

## ⇒ Installing Wazuh Agents on Windows and Linux

### **Background:**

The Wazuh platform provides XDR and SIEM features to protect your cloud, container, and server workloads. These include log data analysis, intrusion and malware detection, file integrity monitoring, configuration assessment, vulnerability detection, and support for regulatory compliance.

The Wazuh solution is based on the Wazuh agent, which is deployed on the monitored endpoints, and on three central components: the Wazuh server, the Wazuh indexer, and the Wazuh dashboard.

The **Wazuh indexer** is a highly scalable, full-text search and analytics engine. This central component indexes and stores alerts generated by the Wazuh server.

The **Wazuh server** analyzes data received from the agents. It processes it through decoders and rules, using threat intelligence to look for well-known indicators of compromise (IOCs). A single server can analyze data from hundreds or thousands of agents, and scale horizontally when set up as a cluster. This central component is also used to manage the agents, configuring and upgrading them remotely when necessary.

The **Wazuh dashboard** is the web user interface for data visualization and analysis. It includes out-of-the-box dashboards for security events, regulatory compliance (e.g., PCI DSS, GDPR, CIS, HIPAA, NIST 800-53), detected vulnerable applications, file integrity monitoring data, configuration assessment results, cloud infrastructure monitoring events, and others. It is also used to manage Wazuh configuration and to monitor its status.

**Wazuh agents** are installed on endpoints such as laptops, desktops, servers, cloud instances, or virtual machines. They provide threat prevention, detection, and response capabilities. They run on operating systems such as Linux, Windows, macOS, Solaris, AIX, and HP-UX.

Today, we are going to install Wazuh agent

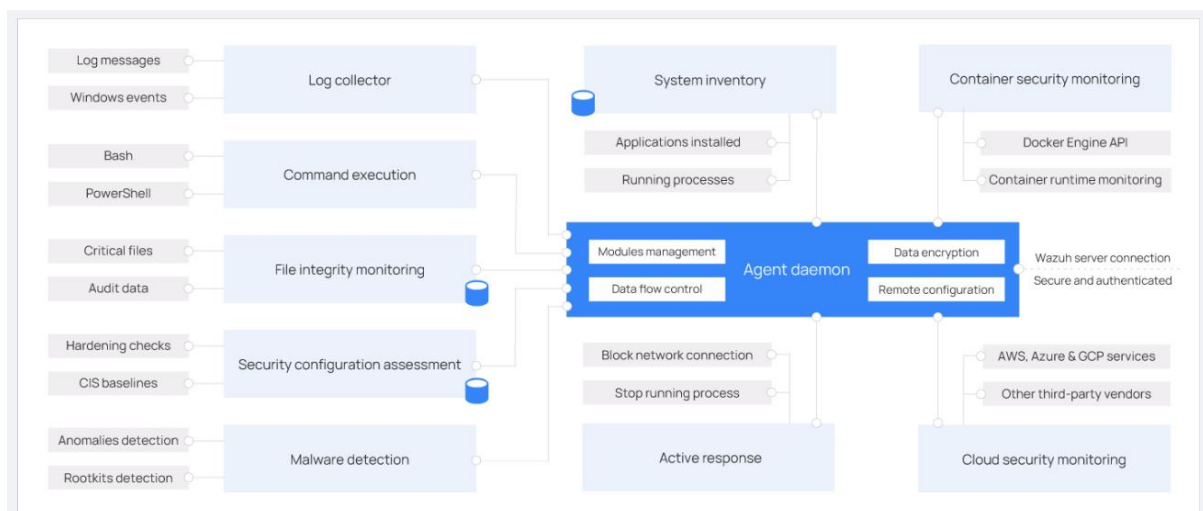
### **Wazuh agent**

The Wazuh agent is multi-platform and runs on the endpoints that the user wants to monitor. It communicates with the Wazuh server, sending data in near real-time through an encrypted and authenticated channel.

The agent was developed considering the need to monitor a wide variety of different endpoints without impacting their performance. It is supported on the most popular operating systems, and it requires 35 MB of RAM on average

The Wazuh agent runs on Linux, Windows, macOS, Solaris, AIX, and other operating systems. It can be deployed to laptops, desktops, servers, cloud instances, containers, or virtual machines. The agent helps to protect your system by providing threat prevention, detection, and response capabilities. It is also used to collect different types of system and application data that it forwards to the Wazuh server through an encrypted and authenticated channel.

