Implementation and Configuration of Wazuh Server

Integrating Wazuh Agents for Cross-Platform Endpoint Visibility and Alerting

Kayvon Karimi

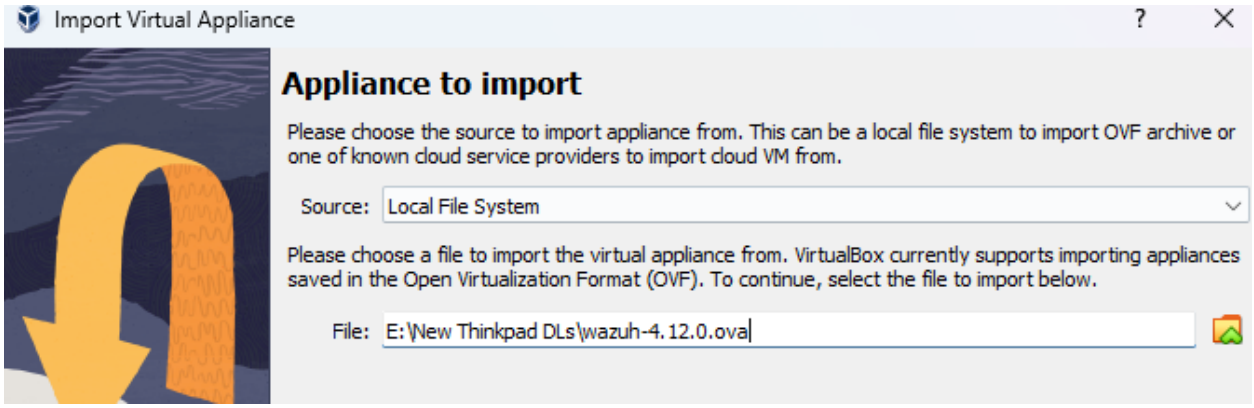
August 4th, 2025

Introduction

For this project, I set up a Wazuh server to monitor the security of my laptop, a virtual machine (Ubuntu VM), and my AWS EC2-hosted VPN server. I chose a prebuilt OVA to run it locally, establishing it as the central hub for collecting logs and tracking agent activity across all devices. I installed and configured the Wazuh agent on each system to report back to the manager, enabling centralized analysis of threats and system health. This setup mirrors a basic enterprise monitoring environment, reinforcing key concepts like endpoint visibility, system hardening, and secure configuration management.

Setup Wazuh Server

I downloaded the Wazuh VirtualBox OVA file from the Wazuh Documentation link, imported the file into VirtualBox and assigned it to use a bridged network adapter, allowing it to communicate on my local network. This setup enabled the Wazuh manager to receive data from connected agents and serve the dashboard interface for monitoring.



Commands to Run on Wazuh OVA VM

1. **Start Wazuh Indexer**:
    - Run: *sudo systemctl start wazuh-indexer*
    - Verify: *sudo systemctl status wazuh-indexer*
2. **Start Wazuh Dashboard**:
    - Run: *sudo systemctl start wazuh-dashboard*
    - Verify: *sudo systemctl status wazuh-dashboard*

