



# wazuh.

## **Installing Wazuh Agents (Windows & Linux)**

**Lab Created By: MUHAMMAD MOIZ UD DIN RAFAY**

**Follow Me: [linkedin.com/in/moizuddinrafay](https://www.linkedin.com/in/moizuddinrafay)**

Installing the Wazuh agent offers several benefits for enhancing cybersecurity posture and ensuring robust monitoring and response capabilities:

**1. Threat Detection and Monitoring:** The Wazuh agent actively monitors system and application logs, file integrity, and system metrics in real-time. It detects security threats, anomalies, and potential breaches promptly.

**2. Intrusion Detection and Prevention:** By deploying Wazuh agents across your infrastructure, you create a network of sensors that can detect and prevent intrusion attempts, including malware, unauthorized access attempts, and other malicious activities.

**4. Log Management and Analysis:** Wazuh collects, normalizes, and analyzes logs from various sources, providing centralized visibility into system events and security incidents. This aids in forensic analysis, troubleshooting, and auditing activities.

**5. Incident Response and Remediation:** With Wazuh agents in place, security teams can respond swiftly to security incidents, leveraging automated response actions and remediation scripts to contain and mitigate threats effectively.

**6. Scalability and Flexibility:** Wazuh modular architecture allows for easy deployment and management of agents across diverse environments, including on-premises, cloud, and hybrid infrastructures, providing scalability and flexibility as your organization grows.

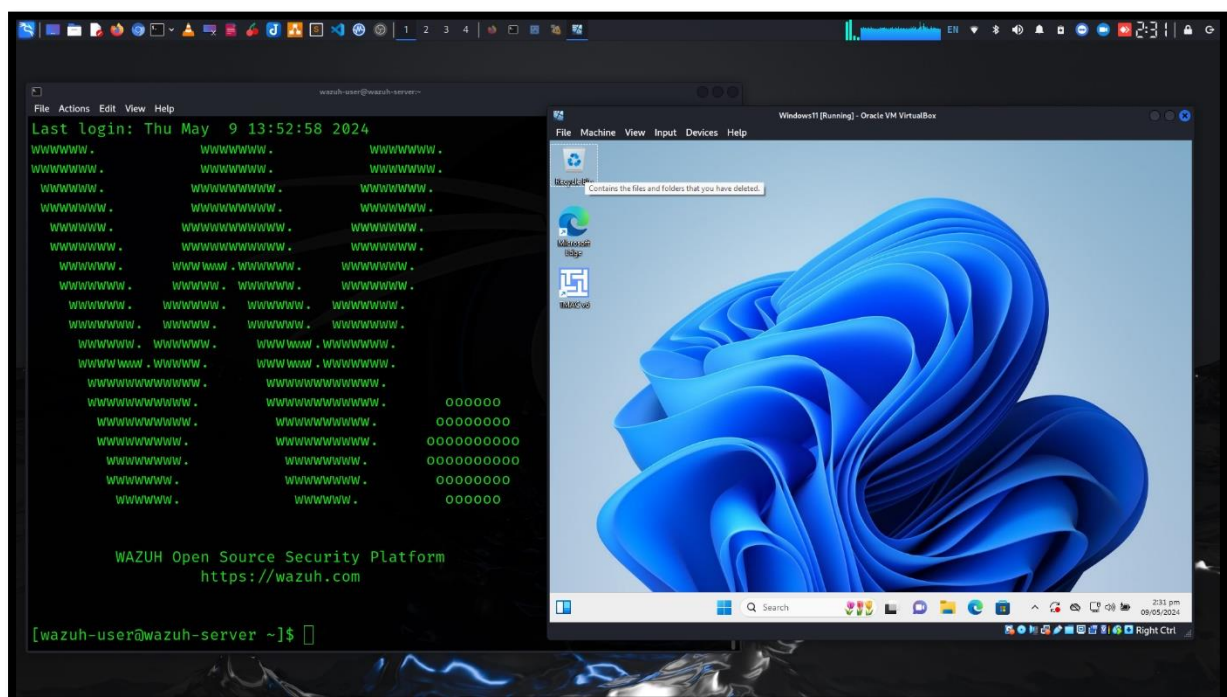
**7. Open Source and Community Support:** Being open-source, Wazuh benefits from an active community of developers and contributors, ensuring continuous improvement, bug fixes, and support from a wide range of users and experts.

## Step 01: Installing Wazuh-Agent on Windows11 OS.

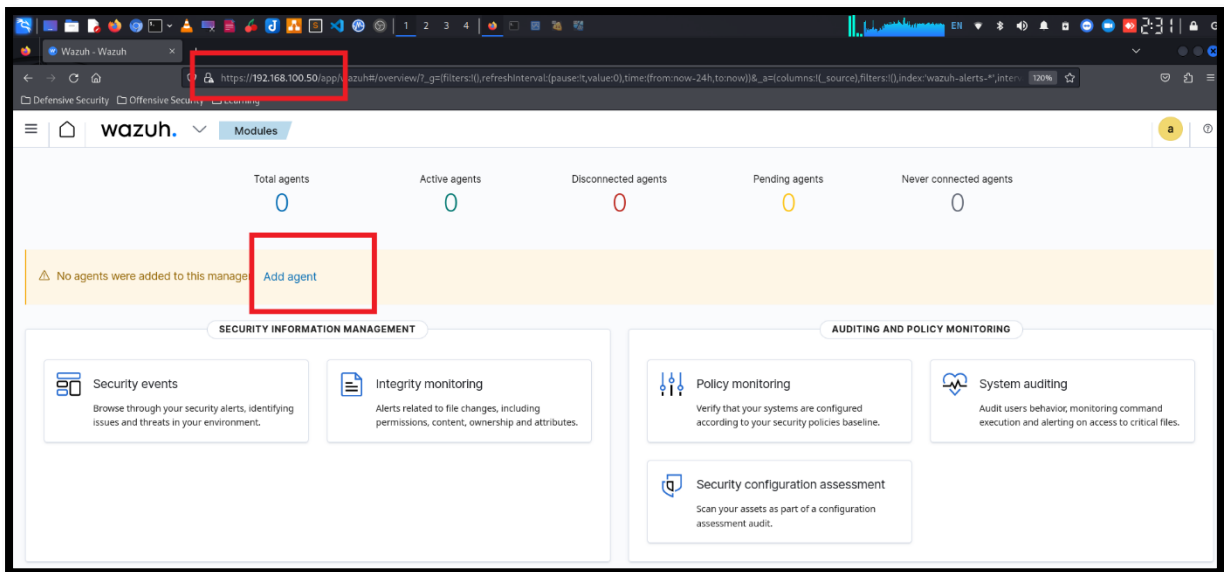
I have installed and running windows 11 and Wazuh Server in my VirtualBox.



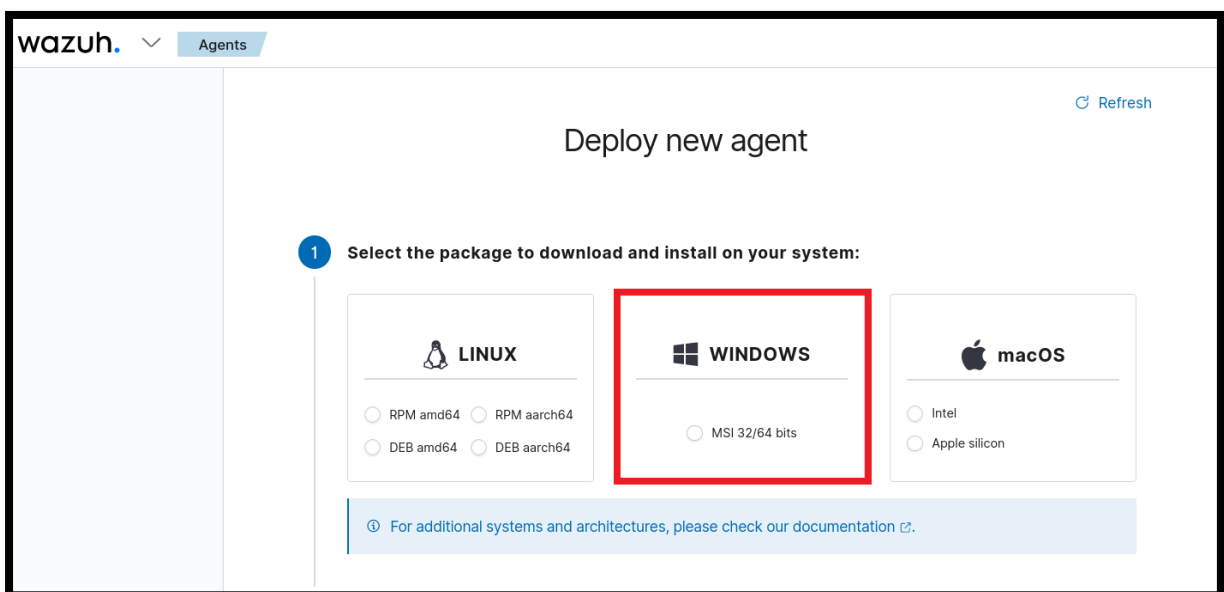
Here is running both Wazuh Server and Wazuh Agent



Now open browser and type the Wazuh Server IP Address in URL. You can also see there is no Active Agents so there is option available “Add agent” click on it.



