



Red Hat Enterprise Linux Release 9.2 Manual Pages on 'sudoreplay.8' command

\$ man sudoreplay.8

SUDOREPLAY(8) BSD System Manager's Manual SUDOREPLAY(8)

NAME

sudoreplay ? replay sudo session logs

SYNOPSIS

sudoreplay [-FhnRS] [-d dir] [-f filter] [-m num] [-s num] ID

sudoreplay [-h] [-d dir] -l [search expression]

DESCRIPTION

sudoreplay plays back or lists the output logs created by sudo. When re? playing, sudoreplay can play the session back in real-time, or the play? back 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, a pattern matching the iolog_file option in the sudoers file, or a path name. Path names may be relative to the iolog_dir option in the sudoers file (unless overridden by the -d option) or fully qualified, beginning with a ?/? character. 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 input and output are connected to a ter? minal and the -n option is not specified, sudoreplay will operate inter?

actively. In interactive mode, sudoreplay will attempt to adjust the terminal size to match that of the session and write directly to the terminal (not all terminals support this). Additionally, it will poll the keyboard and act on the following keys:

?\n? or ?\r? Skip to the next replay event; useful for long pauses.

? ? (space) Pause output; press any key to resume.

?<? Reduce the playback speed by one half.

?>? Double the playback speed.

The session can be interrupted via control-C. When the session has finished, the terminal is restored to its original size if it was changed during playback.

The options are as follows:

-d dir, --directory=dir

Store session logs in dir instead of the default,
/var/log/sudo-io.

-f filter, --filter=filter

Select which I/O type(s) to display. By default, sudoreplay will display the command's standard output, standard error and tty output. The filter argument is a comma-separated list, consisting of one or more of following: stdin, stdout, stderr, ttyin, and ttyout.

-F, --follow

Enable ?follow mode?. When replaying a session, sudoreplay will ignore end-of-file and keep replaying until the log is complete. This can be used to replay a session that is still in progress, similar to ?tail -f?. An I/O log file is considered to be complete when the write bits have been cleared on the session's timing file. Note that versions of sudo prior to 1.9.1 do not clear the write bits upon completion.

-h, --help Display a short help message to the standard output and exit.

-l, --list [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 the POSIX extended regular expression pattern.

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.

host hostname

Evaluates to true if the command was run on the specified hostname.

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 speci-

fied 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.

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 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. A max_wait of zero or less will eliminate the pauses entirely.

-n, --non-interactive

Do not prompt for user input or attempt to re-size the terminal. The session is written to the standard output, not directly to the user's terminal.

-R, --no-resize

Do not attempt to re-size the terminal to match the terminal size of the session.

-S, --suspend-wait

Wait while the command was suspended. By default, sudoreplay will ignore the time interval between when the command was suspended and when it was resumed. If the -S option is specified, sudoreplay will wait instead.

-s, --speed 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, --version

Print the sudoreplay versions 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 speci?

fied, the first second of the specified date is used. The less signifi?

cant 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 Friday in the next (upcoming) week. Not to be confused with ?this Friday? which would match the Friday of the current week.

last week

The current time but 7 days ago. This is equivalent to ?a week ago?.

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.

Note that relative time specifications do not always work as expected.

For example, the ?next? qualifier is intended to be used in conjunction with a day such as ?next Monday?. When used with units of weeks, months, years, etc the result will be one more than expected. For example, ?next week? will result in a time exactly two weeks from now, which is probably not what was intended. This will be addressed in a future version of sudoreplay.

Debugging sudoreplay

sudoreplay versions 1.8.4 and higher support a flexible debugging frame?

work that is configured via Debug lines in the sudo.conf(5) file.

For more information on configuring sudo.conf(5), please refer to its manual.

FILES

/etc/sudo.conf Debugging framework configuration

/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/log.json`

Example session log info (JSON format).

`/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

`script(1)`, `sudo.conf(5)`, `sudo(8)`

AUTHORS

Many people have worked on sudo over the years; this version consists of code written primarily by:

Todd C. Miller

See the CONTRIBUTORS file in the sudo distribution

(<https://www.sudo.ws/contributors.html>) for an exhaustive list of people who have contributed to sudo.

BUGS

If you feel you have found a bug in sudoreplay, please submit a bug report at <https://bugzilla.sudo.ws/>

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/license.html> for complete details.

Sudo 1.9.5p2

May 18, 2020

Sudo 1.9.5p2