CLOUD OPERATIONS MONITORING & INCIDENT RESPONSE SIMULATION

Abstract

Modern IT infrastructures generate continuous streams of system metrics and logs that are essential for maintaining operational stability. In many organizations, a lack of proper monitoring and log analysis results in delayed incident detection and reactive troubleshooting. This project simulates real-world **Cloud Operations (CloudOps)** practices by monitoring system resources, analyzing logs, identifying abnormal behavior, and documenting incidents and recovery procedures. The project emphasizes the core DevOps principle of **"monitor first, fix later."**

1. Introduction

Cloud computing environments require continuous visibility into system behavior to ensure reliability, performance, and availability. Without proper monitoring, IT teams are forced to react blindly to incidents, increasing downtime and operational risk.

This project is designed to provide hands-on experience in Cloud Operations by simulating monitoring and incident response tasks on a cloud-based virtual machine. The focus is on understanding how systems behave under normal and abnormal conditions using basic, freely available tools.

2. Problem Statement

The organization has deployed infrastructure but lacks sufficient visibility into system performance and operational health. When incidents occur, the IT team does not have access to adequate logs or metrics, leading to inefficient troubleshooting. Management requires improved monitoring practices and faster incident analysis to reduce downtime and improve system reliability.

3. Project Objectives

The objectives of this project are:

- To observe system resource usage such as CPU, memory, disk, and processes
- To collect and analyze system and authentication logs
- To identify abnormal system behavior such as CPU spikes and unusual access patterns
- To document incidents, root causes, and corrective actions
- To simulate downtime and recovery procedures

4. Scope of the Project

This project focuses on basic CloudOps monitoring and incident response using free and built-in tools. Advanced features such as automated alerting and paid monitoring platforms are intentionally excluded to emphasize fundamental concepts.

5. Constraints and Assumptions

- No paid monitoring or logging tools are used
- Log analysis is manual or basic
- Real-time alerting is not required
- The primary goal is understanding system behavior
- Proper documentation is mandatory

6. Background Theory

6.1 Cloud Operations (CloudOps)

Cloud Operations refers to the practices involved in managing cloud infrastructure to ensure availability, performance, and security. Key CloudOps activities include monitoring, log analysis, incident response, and system optimization.

6.2 Monitoring

Monitoring involves tracking system metrics such as CPU utilization, memory usage, disk space, and running processes. Continuous monitoring helps detect anomalies before they escalate into major incidents.

6.3 Logging

Logs provide a historical record of system events, user activities, and errors. Log analysis is critical for troubleshooting issues and identifying security incidents.

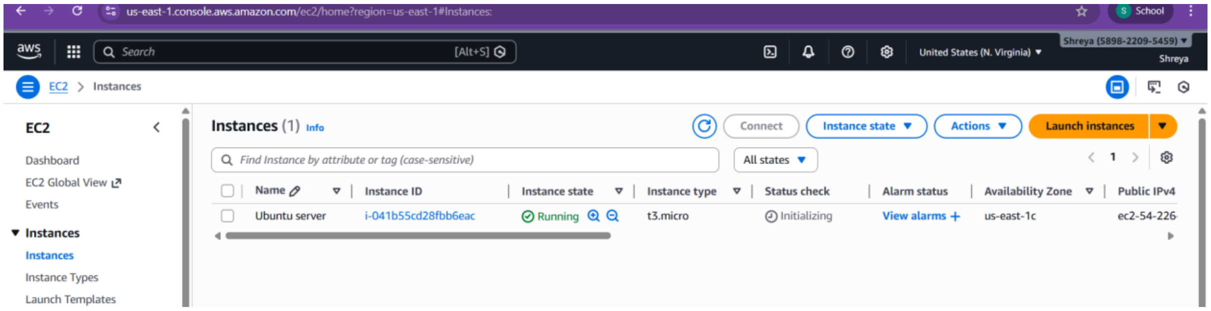
6.4 Incident Response

Incident response is a structured approach to handling unexpected events. It includes detection, analysis, containment, resolution, and recovery.

7. Environment Setup

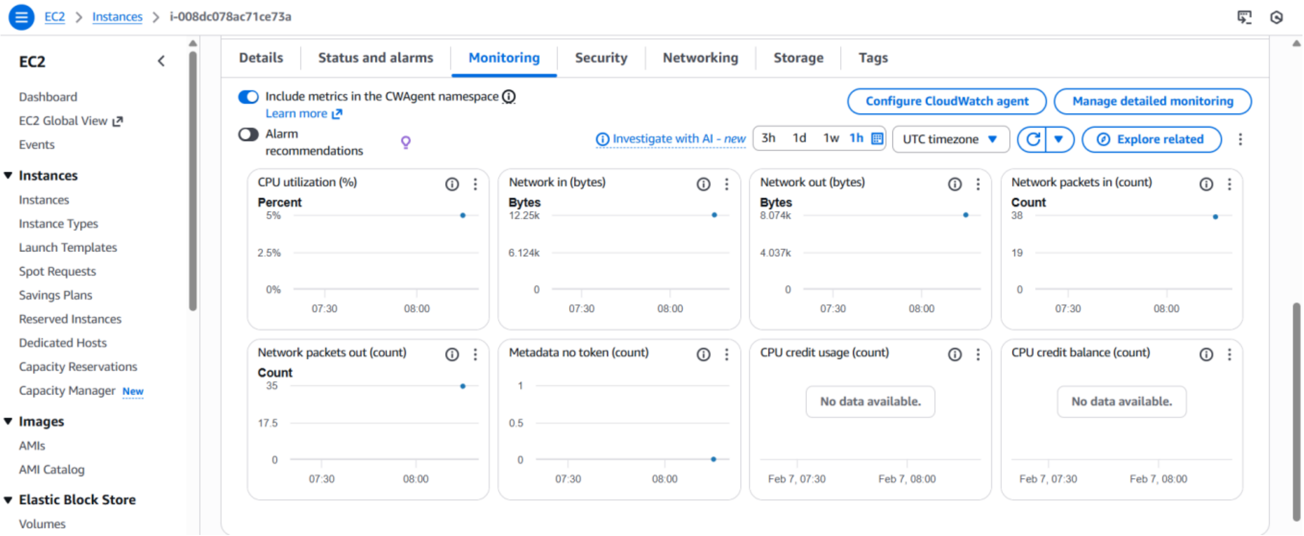
7.1 Cloud Platform

- Platform Used: Amazon Web Services (AWS)
- Service: EC2 (Elastic Compute Cloud)
- Instance Type: Free Tier (t2.micro / t3.micro)
- Operating System: Ubuntu Linux



Instances (1) Info

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
☐	Ubuntu server	i-041b55cd28fbb6eac	✓ Running	t3.micro	Initializing	View alarms +	us-east-1c	ec2-54-226-



7.2 System Preparation

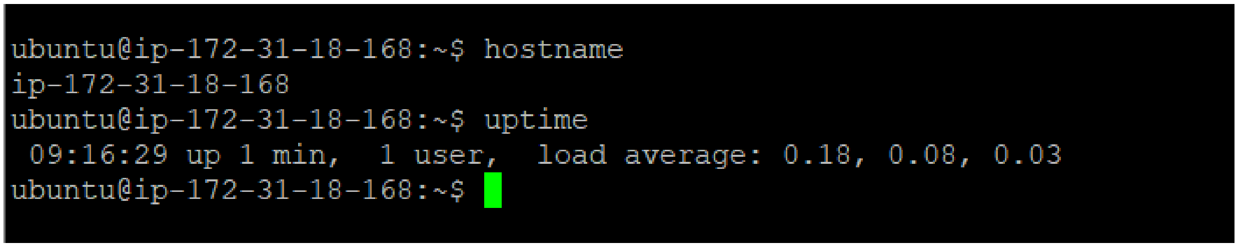
The instance was updated and necessary tools were installed.

```
sudo apt update && sudo apt upgrade -y
sudo apt install htop stress-ng -y
```