When you click on “Add agent”, Wazuh agent deployment wizard is open. You have to select windows package.



Enter the “Server address” in my case it’s “192.168.100.50”

The screenshot shows the Wazuh installation wizard. The first step, 'Select the package to download and install on your system:', has three tabs: LINUX, WINDOWS, and macOS. Under LINUX, there are four radio buttons: RPM amd64, RPM aarch64, DEB amd64, and DEB aarch64. Under WINDOWS, the MSI 32/64 bits option is selected. Under macOS, there are two radio buttons: Intel and Apple silicon. A link for additional systems and architectures is provided. The second step, 'Server address:', explains that this is the address the agent uses to communicate with the server. A text input field labeled 'Assign a server address:' contains the IP address '192.168.100.50', which is highlighted with a red box.

Scroll down a little there is option available “Assign an agent name” you have to enter your agent name here in my case I am using “Windows11” as agent name.

The screenshot shows the 'Optional settings' step of the Wazuh installation wizard. It explains that by default, the deployment uses the hostname as the agent name, but a different agent name can be used. A text input field labeled 'Assign an agent name:' contains the text 'Windows11', which is highlighted with a red box. Below this field is a warning message: 'The agent name must be unique. It can't be changed once the agent has been enrolled.' There is also a section for 'Select one or more existing groups:' with a dropdown menu showing 'default'. The final step, 'Run the following commands to download and install the agent:', provides a command to download and install the agent with specific parameters.

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.3-1.msi -OutFile $(env.tmp)\wazuh-agent; msixexec.exe /i $(env.tmp)\wazuh-agent /q WAZUH_MANAGER='192.168.100.50' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='Windows11' WAZUH_REGISTRATION_SERVER='192.168.100.50'
```

Scroll down little bit more here is Wazuh agent install and download command, copy this command and paste it in windows powershell.

4

Run the following commands to download and install the agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.3-1.msi -OutFile $(env:tmp)\wazuh-agent; msixec.exe /i $(env:tmp)\wazuh-agent /q WAZUH_MANAGER='192.168.100.50' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='Windows11' WAZUH_REGISTRATION_SERVER='192.168.100.50'
```

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.

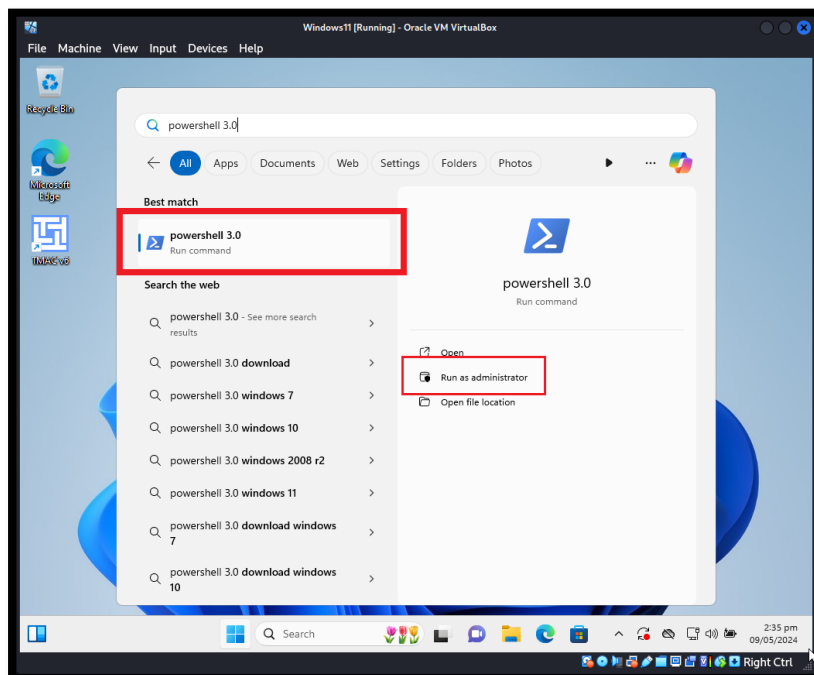
5

Start the agent:

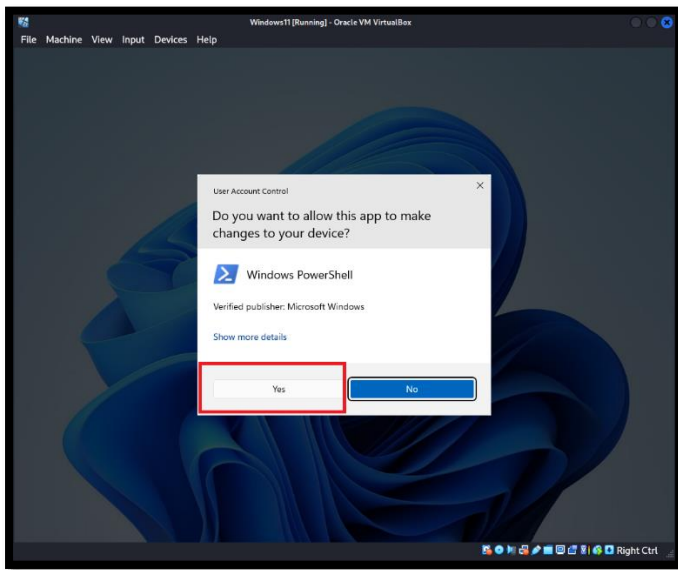
```
NET START WazuhSvc
```

Close

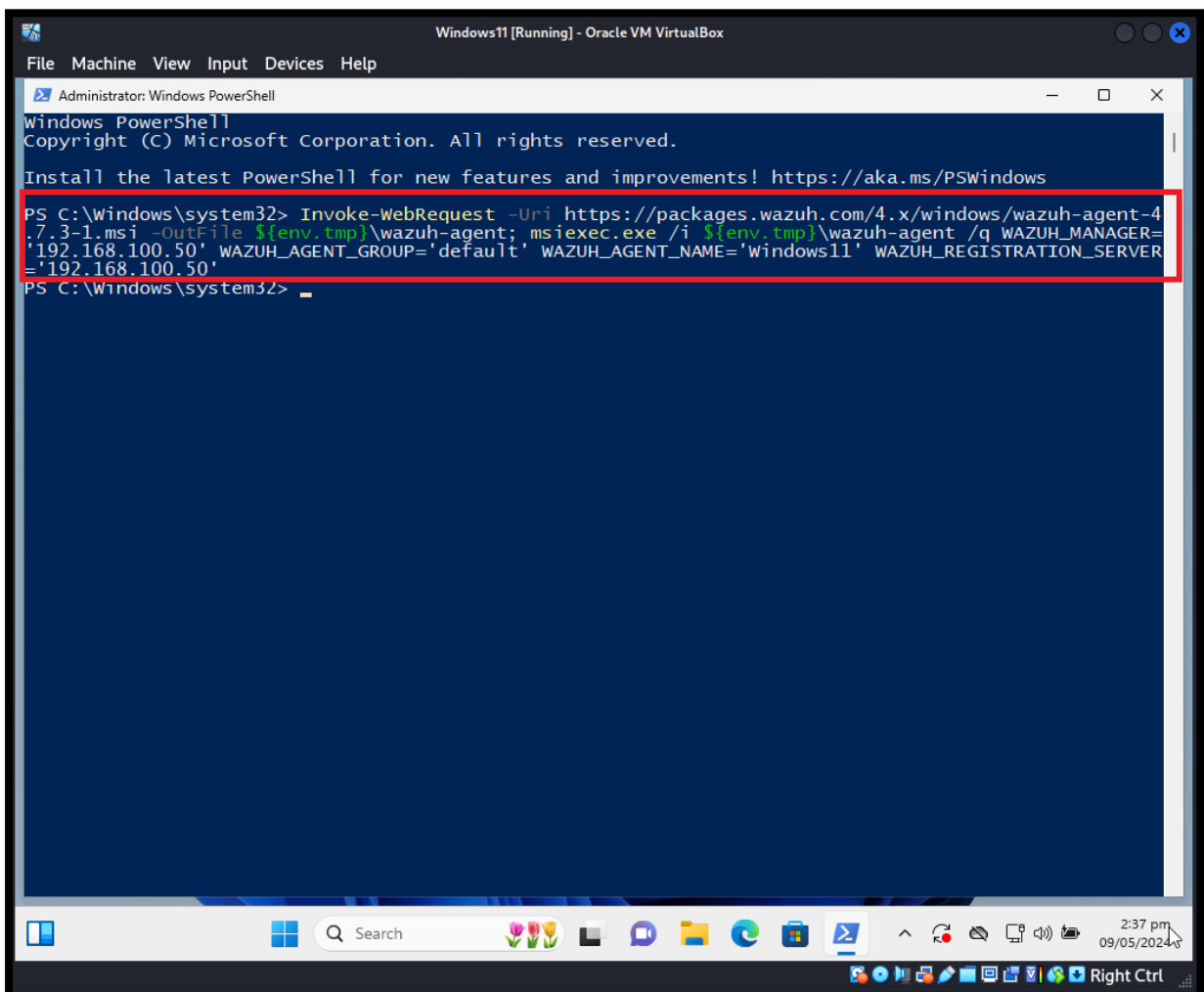
Run powershell 3.0 as administrator permission.



