Project Name : Linux-IAM-Hardening-mini-Users-Groups-Permissions-

Name : Hira yadav

ERP : 6604307

Course : CEH

1. Project Overview

Objective:

Design and implement a **secure file system and access control model** on an Ubuntu server. Identify and fix **3 security misconfigurations** in a pre-configured vulnerable lab environment, and maintain **evidence and audit logs** of all corrective actions.

Tools & Environment:

- Ubuntu Server (Lab VM)
- Kali Linux (Attacker VM - for testing)
- sudo access enabled
- auditd, chmod, chown, and find utilities

2. Baseline Policy Document

Role	Privileges	Sudo Access	File Access
Admin	Manage users, services, and software	useradd, usermod, systemctl, apt	Full access to /srv/project
Dev	Modify project files, restart app service	systemctl restart/status project.service only	Write to /srv/project, read-only for others
Auditor	Read logs and audit evidence only	None	Read-only/srv/project, /var/log/audit

3. Implementation Steps

a) User and group creation

commands:

sudo groupadd

sudo useradd

Example :

sudo groupadd devteam

sudo useradd -m -s /bin/bash -G devteam dev1

b) Configure Sudoers (Least Privilege)

Created/etc/sudoers.d/roles-admin and /etc/sudoers.d/roles-dev

c) Step 3: Secure Project Directory

This step creates a secure project directory /srv/project with restricted access. Ownership, permissions, and ACLs are configured so only authorized groups (dev and auditor) can access it safely

sudo mkdir -p /srv/project

sudo chown:proj/srv/project

sudo chmod 770/srv/project

sudo setfacl -m g:dev:rwx/srv/project

sudo setfacl -m g:auditor:r-x/srv/project

Verification:

getfacl/srv/project

d) Enable auditing

This step enables the auditd service to monitor critical system files. It logs any changes to /etc/passwd and /etc/sudoers for tracking user and privilege modifications.

sudo apt install auditd -y

sudo systemctl enable auditd --now

sudo auditctl-w/etc/passwd -p wa -k identity

sudo auditctl-w/etc/sudoers -p wa -k identity

e) Vulnerability Discovery & Fixes

World-writable /etc/cron.d/test	Unauthorized users could add jobs	sudo chmod 600 /etc/cron.d/test
Sudo NOPASSWD for 2 devs	Privilege escalation	Removed from /etc/sudoers.d/roles-dev
Weak permissions on /srv/project	Read/write for all users	sudo chmod 770/srv/project and reset ACL

f) Network Check

This step scans and verifies active network ports and sockets. Results are saved as evidence to confirm unnecessary ports are closed and only required services are running.

Scanned and Verified

sudo ss -tulpn > ~/evidence/ports_after_closure.txt

sudo lsof -i -Pn > ~/evidence/open_sockets_after.txt

sudo nmap -p 8080 127.0.0.1 > ~/evidence/nmap_8080_check.txt

g) Remediation Checklist

Task	Status
Remove world-writable files	✅
Disable unnecessary sudo NOPASSWD	✅
Lock down file permissions	✅
Enable audit logging	✅
Close unused ports	✅
Generate evidence folder	✅

h) Summary

Users: 3 created (alice, bob, charlie)

Groups: 3 configured (admin, dev, auditor)

