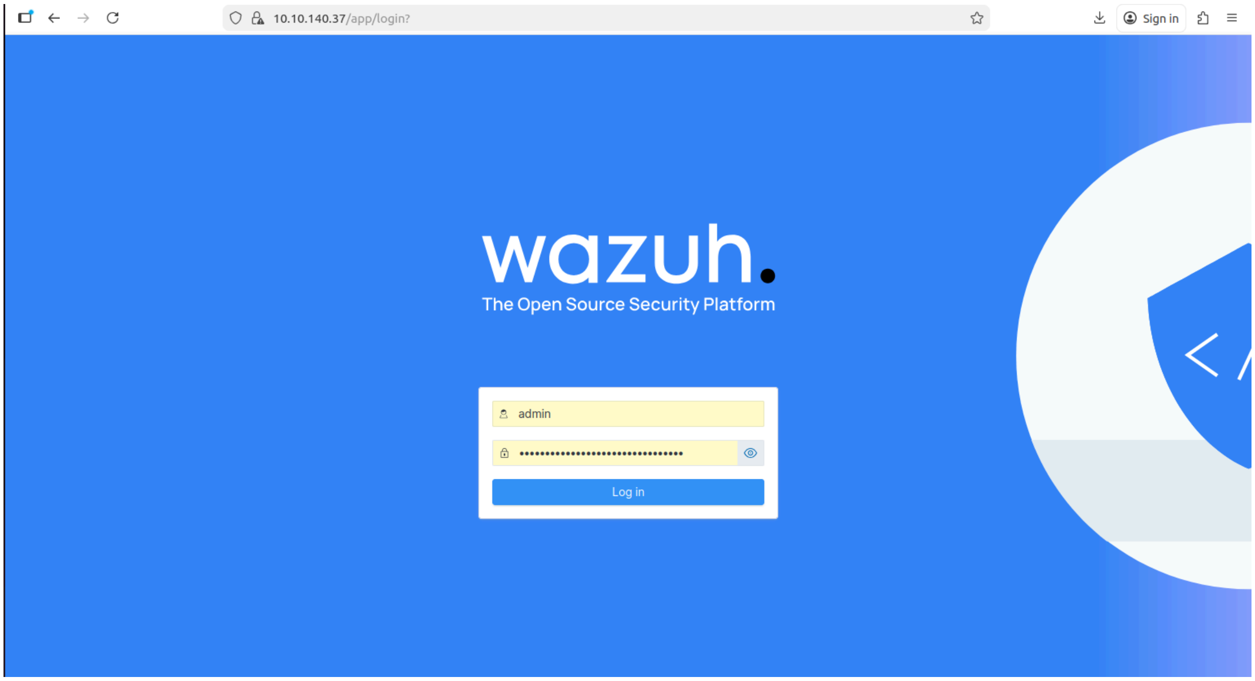
Agent Installation on Window Server

Introduction

After installing the Wazuh Server on Ubuntu operating system, the next step is to install the Wazuh Agent on Windows Server.
The Agent is required to collect the logs, events and system information from the Windows server and send them to Wazuh Server.

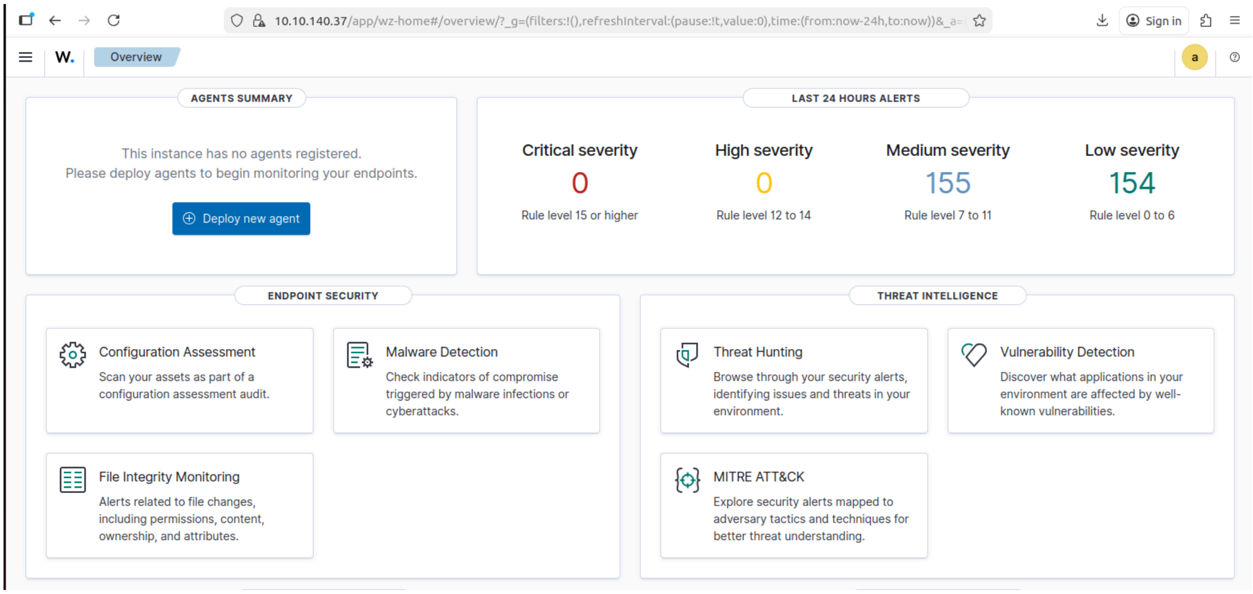
We installed the agent by using Wazuh Dashboard and clicking on the “Deploy New Agent” option.
Before installing the agent, ensure that the server machine and the agent machine are on the same network.
Checking communication between both systems is important because the Windows agent needs to connect to the Wazuh Manager.

