

Cómo acceder a un NTFS desde una distribución live de Linux

AL ROJO VIVO

www.fotolia.de/Eisenhans

Muchas veces, lo único que necesitas para recuperar un ordenador caído por un problema del sistema (o un ataque de virus) es una distro live de Linux. El creador de Knoppix, Klaus Knopper, te ofrece algunos consejos para acceder a un NTFS desde una de ellas. **POR KLAUS KNOPPER**

Las distribuciones lives están diseñadas para arrancar desde un disco CD o DVD, en un ordenador que podría tener un sistema diferente en el disco duro. En la mayoría de los casos, se trata de un PC Windows con su HD formateado para NTFS. Este artículo cubre casi todos los datos importantes que necesitas saber a la hora de acceder a un NTFS desde un sistema Linux live.

Linux y NTFS

Como aprenderás más adelante, actualmente hay, al menos, tres implementaciones de soporte NTFS [1] de Código Abierto en GNU / Linux:

- libntfs, del proyecto Linux-NTFS, y una colección de herramientas del userspace para manejar NTFS, similares a mtools. Las herramientas incluyen la utilidad ntfsmount, que utiliza el modelador de kernel FUSE (Filesystem en Userspace) [3], para conectar una partición NTFS a un punto de montaje usando libntfs. Con libntfs no sólo es posible leer,

sino también escribir en NTFS, con la limitación de que no se puede

hacer una reorganización del índice. Esto significa que sólo 9 archivos o

Knoppicilin

Knoppicilin ("Knoppicilina") es un derivado especial de Knoppix. Se trata de un escáner de virus para instalaciones de Windows, basado en los sistemas live GNU / Linux, y que ocupa muy poco espacio (alrededor de 200 MB). Suele haber varios escáners instalados, tanto comerciales como gratuitos. Por causa de las licencias de propietario de algunos escáners y sus bases de datos, Knoppicilin no se distribuye gratuitamente (al contrario que Knoppix), pero se puede encontrar (como add-on incluido) en la revista alemana c't. Knoppicilin se ha traducido parcialmente al inglés, aunque la mayoría de su texto sigue en alemán.

Dado que un escáner de virus debe ser capaz no sólo de detectarlos, sino también de eliminarlos (o al menos desactivarlos), la función lectura/escritura de ntfsmount resulta algo insuficiente. Borrar un archivo de un NTFS, utilizando nfmount, no siempre es posible, y la tarea está condenada al fracaso si el archivo es algo más que una

hoja en el árbol del sistema de archivos. Con el objetivo de destruir los virus de un modo fiable, se ha añadido un parche al ntfsmount que, en caso de que no pueda borrar un archivo infectado, simplemente trunca su contenido y lo convierte en tamaño cero, para después enviar al escáner un mensaje de borrado exitoso (lo que, de hecho, no deja de ser un pequeño truco). Sobre escribir el archivo habría sido un problema menor, siempre que hubiera disponible una copia que funcionara correctamente (cosa que no siempre ocurre).

ntfs-3g, con soporte de lectura/escritura no restringido para NTFS (diseñado por Szakacsits Szabolcs), ha convertido este parche en algo innecesario en el reciente lanzamiento de Knoppicilin. En él, el borrado de archivos (junto con la reorganización de la estructura interna del índice de archivos NTFS) está perfectamente implementada.

