11.1.11 Practice Questions

Candidate: Ethan Bonavida (suborange)
Date: 12/6/2022 10:53:47 pm • **Time Spent:** 01:11

Score: 100% Passing Score: 80%

Question 1: ✔ Correct

What is the full path to the directory that contains log files, including secure, messages, [application], and kern.log?

/var/log ✔

Explanation

The /var/log directory contains log files, including secure, messages, [application], and kern.log.

- /var/log/secure logs any attempts to log in as the root user or attempts to use the **su** command.
- /var/log/messages is the default file for storing system messages on systems running init.
- /var/log/[application] stores application specific log entries.
- /var/log/kern.log store kernel specific log entries.

References

11.1.2 Log File Facts

q_log_com_f_01.question.fex

Question 2: ✔ Correct

Which of the following commands shows failed login attempts on the system?

- **lastb**
- **lastlog**
- **tail**
- **sar**

Explanation

lastb shows all failed login attempts on the system.

lastlog shows a list of the dates and times for the last login for each user.

sar views system statistics.

tail shows the last 10 lines of a file.

References

11.1.7 Log File Display Facts

q_log_com_f_lp5_lastb.question.fex

Question 3: ✔ Correct

Linux systems that use SysVinit (init) use the syslogd daemon to manage logging.

Which of the following daemons is used on newer system-based distributions to provide a local system log file?

- journald
- syslog
- systemctl
- rsyslog

Explanation

Newer Linux distributions that are based on systemd do not use syslog anymore. Instead, they use the journald daemon to manage logging.

Older init-based Linux distributions use the syslog daemon to manage system logging.

rsyslog is a lightweight daemon that provides centralized logs.

systemctl manages network services on systemd-based distributions. (journalctl is used to view the entire journal on system running journald.)

References

11.1.5 journald Logging Facts

q_journald_f_lp5_journald.question.fex

Question 4: ✔ Correct

Which of the following commands manages, compresses, renames, and deletes log files based on a specific criteria such as size or date?

- lastlog
- **logrotate**
- dmesg
- logger

Explanation

logrotate manages, compresses, renames, and deletes log files based on specific criteria (such as size or date).

lastlog shows a list of the dates and times for the last login for each user.

logger changes the message severity and where logged messages are sent.

dmesg views the boot logs and troubleshoots hardware errors. The **dmesg** command shows information about all the hardware controlled by the kernel and displays error messages as they occur.

References

11.1.9 logrotate Facts

q_logs_lp5_logrotate.question.fex