First open the Wazuh Dashboard using the IP address of Ubuntu host system.


10.10.140.37/app/login?

wazuh.
The Open Source Security Platform

admin
••••••••••••••••••••••••••••••••••



10.10.140.37/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=

Overview

AGENTS SUMMARY

This instance has no agents registered.
Please deploy agents to begin monitoring your endpoints.

Deploy new agent

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	155	154
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

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

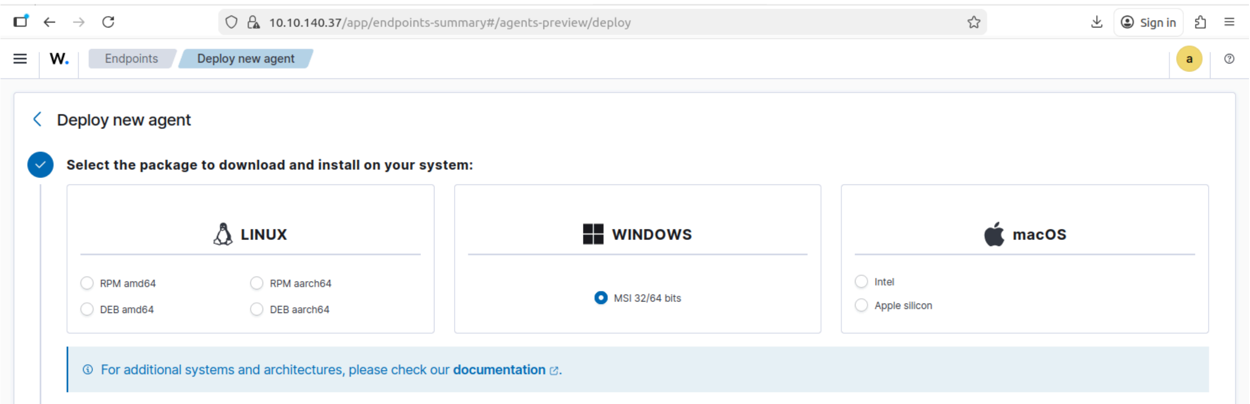
THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

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

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

Click on “Deploy New Agent”
Now select the endpoint where we want to deploy our Agent as we installed the Agent on Windows Server so we select it.



10.10.140.37/app/endpoints-summary#/agents-preview/deploy

Endpoints › Deploy new agent

Deploy new agent

Select the package to download and install on your system:

