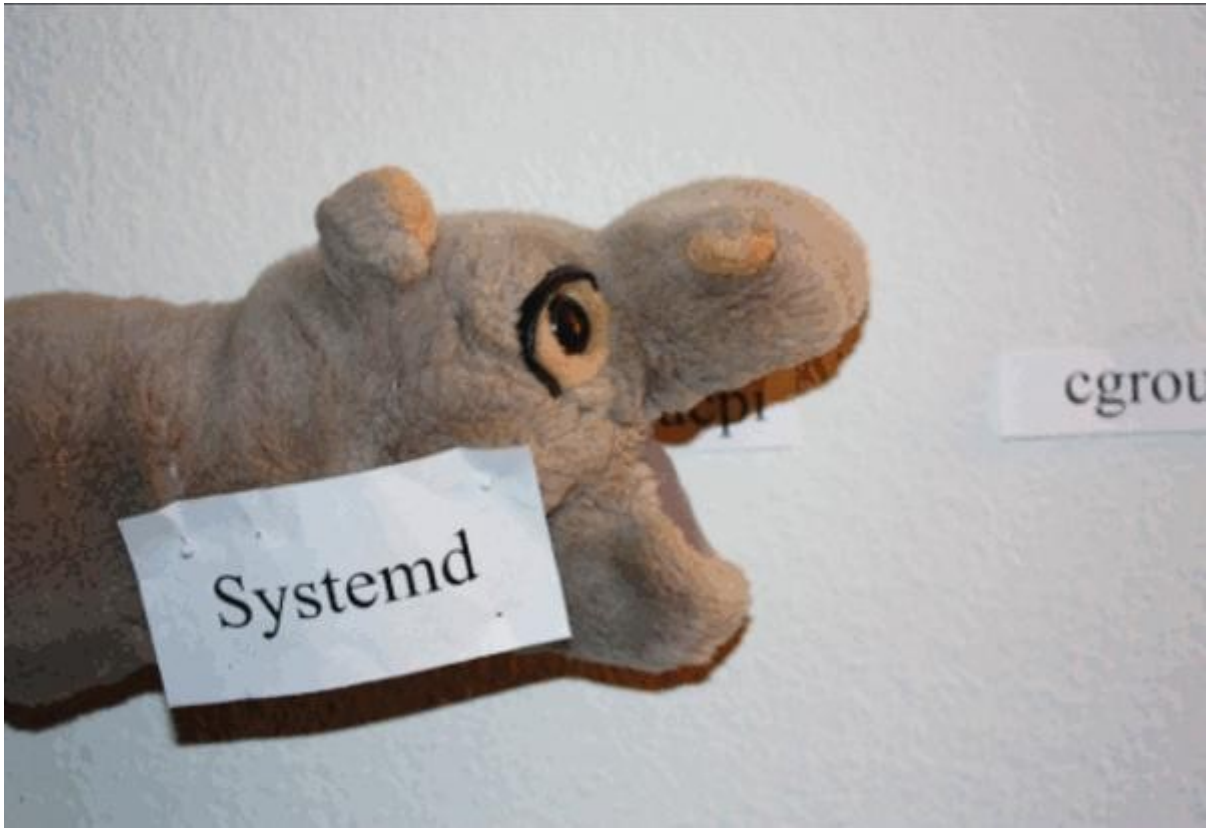
systemd für Admins



Jonas Genannt

systemd / Debian

- „Subject: Dropping upstart jobs (or not)“
  - „Another piece of diversity lost in the open source world. systemd is winning the war.“
  - „John Lennon & Yoko Ono: WAR IS OVER!“
  - „You are wrong: this war was won long ago:“
  - „Can we please not turn this into another argument about systemd, please? We have more urgent business to deal with, such as finding every possible cute cat gif in /dev/random.“

systemd

- systemd-timesyncd
- systemd-timers
- systemd-journald
- systemd-nspawn
- systemd-networkd
- systemd-resolved
- systemd-tmpfiles
- Units / Services
  - Conditions
  - „Security“
  - Instances
  - Overrides

systemd-timesycnd

- NTP Client
  - SNTP
    - Spricht nur mit „einem“ NTP Server zur gleichen Zeit
    - Fallback möglich

systemd-timers

- Cron „Ersatz“

systemctl list-timers

```
jonas@swetlana:~$ sudo  systemctl list-timers
NEXT                         LEFT     LAST                         PASSED       UNIT                         ACTIVATES
Fri 2016-06-10 18:07:00 CEST  20h left Thu 2016-06-09 18:07:00 CEST  3h 22min ago systemd-tmpfiles-clean.timer systemd-tmpfiles-clean.service

1 timers listed.
Pass --all to see loaded but inactive timers, too.
```

