

UT04

Windows 10 Gestión del almacenamiento

Contenidos

1. Organización del almacenamiento
2. Configuración de discos en Windows
3. Sistemas de archivos
4. **El sistema de ficheros NTFS**
5. Carpetas compartidas

4.- EL SISTEMA DE ARCHIVOS NTFS

Como hemos dicho, el sistema de archivos es el componente del sistema operativo encargado de gestionar los espacios de almacenamiento y la forma en que los archivos se guardan en ellos. Todos los sistemas operativos de Microsoft trabajan actualmente con NTFS, por lo que veremos en detalle su funcionamiento.

4.1.- Directorios

4.1.1- Características de los directorios

Un **directorio** es un contenedor de archivos y/o directorios. En esencia, un directorio simplemente es un tipo de archivo que almacena información acerca de los archivos y directorios que contiene.

En todos los sistemas de archivos existe un directorio especial, el **directorio raíz**. Este es el primer directorio de la jerarquía y de él parte toda la estructura de almacenamiento. En Windows el directorio raíz corresponde con cada una de las unidades de almacenamiento del sistema, identificada mediante la **letra de unidad** seguida del carácter :, por ejemplo, el disco C: o E:.

Al igual que los archivos, los directorios o carpetas tienen características que los definen:

- **Nombre:** cada directorio está identificado por un nombre. El nombre es obligatorio y sus reglas están determinadas por el sistema de ficheros.
- **Tamaño:** determinado por el tamaño de todos los ficheros y directorios que contiene.
- **Ubicación:** todo directorio está ubicado dentro de otro directorio, hasta llegar al directorio raíz, que no tiene directorio padre. Esto hace que los directorios se distribuyan en una estructura jerárquica o en forma de árbol. Cada directorio se identifica mediante una **ruta** que está determinada por todos los directorios que hay que recorrer desde el directorio raíz hasta él.
- **Información sobre el directorio:** por ejemplo, fecha de creación, permisos, oculto,...

4.1.2.- Directorios especiales

En todo sistema hay tres tipos de directorios especiales:

- **Directorio raíz:** como hemos dicho, el directorio raíz es del que parten todos los directorios del sistema. En Linux hay un único directorio raíz para el sistema, mientras que en Windows hay un

directorio raíz para cada unidad de almacenamiento, es decir, cada unidad de almacenamiento tiene su propio árbol de directorios.

- **Directorio actual:** este directorio se encuentra dentro de cada directorio, y apunta a él mismo. Se identifica por el carácter punto (.)
- **Directorio padre:** de forma análoga al directorio actual, cada directorio también contiene un directorio especial que apunta al directorio que lo contiene, es decir, a su directorio padre. Se identifica por los caracteres punto punto (..)

4.2.- Archivos

Los **archivos** o **ficheros** representan una colección de información localizada o almacenada en alguna parte del sistema de archivos. Técnicamente hablando, un archivo es un flujo de bytes tratado por el sistema operativo como una entidad única. Es un conjunto de bits que referencian algún tipo de información específica como un texto, un gráfico, un sonido, ... Los archivos son el conjunto organizado de informaciones de un mismo tipo y que pueden utilizarse en un mismo tratamiento.

4.2.1.- Características de los archivos

Algunas de las características de un archivo son:

- **Nombre y extensión:** cada archivo está identificado por un nombre y una extensión. El nombre es obligatorio mientras que la extensión es opcional y suele identificar el tipo de archivo. En NTFS se permite cualquier tipo de carácter en el nombre de los archivos. Los únicos caracteres que no se permiten son: \ / : * ; " < > |. Otra cuestión a tener en cuenta es que Windows no distingue entre mayúsculas y minúsculas.
- **Ruta:** cada archivo tiene una ubicación dentro del árbol de directorios. La ruta indica todos los directorios por los que hay que pasar desde el directorio raíz hasta llegar al directorio que contiene el archivo. La combinación de ruta más nombre de archivo debe ser única. En Windows la ruta se representa comenzando con la letra de unidad y separando los directorios con el carácter contrabarra (\). NTFS tiene un límite de 260 caracteres para el nombre de los ficheros incluida la ruta, aunque en Windows 10 es posible habilitar el uso de rutas más largas.
- **Tamaño:** los archivos tienen un tamaño que indica la cantidad de datos que contienen. Recuerda que es diferente el tamaño real del archivo del tamaño que ocupa en disco debido a que debe ocupar un número exacto de clústeres.
- **Tipo:** hay archivos de muchos tipos, pero una posible diferenciación es entre archivos ejecutables (extensión COM y EXE) y no ejecutables.