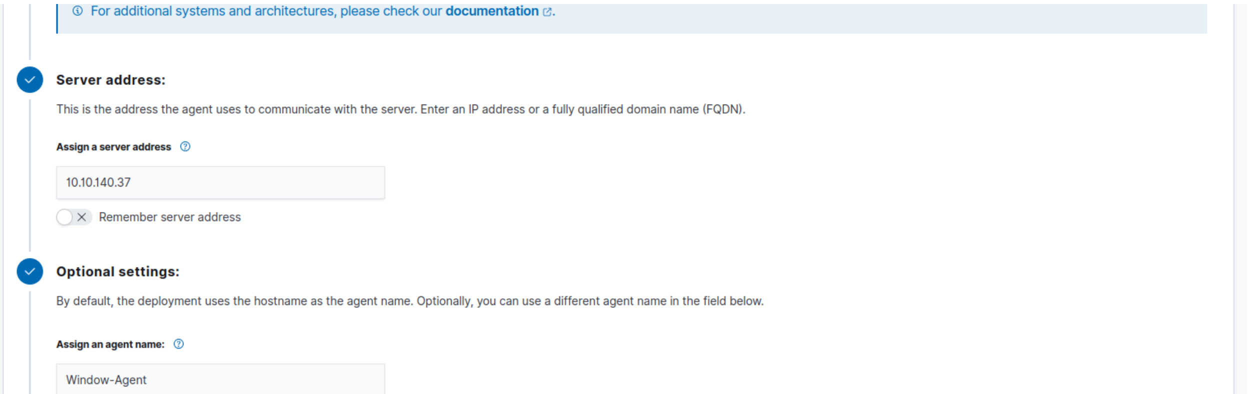
LINUX
○ RPM amd64 ○ RPM aarch64
○ DEB amd64 ○ DEB aarch64

WINDOWS
● MSI 32/64 bits

macOS
○ Intel
○ Apple silicon

For additional systems and architectures, please check our **documentation**.

Now give the Manager IP and also give the agent name.



ⓘ 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

10.10.140.37

Remember server address

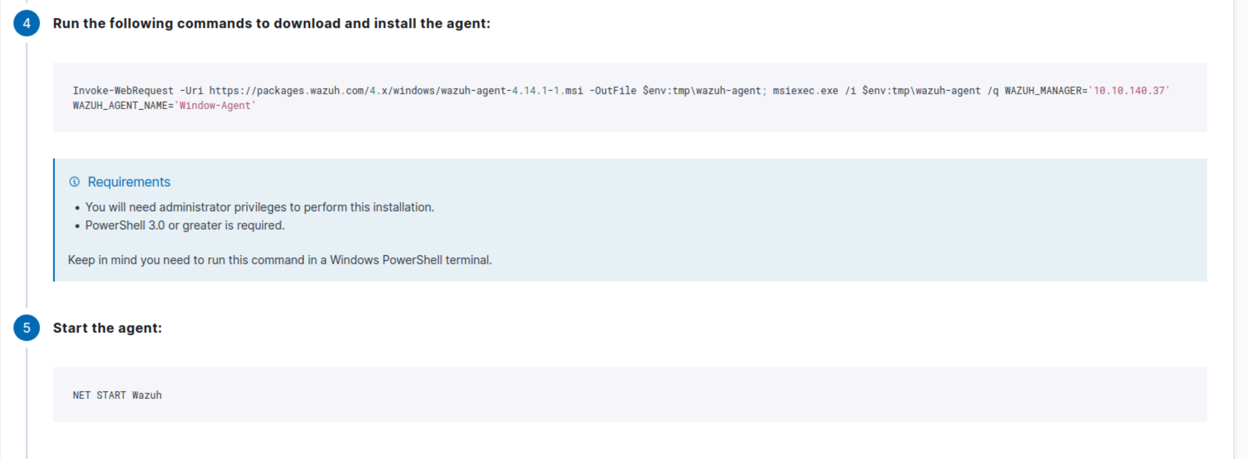
Optional settings:

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:

Window-Agent

Now run the following command on the WindowS Server.



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

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.1-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='10.10.140.37'
WAZUH_AGENT_NAME='Window-Agent'
```

ⓘ Requirements

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

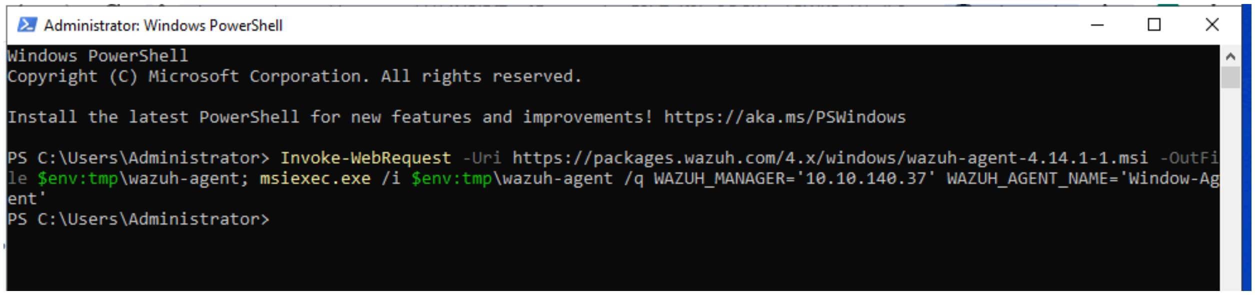
Keep in mind you need to run this command in a Windows PowerShell terminal.

5 **Start the agent:**

