🛡️ Wazuh SIEM Setup & Windows Agent Log Collection – My Beginner-Level SOC Project

Prepared by: Faizanullah Syed
Email: faizanullah.syed19@gmail.com

✅ Project Overview:

I set up a basic **Security Information and Event Management (SIEM)** environment using **Wazuh.** My goal was to monitor a Windows system's logs in real-time to understand how a SOC works.

🔧 Tools Used:

- **Wazuh OVA File**
- **VirtualBox**
- **Windows OS (Agent Machine)**
- **Pastebin (for command transfer)**
- **Browser (to access Wazuh Dashboard via HTTPS)**

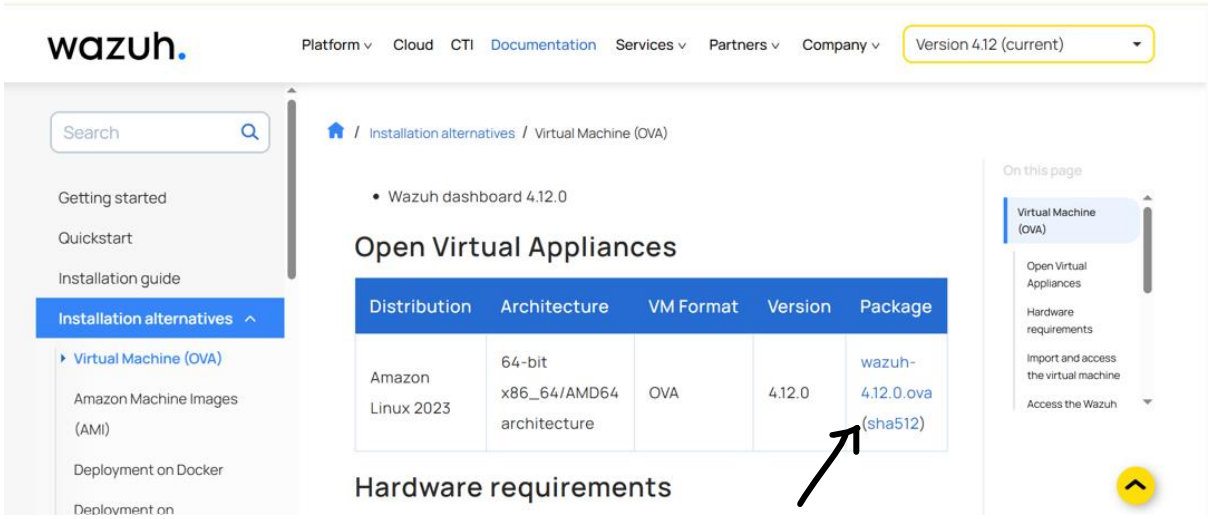
Objective:

To deploy a working Wazuh Security Information and Event Management (SIEM) environment in a virtual machine and successfully monitor logs from a Windows system.

