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

What's a runbook?

A runbook is a short, repeatable checklist you follow during an incident: the exact commands you run, what you observed, and the next actions if the issue persists. Keep it concise so you can reuse it under pressure.

Target service: ssh

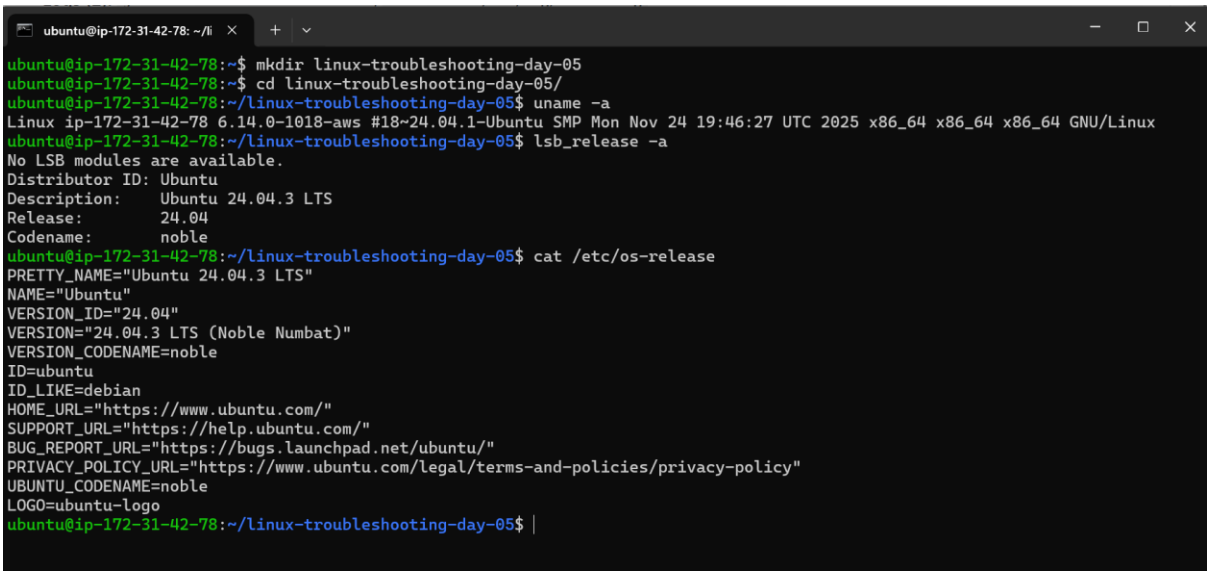
Why chosen: Critical system access service

STEP 1. Environment Basics Snapshot

uname -a → Displays complete system info(kernel version, architecture, hostname, OS type)

lsb_release -a → Shows Linux distribution details (Ubuntu version, release, codename).

cat /etc/os-release → Prints detailed OS metadata (OS name, version, LTS info, codename, URLs).



What I understood:

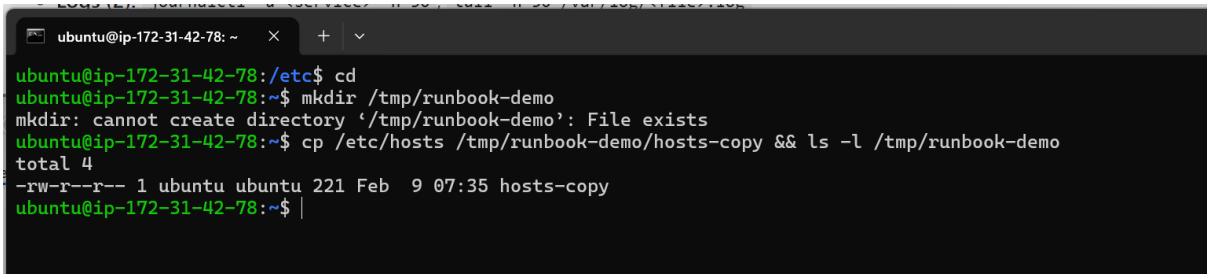
- OS: **Ubuntu 24.04.3 LTS**
- Codename: **Noble**
- Kernel: **6.14.0-1018-aws**
- Architecture: **x86_64**
- Environment: **AWS EC2 (Ubuntu user)**

