Learn Linux

How to Check System Logs on Linux [Complete Usage Guide]

System Logs in a Linux system display a timeline of events for specific processes and parts of the system, making it easier for system administration activities such as troubleshooting, managing, and monitoring.

Updated: March 16, 2019

In today's Learn Linux guide, we will present you a comprehensive guide on what are system logs, where to find them, and how to use them to effectively manage a Linux system.

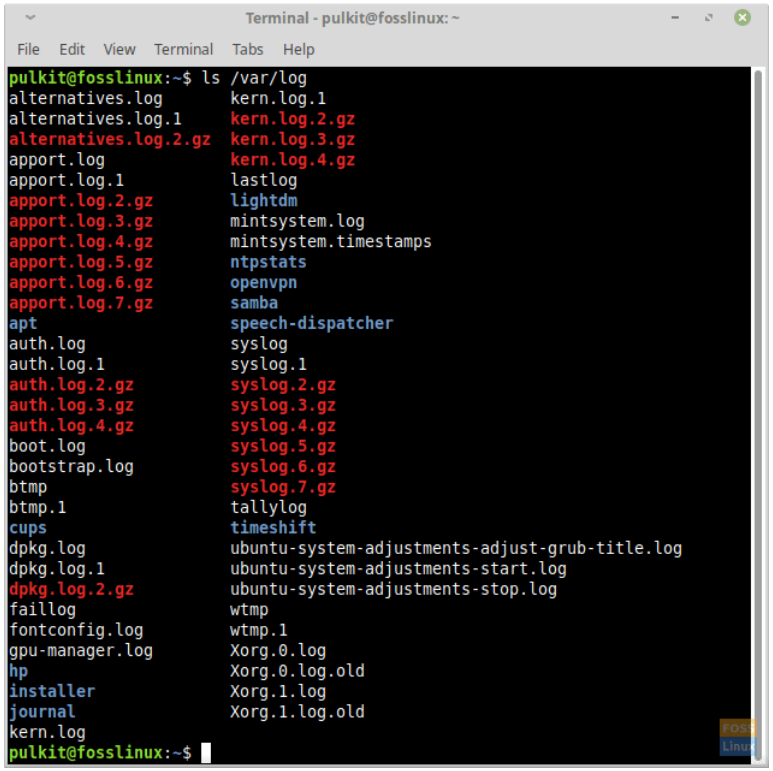
Note that all the Linux distros including the popular ones namely Debian, Ubuntu, Arch Linux, Linux Mint, Fedora, and CentOS have log files and it is common to Linux.

What are System Logs

The **log files** in a Linux system display a timeline of events for specific processes and parts of the system. For example, there are log files for *dpkg*, which have the information of all the programs installed, updated, and removed from your system, since the day it has been running.

Where to find the System Logs

You can find the log files in **/var/log** directory.



System logs list

These files are stored as plain text and are easy to read. You can use any GUI or CLI based text editor to read these files.

Why Logs exist

The system logs are time-based records of all significant changes occurring on your system. It means that they can be used to trace back any change that may have caused an adverse effect on your system. It also helps system administrators to keep track of the activities taking place on an employee's system.

Here are the details of some of the critical log files:

- **dpkg.log –** It keeps a log of all the programs that are installed, or removed or even updated in a system that uses DPKG package management. These systems include Ubuntu and all its derivatives, Linux Mint, Debian and all distributions based on Debian.
- **yum.log –** This is similar to the dpkg.log file and keeps a record of the changes made to all programs on the system. It is present in systems that use Yum package management.
- **kern.log** – This log contains the system's kernel data. Here you can find the record of changes made to the kernel. That is really a lot of information, due to which you might even find many versions of this file.
- **boot.log** – This log contains the services and processes that are running when you start up your system. If you have configured your system not to show a splash-screen graphic but the boot text on starting up, you might have seen a lot of text, that begins with [OK] or [Failed] when your system boots up. The boot log is shown from this file.
- **Xorg.0.log** – This file contains the data of the X Server program. X Server is the service that is responsible for the existence of the graphical interface on your system. If you have any issues with the GUI, you can check this log to pinpoint any errors.

