

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

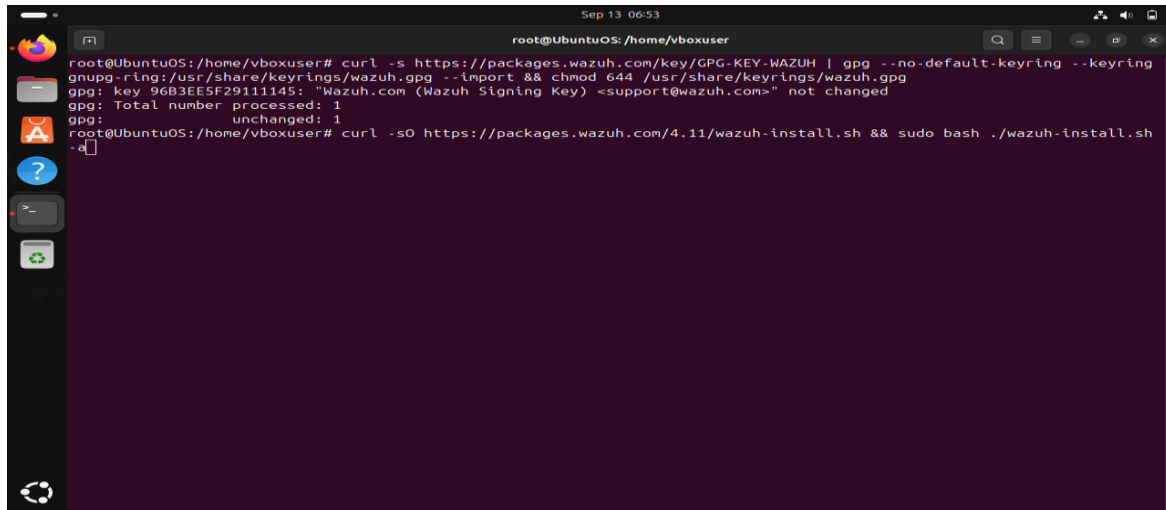
- To set up and operate a functional Wazuh SIEM environment.
 - To deploy an agent on a client machine (Kali Linux).
 - To monitor system activities such as failed logins, privilege escalation, and vulnerabilities.
 - To create alert rules and notifications for security events.
-

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.

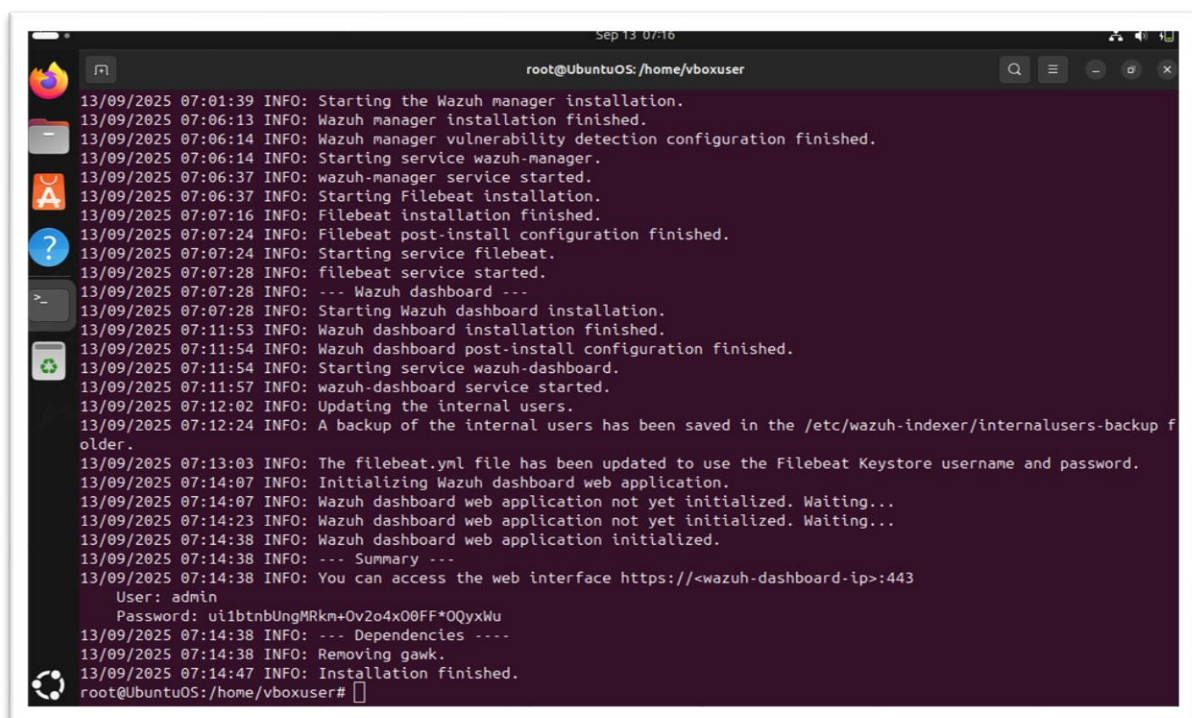
Step 1 Install Wazuh Manager & Dashboard

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

A terminal window titled 'root@UbuntuOS: /home/vboxuser' showing the execution of two curl commands. The first command imports a GPG key from Wazuh. The second command downloads and runs the Wazuh installation script. The output shows the GPG key being imported successfully and the installation script being executed.

