

Linux Troubleshooting Runbook – Day 05


CPU, Memory, Disk, Network & Logs Health Analysis

Target Service: **SSH (sshd)**

This runbook documents a structured troubleshooting drill performed on an Ubuntu Linux system. The goal was to capture real system metrics, analyze logs, and validate service health using standard Linux commands. Screenshots of each step are included as evidence.

1. Environment Validation

- Kernel and OS version verified.
- Ubuntu 24.04.3 LTS detected.
- System architecture x86_64 confirmed.

A terminal window titled 'ubuntu@ip-172-31-0-222: ~' with standard window controls. The terminal shows the execution of 'uname -a' and 'cat /etc/os-release'. The 'uname -a' output includes the kernel version 6.14.0-1018-aws and architecture x86_64. The 'cat /etc/os-release' output confirms the system is Ubuntu 24.04.3 LTS (Noble Numbat) with various system URLs and identifiers.

```
ubuntu@ip-172-31-0-222:~$ uname -a
Linux ip-172-31-0-222 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-172-31-0-222:~$ 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-172-31-0-222:~$
```

2. Filesystem Sanity Check

- Temporary directory created successfully.
- File copied without error.
- Filesystem is writable and healthy.

```
root@akashubuntumachine1: /tmp/runbook-demo
root@akashubuntumachine1:/home/ubuntu# cp /etc/hosts /tmp/runbook-demo/
root@akashubuntumachine1:/home/ubuntu# cd /tmp/runbook-demo/
root@akashubuntumachine1:/tmp/runbook-demo# ls -l
total 4
-rw-r--r-- 1 root root 221 Feb  2 11:35 hosts
root@akashubuntumachine1:/tmp/runbook-demo# ls
hosts
root@akashubuntumachine1:/tmp/runbook-demo# cat hosts
127.0.0.1 localhost

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
root@akashubuntumachine1:/tmp/runbook-demo#
```

3. CPU & Memory Health

- CPU usage is minimal.
- Free memory available with no swap usage.
- sshd process consuming negligible resources.

```
ubuntu@akashubuntumachine1: ~
PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
901 root        20   0 1824352 71408 52716 S   0.3   7.3   0:00.52 dockerd
2036 ubuntu     20   0 12348  5796  3616 R   0.3   0.6   0:00.02 top
1 root        20   0 22156 13448  9568 S   0.0   1.4   0:01.15 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

[2]+  Stopped                  top
ubuntu@akashubuntumachine1:~$ free -h
             total        used        free      shared  buff/cache   available
Mem:          957Mi       405Mi       178Mi          940Ki        530Mi        551Mi
Swap:           0B           0B

ubuntu@akashubuntumachine1:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
   Drop-In: /usr/lib/systemd/system/ssh.service.d
            └─ec2-instance-connect.conf
   Active: active (running) since Mon 2026-02-02 11:07:51 UTC; 1h 5min ago
   TriggeredBy: ● ssh.socket
     Docs: man:ssh(8)
           man:ssh_config(5)
   Process: 1298 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1300 (sshd)
     Tasks: 1 (limit: 1121)
    Memory: 11.5M (peak: 12.2M)
       CPU: 203ms
    CGroup: /system.slice/ssh.service
            └─1300 "sshd: /usr/sbin/sshd -D -o AuthorizedKeysCommand /usr/share/ec2-instance-

Feb 02 11:08:29 ip-172-31-0-222 sshd[1304]: Accepted publickey for ubuntu from 103.220.215.193>
Feb 02 11:08:29 ip-172-31-0-222 sshd[1304]: pam_unix(sshd:session): session opened for user ub>
Feb 02 11:21:32 ip-172-31-0-222 sshd[1490]: Accepted publickey for ubuntu from 103.220.215.193>
Feb 02 11:21:32 ip-172-31-0-222 sshd[1490]: pam_unix(sshd:session): session opened for user ub>
Feb 02 11:28:20 ip-172-31-0-222 sshd[1565]: Accepted publickey for ubuntu from 103.220.215.193>
Feb 02 11:28:20 ip-172-31-0-222 sshd[1565]: pam_unix(sshd:session): session opened for user ub>
Feb 02 11:53:07 akashubuntumachine1 sshd[1851]: Accepted publickey for ubuntu from 103.220.215>
Feb 02 11:53:07 akashubuntumachine1 sshd[1851]: pam_unix(sshd:session): session opened for use>
Feb 02 12:07:38 akashubuntumachine1 sshd[1965]: Accepted publickey for ubuntu from 103.220.215>
Feb 02 12:07:38 akashubuntumachine1 sshd[1965]: pam_unix(sshd:session): session opened for use>
lines 1-26/26 (END)
[3]+  Stopped                  systemctl status ssh
ubuntu@akashubuntumachine1:~$
ubuntu@akashubuntumachine1:~$ ps -o pid,pcpu,comm -p 1300
  PID %CPU COMMAND
   1300  0.0  sshd
ubuntu@akashubuntumachine1:~$
```

