Wazuh SIEM Deployment and Monitoring

Name: Imafidon Joseph
Project: Cybersecurity Project
Date: September 14, 2025

1. Introduction

Wazuh is an open-source Security Information and Event Management (SIEM) solution used for threat detection, compliance monitoring, and incident response. It provides log collection, file integrity monitoring, vulnerability detection, and mapping of events to frameworks like MITRE ATT&CK.

This documentation outlines the process of installing Wazuh Manager and Dashboard, deploying agents, configuring alerts, and testing the system.

---

2. Objective

- To set up and operate a functional Wazuh SIEM environment.
- To deploy an agent on a client machine (Kali Linux).
- To monitor system activities such as failed logins, privilege escalation, and vulnerabilities.
- To create alert rules and notifications for security events.

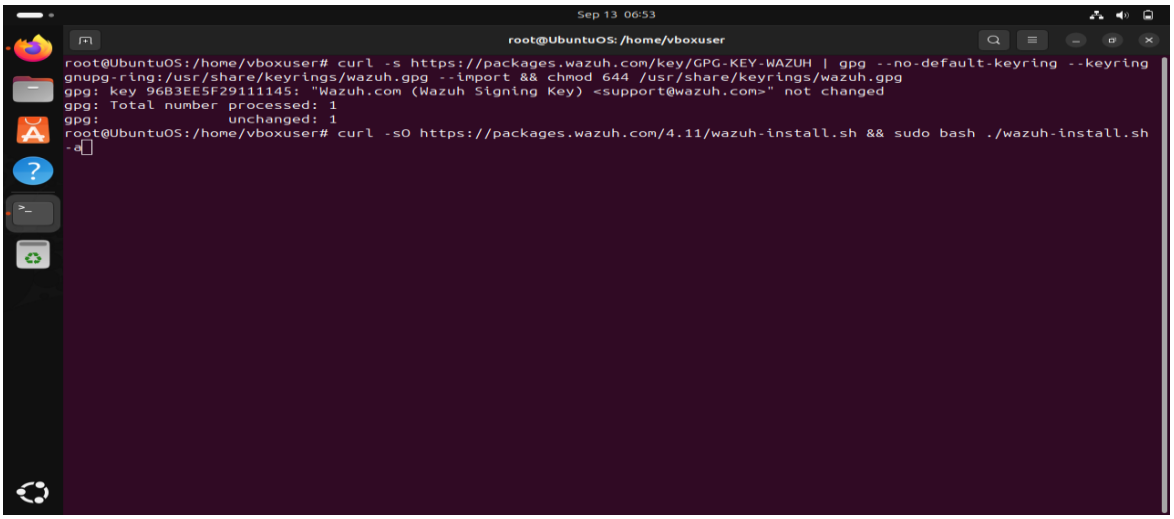
---

3. Requirements

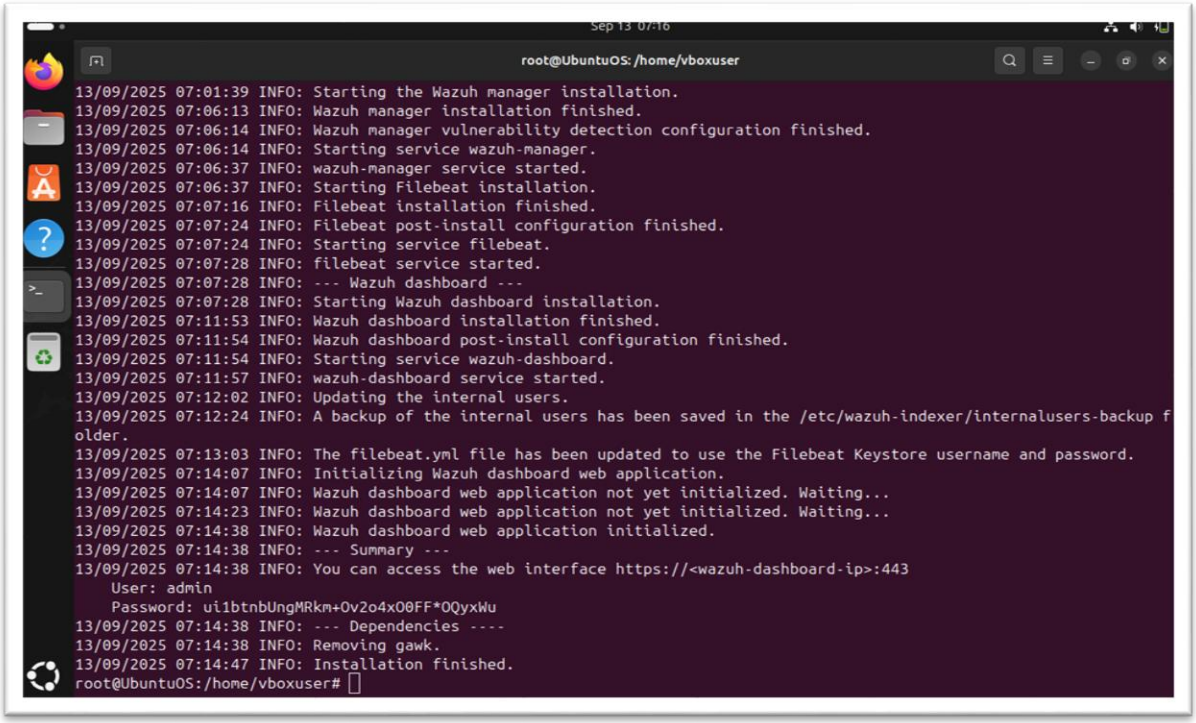
- **Server VM** (Ubuntu with internet access) for Wazuh Manager & Dashboard.
- **Client VM** (Kali Linux/Ubuntu) for Wazuh Agent.
- VirtualBox/VMware with network configured as **Bridged Adapter or Host-only + NAT**.
- Stable internet connection.
- Basic knowledge of Linux commands.

