

NAME

ragrep – grep **argus(8)** user captured data.

COPYRIGHT

Copyright (c) 2000-2012 QoSient. All rights reserved.

SYNOPSIS

ragrep [**options**] **-e** *pattern* [**raoptions**] [**-** *filter-expression*]

ragrep [**options**] **-f** *file* [**raoptions**] [**-** *filter-expression*]

DESCRIPTION

Ragrep reads **argus** data from an *argus-data* source, greps the records based on the regexp specified on the command line, and outputs a valid *argus-stream*.

Ragrep works only on the fields for user captured data. Argus must be started with the configuration option **ARGUS_CAPTURE_DATA_LEN** set to a value greater than 0, to have these data captured. See **argus.conf(5)** for detail.

Ragrep is based on GNU **grep(1)**, so the *regexp* syntax is the same as for **grep(1)**.

OPTIONS

Ragrep, like all ra based clients, supports a number of **ra options** including filtering of input argus records through a terminating filter expression. See **ra(1)** for a complete description of **ra options**. **ragrep(1)** specific options are:

-c Suppress normal output; instead print a count of matching lines for each input file. With the **-v**, **--invert-match** option (see below), count non-matching lines.

-e <regex>

Match regular expression in flow user data fields. Prepend the regex with either "s:" or "d:" to limit the match to either the source or destination user data fields. Examples include:

"^SSH-" - Look for ssh connections on any port.

"s:^GET" - Look for HTTP GET requests in the source buffer.

"d:^HTTP.*Unauth" - Find unauthorized http response.

-f FILE

Obtain patterns from *FILE*, one per line. The empty file contains zero patterns, and therefore matches nothing.

-i Ignore case distinctions in both the *PATTERN* and the input files.

-L Suppress normal output; instead print the name of each input file from which no output would normally have been printed. The scanning will stop on the first match.

-l Suppress normal output; instead print the name of each input file from which output would normally have been printed. The scanning will stop on the first match.

-q Quiet; do not write anything to standard output. Exit immediately with zero status if any match is found, even if an error was detected.

-R Read all files under each directory, recursively; this is equivalent to the **-d recurse** option.

-v Reverse the expression matching logic.

DIAGNOSTICS

Normally, exit status is 0 if selected records are found and 1 otherwise. But the exit status is 2 if an error occurred, unless the **-q** option is used and a selected line is found.

INVOCATION

A sample invocation of **ragrep(1)**. This call reads **argus(8)** data from **inputfile** and greps all http transactions that generated a "404 Not Found" error.

```
ragrep -r inputfile -e "HTTP.*404"
```

SEE ALSO

ra(1), **rarc(5)**, **argus(8)**,

FILES**AUTHORS**

Carter Bullard (carter@qosient.com).

BUGS