

## 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

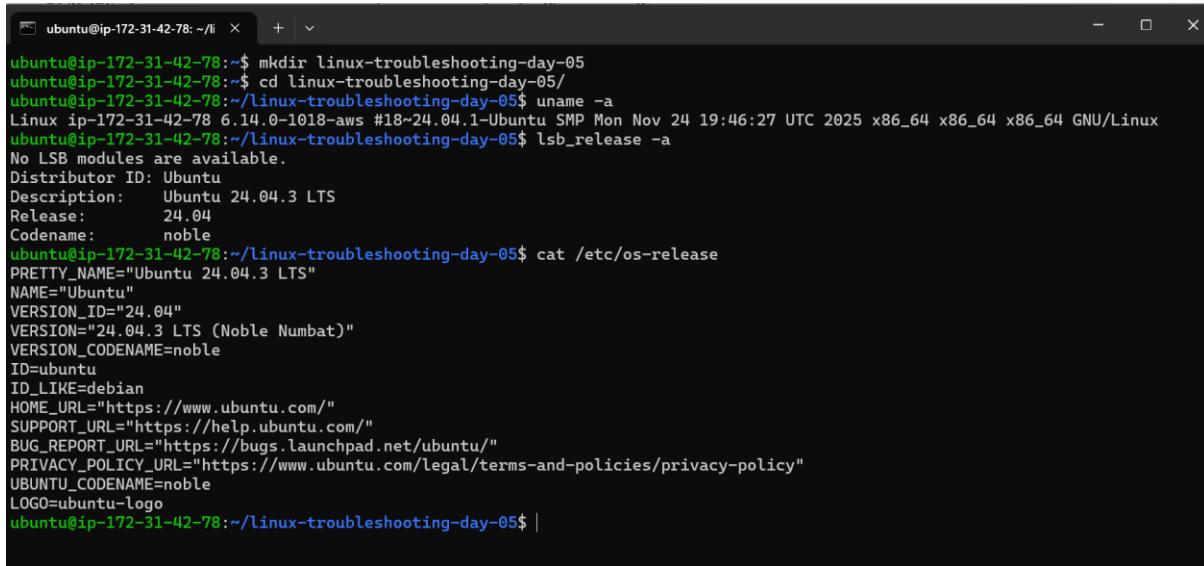
**Why chosen:** Critical system access service

### 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).



The terminal window shows the following sequence of commands and their outputs:

```
ubuntu@ip-172-31-42-78: ~$ mkdir linux-troubleshooting-day-05
ubuntu@ip-172-31-42-78: ~$ cd linux-troubleshooting-day-05/
ubuntu@ip-172-31-42-78: ~/linux-troubleshooting-day-05$ uname -a
Linux ip-172-31-42-78 6.14.0-1018-aws #18~24.04.1-Ubuntu SMP Mon Nov 24 19:46:27 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
ubuntu@ip-172-31-42-78: ~/linux-troubleshooting-day-05$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 24.04.3 LTS
Release:        24.04
Codename:       noble
ubuntu@ip-172-31-42-78: ~/linux-troubleshooting-day-05$ cat /etc/os-release
PRETTY_NAME="Ubuntu 24.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.3 LTS (Noble Numbat)"
VERSION_CODENAME=noble
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-policies/privacy-policy"
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
ubuntu@ip-172-31-42-78: ~/linux-troubleshooting-day-05$ |
```

### 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

```

ubuntu@ip-172-31-42-78:~ x + v
ubuntu@ip-172-31-42-78:~/etc$ cd
ubuntu@ip-172-31-42-78:~/etc$ mkdir /tmp/runbook-demo
mkdir: cannot create directory '/tmp/runbook-demo': File exists
ubuntu@ip-172-31-42-78:~/etc$ cp /etc/hosts /tmp/runbook-demo/hosts-copy && ls -l /tmp/runbook-demo
total 4
-rw-r--r-- 1 ubuntu ubuntu 221 Feb 9 07:35 hosts-copy
ubuntu@ip-172-31-42-78:~/etc$ |

```

## 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

```

ubuntu@ip-172-31-42-78:~ x + v
ubuntu@ip-172-31-42-78:~$ ps aux | grep ssh
root      1205  0.0  0.8 12024 8256 ?          Ss  07:05   0:00 sshd: /usr/sbin/sshd -D -o AuthorizedKeysCommand /usr/sh
are/ec2-instance-connect/eic_runAuthorizedKeys %u %f -o AuthorizedKeysCommandUser ec2-instance-connect [listener] 0 of 10
-100 startups
root      1206  0.0  1.1 14744 10512 ?          Ss  07:05   0:00 sshd: ubuntu [priv]
ubuntu    1319  0.0  0.7 15000 7188 ?          S   07:05   0:00 sshd: ubuntu@pts/0
root      1345  0.0  1.1 14736 10568 ?          Ss  07:11   0:00 sshd: ubuntu [priv]
ubuntu    1400  0.0  0.7 14992 7184 ?          S   07:11   0:00 sshd: ubuntu@pts/1
root      1468  0.0  1.1 14740 10580 ?          Ss  07:25   0:00 sshd: ubuntu [priv]
ubuntu    1524  0.0  0.7 14996 7240 ?          S   07:25   0:00 sshd: ubuntu@pts/2
ubuntu    1619  0.0  0.2  7076  2204 pts/2      S+  07:41   0:00 grep --color=auto ssh
ubuntu@ip-172-31-42-78:~$ |

