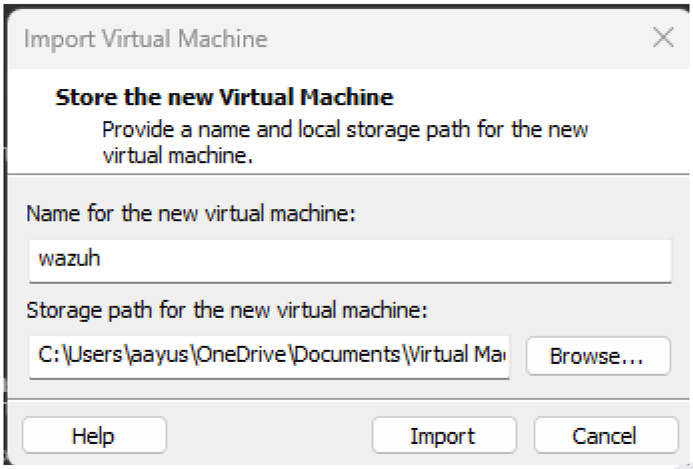
Wazuh

Index

Setting up Wazuh on Virtual Machine (OVA)

1. First download the OVA file.
2. Open and import the ova file in Virtual Box and set up a name and location where you need your data to be stored.



Import Virtual Machine

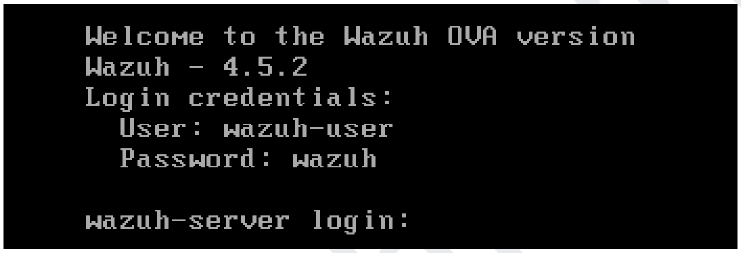
Store the new Virtual Machine

Provide a name and local storage path for the new virtual machine.

Name for the new virtual machine: wazuh

Storage path for the new virtual machine: C:\Users\aayus\OneDrive\Documents\Virtual Ma

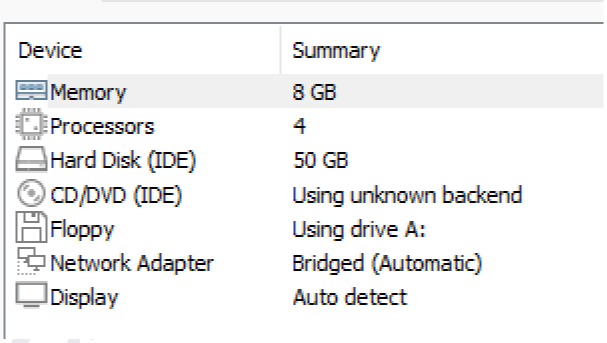
3. Boot in the virtual machine using following credentials:



```
Welcome to the Wazuh OVA version
Wazuh - 4.5.2
Login credentials:
  User: wazuh-user
  Password: wazuh

wazuh-server login:
```

