



NAME : T MANOJ

EMPID : LYAKE2KHS

DATE : 13-02-2025

Task-1

Monitoring Authentication and Security 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"

```
ec2-user@ip-172-31-81-177:~$ sudo cat /var/log/secure | grep "authentication failure"
Mar 11 08:45:26 ip-172-31-81-177 sshd[4073]: Disconnecting authenticating user root 220.81.148.101 port 33702: Too many authentication failures [preauth]
Mar 11 08:45:30 ip-172-31-81-177 sshd[4075]: Disconnecting authenticating user root 220.81.148.101 port 34330: Too many authentication failures [preauth]
Mar 11 08:45:35 ip-172-31-81-177 sshd[4077]: Disconnecting authenticating user root 220.81.148.101 port 34828: Too many authentication failures [preauth]
Mar 11 08:45:43 ip-172-31-81-177 sshd[4081]: Disconnecting invalid user admin 220.81.148.101 port 35900: Too many authentication failures [preauth]
Mar 11 08:45:48 ip-172-31-81-177 sshd[4083]: Disconnecting invalid user admin 220.81.148.101 port 36332: Too many authentication failures [preauth]
Mar 11 08:45:56 ip-172-31-81-177 sshd[4087]: Disconnecting invalid user oracle 220.81.148.101 port 37340: Too many authentication failures [preauth]
Mar 11 08:46:02 ip-172-31-81-177 sshd[4091]: Disconnecting invalid user oracle 220.81.148.101 port 37872: Too many authentication failures [preauth]
Mar 11 08:46:09 ip-172-31-81-177 sshd[4096]: Disconnecting invalid user usuario 220.81.148.101 port 38856: Too many authentication failures [preauth]
Mar 11 08:46:14 ip-172-31-81-177 sshd[4099]: Disconnecting invalid user usuario 220.81.148.101 port 39318: Too many authentication failures [preauth]
Mar 11 08:46:21 ip-172-31-81-177 sshd[4103]: Disconnecting invalid user test 220.81.148.101 port 40324: Too many authentication failures [preauth]
Mar 11 08:46:27 ip-172-31-81-177 sshd[4106]: Disconnecting invalid user test 220.81.148.101 port 40756: Too many authentication failures [preauth]
Mar 11 08:46:33 ip-172-31-81-177 sshd[4112]: Disconnecting invalid user user 220.81.148.101 port 41796: Too many authentication failures [preauth]
Mar 11 08:46:38 ip-172-31-81-177 sshd[4114]: Disconnecting invalid user user 220.81.148.101 port 42246: Too many authentication failures [preauth]
Mar 11 08:46:46 ip-172-31-81-177 sshd[4118]: Disconnecting invalid user ftpuser 220.81.148.101 port 43190: Too many authentication failures [preauth]
Mar 11 08:46:50 ip-172-31-81-177 sshd[4120]: Disconnecting invalid user ftpuser 220.81.148.101 port 43698: Too many authentication failures [preauth]
Mar 11 08:46:57 ip-172-31-81-177 sshd[4124]: Disconnecting invalid user test1 220.81.148.101 port 44582: Too many authentication failures [preauth]
Mar 11 08:47:02 ip-172-31-81-177 sshd[4126]: Disconnecting invalid user test1 220.81.148.101 port 45044: Too many authentication failures [preauth]
Mar 11 08:47:09 ip-172-31-81-177 sshd[4131]: Disconnecting invalid user test2 220.81.148.101 port 45882: Too many authentication failures [preauth]
Mar 11 08:47:15 ip-172-31-81-177 sshd[4134]: Disconnecting invalid user test2 220.81.148.101 port 46642: Too many authentication failures [preauth]
Mar 11 08:47:23 ip-172-31-81-177 sshd[4163]: Disconnecting invalid user ubuntu 220.81.148.101 port 47476: Too many authentication failures [preauth]
Mar 11 08:47:27 ip-172-31-81-177 sshd[4166]: Disconnecting invalid user ubuntu 220.81.148.101 port 48024: Too many authentication failures [preauth]
Mar 11 10:02:54 ip-172-31-81-177 sudo[7635]: pam_unix(sudo:auth): authentication failure; logname=ec2-user uid=1002 suid=0 tty=/dev/pts/3 ruser=hello rhost=
user=hello
Mar 11 10:04:56 ip-172-31-81-177 su[7921]: pam_unix(su:1:auth): authentication failure; logname=ec2-user uid=1001 suid=0 tty=/dev/pts/1 ruser=devops rhost=
user=hello
Mar 11 08:24:57 ip-172-31-81-177 su[1858]: pam_unix(su:1:auth): authentication failure; logname=ec2-user uid=1000 suid=0 tty=/dev/pts/0 ruser=ec2-user rhost=
user=root
Mar 13 08:36:02 ip-172-31-81-177 su[2065]: pam_unix(su:auth): authentication failure; logname=ec2-user uid=1009 suid=0 tty=/dev/pts/0 ruser=ec2-user rhost=
user=mano
Mar 13 08:36:14 ip-172-31-81-177 su[2068]: pam_unix(su:auth): authentication failure; logname=ec2-user uid=1000 suid=0 tty=/dev/pts/0 ruser=ec2-user rhost=
user=mano
[ec2-user@ip-172-31-81-177 ~]$
```