Click “YES” button to run powershell as administrator.

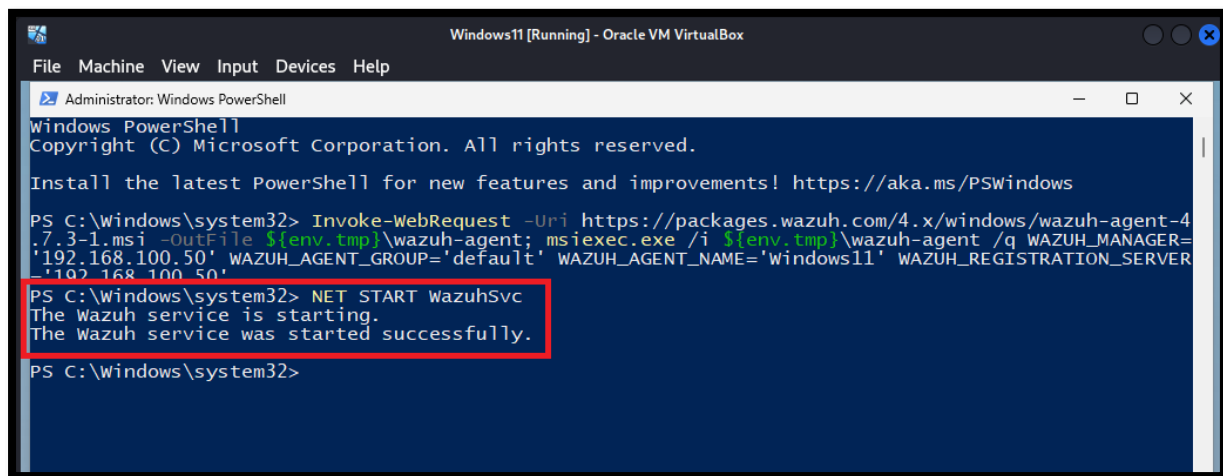


Paste the copied command in powershell and then press Enter.



Wazuh agent is installed now we have to run Wazuh-agent service.

Command: NET START WazuhSvc



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

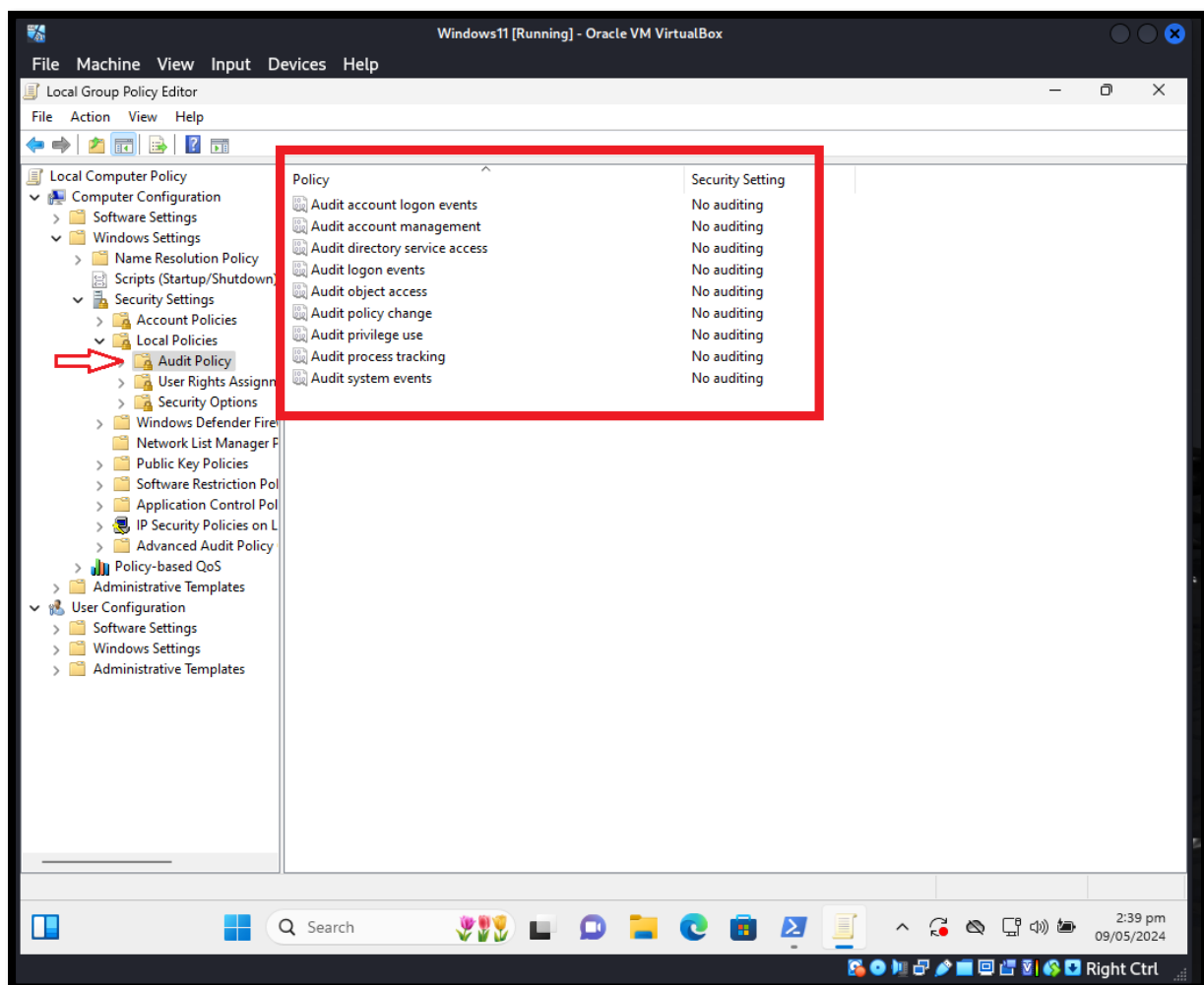
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.3-1.msi -OutFile ${env:tmp}\wazuh-agent; msixexec.exe /i ${env:tmp}\wazuh-agent /q WAZUH_MANAGER='192.168.100.50' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='Windows11' WAZUH_REGISTRATION_SERVER='192.168.100.50'

PS C:\Windows\system32> NET START WazuhSvc
The wazuh service is starting.
The wazuh service was started successfully.