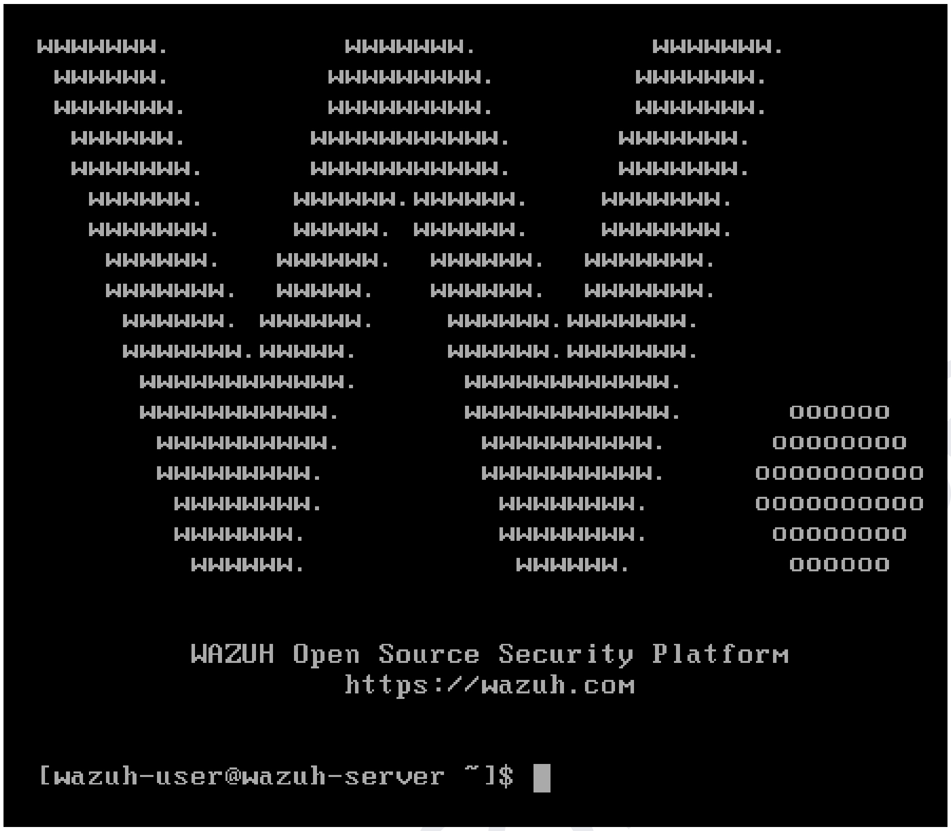
User: wazuh-user Password: wazuh

4. Set VM setting as follows



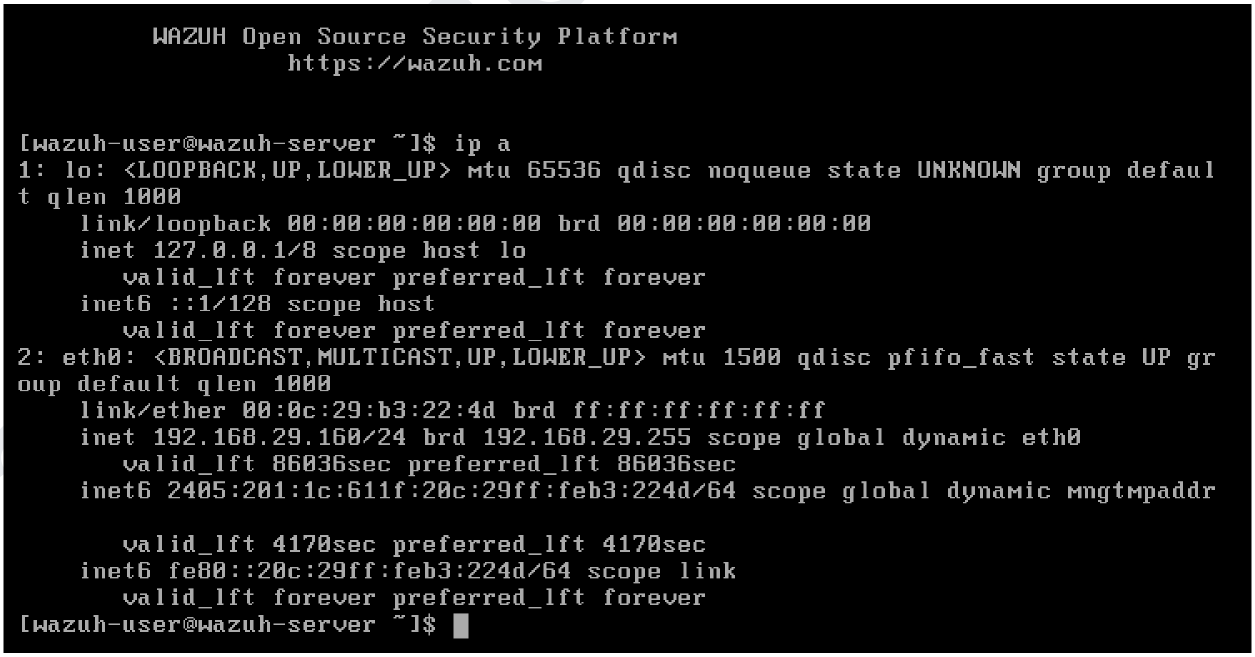
Device	Summary
Memory	8 GB
Processors	4
Hard Disk (IDE)	50 GB
CD/DVD (IDE)	Using unknown backend
Floppy	Using drive A:
Network Adapter	Bridged (Automatic)
Display	Auto detect

