Q.What is an SIEM tool and its role in Cyber security

SIEM is a Security Information and Event Management. It is a system that aggregates log files, security alerts and intrusion prevention systems in one place. So, the security team can analyze the data more easily.

SIEM collects all the information from other security systems like endpoint security and firewall.

Logs and alerts from the system need to be stored centrally so that analysts do not have to visit each individual security product to investigate.

SIEM offers powerful log search features, the ability to trigger alerts using rules and reports that organizations can provide by auditors.

SIEM solutions can generate real time compliance reports for things like general data protection regulation(GDPR), Health Insurance Portability and Accountability Act (HIPPA).

SIEM can help to automate the Security Operation Center (SOC). SOC are looking to automate, make their operation more efficient and reduce their overall risk.

.

WAZUH

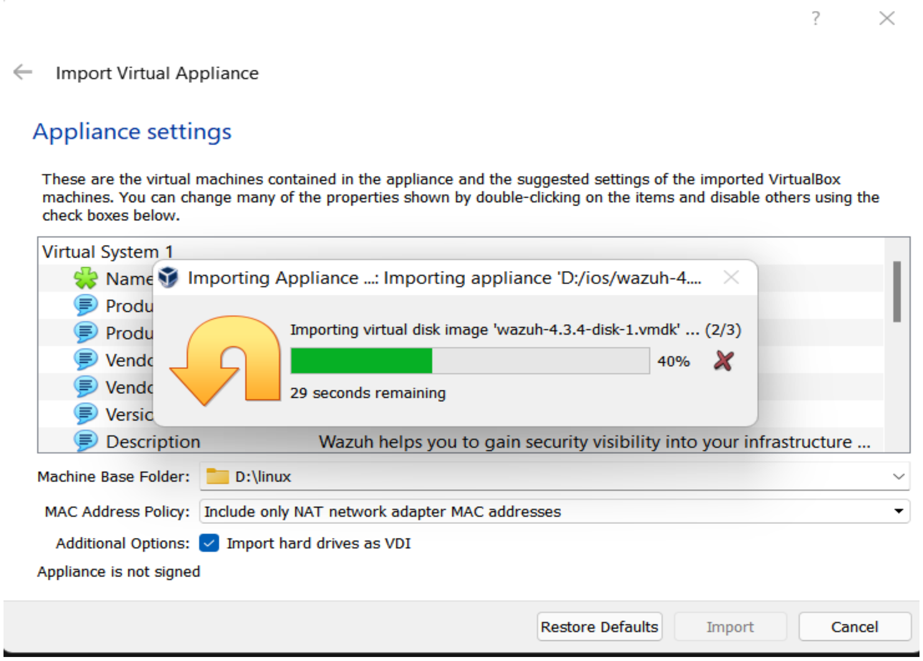
Go to https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html

Click this link https://packages.wazuh.com/4.x/vm/wazuh-4.3.4.ova to download the virtual machine.

Open downloaded file with VirtualBox by right click and **open with VirtualBox** .

It will automatically set according to their requirement and then click on **import** to proceed.

After installing, the machine has to be started.



Import Virtual Appliance

Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Importing Appliance ...: Importing appliance 'D:/ios/wazuh-4....

Importing virtual disk image 'wazuh-4.3.4-disk-1.vmdk' ... (2/3)

40%

29 seconds remaining

Description: Wazuh helps you to gain security visibility into your infrastructure ...

Machine Base Folder: D:\linux

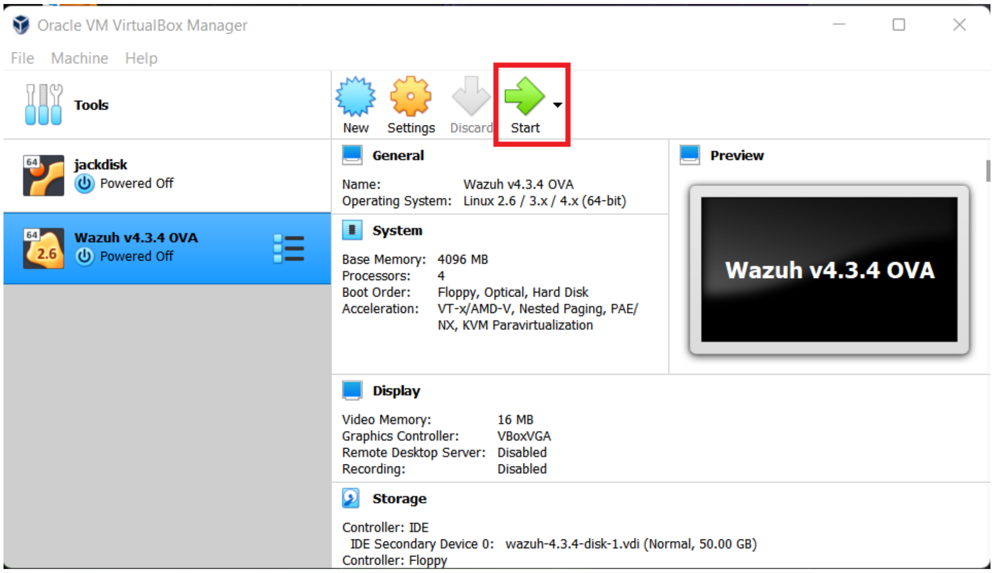
MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: ☑ Import hard drives as VDI

Appliance is not signed

Let's start to see the machine terminal and determine the IP where we will reach wazuh web interface.