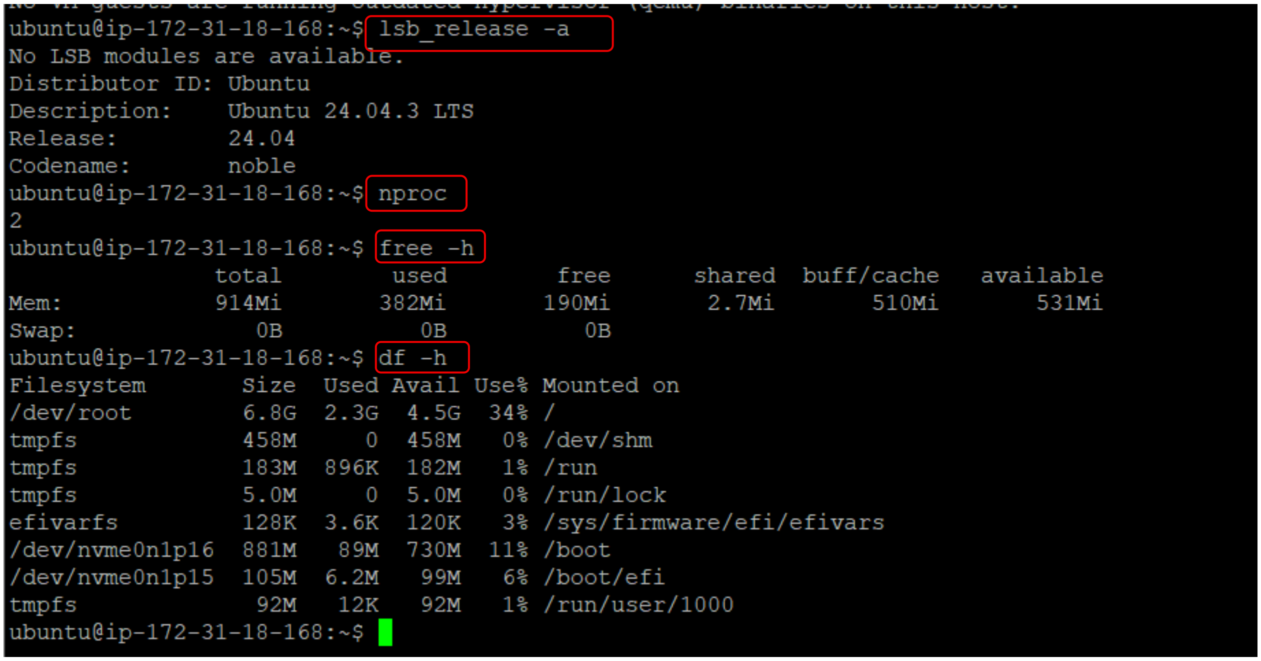
8. Baseline Monitoring (Normal System State)

8.1 Commands Used

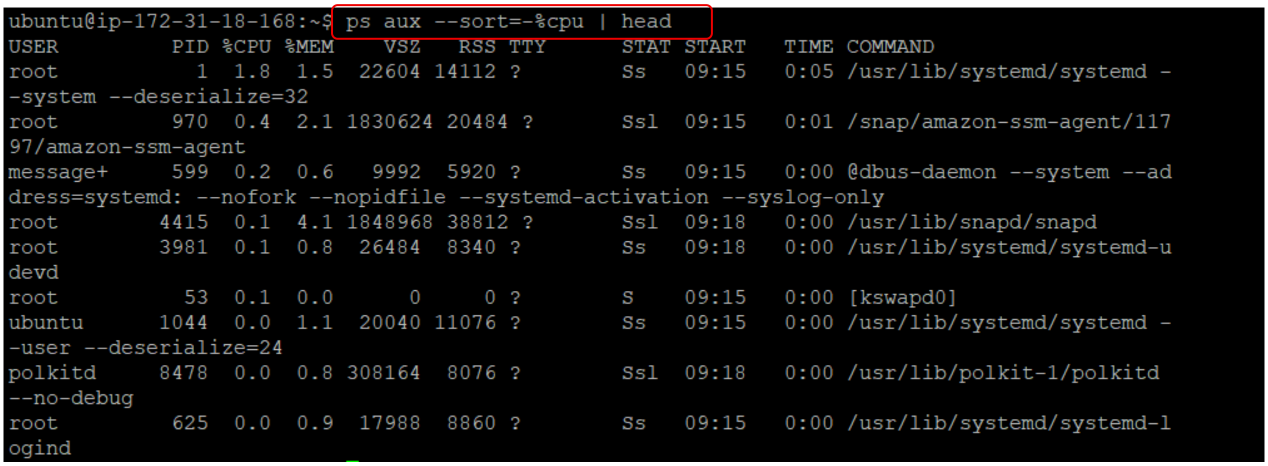
```
hostname
uptime
free -h
df -h
ps aux --sort=-%cpu | head
```



```
ubuntu@ip-172-31-18-168:~$ hostname
ip-172-31-18-168
ubuntu@ip-172-31-18-168:~$ uptime
 09:16:29 up 1 min,  1 user,  load average: 0.18, 0.08, 0.03
ubuntu@ip-172-31-18-168:~$ 
```



```
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-18-168:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 24.04.3 LTS
Release:        24.04
Codename:       noble
ubuntu@ip-172-31-18-168:~$ nproc
2
ubuntu@ip-172-31-18-168:~$ free -h
              total        used        free      shared  buff/cache   available
Mem:          914Mi       382Mi       190Mi       2.7Mi       510Mi       531Mi
Swap:            0B          0B          0B
ubuntu@ip-172-31-18-168:~$ df -h
Filesystem       Size  Used Avail Use% Mounted on
/dev/root        6.8G  2.3G  4.5G  34% /
tmpfs            458M     0  458M   0% /dev/shm
tmpfs            183M  896K  182M   1% /run
tmpfs            5.0M     0  5.0M   0% /run/lock
efivarfs         128K  3.6K  120K   3% /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-172-31-18-168:~$
```



```
ubuntu@ip-172-31-18-168:~$ ps aux --sort=-%cpu | head
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  1.8  1.5  22604 14112 ?        Ss   09:15   0:05 /usr/lib/systemd/systemd -
-system --deserialize=32
root         970  0.4  2.1 1830624 20484 ?       Ssl  09:15   0:01 /snap/amazon-ssm-agent/117
97/amazon-ssm-agent
message+     599  0.2  0.6   9992  5920 ?        Ss   09:15   0:00 @dbus-daemon --system --ad
dress=systemd: --nofork --nopidfile --systemd-activation --syslog-only
root        4415  0.1  4.1 1848968 38812 ?       Ssl  09:18   0:00 /usr/lib/snapd/snapd
root        3981  0.1  0.8  26484  8340 ?        Ss   09:18   0:00 /usr/lib/systemd/systemd-u
devd
root          53  0.1  0.0      0     0 ?        S    09:15   0:00 [kswapd0]
ubuntu      1044  0.0  1.1  20040 11076 ?        Ss   09:15   0:00 /usr/lib/systemd/systemd -
-user --deserialize=24
polkitd     8478  0.0  0.8 308164  8076 ?        Ssl  09:18   0:00 /usr/lib/polkit-1/polkitd
--no-debug
root         625  0.0  0.9  17988  8860 ?        Ss   09:15   0:00 /usr/lib/systemd/systemd-l
ogind
```