```
NET START Wazuh
```

Open the Powershell with administrative privileges and run the following command.

Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.1-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='10.10.140.37' WAZUH_AGENT_NAME='Window-Agent'



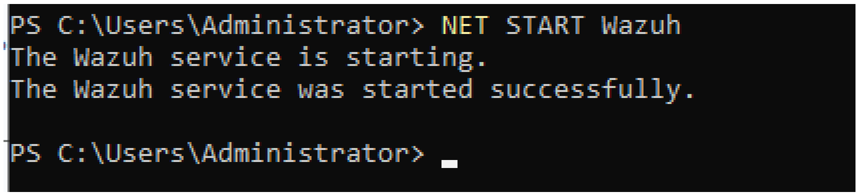
Administrator: Windows PowerShell

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

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

PS C:\Users\Administrator> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.1-1.msi -OutFi
le $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='10.10.140.37' WAZUH_AGENT_NAME='Window-Ag
ent'
PS C:\Users\Administrator>
```

Now run the command given below to start the Agent.
NET START Wazuh

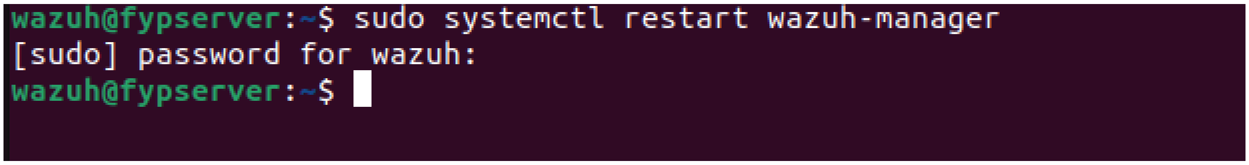


```
PS C:\Users\Administrator> NET START Wazuh
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\Users\Administrator> _
```

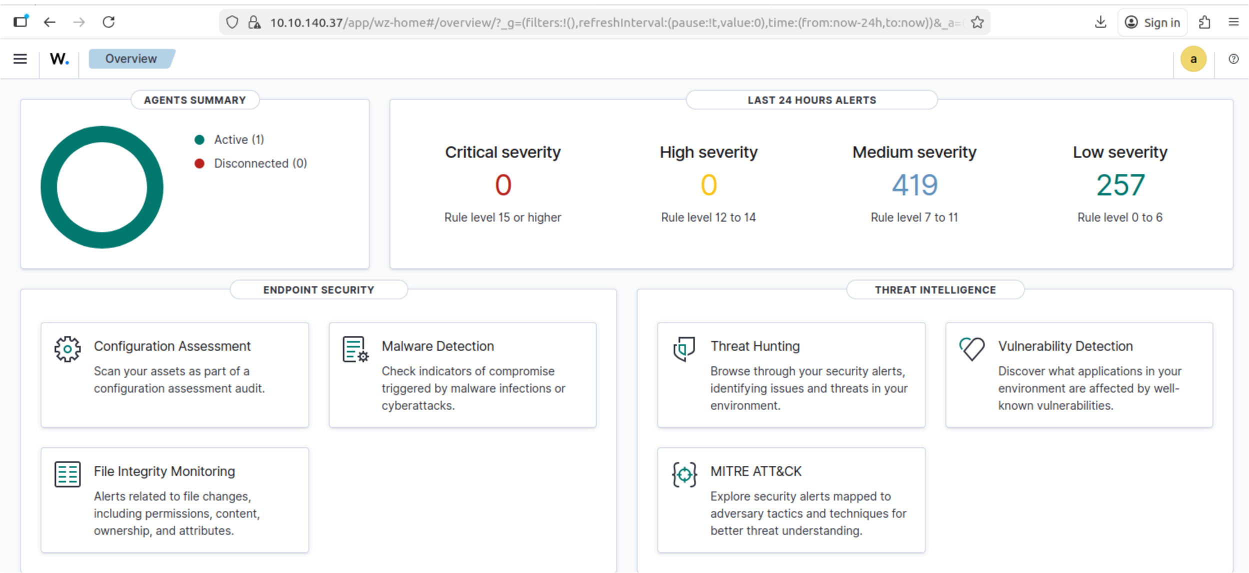
Now restart the Wazuh Manager

Sudo systemctl restart wazuh-manager



```
wazuh@fypserver:~$ sudo systemctl restart wazuh-manager
[sudo] password for wazuh:
wazuh@fypserver:~$
```

After restarting the Wazuh Manager, check the dashboard for a successful Agent connection.