5. After logging in you will get the following screen



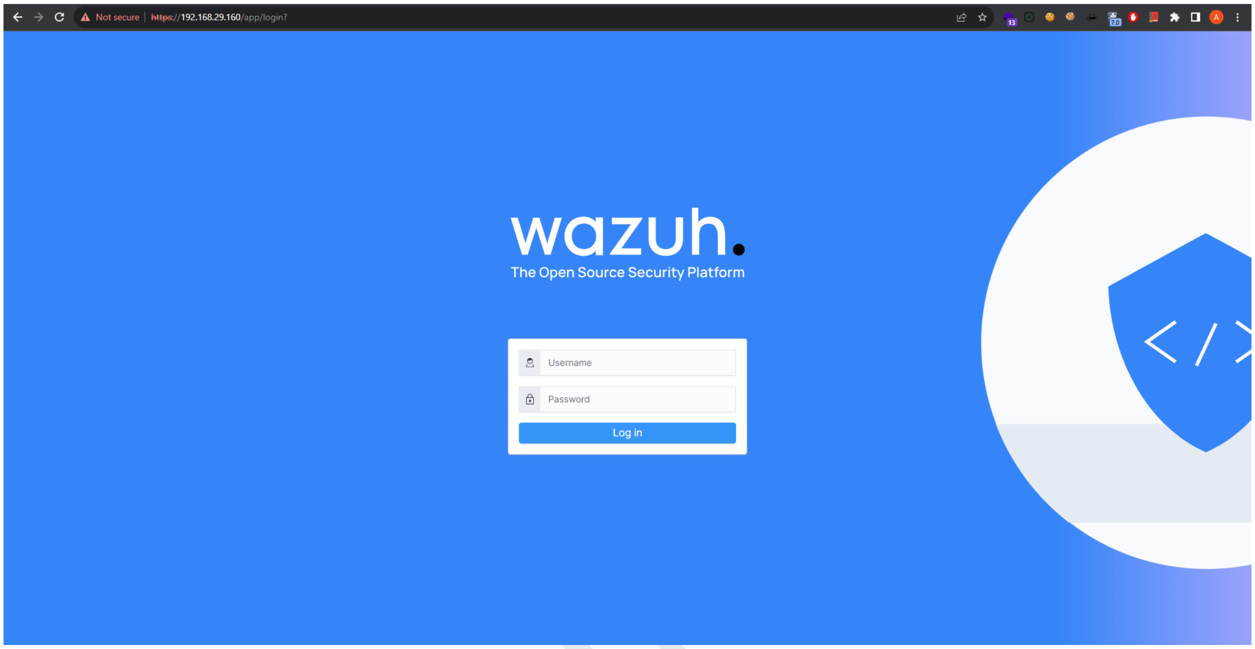
```
wwwwwww.          wwwwwww.          wwwwwww.
 wwwwww.         wwwwwwwww.        wwwwwww.
 wwwwwww.        wwwwwwwww.        wwwwwww.
  wwwwww.       wwwwwwwwwww.      wwwwwww.
  wwwwwww.      wwwwwwwwwww.      wwwwwww.
   wwwwww.     wwwwww.wwwwww.    wwwwwww.
   wwwwwww.    wwwww. wwwwww.    wwwwwww.
    wwwwww.   wwwwww.  wwwwww.  wwwwwww.
    wwwwwww.  wwwww.   wwwwww.  wwwwwww.
     wwwwww. wwwwww.    wwwwww.wwwwwww.
     wwwwwww.wwwww.     wwwwww.wwwwwww.
      wwwwwwwwwwww.      wwwwwwwwwwww.
      wwwwwwwwwww.       wwwwwwwwwwww.      oooooo
       wwwwwwwwww.        wwwwwwwwww.      oooooooo
       wwwwwwwww.         wwwwwwwwww.     oooooooooo
        wwwwwwww.          wwwwwwww.      oooooooooo
        wwwwwww.           wwwwwwww.       oooooooo
         wwwwww.            wwwwww.         oooooo


         WAZUH Open Source Security Platform
                  https://wazuh.com


[wazuh-user@wazuh-server ~]$ 
```

6. Check for the ip address of the server using command **"ip a"**

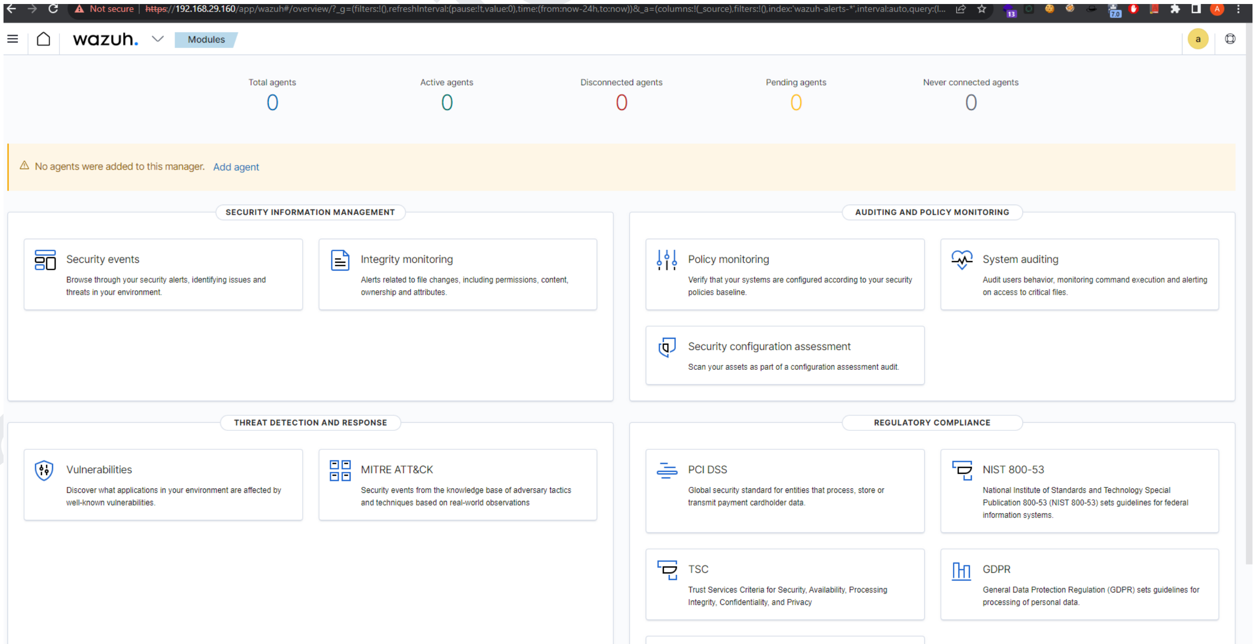


```
         WAZUH Open Source Security Platform
                  https://wazuh.com


[wazuh-user@wazuh-server ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 00:0c:29:b3:22:4d brd ff:ff:ff:ff:ff:ff
    inet 192.168.29.160/24 brd 192.168.29.255 scope global dynamic eth0
       valid_lft 86036sec preferred_lft 86036sec
    inet6 2405:201:1c:611f:20c:29ff:feb3:224d/64 scope global dynamic mngtmpaddr

       valid_lft 4170sec preferred_lft 4170sec
    inet6 fe80::20c:29ff:feb3:224d/64 scope link
       valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]$ 
```