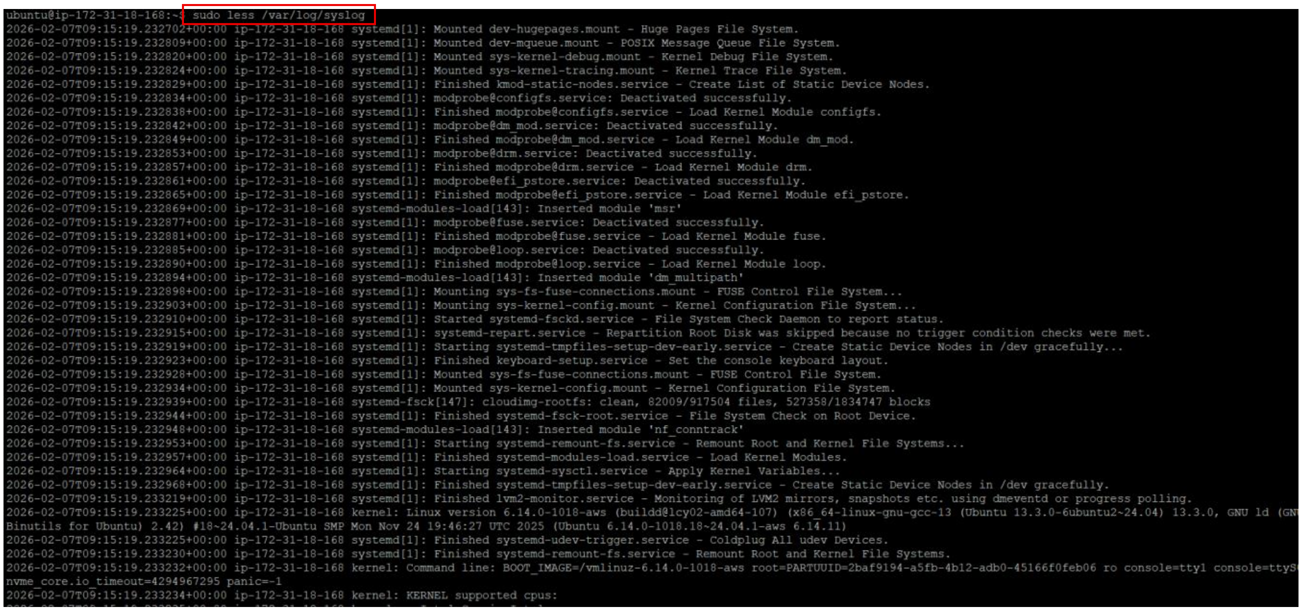
8.2 Observations

- CPU usage was low
- Memory usage was stable
- Disk utilization was within acceptable limits
- No abnormal or high-CPU processes were observed