- /etc/systemd/system/foo.timer

```
jonas@swetlana:/etc/systemd/system$ cat /lib/systemd/system/timers.target.wants/systemd-tmpfiles-clean.timer
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it
#  under the terms of the GNU Lesser General Public License as published by
#  the Free Software Foundation; either version 2.1 of the License, or
#  (at your option) any later version.

[Unit]
Description=Daily Cleanup of Temporary Directories
Documentation=man:tmpfiles.d(5) man:systemd-tmpfiles(8)

[Timer]
OnBootSec=15min
OnUnitActiveSec=1d
```

systemd-journald

- Syslog-Ersatz
  - Remote Logging mit SSL
- journalctl -f
- journalctl -u ssh (unit name)
- „rotate“ problematisch – RFE existiert

systemd-nspawn

- „chroot“
- systemd-nspawn
- machinectl login foobar

systemd-networkd

- Netzwerkkonfiguration
  - ifupdown / syscfg
    - mehre IPs auf ein Interface
    - extra Routen für ein Interface
    - Bridge/Vlans
    - Routing Tables
- .network – Netzwerkkonfiguration
- .link – Netzwerk Device Konfiguration
- .netdev – Virtuelle Network Devices

systemd-networkd

```
# /etc/systemd/network/internal.link
[Match]
MACAdress=12:34:56:78:90:ab
[Link]
Description=internal Network
Name=internal
```

systemd-networkd

```
# /etc/systemd/network/br0.netdev
[NetDev]
Name=br0
Kind=bridge
# /etc/systemd/network/br0-members.network
[Match]
Name=eth*
[Network]
Bridge=br0
# /etc/systemd/network/br0.network
[Match]
Name=br0
[Address]
Address=192.168.0.1/24
```

systemd-resolved

- lokaler DNS / LLMNR Resolver
- DNSSec

/etc/nsswitch.conf

...

hosts: files mymaschines resolve myhostname

...

- systemd-resolve www.google.com

systemd-tmpfiles

- Erzeugen von temp. Verzeichnissen

Unit / Services

```
[Unit]
Description=OpenBSD Secure Shell server
After=network.target auditd.service
ConditionPathExists=!/etc/ssh/sshd_not_to_be_run

[Service]
EnvironmentFile=-/etc/default/ssh
ExecStart=/usr/sbin/sshd -D $SSHD_OPTS
ExecReload=/bin/kill -HUP $MAINPID
KillMode=process
Restart=on-failure
RestartPreventExitStatus=255
Type=notify

[Install]
WantedBy=multi-user.target
Alias=sshd.service
```

Units / Conditions

```
# /lib/systemd/system/hv-kvp-daemon.service
ConditionVirtualization=microsoft


systemctl status hv-kvp-daemon.service
● hv-kvp-daemon.service - Hyper-V KVP Protocol Daemon
   Loaded: loaded (/lib/systemd/system/hv-kvp-daemon.service; enabled)
   Active: inactive (dead)
           start condition failed at Tue 2016-02-16 09:13:57 CET; 3 months
23 days ago
           ConditionVirtualization=microsoft was not met
```

Units / Conditions 2

ConditionArchitecture=, ConditionVirtualization=,
ConditionHost=, ConditionKernelCommandLine=,
ConditionSecurity=, ConditionCapability=,
ConditionACPower=, ConditionNeedsUpdate=,
ConditionFirstBoot=, ConditionPathExists=,
ConditionPathExistsGlob=, ConditionPathIsDirectory=,
ConditionPathIsSymbolicLink=,
ConditionPathIsMountPoint=,
ConditionPathIsReadWrite=,
ConditionDirectoryNotEmpty=, ConditionFileNotEmpty=,
ConditionFileIsExecutable=

systemd - „Security“

```
# /etc/systemd/system/php7.0-fpm.service.d/sec.conf

[Service]

CapabilityBoundingSet= ~ CAP_SYS_ADMIN
CAP_NET_ADMIN CAP_NET_BROADCAST
CAP_SETFCAP CAP_SYS_BOOT CAP_SYS_RAWIO

ProtectSystem=full

PrivateTmp=true

PrivateDevices=true
```

Service Instances

```
# cat haproxy@.service
[Unit]
Description=HAProxy Load Balancer %i

[Service]
EnvironmentFile=-/etc/default/haproxy-%i
ExecStartPre=/usr/sbin/haproxy -f /etc/haproxy/%i.cfg -c -q
ExecStart=/usr/sbin/haproxy-systemd-wrapper -f /etc/haproxy/%i.cfg -p /run/haproxy-%i.pid $EXTRAOPTS
ExecReload=/usr/sbin/haproxy -c -f /etc/haproxy/%i.cfg
ExecReload=/bin/kill -USR2 $MAINPID
KillMode=mixed
Restart=always

[Install]
WantedBy=multi-user.target
```

Unit Override

```
# /etc/systemd/system/varnish.service.d/foo.conf

[Service]

ExecStart=

ExecStart=/usr/sbin/varnishd -j unix,user=vcache
-F -a :6081 -T localhost:6082 -f
/etc/varnish/default.vcl -S /etc/varnish/secret -s
malloc,20m
```

Ende