12 Critical Linux Log Files You Must be Monitoring -

By Marcel

Published: 2020-04-19 · Archived: 2026-04-05 19:41:18 UTC

12 Critical Linux Log Files You Must be Monitoring

Log files are the records that Linux stores for administrators to keep track and monitor important events about the server, kernel, services, and applications running on it. In this post, we'll go over the top Linux log files server administrators should monitor.

Content Recently Updated: Originally posted on Sep 15th, 2015

What are Linux log files

Log files are a set of records that Linux maintains for the administrators to keep track of important events. They contain messages about the server, including the kernel, services and applications running on it.

Linux provides a centralized repository of log files that can be located under the /var/log directory.

The log files generated in a Linux environment can typically be classified into four different categories:

- Application Logs
- Event Logs
- Service Logs
- System Logs

Why monitor Linux log files

Log monitoring is an **integral part** of any server administrator's responsibility.

By monitoring Linux log files, you can gain detailed insight on server performance, security, error messages and underlying issues by. If you want to take a proactive vs. a reactive approach to server management, regular log file analysis is 100% required.

In short, log files allow you to **anticipate upcoming issues** before they actually occur.

Which Linux log files to monitor

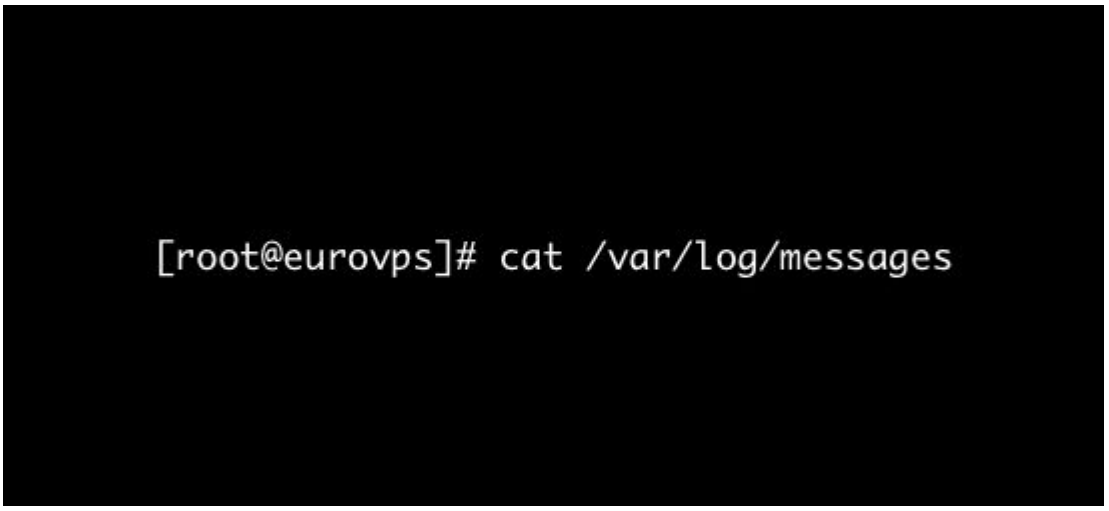
Monitoring and analyzing all of them can be a challenging task.

The sheer volume of logs can sometimes make it frustrating just to drill down and find the right file that contains the desired information.

To make it a little easier for you, we will introduce you to some of the most critical Linux log files that you must be monitoring.

Note: Please note that this is not an all-inclusive list - but just a subset of the important log files that matter the most. The more you can handle, the better it is for the health of your server. Listed below are the bare minimum that you must monitor without fail

