HOW TO SETUP WAZUH ON UBUNTU MACHINE.

To install wazuh on Ubuntu machine, you need to first install Ubuntu on your virtualbox.

Tools Used

- **Ubuntu (VirtualBox VM):** The operating system used for the installation.
- **Curl:** A command-line tool used to fetch installation scripts and repository keys.
- **Systemctl:** For starting, stopping, and managing Wazuh services.
- **APT package manager:** For installing and removing Wazuh components.
- **VirtualBox Settings:** Adjusted system resources (RAM and CPU cores) to meet Wazuh's hardware requirements.

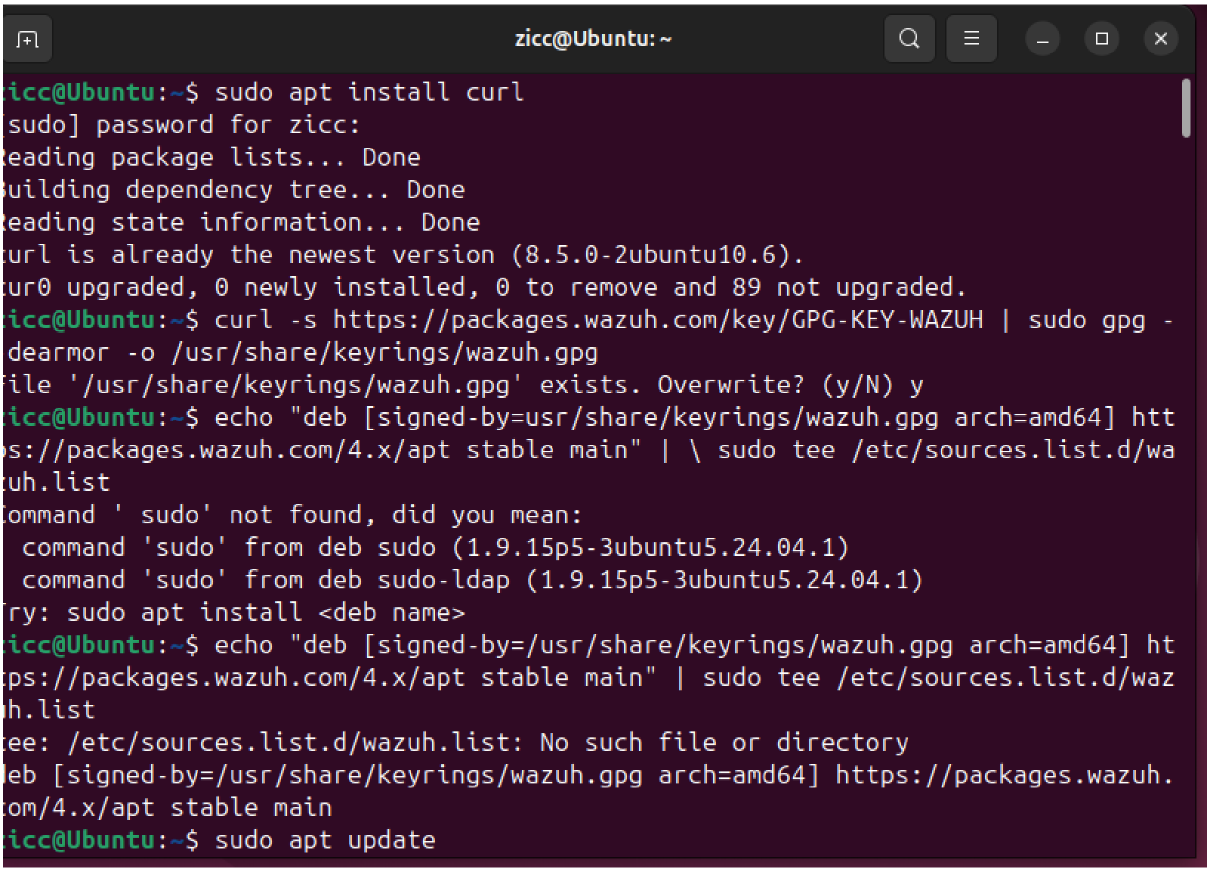
Then use the command **Sudo apt install curl** to install the curl.

