# Introduction

Linux logs are pieces of data that Linux writes. The data is related to what the *server*, *kernel*, *services*, and *applications* running on Linux are doing, with an associated *timestamp*.

For example, here is SSH log from /var/log/auth.log:

May 5 08:57:27 ubuntu-bionic sshd[5544]: pam\_unix(sshd:session): session opened for user vagrant by (uid=0)

Notice how the log contains a few fields (timestamp, hostname, process name, PID) before the message itself.

# Log Locations

In Linux, logs come from different sources. The location and format of your Linux system logs depend on how your distro is configured. But by default, most logs can be found in /var/log directory.

## SystemD Journal

Most Linux distros have [systemd](Linux%20Tutorial.docx) to manage services (like SSH). *Systemd* catches the output of these services (i.e., logs) and writes them to the journal in /var/log/journal directory. The journal is written in a **binary format**, so you’ll use [journalctl](#_JournalD_Commands) to explore it, like:

$ journalctl

...

May **05** **08**:**57**:**27** ubuntu-bionic sshd[**5544**]: pam\_unix(sshd:session): session opened **for** user vagrant **by** (uid=**0**)

...

## Syslog

When there’s no *systemd*, processes like SSH can write to a UNIX socket (e.g., /dev/log) in the *syslog* message format. A *syslog* daemon (e.g., [rsyslog](https://www.rsyslog.com/)) then picks the message, parses it and writes it to various destinations. By default, it writes to files in /var/log/syslog or /var/log/messages depending on your Linux distro.

## Linux Kernel

The Linux kernel writes its own logs to a ring buffer. *Systemd* or the *syslog* daemon can read logs from this buffer, then write to the journal or flat files (typically /var/log/kern.log). You can also see kernel logs directly via dmesg:

$ dmesg -T

...

[Tue May 5 08:41:31 2020] EXT4-fs (sda1): mounted filesystem with ordered data mode. Opts: (null)

...

## Audit Logs

These are a special case of kernel messages designed for auditing actions such as file access. You’d typically have a service to listen for such security logs, like *auditd*. By default, auditd writes audit messages to /var/log/audit/audit.log

## Application Logs

Non-system applications tend to write to /var/log as well. Here are some popular examples:

* Apache HTTPD logs are typically written to /var/log/httpd or /var/log/apache2. HTTP access logs would be in /var/log/httpd/access.log
* MySQL logs typically go to /var/log/mysql.log or /var/log/mysqld.log
* You may have your own apps using a [logging library](https://sematext.com/blog/logging-libraries-vs-log-shippers/) to write to a specific file

NOTE:

* These log sources can interact with each other: *journald* can forward all its messages to *syslog*. Applications can write to *syslog* or the journal. It’s Linux, where everything is configurable.

# JournalD

## What Is JournalD?

Journal logs allow you to view, filter, and manage logs for services managed by systemd.

Journal logs are stored in binary format. We can read, analyze and manipulate the logs using journalctl command line tool.

**Extra info**:

In traditional **SysVinit** system, you have syslog that stores logs in plain text files.

## Enabling Journal Logs

The default location of journald logs is /var/log/journal directory. You should make sure that this directory exists. If not, create it yourself.

Next, in the /etc/systemd/journald.conf file, make sure that the value Storage is set to either auto or persistent.

The journald.conf file shows the default values. So even if there is a # in front of the entries, it means those are the default settings being used. If you want to change anything, you remove the # from that line.

## JournalD Commands

|  |  |
| --- | --- |
| **Command** | **Description** |
| journalctl | View all system logs in reverse chronological order (oldest logs are displayed first).  To reverse the order, add otpion -r.  This command uses less underneath to show logs. Which means you can use the same keys to move around the logs as you do with [the less command](https://linuxhandbook.com/less-command/). |
| journalctl -u <service-name> | View logs for a specific service.  (e.g., journalctl -u ssh).  Note that some logs are set with permission, in this case, you need to add sudo to the command line. |
| journalctl -f | View logs in real-time (similar to tail -f). |
| journalctl --since "YYYY-MM-DD"  --until "YYYY-MM-DD" | View logs from a specific date.  (e.g., journalctl --since "2024-12-20").  (e.g., journalctl --since "yesterday").  (e.g., journalctl --since "1 hour ago"). |
| journalctl -b | View logs from the current boot session.  To list all boot sessions: journalctl --list-boots |
| journalctl -p <priority-string-or-code> | Filter logs by priority.  (e.g., journalctl -p err for error).  (e.g., journalctl -p 2 for critical).  (e.g., journalctl -p 4..6 for warning and info).  Other priority strings are emerg, alert, crit, err, warning, notice, info and debug. Corresponding priority code is from 0 o 7. |
| journalctl \_UID=<uid>  journalctl \_GID=<gid>  journalctl \_PID=<pid> | Filter logs based on UID (User ID), GID (Group ID) and PID (Process ID). |
| journalctl -n <number> | Show the last specified number of logs.  (e.g., journalctl -n 100 for the last 100 logs). |
| journalctl -x | Show extra information on the log entries if available.  (some log entries have additional info that are not displayed in the normal log viewing). |
| journalctl --vacuum-time=<week\_num> | Clean up logs older than the specified time.  (e.g., journalctl --vacuum-time=2weeks two weeks).  You can also change the time frame in hours like 2h, in minutes like 2m, in seconds like 2s, in weeks like 2weeks, or in months like 2months. |
| journalctl --vacuum-size=<size> | Clean up logs to keep the system journal size under the specified limit.  (e.g., journalctl --vacuum-size=500M)  You can specify the size in GB with G, MB with M, KB with K. |
| journalctl --disk-usage | Check journal disk usage |
| systemctl status systemd-journald | Check journal memory usage |

## JournalD Configurations

Configs for JournalD is stored in /etc/systemd/journald.conf.

### Log Rotation

Logs can grow rapidly. Configure log rotation with:

[Journal]

SystemMaxUse=1G

### Log Forwarding

Logs can be forwarded to an external server. This is helpful when you want to integrate journal log with other tools for log visualization or any other purpose.

Enable log forwarding with:

[Journal]

ForwardToSyslog=yes

## Security and Permissions

System logs often contain sensitive information. Understanding who can access these logs is crucial for system security. Here's what you need to know:

# View current log access permissions

$ ls -l /var/log/journal/

# Add user to systemd-journal group

$ sudo usermod -a -G systemd-journal username

# Verify access

$ groups username

# Centralizing and Visualizing Linux Logs

<https://www.loggly.com/ultimate-guide/managing-linux-logs/>

<https://grafana.com/>

<https://prometheus.io/docs/introduction/overview/>