WAZUH MANAGER VIRTUAL LAB SETUP

& Endpoint Policy Configuration

Using **VMware Workstation Pro 17.5** on **Windows 10** Host
With **Kali OS VM** & **Windows Server 2022 VM** Endpoints

Jeffrey Obi
December 2025

Contents

Introduction

Background

Wazuh is a free and open source security platform that provides **extended detection and response** (aka **XDR**) protection, as well as **SIEM** protection for endpoints, network devices, containers and cloud environments.

Wazuh is a relatively simple to deploy **Security Information and Event Monitoring (SIEM)** tool and its multiple capabilities protect devices and network environments for homes and organizations. Via security configuration, it is implemented in supporting **organizational security posture** as well as **compliance** with regulations and standards, while keeping **logs** which ensure **accounting** of activities carried out on monitored devices and in monitored environments.

Goals

In this document, **Wazuh** is deployed in the local lab environment, inside the host machine **(Windows 10 x64).** The **Wazuh** server is added to the virtualizer **(VMware Workstation Pro 17.5)** as a virtual machine for local hosting. Advantages of this deployment include:

- full control,
- easier customization,
- lower cost, privacy and
- avoidance of bandwidth and network connectivity limitations.

The deployed **SIEM tool** will provide monitoring services for endpoints which will be connected via installed **agents.**

First, the Wazuh virtual machine is downloaded to the host machine **(Windows 10 x64),** added to the virtualizer **(VMware Workstation Pro 17.5)** and configured. The endpoints are then configured with added agents, followed by the configuration, testing and examination of some policies.

Current Stack

Host machine:	**Windows 10 x64**
Virtualizer:	**VMware Workstation Pro 17.5**
Virtual Machines:	1. **Kali OS VM**
	2. **Windows Server 2022 VM**

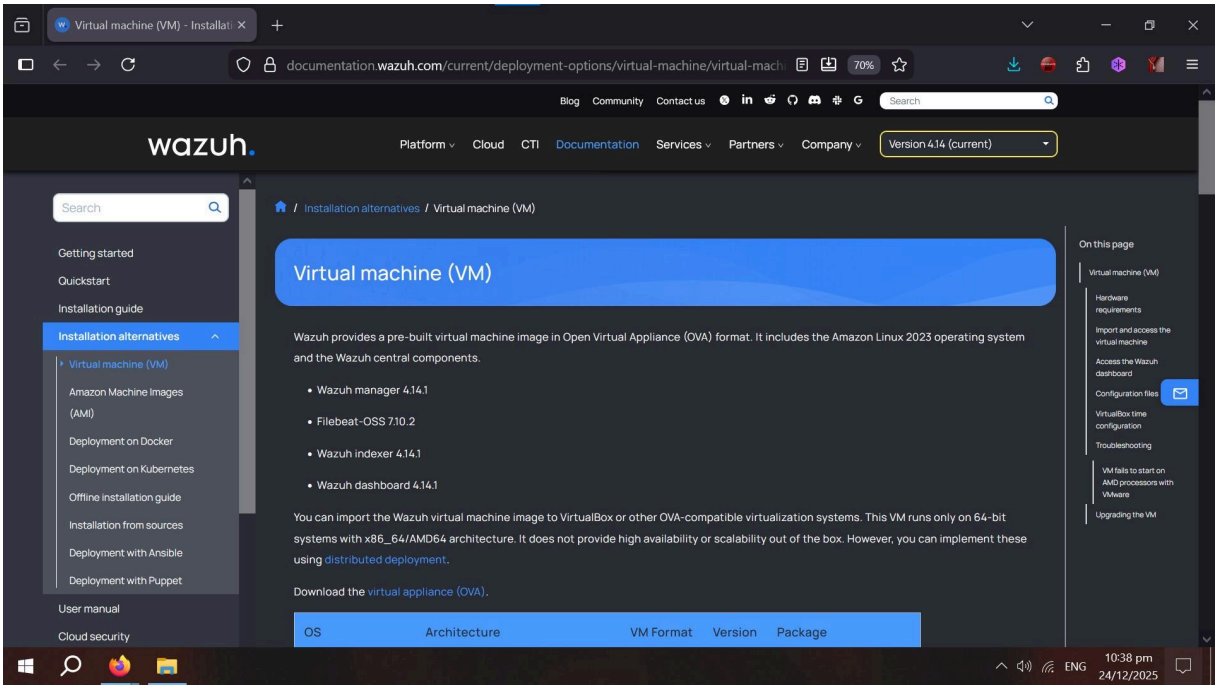
Wazuh Server

Installation, Configuration & Setup

Step 1: Download Wazuh Server

a. On the host machine **(Windows 10 x64)**, launch the browser **(Firefox)**.

b. Visit the Wazuh **Virtual machine (VM) - Installation Alternatives** webpage: `https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html`

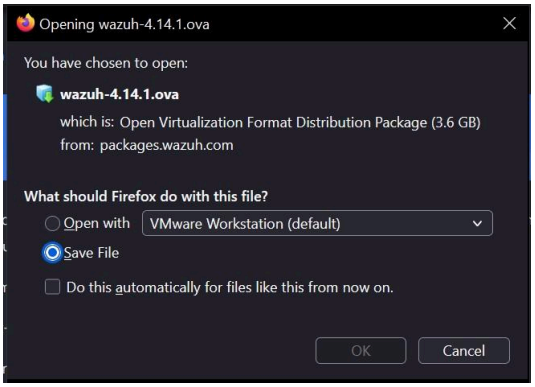


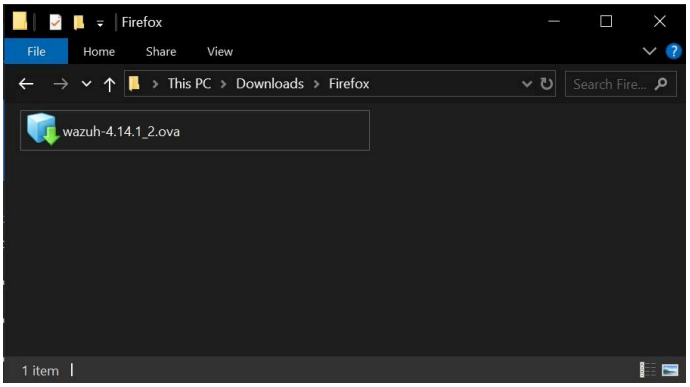
c. Click the Wazuh Virtual Machine download link:

i. On the page, find the table under **"Download the virtual appliance (OVA)."**

ii. Under the **Packages** column, find the **wazuh-4.14.1.ova (sha512)** hyperlink and click it. *This downloads the **wazuh-4.14.1_2.ova** file.*

Note:** An OVA file (Open Virtual Appliance) is a single, compressed archive that packages a virtual machine (VM) along with its configuration, disk images, and other necessary files, making it easy to deploy in virtualizers like the implemented **VMware Workstation Pro 17.5.





Step 2: Configure the Virtualizer Network Environment

a. Launch the virtualizer **(VMware Workstation Pro 17.5)**

b. Launch the **Virtual Network Editor:**

i. Click **Edit** and select **Virtual Network Editor.** *This opens the Virtual Network Editor window.*

c. Configure Virtual Network

i. In the **Virtual Network Editor** window, click **Change Settings** at the bottom right of the window to secure Administrator permissions, in order to modify the network configuration.

ii. In the network adapter data-grid container at the top, select **VMnet8.**

iii. Under **VMnet Information**, ensure **NAT** is selected.

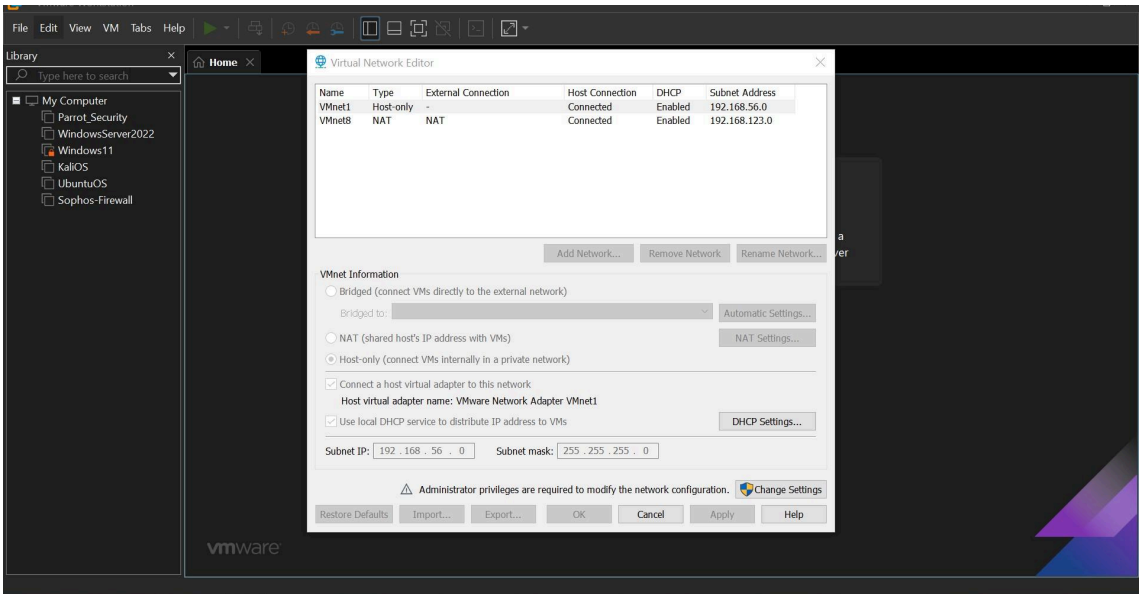
iv. Check the **Use local DHCP service to distribute IP addresses to VMs** box.

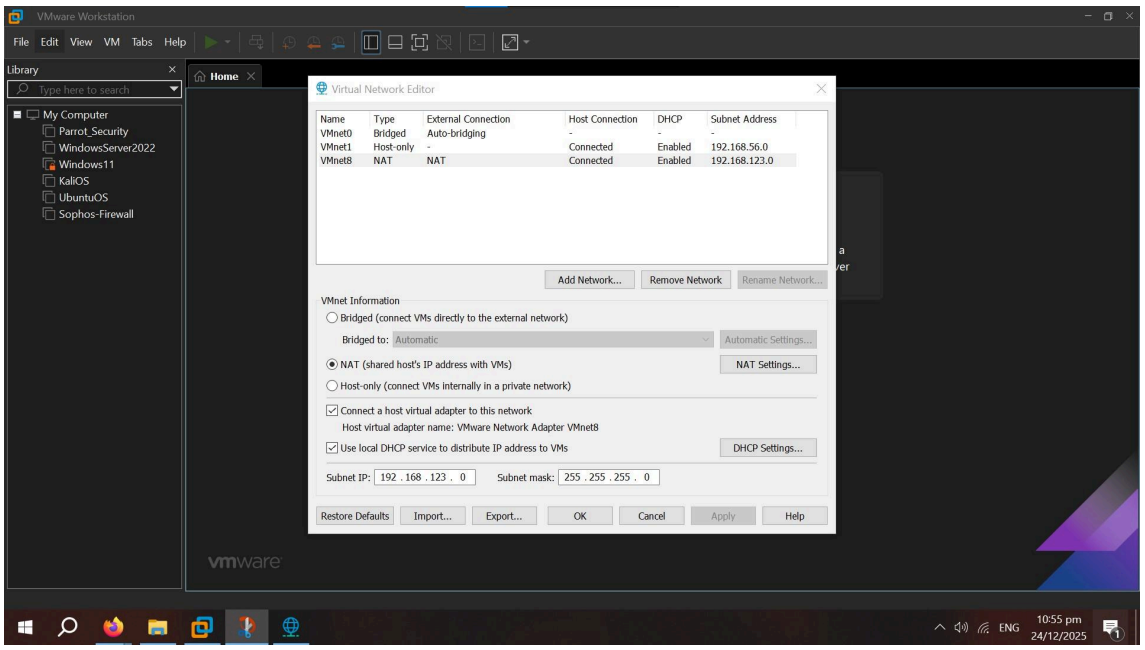
v. Check the **Connect a host virtual adapter to this network** box.

vi. In the **Subnet IP** text box, input `192.168.123.0` (to determine the subnet).

vii. In the **Subnet mask** text box, input `255.255.255.0` (to determine the subnet mask).

viii. Click **Apply** then click **OK**.



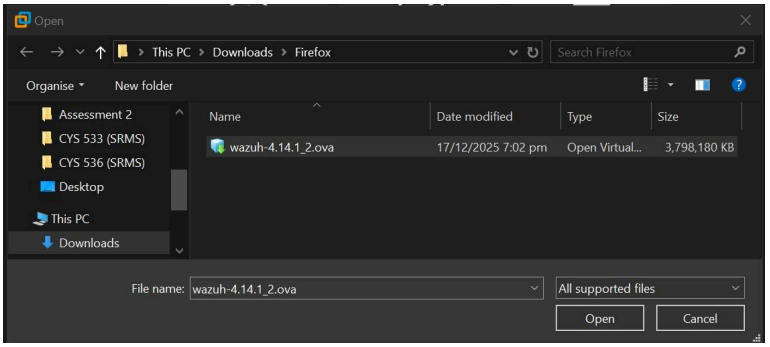


Step 3: Import Wazuh Virtual Machine into Virtualizer

a. Open the Wazuh Virtual Machine.

i. Click **File** then click **Open.**

ii. Locate the downloaded **wazuh-4.14.1_2.ova** file. Select it and click **Open.** *This opens an **Import Virtual Machine** wizard*



b. Configure the Virtual Machine Setup.

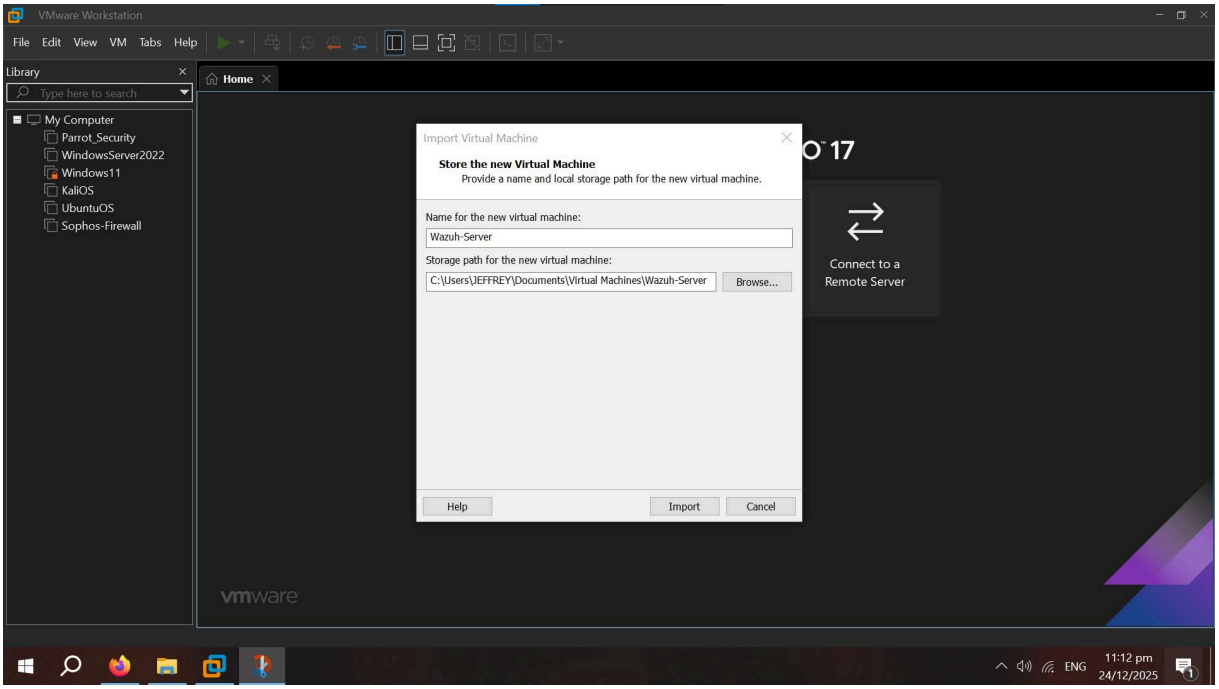
i. On the **Import Virtual Machine** wizard, the first window is **Store the new virtual machine.**

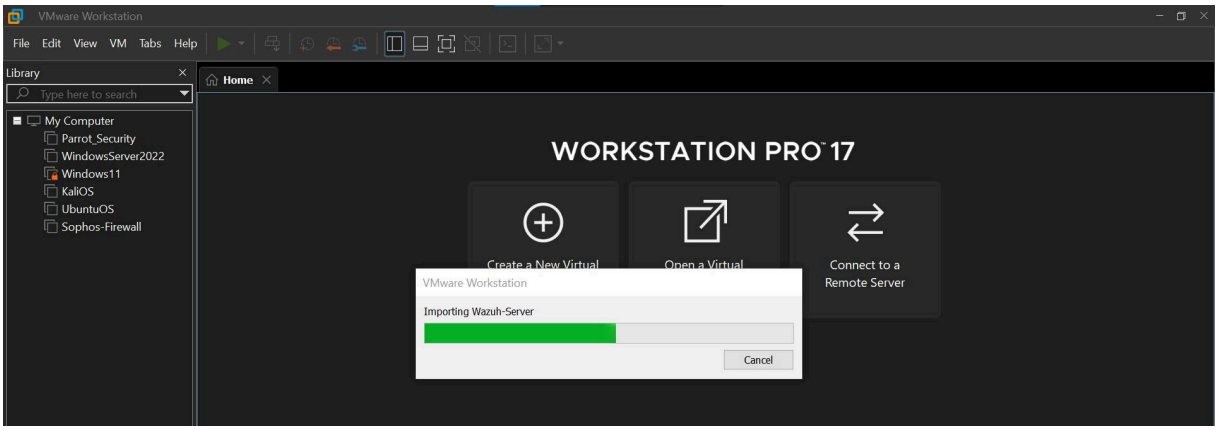
ii. In the **Name for the new virtual machine:** text box, create a name for the virtual machine **(Wazuh-Server)** and input it.

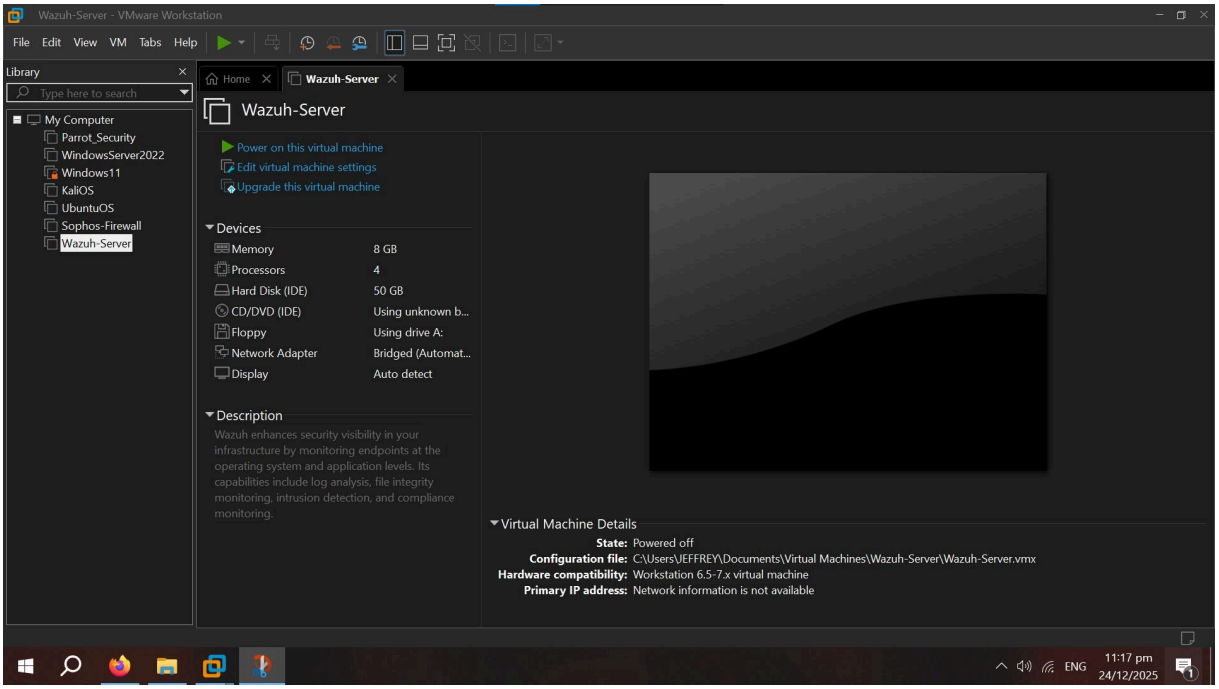
iii. In the **Storage path for the new virtual machine:** text box, type the file path for virtual machine storage path.

iv. Click the **Import** button. *This opens an **Importing Wazuh-Server** progress bar detailing the progress level of the importation process.*

v. When the progress bar completes and then disappears, **Wazuh-Server** virtual machine appears added to the **Library** panel on the **VMware Workstation Pro 17.5** UI, and a **Wazuh-Server** tab is opened.


VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Parrot_Security
WindowsServer2022
Windows11
KaliOS
UbuntuOS
Sophos-Firewall
Home
Import Virtual Machine
Store the new Virtual Machine
Provide a name and local storage path for the new virtual machine.
Name for the new virtual machine:
Wazuh-Server
Storage path for the new virtual machine:
C:\Users\JEFFREY\Documents\Virtual Machines\Wazuh-Server
Browse...
Help
Import
Cancel
Connect to a Remote Server
vmware
ENG
11:12 pm
24/12/2025


VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Parrot_Security
WindowsServer2022
Windows11
KaliOS
UbuntuOS
Sophos-Firewall
Home
WORKSTATION PRO 17
Create a New Virtual
Open a Virtual
Connect to a Remote Server
VMware Workstation
Importing Wazuh-Server
Cancel



Step 4: Access the Wazuh Server Dashboard

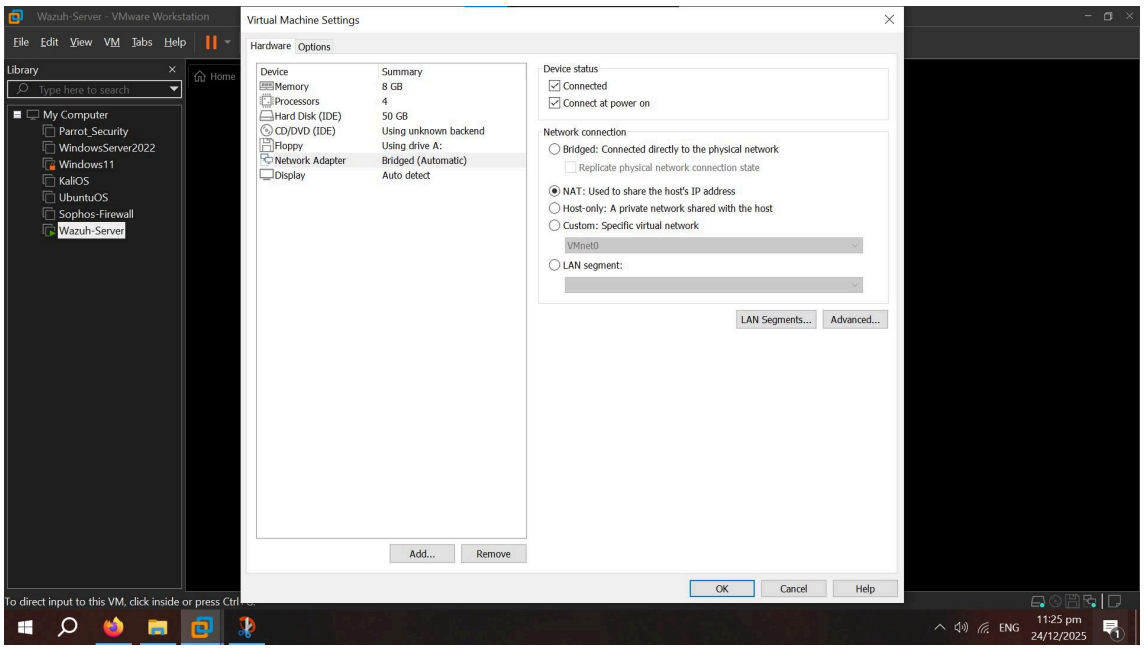
a. Configure Wazuh Virtual Machine Network Settings

i. In the **Wazuh-Server** tab, select **Edit virtual machine settings**. *This opens the **Virtual Machine Settings** window.*

ii. In the ***Virtual Machine Settings*** *window,* there is a **Device** data-grid box. Select **Network Adapter**.

iii. On the right side of the data-grid box, find a **Network connection** section. Select the **NAT** button.

iv. Click the **OK** button at the bottom of the window. *This returns you to the **Wazuh-Server** tab.*



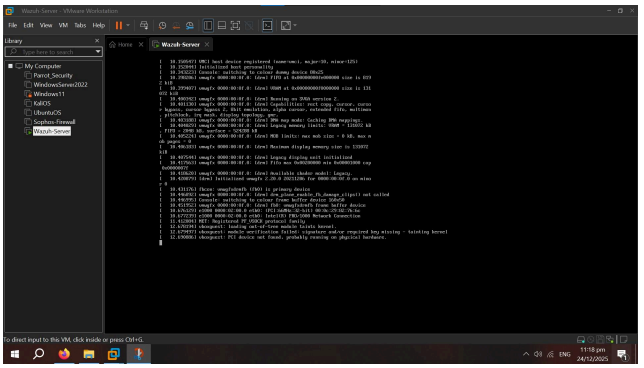
b. Launch the Wazuh Virtual Machine

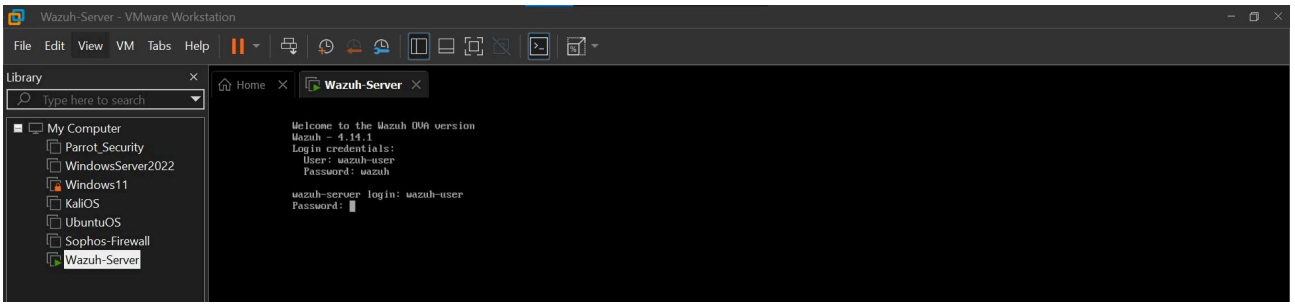
i. In the **Wazuh-Server** tab, select **Power on this virtual machine**. *This launches the* **Wazuh-Server *Virtual Machine***.

