Cybersecurity Operations

Mini-Project Guide

This guide provide step by step the deployment of a security solution Wazuh.

Wazuh, The Open-Source Security Platform.

Wazuh is a free, open source and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response and compliance management.

Hardware requirements.

The following requirements have to be in place before the Wazuh VM can be imported into a host operating system:

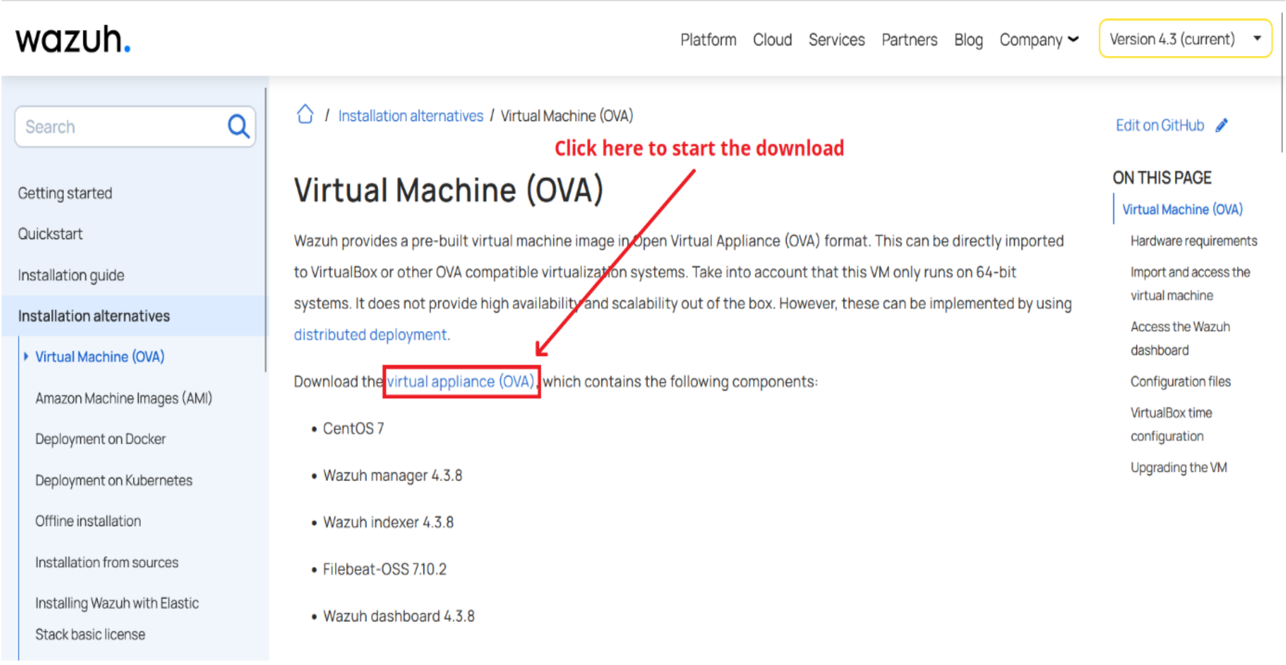
1- The host operating system has to be a 64-bit system.
2- Hardware virtualization has to be enabled on the firmware of the host.
3- A virtualization platform, such as VirtualBox, should be installed.

The Wazuh VM is configured with the following specifications:

CPU : 4 cores
RAM : 8 GB
Storage: 50 GB

1. Installation

1- Download the latest version of Wazuh from the link below: https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html



Click here to start the download

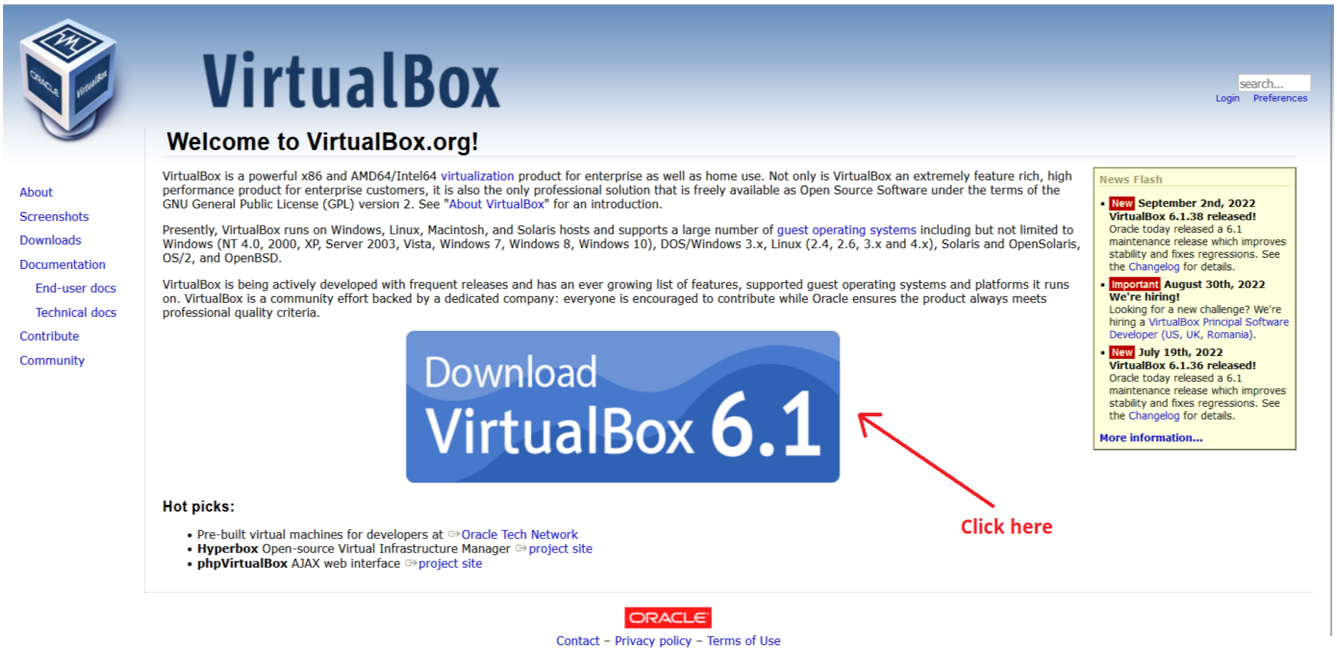
Virtual Machine (OVA)

Wazuh provides a pre-built virtual machine image in Open Virtual Appliance (OVA) format. This can be directly imported to VirtualBox or other OVA compatible virtualization systems. Take into account that this VM only runs on 64-bit systems. It does not provide high availability and scalability out of the box. However, these can be implemented by using distributed deployment.

Download the virtual appliance (OVA), which contains the following components:

- CentOS 7
- Wazuh manager 4.3.8
- Wazuh indexer 4.3.8
- Filebeat-OSS 7.10.2
- Wazuh dashboard 4.3.8

2- Download the latest version of VirtualBox from the link below: https://www.virtualbox.org



Welcome to VirtualBox.org!

VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. Not only is VirtualBox an extremely feature rich, high performance product for enterprise customers, it is also the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 2. See "About VirtualBox" for an introduction.

Presently, VirtualBox runs on Windows, Linux, Macintosh, and Solaris hosts and supports a large number of guest operating systems including but not limited to Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x and 4.x), Solaris and OpenSolaris, OS/2, and OpenBSD.

VirtualBox is being actively developed with frequent releases and has an ever growing list of features, supported guest operating systems and platforms it runs on. VirtualBox is a community effort backed by a dedicated company: everyone is encouraged to contribute while Oracle ensures the product always meets professional quality criteria.

Click here

Hot picks:

- Pre-built virtual machines for developers at Oracle Tech Network
- **Hyperbox** Open-source Virtual Infrastructure Manager project site
- **phpVirtualBox** AJAX web interface project site

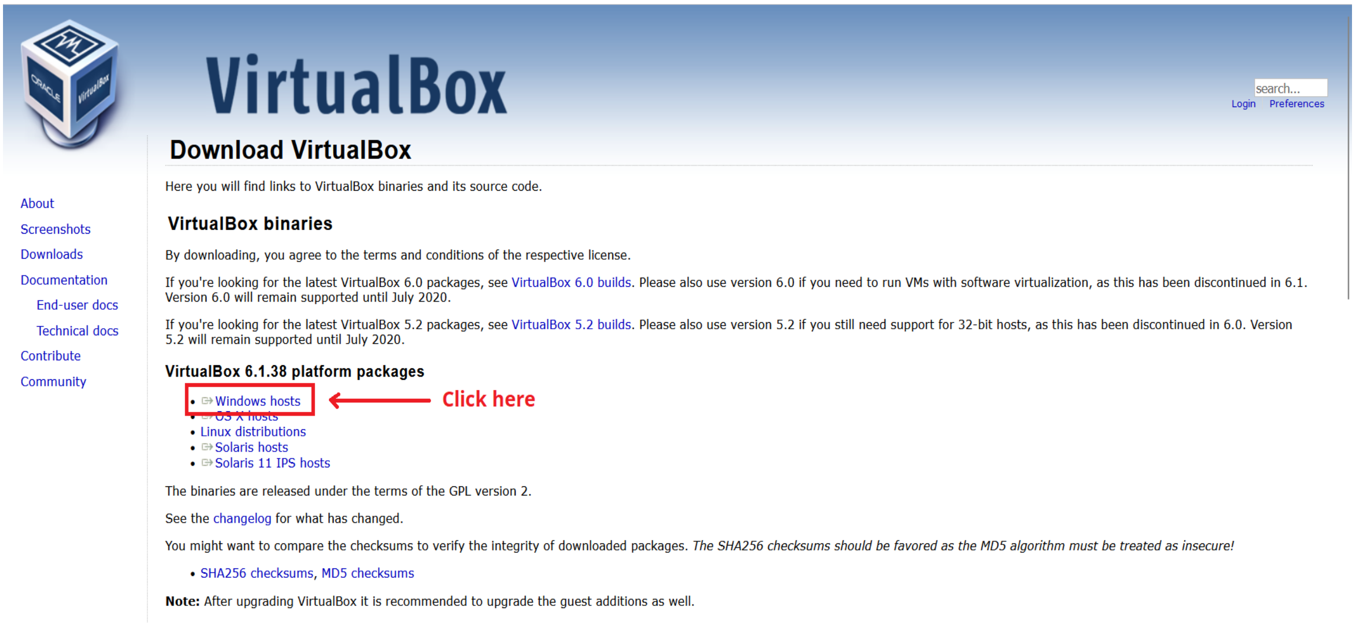
News Flash

- New **September 2nd, 2022**
  VirtualBox 6.1.38 released!
  Oracle today released a 6.1 maintenance release which improves stability and fixes regressions. See the Changelog for details.
- Important **August 30th, 2022**
  We're hiring!
  Looking for a new challenge? We're hiring a VirtualBox Principal Software Developer (US, UK, Romania).
- New **July 19th, 2022**
  VirtualBox 6.1.36 released!
  Oracle today released a 6.1 maintenance release which improves stability and fixes regressions. See the Changelog for details.

More information...

Contact – Privacy policy – Terms of Use

Then click on "Windows hosts" to start the download.



Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

If you're looking for the latest VirtualBox 6.0 packages, see VirtualBox 6.0 builds. Please also use version 6.0 if you need to run VMs with software virtualization, as this has been discontinued in 6.1. Version 6.0 will remain supported until July 2020.

If you're looking for the latest VirtualBox 5.2 packages, see VirtualBox 5.2 builds. Please also use version 5.2 if you still need support for 32-bit hosts, as this has been discontinued in 6.0. Version 5.2 will remain supported until July 2020.

VirtualBox 6.1.38 platform packages

- Windows hosts
- OS X hosts
- Linux distributions
- Solaris hosts
- Solaris 11 IPS hosts

Click here

The binaries are released under the terms of the GPL version 2.