- **wtmp.log/last.log** – These files contain the log-in data of the system. These are used by programs like last to show the names of users *last* logged in to the system.
- **btmp.log** – This shows the failed log-in attempts on the system.

Reading Log Files

Syntax

Here is a sample line of a log file:

```
Mar 15 06:39:46 fosslinux systemd[1]: Started Clean php session files.
```

The general syntax therefore is:

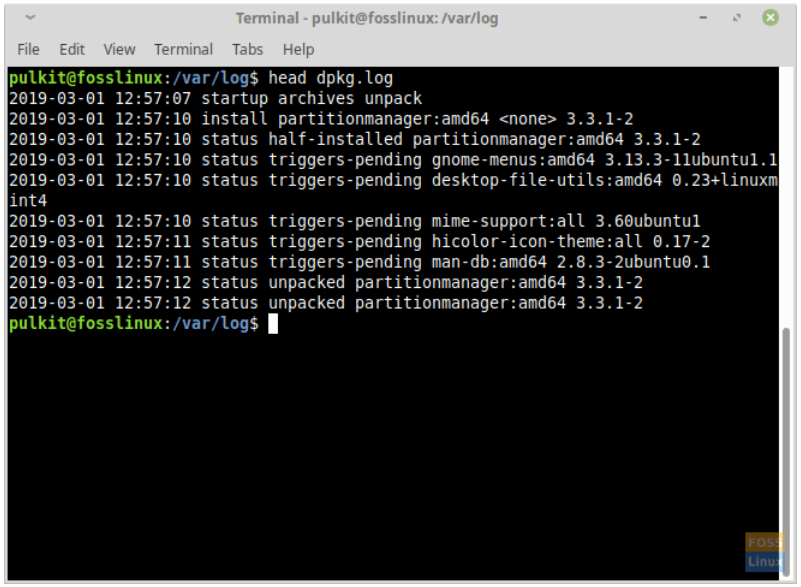
- Date
- Exact time
- Hostname (computer's name)
- Service/process name
- Message

Reading Logs using Terminal

Reading log files is simple and can be done with any basic text editor, but it is highly recommended to use Terminal commands and utilities to read these files. Some of the commands used are:

```
head <filname>
```

To read the first ten lines of the file.

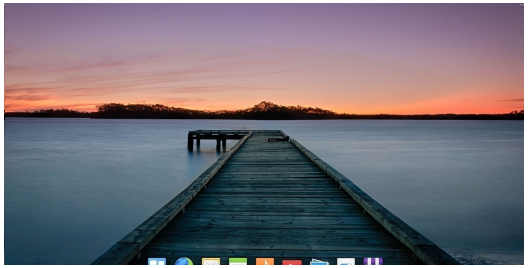


Using the head command on a log file

Distribution Ever Made

Linux is growing faster than ever. As per the latest report, there is a drop in the Windows 10 market share for the first time, and Linux's market share has improved to 2.87% this month. Most of the features in the list were rolled out in the Pop OS 20.04. Let's a detailed look into the new features, how to upgrade, and a ride through video.

Elementary OS 5.1.4 Review: Parental Control Finally Works?



Elementary OS 5.1 Hera has received a point release with a handful of new features and bug fixes, and we will be reviewing the significant changes in this article. For those new to elementary OS, this Ubuntu-based Linux distribution uses their inhouse built Pantheon desktop environment and AppCenter.

