11.1.5 journald Logging Facts

This lesson covers the following topics:

- Journald Configuration
- Commands to View the Journal

Journald Configuration

Linux distributions based on the systemd daemon use the journald daemon for logging.

ⓘ Distributions based on SysVinit (init) use the syslogd daemon to manage logging.

The journald daemon maintains a system log called the journal, which is located in **/var/log/journal/**. The behavior of the journald daemon is configured in **/etc/systemd/journald.conf**. Some of the key configuration parameters in this file include the following:

Parameter	Description
MaxFileSec	Specifies the maximum amount of time to store entries in the journal file before starting a new file.
MaxRetentionSec	Specifies the maximum amount of time to store journal entries. Any entries older then the specified time are automatically deleted from the journal file.
MaxLevelStore	Specifies the maximum log level of messages stored in the journal file. All messages equal to or less than the log level specified are stored. Any messages above the specified level are dropped. This parameter can be set to: • **emerg** (0) • **alert** (1) • **crit** (2) • **err** (3) • **warning** (4) • **notice** (5) • **info** (6) • **debug** (7)
ForwardToSyslog	Configures journald to forward log messages to the traditional syslogd daemon.

Commands to View the Journal

You can view the journal with the following commands:

Command	Function	Example
journalctl	Views the entire journal. The output begins at the beginning of the journal and pauses one page at a time. To exit out of journalctl, press **q**.	**journalctl** Displays the journal, starting with the oldest entries.
journalctl -b	Views system boot messages. The messages from the most recent system boot are displayed by default. To display message from a specific boot, use the following options with this command: - Specify a positive number to display messages from the specified system boot, starting from the beginning of the journal. - Specify a negative number to display messages from the specified system boot starting from the end of the journal.	**journalctl -b 2** Displays messages created during the second boot event from the beginning of the journal. **journalctl -b -2** Displays messages created during the second boot event from the end of the journal.
journalctl -u	Displays only log entries related to a specific service running on the system.	**journalctl -u ntpd** Displays only journal messages relating to the ntpd daemon.
journalctl -f	Displays the last few entries in the journal. The journalctl command then monitors the journal and prints new entries as they are added.	**journalctl -f** Displays the last few entries in the journal and then prints new entries as they are added.