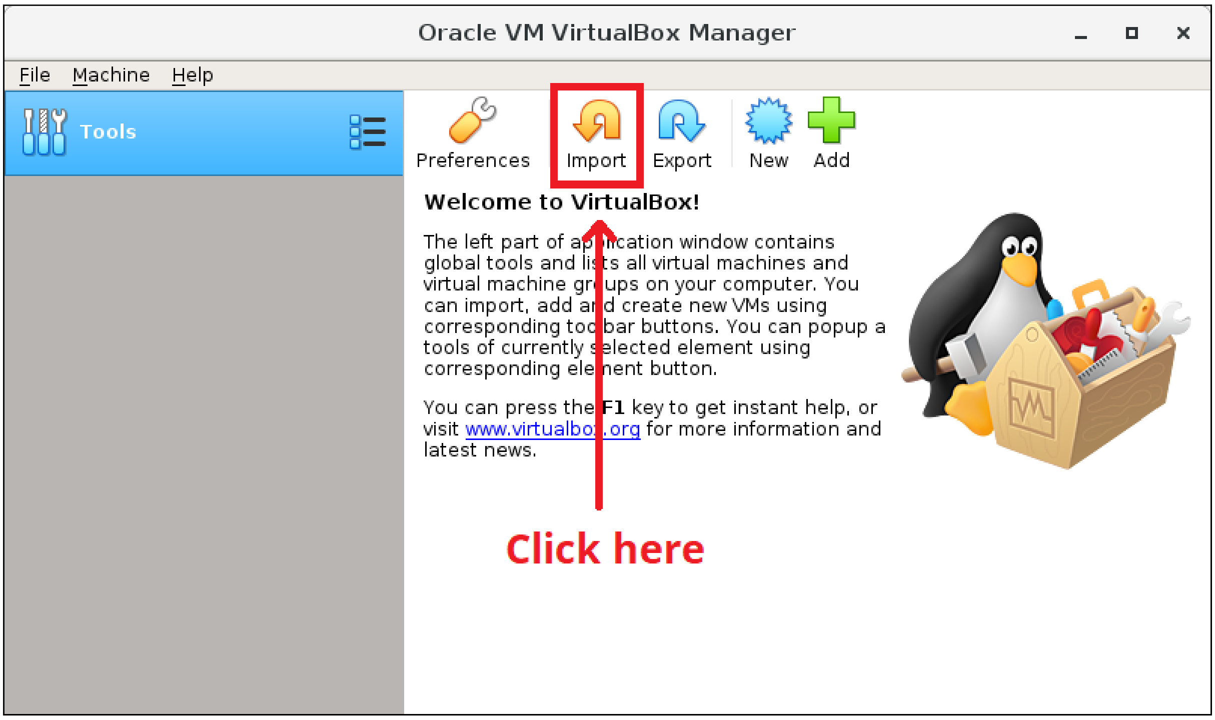
See the changelog for what has changed.

You might want to compare the checksums to verify the integrity of downloaded packages. *The SHA256 checksums should be favored as the MD5 algorithm must be treated as insecure!*

- SHA256 checksums, MD5 checksums

Note: After upgrading VirtualBox it is recommended to upgrade the guest additions as well.

3- After the installation, launch VirtualBox and click on Import.

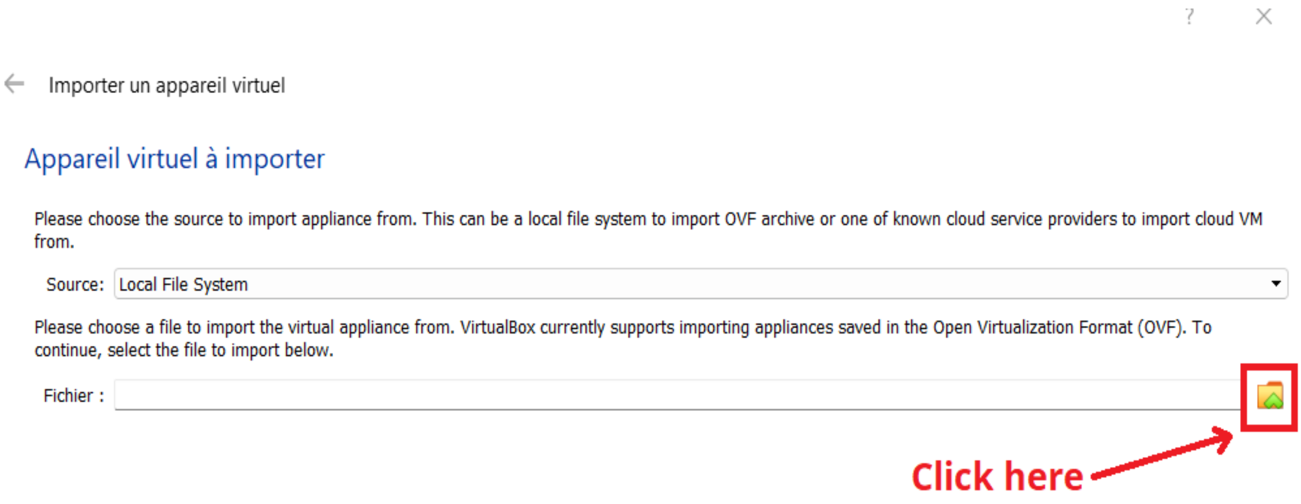


Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

4- Then click on the icon to select the OVA VM previously downloaded.



Appareil virtuel à importer

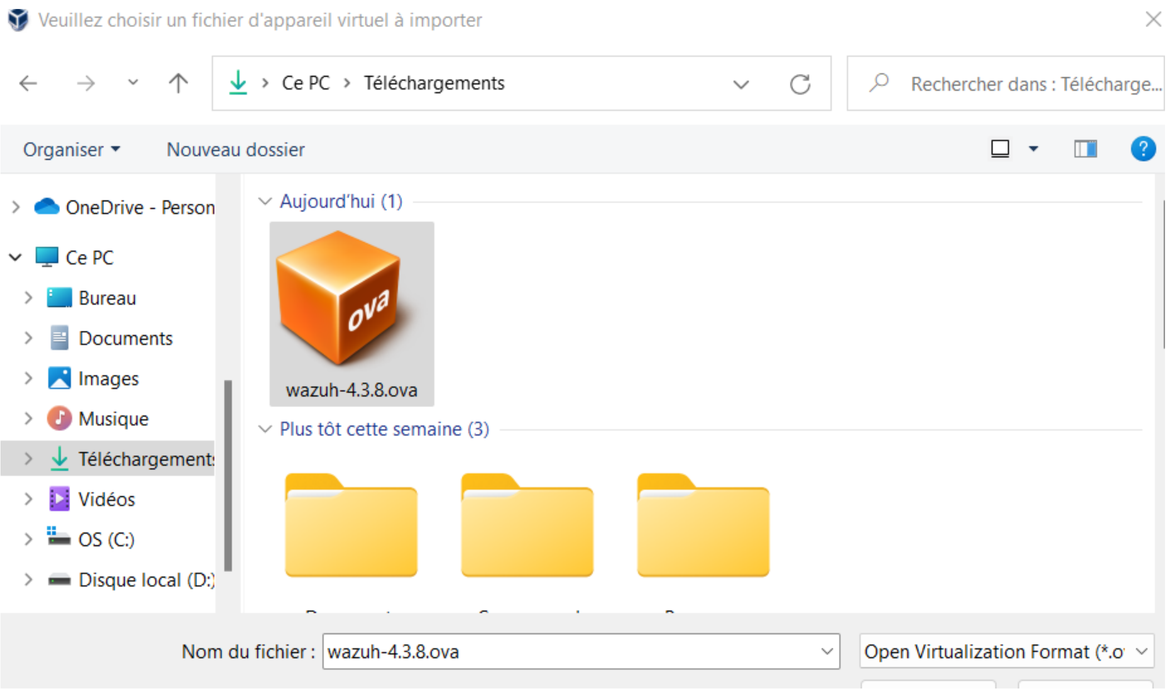
Please choose the source to import appliance from. This can be a local file system to import OVF archive or one of known cloud service providers to import cloud VM from.

Source: Local File System

Please choose a file to import the virtual appliance from. VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

Fichier :

5- Select the OVA VM and click open.



Veuillez choisir un fichier d'appareil virtuel à importer

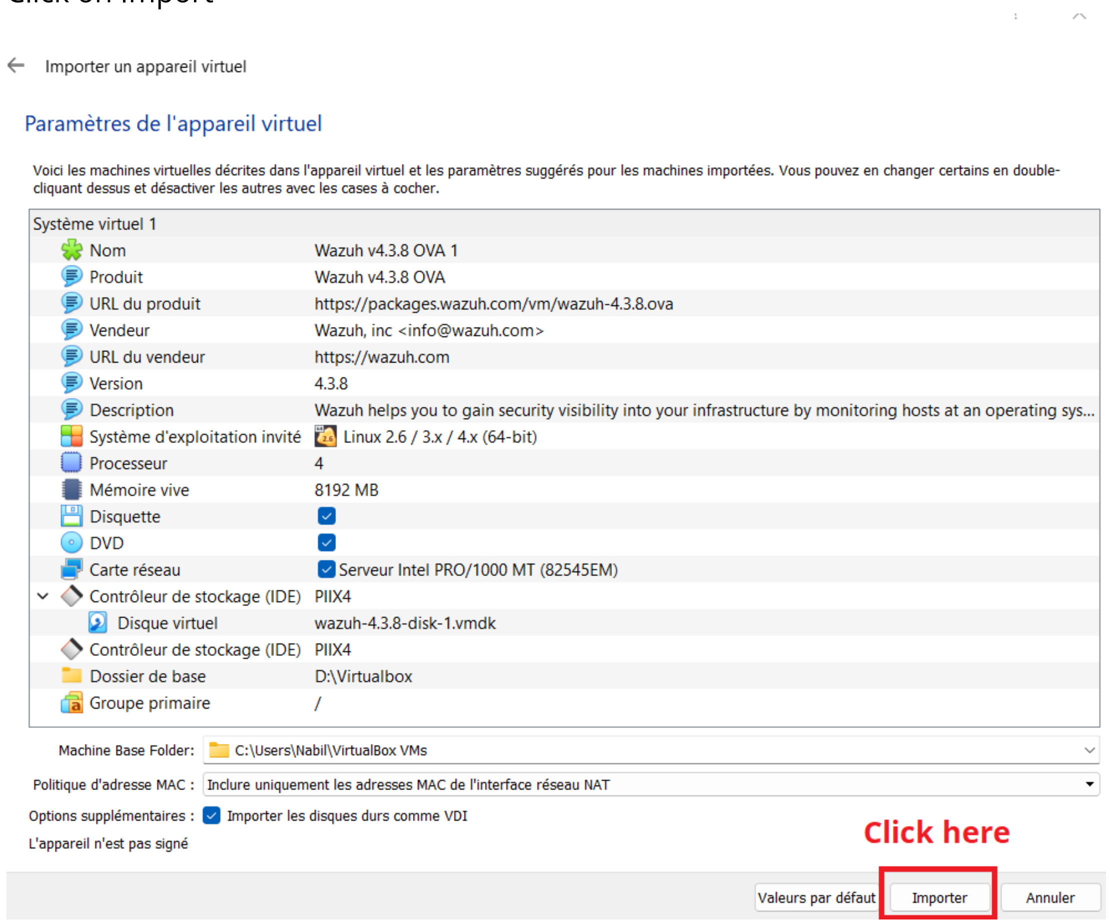
Ce PC > Téléchargements

Rechercher dans : Télécharge...

Nom du fichier : wazuh-4.3.8.ova

Open Virtualization Format (*.o

6- Then, click on Next, and you should see the configuration of the OVA VM. Click on Import



Importer un appareil virtuel

Paramètres de l'appareil virtuel

Voici les machines virtuelles décrites dans l'appareil virtuel et les paramètres suggérés pour les machines importées. Vous pouvez en changer certains en double-cliquant dessus et désactiver les autres avec les cases à cocher.

