

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.

wazuh. Platform Cloud CTI Documentation Services Partners Company Version 4.12 (current)

Search

Getting started
Quickstart
Installation guide
Installation alternatives ^
Virtual Machine (OVA)
Amazon Machine Images (AMI)
Deployment on Docker
Deployment on

/ Installation alternatives / Virtual Machine (OVA)

- Wazuh dashboard 4.12.0

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)

Hardware requirements

On this page

- Virtual Machine (OVA)
- Open Virtual Appliances
- Hardware requirements
- Import and access the virtual machine
- Access the Wazuh

- Started the Wazuh virtual machine.

Oracle VM VirtualBox Manager

File Machine Help

- Preferences... Ctrl+G
- Import Appliance... Ctrl+I
- Export Appliance... Ctrl+E
- Tools
- Check for Updates...
- Reset All Warnings
- Quit Ctrl+Q

New Add Settings Discard Start

General

Name: Wazuh v4.12.0 OVA
Operating System: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)

System

Base Memory: 4050 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VBoxVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: wazuh-4.12.0-disk-1.vdi (Normal, 25.00 GB)
Controller: Floppy
Floppy Device 0: Empty

Audio

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Server (Bridged Adapter, Intel(R) Dual Band Wireless-AC 8265)

USB

Disabled

Preview

Wazuh v4.12.0 OVA

```
Welcome to the Wazuh OVA version
Wazuh - 4.12.0
Login credentials:
User: wazuh-user
Password: wazuh

wazuh-server login: wazuh-user
Password: 
```