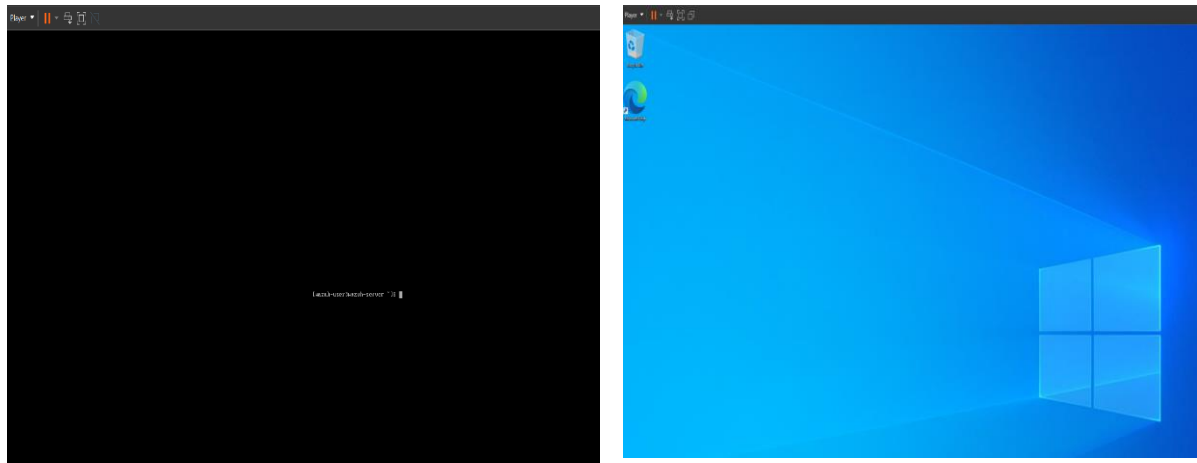
### **Architecture of Wazuh Agent**



## Installation Procedure:

First, we will try to install Wazuh agent in Windows and then in Linux ecosystem.

In my case, I have deployed windows 10 in VMware Workstation 17. I have launched both the Wazuh Environment and windows Environment or instances



Now, try to access the Wazuh dashboard from windows instance by pasting below URL in any browser

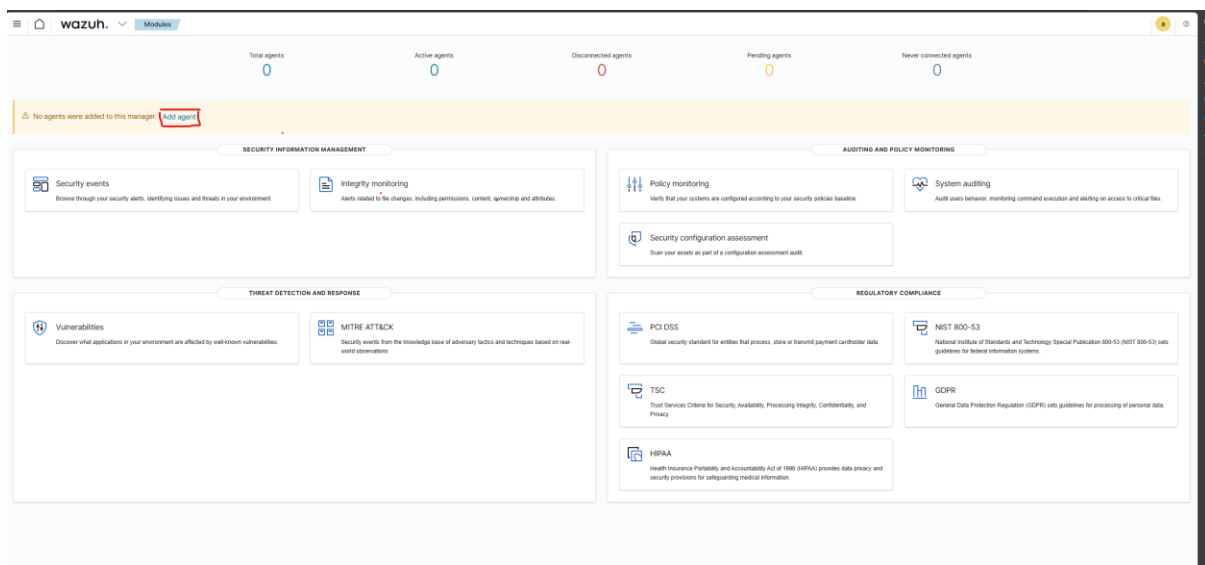
<https://wazuh-server-ip>

in my case

<https://192.168.198.126>

After pasting the URL in your Browser, you can see there are no active agents available.

Click on “Add Agent”, in order to add agent in windows instance.





Since, we are trying to install it in windows instance, choose windows


[Refresh](#)

## 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](#).

Next, Enter your Wazuh-server IP address, in my case its “192.168.198.126”

✓ **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:** [?](#)

Next, you can give any name to your agent and choose option as “default”

✓ **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:** [?](#)

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

**Select one or more existing groups:** [?](#)

✕ ✓

Next, copy the below command to download and install the agent in windows instance.



