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

Author : Lalit Vohra

Categories : Linux Explained, Uncategorized

Date : May 5, 2015

- Facebook
- Twitter
- Google+
- Gmail

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

If you spend lot of time in Linux environment, it is essential that you know where the log files are located, and what is contained in each and every log file.When your systems are running smoothly, take some time to learn and understand the content of various log files, which will help you when there is a crisis and you have to look though the log files to identify the issue.

Log files are files that contain messages about the system, including the kernel, services, and applications running on it. There are different log files for different information. For example, there is a default system log file, a log file just for security messages, and a log file for cron tasks.

Log files can be very useful when trying to troubleshoot a problem with the system such as trying to load a kernel driver or when looking for unauthorized login attempts to the system. This topic discusses where to find log files, how to view log files, and what to look for in log files.

rsyslog Daemon

rsyslog Daemon

Some log files are controlled by a daemon called rsyslogd. The rsyslogd daemon is an enhanced replacement for previous **sysklogd**, and provides extended filtering, encryption protected relaying of messages, various configuration options, input and output modules, support for transportation via the TCP or UDP protocols. Note that **rsyslog** is compatible with **sysklogd**.

/etc/rsyslog.conf controls what goes inside some of the log files.

Have a Look at /etc/rsyslog.conf file:

/etc/rsyslog.conf Configuration file for rsyslog.

#

For more information see

/usr/share/doc/rsyslog-doc/html/rsyslog_conf.html

#

Default logging rules can be found in /etc/rsyslog.d/50-default.conf.

##################

MODULES

##################

$ModLoad imuxsock # provides support for local system logging

$ModLoad imklog # provides kernel logging support

#$ModLoad immark # provides –MARK– message capability

provides UDP syslog reception

```
#$ModLoad imudp

#$UDPServerRun 514

# provides TCP syslog reception

#$ModLoad imtcp

#$InputTCPServerRun 514

# Enable non-kernel facility klog messages

$KLogPermitNonKernelFacility on


###########################

#### GLOBAL DIRECTIVES ####

###########################

#

# Use traditional timestamp format.

# To enable high precision timestamps, comment out the following line.

#

$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# Filter duplicated messages

$RepeatedMsgReduction on

# #

# Set the default permissions for all log files.

#

$FileOwner syslog

$FileGroup adm
```

```
$FileCreateMode 0640

$DirCreateMode 0755

$Umask 0022

$PrivDropToUser syslog

$PrivDropToGroup syslog

# Where to place spool and state files

#$WorkDirectory /var/spool/rsyslog

# Include all config files in /etc/rsyslog.d/

# $IncludeConfig /etc/rsyslog.d/*.conf
```

This is config file, which is very important for us , when we make our server a centralized log server.

As this is very big file.If you analyze this file, you can have look at entries for many log files.

For example, following is the entry in rsyslog.conf for /var/log/messages.

less /etc/rsyslog.conf

1

*.info;mail.none;authpriv.none;cron.none

1 /var/log/messages

2	
3	The same as for many more log files.

In the above output,

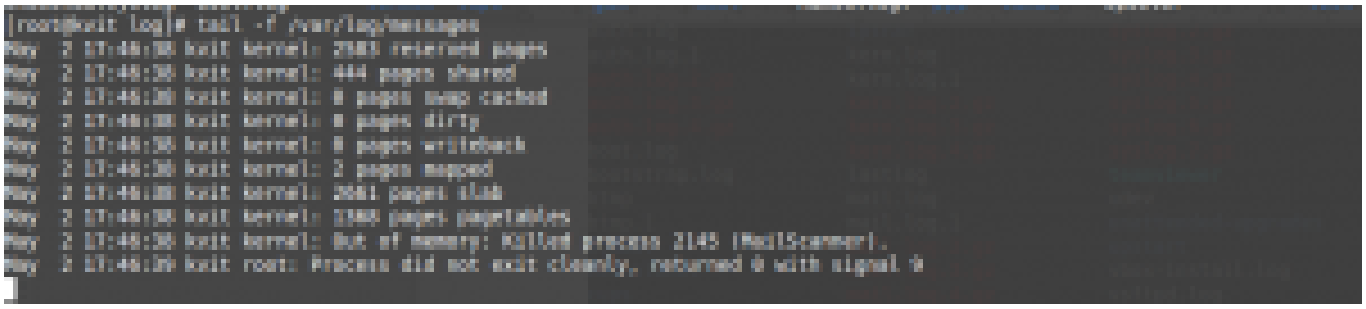
- *.info indicates that all logs with type INFO will be logged.
- mail.none,authpriv.none,cron.none indicates that those error messages should not be logged into the /var/log/messages file(most common logs of server or linux machine , which you can find here in this file.)
- You can also specify *.none, which indicates that none of the log messages will be logged.

