11.1.3 journald Logging

Click one of the buttons to take you to that part of the video.

journald Logging 0:00-0:35

In this lesson, we're going to discuss system logging on Linux. Before we begin, please be aware that older init-based Linux distributions use the syslog daemon to manage system logging, but newer Linux distributions that are based on systemd do not use syslog anymore. Instead, they use the journald daemon to manage logging.

Because most Linux distributions have migrated from init to systemd, we're actually going to focus just on journald logging in this lesson.

View the Journal 0:36-1:04

The journald daemon maintains a system log called the journal. It's located in the path that you see here, /var/log/journal.

You can't view the journal using a standard text manipulation utility like cat or less. Instead, you have to run the journalctl command. If you enter the journalctl command at the shell prompt with no parameters, then the entire journal is displayed one page at a time.

View Boot Messages 1:05-2:45

One of the neat features of the journald daemon is the fact that you can use it to view system message that were generated as the system booted up.

In order to do this, you need to use the -b option with the journalctl command. If you just run —˜journalctl -b', then the log messages from the most recent system boot will be displayed. However, you can also use journalctl to view messages from previous system boots as well.

If you run journalctl -b followed by a positive number, such as four, then the 'journalctl' command is going to just display the boot messages from the specified system boot starting at the beginning of the journal. By specifying 'journalctl -b 4', we will display the messages that were created at the fourth boot found from the beginning of the journal. But you can also go the other direction by specifying a negative number. If we specify 'journalctl -b -2', like we've done here, then we're going to look up the messages from the specified system boot starting at the end of the journal.

In this case, because we've entered 'journalctl -b -2', we're going to see the system messages that were created two boots ago. Frankly, this option is the one I use all of the time. I don't really use a positive number very much because usually, I'm looking for information a specified number of boots back. I don't really know what was in the fourth boot from the beginning of the journal because I may not know what the first boot in the journal even was. It's kind of a vague reference point.

View Service-Specific Messages 2:46-3:30

You can also use the journalctl command to display only the log entries that are related to a specific service running on the system. This is another thing that I use all of the time. It's extremely useful.

To do this, you enter 'journalctl -u' and then the name of the daemon whose related journal entries you want to view. In this case, we want to view all of the journal entries that are related to the sshd daemon running on the system.

Here, you can see information such as which port the daemon listings on. We can see the last connection that was closed by the sshd daemon. We can see the last time that someone logged in and accepted a password for the rtracy user that tells us where that user connected from to the sshd daemon and so on.

Configure the Journal Daemon 3:31-5:27

The behavior of the journal daemon is configured using the /etc/systemd/journald.comf file. Now, this file has many different parameters that you can configure. Some of the more useful ones are listed here. First of all, we have MaxFileSec. This specifies the maximum amount of time to store entries in the journal before starting a new file. Basically, it's the way we manage log rotation with the journal. We also have MaxRetentionSec, which specifies the amount of time to store journal entries. Any entries older than the specified time are automatically deleted from the journal file. We also have ForwardToSyslog. If your system has both the journald and the syslog daemons running, then you can forward your journald messages to the traditional syslog daemon. I never do that, but I guess if you wanted to, you could.

You can also configure MaxLevelStore. This controls the maximum log level of messages stored within the journal file. The way this works is all messages equal to or less than the specified log level will be stored. Any messages above the specified level will not be stored and will be dropped instead. So, you can set this parameter to one of the values shown here: Emerg, which is level zero, in which case only emergency messages would be stored. Alert stores alert and emergency messages. Critical stores critical, alert, and emergency. Errors stores errors, critical alert, and emergencies. Warnings stores warning, error, critical alert, and emergencies. Notice stores notice and everything else above it. Info stores almost everything. Debug does store absolutely everything, and you don't want to use this option, right here, unless you're troubleshooting a system problem. As soon as you're done troubleshooting a problem, you should switch it back to one of these other levels, up here. Otherwise, your log file is going to get real big real fast.

Summary 5:28-5:37

That's it for this lesson. In this lesson, we discussed how you can view the system journal on a distribution that uses systemd using the journalctl command. We also discussed how you can configure the journald daemon using the journald.comp file.
