journalctl Query the journal

CONCEPTS

The journal is a binary, indexed log. Filters narrow it before output, so combine them freely: different fields are ANDed.

Journal all entries
↓ `-b -u -p`
Filters boot, unit, priority
↓ `--since -g`
Time and text narrowed set
↓ `-o -n -r`
Output pager or stdout

Reading the system journal needs root or membership of the systemd-journal, adm or wheel group; otherwise you only see your own entries.

The journal is only kept across reboots if /var/log/journal exists (Storage=persistent or auto in journald.conf). Otherwise -b -1 has nothing.

SELECT ENTRIES

`journalctl -u <unit>`
Logs of a unit

`journalctl -b`
Current boot only

`journalctl -b -1`
Previous boot

`journalctl -k`
Kernel messages (dmesg)

`journalctl -t <name>`
Entries by syslog identifier

`journalctl --user-unit <unit>`
Logs of a user unit

`journalctl -I -u <unit>`
Latest invocation of a unit

`journalctl _PID=<pid>`
Match a process ID

`journalctl --user`
The user journal

TIME AND PRIORITY

`journalctl -p err`
Errors and worse

TIME AND PRIORITY (cont.)

`journalctl -p warning..err`
Priority range

`journalctl --since "<date>"`
From a point in time

`journalctl --until "<date>"`
Up to a point in time

`journalctl -S -1h`
Last hour

`journalctl -S today`
Since midnight

Priority levels

Name	Number
`emerg`	0
`alert`	1
`crit`	2
`err`	3
`warning`	4
`notice`	5
`info`	6
`debug`	7

SEARCH AND FOLLOW

`journalctl -f`
Follow new entries

`journalctl -f -u <unit>`
Follow one unit

`journalctl -n <num>`
Last N entries

`journalctl -g <regex>`
Search messages by pattern

`journalctl -e`
Open pager at the end

`journalctl -r`
Newest entries first

`journalctl --no-pager`
Print without a pager

`journalctl -x`
Add catalog explanations

OUTPUT

`journalctl -o json-pretty`
Entries as readable JSON

`journalctl -o json`
One JSON object per line

`journalctl -o cat`
Messages only

OUTPUT (cont.)

`journalctl -o short-iso`
ISO timestamps

`journalctl -o verbose`
Every field of each entry

Output modes

Mode	Use
`short`	Default, syslog-like
`cat`	Message text only
`verbose`	All fields
`json-pretty`	Debugging fields
`json`	Scripts and jq

FIELDS AND BOOTS

`journalctl --list-boots`
List recorded boots

`journalctl -b <id>`
A specific boot by ID

`journalctl -F <field>`
List values of a field

`journalctl <FIELD>=<value>`
Match any field exactly

DISK AND MAINTENANCE

`journalctl --disk-usage`
Total journal size

`sudo journalctl --vacuum-time=<time>`
Delete archives older than a time

`sudo journalctl --vacuum-size=<size>`
Shrink archives to a size

`sudo journalctl --rotate`
Rotate files now

Cap the journal permanently

```
# /etc/systemd/journald.conf.d/size.conf
[Journal]
SystemMaxUse=500M
MaxRetentionSec=1month
# then: sudo systemctl restart systemd-journald
```

RECIPES

Why did it fail?

```
systemctl status <unit>
journalctl -u <unit> -b -p warning -e
journalctl -I -u <unit> -x
```