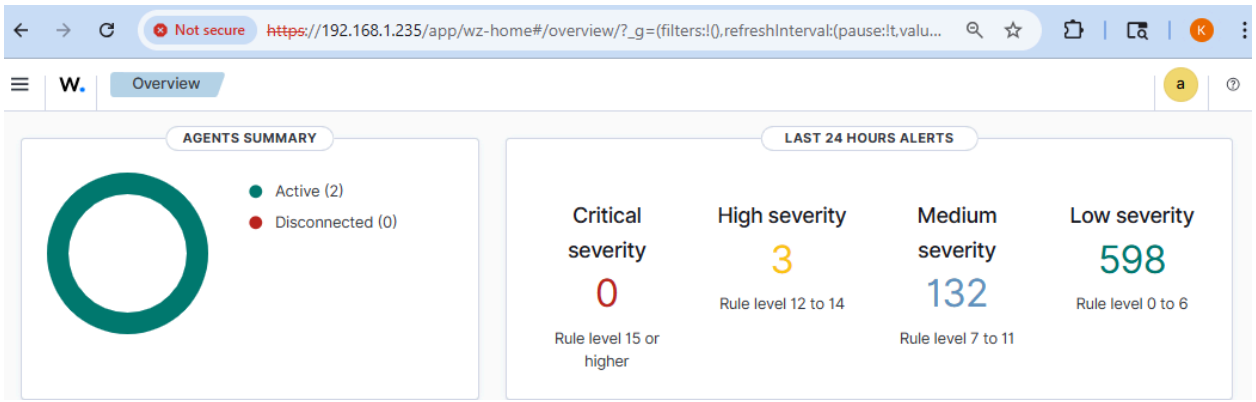
3. **Start Wazuh Manager**:
    - Run: *sudo systemctl start wazuh-manager*
    - Verify: *sudo systemctl status wazuh-manager*

```
● wazuh-indexer.service - wazuh-indexer
     Loaded: loaded (/usr/lib/systemd/system/wazuh-indexer.service; enabled;
     Active: active (running) since Fri 2025-08-08 15:49:24 UTC; 6s ago
       Docs: https://documentation.wazuh.com
```

```
[wazuh-user@wazuh-server ~]$ sudo systemctl start wazuh-dashboard
[wazuh-user@wazuh-server ~]$ sudo systemctl status wazuh-dashboard
● wazuh-dashboard.service - wazuh-dashboard
     Loaded: loaded (/etc/systemd/system/wazuh-dashboard.service; enabled; pr
     Active: active (running) since Fri 2025-08-08 06:47:53 UTC; 9h ago
```

```
wazuh-manager.service - Wazuh manager
   Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled;
   Active: active (running) since Fri 2025-08-08 15:50:57 UTC; 44s ago
```

Accessed Wazuh dashboard at 192.168.1.235. Found the IP address from ‘ip a’ on Wazuh VM.



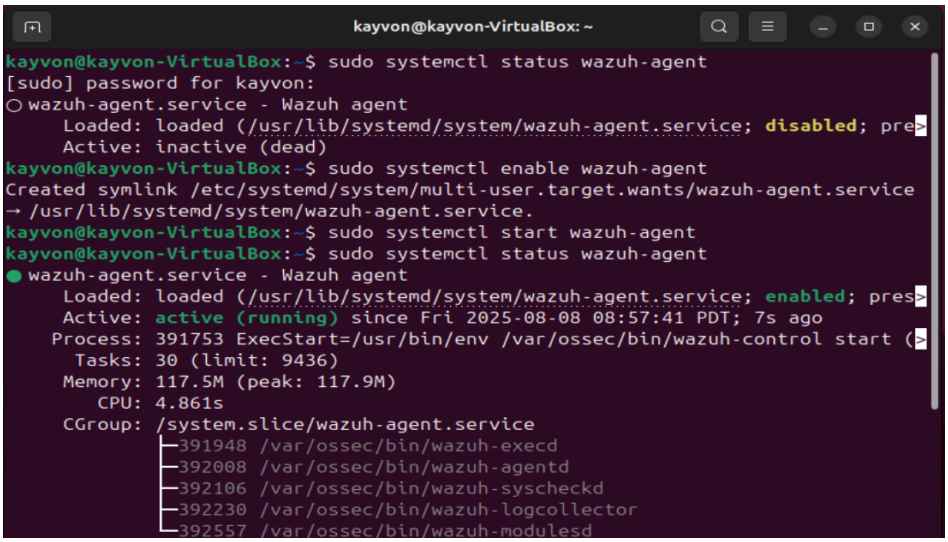
(Screenshot is taken after agents were implemented and active, at this point, no active agents)

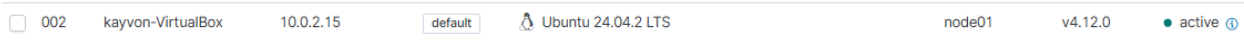
Setup Wazuh Agent on Ubuntu VM

I installed the Wazuh agent on my local Ubuntu VM to connect it directly to the Wazuh server.