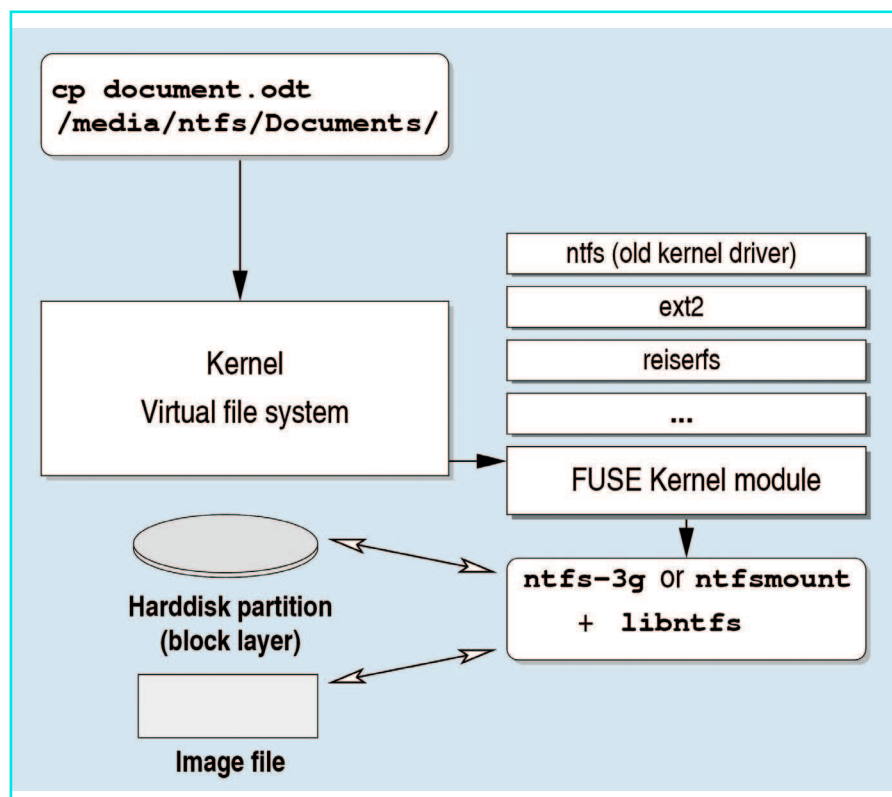


Figura 1: FUSE te permite construir un sistema de archivos que utiliza abstracciones de alto nivel.

subdirectorios se pueden crear por directorio, y esos archivos sólo podrán borrarse bajo determinadas circunstancias. Esto resulta suficiente para modificar archivos o mover un archivo de otra partición a la que tenemos entre manos, pero no para dedicarse a copiar gran número de archivos.

- El driver de kernel ntfs, que es un spinoff de libntfs, pero con la funcionalidad muy reducida (sólo puede sobrescribir archivos ya existentes: ni borrarlos ni crearlos).
- ntfs-3g [4], un fork (o bifurcación)

de libntfs y ntfsmount. En éste se implementan las funciones para reconstruir el sistema de archivos correctamente, así que ntfs-3g permite la lectura y escritura sin restricciones en el NTFS, utilizando el módulo kernel FUSE, exactamente igual que en la antes mencionada ntfsmount de libntfs.

Utilizar FUSE como puente para acceder a un sistema de archivos presenta muchos beneficios. Para empezar, reduce el (por otro lado necesario) esfuerzo para implementar las funciones del kernelspace para el acceso a

los archivos. En kernelspace, tareas como abrir o escribir un archivo no son fáciles: en esencia, tienen que ser implementadas como instrucciones de acceso y cierre para conseguir “páginas” de datos, que a menudo tienen que ser reensambladas y decodificadas antes de enviarse de vuelta al programa que realizó la llamada al sistema. El módulo FUSE permite abstracciones de más alto nivel, como las librerías de funciones, e implementa el input / output (directo o por caché), así que el programador no tiene que encargarse de ello. Esto podría explicar porqué el módulo de sistema de archivos del ntfs kernel se ha quedado un poco atrás en funcionalidad con respecto a las alternativas libntfs y ntfs-3g que trabajan al máximo en FUSE (Figura 1).

Por otro lado, montar un sistema de archivos con FUSE requiere más que un simple comando *mount*, dado que el verdadero interfaz del sistema lo tiene que aportar una herramienta del espacio de usuario. Pero siempre hay maneras con las que seguir utilizando *mount -t ntfs* con las herramientas FUSE, como demostraré en este artículo.

ntfs-3g

Para acceder a una unidad NTFS con ntfs-3g primero tienes que asegurarte de que tu sistema GNU / Linux cumple las siguientes condiciones. La mayoría son precauciones de seguridad que exigen el módulo kernel y la librería FUSE.