7. Hit the browser with the following URL to check if wazuh is up.
   https://<wazuh_server_ip>
   In our case it will be https://192.168.29.160
   You will get the following web page


Not secure | https://192.168.29.160/app/login?
wazuh.
The Open Source Security Platform
Username
Password
Log in

8. Use the default credentials to login
   User: admin Password: admin
9. You will get the following console:


Not secure | https://192.168.29.160/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(),index:'wazuh-alerts-*',interval:auto,query:(l...
wazuh.
Modules
a

Total agents 0

Active agents 0

Disconnected agents 0

Pending agents 0

Never connected agents 0

⚠ No agents were added to this manager. Add agent

SECURITY INFORMATION MANAGEMENT

Security events
Browse through your security alerts, identifying issues and threats in your environment.

Integrity monitoring
Alerts related to file changes, including permissions, content, ownership and attributes.

AUDITING AND POLICY MONITORING

Policy monitoring
Verify that your systems are configured according to your security policies baseline.

System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.

Security configuration assessment
Scan your assets as part of a configuration assessment audit.

THREAT DETECTION AND RESPONSE

Vulnerabilities
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Security events from the knowledge base of adversary tactics and techniques based on real-world observations

REGULATORY COMPLIANCE

PCI DSS
Global security standard for entities that process, store or transmit payment cardholder data.

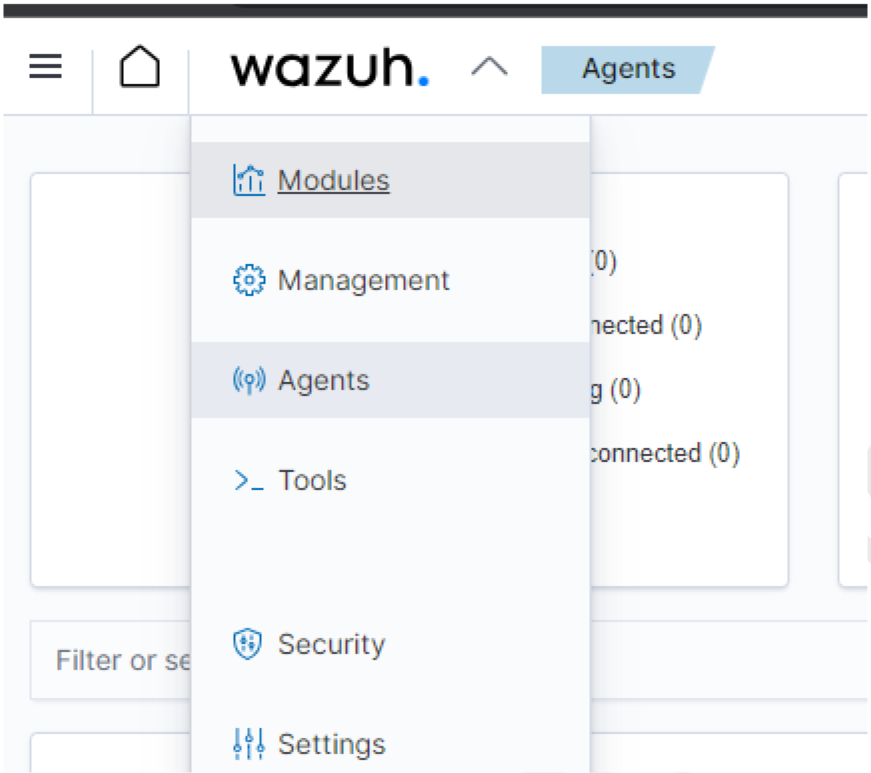
NIST 800-53
National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

