GNU/Linux Logdateien - Informationsquelle und Helfer in der Not

GNU/Linux log files – Source of information and helper in distress

Stand: 27.04.2022 Übersetzung / Translation: FSOG

Wozu Logdateien? / Why log files?

Wenn man sich in GNU/Linux-Umgebungen bewegt, ist es wichtig zu wissen, wo sich die Log-Dateien befinden und welche Informationen darin zu finden sind.

Die Logdateien repräsentieren sozusagen eine visuelle Zeitleiste aller Dinge, die auf einem GNU/Linux System passieren.

Solange das System sauber und problemlos läuft, sollte man sich die Zeit nehmen, sich mit dem Inhalt einiger Log-Dateien vertraut zu machen. Das kann bei auftretenden Problemen immens hilfreich sein, um den Auslöser zu finden.

Bei Anwendungen entscheidet der Entwickler, wo die Logdateien des Programms gespeichert werden. So findet man z.B. für Google Chrome unter „~/.chrome/CrashReports“ Details zu Abstürzen.

GNU/Linux Logdateien sollten einfach zu interpretieren sein, sie liegen ja auch in reiner Textform vor. Und zwar im Verzeichnis /var/log und diversen Unterverzeichnissen. Sie umfassen alles mögliche, z.B. System, Kernel, Paketmanager, und vieles weitere. In diesem Artikel befassen wir uns aber mit den System-Logdateien.

Dieses Dokument besteht aus zwei Teilen: „Traditionelle Logdateien mit syslog“ und der „Neuen Journal-Welt mit systemd“.

Linux logs give you a visual history of everything that’s been happening in the heart of a Linux operating system. So, if anything goes wrong, they give a useful overview of events in order to help you, the administrator, seek out the culprits.

For problems relating to particular apps, the developer decides where best to put the log of events. So with Google Chrome for instance, any time it hangs, you want to look in ‘~/.chrome/Crash Reports’ to discover the gory details of what tripped the system up.

Linux log files should be easy to decipher since they’re stored in text form under the /var/log directory and subdirectory. They cover all kinds of things, like system, kernel, package managers, MySQL and more. But now, we’ll focus on system logs.

This document consists of two parts: „Traditional log files with syslog“ and „New world journals with systemd“.

Grundsätzliches / Introduction

Die Datei /etc/rsyslog.conf bestimmt, was in einige Log-Dateien geschrieben wird.
Beispielsweise ist nachfolgend der Eintrag für /var/log/messages abgefragt.

/etc/rsyslog.conf controls what goes inside some of the log files. For example, following is the entry in rsyslog.conf for /var/log/messages.

```
$ grep "/var/log/messages" /etc/rsyslog.conf
*.info;mail.none;authpriv.none;cron.none        /var/log/messages
```

Erläuterung der obigen Ausgabe:

- *.info – alle Logs des Typs „INFO“ werden aufgezeichnet.
- mail.none,authpriv.none,cron.none – die angegebenen Fehlermeldungen werden nicht in /var/log/messages aufgezeichnet.
- Die Angabe von *.none würde dafür sorgen, dass keine der Log-Meldungen aufgezeichnet wird.

In the above output,

- .info indicates that all logs with type INFO will be logged.
- mail.none,authpriv.none,cron.none indicates that those error messages should not be logged into the /var/log/messages file.
- You can also specify *.none, which indicates that none of the log messages will be logged.

Nachfolgend nun die verschiedenen Log-Dateien, welche sich (mit vielen weiteren) im Verzeichnis /var/log/ befinden. Einige dieser Log-Dateien sind Distributions-Spezifisch. Beispielsweise taucht dpkg.log auf Debian-basierten Systemen (z.B. Ubuntu) auf.

The following are the different log files that are located under /var/log/ directory. Some of these log files are distribution specific. For example, you'll see dpkg.log on Debian based systems (for example, on Ubuntu).

Die wichtigsten Logdateien und ihre Inhalte / Important logfiles and their content