- El módulo FUSE debe estar cargado, y existir un */dev/fuse* que pueda ser leído y modificado por el usuario.
- El archivo o imagen que se va a montar debe permitir lectura y escritura por el usuario.
- El punto de montaje elegido debe permitir lo mismo.
- Además, el usuario debe ser el dueño del punto de montaje.

Si no tienes ninguna partición real de disco duro con NTFS, puedes también utilizar una imagen creada con *dd if=/dev/ntfs-partition of=ntfs.img* en un ordenador distinto, que tenga también un sistema de archivos instalado. Utilizando la utilidad *themkntfs* de ntfsprogs (véase la sección de ntfsprogs en este mismo artículo), podrás crear una imagen de archivo NTFS vacía o una

Leer los avisos

Puede ocurrir que, al intentar montar una partición NTFS en modo escritura con *ntfsmount* o *ntfs-3g*, te encuentres con un mensaje de error que indica “Windows no se ha apagado correctamente”, además de un sistema de archivos NTFS inconsistente. Esto significa que el sistema de archivos no se ha podido montar para lectura y escritura. Este mensaje de error sugiere, incluso, que deberías reiniciar en Windows, para arreglar el problema con el *scandisk* de Windows. Reiniciar entrando en Windows puede ser complicado si éste no se cierra de forma

adecuada, o si sencillamente no tienes Windows instalado.

Todavía no se ha desarrollado una herramienta minuciosa de comprobación y reparación de NTFS para Linux, como *ntfsck*. Pero, por suerte, los paquetes *ntfsprogs* (basados en *libntfs*) incluyen una herramienta llamada *ntfsfix*, que no arregla las inconsistencias pero limpia el diario del sistema de archivos NTFS. Esto implica que la partición podrá montarse para lectura y escritura de nuevo, sin necesitar ninguna herramienta de Windows que lo arregle.

Consigue

X1



por sólo

5'95 €

y además ...
con cada
número de
regalo un
fantástico
DVD 100%
Open Source
¡ Pídelos ya !

www.linux-magazine.es/prueba

partición. Para montar la imagen del sistema de archivos *ntfs.img* en */media/ntfs*:

```
ntfs-3g ntfs.img /media/ntfs
```

Ahora deberías ser capaz de acceder a */media/ntfs* desde cualquier programa, y leer y escribir en este directorio. Para desmontar la imagen más tarde, utiliza el siguiente comando:

```
umount /media/ntfs
```

o bien

```
fusermount -u /media/ntfs
```

Espacio Swap

Si arrancas un sistema con Windows instalado, lo más normal es que te encuentres con un disco duro exclusivamente NTFS. Si el ordenador tiene poca RAM, posiblemente estés en una situación en la que pueda ayudarte utilizar archivos en NTFS como espacio Swap para tu sistema live Linux.

Suponiendo que */dev/sda1* es una partición de disco duro SATA con NTFS (y asumiendo que se cumplen todas las condiciones de FUSE antes mencionadas), el comando para crear un archivo swap de 500 MB y empezar a volcar en él sería como sigue:

```
mkdir /tmp/sda1
ntfs3g /dev/sda1 /tmp/sda1
dd if=/dev/zero of=/
/tmp/sda1/ntfs3g.swap
bs=1M count=500
mkswap /tmp/sda1/ntfs3g.swap
(as root) swapon /
/tmp/sda1/ntfs3g.swap
```

Esto añadirá 500 MB a tu reserva de memoria virtual.

Knoppix y NTFS

Desde su primer lanzamiento público, Knoppix (diseñado como un sistema live GNU/Linux para el trabajo diario, más que como una herramienta para administradores pura) se ha utilizado frecuentemente como un sistema de rescate de archivos para Windows que no son capaces de arrancar o con instalaciones defectuosas. Esto es así gracias a su capacidad de montar una partición NTFS

de, por lo menos, sólo lectura, y crear backups de los contenidos del sistema de archivos.

