2025

Research And Explain The Most Common Commands Used By System Admins In A Linux Environment

MOSSÉ CYBERSECURITY INSTITUTE

AARON AMRAN BIN AMIRUDDIN

Student ID: nxCLnZGLgyOUMpnDw16rtDvYuTF2

Table of Contents

grep

Purpose: grep (global regular expression printer) searches for lines in text files or output streams that matches the specified pattern of characters.

Using Its Output: The command highlights or returns only those lines that contain the search term, making it easier to locate relevant information within logs, configuration files, or command outputs. You can use its output to filter data for further analysis, extract specific details, or debug errors by isolating relevant log entries.

ps

Purpose: ps displays information about the currently running processes. It provides details like process ID (PID), terminal, CPU usage, and command name.

Using Its Output: By reviewing its output, you can identify running processes, monitor resource usage, and troubleshoot system performance issues. For instance, you can use the PID provided by ps to terminate a process with kill or analyze a process consuming high CPU/memory.

lsof

Purpose: lsof (List Open Files) shows all open files and the processes that opened them, including files, directories, network sockets, and devices.

Using Its Output: This command is particularly useful for diagnosing file access issues, identifying which process is locking a file, or troubleshooting network socket issues. You can also use the output to determine which files are in use before unmounting a filesystem.

df

Purpose: df (disk free) reports disk space usage for file systems, showing the amount of used and available space.

Using Its Output: The output helps in monitoring disk space, identifying partitions that are running out of space, and planning for storage allocation. Administrators use this information to manage disk quotas and to schedule clean-up tasks when necessary.

chmod

Purpose: chmod changes the file system mode (permissions) of files and directories, controlling who can read, write, or execute them.

Using Its Output: While chmod itself does not produce an extensive output, its effect is observed in the changed permissions. Administrators can verify permissions using ls -l to ensure that files have the correct access controls, which is crucial for system security.

top

Purpose: top provides a real-time, dynamic view of system processes, including CPU and memory usage, running processes, and overall system load.

Using Its Output: The continuously updating display allows you to monitor system performance, identify resource-hungry processes, and diagnose system bottlenecks. You can also interact with the display (e.g., killing processes directly) based on the information provided.

kill

Purpose: kill sends signals to processes, most commonly used to terminate processes by sending the SIGTERM or SIGKILL signals.

Using Its Output: The command itself typically doesn't produce output unless there's an error. However, by monitoring system messages or using ps/top afterward, you can verify that the intended process has been terminated. It's a fundamental tool for process management and troubleshooting misbehaving processes.

systemctl

Purpose: systemctl is used to control the state of the system and its services on systemd-based systems. It can start, stop, restart, enable, disable, and check the status of services.

Using Its Output: The command provides detailed service statuses, logs, and error messages. Administrators use this information to ensure that critical services are running, to troubleshoot service failures, or to check dependency and status details of services.

ss

Purpose: ss (Socket Statistics) is used to display information about network sockets, including TCP, UDP, and other types of network connections.

Using Its Output: The command outputs details like local and remote addresses, connection states, and the processes owning the sockets. This is invaluable for diagnosing network issues, analyzing active connections, and monitoring open ports for security audits.

ip

Purpose: The ip command is a powerful utility for network interface configuration and management, replacing older tools like ifconfig. It handles tasks such as configuring IP addresses, routing, and network interfaces.

Using Its Output: The output provides comprehensive details about network configurations, routes, and interface statuses. Administrators use this information to verify network settings, diagnose connectivity issues, and perform dynamic network adjustments.

find

Purpose: find searches for files and directories within a specified directory hierarchy based on various criteria like name, size, type, or modification time.

Using Its Output: The command returns the full paths of files or directories that meet the specified conditions. This output can be piped into other commands for batch processing (such as deletion, archiving, or modification) or used in scripts for automating routine tasks.

du

Purpose: du (Disk Usage) estimates and reports the space used by files and directories.

Using Its Output: The output shows the size of directories and files, which helps in identifying space hogs and managing disk usage. Administrators can use this information to optimize storage, plan capacity, or target directories for cleanup operations.

chown

Purpose: chown changes the ownership of files and directories, assigning them to a specified user and/or group.

Using Its Output: Similar to chmod, chown does not produce significant output by default, but its effect is visible when you list files with ls -l. This tool is essential for managing file ownership and ensuring proper access control across multi-user systems.

sudo

Purpose: sudo allows permitted users to execute commands with elevated privileges, such as those of the superuser or another user, ensuring controlled and logged access to administrative commands.

Using Its Output: While sudo itself is more about permission escalation than output, its usage logs and any errors it reports can provide insights into permission issues or misconfigurations. The logging helps in security auditing and troubleshooting unauthorized access attempts.

tar

Purpose: tar is used for archiving files and directories. It can combine multiple files into a single archive file (often compressed) and extract them when needed.

Using Its Output: The output of tar operations includes listings of archived files when listing content, as well as confirmation messages upon creation or extraction. Administrators use this information to verify the integrity of backups, automate deployment processes, and ensure that archives contain the expected files.

References

James, H. (2024, August 26). *90 Linux Commands frequently used by Linux Sysadmins (updated to 100+)*. Retrieved from linuxblog.io: https://linuxblog.io/90-linux-commands-frequently-used-by-linux-sysadmins/

Tyler Carrigan, N. L. (2021, June 30). *17 Linux commands every sysadmin should know*. Retrieved from redhat.com: https://www.redhat.com/en/blog/linux-commands-to-know