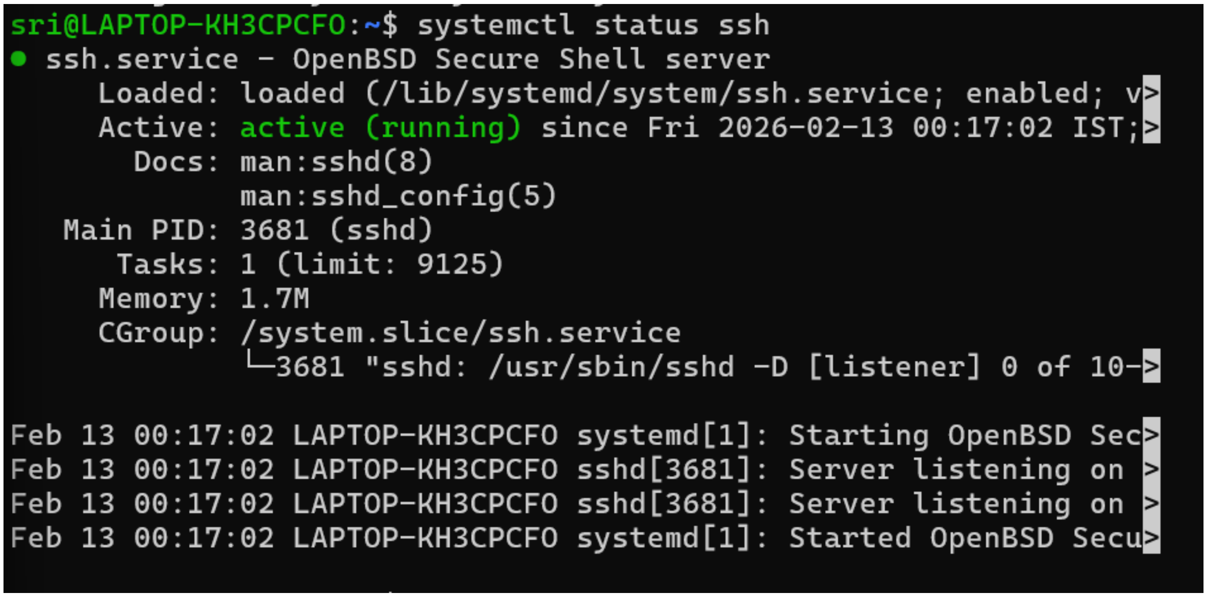
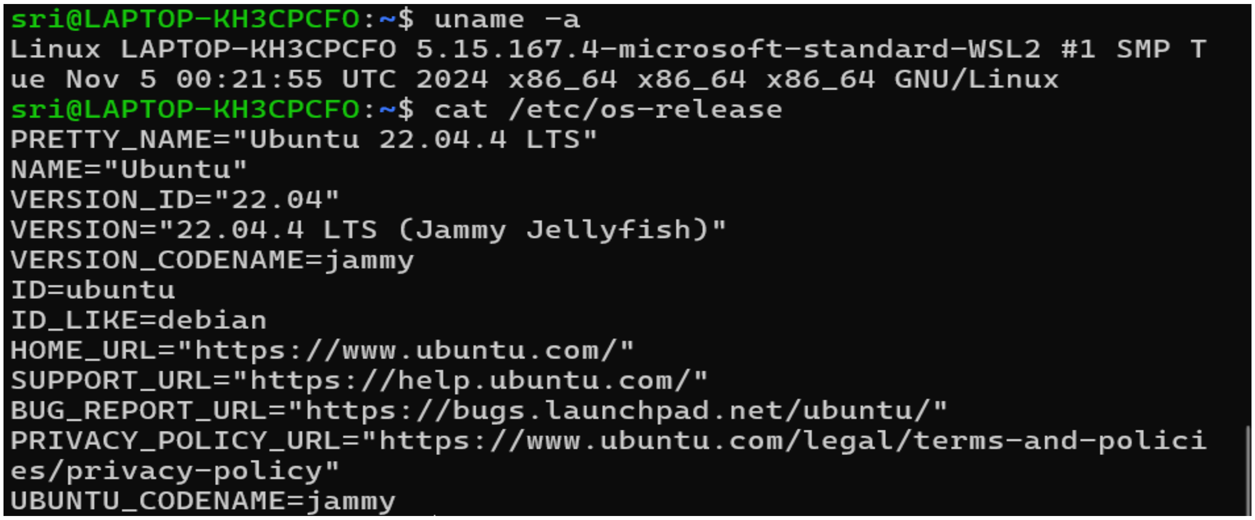
Day 05 – Linux Troubleshooting Drill : CPU, Memory, Logs

- Choose Target Service : systemctl status ssh.