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

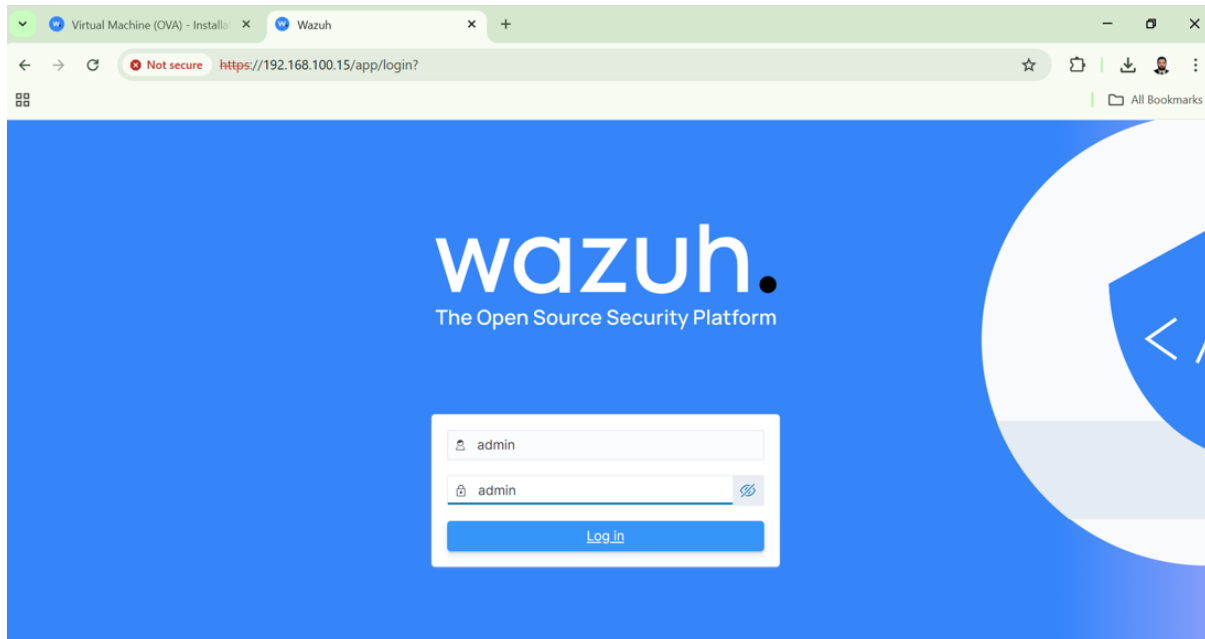
```
WAZUH Open Source Security Platform
https://wazuh.com
[wazuh-user@wazuh-server ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.15 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::a00:27ff:fe4a:6bdf prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:4a:6b:df txqueuelen 1000 (Ethernet)
    RX packets 655 bytes 857055 (836.9 KiB)
    RX errors 0 dropped 6 overruns 0 frame 0
    TX packets 202 bytes 15993 (15.6 KiB)
    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 264 bytes 21136 (20.