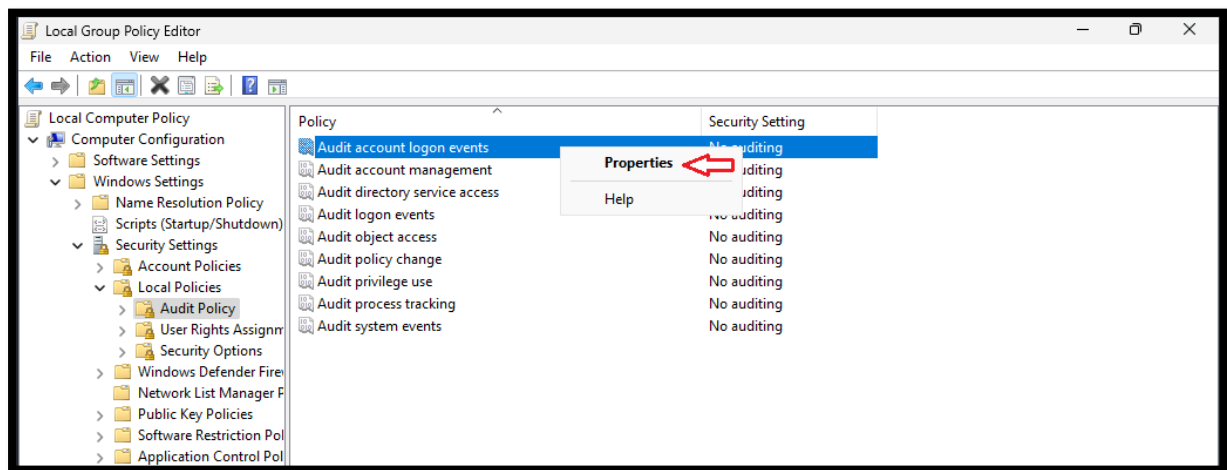
PS C:\Windows\system32>
```

Step 02: Now we have to Enable Windows security logs from “Local Group Policy” select “Windows Setting” > “Local Policy” > Audit Policy. By default windows Audit logs is not configured.

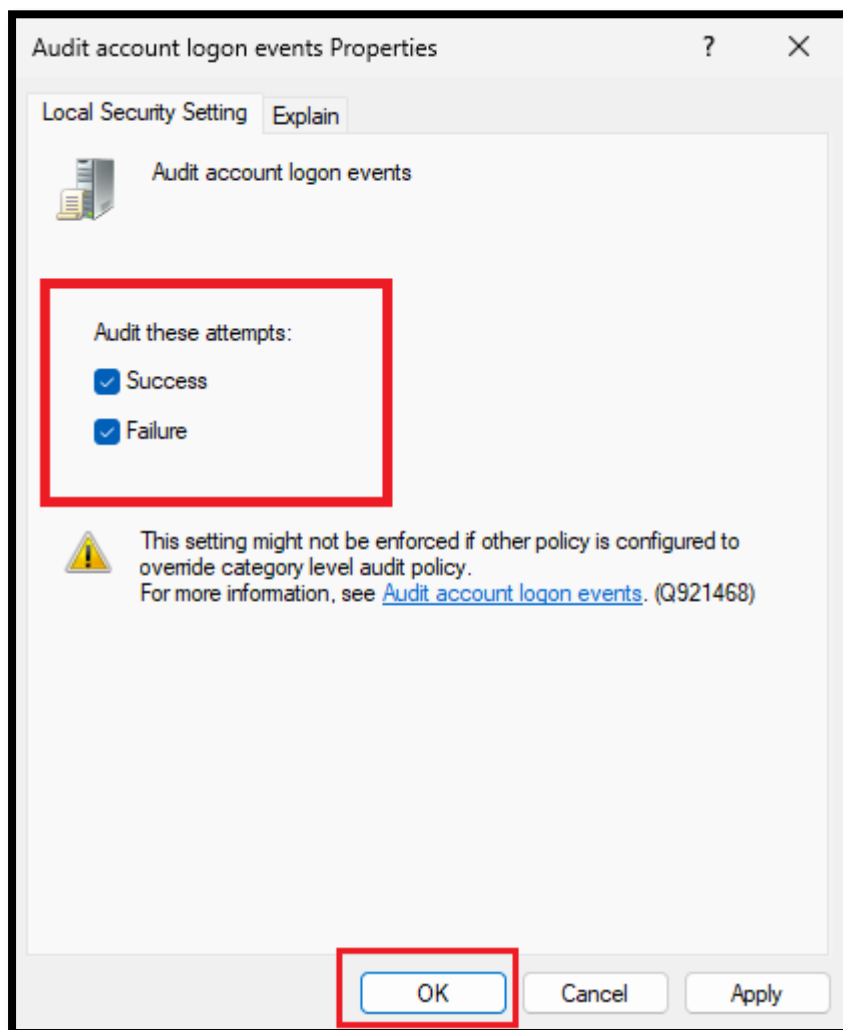




Now we have to configure Audit logs. Right click on “Properties” .












Click on check box “Success and Failure” then click Ok button.

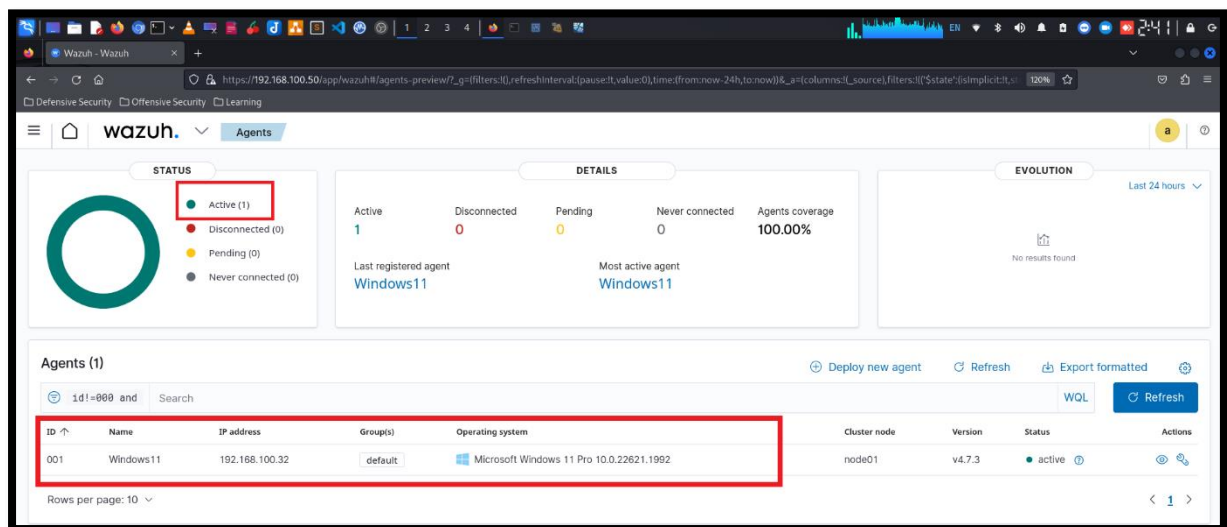


Apply same on all.

Note: For getting windows security logs in Wazuh Server we must have to enable all these Audit policies.

Policy	
 Audit account logon events	Success, Failure
 Audit account management	No auditing
 Audit directory service access	No auditing
 Audit logon events	Success, Failure
 Audit object access	No auditing
 Audit policy change	No auditing
 Audit privilege use	Success, Failure
 Audit process tracking	No auditing
 Audit system events	Success, Failure