Allgemeine Logdateien / Common logfiles

Logdatei / logfile	Bedeutung - Inhalt – Nutzen / Meaning – content - benefit
/var/log/messages (Redhat) /var/log/syslog (Debian)	Beinhaltet globale Systemmeldungen, inklusive der Meldungen, welche während des Systemstarts aufgezeichnet werden. Es werden diverse Dinge in /var/log/messages geschrieben (z.B. mail, cron, daemon, kern, auth, usw.). Contains global system messages, including the messages that are logged during system startup. There are several things that are logged in /var/log/messages including mail, cron, daemon, kern, auth, etc.
/var/log/dmesg	Beinhaltet Informationen zum „kernel ring buffer“. Wenn das System hochfährt, zeigt es viele Informationen über die vom Kernel beim Booten erkannte Hardware auf dem Bildschirm an. Diese Infomationen sind im „kernel ring buffer“ verfügbar und wann immer eine neue Nachricht hereinkommt, wird die alte überschrieben. Der Inhalt dieser Datei kann auch mit dem Befehl dmesg angesehen werden. Contains kernel ring buffer information. When the system boots up, it prints number of messages on the screen that displays information about the hardware devices that the kernel detects during boot process. These messages are available in kernel ring buffer and whenever the new message comes the old message gets overwritten. You can also view the content of this file using the dmesg command.
/var/log/auth.log (Debian) /var/log/secure (Redhat)	Beinhaltet Informationen zur Autorisierung im System, inklusive Logins der Benutzer und die verwendeten Autorisierungs-Mechanismen. Beinhaltet Informationen zu Authentifizierungs- und Authorisierungsprivilegien. Z.B. loggt hier sshd alle Nachrichten (inklusive fehlgeschlagener Anmeldungen). Keep authentication logs for both successful or failed logins, and authentication processes. Storage depends on system type. For Debian/Ubuntu, look in /var/log/auth.log. For Redhat/CentrOS, go to /var/log/secure.
/var/log/boot.log	Beinhaltet Informationen, die beim Booten aufgezeichnet werden. Contains information that are logged when the system boots.

Logdatei / logfile	Bedeutung - Inhalt – Nutzen / Meaning – content - benefit
/var/log/daemon.log	Beinhaltet Informationen, welche von den verschiedenen Hintergrund-daemons erzeugt werden. Contains information logged by the various background daemons that run on the system.
/var/log/dpkg.log	Beinhaltet Informationen, die bei De-/Installation von Paketen mit dem Befehl dpkg aufgezeichnet werden. Contains information that are logged when a package is installed or removed using dpkg command.
/var/log/kern.log	Beinhaltet Informationen, die vom Kernel aufgezeichnet werden. Contains information logged by the kernel. Helpful for you to troubleshoot a custom-built kernel.
/var/log/lastlog	Zeigt die aktuellen Login-Informationen aller Benutzer. Dies ist keine Ascii-Datei. Man sollte den Befehl lastlog verwenden, um diese Informationen anzuzeigen. Displays the recent login information for all the users. This is not an ascii file. You should use lastlog command to view the content of this file.
/var/log/maillog /var/log/mail.log	Beinhaltet Informationen des auf dem System laufenden Mail-Servers. So loggt beispielsweise sendmail Informationen zu allen gesendeten Objekten in dieser Datei. Contains the log information from the mail server that is running on the system. For example, sendmail logs information about all the sent items to this file (for mail server logs, handy for postfix, smtpd, or email-related services info running on your server).
/var/log/user.log	Beinhaltet Informationen über alle Benutzer-Level Logs. Contains information about all user level logs.
/var/log/Xorg.x.log	Nachrichten von X. Log messages from the X.

Logdatei / logfile	Bedeutung - Inhalt – Nutzen / Meaning – content - benefit
/var/log/alternatives.log	Informationen der Update-Alternativen werden hier geloggt. In Ubuntu verwaltet update-alternatives symbolische Links, welche Standard-Befehle bestimmen. Information by the update-alternatives are logged into this log file. On Ubuntu, update-alternatives maintains symbolic links determining default commands.
/var/log/btmp	Beinhaltet Informationen über fehlgeschlagene Anmeldeversuche. Mit dem Befehl last kann man sich die btmp-Datei ansehen. Z.B. „last -f /var/log/btmp | more“ This file contains information about failed login attempts. Use the last command to view the btmp file. For example, “last -f /var/log/btmp | more”
/var/log/wtmp /var/log/utmp	Beinhaltet Login-Informationen. Mit wtmp kann man herausfinden, wer am System angemeldet ist. Der Befehl who nutzt diese Datei für die Anzeige der Informationen. Contains login records. Using wtmp you can find out who is logged into the system. who command uses this file to display the information. /var/log/utmp → current login state by user, /var/log/wtmp → record of each login/logout
/var/log/faillog	Beinhaltet fehlgeschlagene Benutzer-Anmeldungen. Diese Datei kann mit faillog ausgegeben werden. Contains user failed login attemps. Use faillog command to display the content of this file. Hence, handy for examining potential security breaches like login credential hacks and brute-force attacks.
/var/log/cups	Alle Drucker und druckerrelevanten Nachrichten. All printer and printing related log messages.
/var/log/cron	Immer wenn der cron daemon (oder anacron) einen cronjob startet, werden diese Informationen in dieser Datei abgelegt. Whenever cron daemon (or anacron) starts a cron job, it logs the information about the cron job in this file.

Spezielle bzw. spezialisierte Logdateien / More special logfiles

Neben den genannten „Standard“ Log-Dateien beinhaltet das Verzeichnis /var/log eventuell auch noch eines oder mehrere der folgenden Unterverzeichnisse (abhängig von den laufenden bzw. installierten Programmen, der Distribution, etc.).

