Linux logging

Linux has a special directory for storing logs called /var/log. This directory contains logs from the OS itself, services, and various applications running on the system.

**What’s Syslog?**

Syslog is a standard for creating and transmitting logs. The word “syslog” can refer to any of the following.

1. The syslog service, which receives and processes syslog messages. It listens for events by creating a socket located at /dev/log, which applications can write to. It can write messages to a local file or forward messages to a remote server. There are different syslog implementations including [rsyslogd](https://www.rsyslog.com/) and [syslog-ng](https://www.syslog-ng.com/).
2. The syslog protocol ([RFC 5424](https://tools.ietf.org/html/rfc5424)), which is a transport protocol that specifies how to transmit logs over a network. It is also a data format defining how messages are structured. By default, it uses port 514 for plaintext messages and port 6514 for encrypted messages.
3. A syslog message, which is any log formatted in the [syslog message format](https://tools.ietf.org/html/rfc5424#section-6). A syslog message consists of a standardized header and message containing the log’s contents.

More about syslog: <https://www.loggly.com/ultimate-guide/linux-logging-basics/>

<https://www.tutorialspoint.com/python-interface-to-unix-syslog-library-routines>

<https://stackify.com/linux-logs/>

**Severity levels**

* **0**: Emergency. The system is unusable.
* **1**: Alert. A condition has been flagged that should be corrected immediately.
* **2**: Critical. This covers crashes, coredumps, and significant failures in primary applications.
* **3**: Error. An error has been reported, but it is not considered severe.
* **4**: Warning. Brings a condition to your attention that, if ignored, may become an error.
* **5**: Notice. Used to report events that are unusual, but not errors.
* **6**: Information. Regular operational messages. These do not require action.
* **7**: Debug. Messages put into applications to make it easier for them to debug them.

<https://www.howtogeek.com/499623/how-to-use-journalctl-to-read-linux-system-logs/>