journalctl

journalctl command reports OS and system service logs by extracting them from the systemd journaling system.

systemd is the fairly recent approach to managing OS and system services in modern Linux distros, and as part of streamlining services it also improved the way reporting is done – standard and error logs are now managed by systemd journaling system that’s a centralised system queried by journalctl command.

IMPORTANT: journalctl requires root access

Just like standard users couldn’t access OS and system service logs prior to systemd implementation, they still can’t with systemd.
You therefore must use `journalctl` with `sudo`:

```
$ sudo journalctl
-- Logs begin at Thu 2020-01-02 04:11:57 GMT, end at Tue 2020-01-14 11:47:26 GMT. --
Jan 02 04:11:57 srv sshd[4997]: Received disconnect from 192.241.210.224 port 50532: Bye Bye [preauth]
Jan 02 04:11:57 srv sshd[4997]: Disconnected from invalid user bognar 192.241.210.224 port 50532 [preauth]
Jan 02 04:12:05 srv sshd[5000]: Invalid user thisner from 133.130.117.173 port 41826
Jan 02 04:12:05 srv sshd[5000]: pam_unix(sshd:auth): check pass; user unknown
Jan 02 04:12:05 srv sshd[5000]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=133.130.117.173
Jan 02 04:12:07 srv sshd[5000]: Failed password for invalid user thisner from 133.130.117.173 port 41826 ssh2
Jan 02 04:12:08 srv sshd[5000]: Received disconnect from 133.130.117.173 port 41826: Bye Bye [preauth]
Jan 02 04:12:08 srv sshd[5000]: Disconnected from invalid user thisner 133.130.117.173 port 41826 [preauth]
Jan 02 04:12:10 srv sshd[5002]: Invalid user quiller from 117.121.97.115 port 13105
Jan 02 04:12:10 srv sshd[5002]: pam_unix(sshd:auth): check pass; user unknown
```

Reverse `journalctl` logs

As you noticed from previous example, by default `journalctl` starts showing oldest logs it has. This may not be very useful.

Here’s how to make `journalctl` show the latest (most recent)
logs instead: use -r option (-r for reverse).

greys@srv:~ $ sudo journalctl -r
   -- Logs begin at Thu 2020-01-02 04:11:57 GMT, end at Tue 2020-01-14 11:55:08 GMT. --
   Jan 14 11:55:08 srv sudo[1071]: pam_unix(sudo:session): session opened for user root by greys(uid=0)
   Jan 14 11:55:08 srv sudo[1071]:    greys : TTY=pts/0 ; PWD=/home/greys ; USER=root ; COMMAND=/bin/journalctl -r
   Jan 14 11:54:45 srv sshd[1069]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser=
       rhost=49.88.112.75  user=root
   Jan 14 11:54:45 srv sshd[1069]: Disconnected from authenticating user root 49.88.112.75 port 26947 [preauth]
   Jan 14 11:54:45 srv sshd[1069]: Received disconnect from 49.88.112.75 port 26947:11: [preauth]
   Jan 14 11:54:42 srv sshd[1069]: Failed password for root from 49.88.112.75 port 26947 ssh2
   Jan 14 11:54:38 srv sshd[1069]: Failed password for root from 49.88.112.75 port 26947 ssh2
   Jan 14 11:54:35 srv sshd[1069]: Failed password for root from 49.88.112.75 port 26947 ssh2
   Jan 14 11:54:33 srv sshd[1069]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
       rhost=49.88.112.75  user=root
   Jan 14 11:54:25 srv sshd[1067]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser=
       rhost=222.186.52.189  user=root
   Jan 14 11:54:25 srv sshd[1067]: Disconnected from authenticating user root 222.186.52.189 port 62050 [preauth]
   Jan 14 11:54:25 srv sshd[1067]: Received disconnect from 222.186.52.189 port 62050:11: [preauth]
   Jan 14 11:54:25 srv sshd[1067]: Failed password for root from 222.186.52.189 port 62050 ssh2
See Also

- `systemctl command`
- `Linux commands`
- `systemd reference`