Linux Log Files Location And How Do I View Logs Files on Linux?

Author: Vivek Gite Last updated: April 12, 2023 90 comments

I am a new Linux user. I would like to know where are the log files located under Debian/Ubuntu or CentOS/RHEL/Fedora Linux server? How do I open or view log files on Linux operating systems?

Almost all logfiles are located under `/var/log` directory and its sub-directories on Linux. You can change to this directory using the cd command. Of course, you need to be the root user to access log files on Linux or Unix-like operating systems. You can use the following commands to see the log files which are in text format:

Tutorial details	
Difficulty level	Easy
Root privileges	Yes
Requirements	Linux terminal
Category	System Management
OS compatibility	Alma • Alpine • Amazon Linux • Arch • CentOS • Debian • Fedora • Linux • Mint • openSUSE • Pop!_OS • RHEL • Rocky • Stream • SUSE • Ubuntu • WSL
Est. reading time	7 minutes

1. less command
2. more command
3. cat command
4. grep command
5. egrep command
6. tail command
7. zcat command
8. zgrep command
9. zmore command
10. dmesg command
11. journalctl command

How do I view log files on Linux?

Open the Terminal or login as root user using ssh command. Go to /var/log directory using the following cd command:

```
# cd /var/log
```

To list files use the following ls command:

```
# ls
```

Sample outputs from RHEL 6.x server:

```
anaconda.ifcfg.log    boot.log-20111225  cron-20131110.gz       maillog-
20111218      messages-20131103.gz  secure-20131027.gz   spooler-
20131117.gz  up2date-20131117.gz


anaconda.log         btmp              cron-20131117.gz       maillog-20111225
messages-20131110.gz  secure-20131103.gz   squid              uptrack.log


anaconda.program.log  btmp-20120101      cups                  maillog-20120101
messages-20131117.gz  secure-20131110.gz   swinstall.d          uptrack.log.1


anaconda.storage.log  btmp-20131101.gz   dkms_autoinstaller      maillog-
20131027.gz   mysqld.log            secure-20131117.gz   tallylog
uptrack.log.2
```

```
anaconda.syslog      collectl          dmesg                maillog-20131103.gz
ntpstats             setroubleshoot      UcliEvt.log          varnish

anaconda.yum.log     ConsoleKit        dmesg.old            maillog-20131110.gz
prelink              spooler             up2date              wtmp

arcconfig.xml        cron              dracut.log           maillog-20131117.gz
rhsm                 spooler-20111211    up2date-20111211     yum.log

atop                 cron-20111211     dracut.log-20120101    messages
sa                   spooler-20111218    up2date-20111218     yum.log-20120101

audit                cron-20111218     dracut.log-20130101.gz  messages-
20111211     secure              spooler-20111225    up2date-20111225
yum.log-20130101.gz

boot.log             cron-20111225     httpd                messages-20111218
secure-20111211      spooler-20120101    up2date-20120101

boot.log-20111204    cron-20120101     lastlog              messages-20111225
secure-20111218      spooler-20131027.gz  up2date-20131027.gz

boot.log-20111211    cron-20131027.gz   maillog             messages-
20120101     secure-20111225     spooler-20131103.gz  up2date-20131103.gz

boot.log-20111218    cron-20131103.gz   maillog-20111211     messages-
20131027.gz  secure-20120101     spooler-20131110.gz  up2date-
20131110.gz
```

To view a common log file called /var/log/messages use any one of the following command:

```
# less /var/log/messages
```

```
# more -f /var/log/messages
```

```
# cat /var/log/messages
```

```
# tail -f /var/log/messages
# grep -i error /var/log/messages
```

Here is what I see:

```
Jul 17 22:04:25 router  dnsprobe[276]: dns query failed

Jul 17 22:04:29 router last message repeated 2 times

Jul 17 22:04:29 router  dnsprobe[276]: Primary DNS server Is Down... Switching
To Secondary DNS server

Jul 17 22:05:08 router  dnsprobe[276]: Switching Back To Primary DNS server

Jul 17 22:26:11 debian -- MARK --

Jul 17 22:46:11 debian -- MARK --

Jul 17 22:47:36 router  -- MARK --

Jul 17 22:47:36 router  dnsprobe[276]: dns query failed

Jul 17 22:47:38  debian kernel: rtc: lost some interrupts at 1024Hz.

Jun 17 22:47:39  debian kernel: IN=eth0 OUT=
MAC=00:0f:ea:91:04:07:00:08:5c:00:00:01:08:00 SRC=61.4.218.24
DST=192.168.1.100 LEN=60 TOS=0x00 PREC=0x00 TTL=46 ID=21599 DF
PROTO=TCP SPT=59297 DPT=22 WINDOW=5840 RES=0x00 SYN URGP=0
```