So the virtual machine is booting up.



General

Name: Wazuh v4.3.4 OVA
Operating System: Linux 2.6 / 3.x / 4.x (64-bit)

System

Base Memory: 4096 MB
Processors: 4
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

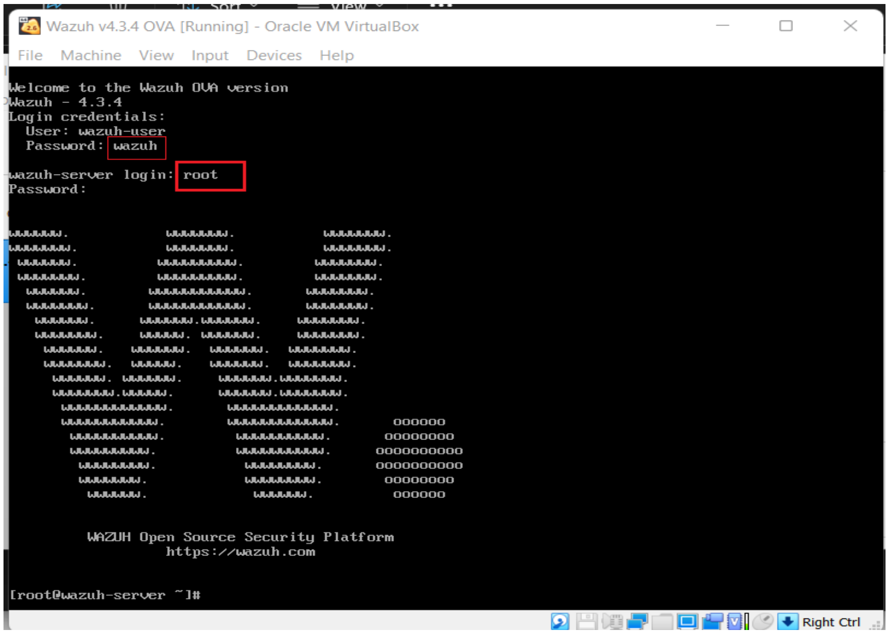
Display

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

Storage

Controller: IDE
IDE Secondary Device 0: wazuh-4.3.4-disk-1.vdi (Normal, 50.00 GB)
Controller: Floppy

The wazuh-server login is ' root' and the password is ' wazuh ' which was mentioned in the documentation.



Wazuh v4.3.4 OVA [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

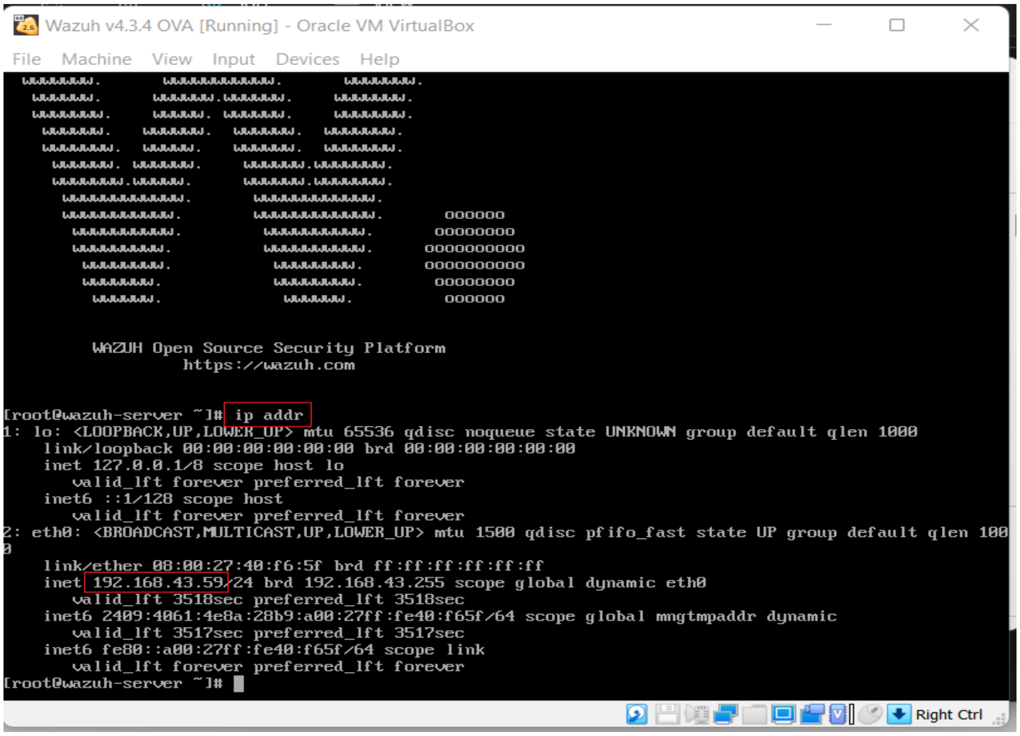
```
Welcome to the Wazuh OVA version
Wazuh - 4.3.4
Login credentials:
  User: wazuh-user
  Password: wazuh

wazuh-server login: root
Password:

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

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

Once logged in we can determine the IP address of the system by typing in' ip addr '. I note that the IP address in this case will be ' 192.168.43.59 ‘

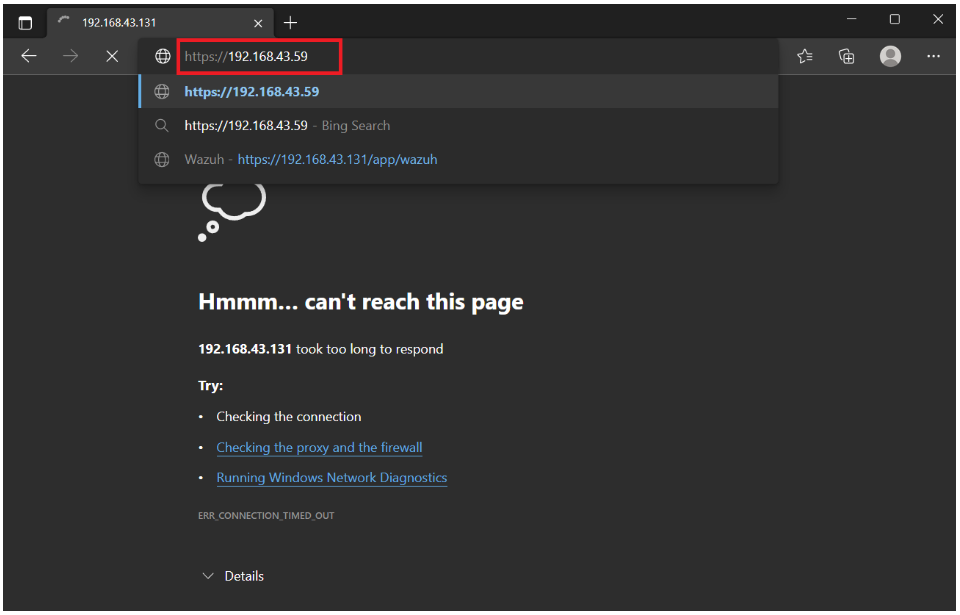


Wazuh v4.3.4 OVA [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

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

[root@wazuh-server ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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 group default qlen 100
0
    link/ether 08:00:27:40:f6:5f brd ff:ff:ff:ff:ff:ff
    inet 192.168.43.59/24 brd 192.168.43.255 scope global dynamic eth0
       valid_lft 3518sec preferred_lft 3518sec
    inet6 2409:4061:4e8a:28b9:a00:27ff:fe40:f65f/64 scope global mngtmpaddr dynamic
       valid_lft 3517sec preferred_lft 3517sec
    inet6 fe80::a00:27ff:fe40:f65f/64 scope link
       valid_lft forever preferred_lft forever
[root@wazuh-server ~]#
```