10.10.140.37/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=
Sign in
W.
Overview
a

AGENTS SUMMARY

- Active (1)
- Disconnected (0)

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	419	257
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

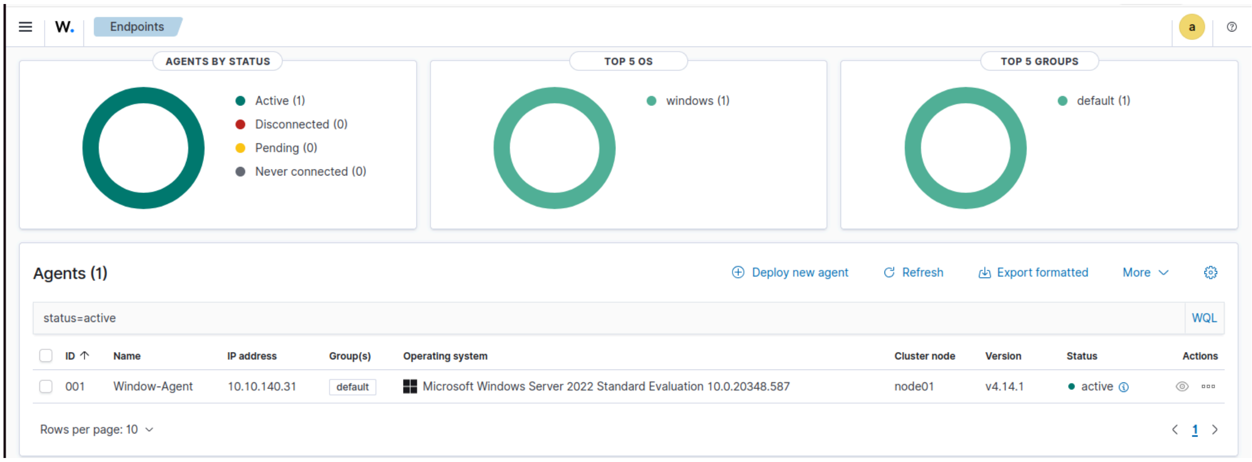
File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

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

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.



AGENTS BY STATUS

- ● Active (1)
- ● Disconnected (0)
- ● Pending (0)
- ● Never connected (0)

TOP 5 OS

- ● windows (1)

TOP 5 GROUPS

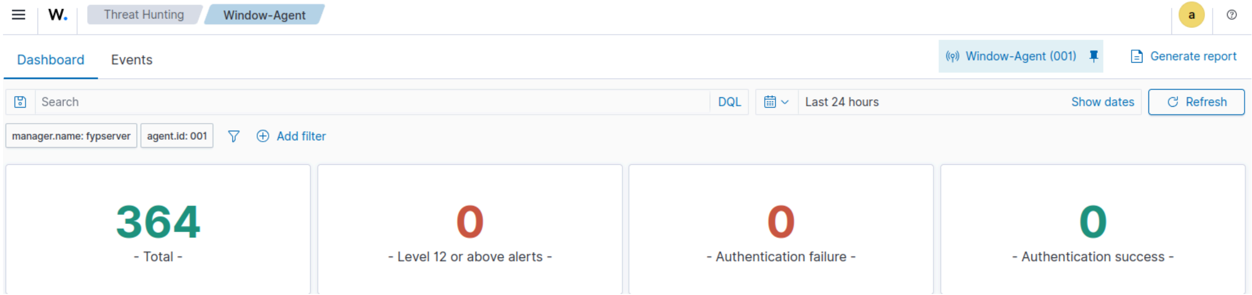
- ● default (1)

Agents (1)

status=active

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Window-Agent	10.10.140.31	default	Microsoft Windows Server 2022 Standard Evaluation 10.0.20348.587	node01	v4.14.1	● active	

We,successfully installed the Wazuh agent and now both are connected.
Windows Agent logs are showing on Wazuh Dashboard.



Last 24 hours

manager.name: fypserver | agent.id: 001

364	0	0	0
- Total -	- Level 12 or above alerts -	- Authentication failure -	- Authentication success -

Summary:

We successfully installed the Wazuh Agent on a Windows machine using the “Deploy new agent” option in the Wazuh Dashboard.
The agent is now connected to the Wazuh Manager and ready to send logs and security data.