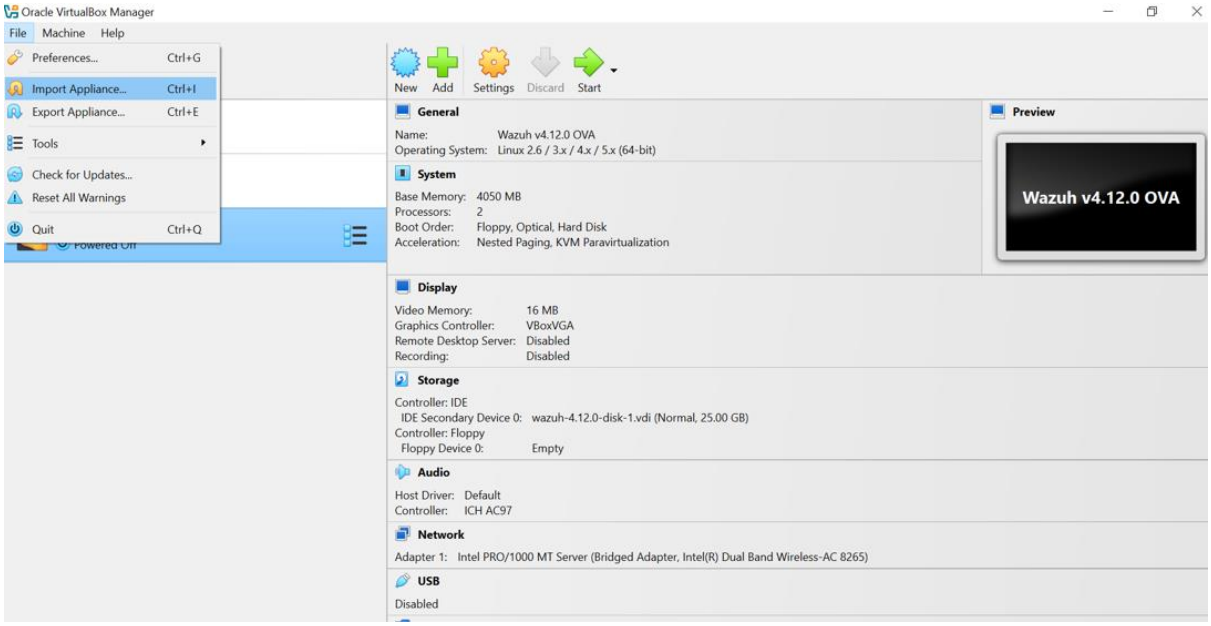
🛠️ Project Steps:

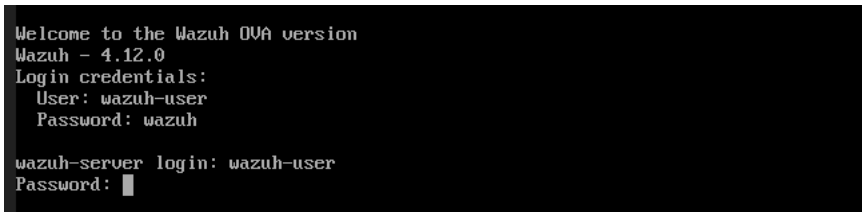
1. Wazuh Deployment:

- Downloaded and imported the official **Wazuh OVA file** into VirtualBox.

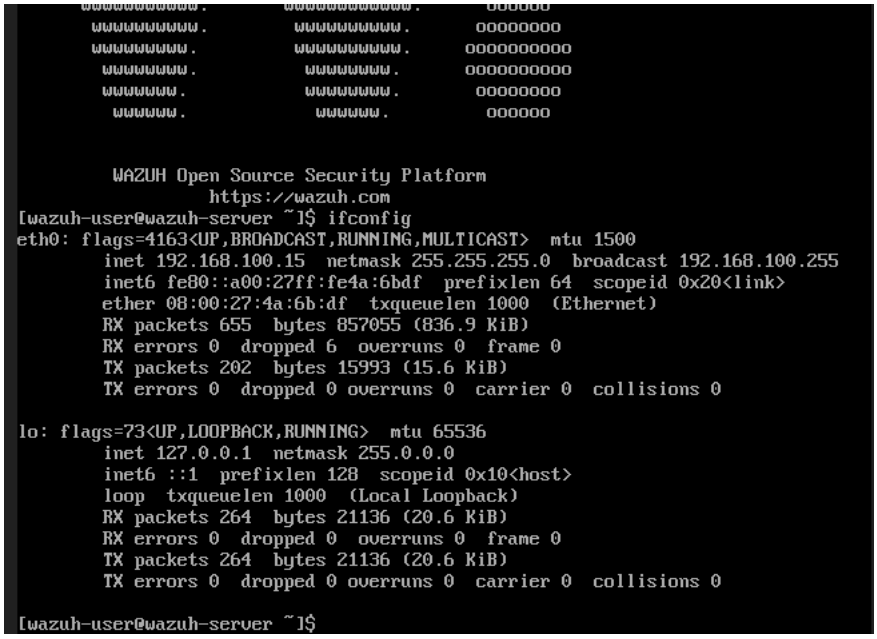


- Started the Wazuh virtual machine.