Task 2

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

Cmd :

```
sudo journalctl --list-boots
```

```
sudo journalctl -b -1
```

```

Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dsetup.service.mount: Mount process exited, code=exited, sta
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dsetup.service.mount: Mount disappeared even though mount p
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dsetup.service.mount: Deactivated successfully.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Unmounted /run/credentials/systemd-tmpfiles-setup.service.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: boot-efi.mount: Deactivated successfully.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Unmounted /boot/efi.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal kernel: audit: type=1131 audit(1741856377.017:168): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:sa
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal kernel: audit: type=1131 audit(1741856377.026:169): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:sa
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Unmounted /boot/efi.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: systemd-fsck@dev-disk-by\x2duuid-7b77\x2d95e7.service: Deactivated successfully.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Stopped File System Check on /dev/disk/by-uuid/7b77-95E7.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: efi.mount: Deactivated successfully.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Unmounted EFI System Partition Automount.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: run-credentials-systemd\x2dtmpfiles\x2dsetup\x2dddev.service.mount: Deactivated successfully.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Unmounted /run/credentials/systemd-tmpfiles-setup-dev.service.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: efi_automount: Deactivated successfully.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Unset automount EFI System Partition Automount.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: systemd-fsck@dev-xvda2.service: Deactivated successfully.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Stopped File System Check on /dev/xvda2.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Removed slice Slice /system/systemd-fsck.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal kernel: XFS (vd3a3): Unmounting Filesystem 4f303782-d5e2-44b3-adb8-1ec1444eaf91
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: boot.mount: Deactivated successfully.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal kernel: audit: type=1131 audit(1741856377.045:170): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:sa
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal kernel: audit: type=1131 audit(1741856377.049:171): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:sa
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal kernel: audit: type=1130 audit(1741856377.055:172): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:sa
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal kernel: audit: type=1131 audit(1741856377.055:173): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:sa
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Unmounted /boot.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Stopped target Preparation for Local File Systems.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Reached target Unset All Filesystems.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: systemd-remount-fs.service: Deactivated successfully.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Stopped Root Root and Kernel File Systems.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: systemd-tmpfiles-setup-dev.service: Deactivated successfully.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Stopped Create Static Device Nodes in /dev.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Reached target System Shutdown.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Reached target Late Shutdown Services.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: systemd-reboot.service: Deactivated successfully.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Finished System Reboot.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Reached target System Reboot.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd[1]: Shutting down.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd-shutdown[1]: Syncing filesystems and block devices.
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd-shutdown[1]: Sending SIGTERM to remaining processes...
Mar 13 08:59:37 ip-172-31-81-177.ec2.internal systemd-journald[516]: Received SIGTERM from PID 1 (systemd-shutdown).

```

```
ec2-user@ip-172-31-81-177:~$ sudo journalctl --list-boots
```

IDX	BOOT ID	FIRST ENTRY	LAST ENTRY
-1	a2b34ae5405b4630a86e5855688387163	Thu 2025-03-13 08:52:22 UTC	Thu 2025-03-13 08:56:00 UTC
0	a0e1383ce7e14e8eb74f00db077de77e	Thu 2025-03-13 08:56:17 UTC	Thu 2025-03-13 08:59:26 UTC

```
ec2-user@ip-172-31-81-177:~$
```

```
[ec2-user@ip-172-31-81-177 ~]$ sudo journalctl --list-boots
```

IDX	ROOT ID	FIRST ENTRY	LAST ENTRY
-2	a2b34ae54054b430a86e5855688387163	Thu 2025-03-13 08:52:22 UTC	Thu 2025-03-13 08:56:00 UTC
-1	a0e1383ce7e14e8eb74f00db077de77e	Thu 2025-03-13 08:56:17 UTC	Thu 2025-03-13 08:59:37 UTC
0	85638f1998eb4cd5bc27632c3522ef04	Thu 2025-03-13 08:59:54 UTC	Thu 2025-03-13 09:02:03 UTC

```
[ec2-user@ip-172-31-81-177 ~]$
```

