NAME

ntfsrecover – Recover updates committed by Windows on an NTFS volume

SYNOPSIS

ntfsrecover [*options*] *device*

DESCRIPTION

ntfsrecover applies to the metadata the updates which were requested on Windows but could not be completed because they were interrupted by some event such as a power failure, a hardware crash, a software crash or the device being unplugged. Doing so, the file system is restored to a consistent state, however updates to user data may still be lost.

Updating the file system generally requires updating several records which should all be made for the file system to be kept consistent. For instance, creating a new file requires reserving an inode number (set a bit in a bit map), creating a file record (store the file name and file attributes), and registering the file in a directory (locate the file from some path). When an unfortunate event occurs, and one of these updates could be done but not all of them, the file system is left inconsistent.

A group of updates which have all to be done to preserve consistency is called a transaction, and the end of updates within a transaction is called the commitment of the transaction.

To protect from unfortunate events, Windows first logs in a special file all the metadata update requests without applying any, until the commitment is known. If the event occurs before the commitment, no update has been made and the file system is consistent. If the event occurs after the update, the log file can be analyzed later and the transactions which were committed can be executed again, thus restoring the integrity of the file system.

ntfsrecover similarly examines the log file and applies the updates within committed transactions which could not be done by Windows.

Currently, ntfs-3g does not log updates, so **ntfsrecover** cannot be used to restore consistency after an unfortunate event occurred while the file system was updated by Linux.

OPTIONS

Below is a summary of all the options that **ntfsrecover** accepts. The normal usage is to use no option at all, as most of these options are oriented towards developers needs.

Nearly all options have two equivalent names. The short name is preceded by **–** and the long name is preceded by **––**. Any single letter options, that don't take an argument, can be combined into a single command, e.g. **–bv** is equivalent to **–b –v**. Long named options can be abbreviated to any unique prefix of their name.

–b, **––backward**

Examine the actions described in the logfile backward from the latest one to the earliest one without applying any update. This may encompass records generated during several sessions, and when Windows is restarted, it often does not restart writing where it ended the previous session, so this leads to errors and bad sequencing when examining the full log file.

–c, **––clusters CLUSTER-RANGE**

Restrict the output generated when using options -b -f -u -p to the actions operating on a cluster within the given cluster range. CLUSTER-RANGE is defined by the first and last cluster numbers separated by a hyphen, for instance 100-109 or 0x3e8-0x3ff. A single number means restricting to a single cluster. The first four log blocks have a special role and they are always shown.

–f, **––forward NUM**

Examine the actions described in the logfile forward from the first one to the last one without applying any update. As the log file is reused circularly, the first one is generally not the earliest.

Moreover when Windows is restarted, it often does not restart writing where it ended the previous sessions, and this leads to errors when examining a log file generated during several sessions.

−h, **−−help**
Show some help information.

−k, **−−kill−fast−restart**
When Windows has been interrupted with fast restart mode activated, part of pending changes are kept in the Windows cache and only the same Windows version can recover them. This option can be used to apply the changes recorded in the log file and drop the ones in the Windows cache. This is dangerous and may cause loss of data.

−n, **−−no-action**
Do not apply any modification, useful when using the options -p, -s or -u.

−p, **−−play COUNT**
Undo COUNT transaction sets and redo a single one, a transaction set being all transactions between two consecutive checkpoints. This is useful for replaying some transaction in the past. As a few actions are not undoable, this is not always possible.

−r, **−−range BLOCK-RANGE**
Examine the actions described in the logfile forward restricted to the requested log file block range without applying any update. The first four log blocks have a special role and they are always examined.

−s, **−−sync**
Sync the file system by applying the committed actions which have not been synced previously. This is the default option, used when none of the options -n, -f, -r, -p and -u are present.

The option -s can be repeated to request applying the committed actions mentioned in the obsolete restart page. This is useful for testing the situations where the latest restart page cannot be read though it can actually be read.

−t, **−−transactions COUNT**
Display the transaction parameters when examining the log file with one of the options --forward, --backward or --range.

−u, **−−undo COUNT**
Undo COUNT transaction sets, thus resetting the file system to some checkpoint in the past, a transaction set being all transactions between two consecutive checkpoints. As a few actions are not undoable, this is not always possible.

−v, **−−verbose**
Display more debug/warning/error messages. This option may be used twice to display even more information.

−V, **−−version**
Show the version number, copyright and license of **ntfsrecover**.

EXAMPLES

Sync an NTFS volume on /dev/sda1.

```
ntfsrecover -s /dev/sda1
```

Display all actions which updated a cluster in range 100 to 119 :

```
ntfsrecover --verbose --backward --clusters=100-119 /dev/sda1
```

BUGS

If you find a bug please send an email describing the problem to the development team:
ntfs−3g−devel@lists.sf.net

AUTHORS

ntfsrecover was written by Jean-Pierre Andre

AVAILABILITY

ntfsrecover is part of the **ntfs-3g** package and is available from:
http://www.tuxera.com/community/

SEE ALSO

ntfs-3g(8), **ntfsfix**(8), **ntfsprogs**(8)