Step 2. Filesystem Sanity Check

Ensure disk is writeable and behave normally.

mkdir /tmp/runbook-demo → Creates a named **runbook-demo** under **/tmp/**

cp /etc/hosts /tmp/runbook-demo/hosts-copy && ls -l /tmp/runbook-demo → Copies the **/etc/hosts** file into **/tmp/runbook-demo** as **hosts-copy**. If the copy succeeds, it lists the directory contents to confirm the file exists



What I understood:

- **Permissions:** -rw-r--r--
  - rw- → Owner can read & write
  - r-- → Group can read only
  - r-- → Others can read only
- **Ownership:** ubuntu
  - user who owns the file: ubuntu
  - Group who owns the file: ubuntu
- **No errors found**

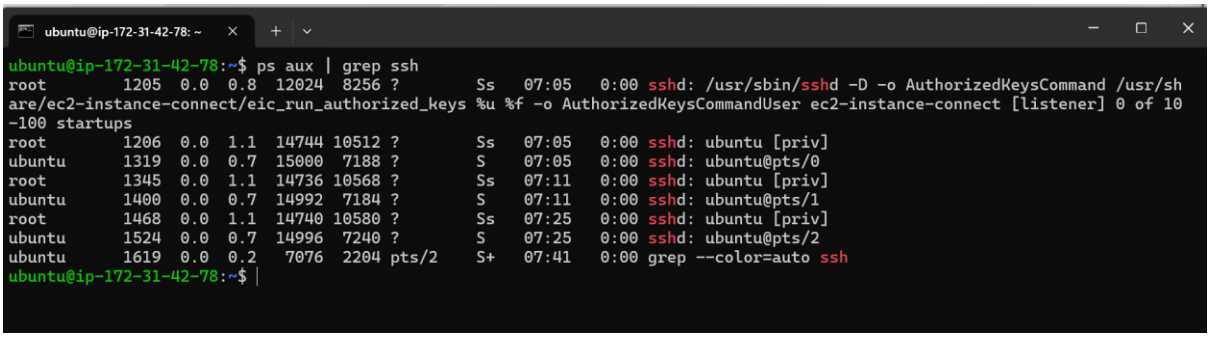
STEP 3. Identify the Service Process

ps aux | grep ssh →

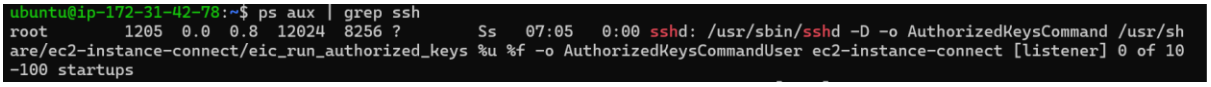