Step 1 Install Wazuh Manager & Dashboard

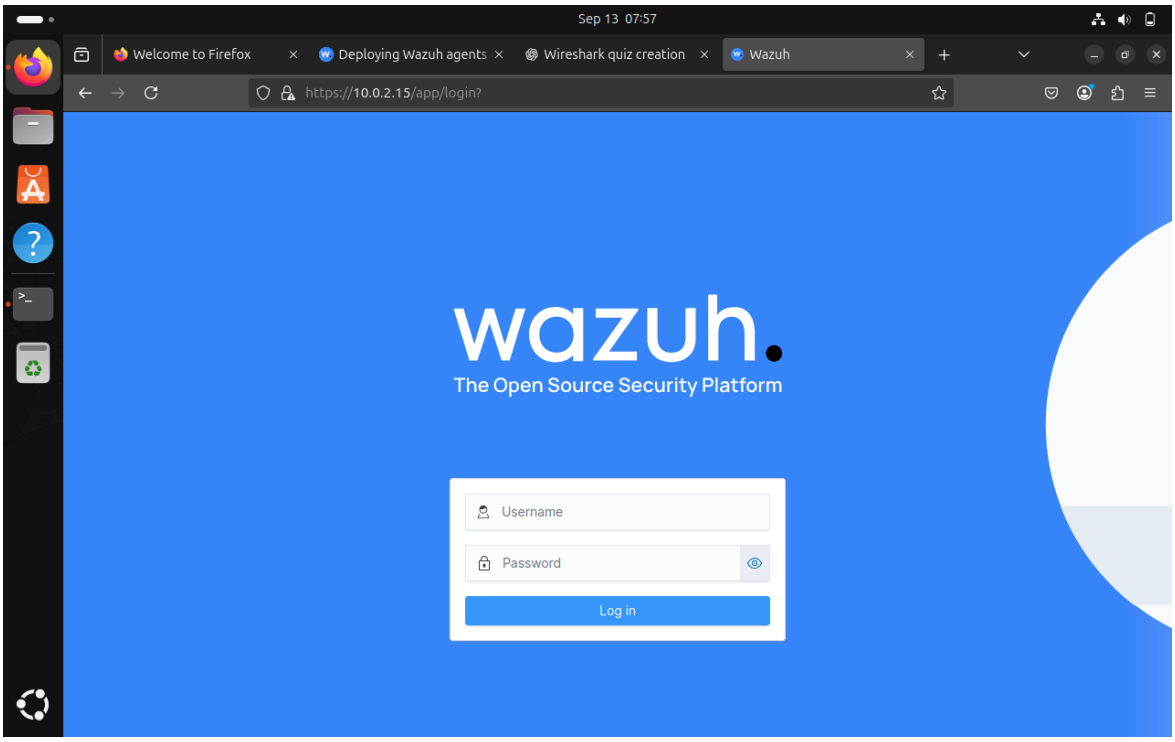
Installed Wazuh Manager, Filebeat, and Dashboard on Ubuntu server using the official installation script. Accessed the dashboard via https://:443.



Run installation script: curl -sO https://packages.wazuh.com/4.x/wazuh-install.sh && sudo bash ./wazuh-install.sh -a



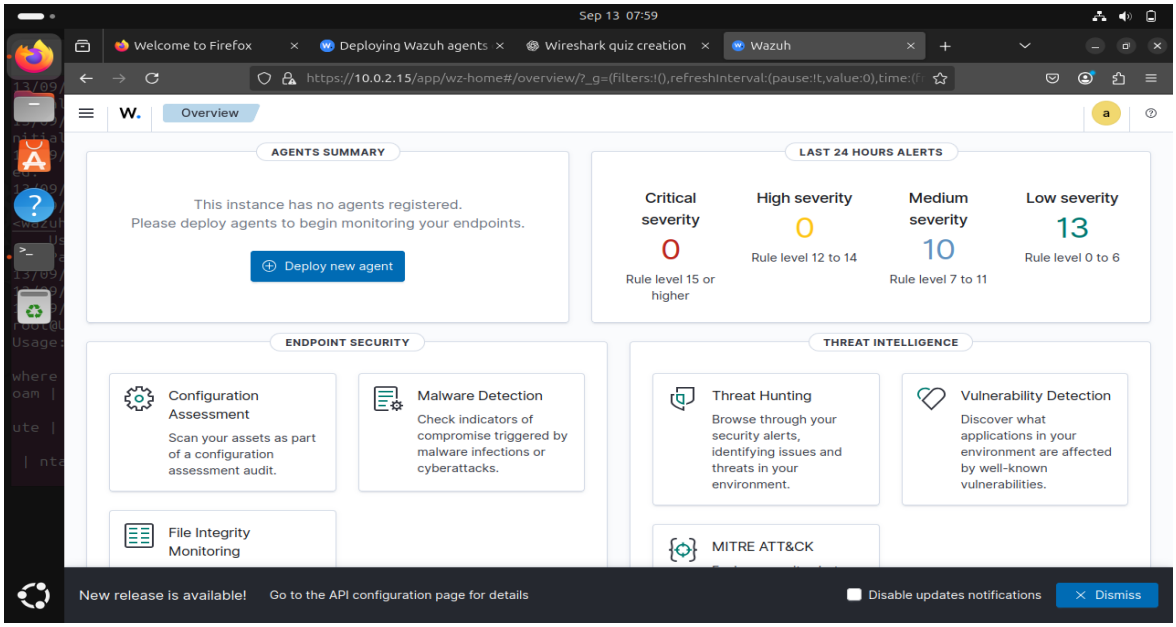
Access dashboard with your IP address, and login with the password given after installation



