

чтение и запись NTFS разделов под Linux/BSD

крис касперски ака мышцх, a.k.a. nezumi, a.k.a. souriz, no-email

половина пользователей Linux/BSD уверена, что поддержка NTFS в них отсутствует. другая половина знает, что NTFS-тома доступны по крайней мере на чтение, но писать они опасаются, наслушавшись ужасных историй о разрушенных данных десятилетней давности, когда уже лет пять как драйвера отлажены и достаточно стабильны. однако, в работе с NTFS есть куча тонкостей, игнорирование которых приводит к развалу файловой системы. как избежать краха? как восстановить поломанный том? мышцх знает. и не только знает, но и рассказывает.

введение

Потребность в работе с NTFS-разделами из-под Linux/BSD возникает достаточно часто, особенно при совместном использовании нескольких операционных систем (одной из которых является NT или что-то производное от нее) на мультизагрузочном винчестере. Проблема в том, что NT крайне враждебно относится к своим конкурентам и "чужеродных" файловых систем она принципиально не "переваривает", а Linux и BSD, из всех файловых систем, входящих в NT, штатным образом поддерживают только FAT12/16/32 (причем, русские имена часто превращаются в "крякозяблы").

Как организовать обмен данными между Linux/BSD и NT? Некоторые предпочитают использовать флешки (благо объем последних уже сопоставим с емкостью жестких дисков и они вполне годятся на роль "файло-обменника"). Еще можно отформатировать один или несколько разделов диска под FAT, однако, поверьте мне парни, — это не лучший выход из ситуации. FAT страдает множеством ограничений: часто теряет кластеры, не поддерживает дисков большого объема, атрибутов защиты и т. д. Чем скорее мы забудем это наследие времен MS-DOS — тем лучше.

Другой вариант — установить NT-драйвер, позволяющей ей работать с Linux/BSD-разделами как со своими собственными. Такие драйвера действительно есть, хотя и не получили большого распространения. Написанные энтузиастами (у которых нет ни средств, ни времени для продвижения их на рынок) они пылятся на серверах, никем не рекламируемые и большинство пользователей даже не подозревает об их существовании. А зря! Взять хотя бы ffsdrv-драйвер, добавляющей в NT поддержку FFS/UFS (основных файловых системы Free/Net/OpenBSD). Отличная штука, которую (вместе с исходными текстами) можно бесплатно скачать с <http://ffsdrv.sourceforge.net>

Установка происходит стандартно и у продвинутых пользователей никаких проблем не вызывает, тем более, что в последних версиях драйвера появился графический менеджер, позволяющий монтировать/демонтировать диски посредством мыши, без возни с командной строкой (см. рис. 1).

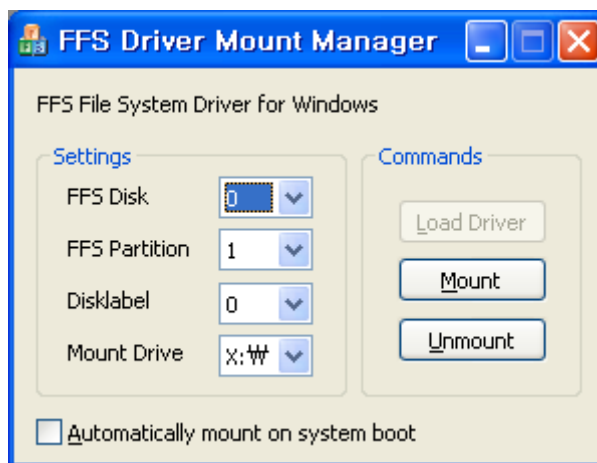


Рисунок 1 графический менеджер драйвера ffsdrv, добавляющего в Windows поддержку файловых систем FFS/UFS

Обратную операцию (т. е. заставить Linux/BSD понимать NTFS) осуществить намного сложнее. И совсем не потому, что NTFS весьма продвинутая файловая система, которая open source программистам не по зубам. Вовсе нет! В мире UNIX встречаются и более навороченные файловые системы (например, ReiserFS). Причина в том, что Microsoft держит NTFS под спудом, отказываясь ее документировать и потому расшифровку всех ключевых структур приходится выполнять путем обратного проектирования, что предъявляет весьма высокие требования к квалификации исследователей, а сама реконструкция спецификации отнимает кучу сил и времени, так что, по большому счету, это не программистская, а хакерская работа.

