journalctl (systemd logs)

Article URL
journalctl (systemd logs)

Author
SecurityHome.eu

Published: 05 November 2024

.

Â

The systemd journal is systemd's own logging system. It is equivalent to the syslog in the init system. It collects and stored kernel logging data, system log messages, standard output, and errors for various systemd services.
A Linux machine with systemd writes the logs to */var/log/journal*

directory.

journalctl allows to filter the logs based on time, service, severity and other things.

The config file is: */etc/systemd/journald.conf*

The journald.conf file shows the default values. So even if there is a # in front of the entries, it means those are the default settings being used. If you want to change anything, you remove the # from that line.

With the command journalctl you can see the logs. But is becomes interesting to use filters.

with -r (reverse) you see the latest logs first
journalctl -r

With -n (number) you can set the number of lines form the log
journalctl -n 25

Like with tail -f, the -f (follow) show the logs in real time. (ctrl+c to quit)
journalctl -f

Show only kernel messages with -k
journalctl -k

You can filter on a specific process.
example logs generated by ssh
journalctl -u ssh

Filter logs by time
journalctl --since "2024-01-01"
journalctl --since=yesterday --until=now
journalctl --since "2024-01-01 01:01:00" --until "2024-02-02"

you can change the timestamps to UTS with --utc
journalctl --utc

Filter logs based on UID, GID and PID
The journal logs can also be filtered on User ID (UID), Group ID (GID) and Process ID (PID).
journalctl _PID=4321

Show only errors in logs with journalctl
journalctl -p 3 -xb

* -p 3 : filter logs for priority 3 (which is error)

* -x : provides additional information on the log (if available)

* b : since last boot (which is the current session)

Priority Code
0 emerg
1 alert
2 crit
3 err
4 warning
5 notice
6 info
7 debug

You might get a surprise when you see the output:
journalctl --disk-usage
This show the diskspace used by the logs.
You can rotate the logs, this will mark the currently active journal logs as archive and create fresh new logs.
sudo journalctl --rotate

To free up space you have several options:
Clear journal log older than x days
sudo journalctl --vacuum-time=7d

Restrict logs to a certain size
sudo journalctl --vacuum-size=100M

Restrict number of archive log files
sudo journalctl --vacuum-files=3