NAME : T MANOJ

EMPID : LYAKE2KHS

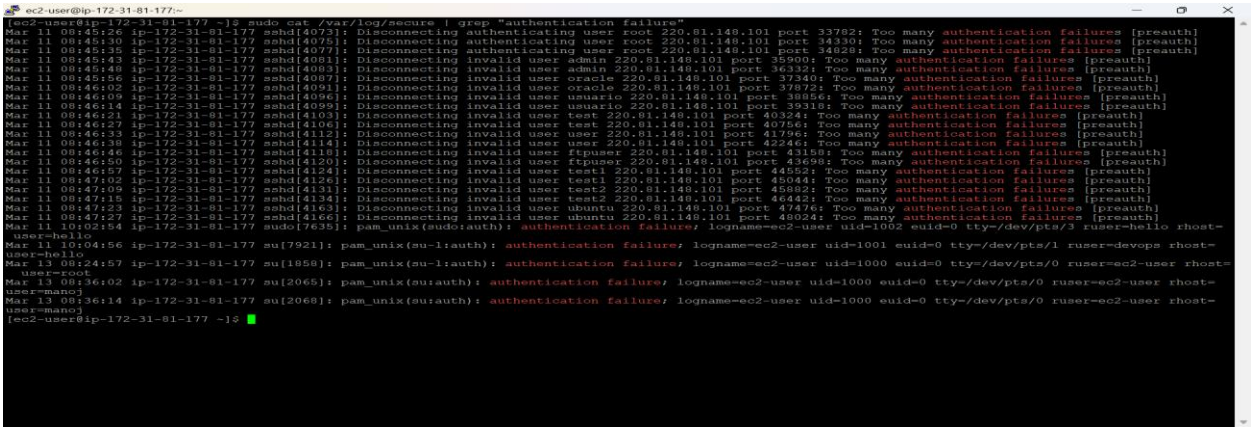
DATE : 13-02-2025

Task –1

Monitoring Authentication and Securty Logs:
Scenario: A company wants to track failed SSH login attempts and potential brute-force attacks.

Cmd :

sudo cat /var/log/secure | grep "authentication failure"



Task 2

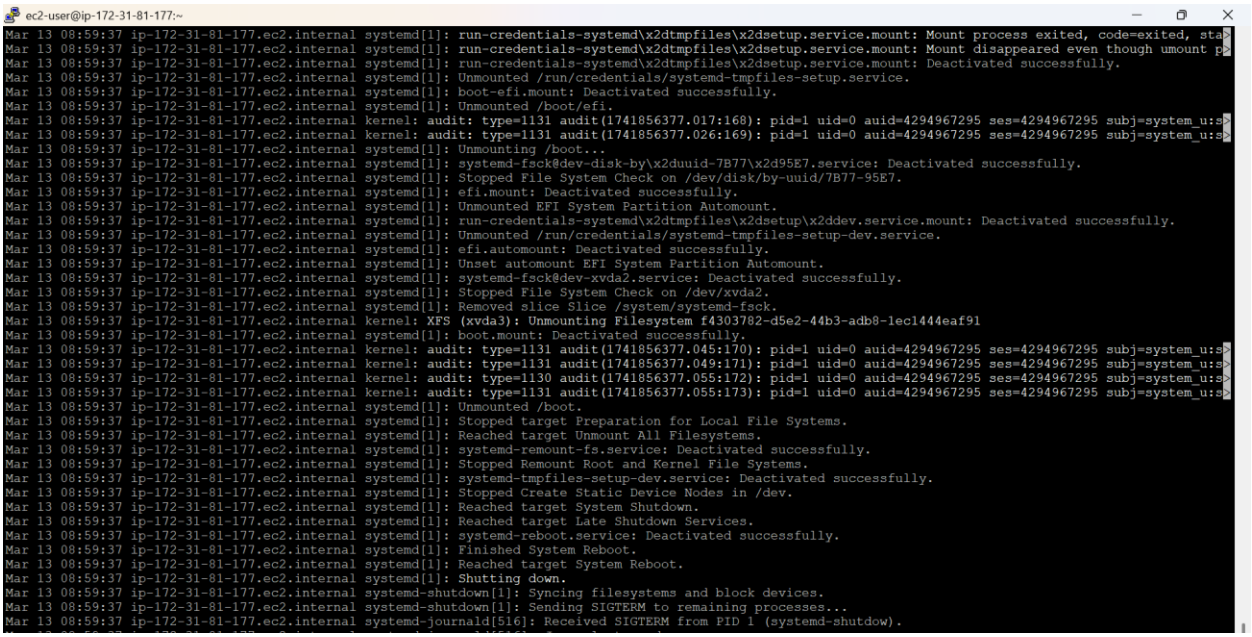
2. Monitoring Boot Issues:

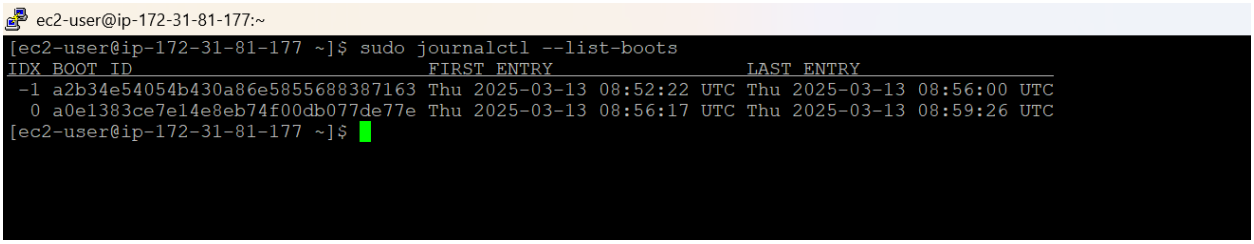
Scenario: A system administrator wants to check why a server failed to boot properly.