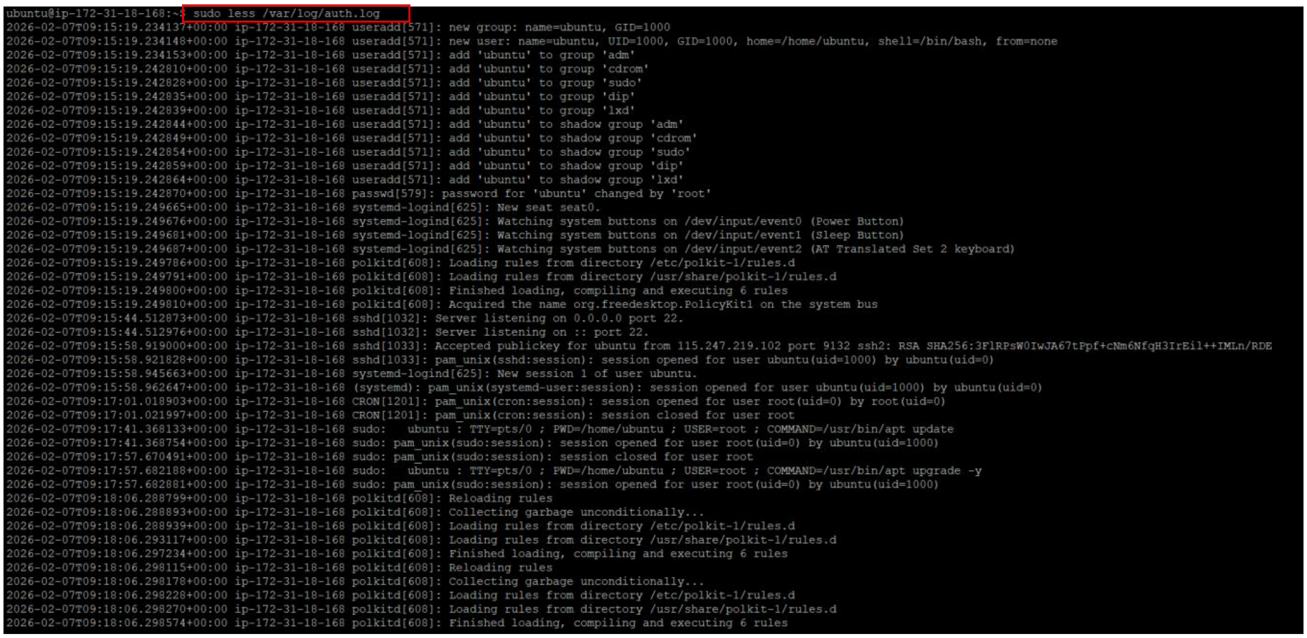
9. Log Collection and Analysis

9.1 Commands Used

```
sudo less /var/log/syslog
sudo less /var/log/auth.log
journalctl -xe
```



```
ubuntu@ip-172-31-18-168:~$ sudo less /var/log/syslog
2026-02-07T09:15:19.232702+00:00 ip-172-31-18-168 systemd[1]: Mounted dev-hugepages.mount - Huge Pages File System.
2026-02-07T09:15:19.232809+00:00 ip-172-31-18-168 systemd[1]: Mounted dev-mqueue.mount - POSIX Message Queue File System.
2026-02-07T09:15:19.232820+00:00 ip-172-31-18-168 systemd[1]: Mounted sys-kernel-debug.mount - Kernel Debug File System.
2026-02-07T09:15:19.232824+00:00 ip-172-31-18-168 systemd[1]: Mounted sys-kernel-tracing.mount - Kernel Trace File System.
2026-02-07T09:15:19.232829+00:00 ip-172-31-18-168 systemd[1]: Finished kmod-static-nodes.service - Create List of Static Device Nodes.
2026-02-07T09:15:19.232834+00:00 ip-172-31-18-168 systemd[1]: modprobe@configfs.service: Deactivated successfully.
2026-02-07T09:15:19.232838+00:00 ip-172-31-18-168 systemd[1]: Finished modprobe@configfs.service - Load Kernel Module configfs.
2026-02-07T09:15:19.232842+00:00 ip-172-31-18-168 systemd[1]: modprobe@dm_mod.service: Deactivated successfully.
2026-02-07T09:15:19.232849+00:00 ip-172-31-18-168 systemd[1]: Finished modprobe@dm_mod.service - Load Kernel Module dm_mod.
2026-02-07T09:15:19.232853+00:00 ip-172-31-18-168 systemd[1]: modprobe@drm.service: Deactivated successfully.
2026-02-07T09:15:19.232857+00:00 ip-172-31-18-168 systemd[1]: Finished modprobe@drm.service - Load Kernel Module drm.
2026-02-07T09:15:19.232861+00:00 ip-172-31-18-168 systemd[1]: modprobe@efi_pstore.service: Deactivated successfully.
2026-02-07T09:15:19.232865+00:00 ip-172-31-18-168 systemd[1]: Finished modprobe@efi_pstore.service - Load Kernel Module efi_pstore.
2026-02-07T09:15:19.232869+00:00 ip-172-31-18-168 systemd-modules-load[143]: Inserted module 'msr'
2026-02-07T09:15:19.232877+00:00 ip-172-31-18-168 systemd[1]: modprobe@fuse.service: Deactivated successfully.
2026-02-07T09:15:19.232881+00:00 ip-172-31-18-168 systemd[1]: Finished modprobe@fuse.service - Load Kernel Module fuse.
2026-02-07T09:15:19.232885+00:00 ip-172-31-18-168 systemd[1]: modprobe@loop.service: Deactivated successfully.
2026-02-07T09:15:19.232890+00:00 ip-172-31-18-168 systemd[1]: Finished modprobe@loop.service - Load Kernel Module loop.
2026-02-07T09:15:19.232894+00:00 ip-172-31-18-168 systemd-modules-load[143]: Inserted module 'dm_multipath'
2026-02-07T09:15:19.232898+00:00 ip-172-31-18-168 systemd[1]: Mounting sys-fs-fuse-connections.mount - FUSE Control File System...
2026-02-07T09:15:19.232903+00:00 ip-172-31-18-168 systemd[1]: Mounting sys-kernel-config.mount - Kernel Configuration File System...
2026-02-07T09:15:19.232910+00:00 ip-172-31-18-168 systemd[1]: Started systemd-fsckd.service - File System Check Daemon to report status.
2026-02-07T09:15:19.232915+00:00 ip-172-31-18-168 systemd[1]: systemd-repart.service - Repartition Root Disk was skipped because no trigger condition checks were met.
2026-02-07T09:15:19.232919+00:00 ip-172-31-18-168 systemd[1]: Starting systemd-tmpfiles-setup-dev-early.service - Create Static Device Nodes in /dev gracefully...
2026-02-07T09:15:19.232923+00:00 ip-172-31-18-168 systemd[1]: Finished keyboard-setup.service - Set the console keyboard layout.
2026-02-07T09:15:19.232928+00:00 ip-172-31-18-168 systemd[1]: Mounted sys-fs-fuse-connections.mount - FUSE Control File System.
2026-02-07T09:15:19.232934+00:00 ip-172-31-18-168 systemd[1]: Mounted sys-kernel-config.mount - Kernel Configuration File System.
2026-02-07T09:15:19.232939+00:00 ip-172-31-18-168 systemd-fsck[147]: cloudimg-rootfs: clean, 82009/917504 files, 527358/1834747 blocks
2026-02-07T09:15:19.232944+00:00 ip-172-31-18-168 systemd[1]: Finished systemd-fsck-root.service - File System Check on Root Device.
2026-02-07T09:15:19.232948+00:00 ip-172-31-18-168 systemd-modules-load[143]: Inserted module 'nf_conntrack'
2026-02-07T09:15:19.232953+00:00 ip-172-31-18-168 systemd[1]: Starting systemd-remount-fs.service - Remount Root and Kernel File Systems...
2026-02-07T09:15:19.232957+00:00 ip-172-31-18-168 systemd[1]: Finished systemd-modules-load.service - Load Kernel Modules.
2026-02-07T09:15:19.232964+00:00 ip-172-31-18-168 systemd[1]: Starting systemd-sysctl.service - Apply Kernel Variables...
2026-02-07T09:15:19.232968+00:00 ip-172-31-18-168 systemd[1]: Finished systemd-tmpfiles-setup-dev-early.service - Create Static Device Nodes in /dev gracefully.
2026-02-07T09:15:19.233219+00:00 ip-172-31-18-168 systemd[1]: Finished lvm2-monitor.service - Monitoring of LVM2 mirrors, snapshots etc. using dmeventd or progress polling.
2026-02-07T09:15:19.233225+00:00 ip-172-31-18-168 kernel: Linux version 6.14.0-1018-aws (buildd@lcy02-amd64-107) (x86_64-linux-gnu-gcc-13 (Ubuntu 13.3.0-6ubuntu2~24.04) 13.3.0, GNU ld (GN
Binutils for Ubuntu) 2.42) #18~24.04.1-Ubuntu SMP Mon Nov 24 19:46:27 UTC 2025 (Ubuntu 6.14.0-1018.18~24.04.1-aws 6.14.11)
2026-02-07T09:15:19.233225+00:00 ip-172-31-18-168 systemd[1]: Finished systemd-udev-trigger.service - Coldplug All udev Devices.
2026-02-07T09:15:19.233230+00:00 ip-172-31-18-168 systemd[1]: Finished systemd-remount-fs.service - Remount Root and Kernel File Systems.