ps aux : list all running process

| : sends output to another command

grep ssh : filters line contain ssh



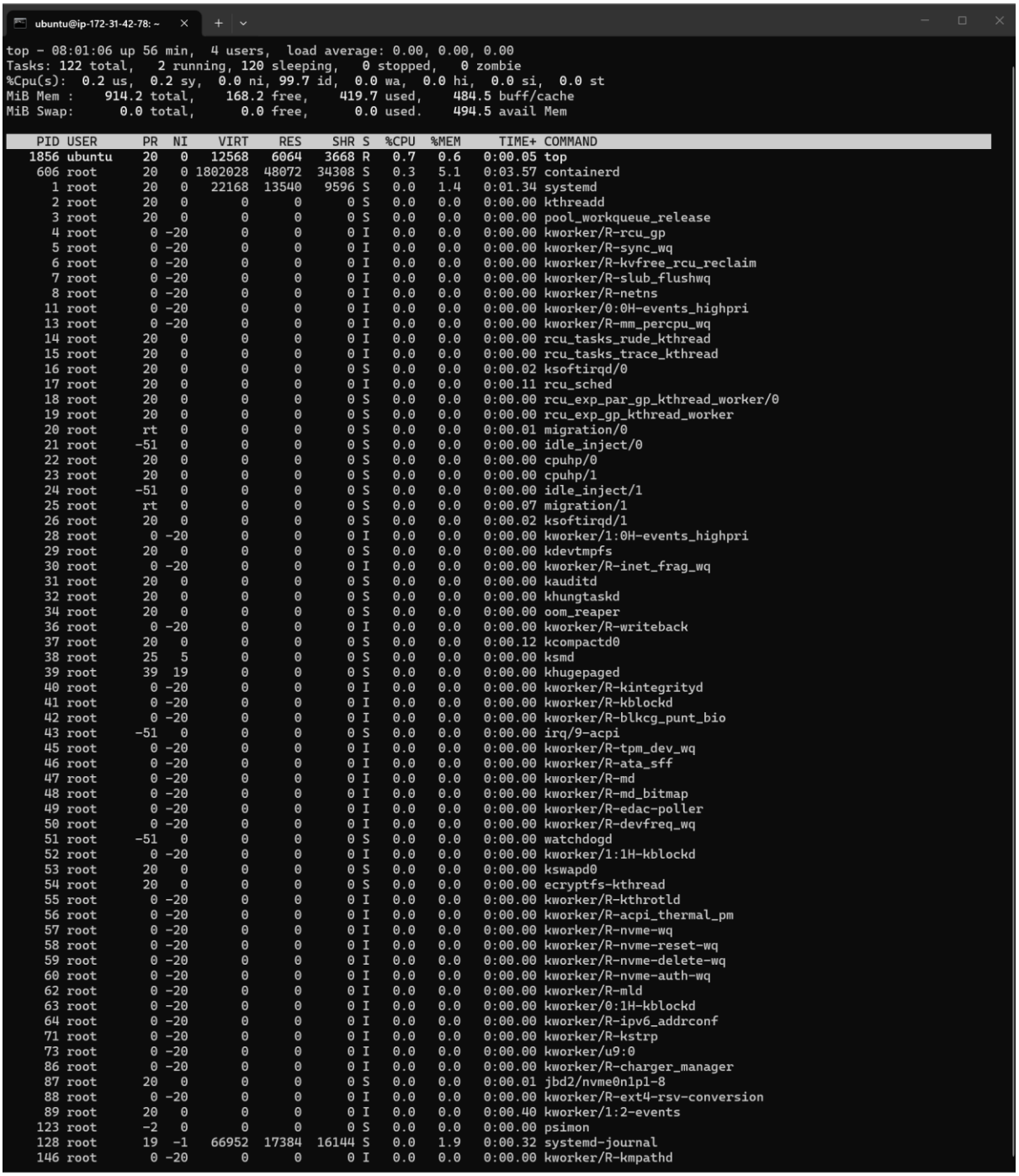
What I understood:



The output confirms the SSH daemon is running, shows multiple active SSH login sessions for user ubuntu, but the **MAIN ssh service** is running with user **root** and having **PID 1205** and displays the temporary privileged processes handling authentication.

STEP 4. CPU & Memory Snapshot

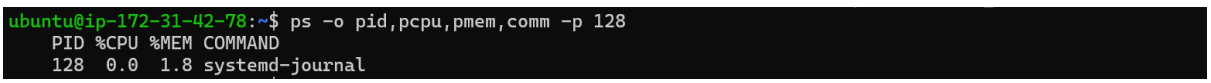
Top → shows live process



ps -o pid,pcpu,pmem,comm -p <PID> →

What it shows:

- Ps → Process state
- -o → shows only the columns ahead of this -o
- pid → Process ID
- pcpu → CPU usage %
- pmem → Memory usage %
- comm → Command name
- -p <PID> → Show information **only for this specific PID (or PIDs)**.