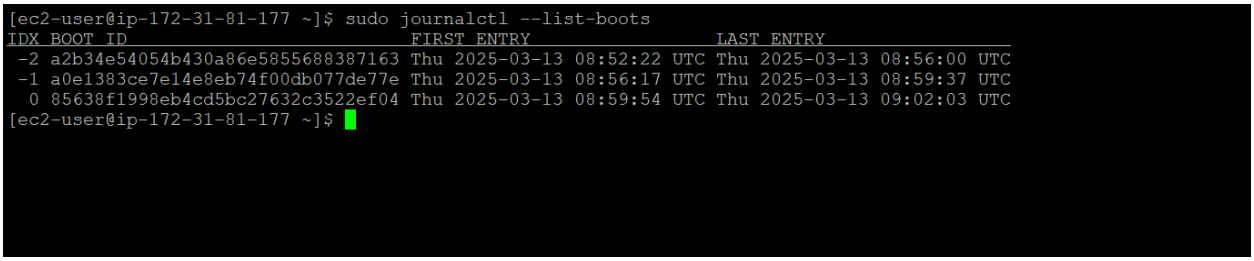
Cmd :

sudo journalctl --list-boots

sudo journalctl -b -1



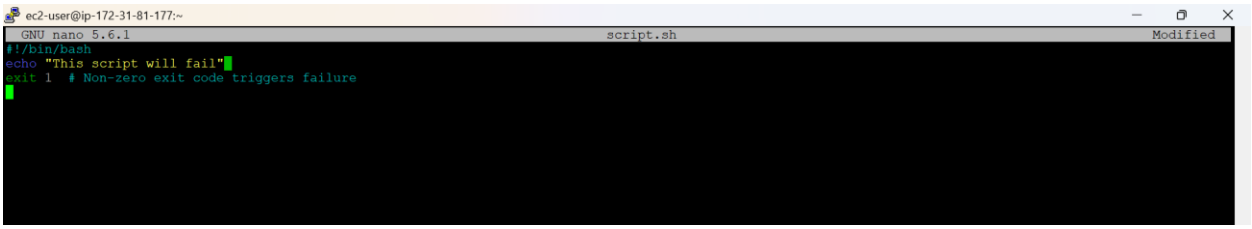


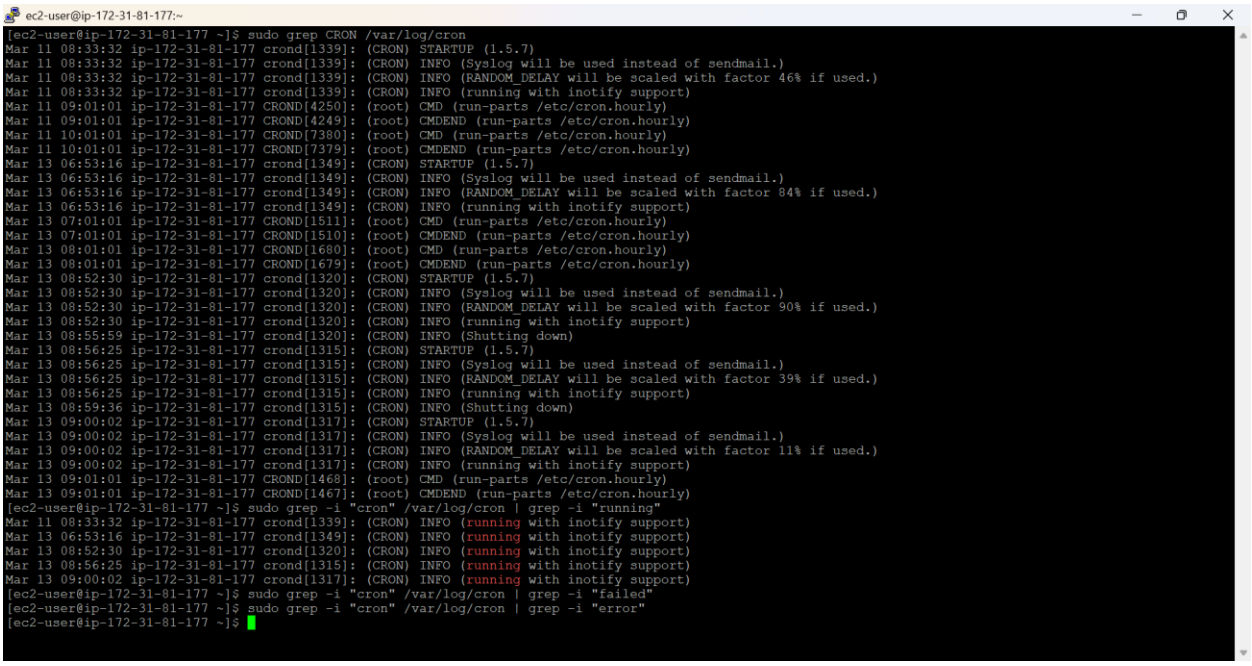


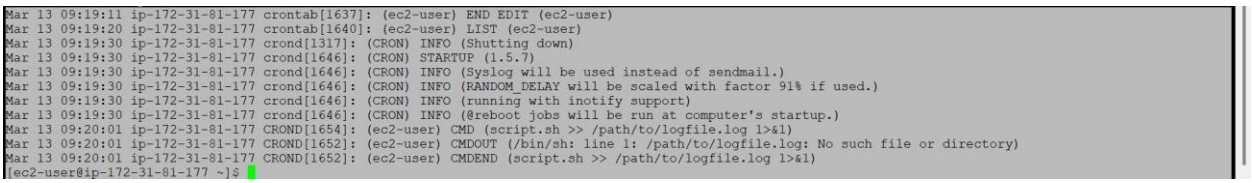
Task 3 :

Monitoring Cron Jobs:
Scenario: A scheduled cron job is not running as expected, and the admin needs to debug it.

Cmd : sudo grep -i "error" /var/log/cron







Task 4:

Monitoring Apache/Nginx Web Server Logs:
Scenario: A DevOps engineer checks if a website is receiving requests.

Cmd :

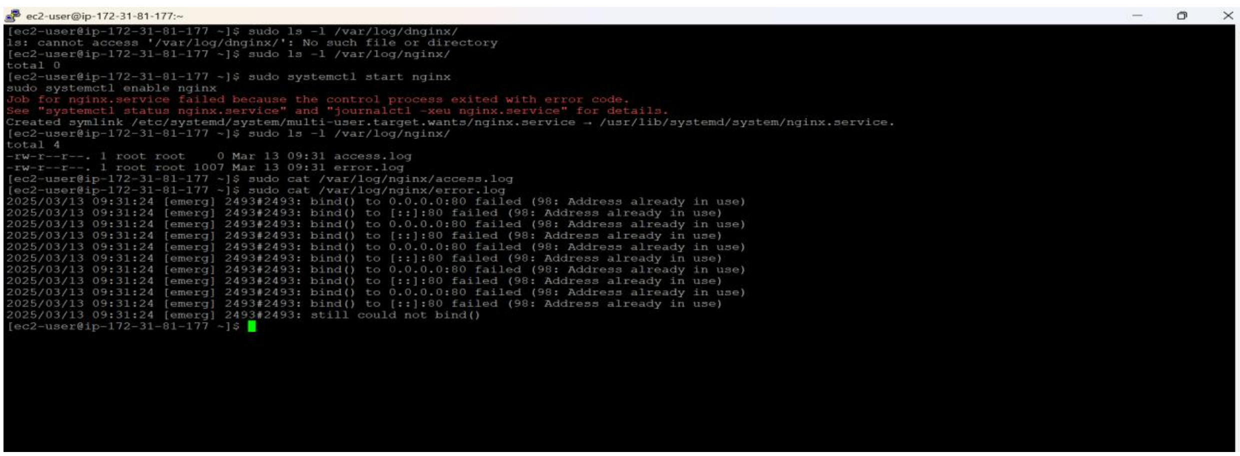
sudo grep "CustomLog" /etc/httpd/conf/httpd.conf

sudo ls -l /var/log/httpd/

For nginx :

sudo ls -l /var/log/httpd/nginx/access.log

sudo ls -l /var/log/httpd/nginx/error.log



Task 5:

Checking Mail Server Logs
Scenario: An email server admin wants to troubleshoot why emails are not being sent.
Cmd:

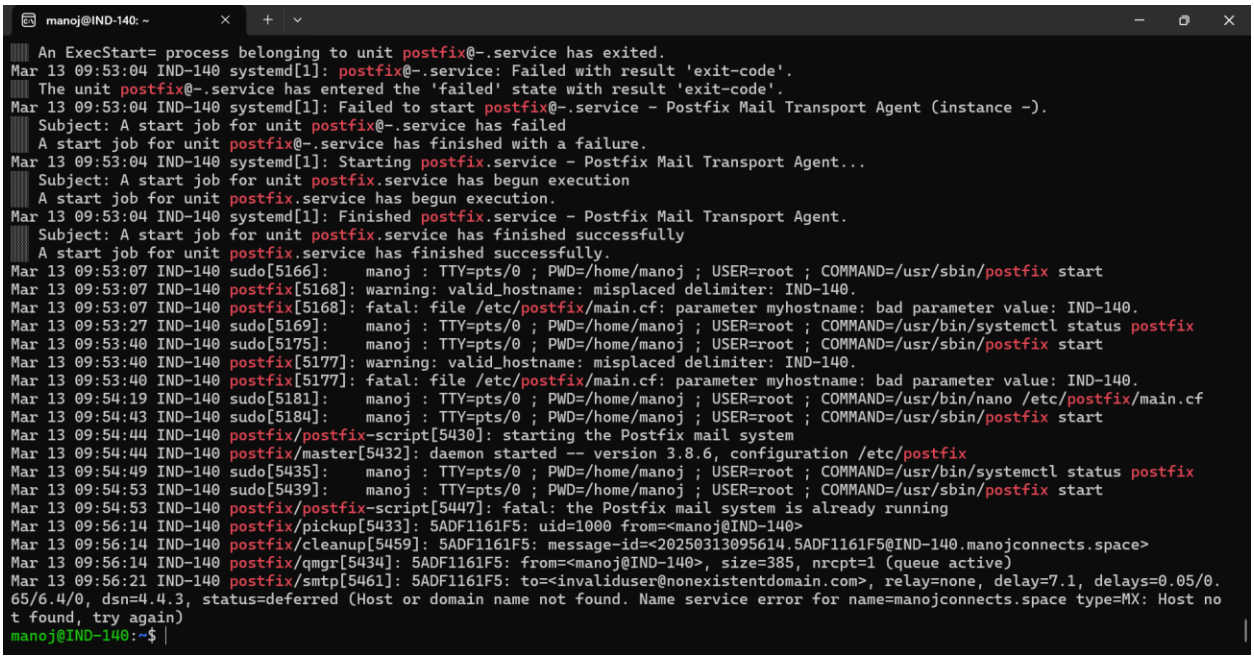
sudo postfix start

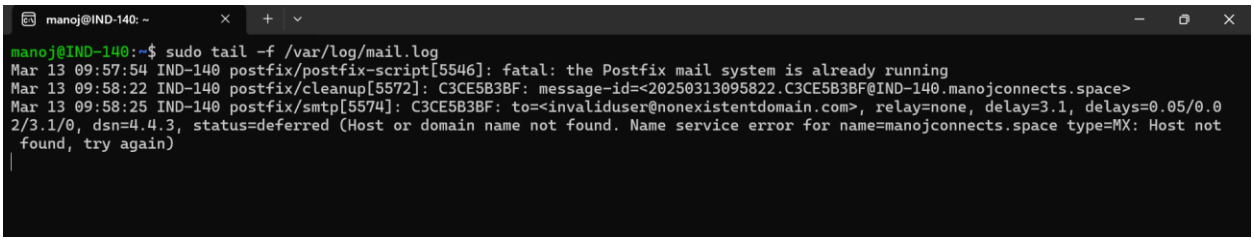
manoj@IND-140:~$ sudo postfix start

echo "Test Email" | mail -s "Failed Test" invaliduser@nonexistentdomain.com

sudo journalctl -xe | grep postfix

sudo tail -f /var/log/mail.log



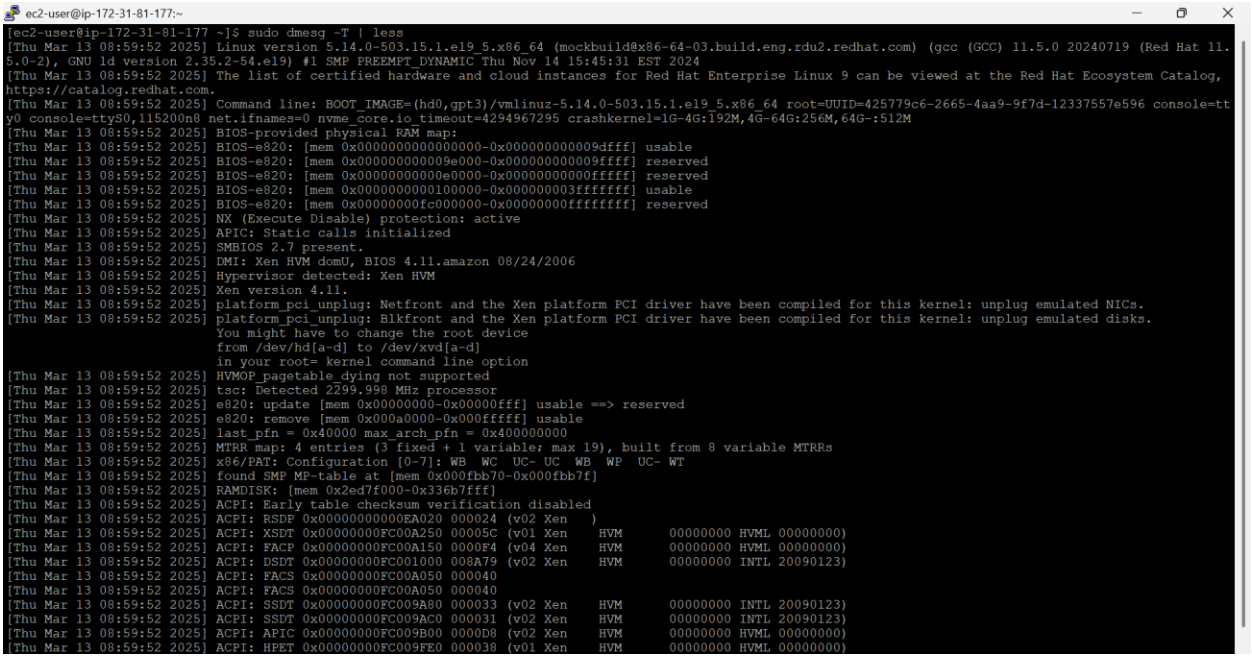


Task 6 :

Checking Kernel and Hardware Issues
Scenario: A sysadmin checks for kernel-related errors after a server crash.