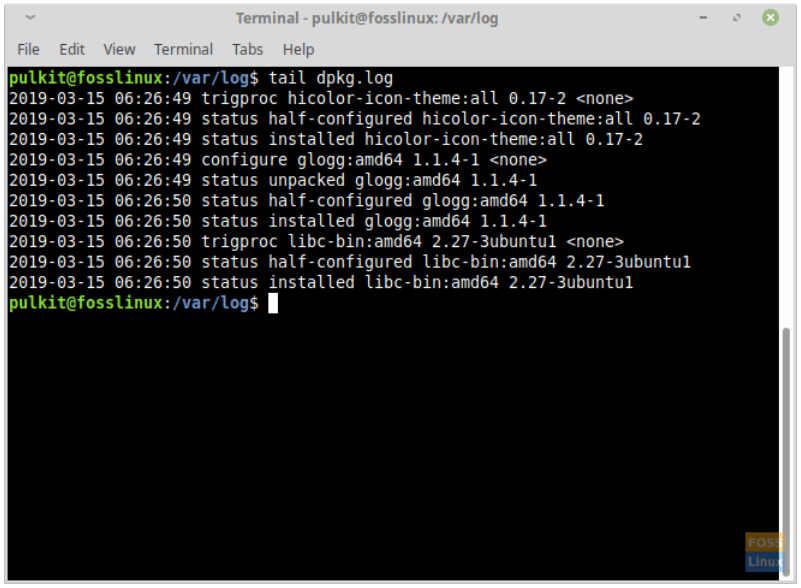
FEATURED

6 Best Linux Distributions for Beginners

Linux Mint vs. Ubuntu – which is best for you?

```
tail <filename>
```

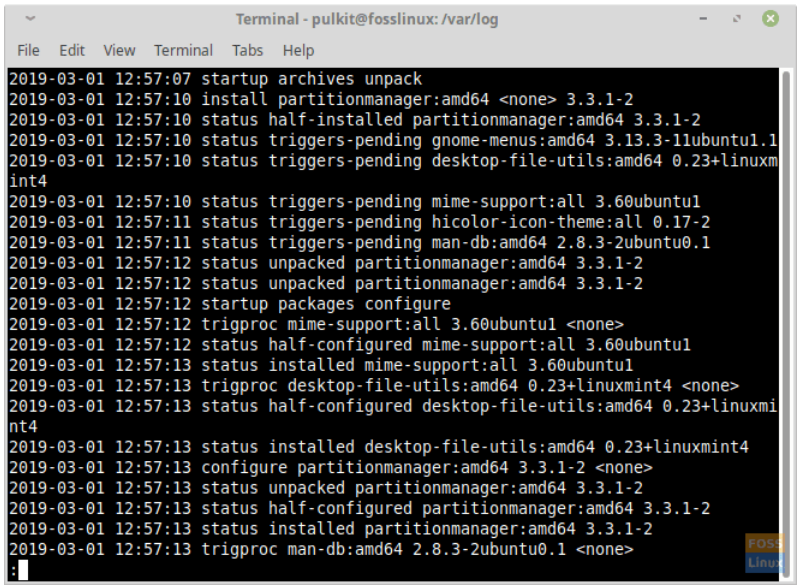
To read the last ten lines of the file.



Using the tail command on the log file

```
less <filename>
```

It is the most advanced utility. You can scroll up and down the file and even search for a word. It provides the most navigational options. You can quit it by pressing Q.



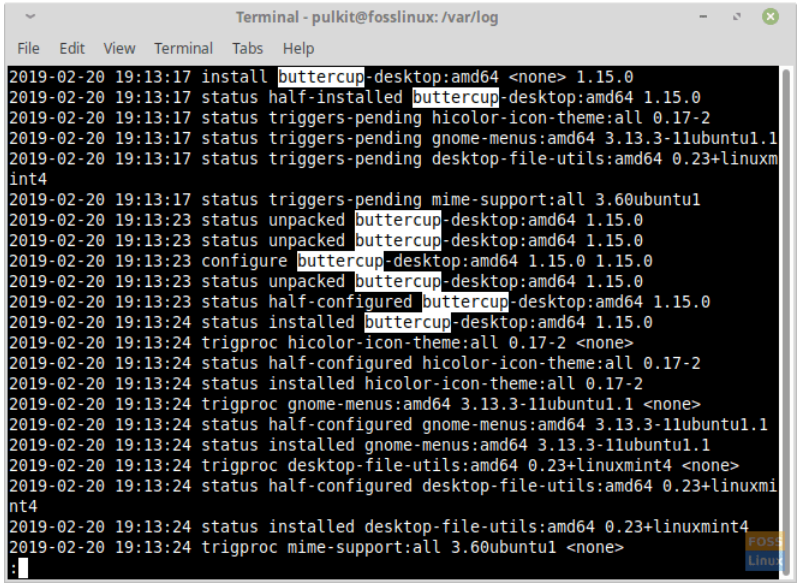
Using less command on a log file

Finding a specific part

Finding a particular part of the file can be done in two ways. First, using the *less* command and next using the *grep* command. For the less command, open the file with:

```
less <filename>
```

