Linux Logs Explained

By Elvis Plesky | April 22, 2024 | Featured, Guides, Product and technology

4 Minutes

Linux logs are the bread and butter of every seasoned Linux pro. They´re like treasure maps, guiding us through the labyrinth of system activities and helping us unravel their mysteries when troubleshooting. If anything goes wrong, they give a useful overview of events in order to help you, the administrator, seek out the culprits.

In this article, we´ll dive deep into the world of Linux logs. By the end of this exploration, you'll be equipped with the knowledge and skills to navigate and leverage logs with confidence and precision.

Linus logs essentials

Linux logs are typically stored in the ***/var/log*** directory and its subdirectories. Within the ***/var/log*** directory, logs are organized into subdirectories based on their respective categories or sources. For example:

1. **System Logs**: System-related logs, such as kernel messages, boot logs, and general system activity logs, are stored directly in the /var/log directory.
2. **Application Logs**: Logs generated by specific applications, such as Apache web server logs (/var/log/apache2/), MySQL database server logs (/var/log/mysql/), and mail server logs (/var/log/mail/), are stored in separate subdirectories.
3. **Service Logs**: Logs generated by system services, daemons, and background processes are typically stored

Organizing logs into specific directories facilitates easy access, management, and analysis, allowing system administrators to efficiently monitor and troubleshoot system activities.

For problems relating to particular apps, the developer decides where best to put the log of events. So with Google Chrome for instance, any time it hangs, you want to look in '~/.chrome/Crash Reports' to discover the gory details of what tripped the system up.

As you can see, **Linux log files** cover all kinds of things, like system, kernel, package managers, MySQL and more. But now, we'll focus on **system logs**.

How can I check Linux logs?

To access the system directory of a Linux or UNIX-style operating system you will need to tap in the **cd** command. From here, you can look at system logs using the **cd /var/log command. Type ls** to bring up the logs in this directory. *Syslog is one of the main ones that you want to be looking at because it keeps track of virtually everything, except* auth-related messages.

You also use **/var/log/syslog** to scrutinise anything that's under the syslog. But picking out one particular thing will take some time because it's usually a pretty big file to wade through. Pressing *Shift+G* will take you all the way to the end, and you'll know you're there because you will see the word "END."

You can also check logs using **dmesg. This** shows the kernel ring buffer and prints everything after sending you to the end of the file. You can then use the **dmesg | less command** to scroll through everything it has produced. If you'd like to see log entries relating to the user facility, use **dmesg –facility=user.**

Finally, as a super-handy command called **tail, which** lets you look over log files. It's so useful because it just displays the last bit of the logs. Which is often where you'll find the source of the difficulty. Use **tail /var/log/syslog** or **tail -f /var/log/syslog. *Tail*** keeps a close eye on the log file, and displays every written to it, which lets you check what's being added to syslog in real time.

For a particular group of lines (say, the last five) type in **tail -f -n 5 /var/log/syslog**, and you'll be able to see them. Use Ctrl+C to turn off the tail command.

Most Valuable Linux Logs Categories

- Event Logs
- Service Logs
- System Logs

Checking each log individually would be a daunting task. So that's why developers rely on log management tools like Retrace. These tools put APM and log management right at your fingertips. With such tools, you have the flexibility to monitor a wide range of metrics tailored to your specific needs. However, certain logs demand immediate attention and should be prioritized for thorough scrutiny. Let´s see which ones.

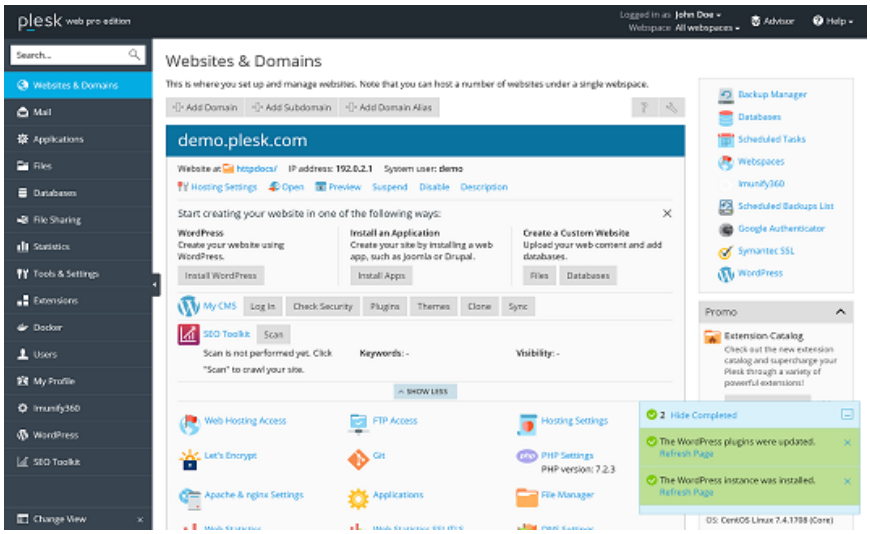
What's in these Linux Logs?

