# systemd

## Mehr als nur ein neues Init-System

*Markus Schade*

# DAS UNTERNEHMEN


Hetzner Online ist ein professioneller Webhosting-Dienstleister und erfahrener Rechenzentrenbetreiber. Wir bieten Lösungen an, die durch Qualität, Stand der Technik und Sicherheit überzeugen. Dabei reicht das Angebot für Homepage-Einsteiger bis zum professionellem Webentwickler:

- Root, Managed und vServer
- Colocation
- Shared Hosting
- Internet Domains
- SSL-Zertifikate

HETZNER ONLINE

# what is systemd

We serve and provide - worldwide.

„systemd is a system and session manager for Linux, compatible with SysV and LSB init scripts. systemd provides aggressive parallelization capabilities, uses socket and D-Bus activation for starting services, offers on-demand starting of daemons, keeps track of processes using Linux cgroups, supports snapshotting and restoring of the system state, maintains mount and automount points and implements an elaborate transactional dependency-based service control logic. It can work as a drop-in replacement for sysvinit“ (Lennart Poettering, 2011)

# what is systemd

We serve and provide - worldwide.

- systemd is a suite of basic building blocks for a Linux system
- too many things for one talk

HETZNER ONLINE

# Am I running systemd?

We serve and provide - worldwide.

- `systemctl`
- `systemctl status`
- `systemctl list-unit-files`
- 
```
systemd-notify --booted &&
    echo "with systemd" ||
    echo "no systemd"
```

# units

We serve and provide - worldwide.

- targets
  - groups of units (like runlevel but more general)
  - multi-user.target.wants/
- services
  - e.g. rsyslogd.service
- sockets – on demand services
- mount, timers, slice, ...

# runlevels / targets



- runlevel 5 → graphical.target
- runlevel 2/3/4 → multi-user.target
- runlevel 0/6 → shutdown.target / reboot.target
  - reboot, halt, shutdown still work
  - `systemctl reboot/poweroff`
- `systemctl isolate <name>.target`

# default.target

We serve and provide - worldwide.

- symlink to a defined target
- `systemctl get-default`
- `systemctl set-default <target>`

HETZNER ONLINE

# daemons / service units



- Old: `service httpd start/stop`
- New: `systemctl start/stop httpd.service`
- `systemctl enable foo.service`
- Need help?

```
# .bashrc
service() {
 sudo systemctl $2 $1
}
```

# timer units



- units that control/start .service units
- cron-like (could be used instead of CRON)
- more flexible
  - `OnBootSec=15min` # 15min after system boot
  - `OnActiveSec=1d` # run again after one day
  - `WakeSystem=true` # from suspend if supported

# configuration

We serve and provide - worldwide.

- `[/usr]/lib/systemd` – default as shipped
  - **DO NOT MODIFY!**
- `/etc/systemd/`
  - local configuration
  - takes precendence over default
  - partial overrides possible
  - local units by sysadmin

# Override examples



- e.g. dont clear tty1 getty on boot
- fully override packaged unit file

```
# cd /etc/systemd/system/getty.target.wants
# rm getty@tty1.service
# cp /lib/systemd/system/getty@.service \
  getty@tty1.service
# sed -i -e 's/^TTYVTDisallocate=.*/TTYVTDisallocate=no/' \
  getty@tty1.service
```

# Override examples

We serve and provide - worldwide.

- fix broken exit code of HAVEGED

  using include

```
# /etc/systemd/system/haveged.service
.include /lib/systemd/system/haveged.service
[Service]
SuccessExitStatus=143
```

HETZNER ONLINE

# override / drop-in

We serve and provide - worldwide.

- using <name>.service.d

```
# /etc/systemd/system/getty@tty1.service.d
# noclear.conf
[Service]
TTYVTDisallocate=no
```

# override conditions

We serve and provide - worldwide.

- don‘t start on virtual machines

```
[Unit]
ConditionVirtualization=no
```

- require a service or start after a unit

```
[Unit]
After=network.target
Require=slapd.service
```

HETZNER ONLINE

# masking



- unit cannot be started (even manually)

```
systemctl mask networking.service

# or

cd /etc/systemd/system
ln -s /dev/null networking.service
```

# keep watch

We serve and provide - worldwide.

- limit memory and restart service if it crashes

```
.include /usr/lib/systemd/system/leakd.service
[Service]
MemoryLimit=1G
Restart=on-failure
```

# caveat

We serve and provide - worldwide.

- Remember!

  After adding/changing units tell systemd

```
# systemctl daemon-reload
```

HETZNER ONLINE

# journald

We serve and provide - worldwide.

