

Lab exercises

Exercise 1 — Explore filesystem and /var/log

1. List top-level directories under / and explain typical purpose of /var, /etc, /usr, /opt, /srv, /home.
2. Inspect /var/log. Which files and directories there? Identify which processes write to the logs you see.
3. Under /var/log/myapp, show the last 10 lines of myapp.log.
4. Count how many ERROR lines are in /var/log/myapp/myapp.log* (including rotated files).
5. Find the most common action= field value in /var/log/myapp/myapp.log*.

Exercise 2 — Users, groups, sudo, and permissions

1. Show all users that were created for the lab. Show each user's primary group and supplementary groups.
2. Make a new user labadmin with home dir and set password LabAdm!23, add to sudo group.
3. Make /srv/shared writable by group devops and confirm student1 can create a file there but student3 (not in group) cannot.
4. Explain the meaning of chmod 775 /srv/shared.
5. Inspect /usr/local/bin/lab-whoami. Explain why student2 running it prints a different uid or why it might not.

Exercise 3 — File text manipulation (grep, awk, sed, head, tail)

1. From /var/log/auth.log.lab, print only the lines with Failed password.
2. From myapp.log, extract columns user and action and produce a sorted list of unique user action pairs with counts.
 - Output format: count user action, sorted descending by count.
3. Using sed, replace code= values in /var/log/auth.log.lab to code=XXXX and show the modified lines (do not edit file in place — stream to stdout).
4. From /etc/myapp.conf, print the value of max_connections only.
5. Show last 20 lines of /var/log/myapp/myapp.log and follow new appended lines (simulate a student watching logs in real-time).