Sudo rules: verified and validated

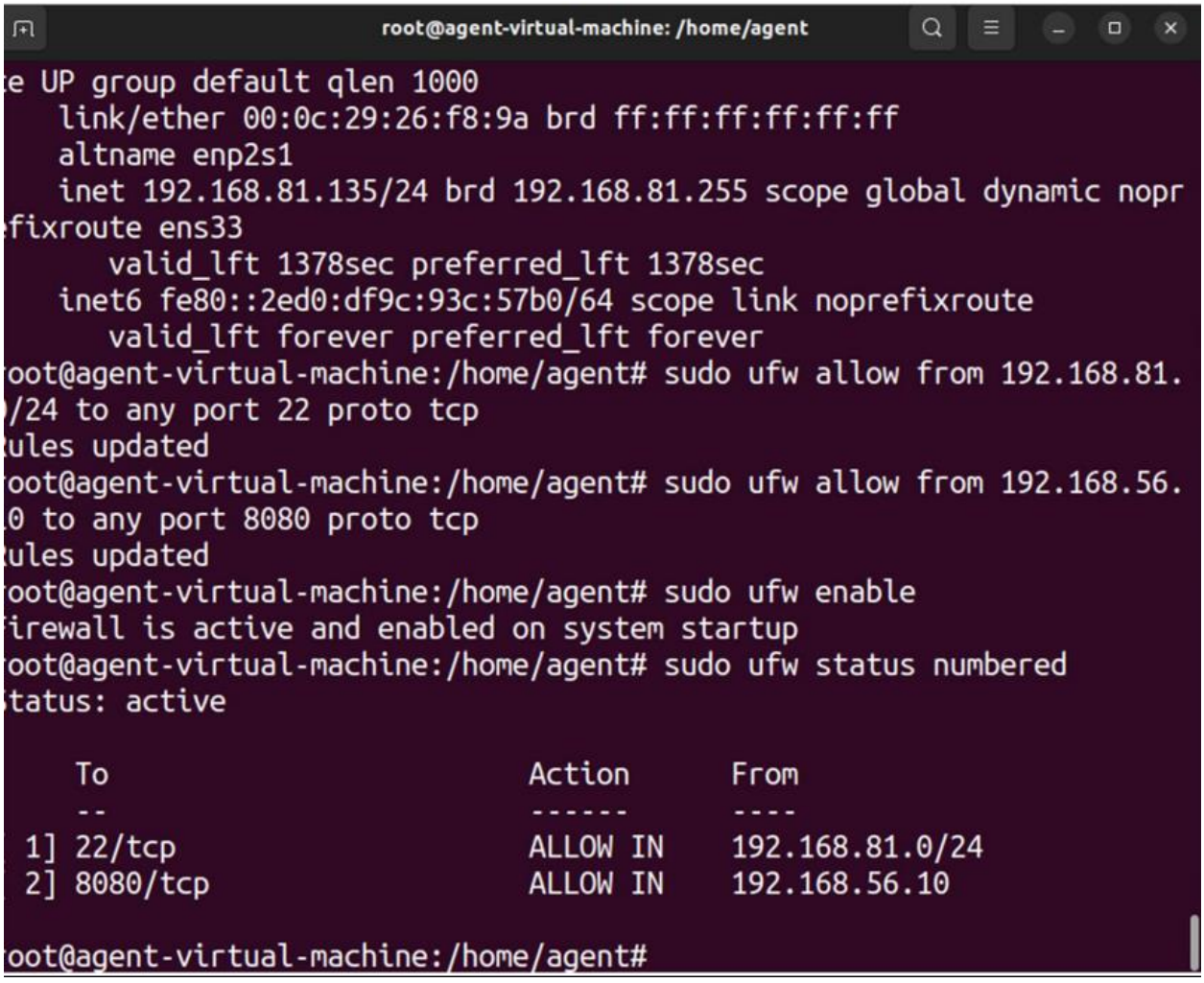
ACLS: configured correctly

Audit logs: functioning

Ports: secure, verified closed

Supporting ScreenShots:

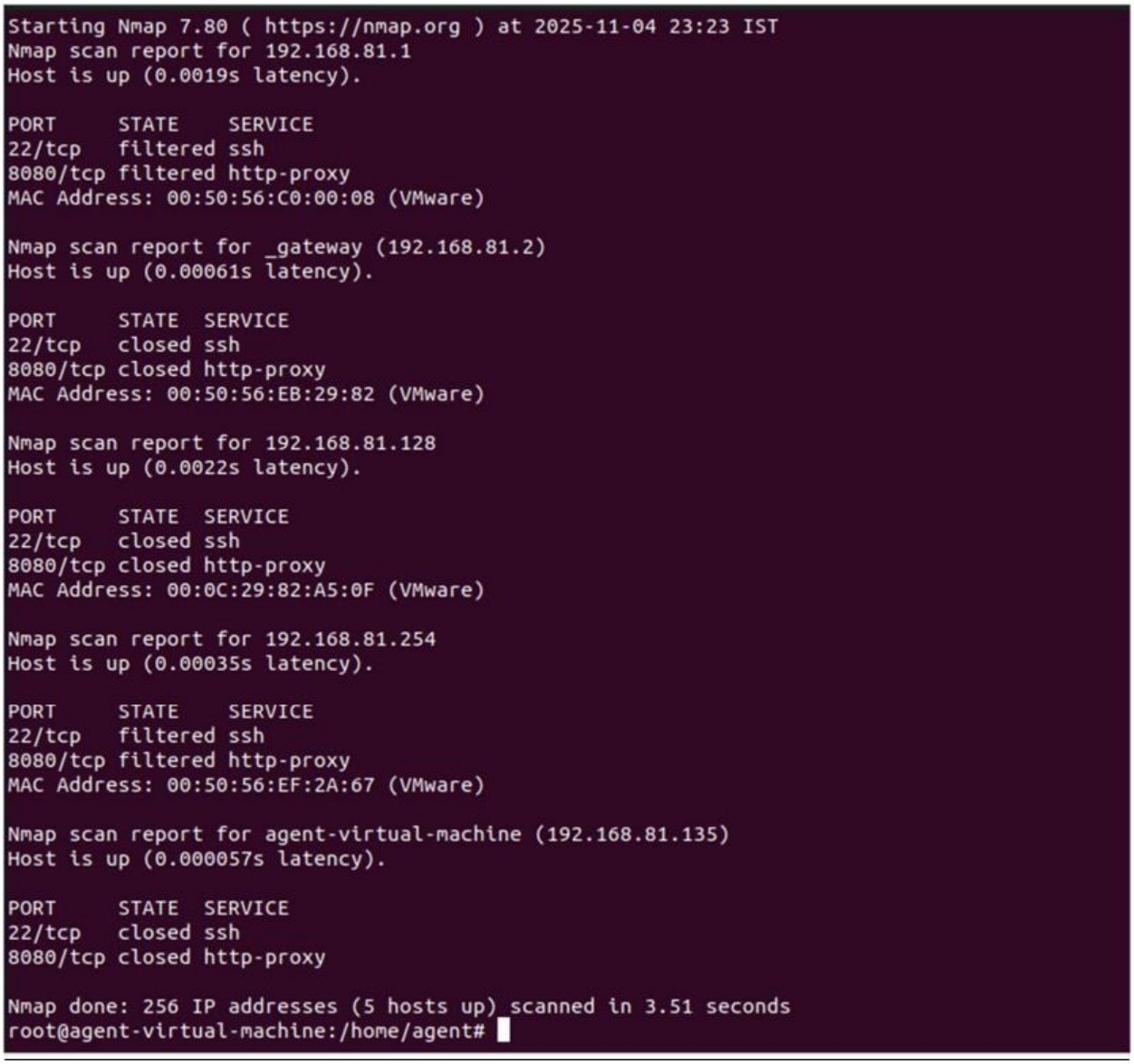
1) Opening ports to listen through



2) Open Ports Enumeration for System Hardening using ss

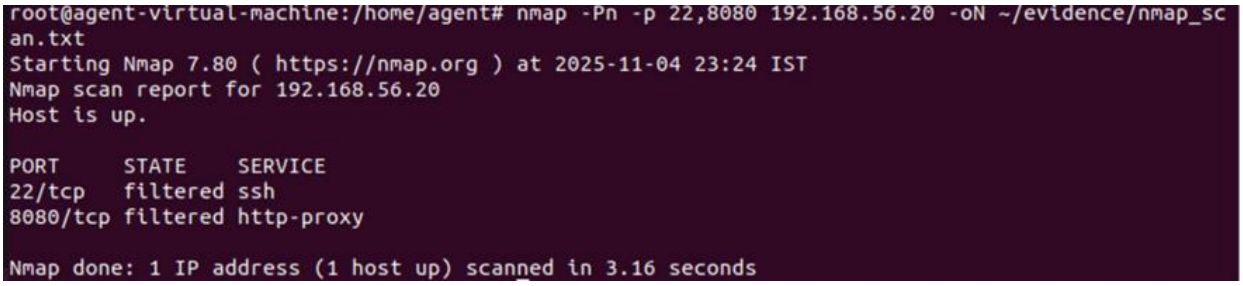
```
root@agent-virtual-machine:/home/agent# sudo ss -tuln
Netid State  Recv-Q Send-Q      Local Address:Port   Peer Address:Port Process
udp   UNCONN 0      0           127.0.0.53%lo:53          0.0.0.0:*
udp   UNCONN 0      0                0.0.0.0:631         0.0.0.0:*
udp   UNCONN 0      0                0.0.0.0:33601       0.0.0.0:*
udp   UNCONN 0      0                0.0.0.0:5353        0.0.0.0:*
udp   UNCONN 0      0                   [::]:53837          [::]:*
udp   UNCONN 0      0                   [::]:5353           [::]:*
tcp   LISTEN 0      128              0.0.0.0:1514        0.0.0.0:*
tcp   LISTEN 0      128              0.0.0.0:1515        0.0.0.0:*
tcp   LISTEN 0      128            127.0.0.1:631         0.0.0.0:*
tcp   LISTEN 0      2048             0.0.0.0:55000       0.0.0.0:*
tcp   LISTEN 0      511              0.0.0.0:443         0.0.0.0:*
tcp   LISTEN 0      4096        127.0.0.53%lo:53          0.0.0.0:*
tcp   LISTEN 0      4096   [::ffff:127.0.0.1]:9200             *:*
tcp   LISTEN 0      2048                [::]:55000          [::]:*
tcp   LISTEN 0      128                [::1]:631            [::]:*
tcp   LISTEN 0      4096   [::ffff:127.0.0.1]:9300             *:*
root@agent-virtual-machine:/home/agent#
```

3) Nmap scan

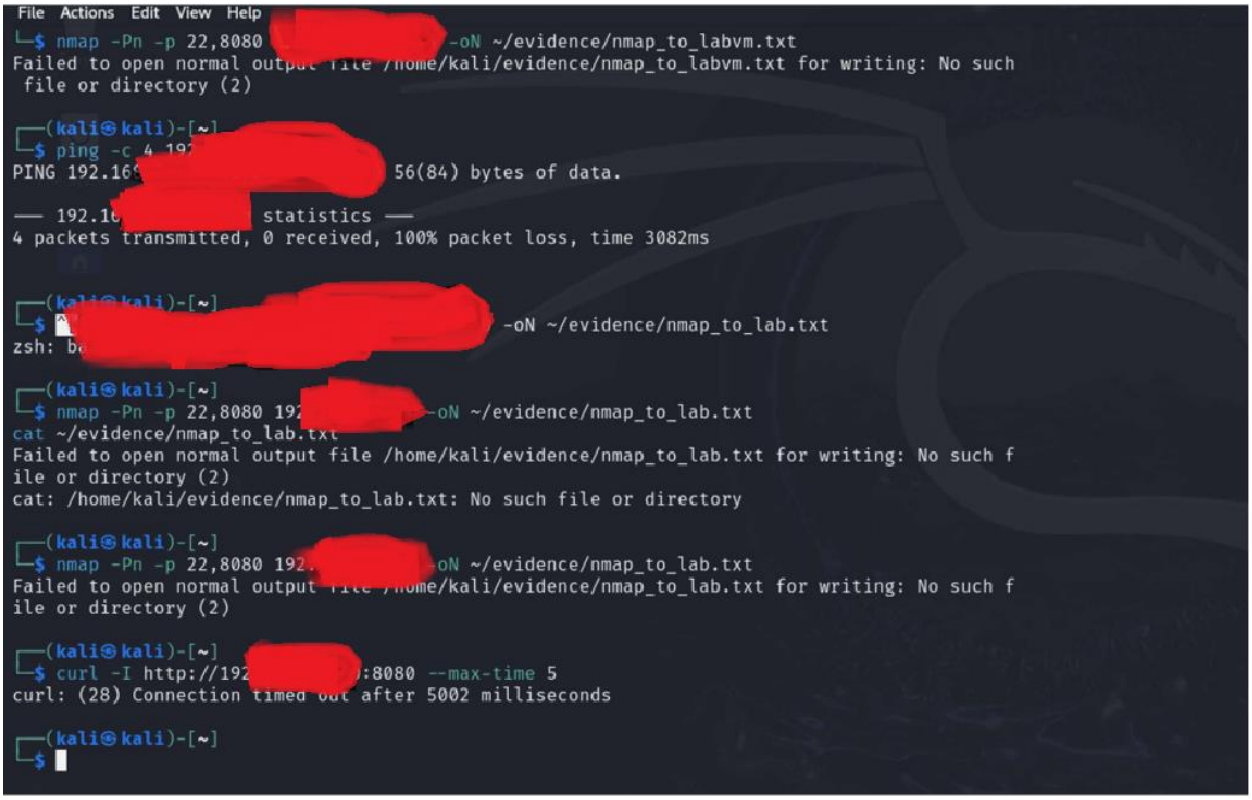


```
Starting Nmap 7.80 ( https://nmap.org ) at 2025-11-04 23:23 IST
Nmap scan report for 192.168.81.1
Host is up (0.0019s latency).

PORT     STATE    SERVICE
22/tcp   filtered ssh
8080/tcp filtered http-proxy
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for _gateway (192.168.81.2)
Host is up (0.00061s latency).

PORT     STATE  SERVICE
22/tcp   closed ssh
8080/tcp closed http-proxy
MAC Address: 00:50:56:EB:29:82 (VMware)

Nmap scan report for 192.168.81.128
Host is up (0.0022s latency).

PORT     STATE  SERVICE
22/tcp   closed ssh
8080/tcp closed http-proxy
MAC Address: 00:0C:29:82:A5:0F (VMware)

Nmap scan report for 192.168.81.254
Host is up (0.00035s latency).

PORT     STATE    SERVICE
22/tcp   filtered ssh
8080/tcp filtered http-proxy
MAC Address: 00:50:56:EF:2A:67 (VMware)

Nmap scan report for agent-virtual-machine (192.168.81.135)
Host is up (0.000057s latency).

PORT     STATE  SERVICE
22/tcp   closed ssh
8080/tcp closed http-proxy

Nmap done: 256 IP addresses (5 hosts up) scanned in 3.51 seconds
root@agent-virtual-machine:/home/agent#
```

4) 4) Nmap port scan command used to check specific ports (22 and 8080) on a target host