Then we need to press the right control key to release our mouse pointer. We can then direct our browser to access the Web Interface at ' https://192.168.43.59 '.



192.168.43.131
https://192.168.43.59
https://192.168.43.59
https://192.168.43.59 - Bing Search
Wazuh - https://192.168.43.131/app/wazuh

Hmmm... can't reach this page

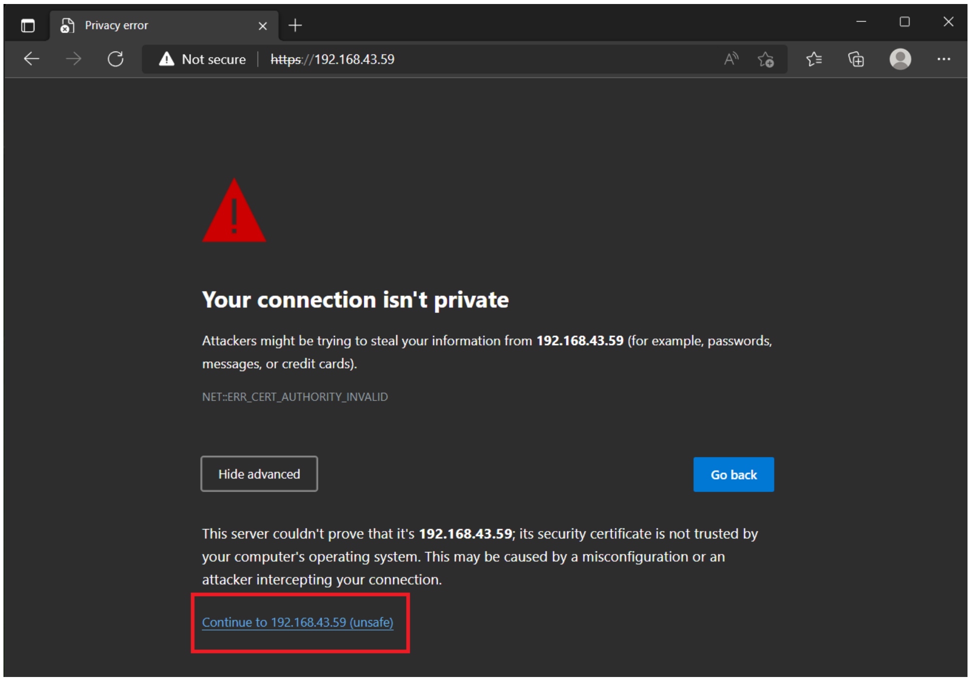
192.168.43.131 took too long to respond

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

There will be a warning that the certificate used by the OVA is not signed by a trusted authority. We ignore and **continue to 192.168.43.59(unsafe)** for testing purposes.



