

# Wazuh Setup Guide

-R.M.NAREN ADITHYA

This document provides step-by-step instructions for setting up Wazuh, including installing the Wazuh server and dashboard, deploying Wazuh agents, and exploring the Wazuh dashboard. Each section includes a placeholder for manually inserting screenshots.

## 1. Wazuh Installation

Step-by-Step Guide: Installing Wazuh Using the Virtual Machine (OVA)

### 1. Download the Wazuh Virtual Appliance (OVA)

- Download the pre-built Wazuh OVA file for version 4.9.2 from [Wazuh's official site](#).



### 2. Check System Requirements

- Ensure your host system is 64-bit.
- Enable hardware virtualization in the firmware (BIOS/UEFI) of your host.
- Install a virtualization platform like VirtualBox or VMware or Hyper-V.

Default Hardware Configuration for Wazuh VM:

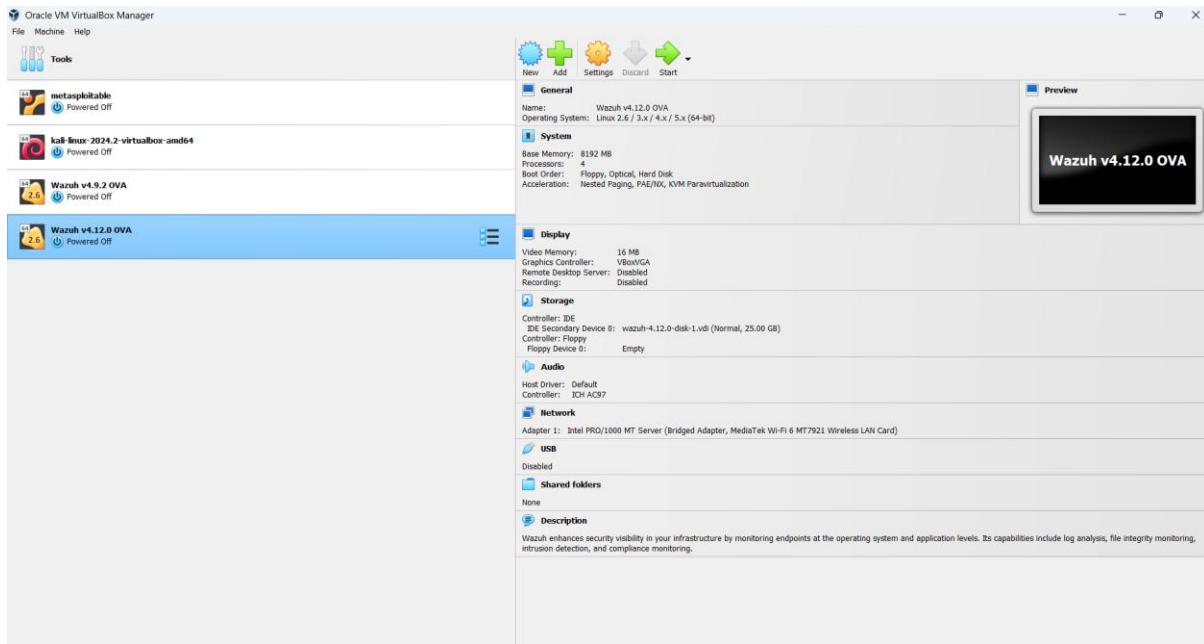
- CPU: 4 cores
- RAM: 8 GB
- Storage: 50 GB

*Note:* Modify the configuration based on your needs.

### 3. Import the OVA File

- Open your virtualization platform (e.g., VMware).
- Import the downloaded OVA file:
  - In VMware, go to File > Open...

- Select the Wazuh OVA file and click on Open
- In the new open windows, give a name to your VM (e.g : Wuzuh Server), choose the path where to store your VM configuraton files and then click on Import.
- Your VM has been successfully imported. You can now add more RAM (e.g: from 8Gb to 10Gb), Storage ( From 50 Gb to 80Gb) and CPUs (4 to 8) if you want or have more resources. Also choose the correct network adapter (e.g, from bridge to NAT) for the sake of this demo.