Logdatei / logfile	Bedeutung - Inhalt – Nutzen / Meaning – content - benefit
/var/log/anaconda.log	Hier werden alle installationsrelevanten Meldungen abgelegt (Fedora). When you install Linux, all installation related messages are stored in this log file.
/var/log/yum.log	Beinhaltet Informationen, wenn ein Paket über yum installiert wurde. Beinhaltet auch Fehler bei der Installation. Contains information that are logged when a package is installed using yum.
/var/log/httpd/ /var/log/apache2	Beinhaltet access_log und error_log des Apache Webservers. A directory containing error_log and access_log files of the Apache httpd daemon. Every error that httpd comes across is kept in the error_log file. Think of memory problems and other system-related errors. access_log logs all requests which come in via HTTP.
/var/log/lighttpd/	Beinhaltet access_log und error_log von light HTTPD Contains light HTTPD access_log and error_log
/var/log/mail/	Dieses Unterverzeichnis beinhaltet zusätzliche Logs vom Mailserver. Z.B. speichert sendmail die gesammelten Mail-Statistiken in der Datei /var/log/mail/statistics. This subdirectory contains additional logs from your mail server. For example, sendmail stores the collected mail statistics in /var/log/mail/statistics file
/var/log/prelink/	Das Programm prelink modifiziert gemeinsame Bibliotheken und verlinkte Binärdateien um den Startvorgang zu beschleunigen. /var/log/prelink/prelink.log beinhaltet Informationen zur .so Datei, die von prelink verändert wurde. Prelink program modifies shared libraries and linked binaries to speed up the startup process. /var/log/prelink/prelink.log contains the information about the .so file that was modified by the prelink.

Logdatei / logfile	Bedeutung - Inhalt – Nutzen / Meaning – content - benefit
/var/log/audit/	Beinhaltet Informationen des Linux audit daemon (auditd). Contains logs information stored by the Linux audit daemon (auditd).
/var/log/setroubleshoot/	SELinux nutzt setroubleshootd (SE Trouble Shoot Daemon) um Probleme im Sicherheitskontext von Dateien festzustellen und legt diese in dieser Datei ab. SELinux uses setroubleshootd (SE Trouble Shoot Daemon) to notify about issues in the security context of files, and logs those information in this log file.
/var/log/samba/	Beinhaltet Informationen welche von samba gespeichert werden. Contains log information stored by samba, which is used to connect Windows to Linux.
/var/log/sa/	Beinhaltet die tägliche sar Datei, welche vom Paket sysstat gesammelt werden. Contains the daily sar files that are collected by the sysstat package.
/var/log/sssd/	Wird vom system security services daemon benutzt (verwaltet Zugriffe auf entfernte Verzeichnisse und Authentifizierungs-Mechanismen). Used by system security services daemon that manage access to remote directories and authentication mechanisms.
/var/log/mariadb/mariadb.log (Redhat) /var/log/mysql/error.log (Debian) /var/log/mysqld.log /var/log/mysql.log	MySQL Logdatei in der alle Debug-, Fehler und Erfolgsmeldungen stehen. Inklusive Starten, Stoppen und Neustarten des MySQL daemon (mysqld). MySQL log file that records every debug, failure and success message, including starting, stopping and restarting of MySQL daemon mysqld.
/var/log/pureftp.log	Beobachtet FTP-Verbindungen mit Hilfe des pureftp-Prozesses. Es gibt Daten zu jeder Verbindung, FTP-Login und Authentifizierungsfehler. Monitors for FTP connections using the pureftp process. Find data on every connection, FTP login, and authentication failure here.

Logdatei / logfile	Bedeutung - Inhalt – Nutzen / Meaning – content - benefit
/var/log/xferlog	Merkt sich FTP Dateitransfers. Beinhaltet Informationen wie Dateinamen und vom Benutzer initiierte Übertragungen. Keeps FTP file transfer sessions. Includes info like file names and user-initiated FTP transfers.

Logdateien verwalten / managing logfiles

Logdateien effektiv zu verwalten ist eine grundlegende Aufgabe jedes GNU/Linux System-Administrators.

Managing log files effectively is an essential task for Linux sysadmins.