Cmd:

sudo dmesg -T | less



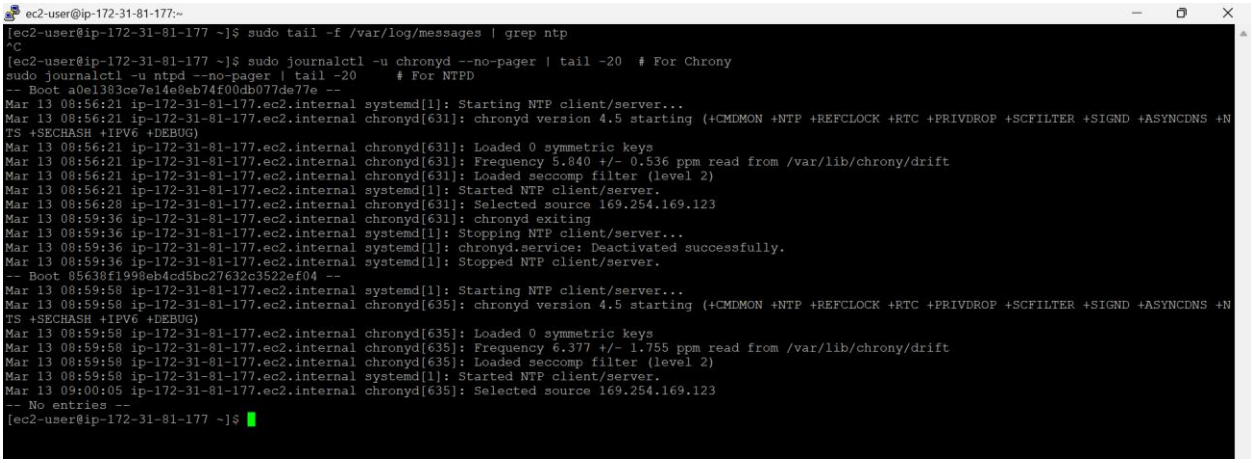
Task 7:

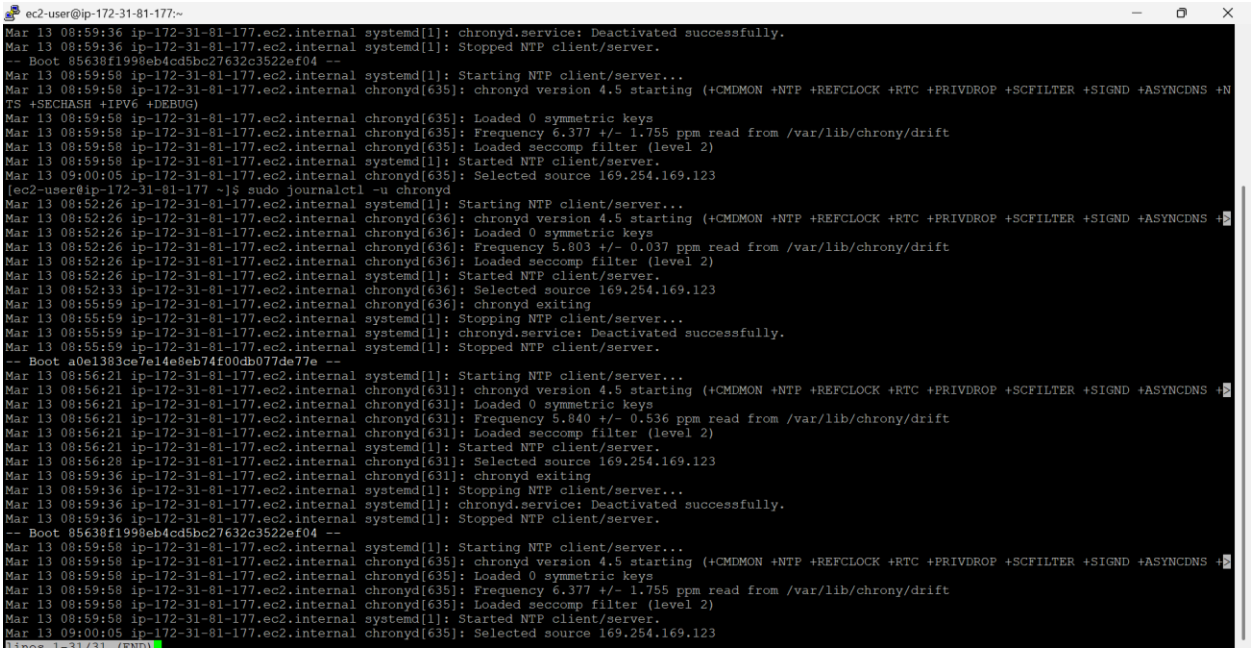
Monitoring Time Synchronization (NTP)
Scenario: A financial institution needs accurate time synchronization for transactions.

Cmd:

sudo journalctl -u chronyd --no-pager | tail -20

sudo journalctl -u ntpd --no-pager | tail -20



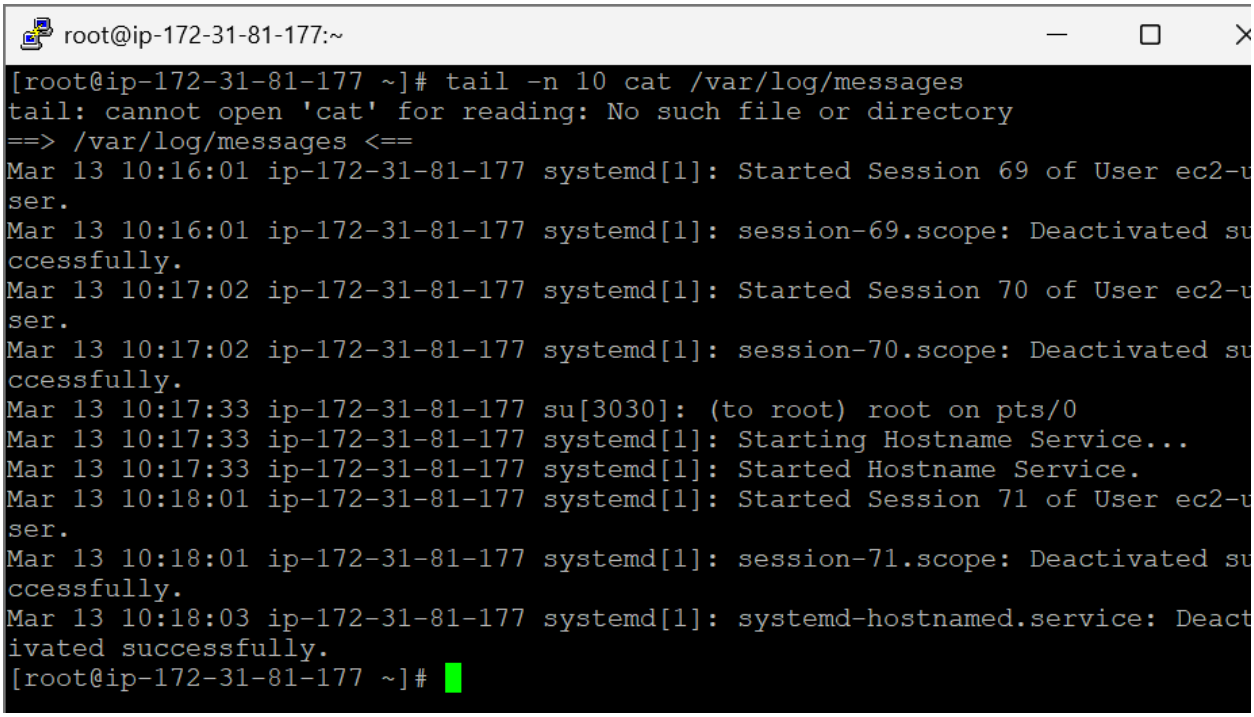


Task 8:

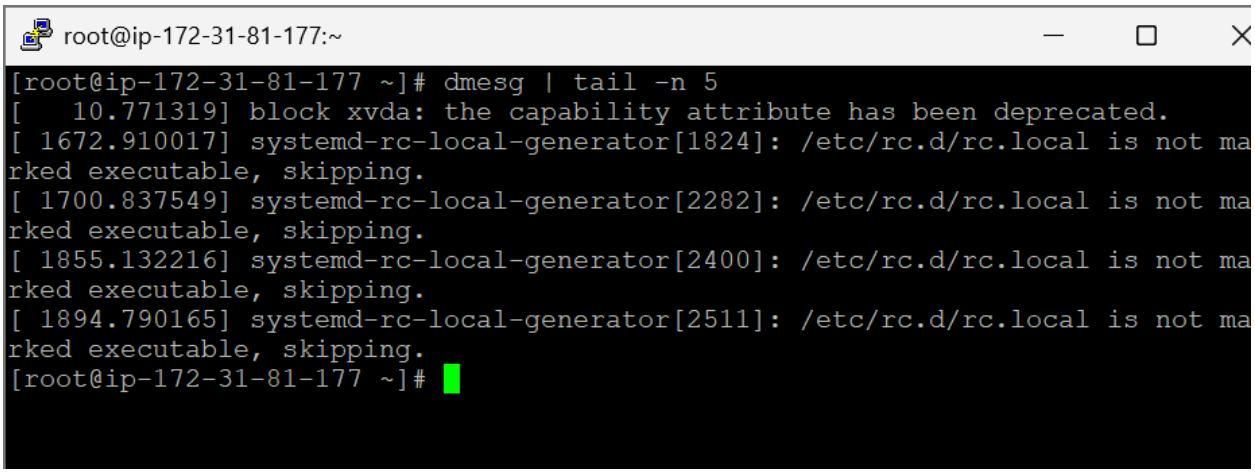
Execute all the log path according to your operating system assigned

Cmd:

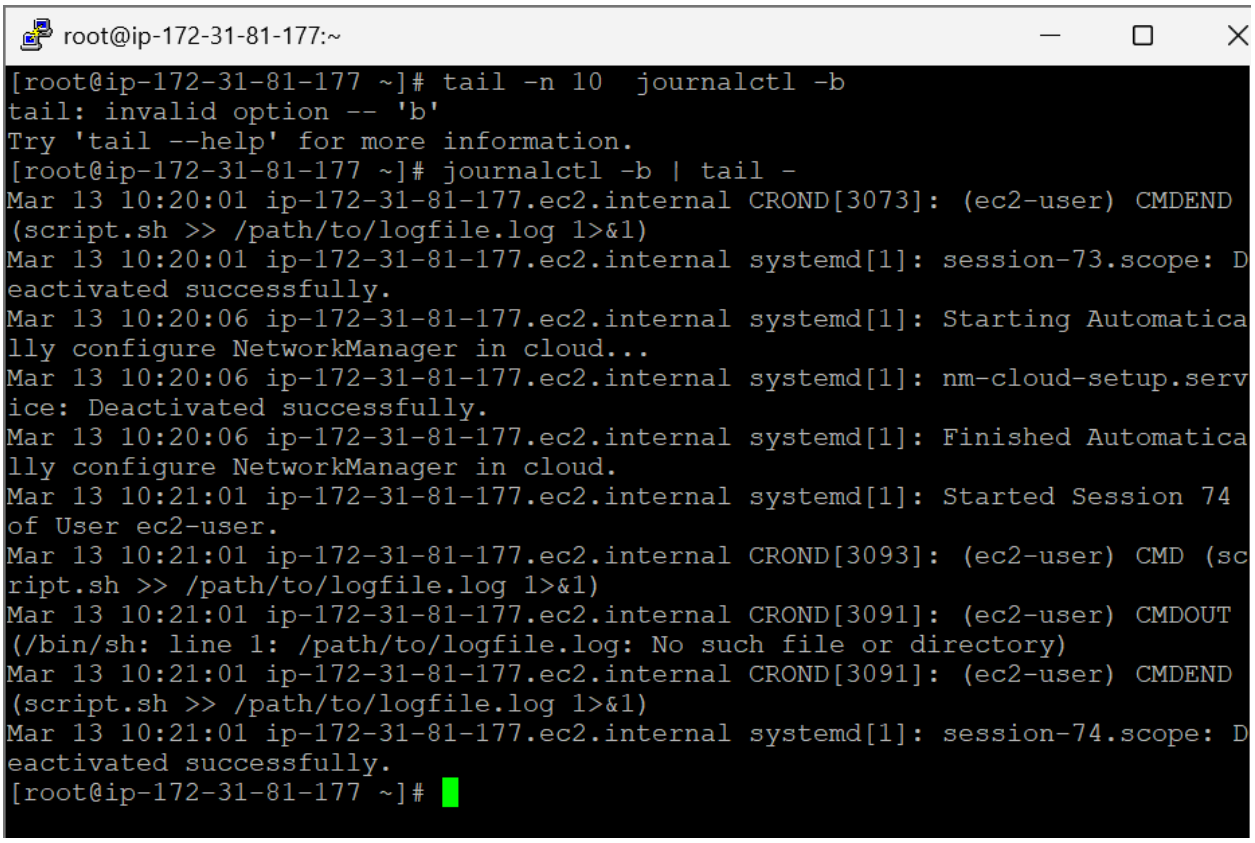
General message : cat /var/log/message



Kernel logs : dmesg | tail -n 5



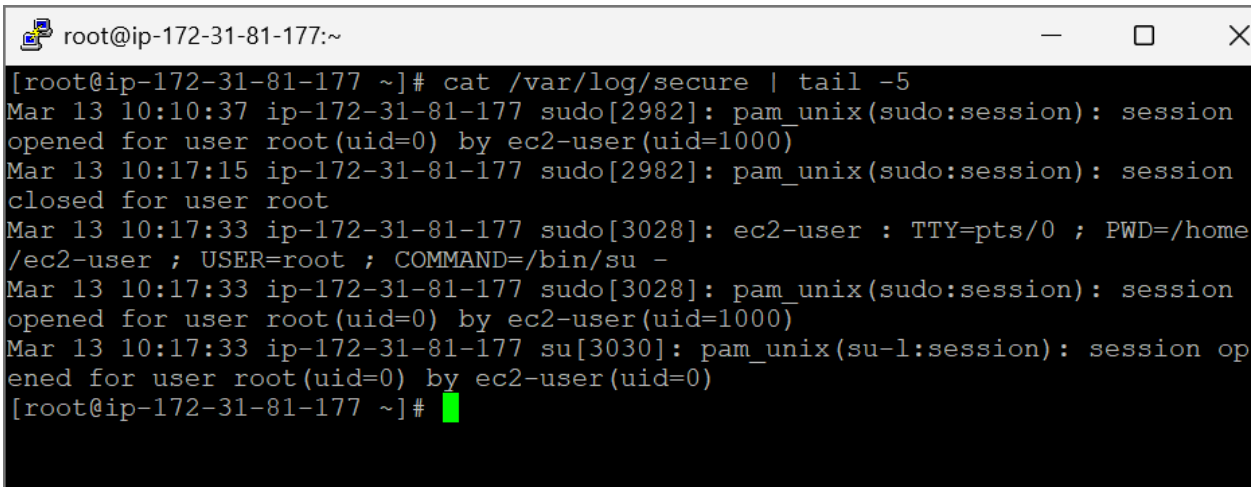
Boot logs : journalctl –b



Authentication

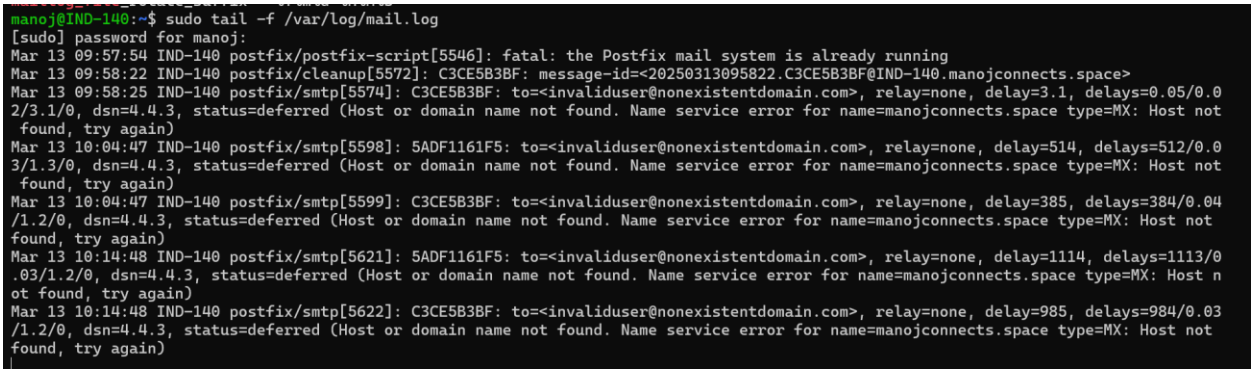
Logs

> cat /var/log/secure

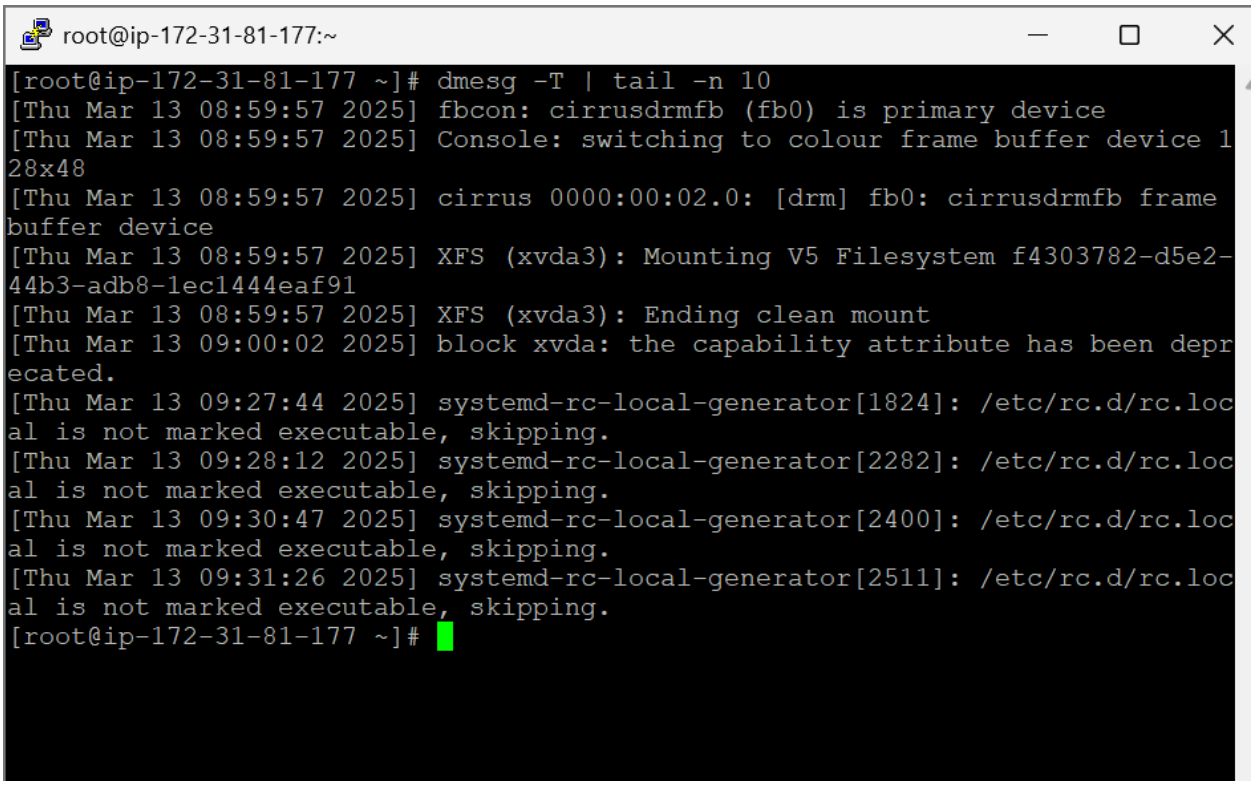


Mail Logs :

sudo tail -f /var/log/mail.log



dmesg


root@ip-172-31-81-177:~
[root@ip-172-31-81-177 ~]# dmesg -T | tail -n 10
[Thu Mar 13 08:59:57 2025] fbcon: cirrusdrmfb (fb0) is primary device
[Thu Mar 13 08:59:57 2025] Console: switching to colour frame buffer device 1
28x48
[Thu Mar 13 08:59:57 2025] cirrus 0000:00:02.0: [drm] fb0: cirrusdrmfb frame
buffer device
[Thu Mar 13 08:59:57 2025] XFS (xvda3): Mounting V5 Filesystem f4303782-d5e2-
44b3-adb8-1ec1444eaf91
[Thu Mar 13 08:59:57 2025] XFS (xvda3): Ending clean mount
[Thu Mar 13 09:00:02 2025] block xvda: the capability attribute has been depr
ecated.
[Thu Mar 13 09:27:44 2025] systemd-rc-local-generator[1824]: /etc/rc.d/rc.loc
al is not marked executable, skipping.
[Thu Mar 13 09:28:12 2025] systemd-rc-local-generator[2282]: /etc/rc.d/rc.loc
al is not marked executable, skipping.
[Thu Mar 13 09:30:47 2025] systemd-rc-local-generator[2400]: /etc/rc.d/rc.loc
al is not marked executable, skipping.
[Thu Mar 13 09:31:26 2025] systemd-rc-local-generator[2511]: /etc/rc.d/rc.loc
al is not marked executable, skipping.
[root@ip-172-31-81-177 ~]#