Common Linux log files names and usage

- `/var/log/messages` : General message and system related stuff
- `/var/log/auth.log` : Authenication logs
- `/var/log/kern.log` : Kernel logs
- `/var/log/cron.log` : Crond logs (cron job)
- `/var/log/maillog` : Mail server logs
- `/var/log/qmail/` : Qmail log directory (more files inside this directory)

- `/var/log/httpd/` : Apache access and error logs directory
- `/var/log/lighttpd/` : Lighttpd access and error logs directory
- `/var/log/nginx/` : Nginx access and error logs directory
- `/var/log/apt/` : Apt/apt-get command history and logs directory
- `/var/log/boot.log` : System boot log
- `/var/log/mysqld.log` : MySQL database server log file
- `/var/log/secure` or `/var/log/auth.log` : Authentication log
- `/var/log/utmp` or `/var/log/wtmp` : Login records file
- `/var/log/yum.log` or `/var/log/dnf.log`: Yum/Dnf command log file.

Printing the Linux kernel ring buffer messages

We use the dmesg command to examine or control the kernel ring buffer. The default action is to display all messages from the kernel ring buffer. For example:

```
$ sudo dmesg
```

```
$ sudo dmesg | grep 'error'
```

```
$ sudo dmesg | grep -i -E 'error|warn|failed'
```

```
$ sudo dmesg | more
```

Sample outputs:

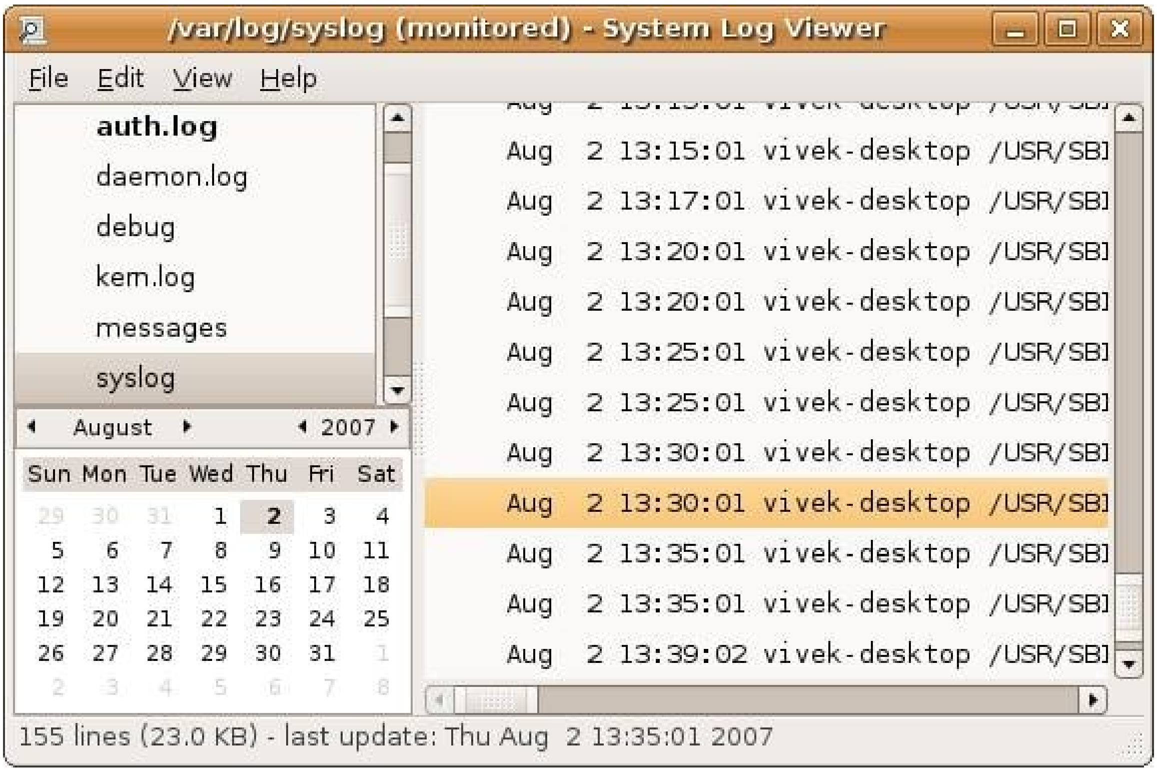
```
[sudo] password for vivek:

[78637.759323] thermal thermal_zone14: failed to read out thermal zone (-61)

[83556.712080] thermal thermal_zone14: failed to read out thermal zone (-61)

[88912.931783] thermal thermal_zone14: failed to read out thermal zone (-61)

[89824.197634] thermal thermal_zone14: failed to read out thermal zone (-61)

[103175.274428] thermal thermal_zone14: failed to read out thermal zone (-61)
```

```
[104087.896937] thermal thermal_zone14: failed to read out thermal zone (-
61)
```