С момента появления NTFS прошло более пятнадцати лет и за это время она была изучена вдоль и поперек. Свободные драйвера уже давно миновали стадию бета-версий, освоившись не только с чтением, но и с записью. Риск разрушения тома из-за ошибки в свободном драйвере больше носит психологический, чем технический характер. Миллионы пользователей Linux/BSD монтируют NTFS-разделы на запись, доверяя свободным драйверам свои данные, и никто не жалуется! Единичные отказы, естественно, случаются, но носят поправимый характер.

Составители UNIX-дистрибутивов, проявляя свойственную им осторожность, либо вообще не включают в них свободные NTFS-драйвера, либо по умолчанию монтируют NTFS-разделы только на чтение, вызывая у пользователей уверенность, что запись реализована черт знает как и лучше держаться от нее подальше. Действительно, NTFS-драйвера не свободны от проблем и неподготовленному пользователю лучше с ними не связываться, однако, все проблемы решаемы! Главное — это желание! Ну и документацию тоже не вредно читать.

Ладно, не будем ходить кругами! В конце концов, NTFS не так страшна, как ее малюют, а мы совсем не девочки и иметь секс с системой нам не впервой. А секса будет много...

Linux

Первые свободные NTFS-драйвера возникли в рамках проекта Linux-NTFS Project, основанного хакером по прозвищу Martin von Loewis в далеком 1995 году (напоминаем, что Microsoft выбросила NTFS на рынок в 1993 году) и объединившего целую плеяду знаменитых кодокопателей, которым потребовалась два года напряженных исследований на расшифровку базовых структур данных и создание первой стабильной версии свободного NTFS-драйвера, включенного в Linux-ядро в 1997 году (версия 2.1.74).

Группа просуществовала до конца девяностых, а затем распалась. Причиной тому послужила мелкая ошибка в драйвере, вылившаяся в крупные неприятности. Драйвер не проверял версию файловой системы, поскольку, в тот момент других версий NTFS попросту не существовало в природе! Но, с выходом W2K, компания Microsoft преподнесла довольно пакостный "сюрприз" в виде несущественных (с точки зрения конечного пользователя), но фатальных (с точки зрения программиста) изменений файловой системы. В базовые структуры данных было добавлена пара новых полей. Соответственно, смещения всех остальных — изменились, а драйвер, ожидающих их по старым адресам, при первой же попытке записи делал из диска кашу, что не самым лучшим образом сказалась на его репутации, которую было уже не поднять и домкратом. Большинство историй о страшных разрушениях типа "дня Помпеи" берут свое начало именно здесь.

В 2002 году вышла новая версия NTFS-драйвера, полностью переписанная с нуля уже в новом командном составе: Anton Altaparmakov (лидер группы, создатель драйвера и служебных NTFS-утилит), Richard Russon, Jakob Kemi (создатели загружаемого модуля ядра), Pawel Kot (портирование нового драйвера в ядро) и другие.

Готовый к установке драйвер (вместе с исходными текстами и реконструированной спецификацией на NTFS) можно бесплатно скачать с сайта <http://www.linux-ntfs.org>, построенного по технологии wiki, существенно упрощающей процесс внесения изменений и уточнений в спецификацию, полученную, как уже говорилось, путем обратного проектирования, и до сих пор не завершенную. Microsoft не стоит на месте и непрерывно модифицирует свою файловую систему, вынуждая хакеров продолжать расшифровку, с которой они справляются вполне успешно и текущая версия свободного драйвера поддерживает NTFS-разделы, созданные следующими операционными системами: NT 4.x, W2K, XP, Server 2003 и Висла (включая 32-битные и 64-битные версии).