What I understood:

- System load: 0.00, 0.00, 0.00 → system idle, no CPU pressure
- CPU: ~99.7% idle → no CPU bottleneck
- Processes: 122 total (2 running, 120 sleeping, 0 zombie) → healthy state
- Memory: ~419 MiB used, swap 0 → normal usage; cache is expected
- Top processes: top (~0.7% CPU), containerd (~5% MEM) → no abnormal activity

Conclusion: System is healthy with no resource contention or runaway processes.

STEP 5. Disk & IO Check

Df -h → Shows total, used, and available disk space in human readable format

```
ubuntu@ip-172-31-42-78: ~
ubuntu@ip-172-31-42-78:~$ df -h
Filesystem       Size  Used Avail Use% Mounted on
/dev/root         19G  2.5G   16G  14% /
tmpfs            458M     0  458M   0% /dev/shm
tmpfs            183M  928K  182M   1% /run
tmpfs            5.0M     0  5.0M   0% /run/lock
efivarfs         128K  3.8K  120K   4% /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
ubuntu@ip-172-31-42-78:~$
```

du -sh /var/log → Check directory size

- -s = summary only
- -h = human-readable

```
ubuntu@ip-172-31-42-78:~$ sudo du -sh /var/log
60M     /var/log
ubuntu@ip-172-31-42-78:~$
```

iostat → shows disk I/O performance

```
ubuntu@ip-172-31-42-78:~$ iostat
Linux 6.14.0-1018-aws (ip-172-31-42-78)         02/09/26        _x86_64_        (2 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0.14    0.01    0.10    0.03    0.03   99.71

Device             tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd
loop0             0.01         0.08         0.00         0.00        345          0          0
loop1             0.03         0.94         0.00         0.00       4271          0          0
loop2             0.01         0.24         0.00         0.00       1082          0          0
loop3             0.01         0.24         0.00         0.00       1097          0          0
loop4             0.02         0.38         0.00         0.00       1736          0          0
loop5             0.01         0.08         0.00         0.00        346          0          0
loop6             0.00         0.00         0.00         0.00         14          0          0
nvme0n1           2.38        95.95         6.59         0.00     437579      30062          0

ubuntu@ip-172-31-42-78:~$
```

vmstat → shows memory, CPU and I/O pressure

```
ubuntu@ip-172-31-42-78:~$ vmstat
procs -----------memory---------- ---swap-- -----io---- -system-- -------cpu-------
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st gu
 2  0      0 169408  22176 475480    0    0    95     6  101    0  0  0 100  0  0  0
ubuntu@ip-172-31-42-78:~$
```

dstat → shows combined real time system view CPU, DISK, net, memory

```
ubuntu@ip-172-31-42-78:~$ dstat
You did not select any stats, using -cdngy by default.
----total-usage---- -dsk/total- -net/total- ---paging-- ---system--
usr sys idl wai stl| read  writ| recv  send|  in   out | int   csw
  0   0  99   0   0|   0     0 |2448B 3416B|   0     0 | 250   220
  0   0 100   0   0|   0     0 |1916B 2450B|   0     0 | 222   197
  0   0 100   0   0|   0     0 |  46B  298B|   0     0 | 110   117
  0   0  99   0   0|   0     0 |  46B  298B|   0     0 | 122   137
  0   0 100   0   0|   0     0 | 122B  388B|   0     0 | 111   116
  0   0  99   0   0|   0    92k|  52B  298B|   0     0 | 142   153
  0   0 100   0   0|   0     0 |  46B  306B|   0     0 | 123   141
  0   0  99   0   0|   0   112k|  46B  298B|   0     0 | 127   135
  1   0 100   0   0|   0     0 |  46B  306B|   0     0 | 108   120
  0   0 100   0   0|   0     0 |  46B  306B|   0     0 | 100   112
  0   0 100   0   0|   0     0 |  46B  298B|   0     0 | 116   135
  0   0  99   0   0|   0     0 |  46B  298B|   0     0 | 104   125
  0   0 100   0   0|   0     0 |  46B  298B|   0     0 | 101   116
  0   0  99   0   0|   0     0 |  46B  298B|   0     0 | 121   125
  0   0 100   0   0|   0     0 |  46B  298B|   0     0 |  94   104
  0   1 100   0   0|   0     0 |  46B  298B|   0     0 | 114   130
  0   0 100   0   0|   0     0 | 122B  396B|   0     0 | 122   134
  0   0 100   0   0|   0     0 |  46B  298B|   0     0 | 111   121
  0   0 100   0   0|   0     0 |  46B  298B|   0     0 |  82   103
  0   0  99   0   0|   0     0 |  46B  298B|   0     0 | 100   113
  0   0 100   0   0|   0     0 | 122B  388B|   0     0 | 125   127
  0   0 100   0   0|   0     0 |  46B  298B|   0     0 | 123   133
  0   1 100   0   0|   0     0 |  52B  298B|   0     0 | 103   107
  0   0  99   0   0|   0     0 |  46B  306B|   0     0 | 100   116
  0   0 100   0   0|   0     0 |  46B  298B|   0     0 |  96    98
  0   0 100   0   0|   0     0 |  46B  298B|   0     0 | 131   148
  0   0 100   0   0|   0     0 | 122B  388B|   0     0 | 146   149
  0   0 100   0   0|   0     0 |  46B  298B|   0     0 | 117   117
  0   0  99   0   0|   0     0 | 122B  388B|   0     0 | 117   117
  0   0  99   0   0|   0     0 |  46B  298B|   0     0 | 115   120
  0   0 100   0   0|   0     0 |  46B  298B|   0     0 | 104   119
  0   0 100   0   0|   0     0 |  74B  340B|   0     0 | 106   119
  0   0  99   0   0|   0     0 |  46B  298B|   0     0 | 105   109
```