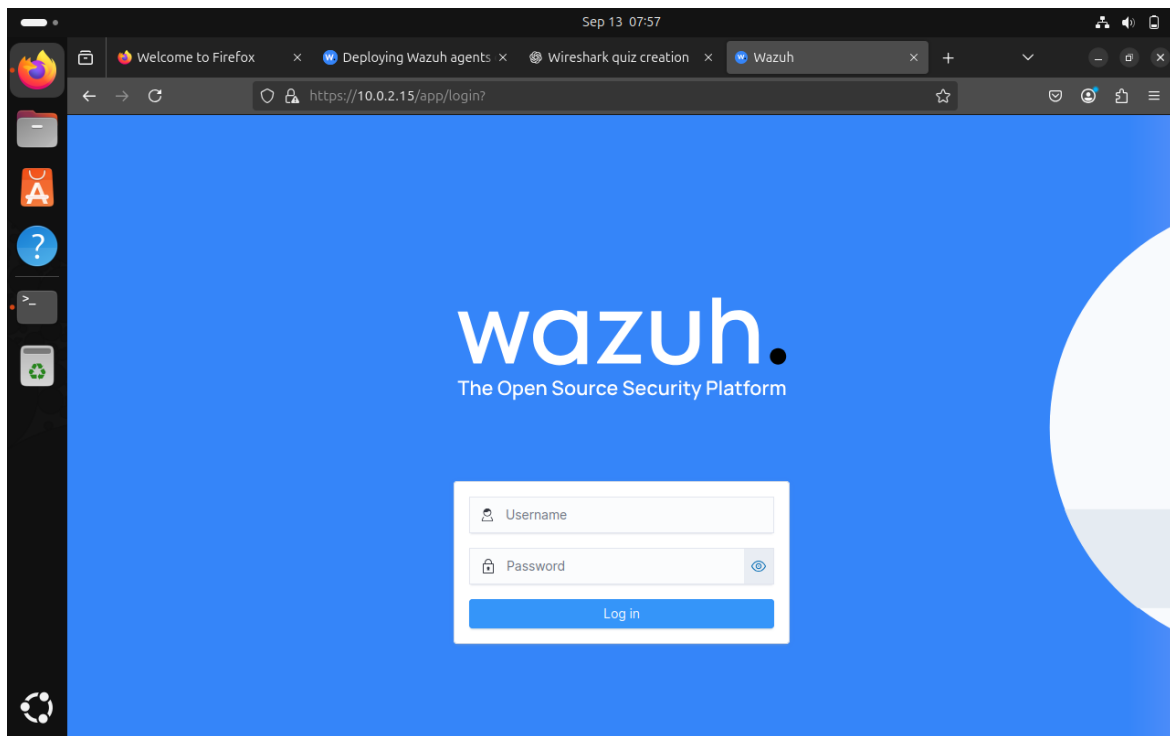
```
root@UbuntuOS: /home/vboxuser
root@UbuntuOS: /home/vboxuser# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring
gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
gpg: key 96B3EE5F29111145: "Wazuh.com (Wazuh Signing Key) <support@wazuh.com>" not changed
gpg: Total number processed: 1
gpg:   unchanged: 1
root@UbuntuOS: /home/vboxuser# curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh && sudo bash ./wazuh-install.sh
-q
```

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

A terminal window titled 'root@UbuntuOS: /home/vboxuser' showing the output of the Wazuh installation script. The log includes timestamps and status messages for the Wazuh manager, Filebeat, and dashboard installation. It concludes with a summary and login credentials for the dashboard.

```
13/09/2025 07:01:39 INFO: Starting the Wazuh manager installation.
13/09/2025 07:06:13 INFO: Wazuh manager installation finished.
13/09/2025 07:06:14 INFO: Wazuh manager vulnerability detection configuration finished.
13/09/2025 07:06:14 INFO: Starting service wazuh-manager.
13/09/2025 07:06:37 INFO: wazuh-manager service started.
13/09/2025 07:06:37 INFO: Starting Filebeat installation.
13/09/2025 07:07:16 INFO: Filebeat installation finished.
13/09/2025 07:07:24 INFO: Filebeat post-install configuration finished.
13/09/2025 07:07:24 INFO: Starting service filebeat.
13/09/2025 07:07:28 INFO: filebeat service started.
13/09/2025 07:07:28 INFO: --- Wazuh dashboard ---
13/09/2025 07:07:28 INFO: Starting Wazuh dashboard installation.
13/09/2025 07:11:53 INFO: Wazuh dashboard installation finished.
13/09/2025 07:11:54 INFO: Wazuh dashboard post-install configuration finished.
13/09/2025 07:11:54 INFO: Starting service wazuh-dashboard.
13/09/2025 07:11:57 INFO: wazuh-dashboard service started.
13/09/2025 07:12:02 INFO: Updating the internal users.
13/09/2025 07:12:24 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
13/09/2025 07:13:03 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
13/09/2025 07:14:07 INFO: Initializing Wazuh dashboard web application.
13/09/2025 07:14:07 INFO: Wazuh dashboard web application not yet initialized. Waiting...
13/09/2025 07:14:23 INFO: Wazuh dashboard web application not yet initialized. Waiting...
13/09/2025 07:14:38 INFO: Wazuh dashboard web application initialized.
13/09/2025 07:14:38 INFO: --- Summary ---
13/09/2025 07:14:38 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: ui1btbnUngMRkm+0v2o4x00FF*0QyxWu
13/09/2025 07:14:38 INFO: --- Dependencies ---
13/09/2025 07:14:38 INFO: Removing gawk.
13/09/2025 07:14:47 INFO: Installation finished.
root@UbuntuOS: /home/vboxuser#
```