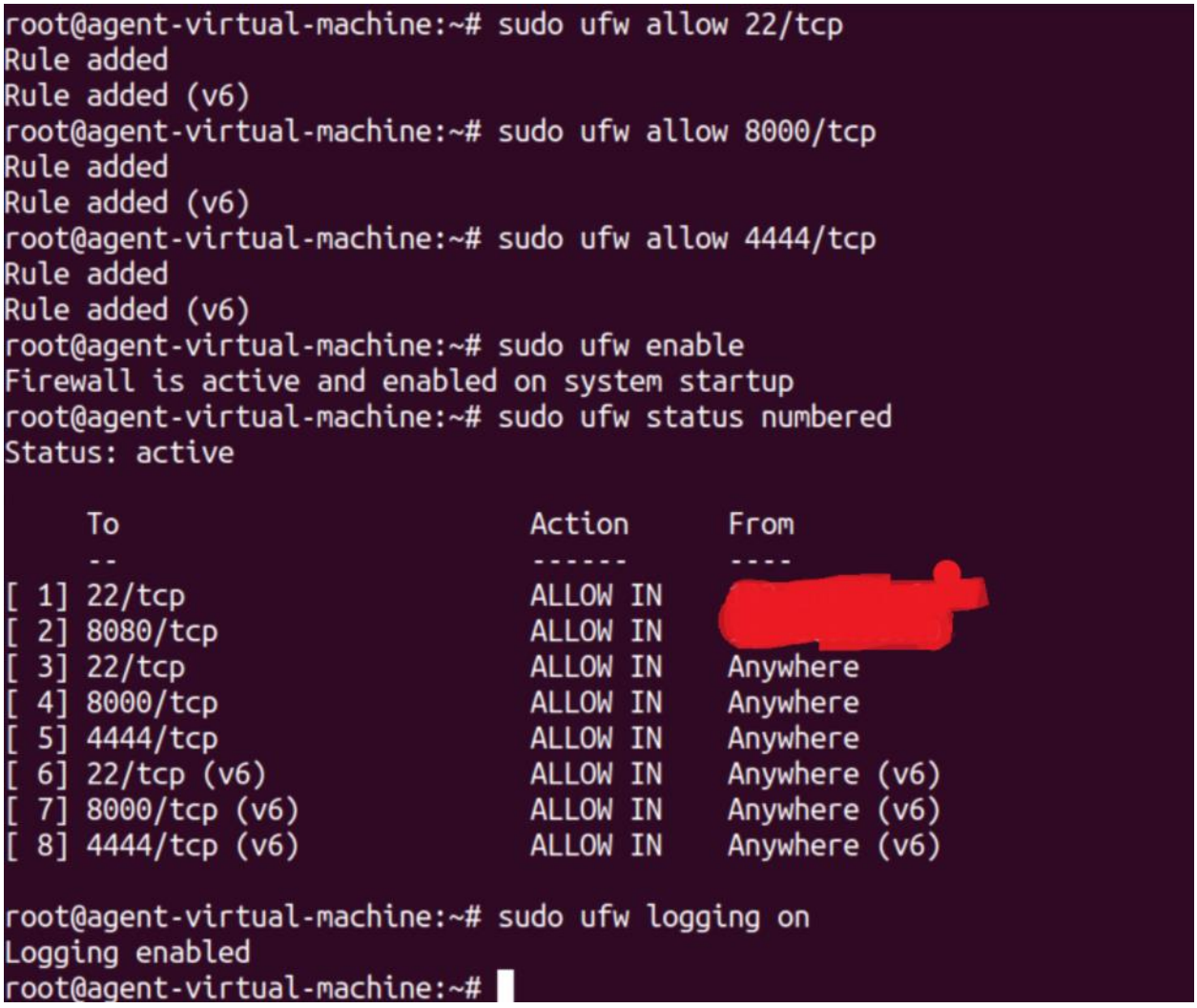
5) Nmap scan from KALI LINUX



6) Verification of Service Termination and Port Closure using ss, lsof, and Nmap

```
root@agent-virtual-machine:/home/agent# sudo systemctl stop project.service
sudo systemctl disable project.service
sudo systemctl status project.service --no-pager
Failed to stop project.service: Unit project.service not loaded.
Failed to disable unit: Unit file project.service does not exist.
Unit project.service could not be found.
root@agent-virtual-machine:/home/agent# sudo systemctl stop project.service
Failed to stop project.service: Unit project.service not loaded.
root@agent-virtual-machine:/home/agent# sudo ss -tulpn | sed -n '1,200p'
Netid State  Recv-Q Send-Q      Local Address:Port  Peer Address:PortProcess
udp   UNCONN 0      0           127.0.0.53%lo:53         0.0.0.0:*    users:(("systemd-resolve",pid=675,fd=13))
udp   UNCONN 0      0                0.0.0.0:631        0.0.0.0:*    users:(("cups-browsed",pid=1032,fd=7))
udp   UNCONN 0      0                0.0.0.0:33601      0.0.0.0:*    users:(("avahi-daemon",pid=858,fd=14))
udp   UNCONN 0      0                0.0.0.0:5353       0.0.0.0:*    users:(("avahi-daemon",pid=858,fd=12))
udp   UNCONN 0      0                   [::]:53837         [::]:*    users:(("avahi-daemon",pid=858,fd=15))
udp   UNCONN 0      0                   [::]:5353          [::]:*    users:(("avahi-daemon",pid=858,fd=13))
tcp   LISTEN 0      128              0.0.0.0:1514       0.0.0.0:*    users:(("wazuh-remoted",pid=1948,fd=4))
tcp   LISTEN 0      128              0.0.0.0:1515       0.0.0.0:*    users:(("wazuh-authd",pid=1834,fd=3))
tcp   LISTEN 0      128            127.0.0.1:631        0.0.0.0:*    users:(("cupsd",pid=963,fd=7))
tcp   LISTEN 0      2048             0.0.0.0:55000      0.0.0.0:*    users:(("python3",pid=1779,fd=42))
tcp   LISTEN 0      511              0.0.0.0:443        0.0.0.0:*    users:(("node",pid=912,fd=19))
tcp   LISTEN 0      4096        127.0.0.53%lo:53         0.0.0.0:*    users:(("systemd-resolve",pid=675,fd=14))
tcp   LISTEN 0      4096   [::ffff:127.0.0.1]:9200             *:*    users:(("java",pid=1038,fd=618))
tcp   LISTEN 0      2048                [::]:55000         [::]:*    users:(("python3",pid=1779,fd=44))
tcp   LISTEN 0      128               [::1]:631           [::]:*    users:(("cupsd",pid=963,fd=6))
tcp   LISTEN 0      4096   [::ffff:127.0.0.1]:9300             *:*    users:(("java",pid=1038,fd=616))
root@agent-virtual-machine:/home/agent# sudo ss -tulpn | grep ':8080'
root@agent-virtual-machine:/home/agent# sudo lsof -i :8080 -Pn
root@agent-virtual-machine:/home/agent# sudo nmap -p 8080 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2025-11-04 23:42 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00012s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
root@agent-virtual-machine:/home/agent# sudo ss -tulpn > ~/evidence/ports_after_closure.txt
sudo lsof -i -Pn > ~/evidence/open_sockets_after.txt
sudo nmap -p 8080 127.0.0.1 > ~/evidence/nmap_8080_check.txt
root@agent-virtual-machine:/home/agent#
```