- **/var/log/syslog** or **/var/log/messages**:
  Shows general messages and info regarding the system. Basically a data log of all activity throughout the global system. Know that everything that happens on Redhat-based systems, like CentOS or Rhel, will go in messages. Whereas for Ubuntu and other Debian systems, they go in Syslog.

- **/var/log/auth.log** or **/var/log/secure**:
  Keep authentication logs for both successful or failed logins, and authentication processes. Storage depends on system type. For Debian/Ubuntu, look in /var/log/auth.log. For Redhat/CentOS, go to /var/log/secure.
- **/var/log/boot.log**: start-up messages and boot info.
- **/var/log/maillog or var/log/mail.log:** is for mail server logs, handy for postfix, smtpd, or email-related services info running on your server.
- **/var/log/kern**: keeps in Kernel logs and warning info. Also useful to fix problems with custom kernels.
- **/var/log/dmesg**: a repository for device driver messages. Use **dmesg** to see messages in this file.
- **/var/log/faillog:** records info on failed logins. Hence, handy for examining potential security breaches like login credential hacks and brute-force attacks.
- **/var/log/cron**: keeps a record of Crond-related messages (cron jobs). Like when the cron daemon started a job.
- **/var/log/daemon.log:** keeps track of running background services but doesn't represent them graphically.
- **/var/log/btmp**: keeps a note of all failed login attempts.
- **/var/log/utmp**: current login state by user.
- **/var/log/wtmp**: record of each login/logout.
- **/var/log/lastlog**: holds every user's last login. A binary file you can read via **lastlog** command.
- **/var/log/yum.log:** holds data on any package installations that used the **yum** command. So you can check if all went well.
- **/var/log/httpd/**: a directory containing error_log and access_log files of the Apache httpd daemon. Every error that httpd comes across is kept in the **error_log** file. Think of memory problems and other system-related errors. **access_log** logs all requests which come in via HTTP.
- **/var/log/mysqld.log** or **/var/log/mysql.log** : MySQL log file that records every debug, failure and success message, including starting, stopping and restarting of MySQL daemon mysqld. The system decides on the directory. RedHat, CentOS, Fedora, and other RedHat-based systems use /var/log/mariadb/mariadb.log. However, Debian/Ubuntu use /var/log/mysql/error.log directory.
- **/var/log/pureftp.log**: monitors for FTP connections using the pureftp process. Find data on every connection, FTP login, and authentication failure here.

plesk
a webpros brand

Does Plesk for Linux keep logs too?



As a Linux-friendly hosting panel, **Plesk** uses **log files** for a wide range of software packages that run under Linux in addition to its own logs. Below, we've compiled a list detailing the locations of **Plesk logs**. And we hope it helps you fix issues.

Plesk System

- Error log: /var/log/sw-cp-server/error_log and /var/log/sw-cp-server/sw-engine.log

These logs capture error messages and other relevant information related to the operation of the SW-CP-Server, which is responsible for managing the Plesk control panel interface and various administrative tasks within Plesk. Monitoring these logs can provide valuable insights into any issues or errors occurring within the SW-CP-Server service, helping sysadmins diagnose and troubleshoot problems effectively.

- Access log: /usr/local/psa/admin/logs/httpsd_access_log

Specifically, this log captures information about HTTP requests made to the Plesk control panel, including details such as the IP address of the client making the request, the requested URL, the HTTP status code returned by the server, and other relevant information. Monitoring this access log can provide valuable insights into who is accessing the Plesk control panel and what actions they are performing, which can be useful for security monitoring, troubleshooting, and performance optimization purposes.

- Panel log: /usr/local/psa/admin/logs/panel.log

This log captures various events and activities related to the Plesk control panel's operation and administration. It includes information about user logins, administrative actions, system events, errors, warnings, and other relevant details. Monitoring the panel log is essential for sysadmins to track changes made to the Plesk environment, diagnose issues, troubleshoot errors, and ensure the smooth functioning of the control panel.