- *sudo systemctl enable wazuh-agent*
- *sudo systemctl start wazuh-agent*

- *sudo systemctl status wazuh-agent*





(Screenshot above shows the Ubuntu VM on VirtualBox shown on Wazuh dashboard)

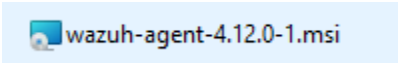
Setup Wazuh Agent on Home Device (Windows Thinkpad)

To get the Wazuh agent running on my home device ("ThinkpadK" Windows laptop), I downloaded the wazuh-agent-4.12.0-1.msi from the Wazuh website, installed it with the default settings, and then opened C:\Program Files (x86)\ossec-agent\ossec.conf in Notepad to set the address to 192.168.1.235 (the IP address for Wazuh server) under the section <client><server>. After saving, I enrolled the agent using *agent-auth.exe -m 192.168.1.235* in an admin PowerShell window, started it with *net start Wazuh*, and confirmed it was active by checking the Wazuh dashboard at https://192.168.1.235 under the Agents tab.

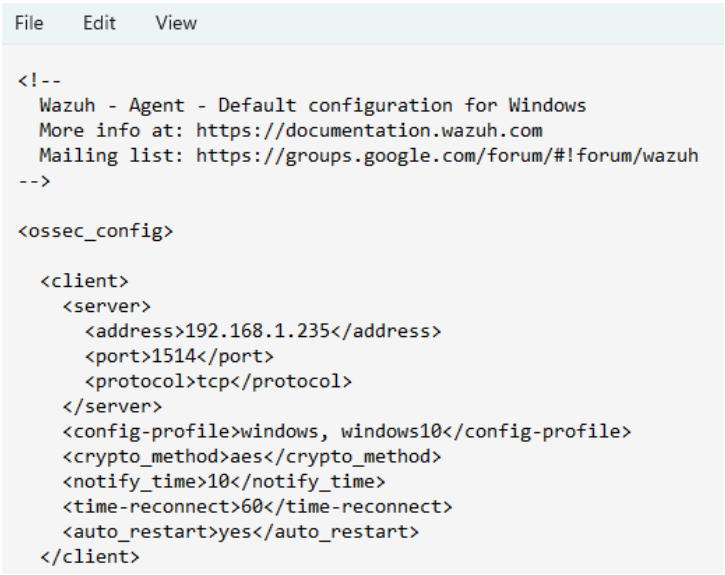
Steps:

1. Downloaded the Agent:
    - Visited Wazuh Downloads and downloaded wazuh-agent-4.12.0-1.msi.
2. Installed the Agent:

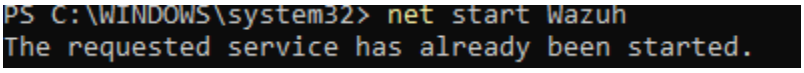
- Double-clicked the .msi file and followed the installation wizard, accepting default settings.



