Project: Wazuh SIEM on Ubuntu

Name : Vaishnavi Madhav Shinde

Roll No : MH-JM-24-07-0103

Course : Cyber Security Specialist

Guided By : Deepyesh Sir.

Ubuntu server setup :

Start the ubantu

Open your terminal and run the following command

```
# sudo apt update
```

```
# sudo apt upgrade
```

```
# curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
# sudo bash ./wazuh-install.sh -a
```

(show password for wazuh log in copy that password)

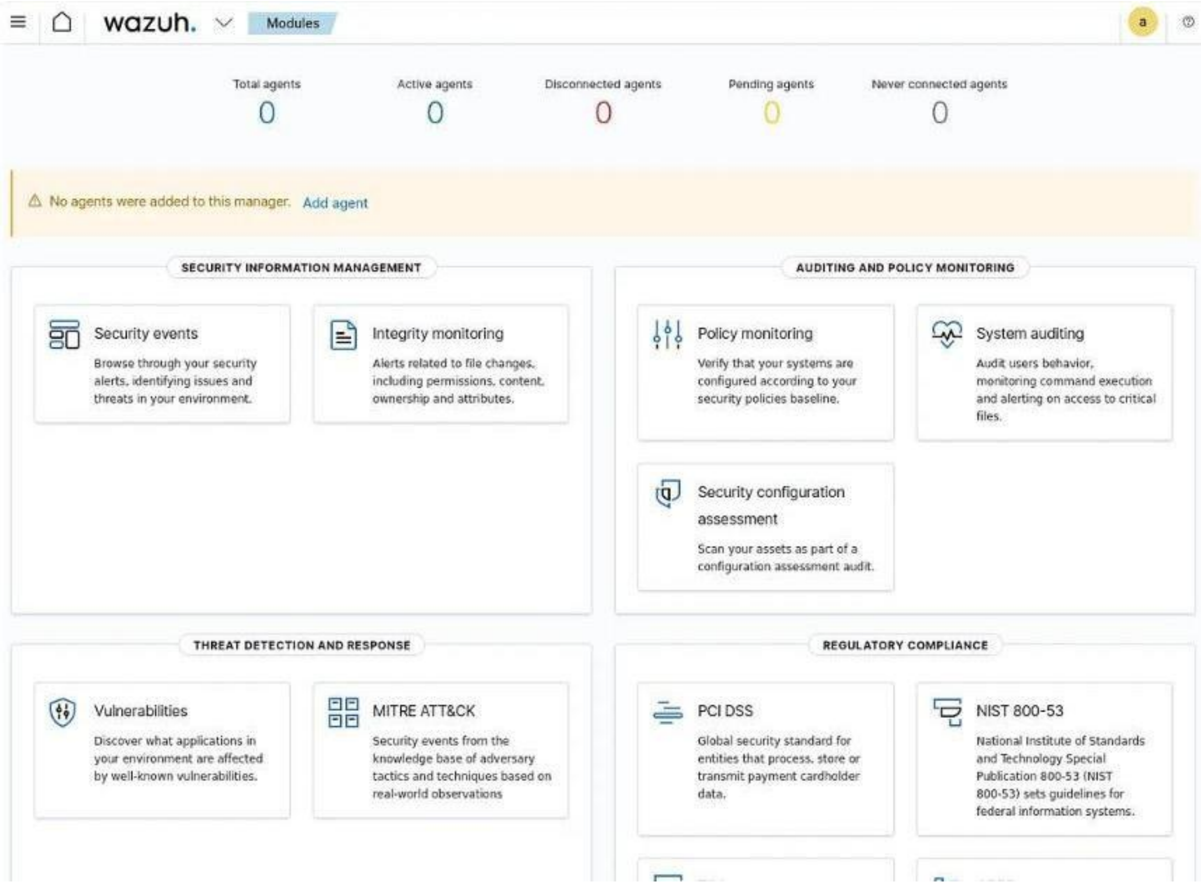
```
# nano user.txt
```

(paste the password)

```
# ss -antlp
```

(showing Linux to display detailed information about active network connections)

The Wazuh server setup has been successfully completed. Retrieve the authentication details displayed in the terminal and store them securely. Open a web browser and enter the server's assigned IP address in the URL bar. Establish a secure connection to the Wazuh dashboard by visiting https://your_server_ip, then log in using the provided credentials to access the system's security monitoring and management interface.



