Day 5. Runbook Notes on Troubleshooting

Command: uname -a

Observation: System is running an AWS-optimized Ubuntu Linux kernel (6.14.0) on x86_64 architecture.

```
ubuntu@ip-172-31-13-238:~$ uname -a
Linux ip-172-31-13-238 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-172-31-13-238:~$ ^C
ubuntu@ip-172-31-13-238:~$ ^C
ubuntu@ip-172-31-13-238:~$
```

Command: lsb_release -a

Observation: System is running Ubuntu 24.04 LTS (noble), confirming a stable LTS environment.

```
ubuntu@ip-172-31-13-238:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 24.04.3 LTS
Release:        24.04
Codename:       noble
```

Command: mkdir /tmp/runbook-demo

Observation: Able to create directory under /tmp, confirming filesystem is writable and responsive.

```
ubuntu@ip-172-31-13-238:~$ mkdir /tmp/runbook-demo
ubuntu@ip-172-31-13-238:~$
```

Command: cp /etc/hosts /tmp/runbook-demo && ls -l /tmp/runbook-demo

Observation: Successfully copied file and verified permissions, confirming normal filesystem read/write operations.

```
ubuntu@ip-172-31-13-238:~$ cp /etc/hosts /tmp/runbook-demo/hosts_bkp && ls -l /tmp/runbook-demo/
total 4
-rw-r--r-- 1 ubuntu ubuntu 221 Jan 30 08:58 hosts_bkp
ubuntu@ip-172-31-13-238:~$
```

Command: free -h

Observation: System has sufficient available memory (~500MB) with no swap usage, indicating no memory pressure.

```
ubuntu@ip-172-31-13-238:~$ free -h
          total    used    free    shared  buff/cache  available
Mem:      914Mi    406Mi   263Mi   2.8Mi   402Mi       507Mi
Swap:     0B       0B      0B
```

Command: pidof cron

Observation: Identified cron service process with PID 577 for targeted resource analysis.

```
ubuntu@ip-172-31-13-238:~$ pidof cron
577
```

Command: ps -o pid,pcpu,pmem,comm -p 577

Observation: cron process is consuming negligible CPU and memory, indicating no resource pressure from the service.

```
ubuntu@ip-172-31-13-238:~$ ps -o pid,pcpu,pmem,comm -p 577
    PID %CPU %MEM COMMAND
    577  0.0  0.3 cron
```

Command: df -h

Observation: All filesystems have sufficient free space; root filesystem usage is ~48%, ruling out disk space issues.

```
ubuntu@ip-172-31-13-238:~$ df -h
Filesystem                     Size  Used Avail Use% Mounted on
/dev/root                      6.8G  3.2G  3.5G  48% /
tmpfs                          458M     0  458M   0% /dev/shm
tmpfs                          183M  964K  182M   1% /run
tmpfs                          5.0M     0  5.0M   0% /run/lock
efivarfs                       128K  4.7K  119K   4% /sys/firmware/efi/efivars
/dev/nvme0n1p16                881M  155M  665M  19% /boot
/dev/nvme2n1                   5.9G   24K  5.6G   1% /consdata2
/dev/nvme0n1p15                105M  6.2M   99M   6% /boot/efi
/dev/mapper/tws_vg-consdata1   7.8G   32K  7.4G   1% /consdata1
tmpfs                           92M   12K   92M   1% /run/user/1000
```

Command: du -sh /var/log

Observation: /var/log uses ~144MB of disk space; no excessive log growth observed. Permission warnings are expected for protected directories.

```
ubuntu@ip-172-31-13-238:~$ du -sh /var/log
du: cannot read directory '/var/log/chrony': Permission denied
du: cannot read directory '/var/log/amazon': Permission denied
du: cannot read directory '/var/log/private': Permission denied
144M    /var/log
```

Command: ss -tulpn

Observation: Expected services like SSH (22) and HTTP (80) are listening; no abnormal open ports detected.

```
ubuntu@ip-172-31-13-238:~$ ss -tulpn
Netid  State    Recv-Q  Send-Q      Local Address:Port    Peer Address:Port    Process
udp    UNCONN   0       0           127.0.0.54:53         0.0.0.0:*
udp    UNCONN   0       0           127.0.0.53%lo:53      0.0.0.0:*
udp    UNCONN   0       0           172.31.13.238%ens5:68 0.0.0.0:*
udp    UNCONN   0       0           127.0.0.1:323         0.0.0.0:*
udp    UNCONN   0       0           [::1]:323             [::]:*
tcp    LISTEN   0       511         0.0.0.0:80            0.0.0.0:*
tcp    LISTEN   0       4096        127.0.0.1:40017       0.0.0.0:*
tcp    LISTEN   0       4096        0.0.0.0:22            0.0.0.0:*
tcp    LISTEN   0       4096        127.0.0.53%lo:53      0.0.0.0:*
tcp    LISTEN   0       4096        127.0.0.54:53         0.0.0.0:*
tcp    LISTEN   0       511         [::]:80               [::]:*
tcp    LISTEN   0       4096        [::]:22               [::]:*
```

