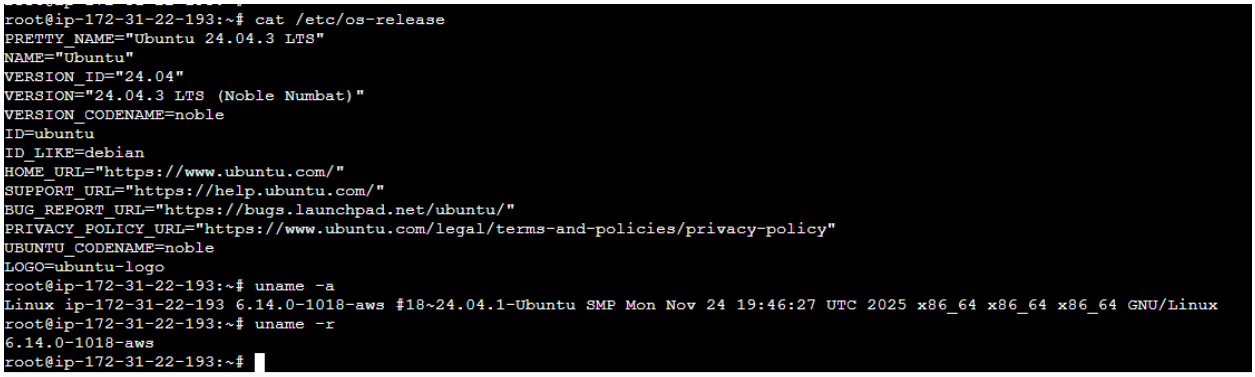
Module -1 : Linux

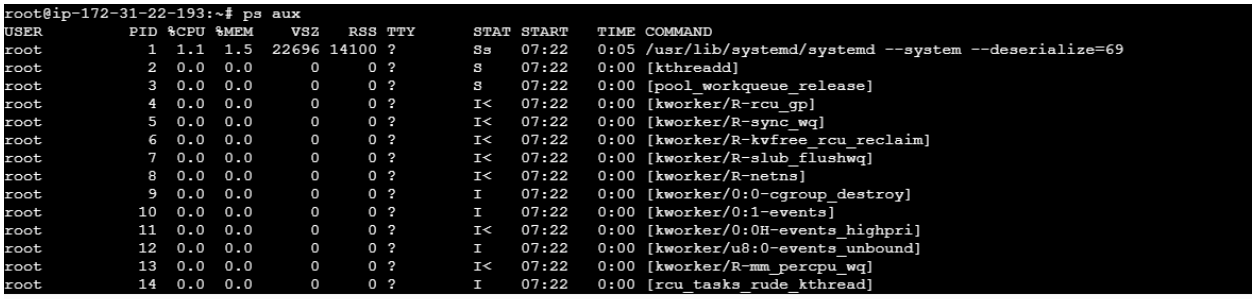
Lab 1: Understanding & Exploring the OS

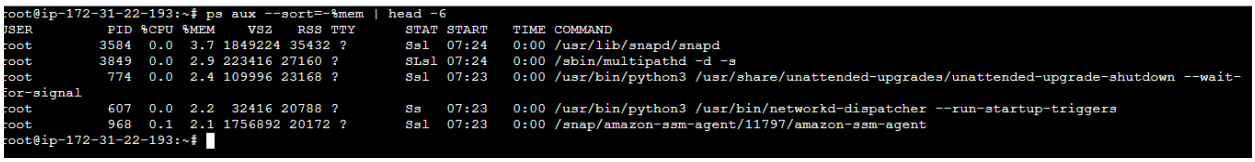
Objective: Identify OS version, kernel info, and processes.
Tasks:

- Find out the OS name, version, and kernel release.



- List all running processes and identify the top 5 memory consumers.