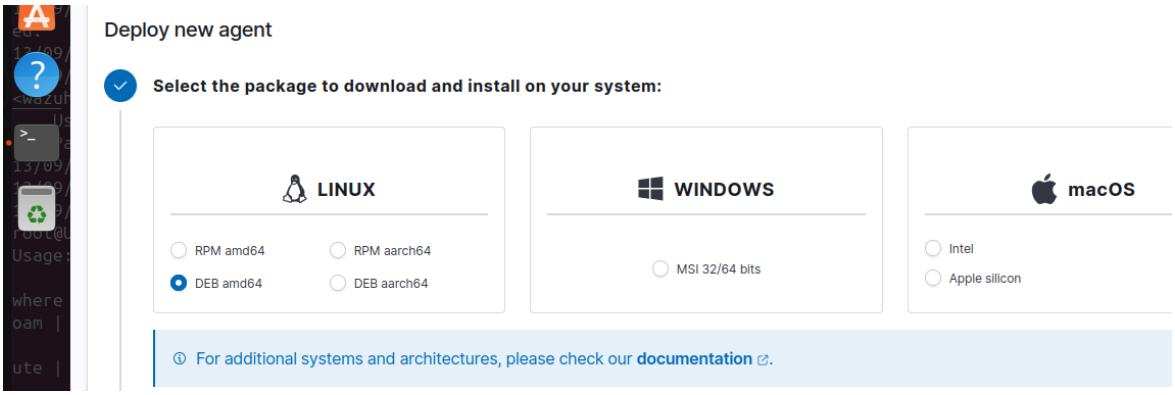
Impute the password and login to your wazor admin account.

Step 2 Deploy Agent on Kali Linux

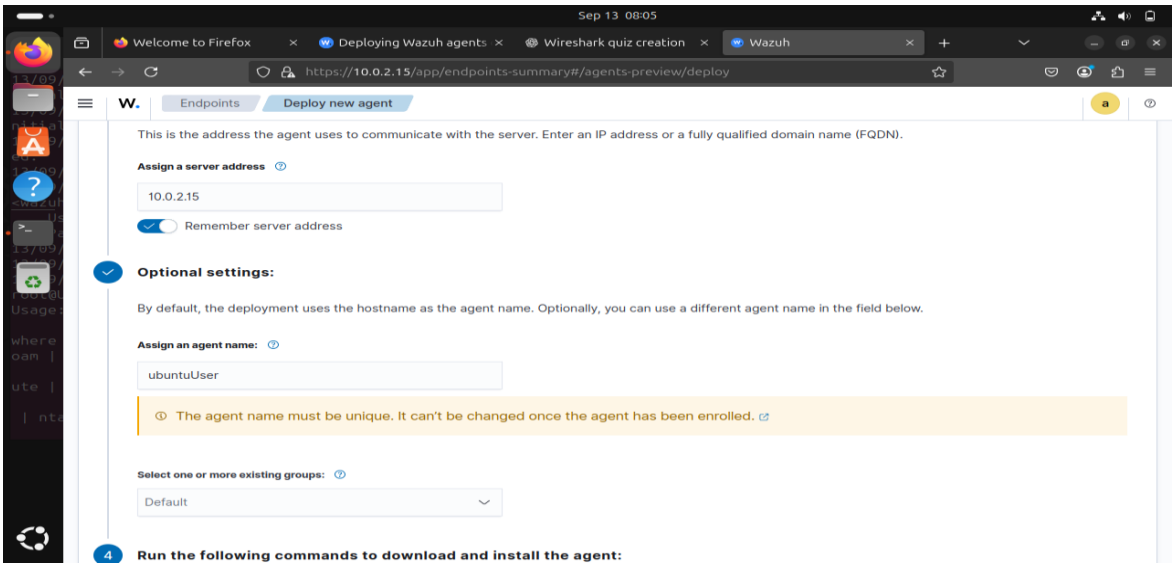
Downloaded and installed the Wazuh agent .deb package, configured ossec.conf with the manager IP, and enabled the agent service.



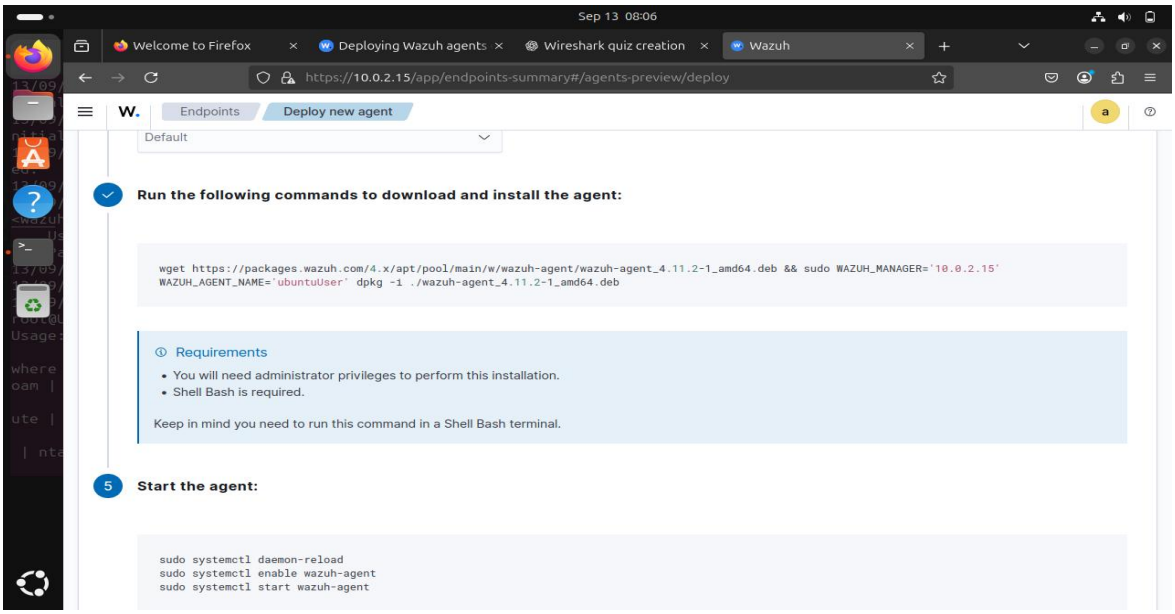
On the Administrator dashboard we need to Deploy an agent in other to be able to get logs from the system, monitor, analyze, detect vulnerability and other function