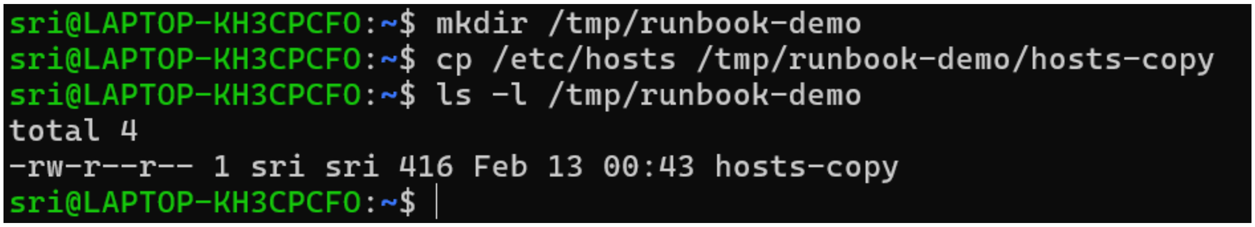
```
sri@LAPTOP-KH3CPCFO:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; v>
     Active: active (running) since Fri 2026-02-13 00:17:02 IST;>
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 3681 (sshd)
      Tasks: 1 (limit: 9125)
     Memory: 1.7M
     CGroup: /system.slice/ssh.service
             └─3681 "sshd: /usr/sbin/sshd -D [listener] 0 of 10->

Feb 13 00:17:02 LAPTOP-KH3CPCFO systemd[1]: Starting OpenBSD Sec>
Feb 13 00:17:02 LAPTOP-KH3CPCFO sshd[3681]: Server listening on >
Feb 13 00:17:02 LAPTOP-KH3CPCFO sshd[3681]: Server listening on >
Feb 13 00:17:02 LAPTOP-KH3CPCFO systemd[1]: Started OpenBSD Secu>
```

- **Environment basics** (Kernel info : uname –r , OS version : cat /etc/os-release)



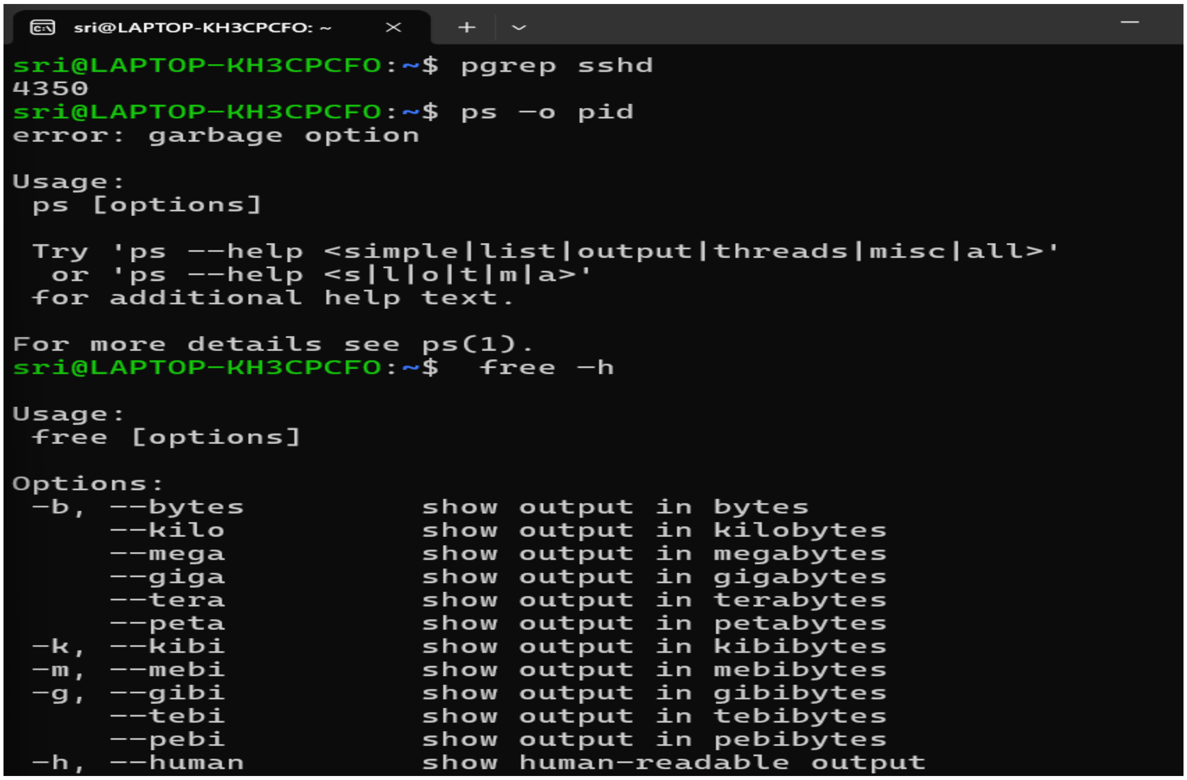
```
sri@LAPTOP-KH3CPCFO:~$ uname -a
Linux LAPTOP-KH3CPCFO 5.15.167.4-microsoft-standard-WSL2 #1 SMP T
ue Nov 5 00:21:55 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
sri@LAPTOP-KH3CPCFO:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 22.04.4 LTS"
NAME="Ubuntu"
VERSION_ID="22.04"
VERSION="22.04.4 LTS (Jammy Jellyfish)"
VERSION_CODENAME=jammy
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-polici
es/privacy-policy"
UBUNTU_CODENAME=jammy
```