Système virtuel 1	
Nom	Wazuh v4.3.8 OVA 1
Produit	Wazuh v4.3.8 OVA
URL du produit	https://packages.wazuh.com/vm/wazuh-4.3.8.ova
Vendeur	Wazuh, inc <info@wazuh.com>
URL du vendeur	https://wazuh.com
Version	4.3.8
Description	Wazuh helps you to gain security visibility into your infrastructure by monitoring hosts at an operating sys...
Système d'exploitation invité	Linux 2.6 / 3.x / 4.x (64-bit)
Processeur	4
Mémoire vive	8192 MB
Disquette	☑
DVD	☑
Carte réseau	☑ Serveur Intel PRO/1000 MT (82545EM)
Contrôleur de stockage (IDE)	PIIX4
Disque virtuel	wazuh-4.3.8-disk-1.vmdk
Contrôleur de stockage (IDE)	PIIX4
Dossier de base	D:\Virtualbox
Groupe primaire	/

Machine Base Folder: C:\Users\Nabil\VirtualBox VMs

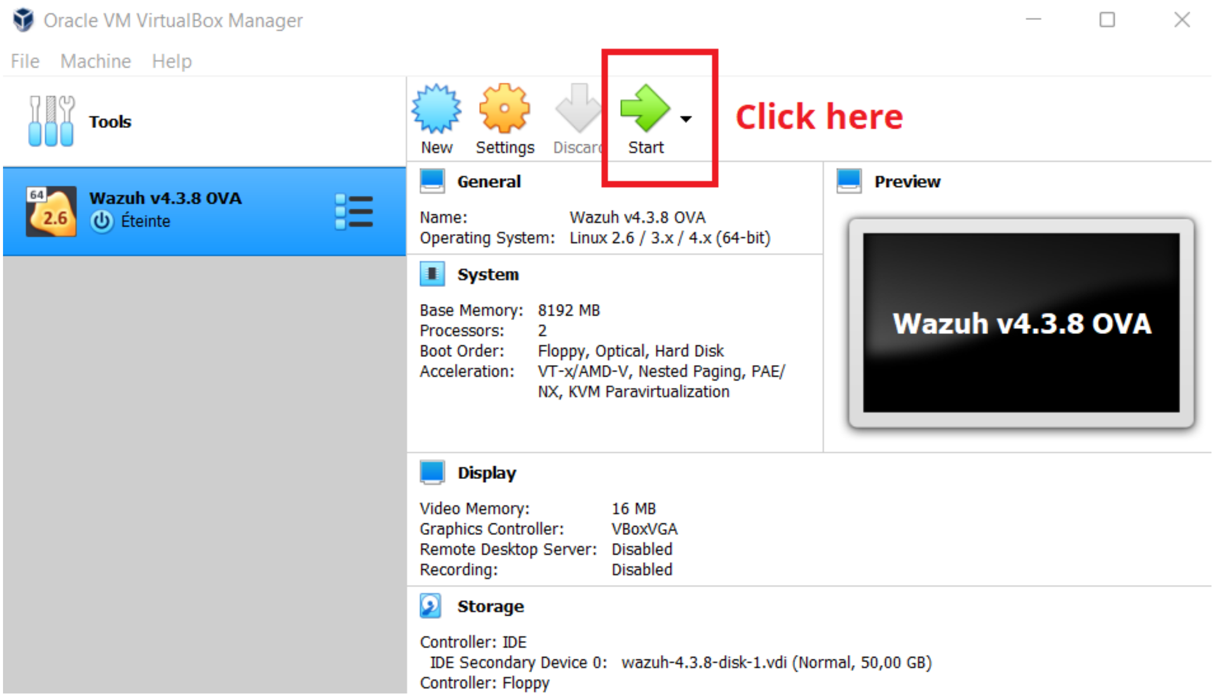
Politique d'adresse MAC : Inclure uniquement les adresses MAC de l'interface réseau NAT

Options supplémentaires : ☑ Importer les disques durs comme VDI

L'appareil n'est pas signé

Click here

7- Now, you should see that your VM has successfully imported.
Click on start to start the machine.



General

Name: Wazuh v4.3.8 OVA
Operating System: Linux 2.6 / 3.x / 4.x (64-bit)

System

Base Memory: 8192 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display

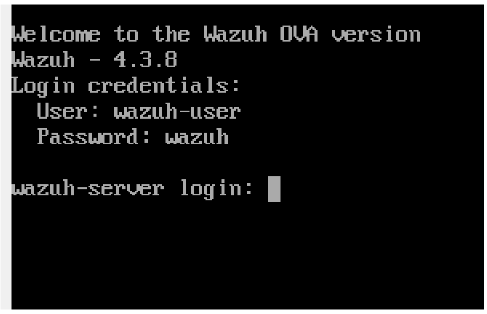
Video Memory: 16 MB
Graphics Controller: VBoxVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: wazuh-4.3.8-disk-1.vdi (Normal, 50,00 GB)
Controller: Floppy

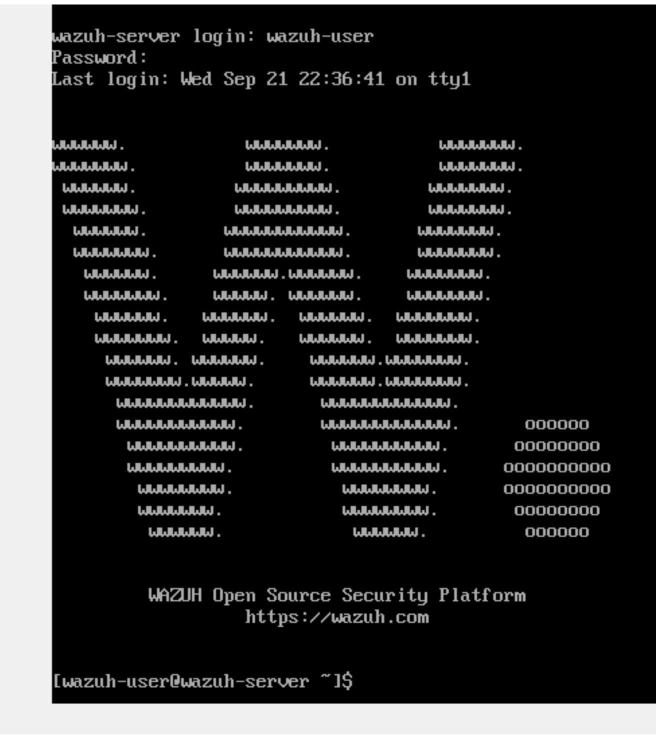
2. Getting started with Wazuh.

1- The first thing to do, is to login using those credentials:
Username: **wazuh-user**
Password: **wazuh**



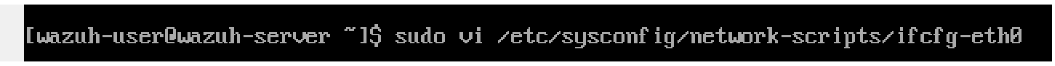
```
Welcome to the Wazuh OVA version
Wazuh - 4.3.8
Login credentials:
  User: wazuh-user
  Password: wazuh

wazuh-server login: 
```

2- The CLI interface will be used for the beginning for basic configuration. However, the GUI will be used for the rest of deployment.



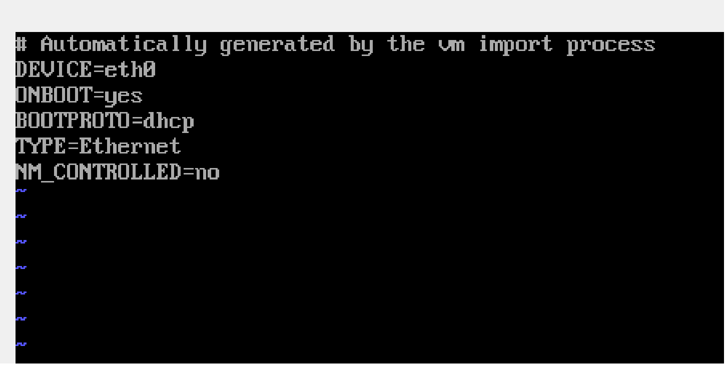
```
wazuh-server login: wazuh-user
Password:
Last login: Wed Sep 21 22:36:41 on tty1


wwwwww.           wwwwwww.          wwwwwww.
wwwwwww.          wwwwwww.          wwwwwww.
 wwwwww.         wwwwwwwww.        wwwwwww.
 wwwwwww.        wwwwwwwww.        wwwwwww.
  wwwwww.       wwwwwwwwwww.      wwwwwww.
  wwwwwww.      wwwwwwwwwww.      wwwwwww.
   wwwwww.     wwwwww.wwwwww.    wwwwwww.
   wwwwwww.    wwwww. wwwwww.    wwwwwww.
    wwwwww.   wwwwww.  wwwwww.  wwwwwww.
    wwwwwww.  wwwww.   wwwwww.  wwwwwww.
     wwwwww. wwwwww.    wwwwww.wwwwwww.
     wwwwwww.wwwww.     wwwwww.wwwwwww.
      wwwwwwwwwwww.      wwwwwwwwwwwww.
      wwwwwwwwwww.       wwwwwwwwwwwww.      oooooo
       wwwwwwwwww.        wwwwwwwwwww.      oooooooo
       wwwwwwwww.         wwwwwwwwwww.     oooooooooo
        wwwwwwww.          wwwwwwwww.      oooooooooo
        wwwwwww.           wwwwwwwww.       oooooooo
         wwwwww.            wwwwwww.         oooooo


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


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

3- It is recommended to fix the IP address of the Wazuh Manager. You can configure a static IP address by modifying "ifcfg-eth0" using the following command:
sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0



```
[wazuh-user@wazuh-server ~]$ sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

4- By default, the server gets an IP address from a DHCP server, so the config should be like this.

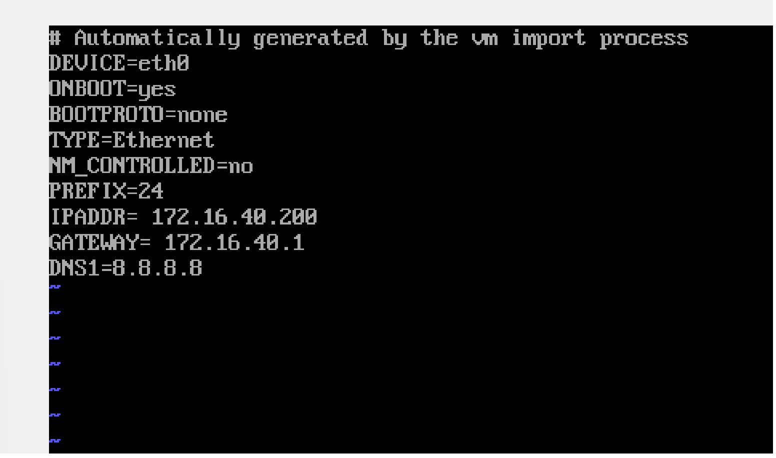


```
# Automatically generated by the vm import process
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
NM_CONTROLLED=no
~
~
~
~
~
~
~
```

5- Press the “ i “ button and edit the config file:
Change the BOOTPROTO value from dhcp to none
Add those lines under NM_CONTROLLED=no :

PREFIX=24
IPADDR=<your IP address>
GATEWAY=<your gateway>
DNS1=8.8.8.8

And now your config file should look like this:



```
# Automatically generated by the vm import process
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=none
TYPE=Ethernet
NM_CONTROLLED=no
PREFIX=24
IPADDR= 172.16.40.200
GATEWAY= 172.16.40.1
DNS1=8.8.8.8
~
~
~
~
~
~
~
```

6- Press “ ESC “ button:

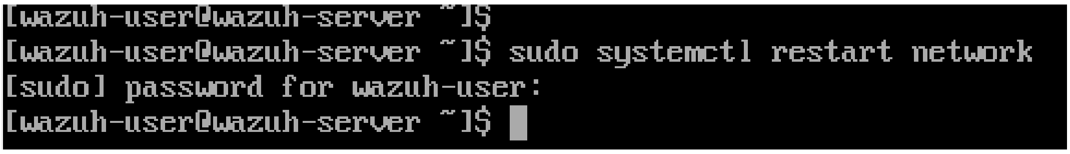
Esc

Press “ : “ button:

:

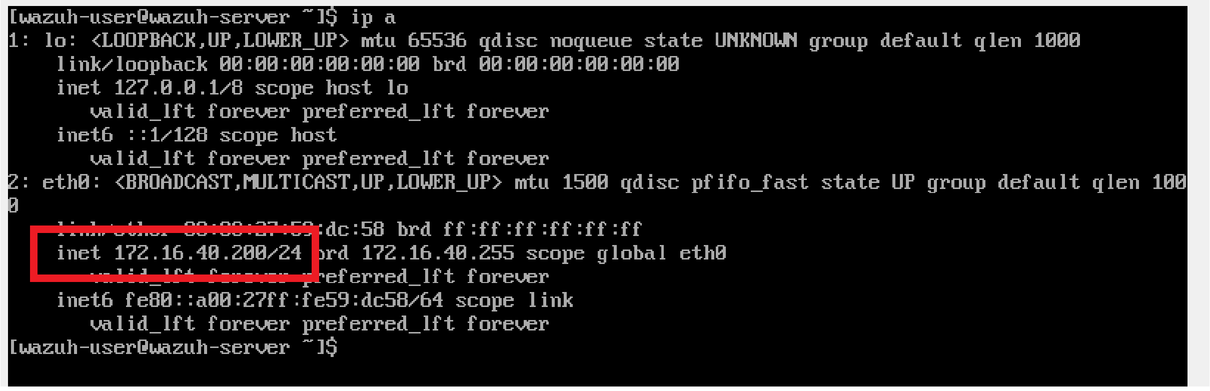
Then type, “ **wq** ” to save and quit.

7- Then you need to restart the network service using the following command:
sudo systemctl restart network
You will be asked to enter your password “**wazuh**”, do it and press enter.



```
[wazuh-user@wazuh-server ~]$
[wazuh-user@wazuh-server ~]$ sudo systemctl restart network
[sudo] password for wazuh-user:
[wazuh-user@wazuh-server ~]$
```

8- The last step is to ensure that the IP has successfully assigned.
Use the command: **ip a**

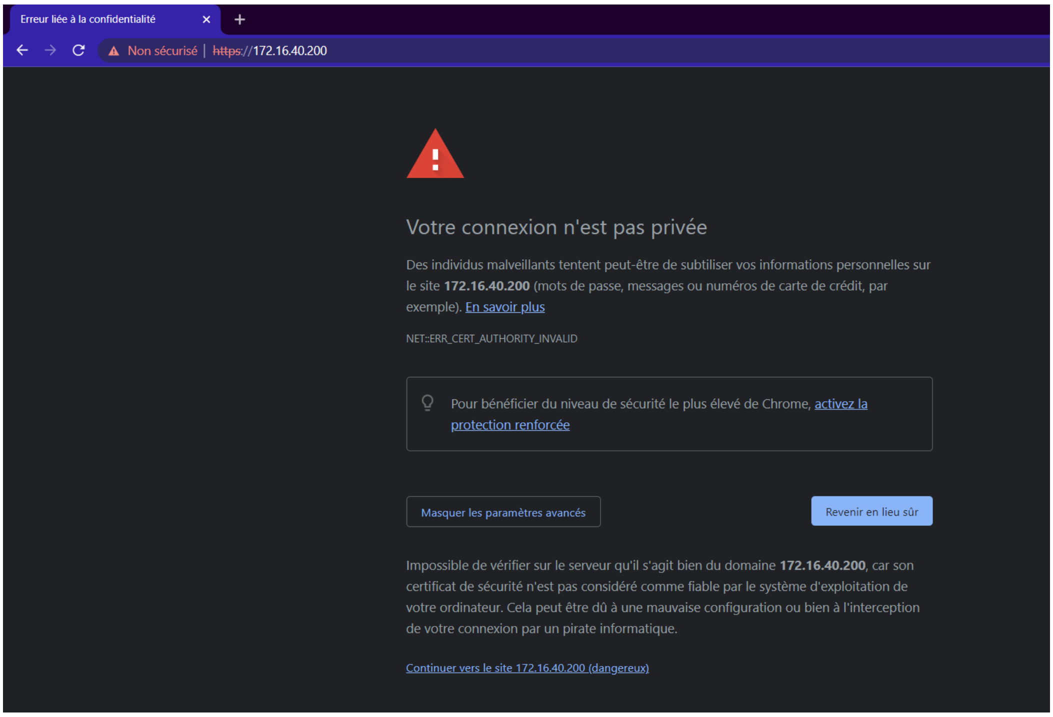


```
[wazuh-user@wazuh-server ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       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 08:00:27:59:dc:58 brd ff:ff:ff:ff:ff:ff
    inet 172.16.40.200/24 brd 172.16.40.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe59:dc58/64 scope link
       valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]$
```

3. GUI interface Access

1. Navigate to your Web browser and type: **https://<your-IP-address>**

You should see a warning like this, don't worry it's only because you don't have a certificate, click on Advanced settings, and click on: Continue.



Erreur liée à la confidentialité
Non sécurisé | https://172.16.40.200

Votre connexion n'est pas privée

Des individus malveillants tentent peut-être de subtiliser vos informations personnelles sur le site **172.16.40.200** (mots de passe, messages ou numéros de carte de crédit, par exemple). En savoir plus

NET::ERR_CERT_AUTHORITY_INVALID

Pour bénéficier du niveau de sécurité le plus élevé de Chrome, activez la protection renforcée

Masquer les paramètres avancés
Revenir en lieu sûr

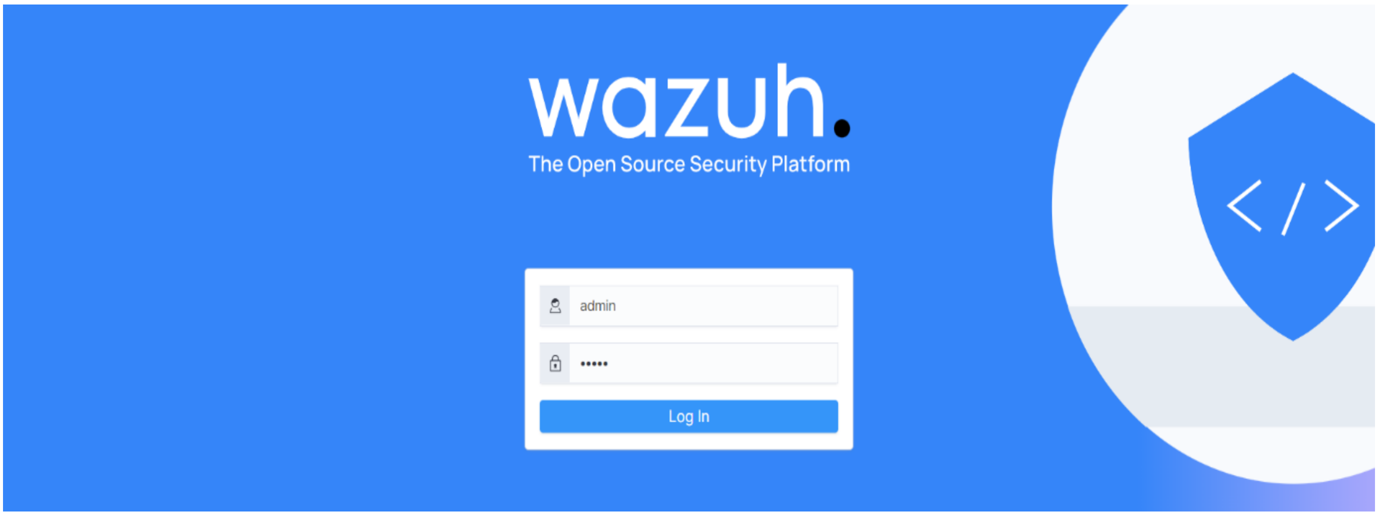
Impossible de vérifier sur le serveur qu'il s'agit bien du domaine **172.16.40.200**, car son certificat de sécurité n'est pas considéré comme fiable par le système d'exploitation de votre ordinateur. Cela peut être dû à une mauvaise configuration ou bien à l'interception de votre connexion par un pirate informatique.

Continuer vers le site 172.16.40.200 (dangereux)

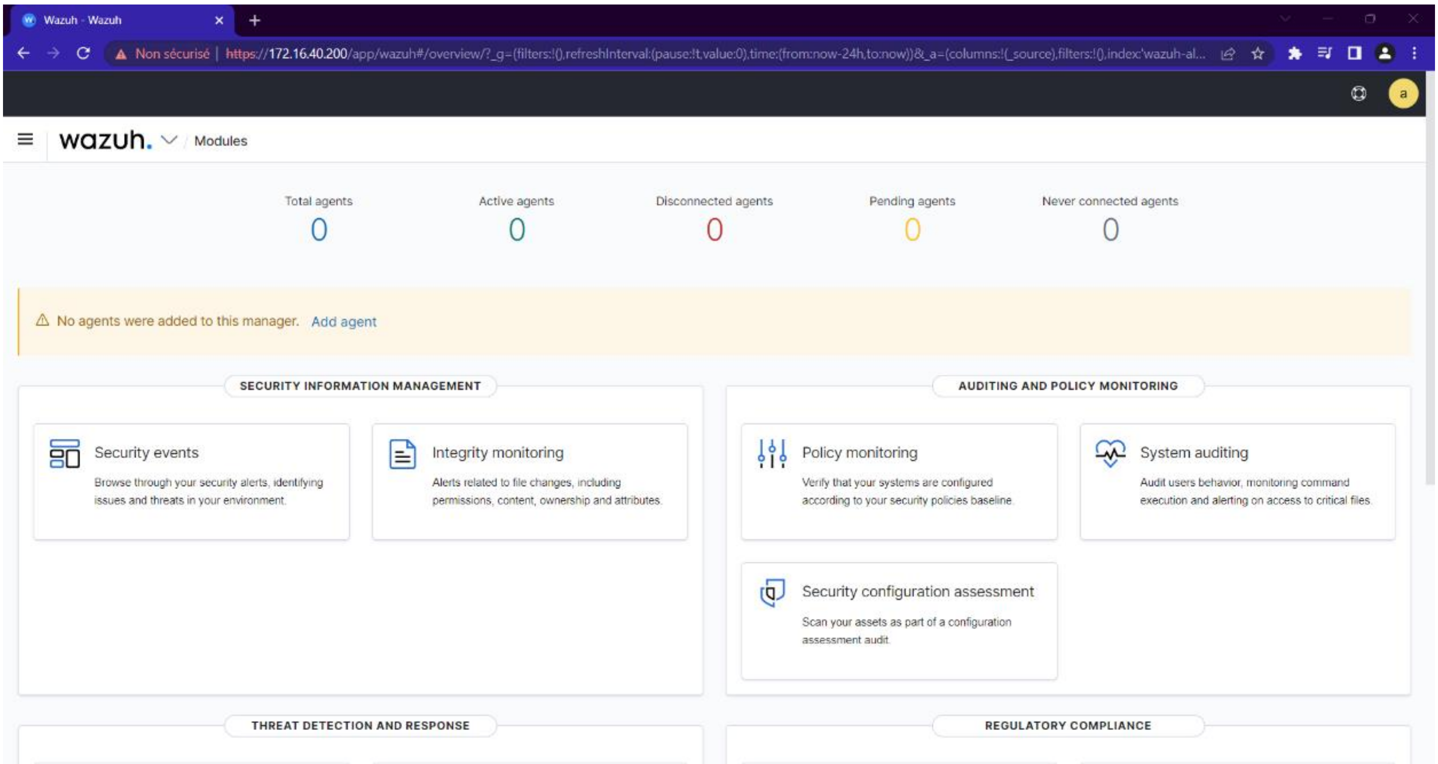
2. Now you are in the Wazuh GUI interface.

