# systemd: journal

Die „Logfiles“ im systemd sind eine binäre Datenbank mit umfassenden Suchwerkzeugen

- contra
  - kein KISS Design
  - schlechte post-mortem Analyse
  - nicht mehr kompatibel zu alten Logauswertungen (z.B. logwatch)
- pro
  - Metainfos nicht mehr fälschbar (weil vom daemon)
  - Außerhalb des laufenden systemd-journald nicht mehr fälschbar (hash)
  - wartungsfrei (kein logrotate)
  - kann applikationsspezifische Werte aufnehmen
  - umfangreiche Abfragemöglichkeiten

## Files

- `/var/log/journal/<machine-id>` ← persistent
- `/run/systemd/journal/<machine-id>` ← dynamisch

Die `machine-id` steht in `/etc/machine-id` und wird automatisch generiert oder mit `systemd-machine-id-setup`. `/var/lib/dbus/machine-id` beachten. Man kann eine Generierung erzwingen, indem man die Datei trunkiert

```
> /etc/machine-id
rm /var/lib/dbus/machine-id
```

[1)].

Das Verzeichnis `/var/log/journal` muss vorhanden sein; systemd loggt andernfalls nur temporär.

## journalctl

gleich ans Ende springen

```
journalctl -e
```

follow file mit allem und catalog

```
journalctl -f -a -x
```

alle Felder aufschlüsseln

```
journalctl -o verbose
```

(alle Felder, die mit '_' beginnen, sind interne Felder und werden intern vom journald gesetzt und

nicht vom Client. Somit sind sie nicht leicht manipulierbar.)

seit dem letztem Boot

```
journalctl -b
```

in einem bestimmten Zeitraum

```
journalctl --since '2016-01-10' --until '2016-01-11 03:00'
```

ab einem bestimmten Level

```
journalctl -p 4
journalctl -p warning
```

## Meldungen eines bestimmten Dienstes

```
journalctl _SYSTEMD_UNIT=ssh.service
journalctl -u ssh.service
journalctl /usr/sbin/sshd
```

### Kernel Meldungen

```
journalctl -k
```

### Ins Journal schreiben

genauer: stdout und stderr mit dem journal verbinden

```
ls | systemd-cat
systemd-cat hostnamectl
```

## Größe beschränken

Defaults für `persistent`: 10% filesystem. Max 4 GiB

/etc/systemd/journald.conf

```
SystemMaxUse=100M
SystemKeepFree=1G
```

### Größe manuell verkleinern

Aktuelle Größe anzeigen:

```
journalctl --disk-usage
```

sollte etwa das selbe sein wie:

```
du -sh /var/log/journal/
```

So lange alte Logs löschen, bis 100M erreicht sind:

```
sudo journalctl --vacuum-size=100M
```

oder: alle Logs löschen, die älter als 2 Tage sind:

```
journalctl --vacuum-time=2days
```

### Persistentes Journal

```
mkdir /var/log/journal
systemctl restart systemd-journald
```

### Boots

Auflisten, letztes boot

```
journalctl --list-boots
journalctl -b
```

Ein bestimmtes boot (mit ID oder ordinal)

```
journalctl -b 76fcd53ed6d54d24b1422e6bb48bab61
journalctl -b -2
```

### Versiegeln

So können die sealing keys erstellt werden

```
journalctl --setup-keys
```

## Doku

- http://0pointer.de/blog/projects/journalctl.html

[1)]

man könnte auch eine id selbst erzeugen mit `dbus-uuidgen > /etc/machineid`