Total agents	Active agents	Disconnected agents	Pending agents	Never connected agents
0	0	0	0	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.

Starting the Wazuh dashboard service :

Enable and start the Wazuh dashboard service

```
# systemctl daemon-reload
```

```
# systemctl enable wazuh-dashboard
```

```
# systemctl start wazuh-dashboard
```

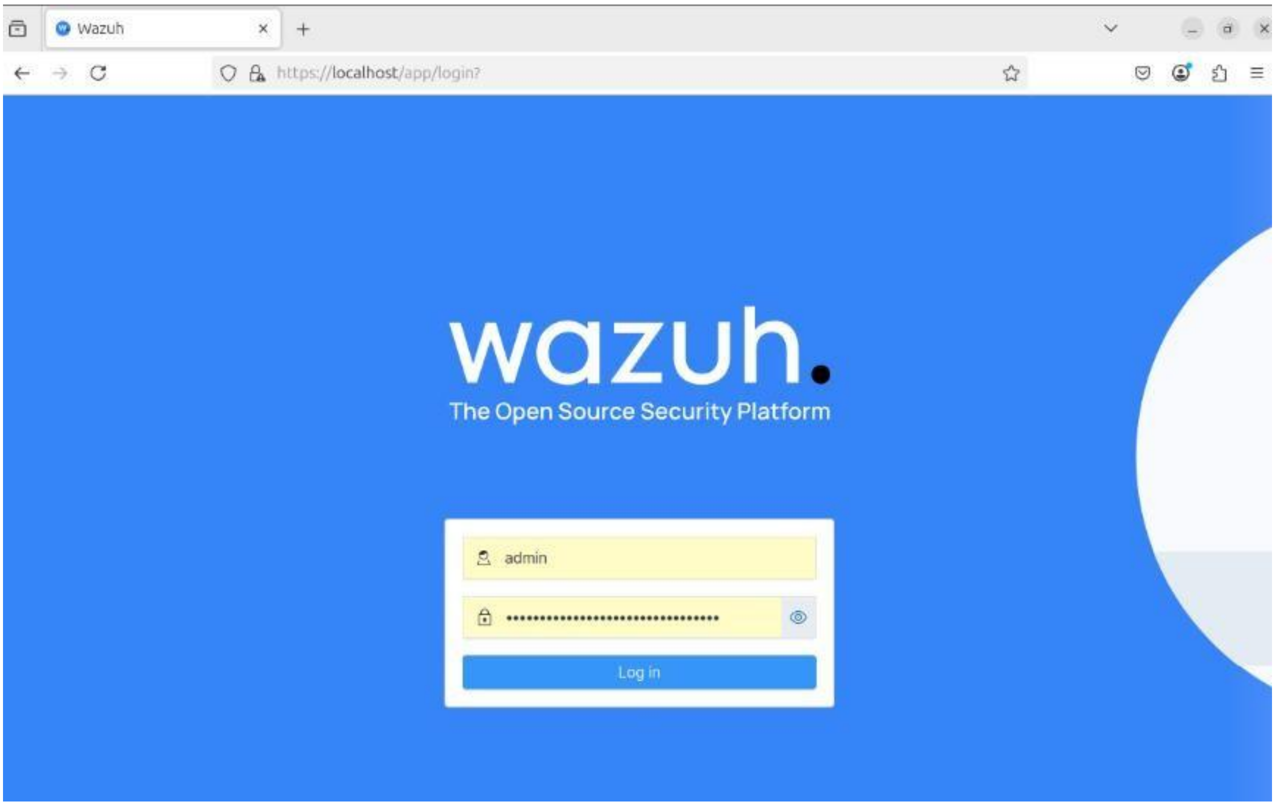
Access the Wazuh web interface with your credentials

URL: https://<wazuh-dashboard-ip>

Username: admin

Password: (paste password from

nano user.txt file)


Wazuh

https://localhost/app/login?

wazuh.