Here you can see “Active agent” and Windows11 is present in Agent list.



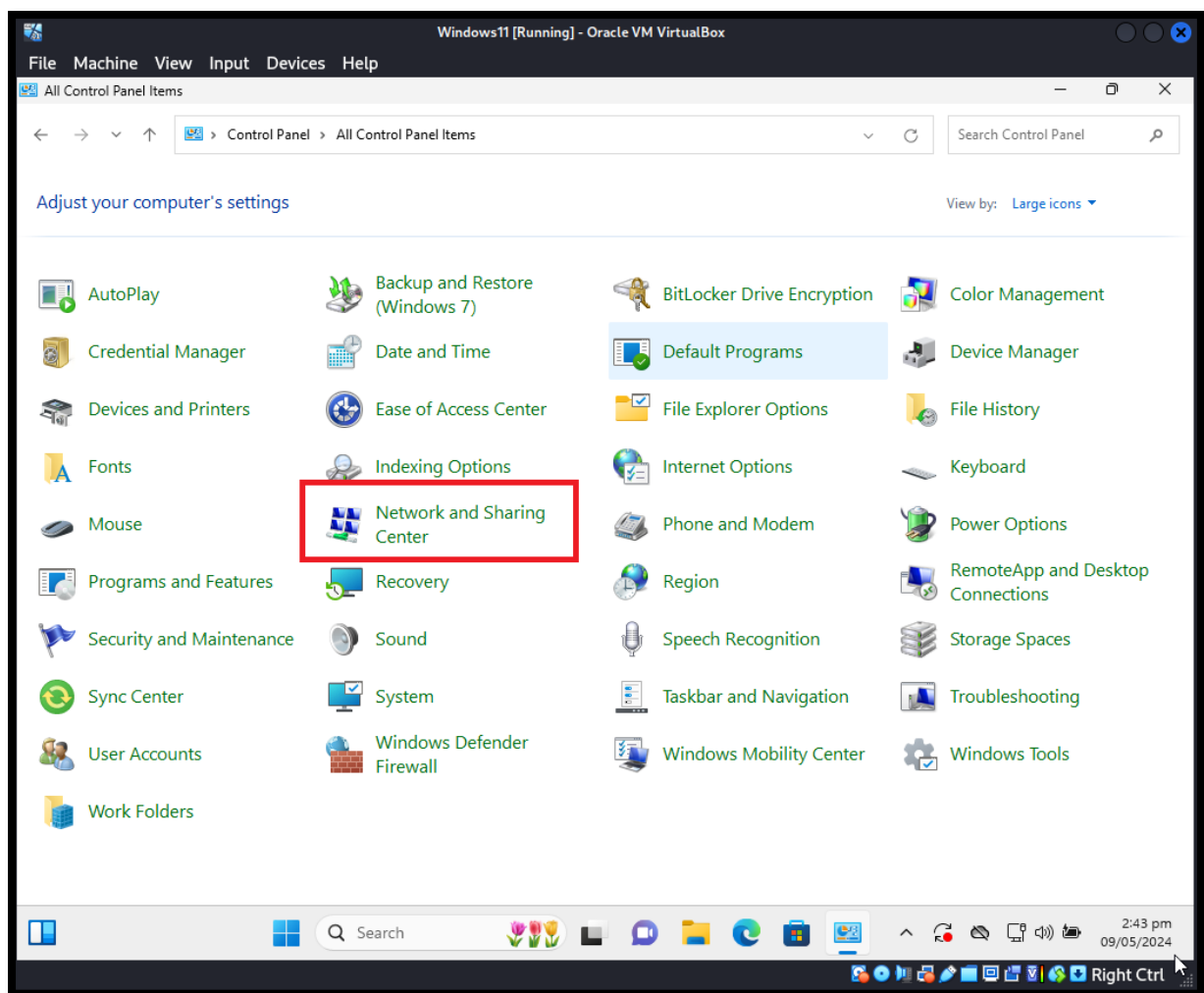
## Additional Configuration:

Step 03: We have to configure static IP Address to windows agent.

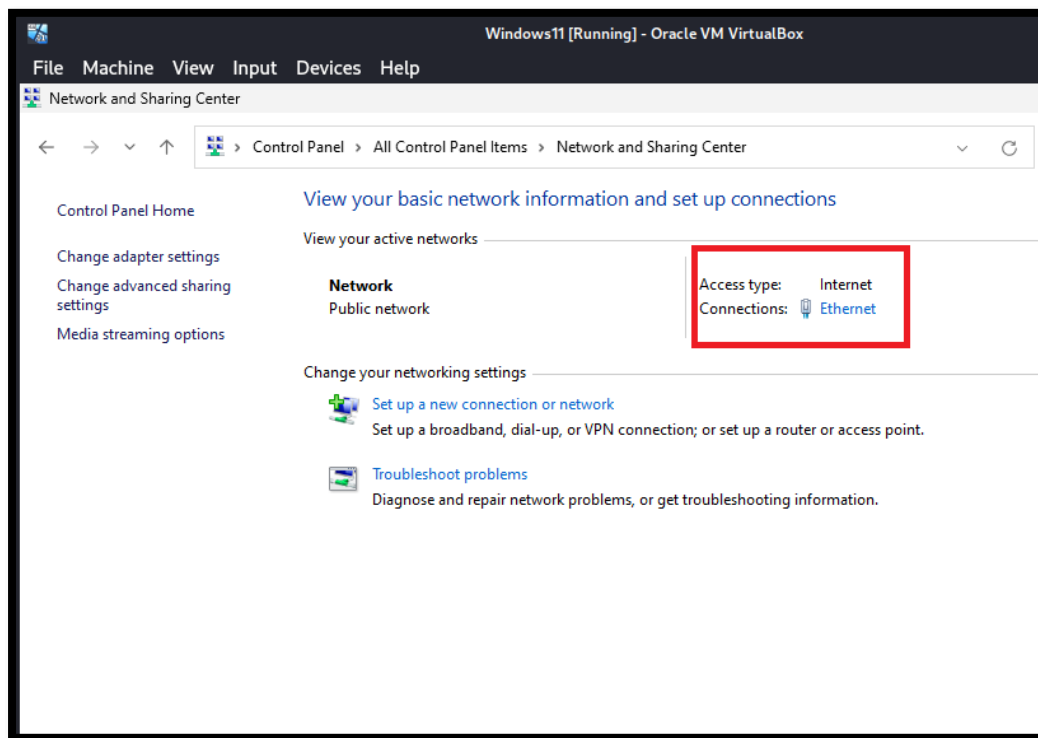
Note: This is very helpful when Wazuh Server or Wazuh Agent both has Static IP Address. Because if you know networking things DHCP Server will change the IP address when lease time expire. So, preventing form this change we have to assign static IP Address.

Follow these steps:

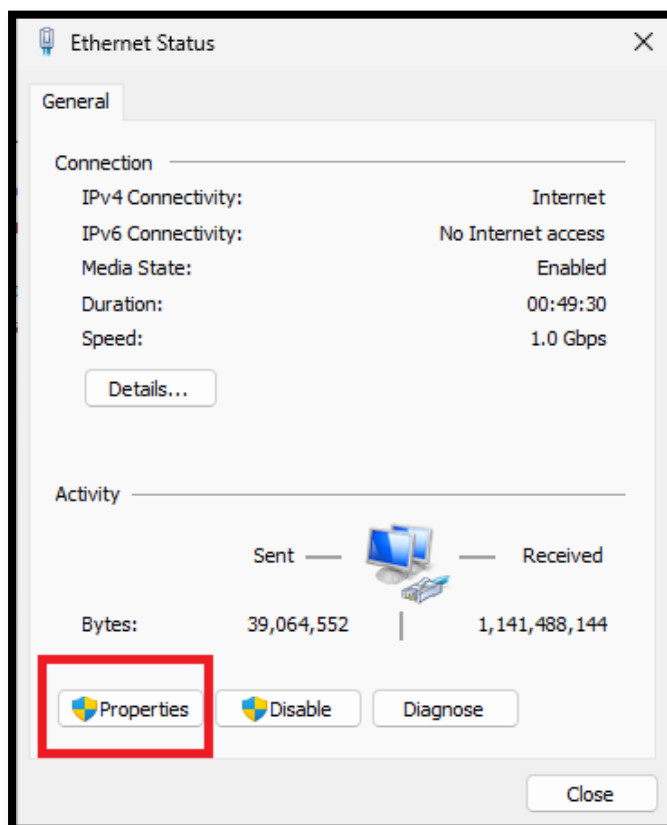
Open Control Panel and select “Network and Sharing Center”



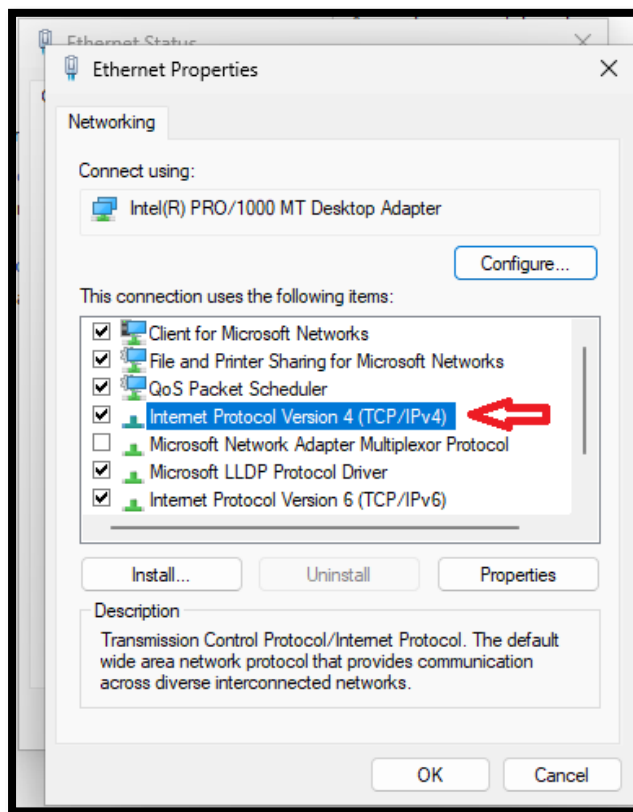
Now click on Connection: Ethernet, if you are using wireless connection then select wireless connection.



Ethernet Status wizard is open now click on “Properties”



When Ethernet Properties is open, Select "Internet Protocol Version 4 (TCP/IPv4)" and double click on it.



Before going further check the current IP Address of you windows.