- Check the system uptime and logged-in users.
  Commands Hint: `uname -a`, `cat /etc/os-release`, `ps aux`, `top`, `w`

```
root@ip-172-31-22-193:~# uptime
 07:32:04 up 9 min,  1 user,  load average: 0.00, 0.05, 0.05
root@ip-172-31-22-193:~# w
 07:32:07 up 9 min,  1 user,  load average: 0.00, 0.05, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU  WHAT
ubuntu            18.206.107.28    07:23    7:34   0.00s  0.02s sshd: ubuntu [priv]
root@ip-172-31-22-193:~# who
ubuntu   pts/0        2026-01-29 07:23 (18.206.107.28)
ubuntu   pts/1        2026-01-29 07:23 (18.206.107.28)
root@ip-172-31-22-193:~#
```

Lab 2: Virtual Machines & Networking

Objective: Set up a Linux VM and configure basic networking.
Tasks:

- Create a new Ubuntu VM using VirtualBox or VMware.
- Assign a static IP and verify connectivity with another VM using `ping`.
- Configure hostname and update `/etc/hosts` file.

```
root@devops-vm:~#
```

Lab 3: Package Management

Objective: Manage software packages.
Tasks:

- Install `nginx`, verify it's running, and check its version.

```
root@devops-vm:~# systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)
     Active: active (running) since Thu 2026-01-29 07:44:11 UTC; 28s ago
       Docs: man:nginx(8)
    Process: 8291 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
    Process: 8293 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
   Main PID: 8323 (nginx)
      Tasks: 3 (limit: 1008)
     Memory: 2.5M (peak: 5.4M)
        CPU: 26ms
     CGroup: /system.slice/nginx.service
             ├─8323 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
             ├─8325 "nginx: worker process"
             └─8326 "nginx: worker process"

Jan 29 07:44:11 devops-vm systemd[1]: Starting nginx.service - A high performance web server and a reverse proxy server...
Jan 29 07:44:11 devops-vm systemd[1]: Started nginx.service - A high performance web server and a reverse proxy server.
root@devops-vm:~# nginx -v
nginx version: nginx/1.24.0 (Ubuntu)
root@devops-vm:~# curl 54.204.56.51
```

```
root@devops-vm:~# curl 54.204.56.51
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
```

- Remove a package safely and clean up dependencies.

```
root@devops-vm:~# sudo apt remove nginx -y
sudo apt autoremove -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required
  nginx-common
Use 'sudo apt autoremove' to remove it.
The following packages will be REMOVED:
  nginx
0 upgraded, 0 newly installed, 1 to remove and 6 not upgraded.
After this operation, 1352 kB disk space will be freed.
(Reading database ... 71799 files and directories currently installed.)
Removing nginx (1.24.0-2ubuntu7.5) ...
Processing triggers for man-db (2.12.0-4build2) ...
```

- Use `apt`, `snap`, or `yum` (depending on OS).
  Commands Hint: `sudo apt update`, `sudo apt install nginx -y`, `systemctl status nginx`

Lab 4: Users, Groups & Permissions

Objective: Manage users and permissions.
Tasks:

- Create a new group `devops` and a user `jenkins`.

```
root@devops-vm:~# sudo groupadd devops
root@devops-vm:~# sudo adduser jenkins
```

- Add the user to the devops group and set a password.

```
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] Yes
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for jenkins
```

- Create a shared directory `/opt/shared` and assign group ownership.
  Commands Hint: `adduser`, `groupadd`, `usermod`, `chown`, `chmod`

```
root@devops-vm:~# sudo mkdir /opt/shared
sudo chown :devops /opt/shared
sudo chmod 2775 /opt/shared
root@devops-vm:~# ls -lrth
total 4.0K
drwx------ 3 root root 4.0K Jan 29 07:23 snap
root@devops-vm:~# cd /opt/shared
root@devops-vm:/opt/shared# ls -lrth
total 0
root@devops-vm:/opt/shared# df -kh
Filesystem       Size  Used Avail Use% Mounted on
/dev/root        6.8G  2.1G  4.7G  31% /
tmpfs            458M     0  458M   0% /dev/shm
tmpfs            183M  884K  182M   1% /run
tmpfs            5.0M     0  5.0M   0% /run/lock
efivarfs         128K  3.6K  120K   3% /sys/firmware/efi/efivars
/dev/nvme0n1p16  881M   89M  730M  11% /boot
/dev/nvme0n1p15  105M  6.2M   99M   6% /boot/efi
tmpfs             92M   12K   92M   1% /run/user/1000
root@devops-vm:/opt/shared# ls -ld /opt/shared
drwxrwsr-x 2 root devops 4096 Jan 29 07:55 /opt/shared
root@devops-vm:/opt/shared#
```

`-a` **adds the user to a new group without removing existing groups.**

👉 It **appends** the group.