Plesk Installer

Monitoring this log is essential for sysadmins to track the progress of Plesk installations and updates, diagnose installation failures or errors, and troubleshoot any issues that may arise during the installation or update process.

- /tmp/autoinstaller3.log

Similar to "/var/log/plesk/installer/autoinstaller3.log", this log also captures detailed information about the installation and update processes performed by the Plesk Installer tool. However, it is stored in the temporary directory ("/tmp/") and may contain temporary logs or data generated during the installation or update process. Monitoring this log can provide additional insights into the installation and update activities, complementing the information available in other Plesk logs.

Web Presence Builder

- Error log: /usr/local/psa/admin/logs/sitebuilder.log

The "Error log" at "/usr/local/psa/admin/logs/sitebuilder.log" records issues and relevant data related to Plesk's Web Presence Builder feature. It's essential for sysadmins to troubleshoot any errors users encounter when creating or editing websites in Plesk.

- Install/upgrade logs: /usr/local/sb/tmp/

The "Install/upgrade logs" directory at "/usr/local/sb/tmp/" stores logs related to installations and upgrades within Plesk's Web Presence Builder feature.

Backup Manager

- Backup logs: /usr/local/psa/PMM/logs/backup-<datetime>

The "Backup logs" directory at "/usr/local/psa/PMM/logs/backup-<datetime>" contains logs specific to the backup process managed by Plesk's Backup Manager.

- Restore log: /usr/local/psa/PMM/logs/restore-<datetime>

The "Restore log" directory at "/usr/local/psa/PMM/logs/restore-<datetime>" stores logs related to the restoration process managed by Plesk's Backup Manager.

Plesk Migrator

- /usr/local/psa/var/modules/panel-migrator/logs/

The "Plesk Migrator" directory at "/usr/local/psa/var/modules/panel-migrator/logs/" is used to store logs related to migration processes facilitated by Plesk's Migration Manager. These logs contain detailed information about the migration of websites, databases, email accounts, and other data from one server to another. They help administrators track the progress of migration tasks, diagnose any errors or issues encountered during the

These logs document various aspects of the migration, including the source and destination servers, migrated data types (such as websites, databases, email accounts), and any errors or warnings encountered during the migration process.

- /usr/local/psa/PMM/logs/migration-<datetime>

Website Import

These logs record details such as the source of the imported website, the progress of the import process, and any errors encountered during the import operation.

- /usr/local/psa/var/modules/site-import/sessions/

Health Monitor Manager

Health Monitor Manager logs contain information about the health status and performance metrics of servers managed by Plesk's Health Monitor Manager service. These logs record system alerts, resource usage statistics, and any anomalies detected during health checks.

- /usr/local/psa/admin/logs/health-alarm.log

Health Monitor Notification Daemon

These logs detail alerts related to server health, resource usage, and any abnormalities detected during monitoring.

- /usr/local/psa/admin/logs/health-alarm.log

FTP

These logs record details such as user login attempts, file uploads, downloads, and any errors encountered during FTP sessions.

- /usr/local/psa/var/log/xferlog
- /var/log/plesk/xferlog
- /var/log/secure

Courier-IMAP

These logs record details such as user login attempts, email retrieval actions, and any errors encountered during IMAP sessions. Monitoring Courier-IMAP logs is essential for sysadmins to troubleshoot email-related issues, diagnose errors, and ensure the smooth functioning of email services hosted on Plesk servers.

Postfix logs document the activities and operations of the Postfix mail server on Plesk servers. These logs record information such as incoming and outgoing email delivery attempts, message routing, and any errors or warnings encountered during mail processing.

- /usr/local/psa/var/log/maillog

Qmail

Qmail logs contain information about the operation and activities of the Qmail mail server on Plesk servers. These logs record details such as incoming and outgoing email delivery attempts, message queue management, and any errors or warnings encountered during mail processing.

- /usr/local/psa/var/log/maillog

Horde

Horde logs document the activities and events occurring within the Horde webmail application integrated with Plesk. These logs capture user interactions, email operations, and system-related messages, providing valuable insights into the usage and performance of the webmail interface.

- Error log: /var/log/psa-horde/psa-horde.log

Roundcube

Monitoring Roundcube logs is essential for sysadmins to troubleshoot user-reported issues, diagnose any errors encountered while using the webmail application, and ensure the smooth operation of email services hosted on Plesk servers.