4.3.- Permisos NTFS

Los **permisos** son un mecanismo que proporciona Windows para determinar qué usuarios y grupos pueden acceder a qué ficheros o carpetas y en qué condiciones. Por ejemplo, se puede establecer que a un fichero solo pueda acceder el usuario *profesor* con permisos de lectura y escritura, mientras que el usuario *alumno* sólo puede acceder con permiso de lectura y el usuario *invitado* no puede acceder para nada.

4.3.1.- Grupos

Hemos mencionado en el párrafo anterior que los permisos se pueden asignar a grupos, pero ¿qué es un grupo? Un grupo simplemente es un conjunto de cuentas de usuario que tienen en común los mismos

permisos y derechos de seguridad. Esto quiere decir que, si dos usuarios del sistema pertenecen a un grupo y hemos dado permiso de lectura de un fichero a ese grupo, ambos usuarios tendrán este permiso.

Todo lo relativo a la gestión de grupos se hace en la consola de *Administración de equipos*, en la rama *Usuarios locales y grupos*. De forma análoga a la rama de usuarios, también se nos mostrará a la derecha una lista de todos los grupos que tengamos en el sistema. Por defecto Windows crea una serie de grupos al instalar el sistema, siendo los más importantes:

- **Administradores:** cualquier usuario que pertenezca a este grupo tendrá privilegios de administrador.
- **Usuarios:** todos los usuarios limitados del sistema pertenecen a este grupo.
- **Todos:** este es un grupo especial ya que no podemos indicar quien pertenece a él o no sino que la permanencia a este grupo viene dada automáticamente por el sistema. Cualquier usuario del sistema, sea quien sea, pertenece a este grupo.
- **Usuarios autenticados:** este también es un grupo especial o pseudo-grupo (la pertenencia o no de usuarios a este grupo viene determinada por el tipo de usuario, no pudiendo nosotros ni añadir ni quitar usuarios de este) que incluye tanto a los usuarios locales como los usuarios del dominio.

Para crear un grupo pulsamos con el botón derecho sobre el fondo y elegimos *Nuevo grupo*. Aquí podremos, además de indicar el nombre del nuevo grupo, qué usuarios pertenecerán a él. También se pueden añadir nuevos usuarios al grupo buscando el usuario en la rama *Usuarios* y yendo a la pestaña *Miembro* de del diálogo de *Propiedades*.

4.3.2.- Asignación de permisos

Lo primero que hay que tener en cuenta es que los permisos se asignan a carpetas o a ficheros. Por lo tanto, primero tenemos que determinar a qué carpeta o fichero se los queremos aplicar y en el menú contextual del fichero seleccionar la opción *Seguridad*. Al acceder a la pestaña *Seguridad* podremos ver que está formada por dos partes:

- En la parte superior hay una lista de los usuarios y grupos que tienen algún tipo de permiso definido sobre el fichero o carpeta. Este listado se denomina **ACL** o **Lista de Control de Acceso (Access Control List)**. Si un usuario no se encuentra en esta lista ni pertenece a un grupo que se encuentre en esta lista entonces no tendrá ningún tipo de permiso sobre el fichero y no podrá acceder a él de ninguna manera.
- En la parte inferior se encuentran los permisos que tenga el usuario. Esta parte cambia según el usuario o grupo que tengamos seleccionado en la parte superior.

Los diferentes permisos que se pueden asignar son:

- **Control total:** permite realizar cualquier tipo de operación con el fichero: leer, escribir, borrar, cambiar los permisos, ...
- **Modificar:** es similar a Control total, pero hay dos cosas que no permite: no permite borrar un fichero y no permite cambiar los permisos que tenga el fichero.
- **Lectura y ejecución:** indica que el usuario puede leer el contenido de un fichero y ejecutarlo si es un programa, pero no permitirá modificar su contenido.
- **Lectura:** similar al anterior, pero si el fichero es un programa no permitirá su ejecución.
- **Escribir:** es prácticamente igual que el permiso Modificar.