Command: curl -I http://localhost

Observation: Local HTTP service (nginx) responds with 200 OK, confirming application and network health.

```
ubuntu@ip-172-31-13-238:~$ curl -I http://localhost
HTTP/1.1 200 OK
Server: nginx/1.24.0 (Ubuntu)
Date: Fri, 30 Jan 2026 09:21:42 GMT
Content-Type: text/html
Content-Length: 615
Last-Modified: Sun, 25 Jan 2026 14:01:34 GMT
Connection: keep-alive
ETag: "6976223e-267"
Accept-Ranges: bytes
```

Command: journalctl -u cron -n 50

Observation: Cron logs show regular job execution and normal service restarts with no recent errors.

```
ubuntu@ip-172-31-13-238:~$ journalctl -u cron -n 50
Jan 30 02:25:01 ip-172-31-13-238 CRON[10758]: pam_unix(cron:session): session closed for user root
Jan 30 02:35:01 ip-172-31-13-238 CRON[10775]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Jan 30 02:35:01 ip-172-31-13-238 CRON[10776]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Jan 30 02:35:01 ip-172-31-13-238 CRON[10775]: pam_unix(cron:session): session closed for user root
Jan 30 02:45:01 ip-172-31-13-238 CRON[10783]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Jan 30 02:45:01 ip-172-31-13-238 CRON[10784]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Jan 30 02:45:01 ip-172-31-13-238 CRON[10783]: pam_unix(cron:session): session closed for user root
Jan 30 02:55:01 ip-172-31-13-238 CRON[10791]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Jan 30 02:55:01 ip-172-31-13-238 CRON[10792]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Jan 30 02:55:01 ip-172-31-13-238 CRON[10791]: pam_unix(cron:session): session closed for user root
Jan 30 03:05:01 ip-172-31-13-238 CRON[10809]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Jan 30 03:05:01 ip-172-31-13-238 CRON[10810]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Jan 30 03:05:01 ip-172-31-13-238 CRON[10809]: pam_unix(cron:session): session closed for user root
Jan 30 03:10:01 ip-172-31-13-238 CRON[10814]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Jan 30 03:10:01 ip-172-31-13-238 CRON[10814]: pam_unix(cron:session): session closed for user root
Jan 30 03:15:01 ip-172-31-13-238 CRON[10822]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Jan 30 03:15:01 ip-172-31-13-238 CRON[10822]: pam_unix(cron:session): session closed for user root
Jan 30 03:17:01 ip-172-31-13-238 CRON[10826]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Jan 30 03:17:01 ip-172-31-13-238 CRON[10827]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)
Jan 30 03:17:01 ip-172-31-13-238 CRON[10826]: pam_unix(cron:session): session closed for user root
Jan 30 03:25:01 ip-172-31-13-238 CRON[10834]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Jan 30 03:25:01 ip-172-31-13-238 CRON[10835]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Jan 30 03:25:01 ip-172-31-13-238 CRON[10834]: pam_unix(cron:session): session closed for user root
Jan 30 03:35:01 ip-172-31-13-238 CRON[10852]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Jan 30 03:35:01 ip-172-31-13-238 CRON[10853]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Jan 30 03:35:01 ip-172-31-13-238 CRON[10852]: pam_unix(cron:session): session closed for user root
Jan 30 03:45:01 ip-172-31-13-238 CRON[10861]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Jan 30 03:45:01 ip-172-31-13-238 CRON[10862]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Jan 30 03:45:01 ip-172-31-13-238 CRON[10861]: pam_unix(cron:session): session closed for user root
Jan 30 03:52:51 ip-172-31-13-238 systemd[1]: Stopping cron.service - Regular background program processing daemon...
Jan 30 03:52:51 ip-172-31-13-238 systemd[1]: cron.service: Deactivated successfully.
Jan 30 03:52:51 ip-172-31-13-238 systemd[1]: Stopped cron.service - Regular background program processing daemon.
Jan 30 03:52:51 ip-172-31-13-238 systemd[1]: cron.service: Consumed 1.025s CPU time, 584.0K memory peak, 0B memory swap peak.
```

Command: tail -n 50 /var/log/nginx/error.log

Observation: No recent errors found in nginx error log, indicating stable application behavior.

```
ubuntu@ip-172-31-13-238:~$ tail -f /var/log/nginx/error.log
```

If this worsens:

1. Restart the affected service and monitor CPU, memory, and logs immediately after the restart.
2. Increase log verbosity (if supported) and capture logs during the issue window.
3. Collect deeper diagnostics such as **strace** or **vmstat/iostat** and escalate with evidence.

linux-troubleshooting-runbook