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

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi -OutFile  
${env.tmp}\wazuh-agent; msixec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='192.168.198.126'  
WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='windowsAgent'  
WAZUH_REGISTRATION_SERVER='192.168.198.126'
```

#### ① 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.

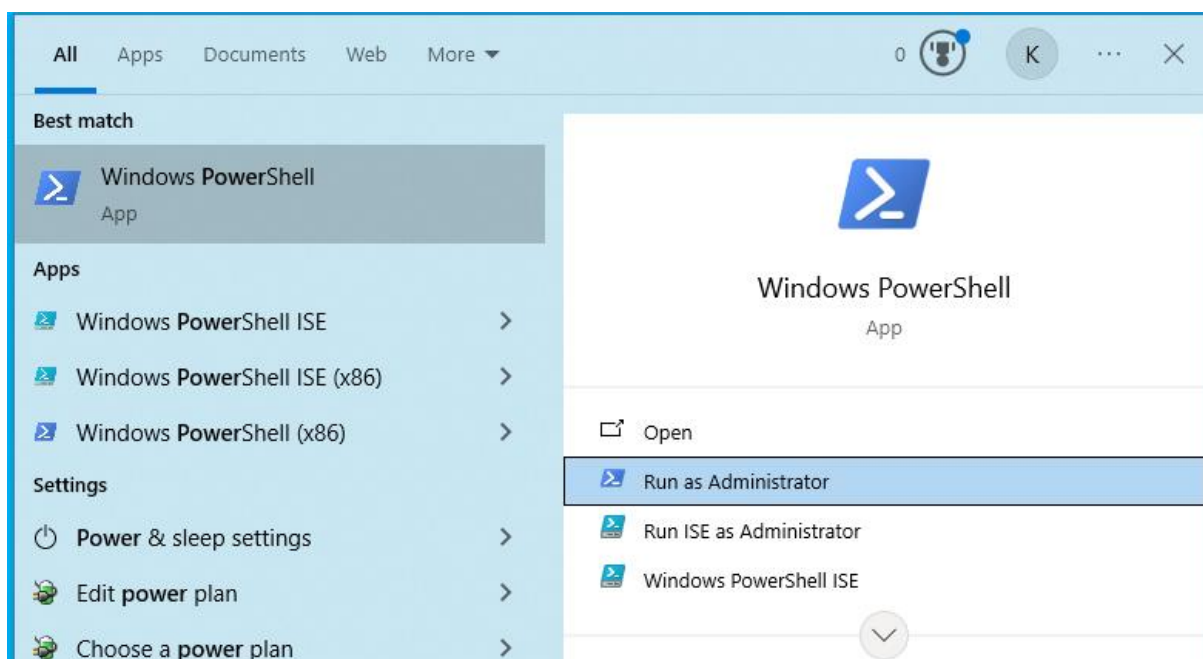
**5**

**Start the agent:**

```
NET START WazuhSvc
```

Note:

You have to paste this command in “PowerShell” which should run with administrative privileges



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

Writing web request
Writing request stream... (Number of bytes written: 1064980)

PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi -OutFile $env:tmp\wazuh-agent; msexec.exe /s $env:tmp\wazuh-agent /q WAZUH_MANAGER=192.168.158.119 WAZUH_AGENT_GROUP="default" WAZUH_AGENT_NAME="WindowsAgent" WAZUH_REGISTRATION_SERVER=192.168.158.119
```

Thus, Wazuh agent is successfully installed in your windows instance, now to run your agent

Command: NET START wazuuhSvc

```
PS C:\Windows\system32> NET START wazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\Windows\system32>
```

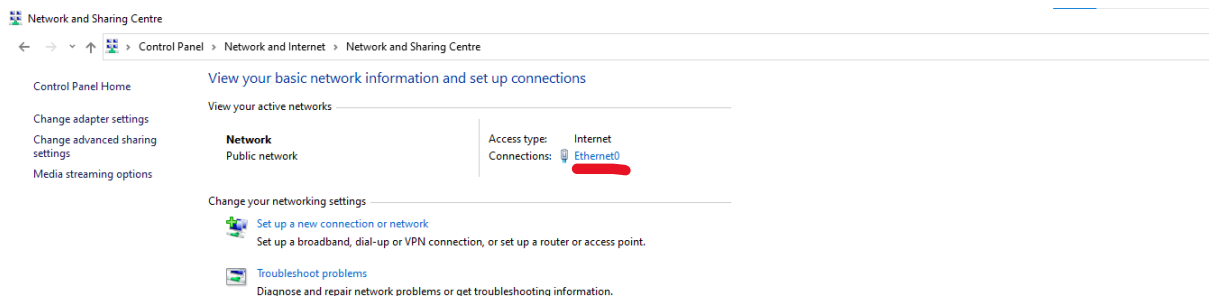
Thus, your Wazuh agent is alive.