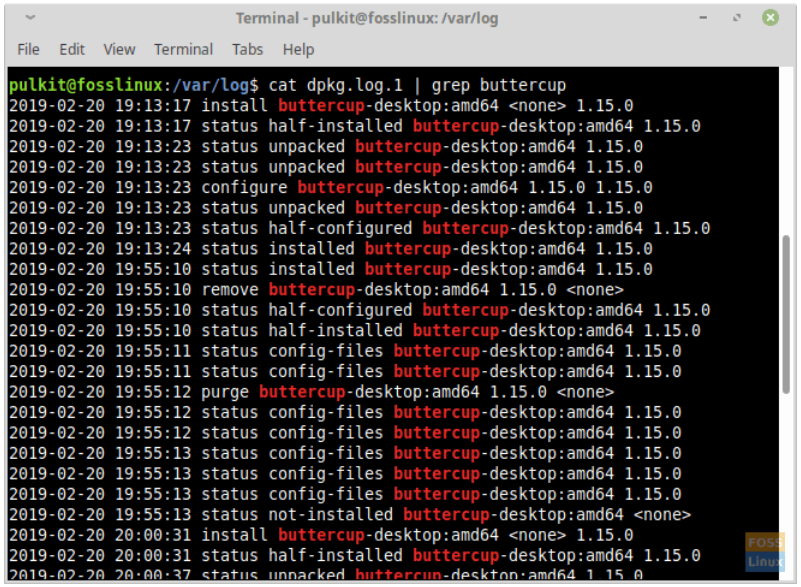
And then to find a part, press '/' key and type the word that you need to search. Press enter and the word that you desired should highlight. To find the next word matching the same pattern, press the N key. To go to the previous matching case, press Shift + N. Again, to quit, press Q.



Using less command to find a specific part

To use the grep method, you also have to use the cat command. So to find a particular part, use this:

```
cat <filename> | grep <keyword>
```