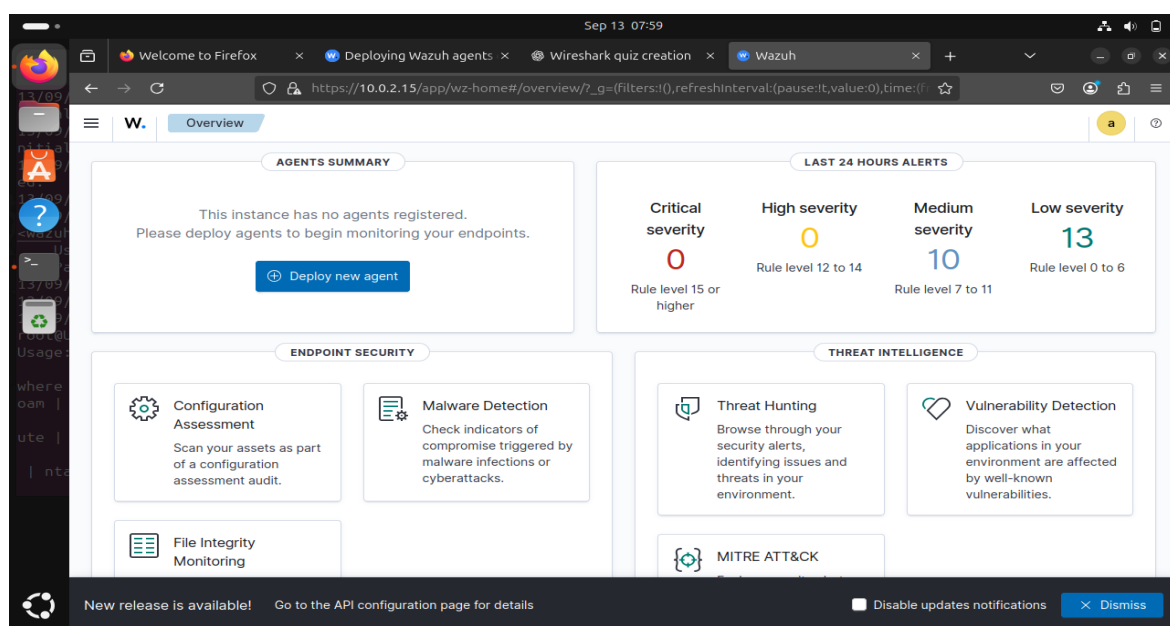
Access dashboard with your IP address, and login with the password given after installation



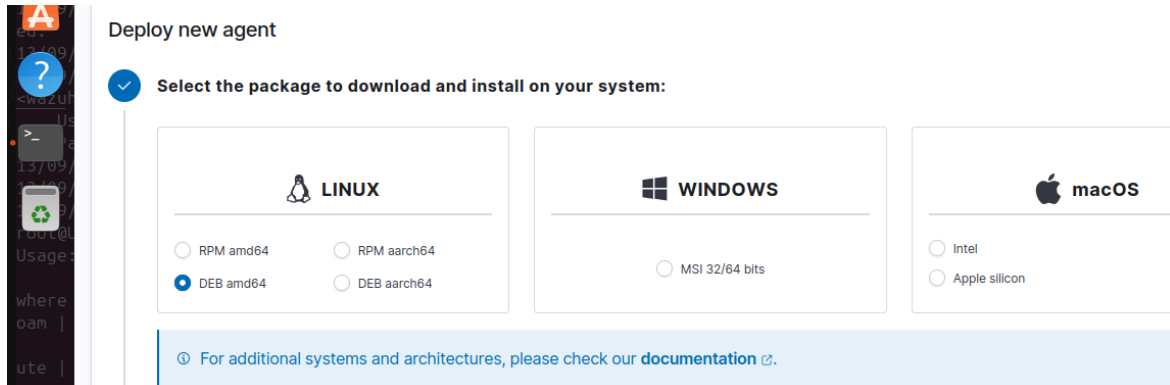
Impute the password and login to your wazor admin account.

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 order to be able to get logs from the system, monitor, analyze, detect vulnerability and other functions



The screenshot shows the 'Deploy new agent' section of the Wazuh Administrator dashboard. It features three main columns for operating systems: LINUX, WINDOWS, and macOS. Under LINUX, there are four radio button options: RPM amd64, RPM aarch64, DEB amd64 (which is selected), and DEB aarch64. Under WINDOWS, there is one radio button option: MSI 32/64 bits. Under macOS, there are two radio button options: Intel and Apple silicon. A blue banner at the bottom of the form contains a link to the documentation.

Deploy new agent

Select the package to download and install on your system:

LINUX

- ☐ RPM amd64
- ☐ RPM aarch64
- ☒ DEB amd64
- ☐ DEB aarch64

WINDOWS

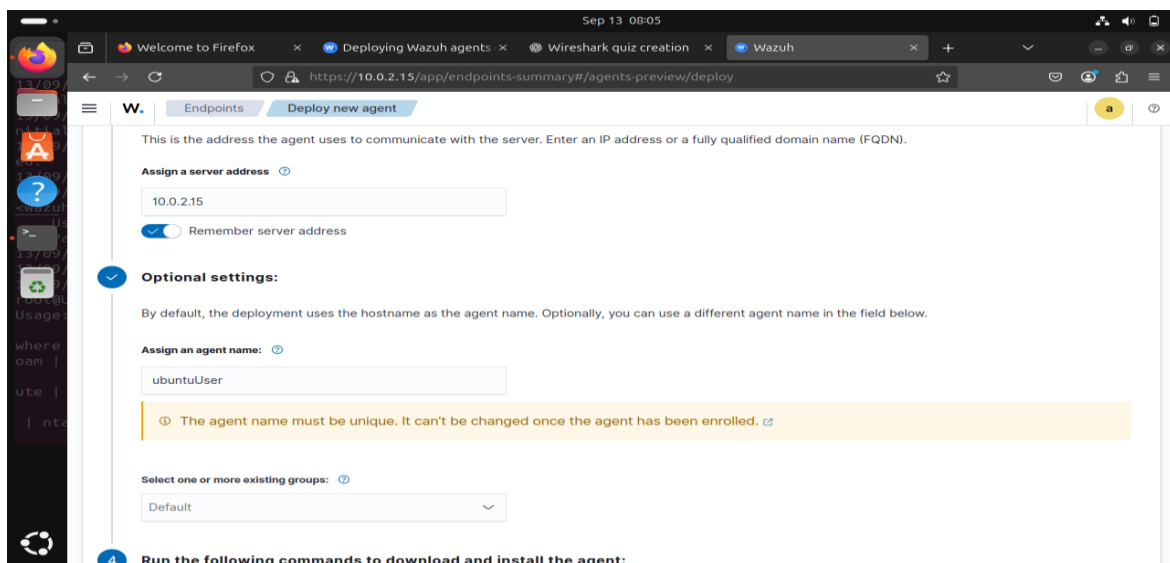
- ☐ MSI 32/64 bits

macOS

- ☐ Intel
- ☐ Apple silicon

For additional systems and architectures, please check our [documentation](#).

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



This screenshot shows the 'Optional settings' section of the 'Deploy new agent' form. It includes a text input field for 'Assign a server address' with the value '10.0.2.15' and a checked 'Remember server address' toggle. Below this is the 'Assign an agent name' section, which has a text input field containing 'ubuntuUser' and a yellow warning message stating that the agent name must be unique and cannot be changed after enrollment. At the bottom, there is a dropdown menu for 'Select one or more existing groups' with 'Default' selected. A blue banner at the bottom of the form provides instructions on how to run commands to download and install the agent.

Endpoints Deploy new agent

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address

10.0.2.15

☒ Remember server address

Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name:

ubuntuUser

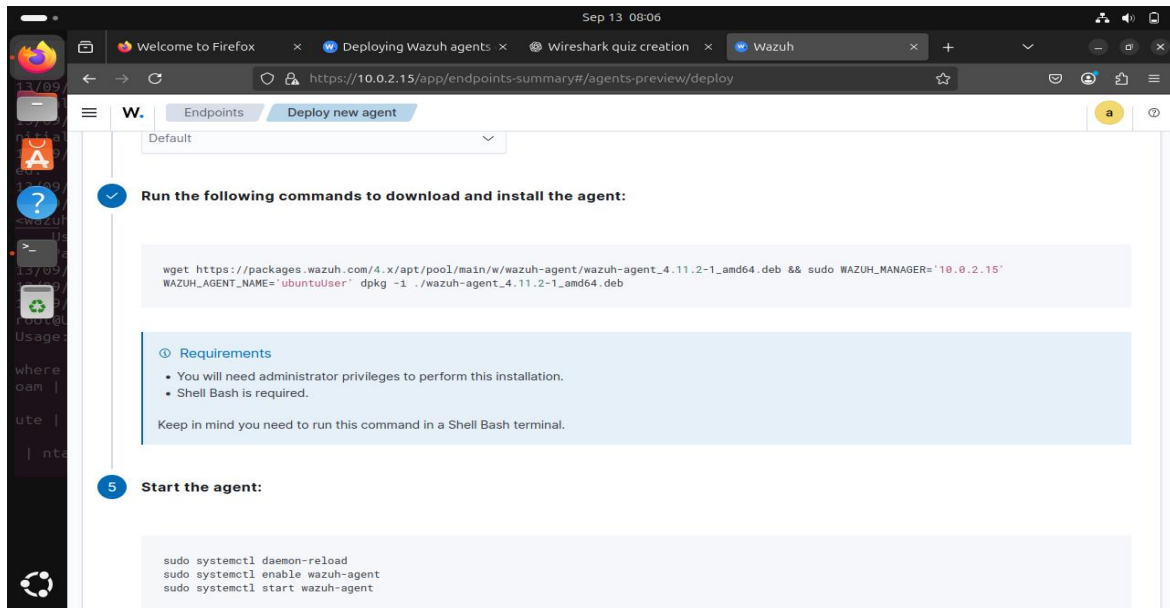
The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups:

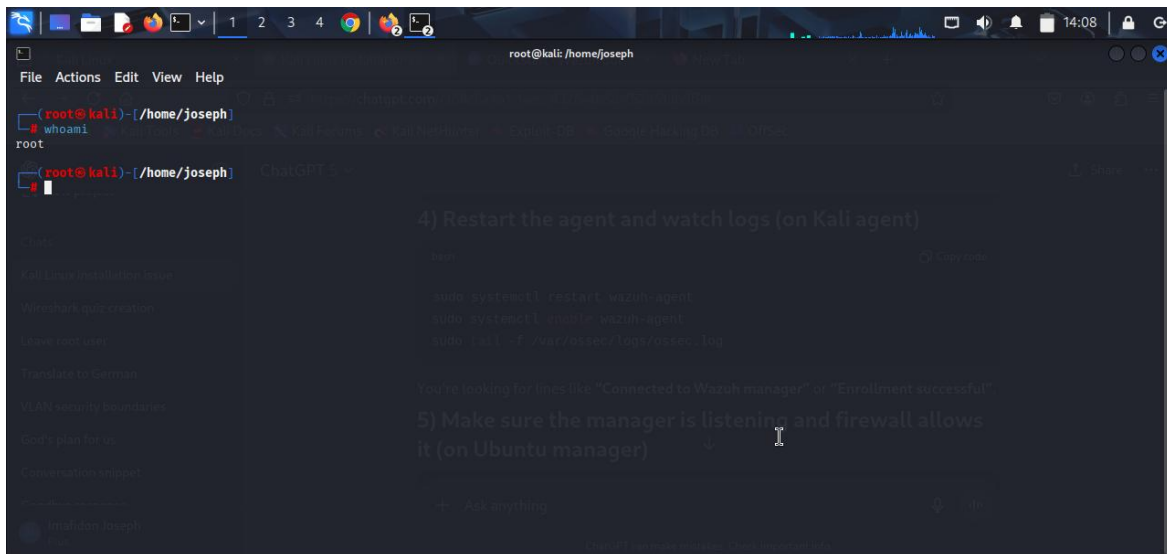
Default

Run the following commands to download and install the agent:

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`.

```
root@kali: /home/joseph

(joseph@kali)-[~]
└─$ sudo bash
[sudo] password for joseph:
(root@kali)-[/home/joseph]
└─$ wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.2-1_amd64.deb && sudo WAZUH_MANAGER='10.0.2.15' WAZUH_AGENT_NAME='kaliA
gent' dpkg -i ./wazuh-agent_4.11.2-1_amd64.deb
--2025-09-14 10:04:36-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.2-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 108.157.78.21, 108.157.78.119, 108.157.78.23, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|108.157.78.21|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11075686 (11M) [application/vnd.debian.binary-package]
Saving to: 'wazuh-agent_4.11.2-1_amd64.deb'

wazuh-agent_4.11.2-1_amd64.deb      100%[=====] 10.56M  5.41MB/s   in 2.0s

2025-09-14 10:04:42 (5.41 MB/s) - 'wazuh-agent_4.11.2-1_amd64.deb' saved [11075686/11075686]

Selecting previously unselected package wazuh-agent.
(Reading database ... 428329 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.11.2-1_amd64.deb ...
Unpacking wazuh-agent (4.11.2-1) ...
Setting up wazuh-agent (4.11.2-1) ...

(root@kali)-[/home/joseph]
└─$
```

```
root@kali: /home/joseph

(joseph@kali)-[~]
└─$ sudo bash
[sudo] password for joseph:
(root@kali)-[/home/joseph]
└─$ wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.2-1_amd64.deb && sudo WAZUH_MANAGER='10.0.2.15' WAZUH_AGENT_NAME='kaliA
gent' dpkg -i ./wazuh-agent_4.11.2-1_amd64.deb
--2025-09-14 10:04:36-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.2-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 108.157.78.21, 108.157.78.119, 108.157.78.23, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|108.157.78.21|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11075686 (11M) [application/vnd.debian.binary-package]
Saving to: 'wazuh-agent_4.11.2-1_amd64.deb'

wazuh-agent_4.11.2-1_amd64.deb      100%[=====] 10.56M  5.41MB/s   in 2.0s

2025-09-14 10:04:42 (5.41 MB/s) - 'wazuh-agent_4.11.2-1_amd64.deb' saved [11075686/11075686]

Selecting previously unselected package wazuh-agent.
(Reading database ... 428329 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.11.2-1_amd64.deb ...
Unpacking wazuh-agent (4.11.2-1) ...
Setting up wazuh-agent (4.11.2-1) ...

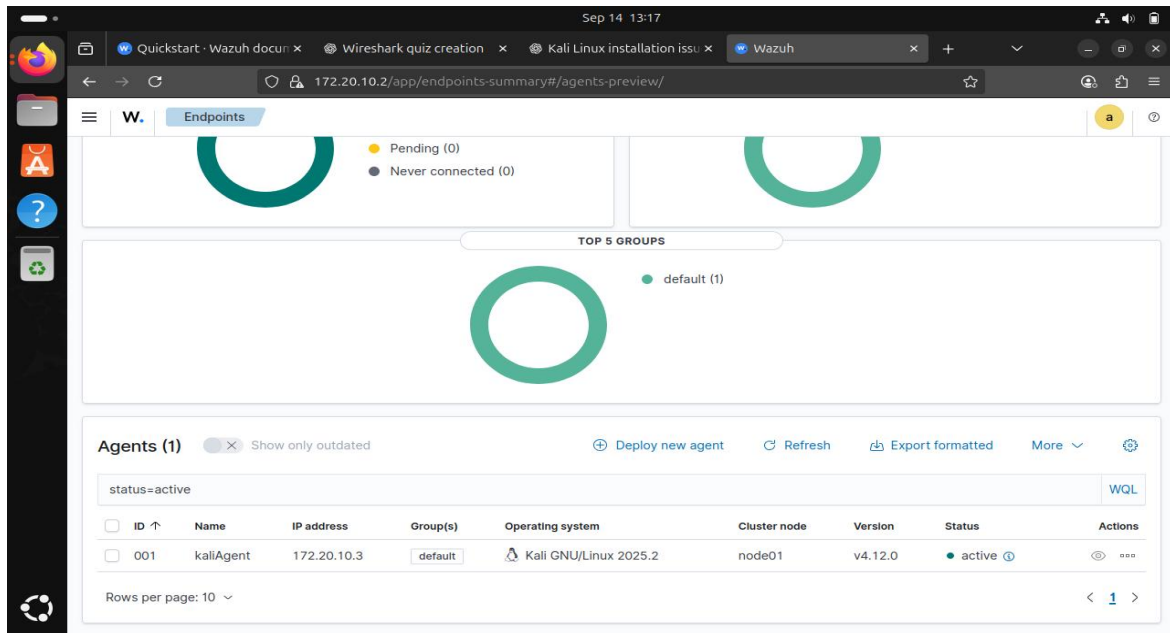
(root@kali)-[/home/joseph]
└─$ sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service' → '/usr/lib/systemd/system/wazuh-agent.service'.

(root@kali)-[/home/joseph]
└─$
```