- Filesystem sanity : (create Temporary Folder - mkdir /tmp/runbook-demo , Copy System file - cp /etc/hosts /tmp/runbook-demo/hosts-copy , To verify : ls -l /tmp/runbook-demo)

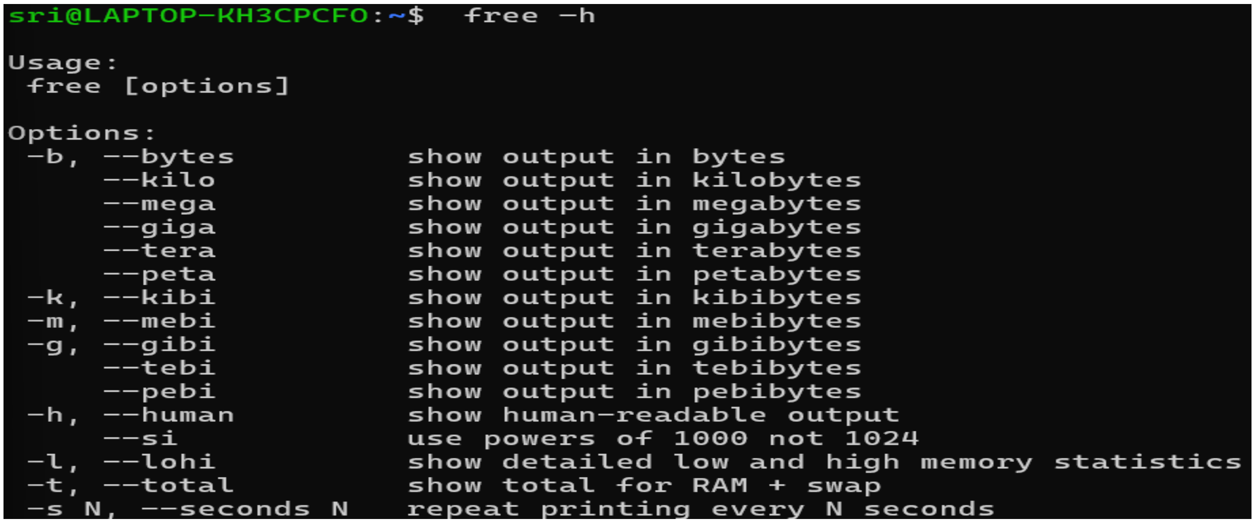


```
sri@LAPTOP-KH3CPCFO:~$ mkdir /tmp/runbook-demo
sri@LAPTOP-KH3CPCFO:~$ cp /etc/hosts /tmp/runbook-demo/hosts-copy
sri@LAPTOP-KH3CPCFO:~$ ls -l /tmp/runbook-demo
total 4
-rw-r--r-- 1 sri sri 416 Feb 13 00:43 hosts-copy
sri@LAPTOP-KH3CPCFO:~$
```

- CPU memory Snapshot : (pgrep sshd , top , htop, ps –o pid , free –h)