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`

```
ec2-user@ip-172-31-81-177:~$ nano script.sh
GNU nano 5.6.1 script.sh Modified
#!/bin/bash
echo "This script will fail"
exit 1 # Non-zero exit code triggers failure

ec2-user@ip-172-31-81-177:~$ sudo grep CRON /var/log/cron
Mar 11 08:33:32 ip-172-31-81-177 crond[1339]: (CRON) STARTUP (1.5.7)
Mar 11 08:33:32 ip-172-31-81-177 crond[1339]: (CRON) INFO (Syslog will be used instead of sendmail.)
Mar 11 08:33:32 ip-172-31-81-177 crond[1339]: (CRON) INFO (RANDOM_DELAY will be scaled with factor 46% if used.)
Mar 11 08:33:32 ip-172-31-81-177 crond[1339]: (CRON) INFO (running with inotify support)
Mar 11 09:01:01 ip-172-31-81-177 CROND[4250]: (root) CMD (run-parts /etc/cron.hourly)
Mar 11 09:01:01 ip-172-31-81-177 CROND[4249]: (root) CMDEND (run-parts /etc/cron.hourly)
Mar 11 10:01:01 ip-172-31-81-177 CROND[7380]: (root) CMD (run-parts /etc/cron.hourly)
Mar 11 10:01:01 ip-172-31-81-177 CROND[7379]: (root) CMDEND (run-parts /etc/cron.hourly)
Mar 13 06:53:16 ip-172-31-81-177 crond[1349]: (CRON) STARTUP (1.5.7)
Mar 13 06:53:16 ip-172-31-81-177 crond[1349]: (CRON) INFO (Syslog will be used instead of sendmail.)
Mar 13 06:53:16 ip-172-31-81-177 crond[1349]: (CRON) INFO (RANDOM_DELAY will be scaled with factor 84% if used.)
Mar 13 06:53:16 ip-172-31-81-177 crond[1349]: (CRON) INFO (running with inotify support)
Mar 13 07:01:01 ip-172-31-81-177 CROND[1511]: (root) CMD (run-parts /etc/cron.hourly)
Mar 13 07:01:01 ip-172-31-81-177 CROND[1510]: (root) CMDEND (run-parts /etc/cron.hourly)
Mar 13 08:01:01 ip-172-31-81-177 CROND[1680]: (root) CMD (run-parts /etc/cron.hourly)
Mar 13 08:01:01 ip-172-31-81-177 CROND[1679]: (root) CMDEND (run-parts /etc/cron.hourly)
Mar 13 08:52:30 ip-172-31-81-177 crond[1320]: (CRON) STARTUP (1.5.7)
Mar 13 08:52:30 ip-172-31-81-177 crond[1320]: (CRON) INFO (Syslog will be used instead of sendmail.)
Mar 13 08:52:30 ip-172-31-81-177 crond[1320]: (CRON) INFO (RANDOM_DELAY will be scaled with factor 90% if used.)
Mar 13 08:52:30 ip-172-31-81-177 crond[1320]: (CRON) INFO (running with inotify support)
Mar 13 08:55:59 ip-172-31-81-177 crond[1320]: (CRON) INFO (Shutting down)
Mar 13 08:56:25 ip-172-31-81-177 crond[1315]: (CRON) STARTUP (1.5.7)
Mar 13 08:56:25 ip-172-31-81-177 crond[1315]: (CRON) INFO (Syslog will be used instead of sendmail.)
Mar 13 08:56:25 ip-172-31-81-177 crond[1315]: (CRON) INFO (RANDOM_DELAY will be scaled with factor 39% if used.)
Mar 13 08:56:25 ip-172-31-81-177 crond[1315]: (CRON) INFO (running with inotify support)
Mar 13 08:59:36 ip-172-31-81-177 crond[1315]: (CRON) INFO (Shutting down)
Mar 13 09:00:02 ip-172-31-81-177 crond[1317]: (CRON) STARTUP (1.5.7)
Mar 13 09:00:02 ip-172-31-81-177 crond[1317]: (CRON) INFO (Syslog will be used instead of sendmail.)
Mar 13 09:00:02 ip-172-31-81-177 crond[1317]: (CRON) INFO (RANDOM_DELAY will be scaled with factor 11% if used.)
Mar 13 09:00:02 ip-172-31-81-177 crond[1317]: (CRON) INFO (running with inotify support)
Mar 13 09:01:01 ip-172-31-81-177 CROND[1468]: (root) CMD (run-parts /etc/cron.hourly)
Mar 13 09:01:01 ip-172-31-81-177 CROND[1467]: (root) CMDEND (run-parts /etc/cron.hourly)
ec2-user@ip-172-31-81-177:~$ sudo grep -i "cron" /var/log/cron | grep -i "running"
Mar 11 08:33:32 ip-172-31-81-177 crond[1339]: (CRON) INFO (running with inotify support)
Mar 13 06:53:16 ip-172-31-81-177 crond[1349]: (CRON) INFO (running with inotify support)
Mar 13 08:52:30 ip-172-31-81-177 crond[1320]: (CRON) INFO (running with inotify support)
Mar 13 08:56:25 ip-172-31-81-177 crond[1315]: (CRON) INFO (running with inotify support)
Mar 13 09:00:02 ip-172-31-81-177 crond[1317]: (CRON) INFO (running with inotify support)
ec2-user@ip-172-31-81-177:~$ sudo grep -i "cron" /var/log/cron | grep -i "failed"
ec2-user@ip-172-31-81-177:~$ sudo grep -i "cron" /var/log/cron | grep -i "error"
ec2-user@ip-172-31-81-177:~$

Mar 13 09:19:11 ip-172-31-81-177 crontab[1637]: (ec2-user) END EDIT (ec2-user)
Mar 13 09:19:20 ip-172-31-81-177 crontab[1640]: (ec2-user) LIST (ec2-user)
Mar 13 09:19:30 ip-172-31-81-177 crond[1317]: (CRON) INFO (Shutting down)
Mar 13 09:19:30 ip-172-31-81-177 crond[1646]: (CRON) STARTUP (1.5.7)
Mar 13 09:19:30 ip-172-31-81-177 crond[1646]: (CRON) INFO (Syslog will be used instead of sendmail.)
Mar 13 09:19:30 ip-172-31-81-177 crond[1646]: (CRON) INFO (RANDOM_DELAY will be scaled with factor 91% if used.)
Mar 13 09:19:30 ip-172-31-81-177 crond[1646]: (CRON) INFO (running with inotify support)
Mar 13 09:19:30 ip-172-31-81-177 crond[1646]: (CRON) INFO (@reboot jobs will be run at computer's startup.)
Mar 13 09:20:01 ip-172-31-81-177 CROND[1654]: (ec2-user) CMD (script.sh >> /path/to/logfile.log 1>&1)
Mar 13 09:20:01 ip-172-31-81-177 CROND[1652]: (ec2-user) CMDOUT (/bin/sh: line 1: /path/to/logfile.log: No such file or directory)
Mar 13 09:20:01 ip-172-31-81-177 CROND[1652]: (ec2-user) CMDEND (script.sh >> /path/to/logfile.log 1>&1)
ec2-user@ip-172-31-81-177:~$
```

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/

```
ec2-user@ip-172-31-81-177:~  
[ec2-user@ip-172-31-81-177 ~]$ sudo grep "CustomLog" /etc/httpd/conf/httpd.conf  
# a CustomLog directive (see below).  
#CustomLog "logs/access_log" common  
CustomLog "logs/access_log" combined  
[ec2-user@ip-172-31-81-177 ~]$ sudo ls -l /var/log/httpd/  
total 4  
-rw-r--r--. 1 root root 0 Mar 13 09:28 access_log  
-rw-r--r--. 1 root root 689 Mar 13 09:28 error_log  
[ec2-user@ip-172-31-81-177 ~]$ sudo cat /var/log/httpd/access_log  
[ec2-user@ip-172-31-81-177 ~]$ sudo cat /var/log/httpd/error_log  
[Thu Mar 13 09:28:13.517944 2025] [core:notice] [pid 2087:tid 2087] SELinux policy enabled; httpd running as context system_u:system_r:httpd_t:s0  
[Thu Mar 13 09:28:13.518512 2025] [suexec:notice] [pid 2087:tid 2087] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)  
[Thu Mar 13 09:28:13.529453 2025] [lbmethod:heartbeat:notice] [pid 2087:tid 2087] AH02282: No slotmem from mod_heartbeat  
[Thu Mar 13 09:28:13.539331 2025] [mpm_event:notice] [pid 2087:tid 2087] AH00489: Apache/2.4.62 (Red Hat Enterprise Linux) configured -- resuming normal operations  
[Thu Mar 13 09:28:13.539346 2025] [core:notice] [pid 2087:tid 2087] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'  
[ec2-user@ip-172-31-81-177 ~]$
```