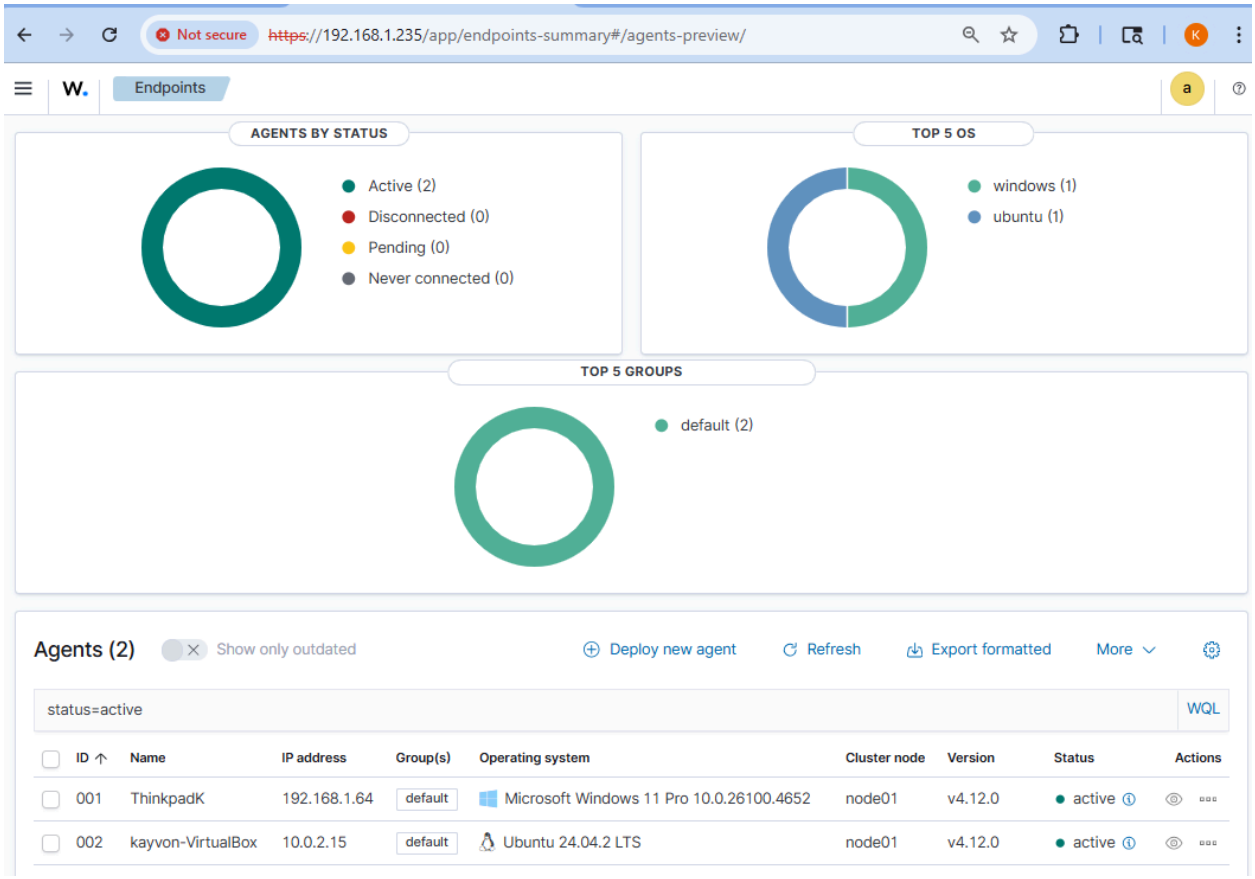
3. Configured the Agent:
    - Opened *C:\Program Files (x86)\ossec-agent\ossec.conf* in Notepad (Run as Administrator).
    - Edited the <address> tag to <address>192.168.1.235</address> under <client><server>.
    - Saved the file.



4. Enrolled the Agent:
    - Opened PowerShell as Administrator and ran: *& 'C:\Program Files (x86)\ossec-agent\agent-auth.exe' -m 192.168.1.235.*
5. Started the Agent:
    - Ran: *net start Wazuh* to start the service.
    - Verified with: *net start | find "Wazuh"* to confirm it was running.



6. Confirmed Dashboard Connection:
    - Refreshed the Wazuh dashboard at https://192.168.1.235 (login: admin/admin) and checked the Agents tab, where "ThinkpadK" was listed as Active.



Setup Wazuh Agent on AWS EC2 Instance

To connect the AWS EC2 instance to our Wazuh server, I used Tailscale to create a secure, private network between the instance and the Wazuh server. This was a new process after troubleshooting for several days.

Instead of using the PuTTY app, I SSH'd into the AWS EC2 instance through PowerShell with the command:

ssh -i "vpn-key.pem" ubuntu@34.226.208.129

1. Connect to the EC2 instance via SSH
2. I ran: *sudo systemctl start wazuh-agent*
3. I verified with: *sudo systemctl status wazuh-agent*

```
● wazuh-agent.service - Wazuh agent
     Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor p>
     Active: active (running) since Fri 2025-08-08 00:59:22 UTC; 16h ago
    Process: 91920 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (c>
```

4. Install Tailscale on EC2 by running the Tailscale installation script:
   curl -fsSL https://tailscale.com/install.sh | sh
5. After installation, I ran:
   sudo tailscale up

```
Installation complete! Log in to start using Tailscale by running:

sudo tailscale up
ubuntu@ip-172-31-22-21:~$ sudo tailscale up

To authenticate, visit:

        https://login.tailscale.com/a/1c483f42011e3d

Success.
```

This generated a URL for authentication, which I opened in my browser to log into my Tailscale account. Once authenticated, the EC2 instance appeared in my Tailscale admin console.