I tried adding the wazuh GPG Key **curl -sO https://packages.wazuh.com/4.x/wazuh-repository.key && sudo gpg --no-default-keyring --keyring /usr/share/keyrings/wazuh-archive-keyring.gpg --import ./wazuh-repository.key.**

The error code was: **no default keyring**. I furthered by adding the wazuh repository.

echo "deb [signed-by=/usr/share/keyrings/wazu-archive-keyring.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list

This gave an error of no file or directory.



```
icc@Ubuntu:~$ sudo apt install curl
sudo] password for zicc:
eading package lists... Done
uilding dependency tree... Done
eading state information... Done
url is already the newest version (8.5.0-2ubuntu10.6).
ur0 upgraded, 0 newly installed, 0 to remove and 89 not upgraded.
icc@Ubuntu:~$ curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo gpg -
dearmor -o /usr/share/keyrings/wazuh.gpg
ile '/usr/share/keyrings/wazuh.gpg' exists. Overwrite? (y/N) y
icc@Ubuntu:~$ echo "deb [signed-by=usr/share/keyrings/wazuh.gpg arch=amd64] htt
s://packages.wazuh.com/4.x/apt stable main" | \ sudo tee /etc/sources.list.d/wa
uh.list
ommand ' sudo' not found, did you mean:
 command 'sudo' from deb sudo (1.9.15p5-3ubuntu5.24.04.1)
 command 'sudo' from deb sudo-ldap (1.9.15p5-3ubuntu5.24.04.1)
ry: sudo apt install <deb name>
icc@Ubuntu:~$ echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg arch=amd64] ht
ps://packages.wazuh.com/4.x/apt stable main" | sudo tee /etc/sources.list.d/waz
h.list
ee: /etc/sources.list.d/wazuh.list: No such file or directory
leb [signed-by=/usr/share/keyrings/wazuh.gpg arch=amd64] https://packages.wazuh.
om/4.x/apt stable main
icc@Ubuntu:~$ sudo apt update
```

At this point, I knew something was wrong and decided to start it all over again, so I used the following command to delete everything I have installed about wazuh and start afresh.

Commands.

sudo systemctl stop wazuh-dashboard

sudo apt-get purge wazuh-dashboard

sudo systemctl stop wazuh-manager

sudo apt-get purge wazuh-manager

sudo rm -rf /var/ossec

sudo rm -rf /etc/filebeat

sudo systemctl stop wazuh-indexer

sudo apt-get purge wazuh-indexer

sudo rm -rf /var/lib/wazuh-indexer

sudo rm -rf /var/log/wazuh-indexer

sudo apt-get purge opensearch opensearch-dashboards filebeat

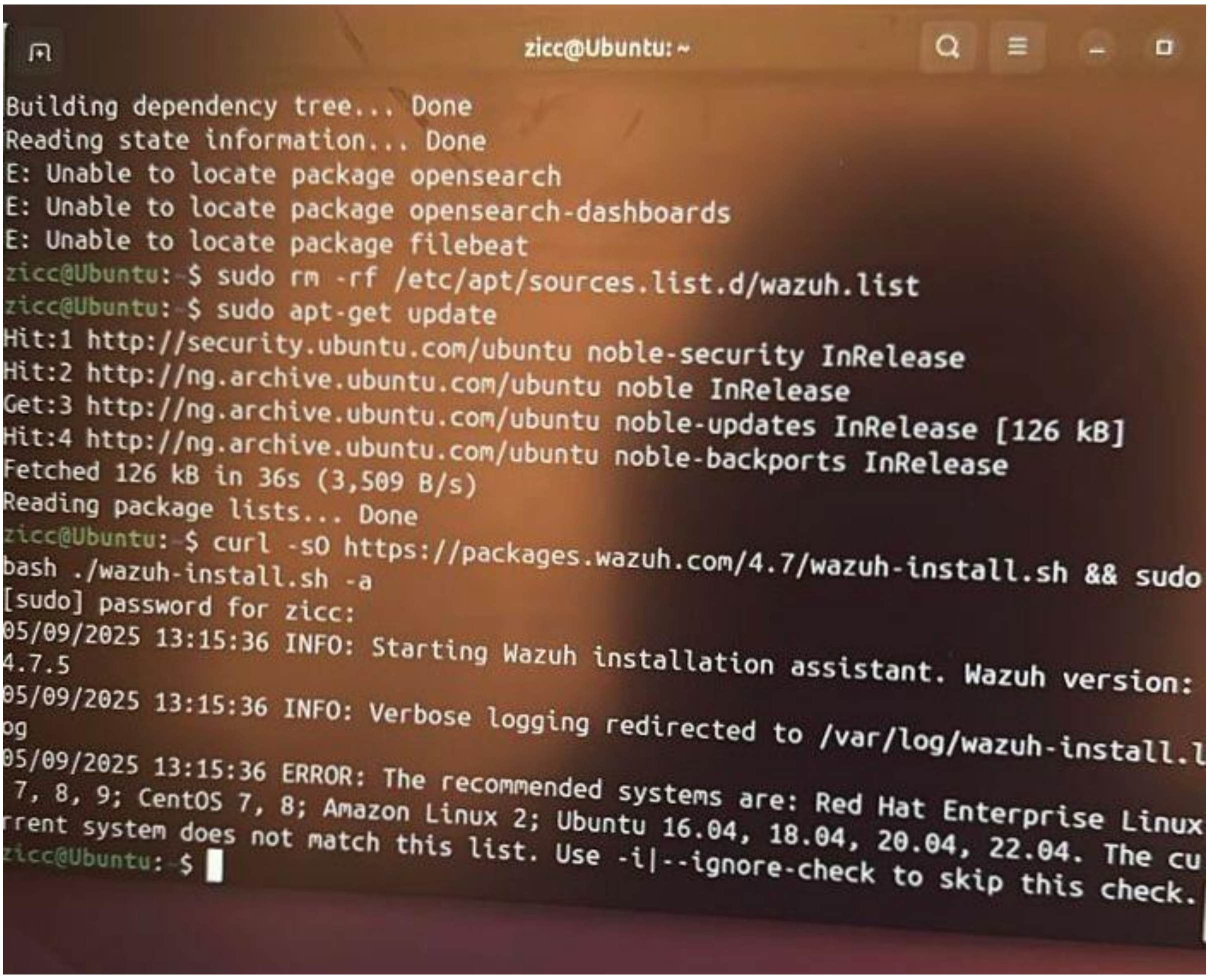
sudo rm -rf /etc/apt/sources.list.d/wazuh.list