GUI tool to view log files on Linux

System Log Viewer is a graphical, menu-driven viewer that you can use to view and monitor your system logs. This tool is only useful on your Linux powered laptop or desktop system. Most server do not have X Window system installed. You can start System Log Viewer in the following ways:

Click on System menu > Choose Administration > System Log:

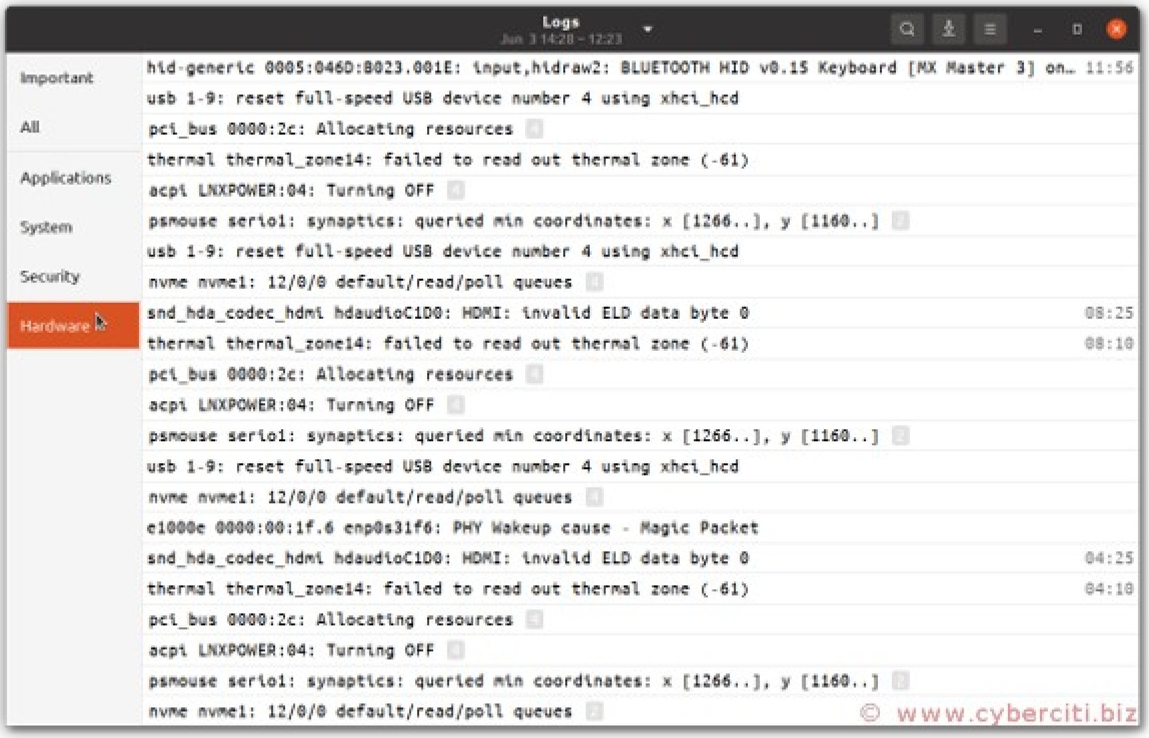


```
Aug  2 13:15:01 vivek-desktop /USR/SBI
Aug  2 13:17:01 vivek-desktop /USR/SBI
Aug  2 13:20:01 vivek-desktop /USR/SBI
Aug  2 13:20:01 vivek-desktop /USR/SBI
Aug  2 13:25:01 vivek-desktop /USR/SBI
Aug  2 13:25:01 vivek-desktop /USR/SBI
Aug  2 13:30:01 vivek-desktop /USR/SBI
Aug  2 13:30:01 vivek-desktop /USR/SBI
Aug  2 13:35:01 vivek-desktop /USR/SBI
Aug  2 13:35:01 vivek-desktop /USR/SBI
Aug  2 13:39:02 vivek-desktop /USR/SBI
```