For nginx :

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

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

```
ec2-user@ip-172-31-81-177:~  
[ec2-user@ip-172-31-81-177 ~]$ sudo ls -l /var/log/nginx/  
ls: cannot access '/var/log/nginx/': No such file or directory  
[ec2-user@ip-172-31-81-177 ~]$ sudo ls -l /var/log/nginx/  
total 0  
[ec2-user@ip-172-31-81-177 ~]$ sudo systemctl start nginx  
sudo systemctl enable nginx  
Job for nginx.service failed because the control process exited with error code.  
See "systemctl status nginx.service" and "journalctl -xeu nginx.service" for details.  
Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service -> /usr/lib/systemd/system/nginx.service.  
[ec2-user@ip-172-31-81-177 ~]$ sudo ls -l /var/log/nginx/  
total 4  
-rw-r--r--. 1 root root 0 Mar 13 09:31 access_log  
-rw-r--r--. 1 root root 1007 Mar 13 09:31 error_log  
[ec2-user@ip-172-31-81-177 ~]$ sudo cat /var/log/nginx/access_log  
[ec2-user@ip-172-31-81-177 ~]$ sudo cat /var/log/nginx/error_log  
2025/03/13 09:31:24 [emerg] 2493#2493: bind() to 0.0.0.0:80 failed (98: Address already in use)  
2025/03/13 09:31:24 [emerg] 2493#2493: bind() to [::]:80 failed (98: Address already in use)  
2025/03/13 09:31:24 [emerg] 2493#2493: bind() to 0.0.0.0:80 failed (98: Address already in use)  
2025/03/13 09:31:24 [emerg] 2493#2493: bind() to [::]:80 failed (98: Address already in use)  
2025/03/13 09:31:24 [emerg] 2493#2493: bind() to 0.0.0.0:80 failed (98: Address already in use)  
2025/03/13 09:31:24 [emerg] 2493#2493: bind() to [::]:80 failed (98: Address already in use)  
2025/03/13 09:31:24 [emerg] 2493#2493: bind() to 0.0.0.0:80 failed (98: Address already in use)  
2025/03/13 09:31:24 [emerg] 2493#2493: bind() to [::]:80 failed (98: Address already in use)  
2025/03/13 09:31:24 [emerg] 2493#2493: still could not bind()  
[ec2-user@ip-172-31-81-177 ~]$
```

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

```
manoj@IND-140: ~  
An ExecStart= process belonging to unit postfix@-.service has exited.  
Mar 13 09:53:04 IND-140 systemd[1]: postfix@-.service: Failed with result 'exit-code'.  
The unit postfix@-.service has entered the 'failed' state with result 'exit-code'.  
Mar 13 09:53:04 IND-140 systemd[1]: Failed to start postfix@-.service - Postfix Mail Transport Agent (instance -).  
Subject: A start job for unit postfix@-.service has failed  
A start job for unit postfix@-.service has finished with a failure.  
Mar 13 09:53:04 IND-140 systemd[1]: Starting postfix.service - Postfix Mail Transport Agent...  
Subject: A start job for unit postfix.service has begun execution  
A start job for unit postfix.service has begun execution.  
Mar 13 09:53:04 IND-140 systemd[1]: Finished postfix.service - Postfix Mail Transport Agent.  
Subject: A start job for unit postfix.service has finished successfully  
A start job for unit postfix.service has finished successfully.  
Mar 13 09:53:07 IND-140 sudo[5166]: manoj : TTY=pts/0 ; PWD=/home/manoj ; USER=root ; COMMAND=/usr/sbin/postfix start  
Mar 13 09:53:07 IND-140 postfix[5168]: warning: valid_hostname: misplaced delimiter: IND-140.  
Mar 13 09:53:07 IND-140 postfix[5168]: fatal: file /etc/postfix/main.cf: parameter myhostname: bad parameter value: IND-140.  
Mar 13 09:53:27 IND-140 sudo[5169]: manoj : TTY=pts/0 ; PWD=/home/manoj ; USER=root ; COMMAND=/usr/bin/systemctl status postfix  
Mar 13 09:53:40 IND-140 sudo[5175]: manoj : TTY=pts/0 ; PWD=/home/manoj ; USER=root ; COMMAND=/usr/sbin/postfix start  
Mar 13 09:53:40 IND-140 postfix[5177]: warning: valid_hostname: misplaced delimiter: IND-140.  
Mar 13 09:53:40 IND-140 postfix[5177]: fatal: file /etc/postfix/main.cf: parameter myhostname: bad parameter value: IND-140.  
Mar 13 09:54:19 IND-140 sudo[5181]: manoj : TTY=pts/0 ; PWD=/home/manoj ; USER=root ; COMMAND=/usr/bin/nano /etc/postfix/main.cf  
Mar 13 09:54:43 IND-140 sudo[5184]: manoj : TTY=pts/0 ; PWD=/home/manoj ; USER=root ; COMMAND=/usr/sbin/postfix start  
Mar 13 09:54:44 IND-140 postfix/postfix-script[5430]: starting the Postfix mail system  
Mar 13 09:54:44 IND-140 postfix/master[5432]: daemon started -- version 3.8.6, configuration /etc/postfix  
Mar 13 09:54:49 IND-140 sudo[5435]: manoj : TTY=pts/0 ; PWD=/home/manoj ; USER=root ; COMMAND=/usr/bin/systemctl status postfix  
Mar 13 09:54:53 IND-140 sudo[5439]: manoj : TTY=pts/0 ; PWD=/home/manoj ; USER=root ; COMMAND=/usr/sbin/postfix start  
Mar 13 09:54:53 IND-140 postfix/postfix-script[5447]: fatal: the Postfix mail system is already running  
Mar 13 09:56:14 IND-140 postfix/pickup[5433]: 5ADF1161F5: uid=1000 from=<manoj@IND-140>  
Mar 13 09:56:14 IND-140 postfix/cleanup[5459]: 5ADF1161F5: message-id=<20250313095614.5ADF1161F5@IND-140.manojconnects.space>  
Mar 13 09:56:14 IND-140 postfix/qmgr[5434]: 5ADF1161F5: from=<manoj@IND-140>, size=385, nrcpt=1 (queue active)  
Mar 13 09:56:21 IND-140 postfix/smtp[5461]: 5ADF1161F5: to=<invaliduser@nonexistentdomain.com>, relay=none, delay=7.1, delays=0.05/0.0  
65/6.4/0, dsn=4.4.3, status=deferred (Host or domain name not found. Name service error for name=manojconnects.space type=MX: Host no  
t found, try again)  
manoj@IND-140: ~$
```

```
manoj@IND-140: ~  
manoj@IND-140:~$ sudo tail -f /var/log/mail.log  
Mar 13 09:57:54 IND-140 postfix/postfix-script[5546]: fatal: the Postfix mail system is already running  
Mar 13 09:58:22 IND-140 postfix/cleanup[5572]: C3CE5B3BF: message-id=<20250313095822.C3CE5B3BF@IND-140.manojconnects.space>  
Mar 13 09:58:25 IND-140 postfix/smtp[5574]: C3CE5B3BF: to=<invaliduser@nonexistentdomain.com>, relay=none, delay=3.1, delays=0.05/0.0  
2/3.1/0, dsn=4.4.3, status=deferred (Host or domain name not found. Name service error for name=manojconnects.space type=MX: Host no  
t found, try again)  
|
```