What I understood:

- **Disk space:** Root filesystem is only **14% used**; all partitions have ample free space. No disk capacity risk.
- **Logs:** /var/log is **~60 MB**, which is small and well within normal limits.
- **Disk I/O:** iostat shows **very low I/O activity** and **negligible iowait**; storage is not a bottleneck.
- **Memory:** vmstat shows **no swap usage**, sufficient free memory, and healthy buffer/cache usage.
- **CPU:** System is mostly **idle (~100% idle)** with no CPU or I/O pressure.

The system is healthy and stable with no CPU, memory, disk, or I/O contention observed. No immediate remediation required.

STEP 6. Network Sanity

ss -tulpn | grep ssh →checks whether the **SSH service is listening on a network port**.

- **ss** → shows network connections and listening ports
- **-t** → TCP sockets
- **-u** → UDP sockets
- **-l** → Listening ports only
- **-p** → Show process using the port
- **-n** → Show numeric ports

- **| grep ssh** → Filters output to show only **SSH-related entries**

curl -I localhost → checks whether a **web service is responding on the local machine**.

ping localhost → checks **basic network connectivity to the local machine**.

```
ubuntu@ip-172-31-42-78:~$ ss -tulpn | grep ssh
ubuntu@ip-172-31-42-78:~$ sudo ss -tulpn | grep ssh
tcp   LISTEN 0      4096             0.0.0.0:22        0.0.0.0:*    users:(("sshd",pid=1205,fd=3),("systemd",pid=1,fd=196))

tcp   LISTEN 0      4096                [::]:22           [::]:*    users:(("sshd",pid=1205,fd=4),("systemd",pid=1,fd=197))

ubuntu@ip-172-31-42-78:~$ curl -I localhost
HTTP/1.1 200 OK
Server: nginx/1.24.0 (Ubuntu)
Date: Mon, 09 Feb 2026 08:38:05 GMT
Content-Type: text/html
Content-Length: 615
Last-Modified: Sun, 08 Feb 2026 13:14:40 GMT
Connection: keep-alive
ETag: "69888c40-267"
Accept-Ranges: bytes

ubuntu@ip-172-31-42-78:~$ ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.034 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.034 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.035 ms
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.038 ms
64 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.033 ms
```

What I understood:

- SSH service: sshd is running and listening on port 22 for both IPv4 (0.0.0.0:22) and IPv6 ([::]:22), managed by systemd. No port or binding issues.
- HTTP service: curl -I localhost returns HTTP/1.1 200 OK, confirming a local nginx (v1.24.0) web server is running and responding on port 80.
- Network stack: ping localhost succeeds with low latency, confirming the loopback interface and local networking are healthy.