- Error log: /var/log/plesk-roundcube/errors

SpamAssassin

Monitoring SpamAssassin logs is crucial for sysadmins to assess the effectiveness of spam filtering, identify false positives or false negatives, and fine-tune spam detection rules to optimize email security.

- /usr/local/psa/var/log/maillog

Parallels Premium Antivirus

Parallels Premium Antivirus logs contain records of antivirus scanning activities performed by the Parallels Premium Antivirus service within Plesk. These logs document scan results, detected threats, and any actions taken by the antivirus software to mitigate security risks.

- /usr/local/psa/var/log/maillog

Watchdog (monit) logs capture monitoring and alerting events generated by the Watchdog service in Plesk. These logs provide detailed information about system health checks, service availability, resource usage, and any issues detected by the monitoring system. Monitoring Watchdog logs is essential for ensuring the stability, performance, and security of servers managed by Plesk.

- /usr/local/psa/var/modules/watchdog/log/wdcollect.log
- /var/log/wdcollect.log
- /usr/local/psa/var/modules/watchdog/log/monit.log
- /var/log/plesk/modules/wdcollect.log

Let's Encrypt

Let's Encrypt logs track the issuance and renewal of SSL/TLS certificates managed by the Let's Encrypt service within Plesk. These logs provide valuable information about certificate generation, renewal attempts, validation challenges, and any errors encountered during the process.

- /usr/local/psa/admin/logs/panel.log

Plesk-PHP

Plesk-PHP logs document the activities and errors related to the PHP-FPM service integrated with Plesk. These logs provide insights into the performance, execution, and errors encountered by PHP scripts running on the server. They are essential for troubleshooting PHP-related issues, diagnosing script errors, and optimizing the performance of PHP applications hosted on Plesk servers.

- /var/log/plesk-php7x-fpm/

Acronis Backup

The logs for Acronis Backup are used to track and record all activities related to backup and recovery operations performed by the Acronis Backup service. They provide detailed information about the status of backups, any errors or warnings encountered during the process, and other relevant data to ensure the reliability and integrity of the backup system.

- /var/log/plesk/panel.log
- /var/log/trueimage-setup.log
- /opt/psa/var/modules/acronis-backup/srv/log/

Conclusion

This includes managing logs well and focusing on critical ones. Also, optimize log analysis for system health. That means knowing where to look, prioritizing the crucial stuff, and fine-tuning your analysis for maximum efficiency. Nail these fundamentals, and you'll be running your Linux setup like a well-oiled machine, spotting issues before they even have a chance to surface.

Now that we've explored Linux logs, which ones are the most important in your experience? Share your thoughts with us in the comments below. Your input can help other admins improve their log management strategies and keep their systems running smoothly.

Elvis Plesky

Our fun and curious team mascot's always plugged into the latest trends. He's here to share his knowledge and help you solve your tech problems.

One comment

Mari Bratton

OCT 27, 2019 / 7:41 AM # LINK REPLY

I'm a noob to the ncl challenges and some of your info has helped when I was looking for a dns attack on a apache server.

Add a Comment

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Website

plesk
a webpros brand

GET LATEST NEWS AND TIPS

Name

Email

— Please Select —

Yes, please, I agree to receiving my personal Plesk Newsletter! WebPros International GmbH and other WebPros group companies may store and process the data I provide for the purpose of delivering the newsletter according to the WebPros Privacy Policy. In order to tailor its offerings to me, Plesk may further use additional information like usage and behavior data (Profiling). I can unsubscribe from the newsletter at any time by sending an email to privacy@plesk.com or use the unsubscribe link in any of the newsletters.

Submit

RELATED POSTS

Easy Steps to List All Open Linux Ports
Read More »

Recommended OSs for Plesk
Read More »

How to Use Cgroups Manager to Increase Website Performance Through Resource Isolation on Linux
Read More »

KNOWLEDGE BASE

Setting Up Custom Error Pages on Linux Servers
Read More »

(Plesk for Linux) System Updates
Read More »

Apache fails to start on a Plesk server after Apache update on CentOS 7 / RHEL 7
Read More »

Vulnerability PFSI-62465 in Plesk
Read More »

Plesk Onyx Linux – Plesk installer fails to start
Read More »

Problem with Plesk Onyx 17.5.3 (Stable) on OS: CentOS Linux 7.4.1708
Read More »

plesk
a webpros brand

COMPANY

PRODUCT

KNOWLEDGE BASE

PROGRAMS

COMMUNITY

Follow us:

Managed with ♥ with Plesk WP Toolkit