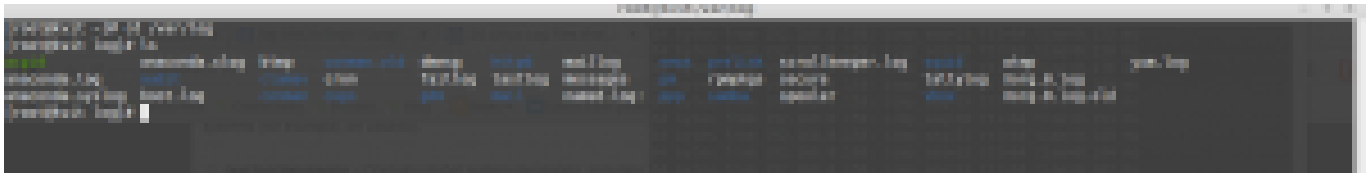
1

Different log files and their features

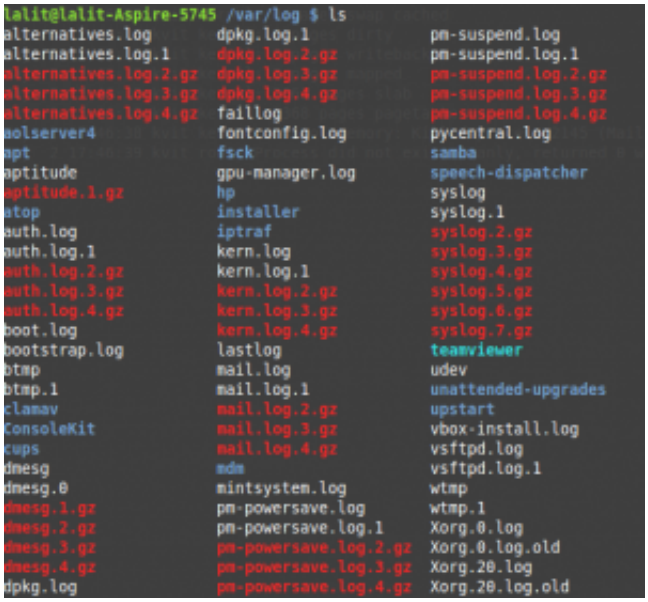
Different log files and their features. The following are the different log files that are located under /var/log/ directory. Some of these log files are distribution specific. For example, you'll see dpkg.log on Debian based systems (for example, on Ubuntu). Almost all log files are located under /var/log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

1./var/log/messages – Contains global system messages, including the messages that are logged during system start up. There are several things that are logged in /var/log/messages including mail, cron, daemon, kern, auth, etc .DHCP and DNS related logs for our servers also captured in /var/log/messages. Have a look at these logs of my machine Centos 5.x