/var/log/messages



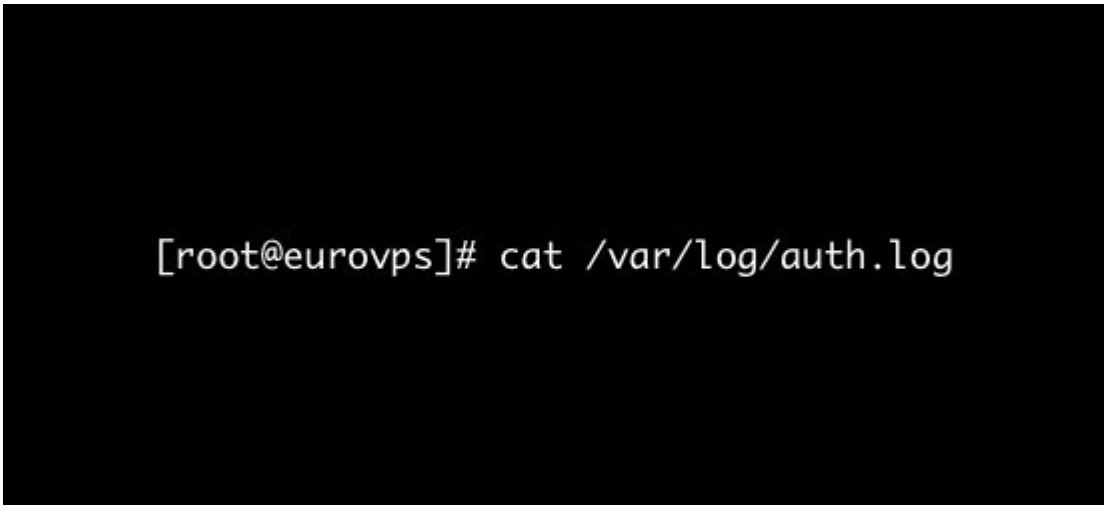
What's logged here?:

- This log file contains generic system activity logs.
- It is mainly used to store informational and non-critical system messages.
- In Debian-based systems, /var/log/syslog directory serves the same purpose.

How can I use these logs?:

- Here you can track non-kernel boot errors, application-related service errors and the messages that are logged during system startup.
- This is the first log file that the Linux administrators should check if something goes wrong.
- For example, you are facing some issues with the sound card. To check if something went wrong during the system startup process, you can have a look at the messages stored in this log file.

/var/log/auth.log



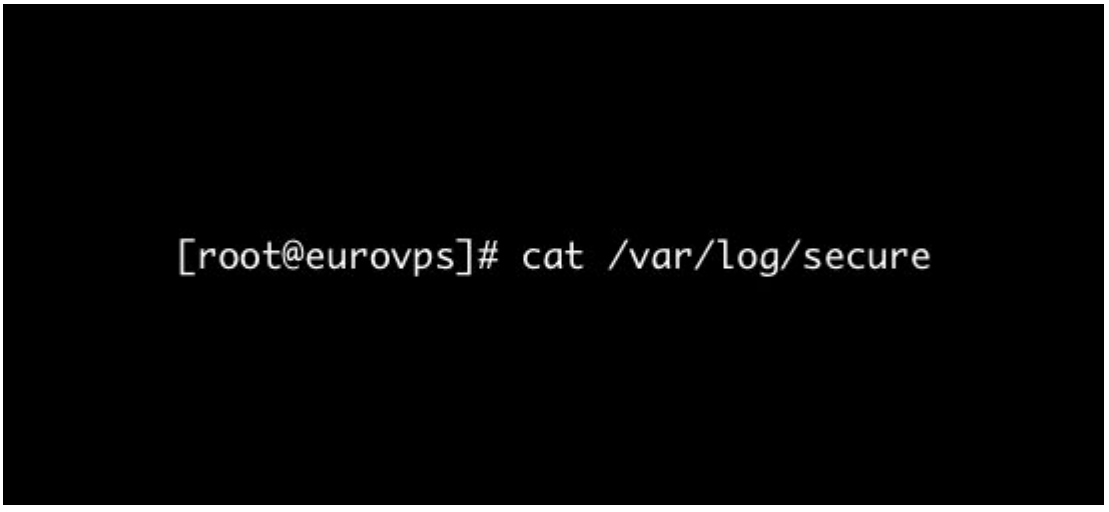
What's logged here?

- All authentication related events in Debian and Ubuntu server are logged here.
- If you're looking for anything involving the user authorization mechanism, you can find it in this log file.

How can I use these logs?:

Suspect that there might have been a security breach in your server? Notice a suspicious javascript file where it shouldn't be? If so, then find this log file asap!

- Investigate failed login attempts
- Investigate brute-force attacks and other vulnerabilities related to user authorization mechanism.