```
C:\> Command Prompt
Microsoft Windows [Version 10.0.22621.1992]
(c) Microsoft Corporation. All rights reserved.

C:\Users\windows11>ipconfig ←

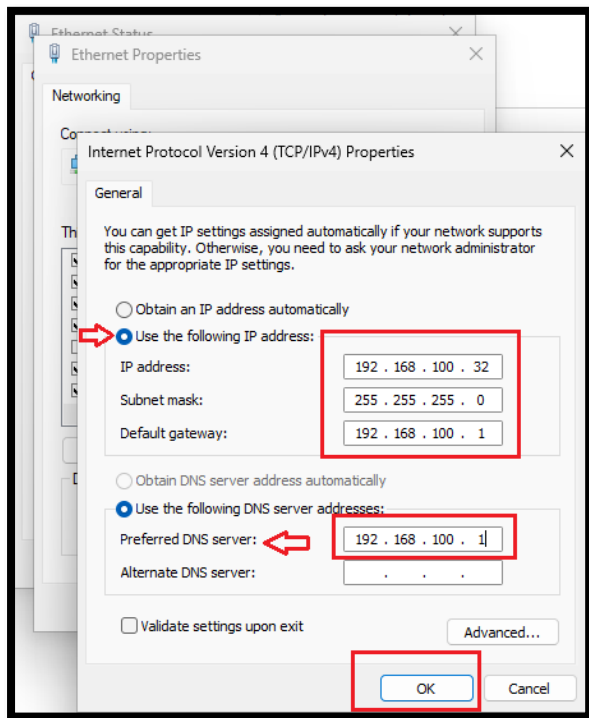
Windows IP Configuration

Ethernet adapter Ethernet:

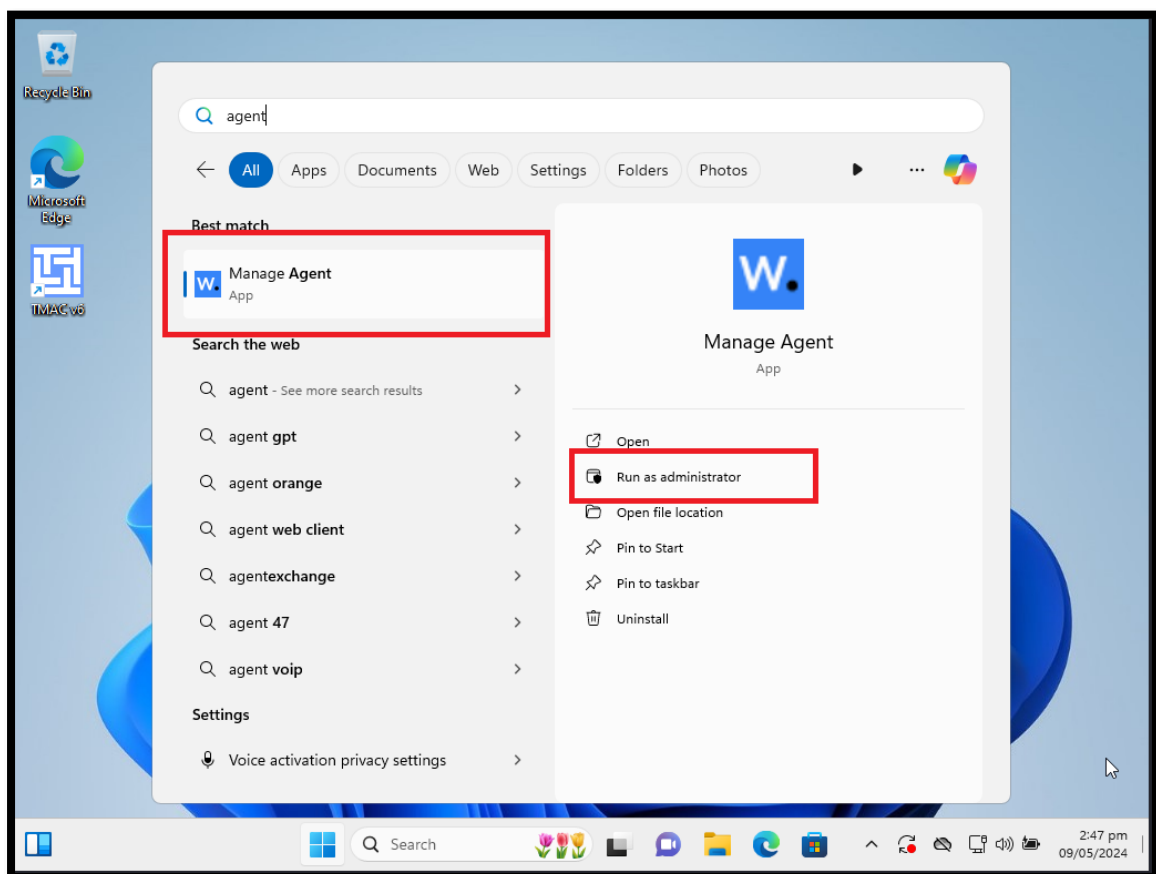
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::c66:a3df:57ce:6337%7
    IPv4 Address. . . . . : 192.168.100.32
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1%7
                                192.168.100.1

C:\Users\windows11>
```

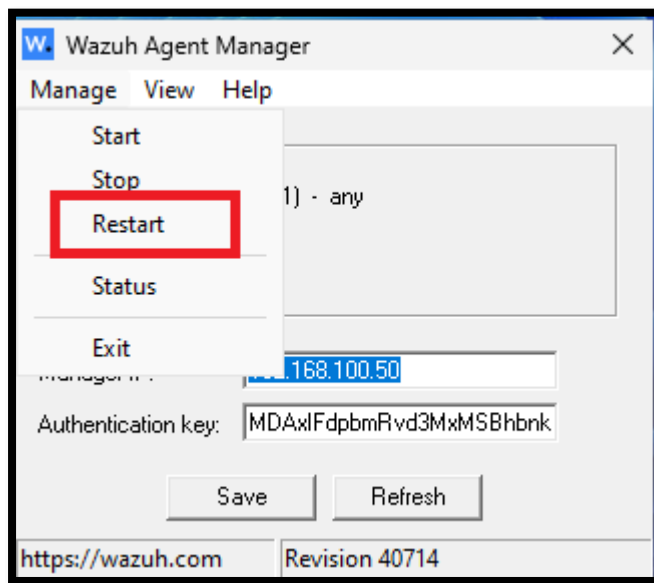
Now Enter the IP setting same as shown in picture, but remember the subnet-mask and default gateway and DNS. It will be different in your LAN.



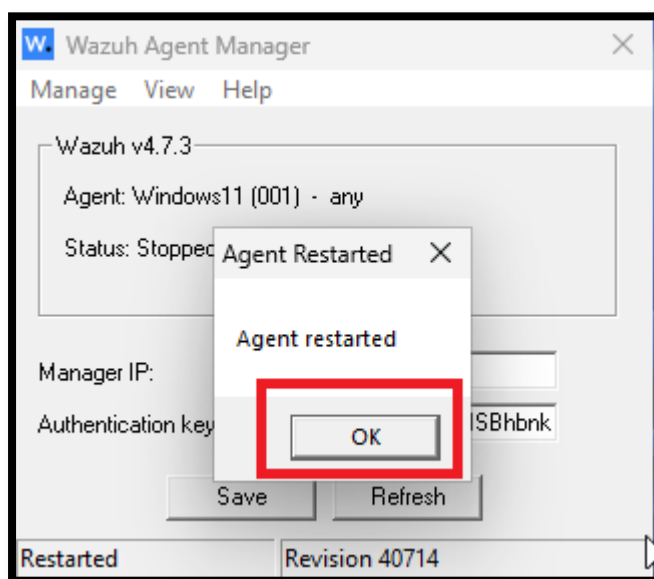
Now we have to restart Wazuh agent. Follow same as shown.



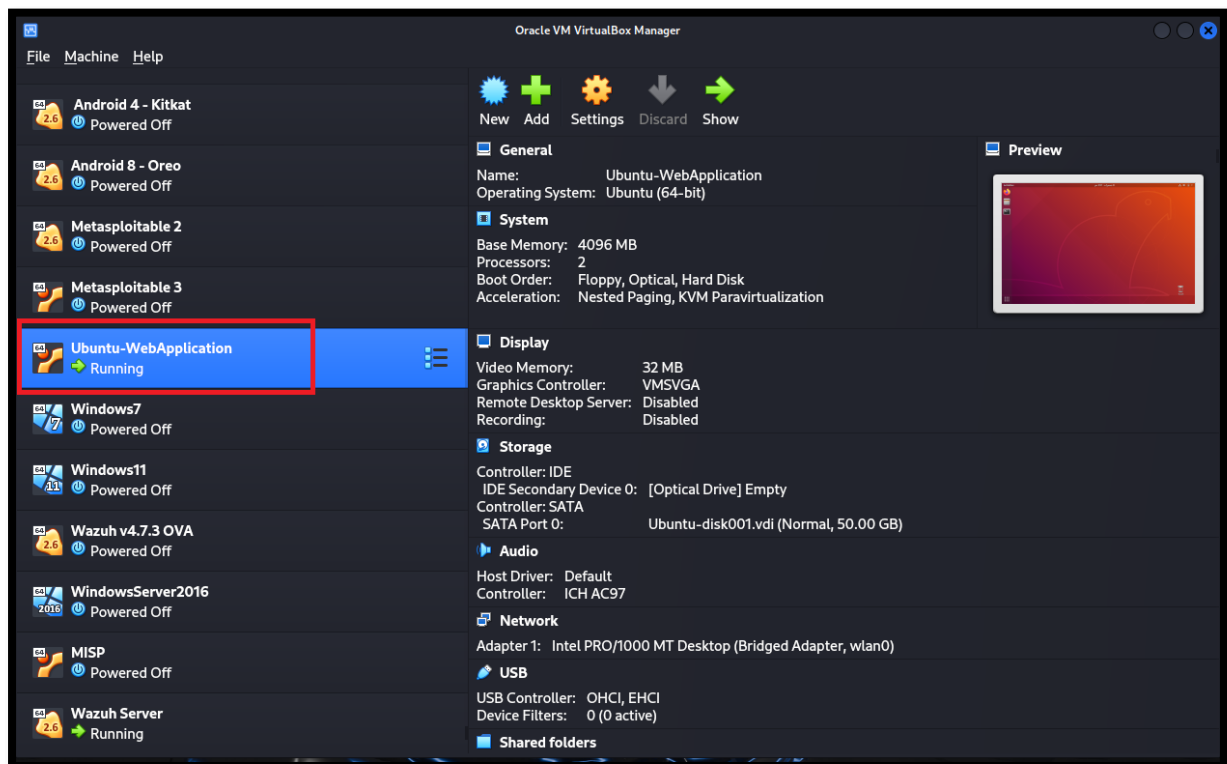
Restart Wazuh-agent.



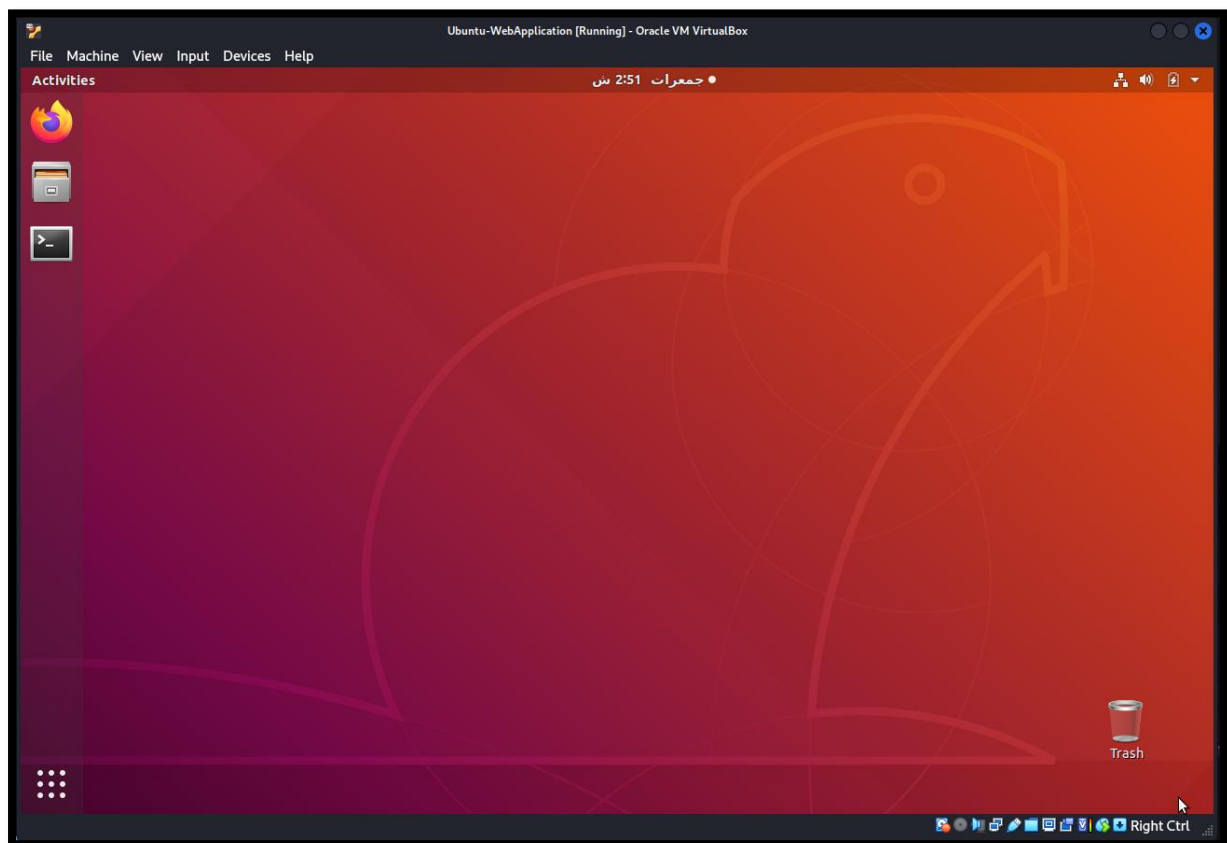
Wazuh-agent is restarted.



Step 04: Now installing Wazuh Agent in Linux (Ubuntu) Machine.



Running Ubuntu Machine.






Check the IP Address of Ubuntu with the command: “ifconfig”