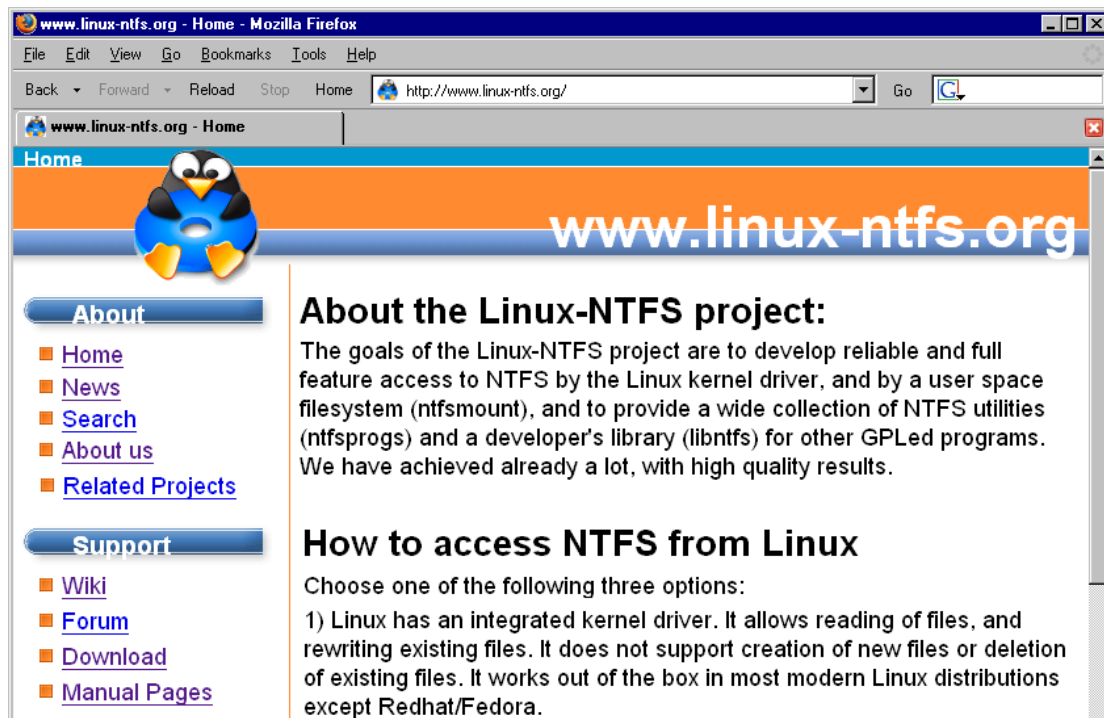


Рисунок 2 главная страница проекта Linux-NTFS, распространяющая открытый NTFS-драйвер и содержащая наиболее полную версию реконструированной спецификации по NTFS

Драйвер превосходно справляется с чтением NTFS-томов, однако, до сих пор не поддерживает запись в сжатые, зашифрованные или разряженные файлы (sparse-files), что, собственно говоря, и неудивительно, поскольку поддержка записи появилась лишь в 2005 году и программистам еще предстоит проделать уйму работы, прежде, чем они доведут ее до ума.

Практически все крупные дистрибутивы (за исключением RedHat/Fedora) уже поддерживают NTFS и потому конечным пользователям совершать дополнительные телодвижения нет никакой необходимости — ну разве что установить более свежую версию драйвера (*примечание: RedHat и Fedora включают в себя альтернативный открытый драйвер "NTFS-3G", о котором мы расскажем чуть ниже*).

Проверить: поддерживает ли ваш дистрибутив NTFS поможет команда: "cat /proc/filesystems", и, если, NTFS действительно поддерживается, смонтировать том можно так:

```
# mkdir /mnt/windows
# mount /dev/hda1 /mnt/windows -t ntfs -r -o nls=utf8
```

Листинг 1 монтирование NTFS-разделов (ключ -r означает "монтирование только на чтение", если его убрать, то раздел будет доступен и на запись)

Размонтирование диска осуществляется следующим образом:

```
# umount /mnt/windows
# umount /dev/hda1
```

Листинг 2 размонтирование NTFS-разделов

А как быть, если нам очень хочется получить полноценную поддержку NTFS, включающую в себя работу с журналом транзакций, запись в сжатые или разряженные файлы? Тогда можно воспользоваться одной из многочисленных "оберток" вокруг штатного драйвера NTFS.SYS, погружающих его в виртуальную среду, эмулирующую исполнительную подсистему NTOSKRNL.EXE и обеспечивающую прозрачный ввод/вывод.