sudo apt-get update.

The following commands are to remove wazuh dashboard, wazuh indexer and wazuh manager from the directories.

After these command prompts, I ran this command to install the wazuh afresh.

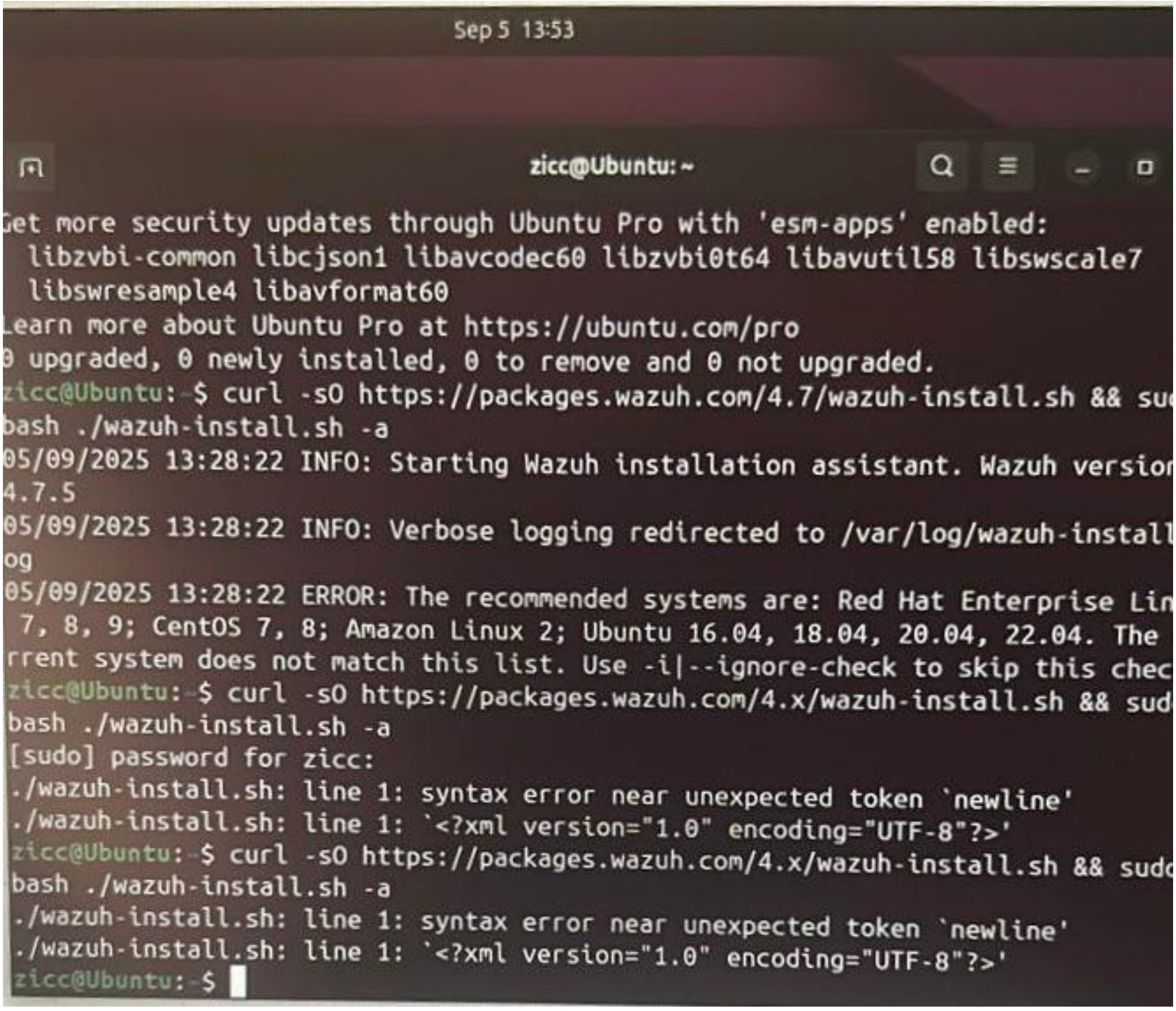
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh –a



```
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package opensearch
E: Unable to locate package opensearch-dashboards
E: Unable to locate package filebeat
zicc@Ubuntu:~$ sudo rm -rf /etc/apt/sources.list.d/wazuh.list
zicc@Ubuntu:~$ sudo apt-get update
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://ng.archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://ng.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:4 http://ng.archive.ubuntu.com/ubuntu noble-backports InRelease
Fetched 126 kB in 36s (3,509 B/s)
Reading package lists... Done
zicc@Ubuntu:~$ curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo
bash ./wazuh-install.sh -a
[sudo] password for zicc:
05/09/2025 13:15:36 INFO: Starting Wazuh installation assistant. Wazuh version:
4.7.5
05/09/2025 13:15:36 INFO: Verbose logging redirected to /var/log/wazuh-install.l
og
05/09/2025 13:15:36 ERROR: The recommended systems are: Red Hat Enterprise Linux
 7, 8, 9; CentOS 7, 8; Amazon Linux 2; Ubuntu 16.04, 18.04, 20.04, 22.04. The cu
rrent system does not match this list. Use -i|--ignore-check to skip this check.
zicc@Ubuntu:~$ █
```