```
ubuntu-victim@ubuntuvictim: ~  
File Edit View Search Terminal Help  
ubuntu-victim@ubuntuvictim:~$ ifconfig  
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.100.26 netmask 255.255.255.0 broadcast 192.168.100.255  
    inet6 fe80::45d:86e7:b35d:f8d prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:71:32:d0 txqueuelen 1000 (Ethernet)  
    RX packets 3612 bytes 5000342 (5.0 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 2114 bytes 216040 (216.0 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 152 bytes 32419 (32.4 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 152 bytes 32419 (32.4 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
ubuntu-victim@ubuntuvictim:~$
```


Go to deploy new agent wizard again and select LINUX, I am selecting DEB amd64. You can select according to your architecture.

### Deploy new agent

✓ Select the package to download and install on your system:

 **LINUX**  
  
☐ RPM amd64 ☐ RPM aarch64  
☒ DEB amd64 ☐ DEB aarch64

 **WINDOWS**  
  
☐ MSI 32/64 bits

 **macOS**  
  
☐ Intel  
☐ Apple silicon

① For additional systems and architectures, please check our [documentation](#).

✓ Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FDQN).

Assign a server address: ②

Follow the same setting as shown.

**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:** ?

Ubuntu

① The agent name must be unique. It can't be changed once the agent has been enrolled. [?](#)

**Select one or more existing groups:** ?

Default

Copy the download and install agent command and paste it in to ubuntu machine terminal.

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

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.3-1_amd64.deb &&
sudo WAZUH_MANAGER='192.168.100.50' WAZUH_AGENT_NAME='Ubuntu' dpkg -i ./wazuh-agent_4.7.3-1_amd64.deb
```

① **Requirements**

- You will need administrator privileges to perform this installation.
- Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.