You should sign in with those credentials:

Username: **admin**
Password: **admin**



This is the **Wazuh Manager** home page.



Wazuh - Wazuh

Non sécurisé | https://172.16.40.200/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(),index:'wazuh-al...

wazuh. / Modules

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.

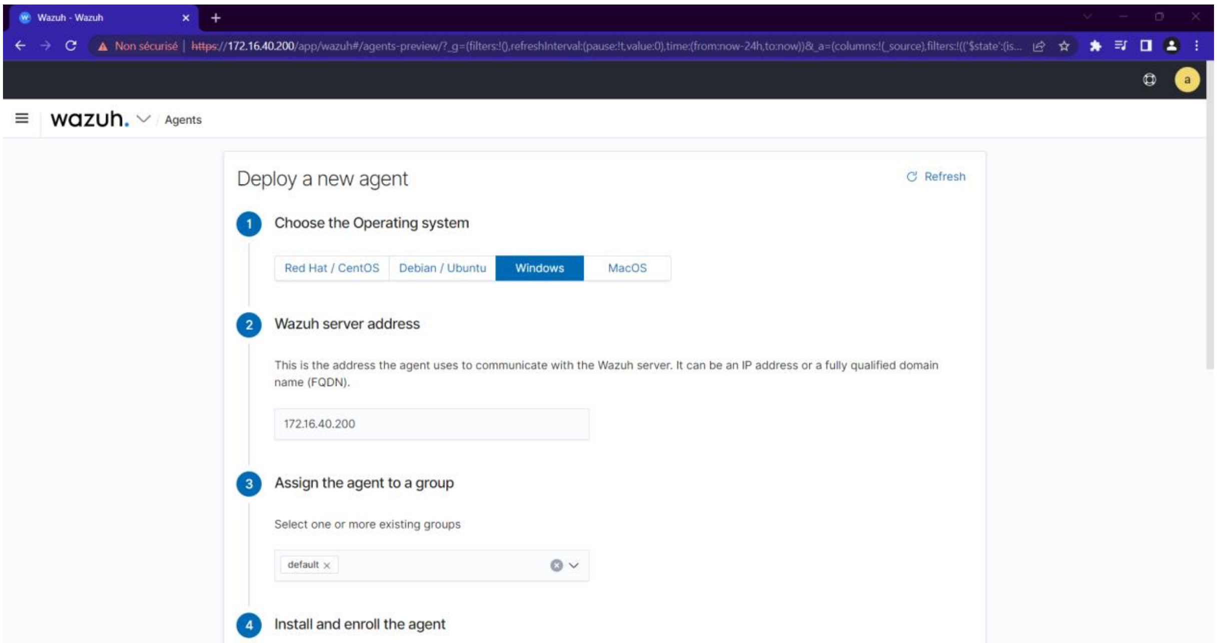
THREAT DETECTION AND RESPONSE

REGULATORY COMPLIANCE

3. The next step is to add agents in other VMs or Physical machines that already have successful connectivity with the Wazuh Manager:

A. Deploy a Windows Wazuh Agent:

1.Choose the operating system --> Windows
2.Wazuh server address --> ex: 172.16.40.200
3.Assign the agent to a group --> default



Wazuh - Wazuh

Non sécurisé | https://172.16.40.200/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(('$state':(is...

wazuh. / Agents

Deploy a new agent

Refresh

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).

172.16.40.200

3 Assign the agent to a group

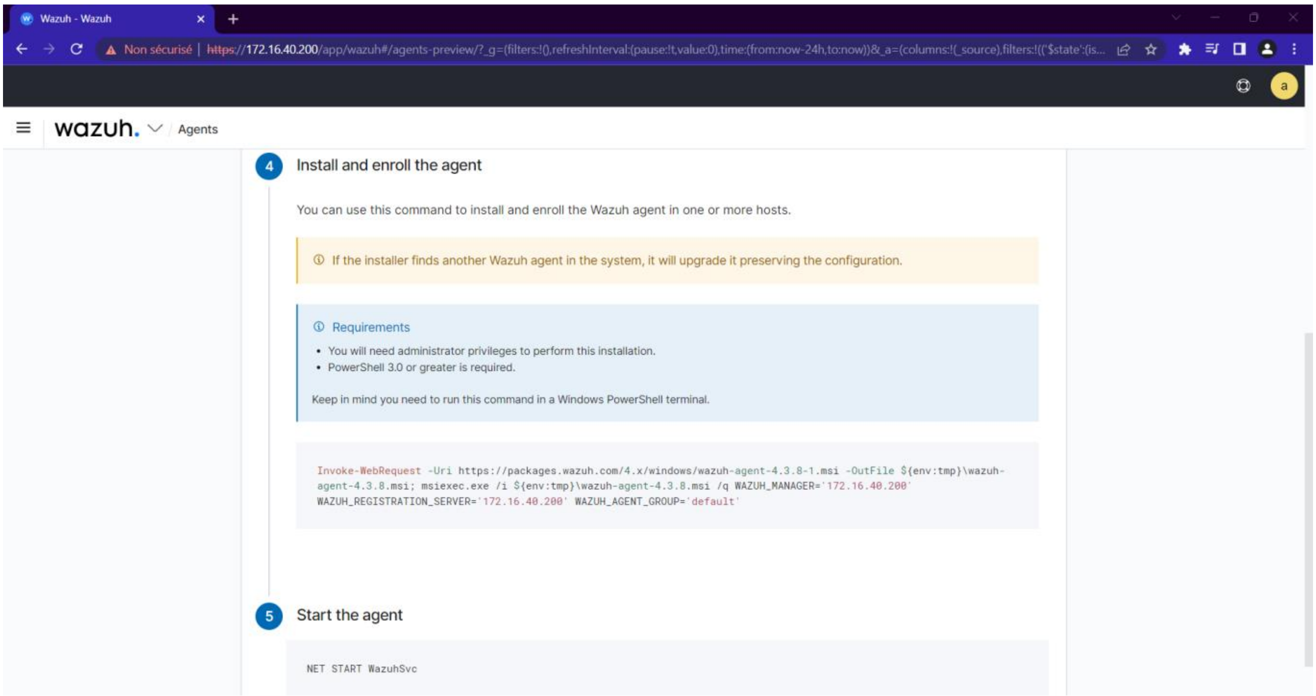
Select one or more existing groups

default ×

4 Install and enroll the agent

Note: you can create multiple groups, and assign each host to the appropriate one.

4.Install and enroll the agent


Wazuh - Wazuh
Non sécurisé | https://172.16.40.200/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(('$state':(is...
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.

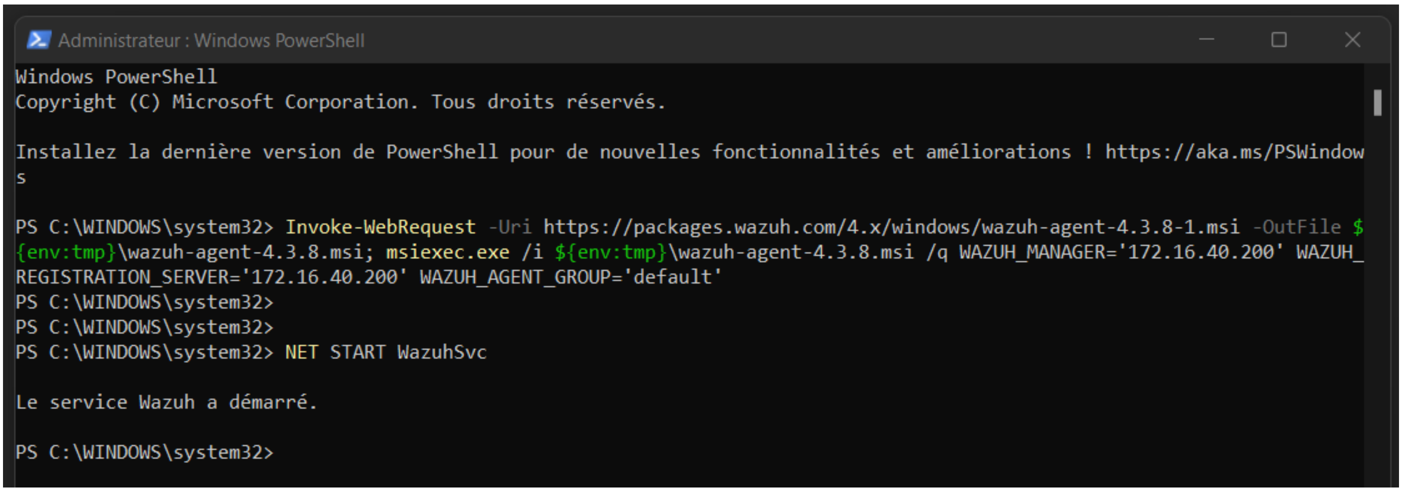
Keep in mind you need to run this command in a Windows PowerShell terminal.

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.8-1.msi -OutFile ${env:tmp}\wazuh-
agent-4.3.8.msi; msiexec.exe /i ${env:tmp}\wazuh-agent-4.3.8.msi /q WAZUH_MANAGER='172.16.40.200'
WAZUH_REGISTRATION_SERVER='172.16.40.200' WAZUH_AGENT_GROUP='default'
```

5 Start the agent

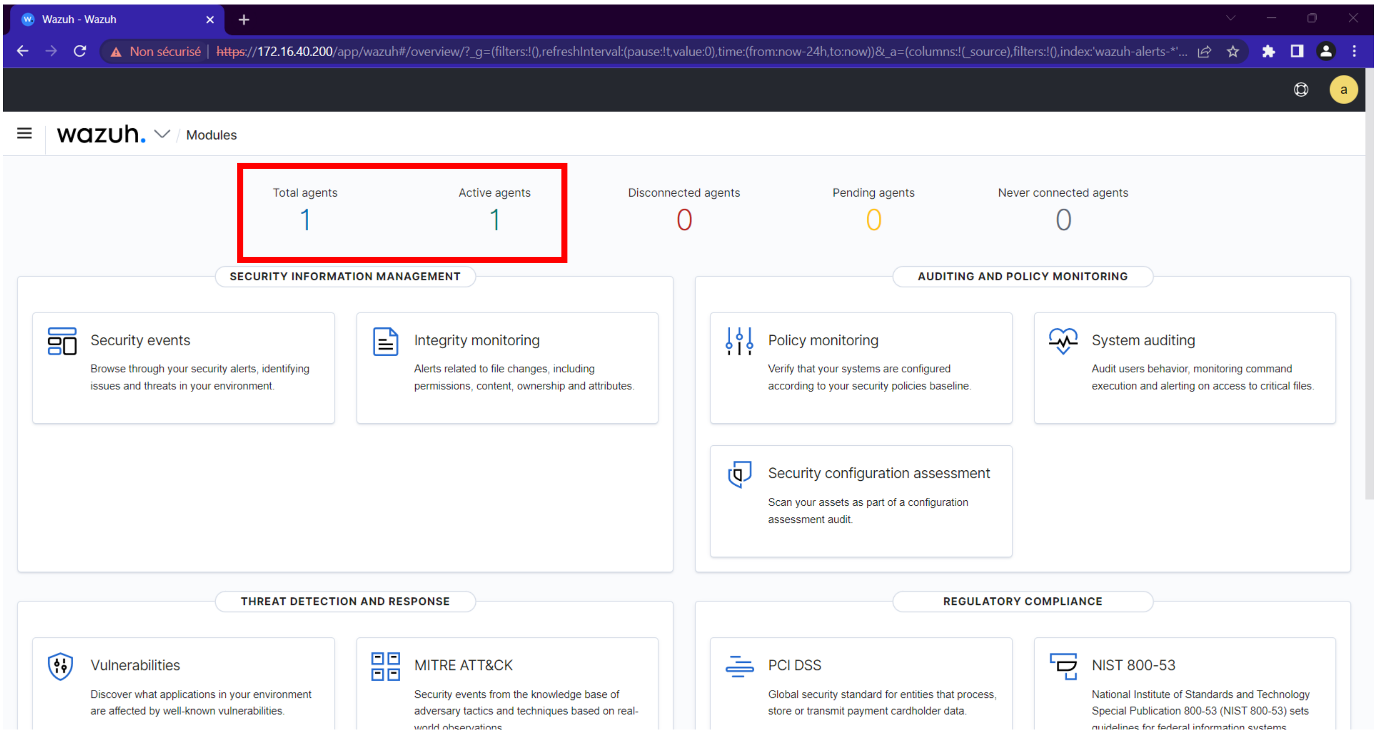
```
NET START WazuhSvc
```

You need to execute the provided commands in the windows hosts using PowerShell terminal (run as administrator), and do not forget to start the wazuh agent with the command: “ **NET START WazuhSvc** “



```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindow
s

PS C:\WINDOWS\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.8-1.msi -OutFile $
{env:tmp}\wazuh-agent-4.3.8.msi; msiexec.exe /i ${env:tmp}\wazuh-agent-4.3.8.msi /q WAZUH_MANAGER='172.16.40.200' WAZUH_
REGISTRATION_SERVER='172.16.40.200' WAZUH_AGENT_GROUP='default'
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> NET START WazuhSvc

Le service Wazuh a démarré.

