Network Protection for Energy Control Systems

CSP004_C_E

PRESENTATION BY:
DR. STEFAN SCHAUER
DR. ABDELKADER SHAABAN
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Network Protection for Energy Control Systems

These slides outline the essential offensive tools that will be used in this course.

These tools are intended for use within this course to demonstrate how different tools can be employed for various cyberattack activities and address existing security weaknesses to avoid or mitigate related cyber risks. Therefore, all these practical activities are solely intended for educational purposes ONLY and not for any other malicious or unauthorized activities.

SIEM

Wazuh

Wazuh

- Wazuh **delivers** robust security **monitoring** and **protection** for IT **assets** using:
  - **Security Information and Event Management** (**SIEM**) and
  - **Extended Detection and Response** (**XDR**) capabilities.

- Wazuh can be used in multiple **use cases** as **follows**:

Configuration Assessment

Malware Detection

File Integrity Monitoring

Threat Hunting

Log Data Analysis

Vulnerability Detection

Workload Protection

Posture Management

Containers Security

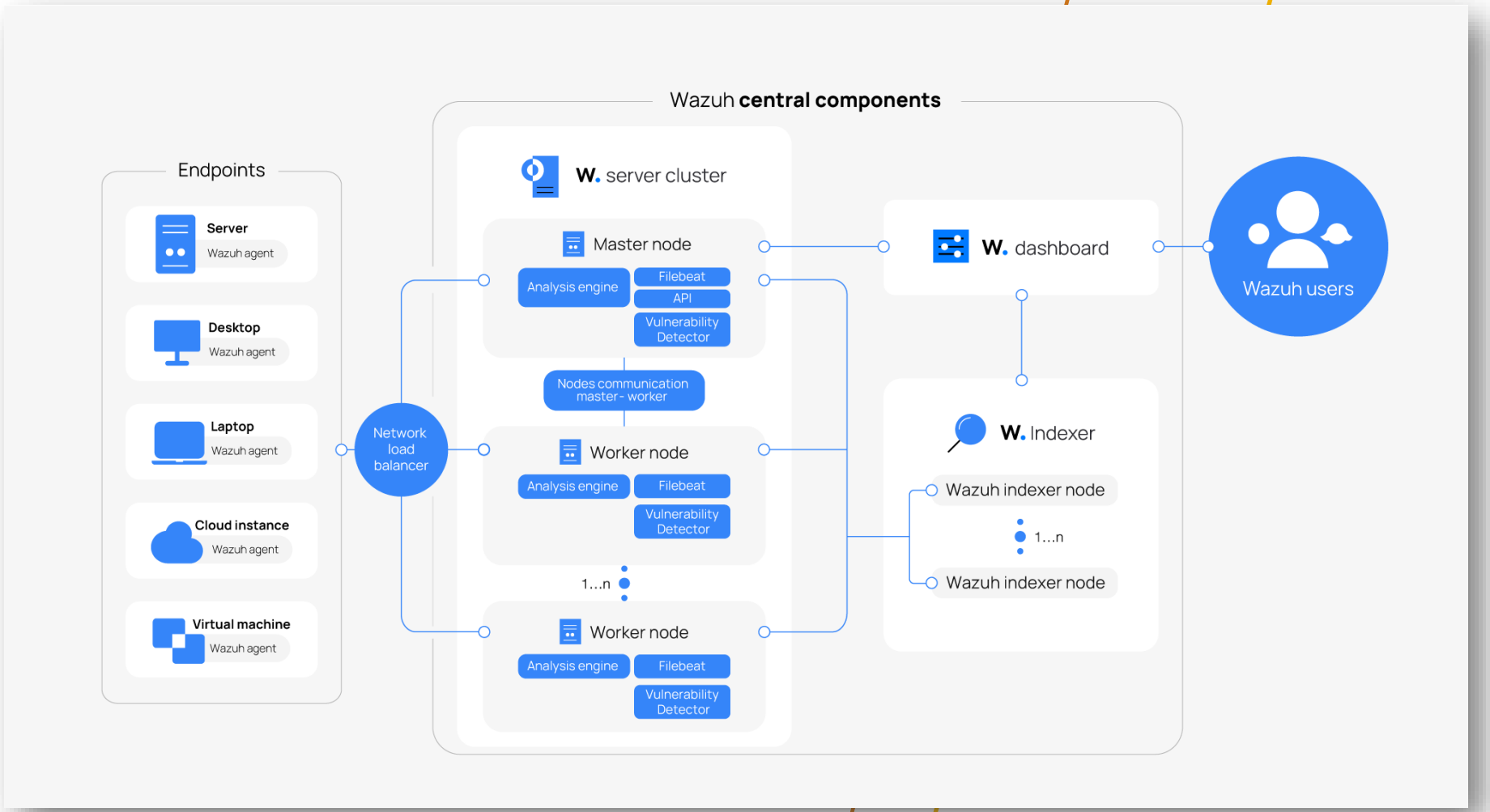
IT Hygiene

Regulatory Compliance

Incident Response

Overview | Wazuh

Wazuh: Central Components



Architecture - Getting started with Wazuh · Wazuh documentation

Wazuh: Central Components

W. indexer

The Wazuh **indexer** is a highly **scalable**, **full-text search** and **analytics** engine.

This central component **indexes** and **stores alerts generated** by the Wazuh server.

W. server

The Wazuh **server analyzes data received** from the **agents** and processes it using threat intelligence.

A **single server** can **analyze data** from **thousands** of **agents**, and scale when set up as a **cluster**.

It is also used to **manage** the **agents**, configuring them **remotely** when necessary.

W. dashboard

The Wazuh **dashboard** is the web **user interface** for data **visualization**, **analysis**, and management.

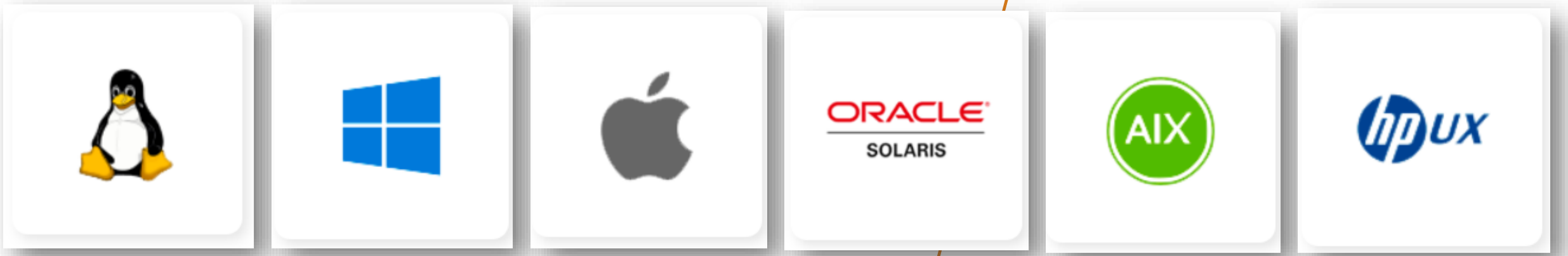
It includes **dashboards** for regulatory **compliance**, **vulnerabilities**, **file integrity**, **configuration assessment**, and cloud **infrastructure events**, among others.

Install | Wazuh

Wazuh Agents

W. agent

Wazuh **agents** are installed on **endpoints** such as **laptops**, **desktops**, **servers**, **cloud instances**, or **virtual machines**. They provide **threat prevention**, **detection**, and **response capabilities**.



Install | Wazuh

Installing Wazuh Server

- 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.

- Select the **Wazuh version** from the **top-right part** of the page.

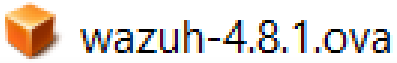
- Then **download** the virtual appliance (OVA), which **contains** the following **components**:
  - Amazon Linux 2
  - Wazuh manager 4.8.1
  - Wazuh indexer 4.8.1
  - Filebeat-OSS 7.10.2
  - Wazuh dashboard 4.8.1

- More details about the **installation** can be found on the Wazuh documentation page.

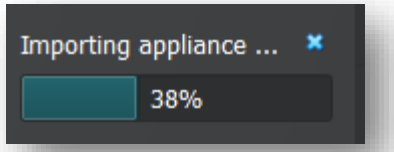
Virtual Machine (OVA) - Installation alternatives (wazuh.com)

