Einfache Tipps für mehr Sicherheit mit systemd

Michael F. Schönitzer

28. Oktober 2016

Unit-Files

```
[Unit]
Description=Privoxy Web Proxy
After=network.target

[Service]
Type=forking
PIDFile=/run/privoxy.pid
ExecStart=/usr/bin/privoxy [...]
SuccessExitStatus=15
## Add Security-Options here! ##

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

Unit-Files

- /etc/systemd/system/*

Unit-Files

- /etc/systemd/system/*
- /run/systemd/system/*

Unit-Files

- /etc/systemd/system/*
- ~~/run/systemd/system/*~~

Unit-Files

- /etc/systemd/system/*
- ~~/run/systemd/system/*~~
- /usr/lib/systemd/system/*

Unit-Files

- /etc/systemd/system/*
- ~~/run/systemd/system/*~~
- /usr/lib/systemd/system/*

Unit-Files

- /etc/systemd/system/*
- ~~/run/systemd/system/*~~
- /usr/lib/systemd/system/*

Defaults:

- /etc/systemd/system.conf

Well Known

User=

Group=

SupplementaryGroups=

Fileaccess

ReadWriteDirectories=/var/cache

ReadOnlyDirectories=/

InaccesiblyDirectories=/etc

Fileaccess

```
ReadWriteDirectories=/var/cache

ReadOnlyDirectories=/

InaccesiblyDirectories=/etc


ProtectHome=yes

ProtectSystem=yes
```

Special Files

PrivateTmp=yes

PrivateDevices=yes

DeviceAllow=/dev/sda5 rw

Networkaccess

```
PrivateNetwork=yes

RestrictAddressFamilies=AF_UNIX AF_INET AF_INET6
```

Joining Namespaces

JoinsNamespaceOf=

Make mounts local

```
MountFlags=slave
```

Chroot

RootDirectory=

Usefull limits

LimitFSIZE=0

TaskMax=100

Inhibit jailbreaks

NoNewPrivileges=yes

Restrict rights

CapabilityBoundingSet=

- ⇝ man 7 capabilities
- ⇝ http://rhelblog.redhat.com/2016/10/17/secure-your-containers-with-this-one-weird-trick/

AmbientCapabilities=

Filter System Calls

SystemCallArchitectures=x86 x86-64 / native

SystemCallFilter=

- @clock
- @cpu-emulation
- @debug
- @io-event
- @ipc
- @keyring
- @module
- @mount
- @network-io
- @obsolete
- @privileged
- @process
- @raw-io

Thank you for your attention