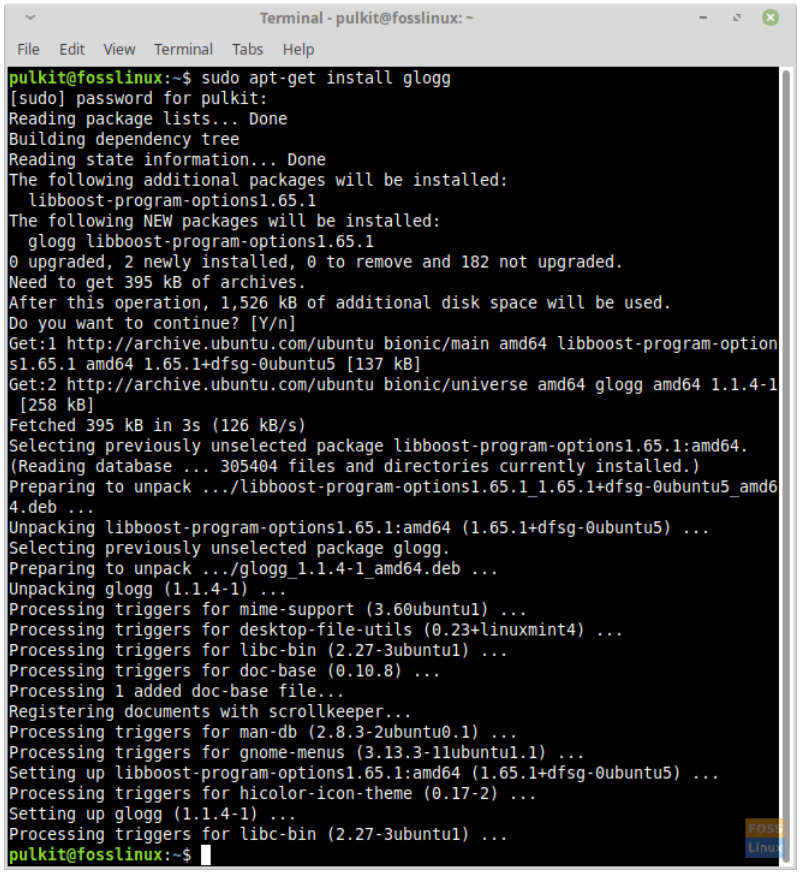
Finding a part using grep

GUI method

If you need to use a GUI program, you can use the **glogg**. It is an excellent program that efficiently displays logs. According to the website, it is a GUI combination of the *less* and *grep* commands.

You can install it using the command line. For Ubuntu (and derivatives), Linux Mint and other distributions that use APT management:

```
sudo apt-get install glogg
```



Installing glogg on Linux Mint

For Fedora and derivatives:

```
sudo yum install glogg
```

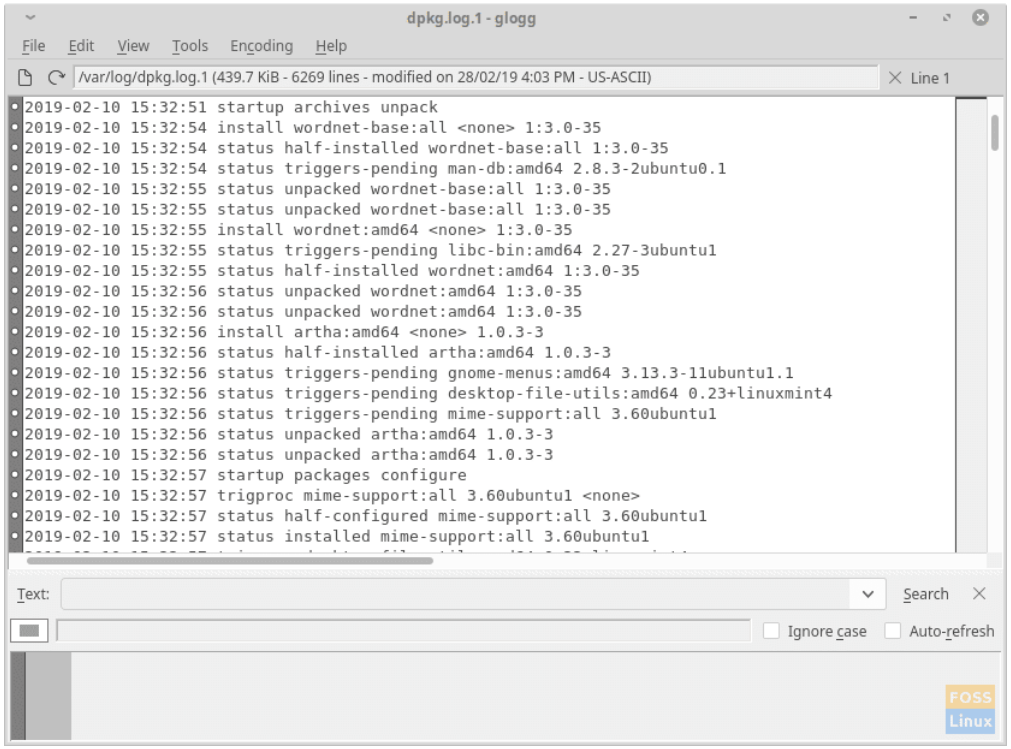
For Arch and derivatives:

```
sudo pacman -S glogg
```

You can find instructions or additional help here.