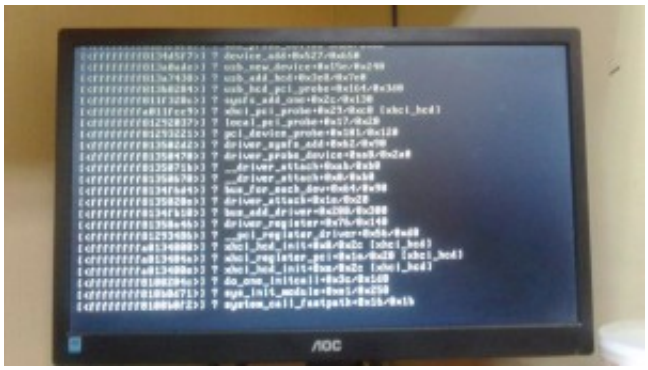




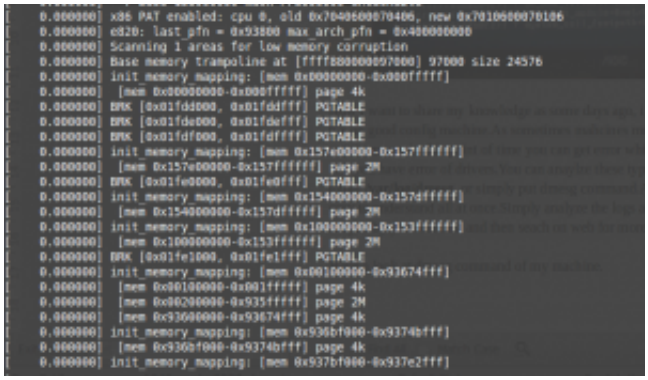
Now have a look at my linux mint(Debian machine).



2. /var/log/dmesg – 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.



Now i want to share my knowledge as some days ago, i had problem in getting installation of Centos 6.x on good configuration machine.As sometimes machines motherboard does not matched with OS requirements.At this point of time you can get error while installation (snapshot above), but if it is installed and then still you have error of drivers.You can analyse these type of kernel buffers, drivers related errors in either **/var/log/dmesg** or simply put dmesg command.As these logs are very wide long file,it is not easy to understand all at once.Simply analyse the logs and gets the lines you can understand and analyse by yourself first and then search on web for more. Have a look at dmesg command of my machine.



This is the snapshot of dmesg command.As you can not view these logs at once.You have to use dmesg command like. It will help you to view more easily and you can use up and down keys for to view and more comfortable format for view.

How to view files and logs.

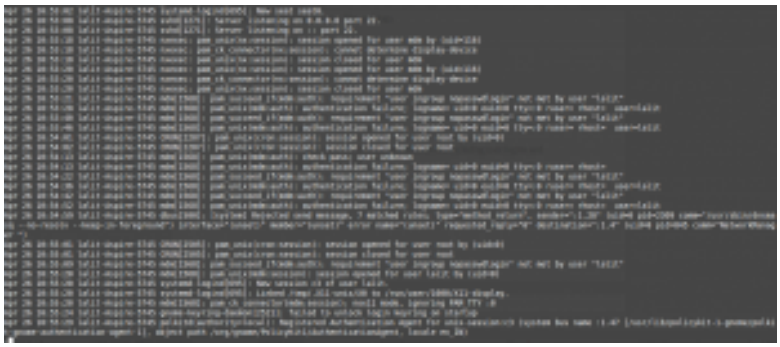
Have a look at some types to view files and logs.

1. less command
2. more command

3. cat command
4. grep command
5. tail command
6. zcat command
7. zgrep command
8. zmore command

More log files

3. /var/log/auth.log – Contains system authorization information, including user logins and authentication machinsm that were used. Have a look at this snapshot and these lines which i have taken from this snapshot.



Apr 26 10:54:36 lalit-Aspire-5745 mdm[1568]: pam_unix(mdm:auth): authentication failure; logname= uid=0 euid=0 tty=:0 ruser= rhost= user=lalit

Apr 26 10:54:42 lalit-Aspire-5745 mdm[1568]: pam_succeed_if(mdm:auth): requirement “user ingroup nopasswdlogin” not met by user “lalit”.