Your connection isn't private

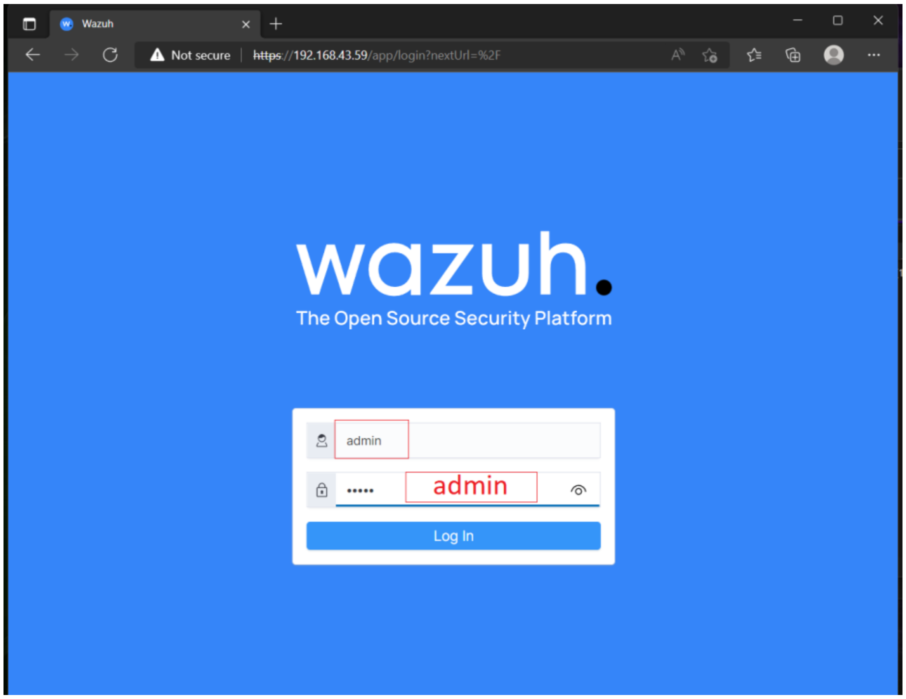
Attackers might be trying to steal your information from **192.168.43.59** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

This server couldn't prove that it's **192.168.43.59**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Continue to 192.168.43.59 (unsafe)

Then here on the web page, we will have to give the user ID and password.
User id - **admin** and Password- **admin.**

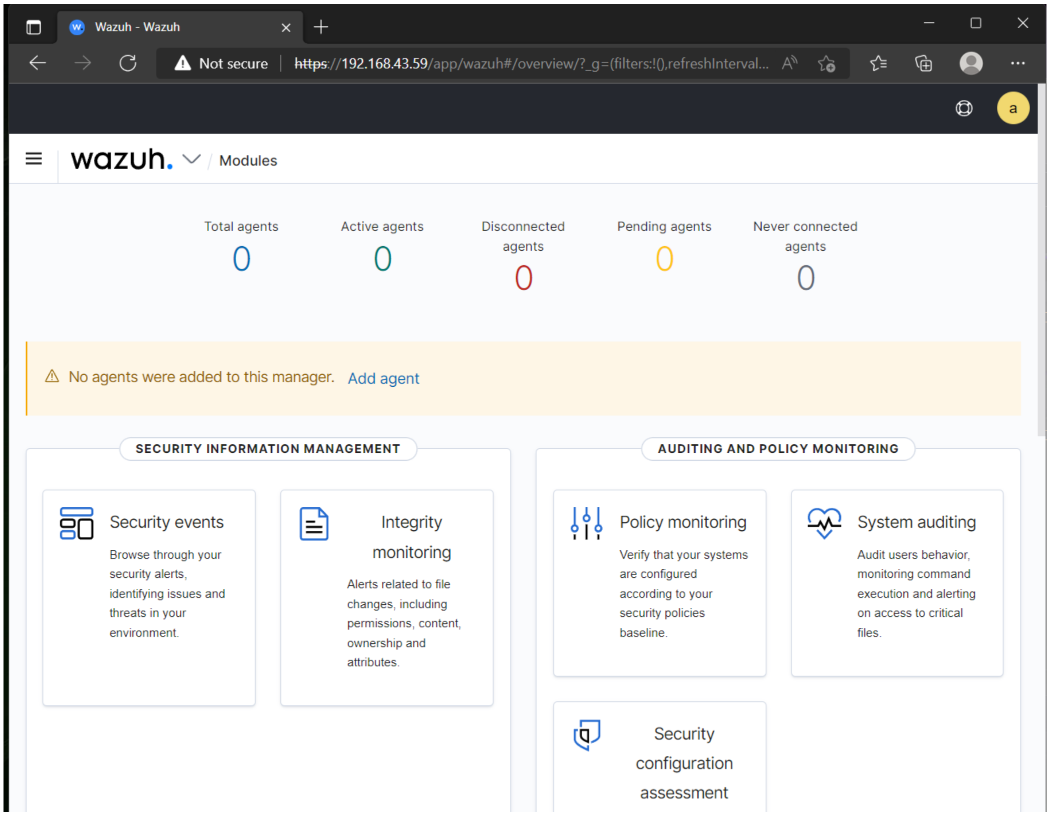


https://192.168.43.59/app/login?nextUrl=%2F

admin

••••• admin

The web page will now load the Kibana Web Interface and on the left-hand column,we will find the Wazuh icon that will take us to the Wazuh Web Interface with Kibana.



https://192.168.43.59/app/wazuh#/overview/?_g=(filters:!(),refreshInterval...