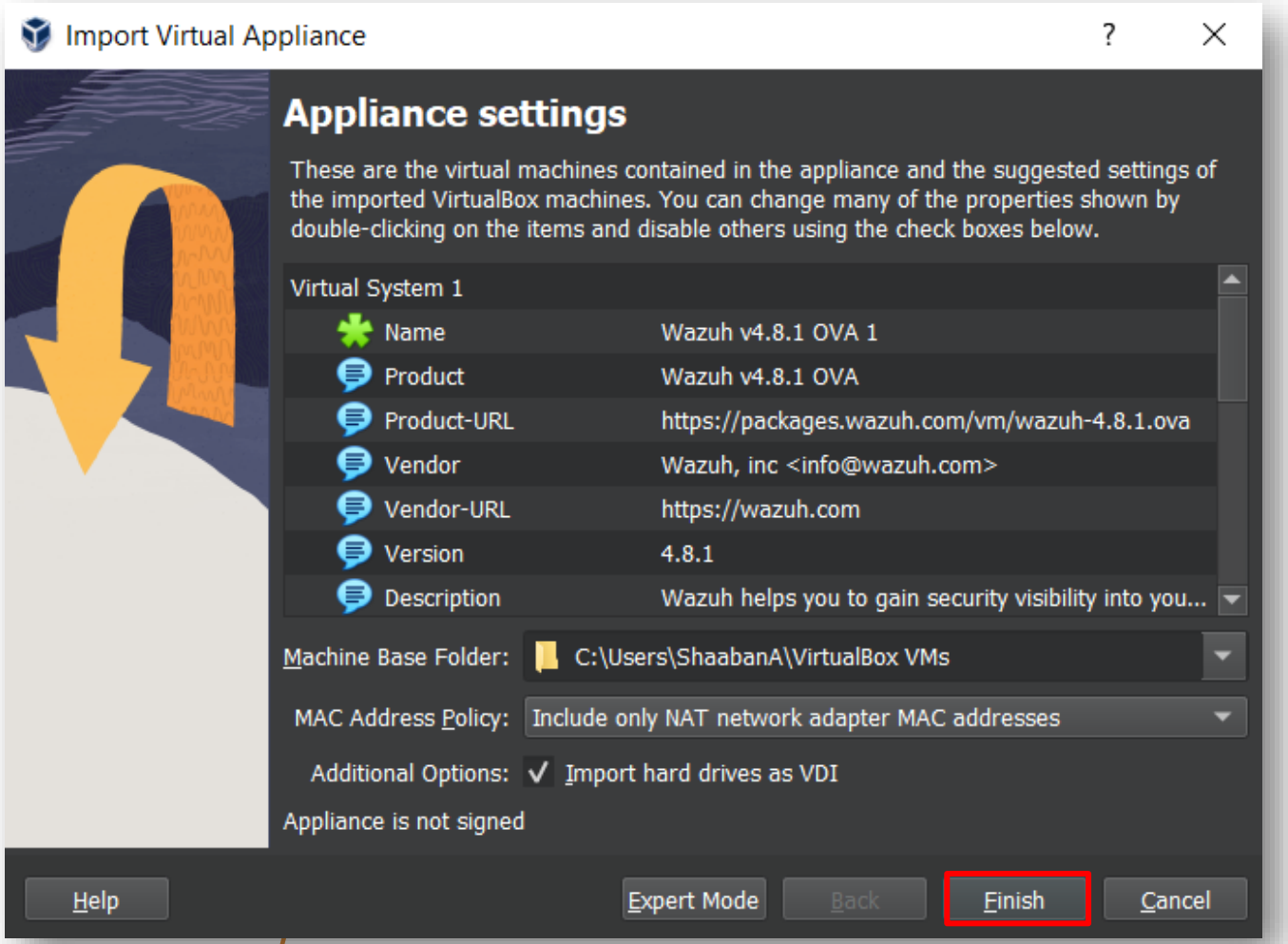
Installing Wazuh Server

- Navigate to the **downloaded .ova** file and **double-click** on it.



- Press **Finish** and then **wait** until the **VM** is **successfully** imported.



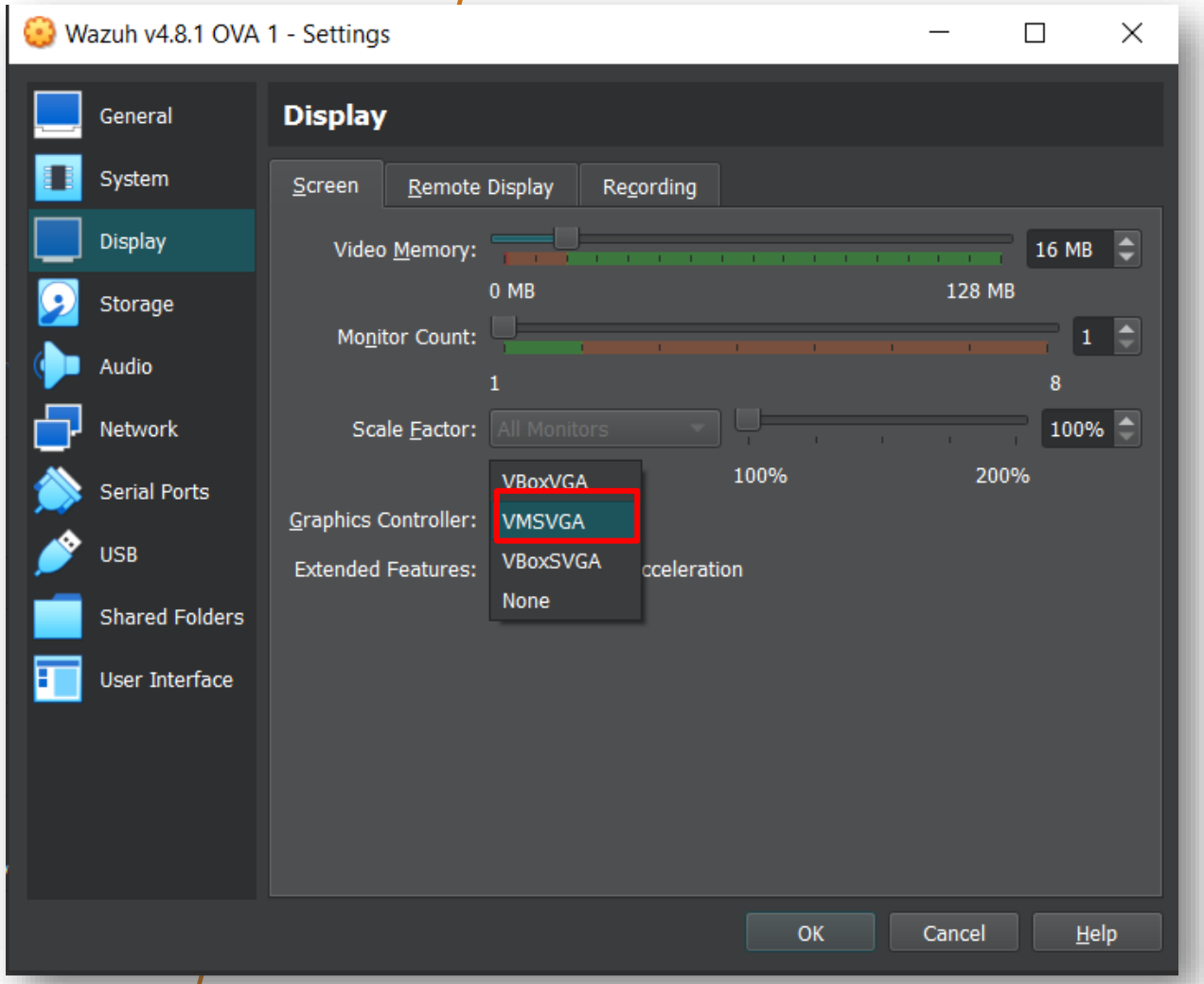


Installing Wazuh Server

- Select the **imported** VM of Wazuh, and go to **Settings** > **Display**.

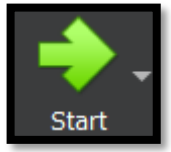
- Selct the **VMSVGA** in the **Graphics Controller.**