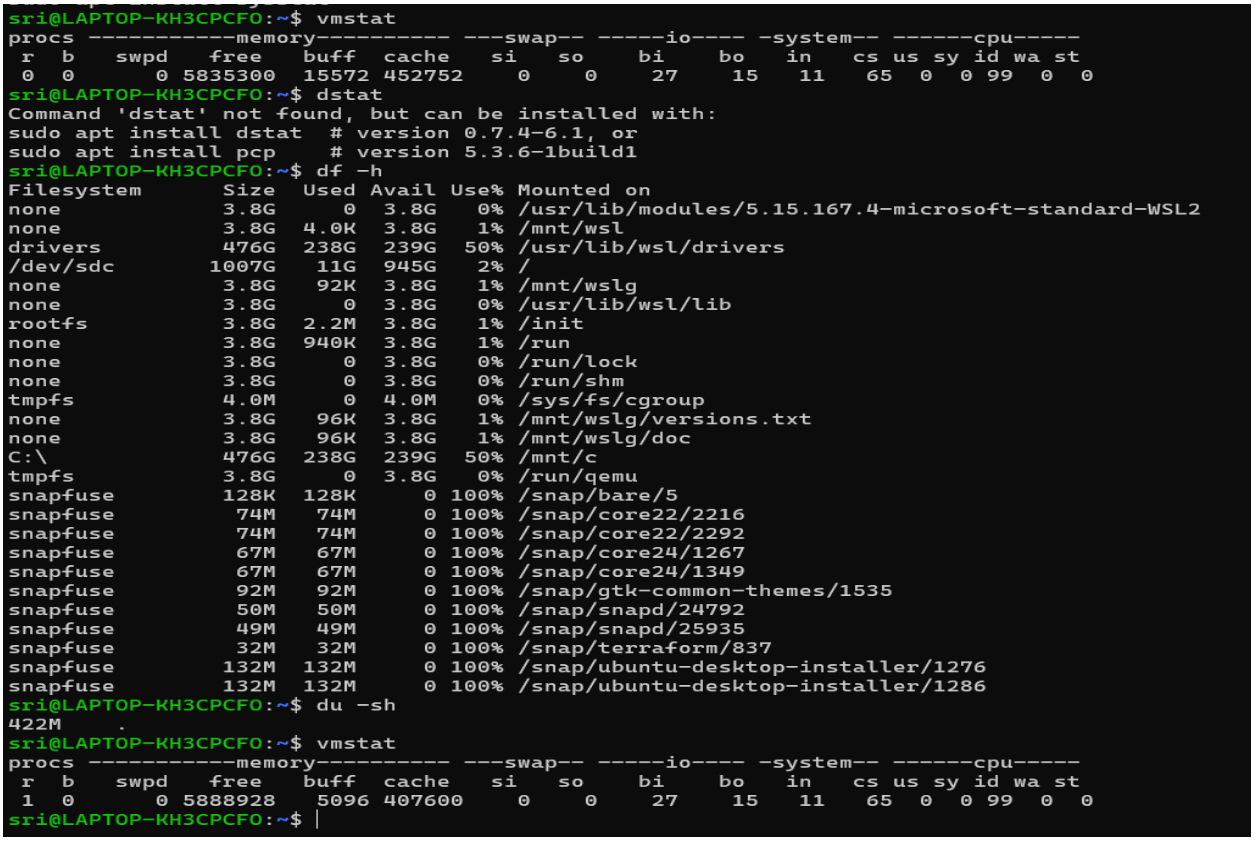


```
sri@LAPTOP-KH3CPCFO:~$ pgrep sshd
4350
sri@LAPTOP-KH3CPCFO:~$ ps -o pid
error: garbage option

Usage:
 ps [options]

 Try 'ps --help <simple|list|output|threads|misc|all>'
  or 'ps --help <s|l|o|t|m|a>'
 for additional help text.

For more details see ps(1).
sri@LAPTOP-KH3CPCFO:~$  free -h

Usage:
 free [options]

Options:
 -b, --bytes         show output in bytes
     --kilo          show output in kilobytes
     --mega          show output in megabytes
     --giga          show output in gigabytes
     --tera          show output in terabytes
     --peta          show output in petabytes
 -k, --kibi          show output in kibibytes
 -m, --mebi          show output in mebibytes
 -g, --gibi          show output in gibibytes
     --tebi          show output in tebibytes
     --pebi          show output in pebibytes
 -h, --human         show human-readable output
```