### **Optional:**

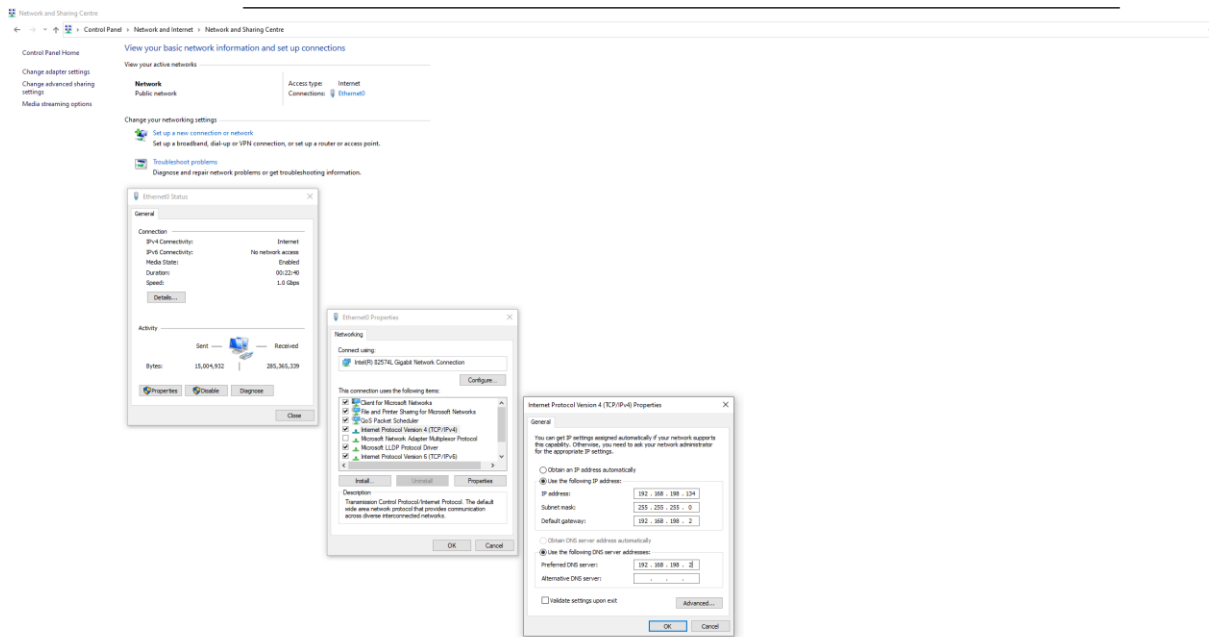
In order to convert your Windows IP address into static IP

Workflow →

Control Panel → Network and Internet → Network and Sharing Centre → click on Ethernet0



Properties → double click on “Internet protocol Version 4(TCP/IPv4)” → select “Use the following IP address”



