Journal

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

redhat.

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

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

redhat.

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)