- Press **ok**

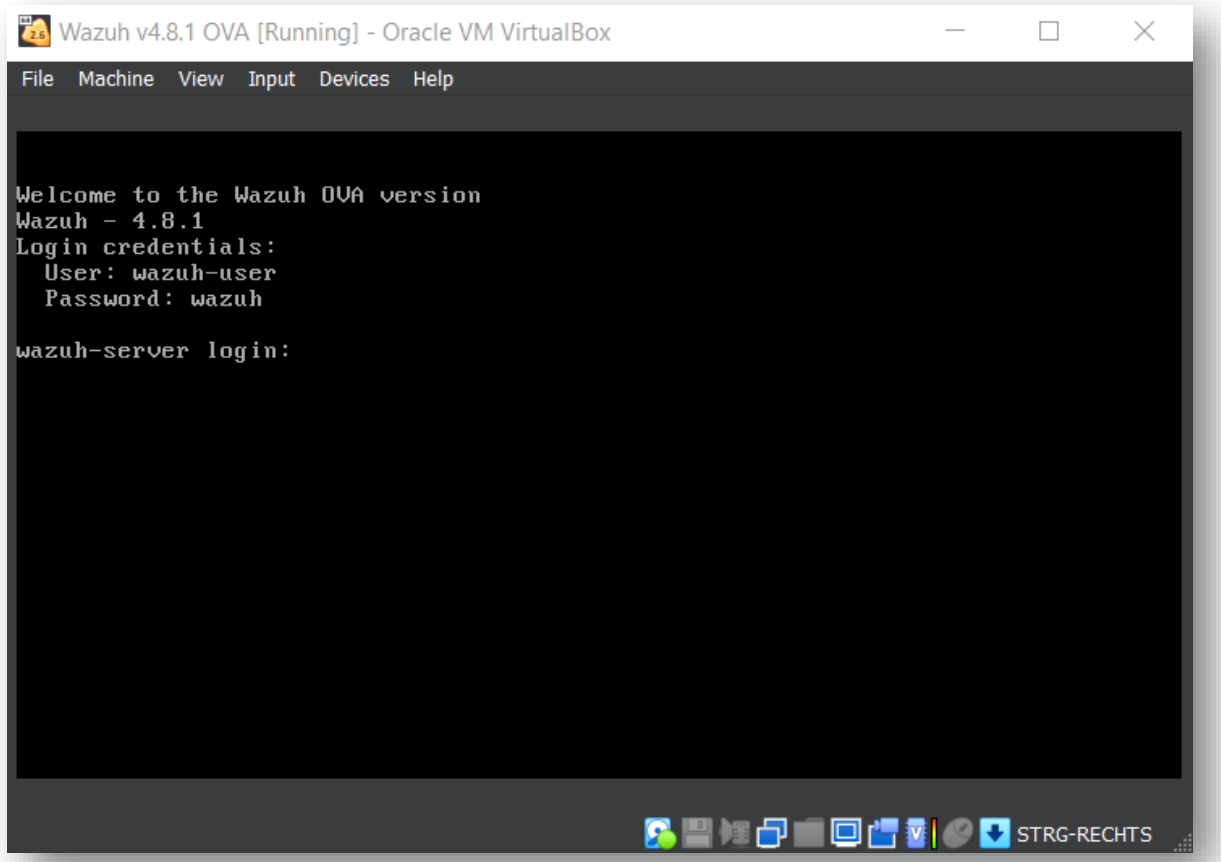


Launching Wazuh Server

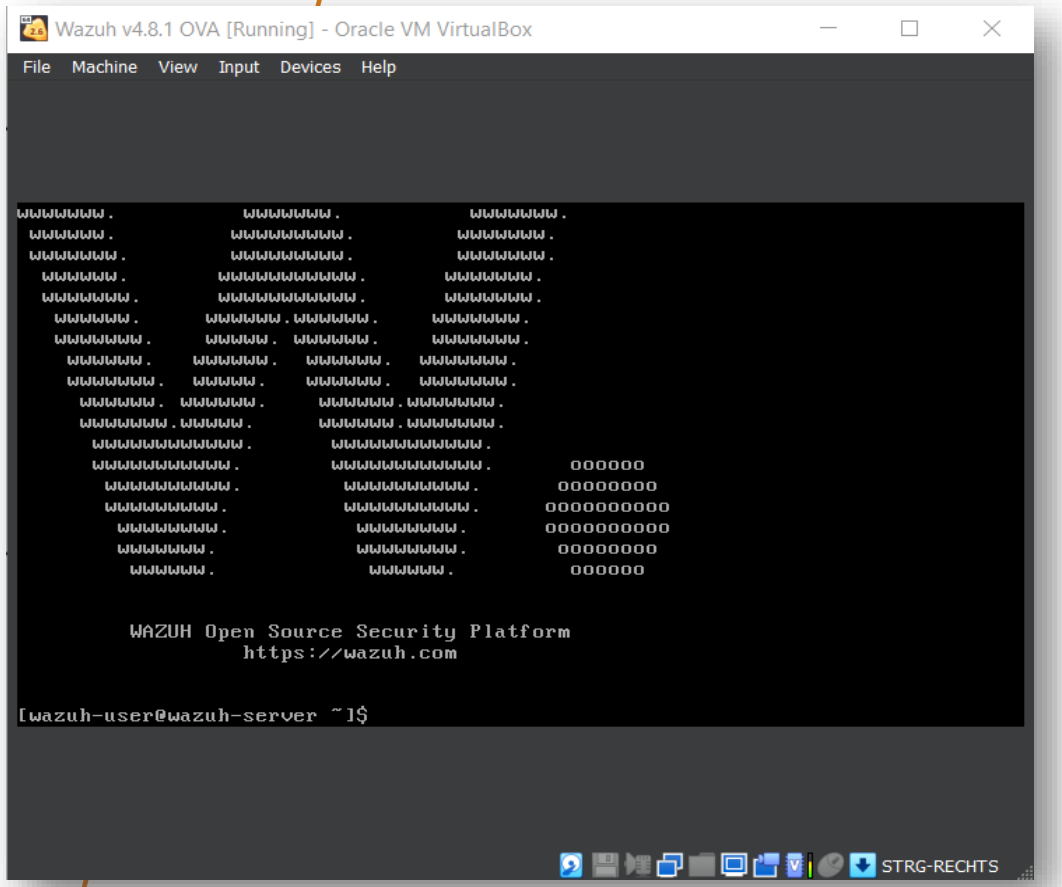
Press the **start button**.



Wait until you reach the **login** screen.



- Enter the **user** and **password**.
- **By default**:
  - **User**: wazuh-user
  - **Password**: wazuh

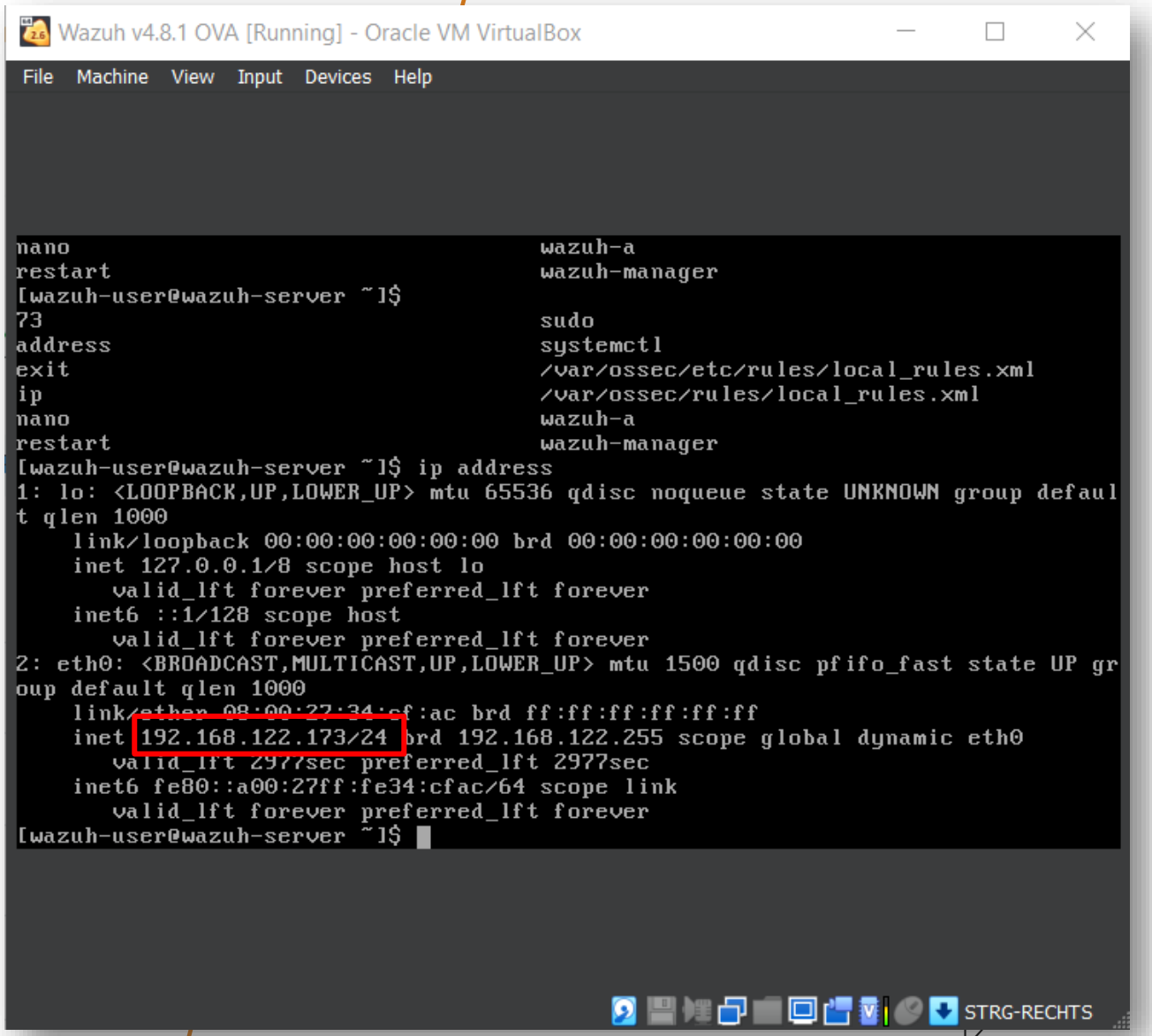


The Wazuh server has been **successfully installed** and **launched**.

Launching Wazuh Server

- First, we need to find the **IP address** of the Wazuh server.

- Go to the **Wazuh server** and type `**ip address**`.



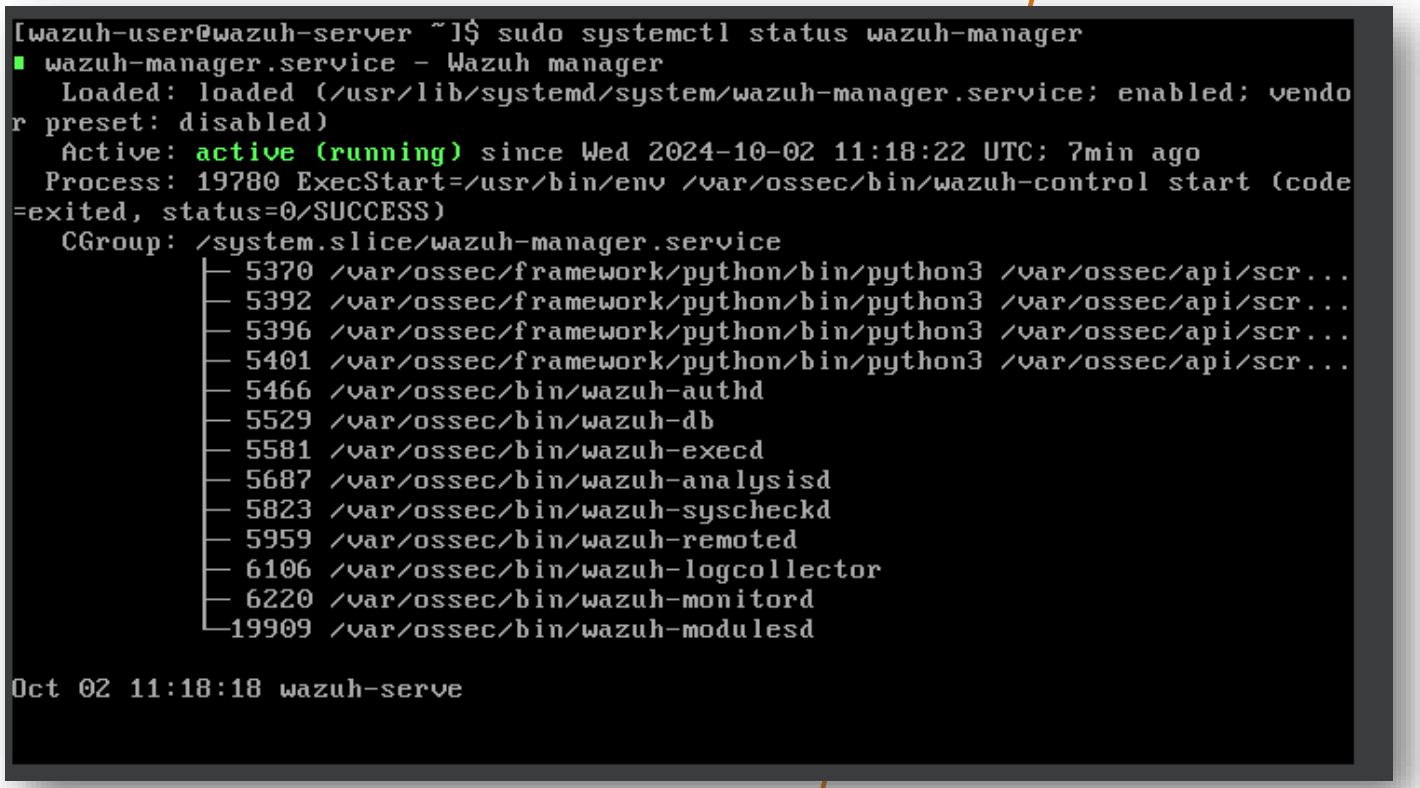
Launching Wazuh Server

Note that **sometimes** the **Wazuh manager** does **not start correctly**. Ensure the **status** of the **manager** from the **Wazuh server** by using:

sudo systemctl status wazuh-manager | grep running

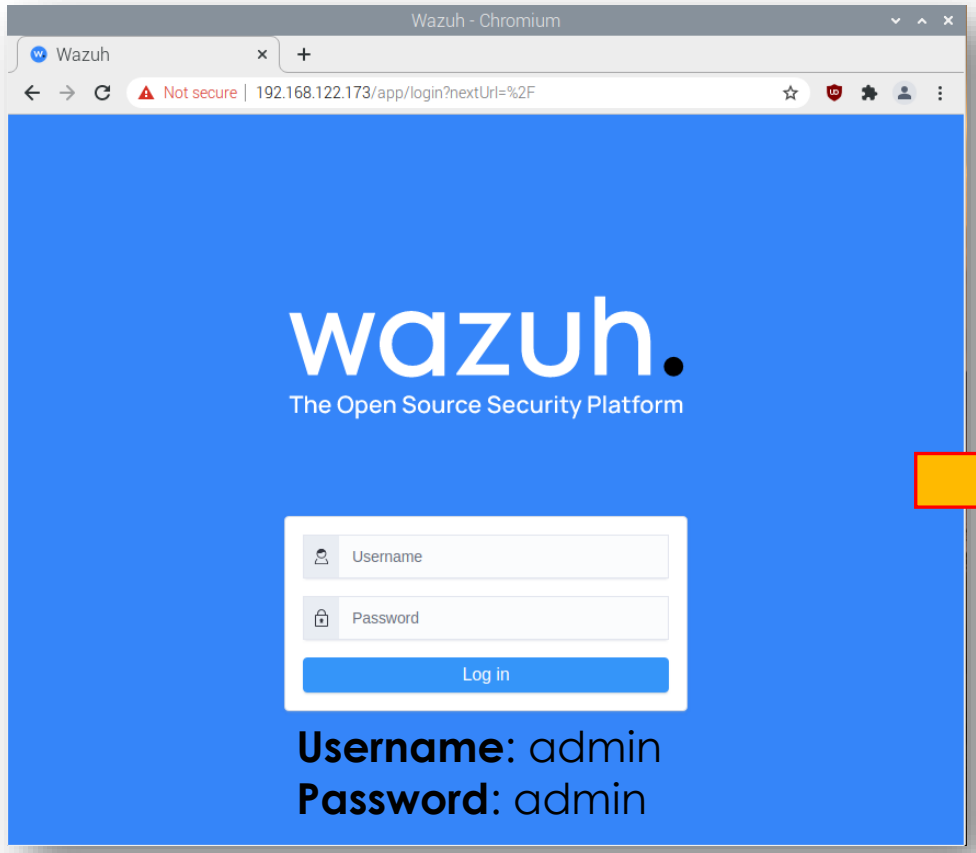
If it is not **started**, **restart** it with:

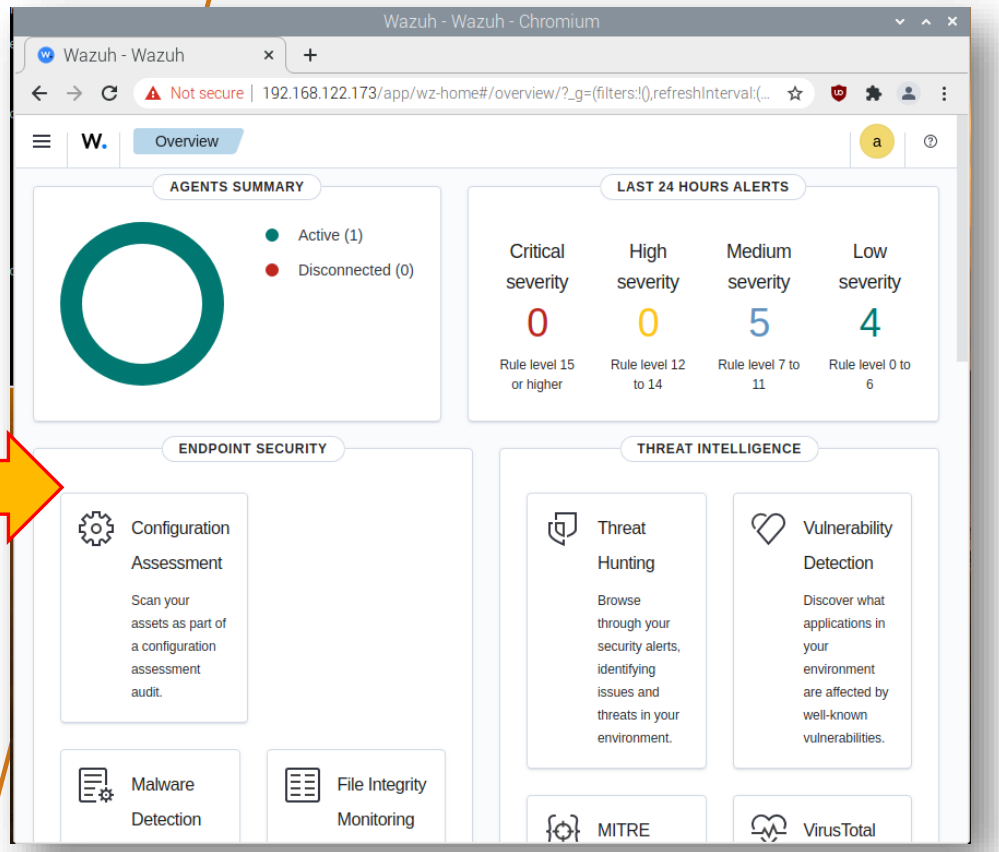
sudo systemctl restart wazuh-manager



Installing Agent (Endpoint)

- Open the **web browser** on the **Agent** and visit:
  https://wazuh-server-ip-address
- In our case the server-ip is **192.168.122.173**
  https://192.168.122.173

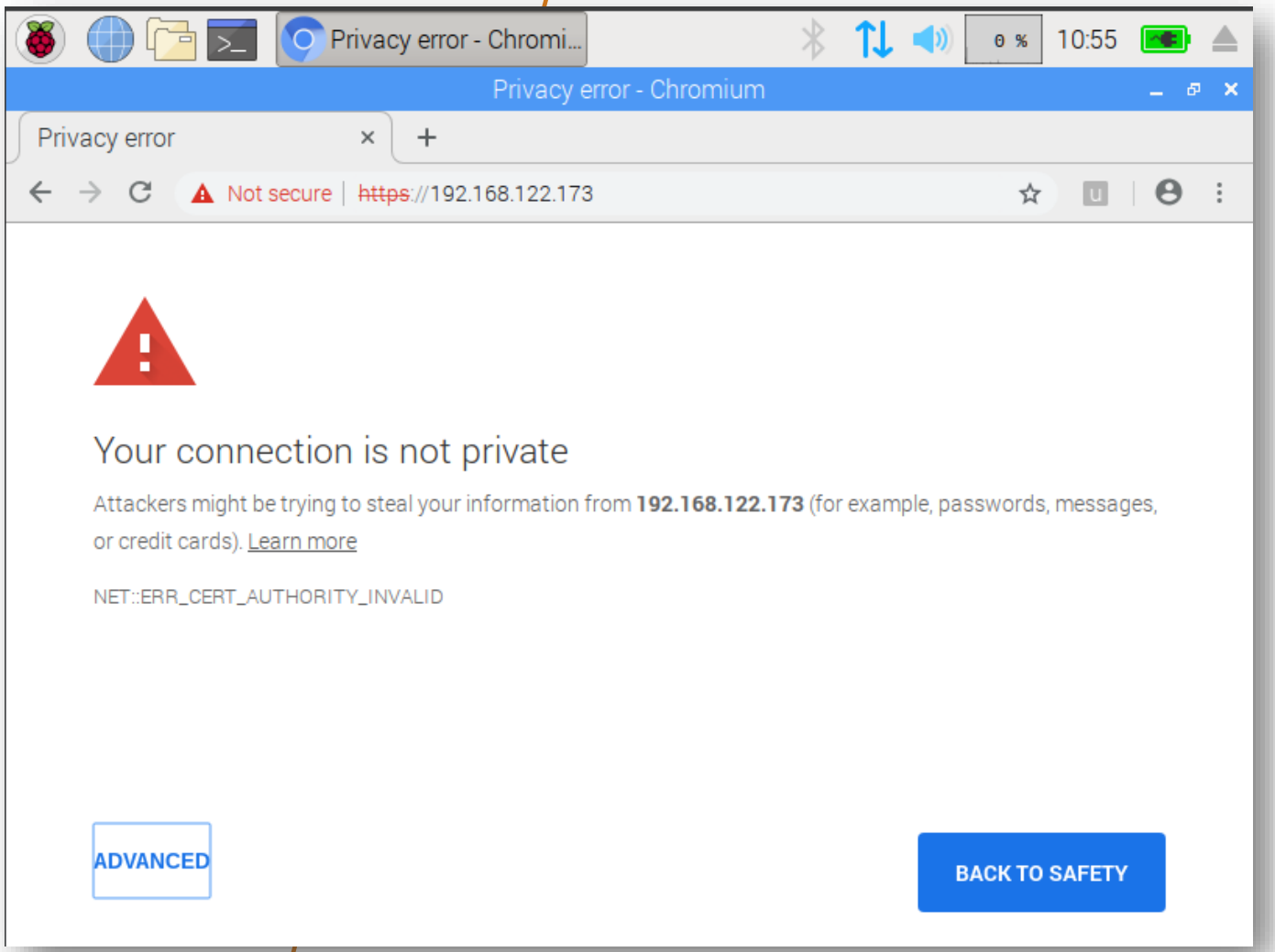




Installing Agent (Endpoint)