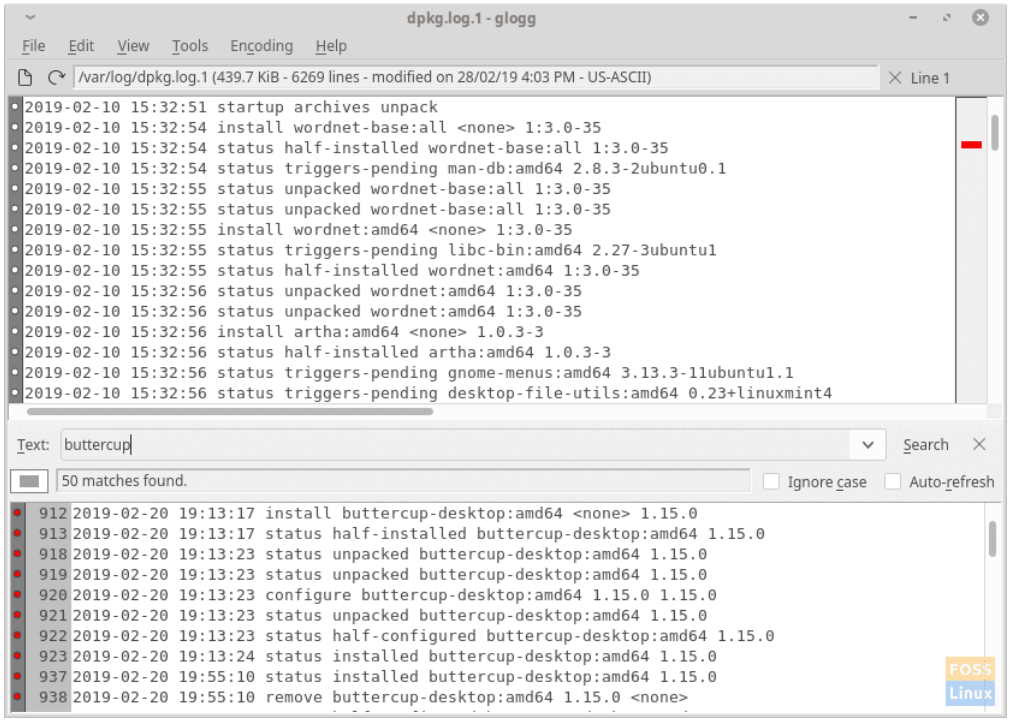
Usage

The usage of glogg is simple. Just launch the application from your application launcher, and click on the ‘Open File’ icon located on the left of the address bar after the reload button. Navigate to the log file that you want to open (probably in the /var/log directory), and open it.



Displaying logs using glogg

You can use the box present below the displayed content of the file to search for specific parts. The results should be displayed in a box below.



Finding logs on glogg

Log Rotation

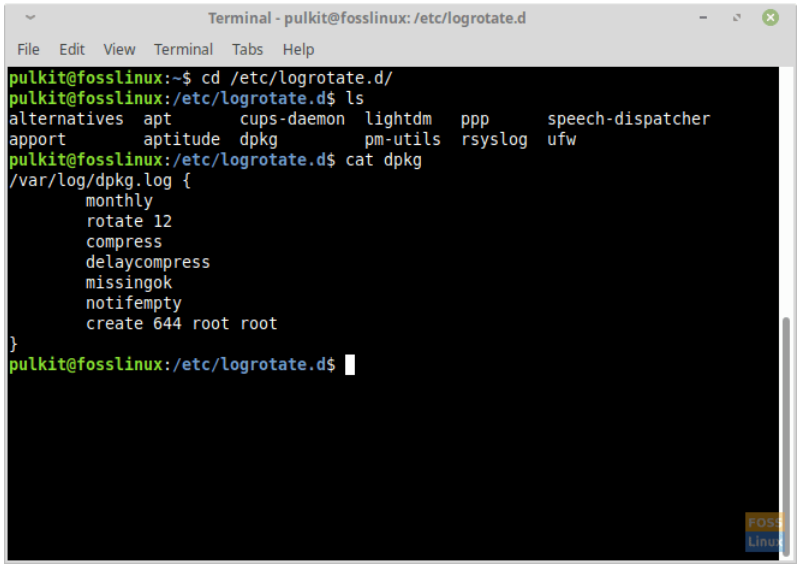
The system log files are rotated where new versions get created periodically. It is easy to tell if a log is rotated by looking at the original file name. Like *dpkg.log.1* is an older version of *dpkg.log*. The information about the rotation of the log files is contained in the *logrotate* file and the *logrotate.d* directory. You can access them using:

```
cd /etc/logrotate.d/
```

```
ls
```