PS C:\WINDOWS\system32>
```

Going back to the Wazuh Manager home page, we can see our new agent is successfully deployed, and its state is: Active.


Wazuh - Wazuh
Non sécurisé | https://172.16.40.200/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(),index:'wazuh-alerts-*'...
wazuh.
Modules

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.

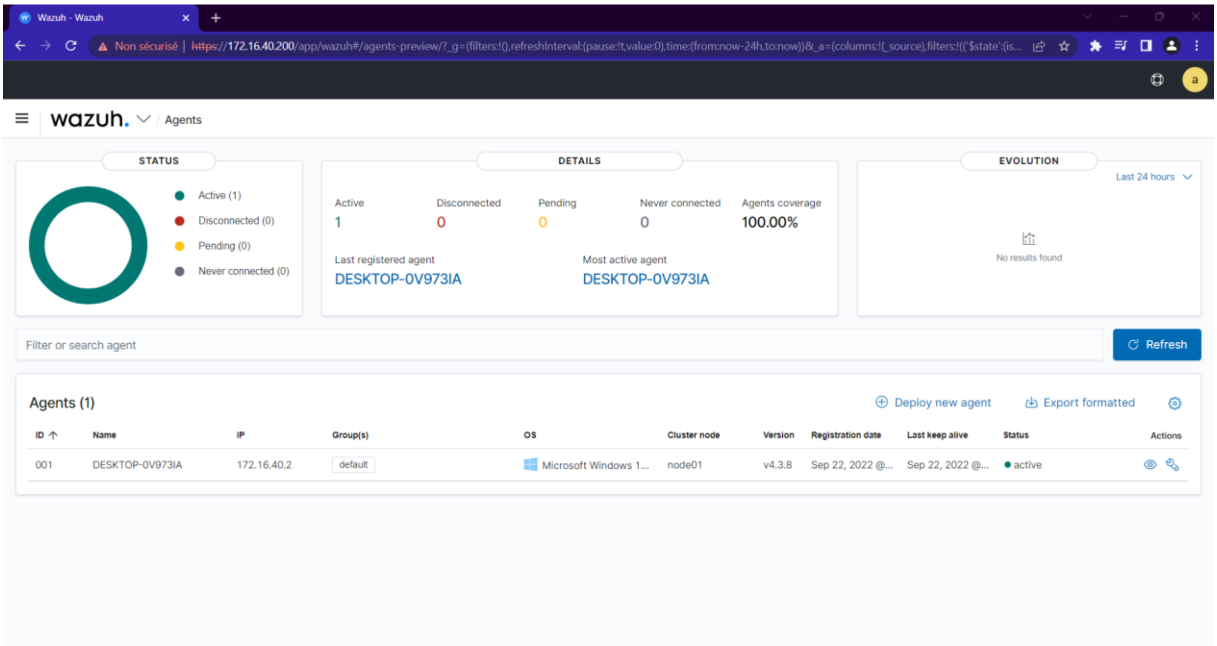
MITRE ATT&CK
Security events from the knowledge base of adversary tactics and techniques based on real-world observations

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

Click on the Active agent to see more details about it.


Wazuh - Wazuh
Non sécurisé | https://172.16.40.200/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(('$state':(is...
wazuh.
Agents
EVOLUTION
Last 24 hours
No results found
Filter or search agent
Refresh
Deploy new agent
Export formatted

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: DESKTOP-0V973IA

Most active agent: DESKTOP-0V973IA

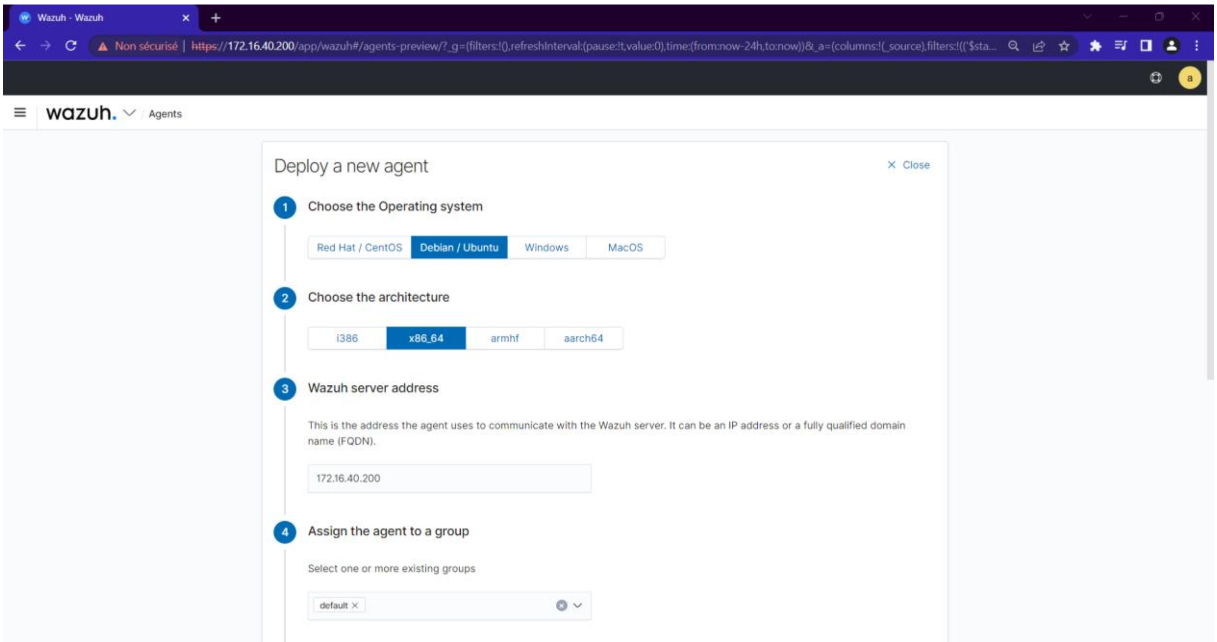
Agents (1)

ID ↑	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status	Actions
001	DESKTOP-0V973IA	172.16.40.2	default	Microsoft Windows 1...	node01	v4.3.8	Sep 22, 2022 @...	Sep 22, 2022 @...	● active	

B. Deploy a Linux Wazuh Agent:

Add new agents

1.Choose the operating system --> linux (choose either Debian or RedHat distribution)
2.Choose the architecture --> x86_64
3.Wazuh server address --> 172.16.40.200
4.Assign the agent to a group --> default



Deploy a new agent

1 Choose the Operating system

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

2 Choose the architecture

i386 | **x86_64** | armhf | aarch64

3 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).

172.16.40.200

4 Assign the agent to a group

Select one or more existing groups

default

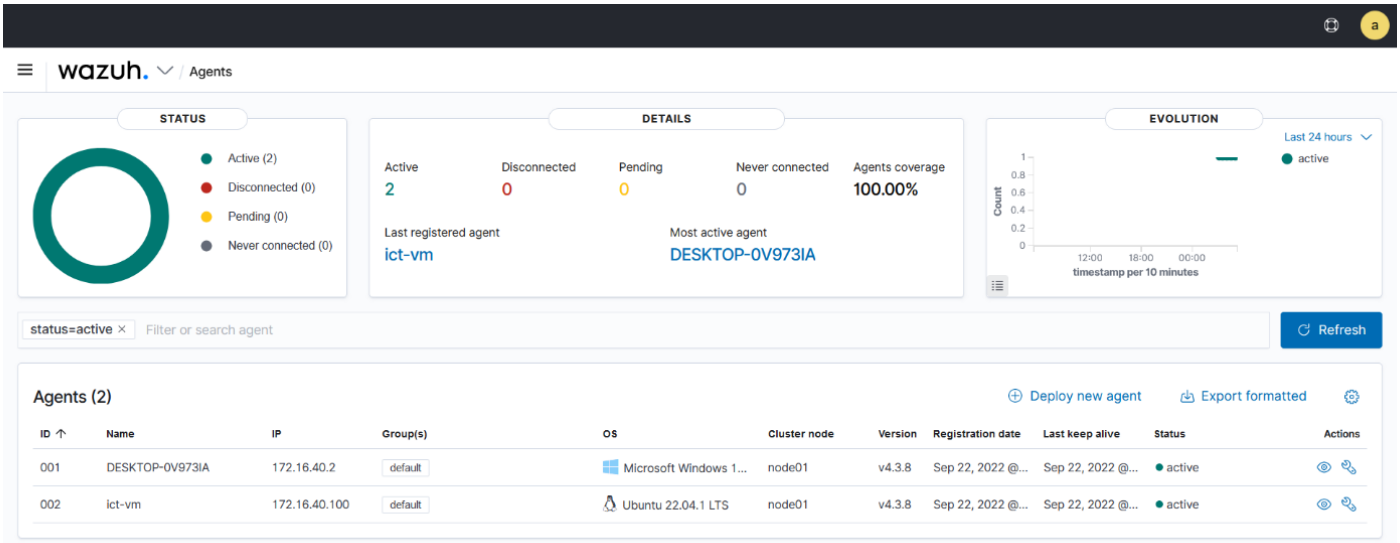
Wazuh - Wazuh
Non sécurisé | https://172.16.40.200/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(('$sta...
wazuh.
Agents
Close

5- Install and enroll the agent

You should use the provided commands to install Wazuh agent in the Debian distro hosts.

6.Start the agent

After installing the agent and starting the service, we can see the Linux agent is added.



STATUS

Active (2)
Disconnected (0)
Pending (0)
Never connected (0)

DETAILS

Active	Disconnected	Pending	Never connected	Agents coverage
2	0	0	0	100.00%

Last registered agent: ict-vm
Most active agent: DESKTOP-0V973IA

status=active

Agents (2)

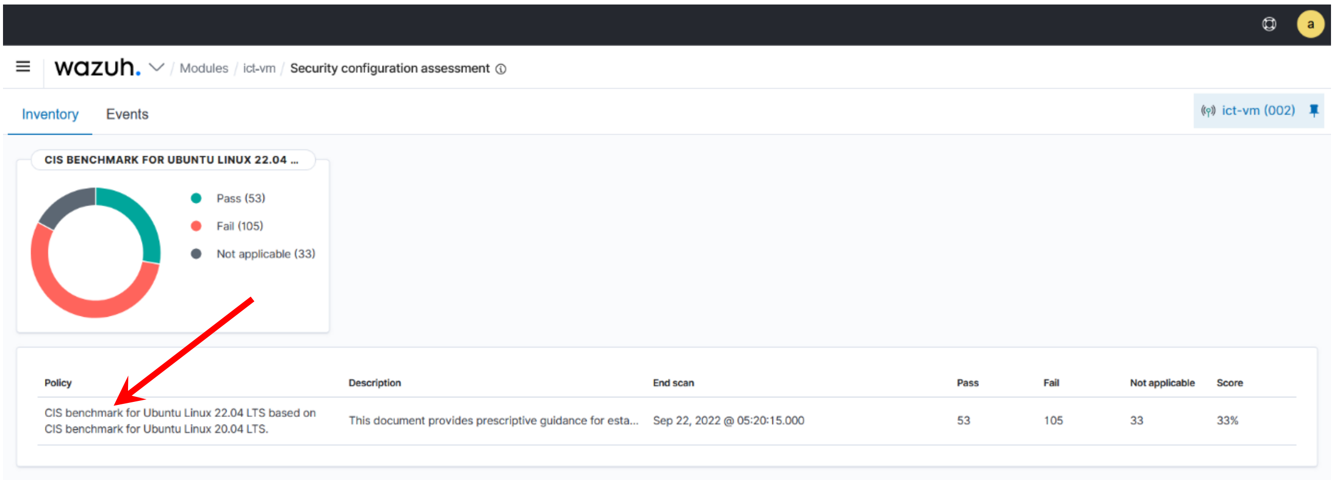
ID	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status	Actions
001	DESKTOP-0V973IA	172.16.40.2	default	Microsoft Windows 1...	node01	v4.3.8	Sep 22, 2022 @...	Sep 22, 2022 @...	● active	
002	ict-vm	172.16.40.100	default	Ubuntu 22.04.1 LTS	node01	v4.3.8	Sep 22, 2022 @...	Sep 22, 2022 @...	● active	

4. Security Configuration Assessment – SCA

SCA performs scans to discover exposures or misconfigurations in monitored hosts. Those scans assess the configuration of the hosts using policy files that contain rules to be tested against the actual configuration of the host.

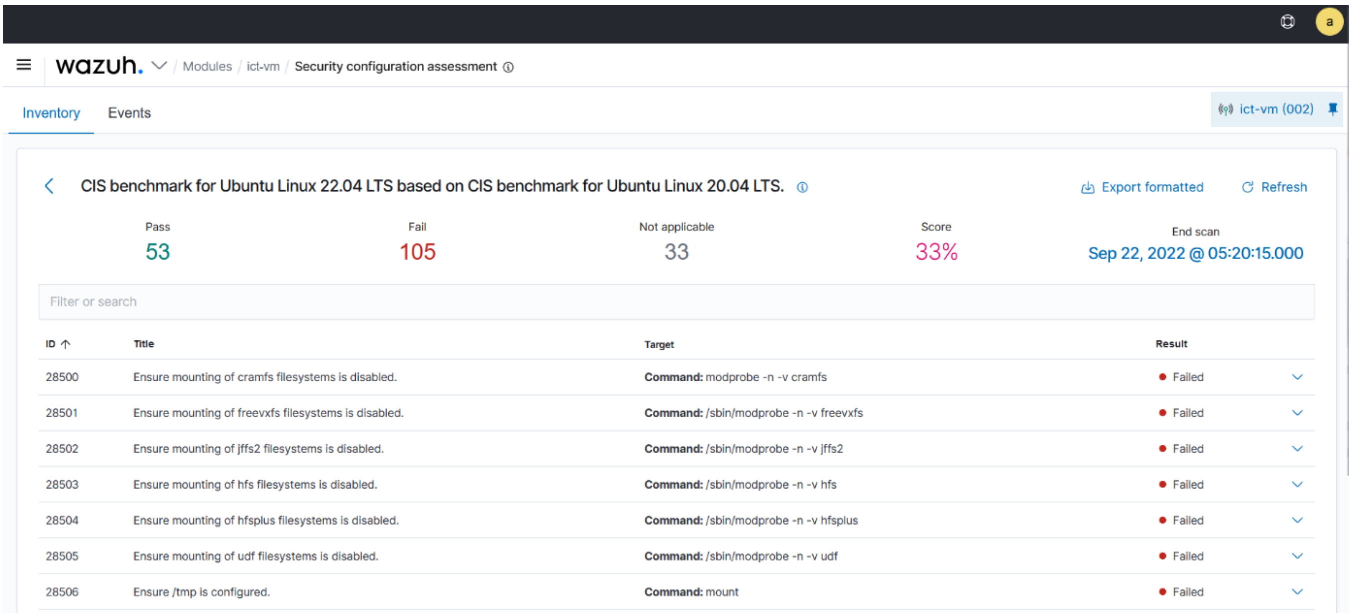
For example, SCA could assess whether it is necessary to change password related configuration, remove unnecessary software, disable unnecessary services, or audit the TCP/IP stack configuration.

Wazuh is distributed with a set of policies, most of them based on the **CIS benchmarks**, a well-established standard for ensuring **Compliance Management**.



Policy	Description	End scan	Pass	Fail	Not applicable	Score
CIS benchmark for Ubuntu Linux 22.04 LTS based on CIS benchmark for Ubuntu Linux 20.04 LTS.	This document provides prescriptive guidance for esta...	Sep 22, 2022 @ 05:20:15.000	53	105	33	33%

A summary is shown in the main page of SCA. For more details you can click on CIS benchmark.



CIS benchmark for Ubuntu Linux 22.04 LTS based on CIS benchmark for Ubuntu Linux 20.04 LTS.

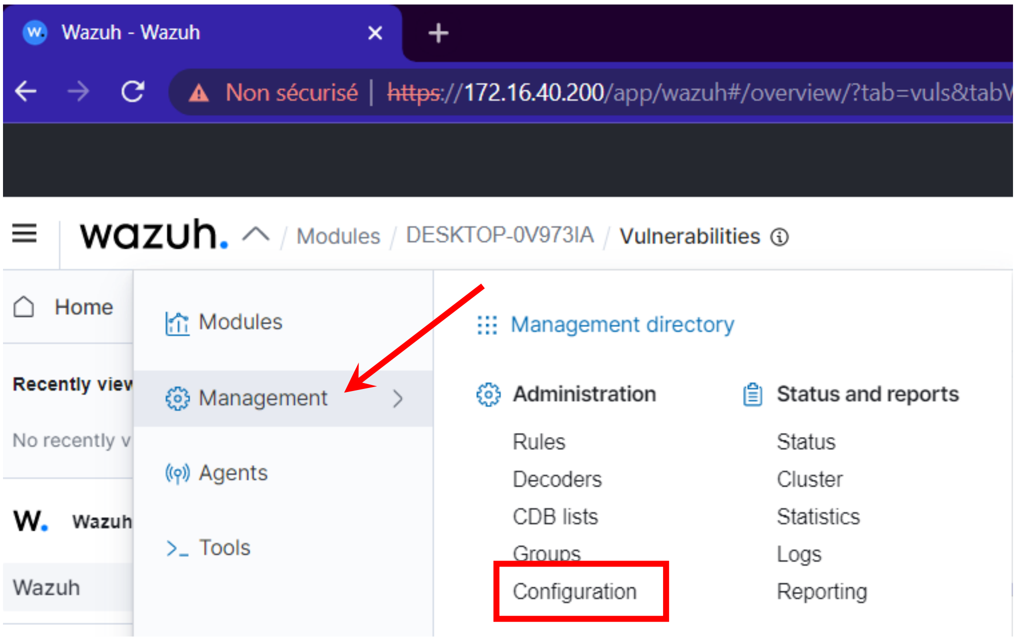
Pass	Fail	Not applicable	Score	End scan
53	105	33	33%	Sep 22, 2022 @ 05:20:15.000

ID ↑	Title	Target	Result
28500	Ensure mounting of cramfs filesystems is disabled.	**Command:** modprobe -n -v cramfs	● Failed
28501	Ensure mounting of freevxfs filesystems is disabled.	**Command:** /sbin/modprobe -n -v freevxfs	● Failed
28502	Ensure mounting of jffs2 filesystems is disabled.	**Command:** /sbin/modprobe -n -v jffs2	● Failed
28503	Ensure mounting of hfs filesystems is disabled.	**Command:** /sbin/modprobe -n -v hfs	● Failed
28504	Ensure mounting of hfsplus filesystems is disabled.	**Command:** /sbin/modprobe -n -v hfsplus	● Failed
28505	Ensure mounting of udf filesystems is disabled.	**Command:** /sbin/modprobe -n -v udf	● Failed
28506	Ensure /tmp is configured.	**Command:** mount	● Failed

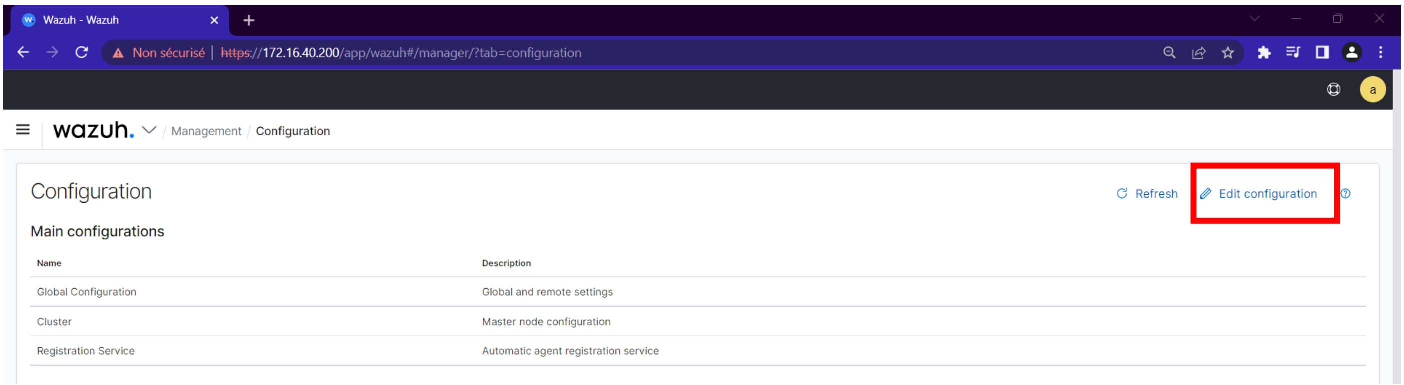
This is an example of SCA for the Linux machine. You can open each control to see the whole description about it, the risk behind, the remediation...

5. Customizing SCA interval scan.

We can customize SCA options by clicking on the Management > Configuration



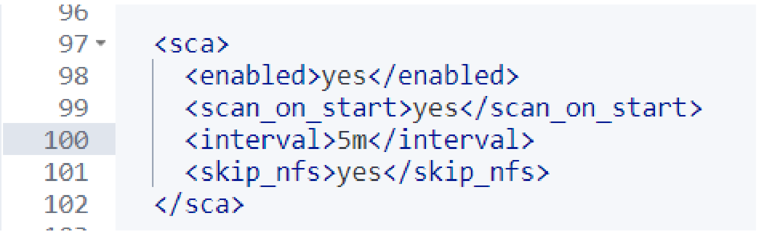
And then Edit the configuration.


Wazuh - Wazuh
Non sécurisé | https://172.16.40.200/app/wazuh#/manager/?tab=configuration
wazuh.
Management / Configuration
Configuration
Refresh
Edit configuration

Main configurations

Name	Description
Global Configuration	Global and remote settings
Cluster	Master node configuration
Registration Service	Automatic agent registration service

Scroll down until you see SCA section, edit the interval value to be 5m (for example), and make sure that scan on start is enabled: “ yes “, Save and restart the manager.