Task 6 :

Checking Kernel and Hardware Issues

Scenario: A sysadmin checks for kernel-related errors after a server crash.

Cmd:

`sudo dmesg -T | less`


```

ec2-user@ip-172-31-81-177:~
[ec2-user@ip-172-31-81-177 ~]$ sudo dmesg -T | less
[Thu Mar 13 08:59:52 2025] Linux version 5.14.0-503.15.1.el9_5.x86_64 (mockbuild@x86-64-03.build.eng.rdu2.redhat.com) (gcc (GCC) 11.5.0 20240719 (Red Hat 11.5.0-2), GNU ld version 2.35.2-54.el9) #1 SMP PREEMPT_DYNAMIC Thu Nov 14 15:45:31 EST 2024
[Thu Mar 13 08:59:52 2025] The list of certified hardware and cloud instances for Red Hat Enterprise Linux 9 can be viewed at the Red Hat Ecosystem Catalog,
https://catalog.redhat.com.
[Thu Mar 13 08:59:52 2025] Command line: BOOT_IMAGE=(hd0,gpt3)/vmlinuz-5.14.0-503.15.1.el9_5.x86_64 root=UUID=425779c6-2665-4aa9-9f7d-12337557e596 console=tty0 console=ttyS0,115200n8 net.ifnames=0 nvme_core.io_timeout=4294967295 crashkernel=1G-4G:192M,4G-64G:256M,64G-512M
[Thu Mar 13 08:59:52 2025] BIOS-provided physical RAM map:
[Thu Mar 13 08:59:52 2025] BIOS-e820: [mem 0x0000000000000000-0x000000000009dfff] usable
[Thu Mar 13 08:59:52 2025] BIOS-e820: [mem 0x000000000009e000-0x000000000009ffff] reserved
[Thu Mar 13 08:59:52 2025] BIOS-e820: [mem 0x00000000000a0000-0x000000000000ffff] reserved
[Thu Mar 13 08:59:52 2025] BIOS-e820: [mem 0x0000000000100000-0x00000000003fffffff] usable
[Thu Mar 13 08:59:52 2025] BIOS-e820: [mem 0x00000000fc000000-0x00000000ffffffff] reserved
[Thu Mar 13 08:59:52 2025] NX (Execute Disable) protection: active
[Thu Mar 13 08:59:52 2025] APIC: Static calls initialized
[Thu Mar 13 08:59:52 2025] SMBIOS 2.7 present.
[Thu Mar 13 08:59:52 2025] DMI: Xen HVM domU, BIOS 4.11.amazon 08/24/2006
[Thu Mar 13 08:59:52 2025] Hypervisor detected: Xen HVM
[Thu Mar 13 08:59:52 2025] Xen version 4.11.
[Thu Mar 13 08:59:52 2025] platform_pci_unregister: Netfront and the Xen platform PCI driver have been compiled for this kernel: unplug emulated NICs.
[Thu Mar 13 08:59:52 2025] platform_pci_unregister: Blkfront and the Xen platform PCI driver have been compiled for this kernel: unplug emulated disks.
You might have to change the root device
from /dev/hd[a-d] to /dev/xvd[a-d]
in your root= kernel command line option
[Thu Mar 13 08:59:52 2025] HVMOP pagetable dying not supported
[Thu Mar 13 08:59:52 2025] tsc: Detected 2299.998 MHz processor
[Thu Mar 13 08:59:52 2025] e820: update [mem 0x00000000-0x0000ffff] usable ==> reserved
[Thu Mar 13 08:59:52 2025] e820: remove [mem 0x000a0000-0x000fffff] usable
[Thu Mar 13 08:59:52 2025] last_pfn = 0x40000 max_arch_pfn = 0x400000000
[Thu Mar 13 08:59:52 2025] MTRR map: 4 entries (3 fixed + 1 variable; max 19), built from 8 variable MTRRs
[Thu Mar 13 08:59:52 2025] x86/PAT Configuration [0-7]: WB WC UC- UC WB WP UC- WT
[Thu Mar 13 08:59:52 2025] found SMP MP-table at [mem 0x000fbb70-0x000fbb7f]
[Thu Mar 13 08:59:52 2025] RAMDISK: [mem 0x2ed7f000-0x336b7fff]
[Thu Mar 13 08:59:52 2025] ACPI: Early table checksum verification disabled
[Thu Mar 13 08:59:52 2025] ACPI: RSDP 0x000000000000EA020 000024 (v02 Xen )
[Thu Mar 13 08:59:52 2025] ACPI: XSDT 0x00000000FC00A250 00005C (v01 Xen HVM 00000000 HVML 00000000)
[Thu Mar 13 08:59:52 2025] ACPI: FACP 0x00000000FC00A150 000074 (v04 Xen HVM 00000000 HVML 00000000)
[Thu Mar 13 08:59:52 2025] ACPI: DSDT 0x00000000FC001000 008A79 (v02 Xen HVM 00000000 HVML 20090123)
[Thu Mar 13 08:59:52 2025] ACPI: FACS 0x00000000FC00A050 000040
[Thu Mar 13 08:59:52 2025] ACPI: FACS 0x00000000FC00A050 000040
[Thu Mar 13 08:59:52 2025] ACPI: SSDT 0x00000000FC009A80 000033 (v02 Xen HVM 00000000 HVML 20090123)
[Thu Mar 13 08:59:52 2025] ACPI: SSDT 0x00000000FC009AC0 000031 (v02 Xen HVM 00000000 HVML 20090123)
[Thu Mar 13 08:59:52 2025] ACPI: APIC 0x00000000FC009B00 0000D8 (v02 Xen HVM 00000000 HVML 00000000)
[Thu Mar 13 08:59:52 2025] ACPI: HPET 0x00000000FC009FE0 000038 (v01 Xen HVM 00000000 HVML 00000000)

