Journalctl Cheat Sheet

by Igor Bugayov (airlove) via cheatography.com/38112/cs/11906/

Useful Switches

-f

Show new log entries as they are added.

example: **journalctl -u mysql.service -f**

-k

Show kernel messages.

example: Kernel logs from five boots ago; **journalctl -k -b -5**

-u

Show messages for specified systemd service.

example: **journalctl -u httpd -u apache2**

-b

Show current boot messages.

Logs from the last boot, use the **-1** modifier; to see boot logs from two boots ago, use **-2**; and so on. List system boots with: **journalctl --list-boots**

-r

Show the messages in reverse order; latest first.

-p

Show the messages by priority

example: **journalctl -p err**

Shows you all messages marked as error, critical, alert, or emergency.

Time Ranges

journalctl --since "1 hour ago"

Show journal messages logged within the last hour:

journalctl --since 09:00 --until "1 hour ago"

Show reports starting at 9:00 AM and continuing until an hour ago

Time Ranges (cont)

journalctl --since yesterday

Show journal messages logged since yesterday:

journalctl --since "2 days ago"

Show logged in the last two days

journalctl --since "2017-05-23 23:15:00" --until "2017-05-23 23:20:00"

All messages logged on or after the since parameter and logged on or before the until parameter will be shown:

*Hint: If components of the above format are left off, some defaults will be applied. For instance, if the date is omitted, the current date will be assumed. If the time component is missing, "00:00:00" (midnight) will be substituted. The seconds field can be left off as well to default to "00":

By Process, User, or Group ID

journalctl _PID=123

Show messages produced by a specific process ID:

*Hint: Find the PID for a specific service: **systemctl status** *SERVICE*

journalctl _UID=100

Show messages belonging to a specific user ID:

example: **journalctl _UID=100 _UID=200 --since today**

*Hint: You can find your user ID by typing: **id -u** *USERNAME*

journalctl _GID=800

Show messages belonging to a specific group ID:

By Priority

You can use either the priority name or its corresponding numeric value. In order of highest to lowest priority:

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

The above numbers or names can be used interchangeably with the **-p** option.
Selecting a priority will display messages marked at the specified level *and those above it.*

Access control and config

usermod -a -G adm *USER*

Add USER to adm group

* Hint: by default, Journal users can only watch their own logs, unless they are root or in the adm group.

nano /etc/systemd/journald.conf

Edit the journal config file

ForwardToConsole=yes TTYPath=/-dev/tty12

Forward the Journal to /dev/ttyX

*Hint: Add changes to journal config file

By **Igor Bugayov** (airlove)
cheatography.com/airlove/

Published 23rd May, 2017.
Last updated 25th May, 2017.

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com

Journalctl Cheat Sheet

by Igor Bugayov (airlove) via cheatography.com/38112/cs/11906/

Advanced Filtering

journalctl /usr/bin/bash

Show messages related to a specific executable, specify the full path to the executable

journalctl _HOSTNAME=myhost

Show messages for specified hostname.

journalctl _COMM=avahi-daemon

The name, the executable path, and the command line of the process the journal entry originates from

journalctl -F

The -F option can be used to show all of the available values for a given journal field.

journalctl _SE *<TAB>*

Tab completion works on fields

journalctl _SELINUX_CONTEXT= *<TAB>*

Tab completion also works on labels in fields

journalctl _SELINUX_CONTEXT=system_u:system_r:policykit_t:s0

Show messages logged under PolicyKit's security label.

For a full list of common, well-known fields, see the man page.

Output

Control the formatting of journal entries.

journalctl -o short

The default and generates an output that is mostly identical to the formatting of classic syslog files, showing one line per journal entry.

journalctl -o short-full

Very similar, but shows timestamps in the format --since= and --until= options

Output (cont)

journalctl -o verbose

Show the full-structured entry items with all fields.

journalctl -o json-pretty

Formats entries as JSON data structures, in multiple lines in order to make them more readable by humans.

journalctl -o export

Serializes the journal into a binary (but mostly text-based) stream suitable for backups and network transfer

Import the binary stream back into native journald format with journal-remote

By **Igor Bugayov** (airlove)
cheatography.com/airlove/

Published 23rd May, 2017.
Last updated 25th May, 2017.

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com