Достоинство этого метода в том, что мы получаем 100% совместимость с NTFS-разделом и потому риск утратить данные — минимален. К тому же, "родной" NTFS-драйвер обеспечивает намного более высокое быстродействие, правда, эмулятор исполнительной системы отъедает не хилое количество памяти, что есть главный и, пожалуй, единственный

существенный недостаток. Естественно, помимо "обертки" нам потребуется дистрибутив Windows, поскольку, лицензионные соглашения запрещают свободное распространение его компонентов. Но это не проблема! Если у нас есть NTFS-раздел, то, логично предположить, что у нас имеется по меньшей мере одна копия Windows, поскольку у True-Unix'оидов потребности в работе с NTFS просто не возникает.

Осталось решить какую из всех "оберток" выбрать? Мысльх долгое время пользуется "оберткой" от Jan'a Kratochvil'a, которую рекомендует и всем остальным. Последнюю версию, выпущенную в начале 2006 года, можно бесплатно скачать с <http://www.jankratochvil.net/project/captive/>

```
# Jan Kratochvil: Captive: The first free NTFS read/write filesystem for GNU/Linux (p1 of 5)
# [1]prev [2]next [3]up

Jan Kratochvil

[4]Projects [5]Products [6]CVS [7]Resume [8]Contact

Projects

[9]UNIX [10]UNIX-devel [11]Web [12]Amiga [13]MS-Windows [14]MS-DOS [15]Patches

Captive: The first free NTFS read/write filesystem for GNU/Linux

o [16]Download o [17]NEWS o [18]Testimonials o [19]Internet Press o [20]Installation
Notes o [21]Mailing Lists o [22]See Also

This project is no longer maintained.

Project implements the first full read/write free access to NTFS disk drives. You can
mount your Microsoft Windows NT, 200x or XP partition as a transparently accessible volume
for your GNU/Linux.

This compatibility was achieved in the [23]Wine way by using the original Microsoft
Windows ntfs.sys driver. It emulates the required subsystems of the Microsoft Windows
kernel by reusing one of the original ntoskrnl.exe, [24]ReactOS parts, or this project's
own reimplementations, on a case by case basis. Project includes the first open source
MS-Windows kernel API for Free operating systems. Involvement of the original driver files
was chosen to achieve the best and unprecedented filesystem compatibility and safety.

As opposed to other projects this is currently the only software supporting the full
read/write access including the possibility to create/delete files, modify directories
etc.

Download
-more- http://www.jankratochvil.net/project/Rel.pm?rel=prev&project=captive
```

Рисунок 3 домашняя страничка Jan'a Kratochvil'a — создателя бесплатной "обертки" вокруг стандартного драйвера NTFS.SYS, "погружающего" его в Linux

Архитектурно она состоит из свободной библиотеки FUSE, что расшифровывается как Filesystem in Userspace — файловые системы в пользовательском пространстве (<http://fuse.sourceforge.net>), эмулятора исполнительной подсистемы NT, написанного на базе фрагментов исходных текстов, "позаимствованных" из открытого проекта ReactOS (<http://www.reactos.com>), транслятора запросов ввода/вывода, написанного непосредственного самим Jan'ом Kratochvil'ом, ну и драйвера NTFS.SYS, который пользователь должен самостоятельно "выдрать" из Windows-дистрибутива.

Монтирование дисков осуществляется вполне стандартным путем:

```
# mkdir /mnt/dosc
# mount -t captive-ntfs /dev/hda1 /mnt/dosc
```

Листинг 3 монтирование NTFS-разделов через "обертку"

Кстати говоря, поскольку данная "обертка" реализована как прикладной процесс, то, с одной стороны, она не "уронит" ядро, если что-нибудь пойдет не так, с другой же, "продвинутый" (в кавычках) пользователь может "покидать" процесс, не дав драйверу сохранить на диск модифицированные данные, что чревато крахом всего дискового тома.

xBSD

Популярность BSD-подобных систем намного ниже, чем у Linux'a, а на рабочих станциях они вообще редкость, "благодаря" чему NTFS-драйвера под них появились с большим опозданием.