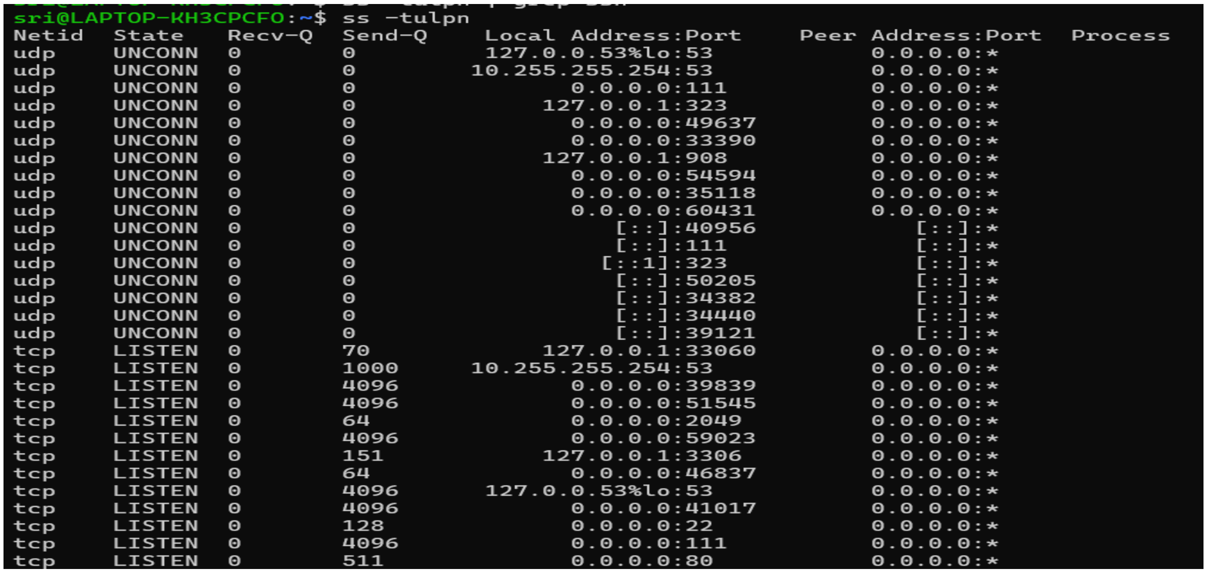
```
sri@LAPTOP-KH3CPCFO:~$  free -h

Usage:
 free [options]

Options:
 -b, --bytes         show output in bytes
     --kilo          show output in kilobytes
     --mega          show output in megabytes
     --giga          show output in gigabytes
     --tera          show output in terabytes
     --peta          show output in petabytes
 -k, --kibi          show output in kibibytes
 -m, --mebi          show output in mebibytes
 -g, --gibi          show output in gibibytes
     --tebi          show output in tebibytes
     --pebi          show output in pebibytes
 -h, --human         show human-readable output
     --si            use powers of 1000 not 1024
 -l, --lohi          show detailed low and high memory statistics
 -t, --total         show total for RAM + swap
 -s N, --seconds N   repeat printing every N seconds
```

- Disk /IO : (df –h , du –sh , vmstat)