```
<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>5m</interval>
  <skip_nfs>yes</skip_nfs>
</sca>
```

6. Vulnerability Management

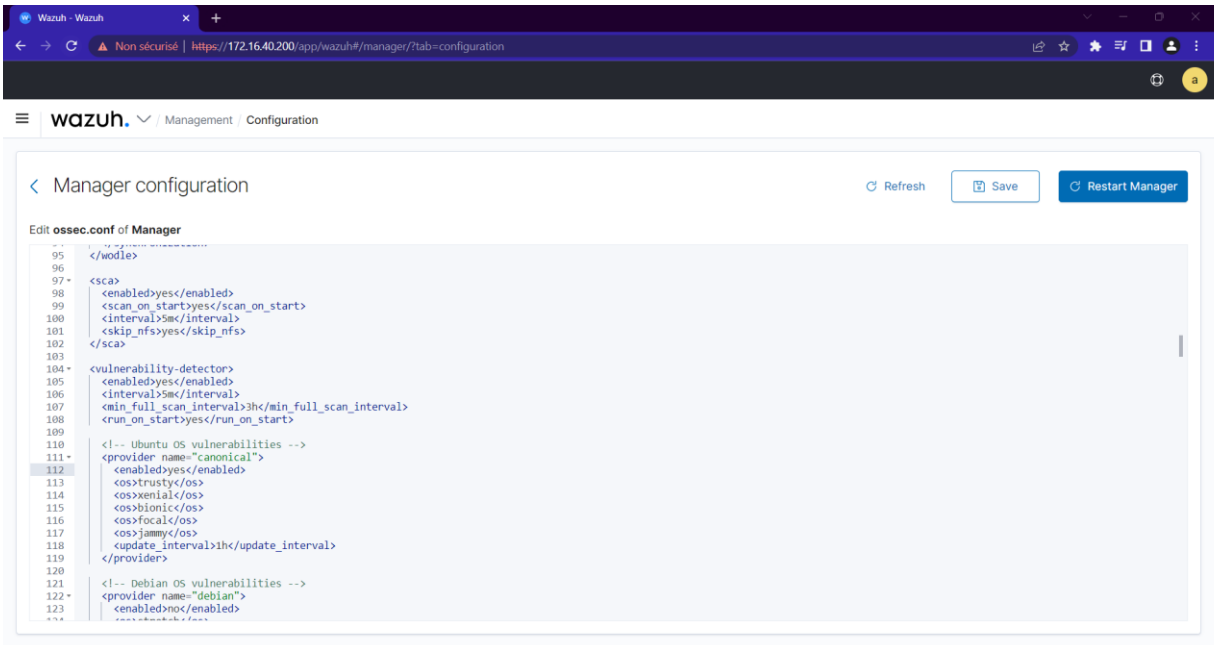
To be able to detect vulnerabilities, agents can natively collect a list of installed applications (System inventory), sending it periodically to the manager. Also, the manager builds a global vulnerability database from publicly available CVE repositories.

Vulnerability detector is enabled by default, but only Windows system that can be scanned, so we need to enable vulnerability detector for the other systems we need to scan.

To do that we will go edit the config file in: Management > Configuration (as shown in previous section), scroll down until you see vulnerability detector section.

Enable each system you want by modifying the value <enabled> by yes.

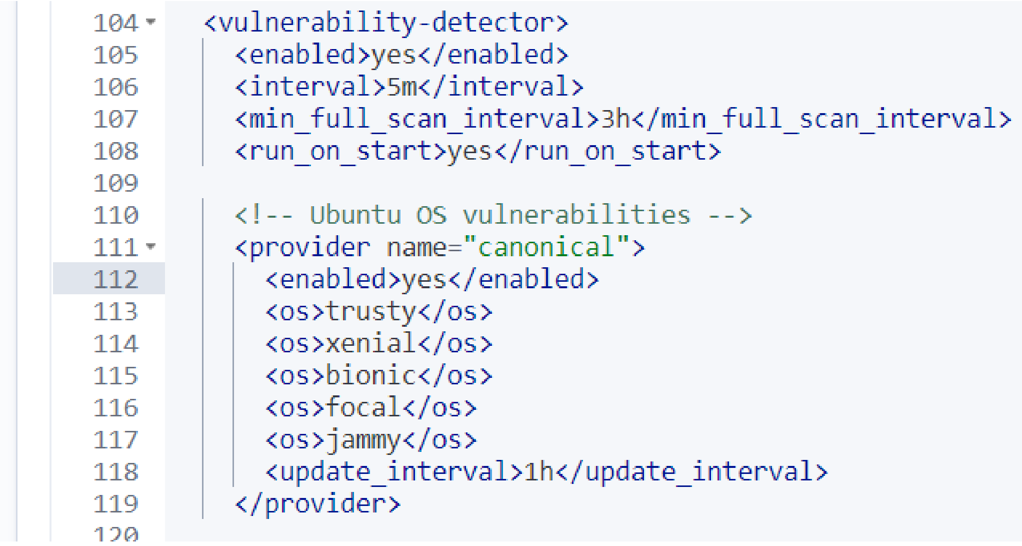
You can also edit the interval of time between scans, the interval of doing update…


Wazuh - Wazuh
Non sécurisé | https://172.16.40.200/app/wazuh#/manager/?tab=configuration
wazuh.
Management / Configuration
Refresh
Save
Restart Manager

Manager configuration

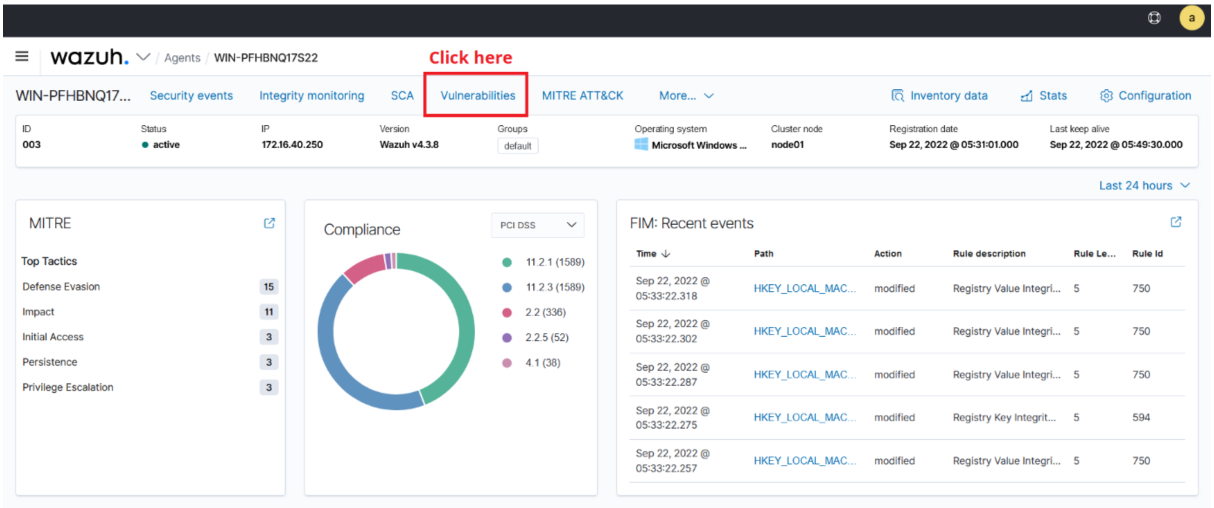
Edit **ossec.conf** of **Manager**

