NAME

netchecker — keep a watch at established connections

SYNOPSIS

netchecker [**-1**] [**-c**] [**-D**] [**-d**] [**-E** *filename*] [**-e**] [**-g**] [**-i**] [**-L**] [**-n**]
[**-o** *filename*] [**-P**] [**-p** *hostname*] [**-q**] [**-R** *time*] [**-r**] [**-s**]
[**-t** *timer*] [**-v**] *conffilename*

DESCRIPTION

Given a configuration file and the output of the netstat(1) utility, **netchecker** will detect missing connections and established connections that should not at this time.

If a condition is realized, depending of the options used, **netchecker** will notify the end user using syslog(3) with LOG_ERR priority (with **-s**), sending UDP datagram to a given host (with **-p** but no **-d**), writing to standard output (with **-d**) or to a file (with **-d** and **-o**).

The **netchecker** utility need to get information from netstat(1) or lsof(1) utilities. With **-P** (Linux only), it reads /proc/net/tcp directly. This output is obtained using "/usr/bin/netstat -p tcp" on FreeBSD, "/usr/bin/netstat -P tcp" on Solaris and Linux. When in lsof(1) mode, output is obtained using "/files/misc/bin/lsof -sli TCP". Otherwise, you can adapt the code to your wish.

The following options are available:

-1 Run once then quit.

-c Display configuration file then quit.

-D Dump netstat(1) output line by line. Use **-o** *filename* to redirect output to *filename* instead of stdout.

-d Add more debugging information (multiple **-d** are allowed to increase verbosity). Notifications over network are disabled.

-E *filename*
Read sockets to exclude from the file *filename*. They will simply be ignored by the program. The regex(3) interface will be used for the search. This option is only of interest when **-e** is set (using command line option or directive in configuration file).

-e Detect established sockets that are not in configuration file *conffilename*, nor in the list of excluded sockets (if **-E** or *#excluded_rule* is used).

-g Guess dot. Both : and . are considered as dot.

-i Output compatible with itrs(1) third party software. Use this option for testing purpose.

-L Turn on lsof(1) mode. Pid of process that created the socket is displayed.

-n Numerical addresses for host, port or user names (netstat -n).

-o *filename*
Send output to *filename* instead of stdout.

-P On Linux, read information from /proc/net/tcp.

-p *hostname*
Send UDP datagram to *hostname*.

-q Quiet output if level=0.

-R *time*
: Run until *time* (in HHMM format) and display informations about connections. This will help getting a configuration file.

-r
: Use `regex`(3) interface to compare hosts and ports. Otherwise, a simplier matching is done, with a * character replacing one or many other characters.

-s
: Notify the end user using `syslog`(3) with `LOG_ERR` priority.

-t *timer*
: Rescan every *timer* second (default 30), if **-1** is not set.

-v
: Print version and exit.

CONFIGURATION FILE

The configuration is a text file with space separated fields. Each position references a field:

- starting time in HHMM format
- ending time in HHMM format
- options in a comma separated list of *tag=value* pairs, space not allowed
- dot separated source host and port. Use the **-r** option to change how matching is done
- dot separated destination host and port. Use the **-r** option to change how matching is done

A common configuration file:

```
#
#
0000 2400 level=100 myhost.* myhost.6000
```

The options are:

- *category=string*, this option can be used to assign categories to configuration lines

  ```
  0000 2400 level=100,category=X11 myhost.* myhost.6000
  ```

- *comment="this is a comment"*, this option can be used to differenciate configuration lines in addition to the **-i** command line option. The first character, the comment delimiter, is required to mark the end but can be escaped at any other position

  ```
  0000 2400 level=100,comment="X server" myhost.* myhost.6000
  ```

- *delay=number*, this option will give connections a delay of *number* minutes relative to starting time before being found as missing

- *level=number*, this option was made to indicate severity from 0 to 100, CRITICAL if above 50, WARNING if above 20 and STANDBY otherwise but this option is just used with **-i** command line option. If number is 0, no error will be output concerning this line, this is useful to allow zero or more connections. If number is 0 and **-q** is used, output concerning this line will be suppressed. Default is 90

- *weekday=7digitsbinarynumber*, this option hides the line for given days in a week. For example, 0111101 refers to Sunday and Friday

- *pidfile=/path/to/file.pid*, this option can be used to indicate the pid file associated with the process the connection belongs to. This is useful when the pid is collected as in `lsof`(1) mode

- *probehost=hostname*, this option can be used to add a probehost for this configuration line only, in addition to the **-p** command line option

- *repeat=number*, this option will replace the need to write the exact same line

Unless escaped, the # character is considered as starting a comment. All characters until the end of the line are removed.

There are also directives you can add to your configuration file, starting at column 1. These directives can override equivalent command line options:

- *#category string*, same as previous description but applies to all lines in the config file
- *#catprocmode_flag 0* or *#catprocmode_flag off Ns*, (Linux only) use it to disable the **-P** command line option
- *#catprocmode_flag 1* or *#catprocmode_flag on Ns*, (Linux only) use /proc/net/tcp directly to get information. same as using **-P** command line option
- *#excluded_flag 0* or *#excluded_flag off*, use it to disable the **-e** command line option
- *#excluded_flag 1* or *#excluded_flag on*, same as using **-e** command line option
- *#excluded_rule entry*, add this *entry* to the list of excluded sockets. This directive is only of interest when **-e** is set (using command line option or directive in configuration file)

  ```
  # do not check local sockets on this host
  #excluded_flag on
  #excluded_rule localhost/.*=localhost/.*
  ```

- *#lsofmode_flag 1* or *#lsofmode_flag on*, same as using **-L** command line option
- *#numeric_flag 1* or *#numeric_flag on*, same as using **-n** command line option
- *#numeric_flag 0* or *#numeric_flag off*, use it to disable the **-n** command line option
- *#probehost hostname*, send UDP datagram to this host, this directive is equivalent to the **-p** *hostname* command line option
- *#sockets number*, this option will detect an important number of sockets. The parameter *number* is the number of sockets. Default is 100
- *#weekday 7digitsbinarynumber*, same as previous description but applies to all lines in the config file
- *#quiet_flag 1* or *#quiet_flag on*, same as using **-q** command line option
- *#quiet_flag 0* or *#quiet_flag off*, use it to disable the **-q** command line option
- *#regex_flag 1* or *#regex_flag on*, use regex(3) interface to compare hosts and ports, this directive override **-r** command line option

BUGS

Ordering lines in configuration file is important because the first match is chosen according to host name and port.

SEE ALSO

netstat(1), regex(3), syslog(3)

AUTHORS

The **netchecker** utility and this manual page were written by Philippe Charnier ⟨charnier@xp11.frmug.org⟩.