Das Programm logrotate, mit dem Protokolldateien „gedreht“ werden (indem die ältesten aus Ihrem System entfernt und neue Protokolldateien erstellt werden), bietet dafür folgende Operationen an:

The logrotate program, which „rotates“ log files (by removing the oldest ones from your system and creating new log files), offers the following operations for this purpose:

- Die Logdatei rotieren, wenn sie eine bestimmte Größe erreicht hat
  Rotate the log file when file size reaches a specific size
- Weiterloggen der Informationen in die neu erstellte Datei, nach dem rotieren der alten
  Continue to write the log information to the newly created file after rotating the old log file
- Die rotierten Logdateien komprimieren
  Compress the rotated log files
- Festlegen von Kompressionseinstellungen für die rotierten Logdateien
  Specify compression option for the rotated log files
- Rotieren der alten Logdateien mit Datum im Dateinamen
  Rotate the old log files with the date in the filename
- Ausführen benutzerdefinierter Shell-Skripte direkt nach dem Rotieren
  Execute custom shell scripts immediately after log rotation
- Entfernen älterer rotierter Logdateien
  Remove older rotated log files

Logdateien anzeigen / view log files

Um Log-Dateien anzuzeigen, kann eine der folgenden Möglichkeiten verwendet werden.

Aber bitte **nicht** „cat | more“...

To view the log files use any one of the following methods. But, please don’t do „cat | more“...

- **vi / view**: Wenn man mit den vi-Befehlen vertraut ist, kann dieser benutzt werden. View ist jedoch sicherer, da der „nur-lesen-Modus“ verwendet wird.
  If you are comfortable with the vi commands, use vi editor. However, view is safer, because it uses read-only mode.
- **tail** : Wenn der Inhalt der Log-Datei(en) in Echtzeit angesehen werden soll, benutzt man: tail -f.
  Es ist auch möglich, mehrere Log-Dateien gleichzeitig zu beobachten:
  tail -f /var/log/syslog -f /var/log/auth.log
  If you want to view the content of the log files real time, as the application is writing to it, use “tail -f”. You can also view multiple log files at the same time (using “tail -f”).
- **grep** : Wenn man genau weiß, was man in der Log-Datei sucht, kann man schnell mit dem Befehl grep nach einem Muster suchen.
  If you know exactly what you are looking for in a log file, you can quickly use grep command to grep a pattern.
- **less** : Der Befehl less ist für die Anzeige von Log-Dateien sehr gut geeignet.
  The less command is very powerful to browse log files.

Man verwendet var/log/syslog auch, um alles was sich unter syslog befindet genauer zu untersuchen. Allerdings ist es eine zeitraubende Angelegenheit eine spezielle Sache herauszusuchen, da es sich um eine recht große Datei handelt, die man durchgehen muss. Mit der Tastenkombination Shift+G springt man ganz ans Ende. Und dort steht tatsächlich auch „END“.

You also use /var/log/syslog to scrutinize anything that’s under the syslog. But picking out one particular thing will take some time because it’s usually a pretty big file to wade through. Pressing Shift+G will take you all the way to the end, and you’ll know you’re there because you will see the word “END.”

Auch dmesg kann zur Sichtung von Logdateien verwendet werden. Dies zeigt den „Kernel Ring Buffer“ an. Mit dem Befehl „dmesg | less“ kann man sich durchscrollen.

Eine weitere Einschränkung kann man durch „dmesg -facility=user“ einstellen.

You can also check logs using dmesg. This shows the kernel ring buffer and prints everything after sending you to the end of the file. You can use the dmesg | less command to scroll through everything it has produced. If you’d like to see log entries relating to the user facility, use dmesg -facility=user.

Ein weiteres, extrem praktisches Werkzeug ist tail. Es listet lediglich die letzten Zeilen der Logdatei.

Also dort, wo man häufig die Ursache für Probleme findet.

Mit „tail /var/log/syslog“ oder „tail -f /var/log/syslog“ kann man die Datei in Echtzeit verfolgen.

Für eine spezielle Anzahl nimmt man „tail -f -n 5 /var/log/syslog“ (die 5 letzten Zeilen).

Mit „Strg+C“ beendet man tail.

Finally, as a super-handy command called tail, which lets you look over log files. It’s so useful because it just displays the last bit of the logs. Which is often where you’ll find the source of the difficulty. Use tail /var/log/syslog or tail -f /var/log/syslog. Tail keeps a close eye on the log file, and displays every written to it, which lets you check what’s being added to syslog in real time.

For a particular group of lines (say, the last five) type in tail -f -n 5 /var/log/syslog, and you’ll be able to see them. Use Ctrl+C to turn off the tail command.

Schöne neue Welt mit journald / Brave new world with journald

Was ist journald? Was ist journalctl? What is journald? What is journalctl?

Journald ist der daemon von systemd welcher Logdateien aus verschiedenen Quellen wie syslog sammelt. Journalctl ist das Werkzeug zur Interaktion mit den Journal-Logs.

Mit journalctl kann man Logdateien lesen, Echtzeit-überwachen, filtern (nach Zeit, Dienst, Status und weiteren Parametern).

journald is the daemon from systemd that collects the logs from various log sources like syslog.

journalctl is the command line tool that lets you interact with the journal logs.