2026-02-07T09:15:19.233232+00:00 ip-172-31-18-168 kernel: Command line: BOOT_IMAGE=/vmlinuz-6.14.0-1018-aws root=PARTUUID=2baf9194-a5fb-4b12-adb0-45166f0feb06 ro console=tty1 console=ttyS
nvme_core.io_timeout=4294967295 panic=-1
2026-02-07T09:15:19.233234+00:00 ip-172-31-18-168 kernel: KERNEL supported cpus:
```



```
ubuntu@ip-172-31-18-168:~$ sudo less /var/log/auth.log
2026-02-07T09:15:19.234137+00:00 ip-172-31-18-168 useradd[571]: new group: name=ubuntu, GID=1000
2026-02-07T09:15:19.234148+00:00 ip-172-31-18-168 useradd[571]: new user: name=ubuntu, UID=1000, GID=1000, home=/home/ubuntu, shell=/bin/bash, from=none
2026-02-07T09:15:19.234153+00:00 ip-172-31-18-168 useradd[571]: add 'ubuntu' to group 'adm'
2026-02-07T09:15:19.242810+00:00 ip-172-31-18-168 useradd[571]: add 'ubuntu' to group 'cdrom'
2026-02-07T09:15:19.242828+00:00 ip-172-31-18-168 useradd[571]: add 'ubuntu' to group 'sudo'
2026-02-07T09:15:19.242835+00:00 ip-172-31-18-168 useradd[571]: add 'ubuntu' to group 'dip'
2026-02-07T09:15:19.242839+00:00 ip-172-31-18-168 useradd[571]: add 'ubuntu' to group 'lxd'
2026-02-07T09:15:19.242844+00:00 ip-172-31-18-168 useradd[571]: add 'ubuntu' to shadow group 'adm'
2026-02-07T09:15:19.242849+00:00 ip-172-31-18-168 useradd[571]: add 'ubuntu' to shadow group 'cdrom'
2026-02-07T09:15:19.242854+00:00 ip-172-31-18-168 useradd[571]: add 'ubuntu' to shadow group 'sudo'
2026-02-07T09:15:19.242859+00:00 ip-172-31-18-168 useradd[571]: add 'ubuntu' to shadow group 'dip'
2026-02-07T09:15:19.242864+00:00 ip-172-31-18-168 useradd[571]: add 'ubuntu' to shadow group 'lxd'
2026-02-07T09:15:19.242870+00:00 ip-172-31-18-168 passwd[579]: password for 'ubuntu' changed by 'root'
2026-02-07T09:15:19.249665+00:00 ip-172-31-18-168 systemd-logind[625]: New seat seat0.
2026-02-07T09:15:19.249676+00:00 ip-172-31-18-168 systemd-logind[625]: Watching system buttons on /dev/input/event0 (Power Button)
2026-02-07T09:15:19.249681+00:00 ip-172-31-18-168 systemd-logind[625]: Watching system buttons on /dev/input/event1 (Sleep Button)
2026-02-07T09:15:19.249687+00:00 ip-172-31-18-168 systemd-logind[625]: Watching system buttons on /dev/input/event2 (AT Translated Set 2 keyboard)
2026-02-07T09:15:19.249786+00:00 ip-172-31-18-168 polkitd[608]: Loading rules from directory /etc/polkit-1/rules.d
2026-02-07T09:15:19.249791+00:00 ip-172-31-18-168 polkitd[608]: Loading rules from directory /usr/share/polkit-1/rules.d
2026-02-07T09:15:19.249800+00:00 ip-172-31-18-168 polkitd[608]: Finished loading, compiling and executing 6 rules
2026-02-07T09:15:19.249810+00:00 ip-172-31-18-168 polkitd[608]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
2026-02-07T09:15:44.512873+00:00 ip-172-31-18-168 sshd[1032]: Server listening on 0.0.0.0 port 22.
2026-02-07T09:15:44.512976+00:00 ip-172-31-18-168 sshd[1032]: Server listening on :: port 22.
2026-02-07T09:15:58.919000+00:00 ip-172-31-18-168 sshd[1033]: Accepted publickey for ubuntu from 115.247.219.102 port 9132 ssh2: RSA SHA256:3FlRPsW0IwJA67tPpf+cNm6NfqH3IrEil++IMLn/RDE
2026-02-07T09:15:58.921828+00:00 ip-172-31-18-168 sshd[1033]: pam_unix(sshd:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
2026-02-07T09:15:58.945663+00:00 ip-172-31-18-168 systemd-logind[625]: New session 1 of user ubuntu.
2026-02-07T09:15:58.962647+00:00 ip-172-31-18-168 (systemd): pam_unix(systemd-user:session): session opened for user ubuntu(uid=1000) by ubuntu(uid=0)
2026-02-07T09:17:01.018903+00:00 ip-172-31-18-168 CRON[1201]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2026-02-07T09:17:01.021997+00:00 ip-172-31-18-168 CRON[1201]: pam_unix(cron:session): session closed for user root
2026-02-07T09:17:41.368133+00:00 ip-172-31-18-168 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/apt update
2026-02-07T09:17:41.368754+00:00 ip-172-31-18-168 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu(uid=1000)
2026-02-07T09:17:57.670491+00:00 ip-172-31-18-168 sudo: pam_unix(sudo:session): session closed for user root
2026-02-07T09:17:57.682188+00:00 ip-172-31-18-168 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/apt upgrade -y
2026-02-07T09:17:57.682881+00:00 ip-172-31-18-168 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ubuntu(uid=1000)
2026-02-07T09:18:06.288799+00:00 ip-172-31-18-168 polkitd[608]: Reloading rules
2026-02-07T09:18:06.288893+00:00 ip-172-31-18-168 polkitd[608]: Collecting garbage unconditionally...
2026-02-07T09:18:06.288939+00:00 ip-172-31-18-168 polkitd[608]: Loading rules from directory /etc/polkit-1/rules.d
2026-02-07T09:18:06.293117+00:00 ip-172-31-18-168 polkitd[608]: Loading rules from directory /usr/share/polkit-1/rules.d
2026-02-07T09:18:06.297234+00:00 ip-172-31-18-168 polkitd[608]: Finished loading, compiling and executing 6 rules
2026-02-07T09:18:06.298115+00:00 ip-172-31-18-168 polkitd[608]: Reloading rules
2026-02-07T09:18:06.298178+00:00 ip-172-31-18-168 polkitd[608]: Collecting garbage unconditionally...
2026-02-07T09:18:06.298228+00:00 ip-172-31-18-168 polkitd[608]: Loading rules from directory /etc/polkit-1/rules.d
2026-02-07T09:18:06.298270+00:00 ip-172-31-18-168 polkitd[608]: Loading rules from directory /usr/share/polkit-1/rules.d
2026-02-07T09:18:06.298574+00:00 ip-172-31-18-168 polkitd[608]: Finished loading, compiling and executing 6 rules
```

