NAME

sudoreplay - replay sudo session logs

SYNOPSIS

sudoreplay [**-h**] [**-d** *directory*] [**-f** *filter*] [**-m** *max_wait*] [**-s** *speed_factor*] ID

sudoreplay [**-h**] [**-d** *directory*] **-l** [search expression]

DESCRIPTION

sudoreplay plays back or lists the output logs created by **sudo**. When replaying, **sudoreplay** can play the session back in real-time, or the playback speed may be adjusted (faster or slower) based on the command line options.

The *ID* should either be a six character sequence of digits and upper case letters, e.g. 0100A5, or a pattern matching the *iolog_file* option in the *sudoers* file. When a command is run via **sudo** with *log_output* enabled in the *sudoers* file, a TSID=ID string is logged via syslog or to the **sudo** log file. The *ID* may also be determined using **sudoreplay**'s list mode.

In list mode, **sudoreplay** can be used to find the ID of a session based on a number of criteria such as the user, tty or command run.

In replay mode, if the standard output has not been redirected, **sudoreplay** will act on the following keys:

' ' (space)	Pause output; press any key to resume.
'<'	Reduce the playback speed by one half.
'>'	Double the playback speed.

The options are as follows:

-d *directory* Use *directory* to for the session logs instead of the default, */var/log/sudo-io*.

-f *filter* By default, **sudoreplay** will play back the command's standard output, standard error and tty output. The **-f** option can be used to select which of these to output. The *filter* argument is a comma-separated list, consisting of one or more of following: *stdout*, *stderr*, and *ttyout*.

-h The **-h** (*help*) option causes **sudoreplay** to print a short help message to the standard output and exit.

-l [*search expression*]

Enable ''list mode''. In this mode, **sudoreplay** will list available sessions in a format similar to the **sudo** log file format, sorted by file name (or sequence number). If a *search expression* is specified, it will be used to restrict the IDs that are displayed. An expression is composed of the following predicates:

command *pattern*

Evaluates to true if the command run matches *pattern*. On systems with POSIX regular expression support, the pattern may be an extended regular expression. On systems without POSIX regular expression support, a simple substring match is performed instead.

cwd *directory*

Evaluates to true if the command was run with the specified current working directory.

fromdate *date*

Evaluates to true if the command was run on or after *date*. See *Date and time format* for a description of supported date and time formats.

group *runas_group*

Evaluates to true if the command was run with the specified *runas_group*. Note that unless a *runas_group* was explicitly specified when **sudo** was run this field will be empty in the log.

runas *runas_user*

Evaluates to true if the command was run as the specified *runas_user*. Note that **sudo** runs commands as user *root* by default.

todate *date*

Evaluates to true if the command was run on or prior to *date*. See *Date and time format* for a description of supported date and time formats.

tty *tty name*

Evaluates to true if the command was run on the specified terminal device. The *tty name* should be specified without the */dev/* prefix, e.g. *tty01* instead of */dev/tty01*.

user *user name*

Evaluates to true if the ID matches a command run by *user name*.

Predicates may be abbreviated to the shortest unique string (currently all predicates may be shortened to a single character).

Predicates may be combined using *and*, *or* and *!* operators as well as '(' and ')' grouping (note that parentheses must generally be escaped from the shell). The *and* operator is optional, adjacent predicates have an implied *and* unless separated by an *or*.

-m *max_wait* Specify an upper bound on how long to wait between key presses or output data. By default, **sudoreplay** will accurately reproduce the delays between key presses or program output. However, this can be tedious when the session includes long pauses. When the **-m** option is specified, **sudoreplay** will limit these pauses to at most *max_wait* seconds. The value may be specified as a floating point number, e.g. *2.5*.

-s *speed_factor*

This option causes **sudoreplay** to adjust the number of seconds it will wait between key presses or program output. This can be used to slow down or speed up the display. For example, a *speed_factor* of *2* would make the output twice as fast whereas a *speed_factor* of *.5* would make the output twice as slow.

-V The **-V** (*version*) option causes **sudoreplay** to print its version number and exit.

Date and time format

The time and date may be specified multiple ways, common formats include:

HH:MM:SS am MM/DD/CCYY timezone

24 hour time may be used in place of am/pm.

HH:MM:SS am Month, Day Year timezone

24 hour time may be used in place of am/pm, and month and day names may be abbreviated. Note that month and day of the week names must be specified in English.

CCYY-MM-DD HH:MM:SS

ISO time format

DD Month CCYY HH:MM:SS

The month name may be abbreviated.

Either time or date may be omitted, the am/pm and timezone are optional. If no date is specified, the current day is assumed; if no time is specified, the first second of the specified date is used. The less significant parts of both time and date may also be omitted, in which case zero is assumed.

The following are all valid time and date specifications:

now The current time and date.

tomorrow
Exactly one day from now.

yesterday
24 hours ago.

2 hours ago
2 hours ago.

next Friday
The first second of the next Friday.

this week
The current time but the first day of the coming week.

a fortnight ago
The current time but 14 days ago.

10:01 am 9/17/2009
10:01 am, September 17, 2009.

10:01 am
10:01 am on the current day.

10 10:00 am on the current day.

9/17/2009
00:00 am, September 17, 2009.

10:01 am Sep 17, 2009
10:01 am, September 17, 2009.

FILES

/var/log/sudo-io The default I/O log directory.

/var/log/sudo-io/00/00/01/log Example session log info.

/var/log/sudo-io/00/00/01/stdin
Example session standard input log.

/var/log/sudo-io/00/00/01/stdout
Example session standard output log.

/var/log/sudo-io/00/00/01/stderr
Example session standard error log.

/var/log/sudo-io/00/00/01/ttyin
Example session tty input file.

/var/log/sudo-io/00/00/01/ttyout
Example session tty output file.

/var/log/sudo-io/00/00/01/timing
Example session timing file.

Note that the *stdin*, *stdout* and *stderr* files will be empty unless **sudo** was used as part of a pipeline for a particular command.

EXAMPLES

List sessions run by user *millert*:

```
# sudoreplay -l user millert
```

List sessions run by user *bob* with a command containing the string vi:

```
# sudoreplay -l user bob command vi
```

List sessions run by user *jeff* that match a regular expression:

```
# sudoreplay -l user jeff command '/bin/[a-z]*sh'
```

List sessions run by jeff or bob on the console:

```
# sudoreplay -l ( user jeff or user bob ) tty console
```

SEE ALSO

sudo(8), script(1)

AUTHORS

Todd C. Miller

BUGS

If you feel you have found a bug in **sudoreplay**, please submit a bug report at https://www.sudo.ws/sudo/bugs/

SUPPORT

Limited free support is available via the sudo-users mailing list, see https://www.sudo.ws/mailman/listinfo/sudo-users to subscribe or search the archives.

DISCLAIMER

sudoreplay is provided ''AS IS'' and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. See the LICENSE file distributed with **sudo** or https://www.sudo.ws/sudo/license.html for complete details.