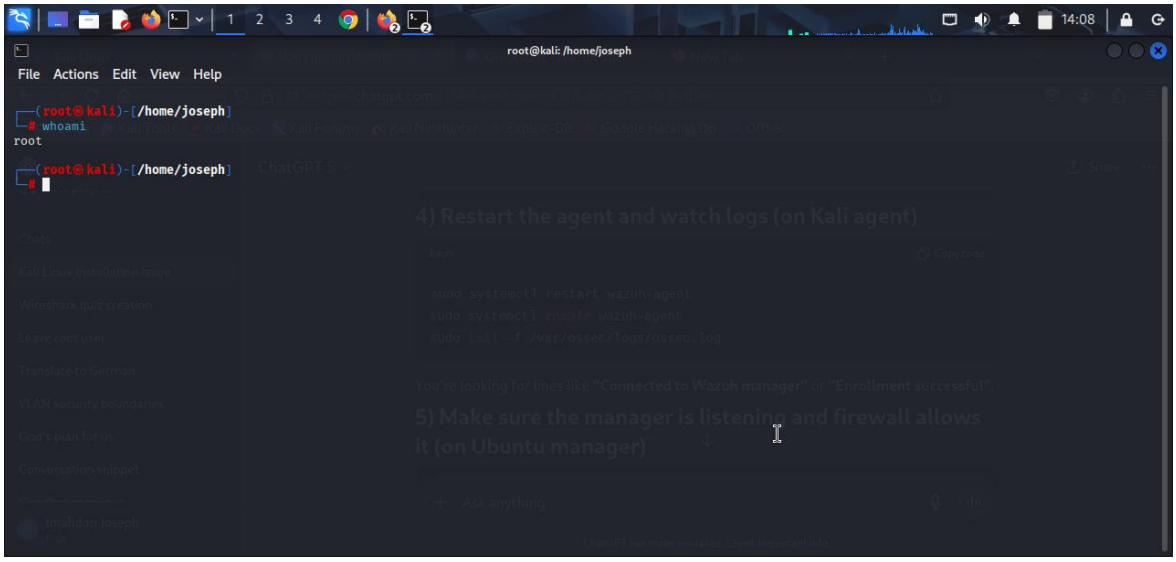
We will be using Kali Linux as our agent, so we will choose DEB amd64



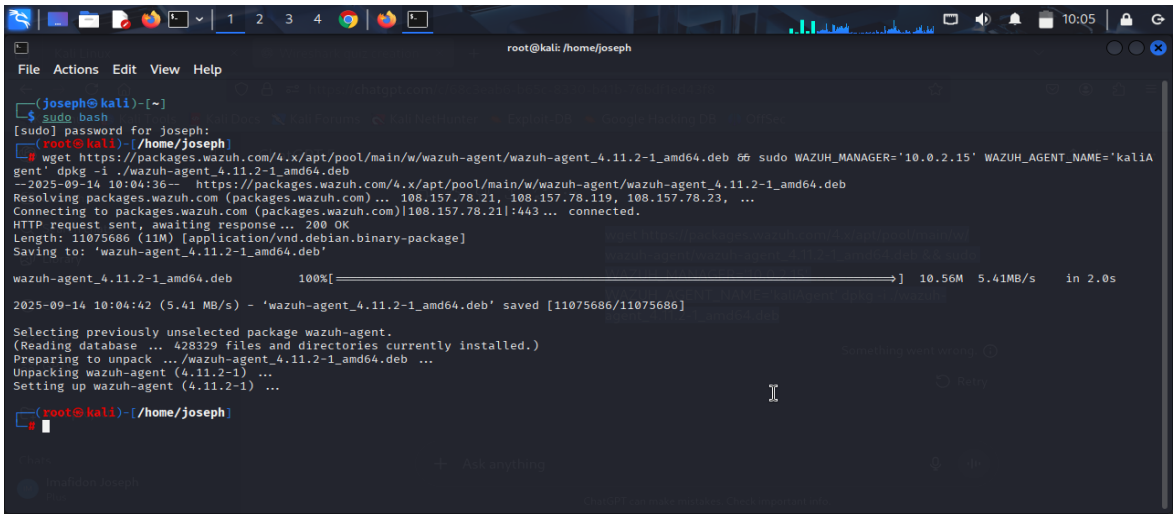
We will use our IP Address as the server address we can give our agent name any name we choose to use

