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

www.cyberciti.biz/faq/linux-log-files-location-and-how-do-i-view-logs-files/

by Vivek Gite on July 17, 2006 last updated December 6, 2014 in Commands , File system , Linux

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. You need be the root user to view or access log files on Linux or Unix like operating systems. You can use the following commands to see the log files:

1. less command
2. more command
3. cat command
4. grep command
5. tail command
6. zcat command
7. zgrep command
8. zmore 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
```

Sample outputs:

```
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/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` : Yum command log file.

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:
```

Sample outputs:

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.

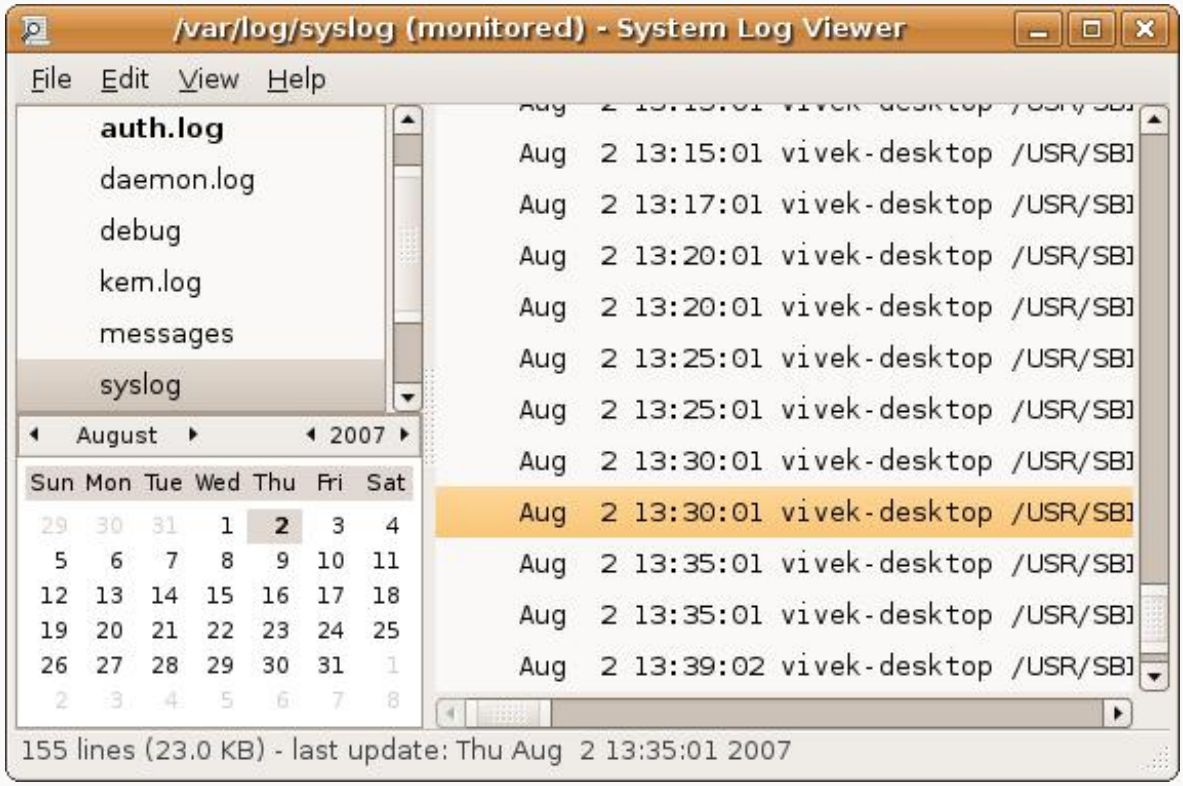

Fig.01 Gnome log file viewer