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.

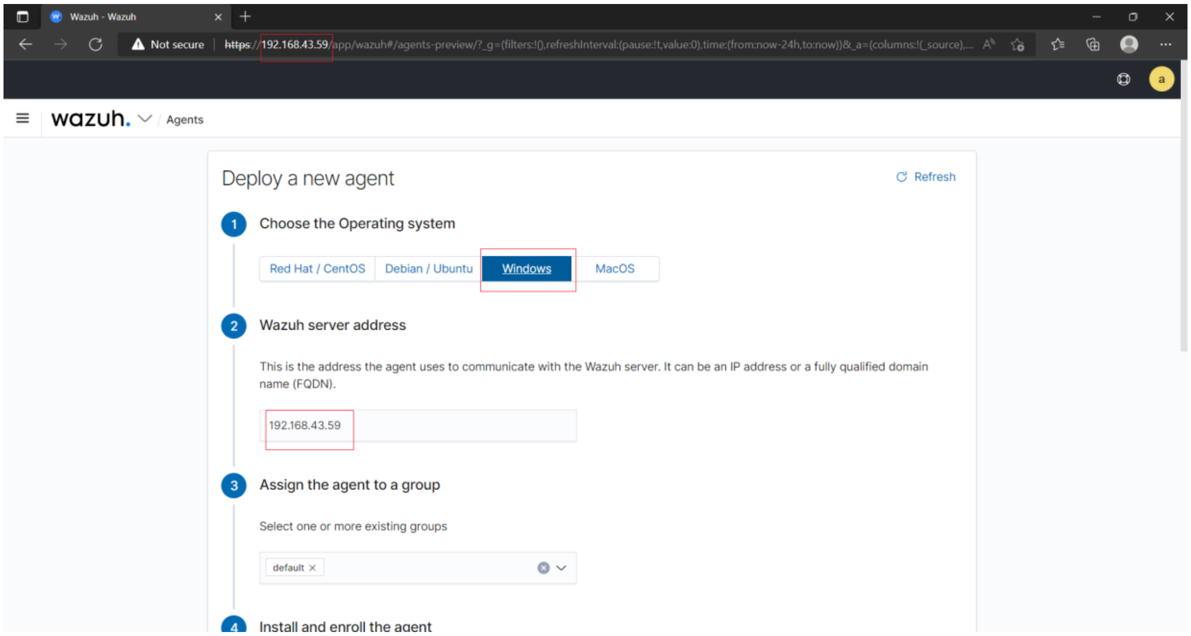
AUDITING AND POLICY MONITORING

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

There we will have access to the dashboard of the Wazuh. We can see that no agents have been registered to this manager. If we click on the **Add agents** link or on the Agent tab. We will be directed to the interface which will provide guidance on how to deploy Wazuh agents on several operating systems .


Wazuh - Wazuh
Not secure
https://192.168.43.59/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),...
wazuh.
Agents
Refresh

Deploy a new agent

1 Choose the Operating system

Red Hat / CentOS | Debian / Ubuntu | Windows | MacOS

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).