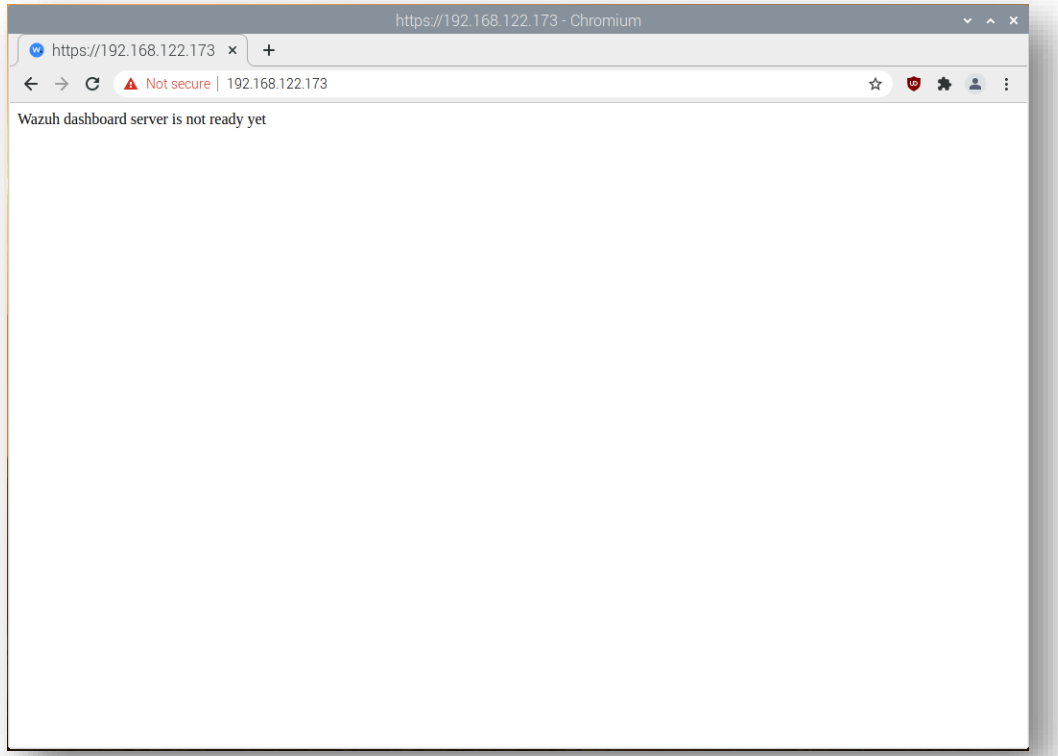
- The **browser** may block the connection to the **web server** due to **security settings** that prevent **unverified** connections.

- Therefore, click on '**ADVANCED**' and then proceed to the link for the IP Server (**it's safe, don't worry** 😉).



Launching Wazuh Server

You may **encounter** the following **screen** when visiting the **Wazuh manager page**. This could happen because, at times, the **Wazuh index does not start correctly**.



Check if the **indexer's** status is **active**; otherwise, you need to restart it. **Check the status using**:

sudo systemctl status wazuh-indexer

```
[wazuh-user@wazuh-server ~]$ sudo systemctl restart wazuh-manager.service
[wazuh-user@wazuh-server ~]$ sudo systemctl status wazuh-manager.indexer
Unit wazuh-manager.indexer.service could not be found.
[wazuh-user@wazuh-server ~]$ sudo systemctl status wazuh-indexer
● wazuh-indexer.service - Wazuh-indexer
     Loaded: loaded (/usr/lib/systemd/system/wazuh-indexer.service; enabled; vendo
r preset: disabled)
     Active: failed (Result: timeout) since Fri 2024-10-04 10:28:04 UTC; 15min ago
       Docs: https://documentation.wazuh.com
    Process: 3710 ExecStart=/usr/share/wazuh-indexer/bin/systemd-entrypoint -p ${P
ID_DIR}/wazuh-indexer.pid --quiet (code=exited, status=143)
   Main PID: 3710 (code=exited, status=143)

Oct 04 10:25:42 wazuh-server systemd-entrypoint[3710]: at org.opensearch.boot...
Oct 04 10:25:42 wazuh-server systemd-entrypoint[3710]: at org.opensearch.boot...
Oct 04 10:25:42 wazuh-server systemd-entrypoint[3710]: at org.opensearch.boot...
Oct 04 10:25:42 wazuh-server systemd-entrypoint[3710]: at org.opensearch.boot...
Oct 04 10:25:42 wazuh-server systemd-entrypoint[3710]: at org.opensearch.boot...
Oct 04 10:25:42 wazuh-server systemd-entrypoint[3710]: at org.opensearch.cli....
Oct 04 10:25:42 wazuh-server systemd-entrypoint[3710]: at org.opensearch.cli....
Oct 04 10:25:42 wazuh-server systemd-entrypoint[3710]: at org.opensearch.cli....
Oct 04 10:25:42 wazuh-server systemd-entrypoint[3710]: at org.opensearch.boot...
Oct 04 10:25:42 wazuh-server systemd-entrypoint[3710]: at org.opensearch.boot...
Hint: Some lines were ellipsized, use -l to show in full.
[wazuh-user@wazuh-server ~]$ sudo systemctl status wazuh-indexer
```

If you see **something** similar to the above **screenshot**, then you need to start the **indexer** on the server using: **sudo systemctl restart wazuh-indexer**

Launching Wazuh Server

Check the **indexer's status again:**

sudo systemctl status wazuh-indexer

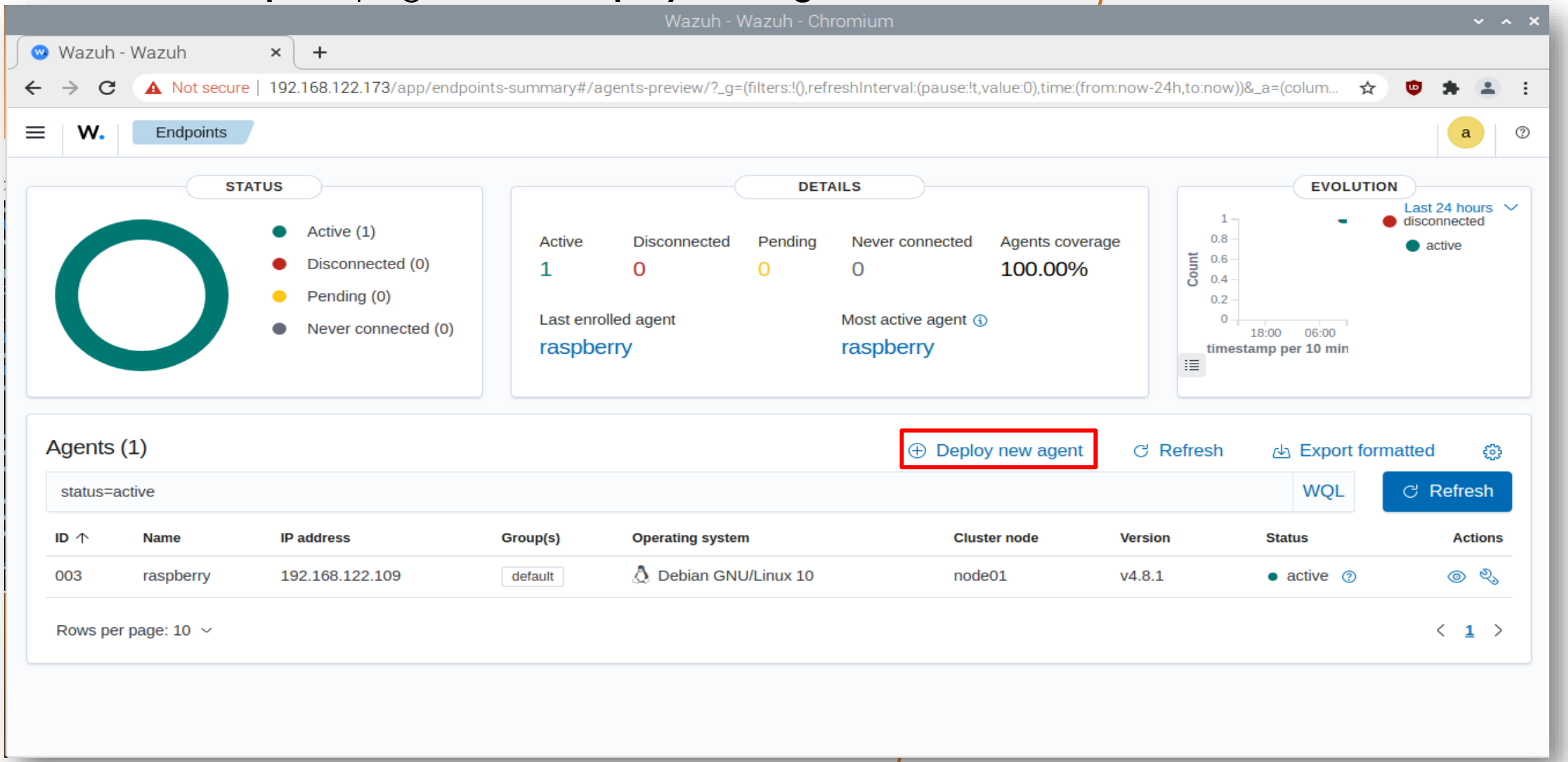
```
Oct 04 10:25:42 wazuh-server systemd-entrypoint[3710]: at org.opensearch.cli....
Oct 04 10:25:42 wazuh-server systemd-entrypoint[3710]: at org.opensearch.boot...
Oct 04 10:25:42 wazuh-server systemd-entrypoint[3710]: at org.opensearch.boot...
Hint: Some lines were ellipsized, use -l to show in full.
[wazuh-user@wazuh-server ~]$ sudo systemctl start wazuh-indexer
[wazuh-user@wazuh-server ~]$ sudo systemctl status wazuh-indexer
● wazuh-indexer.service - Wazuh-indexer
   Loaded: loaded (/usr/lib/systemd/system/wazuh-indexer.service; enabled; vendo
r preset: disabled)
   Active: active (running) since Fri 2024-10-04 10:49:39 UTC; 17s ago
     Docs: https://documentation.wazuh.com
 Main PID: 20779 (java)
   CGroup: /system.slice/wazuh-indexer.service
           └─20779 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopens...

Oct 04 10:49:04 wazuh-server systemd-entrypoint[20779]: WARNING: A terminally...
Oct 04 10:49:04 wazuh-server systemd-entrypoint[20779]: WARNING: System::setS...
Oct 04 10:49:04 wazuh-server systemd-entrypoint[20779]: WARNING: Please consi...
Oct 04 10:49:04 wazuh-server systemd-entrypoint[20779]: WARNING: System::setS...
Oct 04 10:49:07 wazuh-server systemd-entrypoint[20779]: WARNING: A terminally...
Oct 04 10:49:07 wazuh-server systemd-entrypoint[20779]: WARNING: System::setS...
Oct 04 10:49:07 wazuh-server systemd-entrypoint[20779]: WARNING: Please consi...
Oct 04 10:49:07 wazuh-server systemd-entrypoint[20779]: WARNING: System::setS...
Hint: Some lines were ellipsized, use -l to show in full.
[wazuh-user@wazuh-server ~]$
```