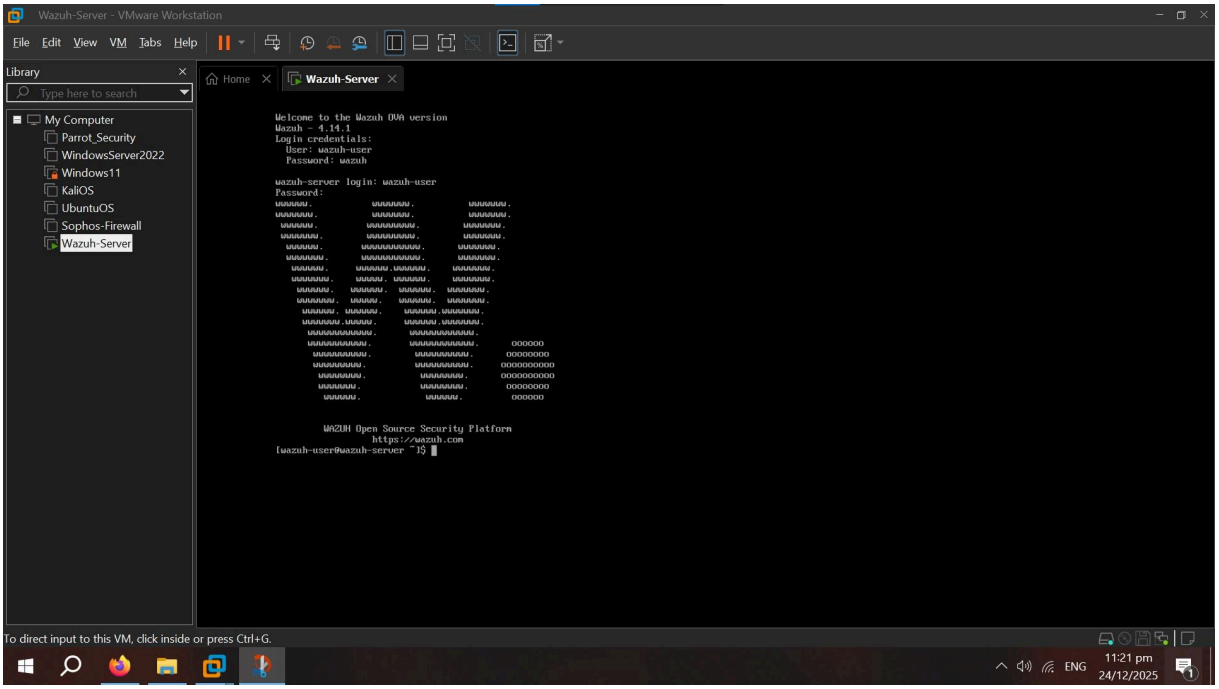
ii. The virtual machine presents with a **Command Line Interface (CLI)** and opens, running through commands, until it gets to the login page.

iii. In the login page titled **Welcome to the Wazuh OVA version Wazuh - 4.14.1,** enter the required credentials for the following categories:

- For **wazuh-server login,** input **`wazuh-user`**. Press **Enter**.
- For **password,** input **`wazuh`**. Press **Enter**. *This reveals a text-based graphic of the* ***Wazuh*** *logo and grants access to the virtual machine terminal.*







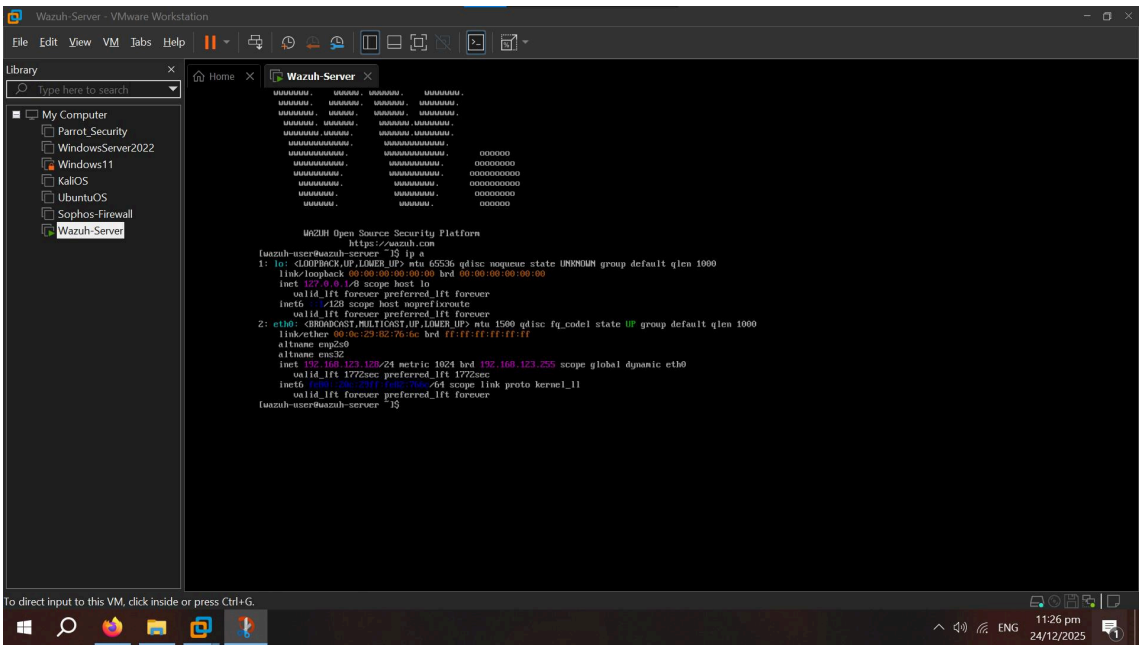
c. Retrieve the virtual Machine IP address

i. In the **Wazuh-Server Virtual Machine** terminal, type and run the command:

```
ip a
```

ii. This command returns network information about the virtual machine, including its IP address: **192.168.123.128**

This IP address would be used to access the Wazuh web-console from the browser.



d. Log-in to the Web Console

i. Launch the **Firefox** browser from the host machine **(Windows 10 x64).**

ii. In the address bar, type in the **Wazuh-Server Virtual Machine** IP address**:**

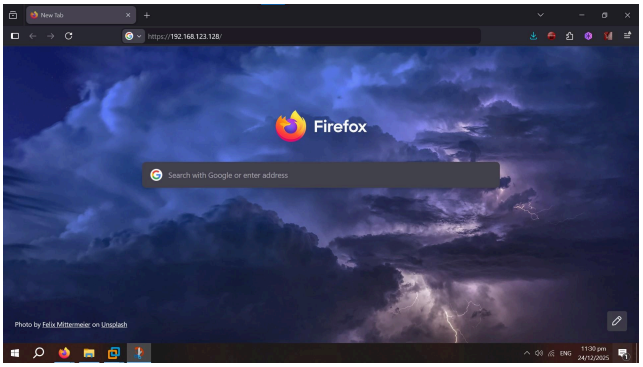
192.168.123.128

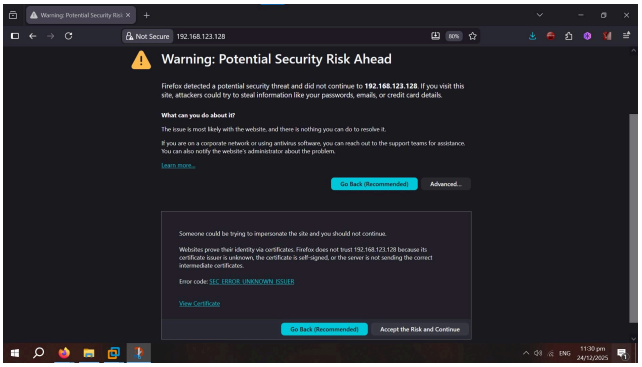
Press **Enter.**

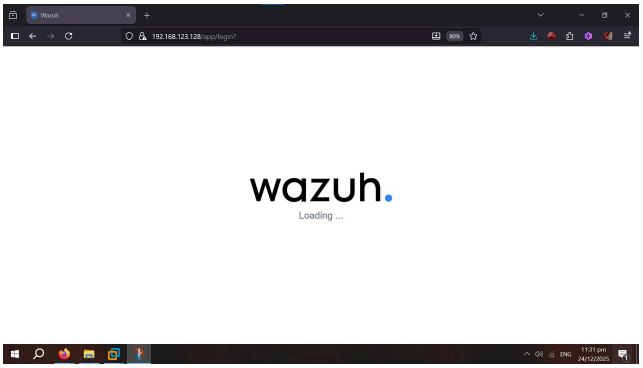
iii. The browser returns a warning about a potential security risk regarding the link. This is because the IP is being accessed via an unprotected web port (HTTPS). It is safe, so proceed. *This opens a loading page with the Wazuh logo.*

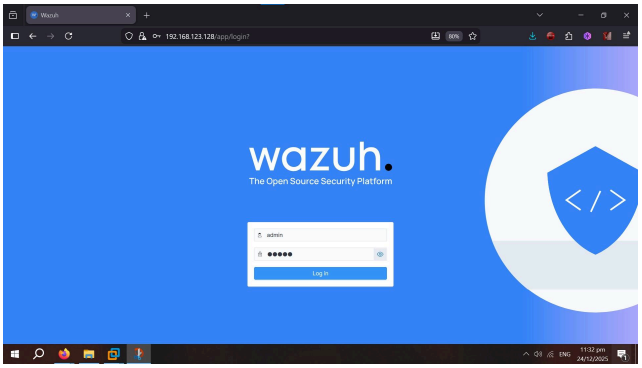
iv. The Wazuh loading page leads to a login page. Input the following credentials:
   - **Username** (first text box): **`admin`**
   - **Password** (second text box): **`admin`**

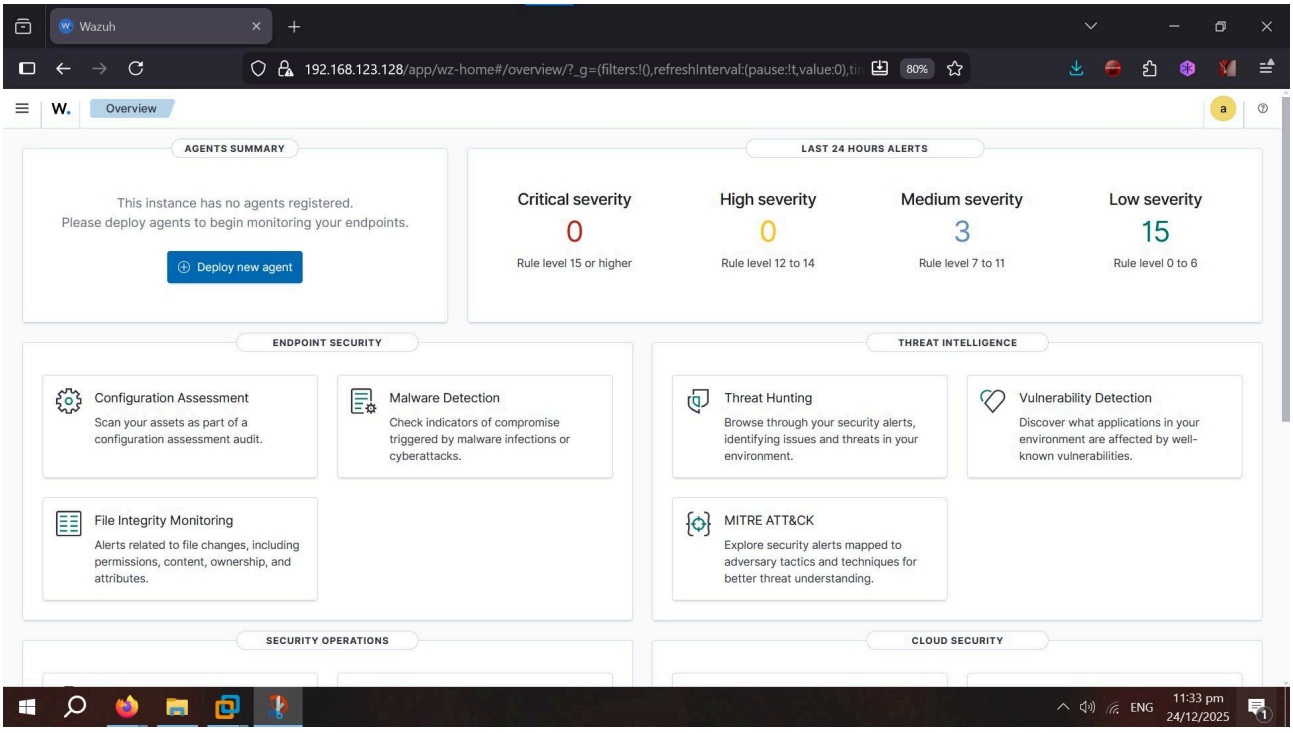
v. Click the **Login** button. *This delivers the **Overview** page of the web console.*











Wazuh Agents

Deploying New Agents on Endpoints

Step 5: Add Agent (Kali VM Endpoint)

a. Configure Kali Virtual Machine Network Settings:

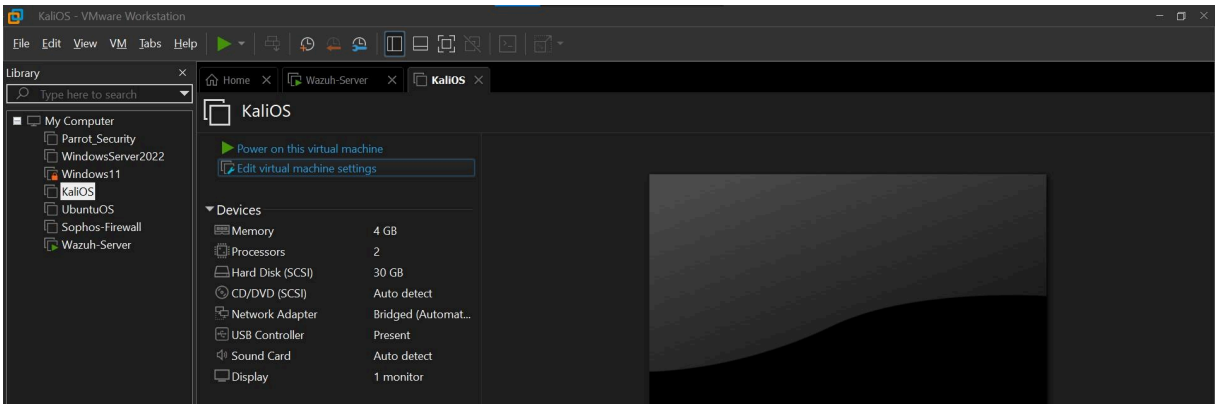
i. In the **Library** panel, select the Kali Virtual Machine **(KaliOS).** *This opens a **KaliOS** tab.*

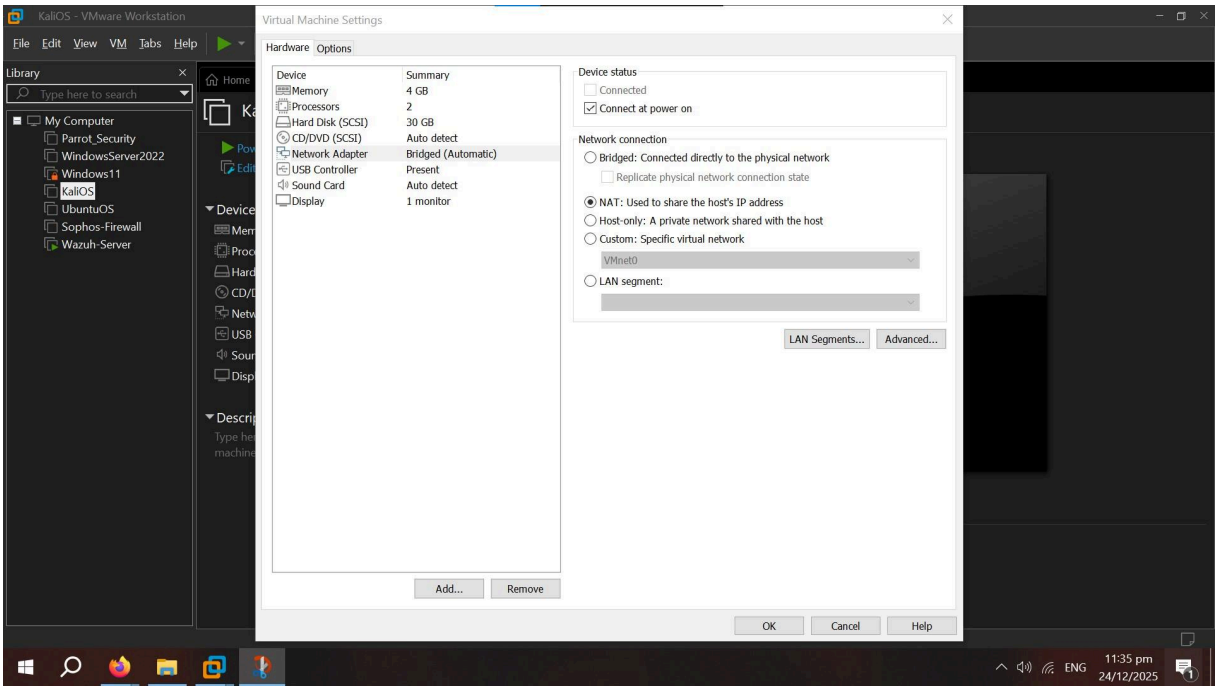
ii. In the **KaliOS** tab, select **Edit virtual machine settings**. *This opens the **Virtual Machine Settings** window.*

iii. In the ***Virtual Machine Settings*** *window,* there is a **Device** data-grid box. Select **Network Adapter**.

iv. On the right side of the data-grid box, find a **Network connection** section. Select the **NAT** button.

v. Click the **OK** button at the bottom of the window. *This returns you to the **KaliOS** tab.*

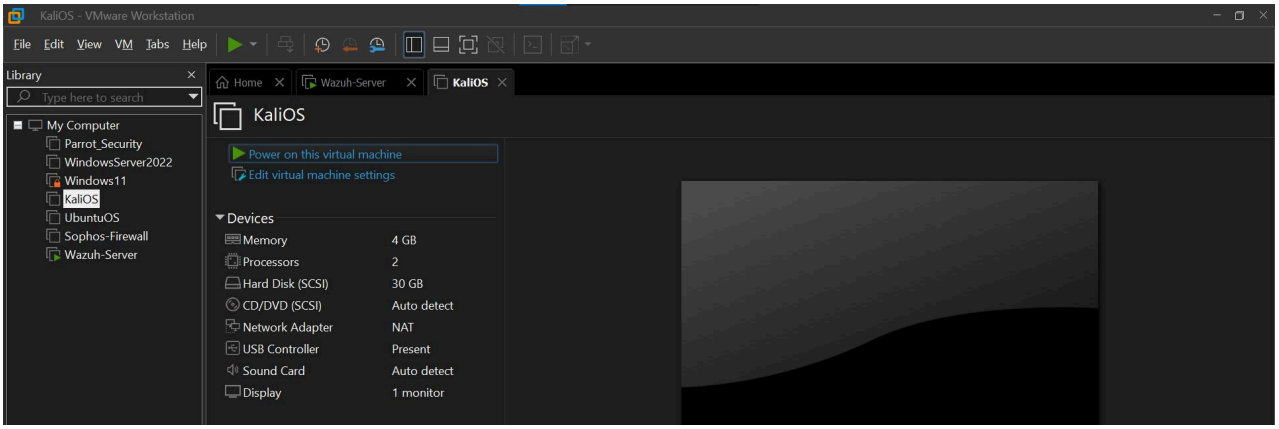


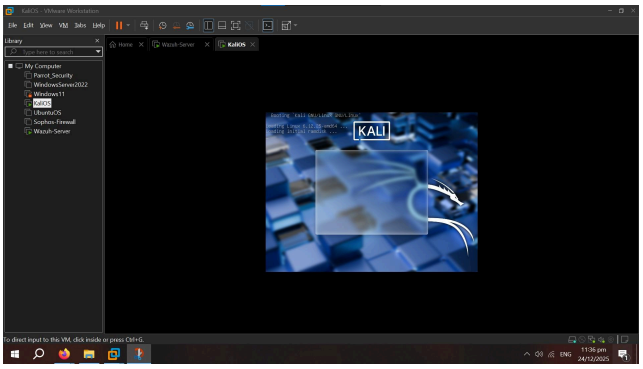


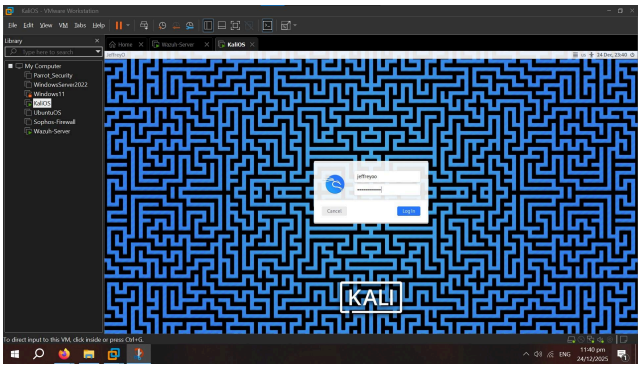
b. Launch the KaliOS Virtual Machine

i. In the **KaliOS** tab, select **Power on this virtual machine**. *This launches the* **KaliOS *Virtual Machine***.

ii. The virtual machine boots through a GNU prompt and some loading screens to a sign-in screen. Input the username and password in the relevant text boxes and click the **Log In** button. *This grants access to the machine and launches the* ***Desktop*** *screen*.







c. Check Connectivity from KaliOS to Wazuh-Server Virtual Machines:

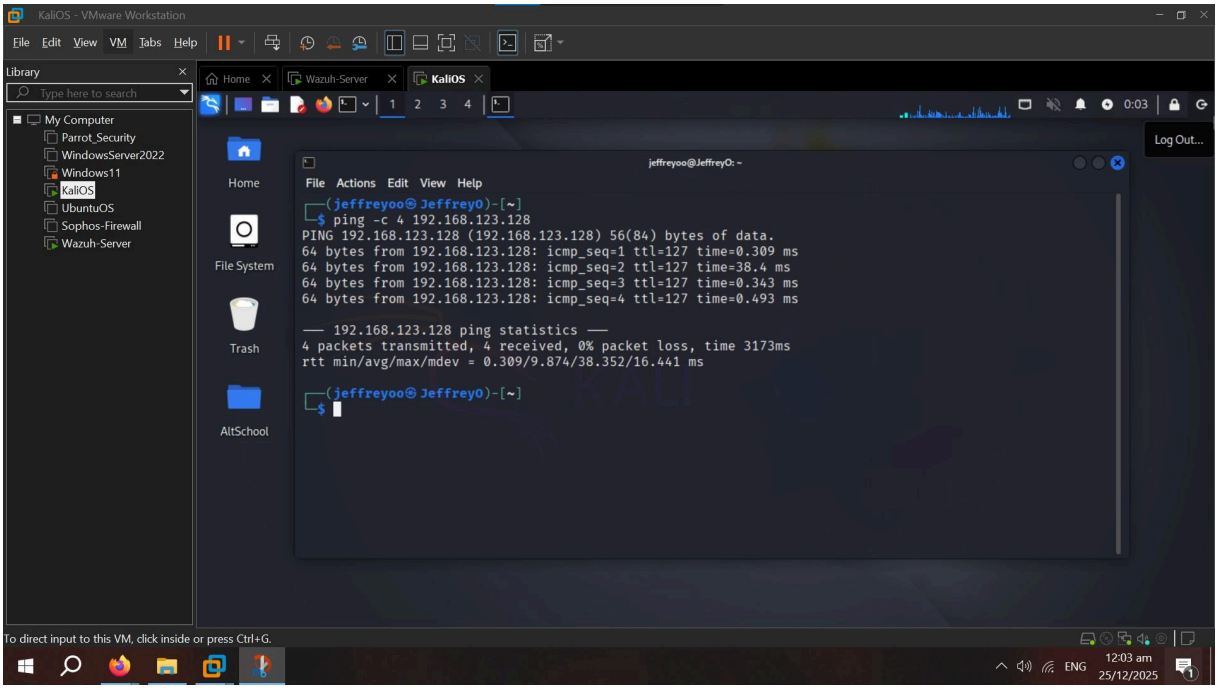
i. From the **KaliOS** Desktop screen, launch the **Terminal** by clicking the icon from the taskbar.

ii. In the **Terminal,** type the following command to ping the Wazuh-Server virtual machine with 4 ICMP echo request packets:

```
ping -c 4 192.168.123.128
```

iii. The command returned a success, indicating all 4 packets returned, with 0% packets lost.

iv. Connectivity is confirmed.



d. Access the Wazuh-Server Web-Console from Kali Virtual Machine:

i. Close the **Terminal** window and return to the **Desktop** screen.

ii. Click the **Firefox** icon on the taskbar and launch the browser.

iii. On the **Firefox** address bar, type in the **Wazuh-Server Virtual Machine** IP address**:**

`192.168.123.128`

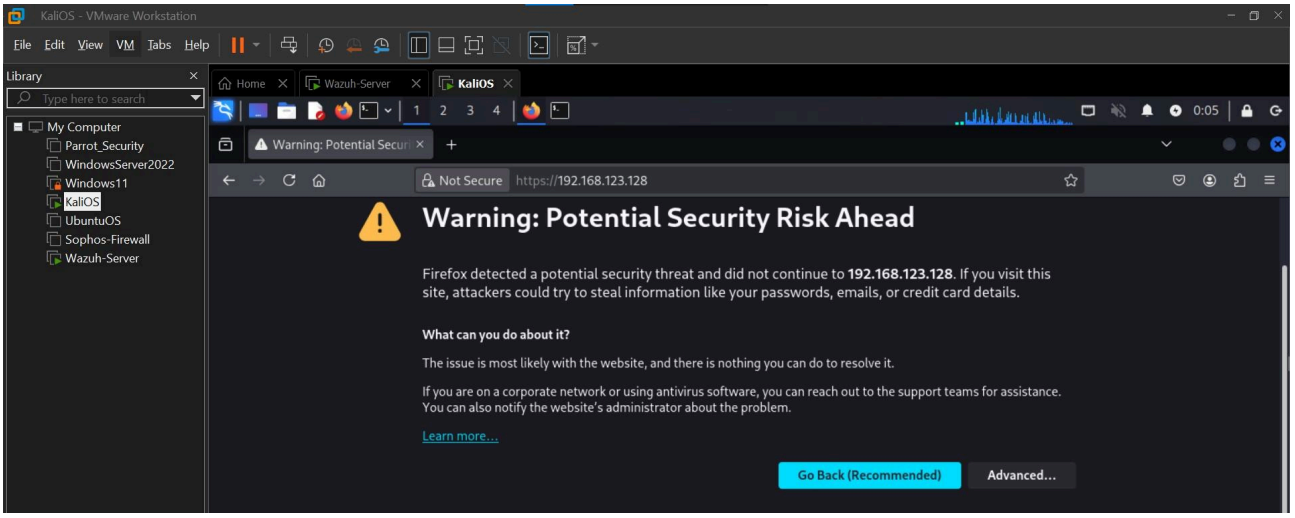
Press **Enter.**

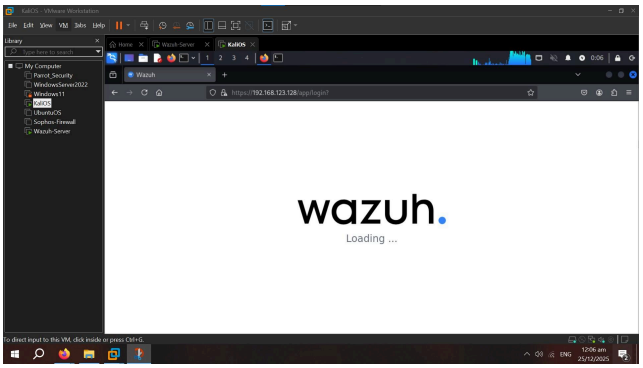
iv. The browser returns a warning about a potential security risk regarding the link. This is because the IP is being accessed via an unprotected web port (HTTPS). It is within a local and safe virtual environment, so proceed. *This opens a loading page with the Wazuh logo.*

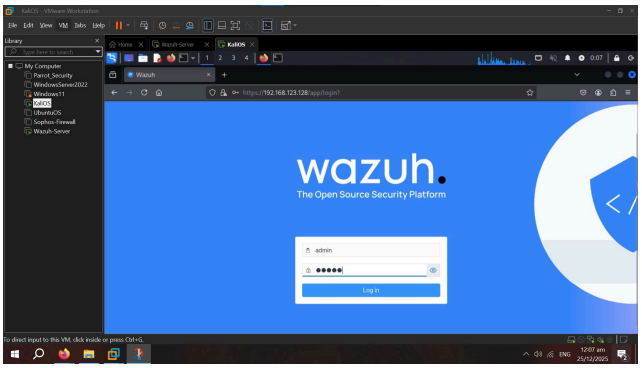
v. The Wazuh loading page leads to a login page. Input the following credentials:

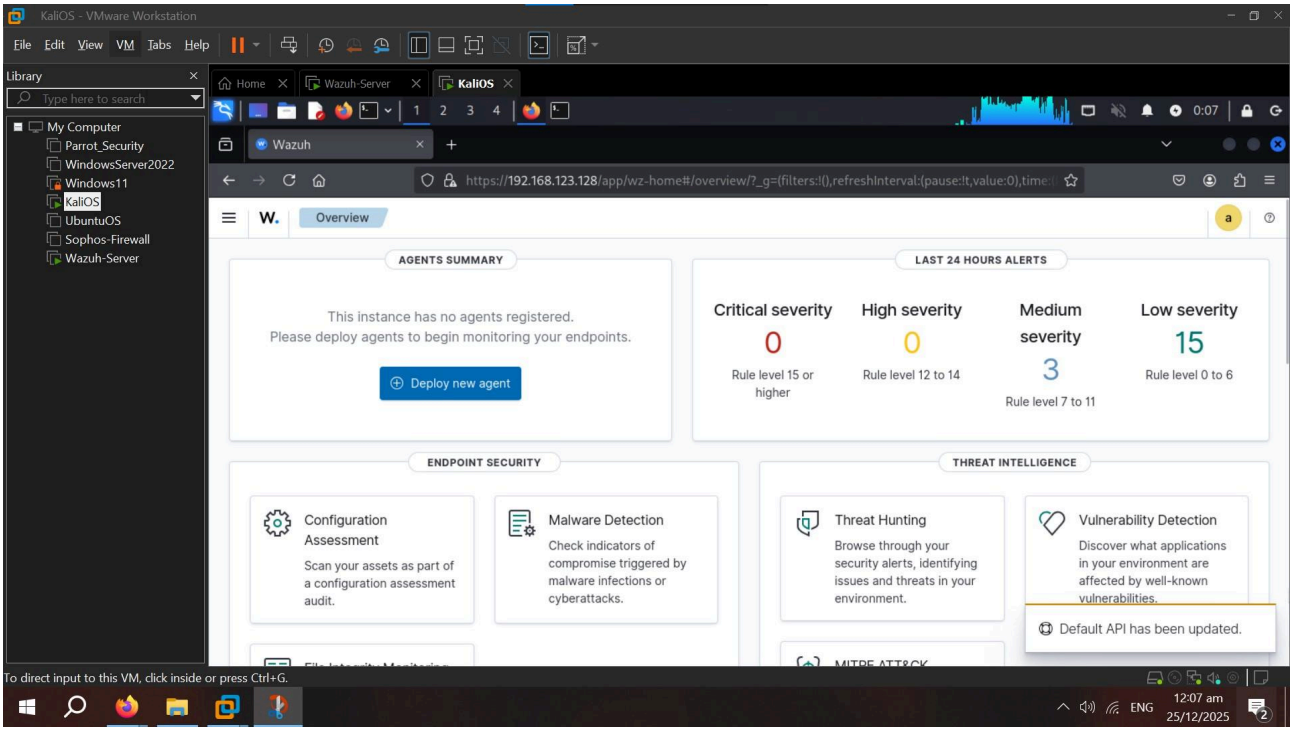
- **Username** (first text box): `admin`
- **Password** (second text box): `admin`

vi. Click the **Login** button. *This delivers the **Overview** page of the web console.*









e. Deploy New Agent to the Kali Virtual Machine:

i. On the **Overview** page, you will find an **Agents Summary** section/widget. Click the **Deploy new agent** button inside it. *This opens a **Deploy new agent** page.*

ii. On the **Deploy new agent** page, configure the following:

- In the **Select the package to download and install on your system** section, select **DEB amd64**
- In the **Server address** section, input the Wazuh-Server address from **(Step 4d)** into the **Assign a server address** text box.
- In the **Optional settings** section, input the KaiOS agent name (Kali-Agent) into the **Assign an agent name** text box.
- Also, in the **Optional settings** section, in the **Select one or more existing groups** drop-down menu, select **default.**
- In the **Run the following commands to download and install the agent** section, there is a command with the option to copy it, as is provided in the user interface. It will look like the following:

```
wget -O -
[https://packages.wazuh.com/key/GPG-KEY-WAZUH](https://packages.wazuh.com/key/GPG-KEY-WAZUH) | gpg
--no-default-keyring --keyring
gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod
644 /usr/share/keyrings/wazuh.gpg && echo "deb
[signed-by=/usr/share/keyrings/wazuh.gpg]
[https://packages.wazuh.com/4.x/apt/](https://packages.wazuh.com/4.x/apt/) stable main" | tee -a
```

```
/etc/apt/sources.list.d/wazuh.list && apt-get update
WAZUH_MANAGER="192.168.126.128" apt-get install wazuh-agent
```

Copy this command.

iii. Keeping the **Firefox** browser open, launch the **Terminal.**

iv. Paste the copied command into the **Terminal** and run it. Agree/comply with any prompts and use your linux password where **sudo** appears necessary. After about a minute, the command finishes running. This installs Wazuh agent on the **KaliOS** virtual machine using configurations based on earlier provided details. *Do not close the **Terminal.***

v. Return to the **Firefox** browser. In the **Deploy new agent** page, continue from Step 5e-ii in the following ways:

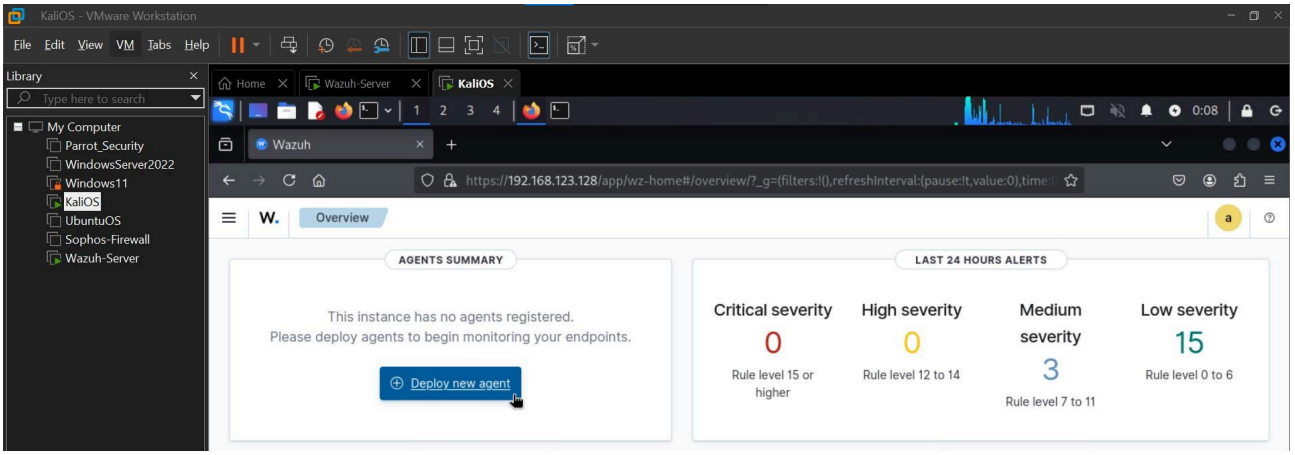
- In the **Start the agent** section, there are 3 commands with the option to copy them, as is provided in the web interface.

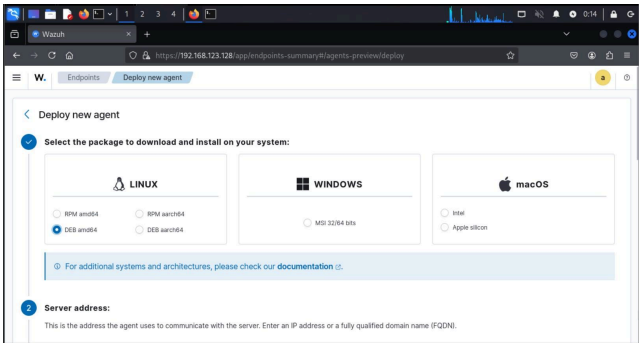
```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

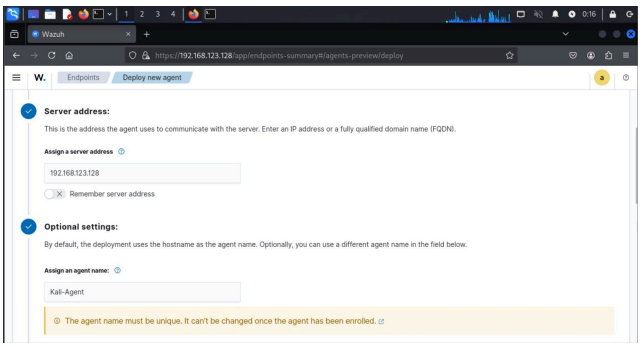
Copy these commands.

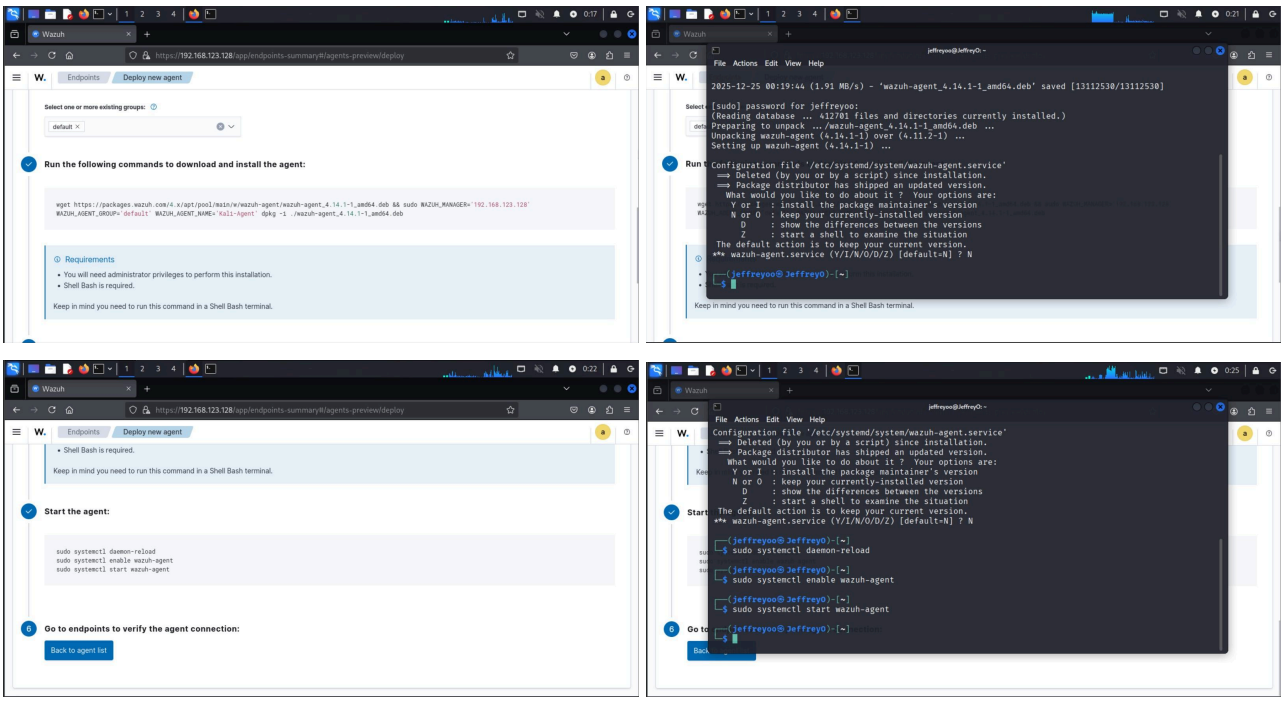
vi. Return to the **Terminal.**

vii. Paste the copied commands into the **Terminal** and run them sequentially. *This enables and starts **Kali-Agent,** the **Wazuh agent** on the **KaliOS** virtual machine.*









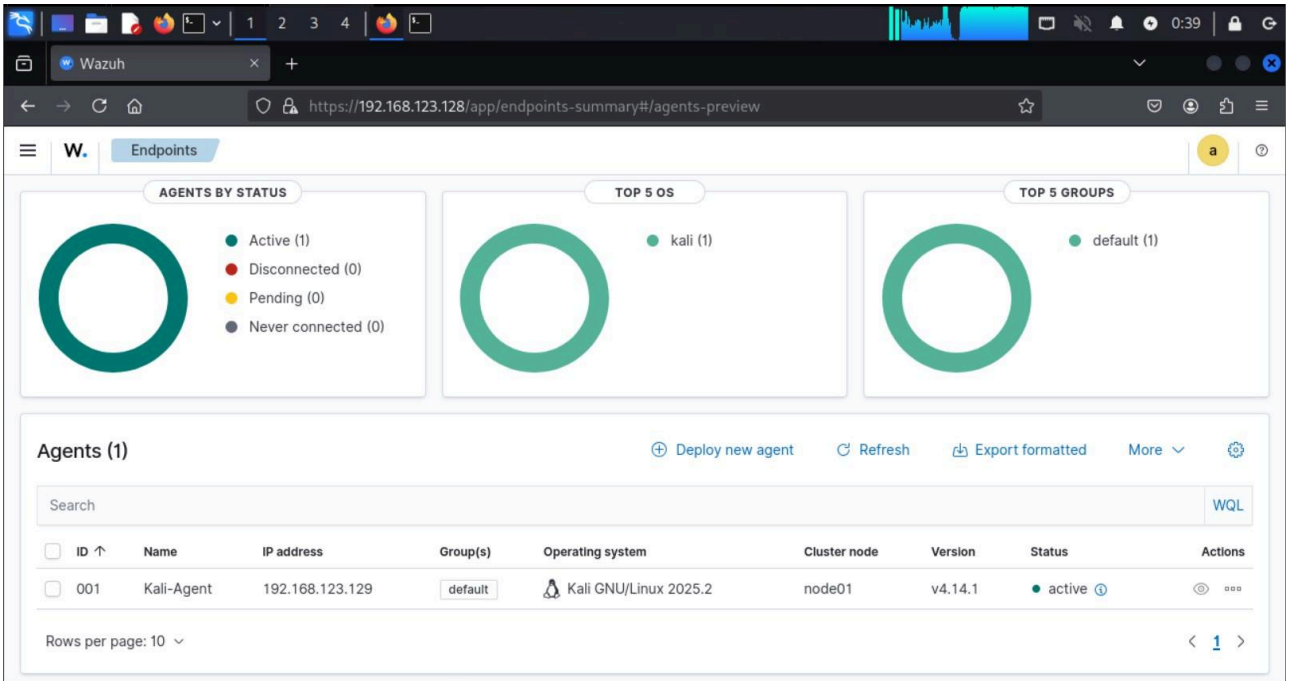
f. Confirm Agent Addition:

i. Return to the **Firefox** browser.

ii. Click the **hamburger/menu icon** in the top left. This brings out a sidebar menu.

iii. In the Sidebar Menu, click the Server Management drop-down menu and click Endpoint Summary. This opens an **Endpoints** page.

iv. In the **Agents by Status** section, there is a "(1)" in front of **Active** [Active (1)], indicating that one agent has been added. Also, in the **Agents** section, the Kali-Agent agent is listed as the sole added agent.



Step 6: Add Agent (Windows Server 2022 VM Endpoint)

a. Configure Windows Server 2022 Virtual Machine Network Settings:

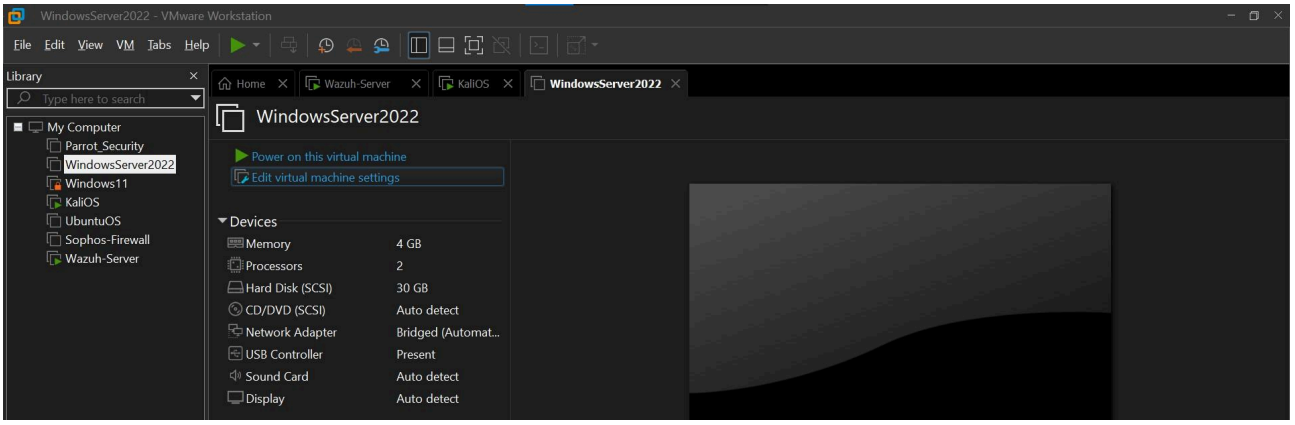
i. In the **Library** panel, select the Windows Server 2022 Virtual Machine **(WindowsServer2022).** *This opens a **WindowsServer2022** tab.*

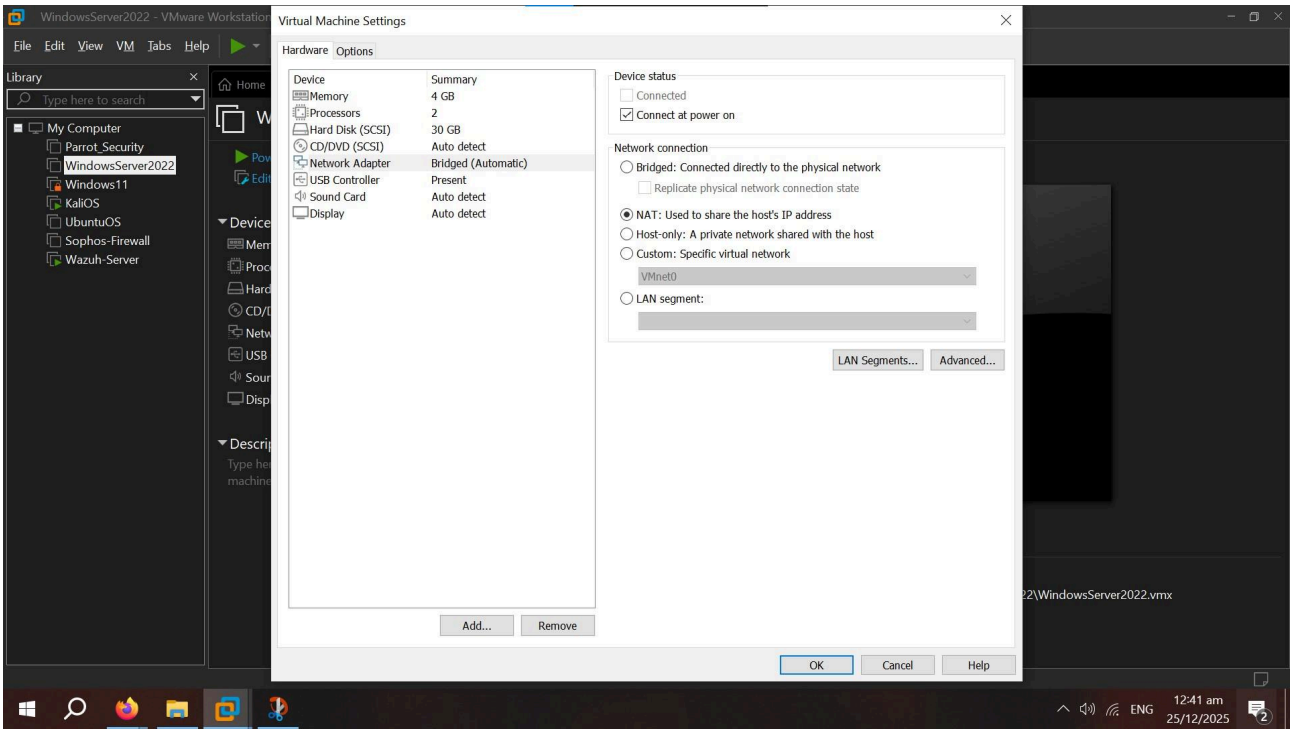
ii. In the **WindowsServer2022** tab, select **Edit virtual machine settings**. *This opens the **Virtual Machine Settings** window.*

iii. In the ***Virtual Machine Settings*** *window,* there is a **Device** data-grid box. Select **Network Adapter**.

iv. On the right side of the data-grid box, find a **Network connection** section. Select the **NAT** button.

v. Click the **OK** button at the bottom of the window. *This returns you to the **WindowsServer2022** tab.*

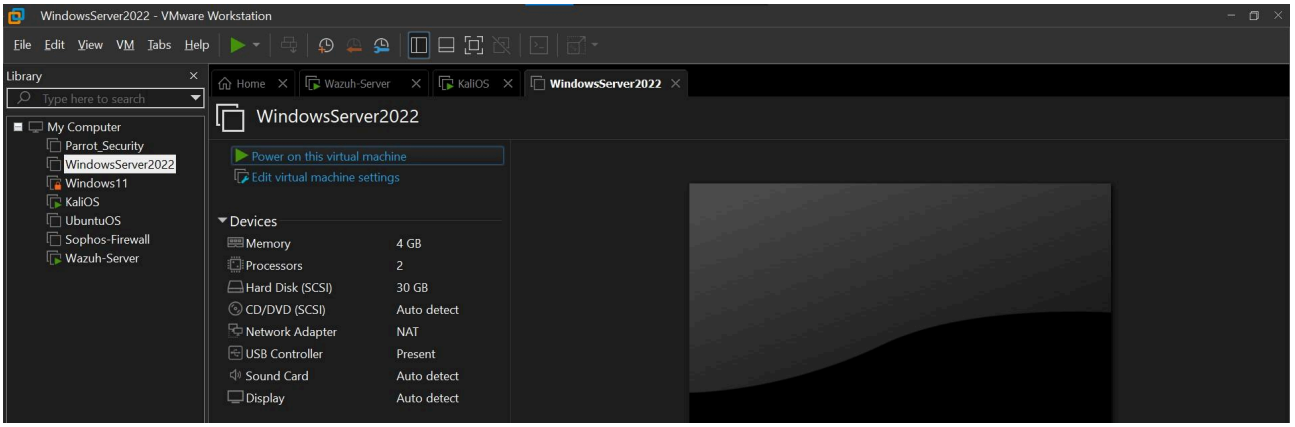


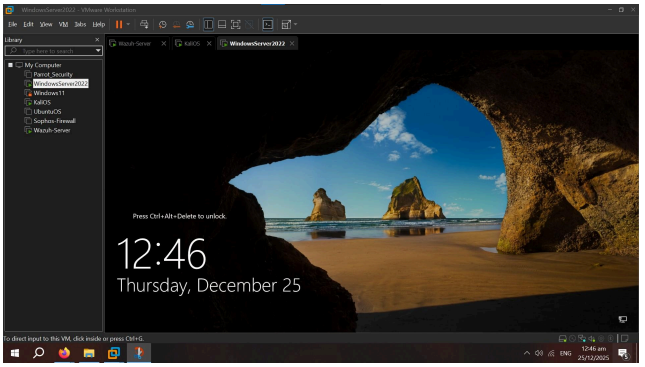


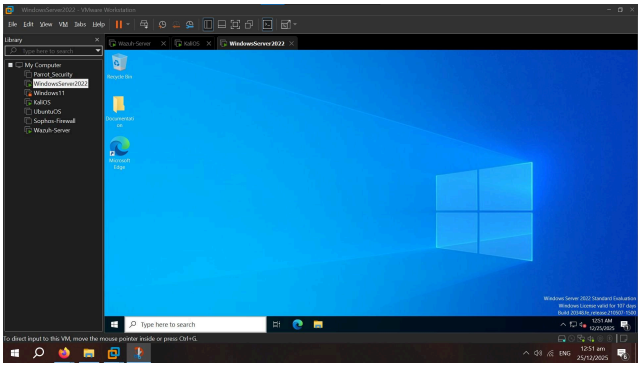
b. Launch the **WindowsServer2022** Virtual Machine

i. In the **WindowsServer2022** tab, select **Power on this virtual machine**. *This launches the* **WindowsServer2022** ***Virtual Machine***.

ii. The virtual machine boots into the sign-in screen. Input the password in the text box and press **Enter**. *This grants access to the machine and launches the* ***Desktop***.







c. Check Connectivity from **WindowsServer2022** to Wazuh-Server Virtual Machines:

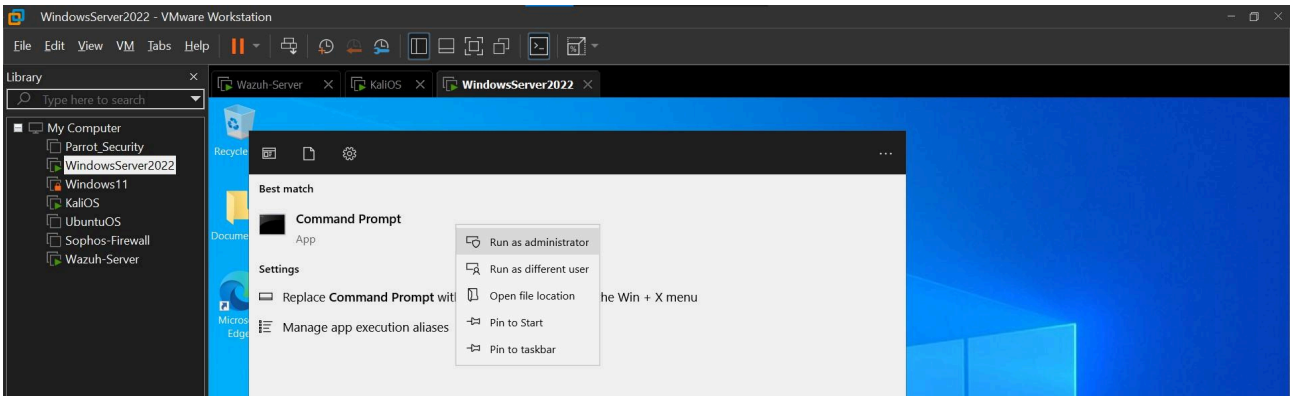
i. Launch the **Start Menu** and search for **Command Prompt.** Right-click the icon and select **Run as administrator.**

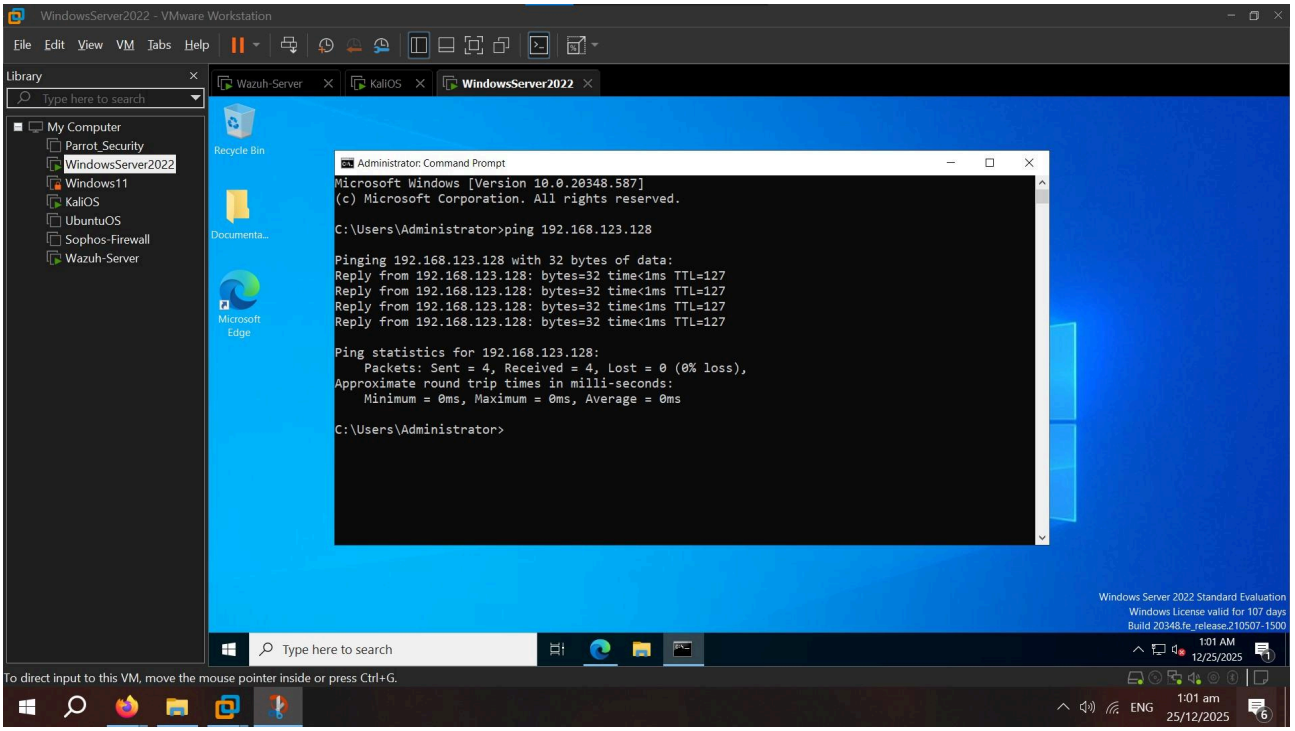
ii. In the **Command Prompt** interface, type the following command to ping the Wazuh-Server virtual machine with 4 ICMP echo request packets:

```
ping 192.168.123.128
```

iii. The command returned a success, indicating all 4 packets returned, with 0% packets lost.

iv. Connectivity is confirmed.





d. Access the Wazuh-Server Web-Console from Kali Virtual Machine:

i. Close the **Command Prompt** window and return to the **Desktop** screen.

ii. Double-click the **Microsoft Edge** icon on the **Desktop** and launch the browser.

iii. In the **Microsoft Edge** address bar, type in the **Wazuh-Server Virtual Machine** IP address**:**

`192.168.123.128`

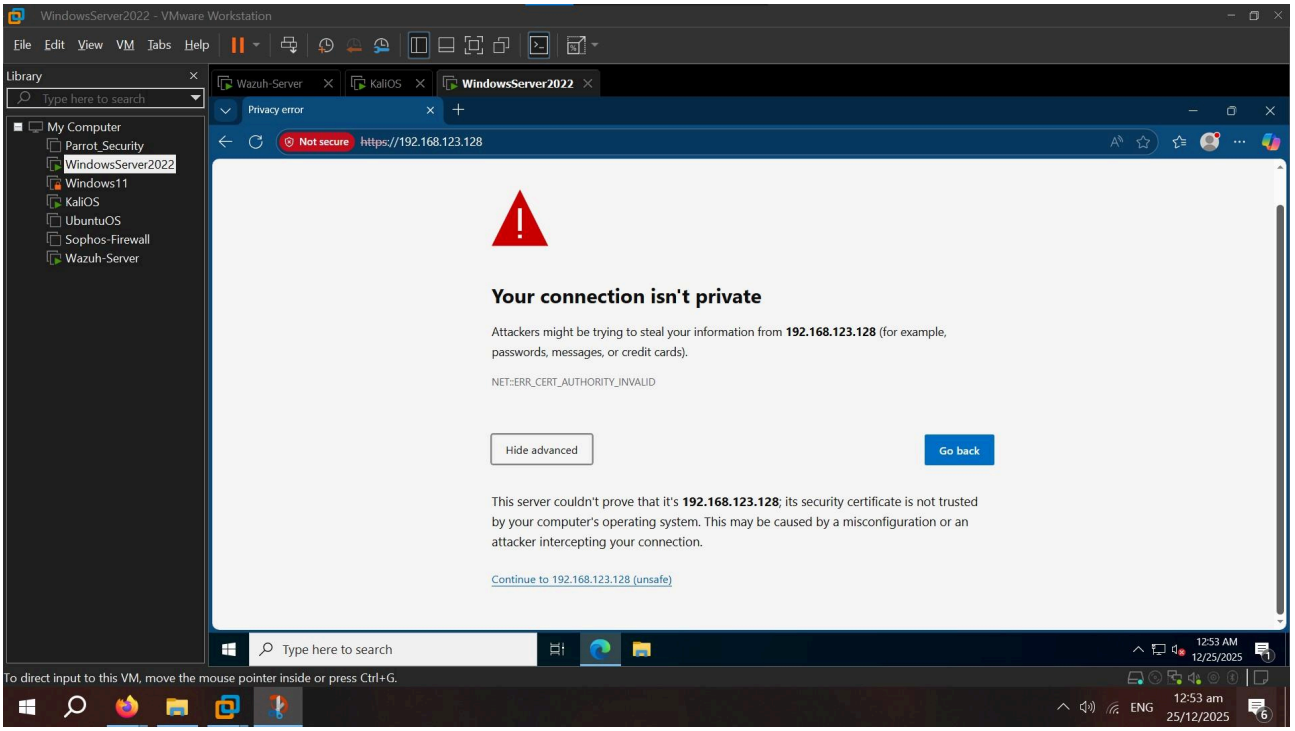
Press **Enter.**

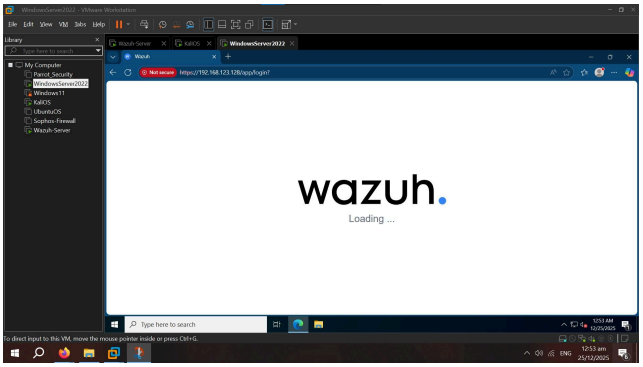
iv. The browser returns a **"Your connection isn't private"** warning about a potential security risk regarding the address. This is because the IP is being accessed via an unprotected web port (HTTPS). It is safe, so proceed. *This opens a loading page with the Wazuh logo.*

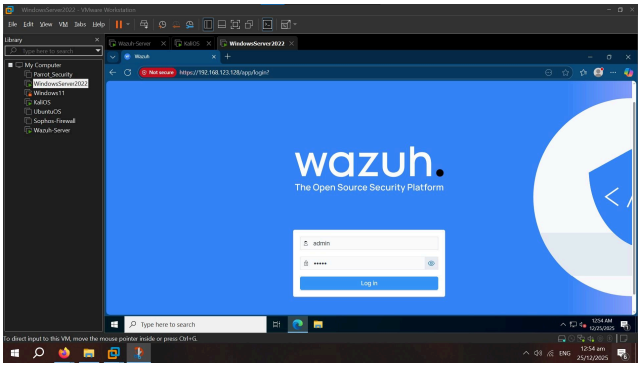
v. The Wazuh loading page leads to a login page. Input the following credentials:

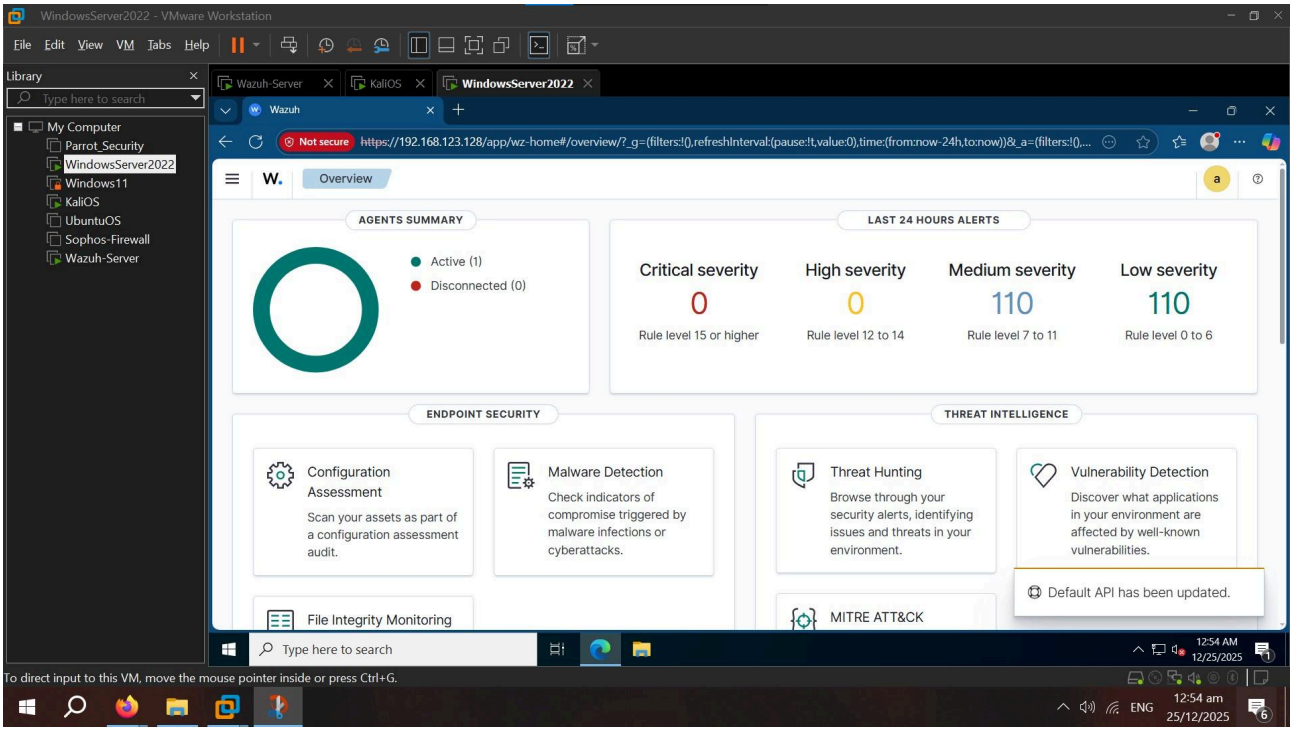
- **Username** (first text box): `admin`
- **Password** (second text box): `admin`

vi. Click the **Login** button. *This delivers the **Overview** page of the web console.*


WindowsServer2022 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Parrot_Security
WindowsServer2022
Windows11
KaliOS
UbuntuOS
Sophos-Firewall
Wazuh-Server
Wazuh-Server
KaliOS
WindowsServer2022
Privacy error
Not secure
https://192.168.123.128
Your connection isn't private
Attackers might be trying to steal your information from 192.168.123.128 (for example, passwords, messages, or credit cards).
NET::ERR_CERT_AUTHORITY_INVALID
Hide advanced
Go back
This server couldn't prove that it's 192.168.123.128; 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 192.168.123.128 (unsafe)
Type here to search
12:53 AM
12/25/2025
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG
12:53 am
25/12/2025


wazuh.
Loading ...


wazuh.
The Open Source Security Platform
admin
Log in



e. Deploy New Agent to the Windows Server 2022 Virtual Machine:

i. On the **Overview** page, you will find an **Agents by Status** section. It shows **"Active (1)"** and **"Disconnected (0)"** which indicates there is one added agent that's active. Click the **Active (1)** hyperlink inside it. *This opens the **Endpoints** page.*

ii. On the **Endpoints** page, you will find an **Agents (1)** section/widget with the Kali-Agent agent on the data-grid. Click the **Deploy new agent** text above it. *This opens a **Deploy new agent** page.*

iii. On the **Deploy new agent** page, configure the following:

- In the **Select the package to download and install on your system** section, select **MSI 32/64 bits.**
- In the **Server address** section, input the Wazuh-Server address from **(Step 4d)** into the **Assign a server address** text box.
- In the **Optional settings** section, input the **Windows Server 2022** agent name **(WinServ22-Agent)** into the **Assign an agent name** text box.
- Also, in the **Optional settings** section, in the **Select one or more existing groups** drop-down menu, select **default.**
- In the **Run the following commands to download and install the agent** section, there is a command with the option to copy it, as is provided in the user interface. It looks like the following:

```
Invoke-WebRequest -Uri
[https://packages.wazuh.com/4.x/windows/wazuh-agent-4.x.x-1
.msi](https://packages.wazuh.com/4.x/windows/wazuh-agent-4.
x.x-1.msi) -OutFile ${env:tmp}\wazuh-agent.msi; msiexec.exe
/i ${env:tmp}\wazuh-agent.msi /q
WAZUH_MANAGER='192.168.126.128'
```

```
WAZUH_REGISTRATION_SERVER='192.168.126.128'
```

Copy this command.

iv. Minimize the **Microsoft Edge** browser, launch **Start Menu** and search **Windows PowerShell.**

v. Right-click the **Windows PowerShell** icon and select **Run as administrator.** *This launches **Windows PowerShell** with administrator privileges.*

vi. Paste the copied command into the **Windows PowerShell** interface and run it. A **Writing web request** band pops up inside the **Windows PowerShell** interface. This installs Wazuh agent on the **WindowsServer2022** virtual machine using configurations based on earlier provided details. *Do not close the **Windows PowerShell** window.*

vii. Return to the **Microsoft Edge** browser. In the **Deploy new agent** page, continue from **Step 6e-ii** in the following ways:

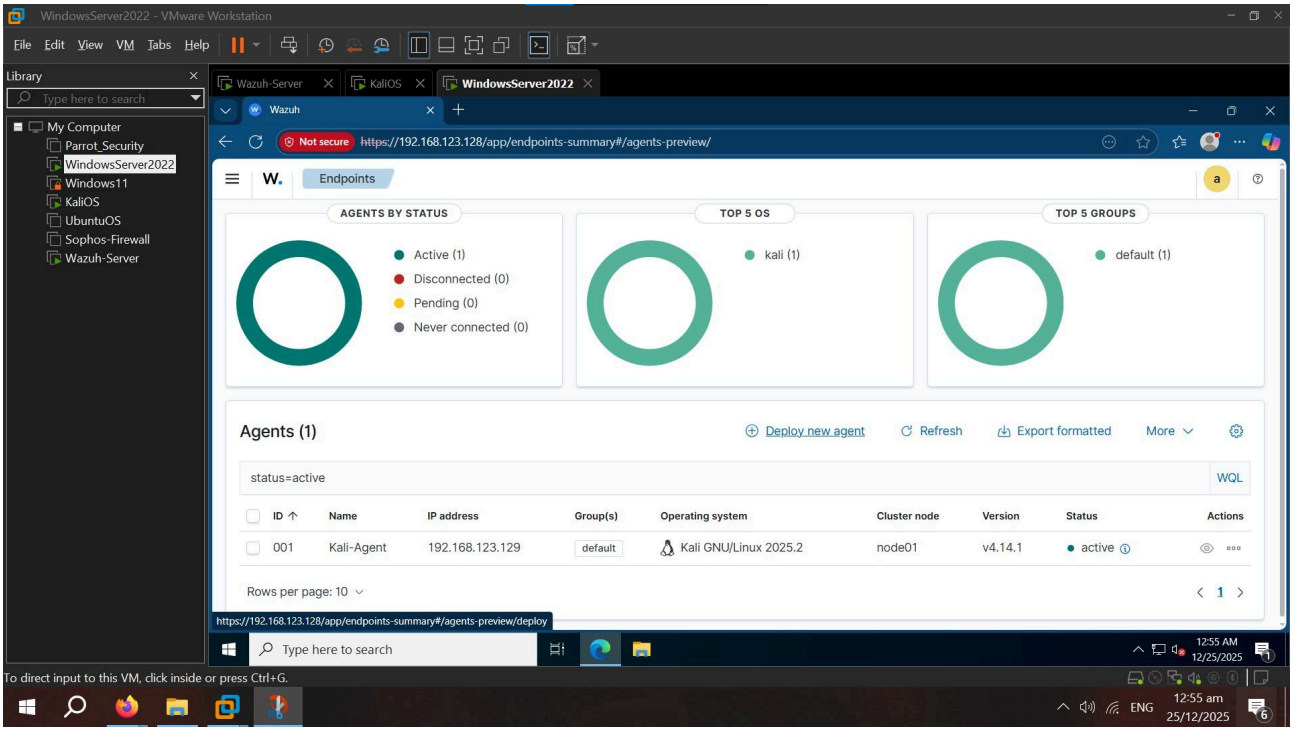
- In the **Start the agent** section, there is one command with the option to copy it, as is provided in the web interface. It looks like the following:

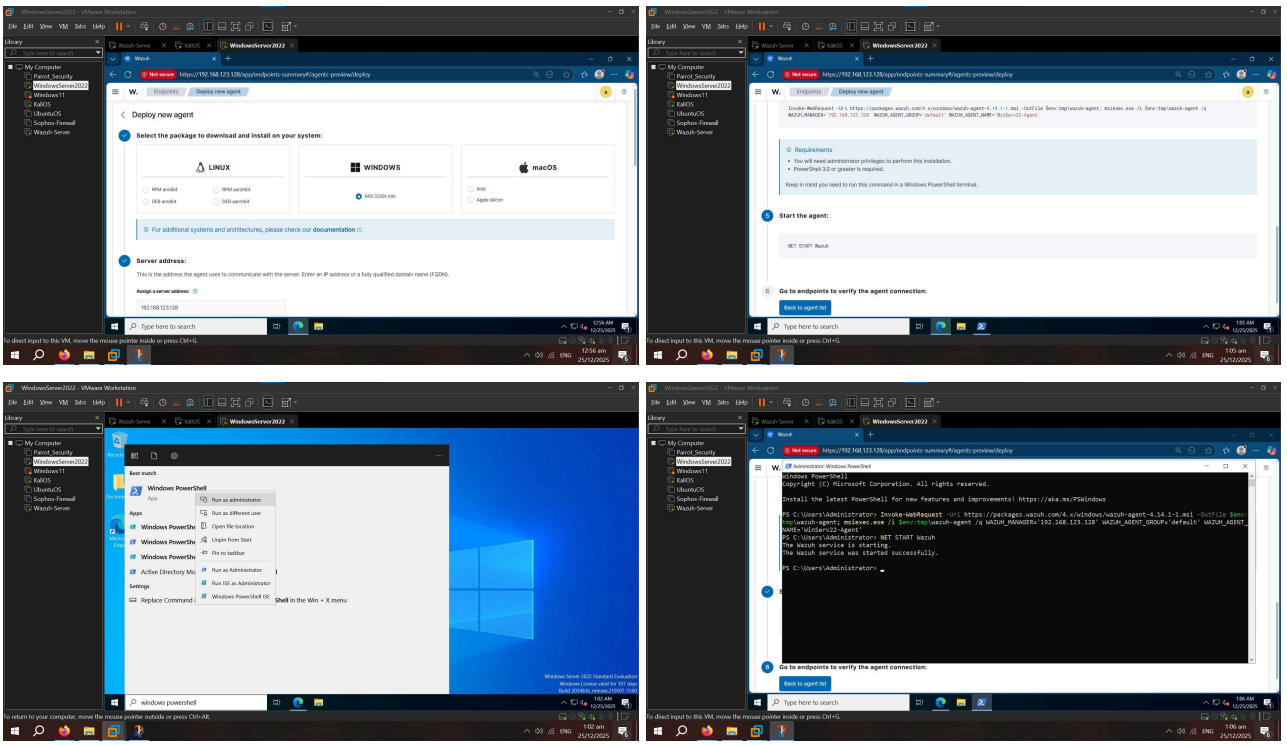
```
NET Start Wazuh
```

Copy this command.

viii. Return to the **Windows PowerShell** window.

ix. Paste the copied commands into the **Windows PowerShell** interface and run them sequentially. *This enables and starts **WinServ22-Agent,** the **Wazuh agent** on the **WindowsServer2022** virtual machine.*





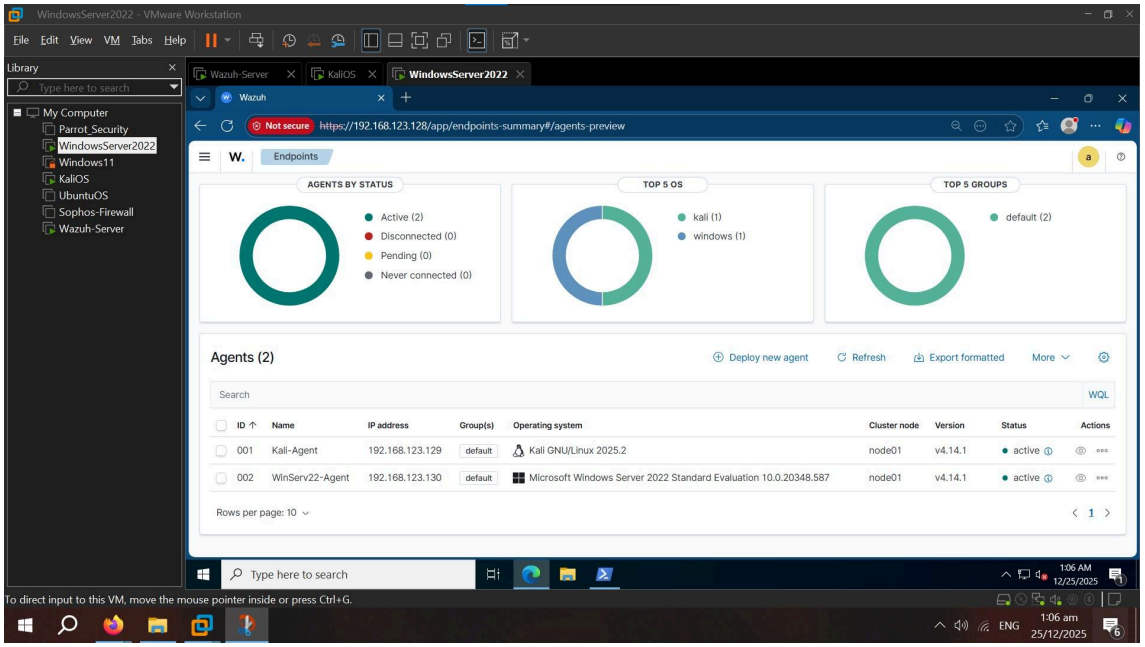
f. Confirm Agent Addition:

i. Return to the **Firefox** browser.

ii. Click the **hamburger/menu icon** in the top left. This brings out a sidebar menu.

iii. In the Sidebar Menu, click the Server Management drop-down menu and click Endpoint Summary. This opens an **Endpoints** page.

iv. In the **Agents by Status** section, there is a “(2)” in front of **Active** [Active (2)], indicating that two agents have been added. Also, in the **Agents** section, the Windows agent **(WinServ22-Agent),** and the Kali Linux agent **(Kali-Agent)** are listed.



Appearance Modification

Switching on Dark Mode

Step 7: Activate Dark-Mode Theme on Wazuh Web-Console

a. Access Appearance Settings:

i. Return to the **Firefox** browser on the host **(Windows 10 x64)** and access the **Overview** page.

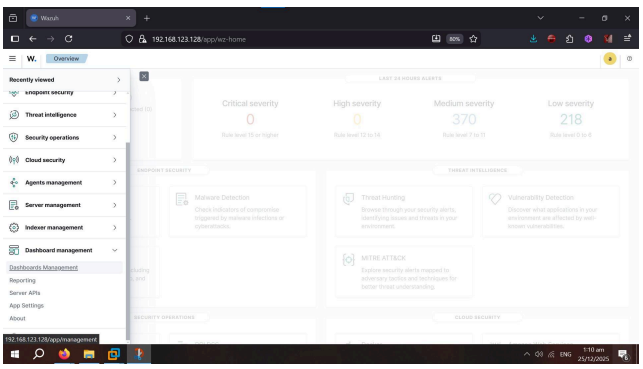
ii. On the **Overview** page, click the hamburger/menu icon on the top-left side of the page. This opens a side-bar navigation menu.

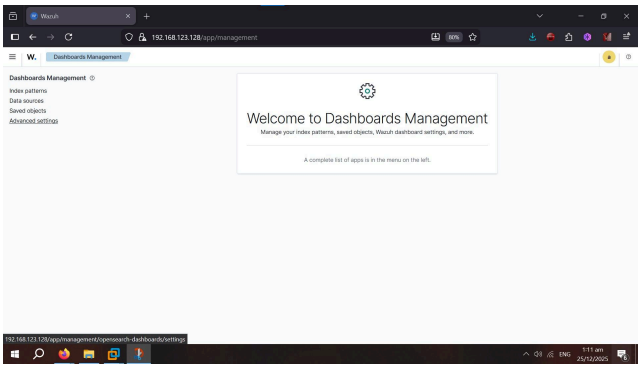
iii. Scroll down to the **Dashboard management** dropdown button. Click it

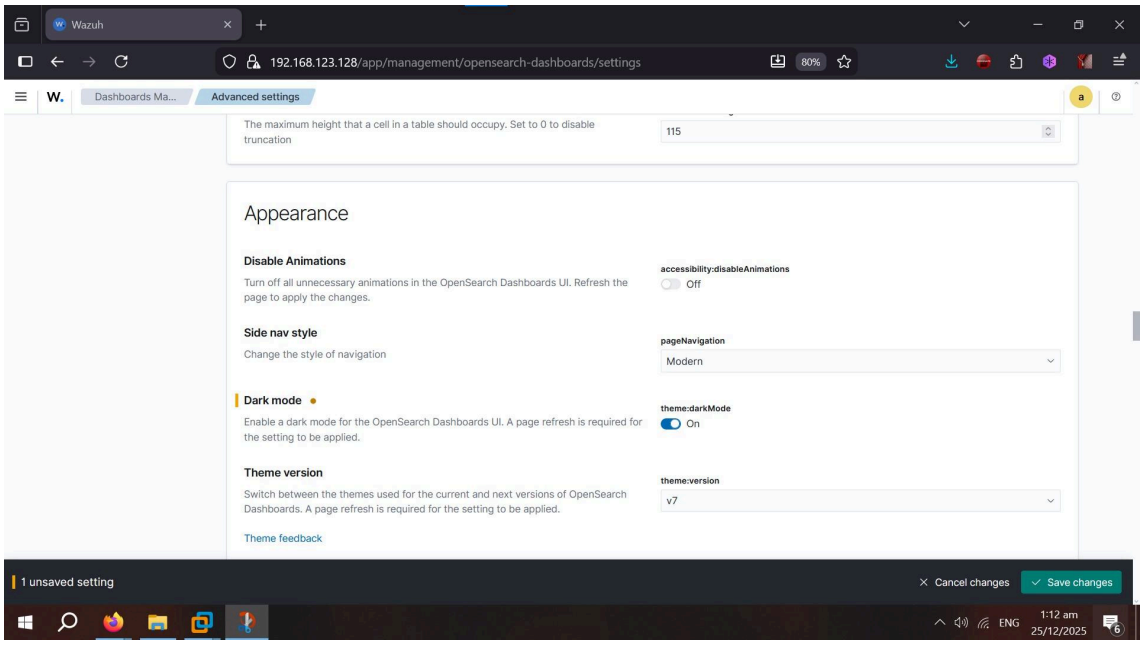
iv. Find the **Dashboards Management** hyperlink under the **Dashboard management** dropdown button. Click the link. *This opens a **Dashboards Management** page.*

v. On the **Dashboards Management** page, locate the **Advanced settings** hyperlink on the top-left side of the page. Click it. *This opens the **Advanced settings** page.*

vi. On the **Advanced settings** page, scroll down to the **Appearance** section.



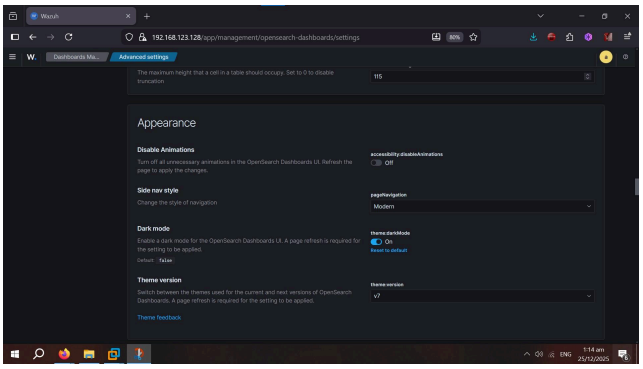


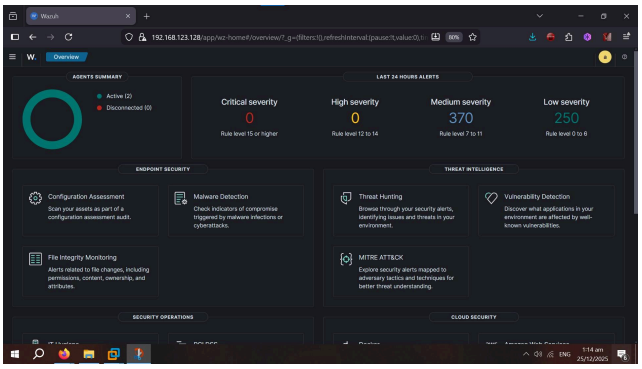


b. Activate Dark Mode Theme:

i. In the **Appearance** section, locate the **Dark mode** option.

ii. Beside the **Dark mode** option, under **theme:darkMode,** locate a toggle button, currently set to **Off.** Click the toggle button and turn it **On.** Click the green **Save changes** button on the prompt which appears at the bottom of the screen.
iii. Reload the page by pressing **F5.** The dark mode theme is now activated.
iv. Click the Wazuh logo icon on the left side of the top navigation bar. This returns you to the **Overview** page, with the dark-mode theme activated.





File Integrity Monitoring (FIM)

Surveilling Files for Modifications

Step 8: Set Up File for Monitoring (Kali VM Endpoint)

a. Create File for Monitoring:
i. Return to the **KaliOS** VM on the virtualizer **(VMware Workstation Pro 17.5)**
ii. Launch the **Terminal** (Step 5c-i).
iii. Type the following command to change working directory:

```
cd /home/jeffreyoo/Desktop/AltSchool/
```

iv. Type the following command to create the directory to be monitored:

```
mkdir Assessment_2
```

v. Type the following command to create the directory to be monitored:

```
cd Assessment_2
```

vi. Type the following command to create the file to be monitored **(secrets.txt):**

```
touch secrets.txt
```

vii. Type the following command to confirm that the monitored file **(secrets.txt)** has been created in the current directory:

```
ls
```

Return:

```
secrets.txt
```

b. Publish Content to the Monitored FIle:
i. Type the following command to write text to the monitored file **(secrets.txt):**

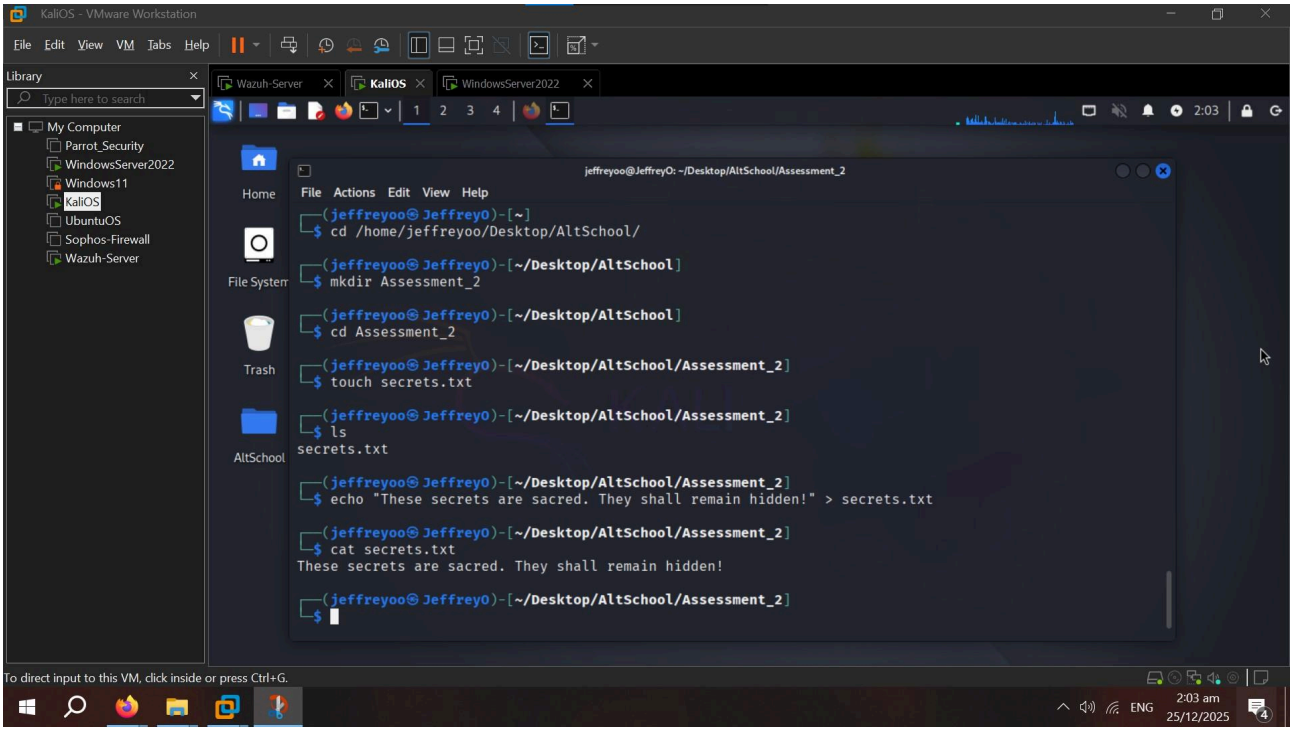
```
echo "These secrets are sacred. They shall remain hidden!" > secrets.txt
```

ii. Type the following command to confirm the content has been written to the file:

```
cat secrets.txt
```

Return:

```
These secrets are sacred. They shall remain hidden!
```



Step 9: Set Up File for Monitoring (Windows Server 2022 VM Endpoint)

a. Create File for Monitoring:

i. Return to the **KaliOS** VM on the virtualizer **(VMware Workstation Pro 17.5)**

ii. On the **Desktop,** create a folder for monitoring and name it **(Secrets).**

iii. Open the folder **(Secrets).** Right-click inside the folder window, select **New** and select **Text Document.** *This creates a new and empty text document inside the* **Secrets** folder, *named* ***New Text Document.txt.***

iv. Right-click the **New Text Document.txt** file and select **Rename.** Rename the file to **Secrets.txt**

b. Publish Content to the Monitored FIle:

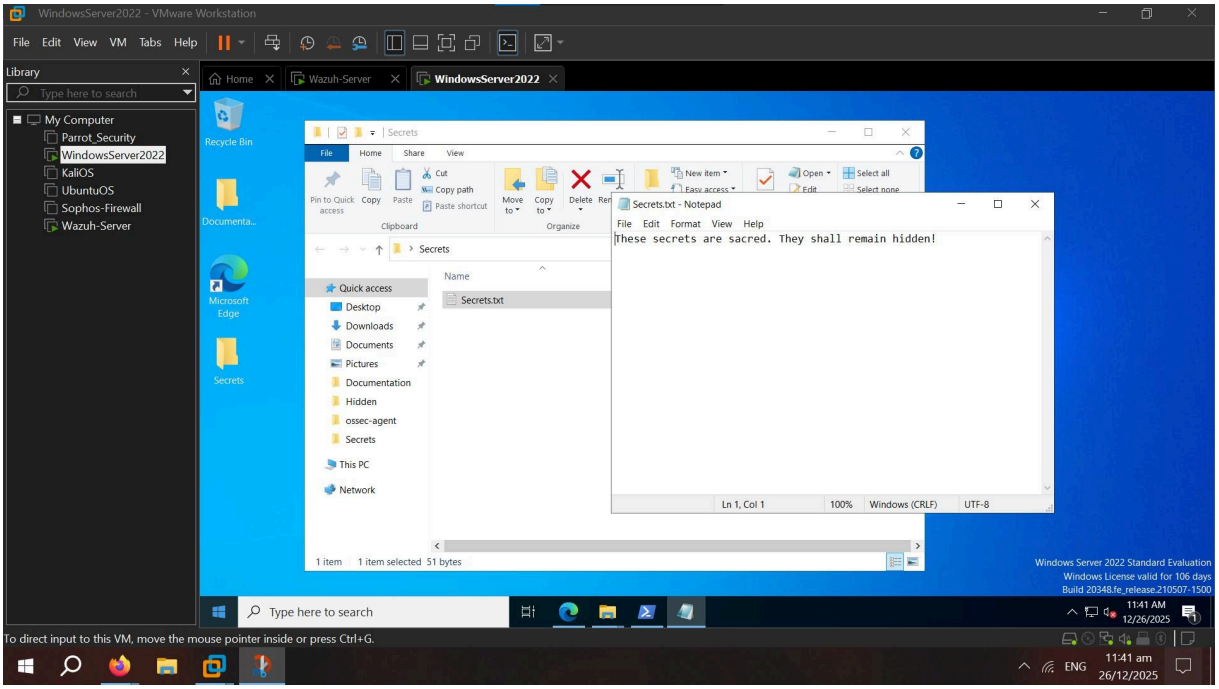
i. Open **Secrets.txt** by double-clicking the file. *This opens the file in a* ***Notepad*** *window.*

ii. In the text area of the **Notepad** window, type the following text:

```
These secrets are sacred. They shall remain hidden!
```

iii. Type **Control+S** to save the file.

iv. Close the **Notepad** window.



Step 10: Configure Directories for File Integrity Monitoring

a. Configure File Integrity Monitoring Directory in **KaliOS** VM

i. Return to **KaliOS** VM.

ii. Return to the **Terminal.**

iii. Type the following command to modify the **ossec.conf** file:

```
sudo nano /var/ossec/etc/ossec.conf
```

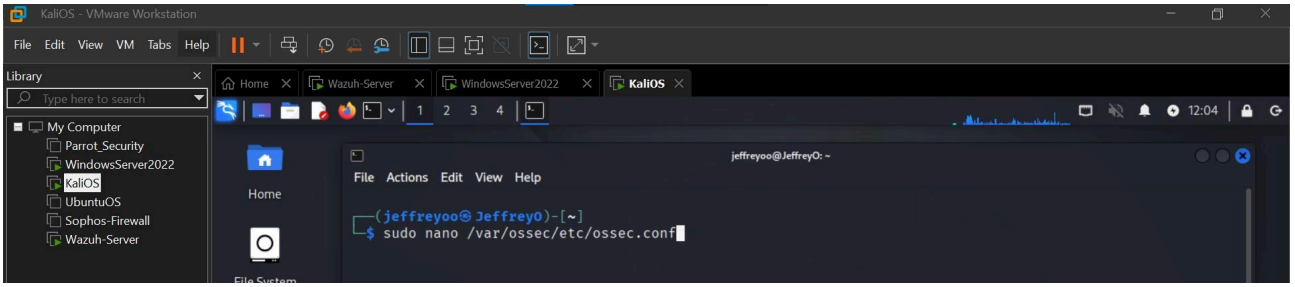
This launches the **nano** interface within the **Terminal** CLI, showing the contents of the **ossec.conf** file for editing.

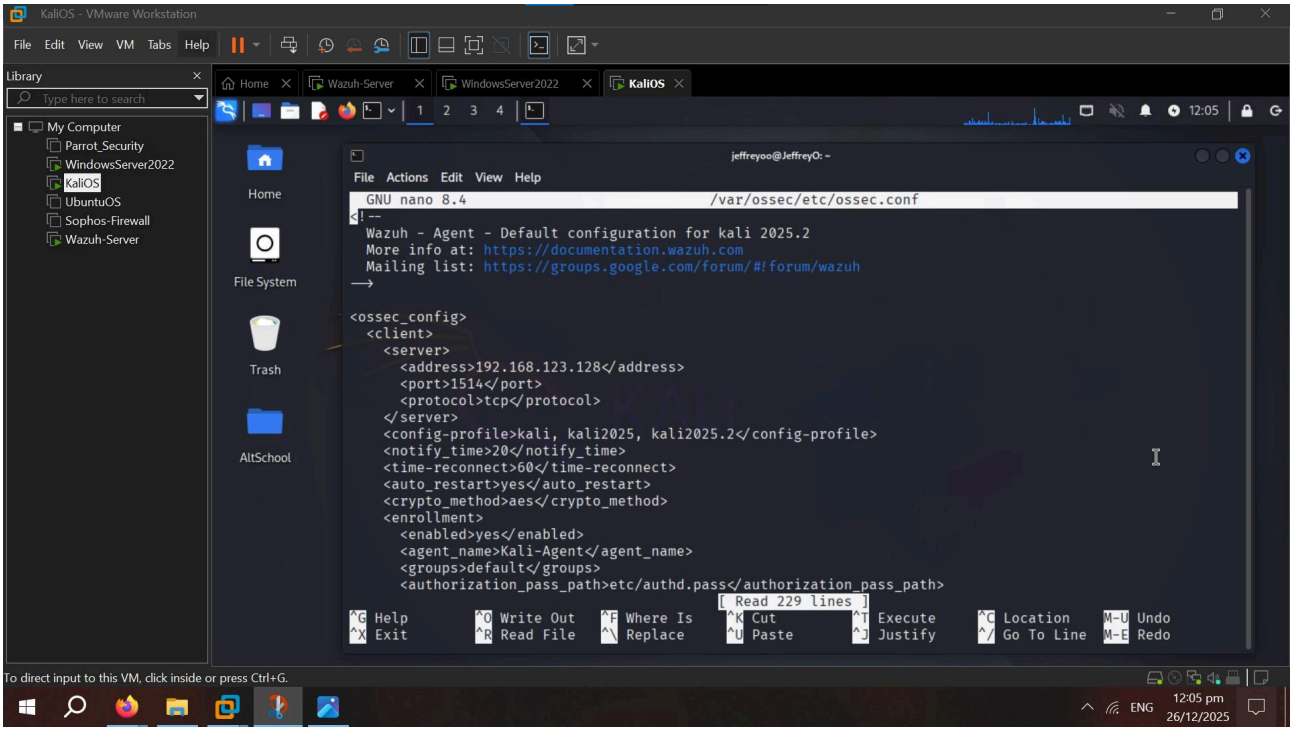
iv. Navigate to the **<syscheck>** section and include the following line below it:

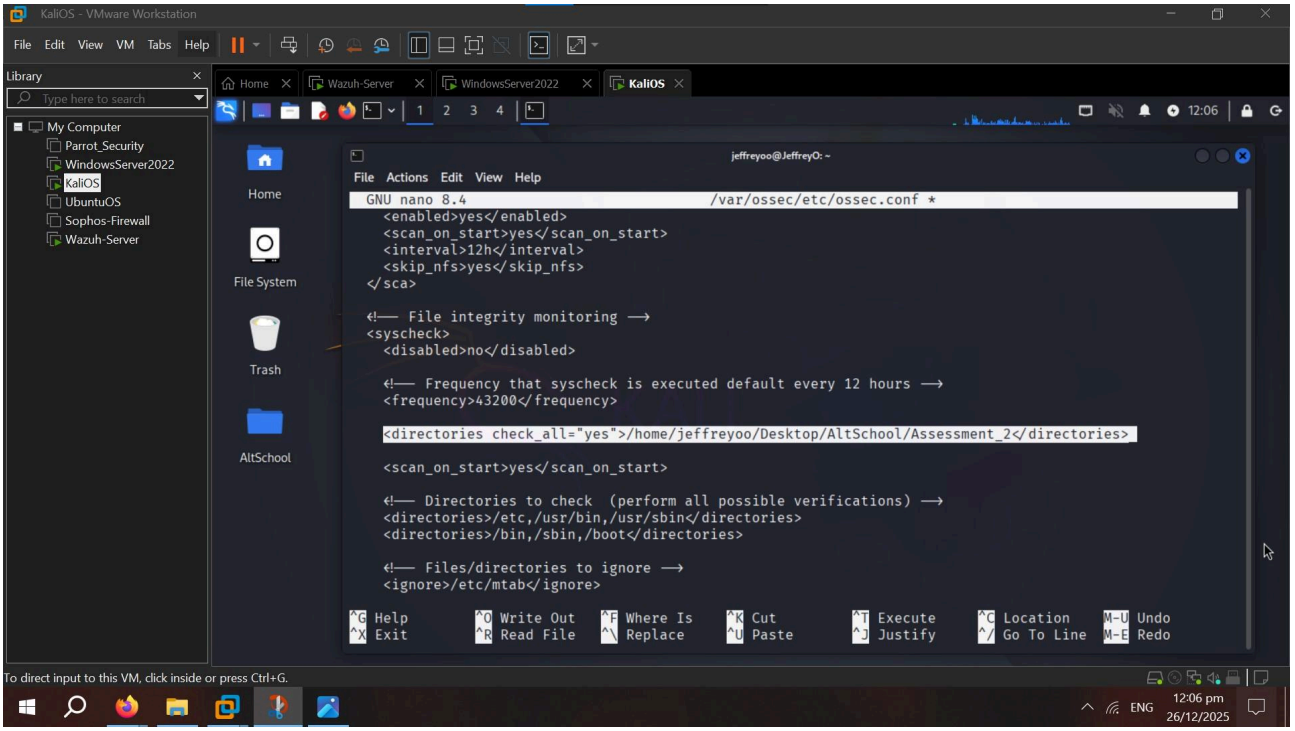
```
<directories check_all="yes">/home/jeffreyoo/Desktop/AltSchool/Assessment_2</directories>
```

This includes the directory of the monitored file **(secrets.txt)** into the **Wazuh File Integrity Monitoring** system.

v. Press **Control+O** to bring up the prompt to write changes to the file. Press **Enter** to confirm. Press **Control+X** to close the **nano** interface and return to the **Terminal** commands.





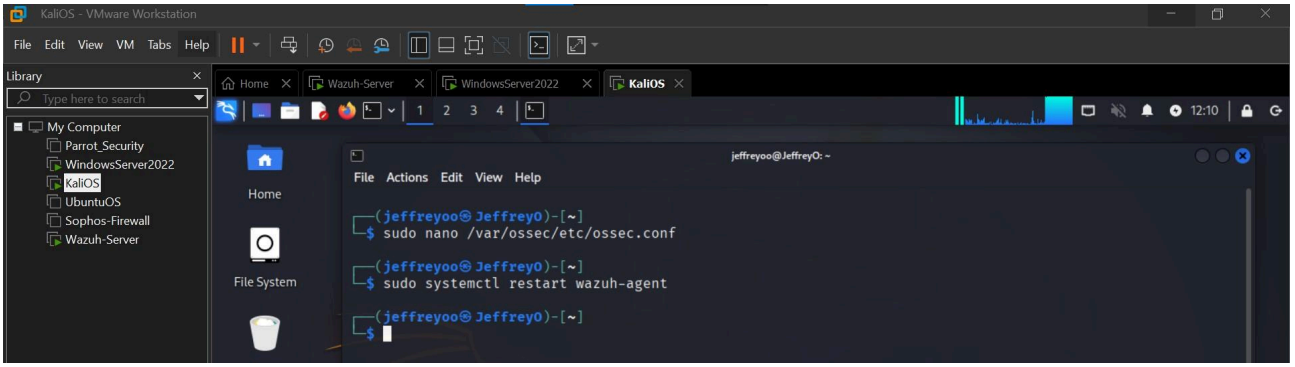


b. Restart the **KaliOS** Agent.

i. Restart the **Wazuh Agent** using the following command:

```
sudo systemctl restart wazuh-agent
```

This restart causes the changes to take effect.



c. Configure File Integrity Monitoring Directory in **WindowsServer2022** VM.

i. Return to **WindowsServer2022** VM.

ii. From the **Desktop** screen, launch the **Start Menu** and search **Notepad.**

iii. Richt-click the **Notepad** icon and select **Run as administrator.** *This opens a **Notepad** instance window with administrator privileges.*

iv. From the menu bar, select **File,** then select **Open** from the drop-down menu. *This opens an **Open dialog,** in which the file to be opened is chosen.*

v. In the **Open dialog,** at the bottom, next to the **File name:** text box, is the **Extension filter,** already set to **Text Documents (*.txt).** Select the drop-down menu and select **All Files (*.*).**

vi. Navigate to the following file and select it:

```
C:\Program Files (x86)\ossec-agent\ossec.conf
```

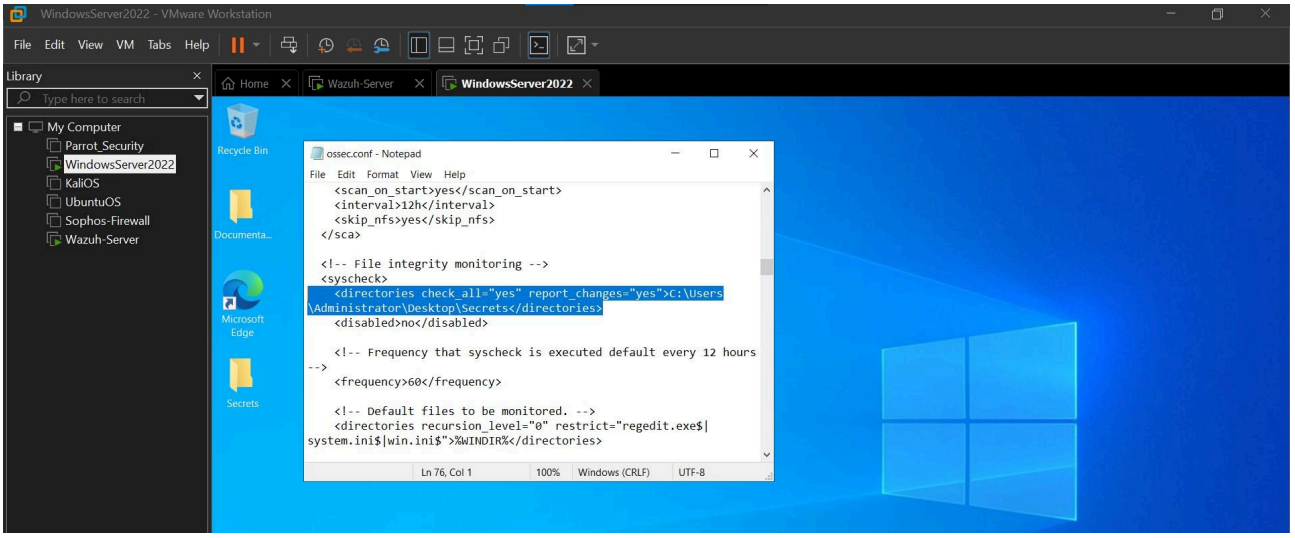
vii. Click the **Open** button. *This opens the file in a **Notepad** window.*

viii. In the **Notepad** window, navigate to the **<syscheck>** section and include the following line below it:

```
<directories
check_all="yes">C:\Users\Administrator\Desktop\Secrets</direct
ories>
```

This includes the directory of the monitored file **(secrets.txt)** into the **Wazuh File Integrity Monitoring** system.

ix. Press **Control+S** to save the file. Close the **Notepad** windows.



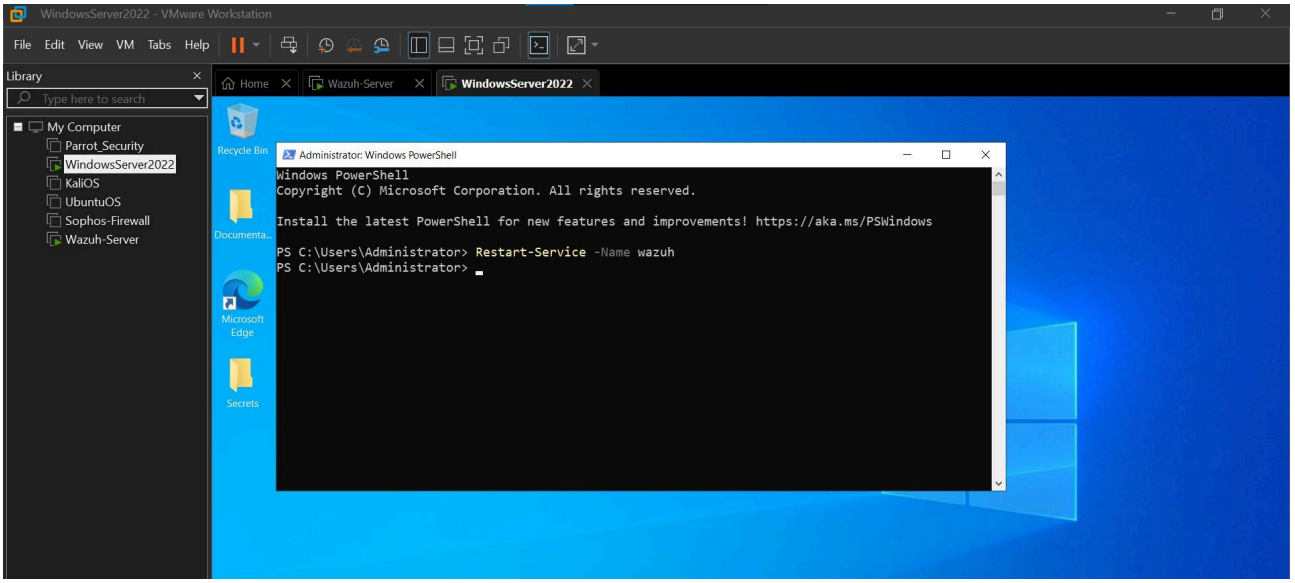
d. Restart the **WindowsServer2022** Agent.

i. Return to **Windows Powershell** *(already launched as administrator).*

ii. Restart the **Wazuh Agent** by typing the following command:

```
sudo systemctl restart wazuh-agent
```

This restart causes the changes to take effect.



Step 11: Confirm Recognition of Monitored Files via Web-Console

a. Access the File Inventory on the Wazuh Web-Console:

i. Return to the **Firefox** browser on the host machine **(Windows 10 x64)** and access the **Overview** page.

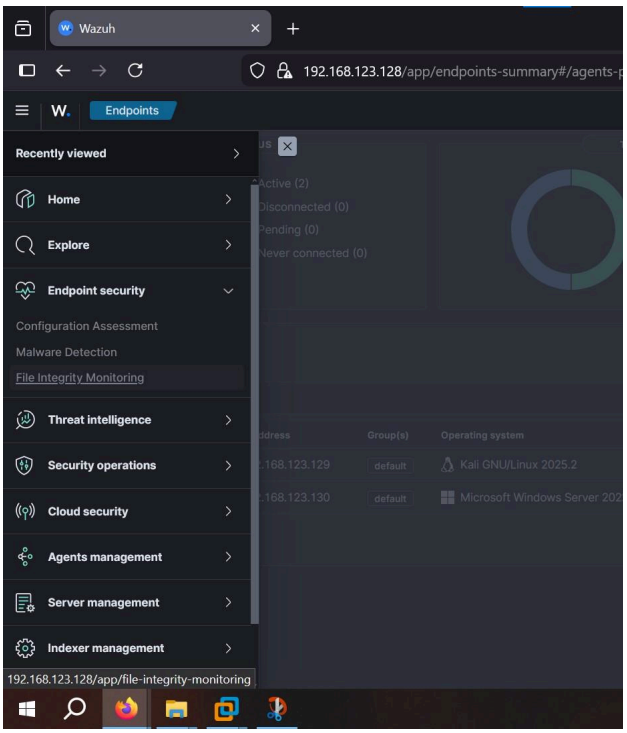
ii. On the **Overview** page, click the hamburger/menu icon on the top-left side of the page. This opens a side-bar navigation menu.

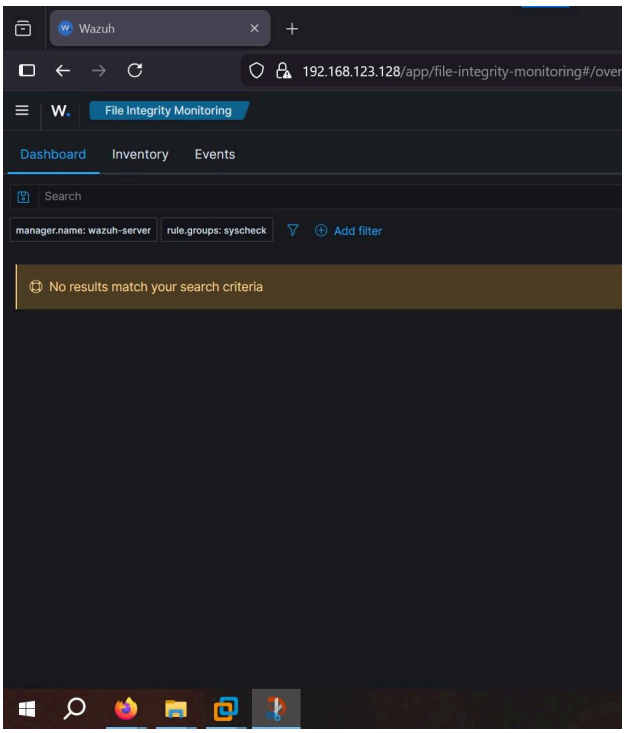
iii. Scroll down to the **Endpoint security** dropdown button. Click it

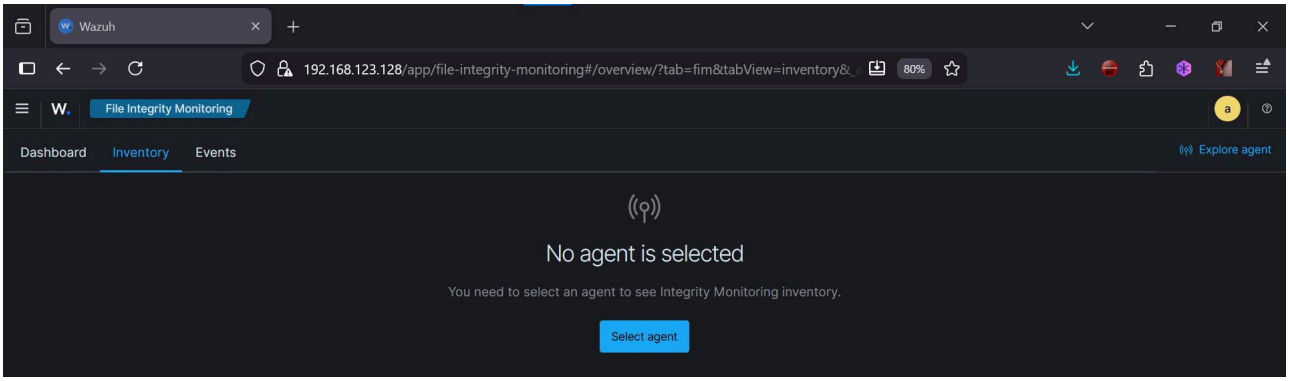
iv. Find the **File Integrity Monitoring** hyperlink under the **Endpoint security** dropdown button. Click the link. *This opens a **File Integrity Monitoring** page and defaults to the **Dashboard** tab as shown on the top navigation bar.*
v. Navigate to the **Inventory** tab via the top navigation bar. *This opens the **Inventory** page.*
vi. On the **Inventory** page, no files are displayed because no agent has been selected.

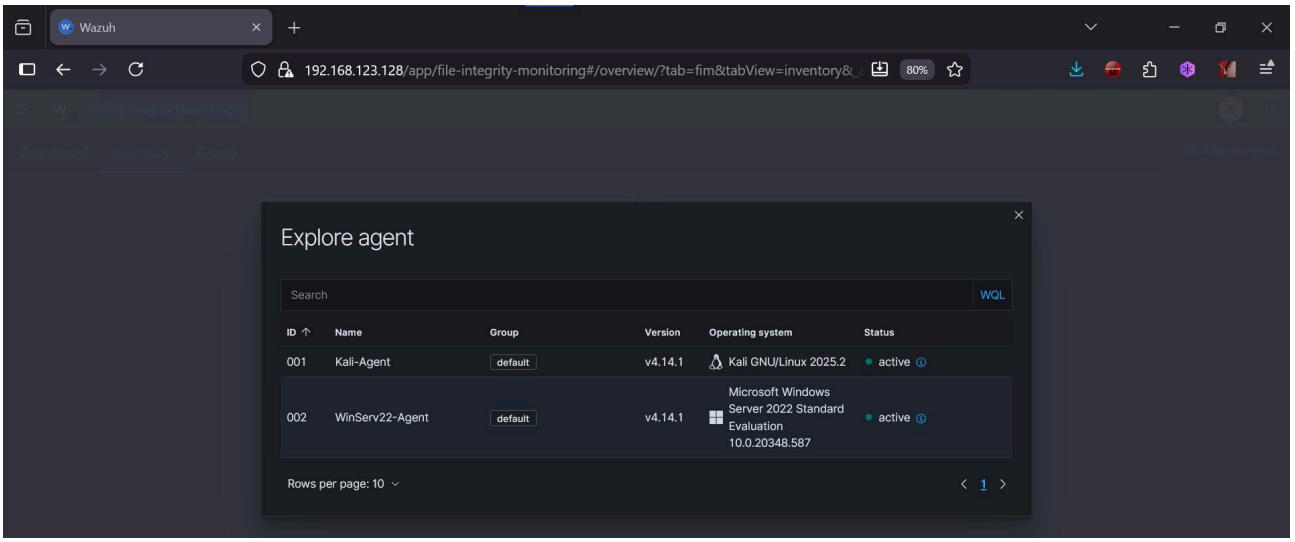
b. Confirm Recognition of Monitored File in **KaliOS VM:**
i. On the **Inventory** page, under the "No agent is selected" notice, locate and click the **Select agent** button on the top-left side of the page. Click it. *This opens the **Explore agent** card.*
ii. On the **Explore agent** card, the added agents are listed to be selected for inventory exploration. Select the **Kali-Agent** row to access the file inventory for **Kali OS VM.**
iii. The File Integrity Monitoring page for Kali-Agent opens and defaults to the **Dashboard** tab as shown on the top navigation bar.
iv. Navigate to the **Inventory** tab via the top navigation bar. *This opens the **Inventory** page.*
v. On the **Inventory** page, inside the **Search** text box, type **"secrets.txt"**and press **Enter.**
vi. Among the returned results, the monitored file which was created in **KaliOS VM (secrets.txt)** can be found, along with its file path.

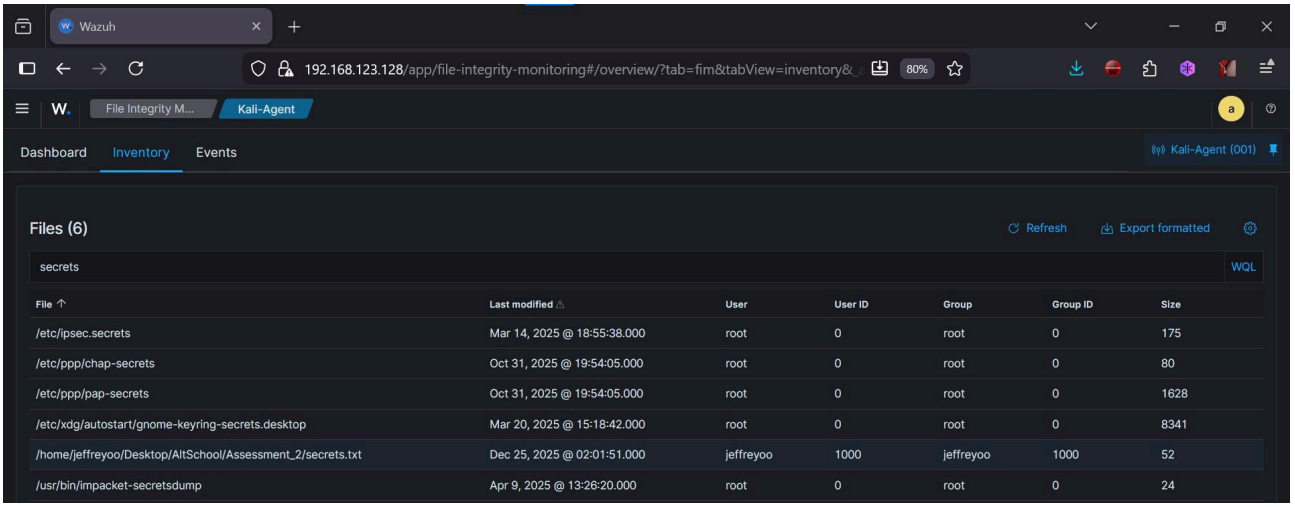
c. Confirm Recognition of Monitored File in **WindowsServer2022 VM:**
i. On the right side of the top navigation bar, locate and click the **pin icon** next to **"Kali-Agent (001)."** This returns the screen to the **Explore agents** card (from **Step 10-b-i**)
ii. On the **Explore agent** card, the added agents are listed to be selected for inventory exploration. Select the **WinServ22-Agent** row to access the file inventory for **WindowsServer2022** VM.
iii. The File Integrity Monitoring page for Kali-Agent opens and defaults to the **Dashboard** tab as shown on the top navigation bar.
iv. Navigate to the **Inventory** tab via the top navigation bar. *This opens the **Inventory** page.*
v. On the **Inventory** page, inside the **Search** text box, type **"secrets.txt"** and press **Enter.**
vi. Among the returned results, the monitored file which was created in **WindowsServer2022** VM **(secrets.txt)** can be found, along with its file path.

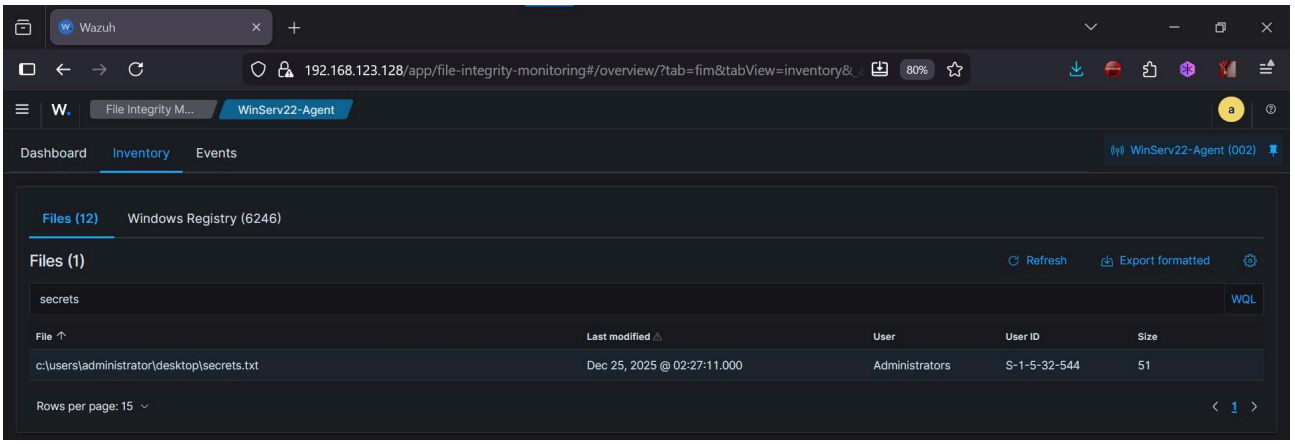

Wazuh
192.168.123.128/app/endpoints-summary#/agents-p
Endpoints
Recently viewed
Home
Explore
Endpoint security
Configuration Assessment
Malware Detection
File Integrity Monitoring
Threat intelligence
Security operations
Cloud security
Agents management
Server management
Indexer management
192.168.123.128/app/file-integrity-monitoring


Wazuh
192.168.123.128/app/file-integrity-monitoring#/over
File Integrity Monitoring
Dashboard
Inventory
Events
Search
manager.name: wazuh-server
rule.groups: syscheck
Add filter
No results match your search criteria


Wazuh
192.168.123.128/app/file-integrity-monitoring#/overview/?tab=fim&tabView=inventory&
80%
File Integrity Monitoring
Dashboard
Inventory
Events
Explore agent
No agent is selected
You need to select an agent to see Integrity Monitoring inventory.
Select agent


Wazuh
192.168.123.128/app/file-integrity-monitoring#/overview/?tab=fim&tabView=inventory&
80%
Explore agent
Search
WQL
ID
Name
Group
Version
Operating system
Status
001
Kali-Agent
default
v4.14.1
Kali GNU/Linux 2025.2
active
002
WinServ22-Agent
default
v4.14.1
Microsoft Windows Server 2022 Standard Evaluation 10.0.20348.587
active
Rows per page: 10
1





Step 12: Test 1—Modify Monitored Files

a. Modify the Monitored File on **KaliOS** VM:

i. Return to **KaliOS** VM.

ii. Return to the **Terminal.**

iii. Type the following command to confirm the monitored file **(secrets.txt)** is present in the working directory:

```
ls
```

Return:

```
secrets.txt
```

iv. Type the following command to append text **(“Extra!”)** to body of the monitored file:

```
Echo “Extra!” >> secrets.txt
```

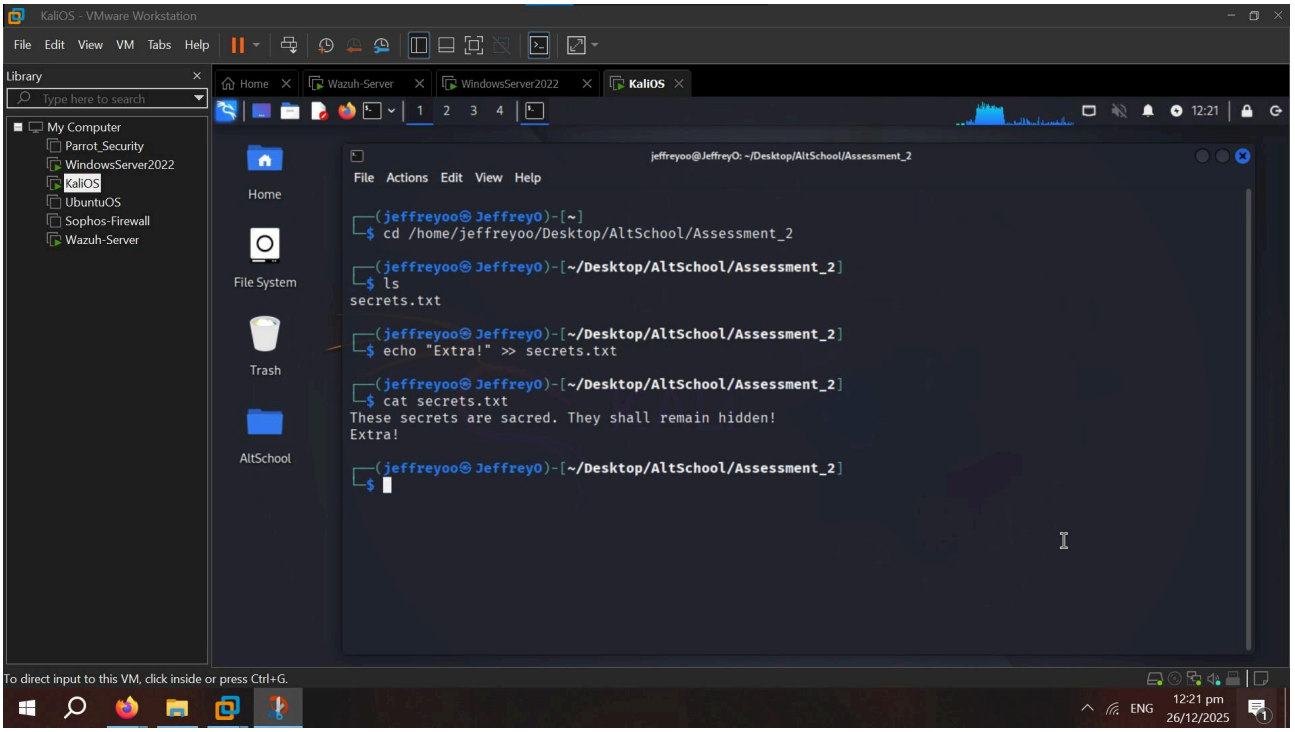
v. Type the following command to confirm the text **(“Extra!”)** has been successfully appended to the monitored file:

```
cat secrets.txt
```

Return:

These secrets are sacred. They shall remain hidden!
Extra!

vi. The above confirms that the monitored file, **secrets.txt,** located in **KaliOS** VM, has truly been modified.



b. Modify the Monitored File on **WindowsServer2022** VM:

i. Return to **WindowsServer2022** VM.

ii. On the **Desktop,** locate and open the **Secrets** folder. *Inside the folder, you will find a text document named* ***Secrets.txt.***

iii. Double-click the **Secrets.txt** file to open it. *This launches the file in a* ***Notepad*** *window.*

iv. In the **Notepad** windows, type the following text in the line under the existing text:

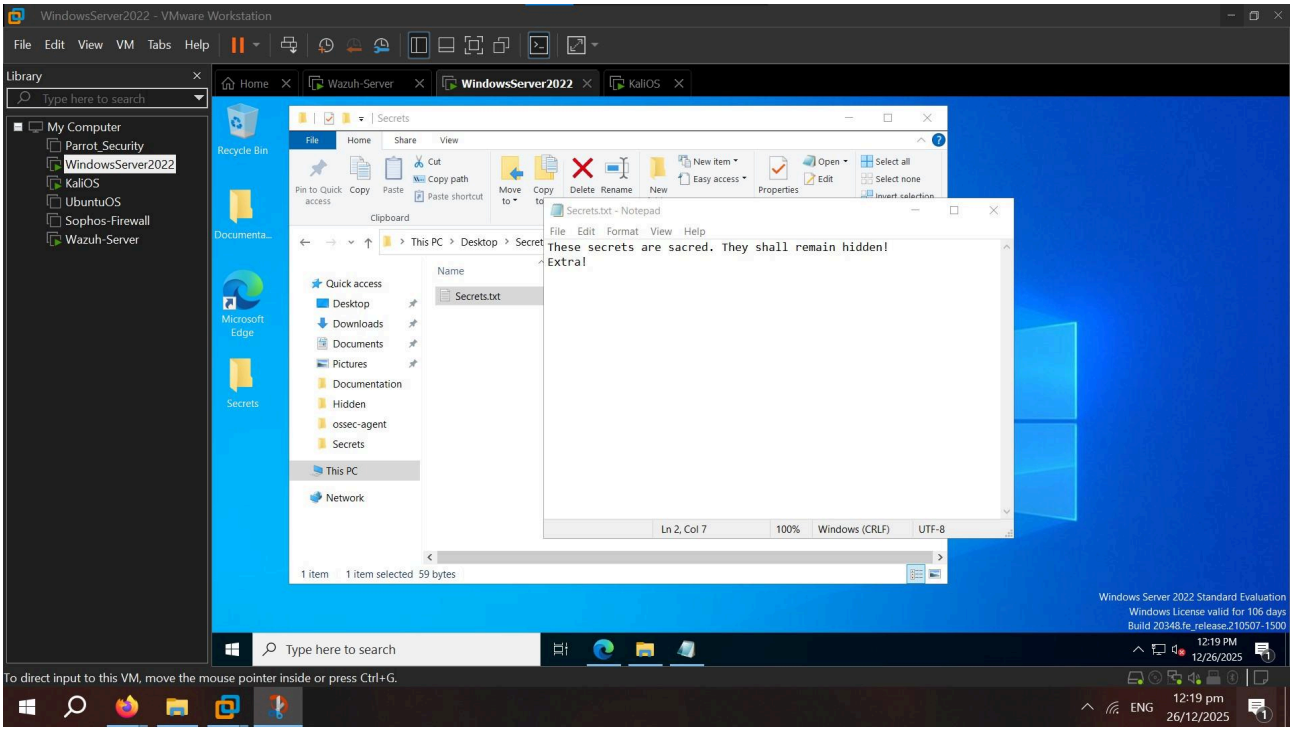
Extra!

v. The above appendment makes the body of text in the **secrets.txt** file, the following:

These secrets are sacred. They shall remain hidden!
Extra!

vi. Press **Control+S** to save the file, and then close the **Notepad** window.

vii. The above confirms that the monitored file, **secrets.txt,** located in **WindowsServer2022** VM, has truly been modified



Step 13: Confirm File Integrity Monitoring for File Modification

a. Confirm File Integrity Monitoring for Modified File on **Kali OS** VM.

i. Return to the **Firefox** browser on the host machine **(Windows 10 x64)** and access the Wazuh Web Console.

ii. Return to the **File Integrity Monitoring** page and navigate to the **Inventory** tab (as shown in **Step 11a-v**).

iii. Click the **Select agent** button on the screen. *This opens the **Explore agent** card.*

iv. On the **Explore agent** card, the two added agents are listed to be selected for inventory exploration. Select the **Kali-Agent** row to access the file inventory for **Kali OS** VM.

v. The **File Integrity Monitoring** page for **Kali-Agent** opens and defaults to the **Dashboard** tab as shown on the top navigation bar.

vi. Navigate to the **Inventory** tab via the top navigation bar. *This opens the **Inventory** page.*

vii. On the **Inventory** page, inside the **Search** text box, type **"secrets.txt"** and press **Enter.**

viii. Among the returned results, the monitored file which was created in **KaliOS** VM **(secrets.txt)** can be found, along with its file path.

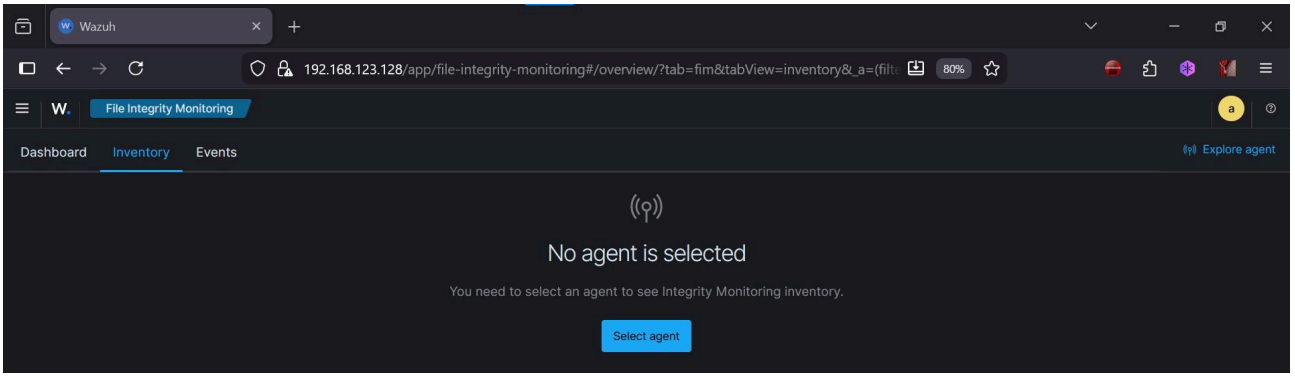
ix. Click the monitored file **(secrets.txt)** and this opens a right-side **details panel.**

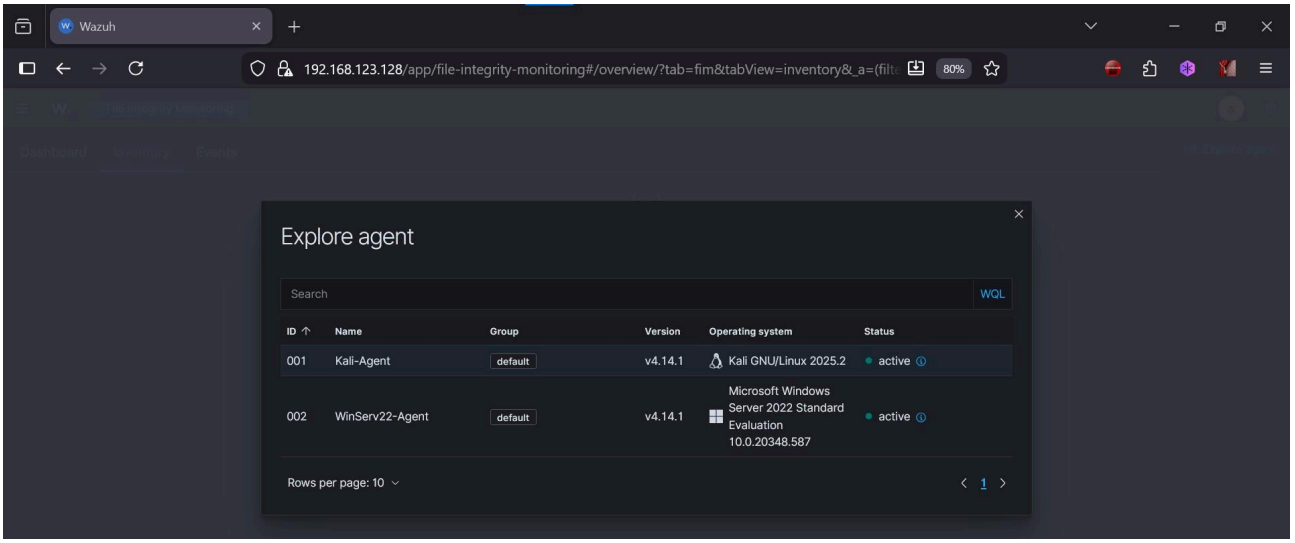
x. In the right-side details panel, under the **Recent events** section, locate the entry with **Integrity checksum changed** under the **Description** column and **550** under the **Rule ID** column.

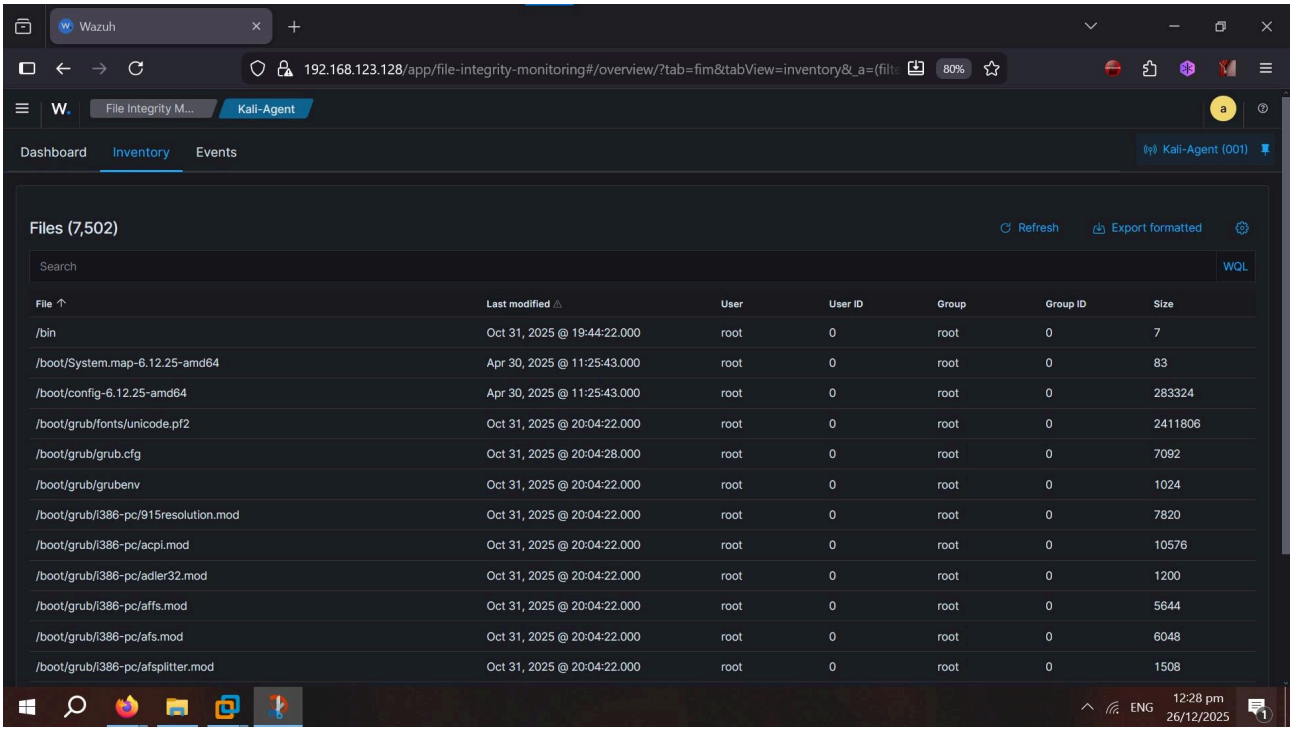
Note: Inside the **details panel,** to the right of the **Search** text box is a **Show dates** box. This box is where the time range for any executed search is configured. For

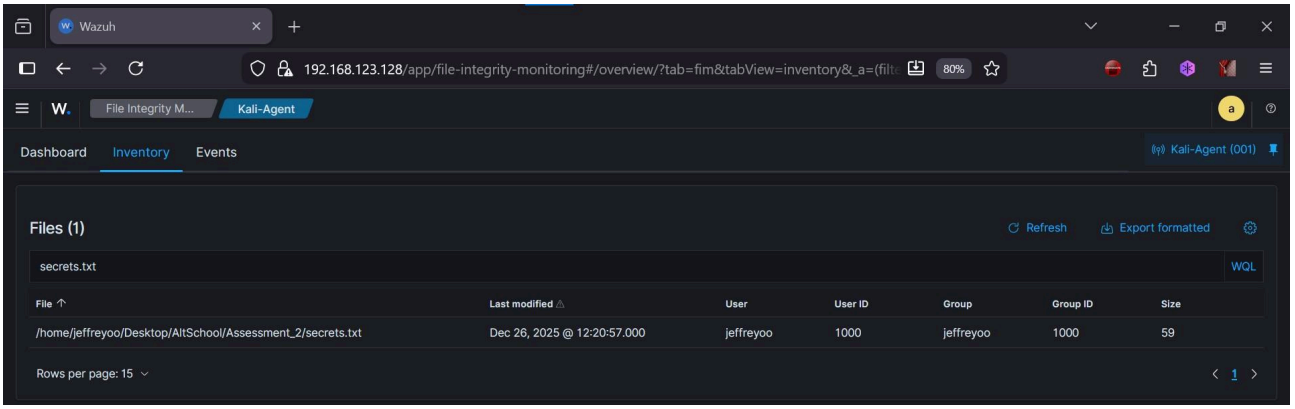
monitoring recent events, setting the start time one that is not too far back and setting the end time to **Now** is best.

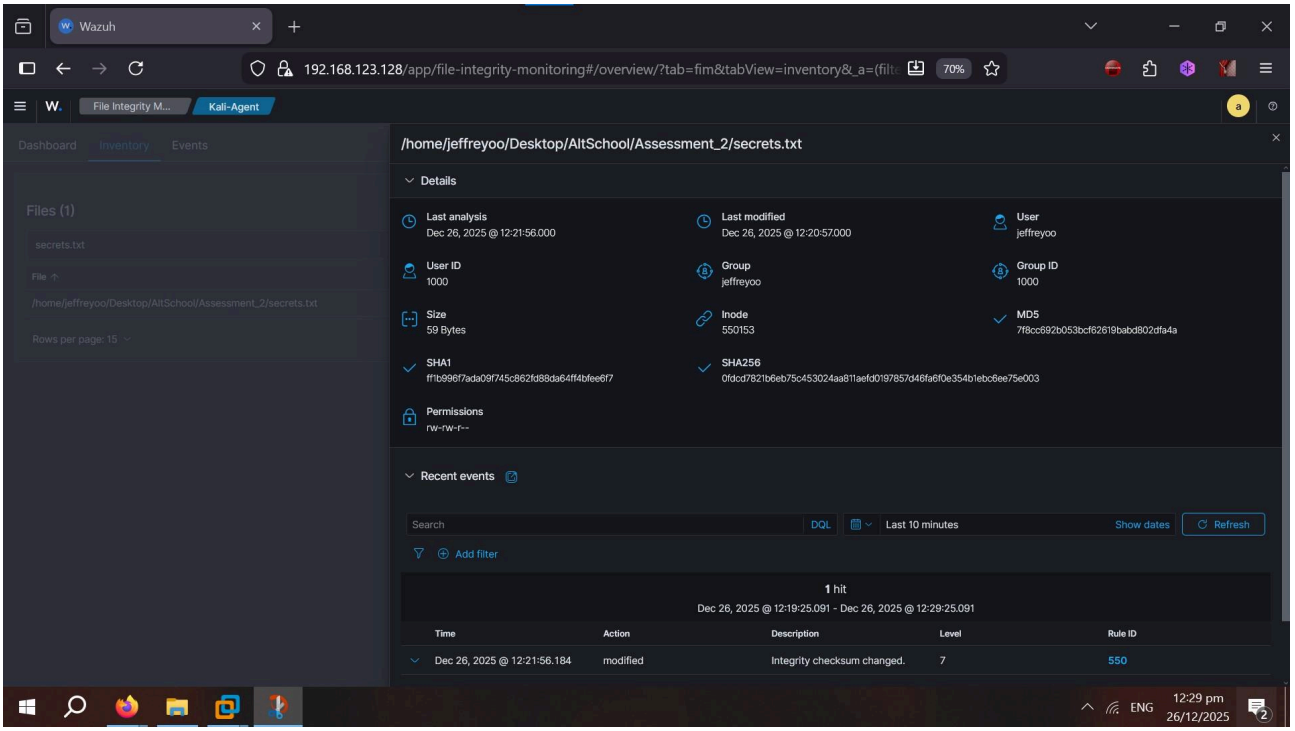
xi. That entry indicates a modification to the monitored file has been identified by Wazuh.






Wazuh
192.168.123.128/app/file-integrity-monitoring#/overview/?tab=fim&tabView=inventory&_a=(filt
80%
File Integrity M...
Kali-Agent
Dashboard
Inventory
Events
Kali-Agent (001)
Files (7,502)
Refresh
Export formatted
Search
WQL
File
Last modified
User
User ID
Group
Group ID
Size
/bin Oct 31, 2025 @ 19:44:22.000 root 0 root 0 7
/boot/System.map-6.12.25-amd64 Apr 30, 2025 @ 11:25:43.000 root 0 root 0 83
/boot/config-6.12.25-amd64 Apr 30, 2025 @ 11:25:43.000 root 0 root 0 283324
/boot/grub/fonts/unicode.pf2 Oct 31, 2025 @ 20:04:22.000 root 0 root 0 2411806
/boot/grub/grub.cfg Oct 31, 2025 @ 20:04:28.000 root 0 root 0 7092
/boot/grub/grubenv Oct 31, 2025 @ 20:04:22.000 root 0 root 0 1024
/boot/grub/i386-pc/915resolution.mod Oct 31, 2025 @ 20:04:22.000 root 0 root 0 7820
/boot/grub/i386-pc/acpi.mod Oct 31, 2025 @ 20:04:22.000 root 0 root 0 10576
/boot/grub/i386-pc/adler32.mod Oct 31, 2025 @ 20:04:22.000 root 0 root 0 1200
/boot/grub/i386-pc/affs.mod Oct 31, 2025 @ 20:04:22.000 root 0 root 0 5644
/boot/grub/i386-pc/afs.mod Oct 31, 2025 @ 20:04:22.000 root 0 root 0 6048
/boot/grub/i386-pc/afsplitter.mod Oct 31, 2025 @ 20:04:22.000 root 0 root 0 1508
ENG
12:28 pm
26/12/2025


Wazuh
192.168.123.128/app/file-integrity-monitoring#/overview/?tab=fim&tabView=inventory&_a=(filt
80%
File Integrity M...
Kali-Agent
Dashboard
Inventory
Events
Kali-Agent (001)
Files (1)
Refresh
Export formatted
secrets.txt
WQL
File
Last modified
User
User ID
Group
Group ID
Size
/home/jeffreyoo/Desktop/AltSchool/Assessment_2/secrets.txt Dec 26, 2025 @ 12:20:57.000 jeffreyoo 1000 jeffreyoo 1000 59
Rows per page: 15
1



b. Confirm File Integrity Monitoring for Modified File on **WindowsServer2022** VM.

i. Close the **details panel** and click the pin icon on the right side of the top navigation bar. *This returns the screen to the **Explore agent** card.*

ii. On the **Explore agent** card, the two added agents are listed to be selected for inventory exploration. Select the **WinServ22-Agent** row to access the file inventory for **WindowsServer2022** VM.

iii. The **File Integrity Monitoring** page for **WinServ22-Agent** opens and defaults to the **Dashboard** tab as shown on the top navigation bar.

iv. Navigate to the **Inventory** tab via the top navigation bar. *This opens the **Inventory** page.*

v. On the **Inventory** page, inside the **Search** text box, type **"secrets.txt"** and press **Enter.**

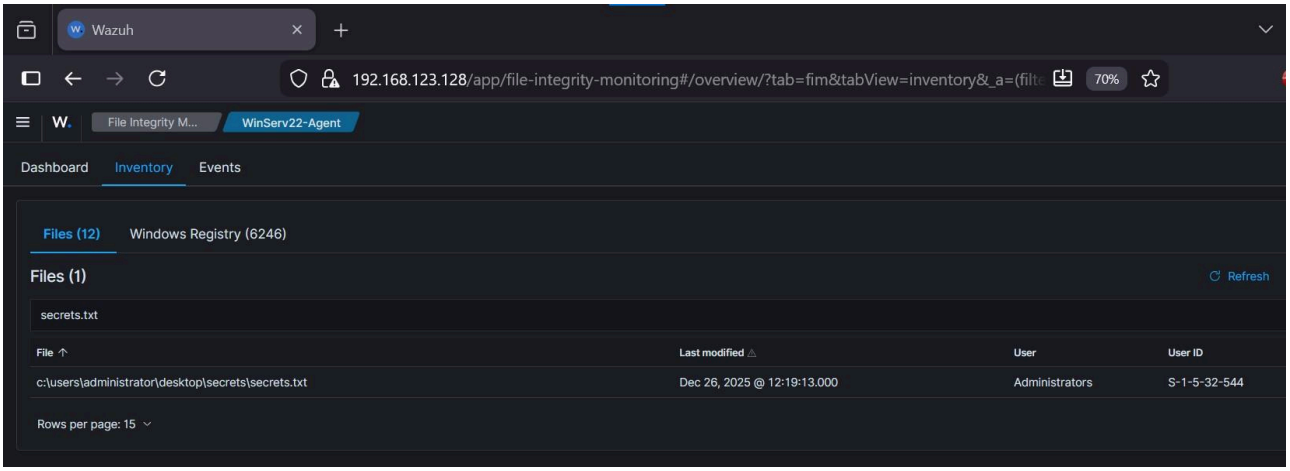
vi. Among the returned results, the monitored file which was created in **WindowsServer2022** VM **(secrets.txt)** can be found, along with its file path.

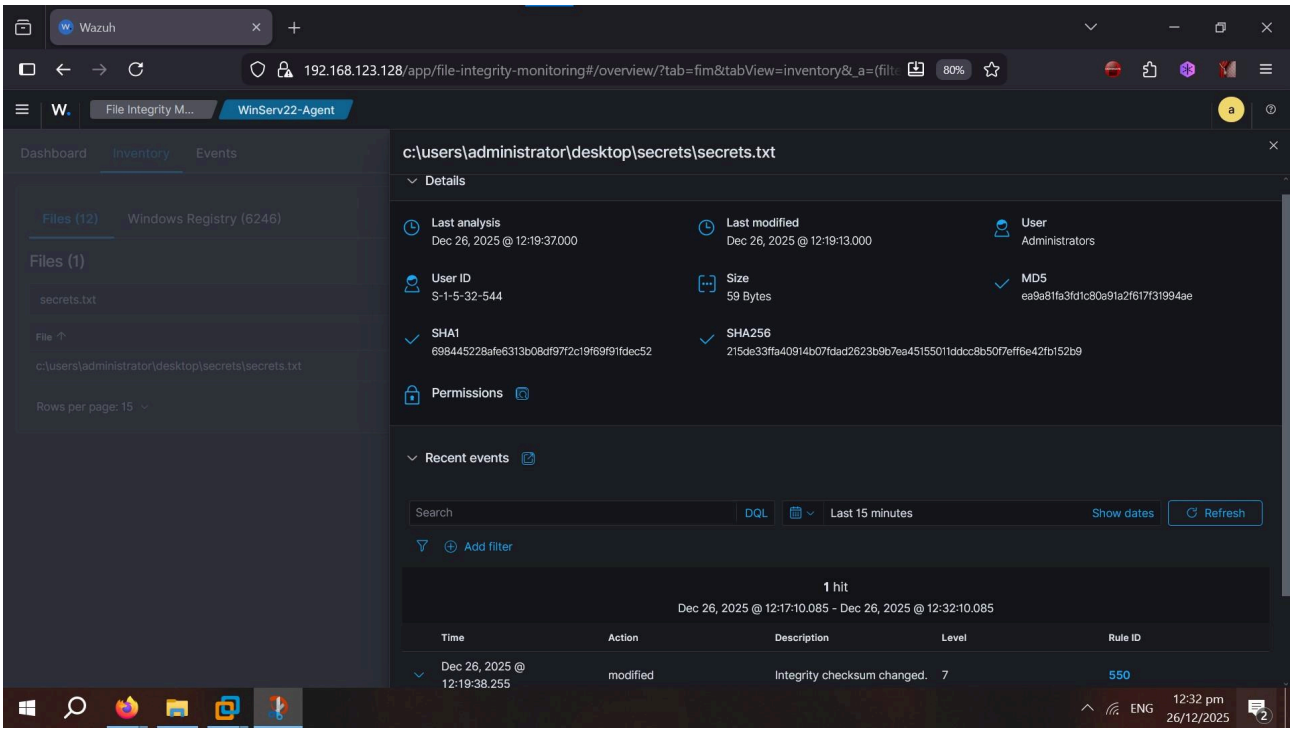
vii. Click the monitored file **(secrets.txt)** and this opens a right-side **details panel.**

viii. In the right-side details panel, under the **Recent events** section, locate the entry with **Integrity checksum changed** under the **Description** column and **550** under the **Rule ID** column.

Note: Inside the **details panel,** to the right of the **Search** text box is a **Show dates** box. This box is where the time range for any executed search is configured. For monitoring recent events, setting the start time one that is not too far back and setting the end time to **Now** is best.

ix. That entry indicates a modification on the monitored file has been identified by Wazuh.





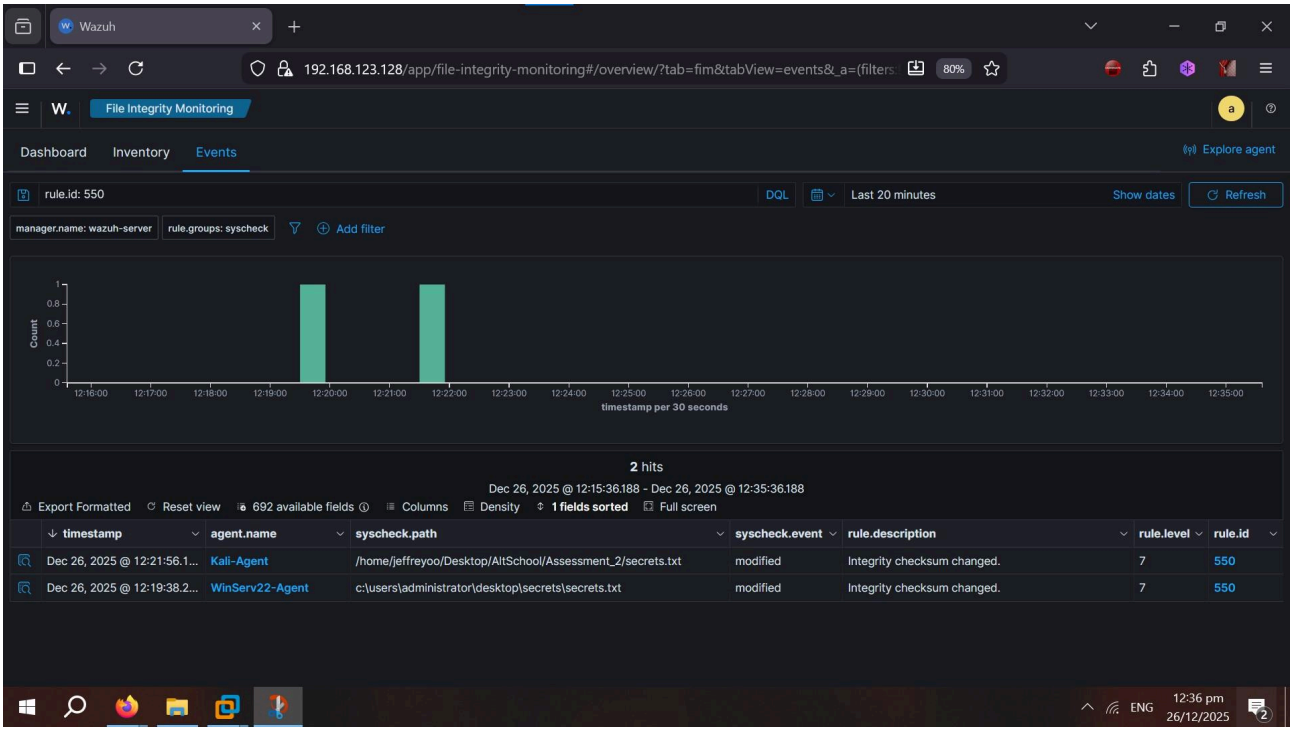
c. Confirm File Integrity Monitoring for File Modification on both VMs.

i. Close the **details panel** and click the pin icon on the right side of the top navigation bar. *This returns the screen to the **Explore agent** card.*

ii. Close the **Explore agent** card. This returns the screen to the **Inventory** tab in the **File Integrity Monitoring** page. Navigate to the **Events** tab.

iii. In the **Search** text box, type **rule.id: 550** and press **Enter.**

iv. This returns two listed results, which are the **secrets.txt** files from both VMs, confirming that these files from both agents were indeed modified.



Step 14: Test 2—Delete Monitored Files

a. Delete the Monitored File on **KaliOS** VM:

i. Return to **KaliOS** VM.

ii. Return to the **Terminal.**

iii. Type the following command to change to the monitored directory:

```
cd /home/jeffreyoo/Desktop/AltSchool/Assessment_2
```

iv. Type the following command to confirm that the monitored file **(secrets.txt)** is present in the current directory:

```
ls
```

Return:

```
secrets.txt
```

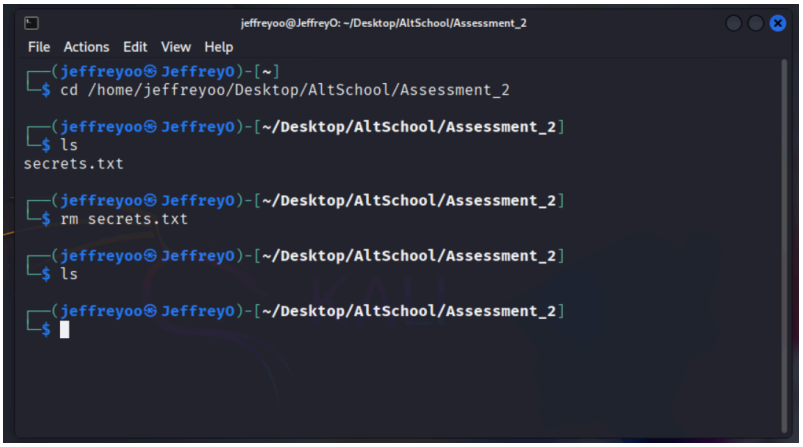
v. Type the following command to delete the monitored file **(secrets.txt)**:

```
rm secrets.txt
```

vi. Type the following command to confirm that the monitored file **(secrets.txt)** has been deleted from the monitored directory:

```
ls
```

Nothing was returned, confirming the file has been deleted.

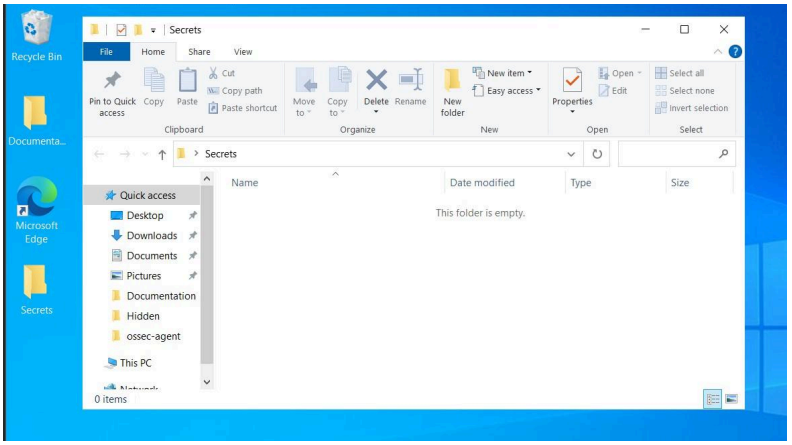


b. Delete the Monitored File on **WindowsServer2022** VM:

i. Return to **WindowsServer2022** VM.

ii. On the **Desktop,** locate and open the monitored folder named **Secrets**. *Inside the folder, you will find the monitored text document named* ***secrets.txt.***

iii. Click the **secrets.txt** file and press **Delete**. *This deletes the file.*



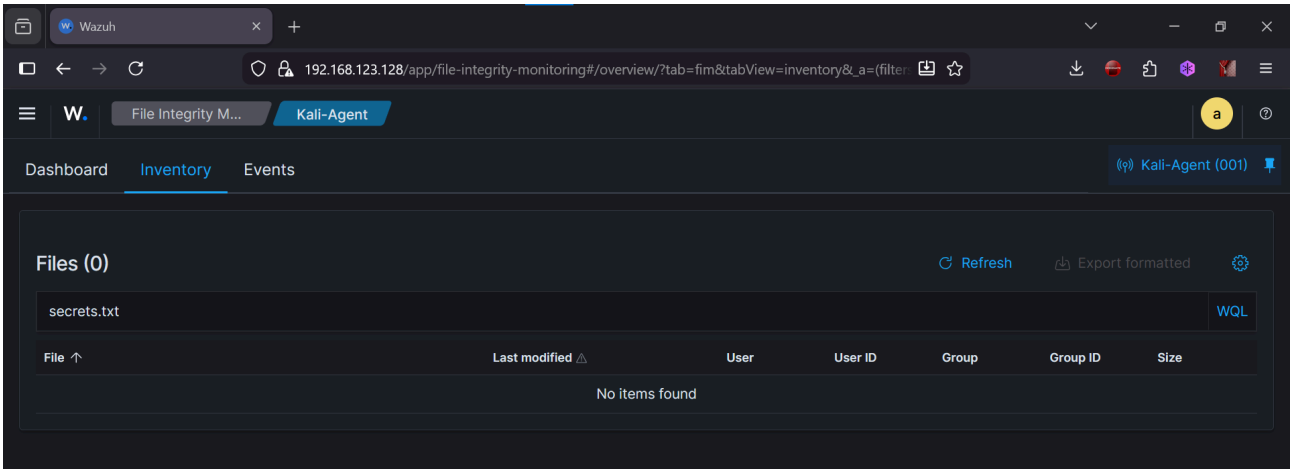
Step 15: Confirm File Integrity Monitoring for File Deletion

a. Confirm File Integrity Monitoring for Deleted File on **Kali OS** VM.

i. Return to the **Firefox** browser on the host machine **(Windows 10 x64)** and access the Wazuh Web Console.

ii. Repeat the steps from **Step 13-a-ii** to **Step 13-a-vii**.

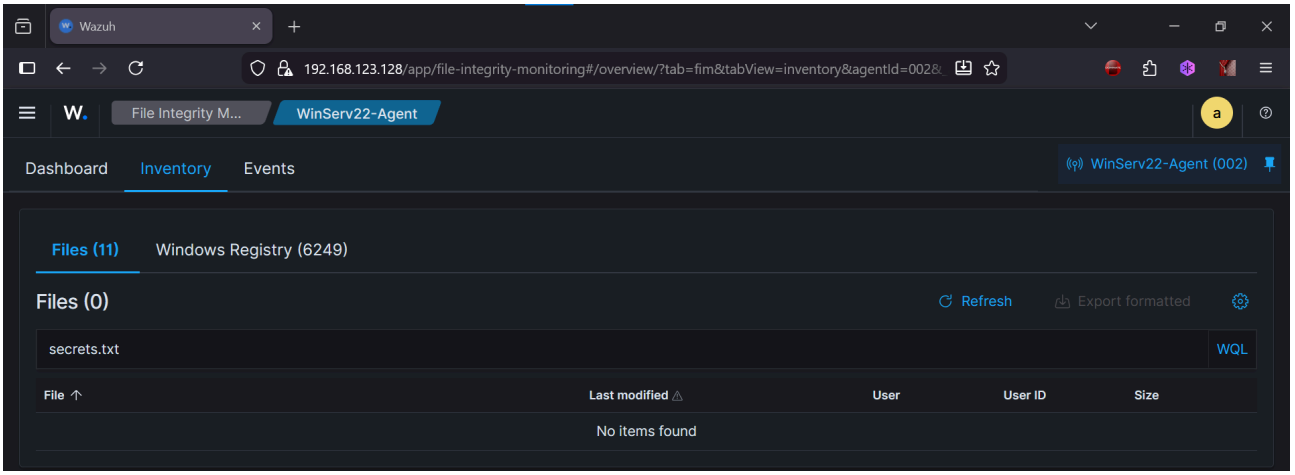
iii. Among the returned results, the monitored file which was created in **KaliOS** VM **(secrets.txt)** is absent, indicating it was deleted.



b. Confirm File Integrity Monitoring for Deleted File on **WindowsServer2022** VM.

i. Repeat the steps from **Step 13-b-i** to **Step 13-b-v**.

ii. Among the returned results, the monitored file which was created in **WindowsServer2022** VM **(secrets.txt)** is absent, indicating it was deleted.

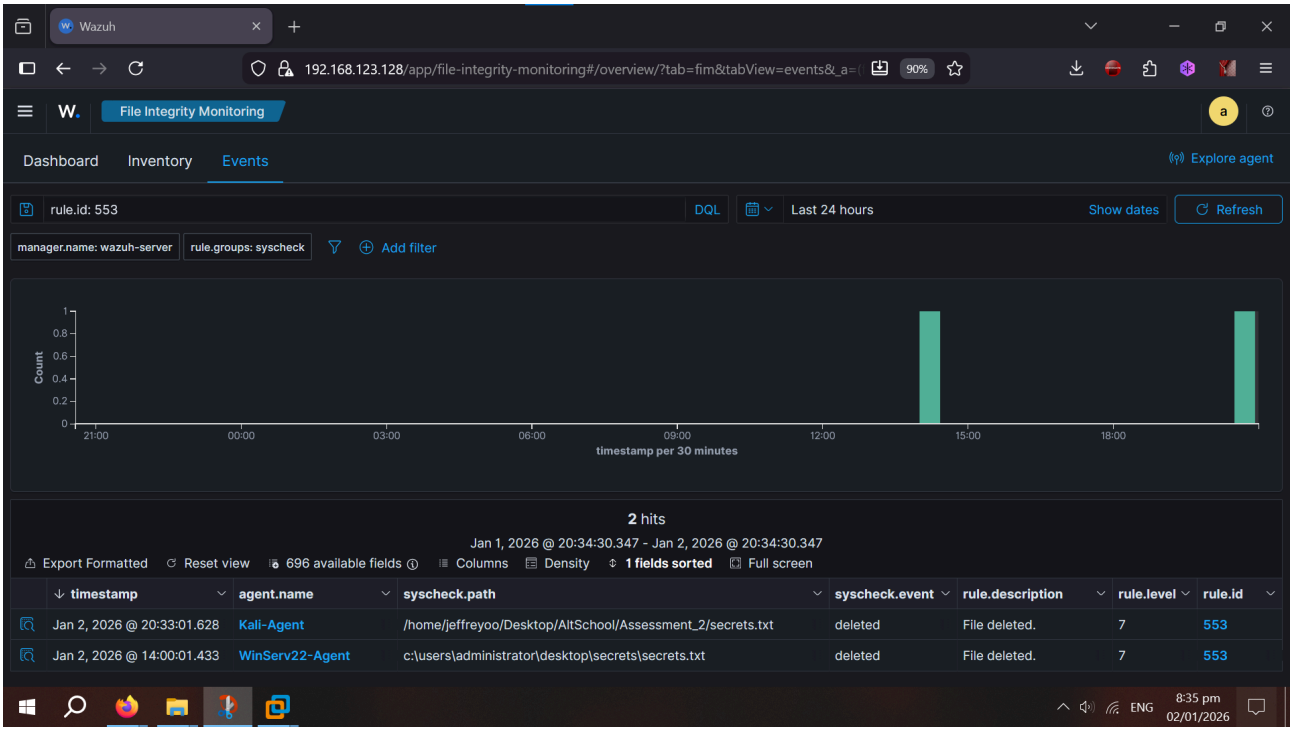


c. Confirm File Integrity Monitoring for File Deletion on both VMs.

i. Repeat the steps from **Step 13-c-i** to **Step 13-c-ii**.

ii. In the **Search** text box, type **rule.id: 553** and press **Enter.**

iii. This returns two listed results, which are the **secrets.txt** files from both VMs, confirming that these files from both agents were indeed deleted.



General Security Alerts

Reviewing Daily Security Events

Step 16: Examine General Security Logs and Alerts

a. Navigate to the **Threat Hunting** Page:

i. On the **Firefox** browser on the host machine **(Windows 10 x64),** return to the **Overview** page on the Wazuh Web Console.

ii. On the **Overview** page, click the hamburger/menu icon on the top-left side of the page. This opens a side-bar navigation menu.

iii. Scroll down to the **Threat intelligence** dropdown button. Click it.

iv. Find the **Threat Hunting** hyperlink under the **Threat intelligence** dropdown button. Click the link. *This opens a **Threat Hunting** page and defaults to the **Dashboard** tab as shown on the top navigation bar.*

v. **Note:** In previous versions of **Wazuh,** this page was called **Security Events** and the pathway to this page was **Wazuh Menu → Modules → Security Events** (as is shown in the Assessment guide). So far, the page name has been updated to **Threat Hunting.**

b. Review Security Events & Alerts:

i. On the **Dashboard** page, observe and review the security information (including alerts) displayed on the web interface using numerical reports, graphs and pie charts contained in widgets.

ii. Navigate to the **Events** tab via the top navigation bar. *This opens the **Events** page.*

iii. On the **Events** page, observe and review the security events displayed on the web interface in 2 sections:
- **Section 1:** a panel containing a histogram (bar graph) with **Count** (number of security events) on the y-axis and **timestamp per minute** (time intervals) along the x-axis.
- **Section 2:** a data grid displaying security events in sorted rows, under **timestamp, agent.name, rule.description, rule.level and rule.id** columns.

iv. The information displayed on both **Dashboard** and **Inventory** tabs, under **Threat Hunting** confirm the functionality of the **Wazuh** server, as well as the connected agents and the active monitoring status.

v. **Note:** To the right of the **Search** text box is a **Show dates** box. This box is where the time range for any executed search is configured. For monitoring recent events, setting a start time that is not too far back, and setting the end time to **Now,** is best.

PCI DSS & GDPR Regulations

Checking Compliance

Step 17: Examine General PCI DSS Security Logs

a. Access **PCI DSS** Dashboard:

i. On the **Firefox** browser on the host machine **(Windows 10 x64),** return to the **Overview** page on the Wazuh Web Console.

ii. On the **Overview** page, click the hamburger/menu icon on the top-left side of the page. This opens a side-bar navigation menu.

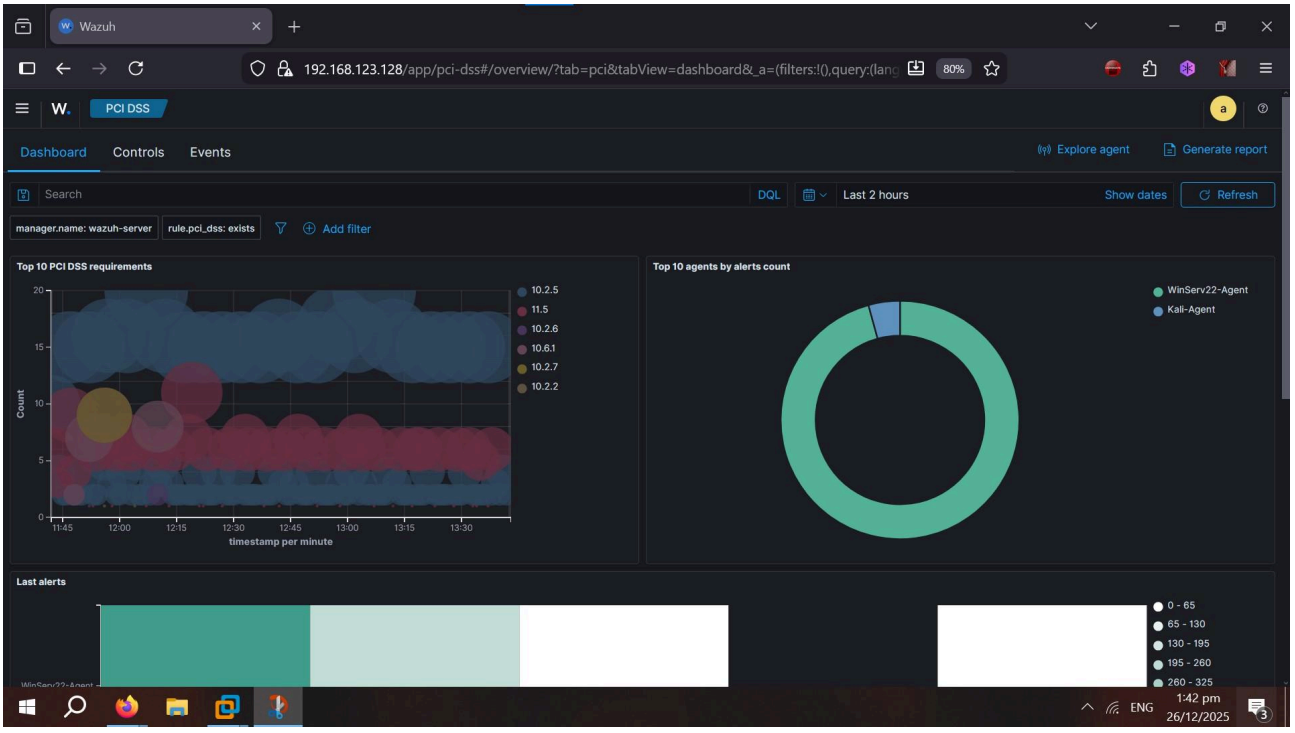
iii. Scroll down to the **Security Operations** dropdown button. Click it.

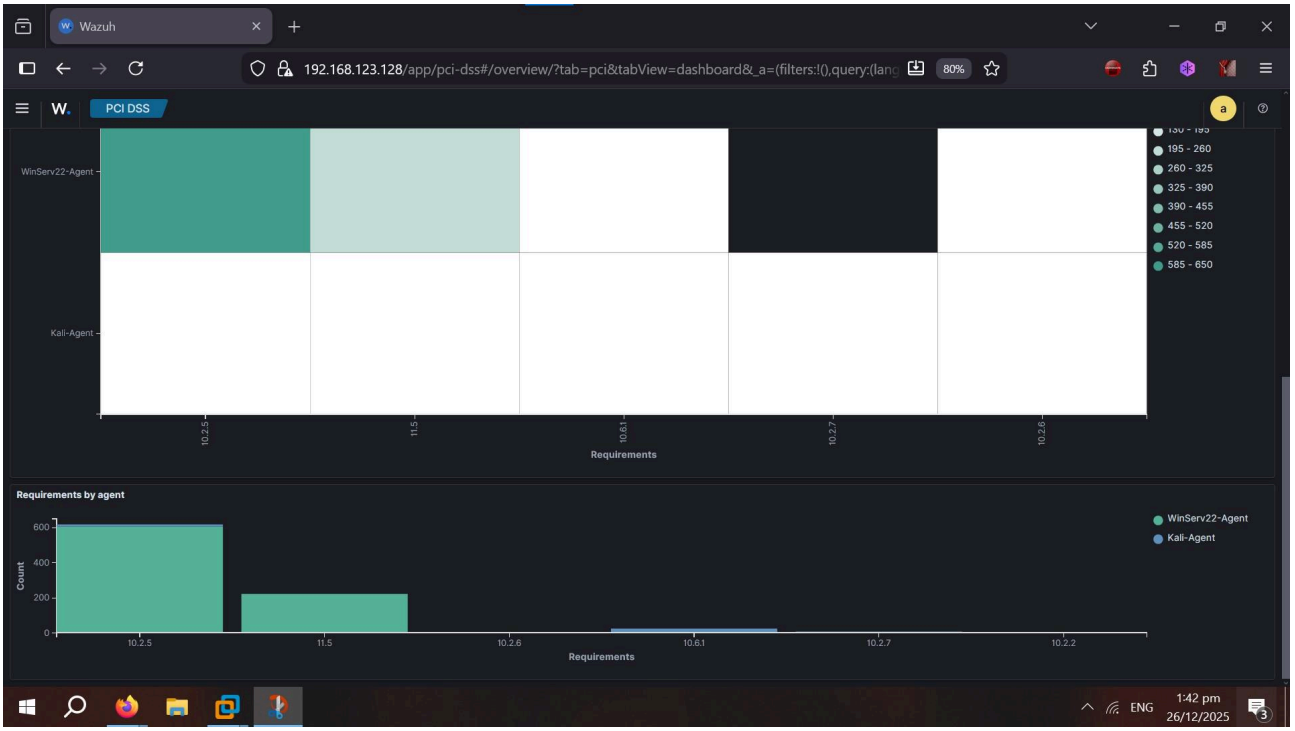
iv. Find the **PCI DSS** hyperlink under the **Security Operations** dropdown button. Click the link. *This opens a **PCI DSS** page and defaults to the **Dashboard** tab as shown on the top navigation bar.*

b. Review **PCI DSS** Dashboard:

i. On the **Dashboard** page, observe and review the security information (including alerts) displayed on the web interface in the following widgets:

- **Top 10 PCI DSS requirements:** a **colour bubble chart** with **Count** (number of security events) along the y-axis, **timestamp per minute** (time intervals) along the x-axis, and bubbles of different colours, each indicating a different PCI DSS requirement, as indicated on the included key. This **colour bubble chart** shows how much and how frequently the different **PCI DSS** requirements are complied with.
- **Top 10 agents by alerts count:** a **donut chart** which displays the alert distribution proportion between the added agents.
- **Last alerts:** a **heatmap chart** which uses a colour matrix to indicate the amount of alerts according to the included colour scale. The added agents are on the vertical y-axis and **Requirements** on the horizontal x-axis. Each cell colour indicates the volume of alerts as compared to the others, within the given recent time range.
- **Requirements by agent:** a **segmented bar chart** with **Count** (number of security events) along the vertical y-axis, and **Requirements** (PCI DSS requirements displayed by code) on the horizontal x-axis. With the added agents given a colour code in the included key, this **segmented bar chart** displays a comparison between the number of requirements met by each agent by stacking them for visual clarity.





c. Review **PCI DSS** Security Events:

i. Return to the **Threat Hunting** page (**Dashboard** tab) (as shown in **Step 16-a-iv**)

ii. In the **Search** text box, type in the following:

```
rule.pci_dss: *
```

The above search query applies a **PCI DSS** rule filter to the information displayed on the page.

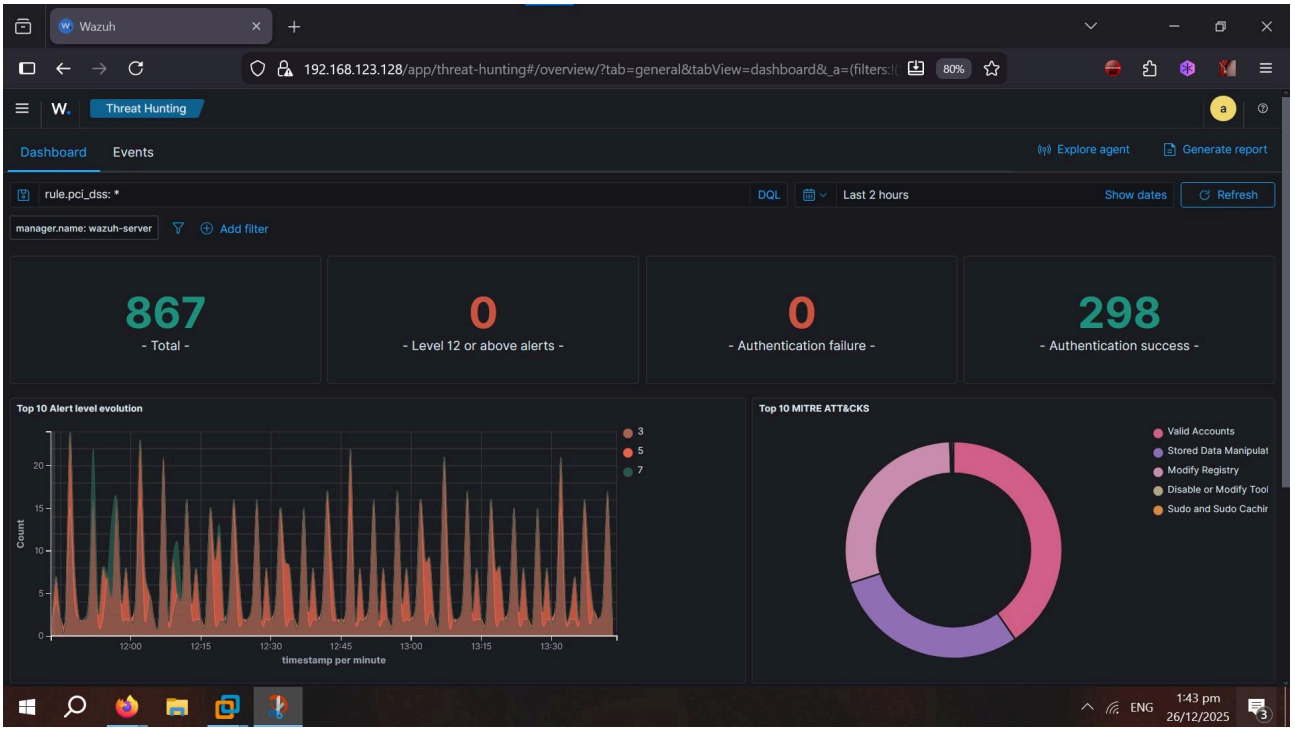
iii. In the **Show dates** text box, located to the right of the **Search** text box, configure the time range within which the search filter should be applied.

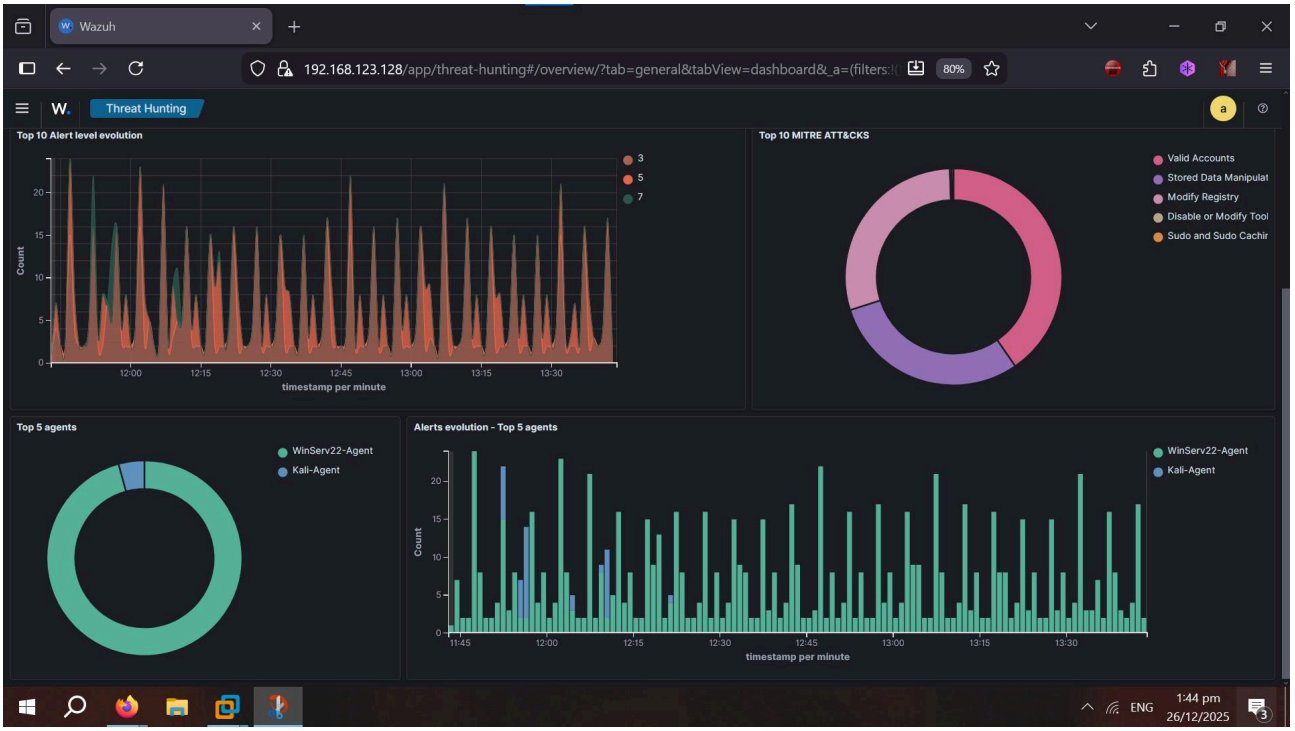
iv. Press **Enter.**

v. With the search filter and time range applied, observe and review the security information (including alerts) displayed on the web interface in the following widgets:

- **Total:** a number indicating a total of all alerts.
- **Level 12 or above alerts:** a number indicating a total of all alerts which are of a level 12 severity and above.
- **Authentication failure:** a number indicating a total of all authentication failures.
- **Authentication success:** a number indicating a total of all authentication successes.
- **Top 10 Alert level evolution:** a **graph** with **Count** (number of security events) along the y-axis, **timestamp per minute** (time intervals) along the x-axis, and each alert-level number, colour coded in an included key. This graph is used to determine the trends of different alert levels across time intervals.

- **Top 10 MITRE ATT&CKS:** a **donut chart** which displays the distribution of all attacks by proportion across each “Top 10 MITRE ATT&CK”. Each relevant “Top 10 MITRE ATT&CK” attack is included in a colour coded key.
- **Top 5 agents:** a **donut chart** which displays the distribution of all relevant alerts by proportion across each added agent. Each agent is included in a colour coded key.
- **Alerts evolution - Top 5 agents:** a **segmented bar chart** with **Count** (number of security events) along the y-axis, **timestamp per minute** (time intervals) along the x-axis, and each added agent, colour coded in an included key. This **segmented bar chart** displays a comparison between the number of alerts generated by each agent, as well as total number of alerts generated, distributed across time intervals.





Step 18: Examine General GDPR Security Logs

a. Access **GDPR** Dashboard:

i. On the **Firefox** browser on the host machine **(Windows 10 x64),** return to the **Overview** page on the Wazuh Web Console.

ii. On the **Overview** page, click the hamburger/menu icon on the top-left side of the page. This opens a side-bar navigation menu.

iii. Scroll down to the **Security Operations** dropdown button. Click it.

iv. Find the **GDPR** hyperlink under the **Security Operations** dropdown button. Click the link. *This opens a **GDPR** page and defaults to the **Dashboard** tab as shown on the top navigation bar.*

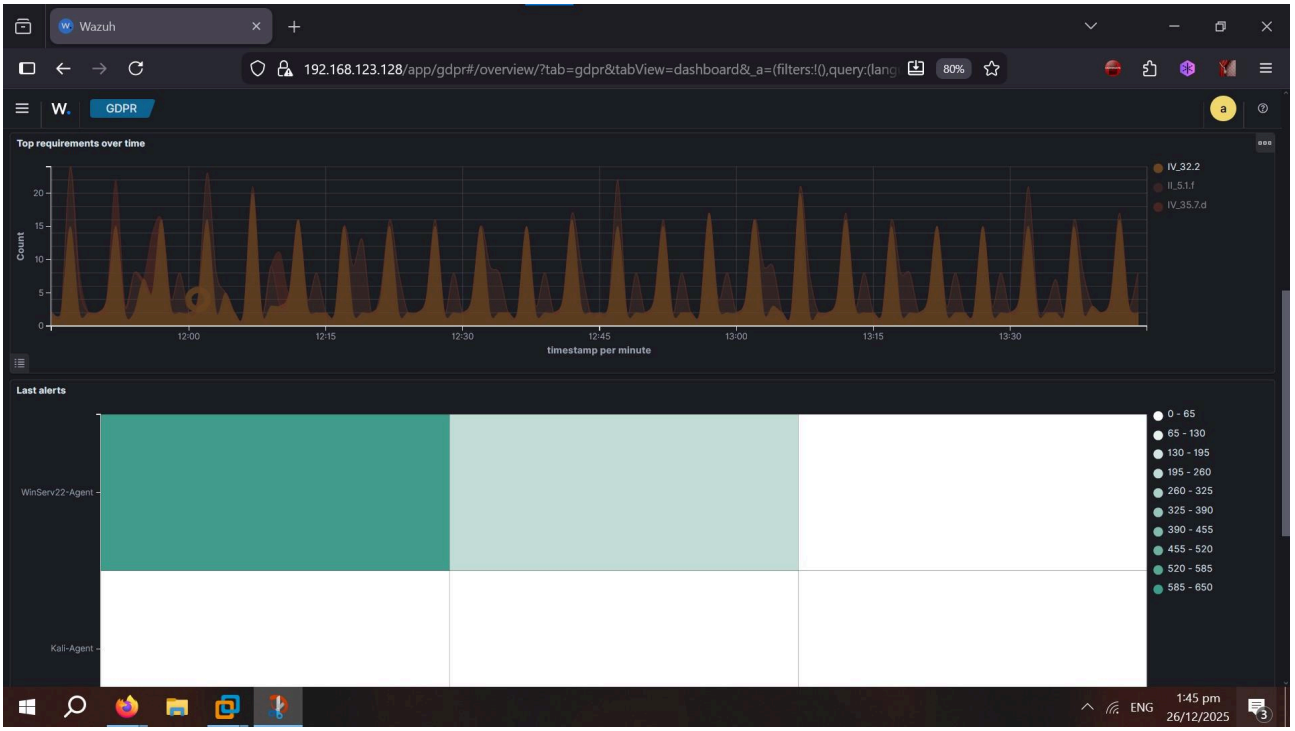
b. Review **GDPR** Dashboard:

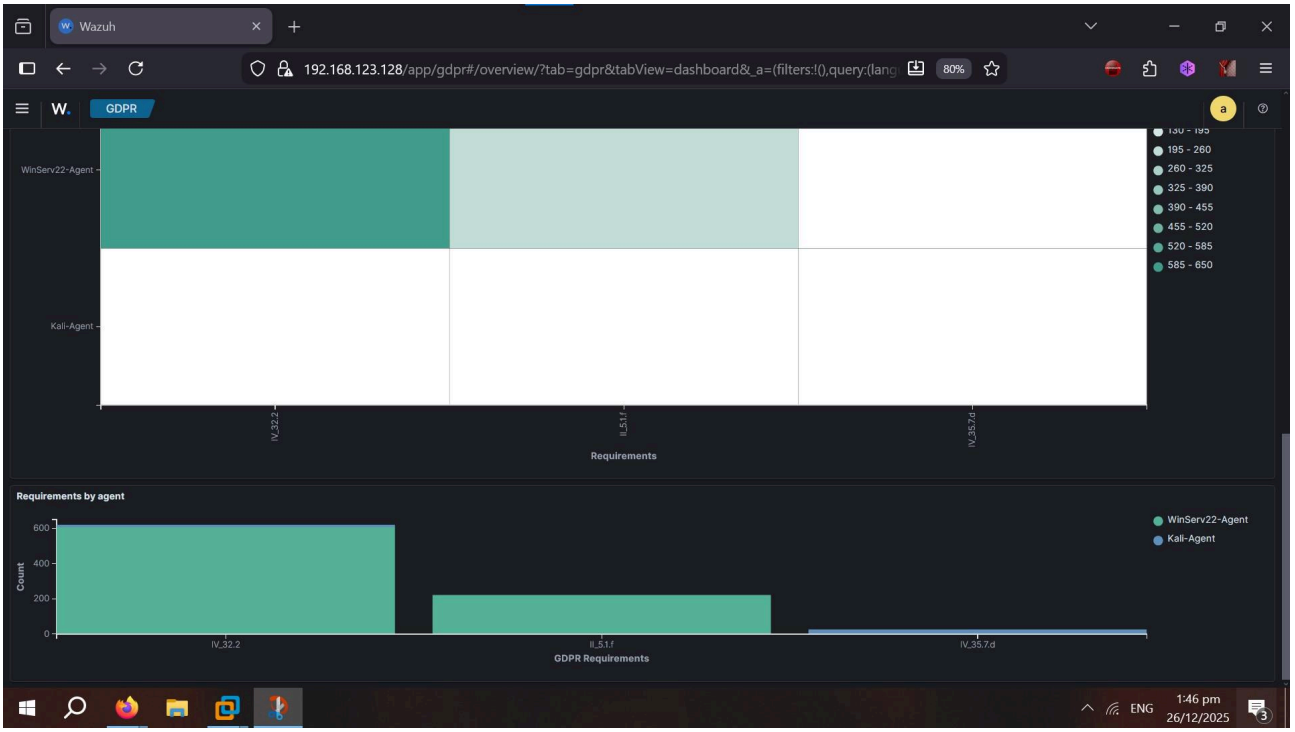
i. On the **Dashboard** page, observe and review the security information (including alerts) displayed on the web interface in the following widgets:

- **Top 10 agents by alerts number:** a **donut chart** which displays the alert distribution proportion between the added agents.
- **GDPR requirements:** a **colour bubble chart** with **Count** (number of requirements) along the y-axis, **timestamp per minute** (time intervals) along the x-axis, and bubbles of different colours, each indicating a different **GDPR** requirement, as indicated on the included key. This **colour bubble chart** shows how much and how frequently the different **GDPR** requirements are active.
- **Top requirements over time:** an **area chart** with **Count** (number of requirements) along the y-axis, **timestamp per minute** (time intervals) along the x-axis, and bubbles of different colours, each indicating a different **GDPR** requirement, as indicated on the included key. It illustrates the frequency of

the most active requirements, comparatively revealing that information about them in contrast to one another.

- **Last alerts:** a **heatmap chart** which uses a colour matrix to indicate the amount of alerts according to the included colour scale. The added agents are on the vertical y-axis and **Requirements** on the horizontal x-axis. Each cell colour indicates the volume of alerts as compared to the others, within the given recent time range.
- **Requirements by agent:** a **segmented bar chart** with **Count** (number of **GDPR** requirements) along the vertical y-axis, and **GDPR Requirements** (**GDPR** requirements displayed by code) on the horizontal x-axis. With the added agents given a colour code in the included key, this **segmented bar chart** displays a comparison between the number of requirements met by each agent by stacking them for visual clarity.





c. Review **GDPR** Security Events:

i. Return to the **Threat Hunting** page (**Dashboard** tab) (as shown in **Step 16-a-iv**)

ii. In the **Search** text box, type in the following:

```
rule.gdpr: *
```

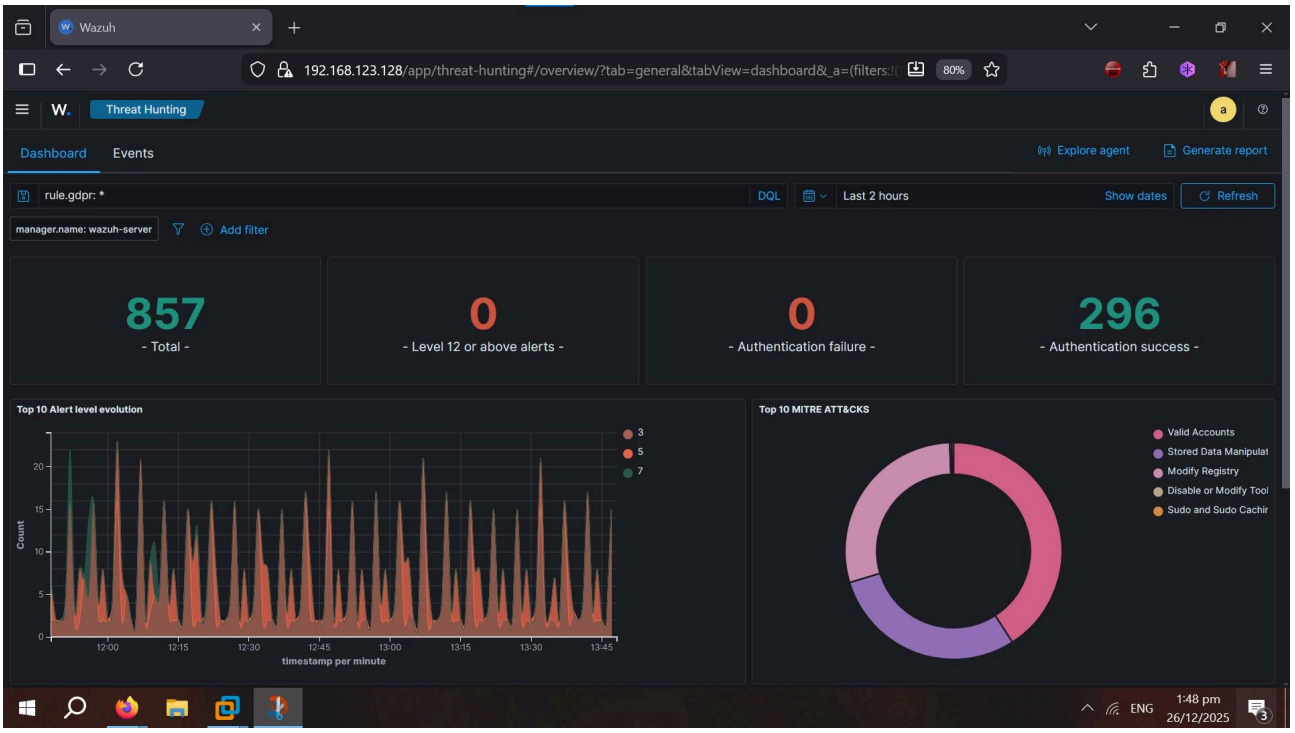
The above search query applies a **GDPR** rule filter to the information displayed on the page.

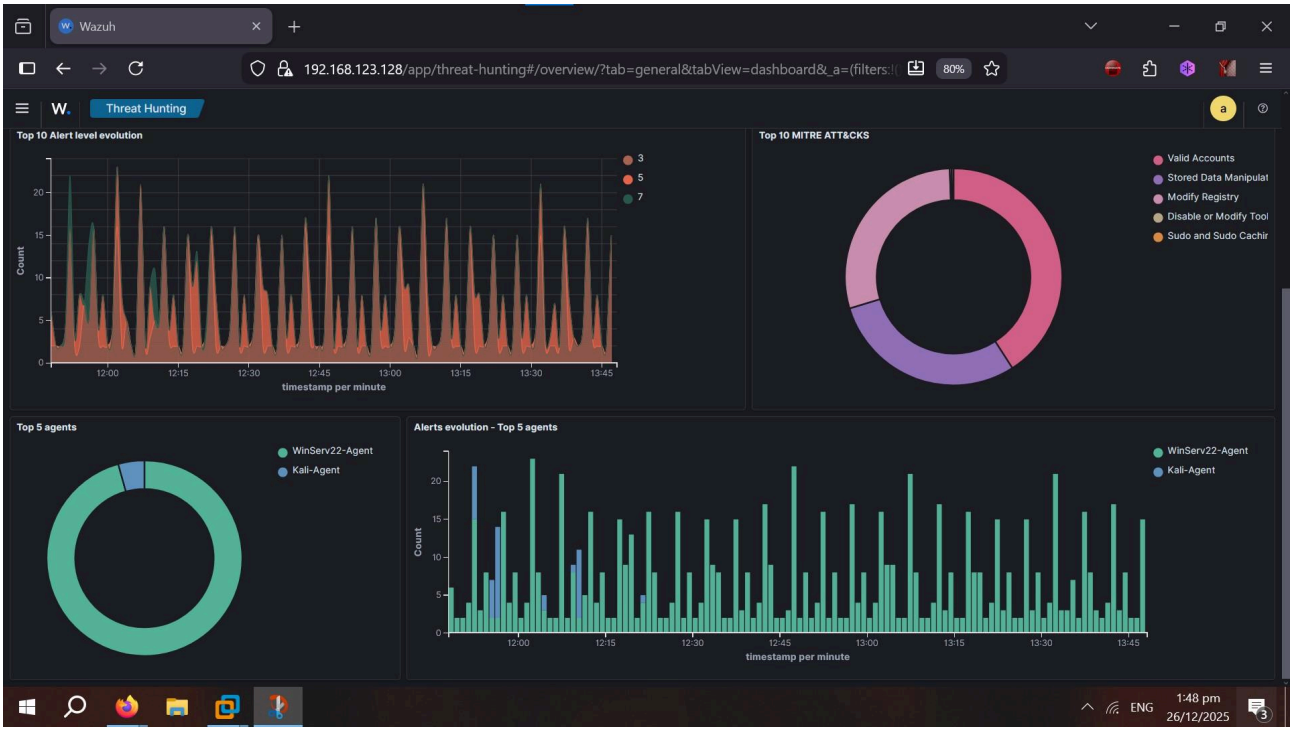
iii. In the **Show dates** text box, located to the right of the **Search** text box, configure the time range within which the search filter should be applied.

iv. Press **Enter.**

v. With the search filter and time range applied, observe and review the security information (including alerts) displayed on the web interface in widgets (similar to that of the **PCI DSS** session from **Step 17-c-v**):

- Total
- Level 12 or above alerts
- Authentication failure
- Authentication success
- Top 10 Alert level evolution
- Top 10 MITRE ATT&CKS
- Top 5 agents
- Alerts evolution - Top 5 agents





Conclusion

Review & Lessons Learned

Review

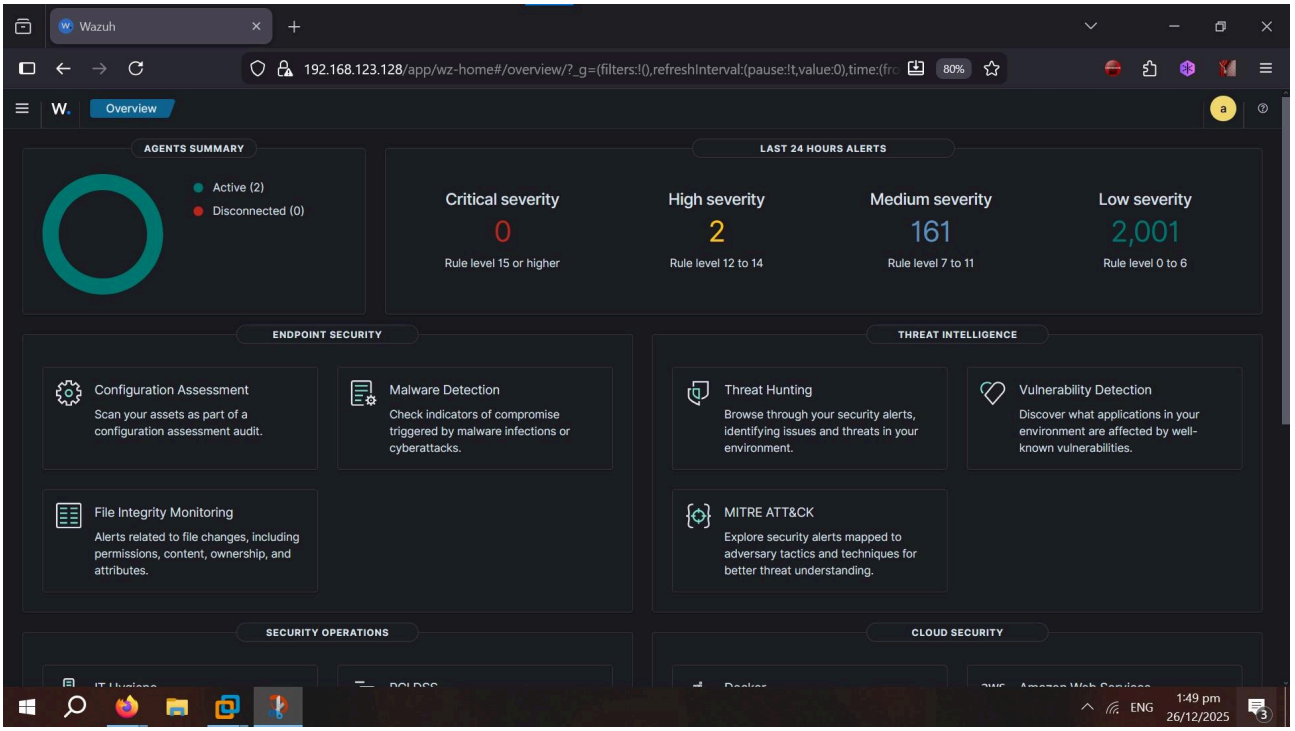
In this project, I preconfigured the virtualizer **(VMware Workstation Pro 17.5)** and integrated the **Wazuh** virtual machine. I accessed the web-console and deployed two agents: a Linux agent (Kali) and a Windows agent (Windows Server 2022); then I configured the appearance of the web console by activating “Dark mode” for easier use.

I added unique folders and contained files for monitoring on both endpoints and configured File Integrity Monitoring rules on the configuration files. After confirming that monitoring is active, I modified the monitored files and Wazuh server recorded the modification.

I also explored general security events, as well as **GDPR** and **PCI DSS** compliance information, exploring the data widgets and learning to interpret the different graphical representations of the data.

Lessons Learned

Given the options and capabilities hosted on Wazuh, it proves a robust tool for comprehensive and exhaustive endpoint monitoring and it remains a capable tool for any Cybersecurity professional.


Wazuh
192.168.123.128/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(fr
80%
Overview
AGENTS SUMMARY
Active (2)
Disconnected (0)
LAST 24 HOURS ALERTS
Critical severity
0
Rule level 15 or higher
High severity
2
Rule level 12 to 14
Medium severity
161
Rule level 7 to 11
Low severity
2,001
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.
SECURITY OPERATIONS
CLOUD SECURITY
ENG
1:49 pm
26/12/2025