9.2 Observations

- Normal system boot and service initialization logs

- Successful SSH login records
- No errors or failed login attempts during baseline state

Screenshot Attachment: System and authentication logs

10. Incident Simulation

10.1 CPU Stress Simulation

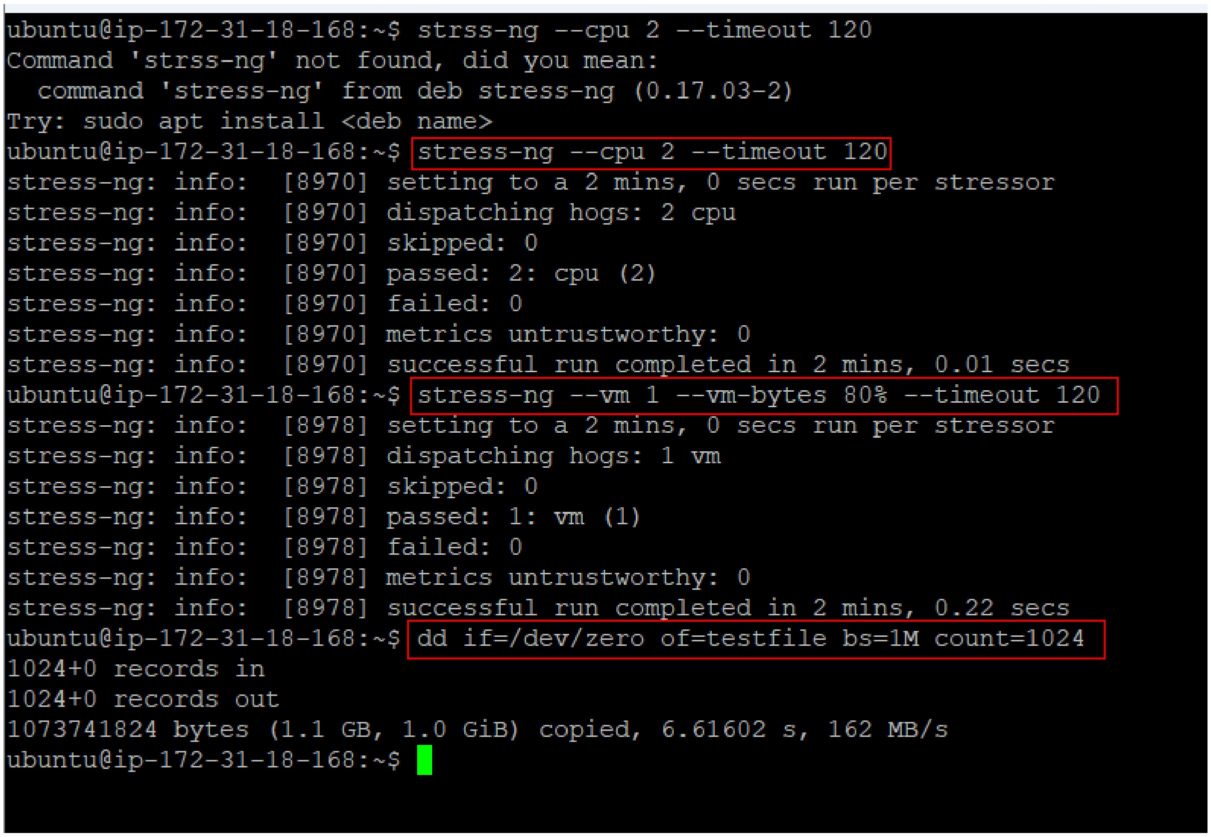
stress-ng --cpu 2 --timeout 120

10.2 Memory Stress Simulation

stress-ng --vm 1 --vm-bytes 80% --timeout 120

10.3 Disk I/O Simulation

dd if=/dev/zero of=testfile bs=1M count=1024



```
ubuntu@ip-172-31-18-168:~$ strss-ng --cpu 2 --timeout 120
Command 'strss-ng' not found, did you mean:
  command 'stress-ng' from deb stress-ng (0.17.03-2)
Try: sudo apt install <deb name>
ubuntu@ip-172-31-18-168:~$ stress-ng --cpu 2 --timeout 120
stress-ng: info:  [8970] setting to a 2 mins, 0 secs run per stressor
stress-ng: info:  [8970] dispatching hogs: 2 cpu
stress-ng: info:  [8970] skipped: 0
stress-ng: info:  [8970] passed: 2: cpu (2)
stress-ng: info:  [8970] failed: 0
stress-ng: info:  [8970] metrics untrustworthy: 0
stress-ng: info:  [8970] successful run completed in 2 mins, 0.01 secs
ubuntu@ip-172-31-18-168:~$ stress-ng --vm 1 --vm-bytes 80% --timeout 120
stress-ng: info:  [8978] setting to a 2 mins, 0 secs run per stressor
stress-ng: info:  [8978] dispatching hogs: 1 vm
stress-ng: info:  [8978] skipped: 0
stress-ng: info:  [8978] passed: 1: vm (1)
stress-ng: info:  [8978] failed: 0
stress-ng: info:  [8978] metrics untrustworthy: 0
stress-ng: info:  [8978] successful run completed in 2 mins, 0.22 secs
ubuntu@ip-172-31-18-168:~$ dd if=/dev/zero of=testfile bs=1M count=1024
1024+0 records in
1024+0 records out
1073741824 bytes (1.1 GB, 1.0 GiB) copied, 6.61602 s, 162 MB/s
ubuntu@ip-172-31-18-168:~$ 
```

10.4 Observations

- CPU usage increased significantly
- Memory consumption approached system limits

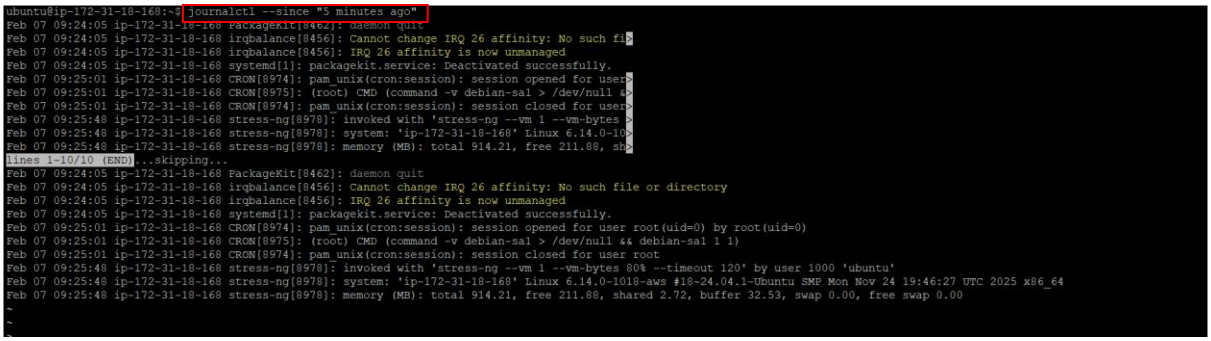
- Disk I/O activity increased temporarily