Первый экспериментальный драйвер (кстати говоря, написанный российским программистом, скрывающимся под ником "семен") датируется 1999 годом (т. е. спустя целых два года после выхода стабильной версии открытого Linux-драйвера — для компьютерной индустрии это огромный срок!). Однако, после выхода нескольких бета-версий, пыл автора начал постепенно угасать и менее чем через полгода достиг абсолютного нуля. Обещанная полнофункциональная версия так и не вышла, в чем можно убедиться посетив сайт: <http://iclub.nsu.ru/~semen/ntfs/>

Поисковики позволяют найти несколько аналогичных проектов, стартовавших приблизительно в то же самое время и кончивших свою жизнь аналогичным образом. Оно и понятно. Количество пользователей BSD невелико, программистов среди них еще меньше, да и денег в создание NTFS-драйвера никто вкладывать не собирается.

Ситуация изменилась с выходом Mac OS X, основанной как известно, на ядре BSD, и, будучи коммерческим продуктом, агрессивно продвигаемым на рынок, сумевшей собрать целую армию пользователей, реально заинтересованных в работе с NTFS. Спрос в очередной раз породил предложение и Anton Altaparmakov перенес открытый NTFS-драйвер с Linux'a на OS X, отбранив от основного проекта побочный продукт под названием "NTFS-3G project", в настоящее время поддерживающий Mac OS X, FreeBSD, NetBSD, BeOS и Haiku.

Последнюю версию драйвера, датируемую 17 июня 2007 года (вместе с исходными текстами и документацией, разумеется) можно бесплатно скачать с сайта <http://www.ntfs-3g.org>, однако, возможно, что ничего скачивать и не потребуется, поскольку, некоторые дистрибутивы (как, например, PC-BSD), уже включают в себя NTFS-3G драйвер (естественно, "второй" или даже "третьей" свежести).

Монтирование диска может осуществляться как командой mount (см. листинг 4), так и непосредственно самой утилитой ntfs-3g (см. листинг 5):

```
# mount -t ntfs-3g /dev/hda1 /mnt/windows -o locale=hu_HU.utf8
```

Листинг 4 монтирование NTFS-разделов под xBSD командной mount

```
# ntfs-3g /dev/ntfs-test /mnt/ntfs
```

Листинг 5 монтирование NTFS-разделом под xBSD утилитой ntfs-3g

Кстати говоря, при попытке использования драйвера NTFS-3G под виртуальной машиной VMWare версии 5.0 и выше последняя кончает свою жизнь крахом, для преодоления которого достаточно добавить в .vmx файл следующую строку:

```
mainMem.useNamedFile=FALSE
```

Листинг 6 конфигурирование VMWare для поддержки NTFS-3G

Помимо описанной, существуют и другие проблемы, однако, все они описаны в документации, прилагаемой к драйверу NTFS-3G, которую следует прочитать до его установки, а не после, как это делает большинство.

