



**wazuh.**

**Installation guide  
Beginner Friendly**


By:  
Muhammad Ahmad

## What is Wazuh?

It is a widely used, free platform that provides XDR (Extended Detection and Response) and SIEM (Security Information and Event Management) capabilities. It can be installed on various devices, including containers, clouds, and host endpoints. It can perform multiple functions like **log monitoring, incident response and analysis, regulatory compliance, rule-based actions**, and a lot more. It can also be installed on agentless devices such as **firewalls, switches, routers, etc.**

## Wazuh Components

### 1. Wazuh Indexer:

 It provides the storage of all the logs and also for the alerts generated by Wazuh server. It provides an analytical engine and full text-based search facility, we can filter out data based on certain conditions and baselines.

### 2. Wazuh Server:

It is the central component of the Wazuh security platform that analyzes the data from **agents, external APIs, and Network devices** etc. It generates alerts and responses based on rulesets that make it easier for professionals to identify anomalies.

### 3. Wazuh Dashboard

As the name suggests, it is a dashboard that effectively displays real-time threats and logs. It uses graphs, charts, and tables to display in a clear manner. It is like the display board of the Wazuh platform.

- **Wazuh Agent**

It is installed on the endpoints, and it is universal. It can be installed on any type of operating system. It is a collector that gathers all logs, telemetry, and system data from endpoints.

## Installing wazuh server

Installing wazuh is very simple as they provide a very user-friendly documentation. We can also use quick installation for small organization or for home-lab project. You can check it out here. [documentation.wazuh.com](https://documentation.wazuh.com)

## Hardware requirements

hardware for a quickstart deployment:

Agents	CPU	RAM	Storage (90 days)
1-25	4 vCPU	8 GiB	50 GB
25-50	8 vCPU	8 GiB	100 GB
50-100	8 vCPU	8 GiB	200 GB

We recommend a distributed deployment. Multi-node cluster configuration is available for

such as for 1 to 3 agents

- 1 or 2+ vCPU
- 2 to 4+ GiB of Ram
- Storage based on you disk size.

You can have less than this if you are doing it for your cyber security analyst lab project or just doing for fun based on you usage.

Here, I have provided the simplified steps from their documentation.

### Step 1: Download the wazuh assistant

```
curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh
```

### Step 2: Run the installation file of wazuh assistant

```
sudo bash ./wazuh-install.sh -a
```

Grab a cup of coffee because it is gonna take few time.

After successful installation and you are good to go!

### Step 3: Copy the passwords from the file

You can find the passwords for all the Wazuh indexer and Wazuh API users in the wazuh-passwords-txt file inside wazuh-install-files.tar. To print them, run the following command:

```
$ sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
```

### Step 4: Open the Wazuh dashboard

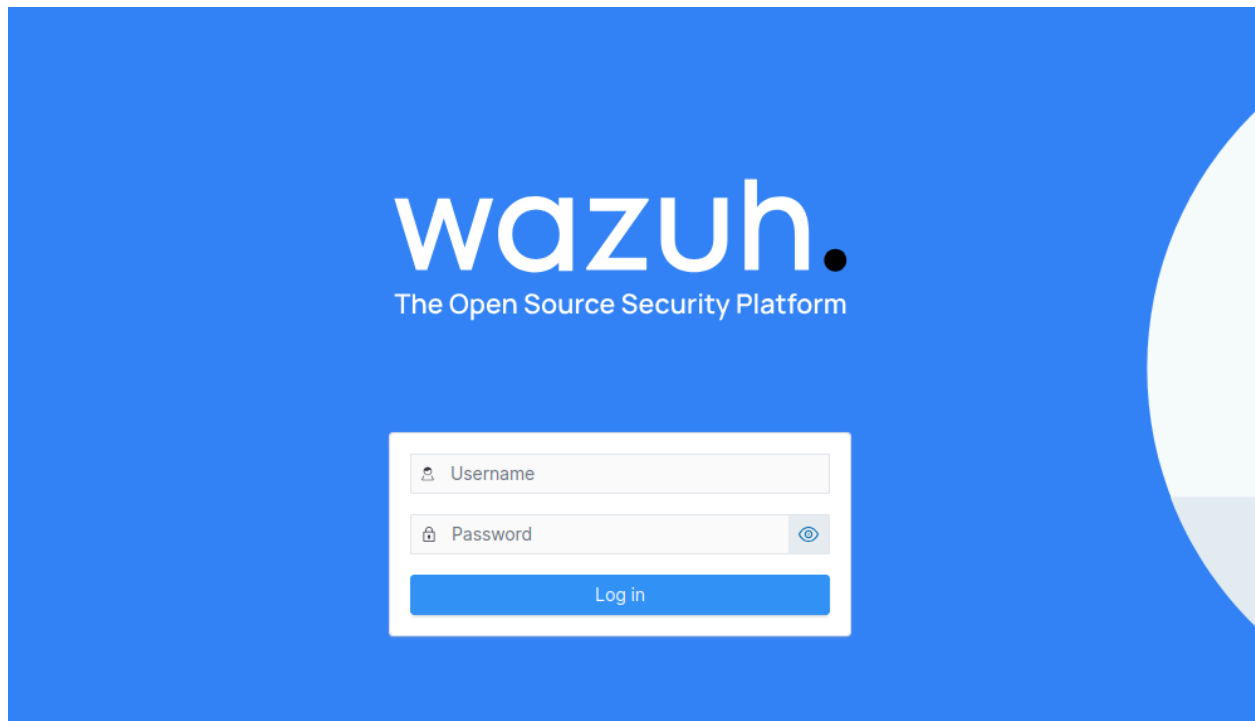
Go to your web browser and type the ip address of you virtual box machine you can find it using the command