- Reinstall the Wazuh Agent
- Since a previous agent installation was already present, I stopped and removed it:
  sudo systemctl stop wazuh-manager wazuh-agent
  sudo apt remove --purge wazuh-manager wazuh-agent -y

- Install the Wazuh Agent with the Correct Manager Address using the Wazuh server's Tailscale IP as the manager address:

  curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo gpg --dearmor -o /usr/share/keyrings/wazuh.gpg
  echo 'deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main' | sudo tee

/etc/apt/sources.list.d/wazuh.list

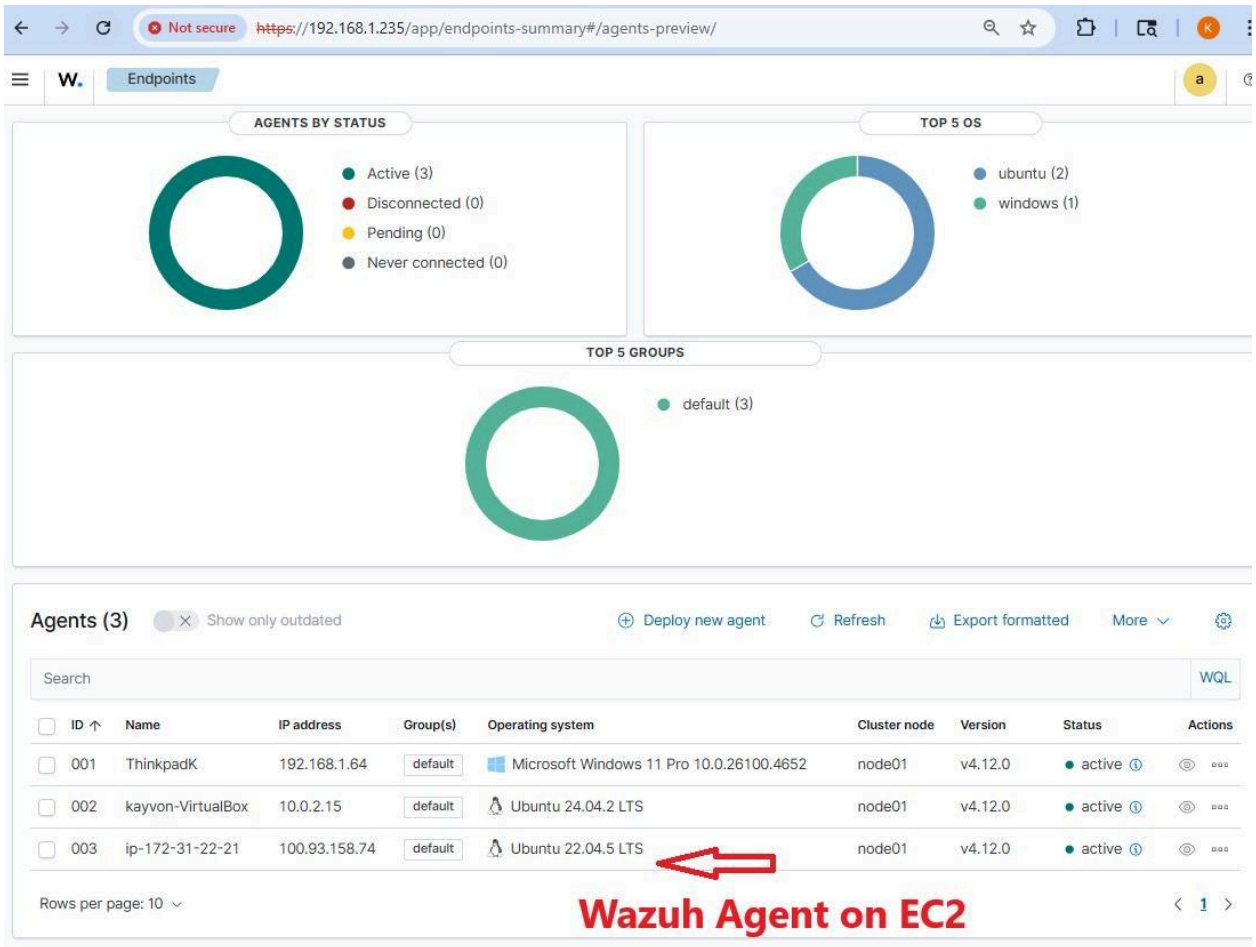
sudo apt update

sudo WAZUH_MANAGER="100.65.50.68" apt install -y wazuh-agent

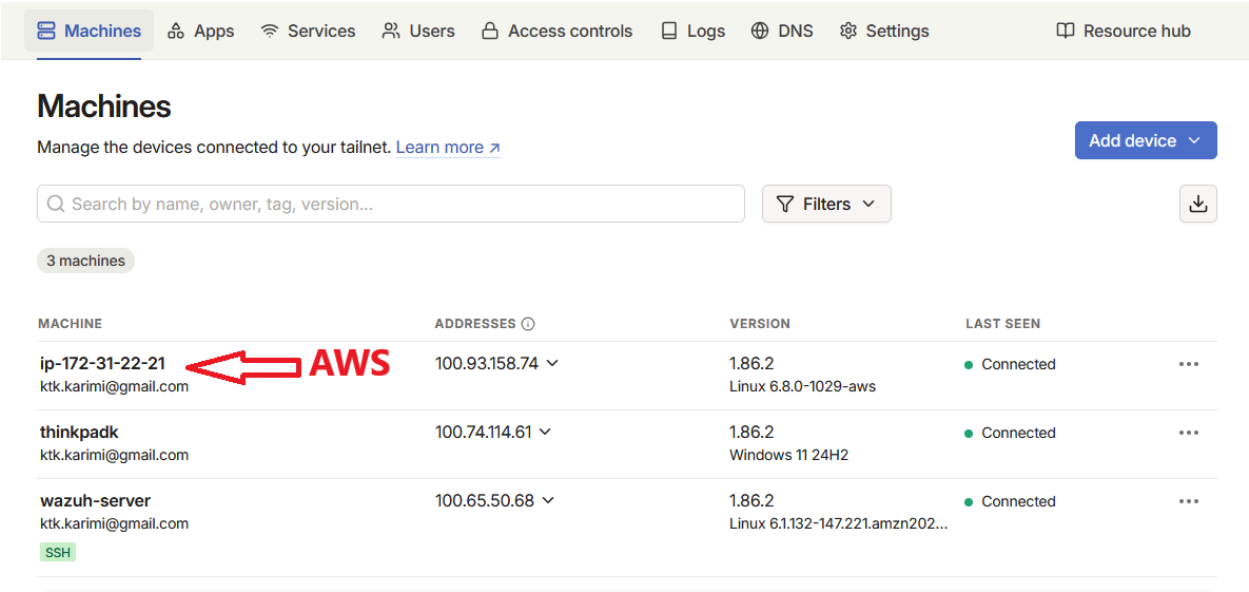
sudo systemctl enable --now wazuh-agent

- Verification

  Once installed, I confirmed the agent appeared in the Wazuh dashboard. The EC2 instance was successfully connected and reporting to the manager.



The screenshot shows the Tailscale admin console with the AWS EC2 instance (ip-172-31-22-21) connected. The IP address here matches the Wazuh dashboard entry for the EC2 Wazuh agent, verifying connection between the EC2 instance and the Wazuh server.



This setup successfully demonstrates the integration of Wazuh agents across three different systems: a Windows 11 host, an Ubuntu VirtualBox VM, and an AWS EC2 Ubuntu instance. Using Tailscale provided secure connectivity to the EC2 instance, enabling agent installation and registration without direct public exposure. The IP address between the Tailscale admin console and the Wazuh dashboard verifies that the EC2 agent is active and communicating with the Wazuh server.