



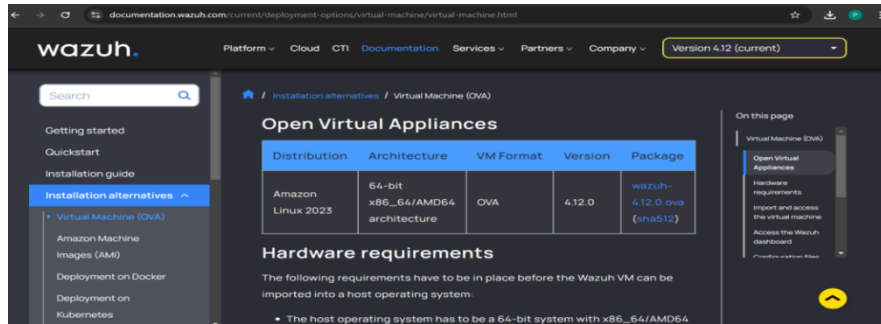
# INSTALLING **WAZUH** AND WAZUH **AGENTS**

## STEP-BY-STEP GUIDE

## TABLE OF CONTENTS

<b><u>Downloading .OVA files</u></b>	<b><u>3</u></b>
<b><u>Network Setting</u></b>	<b><u>4</u></b>
<b><u>Start the Machine</u></b>	<b><u>4</u></b>
<b><u>Acessing Wazuh Dashboard</u></b>	<b><u>5</u></b>
<b><u>Navigating Dashboard</u></b>	<b><u>6</u></b>
<b><u>Deploying Wazuh Agent</u></b>	<b><u>6</u></b>
Windows	6
Linux	8
<b><u>Verification</u></b>	<b><u>9</u></b>

# 1- Downloading .OVA file to install Wazuh in Window Operating System



The Packages List tells us about the Version File format and Distribution of the Wazuh Current version.

Open Virtual Appliances				
Distribution	Architecture	VM Format	Version	Package
Amazon Linux 2023	64-bit x86_64/AMD64 architecture	OVA	4.12.0	wazuh-4.12.0.ova (sha512)

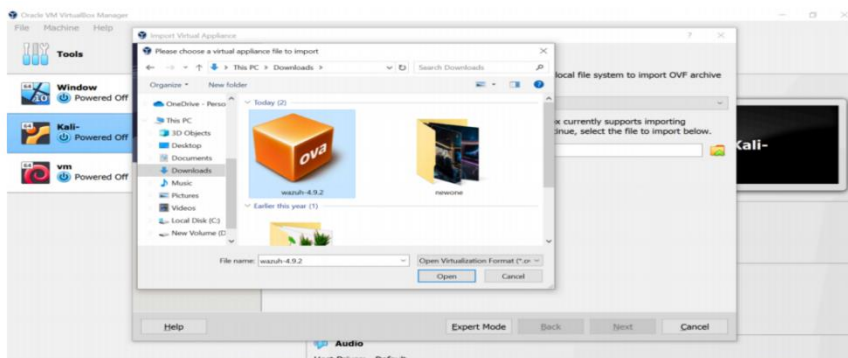
Importing the Wazuh OVA file in Virtual Box.

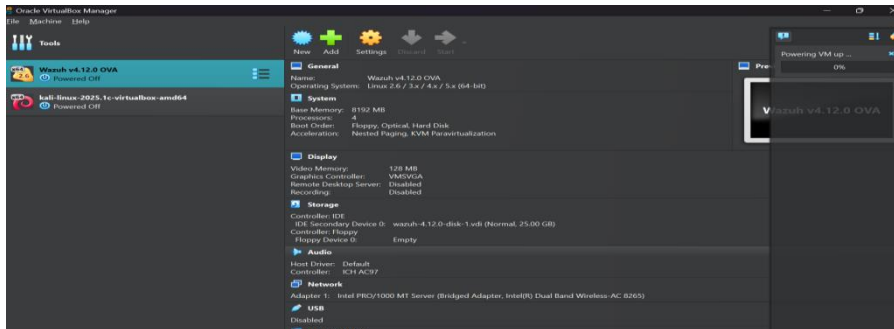
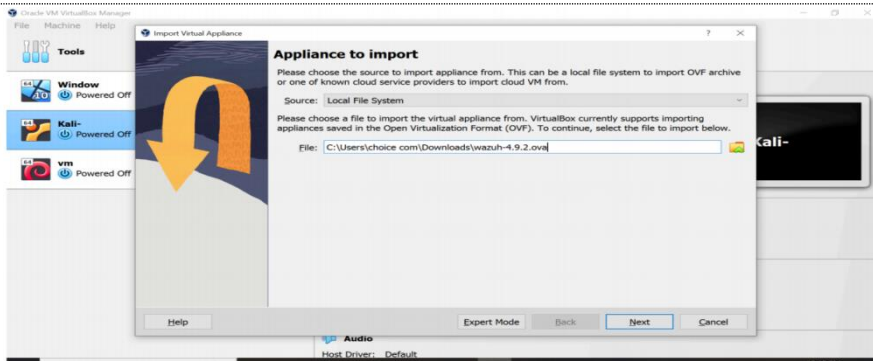