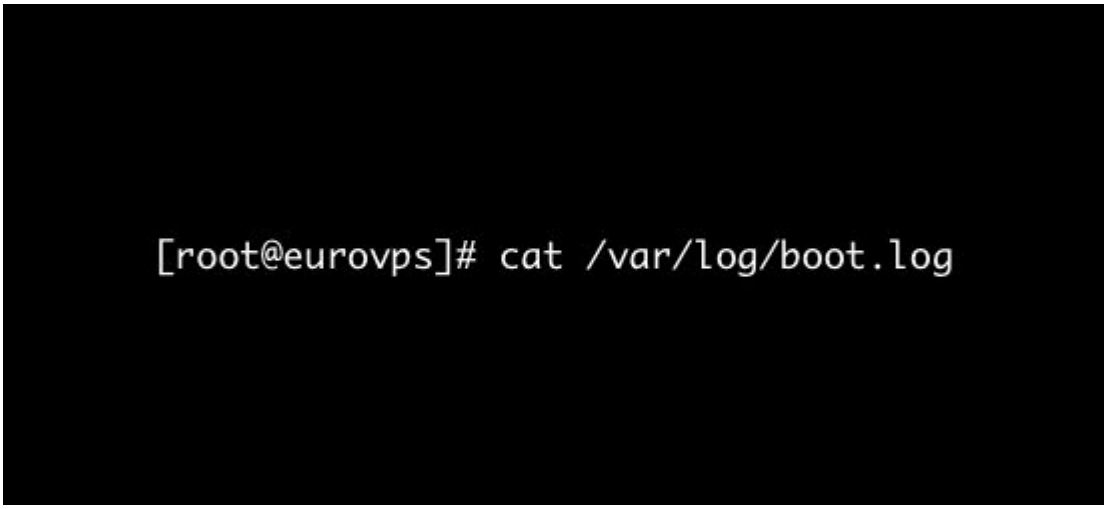
What's logged here?

RedHat and CentOS based systems use this log file instead of /var/log/auth.log.

- It is mainly used to track the usage of authorization systems.
- It stores all security related messages including authentication failures.
- It also tracks sudo logins, SSH logins and other errors logged by system security services daemon.

How can I use these logs?:

- All user authentication events are logged here.
- This log file can provide detailed insight about unauthorized or failed login attempts
- Can be very useful to detect possible hacking attempts.
- It also stores information about successful logins and tracks the activities of valid users.



What's logged here?

- The system initialization script, /etc/init.d/bootmisc.sh, sends all bootup messages to this log file
- This is the repository of booting related information and messages logged during system startup process.

How can I use these logs?:

- You should analyze this log file to investigate issues related to improper shutdown, unplanned reboots or booting failures.
- Can also be useful to determine the duration of system downtime caused by an unexpected shutdown.

dmesg

What's logged here?

- This log file contains Kernel ring buffer messages.
- Information related to hardware devices and their drivers are logged here.
- As the kernel detects physical hardware devices associated with the server during the booting process, it captures the device status, hardware errors and other generic messages.

How can I use these logs?:

- This log file is useful for dedicated server customers mostly.
- If a certain hardware is functioning improperly or not getting detected, then you can rely on this log file to troubleshoot the issue.
- Or, you can purchase a managed server from us and we'll monitor it for you.

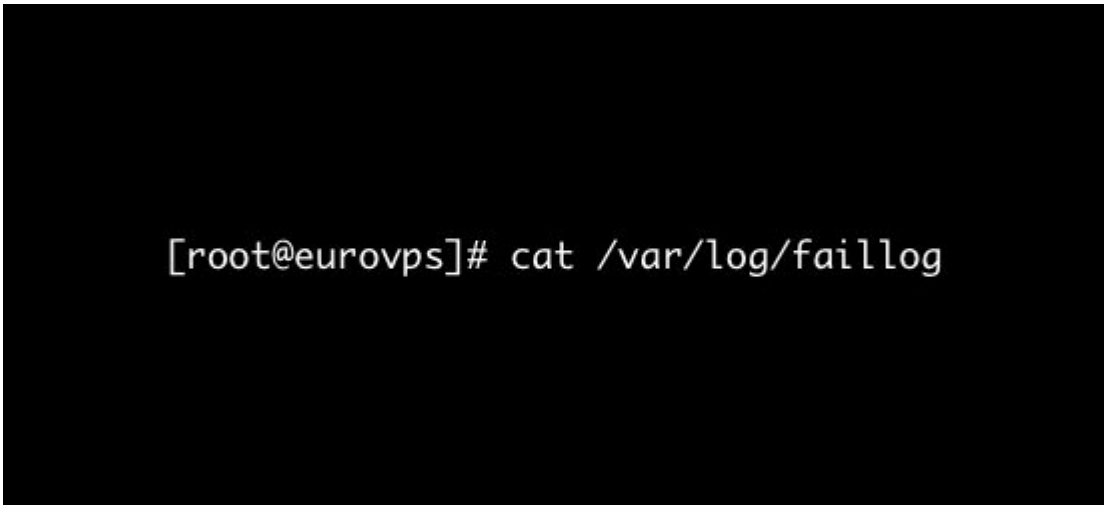
What's logged here?