Opening ports



Listening Ports

```
Netid State  Recv-Q Send-Q      Local Address:Port  Peer Address:PortProcess
udp   UNCONN 0      0               0.0.0.0:46105      0.0.0.0:*    users:(("avahi-daemon",pid=986,fd=14))
udp   UNCONN 0      0               0.0.0.0:5353       0.0.0.0:*    users:(("avahi-daemon",pid=986,fd=12))
udp   UNCONN 0      0          127.0.0.53%lo:53        0.0.0.0:*    users:(("systemd-resolve",pid=649,fd=13))
udp   UNCONN 0      0                  [::]:5353          [::]:*    users:(("avahi-daemon",pid=986,fd=13))
udp   UNCONN 0      0                  [::]:53461         [::]:*    users:(("avahi-daemon",pid=986,fd=15))
tcp   LISTEN 0      2048            0.0.0.0:55000      0.0.0.0:*    users:(("python3",pid=1916,fd=42))
tcp   LISTEN 0      5               0.0.0.0:8000       0.0.0.0:*    users:(("python3",pid=14829,fd=3))
tcp   LISTEN 0      128             0.0.0.0:1515       0.0.0.0:*    users:(("wazuh-authd",pid=1970,fd=3))
tcp   LISTEN 0      128             0.0.0.0:1514       0.0.0.0:*    users:(("wazuh-remoted",pid=2069,fd=4))
tcp   LISTEN 0      128           127.0.0.1:631        0.0.0.0:*    users:(("cupsd",pid=11126,fd=7))
tcp   LISTEN 0      4096       127.0.0.53%lo:53        0.0.0.0:*    users:(("systemd-resolve",pid=649,fd=14))
tcp   LISTEN 0      128             0.0.0.0:22         0.0.0.0:*    users:(("sshd",pid=15648,fd=3))
tcp   LISTEN 0      511             0.0.0.0:443        0.0.0.0:*    users:(("node",pid=1024,fd=19))
tcp   LISTEN 0      1               0.0.0.0:4444       0.0.0.0:*    users:(("nc",pid=14929,fd=3))
tcp   LISTEN 0      2048               [::]:55000         [::]:*    users:(("python3",pid=1916,fd=44))
tcp   LISTEN 0      4096   [::ffff:127.0.0.1]:9300            *:*    users:(("java",pid=1244,fd=616))
tcp   LISTEN 0      128             [::1]:631          [::]:*    users:(("cupsd",pid=11126,fd=6))
tcp   LISTEN 0      4096   [::ffff:127.0.0.1]:9200            *:*    users:(("java",pid=1244,fd=618))
tcp   LISTEN 0      128                [::]:22            [::]:*    users:(("sshd",pid=15648,fd=4))
~
```

Log Reports

Nov 13 20:50:41 agent-virtual-machine NetworkManager[990]: <info> [1763047241.9975] manager: enable requested (sleeping: no enabled: no)

Nov 13 20:50:41 agent-virtual-machine NetworkManager[990]: <info> [1763047241.9976] device (ens33): state change: unmanaged -> unavailable (reason 'man

aged', sys-iface-state: 'external')

Nov 13 20:50:42 agent-virtual-machine kernel: [2618.755282] e1000: ens33 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None

Nov 13 20:50:42 agent-virtual-machine NetworkManager[990]: <info> [1763047242.0131] device (ens33): state change: unavailable -> disconnected (reason 'none', sys-iface-state: 'managed')

Nov 13 20:50:42 agent-virtual-machine NetworkManager[990]: <info> [1763047242.0161] policy: auto-activating connection 'Wired connection 1' (4492c2aa-8603-3e9c-85da-4f5504ab8fda)

Nov 13 20:50:42 agent-virtual-machine NetworkManager[990]: <info> [1763047242.0170] device (ens33): Activation: starting connection 'Wired connection 1' (4492c2aa-8603-3e9c-85da-4f5504ab8fda)

Nov 13 20:50:42 agent-virtual-machine NetworkManager[990]: <info> [1763047242.0172] device (ens33): state change: disconnected -> prepare (reason 'none', sys-iface-state: 'managed')

Nov 13 20:50:42 agent-virtual-machine NetworkManager[990]: <info> [1763047242.0174] manager: NetworkManager state is now CONNECTING

Nov 13 20:50:42 agent-virtual-machine NetworkManager[990]: <info> [1763047242.0176] device (ens33): state change: prepare -> config (reason 'none', sys-iface-state: 'managed')

Nov 13 20:50:42 agent-virtual-machine NetworkManager[990]: <info> [1763047242.0192] device (ens33): state change: config -> ip-config (reason 'none', sys-iface-state: 'managed')

Nov 13 20:50:42 agent-virtual-machine avahi-daemon[986]: Joining mDNS multicast group on interface ens33.IPv6 with address fe80::2ed0:df9c:93c:57b0.

Nov 13 20:50:42 agent-virtual-machine NetworkManager[990]: <info> [1763047242.0223] dhcp4 (ens33): activation: beginning transaction (timeout in 45 seconds)

Nov 13 20:50:42 agent-virtual-machine avahi-daemon[986]: New relevant interface ens33.IPv6 for mDNS.