You should now see the status as "**active**." 😊

Installing Agent (Endpoint)

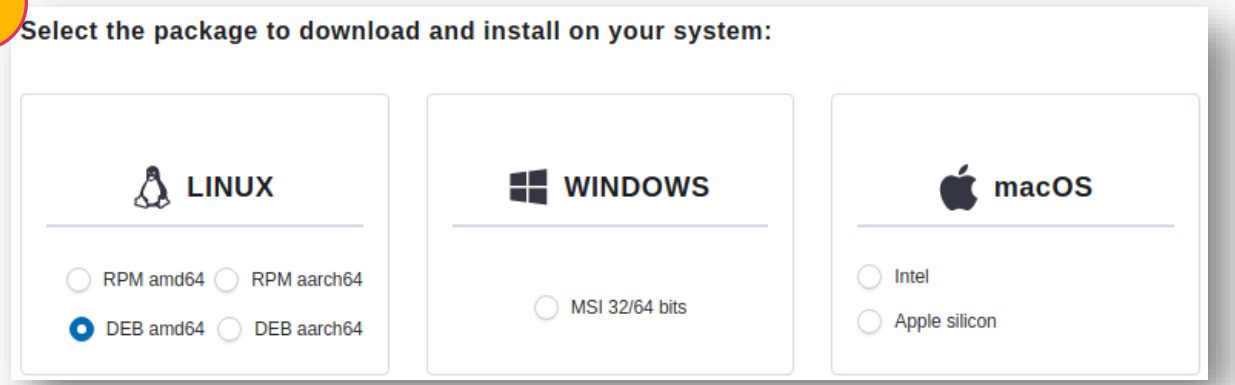
From the **endpoint** page, select **Deploy new agent**



Installing Agent (Endpoint)

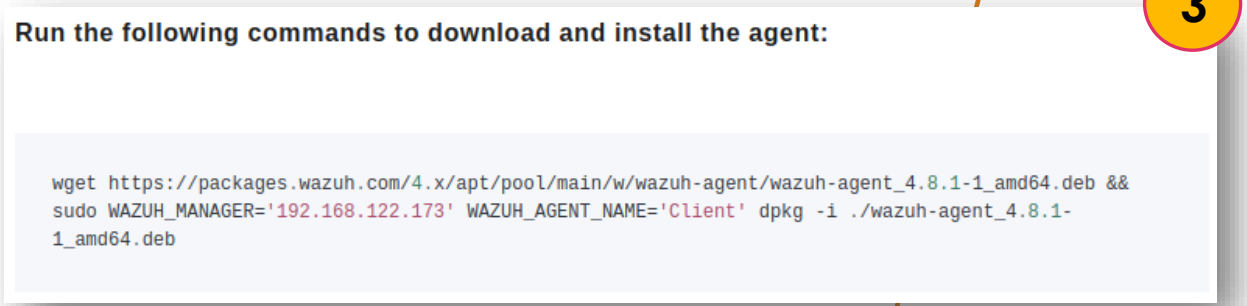
- Select the **OS** of your **agent**, in our case is Linux

1



2

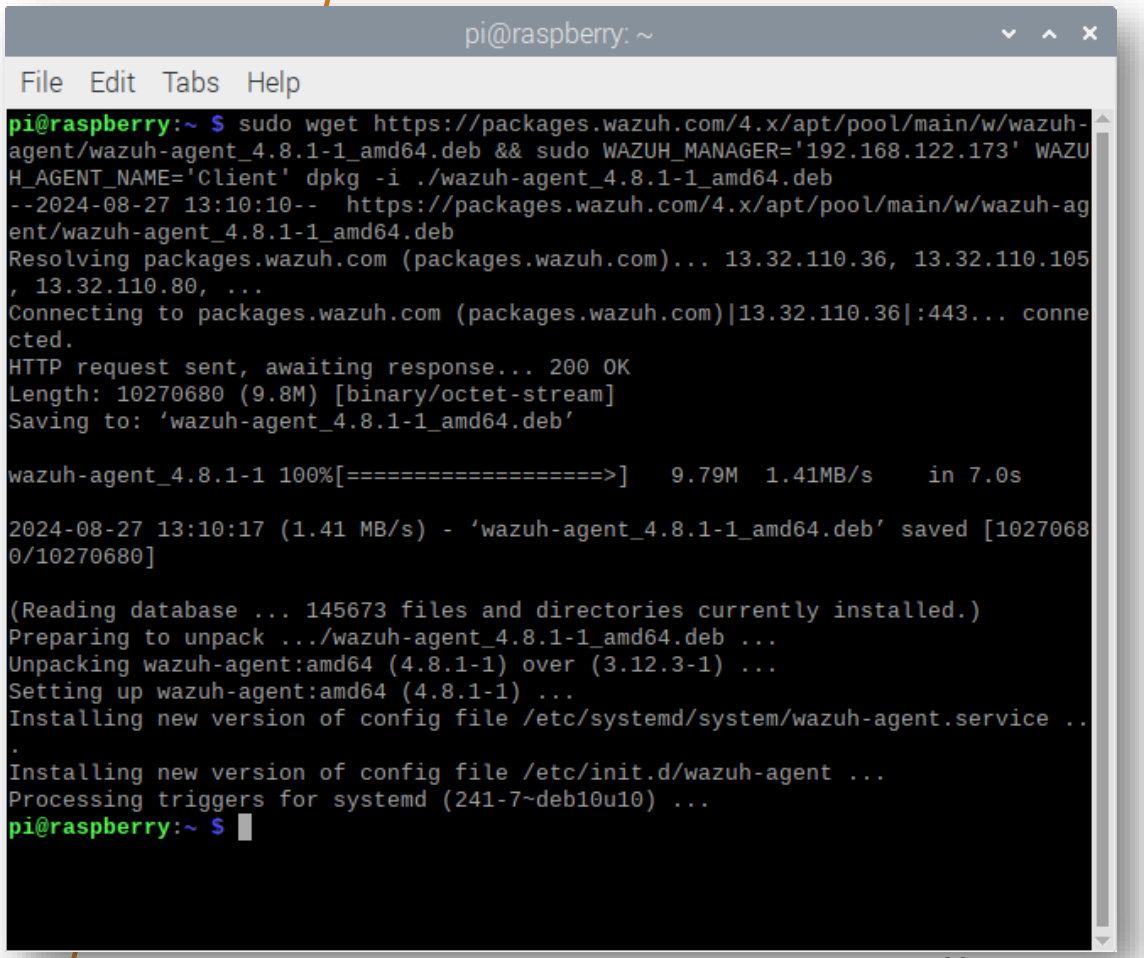
3



Copy and **execute** this command
(**sudo** may be needed)

Installing Agent (Endpoint)

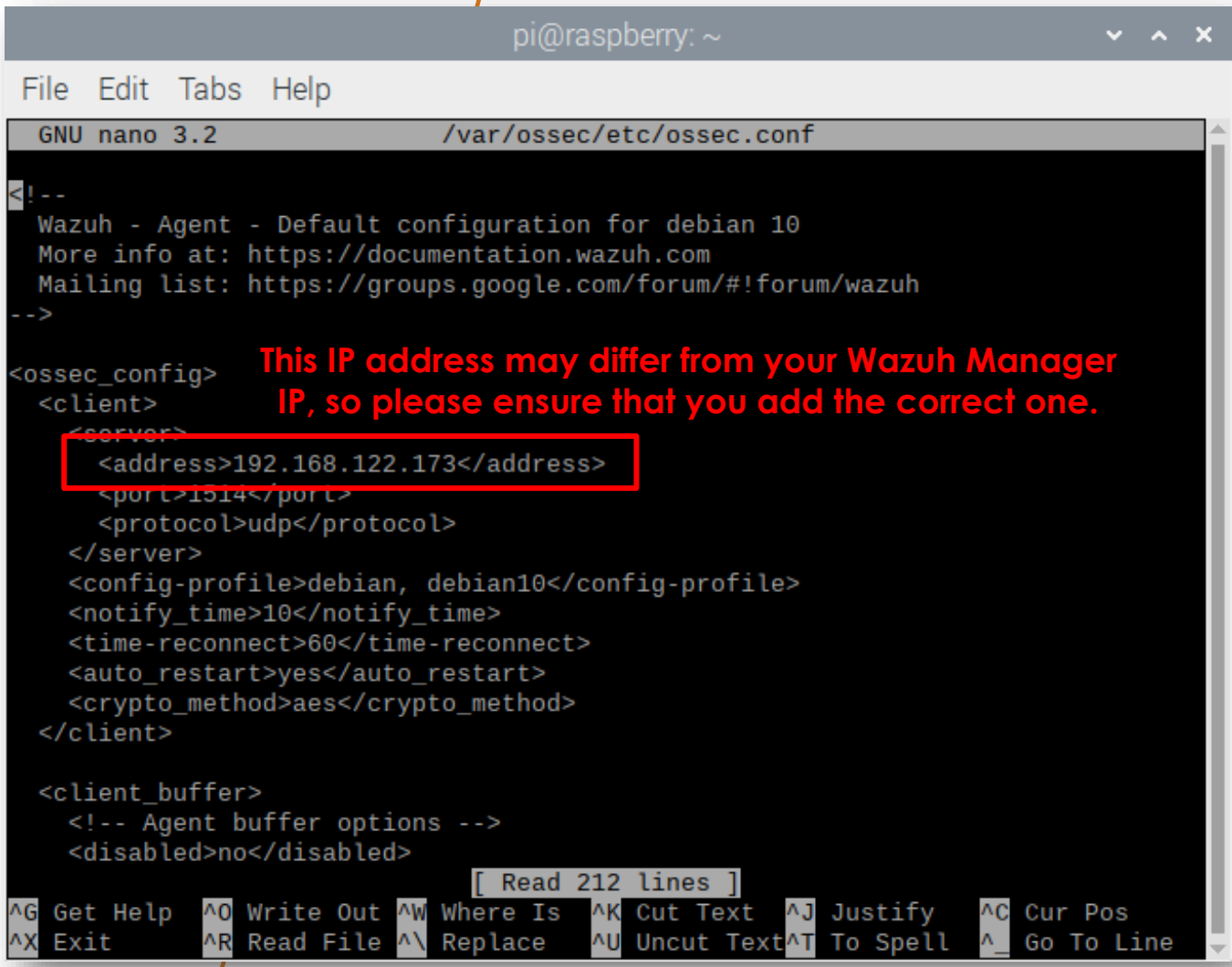
Sudo wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.8.1-1_amd64.deb && sudo WAZUH_MANAGER='192.168.122.173' WAZUH_AGENT_NAME='Client' dpkg -i ./wazuh-agent_4.8.1-1_amd64.deb



Installing Agent (Endpoint)

Update the **server IP** in the **ossec.conf** file on the **agent** side.