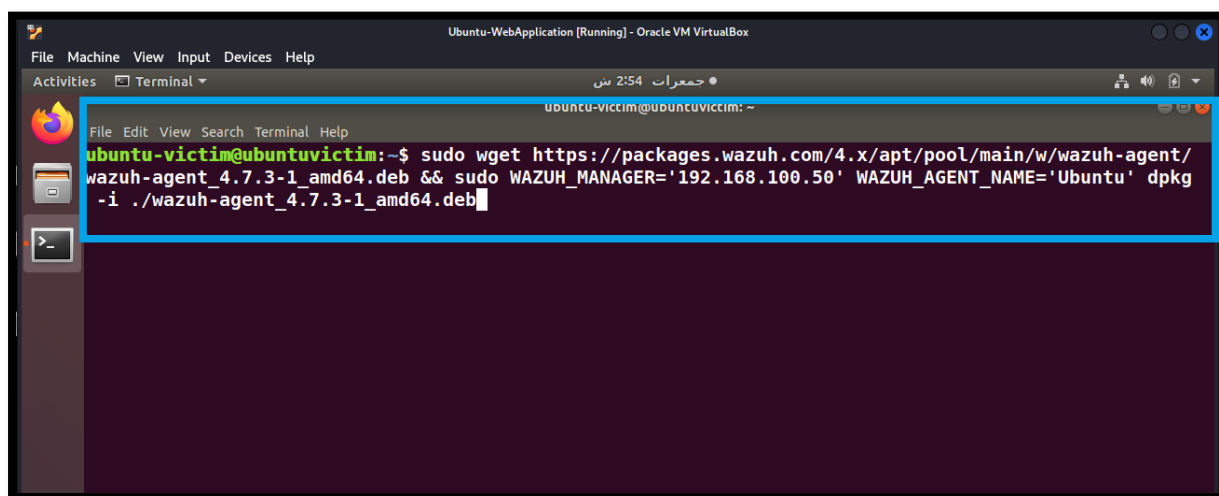
**5 Start the agent:**

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

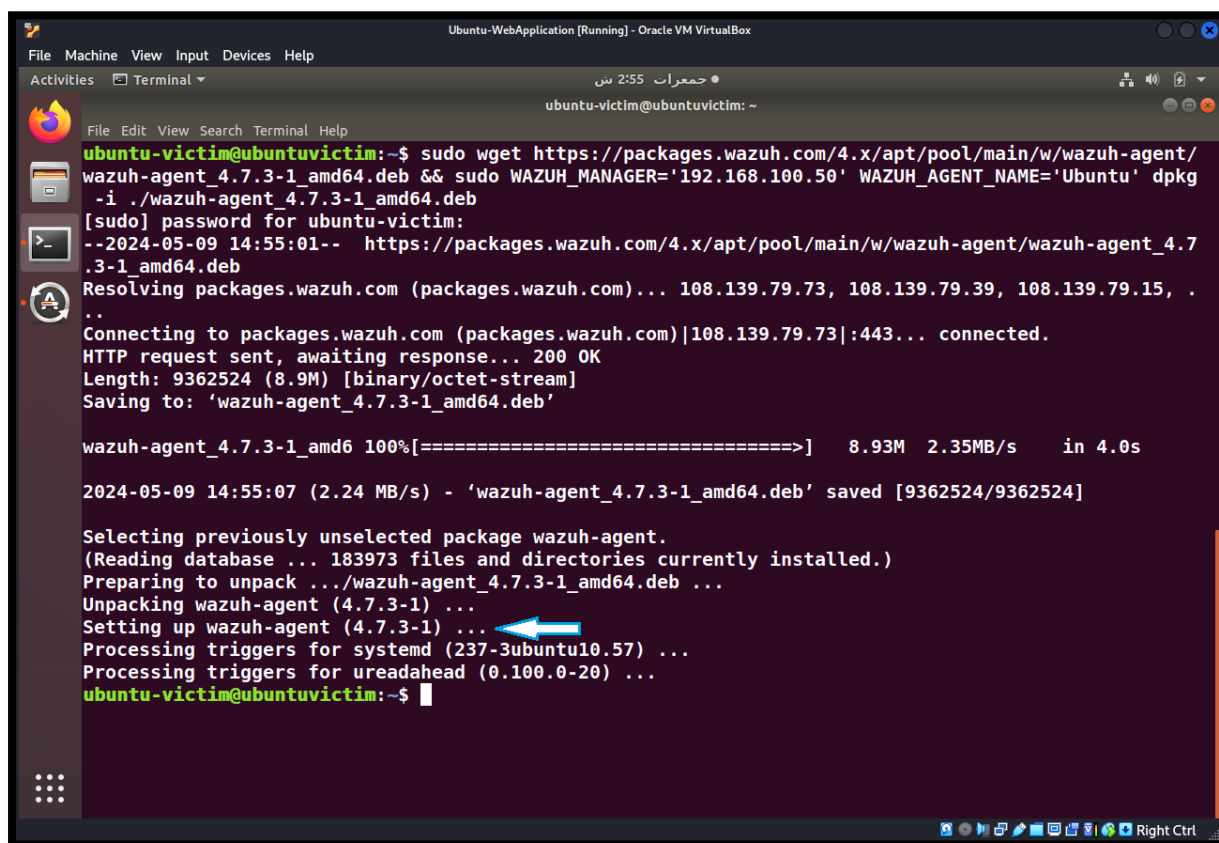
Close

Here is you can see “Start the agent” after install Wazuh agent enter these commands as shown in figure.

Paste the command with sudo rights.

A terminal window titled 'Ubuntu-WebApplication [Running] - Oracle VM VirtualBox'. The terminal shows the command: `ubuntu-victim@ubuntuvictim:~$ sudo wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.3-1_amd64.deb && sudo WAZUH_MANAGER='192.168.100.50' WAZUH_AGENT_NAME='Ubuntu' dpkg -i ./wazuh-agent_4.7.3-1_amd64.deb`. The command is highlighted with a blue box.

Wazuh-Agent is installed on Ubuntu.

A terminal window showing the output of the installation command. It includes the download progress, file saving, and the dpkg command output. The output shows that the package is being unpacked and configured. A blue arrow points to the line 'Setting up wazuh-agent (4.7.3-1) ...'.

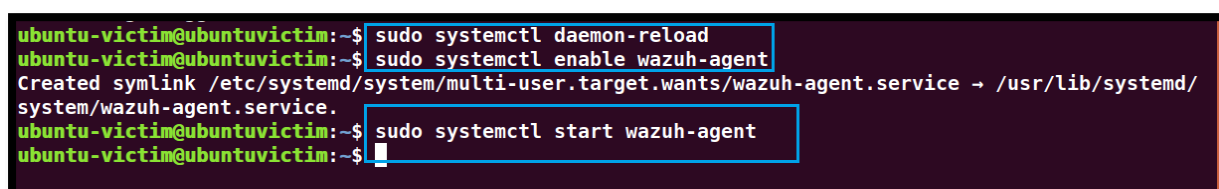
```
ubuntu-victim@ubuntuvictim:~$ sudo wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.3-1_amd64.deb && sudo WAZUH_MANAGER='192.168.100.50' WAZUH_AGENT_NAME='Ubuntu' dpkg -i ./wazuh-agent_4.7.3-1_amd64.deb
[sudo] password for ubuntu-victim:
--2024-05-09 14:55:01-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.3-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 108.139.79.73, 108.139.79.39, 108.139.79.15, .
.
Connecting to packages.wazuh.com (packages.wazuh.com)|108.139.79.73|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9362524 (8.9M) [binary/octet-stream]
Saving to: 'wazuh-agent_4.7.3-1_amd64.deb'

wazuh-agent_4.7.3-1_amd64 100%[=====] 8.93M 2.35MB/s in 4.0s

2024-05-09 14:55:07 (2.24 MB/s) - 'wazuh-agent_4.7.3-1_amd64.deb' saved [9362524/9362524]

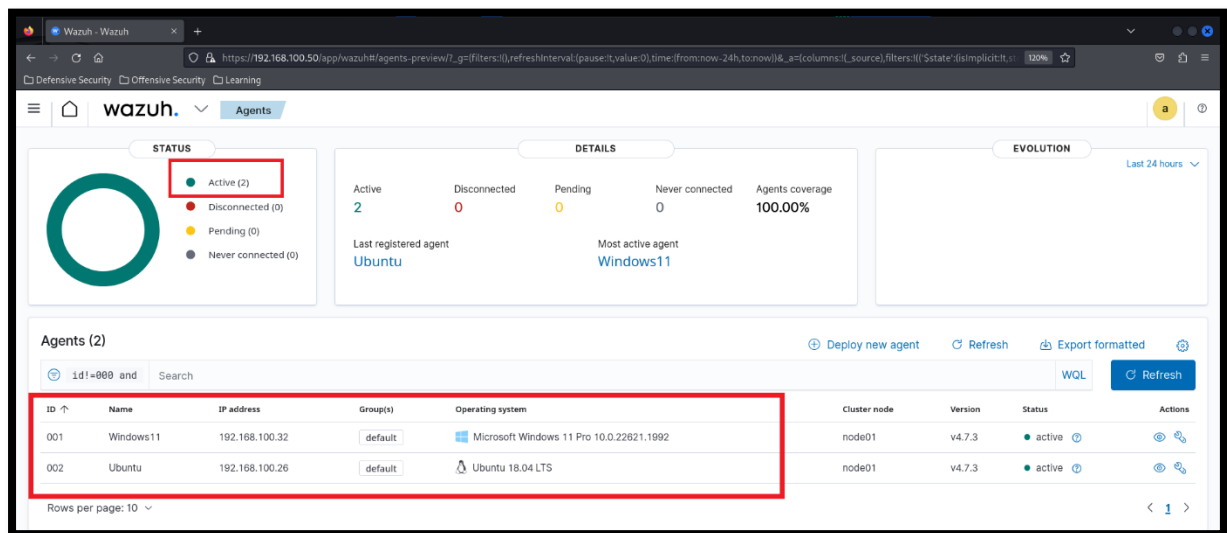
Selecting previously unselected package wazuh-agent.
(Reading database ... 183973 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.7.3-1_amd64.deb ...
Unpacking wazuh-agent (4.7.3-1) ...
Setting up wazuh-agent (4.7.3-1) ...
Processing triggers for systemd (237-3ubuntu10.57) ...
Processing triggers for ureadahead (0.100.0-20) ...
ubuntu-victim@ubuntuvictim:~$
```

After the installation of Wazuh-Agent, paste these commands.

A terminal window showing the commands to start Wazuh-Agent. The commands are: `sudo systemctl daemon-reload`, `sudo systemctl enable wazuh-agent`, and `sudo systemctl start wazuh-agent`. The first two commands are highlighted with blue boxes.

```
ubuntu-victim@ubuntuvictim:~$ sudo systemctl daemon-reload
ubuntu-victim@ubuntuvictim:~$ sudo systemctl enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /usr/lib/systemd/system/wazuh-agent.service.
ubuntu-victim@ubuntuvictim:~$ sudo systemctl start wazuh-agent
ubuntu-victim@ubuntuvictim:~$
```

Now open Wazuh Dashboard again and see there is Active Agents.



We successfully install Windows and Linux agents.

## SUMMARY

In summary, installing Wazuh agents helps organizations establish a proactive security posture, enabling them to detect, respond to, and mitigate security threats effectively, thereby safeguarding their assets, data, and reputation.