Windows `ipconfig`

Linux `ifconfig`

```
https://<Virtual_Machine_IP_ADDRESS>
```

Modern browser will show it as a malicious website but trust me it's the dashboard and open it anyways.

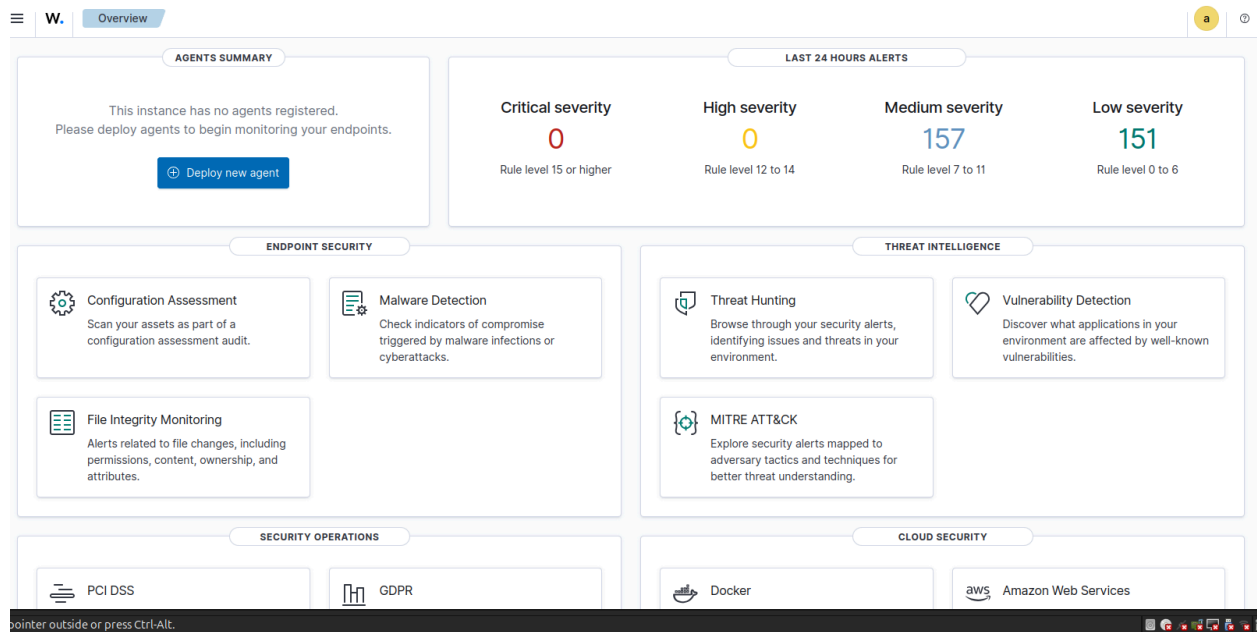


**Username:** admin

**Password:** you copied from the file above.

Type your credentials and voila, you are just done with the setup of your Wazuh indexer, server, and Wazuh dashboard.

