Linux Processes, Jobs, Logs.

By Vignesh S

Process:

Fundamental concept that represents a running instance of a program.A process is an independent execution unit with its own memory space, resources, and control flow.

Program vs. Process:

A program is a static set of instructions stored on disk, while a process is the dynamic execution of those instructions in memory. A single program can give rise to multiple processes if it's executed multiple times.

The ps Command:

The ps command allows you to view a snapshot of currently running processes. You can use various options to customize the output:

ps aux: Displays a comprehensive list of all running processes, including user, CPU usage, memory utilization, and more.

ps -ef: Similar to ps aux, but the format might vary slightly depending on the distribution.

ps -eH: Displays a hierarchical view of processes, showing parent-child relationships.

The kill command is used to send signals to processes.
Basic Syntax: kill [signal] PID

kill 1234: Sends the default SIGTERM signal to the process with PID 1234.
kill -9 5678: Sends the SIGKILL signal to the process with PID 5678, forcefully terminating it.

SIGTERM (15): Request for process termination.
SIGKILL (9): Immediate and forceful termination.
SIGINT (2): Interrupt signal, often sent by Ctrl+C.
SIGHUP (1): Hangup signal, often used to indicate the termination of a terminal session.

Ps -aux / ps
Vi & (fg, bg)
Sleep 100 fg/bg
Kill -<SIGTERM> <PID>
Jobs
Fg Jobid
To send foreground job to bg ctrl+z (terminate) and then bg.

CRON JOB

A cron job is a scheduled task that runs automatically at specific intervals on a Unix-like operating system, such as Linux. These tasks are useful for automating various system maintenance, backups, data processing, and more. Let's start by understanding the basic concepts of cron jobs.

Cron Syntax:

```
* * * * *
| | | | |
| | | | +----- Day of the week (0 - 6) (Sunday = 0)
| | | +------- Month (1 - 12)
| | +--------- Day of the month (1 - 31)
| +----------- Hour (0 - 23)
+------------- Minute (0 - 59)
```

- crontab -l
- crontab -e

LOGS:

Logs are essential records generated by various software applications and system processes in a Linux environment.

They provide valuable information about the system's health, activities, errors, and events.

Analyzing logs is crucial for troubleshooting issues, monitoring system performance, identifying security breaches, and maintaining a stable and reliable system.

System Logs (syslog):

System logs, often referred to as syslog logs, provide a centralized location for recording various events and messages generated by the operating system, system services, and applications.

These logs are crucial for monitoring system health, identifying errors, diagnosing problems, and maintaining the system

. Auth Logs (auth.log):

The auth.log file contains authentication-related events and messages. It records information about user logins, logouts, authentication failures, and other security-related events.

Monitoring the auth.log is essential for tracking unauthorized access attempts and ensuring the security of the system. This log file is commonly found in the **/var/log/** directory.

DPKG Logs (dpkg.log):

The dpkg.log file records all the actions performed using the Debian Package Manager (dpkg).

This includes installation, removal, and updates of software packages on a Debian-based system.

The log helps track changes made to the software configuration and can be useful for diagnosing issues related to package management.

Journal Logs (journalctl):

Journal logs are part of the systemd logging system, which is a modern replacement for traditional system logs.

journalctl provides access to the logs stored in the systemd journal.

This journal system captures logs from the kernel, system services, and applications. It offers features like structured logging, efficient storage, and easy searching.

Application Logs:
These logs are generated by various applications and services running on the system.

They can be found in directories like **/var/log/nginx/, /var/log/apache2/,** etc.

User Logs:
These logs contain information about user activities, including login/logout events, commands executed, and more. They are typically stored in the user's home directory, specifically **~/.bash_history.**

Common Log Commands:

tail: Displays the last few lines of a log file. Useful for real-time monitoring. Example: tail -n 50 /var/log/syslog

less or more: Allows you to view log files page by page. Example: less /var/log/auth.log

grep: Searches for specific keywords or patterns within log files. Example: grep "error" /var/log/syslog

Journalctl: Views systemd journal logs. Example: journalctl -xe

dmesg: Displays kernel ring buffer messages. Example: dmesg | grep -i "error"

cat: Displays the entire content of a log file. Example: cat /var/log/messages