With journalctl, you can read logs, monitor the logs in real time, filter the logs based on time, service, severity and other parameters.

Systemd ist Standard bei den meisten großen Distributionen. Eine Hauptfunktion von systemd ist das Sammeln von Logdateien und das Bereitstellen der Werkzeuge zu deren Analyse.

In traditionellen Systemen speichert syslog in einfachen Textdateien. Lesen und Auswerten dieser Dateien erfolgt mit find, grep, cut und weiteren Befehlen.

Systemd sammelt Logdatein aus mehr Quellen als syslog und speichert diese in einem Binärformat. Hierfür wird ein Befehlszeilen-Werkzeug zum Lesen, Auswerten und Bearbeiten der Logdateien mitgeliefert.

systemd is the default on most of the major Linux distributions. One of the main features of systemd is the way it collects logs and the tools it gives for analyzing those logs.

In traditional SysVinit system, you have syslog that stores logs in plain text files. Reading and analyzing those files require the use of find, grep, cut and many other commands.

systemd collects logs from more sources than syslog, keeps the journal logs in binary format and gives you a command line tool to read, analyze and manipulate the logs. This is more streamlined than the syslogs.

Aktivieren der Journal Logs / Activating the journal

Einige GNU/Linux Distributionen, speziell die „Großen“ Desktops haben die Logs nicht automatisch aktiviert.

Der Standard-Speicherort der journald Logdateien ist /var/log/journal. Man sollte sicherstellen, dass es dieses Verzeichnis gibt. Falls nicht, sollte man es selbst anlegen.

Als nächstes sollte man sicherstellen, das in der Konfigurationsdatei /etc/systemd/journald.conf der Wert für “storage” entweder auto oder persistent lautet.

Die Datei journald.conf zeigt die Standard-Einstellungen. Also selbst wenn vor den Einstellungen ein „#“ steht, sind das die Standard-Einstellungen, welche verwendet werden.

Wenn man etwas verändern möchte, muss man das „#“ aus der Zeile entfernen.

Some Linux distributions, specially the desktop ones, don't enable the journal logs by default.

The default location of journald logs is /var/log/journal directory. You should make sure that this directory exists. If not, create it yourself. Next, in the /etc/systemd/journald.conf file make sure that the value Storage is set to either auto or persistent.

The journald.conf file shows the default values. So even if there is a # in front of the entries, it means those are the default settings being used. If you want to change anything, you remove the # from that line.

Lesen und Suchen mit journalctl / Read and search with journalctl

Wenn man einfach journalctl im Terminal eingibt, werden die Logdateien in chronologischer Abfolge angezeigt.

Journalctl verwendet „less“ unter der Haube, um die Logdateien anzuzeigen.

Dies bedeutet, dass man die selben Tastenkombinationen verwenden kann.

Nachfolgend eine kleine Auffrischung:

If you just type journalctl in the terminal, it will show the journal logs in chronological order.

journalctl uses less underneath to show you the logs. Which means you can use the same keys to move around the logs as you do with the less command.

If you don't remember that, here's a quick recall:

Taste / Key	Bedeutung / Meaning
Pfeiltasten / Arrow keys	Jeweils eine Zeile bewegen. Move by one line.
Leertaste / Space	Eine Seite nach unten bewegen. Move down one page.
b	Eine Seite nach oben bewegen. Move up one page.
g	Gehe zur ersten Zeile. Go to the first line.
G	Gehe zur letzten Zeile. Go to the last line.
100g	Gehe zur 100. Zeile. Go to the 100th line.
/string	Suche nach der Zeichenfolge von aktueller Position. Search for the string from current position.
n/N	Springe zur nächsten oder vorherigen Fundstelle. Go to the next or previous search match.
q	Die Logdateien verlassen. Exit the logs.

Zeige Logs in umgekehrter zeitlicher Abfolge / Show logs in reverse chronological order

Wie bereits erwähnt, werden die Logdateien in chronologischer Reihenfolge angezeigt. Dies bedeutet, die Ältesten werden zuerst angezeigt.

Wenn man die aktuellsten zuerst sehen möchte, kann man die Journale mit dem Parameter „-r“ in umgekehrter Reihenfolge anzeigen.

As you noticed, the logs are shown in chronological order. This means the oldest stored logs are displayed first.

If you want to see the recent logs first, you can display the journal logs in reverse order with the option „-r“.

Nur Anzahl N Zeilen anzeigen / Display only N recent lines of journal logs

Anstatt alle Logdateien anzuzeigen kann man mit dem Parameter „-n“ auch eine anzugebende Anzahl Zeilen anzeigen lassen. „journalctl -n 25“ zeigt beispielsweise die 25 aktuellsten Zeilen.

Instead of showing all logs, you can choose to display only a certain number of lines from log using the „-n“ option. For example, the command „journalctl -n 25“ will display most recent 25 lines of the logs.