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

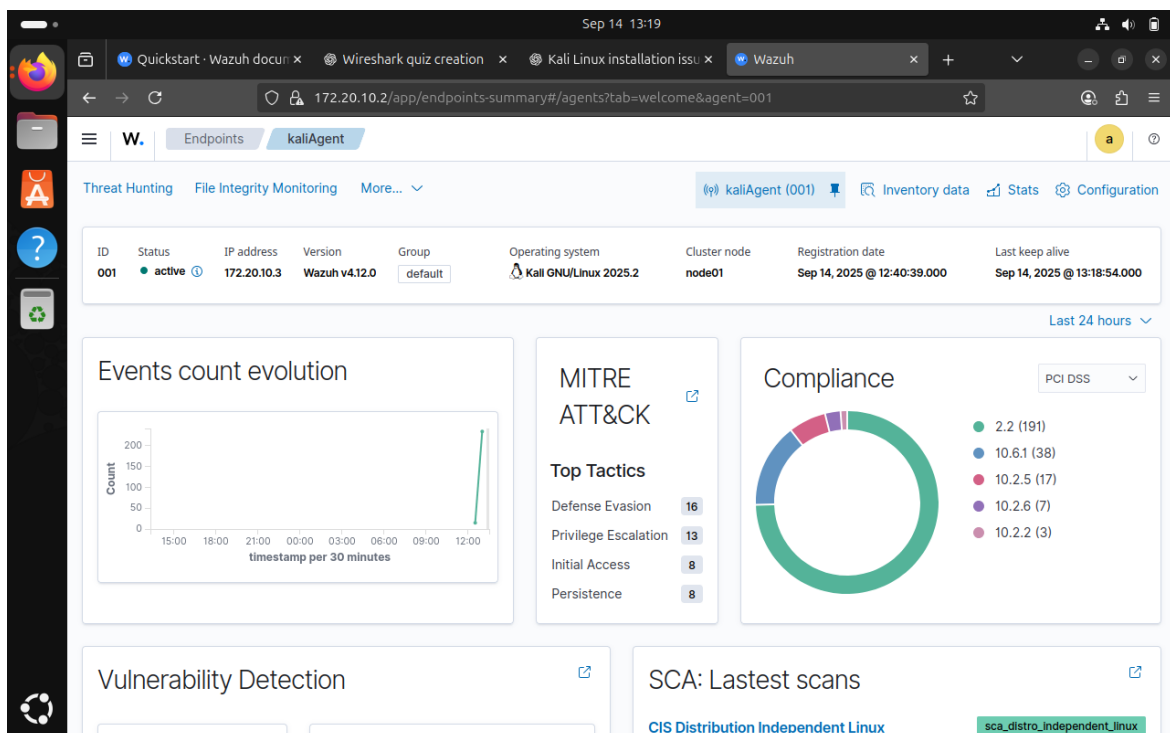
Verified in the Wazuh Dashboard that the Kali agent appeared as active.



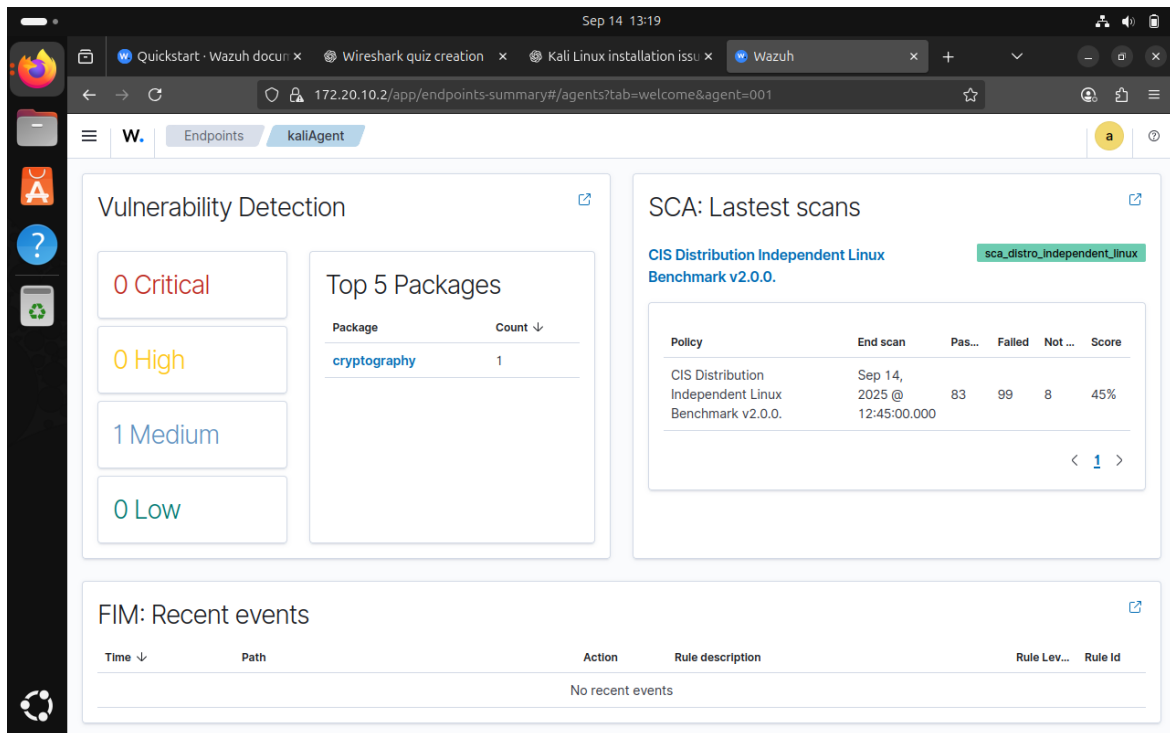
As it is seen in the picture above our agent is up and running.