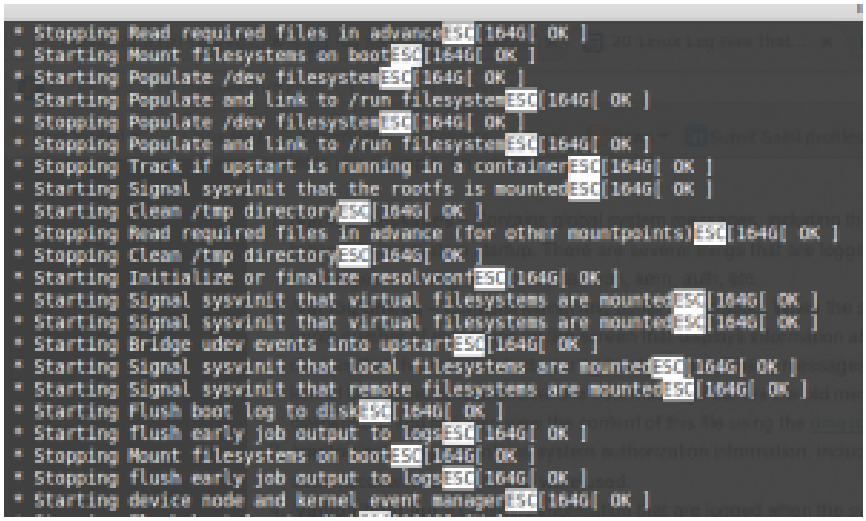
Here you can analyze that some where you can see authorization failure , it shows that i had given wrong Password for lalit user to login ,due to which it shows authorization failure in logs with reason also as required password not met by user lalit.

tail -f /var/log/auth.log Remember if you want to view all the previous logs in log file , you can use less command ,other then this if you want to view real time logs, you can use tail command with -f option.

-f, –follow[={name|descriptor}] output appended data as the file grows; -f, –follow, and –follow=descriptor are equivalent

4. **/var/log/boot.log** – Contains information that are logged when the system boots lalit@lalit-Aspire-5745 /var/log $ less boot.log Have a look at this snapshot for this log, you will get better

understanding

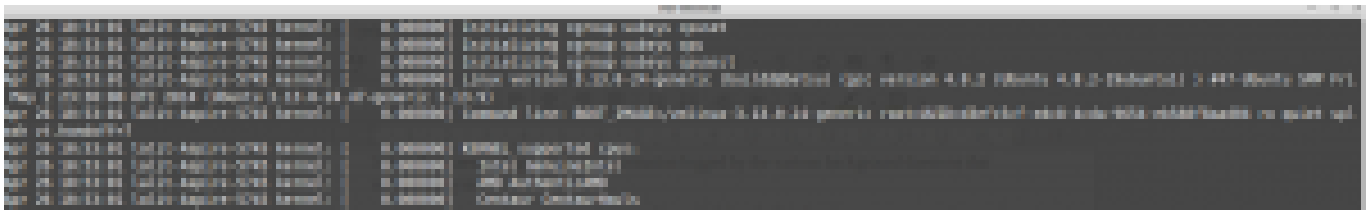


If look at linux machine initially ,when you boot or reboot linux machine.Initially it will show you all the file-systems that it is mounting or many others events which takes place while going through this phase.Contains information and grub, boot-able files, file-systems.