192.168.43.59

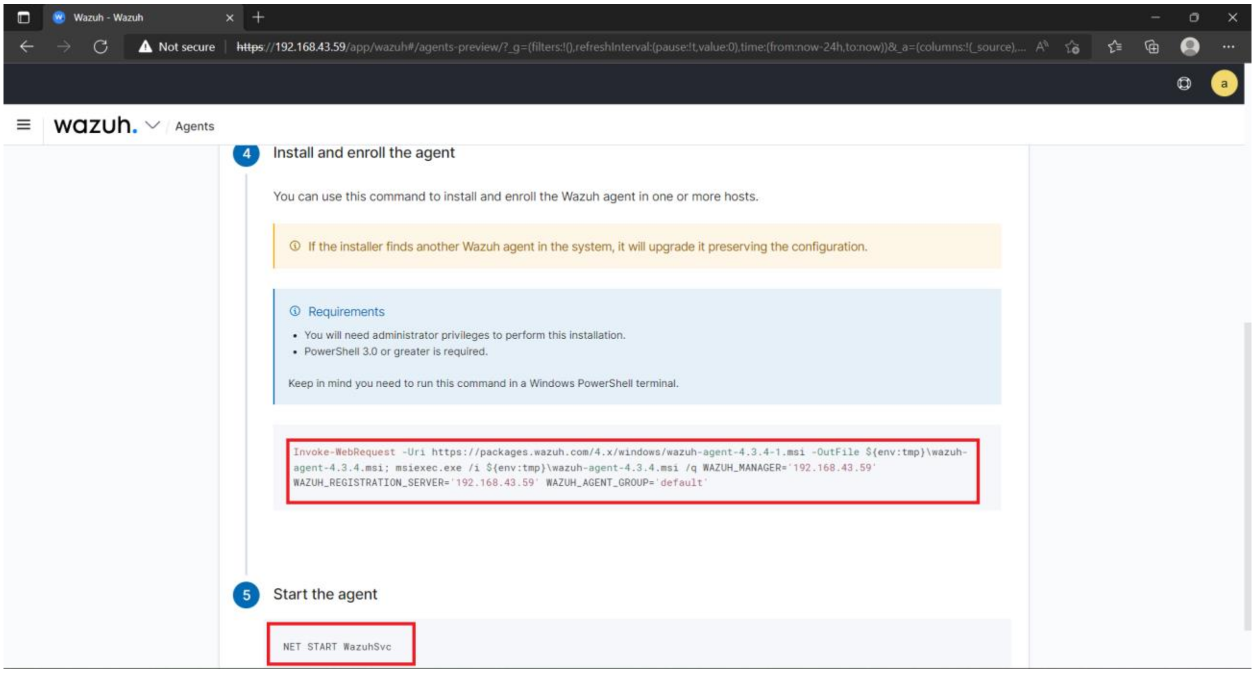
3 Assign the agent to a group

Select one or more existing groups

default ×

4 Install and enroll the agent

We can select Windows and provide the IP address where we can find the Wazuh manager. This will provide us with a command that we can copy and paste onto our systems to download, install, register and configure the Wazuh agent without any further interaction.


Wazuh - Wazuh
Not secure
https://192.168.43.59/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),...
wazuh.
Agents

4 Install and enroll the agent

You can use this command to install and enroll the Wazuh agent in one or more hosts.

ⓘ 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.

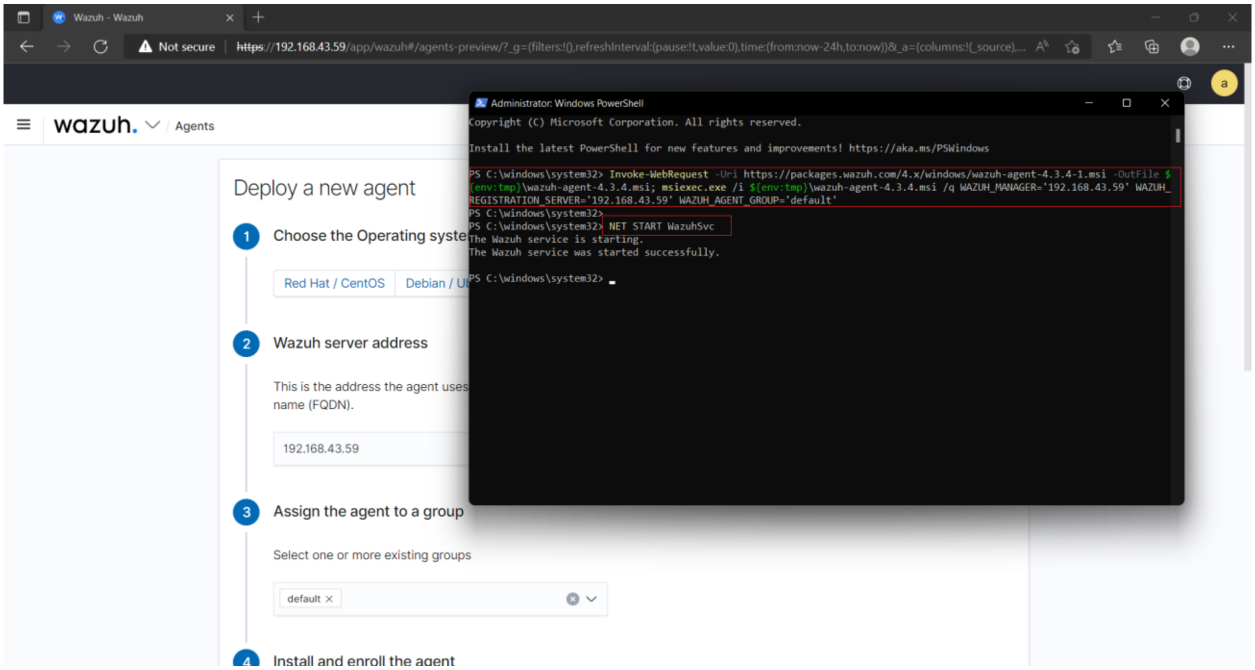
Keep in mind you need to run this command in a Windows PowerShell terminal.

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.4-1.msi -OutFile ${env:tmp}\wazuh-agent-4.3.4.msi; msiexec.exe /i ${env:tmp}\wazuh-agent-4.3.4.msi /q WAZUH_MANAGER='192.168.43.59' WAZUH_REGISTRATION_SERVER='192.168.43.59' WAZUH_AGENT_GROUP='default'
```

5 Start the agent