After opening the Virtual Box go to File> Then Import Appliances.



Now Select the Ova Wazuh File.

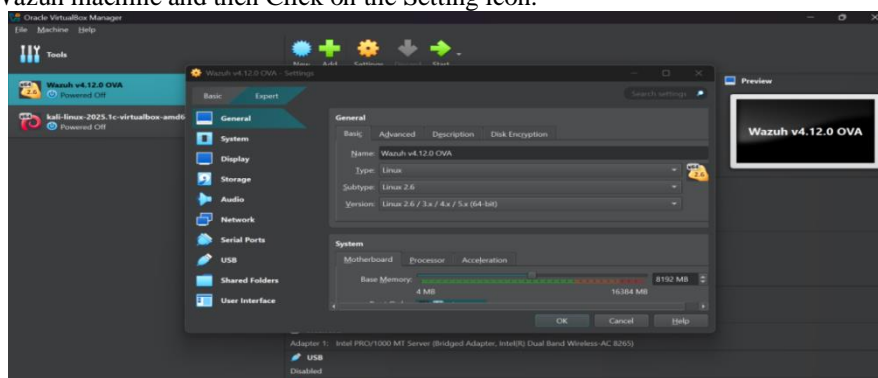




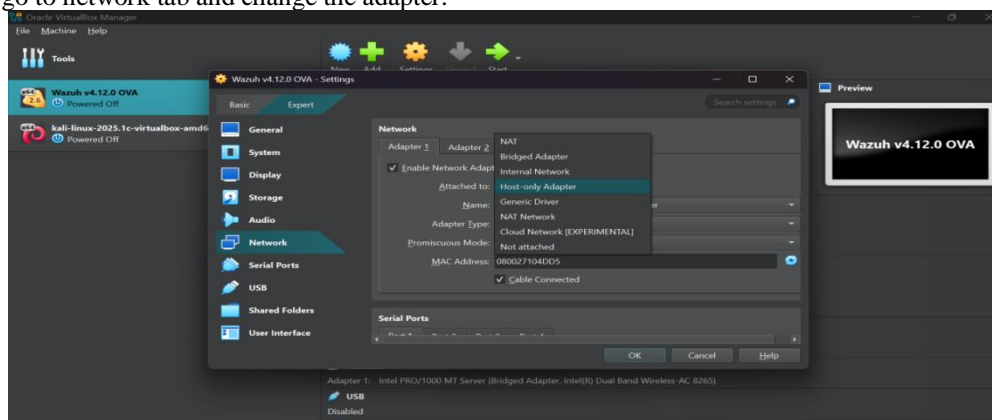
Wazuh File imported successfully.

## 2- Changing the Network Setting to “Host-only-Adapter”

Select the Wazuh machine and then Click on the Setting icon.



Now go to network tab and change the adapter.



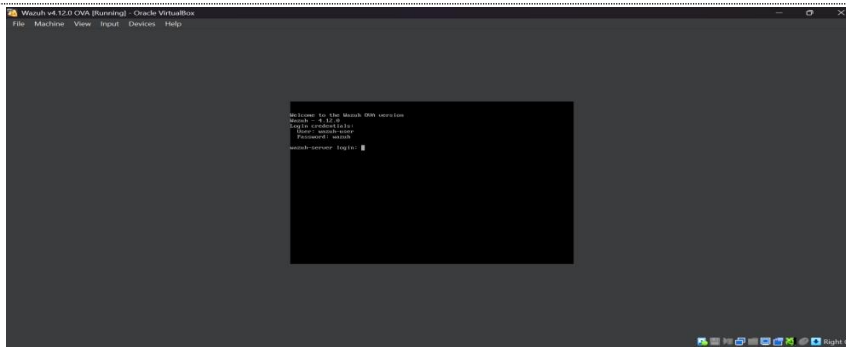
Select Host Only adapter then Hit OK.