#### 4. Start the Virtual Machine

- Start the VM from your virtualization platform by clicking on Power on this virtual machine.
- Login credentials for the VM:
  - Username: wazuh-user
  - Password: wazuh

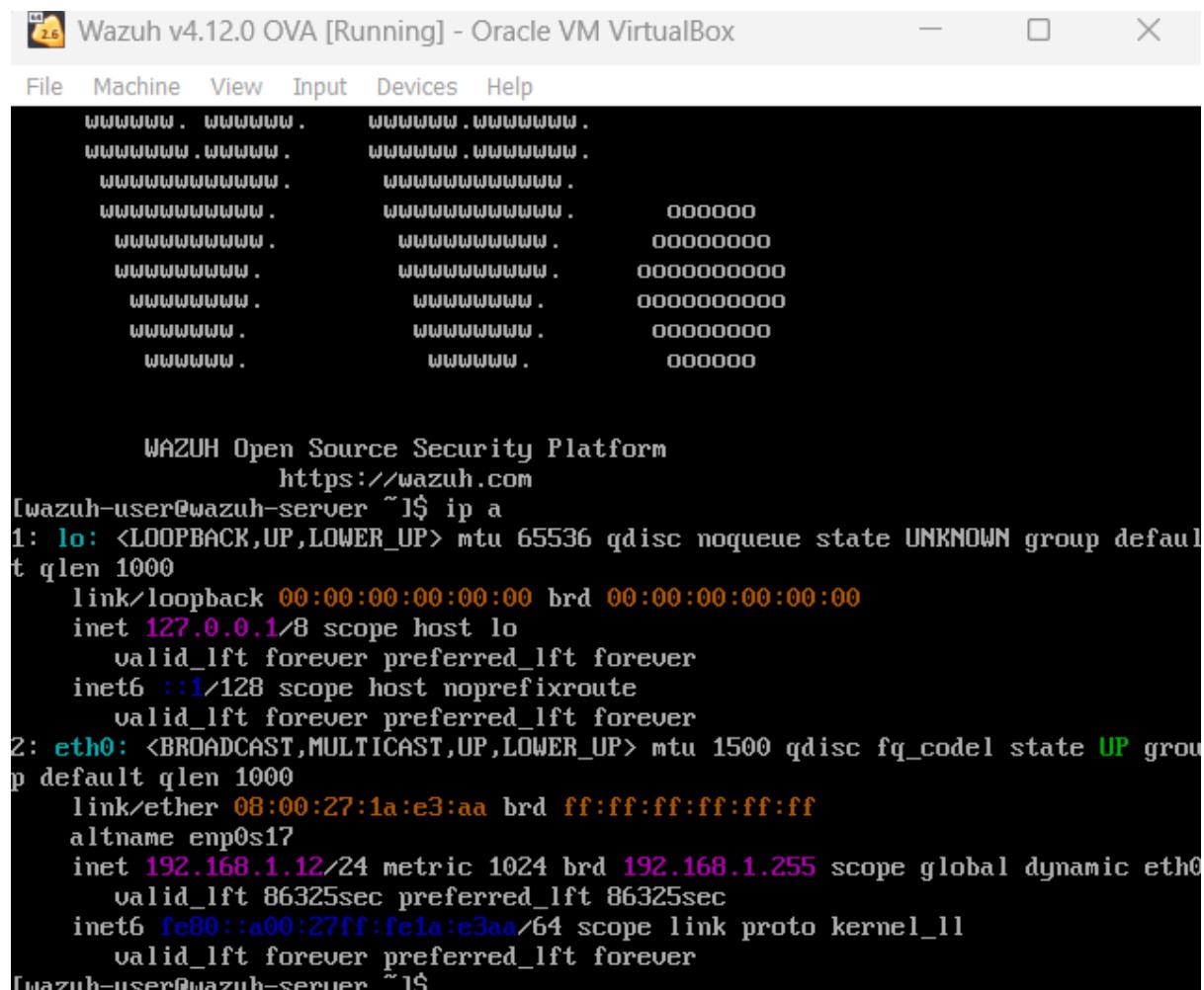


Welcome to the Wazuh OVA version  
Wazuh - 4.12.0  
Login credentials:  
User: wazuh-user  
Password: wazuh  
  
wazuh-server login: wazuh-user  
Password:

## 6. Find the VM's IP Address

- Inside the VM, run the following command to get the IP address:

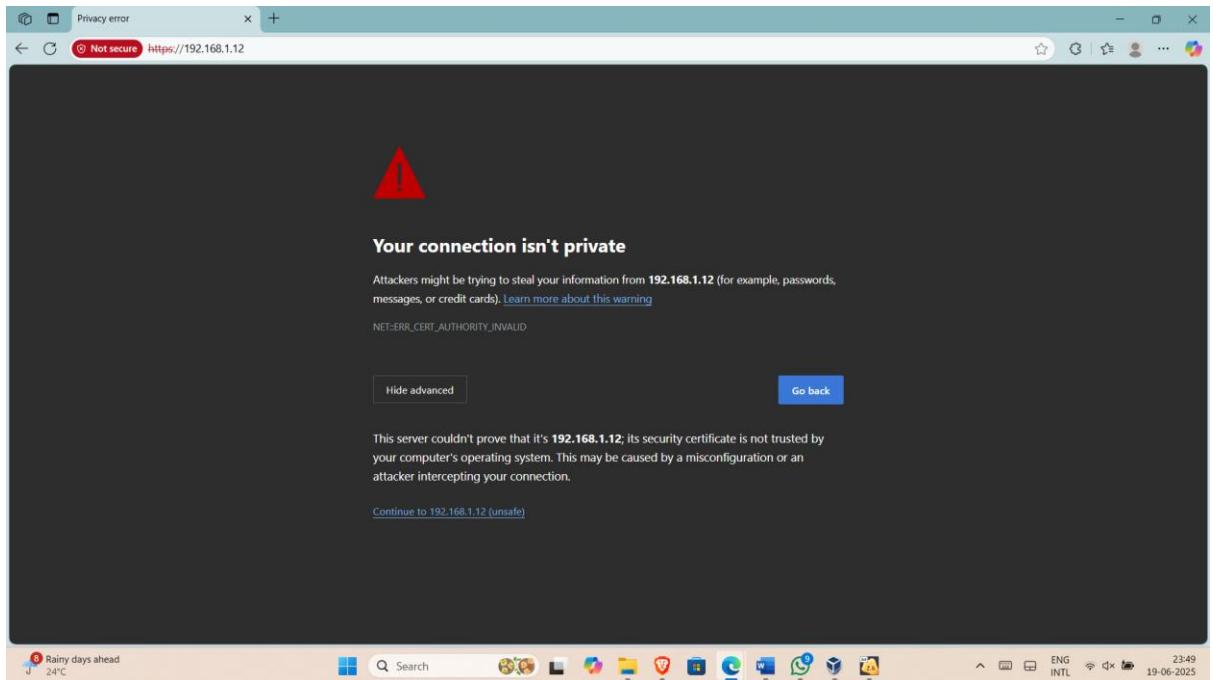
```
ip a
```



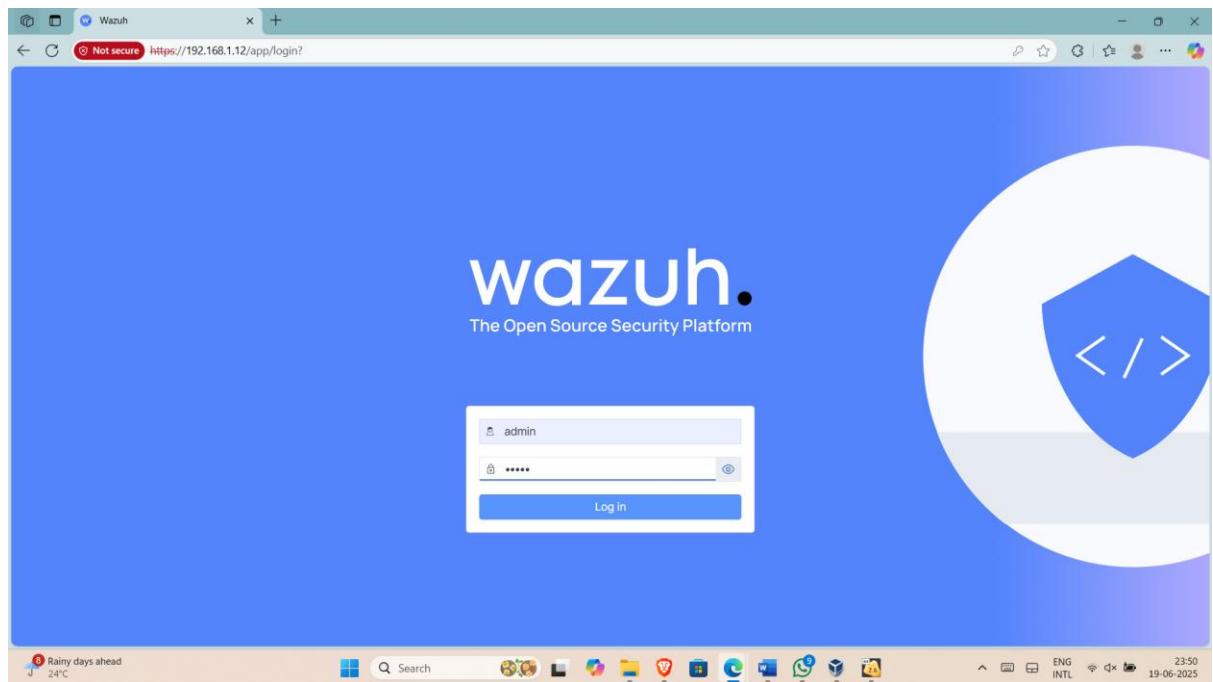
```
File Machine View Input Devices Help  
[wazuh-user@wazuh-server ~]$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:1a:e3:aa brd ff:ff:ff:ff:ff:ff  
    altname enp0s17  
    inet 192.168.1.12/24 metric 1024 brd 192.168.1.255 scope global dynamic eth0  
        valid_lft 86325sec preferred_lft 86325sec  
    inet6 fe80::a00:27ff:fe1a:e3aa/64 scope link proto kernel ll  
        valid_lft forever preferred_lft forever  
[wazuh-user@wazuh-server ~]$
```