Logdateien in Echtzeit anzeigen / Show journal logs in real time

Aktuelle Logdateien anzuzeigen ist eine Sache, diese in Echtzeit anzuzeigen erreicht man mit dem Parameter „-f“ (wie bei tail). Mit Strg+C verlässt man die Echtzeit-Beobachtung.

Viewing recent logs is one thing, if you want to see the logs in real time, you can use the „-f“ option (like in tail). This will display the logs in real time in the follow mode.

Use Ctrl+C command to exit the real time view.

Nur Kernel-Meldungen anzeigen / Show only kernel messages

Systemd vereinigt Logdateien verschiedenster Quellen. Wenn man lediglich Kernel-Meldungen sehen möchte, verwendet man den Parameter „-k“.

The systemd journal accumulates logs from different sources. If you just want to see Linux kernel logs, you can use the option „-k“.

Mit sudo alle Logdateien anzeigen / Use sudo to see all journal logs

Systemd ist recht eigenwillig, welche Logdateien es welchem Benutzer anzeigt.

Es zeigt einige Logdateien, einem regulären Benutzer jedoch nicht alle.

Wenn man alle Logdateien sehen möchte, muss man den Befehl mit sudo aufrufen.

Systemd is protective about what kind of logs to show to which user.

It may show some logs but not all the logs if you are a regular user.

If you want access to all the logs, you should use sudo.

Anzeigen der Logs einer bestimmten Sitzung / Show messages from a particular boot session

Das ist eine exzellente Funktion von journald. Journalctl ermöglicht es mit der Option „-b“ auf Logdateien einer bestimmten Boot-Sitzung zuzugreifen.

Man kann sich alle Boot-Sitzungen mit „--list-boots“ anzeigen lassen.

Die Ausgabe zeigt die Sitzungen mit der Bootzeit und einer Zahl, welche dieser zugewiesen ist.

This is an excellent feature of jounrald. The journalctl command allows you to access logs belonging to a specific boot session using the option „-b“. You can list all the boot sessions with „--list-boots“ flag. The output will show the boot sessions with the boot time and an integer assigned to the boot sessions.

```
-5 513008ead8464c23aab732a2feed5277 Sun 2020-07-12 20:43:38 IST—Sun 2020-07-12 22:40:02 IST
-4 caff16e3f46a4479b5287fb9e294f610 Mon 2020-07-13 07:36:04 IST—Mon 2020-07-13 19:13:44 IST
-3 5665f41cc50a4dec9955efacc2596d68 Mon 2020-07-13 20:30:55 IST—Mon 2020-07-13 22:20:34 IST
-2 c7d17407b0bd476a930af503f64b6006 Tue 2020-07-14 07:58:41 IST—Tue 2020-07-14 18:50:04 IST
-1 7ab5e04518ec455abe0e2c86fdaa46fa Tue 2020-07-14 21:19:27 IST—Tue 2020-07-14 22:42:11 IST
0 91856e86d4ee4e828717913deb288568 Wed 2020-07-15 08:11:51 IST—Wed 2020-07-15 17:14:10 IST
```

Boot-Sitzung 0 ist die aktuelle Sitzung. Boot Sitzung -1 ist die letzte Sitzung, usw.

Um die Vorvorletzte Sitzung anzuzeigen wird folgendes eingegeben:

Boot session 0 is the current boot session. Boot session -1 is the last booted session and so on.

To show the session bevor the last one, you have to type the following:

```
journalctl -b -2
```

Logdateien nach einem bestimmten Dienst filtern / Filter journal logs for a specific systemd service

Filtern ist eine wichtige Funktion bei Logdateien. Man kann Logdateien mit „journalctl -u dienst“ basierend auf systemd Diensten filtern.

Filtering is a strong point of journal logs. You can filter logs based on the systemd services with „journalctl -u service_name“.

Wenn man beispielsweise Logdateien von SSH anzeigen will, verwendet man das:

For example, if you want to see logs generated by SSH, you can use it like this:

```
journalctl -u ssh
```

Man muss natürlich die Namen der Dienste kennen.

You'll need to know the systemd service name of course.

Logdateien auf einen bestimmten Zeitintervall filtern / Filter logs for a certain time interval

Dies ist ein weiteres Beispiel für die Zeichenketten-Filterung der Journale.

Man kann Logdateien mit verschiedenen Methoden nach einem bestimmten Zeitraum filtern.

Und das sogar mit „natürlicher“ Sprache. (Englische) Begriffe wie „yesterday“, „today“ und „tomorrow“ werden erkannt.

This is another example of the string filtering capability of the journal logs. You can filter logs for a certain time period and there are various ways to do that.