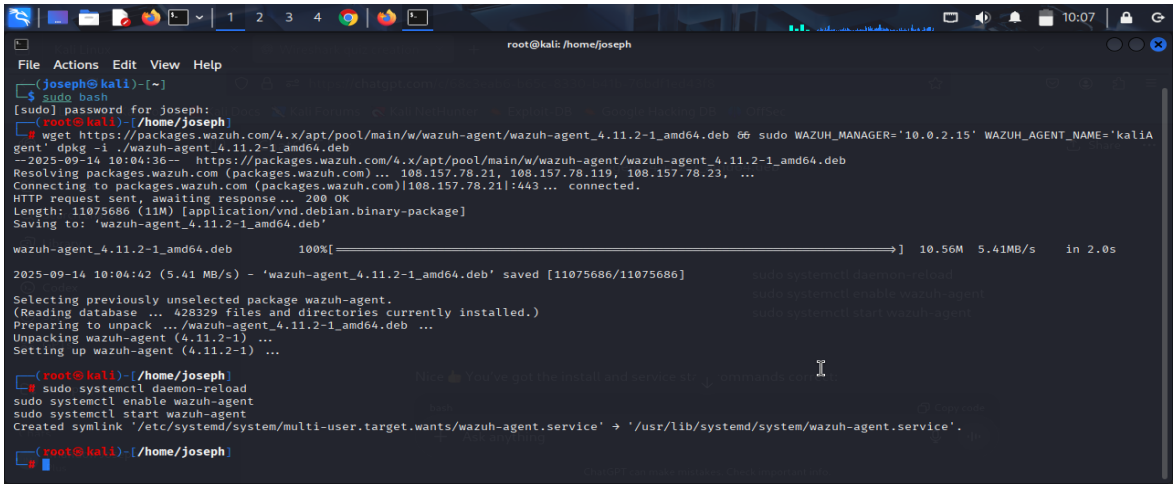


Run the following commands on your Agent system.



In other to run the command we have to login to root user, to do that we can simply type sudo su or sudo bash.

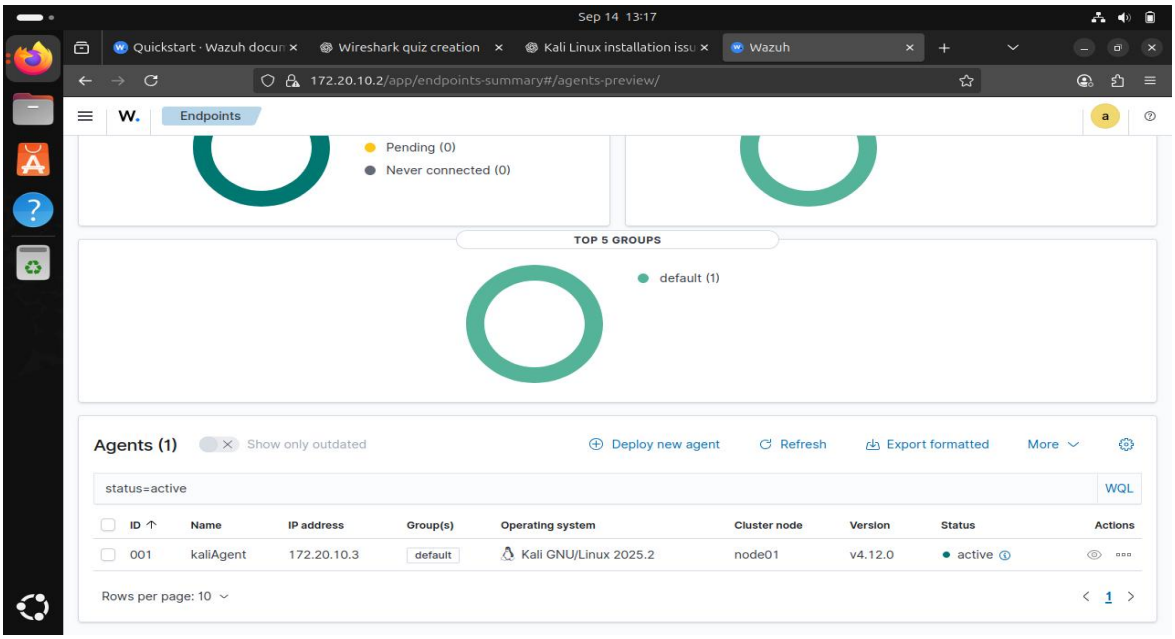




After running the two commands we will go back to our wazuh dashboard to see if our agent has been displayed.

Step 3 Verify Agent Connection

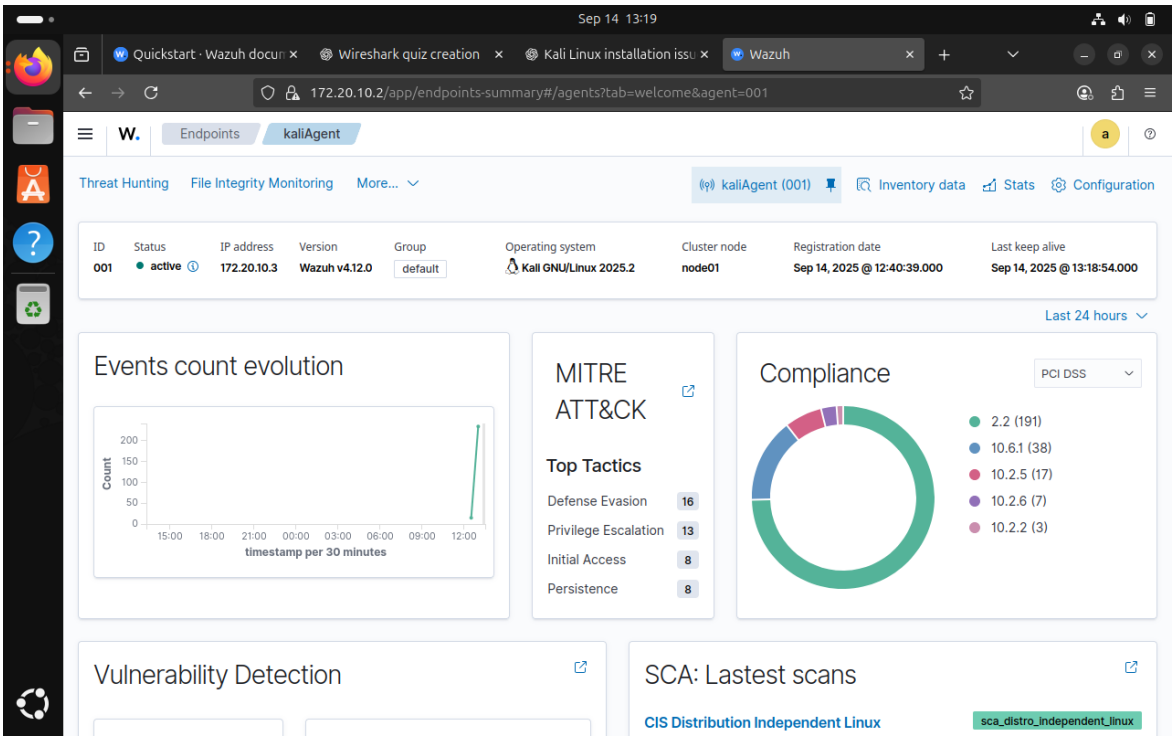
Verified in the Wazuh Dashboard that the Kali agent appeared as active.