## 7. Access the Wazuh Dashboard

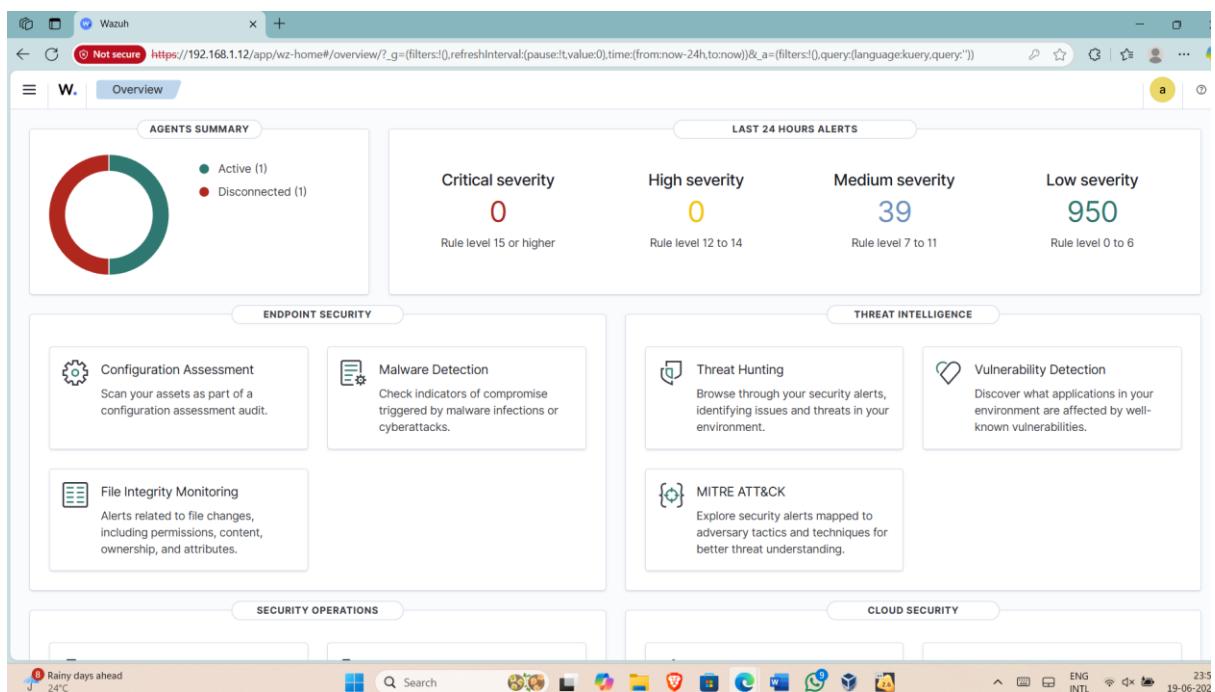
- Open a web browser from another computer on the same network (e.g., Debian or Windows) and navigate to:
- `https://<wazuh_server_ip>`
- Replace `<wazuh_server_ip>` with the IP address obtained in the previous step.
- If pop-up windows open, click on Advanced and then click on Accept the Risk and Continue



- Dashboard login credentials:
  - Username: admin
  - Password: admin



- You have successfully install the wauh server using the OVA file.



## 2. Deploy Wazuh Agent

### Step 1: Install Wazuh Agent on Linux

## **1. Add Wazuh Repository:**

- For Debian/Ubuntu, add the Wazuh repository:
- echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list
- wget -qO - https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add -
- sudo apt-get update

## **2. Install Wazuh Agent:**

- Install the agent:
- sudo apt-get install wazuh-agent

## **3. Configure Agent:**

- Edit the configuration file /var/ossec/etc/ossec.conf to point to the Wazuh manager:
  - <client>
  - <server>
  - <address><your-wazuh-manager-ip></address>
  - </server>
  - </client>

```
<ossec_config>
  <client>
    <server>
      <address>192.168.1.12</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>kali, kali2024, kali2024.2</config-profile>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
  </client>
```

## **4. Start Agent:**

- Enable and start the Wazuh agent:
- sudo systemctl enable wazuh-agent
- sudo systemctl start wazuh-agent