Step 4 Dashboard Analysis

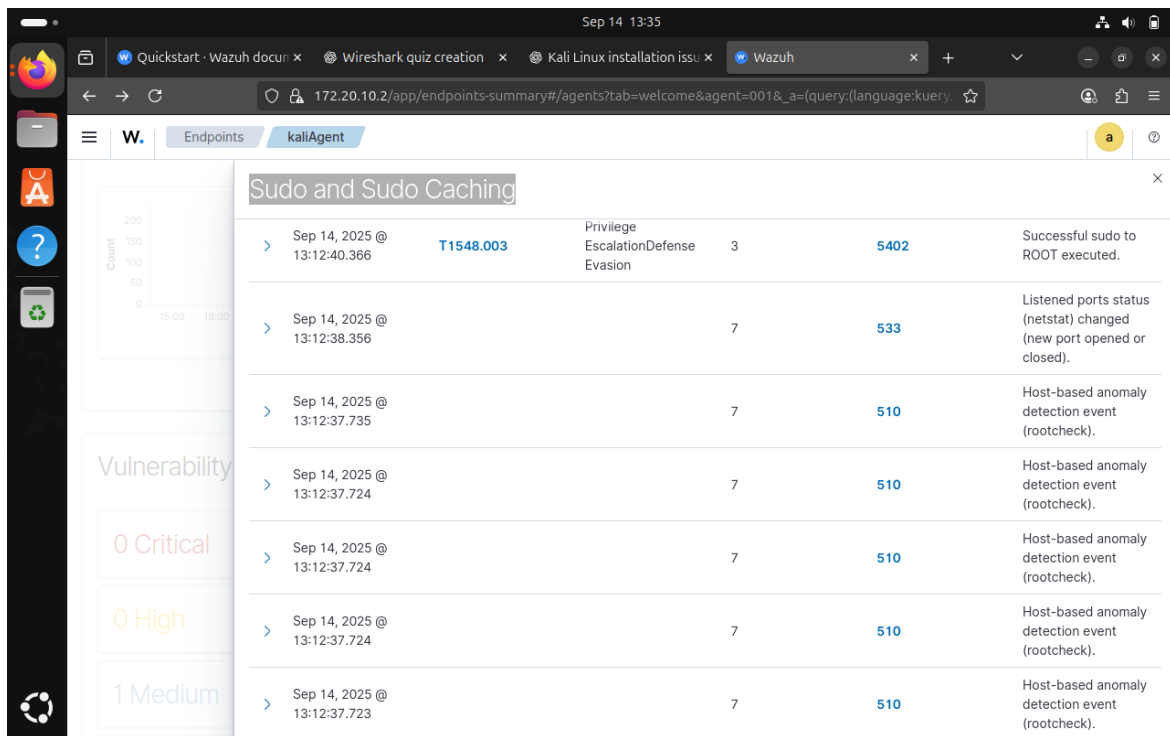
Observed events evolution, MITRE ATT&CK; detections, vulnerability scans, and compliance results.



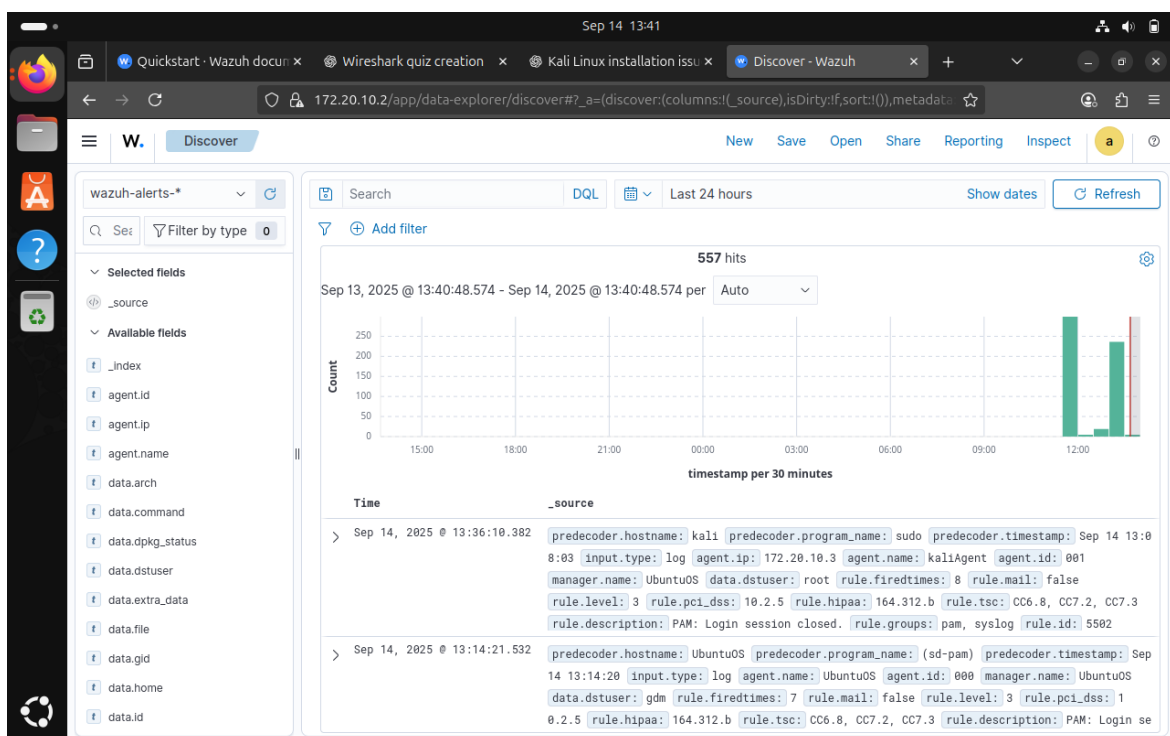
This dashboard gives you a **quick health and threat overview** of your monitored agent: system status, attack detections, compliance gaps, and vulnerabilities.



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.