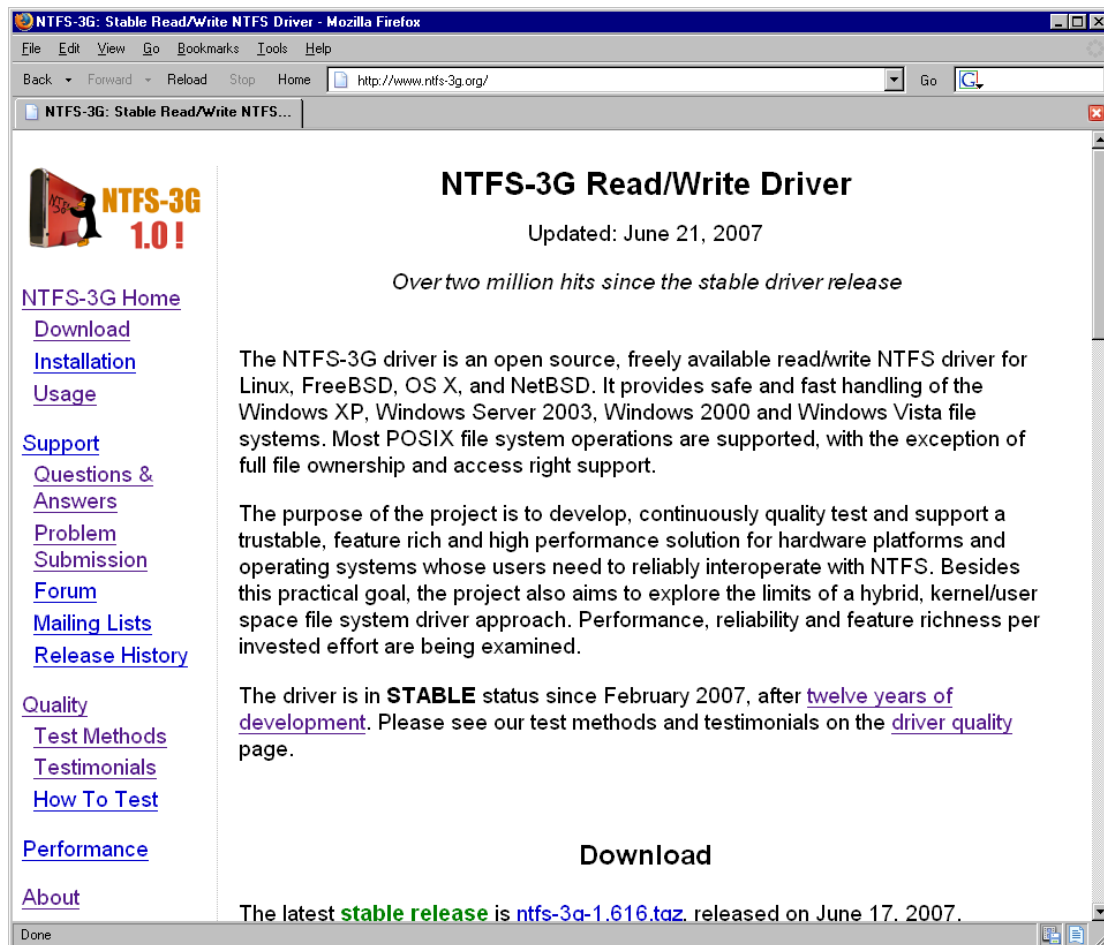


Рисунок 5 главная страничка проекта NTFS-3G Project

закключение

Microsoft, похоже, утратила к NTFS всякий интерес и, вопреки громким заявлениям о создании файловой системы нового поколения, Висла вышла с той же самой версий NTFS, что и XP. Благодаря этому обстоятельству, хакеры получили огромное преимущество, успев завершить расшифровку основных структур данных и выпустить открытые драйвера, поддерживающие более или менее полноценную работу с NTFS-разделами без угрозы потери данных.

>>> врезка меры предосторожности при записи на NTFS-разделы

- ❑ _перед_ записью данных на NTFS-раздел из Linux/BSD настоятельно рекомендуется загрузить Windows и запустить chkdsk, чтобы убедиться в отсутствии ошибок. дело в том, что штатный драйвер автоматически диагностирует дефекты файловой системы, блокируя запись до момента их исправления, а свободные драйвера — нет;
- ❑ _после_ удаления/перемещения большого количества файлов и/или каталогов из-под Linux/BSD обязательно загрузите Windows и запустите chkdsk, поскольку, свободные драйвера не учитывают ряд тонкостей NTFS, что ведет к накоплению мелких ошибок;
- ❑ при проверке тома, "пописанного" свободными NTFS-драйверами, chkdsk, как правило, выдает сообщения об ошибках, однако, это не повод для волнений. читайте документацию, прилагаемую к драйверу — в ней перечислены все не критичные ошибки и коротко описаны причины их появления;
- ❑ никогда, ни при каких обстоятельствах не монтируйте NTFS-раздел на запись, если работа Windows была завершена неправильно! в этом случае в журнале транзакций могут остаться одна или более записей, обеспечивающих "откат" при последующей загрузке операционной системы, однако, открытые драйвера все еще не поддерживают

транзакции, а последствия "отката" диска, на который уже что-то писалось непредсказуемы;

- раздел, хотя бы однажды заполненный более чем на 90% от своего объема, подвергается намного большему риску при монтировании на запись из-под Linux/BSD, поскольку, при этом происходит усечение области, зарезервированной под метаданные. свободные NTFS-драйвера обрабатывают эту ситуацию не совсем корректно;