You may use natural language to filter the logs. Terms like yesterday, today and tomorrow are recognized.

```
journalctl --since=yesterday --until=now
```

Es können auch Datums oder Datums-Zeit-Kombinationen angegeben werden.

You can also specify date or date time combination:

```
journalctl --since "2022-04-10"
```

```
journalctl --since "2022-04-10 15:10:00" --until "2022-04-12"
```

Die Uhrzeit beginnt um 00:00:00 und bestimmt Tag und Datum.

Es können auch relative Zeitangaben wie „-1h20min“ gemacht werden um 1 Stunde und 20 Minuten in die Vergangenheit zu blicken.

Time starts at 00:00:00 and it determines the day and date.

You can also use relative time like „-1h20min“ to specify 1 hour 20 minutes in the past.

Logdateien auf Basis von UID, GID oder PID filtern / Filter logs based on UID, GID and PID

Wenn man einen Fehler untersucht, will man vielleicht die Logs nach einen bestimmten Prozess mit dessen PID durchsuchen.

Die Logdateien können auch nach Benutzer-ID (UID), Gruppe (GID) und Prozess-ID (PID) gefiltert werden:

If you are debugging an issue, you may want to check the logs for a certain process using its PID.

The journal logs can also be filtered on User ID (UID), Group ID (GID) and Process ID (PID). Below is an example:

```
journalctl _PID=1234
```

Kombinieren von Optionen für ein spezifischeres Ergebnis / Combine more than one options for more tailored log viewing

Es können auch mehrere Optionen kombiniert werden.

Wenn man beispielsweise nur SSH Logdateien von gestern mit UTC Zeitstempeln sehen will:

You can combine several options to view the desired logs.

For example, if you want to see only SSH logs from yesterday in UTC timestamps, you can use:

```
sudo journalctl -u ssh --since=yesterday --utc
```

Eine weitere Anwendungsmöglichkeit ist auch, die Logdateien nach Boot Sitzungen zu filtern.

Für die SSH Logdateien in der aktuellen Sitzung verwendet man:

Another common usage is to filter logs based on boot sessions. If you want to see only the SSH logs in the current session, you can use:

```
sudo journalctl -u ssh -b0
```

Die letzten Logs anzeigen / Viewing the last few logs

Viele Nutzer empfehlen oft, den Befehl „journalctl -xe“ zu verwenden.
You'll often find people suggesting to use „journalctl -xe“.

-e: Jump to the end of the journal logs / springe an das Ende der Logdatei
-x: Show extra information on the log entries (if available) / Zusatzinformationen (wenn verfügbar)

Einige Log-Einträge bieten zusätzliche Informationen, die nicht beim normalen Anzeigen gezeigt werden. Der Schalter „-x“ zeigt diese an.
Some log entries have additional information that are not displayed in the normal log viewing. Using the „-x“ option may display such information.
Anstatt einer einzigen Zeile wie dieser:
What you see as a single line like this:

```
Jul 09 16:33:40 wohnzimmer systemd[1]: Started Run anacron jobs.
```

Könnte es wesentlich mehr Informationen anzeigen:
It could display more information like this:

```
Jul 09 16:33:40 wohnzimmer systemd[1]: Started Run anacron jobs.
-- Subject: A start job for unit anacron.service has finished successfully
-- Defined-By: systemd
-- Support: http://www.ubuntu.com/support
--
-- A start job for unit anacron.service has finished successfully.
--
-- The job identifier is 3702.
```

Die zusätzlichen Informationen helfen, das Umfeld eines Fehlers oder Log-Ereignisses zu klären.
The additional info helps explain the context of an error or log event and the possible solutions.

Nur Fehler in Logdateien anzeigen / Show only errors in logs with journalctl

Um nur Fehler in der aktuellen Sitzung anzuzeigen verwendet man:
To show all the errors in the current session, you can use:

```
journalctl -p 3 -xb
```

Bedeutung der Schalter:
The options mean:
-p 3: filter logs for priority 3 (which is error) / filtern nach Priorität 3 (Fehler)
-x: provides additional information on the log (if available) / Zusatzinformationen (wenn verfügbar)
b: since last boot (which is the current session) / seit dem letzten Bootvorgang (aktuelle Sitzung)

Es können auch andere Prioritäts-Ebenen verwendet werden.
Die folgende Tabelle zeigt die Möglichkeiten.
You can also use other priority levels. This table lists all the priority levels.

Priorität / Priority	Code / Code
0	emerg
1	alert
2	crit
3	err
4	warning
5	notice
6	info
7	debug

Man kann auch Logdateien für einen Ereignis-Bereich anzeigen.
Will man beispielsweise alle Warnungen, Anmerkungen und Infos der aktuellen Sitzung sehen, verwendet man das:
You can also display logs for a range of severity. For example, if you want to see all the warning, notice and info logs from the current session, you can use:

```
journalctl -p 4..6 -b0
```

Es wäre auch möglich gewesen, „warning..info“ statt „4..6“ anzugeben.
You could have also used „warning..info“ in the above command instead of „4..6“.