```
</wodle>

<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>5m</interval>
  <skip_nfs>yes</skip_nfs>
</sca>

<vulnerability-detector>
  <enabled>yes</enabled>
  <interval>5m</interval>
  <min_full_scan_interval>3h</min_full_scan_interval>
  <run_on_start>yes</run_on_start>

  <!-- Ubuntu OS vulnerabilities -->
  <provider name="canonical">
    <enabled>yes</enabled>
    <os>trusty</os>
    <os>xenial</os>
    <os>bionic</os>
    <os>focal</os>
    <os>jammy</os>
    <update_interval>1h</update_interval>
  </provider>

  <!-- Debian OS vulnerabilities -->
  <provider name="debian">
    <enabled>no</enabled>
```



```
<vulnerability-detector>
  <enabled>yes</enabled>
  <interval>5m</interval>
  <min_full_scan_interval>3h</min_full_scan_interval>
  <run_on_start>yes</run_on_start>

  <!-- Ubuntu OS vulnerabilities -->
  <provider name="canonical">
    <enabled>yes</enabled>
    <os>trusty</os>
    <os>xenial</os>
    <os>bionic</os>
    <os>focal</os>
    <os>jammy</os>
    <update_interval>1h</update_interval>
  </provider>
```

To see vulnerabilities of a particular agent we need to select the agent and click on vulnerabilities section.



ID	Status	IP	Version	Groups	Operating system	Cluster node	Registration date	Last keep alive
003	● active	172.16.40.250	Wazuh v4.3.8	default	Microsoft Windows ...	node01	Sep 22, 2022 @ 05:31:01.000	Sep 22, 2022 @ 05:49:30.000

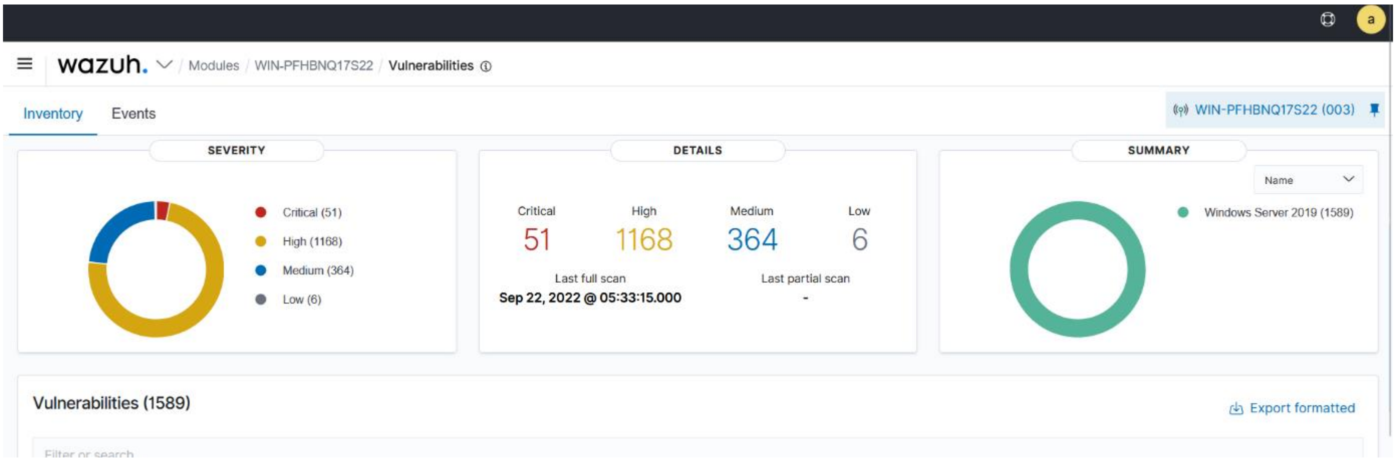
MITRE

Top Tactics	
Defense Evasion	15
Impact	11
Initial Access	3
Persistence	3
Privilege Escalation	3

FIM: Recent events

Time ↓	Path	Action	Rule description	Rule Le...	Rule Id
Sep 22, 2022 @ 05:33:22.318	HKEY_LOCAL_MAC...	modified	Registry Value Integri...	5	750
Sep 22, 2022 @ 05:33:22.302	HKEY_LOCAL_MAC...	modified	Registry Value Integri...	5	750
Sep 22, 2022 @ 05:33:22.287	HKEY_LOCAL_MAC...	modified	Registry Value Integri...	5	750
Sep 22, 2022 @ 05:33:22.275	HKEY_LOCAL_MAC...	modified	Registry Key Integrit...	5	594
Sep 22, 2022 @ 05:33:22.257	HKEY_LOCAL_MAC...	modified	Registry Value Integri...	5	750

As we can see this agent have the following vulnerabilities.



DETAILS

Critical	High	Medium	Low
51	1168	364	6

Last full scan
Sep 22, 2022 @ 05:33:15.000

Last partial scan
-

Vulnerabilities (1589)

You can also check the Log management section, you can enable File Integrity Monitoring, and also integrate VirusTotal...

Good luck.