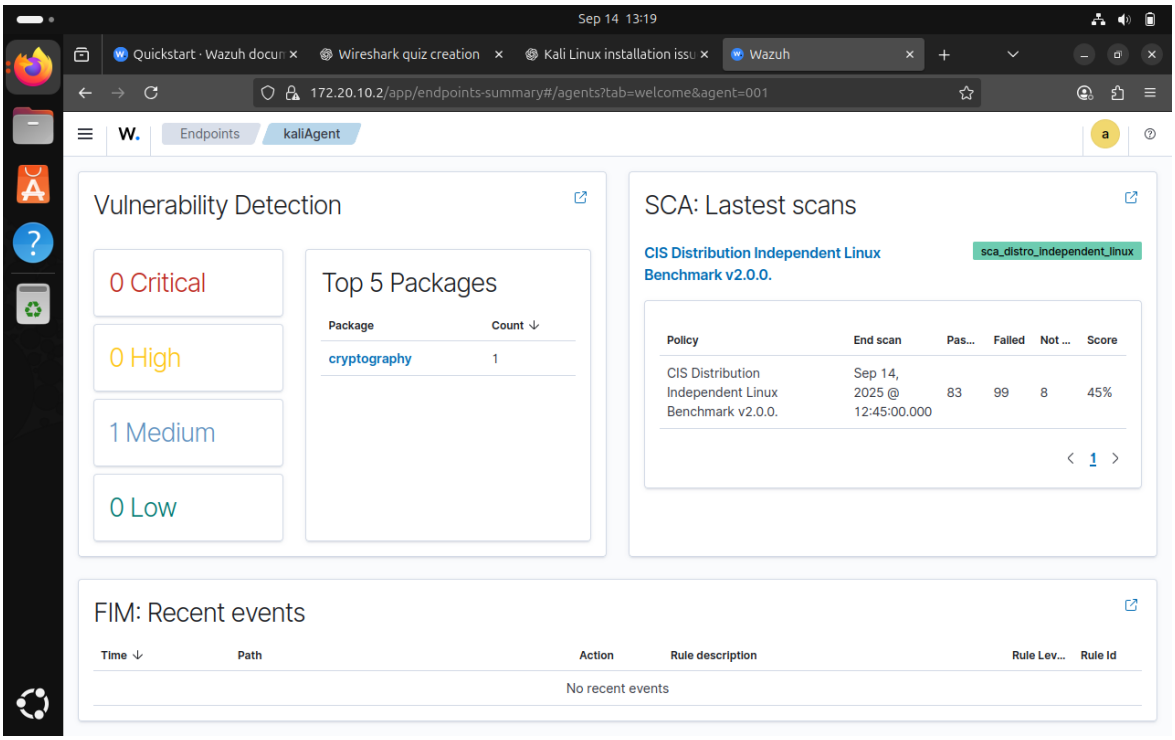
As it is seen in the picture above our agent is up and running.

Step 4 Dashboard Analysis

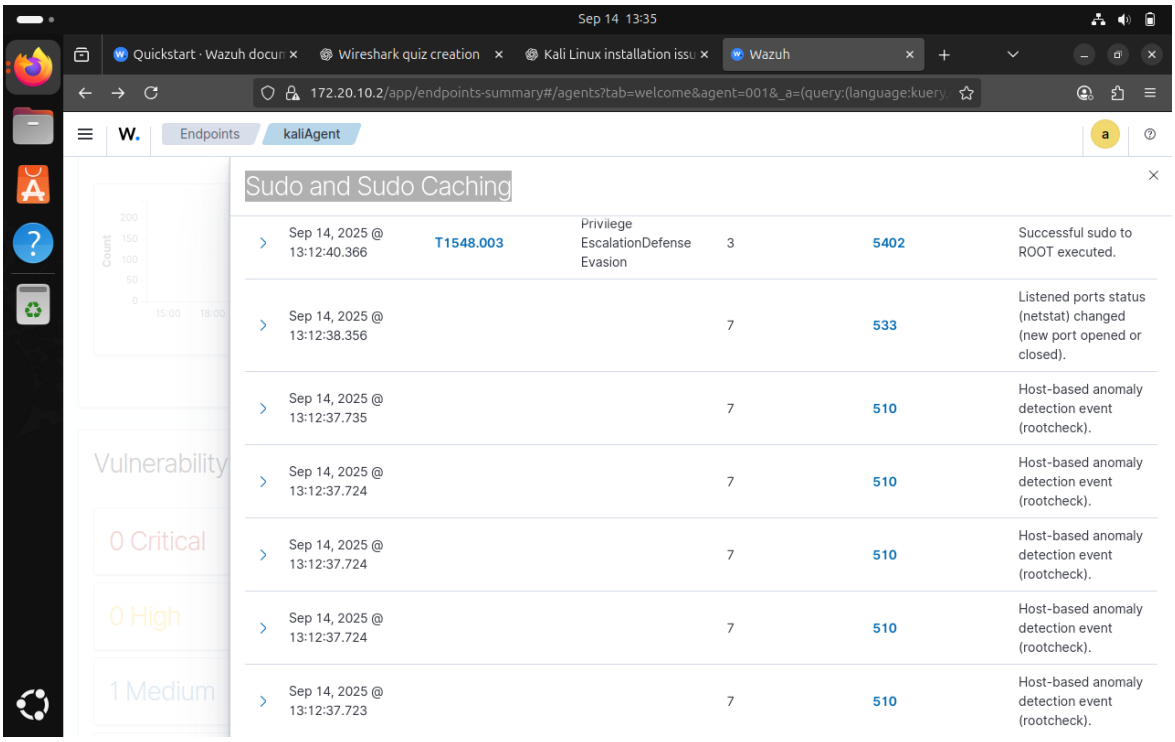
Observed events evolution, MITRE ATT&CK; detections, vulnerability scans, and compliance results.