```

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
```

```

ec2-user@ip-172-31-81-177:~
[ec2-user@ip-172-31-81-177 ~]$ sudo tail -f /var/log/messages | grep ntp
^C
[ec2-user@ip-172-31-81-177 ~]$ sudo journalctl -u chronyd --no-pager | tail -20 # For Chrony
sudo journalctl -u ntpd --no-pager | tail -20 # For NTPD
-- Boot a0e1383ce7e14e8eb74f00db077de77e --
Mar 13 08:56:21 ip-172-31-81-177.ec2.internal systemd[1]: Starting NTP client/server...
Mar 13 08:56:21 ip-172-31-81-177.ec2.internal chronyd[631]: chronyd version 4.5 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +SCFILTER +SIGND +ASYNCDNS +N
TS +SECHASH +IPV6 +DEBUG)
Mar 13 08:56:21 ip-172-31-81-177.ec2.internal chronyd[631]: Loaded 0 symmetric keys
Mar 13 08:56:21 ip-172-31-81-177.ec2.internal chronyd[631]: Frequency 5.840 +/- 0.536 ppm read from /var/lib/chrony/drift
Mar 13 08:56:21 ip-172-31-81-177.ec2.internal chronyd[631]: Loaded seccomp filter (level 2)
Mar 13 08:56:21 ip-172-31-81-177.ec2.internal systemd[1]: Started NTP client/server.
Mar 13 08:56:28 ip-172-31-81-177.ec2.internal chronyd[631]: Selected source 169.254.169.123
Mar 13 08:59:36 ip-172-31-81-177.ec2.internal chronyd[631]: chronyd exiting
Mar 13 08:59:36 ip-172-31-81-177.ec2.internal systemd[1]: Stopping NTP client/server...
Mar 13 08:59:36 ip-172-31-81-177.ec2.internal systemd[1]: chronyd.service: Deactivated successfully.
Mar 13 08:59:36 ip-172-31-81-177.ec2.internal systemd[1]: Stopped NTP client/server.
-- Boot 0563081990eb4cd50bc7632c3522ef04 --
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal systemd[1]: Starting NTP client/server...
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal chronyd[635]: chronyd version 4.5 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +SCFILTER +SIGND +ASYNCDNS +N
TS +SECHASH +IPV6 +DEBUG)
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal chronyd[635]: Loaded 0 symmetric keys
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal chronyd[635]: Frequency 6.377 +/- 1.755 ppm read from /var/lib/chrony/drift
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal chronyd[635]: Loaded seccomp filter (level 2)
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal systemd[1]: Started NTP client/server.
Mar 13 09:00:05 ip-172-31-81-177.ec2.internal chronyd[635]: Selected source 169.254.169.123
-- No entries --
[ec2-user@ip-172-31-81-177 ~]$

```

