

11.1 System Logging

As you study this section, answer the following questions:

- What is the role of the syslog daemon?
- What is the function of **logrotate** utility?
- Which commands can you use to view text-based log files?
- Which command show all failed login attempts on the system?

In this section, you will learn to:

- Configure journald.
- View log files.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Linux Pro	<p>4.3 Monitor and manage system access</p> <ul style="list-style-type: none"> • Monitor logging
CompTIA Linux+	<p>1.2 Given a scenario, install, configure, and monitor kernel modules.</p> <ul style="list-style-type: none"> • Commands <ul style="list-style-type: none"> ◦ dmesg <p>3.4 Given a scenario, implement logging services.</p> <ul style="list-style-type: none"> • Key file locations <ul style="list-style-type: none"> ◦ /var/log/secure ◦ /var/log/messages ◦ /var/log/[application] ◦ /var/log/kern.log • Log management <ul style="list-style-type: none"> ◦ Third-party agents ◦ logrotate ◦ /etc/rsyslog.conf ◦ journald: journalctl • lastb <p>4.1 Given a scenario, analyze system properties and remediate accordingly.</p> <ul style="list-style-type: none"> • CPU monitoring and configuration <ul style="list-style-type: none"> ◦ sar