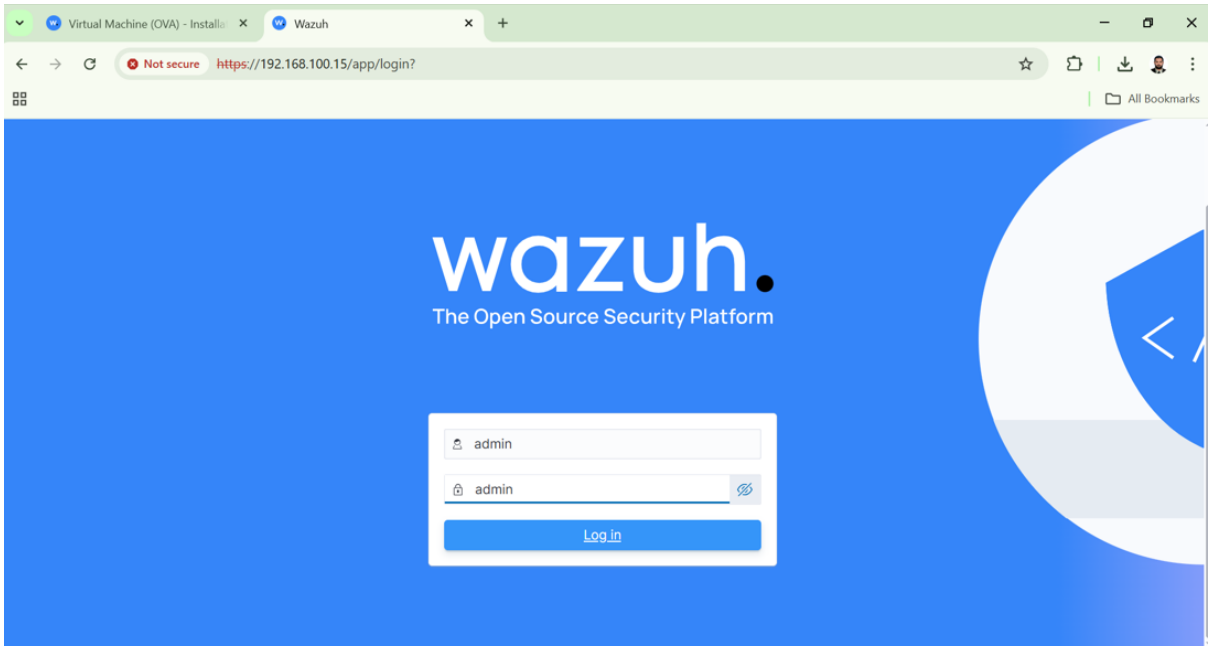


- Obtained the VM IP and accessed Wazuh Dashboard through browser:



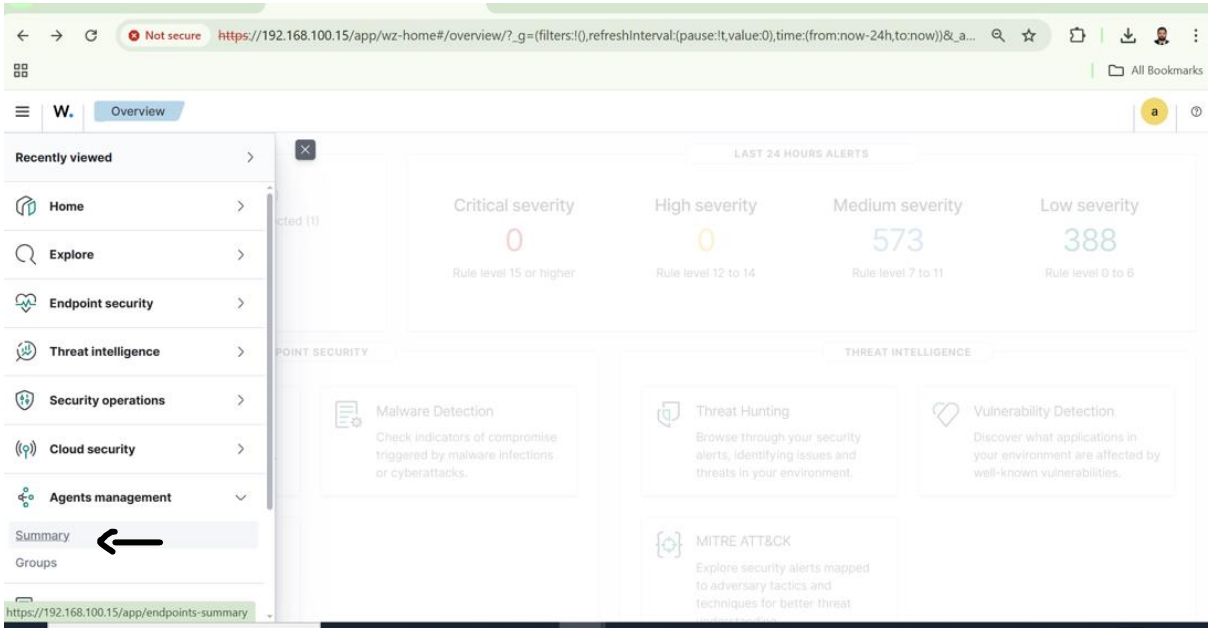
➤ https://<VM-IP>

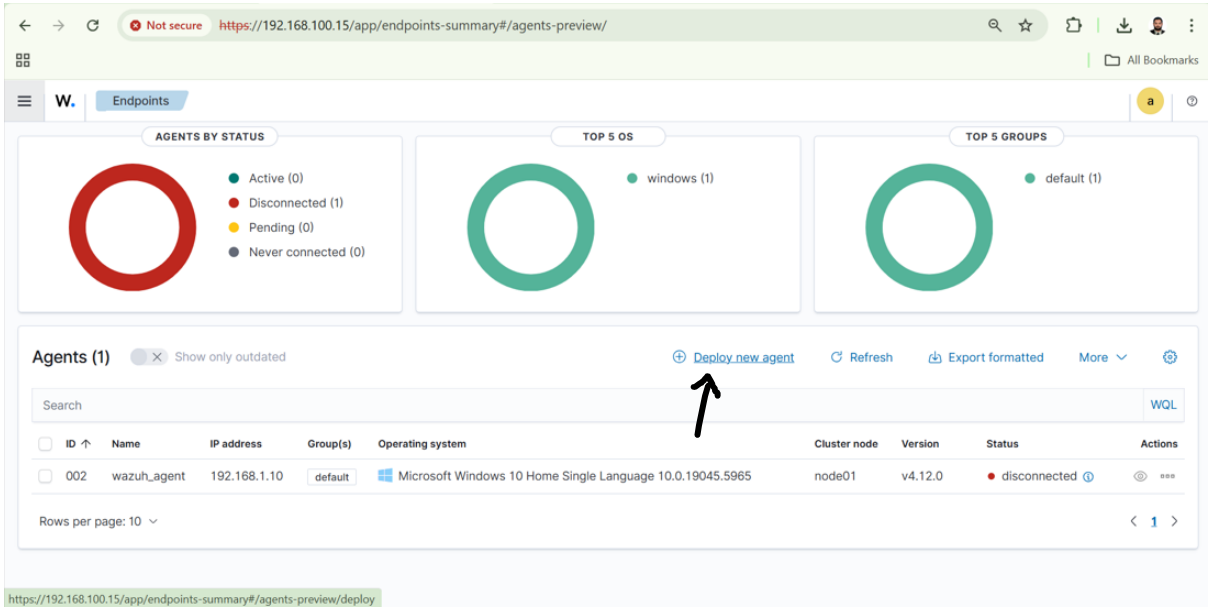
- Logged in using default credentials and changed them after first login.

