System-Logs

Nützliche Tools und Logdateien für die Informationsgewinnung



System-Logs? Wozu das denn?

Die erste Frage, die sich jemandem stellt, der dieses Thema hört, ist vermutlich:
„Wozu brauche ich das?“

Logdateien sind die wichtigste Grundlage der Fehlersuche!

System-Logs – Wieso sind die wichtig?

Logdateien sind die wichtigste Informationsquelle bei Fehlern.

Sie protokollieren:

- Systemstarts
- Hardware-Ereignisse
- Anmeldungen
- Programmfehler
- Netzwerkprobleme
- ...



System-Logs – Grafischer Ansatz

Wichtiger Merksatz:

Wenn etwas nicht funktioniert, stehen die Hinweise meist bereits in den Logdateien

System-Logs – Wo befinden sie sich?

Die wichtigsten Logdateien stehen klassischerweise in /var/log/:

- /var/log/syslog
- /var/log/auth.log
- /var/log/kern.log

“Moderne” Logs erreicht man mit journalctl

System-Logs – Die drei wichtigsten

Die drei wichtigsten Logdateien sind:

- /var/log/syslog

Hier landen allgemeine Systemmeldungen

- /var/log/auth.log

Hier stehen alle Infos zu Anmeldungen und sudo-Befehlen

- journalctl

Zentrale Analyse aller Systemdienste



System-Logs – Logdateien richtig lesen

Auf welche Schlüsselwörter sollte man beim inspizieren von Logdateien besonders achten?

- Error, failed, critical, panic, denied

Wichtige Regeln:

- Zeitstempel beachten
- Immer mehrere Zeilen lesen
- Nach dem ersten Fehler suchen
- Warnungen nicht mit Fehlern verwechseln

System-Logs – Werkzeug #1

Das wichtigste Analysewerkzeug ist *journalctl*:

- Infos zum aktuellen Start: journalctl -b
- Nur Fehler: journalctl -p err
- Live-Monitoring: journalctl -f

System-Logs – Werkzeug #2

Für große Logdateien steht das Werkzeug *less* bereit.

less ist ein Pager zum Anzeigen von (Text-) Dateien auf der Kommandozeile:

- less /var/log/syslog
  - Suche: */error*
  - Weiterblättern: *n*

less bietet sich durch seine Schnelligkeit und Ressourcenschonung an und ist deshalb das Standardwerkzeug vieler Administratoren.

System-Logs – Werkzeug #3

Zur gezielten Filterung verwendet man am Besten *grep*.

Mit grep lassen sich Dateien nach bestimmten Textstücken durchsuchen.

Die Suchmuster, sogenannte „regular expressions“ sind vielfältig einsetzbar, und werden nicht nur von grep verwendet.

- Suche nach Fehlern: grep -i error /var/log/syslog
- Mehrere Kriterien: grep -Ei “error|fail|critical”

Mit *grep* lassen sich in Sekunden relevante Meldungen

FreieSoftwareOG.org

System-Logs – Werkzeug #4

Zur Beobachtung der letzten Meldungen eignet sich *tail*:

- Letzte (10) Zeilen: tail /var/log/syslog
- Live-Monoitoring: tail -f /var/log/syslog

Typische Anwendung von *tail*: Während man versucht einen Fehler zu reproduzieren.

System-Logs - Hands-On

```
journalctl -b -p err | tail -20
```

Anzeige der letzten Fehler des aktuellen Starts:

- Erscheinen Fehler?
- Sind sie aktuell?
- Lassen sie sich erklären?

System-Logs – Typische Fehlersuche

Beispiel: Dienst startet nicht

- Status prüfen: systemctl status nginx
- Journal anzeigen: journalctl -u nginx
- Nur Fehler: journalctl -u nginx -p err

Vorgehensweise:

- Problem identifizieren
- Passende Logs prüfen
- Fehlerursache finden
- Korrektur testen

FreieSoftwareOG.org

System-Logs – Best Practices

Die wichtigsten Regeln:

- Den Zeitpunkt des Problems, sowie evtl. davor getätigte Aktionen notieren
- Zuerst (entsprechende) Logs prüfen
- Nach „error“ und „failed“ suchen
- Immer den ersten Fehler analysieren
- Änderungen dokumentieren
- Nach jeder Änderung erneut testen

  → Ceteris Paribus[1]



1 - https://de.wikipedia.org/wiki/Ceteris_paribus

System-Logs – Wie poste ich das?