## 3- Start the machine

Click on the start button to start the wazuh. After stating Enter the Username and Password

**Username:** wazuh-user

**Password:** wazuh



Enter Username and Password then press Enter. After login write these commands:

```
sudo systemctl start wazuh-dashboard  
sudo systemctl start wazuh-indexer
```

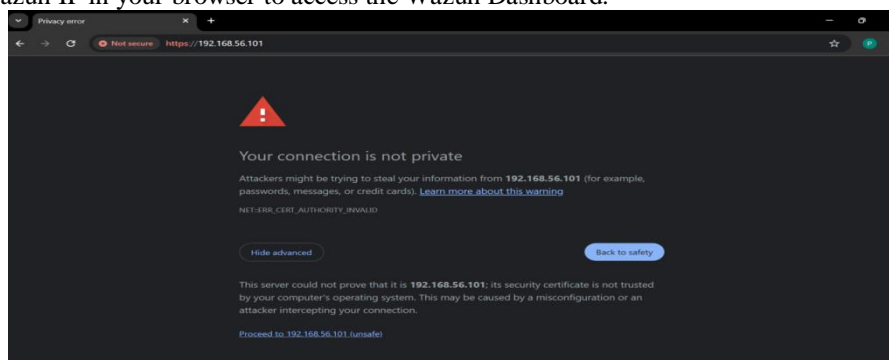
After command write “IP a” to check IP Address of your Wazuh machine.



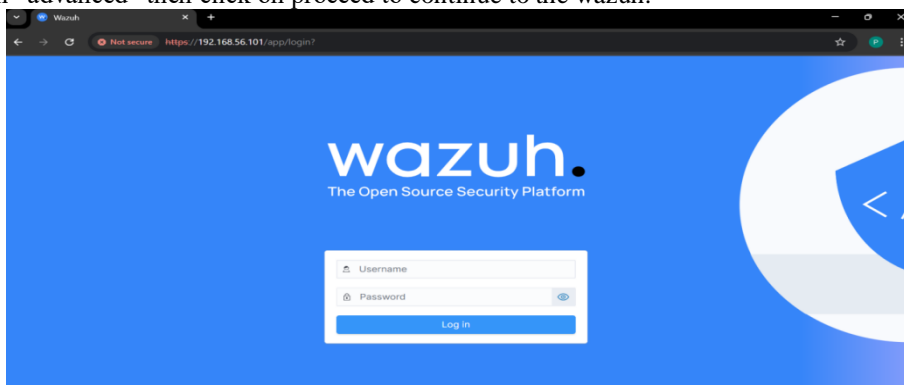
My wazuh IP address is **192.168.56.101**

## 4-Accessing Wazuh Dashboard

Type Wazuh IP in your browser to access the Wazuh Dashboard.



Click on “advanced” then click on proceed to continue to the wazuh.

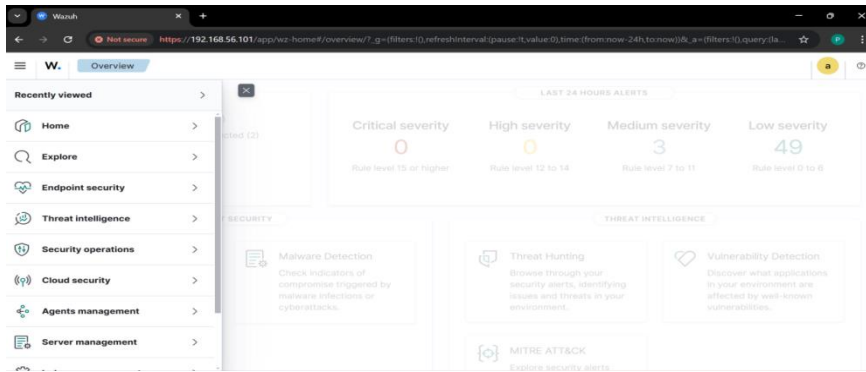


To login to wazuh Dashboard Enter Username and password:

Username: **admin**

Password: **admin.**

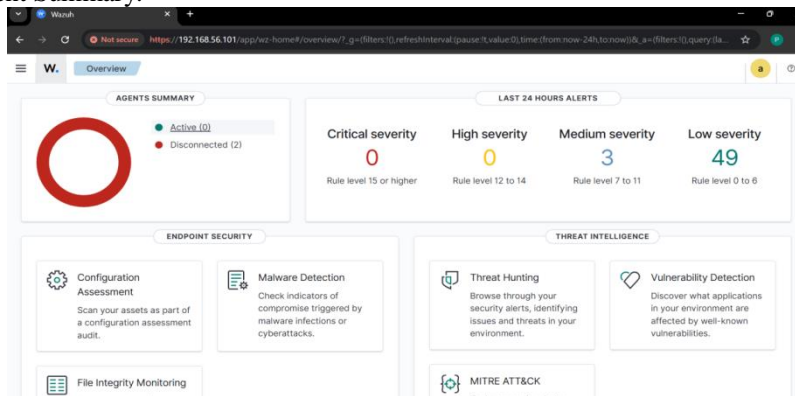
## 5-Navigating the Dashboard



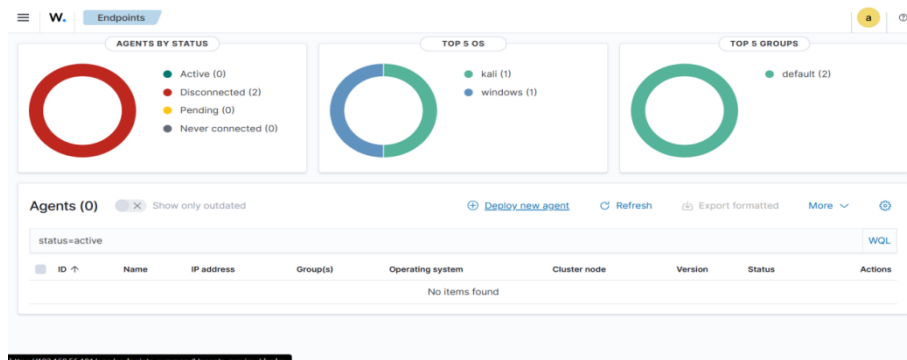
## 6-Deploying Wazuh Agent

### WINDOWS:

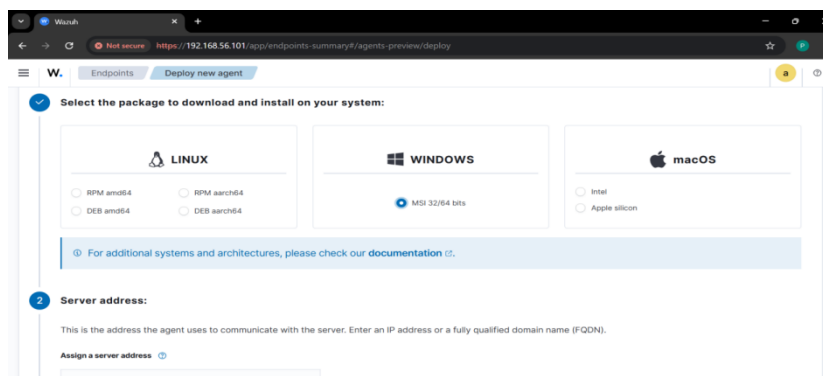
Go to agent Summary.



Click on “Deploy a new Agent”



Select Windows.



Add IP address that is server's IP address. And also assign a agent name.

Wazuh

Endpoints Deploy new agent

**Server address:**

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**

192.168.56.101

☐ 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:**

Win12Dows

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

Run the given Command in Powershell administer.