Core services (SSH and HTTP) are operational, ports are listening correctly, and local network connectivity is functioning as expected. No service or network issues detected.

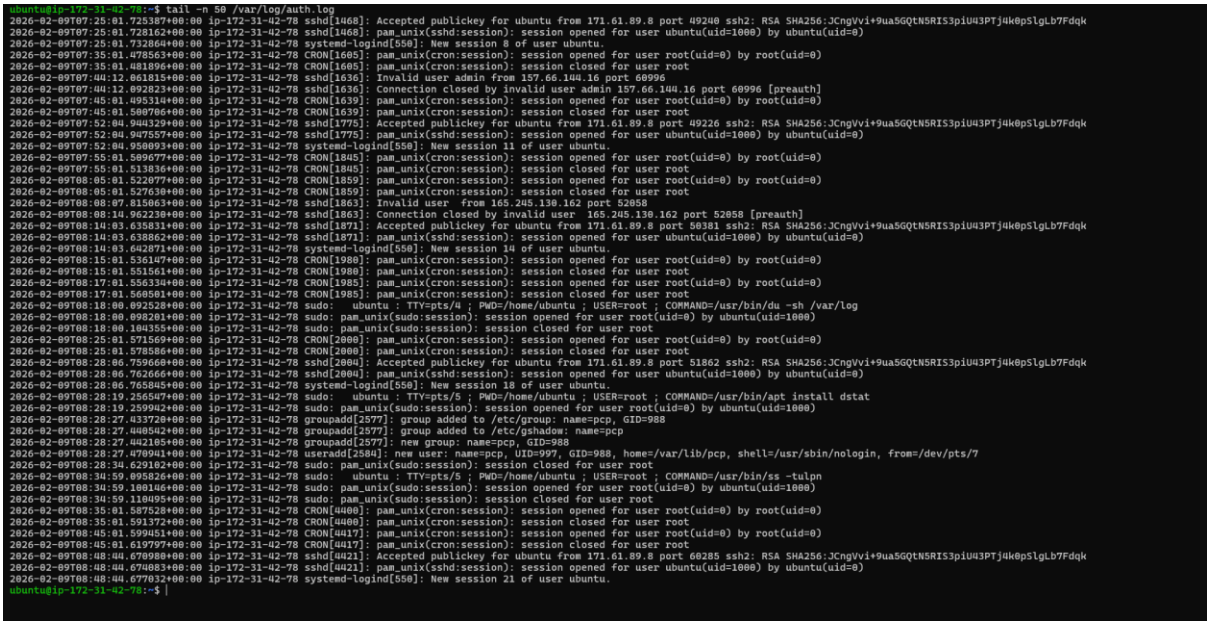
STEP 7. Log Investigation

journalctl -u ssh -n 50 → shows the last 50 log entries for the SSH service.

