Be smart. Think open source.

Modul "journald" [SSA 1002]

systemd-journald Daemon

- Dienst der von systemd verwaltet wird
- Sammelt alle Logs an einer zentralen Stelle
- Binary Format mit diversen Vorteilen gegenüber Plain-Text Format

Probleme herkömmlicher syslog Dienste 1/2

- Bisher wurden sämtliche Logs nach einem beliebigen Muster geschrieben (abhängig vom Dienst/Tool) – automatische Loganalyse schwierig
- Timestamps enthielten meist keine Zeitzonen Infos
- Binary Daten konnten bisher nicht direkt ins syslog geschrieben werden (coredumps, firmware dumps, SCSI sense data)

Probleme herkömmlicher syslog Dienste 2/2

- Viele verschiedene Logs (syslog, lastlog, audit, kernel logs, etc.)
- Log Files sind relativ einfach manipulierbar, Angreifer können Informationen zu einem Angriff relativ einfach verstecken
- Early boot / late shutdown Informationen meist nicht vorhanden

Background Log Format

- Die einzigen Meta Daten, die bei herkömmlichen syslog Implementationen mitgeschickt werden, sind Quelle (Facility), Priorität, Timestamp, PID, Hostname/IP
- Der Serber verifiziert diese Informationen meist nicht und legt diese eins zu eins ab
- Die meisten Informationen sind optional und es ist nicht präzise vorgeschrieben, wie die Syntax aussieht; dadurch variieren die Logs je nach Syslog Implementation stark

Konfiguration von journald 1/2

- /etc/systemd/journald.conf

```
man 5 journald.conf
```

- *Storage* definiert, ob das Log persistent ist persistent = persistent in /var/log/journal volatile = nur im Memory auto = persistent in /var/log/journal wenn vorhanden
- *Compress* definiert, ob Kompression eingeschaltet ist

Konfiguration von journald 2/2

- Seal definiert, ob persistente journal Files mit einem Key signiert werden, um diese vor Manipulationen zu schützen
- *ForwardToXYZ* definiert, ob journald Nachrichten an einen herkömmlichen syslog Dienst, den Kernel log buffer (kmesg), etc. weitergeleitet werden sollen
- Nach Änderungen:

```
systemctl restart systemd-journald
```

nicht vergessen!

Loganalyse mit journalctl 1/6

- journalctl ist ein high-level Zugang zu den Logs
- Nützliche Filter sind direkt integriert:
- Boot Nummer / System Starts
- Zeit Intervall
- Spezifische Log Felder

Loganalyse mit journalctl 2/6

- Logs eines spezifischen Tools analysieren

```
journalctl /usr/sbin/httpd
```

-f Fortlaufende Anzeige

-e Zeigt die letzten Einträge

-r Umgekehrte Reihenfolge

- Logs eines spezifischen systemd Units anzeigen

```
journalctl -u mariadb
```

Loganalyse mit journalctl 3/6

- Filterung nach System Starts ist nützlich, um z.B. Probleme nach dem ersten Reboot infolge eines Updates zu finden
- Beispiel:

```
journalctl --list-boot

journalctl -b 42
```

Loganalyse mit journalctl 4/6

- Filterung basierend auf einem Zeitintervall sind nützlich, um Probleme, die in einem bestimmten Zeitraum passiert sind, zu analysieren
- Beispiele:

```
journalctl --since "2014-06-30 9:17:16"

journalctl --since "now"

journalctl --since "today" --until "11:00"
```

Loganalyse mit journalctl 5/6

- Zeitangaben, siehe man 7 system.time
- Annahme, aktuelle Zeit: 2016-08-23 18:15:22
- "11:00" 2016-08-23 11:12:00
- "now" 2016-08-23 18:15:22
- "+3h30min" 2016-08-23 21:45:22

Loganalyse mit journalctl 6/6

- Filterung nach einem spezifischen Log Feld ist nützlich, um z.B. Probleme eines spezifischen Prozesses, eines spezifischen Benutzers, etc. zu finden
- `man 7 systemd.journal-fields`
- Beispiele:

```
journalctl _PID=507 --since "today"

journalctl _UID=1000

journalctl _SYSTEMD_UNIT=httpd.service
```

Limitierung Log Grösse

- Parameter in journal.conf

[System|Runtime]MaxUse

[System|Runtime]MaxFileSize

[System|Runtime]MaxFiles

- System = on Disk (persistent) Files
- Runtime = in Memory Files
- `man 5 journald.conf`

Limitierung Log Grösse 2/4

- **[System|Runtime]MaxUse** definiert, wie viel Platz das journal maximal belegen darf
- Default ist 10% der Partitionsgrösse auf welcher das Journal liegt
- Dieser Wert beinhaltet alle journal Files (auch rotierte)

Limitierung Log Grösse 3/4

- **[System|Runtime]MaxFileSize** definiert, wie gross individuelle Journal Files werden dürfen
- Default ist 1/8 der Grösse von **[System|Runtime]MaxUse** damit sieben Rotationen möglich sind

Limitierung Log Grösse 4/4

- **[System|Runtime]MaxFiles** definiert, wie viele individuelle Journal Files maximal aufbewahrt werden
- Deafult ist 100

Attribution / License

Feel Free to Contact Us

www.adfinis-sygroup.ch

Tech Blog

GitHub

info@adfinis-sygroup.ch

Twitter