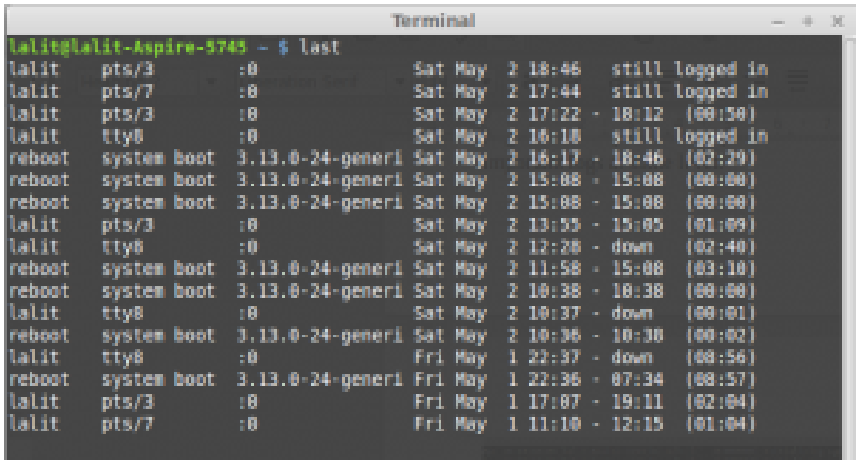
5. **/var/log/daemon.log** – Contains information logged by the various background daemons that runs on the system Note: Daemons are the services in linux,such as vsfpd, httpd, dhcpd.A *daemon* is a type of program that runs on Unix-like operating systems unobtrusively in the background, rather than under the direct control of a user, waiting to be activated by the occurrence of a specific event or condition. Unix-like systems typically run numerous daemons, mainly to accommodate requests for services from other computers on a network, but also to respond to other programs and to hardware activity.

6. /var/log/dpkg.log – Contains information that are logged when a package is installed or removed using dpkd command. These are basically on debain based operating systrems.

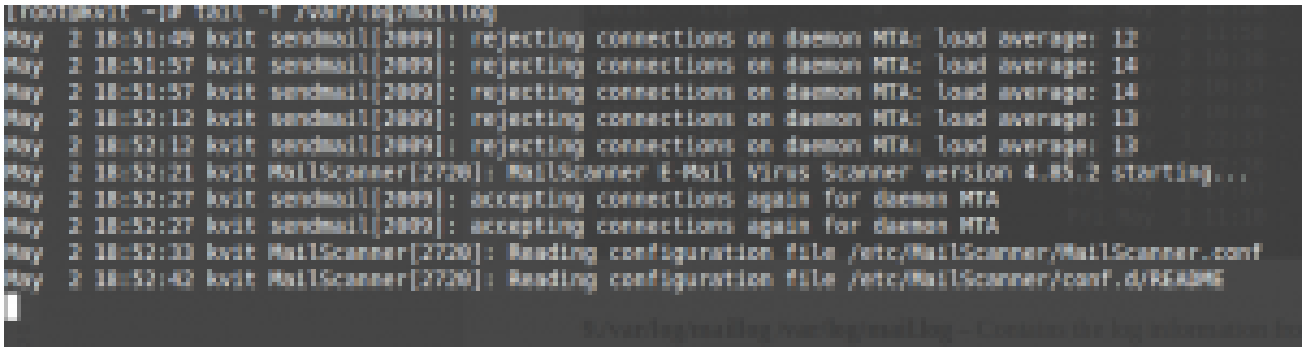
7. **/var/log/kern.log** – Contains information logged by the kernel. Helpful for you to troubleshoot a custom-built kernel. These logs basically shows us the kernel informations and process , memory ,registers at deep level.So experience makes us better to understand these logs.As these are very important logs at some level.



8. /var/log/lastlog – 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. In some linux machines these logs are not human readable format, so you can use alternate command at any time in machine or server to view logs related to user activities and reboot by last command. # last Here you can see that lalit has login at following terminals(below snapshot),at particular time and showing the time which machine rebooted.So, it is also very much important logs at the time when your server got hacked or you see some nasty events on server.It will help you a lot.



9./var/log/maillog /var/log/mail.log – 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. These are very important logs as we are working on mail servers (Like zimbra , sendmail, postfix, exim,qmail).So to view any activity on mail servers whether mails are sent or not,mails are in quese,spamming or any events related to mail servers. This snapshot is example of maillogs of sendmail server, which i have installed on my linux machine.While having at real time , you can also real time feeling of anylyzing these logs.



Some more log files

10. /var/log/user.log – Contains information about all user level logs.

11./var/log/Xorg.x.log – Log messages from the X or Deskop related logs.As mostly we keep our linux servers at cli mode or runlevel 3.Some we need to have access to vnc servers or some desktop related activities, we some X or Desktop.At these times these logs are very much important to troubleshoot errors.