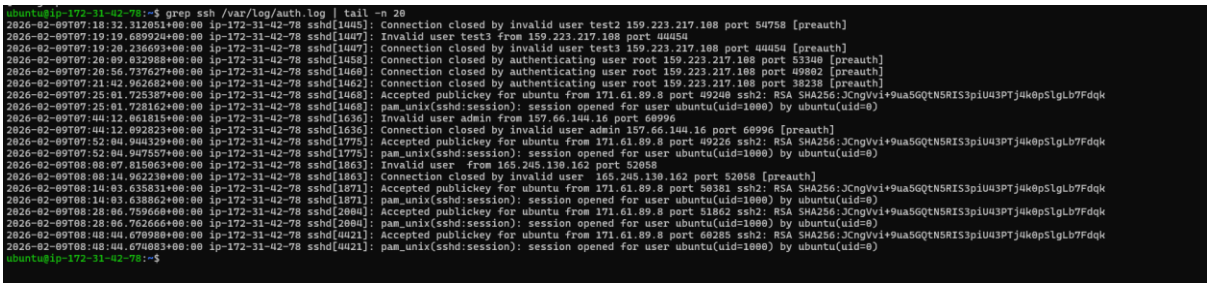
Journalctl → is a tool to query systemd logs

```
ubuntu@ip-172-31-42-78:~$ journalctl -u ssh -n 45
Feb 08 19:15:43 ip-172-31-42-78 sshd[1822]: Connection closed by authenticating user root 188.166.13.91 port 56396 [preauth]
Feb 08 19:16:54 ip-172-31-42-78 sshd[1824]: Connection closed by authenticating user root 188.166.13.91 port 54958 [preauth]
Feb 08 19:18:00 ip-172-31-42-78 sshd[1829]: Accepted publickey for ubuntu from 171.61.89.8 port 62735 ssh2: RSA SHA256:JCngVvi+9ua5GQtN5RIS3piU43PTj4k0pSlgLb7Fdqk
Feb 08 19:18:00 ip-172-31-42-78 sshd[1829]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
Feb 08 19:18:05 ip-172-31-42-78 sshd[1939]: Connection closed by 188.166.13.91 port 52316
Feb 08 19:18:06 ip-172-31-42-78 sshd[1940]: Connection closed by authenticating user root 188.166.13.91 port 52324 [preauth]
Feb 08 19:19:11 ip-172-31-42-78 sshd[1946]: Connection closed by 188.166.13.91 port 33724
Feb 08 19:24:08 ip-172-31-42-78 sshd[1956]: Accepted publickey for ubuntu from 171.61.89.8 port 63326 ssh2: RSA SHA256:JCngVvi+9ua5GQtN5RIS3piU43PTj4k0pSlgLb7Fdqk
Feb 08 19:24:08 ip-172-31-42-78 sshd[1956]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
Feb 08 21:03:06 ip-172-31-42-78 sshd[1126]: Received signal 15; terminating.
Feb 08 21:03:06 ip-172-31-42-78 systemd[1]: Stopping ssh.service - OpenBSD Secure Shell server...
Feb 08 21:03:06 ip-172-31-42-78 systemd[1]: ssh.service: Deactivated successfully.
Feb 08 21:03:06 ip-172-31-42-78 systemd[1]: Stopped ssh.service - OpenBSD Secure Shell server.
-- Boot f60c4e43a9c9477086598be72124cafc --
Feb 09 07:05:16 ip-172-31-42-78 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Feb 09 07:05:16 ip-172-31-42-78 sshd[1205]: Server listening on 0.0.0.0 port 22.
Feb 09 07:05:16 ip-172-31-42-78 sshd[1205]: Server listening on :: port 22.
Feb 09 07:05:16 ip-172-31-42-78 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Feb 09 07:05:18 ip-172-31-42-78 sshd[1206]: Accepted publickey for ubuntu from 171.61.89.8 port 62109 ssh2: RSA SHA256:JCngVvi+9ua5GQtN5RIS3piU43PTj4k0pSlgLb7Fdqk
Feb 09 07:05:18 ip-172-31-42-78 sshd[1206]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
Feb 09 07:11:31 ip-172-31-42-78 sshd[1345]: Accepted publickey for ubuntu from 171.61.89.8 port 54020 ssh2: RSA SHA256:JCngVvi+9ua5GQtN5RIS3piU43PTj4k0pSlgLb7Fdqk
Feb 09 07:11:31 ip-172-31-42-78 sshd[1345]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
Feb 09 07:16:33 ip-172-31-42-78 sshd[1423]: Connection closed by 159.223.217.108 port 35916
Feb 09 07:17:42 ip-172-31-42-78 sshd[1443]: Invalid user test1 from 159.223.217.108 port 39126
Feb 09 07:17:42 ip-172-31-42-78 sshd[1443]: Connection closed by invalid user test1 159.223.217.108 port 39126 [preauth]
Feb 09 07:18:31 ip-172-31-42-78 sshd[1445]: Invalid user test2 from 159.223.217.108 port 54758
Feb 09 07:18:32 ip-172-31-42-78 sshd[1445]: Connection closed by invalid user test2 159.223.217.108 port 54758 [preauth]