Nov 13 20:50:42 agent-virtual-machine avahi-daemon[986]: Registering new address record for fe80::2ed0:df9c:93c:57b0 on ens33.*.

Nov 13 20:50:42 agent-virtual-machine NetworkManager[990]: <info> [1763047242.0451] dhcp4 (ens33): state changed new lease, address=------

Nov 13 20:50:42 agent-virtual-machine avahi-daemon[986]: Joining mDNS multicast group on interface ens33.IPv4 with address -------.

Nov 13 20:50:42 agent-virtual-machine avahi-daemon[986]: New relevant interface ens33.IPv4 for mDNS.

Nov 13 20:50:42 agent-virtual-machine avahi-daemon[986]: Registering new address record for 192.168.81.135 on ens33.IPv4.

Nov 13 20:50:42 agent-virtual-machine NetworkManager[990]: <info> [1763047242.0518] device (ens33): state change: ip-config -> ip-check (reason 'none', sys-iface-state: 'managed')

Nov 13 20:50:42 agent-virtual-machine NetworkManager[990]: <info> [1763047242.0590] device (ens33): state change: ip-check -> secondaries (reason 'none', sys-iface-state: 'managed')

Nov 13 20:50:42 agent-virtual-machine NetworkManager[990]: <info> [1763047242.0600] device (ens33): state change: secondaries -> activated (reason 'none', sys-iface-state: 'managed')

Nov 13 20:50:42 agent-virtual-machine NetworkManager[990]: <info> [1763047242.0616] manager: NetworkManager state is now CONNECTED_LOCAL

Nov 13 20:50:42 agent-virtual-machine NetworkManager[990]: <info> [1763047242.0619] manager: NetworkManager state is now CONNECTED_SITE

Nov 13 20:50:42 agent-virtual-machine NetworkManager[990]: <info> [1763047242.0620] policy: set 'Wired connection 1' (ens33) as default for IPv4 routing and DNS

Nov 13 20:50:42 agent-virtual-machine NetworkManager[990]: <info> [1763047242.0629] device (ens33): Activation: successful, device activated.

Nov 13 20:50:42 agent-virtual-machine systemd-resolved[649]: ens33: Bus client set search domain list to: localdomain

Nov 13 20:50:42 agent-virtual-machine systemd-resolved[649]: ens33: Bus client set default route setting: yes

Nov 13 20:50:42 agent-virtual-machine systemd-resolved[649]: ens33: Bus client set DNS server list to: ----

Nov 13 20:50:43 agent-virtual-machine NetworkManager[990]: <info> [1763047243.1424] manager: NetworkManager state is now CONNECTED_GLOBAL

Nov 13 20:50:49 agent-virtual-machine gsd-color[3464]: unable to get EDID for xrandr-Virtual-1: unable to get EDID for output

Nov 13 20:50:49 agent-virtual-machine gsd-color[3464]: unable to get EDID for xrandr-Virtual-1: unable to get EDID for output

Nov 13 20:50:49 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 38 with keysym 38 (keycode 11).

Nov 13 20:50:49 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 31 with keysym 31 (keycode a).

Nov 13 20:50:49 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 32 with keysym 32 (keycode b).

Nov 13 20:50:49 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 33 with keysym 33 (keycode c).

Nov 13 20:50:49 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 34 with keysym 34 (keycode d).

Nov 13 20:50:49 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 35 with keysym 35 (keycode e).

Nov 13 20:50:49 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 36 with keysym 36 (keycode f).

Nov 13 20:50:49 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 37 with keysym 37 (keycode 10).

Nov 13 20:50:49 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 39 with keysym 39 (keycode 12).

Nov 13 20:50:51 agent-virtual-machine systemd[1]: apt-daily-upgrade.service: Deactivated successfully.

Nov 13 20:50:51 agent-virtual-machine systemd[1]: Finished Daily apt upgrade and clean activities.

Nov 13 20:50:51 agent-virtual-machine systemd[1]: apt-daily-upgrade.service: Consumed 8.922s CPU time.

Nov 13 20:50:53 agent-virtual-machine systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.

Nov 13 20:51:03 agent-virtual-machine kernel: [2640.305292] workqueue: psi_avgs_work hogged CPU for >20000us 4 times, consider switching to WQ_UNBOUND

Nov 13 20:51:34 agent-virtual-machine update-notifier.desktop[13232]: #015Reading package lists... 0%#015#015Reading package lists... 100%#015#015Readin

g package lists... Done

Nov 13 20:51:35 agent-virtual-machine update-notifier.desktop[13232]: #015Building dependency tree... 0%#015#015Building dependency tree... 0%#015#015Building dependency tree... 50%#015#015Building dependency tree... 50%#015#015Building dependency tree... 61%#015#015Building dependency tree... Done

Nov 13 20:51:35 agent-virtual-machine update-notifier.desktop[13232]: #015Reading state information... 0% #015#015Reading state information... 0%#015#015Reading state information... Done

Nov 13 20:51:54 agent-virtual-machine update-notifier.desktop[13474]: WARNING:root:Error loading .desktop file /usr/share/applications/evolution-calendar.desktop: constructor returned NULL

Nov 13 20:52:22 agent-virtual-machine anacron[8106]: Job `cron.daily' started

Nov 13 20:52:22 agent-virtual-machine anacron[14146]: Updated timestamp for job `cron.daily' to 2025-11-13

Nov 13 20:52:22 agent-virtual-machine cracklib: no dictionary update necessary.

Nov 13 20:52:22 agent-virtual-machine anacron[8106]: Job `cron.daily' terminated

Nov 13 20:52:22 agent-virtual-machine anacron[8106]: Normal exit (1 job run)

Nov 13 20:52:22 agent-virtual-machine systemd[1]: anacron.service: Deactivated successfully.

Nov 13 20:52:22 agent-virtual-machine systemd[1]: Started Run anacron jobs.

Nov 13 20:52:22 agent-virtual-machine anacron[14176]: Anacron 2.3 started on 2025-11-13

Nov 13 20:52:22 agent-virtual-machine anacron[14176]: Will run job `cron.daily' in 5 min.

