

# Journal

- Indexed
- Formatted
  - Errors in red
  - Warnings in bold
- Security
- Reliability
- Intelligently rotated

<http://0pointer.de/blog/projects/journalctl.html>

# Journal

- Does not replace rsyslog in RHEL 7
  - rsyslog is enabled by default
- The journal is not persistent by default.
  - Enable persistence: ``mkdir /var/log/journal``
- Stored in key-value pairs
  - `journalctl [tab] [tab]`
  - Man 7 `systemd.journal-fields`
- Collects event metadata along with the message
- Simple to filter
  - Interleave units, binaries, etc.

# Journal – journalctl

```
root@host151:~  
File Edit View Search Terminal Help  
Oct 28 15:04:58 host151.local chronyd[329]: System clock wrong by -31.975399 seconds, adjustment  
Oct 28 15:04:26 host151.local chronyd[329]: System clock was stepped by -31.975 seconds  
Oct 28 15:04:26 host151.local systemd[1]: Time has been changed  
Oct 28 15:04:52 host151.local systemd[1]: Starting Stop Read-Ahead Data Collection...  
Oct 28 15:04:52 host151.local systemd[1]: Started Stop Read-Ahead Data Collection.  
Oct 28 15:05:32 host151.local chronyd[329]: Selected source 174.133.168.194  
Oct 28 15:06:08 host151.local sshd[2040]: Accepted password for root from 192.168.122.1 port 4512  
Oct 28 15:06:08 host151.local systemd[1]: Starting user-0.slice.  
Oct 28 15:06:08 host151.local systemd[1]: Created slice user-0.slice.  
Oct 28 15:06:08 host151.local systemd[1]: Starting User Manager for 0...  
Oct 28 15:06:08 host151.local systemd[1]: Starting Session 1 of user root.  
Oct 28 15:06:08 host151.local systemd[1]: Started Session 1 of user root.  
Oct 28 15:06:08 host151.local systemd-logind[322]: New session 1 of user root.  
Oct 28 15:06:08 host151.local sshd[2040]: pam_unix(sshd:session): session opened for user root by  
Oct 28 15:06:08 host151.local systemd[2044]: pam_unix(systemd-user:session): session opened for u  
Oct 28 15:06:08 host151.local systemd[2044]: Failed to open private bus connection: Failed to con  
Oct 28 15:06:08 host151.local systemd[2044]: Mounted /sys/kernel/config.  
Oct 28 15:06:08 host151.local systemd[2044]: Stopped target Sound Card.  
Oct 28 15:06:08 host151.local systemd[2044]: Starting Default.  
Oct 28 15:06:08 host151.local systemd[2044]: Reached target Default.  
Oct 28 15:06:08 host151.local systemd[2044]: Startup finished in 11ms.  
Oct 28 15:06:08 host151.local systemd[1]: Started User Manager for 0.  
lines 962-983/983 (END)
```

# Using the Journal

- Tail the journal: ``journalctl -f``
- Show X number of lines: ``journalctl -n 50``
- View from boot: ``journalctl -b``
- Filter by priority: ``journalctl -p [level]``

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

# Using the Journal

- Other useful filters:
  - -r reverse order
  - -u [unit]
  - binary e.g. /usr/sbin/dnsmasq [additional binaries]
  - --since=yesterday or YYYY-MM-DD (HH:MM:SS)
  - --until=YYYY-MM-DD
- View entire journal
  - journalctl -o verbose (useful for grep)