- integrated logging system
- standalone or with syslog(-ng)/rsyslog
- default non-persistent
- stored binary-format
- provides forward secure sealing

# journald



- Forward to syslog and output on tty12

```
#/etc/systemd/journald.conf
ForwardToSyslog=yes
ForwardToConsole=yes
TTYPath=/dev/tty12
MaxLevelConsole=info
```

- Show log from specific unit

```
journalctl -u sshd.service
```

# what‘s my name?

We serve and provide - worldwide.

- `hostnamectl`
  - hostname, virtualization,  OS, arch, etc.
  - /etc/hostname, /etc/machine-info, /etc/os-release
  - /etc/machine-id
    - unique 128bit string (on install or on boot if missing)
  - `systemd-detect-virt`

# out of time?

We serve and provide - worldwide.

- `timedatectl`
- time, date and timezone in one tool
- shows DST if and when it starts/ends
- shows if RTC is in local TZ
  - `timedatectl set-local-rtc true`

# systemd-timesyncd

We serve and provide - worldwide.

- ntpd/chrony
  - no option to run as client only
  - CVE-2013-5211 (DRDoS/Amplification - monlist)
- systemd-timesyncd – SNTP Client
- since systemd >= 213 (not in RHEL7)
- `# timedatectl set-ntp true`

# systemd-timesyncd

We serve and provide - worldwide.

```
# /etc/systemd/timesyncd.conf

# systemctl status systemd-timesyncd
  systemd-timesyncd.service - Network Time Synchronization
…
systemd-timesyncd[292]: Using NTP server
[2a01:4f8:0:a0a1::2:1]:123 (ntp1.hetzner.de).
systemd-timesyncd[292]: interval/delta/delay/jitter/drift
32s/+1.572s/0.003s/0.000s/+0ppm
```

# systemd-networkd



- since systemd >=210
- for VMs/containers, also works on Ethernet
- fast: less 1ms for DHCP-lease in container
- .netdev – virtual devices (bridges)
- .link – set link properties (MTU, WakeOnLAN)
- .network – IPs, gateway, routes

# simple network config

We serve and provide - worldwide.

```
# /etc/systemd/network/10-dhcp.network
[Match]
Name=em*

[Network]
DHCP=v4
```

HETZNER ONLINE

# bridged networking



```
# /etc/systemd/network/10-br0.netdev
[NetDev]
Name=br0
Kind=bridge

# /etc/systemd/network/15-eth0-br0.network
[Match]
MACAddress=52:54:a1:01:00:01
[Network]
Bridge=br0
```

# bridged networking

We serve and provide - worldwide.

```
# /etc/systemd/network/20-br0.network
[Match]
Name=br0

[Network]
Address=192.168.1.100/24
Gateway=192.168.1.1
```

HETZNER ONLINE

# systemd-nspawn

We serve and provide - worldwide.

- “chroot on steroids“
- provides lightweight containers

```
# debootstrap --arch=amd64 jessie /srv/jessie-tree
# systemd-nspawn -D /srv/jessie-tree/
Spawning container jessie-tree on /srv/jessie-tree.
Press ^] three times within 1s to kill container.
root@jessie-tree:~# passwd

# systemd-nspawn -bD /srv/jessie-tree/
```

# systemd-nspawn



- create a container unit

```
# ln -s /srv/jessie-tree /var/lib/container/jessie
```

- enable and launch container

```
# systemctl enable systemd-nspawn@jessie.service
# systemctl start systemd-nspawn@jessie.service
```

# not so obvious

We serve and provide - worldwide.

- cannot start services in chroot

```
# chroot /mnt systemctl start mysql.service
Running in chroot, ignoring request.
```

# systemd-nspawn

We serve and provide - worldwide.

- cannot launch without systemd

```
# mnt /dev/sda2 /mnt
# systemd-nspawn -D /mnt
# systemctl start mysql
Failed to get D-Bus connection: No connection to
service manager.
```

- launch one service (and its dependencies)

```
# systemd-nspawn -bD /mnt systemd.unit=mysql.service
```

HETZNER ONLINE

# debugging

We serve and provide - worldwide.

- rescue shell (aka single user mode)

```
# mnt /dev/sda2 /mnt
# systemd-nspawn -bD /mnt systemd.unit=rescue.target
```

- emergency shell (minimal systemd env)

```
# systemd-nspawn -bD /mnt systemd.unit=emergency.target
```

- can be passed as kernel options

Fragen? Fragen!

HETZNER ONLINE

# Wir suchen Mitarbeiter!

- 1. Ausbildung Fachinformatiker
- 2. Netz- und Sysadmins
- 3. Software-Entwickler
- 3. Abschlußarbeiten / Praktika / Ferienarbeit

**mehr unter *https://jobs.hetzner.de***

HETZNER ONLINE