```
NET START WazuhSvc
```

Let's bring a terminal with Windows11 machine and paste that command into it to see how it works.Just hit enter and confirm the action, it's as simple as that.


Wazuh - Wazuh
Not secure
https://192.168.43.59/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),...
wazuh.
Agents
Administrator: Windows PowerShell

Deploy a new agent

1 Choose the Operating syste

Red Hat / CentOS | Debian / U

2 Wazuh server address

This is the address the agent uses ... name (FQDN).

192.168.43.59

3 Assign the agent to a group

Select one or more existing groups

default ×

4 Install and enroll the agent

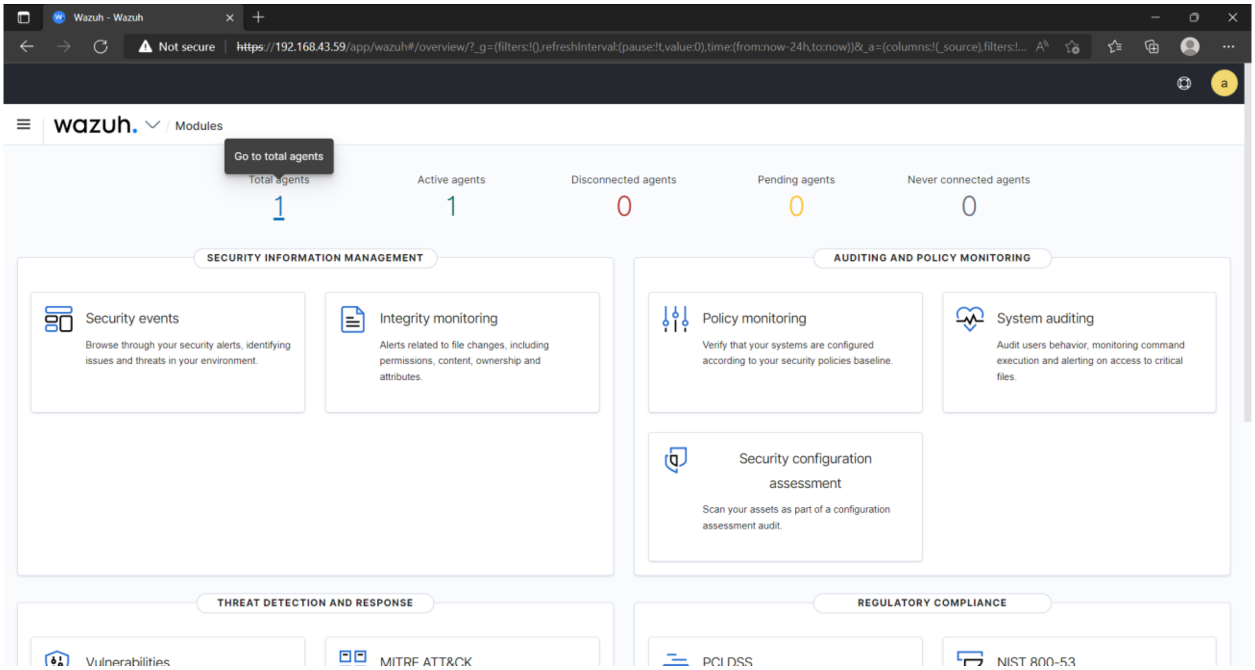
```
Copyright (C) Microsoft Corporation. All rights reserved.