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 264 bytes 21136 (20.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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

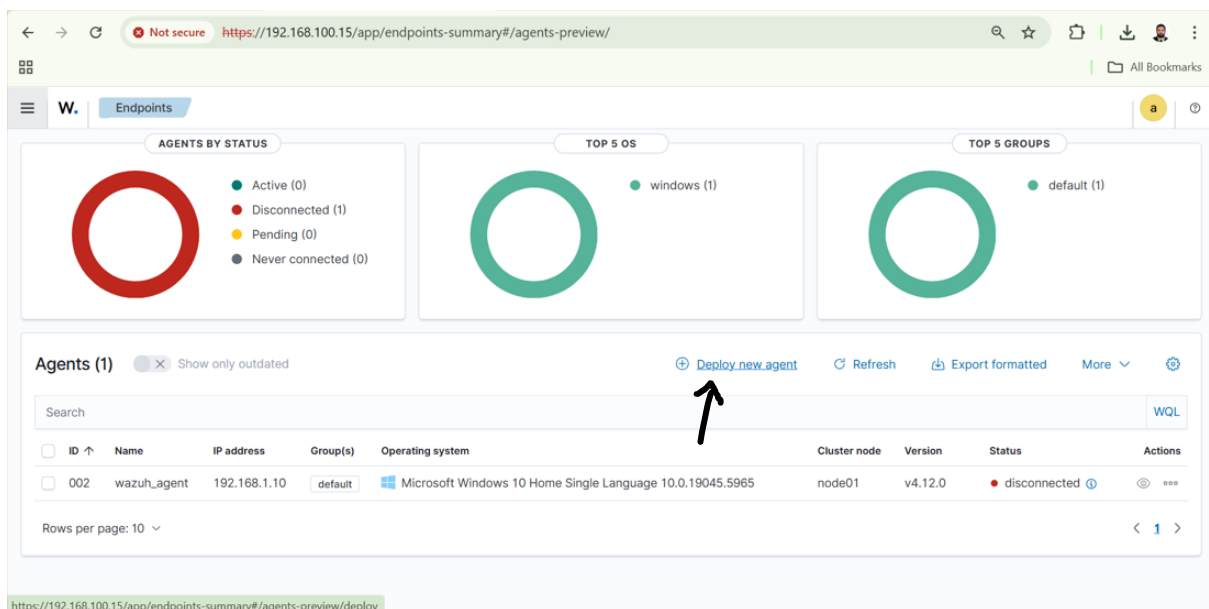
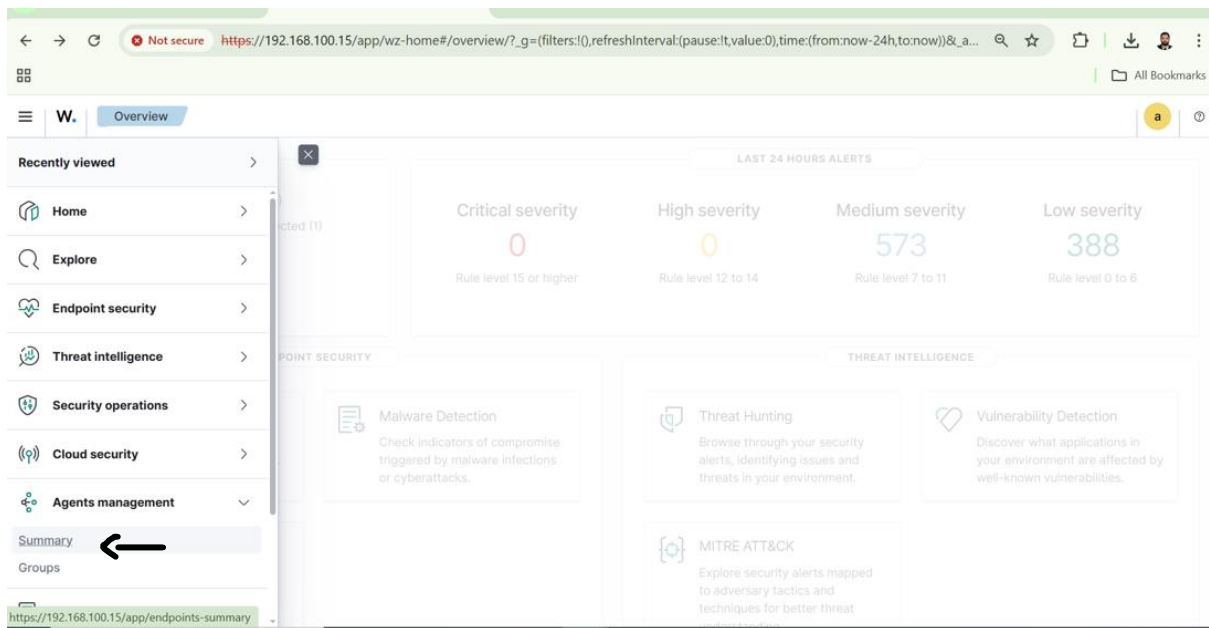
➤ <https://<VM-IP>>

- 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

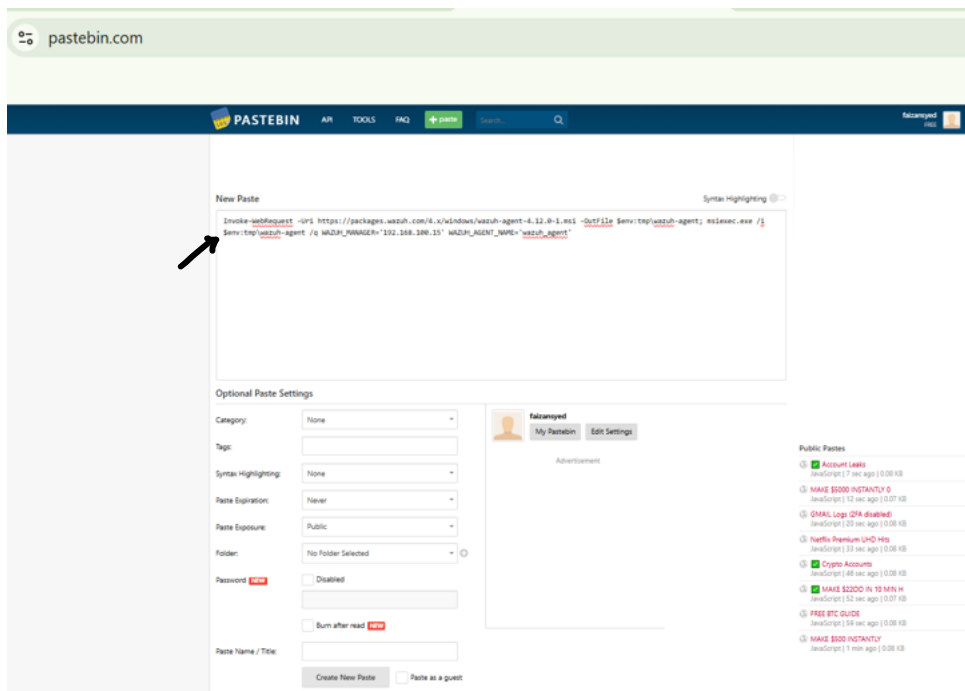
✓ **Run the following commands to download and install the agent:**

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.12.0-1.msi -OutFile $env:tmp\wazuh-agent; msixexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.100.15' WAZUH_AGENT_NAME='wazuh-agent'
```

