DEPLOYING A WAZUH LAB IN VIRTUAL ENVIRONMENT

Step by Step Tutorial

Hafiz Javid
Portfolio

Deploying a Wazuh Lab: Building the Environment and Adding Agents

This tutorial walks through the process of setting up a small Wazuh lab on a single host. Using virtual machines gives you a self-contained environment for experimentation while keeping your main operating system untouched. The lab is structured with one **Wazuh server** running Ubuntu 22.04 LTS and several agents representing different endpoint operating systems.

1. Preparing the virtual environment

Before installing Wazuh, you need an environment that mirrors a small network. I used **Oracle VM VirtualBox** to create four virtual machines: one acts as the Wazuh server and the other three act as agents. The machines are connected via a bridged network so they can communicate as if they were on the same LAN. Figure 1 shows the virtual environment: three Ubuntu machines and one Kali machine, with the server running Ubuntu 22.04 LTS and the agents running Ubuntu 18.04 LTS, Ubuntu 22.04 LTS and Kali Linux 2023.4; the host Windows 11 system serves as an additional agent.

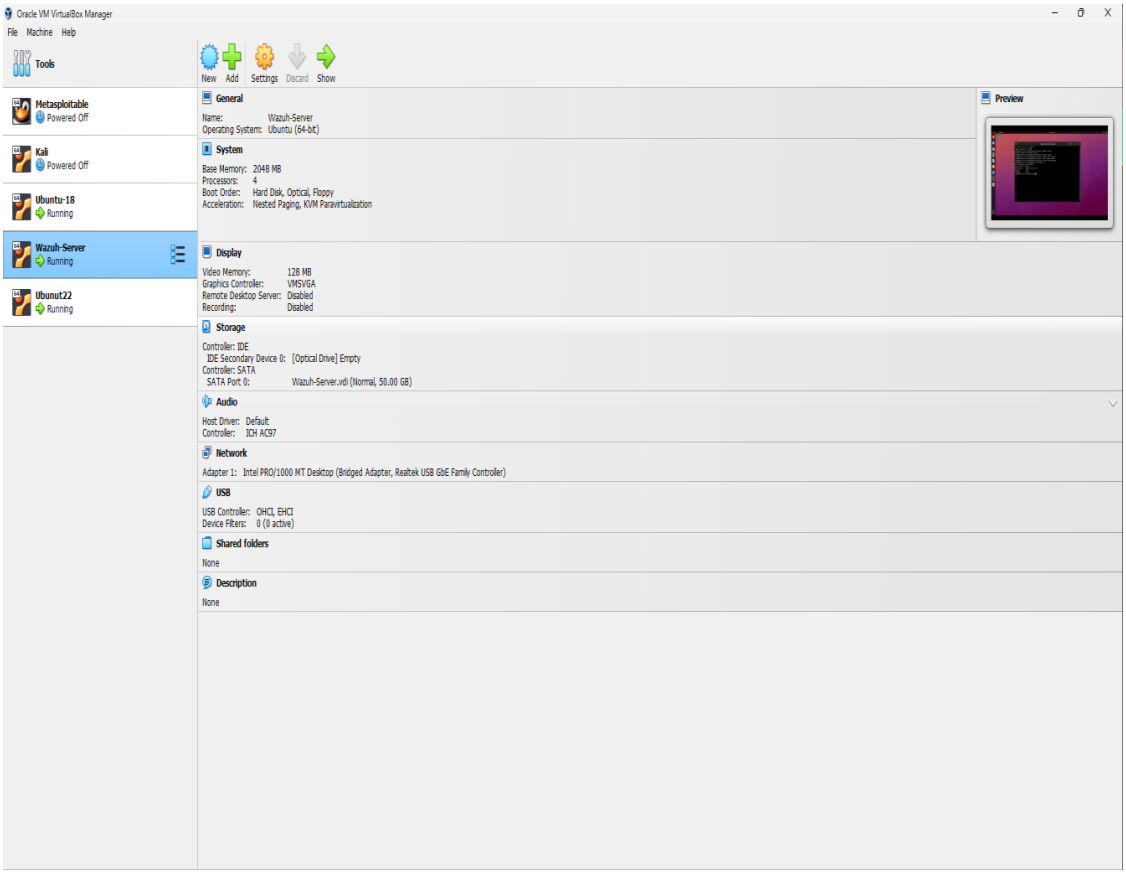

Figure 1 Virtual Environment of Ubuntu machines.