Lab 5: Linux File System & Ownership

Objective: Explore file system hierarchy and permissions.

Tasks:

- Find the mount points and available disk space.

```
root@devops-vm:~# df -kh
Filesystem       Size  Used Avail Use% Mounted on
/dev/root        6.8G  2.1G  4.7G  31% /
tmpfs            458M     0  458M   0% /dev/shm
tmpfs            183M  884K  182M   1% /run
tmpfs            5.0M     0  5.0M   0% /run/lock
efivarfs         128K  3.6K  120K   3% /sys/firmware/efi/efivars
/dev/nvme0n1p16  881M   89M  730M  11% /boot
/dev/nvme0n1p15  105M  6.2M   99M   6% /boot/efi
tmpfs             92M   12K   92M   1% /run/user/1000
root@devops-vm:~# lsblk
NAME         MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0          7:0    0 27.6M  1 loop /snap/amazon-ssm-agent/11797
loop1          7:1    0   74M  1 loop /snap/core22/2163
loop2          7:2    0 50.9M  1 loop /snap/snapd/25577
nvme0n1      259:0    0    8G  0 disk
├─nvme0n1p1  259:1    0    7G  0 part /
├─nvme0n1p14 259:2    0    4M  0 part
├─nvme0n1p15 259:3    0  106M  0 part /boot/efi
└─nvme0n1p16 259:4    0  913M  0 part /boot
root@devops-vm:~# mount
/dev/nvme0n1p1 on / type ext4 (rw,relatime,discard,errors=remount-ro,commit=30)
devtmpfs on /dev type devtmpfs (rw,nosuid,noexec,relatime,size=456788k,nr_inodes=114197,mode=755,inode64)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
```

- Identify file types using `ls -l` and `file`.

```
root@devops-vm:~# ls -l /etc/passwd
file /etc/passwd
-rw-r--r-- 1 root root 1898 Jan 29 07:51 /etc/passwd
/etc/passwd: ASCII text
root@devops-vm:~#
```

- Change ownership of a file to another user.
  Commands Hint: `df -h`, `lsblk`, `du -sh`, `chown`, `chmod`

```
root@devops-vm:~# ls -lrth
total 4.0K
drwx------ 3 root    root    4.0K Jan 29 07:23 snap
-rw-r--r-- 1 jenkins devops     0 Jan 29 08:09 testfile
root@devops-vm:~#
```

  `Jenkins -> user who owns the file`

  `Devops -> Group owning the file.`

Lab 6: Security and System Administration

Objective: Strengthen Linux security.
Tasks:

- Check running services and open ports.

```
root@devops-vm:~# systemctl list-units --type=service --state=running
  UNIT                                      LOAD   ACTIVE SUB     DESCRIPTION
  acpid.service                             loaded active running ACPI event daemon
  chrony.service                            loaded active running chrony, an NTP client/server
  cron.service                              loaded active running Regular background program processing daemon
  dbus.service                              loaded active running D-Bus System Message Bus
  getty@tty1.service                        loaded active running Getty on tty1
  irqbalance.service                        loaded active running irqbalance daemon
  ModemManager.service                      loaded active running Modem Manager
  multipathd.service                        loaded active running Device-Mapper Multipath Device Controller
  networkd-dispatcher.service               loaded active running Dispatcher daemon for systemd-networkd
  polkit.service                            loaded active running Authorization Manager
  rsyslog.service                           loaded active running System Logging Service
  serial-getty@ttyS0.service                loaded active running Serial Getty on ttyS0
  snap.amazon-ssm-agent.amazon-ssm-agent.service loaded active running Service for snap application amazon-ssm-agent.amazon-ssm-agent
  snapd.service                             loaded active running Snap Daemon
  ssh.service                               loaded active running OpenBSD Secure Shell server
  systemd-journald.service                  loaded active running Journal Service
  systemd-logind.service                    loaded active running User Login Management
```

```
root@devops-vm:~# netstat -tulnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1/systemd
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      3328/systemd-resolv
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN      3328/systemd-resolv
tcp6       0      0 :::22                   :::*                    LISTEN      1/systemd
udp        0      0 127.0.0.54:53           0.0.0.0:*                           3328/systemd-resolv
udp        0      0 127.0.0.53:53           0.0.0.0:*                           3328/systemd-resolv
udp        0      0 172.31.22.193:68        0.0.0.0:*                           3152/systemd-networ
udp        0      0 127.0.0.1:323           0.0.0.0:*                           7656/chronyd
udp6       0      0 ::1:323                 :::*                                7656/chronyd
root@devops-vm:~#
```

