de NT.

Disco de emergencia

Un disco de emergencia consiste en un diskette con los ficheros necesarios para poder reparar, o al menos intentarlo, nuestro equipo en el que caso de errores en nuestro sistema de archivos. El disco de emergencia es específico de cada sistema, es decir, un disco de emergencia de un servidor puede que no funcione para reparar otro servidor. Hay que entenderlo como una fotografía del sistema. Siempre que nuestro sistema cambie hay que actualizar esa fotografía. Siempre se debe disponer de un disco de emergencia.

Crear un disco de emergencia

Para crear un disco de emergencia se ejecuta el programa RDISK.EXE que se encuentra dentro de %SYSTEMROOT%\System32. El disco de emergencia se puede crear en la instalación o posteriormente, ejecutando directamente RDISK (rdisk /s para salvar las cuentas de usuario). De hecho cuando se produzcan cambios en nuestro sistema, es conveniente actualizar nuestro disco de emergencia para que contenga esas novedades.

El disco de emergencia contiene fundamentalmente información de configuración del sistema, aspectos de seguridad (SAM), configuración de programas.... Un disco de emergencia típico contiene los ficheros: system._, software._, security._, sam._, default._, ntuser.da_, autoexec.nt y config.nt. Como se puede ver son, básicamente, los ficheros que componen el registro, incluidos los ficheros del perfil.

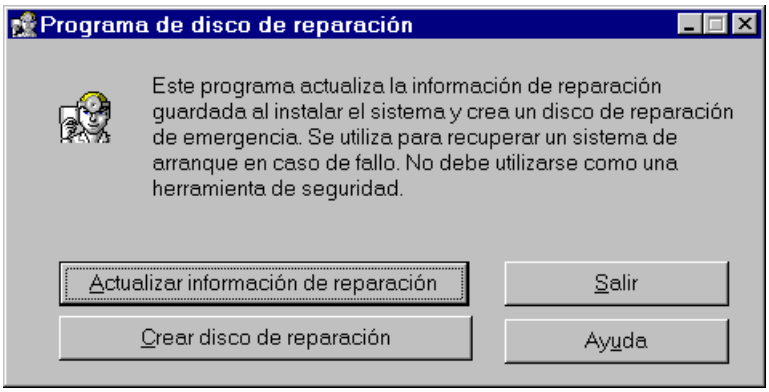

Figura 9 RDISK. Creación de discos de reparación

¿Cuándo hacer un disco de emergencia?

Pues siempre que hagamos un cambio importante. Ejemplos de cambios importantes: añadir, borrar o modificar las particiones de nuestro disco duro o la configuración de nuestro sistema de archivos, cuando se instalen nuevos componentes en nuestro servidor, como un servidor SQL o el Exchange Server, cuando se hagan cambios en el Panel de Control... En todas esas situaciones hay que actualizar nuestro disco de emergencia.

Aunque los discos de emergencia son ABSOLUTAMENTE imprescindibles, tienen un pequeño inconveniente y es que no son discos arrancables, es decir, necesitamos un disco de arranque para iniciar el equipo.

Crear un disco de arranque NT

Un disco de arranque puede ser útil para resolver problemas cuando el sistema no arranca, por ejemplo porque los ficheros BOOT.INI y NTDETECT.COM no son correctos. Aunque normalmente los problemas realmente los resuelve el disco de emergencia, necesitamos crear un diskette con los ficheros imprescindibles para arrancar el sistema NT. Hay que tener en cuenta que no nos servirán los discos de arranque DOS ya que no tendremos acceso con ellos a las particiones NTFS. En cambio los discos de arranque NT si nos proporcionan acceso a las particiones NTFS que, como se ha explicado, son las particiones que se deben emplear en equipos NT.

Disco de arranque NT: versión x86

Para crear el disco de arranque de NT para una plataforma Intel hay que seguir los siguientes pasos:

- Formatear el diskette
- Copiar los ficheros de arranque desde el directorio raíz de NT en el diskette. Esos ficheros son: BOOT.INI, NTDETECT.COM, NTBOOTDD.SYS y NTLDR. Estos ficheros están ocultos. El fichero NTBOOTDD.SYS sólo está presente si empleamos una controladora SCSI. Si no existe en el directorio raíz es que no nos hace falta.

Disco de arranque NT: versión RISC

Los disco de arranque de NT para una plataforma RISC difieren ligeramente respecto a las versiones x86. Hay que seguir los siguientes pasos:

- Formatear el diskette
- Copiar los ficheros OSLOADER.EXE y HAL.DLL.

En las plataformas RISC, la información del BOOT.INI de los equipos x86 se guarda en memoria RAM no volátil. Habrá que modificar el menú de selección de arranque de forma que apunte a la unidad de disco. El nombre ARC (Advanced RISC Computing) para el diskette es el siguiente:

scsi(0)disk(0)fdisk(0)

Habrá que fijar los valores oportunos para:

- OSLOADER: de forma que apunte al diskette
- OSLOADPARTITION: la partición primaria
- OSLOADFILENAME: el path para el directorio \SYSTEMROOT

Restaurar un servidor fallido

Cuando lo peor ocurra y nuestro servidor deje de funcionar, habrá que sustituir el disco duro, instalar un nuevo disco duro y tratar de recuperar el estado anterior a la catástrofe del sistema. Los pasos a seguir son los siguientes:

- El primer paso es reinstalar NT en un nuevo disco.
- Una vez instalado el SO, se puede restaurar el registro y la información de particiones con el disco de emergencia y su comando Reparar.
- Se reinicia el servidor y se recupera la última copia de seguridad.

Todo este proceso puede llevar una cantidad de tiempo importante, lo que puede ser inaceptable en ciertos entornos. Lo mejor en esos casos es hacer un espejo (preferiblemente duplexing en lugar de mirroring) del disco del sistema.

Emplear un disco duro de emergencia

Una alternativa barata y útil a hacer un espejo del disco del sistema, es emplear un disco viejo y reciclarlo para utilizarlo en caso de que falle el disco del sistema. Hace falta que el disco tenga al menos 100Mb y si es portable, mejor que mejor. Para crear ese disco duro de emergencia, instalaremos NT Server y crearemos un disco de arranque con el BOOT.INI preparado para arrancar desde el disco duro de emergencia. Cuando el sistema de archivos falle, simplemente conectaremos el disco duro de emergencia y arrancaremos desde él. Posteriormente y off-line reparemos el disco fallido.