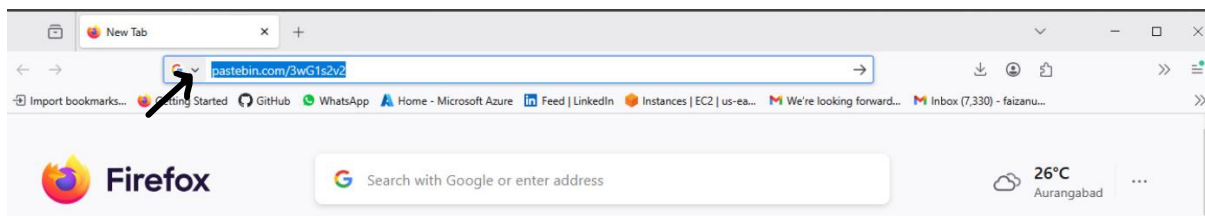
ⓘ Requirements

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



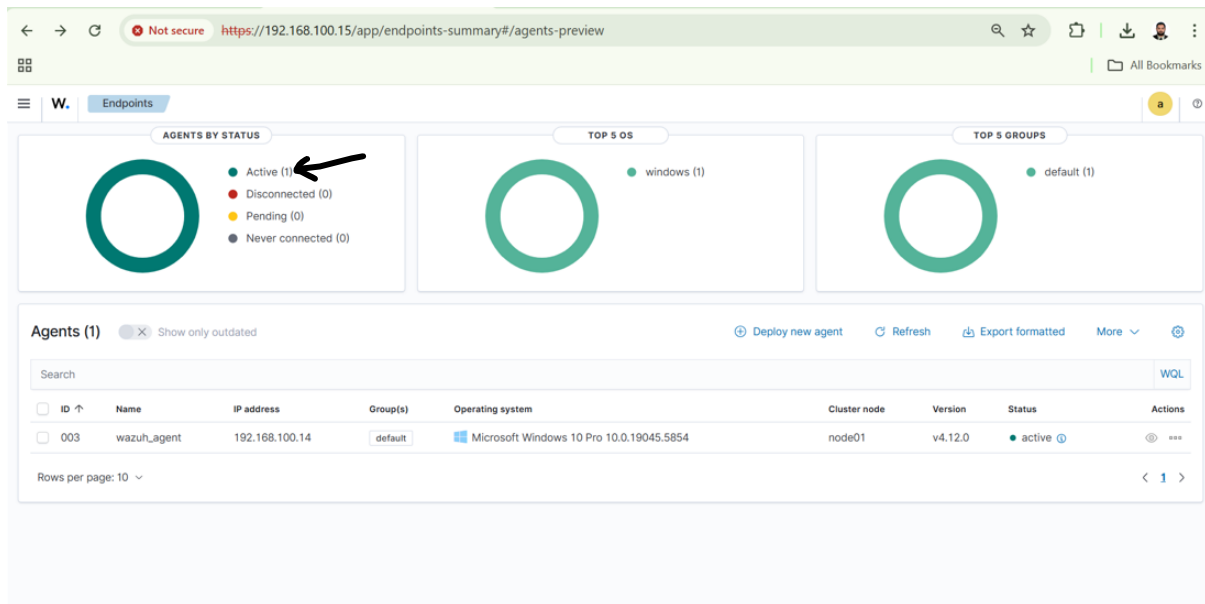
```
PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.12.0-1.msi -OutFile $env:tmp\wazuh-agent; msisexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.100.15' WAZUH_AGENT_NAME='wazuh_agent'
```

```
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**



The screenshot displays the 'Configuration Assessment' page for the 'wazuh_agent'. It shows a table of 395 hits for configuration checks. The table has columns: timestamp, data.sca.check.title, data.sca.check.file, data.sca.check.result, and data.sca.policy. The results show various checks for Windows 10 Enterprise, with some failing and some passing.

timestamp	data.sca.check.title	data.sca.check.file	data.sca.check.result	data.sca.policy
Jul 8, 2025 @ 20:45:26.941	-	-	-	CIS Microsoft Windows 10 Enterprise Benc...
Jul 8, 2025 @ 20:45:22.176	Ensure 'Select when Quality Updates are re...	-	not applicable	CIS Microsoft Windows 10 Enterprise Benc...
Jul 8, 2025 @ 20:45:22.128	Ensure 'Select when Preview Builds and Fe...	-	failed	CIS Microsoft Windows 10 Enterprise Benc...
Jul 8, 2025 @ 20:45:22.073	Ensure 'Manage preview builds' is set to 'DI...	-	passed	CIS Microsoft Windows 10 Enterprise Benc...
Jul 8, 2025 @ 20:45:22.064	Ensure 'Remove access to "Pause updates" ...	-	failed	CIS Microsoft Windows 10 Enterprise Benc...
Jul 8, 2025 @ 20:45:22.046	Ensure 'Configure Automatic Updates: Sche...	-	not applicable	CIS Microsoft Windows 10 Enterprise Benc...
Jul 8, 2025 @ 20:45:21.998	Ensure 'Configure Automatic Updates' is set...	-	passed	CIS Microsoft Windows 10 Enterprise Benc...
Jul 8, 2025 @ 20:45:21.975	Ensure 'No auto-restart with logged on user...	-	passed	CIS Microsoft Windows 10 Enterprise Benc...
Jul 8, 2025 @ 20:45:21.962	Ensure 'Prevent users from modifying settin...	-	failed	CIS Microsoft Windows 10 Enterprise Benc...
Jul 8, 2025 @ 20:45:21.950	Ensure 'Allow networking in Windows Sandb...	-	failed	CIS Microsoft Windows 10 Enterprise Benc...
Jul 8, 2025 @ 20:45:21.937	Ensure 'Allow clipboard sharing with Windo...	-	failed	CIS Microsoft Windows 10 Enterprise Benc...
Jul 8, 2025 @ 20:45:21.926	Ensure 'Allow Remote Shell Access' is set to...	-	failed	CIS Microsoft Windows 10 Enterprise Benc...
Jul 8, 2025 @ 20:45:21.909	Ensure 'Disallow WinRM from storing RunAs...	-	failed	CIS Microsoft Windows 10 Enterprise Benc...
Jul 8, 2025 @ 20:45:21.897	Ensure 'Allow unencrypted traffic' is set to '...	-	passed	CIS Microsoft Windows 10 Enterprise Benc...

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.