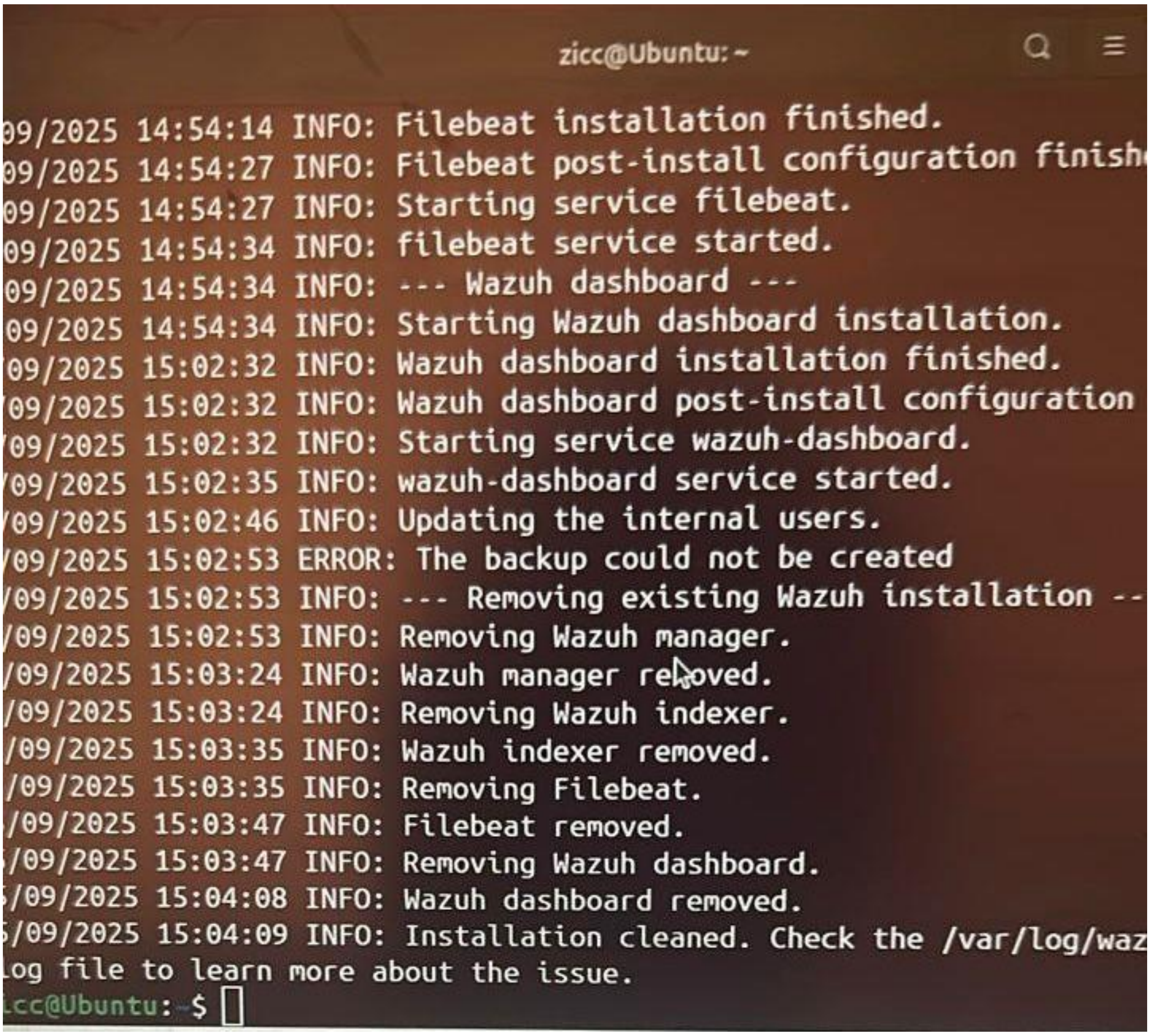
The issue here is that I was running a version of wazuh that was not compatible with my Ubuntu. I was initially meant to install wazuh **version 4.12** on Ubuntu **version 24.04**. the wazuh **version 4.7** is only compatible with Ubuntu **version 22.04** and lower.

