

NAME**nafscii** – NetSA Aggregated Flow printer**SYNOPSIS**

```
nafscii      [--in INPUT_SPECIFIER] [--out OUTPUT_SPECIFIER]
              [--nextdir PROCESSED_INPUT_DIRECTORY]
              [--faildir FAILED_INPUT_DIRECTORY]
              [--poll POLLING_DELAY] [--lock]
              [--log LOG_SPECIFIER] [--loglevel LOG_LEVEL]
              [--verbose] [--version] [--daemon] [--foreground]
```

DESCRIPTION

nafscii takes NAF aggregated flow format files as input, and prints their contents as human-readable, white-space-separated ASCII text. This textual output can then be used for human analysis, or as input to the wide variety of numerical analysis and data management tools that understand whitespace-delimited ASCII data.

nafscii, like all NAF tools, operates by default in **once** mode, though it can also be run as a **daemon**. In daemon mode, **nafscii** will wait for new input to match its input specifier, and move processed input to the **—nextdir** directory. This can be used to build “chains” of daemons for automated batch processing of flow data.

OPTIONS**Input Options**

The input specifier determines where **nafscii** will read its input from. **nafscii** defaults to reading from standard input.

—in *INPUT_SPECIFIER*

INPUT_SPECIFIER is an input specifier. This is a filename, a directory name, a file glob pattern (in which case it should be escaped or quoted to prevent the shell from expanding the glob pattern), or the string **–** to read from standard input.

Output Options

The output specifier determines where **nafscii** will write its output. The output specifier is optional. If reading standard input, output defaults to standard output. If reading from files on disk, output defaults to one file per input file, named as the input file in the same directory as the input file with a **.txt** extension.

—out *OUTPUT_SPECIFIER*

OUTPUT_SPECIFIER is an output specifier. If present, this should be a filename or a directory name, or the string **–** to write to standard output.

Daemon Options

These options are used to run **nafscii** in daemon mode for batch processing of packet and flow files.

—daemon

Run **nafscii** in daemon mode. Instead of processing its input then exiting, **nafscii** will continually look for new input matching its input specifier. This will cause **nafscii** to fork into the background and exit.

—foreground

Instead of forking in **—daemon** mode, stay in the foreground. Useful for debugging.

—lock

Use lockfiles for concurrent file access protection. Highly recommended in **—daemon** mode, especially if two NAF daemons are interacting through a given directory.

—poll *POLLING_DELAY*

POLLING_DELAY is the polling delay in seconds; how long **nafscii** will wait for new input when none is available. The default is 60 seconds.

---nextdir PROCESSED_INPUT_DIRECTORY

When reading from files, if this option is present, input files will be moved to *PROCESSED_INPUT_DIRECTORY* after they are successfully processed. The special string **delete** will cause successfully processed input to be removed instead. This option is required in daemon mode.

---faildir FAILED_INPUT_DIRECTORY

When reading from files, if this option is present, input files will be moved to *FAILED_INPUT_DIRECTORY* if processing failed. The special string **delete** will cause failed input to be removed instead. This option is required in daemon mode.

Logging Options

These options are used to specify how log messages are routed. *nafalizer* can log to standard error, regular files, or the UNIX syslog facility.

---log LOG_SPECIFIER

Specifies destination for log messages. *LOG_SPECIFIER* can be a *syslog* (3) facility name, the special value **stderr** for standard error, or the *absolute* path to a file for file logging. Standard error logging is only available in **---daemon** mode if **---foreground** is present. The default log specifier is **stderr** if available, **user** otherwise.

---loglevel LOG_LEVEL

Specify minimum level for logged messages. In increasing levels of verbosity, the supported log levels are **quiet**, **error**, **critical**, **warning**, **message**, **info**, and **debug**. The default logging level is **warning**.

---verbose

Equivalent to **---loglevel debug**.

---version

If present, print version and copyright information to standard error and exit.

OUTPUT FORMAT

nafscii writes its output in whitespace-delimited ASCII, with one line per record. Each column is separated by at least one whitespace character, and whitespace is forbidden within each column's content. The first line of each output file is a column header. Each column, if present, appears in the following order and has the format described:

date

Date of start of bin, UTC, in *YYYY-MM-DD* (ISO 8601) format.

time

Time of start of bin, UTC, in *hh:mm:ss* (ISO 8601) format.

source

Flow source identifier, from source flow data or **---sid** argument to *nafalizer* (1). The source identifier is printed in hexadecimal format.

sip

Source IP address in dotted-quad format, followed by mask prefix length in CIDR notation, if present. If the mask prefix length is 32, it is omitted along with its preceding slash. If the mask prefix length is 0, the source address is not printed at all.

dip

Destination IP address in dotted-quad format, followed by mask prefix length in CIDR notation, if present. If the mask prefix length is 32, it is omitted along with its preceding slash. If the mask prefix length is 0, the destination address is not printed at all.

sp

Source port in decimal format.

dp

Destination port in decimal format, or ICMP type and code (see **ICMP Type and Code** in *nafalizer* (1)).

proto

IP protocol identifier in decimal format.

shosts

Distinct source host count per record.

dhosts

Distinct destination host count per record.

sports

Distinct source port count per record.

dports

Distinct destination port count per record.

flo Forward flow count in decimal format.

rflo Reverse flow count in decimal format.

pkt Forward packet count in decimal format.

rpkt

Reverse packet count in decimal format.

oct Forward octet count in decimal format.

roct

Reverse octet count in decimal format.

Note again that if a column is not present in the NAF input data, that is, if it was not present in the *nafalize* (1) aggregation expression, it will not appear in the printed output.

SIGNALS

nafscii responds to **SIGINT** or **SIGTERM** by terminating input processing, and exiting.

BUGS

Known issues are listed in the **README** file in the NAF tools source distribution. Note that NAF should be considered alpha-quality software; not every conceivable input and aggregation is exhaustively tested at each release, and specific features may be completely untested. Please be mindful of this before deploying NAF in production environments. Bug reports and feature requests may be sent directly to the author, Brian Trammell, via email at <bht@cert.org>.

AUTHORS

Brian Trammell <bht@cert.org>, for the CERT Network Situational Awareness Group,
<http://www.cert.org/netsa>.

SEE ALSO

nafalize (1), *nafilter* (1)