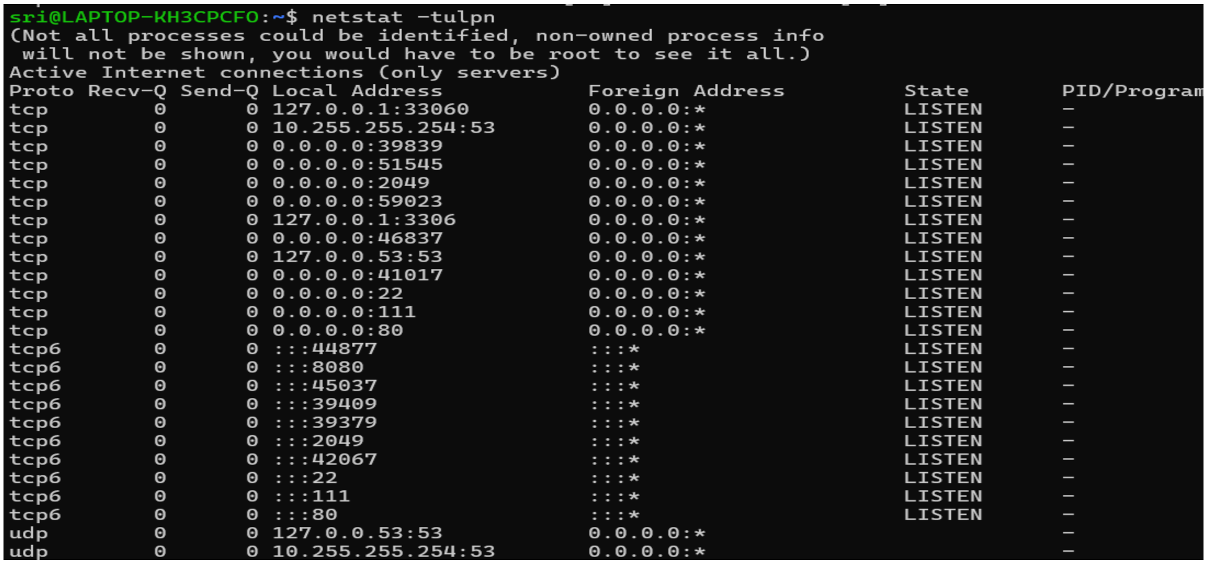


```
sri@LAPTOP-KH3CPCFO:~$ vmstat
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 0  0      0 5835300  15572 452752    0    0    27    15   11   65  0  0 99  0  0
sri@LAPTOP-KH3CPCFO:~$ dstat
Command 'dstat' not found, but can be installed with:
sudo apt install dstat  # version 0.7.4-6.1, or
sudo apt install pcp    # version 5.3.6-1build1
sri@LAPTOP-KH3CPCFO:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
none            3.8G     0  3.8G   0% /usr/lib/modules/5.15.167.4-microsoft-standard-WSL2
none            3.8G  4.0K  3.8G   1% /mnt/wsl
drivers         476G  238G  239G  50% /usr/lib/wsl/drivers
/dev/sdc       1007G   11G  945G   2% /
none            3.8G   92K  3.8G   1% /mnt/wslg
none            3.8G     0  3.8G   0% /usr/lib/wsl/lib
rootfs          3.8G  2.2M  3.8G   1% /init
none            3.8G  940K  3.8G   1% /run
none            3.8G     0  3.8G   0% /run/lock
none            3.8G     0  3.8G   0% /run/shm
tmpfs           4.0M     0  4.0M   0% /sys/fs/cgroup
none            3.8G   96K  3.8G   1% /mnt/wslg/versions.txt
none            3.8G   96K  3.8G   1% /mnt/wslg/doc
C:\             476G  238G  239G  50% /mnt/c
tmpfs           3.8G     0  3.8G   0% /run/qemu
snapfuse        128K  128K     0 100% /snap/bare/5
snapfuse         74M   74M     0 100% /snap/core22/2216
snapfuse         74M   74M     0 100% /snap/core22/2292
snapfuse         67M   67M     0 100% /snap/core24/1267
snapfuse         67M   67M     0 100% /snap/core24/1349
snapfuse         92M   92M     0 100% /snap/gtk-common-themes/1535
snapfuse         50M   50M     0 100% /snap/snapd/24792
snapfuse         49M   49M     0 100% /snap/snapd/25935
snapfuse         32M   32M     0 100% /snap/terraform/837
snapfuse        132M  132M     0 100% /snap/ubuntu-desktop-installer/1276
snapfuse        132M  132M     0 100% /snap/ubuntu-desktop-installer/1286
sri@LAPTOP-KH3CPCFO:~$ du -sh
422M    .
sri@LAPTOP-KH3CPCFO:~$ vmstat
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 1  0      0 5888928   5096 407600    0    0    27    15   11   65  0  0 99  0  0
sri@LAPTOP-KH3CPCFO:~$ |
```

- Network : (ss –tulpn , netstat –tulpn)