I changed the **4.7** to **4.x** and got a new error.



```
Get more security updates through Ubuntu Pro with 'esm-apps' enabled:
  libzvbi-common libcjson1 libavcodec60 libzvbi0t64 libavutil58 libswscale7
  libswresample4 libavformat60
Learn more about Ubuntu Pro at https://ubuntu.com/pro
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
zicc@Ubuntu:~$ curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && su
bash ./wazuh-install.sh -a
05/09/2025 13:28:22 INFO: Starting Wazuh installation assistant. Wazuh versio
4.7.5
05/09/2025 13:28:22 INFO: Verbose logging redirected to /var/log/wazuh-install
og
05/09/2025 13:28:22 ERROR: The recommended systems are: Red Hat Enterprise Lin
 7, 8, 9; CentOS 7, 8; Amazon Linux 2; Ubuntu 16.04, 18.04, 20.04, 22.04. The
rrent system does not match this list. Use -i|--ignore-check to skip this chec
zicc@Ubuntu:~$ curl -sO https://packages.wazuh.com/4.x/wazuh-install.sh && sud
bash ./wazuh-install.sh -a
[sudo] password for zicc:
./wazuh-install.sh: line 1: syntax error near unexpected token `newline'
./wazuh-install.sh: line 1: `<?xml version="1.0" encoding="UTF-8"?>'
zicc@Ubuntu:~$ curl -sO https://packages.wazuh.com/4.x/wazuh-install.sh && sudo
bash ./wazuh-install.sh -a
./wazuh-install.sh: line 1: syntax error near unexpected token `newline'
./wazuh-install.sh: line 1: `<?xml version="1.0" encoding="UTF-8"?>'
zicc@Ubuntu:~$
```