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-4.3.4-1.msi -OutFile ${env:tmp}\wazuh-agent-4.3.4.msi; msiexec.exe /i ${env:tmp}\wazuh-agent-4.3.4.msi /q WAZUH_MANAGER='192.168.43.59' WAZUH_REGISTRATION_SERVER='192.168.43.59' WAZUH_AGENT_GROUP='default'
PS C:\windows\system32>
PS C:\windows\system32> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\windows\system32> _
```

This works not only on Windows but also on centOS, MacOS, another Linux system. We can now reload the agents tab to see our newly registered endpoint being monitored.


Wazuh - Wazuh
Not secure
https://192.168.43.59/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!...
wazuh.
Modules
Go to total agents

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

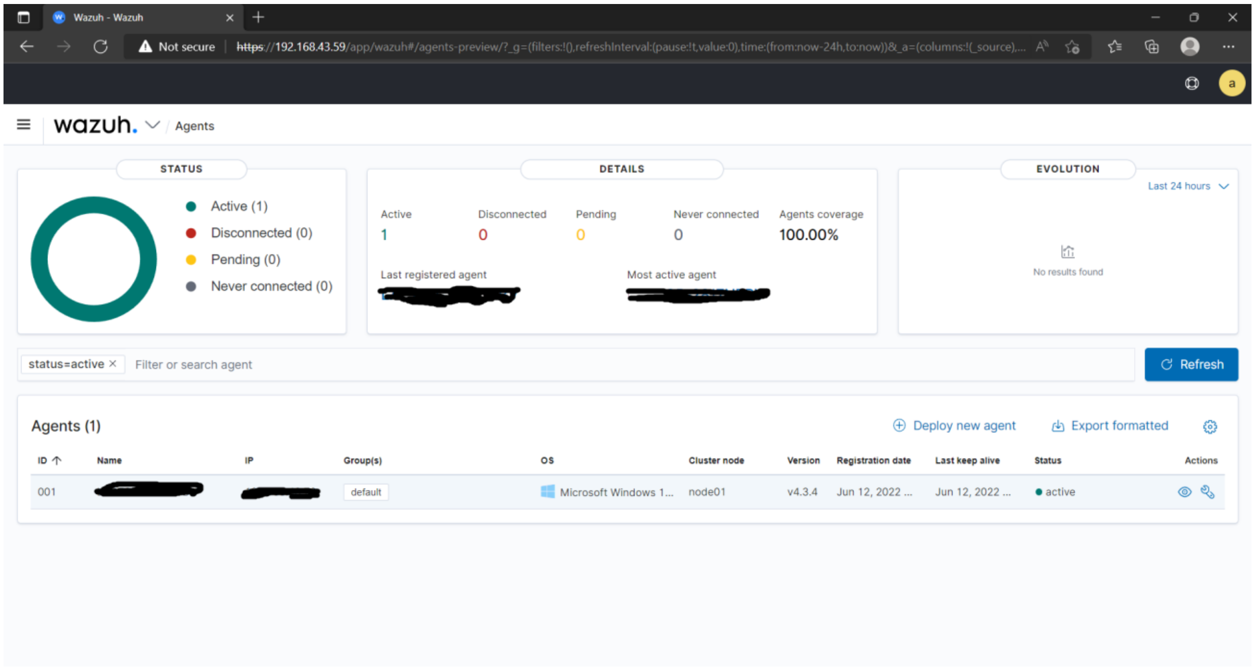
Vulnerabilities

MITRE ATT&CK

REGULATORY COMPLIANCE

PCI DSS

NIST 800-53



Wazuh - Wazuh

Not secure | https://192.168.43.59/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),...

wazuh. / Agents

STATUS

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

DETAILS

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

Last registered agent [redacted]

Most active agent [redacted]

EVOLUTION

Last 24 hours

No results found

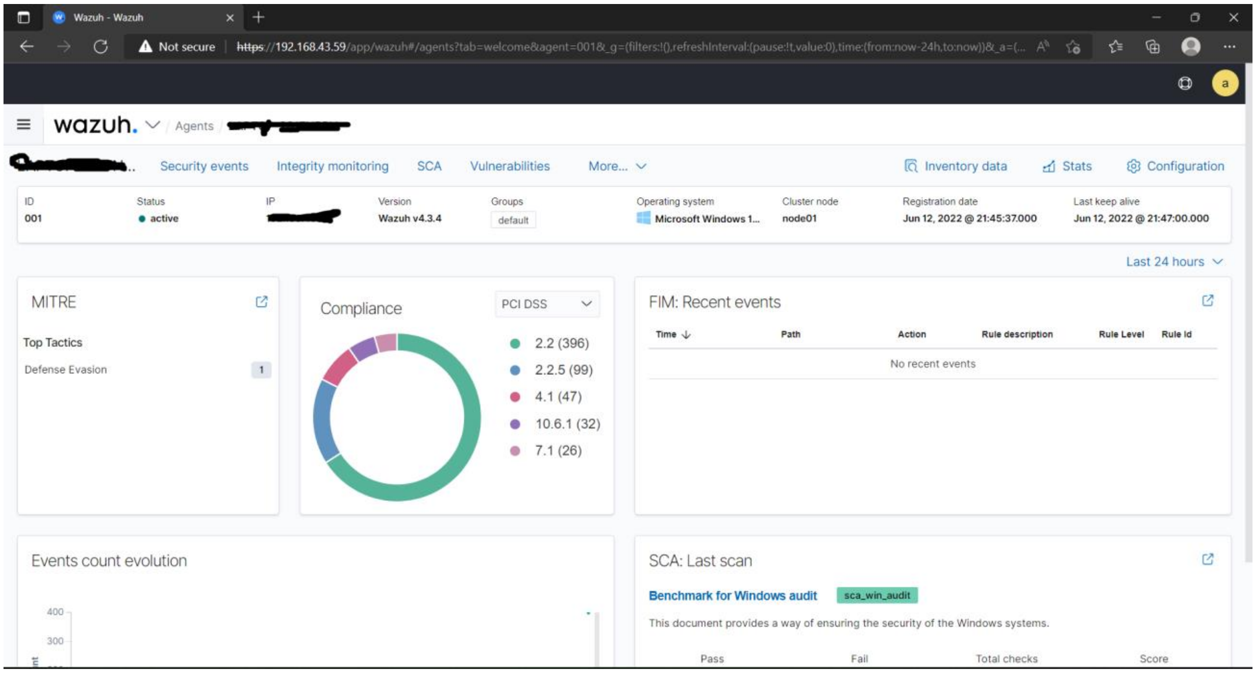
status=active × Filter or search agent

Refresh

Agents (1)

Deploy new agent Export formatted

ID	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status	Actions
001	[redacted]	[redacted]	default	Microsoft Windows 1...	node01	v4.3.4	Jun 12, 2022 ...	Jun 12, 2022 ...	● active	



Wazuh - Wazuh

Not secure | https://192.168.43.59/app/wazuh#/agents?tab=welcome&agent=001&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(...

wazuh. / Agents / [redacted]

[redacted] Security events Integrity monitoring SCA Vulnerabilities More... Inventory data Stats Configuration

ID	Status	IP	Version	Groups	Operating system	Cluster node	Registration date	Last keep alive
001	● active	[redacted]	Wazuh v4.3.4	default	Microsoft Windows 1...	node01	Jun 12, 2022 @ 21:45:37.000	Jun 12, 2022 @ 21:47:00.000

Last 24 hours

MITRE

Top Tactics

Defense Evasion	1

Compliance

PCI DSS

- ● 2.2 (396)
- ● 2.2.5 (99)
- ● 4.1 (47)
- ● 10.6.1 (32)
- ● 7.1 (26)

FIM: Recent events

Time	Path	Action	Rule description	Rule Level	Rule Id

No recent events

Events count evolution

SCA: Last scan

Benchmark for Windows audit sca_win_audit

This document provides a way of ensuring the security of the Windows systems.

Pass	Fail	Total checks	Score

We can then explore the interfaces by going on to overview and select a dashboard to visualize the events being logged by the system. If we go to discover more we may see all the details of any of the registered events.

Click "Agents" to view your agents.
Click "Overview" and then click "Security Events" to view the agent's monitoring events.
Click "Discover" to review any registered events.