4. Disk & I/O Health

- a. Disk utilization below critical threshold.
- b. Log directory size within normal range.
- c. I/O wait is low, no bottleneck detected.

```
root@akashubuntumachine1: /home/ubuntu
root@akashubuntumachine1:/home/ubuntu# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/root        6.8G  2.5G  4.3G  38% /
tmpfs            479M   0  479M   0% /dev/shm
tmpfs            192M  928K  191M   1% /run
tmpfs            5.0M   0   5.0M   0% /run/lock
/dev/xvda16      881M   89M  730M  11% /boot
/dev/xvda15      105M   6.2M  99M   6% /boot/efi
tmpfs            96M   12K   96M   1% /run/user/1000
root@akashubuntumachine1:/home/ubuntu# du -sh /var/log/
68M    /var/log/
root@akashubuntumachine1:/home/ubuntu# iostat
Linux 6.14.0-1018-aws (akashubuntumachine1)      02/02/26      _x86_64_      (1 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0.20    0.02   0.15   0.06   15.65   83.91

Device            tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_wrtn    kB_dscd
loop0              0.01         0.07         0.00         0.00         345         0         0
loop1              0.01         0.23         0.00         0.00        1097         0         0
loop2              0.01         0.23         0.00         0.00        1082         0         0
loop3              0.03         0.90         0.00         0.00        4271         0         0
loop4              0.01         0.07         0.00         0.00         346         0         0
loop5              0.14         5.04         0.00         0.00       23916         0         0
loop6              0.00         0.00         0.00         0.00          14         0         0
xvda               2.65       102.03         9.68         0.00     484458     45946         0

root@akashubuntumachine1:/home/ubuntu# 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
0  0       0 181888  19116 524816    0    0   108    9    63   0  0  0 84  0 16  0
root@akashubuntumachine1:/home/ubuntu#
```

5. Network Validation

- d. SSH listening on port 22.
- e. HTTP service responding with 200 OK.
- f. Network stack functioning correctly.

```
root@akashubuntumachine1: /home/ubuntu
root@akashubuntumachine1:/home/ubuntu# ss -tulpn |grep ssh
tcp  LISTEN 0      4096      0.0.0.0:22      0.0.0.0:*      users: (("sshd",pid=1300,fd
tcp  LISTEN 0      4096      [::]:22        [::]:*        users: (("sshd",pid=1300,fd
root@akashubuntumachine1:/home/ubuntu# curl -I http://localhost
HTTP/1.1 200 OK
Server: nginx/1.24.0 (Ubuntu)
Date: Mon, 02 Feb 2026 12:25:48 GMT
Content-Type: text/html
Content-Length: 615
Last-Modified: Sat, 31 Jan 2026 04:52:42 GMT
Connection: keep-alive
ETag: "697d8a9a-267"
Accept-Ranges: bytes

root@akashubuntumachine1:/home/ubuntu#
```