TSC
Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

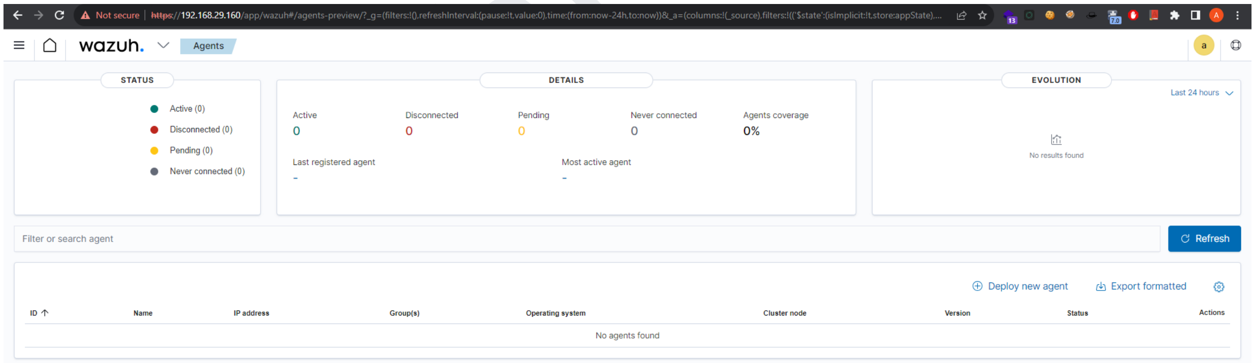
GDPR
General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

Setting up an agent on the endpoint.

Once you login into the wazuh dashboard you can add agents:



On clicking Agents option you will get the following page:


Not secure
https://192.168.29.160/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(('$state':(isImplicit:!t,store:appState),...
wazuh.
Agents

STATUS

- ● Active (0)
- ● Disconnected (0)
- ● Pending (0)
- ● Never connected (0)

DETAILS

Active	Disconnected	Pending	Never connected	Agents coverage
0	0	0	0	0%

Last registered agent
-

Most active agent
-

EVOLUTION

Last 24 hours

No results found

Filter or search agent

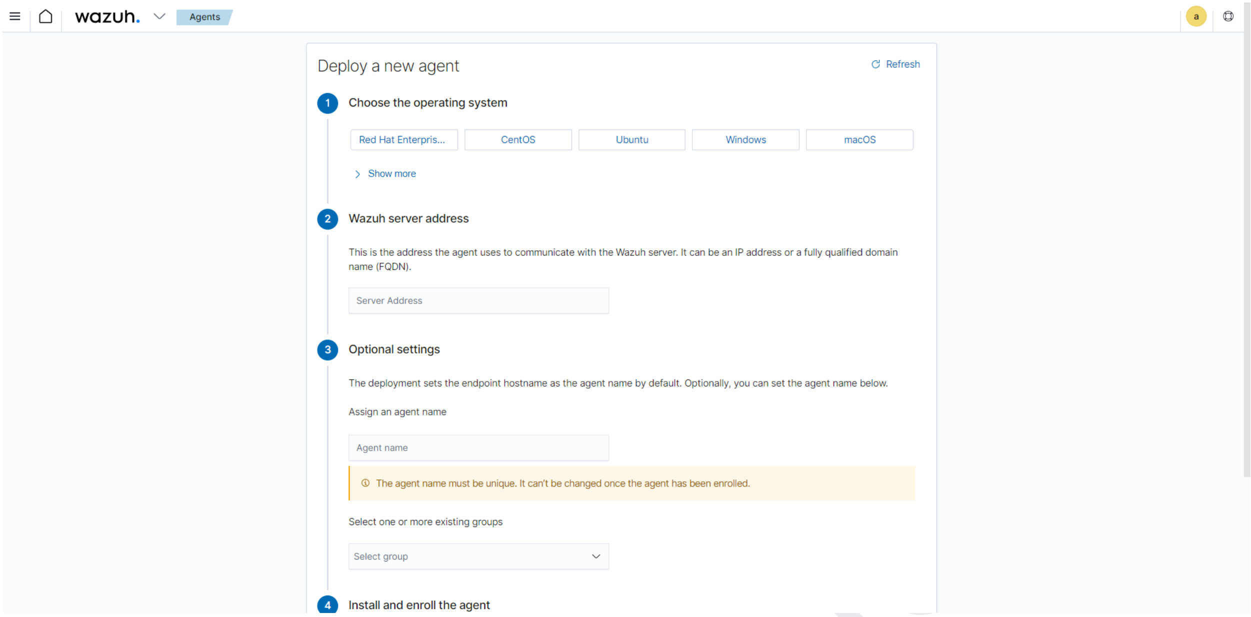
Refresh

Deploy new agent   Export formatted

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
No agents found								

Click on **“Deploy new agent”** option:

You will get the below screen.



