NAME

fail2ban-regex - test Fail2ban "failregex" option

SYNOPSIS

fail2ban-regex [*OPTIONS*] <*LOG*> <*REGEX*> [*IGNOREREGEX*]

DESCRIPTION

Fail2Ban reads log file that contains password failure report and bans the corresponding IP addresses using firewall rules.

This tools can test regular expressions for "fail2ban".

LOG:

string
: a string representing a log line

filename
: path to a log file (*/var/log/auth.log*)

systemd-journal
: search systemd journal (systemd-python required), optionally with backend parameters, see ‘man jail.conf‘ for usage and examples (systemd-journal[journalflags=1]).

REGEX:

string
: a string representing a ’failregex’

filter
: name of filter, optionally with options (sshd[mode=aggressive])

filename
: path to a filter file (filter.d/sshd.conf)

IGNOREREGEX:

string
: a string representing an ’ignoreregex’

filename
: path to a filter file (filter.d/sshd.conf)

OPTIONS

--version
show program’s version number and exit

-h, **--help**
show this help message and exit

-c CONFIG, **--config**=*CONFIG*
set alternate config directory

-d DATEPATTERN, **--datepattern**=*DATEPATTERN*
set custom pattern used to match date/times

--timezone=*TIMEZONE*, **--TZ**=*TIMEZONE*
set time-zone used by convert time format

-e ENCODING, **--encoding**=*ENCODING*
File encoding. Default: system locale

-r, **--raw**
Raw hosts, don’t resolve dns

--usedns=*USEDNS*
DNS specified replacement of tags <HOST> in regexp (’yes’ - matches all form of hosts, ’no’ - IP addresses only)

-L MAXLINES, **--maxlines**=*MAXLINES*
maxlines for multi-line regex.

-m JOURNALMATCH, **--journalmatch**=*JOURNALMATCH*
journalctl style matches overriding filter file. "systemd-journal" only

-l LOG_LEVEL, **--log-level**=*LOG_LEVEL*
Log level for the Fail2Ban logger to use

-V get version in machine-readable short format

-v, **--verbose**
Increase verbosity

--verbosity=*VERBOSE*
Set numerical level of verbosity (0..4)

--verbose-date, **--VD**
Verbose date patterns/regex in output

-D, **--debuggex**
Produce debuggex.com urls for debugging there

--no-check-all
Disable check for all regex's

-o OUT, **--out**=*OUT*
Set token to print failure information only (row, id, ip, msg, host, ip4, ip6, dns, matches, ...)

--print-no-missed
Do not print any missed lines

--print-no-ignored
Do not print any ignored lines

--print-all-matched
Print all matched lines

--print-all-missed
Print all missed lines, no matter how many

--print-all-ignored
Print all ignored lines, no matter how many

-t, **--log-traceback**
Enrich log-messages with compressed tracebacks

--full-traceback
Either to make the tracebacks full, not compressed (as by default)

AUTHOR

Written by Cyril Jaquier <cyril.jaquier@fail2ban.org>. Many contributions by Yaroslav O. Halchenko, Steven Hiscocks, Sergey G. Brester (sebres).

REPORTING BUGS

Report bugs to https://github.com/fail2ban/fail2ban/issues

COPYRIGHT

SEE ALSO

fail2ban-client(1) fail2ban-server(1) fail2ban-jail.conf(5)