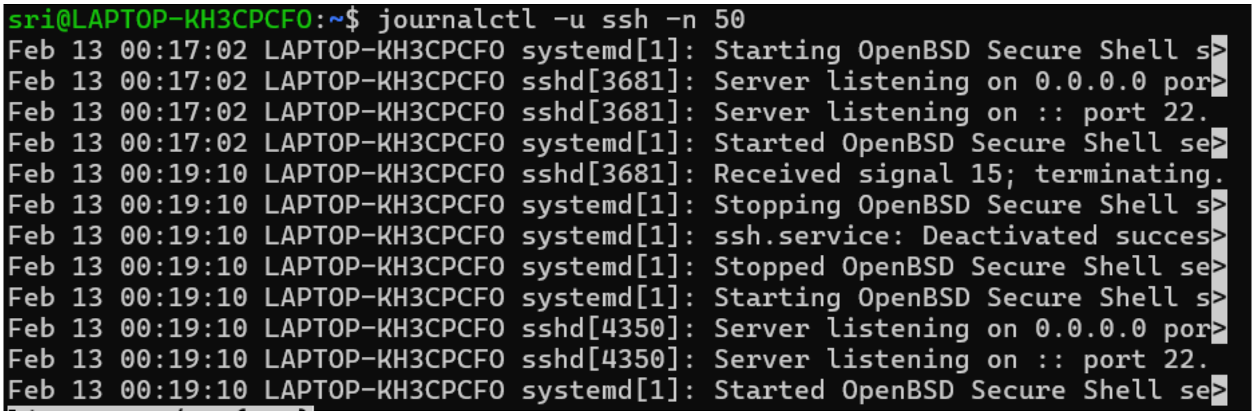


```
sri@LAPTOP-KH3CPCFO:~$ ss -tulpn
Netid  State    Recv-Q   Send-Q     Local Address:Port     Peer Address:Port  Process
udp    UNCONN   0        0          127.0.0.53%lo:53            0.0.0.0:*
udp    UNCONN   0        0        10.255.255.254:53             0.0.0.0:*
udp    UNCONN   0        0               0.0.0.0:111            0.0.0.0:*
udp    UNCONN   0        0             127.0.0.1:323            0.0.0.0:*
udp    UNCONN   0        0               0.0.0.0:49637          0.0.0.0:*
udp    UNCONN   0        0               0.0.0.0:33390          0.0.0.0:*
udp    UNCONN   0        0             127.0.0.1:908            0.0.0.0:*
udp    UNCONN   0        0               0.0.0.0:54594          0.0.0.0:*
udp    UNCONN   0        0               0.0.0.0:35118          0.0.0.0:*
udp    UNCONN   0        0               0.0.0.0:60431          0.0.0.0:*
udp    UNCONN   0        0                  [::]:40956             [::]:*
udp    UNCONN   0        0                  [::]:111               [::]:*
udp    UNCONN   0        0                 [::1]:323               [::]:*
udp    UNCONN   0        0                  [::]:50205             [::]:*
udp    UNCONN   0        0                  [::]:34382             [::]:*
udp    UNCONN   0        0                  [::]:34440             [::]:*
udp    UNCONN   0        0                  [::]:39121             [::]:*
tcp    LISTEN   0        70            127.0.0.1:33060          0.0.0.0:*
tcp    LISTEN   0        1000     10.255.255.254:53             0.0.0.0:*
tcp    LISTEN   0        4096            0.0.0.0:39839          0.0.0.0:*
tcp    LISTEN   0        4096            0.0.0.0:51545          0.0.0.0:*
tcp    LISTEN   0        64              0.0.0.0:2049           0.0.0.0:*
tcp    LISTEN   0        4096            0.0.0.0:59023          0.0.0.0:*
tcp    LISTEN   0        151           127.0.0.1:3306           0.0.0.0:*
tcp    LISTEN   0        64              0.0.0.0:46837          0.0.0.0:*
tcp    LISTEN   0        4096      127.0.0.53%lo:53             0.0.0.0:*
tcp    LISTEN   0        4096            0.0.0.0:41017          0.0.0.0:*
tcp    LISTEN   0        128             0.0.0.0:22             0.0.0.0:*
tcp    LISTEN   0        4096            0.0.0.0:111            0.0.0.0:*
tcp    LISTEN   0        511             0.0.0.0:80             0.0.0.0:*
```

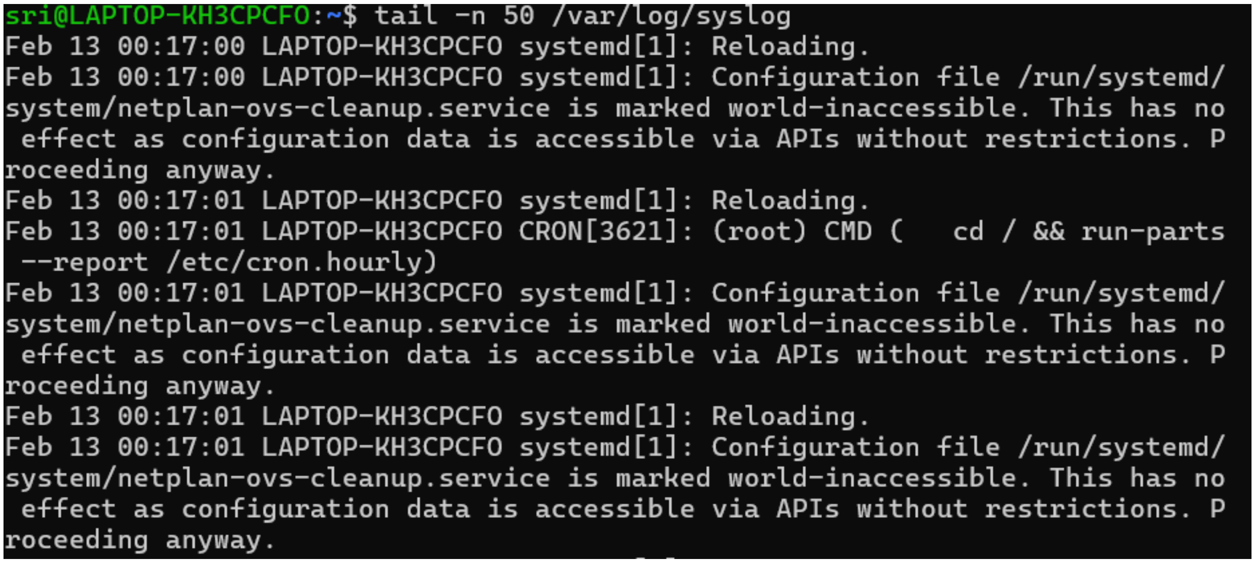


```
sri@LAPTOP-KH3CPCFO:~$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      -
tcp        0      0 10.255.255.254:53       0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:39839           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:51545           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:2049            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:59023           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:46837           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:41017           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::44877                :::*                    LISTEN      -
tcp6       0      0 :::8080                 :::*                    LISTEN      -
tcp6       0      0 :::45037                :::*                    LISTEN      -
tcp6       0      0 :::39409                :::*                    LISTEN      -
tcp6       0      0 :::39379                :::*                    LISTEN      -
tcp6       0      0 :::2049                 :::*                    LISTEN      -
tcp6       0      0 :::42067                :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::111                  :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 10.255.255.254:53       0.0.0.0:*                           -
```

