

NAME

aureport – a tool that produces summary reports of audit daemon logs

SYNOPSIS

aureport [*options*]

DESCRIPTION

aureport is a tool that produces summary reports of the audit system logs. The aureport utility can also take input from stdin as long as the input is the raw log data. The reports have a column label at the top to help with interpretation of the various fields. Except for the main summary report, all reports have the audit event number. You can subsequently lookup the full event with ausearch **-a event number**. You may need to specify start & stop times if you get multiple hits. The reports produced by aureport can be used as building blocks for more complicated analysis.

OPTIONS

-au, --auth

Report about authentication attempts

-a, --avc

Report about avc messages

--comm

Report about commands run

-c, --config

Report about config changes

-cr, --crypto

Report about crypto events

--debug

Write malformed events that are skipped to stderr.

--delete

When used with configuration, integrity, or MAC reports, only include delete or remove operations.

--eoe-timeout seconds

Set the end of event parsing timeout. See **end_of_event_timeout** in *auditd.conf(5)* for details. Note that setting this value will override any configured value found in */etc/auditd/auditd.conf*.

-e, --event

Report about events

--add When used with configuration, integrity, or MAC reports, only include add or create operations.

--escape option

This option determines if the output is escaped to make the content safer for certain uses. The options are *raw*, *tty*, *shell*, and *shell_quote*. Each mode includes the characters of the preceding mode and escapes more characters. That is to say *shell* includes all characters escaped by *tty* and adds more. *tty* is the default.

-f, --file

Report about files and af_unix sockets

--failed

Only select failed events for processing in the reports. The default is both success and failed events.

-h, --host

Report about hosts

- help** Print brief command summary
- i, --interpret**
Interpret numeric entities into text. For example, uid is converted to account name. The conversion is done using the current resources of the machine where the search is being run. If you have renamed the accounts, or don't have the same accounts on your machine, you could get misleading results.
- if, --input *file* | *directory***
Use the given *file* or *directory* instead of the logs. This is to aid analysis where the logs have been moved to another machine or only part of a log was saved. The path length is limited to 4064 bytes.
- input-logs**
Use the log file location from auditd.conf as input for analysis. This is needed if you are using aureport from a cron job.
- integrity**
Report about integrity events
- k, --key**
Report about audit rule keys
- l, --login**
Report about logins
- m, --mods**
Report about account modifications
- ma, --mac**
Report about Mandatory Access Control (MAC) events
- n, --anomaly**
Report about anomaly events. These events include NIC going into promiscuous mode and programs segfaulting.
- node *node-name***
Only select events originating from *node name* string for processing in the reports. The default is to include all nodes. Multiple nodes are allowed.
- nc, --no-config**
Do not include the CONFIG_CHANGE event. This is particularly useful for the key report because audit rules have key labels in many cases. Using this option gets rid of these false positives.
- p, --pid**
Report about processes
- r, --response**
Report about responses to anomaly events
- s, --syscall**
Report about syscalls
- success**
Only select successful events for processing in the reports. The default is both success and failed events.
- summary**
Run the summary report that gives a total of the elements of the main report. Not all reports have a summary.
- t, --log**
This option will output a report of the start and end times for each log.

--tty Report about tty keystrokes

-te, --end [*end-date*] [*end-time*]

Search for events with time stamps equal to or before the given end time. The format of end time depends on your locale. If the date is omitted, **today** is assumed. If the time is omitted, **now** is assumed. Use 24 hour clock time rather than AM or PM to specify time. An example date using the en_US.utf8 locale is 09/03/2009. An example of time is 18:00:00. The date format accepted is influenced by the LC_TIME environmental variable.

You may also use the word: **now**, **recent**, **this-hour**, **boot**, **today**, **yesterday**, **this-week**, **week-ago**, **this-month**, **this-year**. **Now** means starting now. **Recent** is 10 minutes ago. **Boot** means the time of day to the second when the system last booted. **Today** means now. **Yesterday** is 1 second after midnight the previous day. **This-week** means starting 1 second after midnight on day 0 of the week determined by your locale (see **localtime**). **Week-ago** means 1 second after midnight exactly 7 days ago. **This-month** means 1 second after midnight on day 1 of the month. **This-year** means the 1 second after midnight on the first day of the first month.

-tm, --terminal

Report about terminals

-ts, --start [*start-date*] [*start-time*]

Search for events with time stamps equal to or after the given end time. The format of end time depends on your locale. If the date is omitted, **today** is assumed. If the time is omitted, **midnight** is assumed. Use 24 hour clock time rather than AM or PM to specify time. An example date using the en_US.utf8 locale is 09/03/2009. An example of time is 18:00:00. The date format accepted is influenced by the LC_TIME environmental variable.

You may also use the word: **now**, **recent**, **this-hour**, **boot**, **today**, **yesterday**, **this-week**, **week-ago**, **this-month**, **this-year**. **Boot** means the time of day to the second when the system last booted. **Today** means starting at 1 second after midnight. **Recent** is 10 minutes ago. **Yesterday** is 1 second after midnight the previous day. **This-week** means starting 1 second after midnight on day 0 of the week determined by your locale (see **localtime**). **Week-ago** means starting 1 second after midnight exactly 7 days ago. **This-month** means 1 second after midnight on day 1 of the month. **This-year** means the 1 second after midnight on the first day of the first month.

-u, --user

Report about users

-v, --version

Print the version and exit

--virt Report about Virtualization events

-x, --executable

Report about executables

NOTE

The boot time option is a convenience function and has limitations. The time it calculates is based on time now minus /proc/uptime. If after boot the system clock has been adjusted, perhaps by ntp, then the calculation may be wrong. In that case you'll need to fully specify the time. You can check the time it would use by running:

```
date -d "'cut -f1 -d. /proc/uptime' seconds ago"
```

SEE ALSO

ausearch(8), **auditd(8)**, **auditd.conf(5)**.