155 lines (23.0 KB) - last update: Thu Aug 2 13:35:01 2007

Fig.01 Gnome log file viewer

Modern log viewer from Ubuntu desktop:



```
hid-generic 0005:046D:B023.001E: input,hidraw2: BLUETOOTH HID v0.15 Keyboard [MX Master 3] on… 11:56
usb 1-9: reset full-speed USB device number 4 using xhci_hcd
pci_bus 0000:2c: Allocating resources
thermal thermal_zone14: failed to read out thermal zone (-61)
acpi LNXPOWER:04: Turning OFF
psmouse serio1: synaptics: queried min coordinates: x [1266..], y [1160..]
usb 1-9: reset full-speed USB device number 4 using xhci_hcd
nvme nvme1: 12/0/0 default/read/poll queues
snd_hda_codec_hdmi hdaudioC1D0: HDMI: invalid ELD data byte 0                                     08:25
thermal thermal_zone14: failed to read out thermal zone (-61)                                     08:10
pci_bus 0000:2c: Allocating resources
acpi LNXPOWER:04: Turning OFF
psmouse serio1: synaptics: queried min coordinates: x [1266..], y [1160..]
usb 1-9: reset full-speed USB device number 4 using xhci_hcd
nvme nvme1: 12/0/0 default/read/poll queues
e1000e 0000:00:1f.6 enp0s31f6: PHY Wakeup cause - Magic Packet
snd_hda_codec_hdmi hdaudioC1D0: HDMI: invalid ELD data byte 0                                     04:25
thermal thermal_zone14: failed to read out thermal zone (-61)                                     04:10
pci_bus 0000:2c: Allocating resources
acpi LNXPOWER:04: Turning OFF
psmouse serio1: synaptics: queried min coordinates: x [1266..], y [1160..]
nvme nvme1: 12/0/0 default/read/poll queues
```

A note about rsyslogd

All of the above logs are generated using rsyslogd service. It is a system utility providing support for message logging. Support of both internet and unix domain sockets enables this utility to support both local and remote logging. You can view its config file by tying the following command:

```
# vi /etc/rsyslog.conf
```

```
# ls /etc/rsyslog.d/
```

In short /var/log is the location where you should find all Linux logs file. However, some applications such as httpd have a directory within /var/log/ for their own log files. You can rotate log file using logrotate software and monitor logs files using logwatch software.

A note about systemd journal on modern Linux distros

systemd-journald is a system service on modern Linux distro that comes with systemd. It collects and stores logging data. In addition, it creates and maintains structured, indexed journals based on logging information received from various sources such as Linux Kernel log messages via kmsg. Therefore, we need to use the journalctl command to query the contents of the systemd-journald.

Linux journalctl command examples

Without any arguments, all collected logs are shown unfiltered as follows:

```
$ journalctl
```

View all boot messages:

```
$ journalctl -b
```

Want to see kernel logs from previous boot? Try:

```
$ journalctl -k -b -1
```

See log by systemd unit or sevice

Display a live log display from a system service apache.service or nginx.service:

```
$ journalctl -f -u apache
```

```
$ journalctl -f -u nginx
```

The `-u` switch can be used multiple time to save typing at the CLI. For example:

```
$ journalctl -f -u apache.service -u php-cgi.service -u mysqld.service
```

We can follow log in real time. Like `tail -f /var/log/nginx/foo.log`:

```
$ journalctl -u mysqld.service -f
```

```
$ journalctl -u nginx.service -f
```

```
$ journalctl -f
```

Only display last 10 log entries:

```
$ journalctl -n 10 -u nginx.service
```

Executable log

See all logs generated by the D-Bus or app executable

```
$ journalctl /usr/bin/dbus-daemon
```

```
$ journalctl /usr/local/bin/app
```

Time ranges

We can see logs created using time ranges. For instnace:

```
$ journalctl --since "30 min ago"
```

```
$ journalctl --since "1 hour ago"
```

```
$ journalctl --since "1 days ago"
# The date and time format is YYYY-MM-DD HH:MM:SS
# So we can do
```

```
$ journalctl --since "2020-06-06"
$ journalctl --since "2020-06-06 10:42:00"
```

```
$ journalctl --since "2020-06-04 10:42:00" --until "2020-06-07 10:42:00"
```

View log by user ID (UID) or PID

See log for user ID # 300

```
$ sudo journalctl _UID=300
```

View log for PID # 4242

```
$ sudo journalctl _PID=4242
```

Reverse output so that the newest entries are displayed first

Try:

```
$ journalctl -r
```

```
$ journalctl -r -u apache.service
```

Show only Linux kernel messages

```
$ journalctl -k
```

```
$ journalctl --dmesg
```

Filter log files (grep like syntax)

We can filter output to entries where the MESSAGE= field matches the specified regular expression. PERL-compatible regular expressions are used. For instance:

```
$ journalctl -k -g PATTERN
```

```
$ journalctl -u mysqld.service -g PATTERN
```

```
$ journalctl -u nginx.service -g 'error'
```

```
$ journalctl -k -g failed
```

Click to enlarge

Please note that if the pattern is all lowercase, matching is case insensitive. Otherwise, matching is case sensitive. This can be overridden with the `--case-sensitive` option.