```

ec2-user@ip-172-31-81-177:~
Mar 13 08:59:36 ip-172-31-81-177.ec2.internal systemd[1]: chronyd.service: Deactivated successfully.
Mar 13 08:59:36 ip-172-31-81-177.ec2.internal systemd[1]: Stopped NTP client/server.
-- Boot 85638f1998eb4cd5bc27632c3522ef04 --
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal systemd[1]: Starting NTP client/server...
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal chronyd[635]: chronyd version 4.5 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +SCFILTER +SIGND +ASYNCDNS +NTS +SECHASH +IPV6 +DEBUG)
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal chronyd[635]: Loaded 0 symmetric keys
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal chronyd[635]: Frequency 6.377 +/- 1.755 ppm read from /var/lib/chrony/drift
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal chronyd[635]: Loaded seccomp filter (level 2)
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal systemd[1]: Started NTP client/server.
Mar 13 09:00:05 ip-172-31-81-177.ec2.internal chronyd[635]: Selected source 169.254.169.123
[ec2-user@ip-172-31-81-177 ~]$ sudo journalctl -u chronyd
Mar 13 08:52:26 ip-172-31-81-177.ec2.internal systemd[1]: Starting NTP client/server...
Mar 13 08:52:26 ip-172-31-81-177.ec2.internal chronyd[636]: chronyd version 4.5 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +SCFILTER +SIGND +ASYNCDNS +NTS +SECHASH +IPV6 +DEBUG)
Mar 13 08:52:26 ip-172-31-81-177.ec2.internal chronyd[636]: Loaded 0 symmetric keys
Mar 13 08:52:26 ip-172-31-81-177.ec2.internal chronyd[636]: Frequency 5.803 +/- 0.037 ppm read from /var/lib/chrony/drift
Mar 13 08:52:26 ip-172-31-81-177.ec2.internal chronyd[636]: Loaded seccomp filter (level 2)
Mar 13 08:52:26 ip-172-31-81-177.ec2.internal systemd[1]: Started NTP client/server.
Mar 13 08:52:33 ip-172-31-81-177.ec2.internal chronyd[636]: Selected source 169.254.169.123
Mar 13 08:55:59 ip-172-31-81-177.ec2.internal chronyd[636]: chronyd exiting
Mar 13 08:55:59 ip-172-31-81-177.ec2.internal systemd[1]: Stopping NTP client/server...
Mar 13 08:55:59 ip-172-31-81-177.ec2.internal systemd[1]: chronyd.service: Deactivated successfully.
Mar 13 08:55:59 ip-172-31-81-177.ec2.internal systemd[1]: Stopped NTP client/server.
-- Boot a0e1383ce7e14e8eb74f00db077de77e --
Mar 13 08:56:21 ip-172-31-81-177.ec2.internal systemd[1]: Starting NTP client/server...
Mar 13 08:56:21 ip-172-31-81-177.ec2.internal chronyd[631]: chronyd version 4.5 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +SCFILTER +SIGND +ASYNCDNS +NTS +SECHASH +IPV6 +DEBUG)
Mar 13 08:56:21 ip-172-31-81-177.ec2.internal chronyd[631]: Loaded 0 symmetric keys
Mar 13 08:56:21 ip-172-31-81-177.ec2.internal chronyd[631]: Frequency 5.840 +/- 0.536 ppm read from /var/lib/chrony/drift
Mar 13 08:56:21 ip-172-31-81-177.ec2.internal chronyd[631]: Loaded seccomp filter (level 2)
Mar 13 08:56:21 ip-172-31-81-177.ec2.internal systemd[1]: Started NTP client/server.
Mar 13 08:56:28 ip-172-31-81-177.ec2.internal chronyd[631]: Selected source 169.254.169.123
Mar 13 08:59:36 ip-172-31-81-177.ec2.internal chronyd[631]: chronyd exiting
Mar 13 08:59:36 ip-172-31-81-177.ec2.internal systemd[1]: Stopping NTP client/server...
Mar 13 08:59:36 ip-172-31-81-177.ec2.internal systemd[1]: chronyd.service: Deactivated successfully.
Mar 13 08:59:36 ip-172-31-81-177.ec2.internal systemd[1]: Stopped NTP client/server.
-- Boot 85638f1998eb4cd5bc27632c3522ef04 --
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal systemd[1]: Starting NTP client/server...
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal chronyd[635]: chronyd version 4.5 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +SCFILTER +SIGND +ASYNCDNS +NTS +SECHASH +IPV6 +DEBUG)
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal chronyd[635]: Loaded 0 symmetric keys
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal chronyd[635]: Frequency 6.377 +/- 1.755 ppm read from /var/lib/chrony/drift
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal chronyd[635]: Loaded seccomp filter (level 2)
Mar 13 08:59:58 ip-172-31-81-177.ec2.internal systemd[1]: Started NTP client/server.
Mar 13 09:00:05 ip-172-31-81-177.ec2.internal chronyd[635]: Selected source 169.254.169.123

```

Task 8:

Execute all the log path according to your operating system assigned

Cmd:

General message : cat /var/log/message

```

root@ip-172-31-81-177:~
[root@ip-172-31-81-177 ~]# tail -n 10 cat /var/log/messages
tail: cannot open 'cat' for reading: No such file or directory
==> /var/log/messages <==
Mar 13 10:16:01 ip-172-31-81-177 systemd[1]: Started Session 69 of User ec2-user.
Mar 13 10:16:01 ip-172-31-81-177 systemd[1]: session-69.scope: Deactivated successfully.
Mar 13 10:17:02 ip-172-31-81-177 systemd[1]: Started Session 70 of User ec2-user.
Mar 13 10:17:02 ip-172-31-81-177 systemd[1]: session-70.scope: Deactivated successfully.
Mar 13 10:17:33 ip-172-31-81-177 su[3030]: (to root) root on pts/0
Mar 13 10:17:33 ip-172-31-81-177 systemd[1]: Starting Hostname Service...
Mar 13 10:17:33 ip-172-31-81-177 systemd[1]: Started Hostname Service.
Mar 13 10:18:01 ip-172-31-81-177 systemd[1]: Started Session 71 of User ec2-user.
Mar 13 10:18:01 ip-172-31-81-177 systemd[1]: session-71.scope: Deactivated successfully.
Mar 13 10:18:03 ip-172-31-81-177 systemd[1]: systemd-hostnamed.service: Deactivated successfully.
[root@ip-172-31-81-177 ~]#

```

Kernel logs : dmesg | tail -n 5