This is a very important log file as it contains information logged by the kernel.

How can I use these logs?:

- Perfect for troubleshooting kernel related errors and warnings.
- Kernel logs can be helpful to troubleshoot a custom-built kernel.
- Can also come handy in debugging hardware and connectivity issues.

*/var/log/*faillog



What's logged here?

This file contains information on failed login attempts.

How can I use these logs?:

It can be a useful log file to find out any attempted security breaches involving username/password hacking and brute-force attacks.

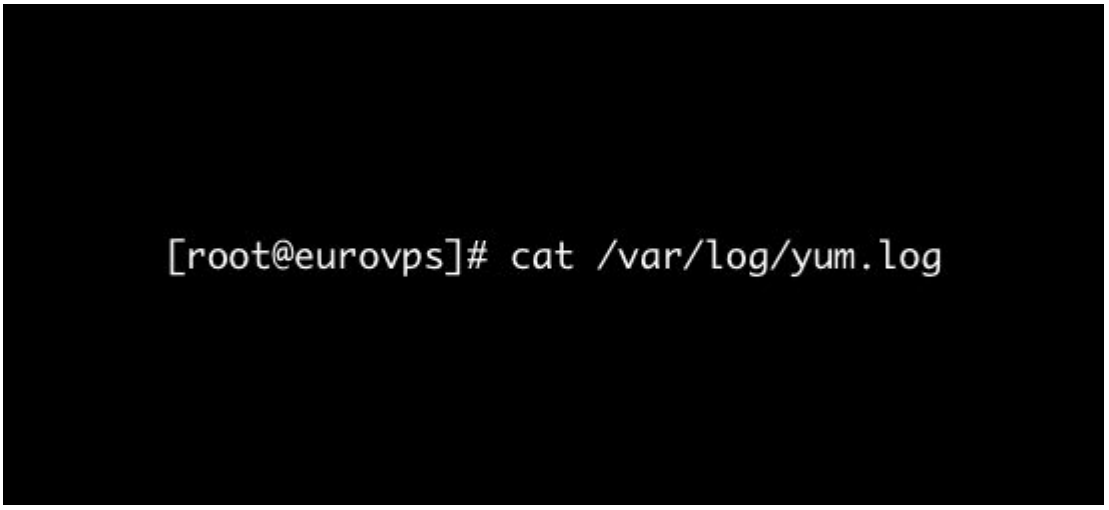
cron

What's logged here?

This log file records information on cron jobs.

How can I use these logs

- Whenever a cron job runs, this log file records all relevant information including successful execution and error messages in case of failures.
- If you're having problems with your scheduled cron, you need to check out this log file.



What's logged here?