- ➢ Logs: (journalctl –u ssh –n 50 , tail –n 50 /var/log/syslog)



```
sri@LAPTOP-KH3CPCFO:~$ journalctl -u ssh -n 50
Feb 13 00:17:02 LAPTOP-KH3CPCFO systemd[1]: Starting OpenBSD Secure Shell s>
Feb 13 00:17:02 LAPTOP-KH3CPCFO sshd[3681]: Server listening on 0.0.0.0 por>
Feb 13 00:17:02 LAPTOP-KH3CPCFO sshd[3681]: Server listening on :: port 22.
Feb 13 00:17:02 LAPTOP-KH3CPCFO systemd[1]: Started OpenBSD Secure Shell se>
Feb 13 00:19:10 LAPTOP-KH3CPCFO sshd[3681]: Received signal 15; terminating.
Feb 13 00:19:10 LAPTOP-KH3CPCFO systemd[1]: Stopping OpenBSD Secure Shell s>
Feb 13 00:19:10 LAPTOP-KH3CPCFO systemd[1]: ssh.service: Deactivated succes>
Feb 13 00:19:10 LAPTOP-KH3CPCFO systemd[1]: Stopped OpenBSD Secure Shell se>
Feb 13 00:19:10 LAPTOP-KH3CPCFO systemd[1]: Starting OpenBSD Secure Shell s>
Feb 13 00:19:10 LAPTOP-KH3CPCFO sshd[4350]: Server listening on 0.0.0.0 por>
Feb 13 00:19:10 LAPTOP-KH3CPCFO sshd[4350]: Server listening on :: port 22.
Feb 13 00:19:10 LAPTOP-KH3CPCFO systemd[1]: Started OpenBSD Secure Shell se>
```



```
sri@LAPTOP-KH3CPCFO:~$ tail -n 50 /var/log/syslog
Feb 13 00:17:00 LAPTOP-KH3CPCFO systemd[1]: Reloading.
Feb 13 00:17:00 LAPTOP-KH3CPCFO systemd[1]: Configuration file /run/systemd/
system/netplan-ovs-cleanup.service is marked world-inaccessible. This has no
 effect as configuration data is accessible via APIs without restrictions. P
roceeding anyway.
Feb 13 00:17:01 LAPTOP-KH3CPCFO systemd[1]: Reloading.
Feb 13 00:17:01 LAPTOP-KH3CPCFO CRON[3621]: (root) CMD (   cd / && run-parts
 --report /etc/cron.hourly)
Feb 13 00:17:01 LAPTOP-KH3CPCFO systemd[1]: Configuration file /run/systemd/
system/netplan-ovs-cleanup.service is marked world-inaccessible. This has no
 effect as configuration data is accessible via APIs without restrictions. P
roceeding anyway.
Feb 13 00:17:01 LAPTOP-KH3CPCFO systemd[1]: Reloading.
Feb 13 00:17:01 LAPTOP-KH3CPCFO systemd[1]: Configuration file /run/systemd/
system/netplan-ovs-cleanup.service is marked world-inaccessible. This has no
 effect as configuration data is accessible via APIs without restrictions. P
roceeding anyway.
```

Quick Findings :

- Service is running normally.
- No CPU or memory spike

- Disk Usage healthy
- No log errors

If this worsens :

1. Restart SSH service safely
2. Increase SSH login verbosity in /etc/ssh/sshd_config
3. Run strace –p <PID> to trace system calls.
4. Check failed login attempts (grep “Failed password”)