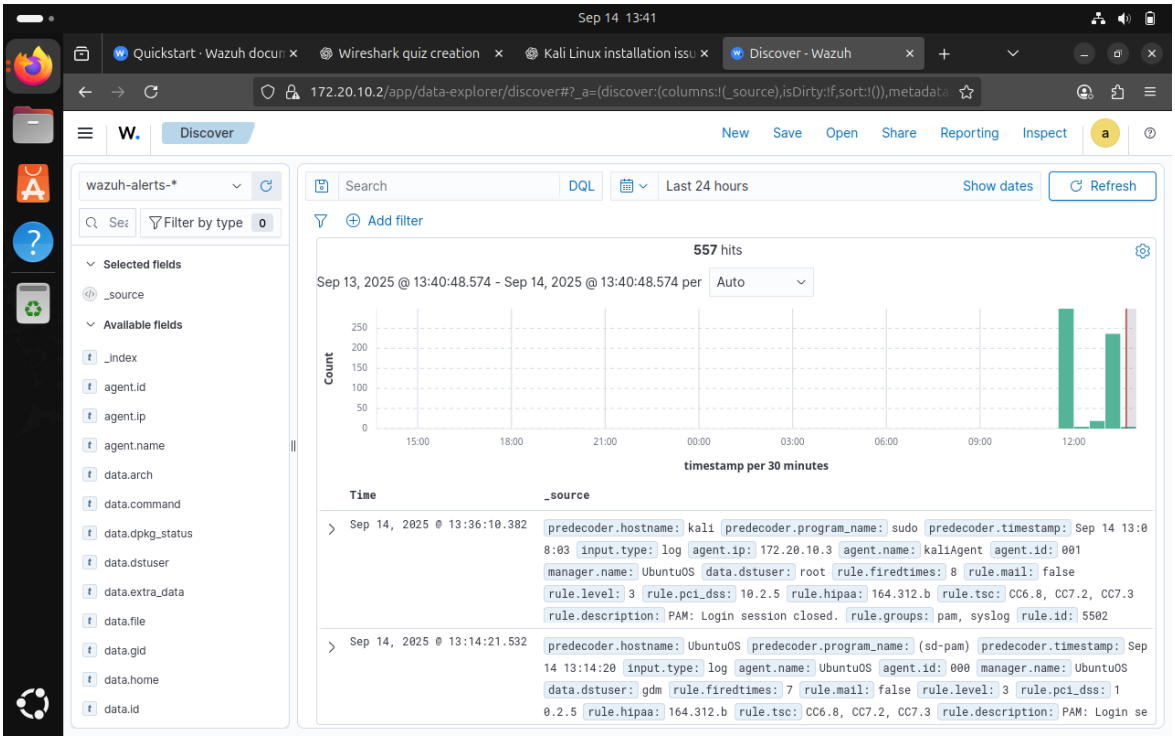
This dashboard gives you a **quick health and threat overview** of your monitored agent: system status, attack detections, compliance gaps, and vulnerabilities.



This is a vulnerability detection dashboard and as it is seen our system is safe from major vulnerabilities, but it has one medium issue and scored low (45%) on CIS compliance.



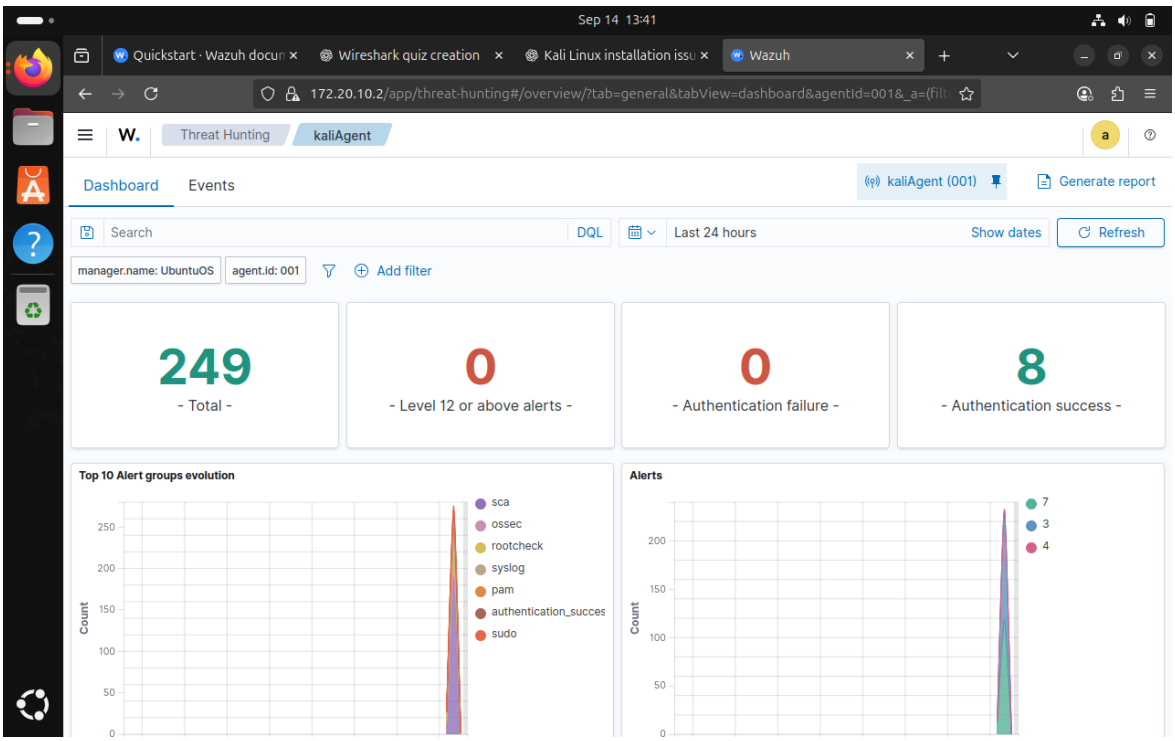
This part of Wazuh shows log activities and commands been run on the system.