Prüfen der Logdatei-Größe / Check how much disk space logs are taking

Journald sammelt Logdateien aus verschiedensten Quellen und speichert diverse Ebenen inklusive Debug-Logdateien. Obwohl Logdateien sehr hilfreich beim Analysieren und Lösen auftretender Probleme sind, können diese durchaus recht groß werden.
Mit dem folgenden Befehl kann man diese Größe ermitteln:
The journald collects logs from various sources and it stores logs of various levels including debug logs. Trust me, while retaining logs help in analyzing and auditing, they can take considerable amount of disk space.
You can check how much disk space the journal logs are taking with this journalctl command:

```
journalctl --disk-usage
```

```
edi@wohnzimmer:~$ journalctl --disk-usage
Archived and active journals take up 2.8G in the file system.
```

Logdateien löschen bzw. bereinigen / delete or clear log files

Das Erste was man tun sollte, ist die Logdateien zu rotieren. Das markiert das aktuelle Journal als aktiv und erzeugt neue Logs. Das ist optional, aber eine gute Angewohnheit.

First thing you should do is to rotate journal files. This will mark the currently active journal logs as archive and create fresh new logs. It's optional but a good practice to do so.

```
sudo journalctl --rotate
```

Es gibt drei Möglichkeiten alte Logdateien zu bereinigen. Man löscht Logdateien, die älter sind als ein gegebenes Datum, sorgt dafür dass die Logdateien eine bestimmte Größe nicht überschreiten oder die Anzahl der Logdateien begrenzt wird.

Now you have three ways to clear old journal logs. You delete logs older than a certain time or you delete older log files so that total log size is limited to the predefined disk space or you limit number of log files.

Journaldateien älter als x Tage löschen / Clear journal log older than x days

Es ist zu bedenken, dass Logdateien wichtig zur Fehlersuche sind und man deshalb nicht alle auf einmal löschen sollte. Ein Beispiel: Aufbewahren aller Logs für zwei Tage.

Der entsprechende Befehl zum Löschen aller Dateien älter als zwei Tage lautet:

Keep in mind that logs are important for auditing purpose so you should not delete all of them at the same time. Let's say you want to keep the log history of just two days. To delete all entries older than two days, use this command:

```
sudo journalctl --vacuum-time=2d
```

Die Ausgabe könnte dann so lauten:

Here's what the output may look like:

```
Vacuuming done, freed 1.6G of archived journals from /var/log/journal/
1b9ab93094fa4978beba80fd3c48a18c
```

Die Zeitspanne kann auch in Stunden (2h), in Minuten (2m), Sekunden (2s) angegeben werden.

Auch längere Zeitspannen sind möglich: 2weeks, 2months

You can also change the provide time frame in hours like 2h, in minutes like 2m, in seconds like 2s. If you want bigger time units, you can 2weeks, 2months as well.

Bestimmte Größe für Logdateien vorgeben / Restrict logs to a certain size

Eine weitere Möglichkeit ist es, die Dateigröße der Logdateien zu beschränken. Damit werden alle Logdateien gelöscht, bis das angegebene Limit erreicht wurde.

Another way is to restrict the log size. With this, it will delete the journal log files until the disk space taken by journal logs falls below the size you specified.

```
sudo journalctl --vacuum-size=100M
```

Das verringert die Logdatei-Größe auf etwa 100MB.

This will reduce the log size to around 100 MB.

```
Vacuuming done, freed 40.0M of archived journals from /var/log/journal/
1b9ab93094fa4978beba80fd3c48a18c.
```

Die Größe kann mit G (für GB), M (für MB) und K (für KB) angegeben werden.

You can specify the size in GB with G, MB with M, KB with K etc.

Anzahl der Logdateien einschränken / Restrict number of log files

Die dritte Möglichkeit besteht darin, die Anzahl der Logdateien zu beschränken.

Journalctl hat normalerweise Logdateien für das System und den Benutzer. Wenn die Logdateien älter werden, werden sie in verschiedenen Dateien archiviert.

Diese Anzahl Archive kann man beschränken. Es soll nur fünf Logdateien geben.

The third way is to limit the number of log files. The journalctl usually has log files for the system and for the users. As the logs get old they are archived in various files.

You can limit the number of archive log files. Let's say you want to have only five log files.

```
journalctl --vacuum-files=5
```

Das entfernt die älteren archivierten Logdateien und lässt lediglich die spezifizierte Anzahl übrig.

It will remove the older archive log files leaving only the specified number of log files.

Quellen / References

https://www.thegeekstuff.com/2011/08/linux-var-log-files/
https://linuxhandbook.com/journalctl-command/