Locking Down Your systemd Services

LinuxCon Europe, Berlin

October 2016

systemd

systemd

Service Management

systemd

Service Management

Security

Unit Files

Unit Files

Service Files

```
[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
```

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

[Service]
ExecStart=/usr/sbin/radvd
Type=forking
PIDFile=/var/run/radvd/radvd.pid
PrivateTmp=yes
ProtectSystem=full
ProtectHome=yes

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

```
User=
```

```
User=

DynamicUser=
```

```
CapabilityBoundingSet=
```

```
CapabilityBoundingSet=

SecureBits=
```

`PrivateTmp=`

PrivateDevices=

`PrivateNetwork=`

`ProtectSystem=no|yes|full|strict`

`ReadWritePaths=`

```
ReadWritePaths=

ReadOnlyPaths=
```

```
ReadWritePaths=

ReadOnlyPaths=

InaccessiblePaths=
```

PrivateUsers=

`RootDirectory=`

`ProtectKernelTunables=`

`ProtectControlGroups=`

```
MountFlags=slave
```

`NoNewPrivileges=`

```
SystemCallFilter=
```

`SystemCallFilter=`

Example: `SystemCallFilter=~@clock @ipc`

`SystemCallArchitecture=`

```
RestrictAddressFamilies=
```

`MemoryDenyWriteExecute=`

`RestrictRealtime=`

`DeviceAllow=`

```
SELinuxContext=
```

```
SELinuxContext=

AppArmorProfile=
```

```
SELinuxContext=

AppArmorProfile=

SmackProcessLabel=
```

Future:

Future:

`ProtectKernelLogs=`

Future:

`ProtectKernelLogs=`

`ProtectClock=`

Future:

`ProtectKernelLogs=`

`ProtectClock=`

`ProtectKernelModules=`

Future:

`ProtectKernelLogs=`

`ProtectClock=`

`ProtectKernelModules=`

`ProtectTracing=`

Future:

`ProtectKernelLogs=`

`ProtectClock=`

`ProtectKernelModules=`

`ProtectTracing=`

`ProtectMount=`

Future:

`ProtectKernelLogs=`

`ProtectClock=`

`ProtectKernelModules=`

`ProtectTracing=`

`ProtectMount=`

`RestrictNamespaces=`

That's all, folks!