Para hacer más fácil el uso de NTFS en modo escritura, Knoppix toma ventaja del hecho de que el comando *mount -t filesystemtype*, usado prácticamente por cada aplicación (también KDE) para montar particiones, llama a */sbin/mount.filesystemtype*, si existe. */sbin/mount.ntfs* es un script de envoltura en Knoppix que construirá las líneas de comando para los montajes NTFS basados en FUSE a partir de las opciones comunes de montaje, y ejecutará una llamada de montaje real, de modo que los usuarios tendrán acceso transparente a las particiones NTFS sin tener que saber nada de las opciones específicas de *fusermount*, *ntfsmount* o *ntfs-3g*. Además, es posible hacer click en una partición NTFS y convertirla en modificable cambiando el status *read / write* (“lectura / escritura”) a través de los iconos en el escritorio Knoppix.

Las opciones de arranque específicas de Knoppix *tohd =* y *fromhd =* te permiten copiar automáticamente los contenidos del CD o DVD live a la partición de disco duro; así podrás tener la unidad CD o DVD libre cuando trabajes con Knoppix. Con la versión 5.1 de Knoppix es posible también NTFS; esto incrementa un poco el tamaño inicial de su *ramdisk* para poder guardar todas las herramientas y unidades necesarias. Por otro lado, te permite utilizar NTFS como un sistema de archivos que sostiene un disco duro virtual, o incluso un archivo de volcado para Linux.

La mayoría de distribuciones live utilizan sus propios scripts de envoltura (casi todos basados en *ntfs-3g*) para facilitar al usuario el acceso a las particiones NTFS.

Escáner de Virus y Alternate Data Streams

Un uso común para las distribuciones live con NTFS es reparar un sistema Windows atacado por un virus (echa un vistazo al cuadro titulado “Knoppicilina”). Un problema de todos los antivirus es el hecho de que NTFS incluye una opción llamada “Alternate Data Streams” (ADS, o “Streams alternativos de datos”), lo que significa que varios archivos distintos pueden existir con el mismo nombre. Los escáners de virus tienden a comprobar

los datos sólo del primero de ellos, lo que implica la posibilidad de que un virus permanezca sin detectar.

ntfs-3g soporta dos formas de manejar streams alternativos de datos. El primer método es parecido al estilo en que Windows maneja las ADS. Para ello, te hará falta llamar al *ntfs-3g* como se indica:

```
ntfs-3g -o
streams_interface=windows
/dev/ntfs-partition
media/ntfs
```

Se puede acceder al stream alternativo dentro de un archivo usando

```
filename:streamname
```

en vez de usar nada más el nombre del archivo. Por desgracia, no hay aún una opción en *ntfs-3g* que te permita observar los componentes ADS en el listado del directorio *ls -l* de forma directa. Quizá es así por los posibles conflictos con archivos que contienen símbolos de dos puntos, lo que está también permitido.

Un método alternativo es la opción *streams_interface=xattr* de *ntfs-3g*. Esto permite ver y modificar el contenido de archivos ADS, utilizando atributos extendidos. Por ejemplo, *getfattr -n ntfs.streams.list filename* lista los streams con nombre dentro del archivo ADS.

Mientras que las características de ADS funcionan perfectamente con las implementaciones de NTFS basadas en FUSE para Linux, lo que permite backups y extracción de este tipo de archivos, ninguno de los escáners de virus de Windows basados en Linux soportan esta capacidad. Así que la mayoría de virus escondidos en archivos ADS permanecerán sin ser descubiertos. ■

RECURSOS

- [1] NTFS en Wikipedia: <http://en.wikipedia.org/wiki/NTFS>
- [2] Proyecto Linux-NTFS: <http://www.linux-ntfs.org>
- [3] Proyecto FUSE: <http://fuse.sourceforge.net>
- [4] *ntfs-3g*: <http://www.ntfs-3g.org>