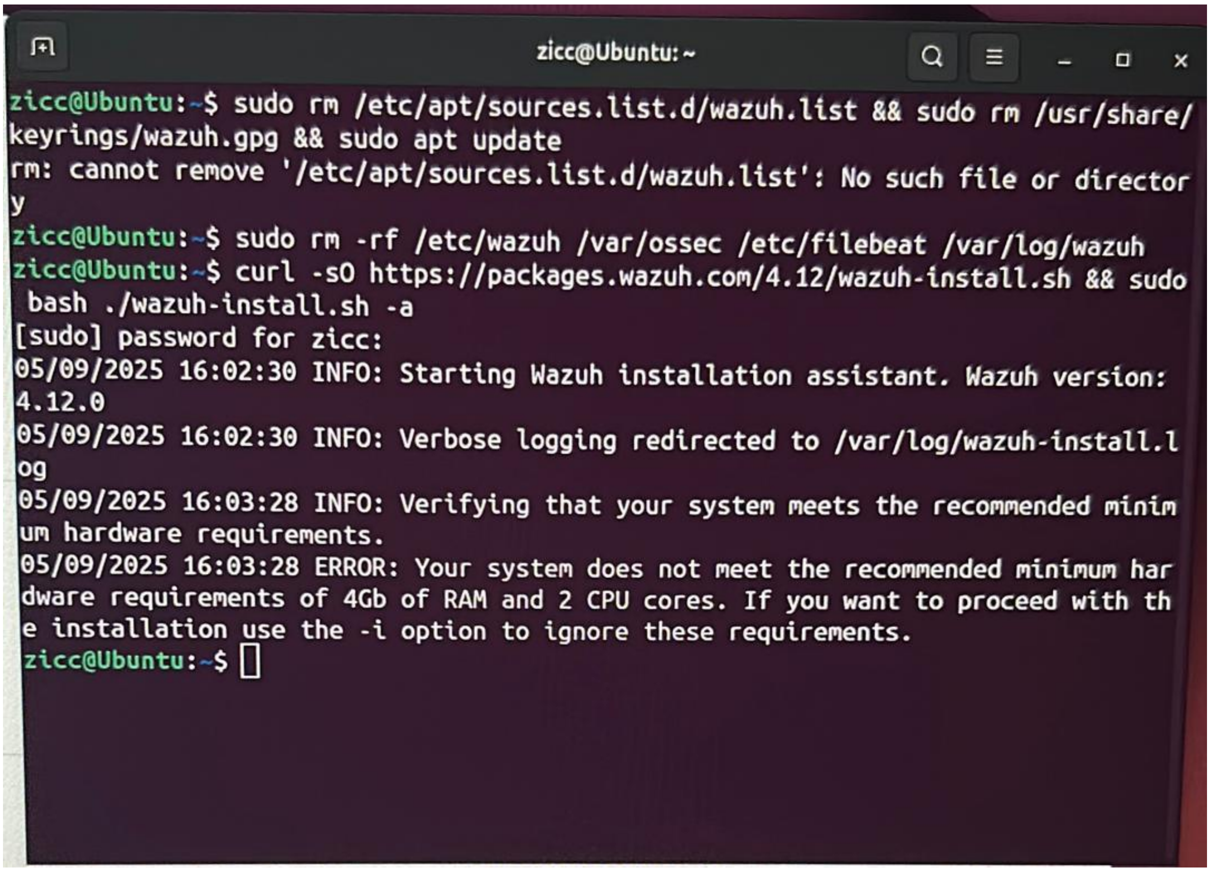
I then used the **–i** to ignore and continue the process, the version of wazuh did not allow it to backup, so it removes it.



```
09/2025 14:54:14 INFO: Filebeat installation finished.
09/2025 14:54:27 INFO: Filebeat post-install configuration finish
09/2025 14:54:27 INFO: Starting service filebeat.
09/2025 14:54:34 INFO: filebeat service started.
09/2025 14:54:34 INFO: --- Wazuh dashboard ---
09/2025 14:54:34 INFO: Starting Wazuh dashboard installation.
09/2025 15:02:32 INFO: Wazuh dashboard installation finished.
/09/2025 15:02:32 INFO: Wazuh dashboard post-install configuration
/09/2025 15:02:32 INFO: Starting service wazuh-dashboard.
/09/2025 15:02:35 INFO: wazuh-dashboard service started.
/09/2025 15:02:46 INFO: Updating the internal users.
/09/2025 15:02:53 ERROR: The backup could not be created
/09/2025 15:02:53 INFO: --- Removing existing Wazuh installation --
/09/2025 15:02:53 INFO: Removing Wazuh manager.
/09/2025 15:03:24 INFO: Wazuh manager removed.
/09/2025 15:03:24 INFO: Removing Wazuh indexer.
/09/2025 15:03:35 INFO: Wazuh indexer removed.
/09/2025 15:03:35 INFO: Removing Filebeat.
/09/2025 15:03:47 INFO: Filebeat removed.
/09/2025 15:03:47 INFO: Removing Wazuh dashboard.
5/09/2025 15:04:08 INFO: Wazuh dashboard removed.
5/09/2025 15:04:09 INFO: Installation cleaned. Check the /var/log/waz
og file to learn more about the issue.
icc@Ubuntu:~$
```

I had to troubleshoot it again by removing everything using the long commands earlier and tried reinstalling it again afresh.