Deploy a new agent

1 Choose the operating system

2 Wazuh server address

This is the address the agent uses to communicate with the Wazuh server. It can be an IP address or a fully qualified domain name (FQDN).

3 Optional settings

The deployment sets the endpoint hostname as the agent name by default. Optionally, you can set the agent name below.

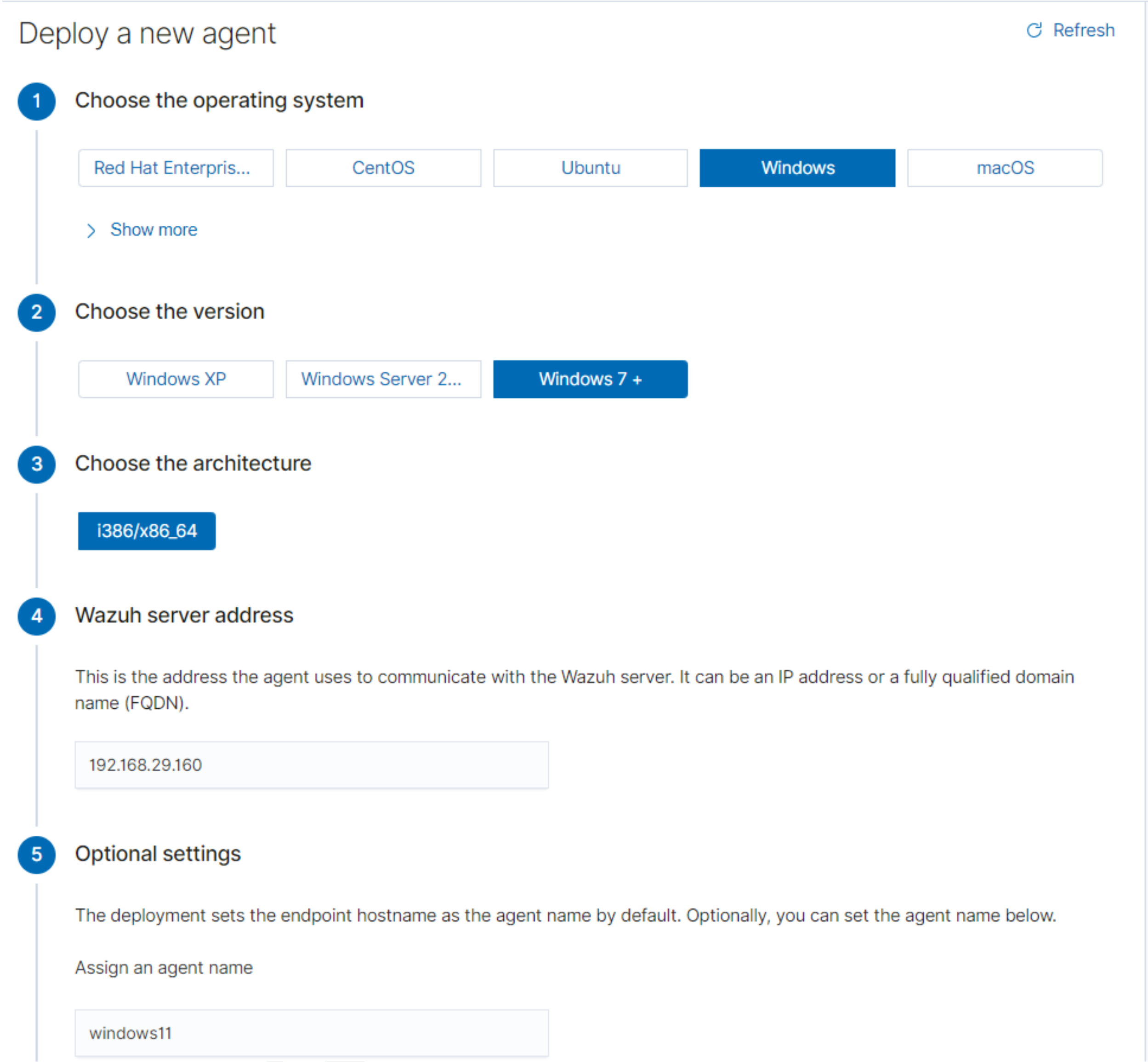
Assign an agent name

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

Select one or more existing groups

4 Install and enroll the agent

Select the required options. For our case the configuration will look like this:



Deploy a new agent

1 Choose the operating system

Red Hat Enterpris... CentOS Ubuntu [✓ Windows] macOS

2 Choose the version

Windows XP Windows Server 2... [✓ Windows 7 +]

3 Choose the architecture

[✓ i386/x86_64]

4 Wazuh server address

This is the address the agent uses to communicate with the Wazuh server. It can be an IP address or a fully qualified domain name (FQDN).