11. Incident Detection And Analysis

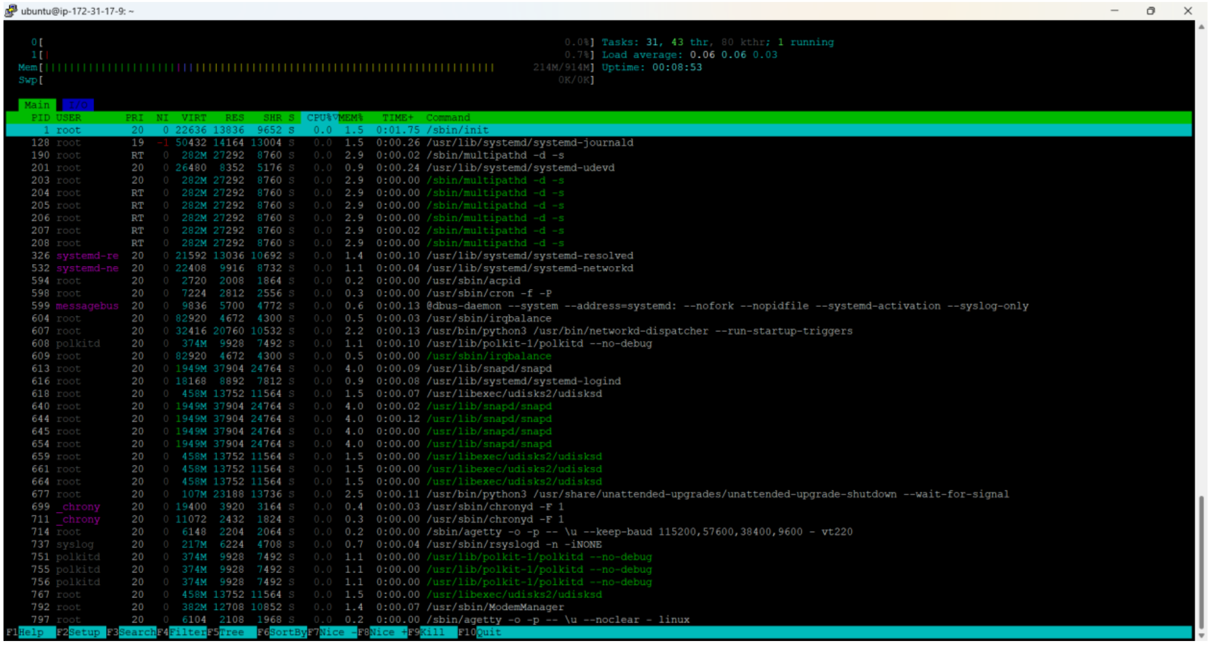
11.1 Detection Method

The incident was detected using manual monitoring tools such as top and log analysis.

```
top
journalctl --since "5 minutes ago"
```



```
ubuntu@ip-172-31-18-168:~$ journalctl --since "5 minutes ago"
Feb 07 09:24:05 ip-172-31-18-168 PackageKit[8462]: daemon quit
Feb 07 09:24:05 ip-172-31-18-168 irqbalance[8456]: Cannot change IRQ 26 affinity: No such fi>
Feb 07 09:24:05 ip-172-31-18-168 irqbalance[8456]: IRQ 26 affinity is now unmanaged
Feb 07 09:24:05 ip-172-31-18-168 systemd[1]: packagekit.service: Deactivated successfully.
Feb 07 09:25:01 ip-172-31-18-168 CRON[8974]: pam_unix(cron:session): session opened for user>
Feb 07 09:25:01 ip-172-31-18-168 CRON[8975]: (root) CMD (command -v debian-sa1 > /dev/null &>
Feb 07 09:25:01 ip-172-31-18-168 CRON[8974]: pam_unix(cron:session): session closed for user>
Feb 07 09:25:48 ip-172-31-18-168 stress-ng[8978]: invoked with 'stress-ng --vm 1 --vm-bytes >
Feb 07 09:25:48 ip-172-31-18-168 stress-ng[8978]: system: 'ip-172-31-18-168' Linux 6.14.0-10>
Feb 07 09:25:48 ip-172-31-18-168 stress-ng[8978]: memory (MB): total 914.21, free 211.88, sh>
lines 1-10/10 (END)...skipping...
Feb 07 09:24:05 ip-172-31-18-168 PackageKit[8462]: daemon quit
Feb 07 09:24:05 ip-172-31-18-168 irqbalance[8456]: Cannot change IRQ 26 affinity: No such file or directory
Feb 07 09:24:05 ip-172-31-18-168 irqbalance[8456]: IRQ 26 affinity is now unmanaged
Feb 07 09:24:05 ip-172-31-18-168 systemd[1]: packagekit.service: Deactivated successfully.
Feb 07 09:25:01 ip-172-31-18-168 CRON[8974]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Feb 07 09:25:01 ip-172-31-18-168 CRON[8975]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Feb 07 09:25:01 ip-172-31-18-168 CRON[8974]: pam_unix(cron:session): session closed for user root
Feb 07 09:25:48 ip-172-31-18-168 stress-ng[8978]: invoked with 'stress-ng --vm 1 --vm-bytes 80% --timeout 120' by user 1000 'ubuntu'
Feb 07 09:25:48 ip-172-31-18-168 stress-ng[8978]: system: 'ip-172-31-18-168' Linux 6.14.0-1018-aws #18~24.04.1-Ubuntu SMP Mon Nov 24 19:46:27 UTC 2025 x86_64
Feb 07 09:25:48 ip-172-31-18-168 stress-ng[8978]: memory (MB): total 914.21, free 211.88, shared 2.72, buffer 32.53, swap 0.00, free swap 0.00
~
~
```



```
    0[                                                                 0.0%] Tasks: 31, 43 thr, 80 kthr; 1 running
    1[|                                                                0.7%] Load average: 0.06 0.06 0.03
  Mem[|||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||214M/914M] Uptime: 00:08:53
  Swp[                                                                0K/0K]

  Main  I/O
    PID USER       PRI  NI  VIRT   RES   SHR S  CPU%▽MEM%   TIME+  Command
      1 root        20   0 22636 13836  9652 S   0.0  1.5  0:01.75 /sbin/init
    128 root        19  -1 50432 14164 13004 S   0.0  1.5  0:00.26 /usr/lib/systemd/systemd-journald
    190 root        RT   0  282M 27292  8760 S   0.0  2.9  0:00.02 /sbin/multipathd -d -s
    201 root        20   0 26480  8352  5176 S   0.0  0.9  0:00.24 /usr/lib/systemd/systemd-udevd
    203 root        20   0  282M 27292  8760 S   0.0  2.9  0:00.00 /sbin/multipathd -d -s
    204 root        RT   0  282M 27292  8760 S   0.0  2.9  0:00.00 /sbin/multipathd -d -s
    205 root        RT   0  282M 27292  8760 S   0.0  2.9  0:00.00 /sbin/multipathd -d -s
    206 root        RT   0  282M 27292  8760 S   0.0  2.9  0:00.00 /sbin/multipathd -d -s
    207 root        RT   0  282M 27292  8760 S   0.0  2.9  0:00.02 /sbin/multipathd -d -s
    208 root        RT   0  282M 27292  8760 S   0.0  2.9  0:00.00 /sbin/multipathd -d -s
    326 systemd-re  20   0 21592 13036 10692 S   0.0  1.4  0:00.10 /usr/lib/systemd/systemd-resolved
    532 systemd-ne  20   0 22408  9916  8732 S   0.0  1.1  0:00.04 /usr/lib/systemd/systemd-networkd
    594 root        20   0  2720  2008  1864 S   0.0  0.2  0:00.00 /usr/sbin/acpid
    598 root        20   0  7224  2812  2556 S   0.0  0.3  0:00.00 /usr/sbin/cron -f -P
    599 messagebus  20   0  9836  5700  4772 S   0.0  0.6  0:00.13 @dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
    604 root        20   0 82920  4672  4300 S   0.0  0.5  0:00.03 /usr/sbin/irqbalance
    607 root        20   0 32416 20760 10532 S   0.0  2.2  0:00.13 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
    608 polkitd     20   0  374M  9928  7492 S   0.0  1.1  0:00.10 /usr/lib/polkit-1/polkitd --no-debug
    609 root        20   0 82920  4672  4300 S   0.0  0.5  0:00.00 /usr/sbin/irqbalance
    613 root        20   0 1949M 37904 24764 S   0.0  4.0  0:00.09 /usr/lib/snapd/snapd
    616 root        20   0 18168  8892  7812 S   0.0  0.9  0:00.08 /usr/lib/systemd/systemd-logind
    618 root        20   0  458M 13752 11564 S   0.0  1.5  0:00.07 /usr/libexec/udisks2/udisksd
    640 root        20   0 1949M 37904 24764 S   0.0  4.0  0:00.02 /usr/lib/snapd/snapd
    644 root        20   0 1949M 37904 24764 S   0.0  4.0  0:00.12 /usr/lib/snapd/snapd
    645 root        20   0 1949M 37904 24764 S   0.0  4.0  0:00.00 /usr/lib/snapd/snapd
    654 root        20   0 1949M 37904 24764 S   0.0  4.0  0:00.00 /usr/lib/snapd/snapd
    659 root        20   0  458M 13752 11564 S   0.0  1.5  0:00.00 /usr/libexec/udisks2/udisksd
    661 root        20   0  458M 13752 11564 S   0.0  1.5  0:00.00 /usr/libexec/udisks2/udisksd
    664 root        20   0  458M 13752 11564 S   0.0  1.5  0:00.00 /usr/libexec/udisks2/udisksd
    677 root        20   0  107M 23188 13736 S   0.0  2.5  0:00.11 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
    699 _chrony     20   0 19400  3920  3164 S   0.0  0.4  0:00.03 /usr/sbin/chronyd -F 1
    711 _chrony     20   0 11072  2432  1824 S   0.0  0.3  0:00.00 /usr/sbin/chronyd -F 1
    714 root        20   0  6148  2204  2064 S   0.0  0.2  0:00.00 /sbin/agetty -o -p -- \u --keep-baud 115200,57600,38400,9600 - vt220
    737 syslog      20   0  217M  6224  4708 S   0.0  0.7  0:00.04 /usr/sbin/rsyslogd -n -iNONE
    751 polkitd     20   0  374M  9928  7492 S   0.0  1.1  0:00.00 /usr/lib/polkit-1/polkitd --no-debug
    755 polkitd     20   0  374M  9928  7492 S   0.0  1.1  0:00.00 /usr/lib/polkit-1/polkitd --no-debug
    756 polkitd     20   0  374M  9928  7492 S   0.0  1.1  0:00.00 /usr/lib/polkit-1/polkitd --no-debug
    767 root        20   0  458M 13752 11564 S   0.0  1.5  0:00.00 /usr/libexec/udisks2/udisksd
    792 root        20   0  382M 12708 10852 S   0.0  1.4  0:00.07 /usr/sbin/ModemManager
    797 root        20   0  6104  2108  1968 S   0.0  0.2  0:00.00 /sbin/agetty -o -p -- \u --noclear - linux
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

11.2 Observations

- High CPU usage visible in process list
- stress-ng process identified as root cause

- Logs confirmed resource-intensive operations

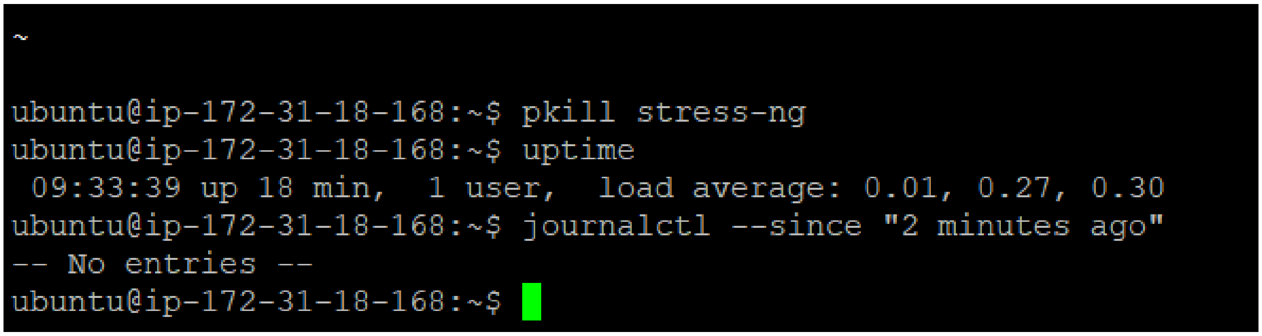
12. Incident Resolution and Recovery

12.1 Corrective Actions

stress-ng

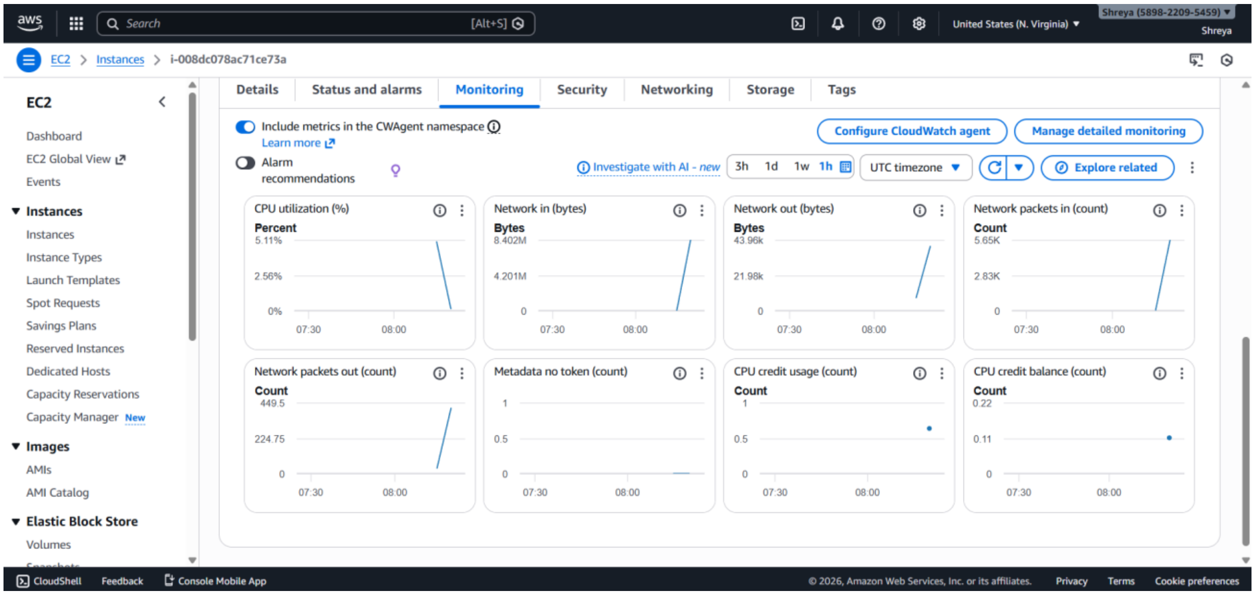
12.2 Recovery Verification

uptime
journalctl --since "2 minutes ago"