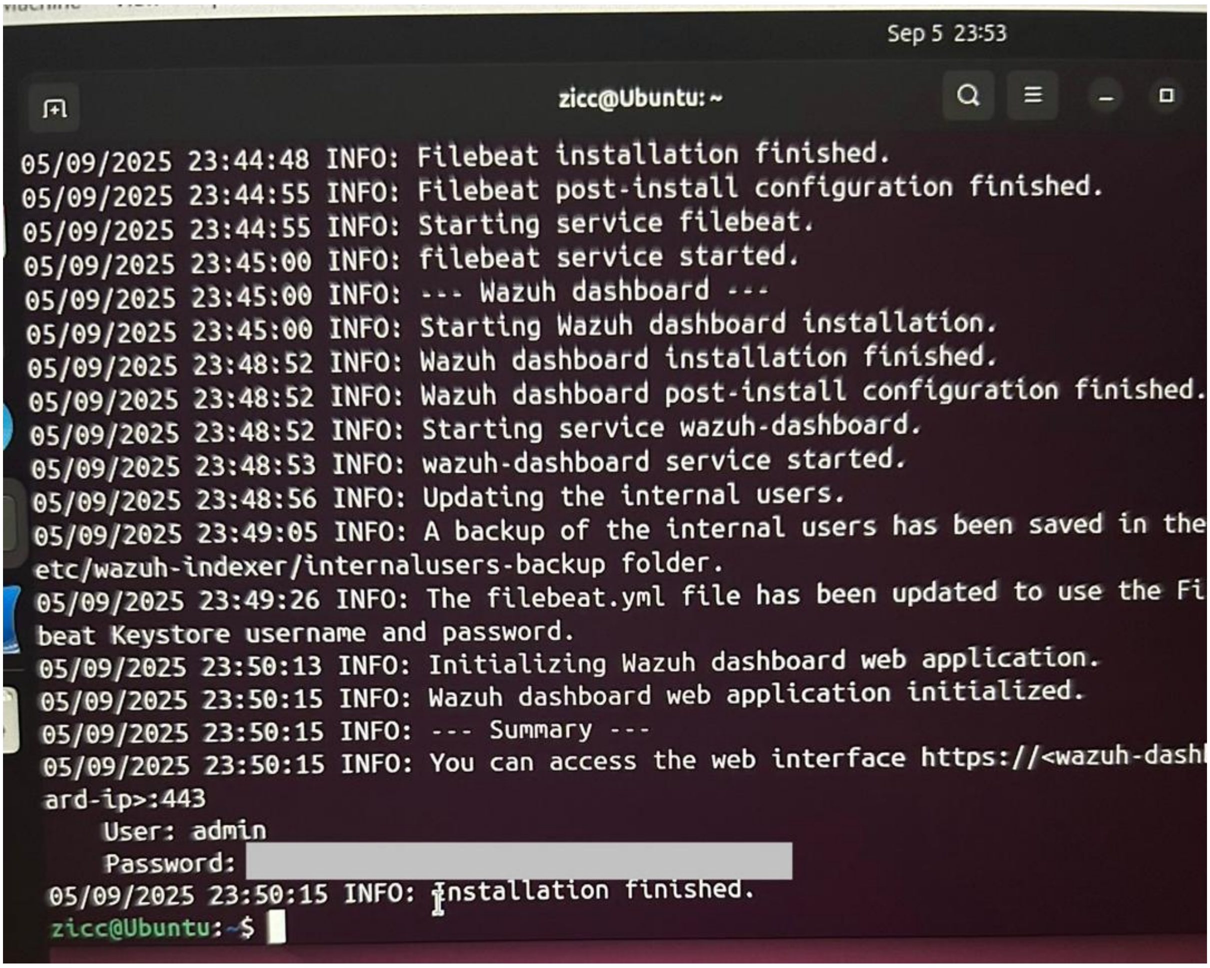
I tried this command **curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh –a**



```
zicc@Ubuntu:~$ sudo rm /etc/apt/sources.list.d/wazuh.list && sudo rm /usr/share/
keyrings/wazuh.gpg && sudo apt update
rm: cannot remove '/etc/apt/sources.list.d/wazuh.list': No such file or director
y
zicc@Ubuntu:~$ sudo rm -rf /etc/wazuh /var/ossec /etc/filebeat /var/log/wazuh
zicc@Ubuntu:~$ curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo
 bash ./wazuh-install.sh -a
[sudo] password for zicc:
05/09/2025 16:02:30 INFO: Starting Wazuh installation assistant. Wazuh version:
4.12.0
05/09/2025 16:02:30 INFO: Verbose logging redirected to /var/log/wazuh-install.l
og
05/09/2025 16:03:28 INFO: Verifying that your system meets the recommended minim
um hardware requirements.
05/09/2025 16:03:28 ERROR: Your system does not meet the recommended minimum har
dware requirements of 4Gb of RAM and 2 CPU cores. If you want to proceed with th
e installation use the -i option to ignore these requirements.
zicc@Ubuntu:~$ 
```

Here, it popped up the error of minimum hardware requirements, so I had to shutdown my Ubuntu machine, go to my virtualbox Ubuntu settings, go to system, increase the base memory to **4GB,** go to processor tab and increase it to **2 CPU Cores,** which are the minimum requirements.

I ran the command again **curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh –a.** and it finally worked!. It gave me my wazuh username and password.