```
root@ip-172-31-81-177:~  
[root@ip-172-31-81-177 ~]# dmesg | tail -n 5  
[ 10.771319] block xvda: the capability attribute has been deprecated.  
[ 1672.910017] systemd-rc-local-generator[1824]: /etc/rc.d/rc.local is not ma  
rked executable, skipping.  
[ 1700.837549] systemd-rc-local-generator[2282]: /etc/rc.d/rc.local is not ma  
rked executable, skipping.  
[ 1855.132216] systemd-rc-local-generator[2400]: /etc/rc.d/rc.local is not ma  
rked executable, skipping.  
[ 1894.790165] systemd-rc-local-generator[2511]: /etc/rc.d/rc.local is not ma  
rked executable, skipping.  
[root@ip-172-31-81-177 ~]#
```

Boot logs : journalctl -b

```
root@ip-172-31-81-177:~  
[root@ip-172-31-81-177 ~]# tail -n 10 journalctl -b  
tail: invalid option -- 'b'  
Try 'tail --help' for more information.  
[root@ip-172-31-81-177 ~]# journalctl -b | tail -  
Mar 13 10:20:01 ip-172-31-81-177.ec2.internal CROND[3073]: (ec2-user) CMDEND  
(script.sh >> /path/to/logfile.log 1>&1)  
Mar 13 10:20:01 ip-172-31-81-177.ec2.internal systemd[1]: session-73.scope: D  
eactivated successfully.  
Mar 13 10:20:06 ip-172-31-81-177.ec2.internal systemd[1]: Starting Automatica  
lly configure NetworkManager in cloud...  
Mar 13 10:20:06 ip-172-31-81-177.ec2.internal systemd[1]: nm-cloud-setup.serv  
ice: Deactivated successfully.  
Mar 13 10:20:06 ip-172-31-81-177.ec2.internal systemd[1]: Finished Automatica  
lly configure NetworkManager in cloud.  
Mar 13 10:21:01 ip-172-31-81-177.ec2.internal systemd[1]: Started Session 74  
of User ec2-user.  
Mar 13 10:21:01 ip-172-31-81-177.ec2.internal CROND[3093]: (ec2-user) CMD (sc  
ript.sh >> /path/to/logfile.log 1>&1)  
Mar 13 10:21:01 ip-172-31-81-177.ec2.internal CROND[3091]: (ec2-user) CMDOUT  
(/bin/sh: line 1: /path/to/logfile.log: No such file or directory)  
Mar 13 10:21:01 ip-172-31-81-177.ec2.internal CROND[3091]: (ec2-user) CMDEND  
(script.sh >> /path/to/logfile.log 1>&1)  
Mar 13 10:21:01 ip-172-31-81-177.ec2.internal systemd[1]: session-74.scope: D  
eactivated successfully.  
[root@ip-172-31-81-177 ~]#
```

Authentication

Logs

> cat /var/log/secure


```
root@ip-172-31-81-177:~  
[root@ip-172-31-81-177 ~]# cat /var/log/secure | tail -5  
Mar 13 10:10:37 ip-172-31-81-177 sudo[2982]: pam_unix(sudo:session): session  
opened for user root(uid=0) by ec2-user(uid=1000)  
Mar 13 10:17:15 ip-172-31-81-177 sudo[2982]: pam_unix(sudo:session): session  
closed for user root  
Mar 13 10:17:33 ip-172-31-81-177 sudo[3028]: ec2-user : TTY=pts/0 ; PWD=/home  
/ec2-user ; USER=root ; COMMAND=/bin/su -  
Mar 13 10:17:33 ip-172-31-81-177 sudo[3028]: pam_unix(sudo:session): session  
opened for user root(uid=0) by ec2-user(uid=1000)  
Mar 13 10:17:33 ip-172-31-81-177 su[3030]: pam_unix(su-l:session): session op  
ened for user root(uid=0) by ec2-user(uid=0)  
[root@ip-172-31-81-177 ~]#
```

Mail Logs :

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

```
manoj@IND-140:~$ sudo tail -f /var/log/mail.log  
[sudo] password for manoj:  
Mar 13 09:57:54 IND-140 postfix/postfix-script[5546]: fatal: the Postfix mail system is already running  
Mar 13 09:58:22 IND-140 postfix/cleanup[5572]: C3CE5B3BF: message-id=<20250313095822.C3CE5B3BF@IND-140.manojconnects.space>  
Mar 13 09:58:25 IND-140 postfix/smtp[5574]: C3CE5B3BF: to=<invaliduser@nonexistentdomain.com>, relay=none, delay=3.1, delays=0.05/0.0  
2/3.1/0, dsn=4.4.3, status=deferred (Host or domain name not found. Name service error for name=manojconnects.space type=MX: Host not  
found, try again)  
Mar 13 10:04:47 IND-140 postfix/smtp[5598]: 5ADF1161F5: to=<invaliduser@nonexistentdomain.com>, relay=none, delay=514, delays=512/0.0  
3/1.3/0, dsn=4.4.3, status=deferred (Host or domain name not found. Name service error for name=manojconnects.space type=MX: Host not  
found, try again)  
Mar 13 10:04:47 IND-140 postfix/smtp[5599]: C3CE5B3BF: to=<invaliduser@nonexistentdomain.com>, relay=none, delay=385, delays=384/0.04  
/1.2/0, dsn=4.4.3, status=deferred (Host or domain name not found. Name service error for name=manojconnects.space type=MX: Host not  
found, try again)  
Mar 13 10:14:48 IND-140 postfix/smtp[5621]: 5ADF1161F5: to=<invaliduser@nonexistentdomain.com>, relay=none, delay=1114, delays=1113/0  
.03/1.2/0, dsn=4.4.3, status=deferred (Host or domain name not found. Name service error for name=manojconnects.space type=MX: Host n  
ot found, try again)  
Mar 13 10:14:48 IND-140 postfix/smtp[5622]: C3CE5B3BF: to=<invaliduser@nonexistentdomain.com>, relay=none, delay=985, delays=984/0.03  
/1.2/0, dsn=4.4.3, status=deferred (Host or domain name not found. Name service error for name=manojconnects.space type=MX: Host not  
found, try again)
```

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 ~]#
```