192.168.29.160

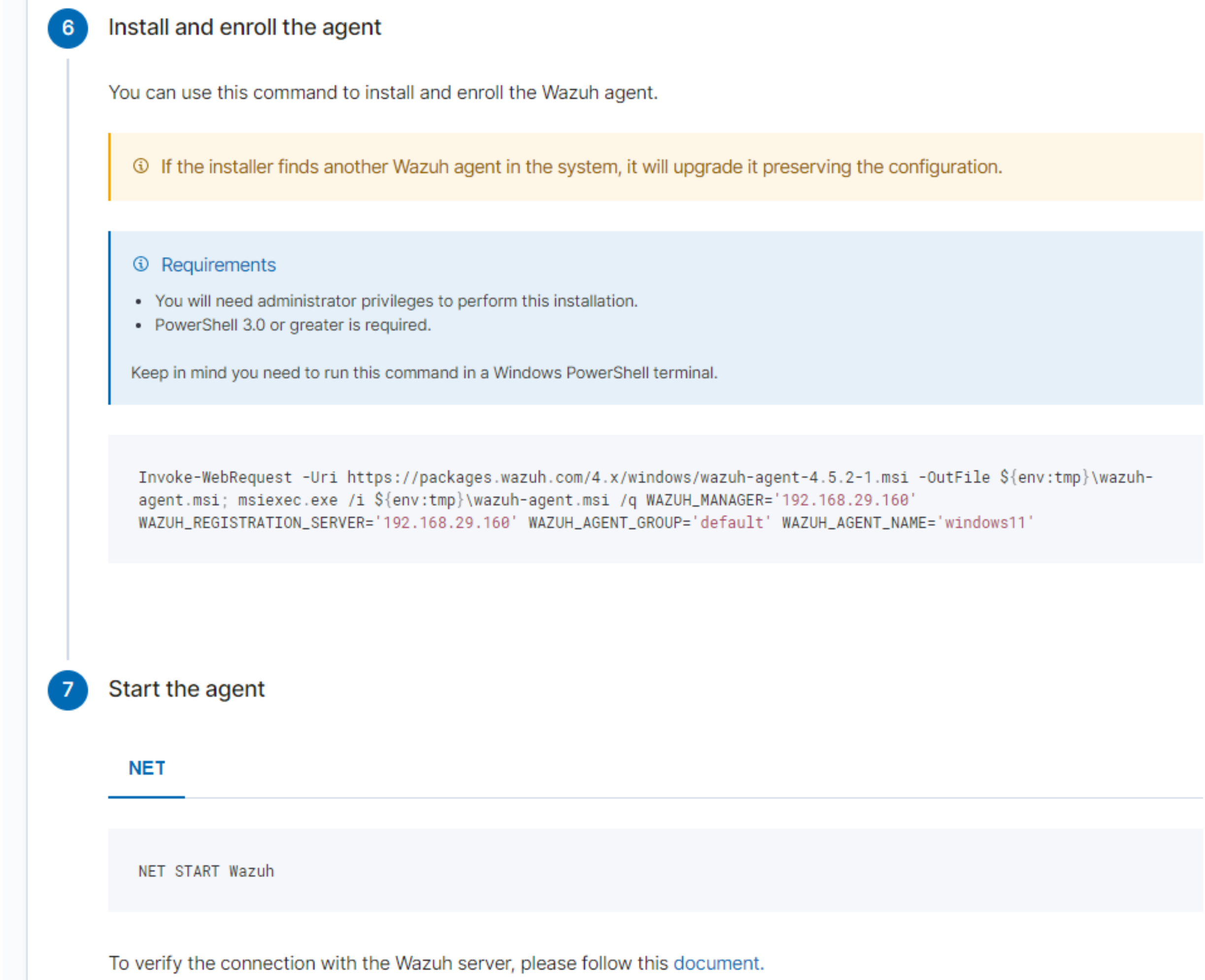
5 Optional settings

The deployment sets the endpoint hostname as the agent name by default. Optionally, you can set the agent name below.

Assign an agent name

windows11

At last wazuh will generate a command which needs to be run with admin privileges to install and start the agent:



6 Install and enroll the agent

You can use this command to install and enroll the Wazuh agent.

ⓘ If the installer finds another Wazuh agent in the system, it will upgrade it preserving the configuration.

ⓘ 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.