Tip: Configure each VM with a bridged network adapter so they obtain IP addresses on the same subnet as your host. This makes it simple for the server and agents to reach each other.

2. Installing the Wazuh server

Wazuh consists of three components: the **indexer**, the **server/manager** and the **dashboard**. While you can install each component manually but in this guide, the recommended is to use the single-command installation script provided by Wazuh, which automates downloading and configuring all components. On your Ubuntu 22.04 server VM, run the following command as **root**:

```
curl -sO https://packages.wazuh.com/4.13/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

This script cleans any previous installation, adds the Wazuh package repository, installs the indexer, manager and dashboard, and outputs credentials for the dashboard. The `-a` flag accepts the licence agreement; the optional `-o` flag overwrites an existing installation. You can use -o flag if you have an existing or partially installed Wazuh setup.

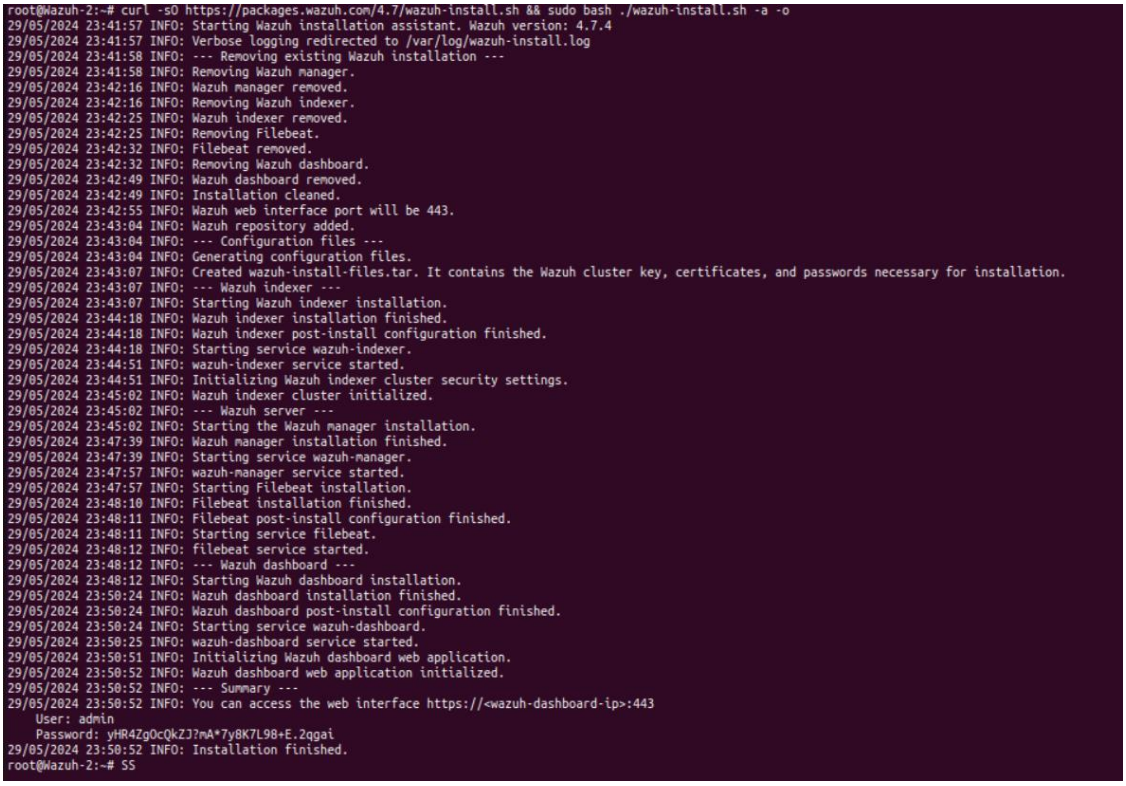

Figure 2 Completion of Wazuh installation.

When the installation completes, note the URL and credentials printed in the terminal – you'll need them to log into the dashboard. To determine the IP address of your server, run

`ip a` and look for the address on your bridged interface. For example, if the server's IP is `192.168.0.17` then your dashboard will be available at `https://192.168.0.17`.

3. Accessing the Wazuh dashboard

Open a web browser on your host or VM and navigate to the URL displayed after installation. Accept the self-signed certificate warning if prompted, then log in using the username and password provided by the installer. The dashboard opens to an overview page showing SIEM, XDR, regulatory compliance and other modules. Since no agents have been deployed yet, the "Agents" section will show **zero** active agents.

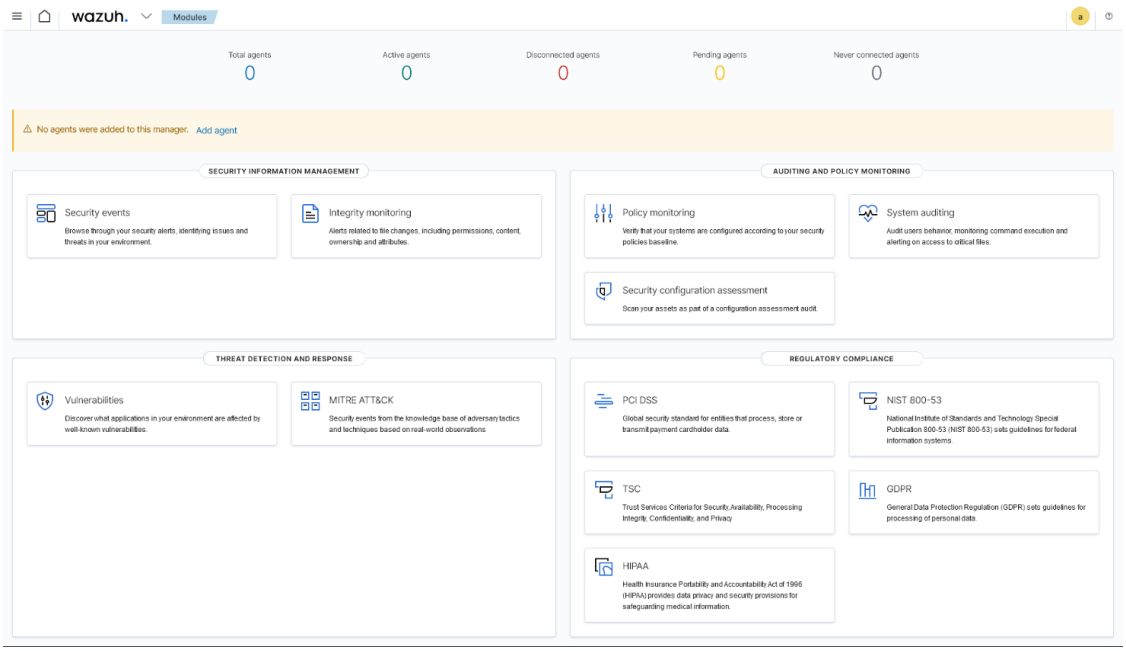

Figure 3 Wazuh dashboard with no agents.

4. Deploying Wazuh agents via the dashboard

