Was man über systemd wissen sollte

Secure Linux Administration Conference 2014

Lennart Poettering

Mai 2014

systemd!

systemd!

Nicht SystemD, nicht systemD, nicht System D oder System-D!

Was ist systemd?

Was ist systemd?

System- und Dienste-Manager auf allen neuen Linux-Distributionen

Was ist systemd?

System- und Dienste-Manager auf allen neuen Linux-Distributionen

Fedora seit 15, Suse, Mandriva, ... und bald auch Debian und Ubuntu

Was ist systemd?

System- und Dienste-Manager auf allen neuen Linux-Distributionen

Fedora seit 15, Suse, Mandriva, ... und bald auch Debian und Ubuntu

Und in RHEL ab RHEL 7

Nicht nur ein Init-System

Nicht nur ein Init-System

Eine Platform!

Nicht nur ein Init-System

Eine Platform!

Die Basis-Komponenten, die ein Betriebssystem ausmachen

Nicht nur ein Init-System

Eine Platform!

Die Basis-Komponenten, die ein Betriebssystem ausmachen

Die Klebe, die alles zusammenhält

Sicherheits-Optionen

Recap: In *Units* werden Dienste und andere System-Komponenten konfiguriert

Recap: In *Units* werden Dienste und andere System-Komponenten konfiguriert

Unit-Dateien haben eine Struktur, die Windows-INI-Dateien ähnelt

```
[Unit]
Description=Router Advertisement Daemon for IPv6

[Service]
ExecStart=/usr/sbin/radvd
Type=forking
PIDFile=/var/run/radvd/radvd.pid

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

User=, Group=

User=, Group=

RootDirectory=

User=, Group=

RootDirectory=

LimitFSIZE=, LimitNPROC=

CapabilityBoundingSet=

CapabilityBoundingSet=

SELinuxContext=, AppArmorProfile=

ReadWriteDirectories=, ReadOnlyDirectories=,
InaccessibleDirectories=

ReadWriteDirectories=, ReadOnlyDirectories=,
InaccessibleDirectories=

PrivateTmp=

ReadWriteDirectories=, ReadOnlyDirectories=,
InaccessibleDirectories=

PrivateTmp=

PrivateNetwork=

ReadWriteDirectories=, ReadOnlyDirectories=,
InaccessibleDirectories=

PrivateTmp=

PrivateNetwork=

PrivateDevices=

SystemCallFilter=

SystemCallFilter=

SystemCallArchitecture=

SystemCallFilter=

SystemCallArchitecture=

RestrictAddressFamilies=

systemd-nspawn

```
# yum -y --releasever=20 --nogpg
      --installroot=/srv/mycontainer
      --disablerepo='*' --enablerepo=fedora
      install systemd passwd yum
      fedora-release vim-minimal
# systemd-nspawn -bD /srv/mycontainer
```

machinectl

systemd-cgls

Container-Unterstützung is direkt in integriert in systemctl, systemd-run, . . .

Das Journal

“Pixel-Perfect” Syslog-Ausgabe

```
# journalctl -n 20
# journalctl -f
# journalctl -b
# journalctl -b -1
# journalctl -e
# journalctl -r
# journalctl -k
# journalctl -u apache
# journalctl -p err
# journalctl --since today
# journalctl --since 2014-01-23
```

```
# journalctl -o verbose
# journalctl _PID=47
# journalctl _COMM=cron
# journalctl _HOSTNAME=delta _PID=1
```

That's all, folks!