```

## What I understood:

```

ubuntu@ip-172-31-42-78:~$ ps aux | grep ssh
root      1205  0.0  0.8 12024 8256 ?          Ss  07:05   0:00 sshd: /usr/sbin/sshd -D -o AuthorizedKeysCommand /usr/sh
are/ec2-instance-connect/eic_runAuthorizedKeys %u %f -o AuthorizedKeysCommandUser ec2-instance-connect [listener] 0 of 10
-100 startups

```

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

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1856	ubuntu	20	0	12568	6064	3668	R	0.7	0.6	0:00.05	top
606	root	20	0	1802028	48072	34308	S	0.3	5.1	0:03.57	containererd
1	root	20	0	22168	13540	9596	S	0.0	1.4	0:01.34	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kthreadd
3	root	20	0	0	0	0	S	0.0	0.0	0:00.00	pool_workqueue_release
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-rcu_gp
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-sync_wq
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-kvfree_rcu_reclaim
7	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-slab_flushwq
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-netsns
11	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/0:0H-events_highpri
13	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-mm_percpu_wq
14	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_rude_kthread
15	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tasks_trace_kthread
16	root	20	0	0	0	0	S	0.0	0.0	0:00.02	ksoftirqd/0
17	root	20	0	0	0	0	I	0.0	0.0	0:00.11	rcu_sched
18	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcu_exp_par_gp_kthread_worker/0
19	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcu_exp_gp_kthread_worker
20	root	rt	0	0	0	0	S	0.0	0.0	0:00.01	migration/0
21	root	-51	0	0	0	0	S	0.0	0.0	0:00.00	idle_inject/0
22	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuhp/0
23	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuhp/1
24	root	-51	0	0	0	0	S	0.0	0.0	0:00.00	idle_inject/1
25	root	rt	0	0	0	0	S	0.0	0.0	0:00.07	migration/1
26	root	20	0	0	0	0	S	0.0	0.0	0:00.02	ksoftirqd/1
28	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/1:0H-events_highpri
29	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kdevtmpfs
30	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-inet_frag_wq
31	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kauditd
32	root	20	0	0	0	0	S	0.0	0.0	0:00.00	khungtaskd
34	root	20	0	0	0	0	S	0.0	0.0	0:00.00	oom_reaper
36	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-writeback
37	root	20	0	0	0	0	S	0.0	0.0	0:00.12	kcompactd0
38	root	25	5	0	0	0	S	0.0	0.0	0:00.00	ksmd
39	root	39	19	0	0	0	S	0.0	0.0	0:00.00	khugepaged
40	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-kintegrityd
41	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-kblockd
42	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-blkcg_punt_bio
43	root	-51	0	0	0	0	S	0.0	0.0	0:00.00	irq/9-acpi
45	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-tpm_dev_wq
46	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-ata_sff
47	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-md
48	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-md_bitmap
49	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-edac-poller
50	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-devfreq_wq
51	root	-51	0	0	0	0	S	0.0	0.0	0:00.00	watchdog
52	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/1:1H-kblockd
53	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kswapd0
54	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cryptptfs-kthread
55	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-kthrotld
56	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-acpi_thermal_pm
57	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-nvme-wq
58	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-nvme-reset-wq
59	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-nvme-delete-wq
60	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-nvme-auth-wq
62	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-mld
63	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/0:1H-kblockd
64	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-ipv6_addrconf
71	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-kstrip
73	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/u9:0
86	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-charger_manager
87	root	20	0	0	0	0	S	0.0	0.0	0:00.01	jbd2/nvme0n1p1-8
88	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-ext4-rsv-conversion
89	root	20	0	0	0	0	I	0.0	0.0	0:00.40	kworker/1:2-events
123	root	-2	0	0	0	0	S	0.0	0.0	0:00.00	psimon
128	root	19	-1	66952	17384	16144	S	0.0	1.9	0:00.32	systemd-journal
146	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/R-kmpathd

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)**.

```
ubuntu@ip-172-31-42-78:~$ ps -o pid,pcpu,pmem,comm -p 128
PID %CPU %MEM COMMAND
128 0.0 1.8 systemd-journal
```

### 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:~$ 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	0	1	100	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	0	1	100	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 19:16:00 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 19:18:06 ip-172-31-42-78 sshd[1900]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
Feb 08 19:18:06 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 19:18:11 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 f66c4e43a9477086598be72124cafc --
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 07:05:16 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 07:05:16 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 07:18:31 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 07:19:19 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 49246 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 52858
Feb 09 08:08:14 ip-172-31-42-78 sshd[1863]: Connection closed by invalid user 165.245.130.162 port 52858 [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[2000]: 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[2000]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
Feb 09 08:48:04 ip-172-31-42-78 sshd[4021]: Accepted publickey for ubuntu from 171.61.89.8 port 60285 ssh2: RSA SHA256:JcNgVvi+9ua5GQtN5RIS3piU43PTj4k0pSlgLb7Fdqk
Feb 09 08:48:04 ip-172-31-42-78 sshd[4021]: 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**