```
~

ubuntu@ip-172-31-18-168:~$ pkill stress-ng
ubuntu@ip-172-31-18-168:~$ uptime
 09:33:39 up 18 min,  1 user,  load average: 0.01, 0.27, 0.30
ubuntu@ip-172-31-18-168:~$ journalctl --since "2 minutes ago"
-- No entries --
ubuntu@ip-172-31-18-168:~$ 
```



12.3 Observations

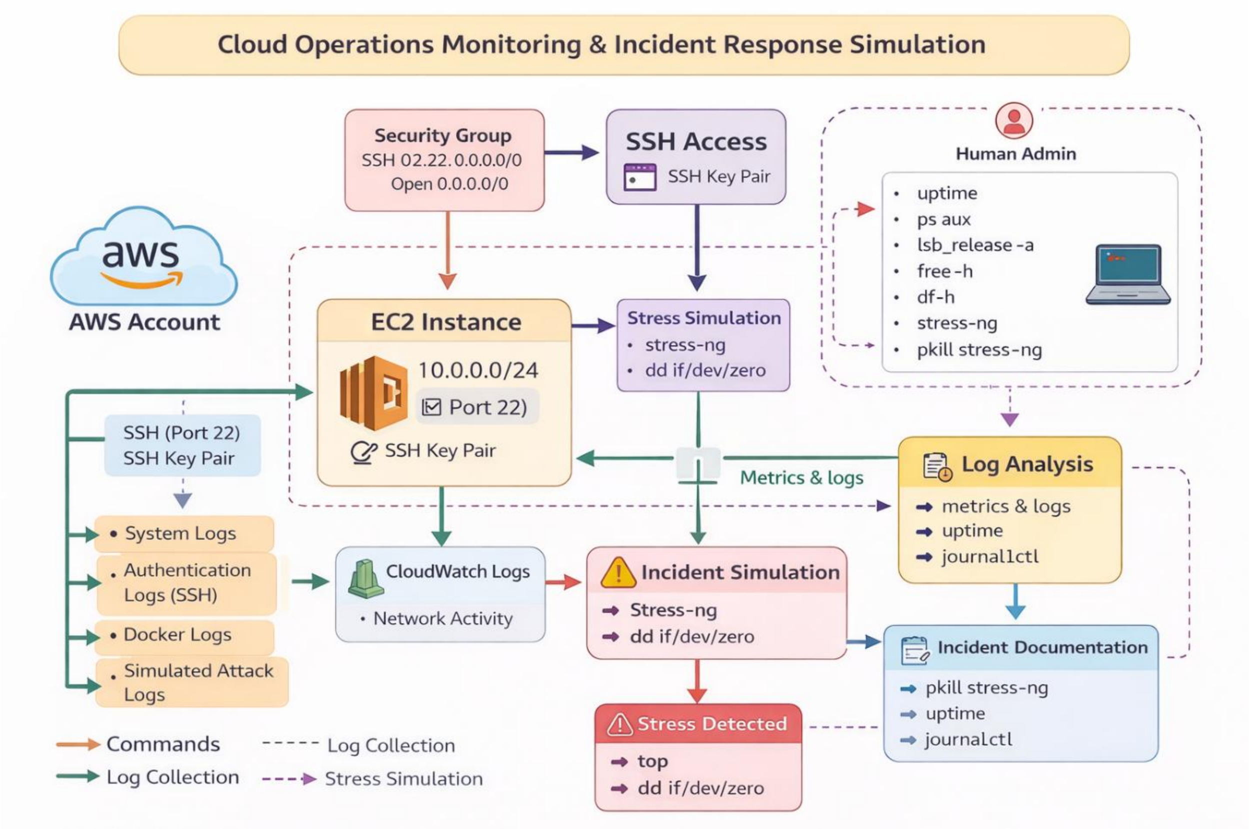
- CPU usage returned to normal levels
- Load average stabilized

- No further errors observed in logs

13. Incident Documentation

Incident Description: High CPU utilization due to stress process
Detection Method: Manual monitoring
Root Cause: CPU stress simulation
Impact: Temporary system slowdown
Resolution: Terminated stress process
Recovery Time: Within minutes

Diagram



14. Results

The project successfully demonstrated the importance of monitoring and log analysis in cloud environments. The incident was detected, analyzed, and resolved efficiently using basic tools.

15. Conclusion

This simulation reinforced the principle of **monitor first, fix later**. By understanding system behavior through metrics and logs, IT administrators can respond to incidents more effectively and reduce downtime. The skills practiced in this project are directly applicable to CloudOps, DevOps, and system administration roles.