Nov 13 20:52:22 agent-virtual-machine anacron[14176]: Will run job `cron.weekly' in 10 min.

Nov 13 20:52:22 agent-virtual-machine anacron[14176]: Jobs will be executed sequentially

Nov 13 20:52:36 agent-virtual-machine snapd[1014]: storehelpers.go:916: cannot refresh: snap has no updates available: "bare", "core22", "gnome-42-2204", "gtk-common-themes", "snap-store", "snapd", "snapd-desktop-integration"

Nov 13 20:53:39 agent-virtual-machine systemd[1]: Starting Update APT News...

Nov 13 20:53:39 agent-virtual-machine systemd[1]: Starting Update the local ESM caches...

Nov 13 20:53:41 agent-virtual-machine systemd[1]: esm-cache.service: Deactivated successfully.

Nov 13 20:53:41 agent-virtual-machine systemd[1]: Finished Update the local ESM caches.

Nov 13 20:55:27 agent-virtual-machine systemd[1]: apt-news.service: Deactivated successfully.

Nov 13 20:55:27 agent-virtual-machine systemd[1]: Finished Update APT News.

Nov 13 20:56:05 agent-virtual-machine systemd[1]: Starting Update APT News...

Nov 13 20:56:05 agent-virtual-machine systemd[1]: Starting Update the local ESM caches...

Nov 13 20:56:05 agent-virtual-machine systemd[1]: apt-news.service: Deactivated successfully.

Nov 13 20:56:05 agent-virtual-machine systemd[1]: Finished Update APT News.

Nov 13 20:56:07 agent-virtual-machine systemd[1]: esm-cache.service: Deactivated successfully.

Nov 13 20:56:07 agent-virtual-machine systemd[1]: Finished Update the local ESM caches.

Nov 13 20:56:28 agent-virtual-machine systemd[1]: Reloading.

Nov 13 20:56:29 agent-virtual-machine systemd[1]: Configuration file /run/systemd/system/netplan-ovs-cleanup.service is marked world-inaccessible. This has no effect as configuration data is accessible via APIs without restrictions. Proceeding anyway.

Nov 13 20:56:29 agent-virtual-machine systemd[1]: Configuration file /etc/systemd/system/wazuh-dashboard.service is marked world-inaccessible. This has no effect as configuration data is accessible via APIs without restrictions. Proceeding anyway.

Nov 13 20:56:30 agent-virtual-machine systemd[1]: Reloading.

Nov 13 20:56:30 agent-virtual-machine systemd[1]: Configuration file /run/systemd/system/netplan-ovs-cleanup.service is marked world-inaccessible. This has no effect as configuration data is accessible via APIs without restrictions. Proceeding anyway.

Nov 13 20:56:30 agent-virtual-machine systemd[1]: Configuration file /etc/systemd/system/wazuh-dashboard.service is marked world-inaccessible. This has no effect as configuration data is accessible via APIs without restrictions. Proceeding anyway.

Nov 13 20:56:30 agent-virtual-machine systemd[1]: Starting Discard unused blocks on filesystems from /etc/fstab...

Nov 13 20:56:30 agent-virtual-machine systemd[1]: Starting OpenBSD Secure Shell server...

Nov 13 20:56:31 agent-virtual-machine systemd[1]: fstrim.service: Deactivated successfully.

Nov 13 20:56:31 agent-virtual-machine systemd[1]: Finished Discard unused blocks on filesystems from /etc/fstab.

Nov 13 20:56:31 agent-virtual-machine systemd[1]: Started OpenBSD Secure Shell server.

Nov 13 20:56:31 agent-virtual-machine systemd[1]: Reloading.

Nov 13 20:56:31 agent-virtual-machine systemd[1]: Configuration file /run/systemd/system/netplan-ovs-cleanup.service is marked world-inaccessible. This has no effect as configuration data is accessible via APIs without restrictions. Proceeding anyway.

Nov 13 20:56:31 agent-virtual-machine systemd[1]: Configuration file /etc/systemd/system/wazuh-dashboard.service is marked world-inaccessible. This has no effect as configuration data is accessible via APIs without restrictions. Proceeding anyway.

Nov 13 20:57:22 agent-virtual-machine anacron[14176]: Job `cron.daily' started

Nov 13 20:57:22 agent-virtual-machine anacron[15849]: Updated timestamp for job `cron.daily' to 2025-11-13

Nov 13 20:57:23 agent-virtual-machine cracklib: no dictionary update necessary.

Nov 13 20:57:23 agent-virtual-machine anacron[14176]: Job `cron.daily' terminated

Nov 13 21:00:07 agent-virtual-machine opensearch-dashboards[1024]: {"type":"log","@timestamp":"2025-11-13T15:30:07Z","tags":["error","opensearch","data"],"pid":1024,"message":"[resource_already_exists_exception]: index [wazuh-statistics-2025.46w/ZNDZdjxyRfCsSa742eM3kg] already exists"}

Nov 13 21:00:07 agent-virtual-machine opensearch-dashboards[1024]: {"type":"log","@timestamp":"2025-11-13T15:30:07Z","tags":["info","plugins","wazuh","cron-scheduler"],"pid":1024,"message":"wazuh-statistics-2025.46w index created"}

Nov 13 21:00:07 agent-virtual-machine opensearch-dashboards[1024]: {"type":"log","@timestamp":"2025-11-

13T15:30:07Z","tags":["info","plugins","wazuh","monitoring"],"pid":1024,"message":"wazuh-monitoring-2025.46w index created"}

Nov 13 21:00:07 agent-virtual-machine opensearch-dashboards[1024]: {"type":"log","@timestamp":"2025-11-13T15:30:07Z","tags":["info","plugins","wazuh","monitoring"],"pid":1024,"message":"Settings added to wazuh-monitoring-2025.46w index"}

Nov 13 21:00:08 agent-virtual-machine opensearch-dashboards[1024]: {"type":"log","@timestamp":"2025-11-13T15:30:08Z","tags":["info","plugins","wazuh","monitoring"],"pid":1024,"message":"Bulk data to index wazuh-monitoring-2025.46w for 1 agents completed"}

Nov 13 21:00:41 agent-virtual-machine rsyslogd: [origin software="rsyslogd" swVersion="8.2112.0" x-pid="1004" x-info="https://www.rsyslog.com"] rsyslogd was HUPed

Nov 13 21:02:22 agent-virtual-machine anacron[14176]: Job `cron.weekly' started

Nov 13 21:02:23 agent-virtual-machine anacron[16285]: Updated timestamp for job `cron.weekly' to 2025-11-13

Nov 13 21:02:23 agent-virtual-machine anacron[14176]: Job `cron.weekly' terminated

Nov 13 21:02:23 agent-virtual-machine anacron[14176]: Normal exit (2 jobs run)

Nov 13 21:02:23 agent-virtual-machine systemd[1]: anacron.service: Deactivated successfully.