12. /var/log/alternatives.log – Information by the update-alternatives are logged into this log file. On Ubuntu, update-alternatives maintains symbolic links determining default commands.

13. /var/log/btmp – This file contains information about failed login attemps. Use the last command to view the btmp file. For example, “last -f /var/log/btmp | more” .

These are some questions in our mind. My /var/log/btmp file is 1.3 GB in size. I’ve read that the file is “Used to store information about failed login”. What does this mean for my server? And can i delete this file?

This means people are trying to brute-force your passwords (common on any public-facing server). One way to reduce this is to change the port for SSH from 22 to something arbitrary.

For some additional security, Deny Hosts can block login attempts after a certain number of failures. Try to complely block it from linux firewall(iptables).

Check the ip and got information of ip and domain from google or some websites which provides these information.

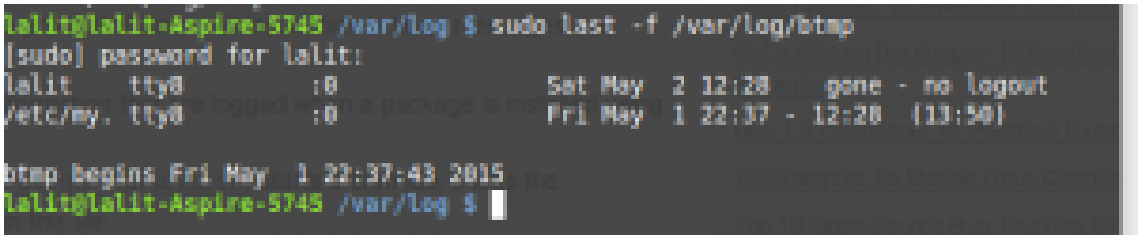
https://**ipinfo**.io/

https://www.**domaininfo**.com/

https://www.whois.net

https://who.is

By these links, you can get ip information and immediately drop these ip's from iptables rule.



Dont be confused with green colour, as in my all documents , green colour is color of my debian based linux mint machine.Which i am using for all my practicals. Note: sudo here i used because i m trying to use root accessible command in debian machine, so requires sudo to put before command. Here i have implemented the command , so it shows that two users lalit and /etc/my. Has tried to access my mahcine but got failed attempts.

14. var/log/cups – All printer and printing related log messages.

15. var/log/anaconda.log – When you install Linux, all installation related messages are stored in this log file

16./var/log/yum.log – Contains information that are logged when a package is installed using yum. **These files logs are very important while we practice linux, because sometimes we use yum to install packages or at same time we yum at two terminals**

.And then we got error Another app is currently holding the yum lock; waiting for it to exit. To find out what's locking up yum, try running

: # ps aux | grep yum

Note the PID number of the process and run this to kill the process.