The Open Source Security Platform

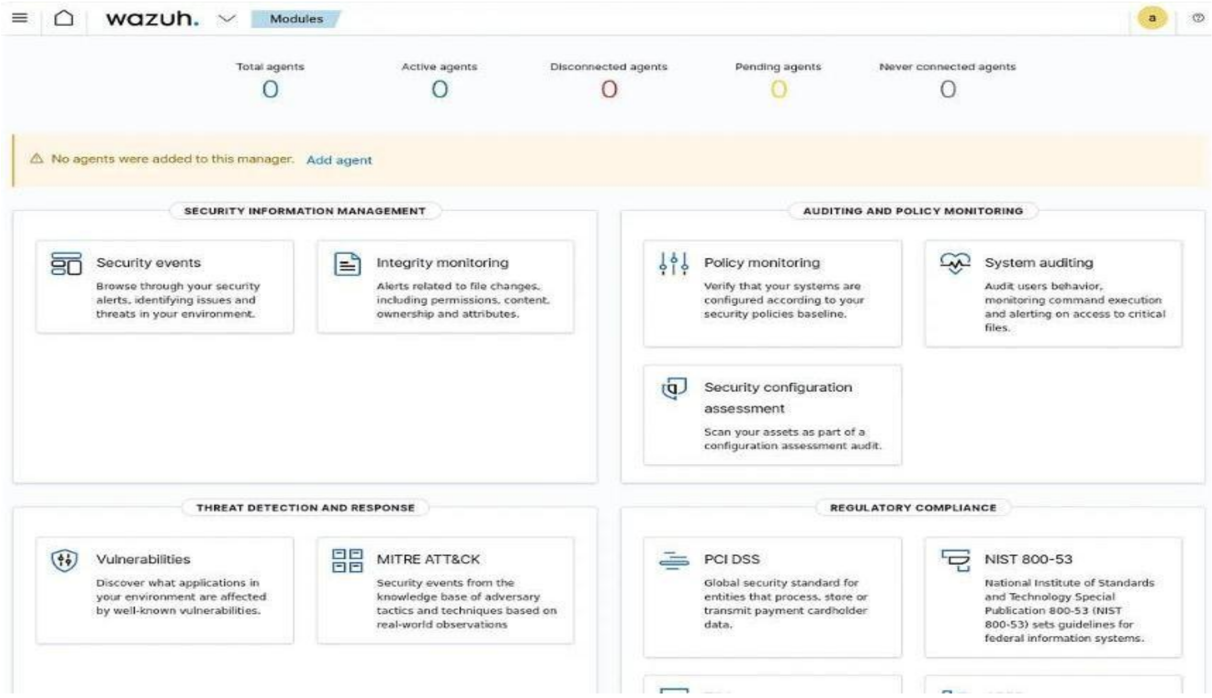
admin

••••••••••••••••••••••••••••••••

Log in

Adding agents :