In order to know your exact subnet mask and default path way,

Go to your command prompt

Cmd: ipconfig

```
C:\Users\kusha>ipconfig

Windows IP Configuration

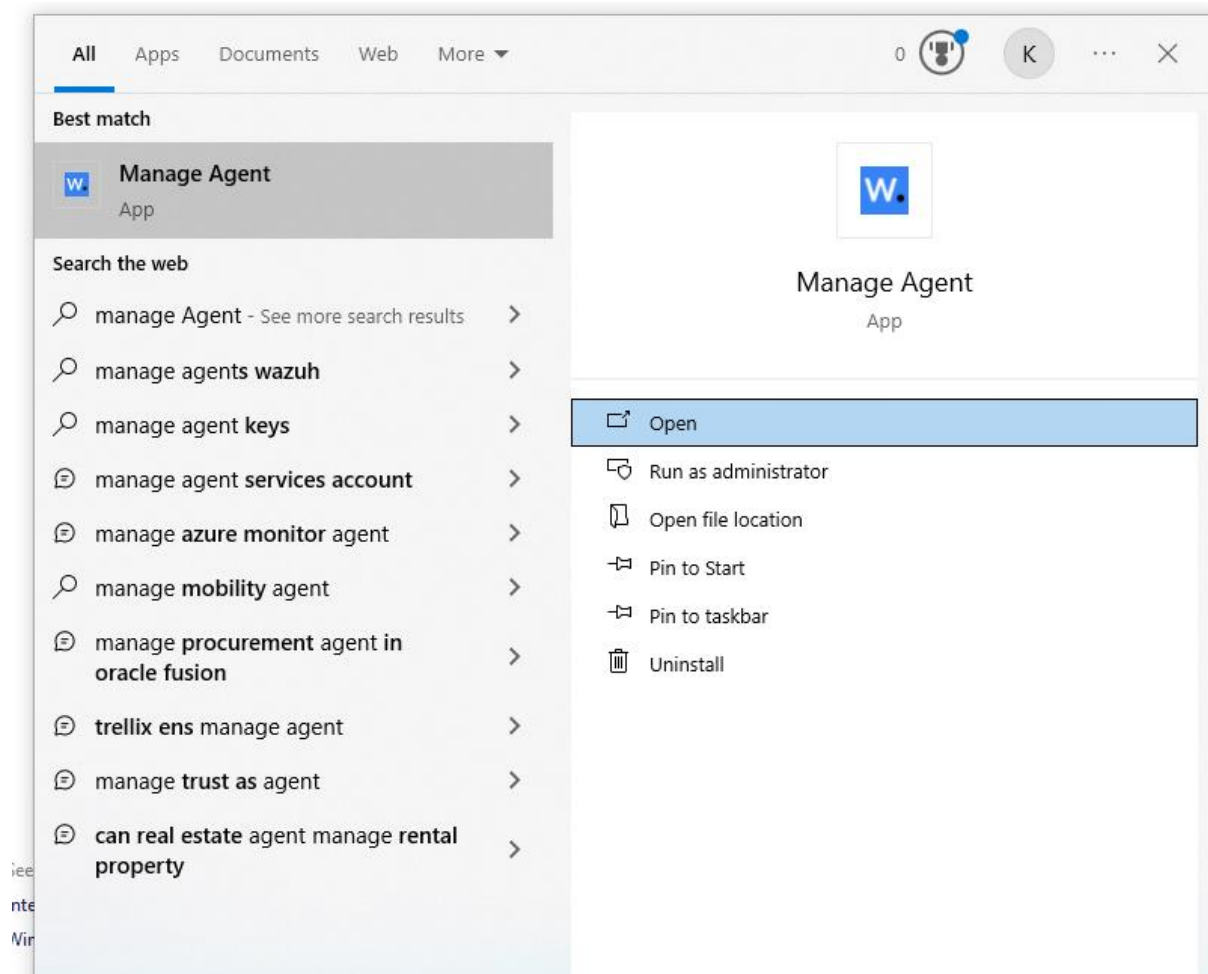
Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::7c9d:652a:fac1:9fe8%6
    IPv4 Address. . . . . : 192.168.198.134
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.198.2

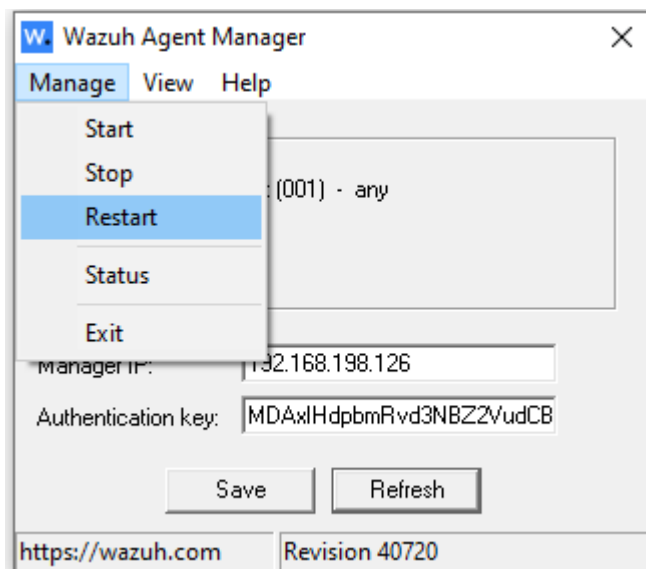
C:\Users\kusha>
```

Now, after assigning your static ip address, your need to restart your service

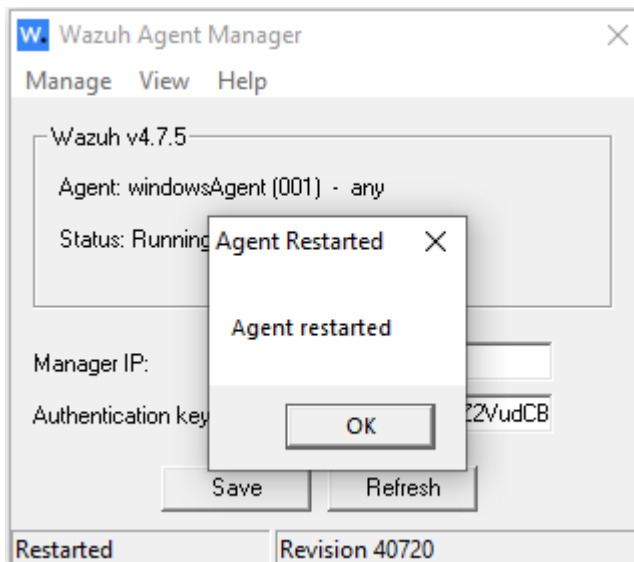
For that, search for “Manage Agent” from your search bar.