Feb 09 07:19:19 ip-172-31-42-78 sshd[1447]: Invalid user test3 from 159.223.217.108 port 44454
Feb 09 07:19:20 ip-172-31-42-78 sshd[1447]: Connection closed by invalid user test3 159.223.217.108 port 44454 [preauth]
Feb 09 07:20:09 ip-172-31-42-78 sshd[1458]: Connection closed by authenticating user root 159.223.217.108 port 53340 [preauth]
Feb 09 07:20:56 ip-172-31-42-78 sshd[1460]: Connection closed by authenticating user root 159.223.217.108 port 49802 [preauth]
Feb 09 07:21:42 ip-172-31-42-78 sshd[1462]: Connection closed by authenticating user root 159.223.217.108 port 38238 [preauth]
Feb 09 07:25:01 ip-172-31-42-78 sshd[1468]: Accepted publickey for ubuntu from 171.61.89.8 port 49240 ssh2: RSA SHA256:JCngVvi+9ua5GQtN5RIS3piU43PTj4k0pSlgLb7Fdqk
Feb 09 07:25:01 ip-172-31-42-78 sshd[1468]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
Feb 09 07:44:12 ip-172-31-42-78 sshd[1636]: Invalid user admin from 157.66.144.16 port 60996
Feb 09 07:44:12 ip-172-31-42-78 sshd[1636]: Connection closed by invalid user admin 157.66.144.16 port 60996 [preauth]
Feb 09 07:52:04 ip-172-31-42-78 sshd[1775]: Accepted publickey for ubuntu from 171.61.89.8 port 49226 ssh2: RSA SHA256:JCngVvi+9ua5GQtN5RIS3piU43PTj4k0pSlgLb7Fdqk
Feb 09 07:52:04 ip-172-31-42-78 sshd[1775]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
Feb 09 08:08:07 ip-172-31-42-78 sshd[1863]: Invalid user  from 165.245.130.162 port 52058
Feb 09 08:08:14 ip-172-31-42-78 sshd[1863]: Connection closed by invalid user  165.245.130.162 port 52058 [preauth]
Feb 09 08:14:03 ip-172-31-42-78 sshd[1871]: Accepted publickey for ubuntu from 171.61.89.8 port 50381 ssh2: RSA SHA256:JCngVvi+9ua5GQtN5RIS3piU43PTj4k0pSlgLb7Fdqk
Feb 09 08:14:03 ip-172-31-42-78 sshd[1871]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
Feb 09 08:28:06 ip-172-31-42-78 sshd[2004]: Accepted publickey for ubuntu from 171.61.89.8 port 51862 ssh2: RSA SHA256:JCngVvi+9ua5GQtN5RIS3piU43PTj4k0pSlgLb7Fdqk
Feb 09 08:28:06 ip-172-31-42-78 sshd[2004]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
Feb 09 08:48:44 ip-172-31-42-78 sshd[4421]: Accepted publickey for ubuntu from 171.61.89.8 port 60285 ssh2: RSA SHA256:JCngVvi+9ua5GQtN5RIS3piU43PTj4k0pSlgLb7Fdqk
Feb 09 08:48:44 ip-172-31-42-78 sshd[4421]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
lines 1-46
```

tail -n 50 /var/log/auth.log → provides a quick snapshot of the latest authentication activity, essential for SSH and access troubleshooting.



grep ssh /var/log/auth.log | tail -n 20 → shows focused view of the latest SSH authentication activity.



What I understood:

SSH service is functioning correctly with secure, key-based access for the ubuntu user.
There are routine background login attempts from external Ips.

If this worsens, what will be our next plan?

- Restart ssh using systemctl restart ssh and monitor logs.
- Enable debug logging temporarily.
- Capture strace on the PID to analyze blocking calls.
- When troubleshooting, always think in this order:
  Context → Resources → Reachability → Evidence → Next Actions