Wazuh default page



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

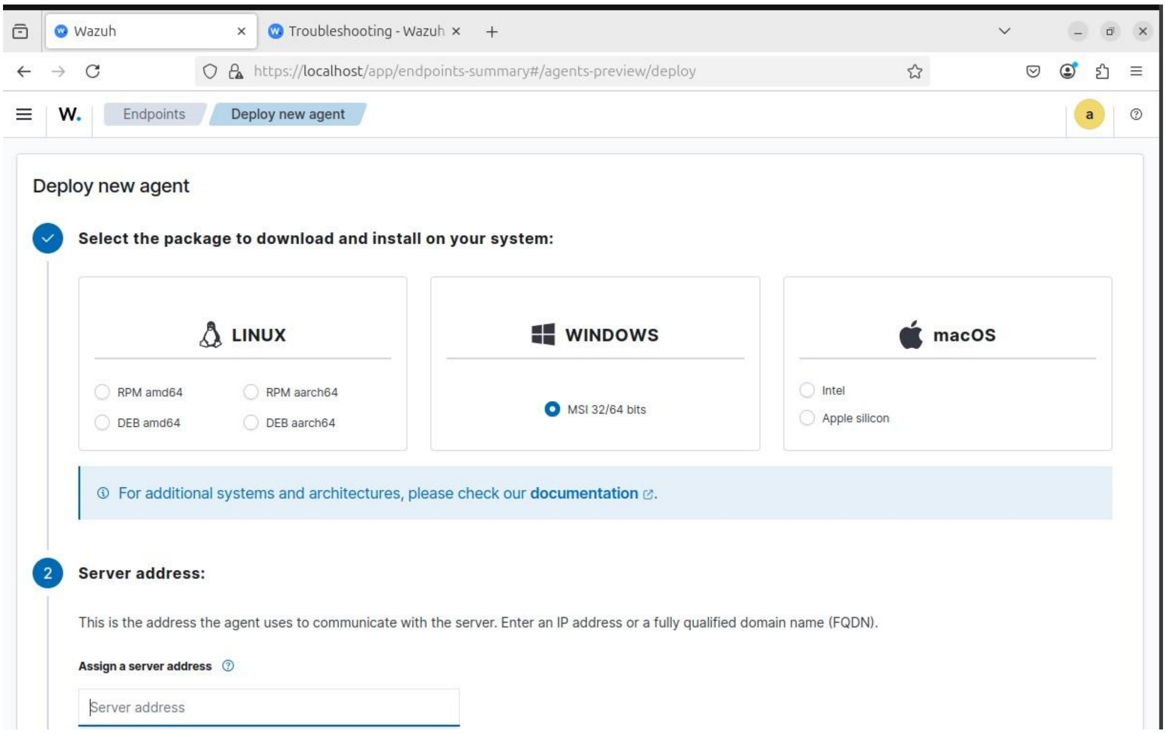
PCI DSS
Global security standard for entities that process, store or transmit payment cardholder data.

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

Add our first agent - Windows Agent.

Click **Add agent**, showing in the image below

Select the agent platform - windows in this case, and enter the wazuh server IP address


Wazuh
Troubleshooting - Wazuh
https://localhost/app/endpoints-summary#/agents-preview/deploy
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**.

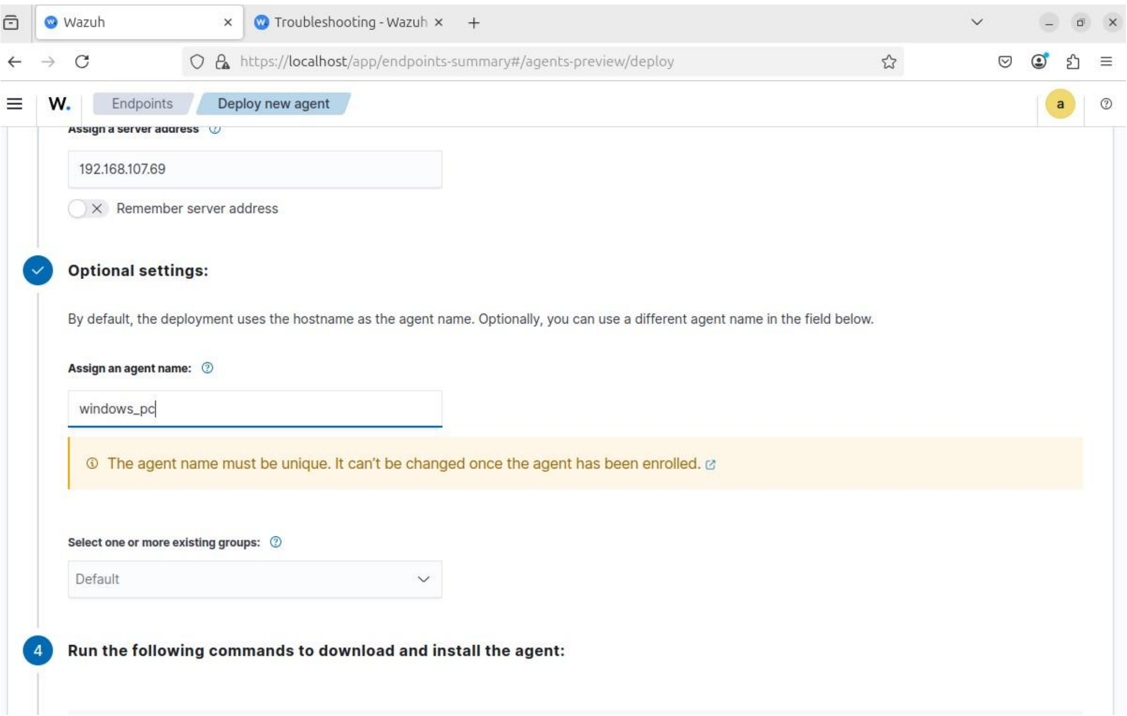
2 Server address:

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

Server address

Assign a name to a agent


Wazuh
Troubleshooting - Wazuh
https://localhost/app/endpoints-summary#/agents-preview/deploy
W.
Endpoints
Deploy new agent
a

Assign a server address

192.168.107.69

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:

windows_pc

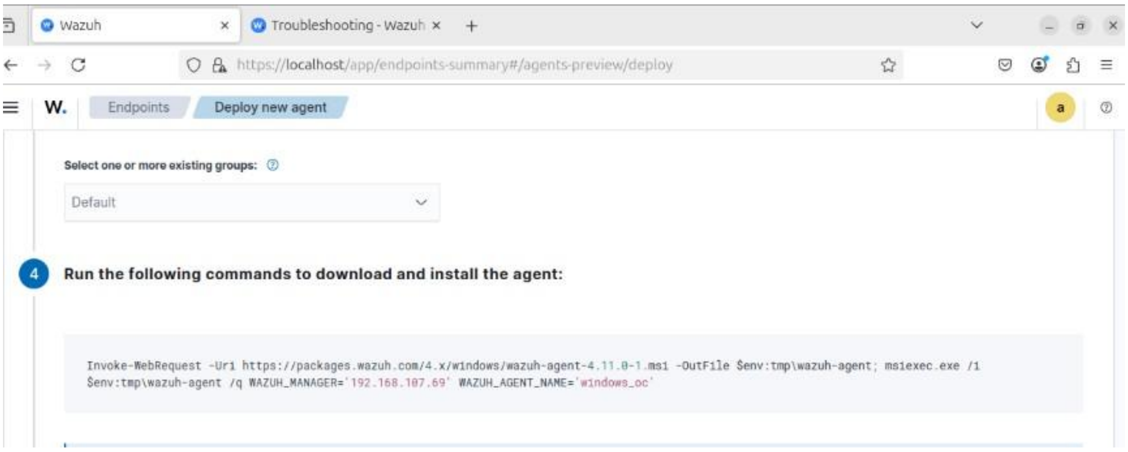
The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups:

Default

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

Copy the powershell command


Wazuh
Troubleshooting - Wazuh
https://localhost/app/endpoints-summary#/agents-preview/deploy
W.
Endpoints
Deploy new agent
a

Select one or more existing groups:

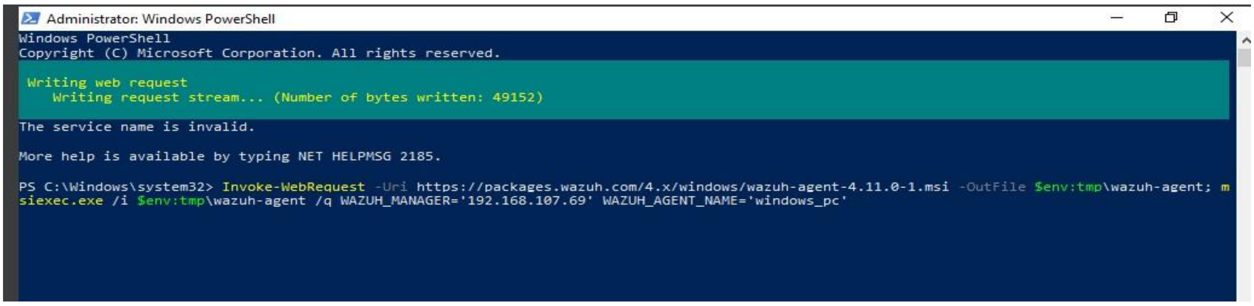
Default

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

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.11.0-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i
$env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.107.69' WAZUH_AGENT_NAME='windows_oc'
```

Start the window

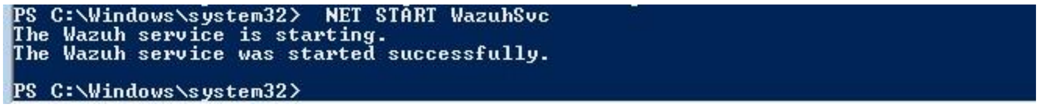
Open Powershell as administrator



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

 Writing web request
    Writing request stream... (Number of bytes written: 49152)
The service name is invalid.

More help is available by typing NET HELPMSG 2185.

PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.11.0-1.msi -OutFile $env:tmp\wazuh-agent; m
siexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.107.69' WAZUH_AGENT_NAME='windows_pc'
```

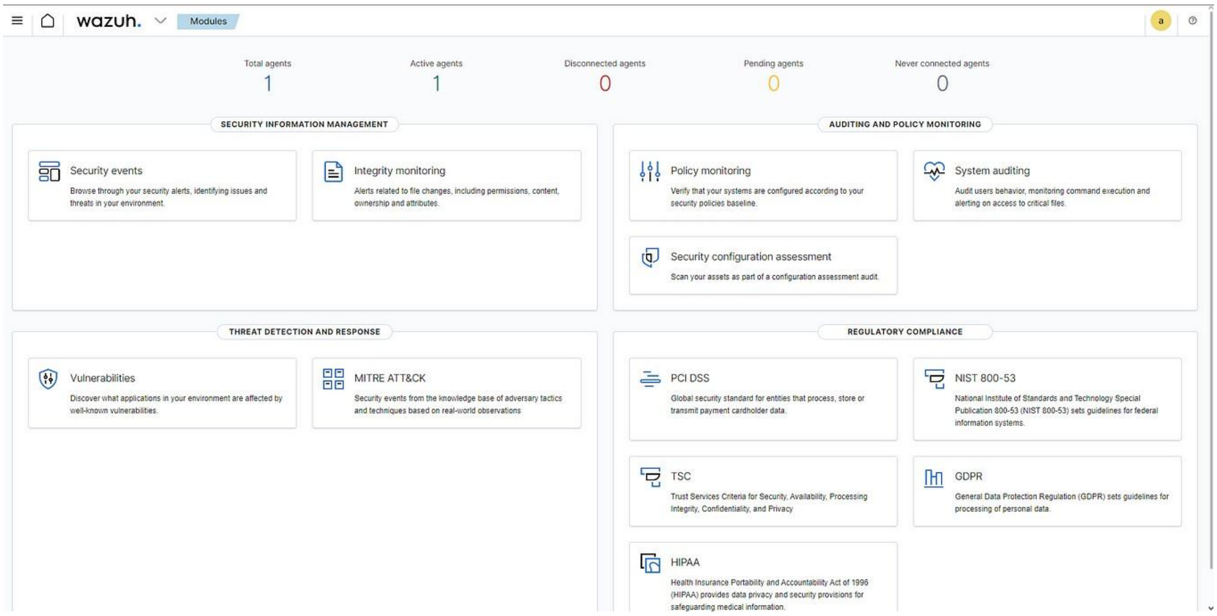
Then start the wazuh service

# NET START WazuhSvc



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

PS C:\Windows\system32>
```

The agent should show up as connected on the dashboard



Total agents	Active agents	Disconnected agents	Pending agents	Never connected agents
1	1	0	0	0

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.

HIPAA
Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security provisions for safeguarding medical information.

Wazuh SIEM has been successfully installed and configured. This setup allows for real-time security monitoring, log analysis, and intrusion detection. Your Wazuh Manager is actively gathering and analyzing logs from multiple systems. The Wazuh Dashboard offers valuable insights into security incidents and vulnerabilities. To maintain optimal performance, ensure consistent monitoring and updates. Your system is now more secure against potential threats!