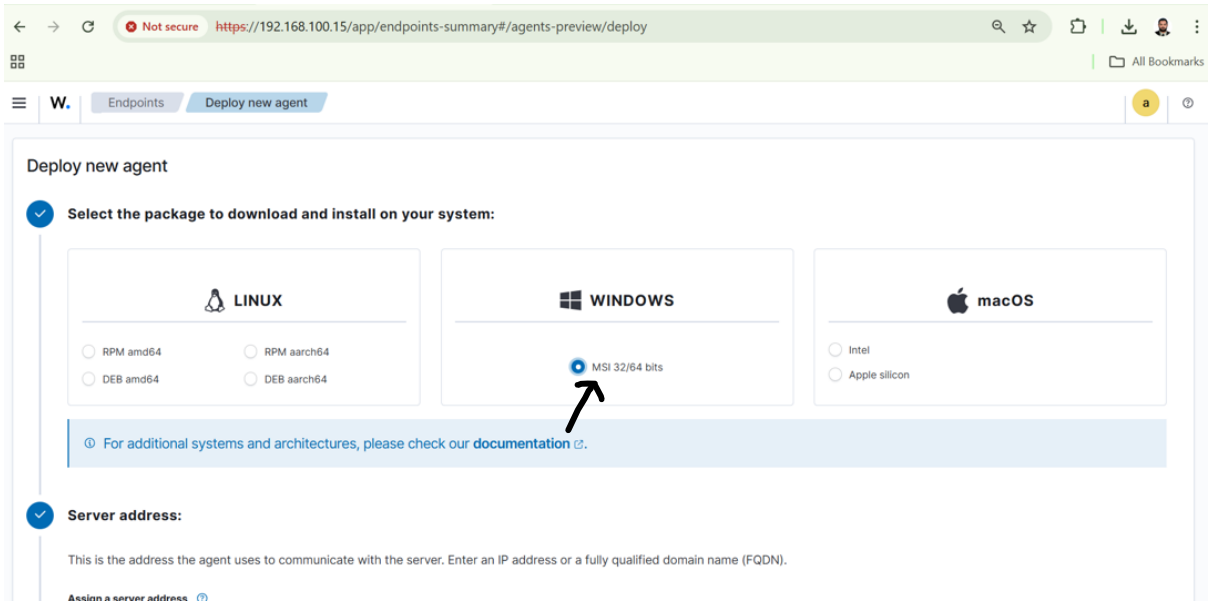


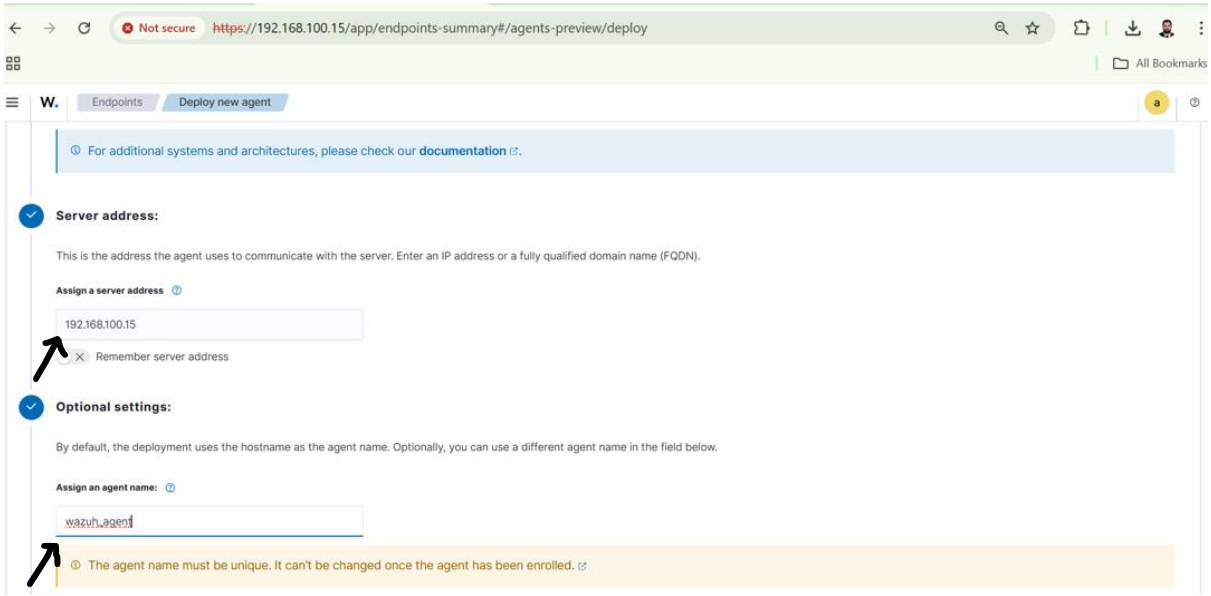
2. Accessing Agent Management:

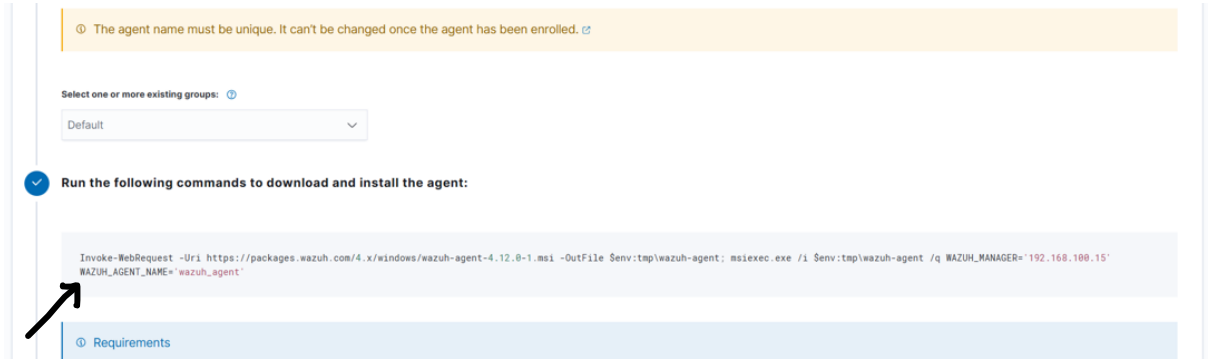
- On the **Wazuh Dashboard**, clicked the ☰ **(Menu)** icon.
- Navigated to **"Agent Management" → "Summary"**
- This section shows a full list of connected agents and their status.
- Click on Deploy New Agent





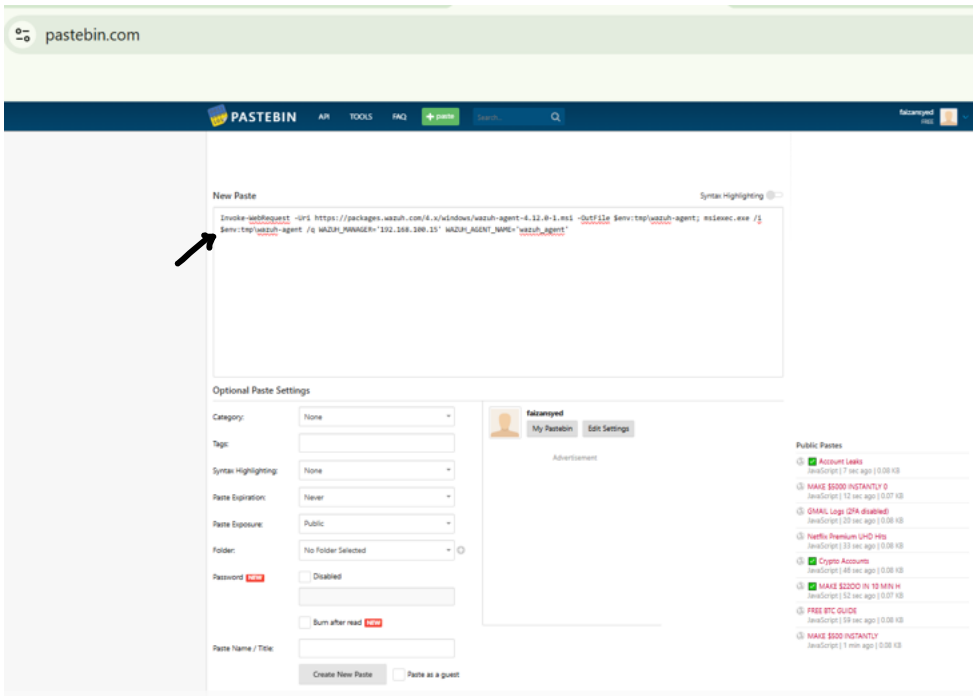

Not secure https://192.168.100.15/app/endpoints-summary#/agents-preview/deploy
All Bookmarks
W.
Endpoints
Deploy new agent
a
Deploy new agent
Select the package to download and install on your system:
LINUX
RPM amd64
RPM aarch64
DEB amd64
DEB aarch64
WINDOWS
MSI 32/64 bits
macOS
Intel
Apple silicon
For 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 (FQDN).
Assign a server address