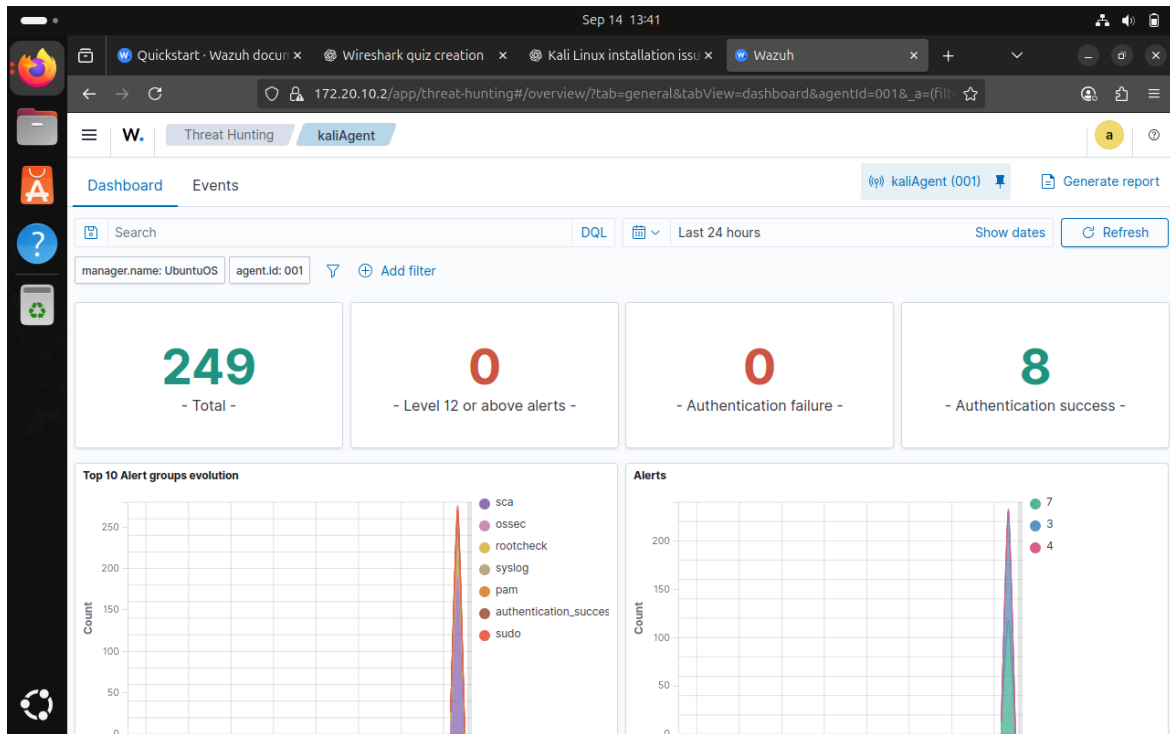
This part of Wazuh shows log activities and commands been run on the system.



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

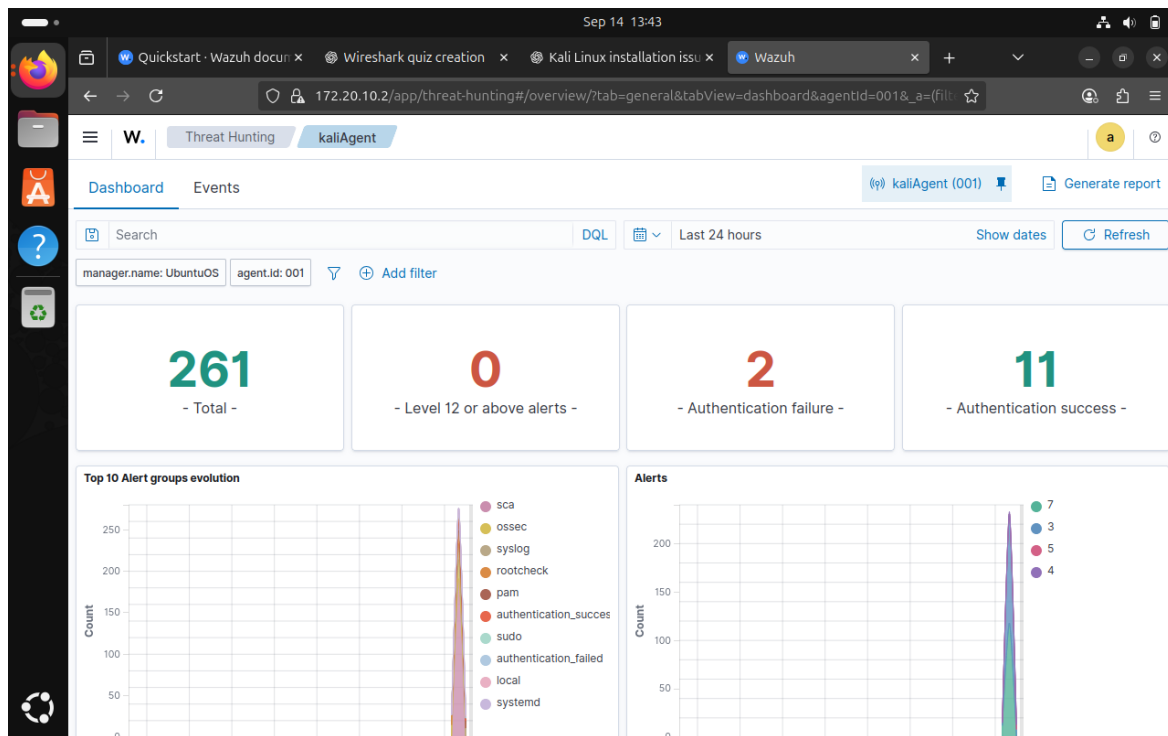
Generated failed SSH login attempts to trigger alerts. Wazuh fired alerts and sent notifications.



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.