kill

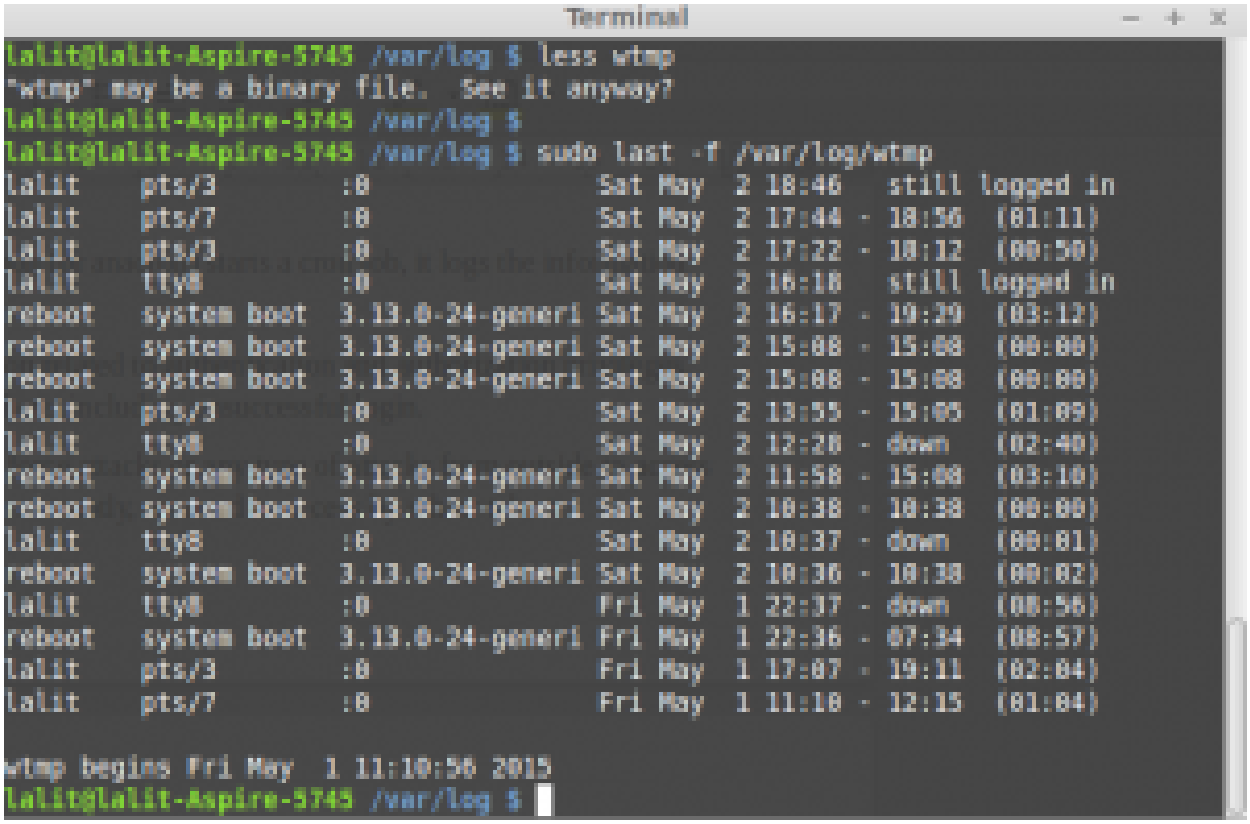
ps aux | grep yum

If not, repeat until the process is killed.

17. /var/log/cron – Whenever cron daemon (or anacron) starts a cron job, it logs the information about the cron job in this file.

18. /var/log/secure – Contains information related to authentication and authorization privileges. For example, sshd logs all the messages here, including unsuccessful login. Very important logs while attacks. Brute force attacks or any type of attacks from outside to access the servers.Because to access linux servers remotly, we need to access by ssh or telnet.

19. /var/log/wtmp or /var/log/utmp – Contains login records. Using wtmp you can find out who is logged into the system. who command uses this file to display the information.



20. /var/log/faillog – Contains user failed login attemps. Use faillog command to display the content of this file. You need to use the faillog command to see the all failed login attempts. Linux records failed login into a special database at /var/log/faillog. To see contents of the failure log database at /var/log/faillog use faillog command. The same command can be used for:

1. Set the failure counters
2. Set or configure the limits.
3. Display failed login information.

21.var/log/audit/ – Contains logs information stored by the Linux audit daemon (auditd).

22.**/var/log/setroubleshoot/** – 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.

23.**/var/log/samba/** – Contains log information stored by samba, which is used to connect Windows to Linux.

24. var/log/sssd/ – Use by system security services daemon that manage access to remote directories and authentication mechanisms.

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

. vi – If you are comfortable with the vi commands, use vi editor for quick log file browsing.

.tail – If you want to view the content of the log files real time, as the application is writting to it, use "tail -f". You can also view multiple log files at the same time (using "tail -f").

.grep – If you know exactly what you are looking for in a log file, you can quickly use grep command to grep a pattern.

. less – Less command is very powerful to browse log files.

For any queries you can contact us at linux@kvit.in.

Lalit Vohra

- Facebook
- Twitter
- Google+
- Gmail