Not secure https://192.168.100.15/app/endpoints-summary#/agents-preview/deploy
All Bookmarks
W.
Endpoints
Deploy new agent
a
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 (FQDN).
Assign a server address
192.168.100.15
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:
wazuh_agent
The agent name must be unique. It can't be changed once the agent has been enrolled.

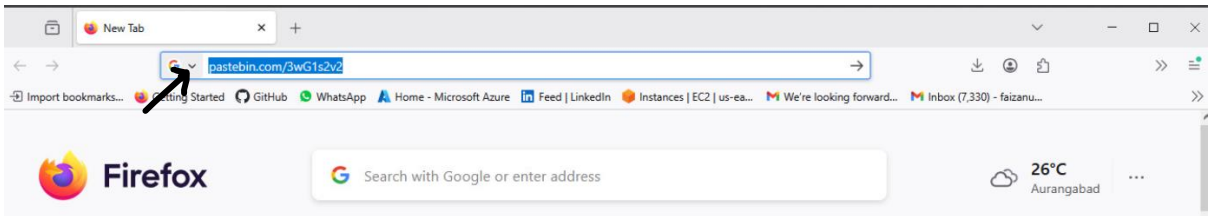

The agent name must be unique. It can't be changed once the agent has been enrolled.
Select one or more existing groups:
Default
Run the following commands to download and install the agent:
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.12.0-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.100.15'
WAZUH_AGENT_NAME='wazuh_agent'
Requirements

3. Windows Agent Setup:

- On the Windows machine, downloaded the **Wazuh Agent Installer**.
- Used **Pastebin** to store the registration command (to avoid typing errors and make copy-pasting easier).
- Opened the Pastebin link in the Windows browser and copied the command.
- Ran the command in PowerShell (as Administrator) to register the Windows machine with the Wazuh Manager.
- Open browser in Windows OS for Collecting Commands from pastebin as shown in screenshots below



Endpoint windows os Agent collect command using pastebin



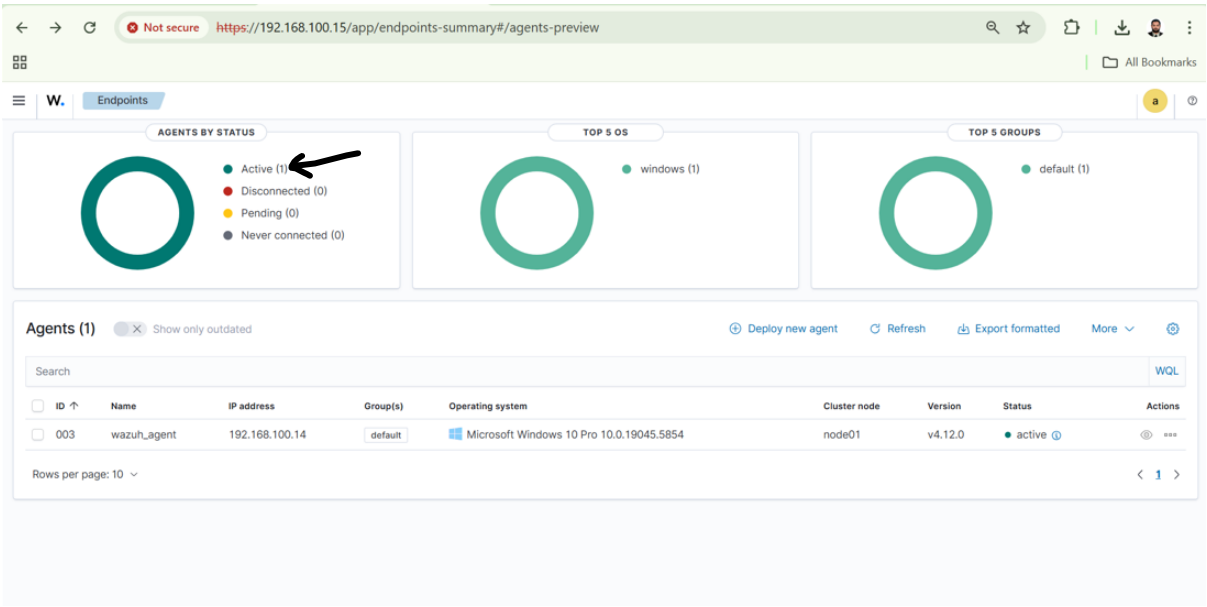

```
PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.12.0-1.msi -OutFile
$env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.100.15' WAZUH_AGENT_NAME='wazuh_agen
t'
```