Cada uno de estos permisos supone un subconjunto de los permisos NTFS especiales, que son permisos muy concretos. En la siguiente tabla se puede ver qué permisos especiales incluye cada uno de los permisos.

Permisos	Control total	Modificar	Leer y ejecutar	Mostrar contenido de carpeta	Lectura	Escritura
Recorrer carpeta / Ejecutar archivo	X	X	X	X		
Listar carpeta / Leer datos	X	X	X	X	X	
Atributos de lectura	X	X	X	X	X	
Atributos extendidos de lectura	X	X	X	X	X	
Crear archivos / Escribir datos	X	X				X
Crear carpetas / Anexar datos	X	X				X
Atributos de escritura	X	X				X
Atributos extendidos de escritura	X	X				X
Eliminar subcarpetas y archivos	X					
Eliminar	X	X				
Permisos de lectura	X	X	X	X	X	X
Cambiar permisos	X					
Tomar posesión	X					
Sincronizar	X	X	X	X	X	X

Si quieres saber exactamente qué incluye cada uno de los permisos especiales en la [esta URL](#) tienes una explicación bastante detallada de los mismos.

Para cada uno de los permisos disponemos de dos pestañas y tenemos las siguientes opciones: no marcar nada, marcar la pestaña permitir y marcar la pestaña denegar.

- **Si no marcamos nada** estamos indicando que el usuario no tiene ese permiso sobre el fichero. Por ejemplo, si no marcamos nada en el permiso *Escribir* queremos decir que el usuario no podrá modificar el contenido del fichero.
- **Si marcamos la pestaña Permitir** estamos dándole ese permiso al usuario, por ejemplo, si permitimos en el permiso *Escribir* el usuario podrá modificar el contenido del fichero.

- Finalmente, **si marcamos la pestaña Denegar** lo que hacemos es denegar explícitamente ese permiso. Aunque parezca que es lo mismo en realidad hay mucha diferencia entre no marcar nada y marcar la pestaña Denegar.
 - Si no marcamos nada no estamos dando ese permiso, pero el usuario podrá adquirirlo por otro camino, por ejemplo, si a un usuario no le damos el permiso de escritura sobre un fichero, pero pertenece a un grupo que, si tiene ese permiso, entonces el usuario podrá escribir en él.
 - Si marcamos la pestaña *Denegar* estamos quitándole explícitamente ese permiso al usuario de forma que, aunque lo tenga permitido por pertenecer a un grupo, el usuario no tendrá el permiso. La opción *Denegar* tiene mayor precedencia que cualquier otra asignación de permisos.

4.3.3.- Herencia de permisos

Cuando trabajes con permisos es probable que te des cuenta de que en algunos ficheros hay una serie de permisos que están marcados en color gris y que no pueden modificarse. El motivo de esto es que **los permisos se heredan**. Es decir, que si asignamos un permiso determinado a una carpeta este mismo permiso se aplicará a todos los ficheros y subcarpetas que contenga la carpeta de forma recursiva.

Esto hace que podamos hablar de dos tipos de permisos:

- **Permisos heredados:** aquellos que tiene un objeto porque el directorio que lo contiene también los tiene.
- **Permisos explícitos:** aquellos que el usuario ha añadido al fichero o carpeta.

Un permiso que esté heredado no puede quitarse, aunque sí que se puede añadir un permiso a mayores (por ejemplo, si está heredado el permiso de lectura nosotros podremos añadir el de escritura) o denegarlo explícitamente.

Otra opción que tenemos para modificar los permisos heredados es **cortar la herencia**. Cuando cortamos la herencia lo que estamos diciendo es que no queremos que el fichero o carpeta en que la cortamos herede los permisos de la carpeta que lo contiene. Para cortar la herencia hemos de ir al botón de *Opciones avanzadas* y ahí hacer click en el botón que pone *Deshabilitar herencia*. Al hacer esto no aparecerá un diálogo dándonos dos opciones:

- **Copiar:** esto quiere decir que los permisos que antes estuvieran heredados (los marcados en gris) se mantendrán, pero no como heredados sino como permisos explícitos (por lo tanto, estarán en verde y podremos modificarlos).
- **Quitar:** con esta opción decimos que cualquier permiso heredado que tenga el fichero o carpeta será quitado del todo. Hay que tener mucho cuidado con esta opción ya que si quitamos los permisos a todos los usuarios nadie podrá acceder al fichero, ni tan siquiera el administrador.

