Rocky Enterprise Linux 9.2 Manual Pages on command 'ntfscat.8'

$ man ntfscat.8

NTFSCAT(8)   System Manager's Manual   NTFSCAT(8)

NAME

   ntfscat - print NTFS files and streams on the standard output

SYNOPSIS

   [options] device [file]

DESCRIPTION

   ntfscat will read a file or stream from an NTFS volume and display the contents on the

   standard output.

   The case of the filename passed to ntfscat is ignored.

OPTIONS

   Below is a summary of all the options that ntfscat accepts. 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 com?

   mand, e.g.   -fv is equivalent to -f -v. Long named options can be abbreviated to any

   unique prefix of their name.

   -a, --attribute TYPE

       Display the contents of a particular attribute type. By default, the unnamed $DATA

       attribute will be shown. The attribute can be specified by a number in decimal or

       hexadecimal, or by name.

       ??

       ?Hex   Decimal Name   ?

       ?0x10   16   "$STANDARD_INFORMATION" ?

       ?0x20   32   "$ATTRIBUTE_LIST"   ?

```
?0x30   48      "$FILE_NAME"            ?
?0x40   64      "$OBJECT_ID"            ?
?0x50   80      "$SECURITY_DESCRIPTOR"  ?
?0x60   96      "$VOLUME_NAME"          ?
?0x70   112     "$VOLUME_INFORMATION"   ?
?0x80   128     "$DATA"                 ?
?0x90   144     "$INDEX_ROOT"           ?
?0xA0   160     "$INDEX_ALLOCATION"     ?
?0xB0   176     "$BITMAP"               ?
?0xC0   192     "$REPARSE_POINT"        ?
?0xD0   208     "$EA_INFORMATION"       ?
?0xE0   224     "$EA"                   ?
?0xF0   240     "$PROPERTY_SET"         ?
?0x100  256     "$LOGGED_UTILITY_STREAM" ?
????????????????????????????????????????????????
```

Notes The attribute names may be given without the leading $ symbol.

If you use the $ symbol, you must quote the name to prevent the shell interpreting

the name.

-n, --attribute-name NAME

Display this named attribute, stream.

-i, --inode NUM

Specify a file by its inode number instead of its name.

-f, --force

This will override some sensible defaults, such as not using a mounted volume. Use

this option with caution.

-h, --help

Show a list of options with a brief description of each one.

-q, --quiet

Suppress some debug/warning/error messages.

-V, --version

Show the version number, copyright and license ntfscat.

-v, --verbose

Display more debug/warning/error messages.

EXAMPLES

Display the contents of a file in the root of an NTFS volume.

    ntfscat /dev/hda1 boot.ini

Display the contents of a file in a subdirectory of an NTFS volume.

    ntfscat /dev/hda1 /winnt/system32/drivers/etc/hosts

Display the contents of the $INDEX_ROOT attribute of the root directory (inode 5).

    ntfscat /dev/hda1 -a INDEX_ROOT -i 5 | hexdump -C

BUGS

There are no known problems with ntfscat. If you find a bug please send an email describ?

ing the problem to the development team:

ntfs-3g-devel@lists.sf.net

AUTHORS

ntfscat was written by Richard Russon, Anton Altaparmakov and Szabolcs Szakacsits. It was

ported to ntfs-3g by Erik Larsson.

AVAILABILITY

ntfscat is part of the ntfs-3g package and is available from:

https://github.com/tuxera/ntfs-3g/wiki/

SEE ALSO

Read libntfs(8) for details how to access encrypted files.

libntfs(8), ntfsls(8), ntfsprogs(8)

ntfs-3g 2021.8.22   September 2007   NTFSCAT(8)