- Stop an unused service and disable it from auto-start.

```
root@devops-vm:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Thu 2026-01-29 08:17:48 UTC; 1min 0s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 9910 (apache2)
      Tasks: 55 (limit: 1008)
     Memory: 5.3M (peak: 5.6M)
        CPU: 41ms
     CGroup: /system.slice/apache2.service
             ├─9910 /usr/sbin/apache2 -k start
             ├─9912 /usr/sbin/apache2 -k start
             └─9913 /usr/sbin/apache2 -k start

Jan 29 08:17:48 devops-vm systemd[1]: Starting apache2.service - The Apache HTTP Server...
Jan 29 08:17:48 devops-vm systemd[1]: Started apache2.service - The Apache HTTP Server.
root@devops-vm:~#
```

```
root@devops-vm:~# sudo systemctl stop apache2
sudo systemctl disable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install disable apache2
Removed "/etc/systemd/system/multi-user.target.wants/apache2.service".
root@devops-vm:~#
```

- Configure `ufw` firewall to allow only SSH and HTTP.
  Commands Hint: `netstat -tuln`, `systemctl disable`, `ufw enable`, `ufw allow ssh`

```
root@devops-vm:~# sudo ufw allow ssh
sudo ufw allow http
sudo ufw enable
sudo ufw status
Rules updated
Rules updated (v6)
Rules updated
Rules updated (v6)
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)

root@devops-vm:~#
```

UFW is host-level

UFW is a **frontend for iptables / nftables**

It controls:

- Incoming traffic
- Outgoing traffic
- Ports (80, 443, 22, etc.)
- Protocols (TCP / UDP)
- Source IPs

How UFW is used in REAL production

🔹 **Typical production setup (Cloud)**

Layer	Tool
Network perimeter	AWS Security Groups / Azure NSG
Subnet level	NACL
Host level	**UFW (optional but recommended)**

```
App level          Auth, TLS, WAF
```

📌 UFW is a **second line of defense**

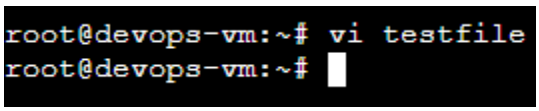
When companies ENABLE UFW in prod

✅ Bastion hosts
✅ Database servers
✅ Jenkins servers
✅ On-prem VMs
✅ Critical VMs with SSH exposure

Lab 7: Working with Vim & Filters

Objective: Use `vim` and shell filters effectively.
Tasks:

- Open a file in `vim`, edit text, and save changes.

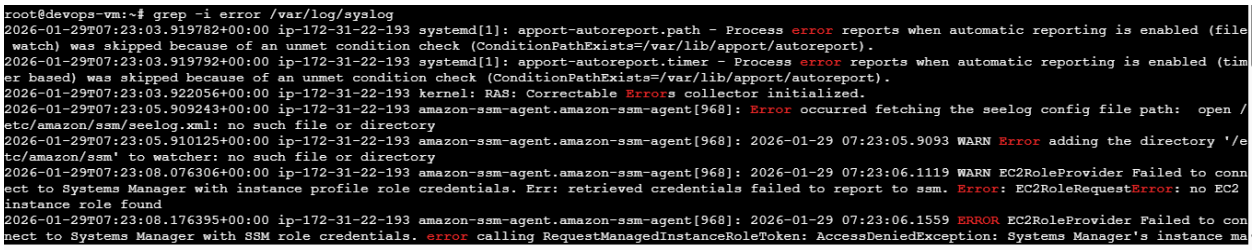


Vim basics

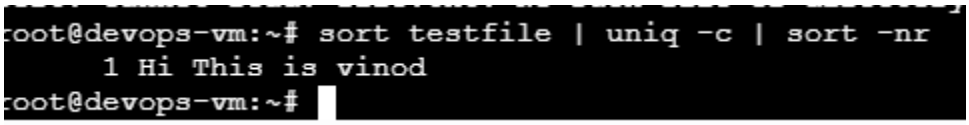
- Insert: `i`
- Save: `:w`

- Exit: `:q`
- Save & exit: `:wq`

- Use filters: extract all error lines from `/var/log/syslog` using `grep`.