5. Log Review

- a. No critical errors in ssh logs.
- b. Successful login sessions observed.
- c. Cron and system activity logged normally.

```
ubuntu@akashubuntumachine1: ~  
ubuntu@akashubuntumachine1:~$ journalctl -u ssh -n 10  
Feb 02 11:21:32 ip-172-31-0-222 sshd[1490]: pam_unix(sshd:session): session opened for user ubuntu>  
Feb 02 11:28:20 ip-172-31-0-222 sshd[1565]: Accepted publickey for ubuntu from 103.220.215.193>  
Feb 02 11:28:20 ip-172-31-0-222 sshd[1565]: pam_unix(sshd:session): session opened for user ubuntu>  
Feb 02 11:53:07 akashubuntumachine1 sshd[1851]: Accepted publickey for ubuntu from 103.220.215>  
Feb 02 11:53:07 akashubuntumachine1 sshd[1851]: pam_unix(sshd:session): session opened for use>  
Feb 02 12:07:38 akashubuntumachine1 sshd[1965]: Accepted publickey for ubuntu from 103.220.215>  
Feb 02 12:07:38 akashubuntumachine1 sshd[1965]: pam_unix(sshd:session): session opened for use>  
Feb 02 12:22:25 akashubuntumachine1 sshd[4382]: Connection closed by 5.101.64.6 port 60023>  
Feb 02 12:42:43 akashubuntumachine1 sshd[4846]: Accepted publickey for ubuntu from 103.220.215>  
Feb 02 12:42:43 akashubuntumachine1 sshd[4846]: pam_unix(sshd:session): session opened for use>  
[1]+  Stopped                  journalctl -u ssh -n 10  
ubuntu@akashubuntumachine1:~$ tail -n 10 /var/log/auth.log  
2026-02-02T12:20:11.404097+00:00 ip-172-31-0-222 groupadd[2588]: new group: name=pcp, GID=988  
2026-02-02T12:20:11.433361+00:00 ip-172-31-0-222 useradd[2595]: new user: name=pcp, UID=997, GI  
D=988, home=/var/lib/pcp, shell=/usr/sbin/nologin, from=/dev/pts/7  
2026-02-02T12:22:25.681359+00:00 ip-172-31-0-222 sshd[4382]: Connection closed by 5.101.64.6 po  
rt 60023  
2026-02-02T12:25:01.815097+00:00 ip-172-31-0-222 CRON[4385]: pam_unix(cron:session): session op  
ened for user root(uid=0) by root(uid=0)  
2026-02-02T12:25:01.821340+00:00 ip-172-31-0-222 CRON[4385]: pam_unix(cron:session): session cl  
osed for user root  
2026-02-02T12:35:01.825825+00:00 ip-172-31-0-222 CRON[4385]: pam_unix(cron:session): session op  
ened for user root(uid=0) by root(uid=0)  
2026-02-02T12:35:01.828576+00:00 ip-172-31-0-222 CRON[4385]: pam_unix(cron:session): session cl  
osed for user root  
2026-02-02T12:42:43.145387+00:00 ip-172-31-0-222 sshd[4846]: Accepted publickey for ubuntu from  
103.220.215.193 port 43160 ssh2: RSA SHA256:koLMPn198RwAWN5wBOINYD1+dZ9/IH7gaJ0R8oGv5E  
2026-02-02T12:42:43.146818+00:00 ip-172-31-0-222 sshd[4846]: pam_unix(sshd:session): session op  
ened for user ubuntu(uid=1000) by ubuntu(uid=0)  
2026-02-02T12:42:43.152517+00:00 ip-172-31-0-222 systemd-logind[535]: New session 19 of user ub  
untu.  
ubuntu@akashubuntumachine1:~$
```

■ Summary & Findings

- d. System is operating within healthy parameters.
- e. No abnormal CPU, memory, disk, or network behavior detected.
- f. SSH service is stable with valid authentication activity.
- g. Logs show no recent critical failures.

■ If This Worsens – Next Actions

- h. Restart the affected service and monitor resource usage.
- i. Increase log verbosity for deeper inspection.
- j. Collect diagnostics using tools like strace, top -H, and iotop.