You can add agents from the **Agents** section of the dashboard. There are two deployment methods: using the web interface or using the `manage_agents` script on the server. The web interface is straightforward and will be used here.

From the **Agents** page, click **Deploy new agent**. A form appears prompting you to select the operating system, enter the server address, optionally set a name and group, and then run generated commands on the client machine. For a Linux agent (e.g. Kali), choose the **Deb** package, enter the server's IP (`192.168.0.17` in the example), and accept the default group. The wizard will generate a single shell command that downloads and installs the agent, and it also provides systemd commands to start the service.

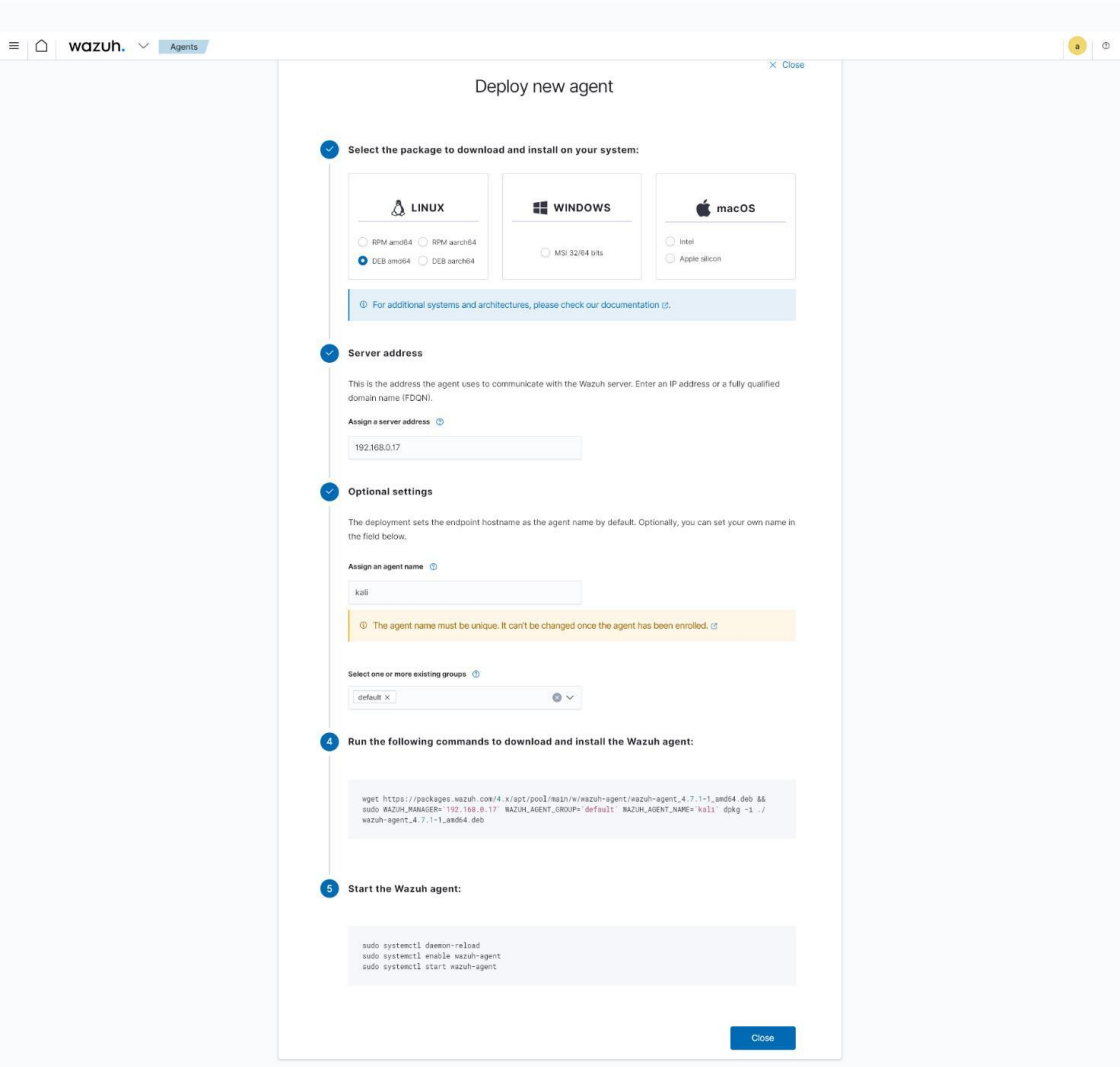

Figure 4 Details of newly deployed agents.

Run the installation command on the agent VM's terminal as root. After installation, enable and start the agent service using the systemd commands shown in the wizard. For example:

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
sudo systemctl status wazuh-agent
```