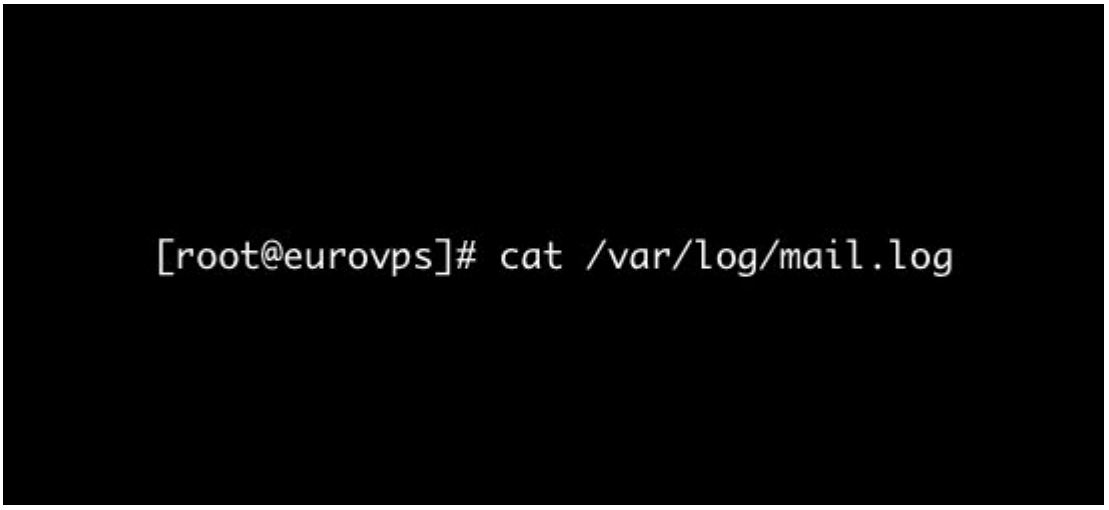
It contains the information that is logged when a new package is installed using the yum command.

How can I use these logs?:

- Track the installation of system components and software packages.
- Check the messages logged here to see whether a package was correctly installed or not.
- Helps you troubleshoot issues related to software installations.

Suppose your server is behaving unusually and you suspect a recently installed software package to be the root cause for this issue. In such cases, you can check this log file to find out the packages that were installed recently and identify the malfunctioning program.

maillog *or /var/log/mail.log*



What's logged here?

All mail server related logs are stored here.

How can I use these logs?

- Find information about postfix, smtpd, MailScanner, SpamAssassain or any other email related services running on the mail server.
- Track all the emails that were sent or received during a particular period
- Investigate failed mail delivery issues.
- Get information about possible spamming attempts blocked by the mail server.
- Trace the origin of an incoming email by scrutinizing this log file.

What's logged here?

- This directory contains the logs recorded by the Apache server.
- Apache server logging information are stored in two different log files – error_log and access_log.

How can I use these logs?:

- The error_log contains messages related to httpd errors such as memory issues and other system related errors.
- This is the place where Apache server writes events and error records encountered while processing httpd requests.
- If something goes wrong with the Apache webserver, check this log for diagnostic information.
- Besides the error-log file, Apache also maintains a separate list of access_log.
- All access requests received over HTTP are stored in the access_log file.
- Helps you keep track of every page served and every file loaded by Apache.
- Logs the IP address and user ID of all clients that make connection requests to the server.
- Stores information about the status of the access requests, – whether a response was sent successfully or the request resulted in a failure.

/var/log/mysqld.log or /var/log/mysql.log

What's logged here?

- As the name suggests, this is the MySQL log file.
- All debug, failure and success messages related to the [mysqld] and [mysqld_safe] daemon are logged to this file.
- RedHat, CentOS and Fedora stores MySQL logs under /var/log/mysqld.log, while Debian and Ubuntu maintains the log in /var/log/mysql.log directory.

How can I use this log?

- Use this log to identify problems while starting, running, or stopping mysqld.
- Get information about client connections to the MySQL data directory
- You can also setup 'long_query_time' parameter to log information about query locks and slow running queries.

Final Takeaway

While monitoring and analyzing all the log files generated by the system can be a difficult task, you can make use of a centralized log monitoring tool to simplify the process.

Some of our customers take advantage of using Nagios Log Server to manage their server logs. There are many opensource options available if that's out of the budget. Needless to say though, monitoring Linux logs manually is hard.

So if you want to take a truly proactive approach to server management, investing in a centralized log collection and analysis platform which allows you to view log data in real-time and set up alerts to notify you when potential threats arise.

- Linux
- Security

Certified ethical hacker and security team leader on EuroVPS support desk. I keep bad stuff out.

20 Ways to Secure Your Linux VPS so You Don’t Get Hacked

Linux VPS servers have their advantages. In fact, Linux VPS are much more secure when compared to other operating system...

How to Prevent Annoying Spam Outbreaks in cPanel and Plesk Servers

We hate spam, you hate spam! We all hate spam! If you are using the cPanel or Plesk control panel, this post goes over a...

10 Effective Ways to Secure your Windows Server from Technological Hooligans

Ready for some Windows server security tips and tricks? For all you security minded Windows Server users, we'll talk abo...