Oft kommt es vor, dass man in einem Hilfeforum dazu aufgefordert wird, die Ausgabe eines Logs im Thread zu posten.
Dies hilft den Profis dort, beim Problem zu helfen.

Aber wie postet man das?
Einfach in meinem Terminal markieren, „Strg+C“ und dann im Forum „Strg+V“?

Das könnte tödlich enden...

System-Logs – Wie poste ich das?

Zum Einen geht dadurch die ursprüngliche (evtl. vorhandene) Formatierung verloren, zum Anderen wird es nicht gern gesehen, einfach wild Text unformtiert in einem Thread zu posten (gilt übrigens auch für Sourcecode).

Zum Glück gibt es da einige Hilfsmittel:

- pastebinit (Tool)
- Imgur (Online)

System-Logs – Was passiert mit denen?

Logrotate passiert…

...damit Logdateien nicht unbeschränkt wachsen und irgendwann die Festplatte belegen, ist meistens das Werkzeug „logrotate“ installiert.

logrotate ist kein daemon, sondern ein Skript, welches über mitinstallierte cron-Einträge regelmäßig ausgeführt wird.

System-Logs – Was passiert mit denen?

Logrotate wurde entwickelt, um die Verwaltung von Logdateien zu vereinfachen.

Die Dateien können automatisch komprimiert, gelöscht oder per Mail verschickt werden.

Dies kann täglich, wöchentlich, monatlich durchgeführt werden, oder wenn eine Logdatei eine vorgegebene Größe überschreitet.

Üblicherweise wird Logrotate einmal am Tag aktiv.

FreieSoftwareOG.org

System-Logs – Was passiert mit denen?

Am Beispiel des „Syslogs“ kann man sehen, wie logrotate arbeitet.
Schaut man sich die Dateien in /var/log an, die den Namen „syslog“ tragen:

```
ls -al /var/log/syslog*
```

so sieht man acht Dateien.

- Die aktuelle „syslog“
- die unkomprimierte „syslog.0“ vom Vortag
- und die „syslog“-Dateien der sechs Tage davor, welche in der Zwischenzeit komprimiert wurden.

FreieSoftwareOG.org

System-Logs – Was passiert mit denen?

```
-rw-r----- 1 root adm  82484 2006-10-15 00:29 syslog
-rw-r----- 1 root adm 163497 2006-10-14 13:06 syslog.0
-rw-r----- 1 root adm  23503 2006-10-13 01:30 syslog.1.gz
-rw-r----- 1 root adm  36587 2006-10-12 11:18 syslog.2.gzls -al /var/log/syslog*
-rw-r----- 1 root adm  38361 2006-10-11 02:47 syslog.3.gz
-rw-r----- 1 root adm  97953 2006-10-10 17:53 syslog.4.gz
-rw-r----- 1 root adm  46201 2006-10-09 11:05 syslog.5.gz
-rw-r----- 1 root adm  35665 2006-10-06 17:21 syslog.6.gz
```

Um genau zu sein, wird syslog nicht von logrotate gepackt, sondern von einem Cronjob.

Dies betrifft auch andere Dateien wie z.B. auth.log.

Eine vollständige Liste kann man sich mit dem Befehl syslogd-listfiles -a anzeigen lassen.

System-Logs - Klassenarbeit

- Zählt 1/3 zur Endnote
- 2/3 sind mündlich, verhalten und Heftführung

Sonstige Themen

- Nächster Di-Day in Freiburg (06.12.)
- xxx

Bitte beachten

Auf der Homepage findet sich immer das aktuelle Datum, sowie das Thema des nächsten Treffens!

Weitergehende Informationen

https://wiki.ubuntuusers.de/systemd/systemctl/

https://wiki.ubuntuusers.de/less/

https://wiki.ubuntuusers.de/grep/

https://wiki.ubuntuusers.de/tail/

https://wiki.archlinux.de/title/Pastebinit

https://imgur.com/upload

Weitere Informationen bekommen Sie hier:

http://www.FreieSoftwareOG.org

und

Kontakt@FreieSoftwareOG.org

oder kommen Sie doch einfach zu unserem regelmäßigen Treffen,

jeden 1. Mittwoch im Monat ab 20:00 Uhr.

(Treffpunkt laut Webseite)



creative commons