En el mismo sitio podemos ver una casilla de verificación con el texto *Reemplazar todas las entradas de permisos de objetos secundarios por entradas de permisos heredables de este objeto* (solo se muestra en carpetas). Se puede decir que el objetivo de esta casilla es el contrario que el del botón *Deshabilitar herencia*. Mientras que cuando deshabilitamos la herencia hacemos que el elemento actual no herede ningún permiso de la carpeta que lo contiene, pasando a tener únicamente permisos explícitos, si marcamos la casilla obligamos a que todos los elementos descendientes del actual (todas las subcarpetas y archivos) hereden los permisos de la carpeta actual. Es decir, estamos deshaciendo la opción *Deshabilitar herencia* que pudiera tener cualquier descendiente.

4.3.4.- Permisos efectivos

Para determinar los permisos que tiene un usuario sobre un elemento (archivo o carpeta) hay que tener en cuenta lo siguiente:

- Los permisos que tenga directamente asignados el usuario.
- Los permisos asignados a cada uno de los grupos a los que pertenezca el usuario se añaden a los permisos que tenga el usuario. Recuerda que pueden ser grupos que hayas creado, pero también hay una serie de grupos especiales del sistema:
 - *Grupo Usuarios*: cualquier usuario creado que no sea administrador es automáticamente añadido a este grupo. Aunque no es recomendable, si puedes sacar a un usuario de este grupo.
 - *Grupo Administradores*: si creamos un usuario e indicamos que tendrá permisos de administración será automáticamente añadido a este grupo. Es posible sacarlo del grupo, pero en ese caso no perderá los privilegios de administrador.
 - *Grupo Usuarios autenticados*: todos los usuarios del sistema pertenecen a este grupo y no podemos sacar a un usuario de este grupo. Perteneces automáticamente a él todos los usuarios que han indicado sesión con un nombre de usuario y una contraseña (aunque ésta puede estar en blanco).
 - *Grupo Todos*: al igual que el grupo anterior, no se puede sacar a un usuario de este grupo ya que es un grupo especial. Incluye todos los usuarios del grupo anterior más usuarios del sistema o especiales que no tienen contraseña, como el usuario Invitado o LOCAL_SERVICE.
- Los permisos marcados como *Denegar*, tanto directamente al usuario como a alguno de los grupos a los que pertenezca, prevalecen sobre cualquier otro permiso.

Como se puede ver, saber los permisos que tiene un usuario requiere comprobar todos los permisos de cada uno de los grupos que tenga un usuario, lo cual puede ser una tarea complicada en entornos con muchos grupos. Para facilitar la labor de conocer qué permisos tiene realmente un usuario determinado sobre un objeto hay una pestaña denominada *Acceso efectivo* en el cuadro de diálogo *Opciones avanzadas* que muestra precisamente esto.

Para ello simplemente tenemos que seleccionar el usuario y nos mostrará si tiene o no tiene autorizado cada uno de los permisos especiales, por lo que fácilmente podremos extrapolarlo para saber que permisos tiene.

4.3.5.- Propietario

Todos los archivos y carpetas tienen un **propietario** que es el usuario que ha creado dicho objeto. El propietario de un objeto tiene la capacidad de cambiar los permisos de dicho objeto, aunque no tenga permisos directamente para ello. Por ejemplo, si borramos todas las entradas de la ACL de un objeto se supone que nadie podrá acceder para nada a dicho objeto, pero sí podrá hacerlo el propietario a pesar de que no esté en la ACL ni él ni ninguno de los grupos a los que pertenezca.

Se puede ver el propietario de un objeto en *Opciones avanzadas*. Desde aquí también puede tomar posesión del objeto cualquier otro usuario que tenga permisos de *Control total* sobre dicho objeto. También puede tomar posesión de un objeto cualquier usuario que pertenezca al grupo *Administradores* aunque no tenga ningún tipo de permiso directamente sobre el objeto.