- Sort and count unique entries from a text file.
  Commands Hint: `vim`, `grep`, `sort`, `uniq`, `awk`, `cut`



This command sorts a file, counts duplicate lines, and displays them in descending frequency order.

S → U → S

Sort → Uniq → Sort

Lab 8: Cron Jobs & Automation

Objective: Schedule automated tasks.
Tasks:

- Create a cron job that backs up `/etc` every day to `/backup/etc`.

```
root@devops-vm:~# sudo mkdir -p /backup/etc
root@devops-vm:~#
```

crontab -l # list cron jobs

crontab -e # edit cron jobs

crontab -r # remove cron jobs (dangerous)

- Verify scheduled jobs for a user.

```
) 1 * * * tar -czf /backup/etc/etc_$(date +\%F).tar.gz /etc >> /var/log/etc_backup.log 2>&1
root@devops-vm:~#
```

- Redirect cron job output to a log file.
  Commands Hint: `crontab -e`, `crontab -l`, `cat /var/log/syslog | grep CRON`

```
root@devops-vm:~# grep CRON /var/log/syslog
2026-01-29T07:23:03.919961+00:00 ip-172-31-22-193 cron[598]: (CRON) INFO (pidfile fd = 3)
2026-01-29T07:23:03.919966+00:00 ip-172-31-22-193 cron[598]: (CRON) INFO (Running @reboot jobs)
2026-01-29T07:25:01.790573+00:00 ip-172-31-22-193 CRON[7740]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
2026-01-29T07:35:01.811493+00:00 ip-172-31-22-193 CRON[7769]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
2026-01-29T07:45:01.824604+00:00 ip-172-31-22-193 CRON[8407]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
2026-01-29T07:55:01.863778+00:00 ip-172-31-22-193 CRON[8715]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
2026-01-29T08:05:01.904786+00:00 ip-172-31-22-193 CRON[8766]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
2026-01-29T08:15:01.989071+00:00 ip-172-31-22-193 CRON[8840]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
2026-01-29T08:17:01.996182+00:00 ip-172-31-22-193 CRON[8951]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)
2026-01-29T08:25:01.024899+00:00 ip-172-31-22-193 CRON[10588]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
2026-01-29T08:35:01.037068+00:00 ip-172-31-22-193 CRON[10616]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
root@devops-vm:~#
```

Lab 9: Archiving & Compression

Objective: Manage file backups.
Tasks:

- Compress `/var/log` using `tar` and `gzip`.

```
root@devops-vm:~# tar -cvzf logs_backup.tar.gz /var/log
tar: Removing leading `/' from member names
/var/log/
/var/log/btmp
/var/log/private/
/var/log/lastlog
/var/log/kern.log
/var/log/sysstat/
/var/log/sysstat/sa29
/var/log/auth.log
/var/log/README
/var/log/wtmp
/var/log/chrony/
/var/log/apache2/
/var/log/apache2/access.log
/var/log/apache2/other_vhosts_access.log
/var/log/apache2/error.log
/var/log/cloud-init.log
/var/log/dpkg.log
```

- Extract the archive to `/tmp/log_backup`.

```
root@devops-vm:~# mkdir /tmp/log_backup
tar -xvzf logs_backup.tar.gz -C /tmp/log_backup
var/log/
var/log/btmp
var/log/private/
var/log/lastlog
var/log/kern.log
var/log/sysstat/
var/log/sysstat/sa29
var/log/auth.log
var/log/README
var/log/wtmp
var/log/chrony/
var/log/apache2/
var/log/apache2/access.log
var/log/apache2/other_vhosts_access.log
var/log/apache2/error.log
var/log/cloud-init.log
var/log/dpkg.log
```

- Verify file integrity after extraction.
  Commands Hint: `tar -cvzf`, `tar -xvzf`, `gzip`, `gunzip`

Lab 10: SSH, SCP & Remote Access

Objective: Secure remote connection and file transfer.
Tasks:

- Generate SSH key pair using `ssh-keygen`.
- Copy the public key to another VM for passwordless SSH.
- Transfer a file securely using `scp`.
  Bonus: Use `ssh` to automate a remote command execution (e.g., `uptime` check).
  Commands Hint: `ssh-keygen`, `ssh-copy-id`, `scp`, `ssh user@host`