Click on Manage → restart

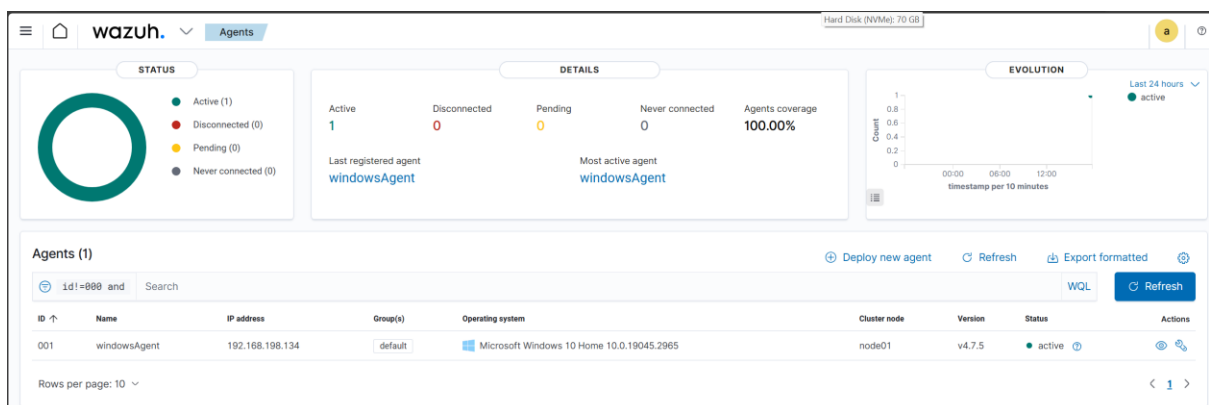






Now, try to open your Wazuh dashboard, you can see that you have successfully added Wazuh agent.

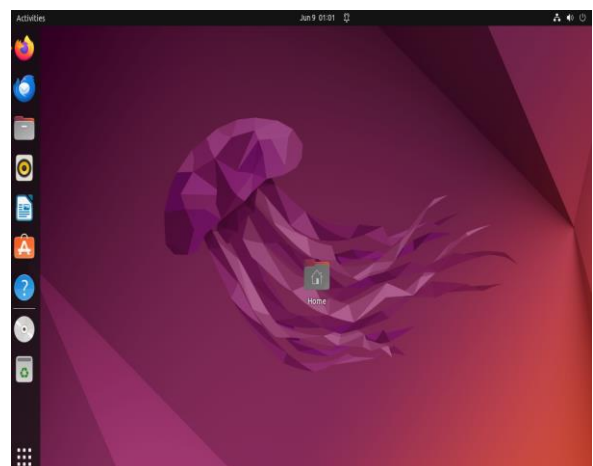
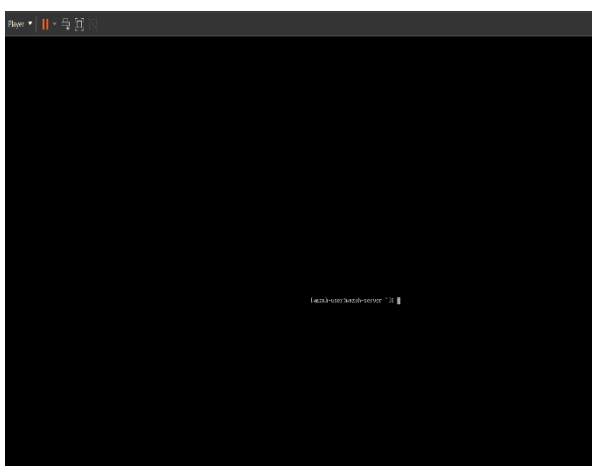
It shows, number of active agents as “1”



Case 02:

For adding Linux agent in Linux instance

In this case I got my Wazuh and Linux instances up and running.



```

project-01@project01-virtual-machine:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.198.133 netmask 255.255.255.0 broadcast 192.168.198.255
    inet6 fe80::62e1:ecd5:8b1f:f662 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:bf:c6:7a txqueuelen 1000 (Ethernet)
    RX packets 1021 bytes 1296275 (1.2 MB)
    RX errors 1 dropped 1 overruns 0 frame 0
    TX packets 697 bytes 47569 (47.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

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 142 bytes 12828 (12.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 142 bytes 12828 (12.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

project-01@project01-virtual-machine:~$

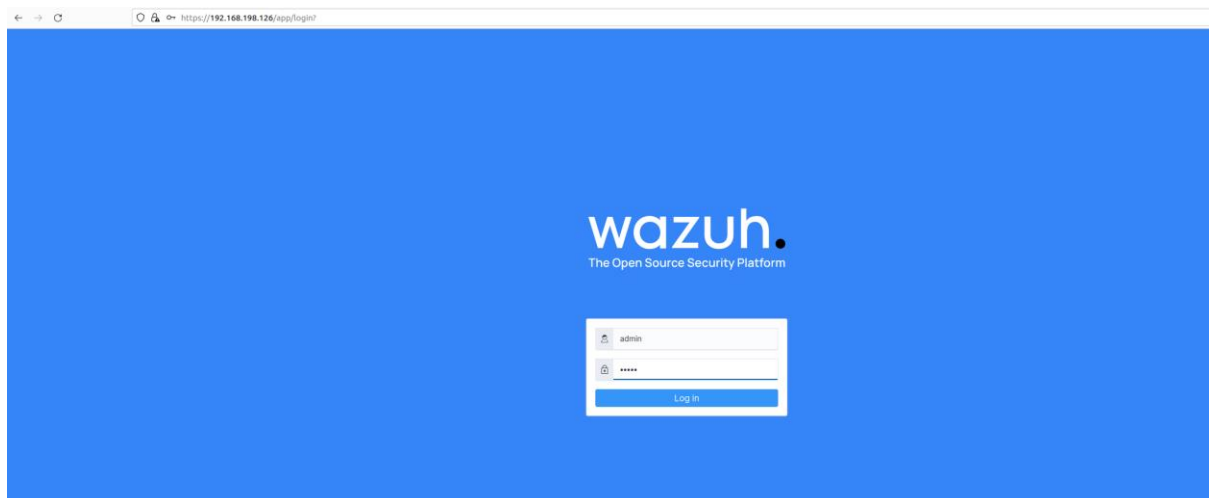
```

Now, try to open your Wazuh dashboard in your Linux Environment by using any Browser

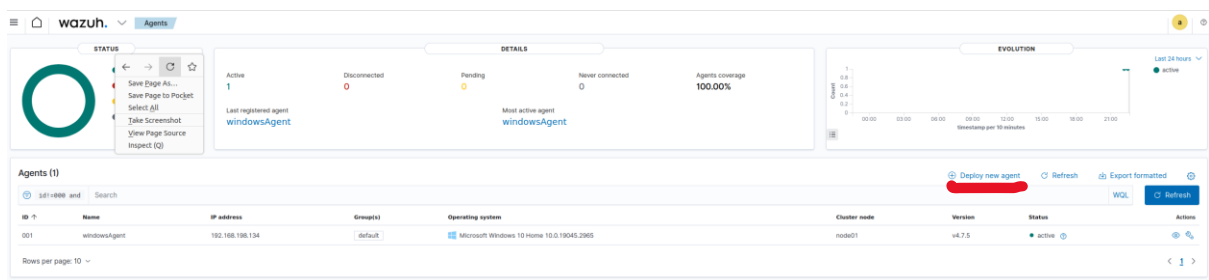
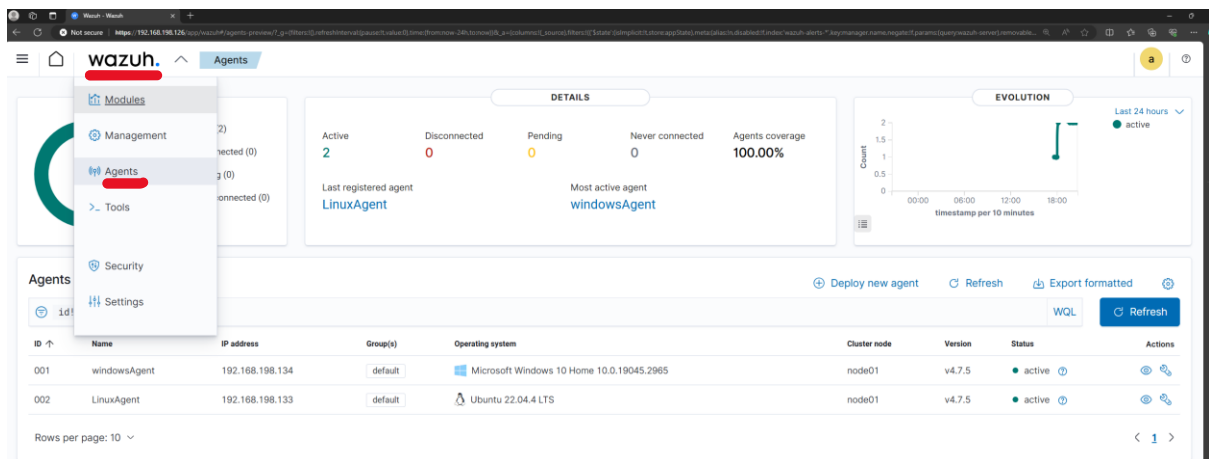
<https://Wazuh-server-IP>

in my case its


<https://192.168.198.126>




Follow the same procedure, again click on “Deploy new Agent” and follow the instruction based on the screenshots given