The screenshot shows a terminal window titled "kali-linux-2024.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal is running as root, indicated by the red "#". The user performs the following commands:

```
root@kali: ~
# systemctl enable wazuh-agent
root@kali: ~
# systemctl start wazuh-agent
root@kali: ~
# systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
   Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; enabled; preset: disabled)
   Active: active (running) since Thu 2025-06-19 14:23:28 EDT; 4min 20s ago
     Invocation: 420f8486c67044f38dce97df42c1096e
   Tasks: 32 (limit: 12460)
   Memory: 1.4G (peak: 1.4G)
     CPU: 56.535s
   CGroup: /system.slice/wazuh-agent.service
           ├─832 /var/ossec/bin/wazuh-execd
           ├─841 /var/ossec/bin/wazuh-agentd
           ├─857 /var/ossec/bin/wazuh-syscheckd
           ├─894 /var/ossec/bin/wazuh-logcollector
           ├─941 /var/ossec/bin/wazuh-modulesd

Jun 19 14:23:22 kali env[797]: Deleting PID file '/var/ossec/var/run/wazuh-syscheckd-868.pid' not used ...
Jun 19 14:23:22 kali env[797]: Deleting PID file '/var/ossec/var/run/wazuh-agentd-847.pid' not used ...
Jun 19 14:23:22 kali env[797]: Deleting PID file '/var/ossec/var/run/wazuh-execd-832.pid' not used ...
Jun 19 14:23:22 kali env[797]: Started wazuh-execd ...
Jun 19 14:23:23 kali env[797]: Started wazuh-agentd ...
Jun 19 14:23:24 kali env[797]: Started wazuh-syscheckd ...
Jun 19 14:23:25 kali env[797]: Started wazuh-logcollector ...
Jun 19 14:23:26 kali env[797]: Started wazuh-modulesd ...
Jun 19 14:23:28 kali env[797]: Completed.
Jun 19 14:23:28 kali systemd[1]: Started wazuh-agent.service - Wazuh agent.

root@kali: ~
```

## Step 2: Install Wazuh Agent on Windows

### 1. Download Agent Installer:

- Download the Windows agent installer from  
<https://packages.wazuh.com/4.x/windows/wazuh-agent-<version>.exe>.

### 2. Run Installer:

- Execute the installer and follow the wizard.
- Enter the Wazuh manager IP when prompted.

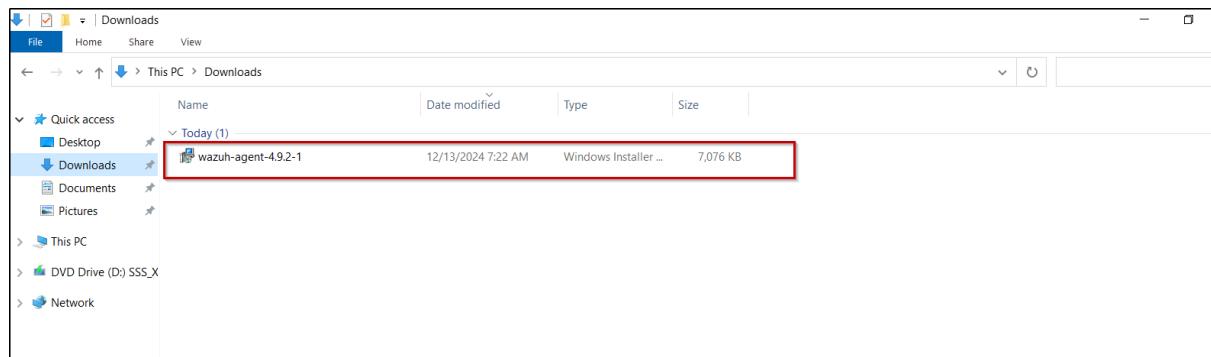
### 3. Verify Agent Status:

- Open a command prompt and check the agent status:
- `net start WazuhSvc`

### Step 3: Connect Agent to Wazuh Manager

#### 1. Register Agent:

- On the Wazuh manager, register the agent:
- `sudo /var/ossec/bin/manage_agents -i <agent-id>`



#### 2. Restart Wazuh Manager:

- Restart the manager to apply changes:
- `sudo systemctl restart wazuh-manager`

#### 3. Verify Connection:

- Check the agent status in the Wazuh dashboard under the "Agents" tab.

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
006	NarenAdithya	192.168.1.6	default	Microsoft Windows 11 Home Single Language 10.0.26100.4349	node01	v4.12.0	active	...
007	kali	10.0.2.15	default	Kali GNU/Linux 2024.2	node01	v4.12.0	active	...