Wazuh

Endpoints Deploy new agent

**4 Run the following commands to download and install the agent:**

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.12.0-1.msi -OutFile $env:tmp\wazuh-agent; msexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER="192.168.56.101" WAZUH_AGENT_NAME="Win12Dows"
```

**Requirements**

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

**5 Start the agent:**

```
NET START WazuhSvc
```

Wazuh

Endpoints Deploy new agent

**5 Start the agent:**

```
NET START WazuhSvc
```

Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.12.0-1.msi -OutFile $env:tmp\wazuh-agent; msexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER="192.168.56.101" WAZUH_AGENT_NAME="Win12Dows"
```

Wazuh

Endpoints Deploy new agent

**5 Start the agent:**

```
NET START WazuhSvc
```

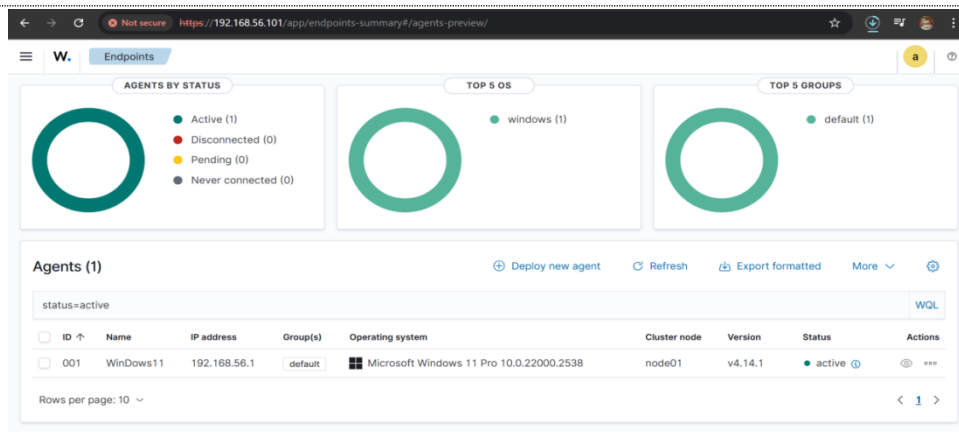
Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.12.0-1.msi -OutFile $env:tmp\wazuh-agent; msexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER="192.168.56.101" WAZUH_AGENT_NAME="Win12Dows"
PS C:\WINDOWS\system32> NET START WazuhSvc
The requested service has already been started.
More help is available by typing NET HELPMSG 2182.

PS C:\WINDOWS\system32>
```



## LINUX:

Add wazuh repository:

- Open Terminal
- Add wazuh repository by running:

Run these commands:

```
wal@kali:~$ sudo apt-get install wazuh-agent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wazuh-agent is already the newest version (4.12.0-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Update your package:

```
wal@kali:~$ sudo apt-get update
Get:1 http://deb.debian.org/debian bullseye InRelease [156 kB]
Get:2 http://deb.debian.org/debian bullseye-updates InRelease [55.4 kB]
Get:3 http://security.debian.org/debian-security bullseye-security InRelease [51.6 kB]
Get:4 http://deb.debian.org/debian bullseye-backports InRelease [55.4 kB]
Fetched 318.4 kB in 1s (31.8 MB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wazuh-agent is already the newest version (4.12.0-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

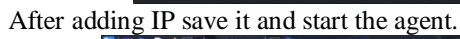
Install Wazuh-agent:

```
wal@kali:~$ sudo apt-get install wazuh-agent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wazuh-agent is already the newest version (4.12.0-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Configure the wazuh-agent

- Open file manager and navigate to `/var/ossec/etc/ossec.conf`
- Find `<address>` tag and set it to your wazuh manager's IP address.





The screenshot shows the Wazuh dashboard interface. At the top, there's a navigation bar with a search icon and a URL bar showing 'https://192.168.56.101/app/endpoints-summary#/agents-preview/'. Below the navigation bar, the main content area is divided into three sections: 'AGENTS BY STATUS', 'TOP 5 OS', and 'TOP 5 GROUPS'. Each section contains a donut chart and a list of items. The 'AGENTS BY STATUS' chart shows 1 Active (green), 1 Disconnected (red), 0 Pending (yellow), and 0 Never connected (grey). The 'TOP 5 OS' chart shows 1 kali (blue) and 1 windows (green). The 'TOP 5 GROUPS' chart shows 2 default (green). Below these charts, there's a section for 'Agents (1)' with a toggle for 'Show only outdated'. Below this, there's a search bar with 'status=active' and a 'WQL' button. A table lists the agents with columns: ID, Name, IP address, Group(s), Operating system, Cluster node, Version, Status, and Actions. The table shows one agent: ID 001, Name kali, IP address 10.0.2.15, Group(s) default, Operating system Kali GNU/Linux 2025.1, Cluster node node01, Version v4.12.0, Status active, and Actions. At the bottom, there's a 'Rows per page: 10' dropdown and a pagination link '1 > 1'.