Nov 13 21:02:42 agent-virtual-machine systemd[1]: Reloading.

Nov 13 21:02:42 agent-virtual-machine systemd[1]: Configuration file /run/systemd/system/netplan-ovs-cleanup.service is marked world-inaccessible. This has no effect as configuration data is accessible via APIs without restrictions. Proceeding anyway.

Nov 13 21:02:42 agent-virtual-machine systemd[1]: Configuration file /etc/systemd/system/wazuh-dashboard.service is marked world-inaccessible. This has no effect as configuration data is accessible via APIs without restrictions. Proceeding anyway.

Nov 13 21:05:11 agent-virtual-machine systemd[3027]: Started VTE child process 16870 launched by gnome-terminal-server process 5897.

Nov 13 21:05:42 agent-virtual-machine NetworkManager[990]: <info> [1763048142.0766] dhcp4 (ens33): state changed new lease, address=------

Nov 13 21:14:12 agent-virtual-machine update-notifier[5045]: gtk_widget_get_scale_factor: assertion 'GTK_IS_WIDGET (widget)' failed

Nov 13 21:14:15 agent-virtual-machine kernel: [4032.174997] workqueue: psi_avgs_work hogged CPU for >20000us 8 times, consider switching to WQ_UNBOUND

Nov 13 21:14:12 agent-virtual-machine update-notifier[5045]: gtk_widget_get_scale_factor: assertion 'GTK_IS_WIDGET (widget)' failed

Nov 13 21:14:34 agent-virtual-machine dbus-daemon[988]: [system] Activating via systemd: service name='net.reactivated.Fprint' unit='fprintd.service' requested by ':1.79' (uid=1000 pid=3199 comm="/usr/bin/gnome-shell " label="unconfined")

Nov 13 21:14:34 agent-virtual-machine systemd[1]: Starting Fingerprint Authentication Daemon...

Nov 13 21:14:35 agent-virtual-machine dbus-daemon[988]: [system] Successfully activated service 'net.reactivated.Fprint'

Nov 13 21:14:35 agent-virtual-machine systemd[1]: Started Fingerprint Authentication Daemon.

Nov 13 21:14:35 agent-virtual-machine gnome-shell[3199]: JS ERROR: Failed to initialize fprintd service: Gio.IOErrorEnum: GDBus.Error:net.reactivated.Fprint.Error.NoSuchDevice: No devices available#012asyncCallback@resource:///org/gnome/gjs/modules/core/overrides/Gio.js:114:23

Nov 13 21:14:38 agent-virtual-machine dbus-daemon[3054]: [session uid=1000 pid=3054] Activating service name='org.freedesktop.FileManager1' requested by ':1.28' (uid=1000 pid=3199 comm="/usr/bin/gnome-shell " label="unconfined")

Nov 13 21:14:39 agent-virtual-machine NetworkManager[990]: <info> [1763048679.4823] agent-manager: agent[7a8ff55515aad8dc,:1.79/org.gnome.Shell.NetworkAgent/1000]: agent registered

Nov 13 21:14:39 agent-virtual-machine ubuntu-appindicators@ubuntu.com[3199]: unable to update icon for software-update-available

Nov 13 21:14:39 agent-virtual-machine ubuntu-appindicators@ubuntu.com[3199]: unable to update icon for livepatch

Nov 13 21:14:40 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 31 with keysym 31 (keycode a).

Nov 13 21:14:40 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 32 with keysym 32 (keycode b).

Nov 13 21:14:40 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 33 with keysym 33 (keycode c).

Nov 13 21:14:40 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 34 with keysym 34 (keycode d).

Nov 13 21:14:40 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 35 with keysym 35 (keycode e).

Nov 13 21:14:40 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 37 with keysym 37 (keycode 10).

Nov 13 21:14:40 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 38 with keysym 38 (keycode 11).

Nov 13 21:14:40 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 39 with keysym 39 (keycode 12).

Nov 13 21:14:40 agent-virtual-machine gnome-shell[3199]: Window manager warning: Overwriting existing binding of keysym 36 with keysym 36 (keycode f).

Nov 13 21:14:44 agent-virtual-machine dbus-daemon[3054]: [session uid=1000 pid=3054] Successfully activated service 'org.freedesktop.FileManager1'

Nov 13 21:14:44 agent-virtual-machine dbus-daemon[3054]: [session uid=1000 pid=3054] Activating service name='org.gnome.ArchiveManager1' requested by ':1.114' (uid=1000 pid=17083 comm="gjs /usr/share/gnome-shell/extensions/ding@rasters" label="unconfined")

Nov 13 21:14:45 agent-virtual-machine dbus-daemon[3054]: [session uid=1000 pid=3054] Successfully activated service 'org.gnome.ArchiveManager1'

Nov 13 21:14:45 agent-virtual-machine gnome-shell[3199]: DING: Detected async api for thumbnails

Nov 13 21:14:45 agent-virtual-machine gnome-shell[3199]: DING: GNOME nautilus 42.6

Nov 13 21:14:54 agent-virtual-machine nautilus[17080]: Could not delete '.meta.isrunning': No such file or directory

Nov 13 21:15:01 agent-virtual-machine opensearch-dashboards[1024]: {"type":"log","@timestamp":"2025-11-

Nov 13 21:15:06 agent-virtual-machine systemd[1]: fprintd.service: Deactivated successfully.

Nov 13 21:17:01 agent-virtual-machine CRON[17169]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)

Nov 13 21:20:42 agent-virtual-machine NetworkManager[990]: <info> [1763049042.0748] dhcp4 (ens33): state changed new lease, address=----------