### 3. Explore Wazuh Dashboard

#### Step 1: Navigate Through Modules

## 1. Access Dashboard:

- Log in to the Wazuh dashboard at <https://<your-server-ip>:5601>.

## 2. Security Events:

- Navigate to the "Security Events" module to view alerts and logs.

## 3. Agents:

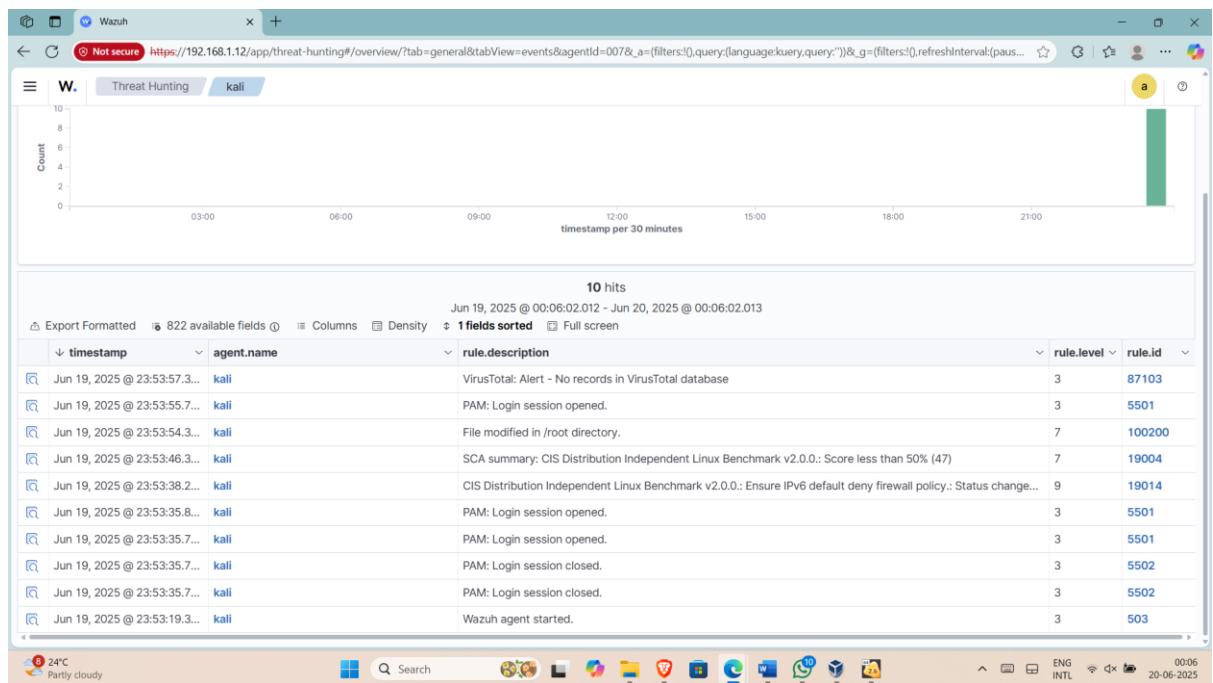
- Go to the "Agents" tab to see connected agents and their status.

## 4. File Integrity Monitoring (FIM):

- Explore the FIM module to monitor file changes on endpoints.

## 5. Syscheck:

- Check the Syscheck module for system integrity alerts.



## Step 2: Identify Top Alerts and Their Sources

### 1. View Top Alerts:

- In the "Security Events" module, sort alerts by severity or frequency.

### 2. Analyze Sources:

- Click on an alert to view details, including the source IP, agent, and rule.

### 3. Create Custom Filters:

- Use the dashboard filters to focus on specific agents or alert types.

## Vulnerability Detection



2 Critical

11 High

10 Medium

6 Low

### Top 5 Packages

Package	Count ↓
Oracle VM VirtualBox 7.0.18	9
Steam	8
Node.js	7
Java(TM) SE Development Kit 21.0.2 (64-bit)	4
Maltego	1