**Here is your Wazuh Dashboard.**



## Installing the Wazuh agent on endpoint (am using Ubuntu)

### Step 1: Installing the GPG key

```
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
```

### Step 2: Adding the repository

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/  
stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
```

### Step 3: Update the package information

```
apt-get update
```

### Step 4: Install the agent

```
apt-get install wazuh-agent
```

**Note:** Compatibility between the Wazuh agent and the Wazuh manager is guaranteed when the Wazuh manager version is later than or equal to that of the Wazuh agent. So after installing you can disable its updates so it can match with server version.

## Linking the Wazuh agent with wazuh server

### Step 1: Edit ossec.conf file on agent machine

```
sudo nano /var/ossec/etc/ossec.conf
```

Inside the **<client>** block, configure the server address like this:

```
<client>
  <server>
    <address>YOUR_WAZUH_SERVER_IP</address>
    <port>1514</port>
    <protocol>tcp</protocol>
  </server>
</client>
```

### Step 2: On wazuh server, add the agent

```
sudo /var/ossec/bin/manage_agents
```

Inside the menu:

- Press **A** to add a new agent
- Enter a name and the agent's IP
- Copy the **generated key**

```

*****
* Wazuh v4.12.0 Agent manager.          *
* The following options are available: *
*****
  (A)dd an agent (A).
  (E)xtract key for an agent (E).
  (L)ist already added agents (L).
  (R)emove an agent (R).
  (Q)uit.
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
    * A name for the new agent: flask_agent
    * The IP Address of the new agent: 172.16.167.130
Confirm adding it?(y/n): y
Agent added with ID 001.

*****
* Wazuh v4.12.0 Agent manager.          *

```

### Step 3: On wazuh agent, import the key

`sudo /var/ossec/bin/manage_agents`

Inside the menu:

- Press **I** to import a key
- Paste the key from the server

```
*****
* Wazuh v4.12.0 Agent manager.      *
* The following options are available: *
*****
  (I)mport key from the server (I).
  (Q)uit.
Choose your action: I or Q: I

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or \'q\' to quit): MDAXIGZsYXNrX2FnZW50IDE9M14xN14xNjc0MTUwIGU2NTk0YmQyYUJ2MjYyN2UzN2M2MTRlY2UzOGNhMzhkMQw0NTQ2YmQ5OTJlMTQ4Y2I0TEYnJzINDA9MzMsY2YI
=

Agent information:
  ID:001
  Name:flask_agent
  IP Address:172.16.167.130

Confirm adding it?(y/n): y
Added.

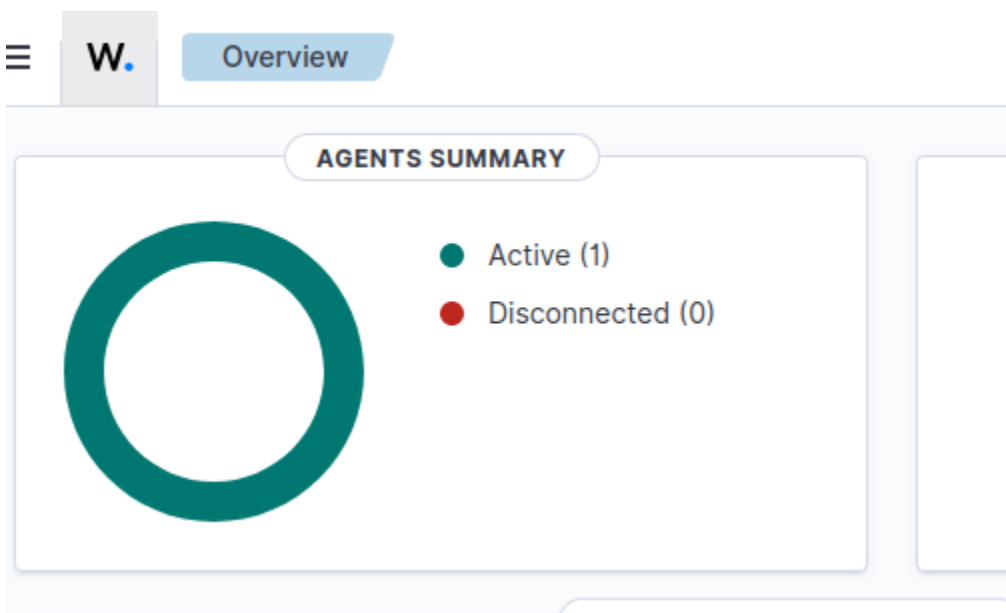
*****
* Wazuh v4.12.0 Agent manager.      *
* The following options are available: *
*****
  (I)mport key from the server (I).
  (Q)uit.
Choose your action: I or Q: q

manage_agents: Exiting.
```

## Step 4: Restart the Wazuh agent

```
sudo systemctl restart wazuh-agent
```

## Verify the linkage between them by opening the Wazuh dashboard



Here you can see its active.