You will see the files containing log-rotation data of all services. To view the contents, enter:

```
cat <filename>
```

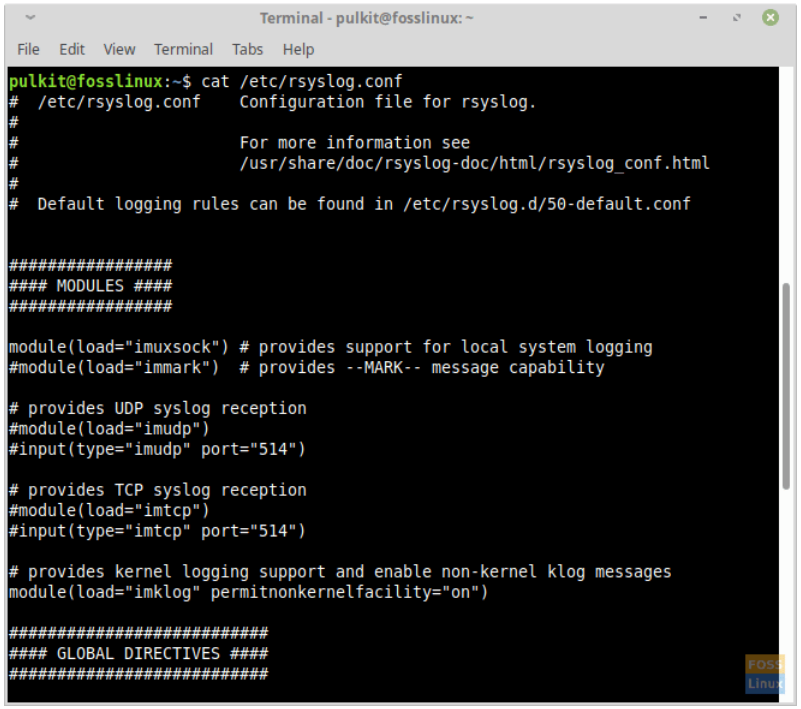


Log-rotation sample file

You can even edit them if you want.

rsyslog

rsyslog is the service that is responsible for creating log files. You can find its configuration files at */etc/rsyslog.conf* and in the */etc/rsyslog.d/* directory. You can make changes to the syntax of the system log entries using these files.



Log files configuration

Conclusion

System logs are a way for the system administrators and users to keep track of the changes going on in the system. They also help in finding errors and issues in the system and help maintain precise and efficient records. They are easy to read and manage, and very useful.

Let us know about any questions or your thought on logs in the comments. Cheers!

TAGS Linux Administration

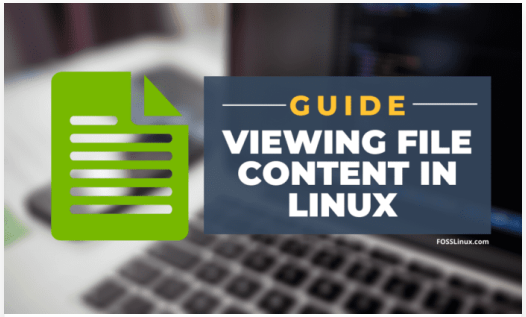
Pulkit Chandak

Pulkit Chandak is a Linux enthusiast and has been using and experimenting with open source software and hardware too since a long time. He is a huge admirer of open source software and wants to ventilate it to all around him. He is interested in reviewing and writing tutorials on Linux and its many distributions. He believes that freedom in software leads to freedom of the mind from the chains of limits.

RELATED POSTS

LEARN LINUX

Top 10 reasons to use KDE as your Desktop Environment



BEGINNER'S GUIDE

The 6 Best Ways to View Files in Linux

LEAVE A REPLY

Comment:

Name:*

Email:*

Save my name, email, and website in this browser for the next time I comment.

Post Comment

FOSS Linux