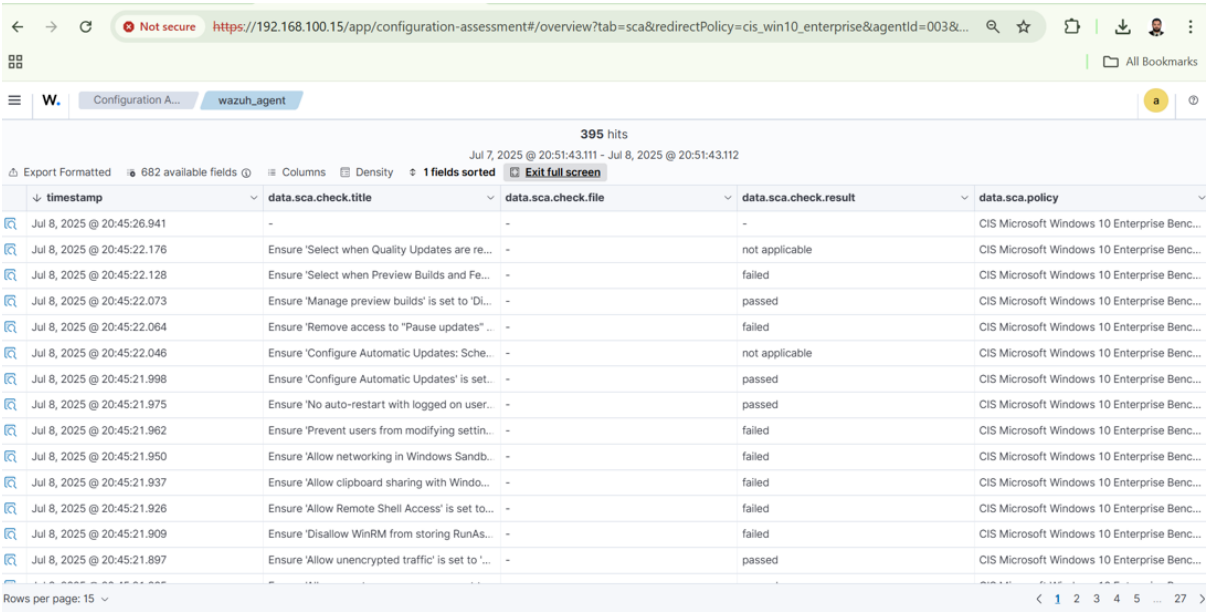
```
PS C:\Windows\system32> NET START Wazuhsvc
The Wazuh service is starting.
The Wazuh service was started successfully.
```

 # NET START Wazuhsvc

4. Log Collection & Verification:

- Back in the **Agent Management > Summary**, checked that the Windows agent appeared and showed a green status (active).
- Confirmed that logs were being received, including:
  - **System logs**
  - **Application logs**
  - **Security logs**





🎯 Outcome:

- Wazuh Manager and Agent were successfully configured and connected.
- Log data from the Windows system was visible and being analyzed in real time.
- Completed a basic but working SOC setup suitable for learning and demonstrations.