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

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

#### 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_4.7.5-1_amd64.deb &&
sudo WAZUH_MANAGER='192.168.198.126' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='linuxAgent' dpkg
-i ./wazuh-agent_4.7.5-1_amd64.deb
```

##### ④ 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
```

Now, copy paste the command which is given in 4<sup>th</sup> step in root privilege mode

```
project-01@project01-virtual-machine:~$ sudo su
root@project01-virtual-machine:/home/project-01# wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.5-1_amd64.deb && sudo WAZUH_MANAGER=
'192.168.198.126' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='linuxAgent' dpkg -i ./wazuh-agent_4.7.5-1_amd64.deb
--2024-06-08 22:35:30-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.5-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 54.240.162.122, 54.240.162.98, 54.240.162.62, ...
Connecting to packages.wazuh.com (packages.wazuh.com)[54.240.162.122]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9378818 (8.9M) [binary/octet-stream]
Saving to: 'wazuh-agent_4.7.5-1_amd64.deb'

wazuh-agent_4.7.5-1_amd64.deb      100%[=====] 8.94M  836KB/s   in 10s

2024-06-08 22:35:41 (883 KB/s) - 'wazuh-agent_4.7.5-1_amd64.deb' saved [9378818/9378818]

Selecting previously unselected package wazuh-agent.
(Reading database ... 199508 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.7.5-1_amd64.deb ...
Unpacking wazuh-agent (4.7.5-1) ...
Setting up wazuh-agent (4.7.5-1) ...
```

After successful installation of Wazuh-agent in Linux Environment, try to reload the and start the agent by following the commands given

Commands:

```
sudo systemctl daemon-reload
```

```
sudo systemctl enable Wazuh-agent
```

```
sudo systemctl start Wazuh-agent
```

```
root@project01-virtual-machine:/home/project-01# sudo systemctl daemon-reload
root@project01-virtual-machine:/home/project-01# sudo systemctl enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /lib/systemd/system/wazuh-agent.service.
root@project01-virtual-machine:/home/project-01# sudo systemctl start wazuh-agent
root@project01-virtual-machine:/home/project-01#
```

Now you can check the status of your Wazuh agent by following the given command

Command:

sudo systemctl status Wazuh-agent

```
root@project01-virtual-machine:/home/project-01# sudo systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
   Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2024-06-08 22:37:03 IST; 26s ago
     Process: 5039 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
    Tasks: 32 (limit: 4554)
   Memory: 401.5M
      CPU: 18.454s
   CGroup: /system.slice/wazuh-agent.service
           └─5649 /var/ossec/bin/wazuh-execd
             └─5659 /var/ossec/bin/wazuh-agentd
               └─5673 /var/ossec/bin/wazuh-syscheckd
                 └─5683 /var/ossec/bin/wazuh-logcollector
                   └─5701 /var/ossec/bin/wazuh-modulesd
                     └─6015 systemctl status cron

Jun 08 22:36:56 project01-virtual-machine systemd[1]: Starting Wazuh agent...
Jun 08 22:36:56 project01-virtual-machine env[5039]: Starting Wazuh v4.7.5...
Jun 08 22:36:57 project01-virtual-machine env[5039]: Started wazuh-execd...
Jun 08 22:36:58 project01-virtual-machine env[5039]: Started wazuh-agentd...
Jun 08 22:36:58 project01-virtual-machine env[5039]: Started wazuh-syscheckd...
Jun 08 22:36:59 project01-virtual-machine env[5039]: Started wazuh-logcollector...
Jun 08 22:37:00 project01-virtual-machine env[5039]: Started wazuh-modulesd...
Jun 08 22:37:02 project01-virtual-machine env[5039]: Completed.
Jun 08 22:37:03 project01-virtual-machine systemd[1]: Started Wazuh agent.
```

Now, you check that there are totally two agents being added(Windows and Linux agents)

The screenshot shows the Wazuh dashboard interface. At the top, there are statistics for agents: Total agents (2), Active agents (2), Disconnected agents (0), Pending agents (0), and Never connected agents (0). The dashboard is divided into several sections: SECURITY INFORMATION MANAGEMENT (Security events, Integrity monitoring), AUDITING AND POLICY MONITORING (Policy monitoring, System auditing, Security configuration assessment), THREAT DETECTION AND RESPONSE (Vulnerabilities, MITRE ATT&CK), and REGULATORY COMPLIANCE (PCI DSS, NIST 800-53, TSC, GDPR, HIPAA). Below the dashboard, there is a table titled 'Agents (2)' showing the details of the two active agents.

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	windowsAgent	192.168.198.134	default	Microsoft Windows 10 Home 10.0.19045.2965	node01	v4.7.5	active	<a href="#">View</a> <a href="#">Refresh</a>
002	LinuxAgent	192.168.198.133	default	Ubuntu 22.04.4 LTS	node01	v4.7.5	active	<a href="#">View</a> <a href="#">Refresh</a>