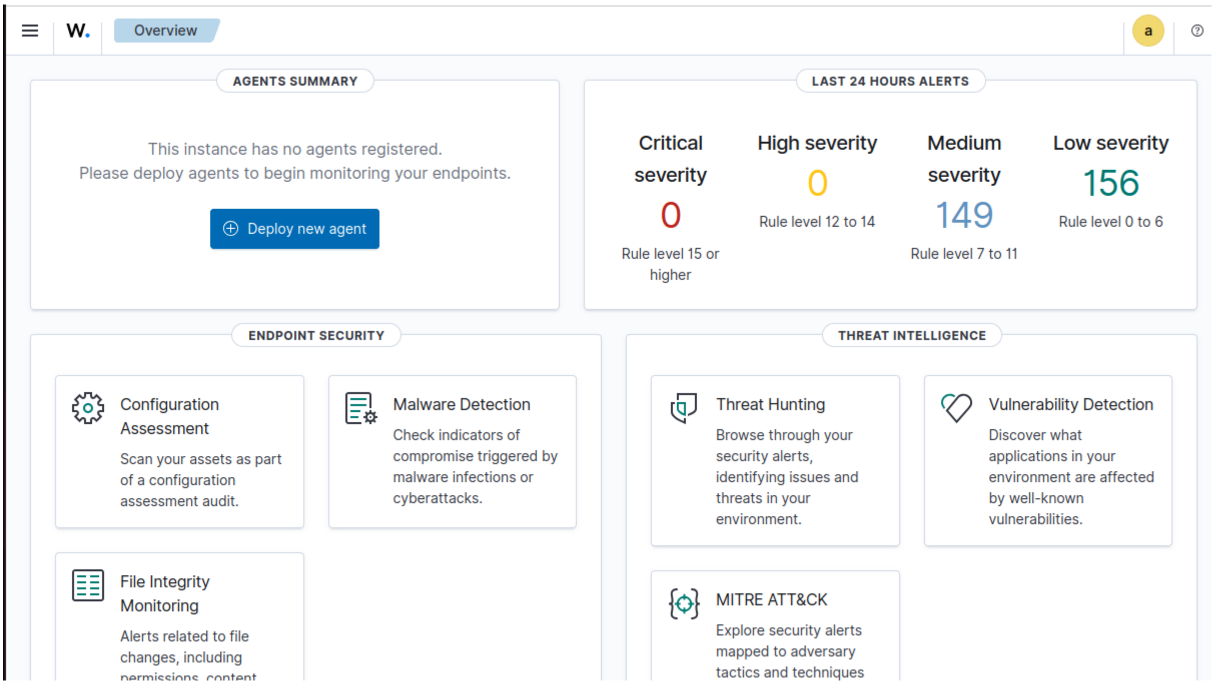


Sep 5 23:53

zicc@Ubuntu: ~

```
05/09/2025 23:44:48 INFO: Filebeat installation finished.
05/09/2025 23:44:55 INFO: Filebeat post-install configuration finished.
05/09/2025 23:44:55 INFO: Starting service filebeat.
05/09/2025 23:45:00 INFO: filebeat service started.
05/09/2025 23:45:00 INFO: --- Wazuh dashboard ---
05/09/2025 23:45:00 INFO: Starting Wazuh dashboard installation.
05/09/2025 23:48:52 INFO: Wazuh dashboard installation finished.
05/09/2025 23:48:52 INFO: Wazuh dashboard post-install configuration finished.
05/09/2025 23:48:52 INFO: Starting service wazuh-dashboard.
05/09/2025 23:48:53 INFO: wazuh-dashboard service started.
05/09/2025 23:48:56 INFO: Updating the internal users.
05/09/2025 23:49:05 INFO: A backup of the internal users has been saved in the
etc/wazuh-indexer/internalusers-backup folder.
05/09/2025 23:49:26 INFO: The filebeat.yml file has been updated to use the Fi
beat Keystore username and password.
05/09/2025 23:50:13 INFO: Initializing Wazuh dashboard web application.
05/09/2025 23:50:15 INFO: Wazuh dashboard web application initialized.
05/09/2025 23:50:15 INFO: --- Summary ---
05/09/2025 23:50:15 INFO: You can access the web interface https://<wazuh-dash
ard-ip>:443
    User: admin
    Password: [redacted]
05/09/2025 23:50:15 INFO: Installation finished.
zicc@Ubuntu:~$
```

I logged into the wazuh using the details.



AGENTS SUMMARY

This instance has no agents registered.
Please deploy agents to begin monitoring your endpoints.

Deploy new agent

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	149	156
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

File Integrity Monitoring
Alerts related to file changes, including permissions, content

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques

Problems I Encountered

During the installation, I Faced several issues:

1. **GPG Key Error:** An error occurred when I was trying to add the Wazuh GPG key due to “no default keyring.”
2. **Repository Error:** Adding the repository failed with “no file or directory.”
3. **Version Compatibility:** Initially, I installed Wazuh version 4.7, which only supports Ubuntu 22.04 and lower. Since the system was running Ubuntu 24.04, it was incompatible.
4. **Minimum Hardware Requirements:** An error was raised which indicated that I had insufficient system resources.i had to reconfigure the VirtualBox VM with at least 4 GB of RAM and 2 CPU cores before the installation could proceed.
5. **Reinstallation Attempts:** After some errors, I removed the Wazuh, Filebeat, Indexer, and related components before I attempted a fresh installation.

What I Learnt

- The importance of using the correct Wazuh version for the Ubuntu release, as my first attempt failed due to incompatibility.
- How to properly clean up failed installations using purge commands and by removing leftover directories.
- That meeting the minimum hardware requirements is essential, so I increased the VM to 4 GB RAM and 2 CPU cores.
- Improved troubleshooting skills while resolving GPG key, repository, and compatibility errors.
- A clearer understanding of how the Wazuh installation script sets up the Manager, Indexer, and Dashboard.

Uses of Wazuh

- Threat Detection and Monitoring.
- Log Data Analysis
- File Integrity Monitoring.

- Incident Response

Conclusion

The installation of Wazuh on Ubuntu was challenging but rewarding. Errors with version compatibility, keys, and repositories pushed me to strengthen my troubleshooting and system administration skills. Once I adjusted hardware resources and used the correct version (Wazuh 4.12 for Ubuntu 24.04), the setup was successful. This project not only taught me how to deploy a SIEM tool but also highlighted the value of persistence, attention to detail, and the role of Wazuh in enhancing security monitoring and operations