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.5.2-1.msi -OutFile ${env:tmp}\wazuh-
agent.msi; msiexec.exe /i ${env:tmp}\wazuh-agent.msi /q WAZUH_MANAGER='192.168.29.160'
WAZUH_REGISTRATION_SERVER='192.168.29.160' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='windows11'
```

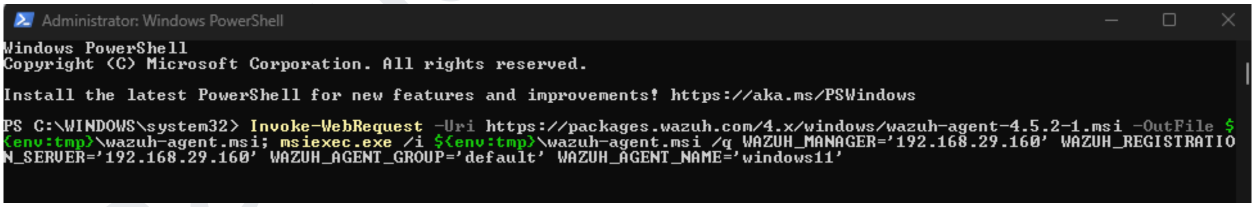
7 Start the agent

NET

```
NET START Wazuh
```

To verify the connection with the Wazuh server, please follow this document.

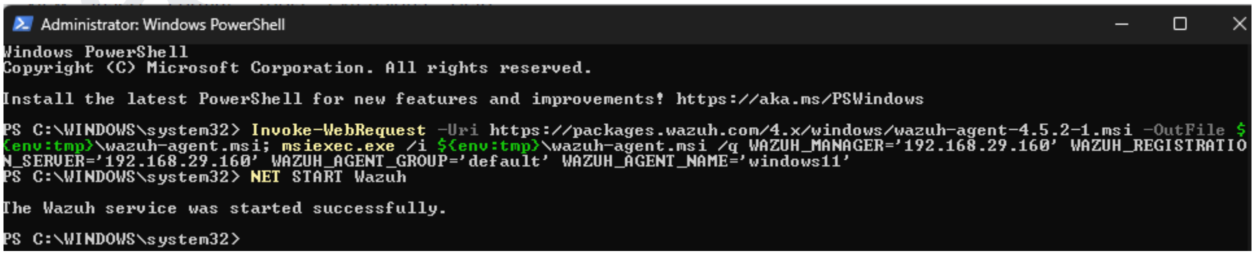
Open powershell with admin permissions and insert the command as shown in wazuh:



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-4.5.2-1.msi -OutFile $
{env:tmp}\wazuh-agent.msi; msiexec.exe /i ${env:tmp}\wazuh-agent.msi /q WAZUH_MANAGER='192.168.29.160' WAZUH_REGISTRATIO
N_SERVER='192.168.29.160' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='windows11'
```

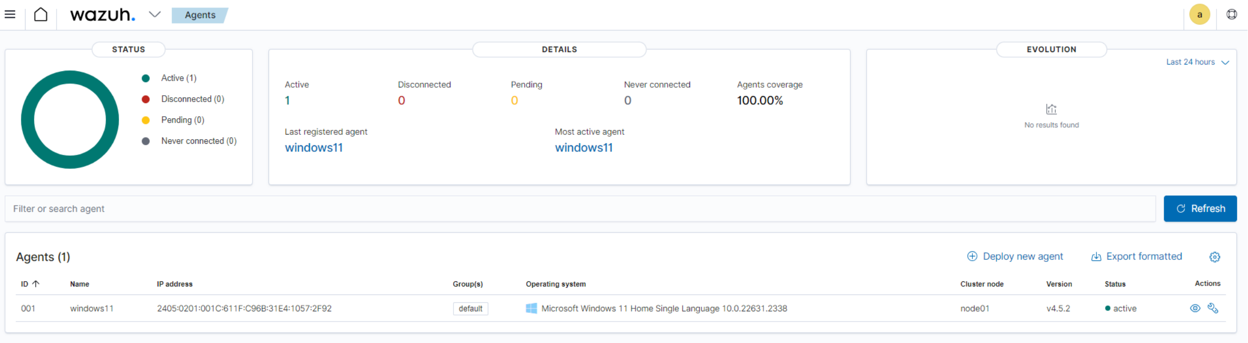
Start the agent:



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-4.5.2-1.msi -OutFile $
{env:tmp}\wazuh-agent.msi; msiexec.exe /i ${env:tmp}\wazuh-agent.msi /q WAZUH_MANAGER='192.168.29.160' WAZUH_REGISTRATIO
N_SERVER='192.168.29.160' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='windows11'
PS C:\WINDOWS\system32> NET START Wazuh

The Wazuh service was started successfully.

PS C:\WINDOWS\system32>
```

Go back to agents page there you can see that your agent is live and running:



Active	Disconnected	Pending	Never connected	Agents coverage
1	0	0	0	100.00%

Last registered agent
windows11

Most active agent
windows11

Agents (1)

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	windows11	2405:0201:001C:611F:C96B:31E4:1057:2F92	default	Microsoft Windows 11 Home Single Language 10.0.22631.2338	node01	v4.5.2	● active	

Till now,we have seen how to set up wazuh and install agent.

Later we will cover every feature of the wazuh.