The last command should report `active (running)` as shown below. If it doesn't, check that the manager IP is correct in the agent's configuration file (`/var/ossec/etc/ossec.conf`). Root privileges are required for these steps.

Figure 5 Status of the Wazuh agent.

Repeat the deployment process for the other agent VMs. Wazuh provides installers for Windows and macOS as well. When deploying the Windows agent, choose the **MSI 64-bit** package from the wizard, enter the server address and download the installer. After running the MSI on your Windows machine, start the Wazuh agent service from the Services app or by running `NET START Wazuh` as administrator.

5. Verifying agent registration

Once each agent service is running, return to the **Agents** page in the dashboard and click **Refresh**. The new agents should appear in the list with green status indicators. The ID, name, IP address and operating system of each agent will be displayed. If an agent appears as **disconnected**, ensure that the service is running on the endpoint and that the `ossec.conf` file contains the correct manager IP.

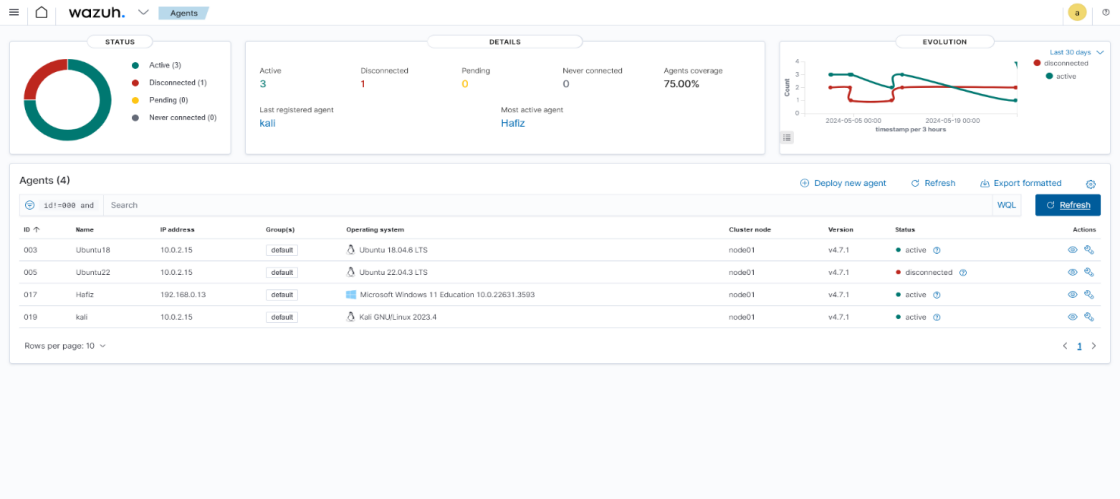

Figure 6 Fourth deployed agent.

In the example above, three agents are active (Ubuntu 18.04, Windows 11 and Kali) while the Ubuntu 22.04 agent is currently disconnected. Hover over the status icon to see details or click the eye icon in the **Actions** column to open the agent detail page.

6. Restarting the Wazuh services

Occasionally you may need to restart the Wazuh indexer and manager to apply configuration changes. On the server VM, run the following commands:

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-indexer
sudo systemctl start wazuh-indexer
sudo systemctl restart wazuh-manager
```

These commands reload systemd configuration, enable and start the indexer and restart the manager. After a restart, wait a moment and then refresh the dashboard to confirm that all services are running and agents reconnect.