This dashboard lets us **search, filter, and drill into raw Wazuh alerts** to see exactly what happened, when, and on which agent system happened

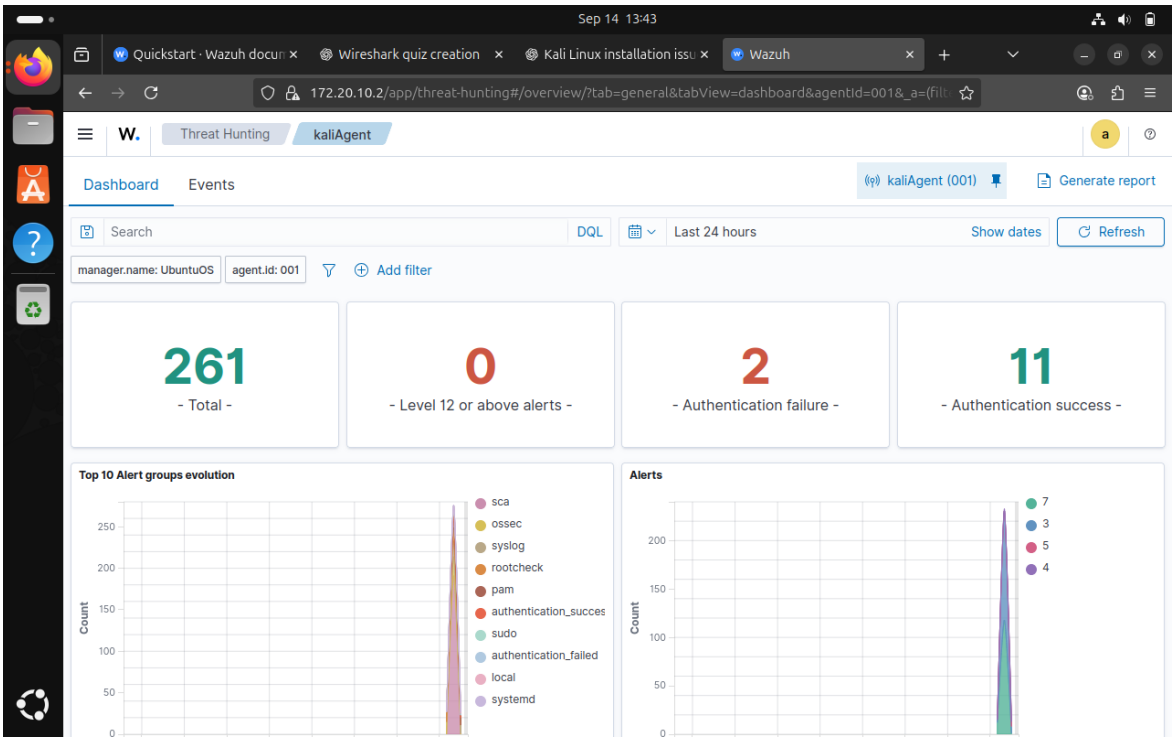
Step 8 Testing

Generated failed SSH login attempts to trigger alerts. Wazuh fired alerts and sent notifications.



This dashboard lets us see failed password attempt on agent system and also successful authentication

I attempted a wrong password on the agent system just to make a little noise on our wazuh dashboard.



As we can see it shows two failed authentication attempt, this can be used to detect brute force attack.

Step 9 Final Notes / Wrap-up

Wazuh SIEM has been successfully deployed and configured.

Capabilities Verified

- **Failed Login Detection**: The system detects and logs multiple authentication failures, with alerts set up for brute-force attempts.
- **Privilege Escalation Monitoring**: Tracks and reports sudo usage and suspicious privilege escalation attempts.
- **Vulnerability Detection**: Identifies vulnerable packages (for example, cryptography) with severity levels (Critical, High, Medium, Low).
- **Compliance Checks**: Benchmarked against CIS, PCI DSS, and HIPAA, providing pass/fail scores and highlighting gaps.

Observations

- Authentication events were successfully captured (both failures and successes).
- Privilege escalation attempts were flagged with MITRE ATT&CK mapping (T1548.003).
- Vulnerability scans reported package-level issues.
- The SCA compliance scan scored 45%, showing areas that need system hardening.

Next Steps

- Fine-tune alerting thresholds, such as failed login attempts.
- Expand monitoring to cover additional agents (beyond kaliAgent).
- Integrate with email or SIEM pipelines for automated alert delivery.

.