Sudo nano /var/ossec/etc/ossec.conf



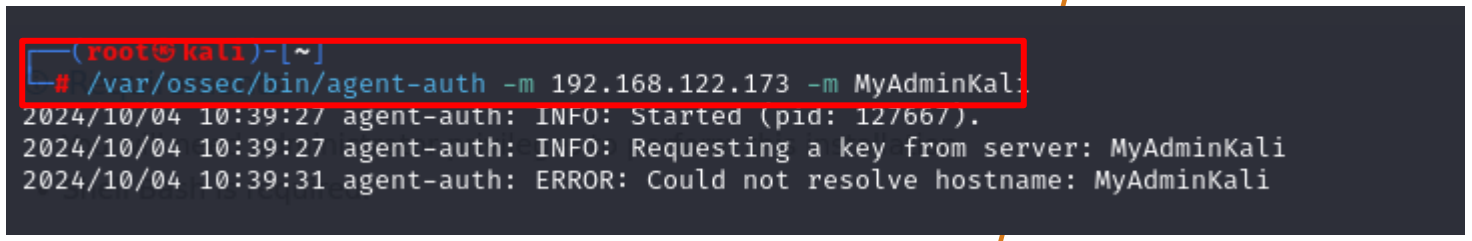
Installing Agent (Endpoint)

Register the **agent** in the **manager** using the following **command**

/var/ossec/bin/agent-auth -m <manager_ip> -A <agent_name>

Replace <**manager_ip**> with the **Wazuh manager's IP address (in our case 192.168.122.173)** and <**agent_name**> with the name of your agent as configured in the manager.

Please note that the agent_name must be unique to prevent duplication, as duplicate agent names will prevent the agent from successfully connecting to the manager.



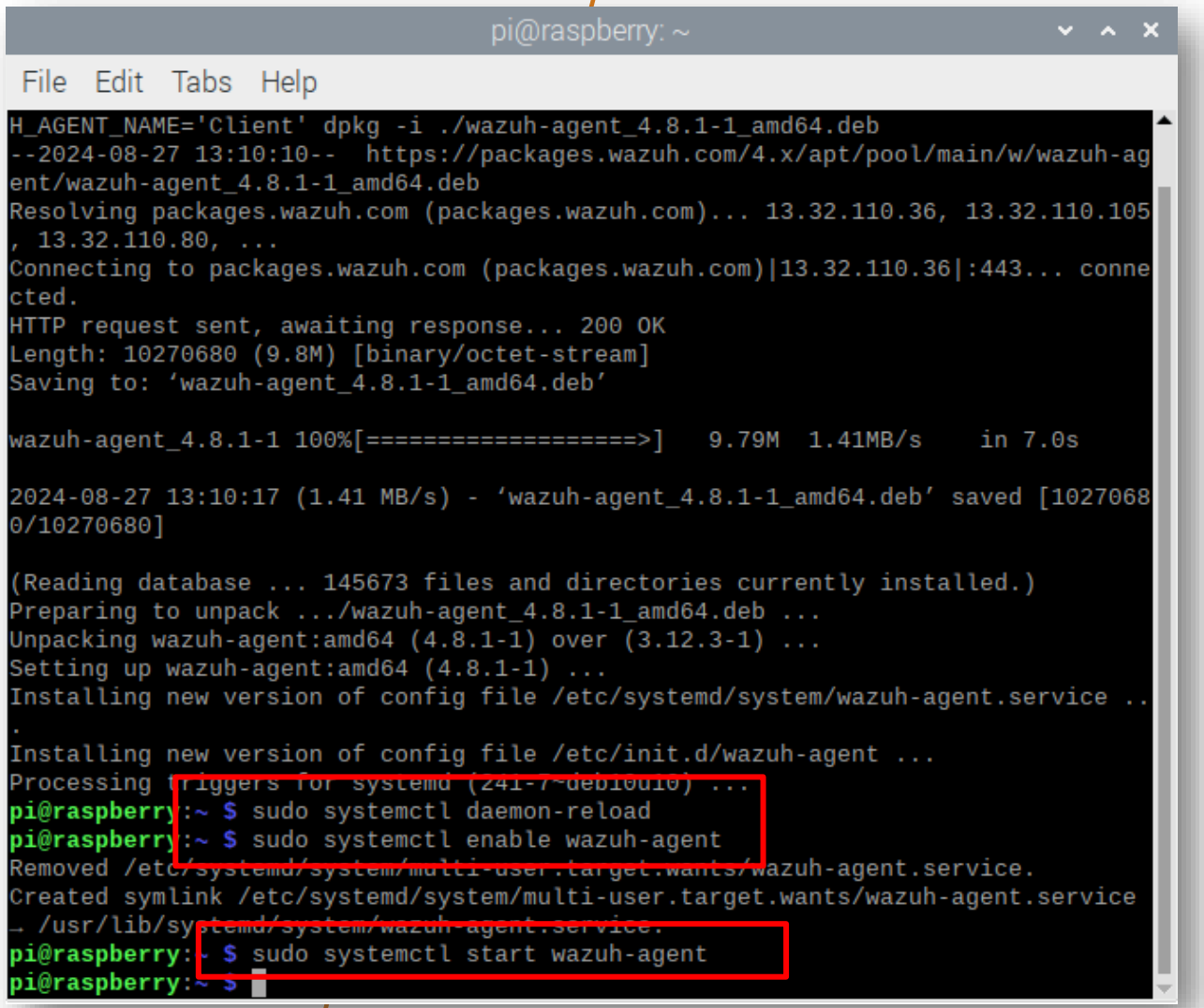
Start the Agent (Endpoint)

Run the agent:

Sudo systemctl daemon-reload

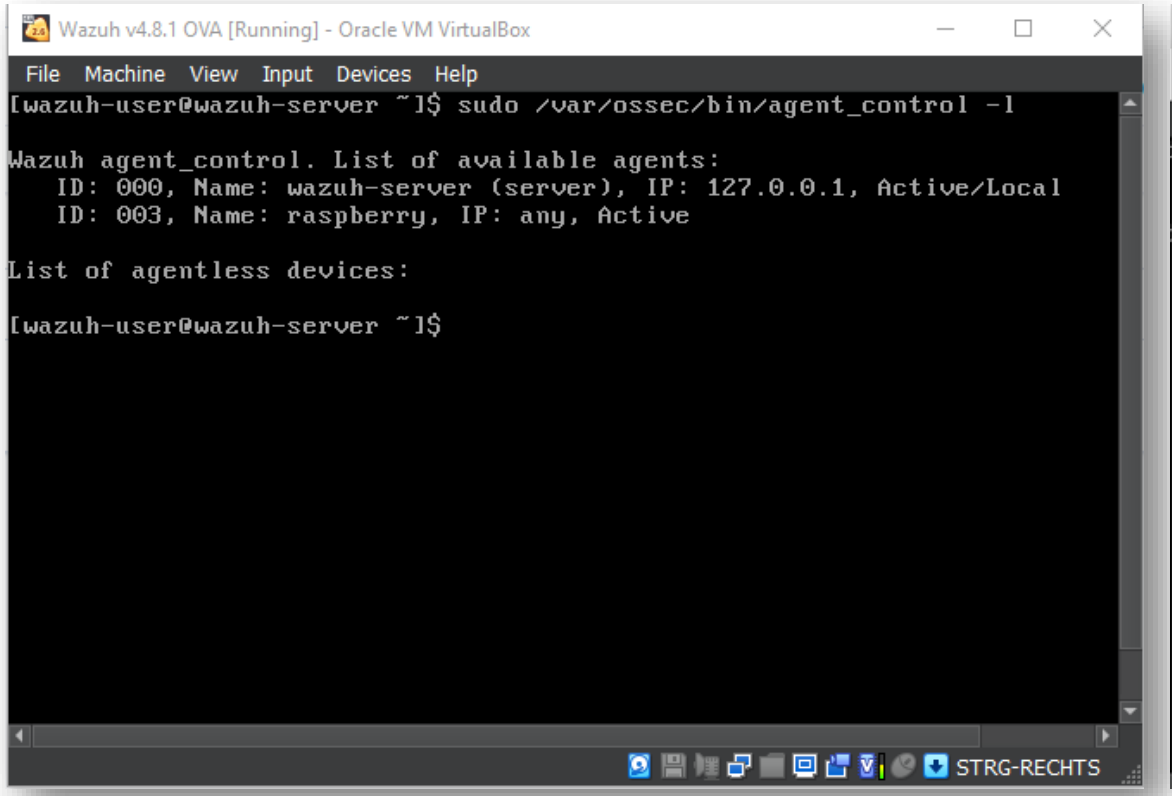
Sudo systemctl enable wazuh-agent

Sudo systemctl start wazuh-agent

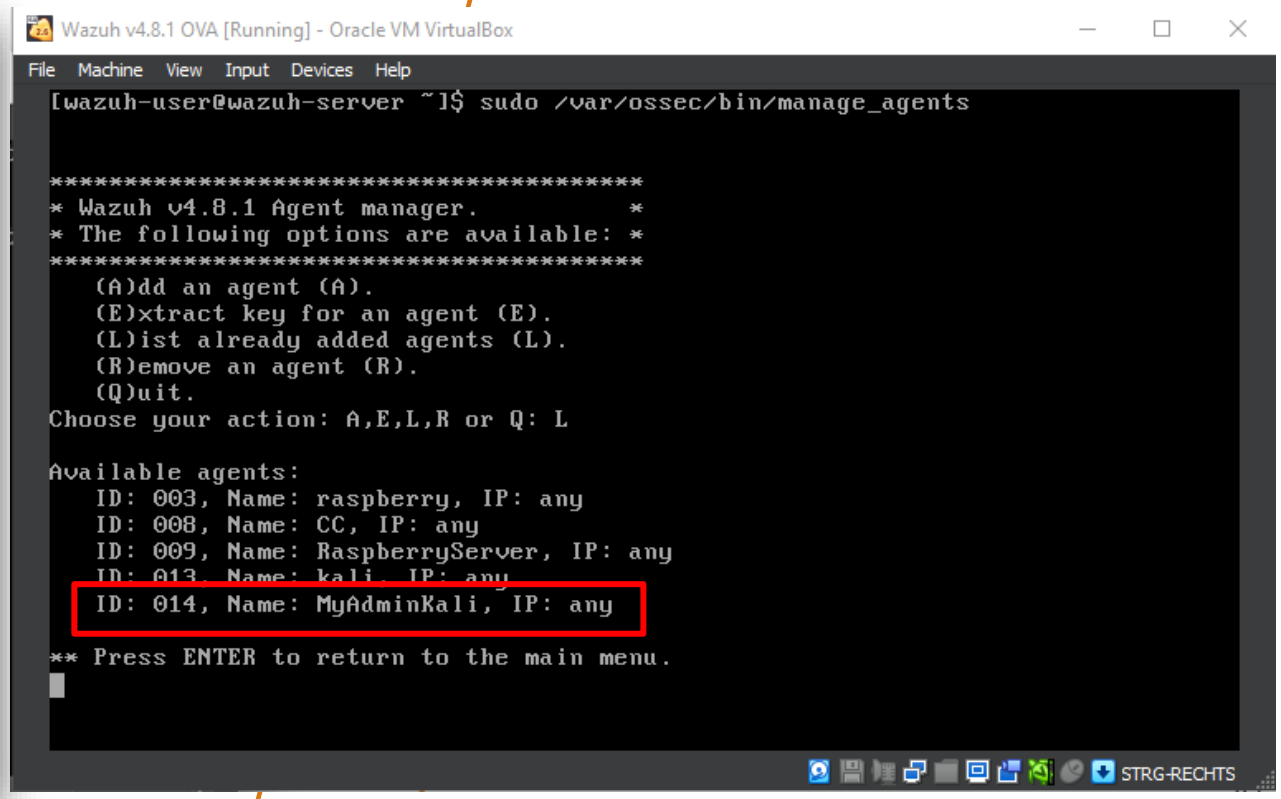


Check Agent List (Endpoint)

Ensure your agent is listed **on the server**.
Listing all agents in the server using:
Sudo /var/ossec/bin/agent_control –l



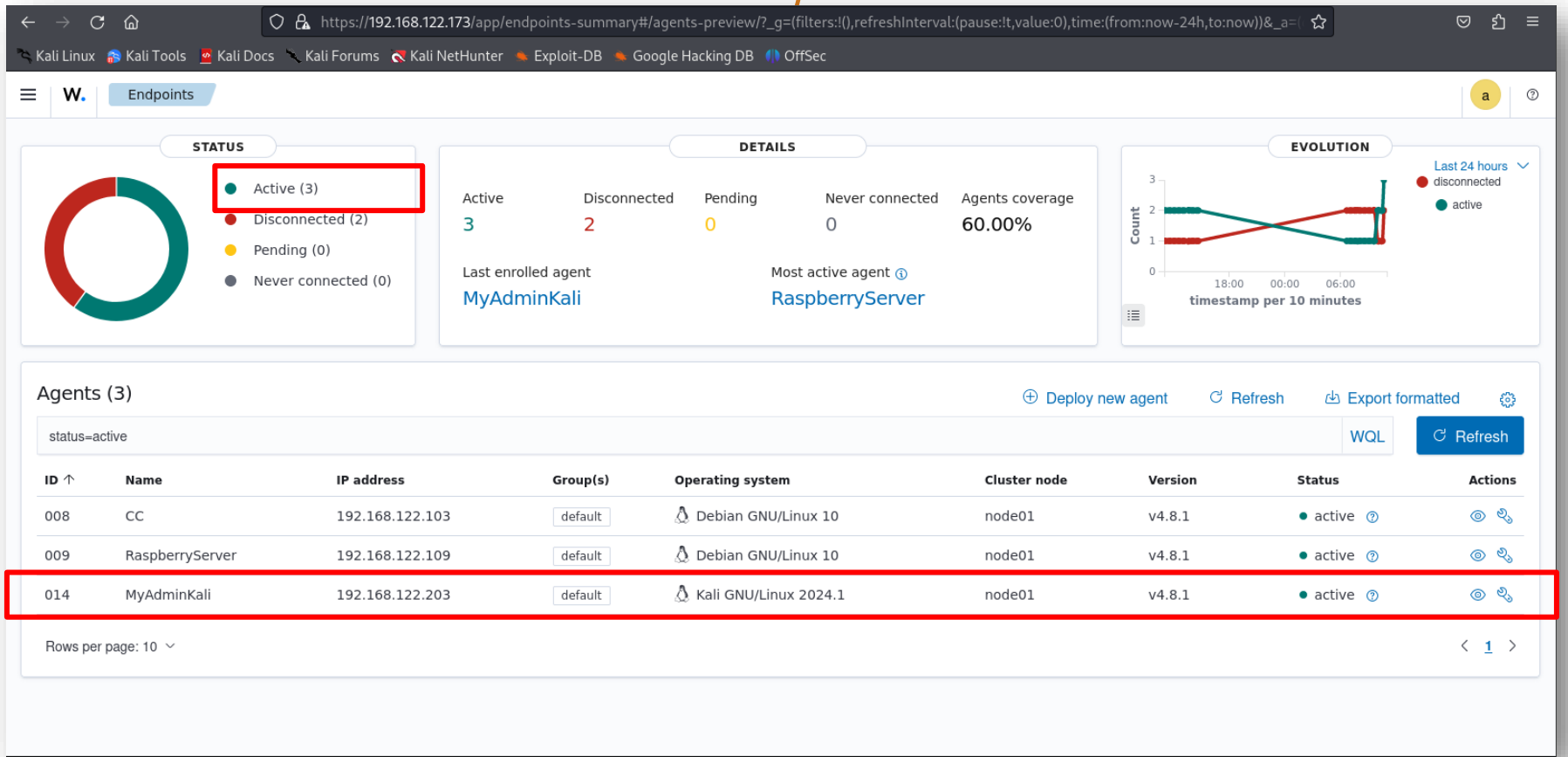
You should now see your recently added agent in the Wazuh server's agent list.



Sudo /var/ossec/bin/manage_agents

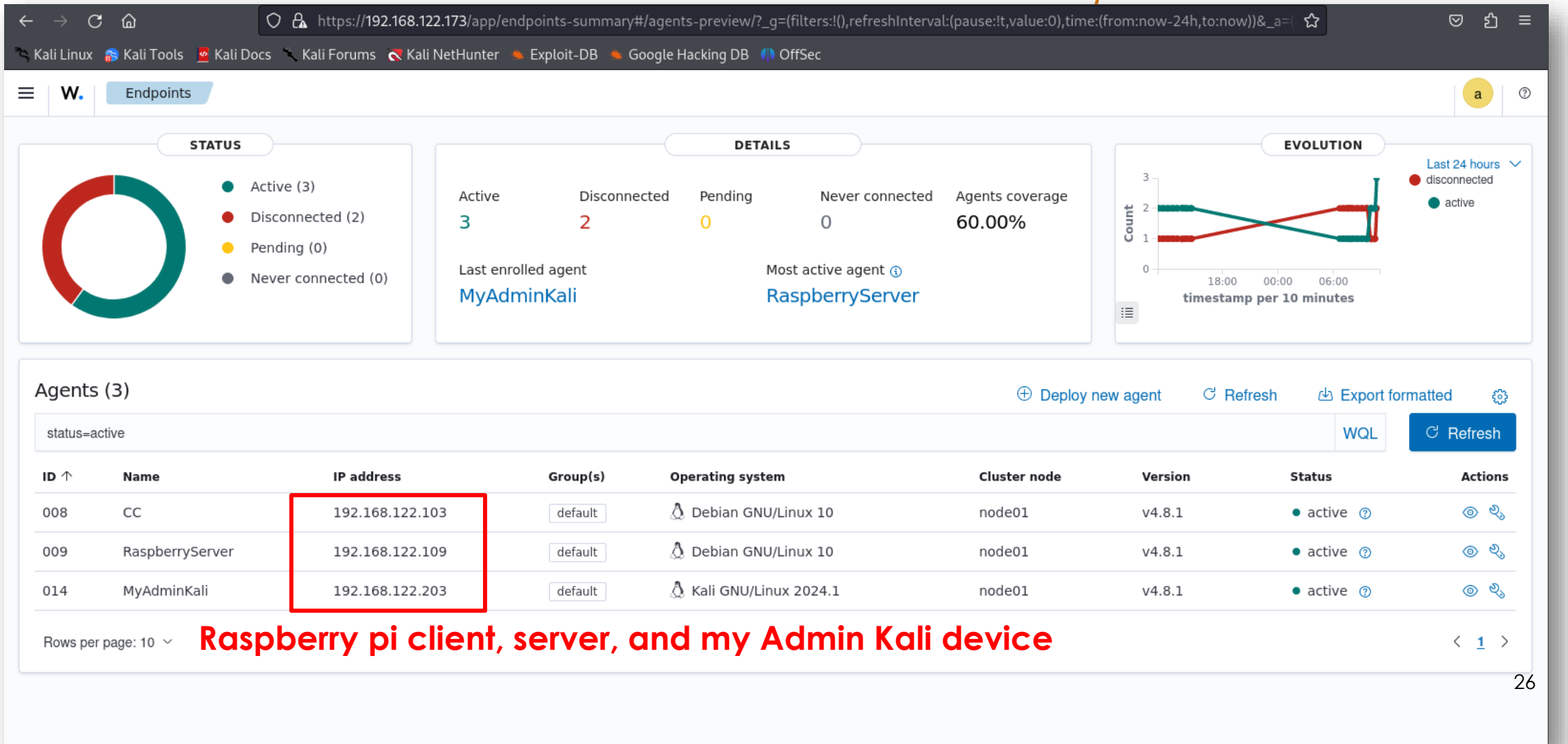
Launching Agent (Endpoint)

- Check the **installed** agent from the **dashboard**.
- **Visit** the **Wazuh server** through the **agent's web browser** using the **Wazuh-IP address**.
- You should now **see** how many **active agents** are actively **running** and **communicating** with the **Wazuh server**.
- In this example, we have **two active agents**.



Launching Agent (Endpoint)

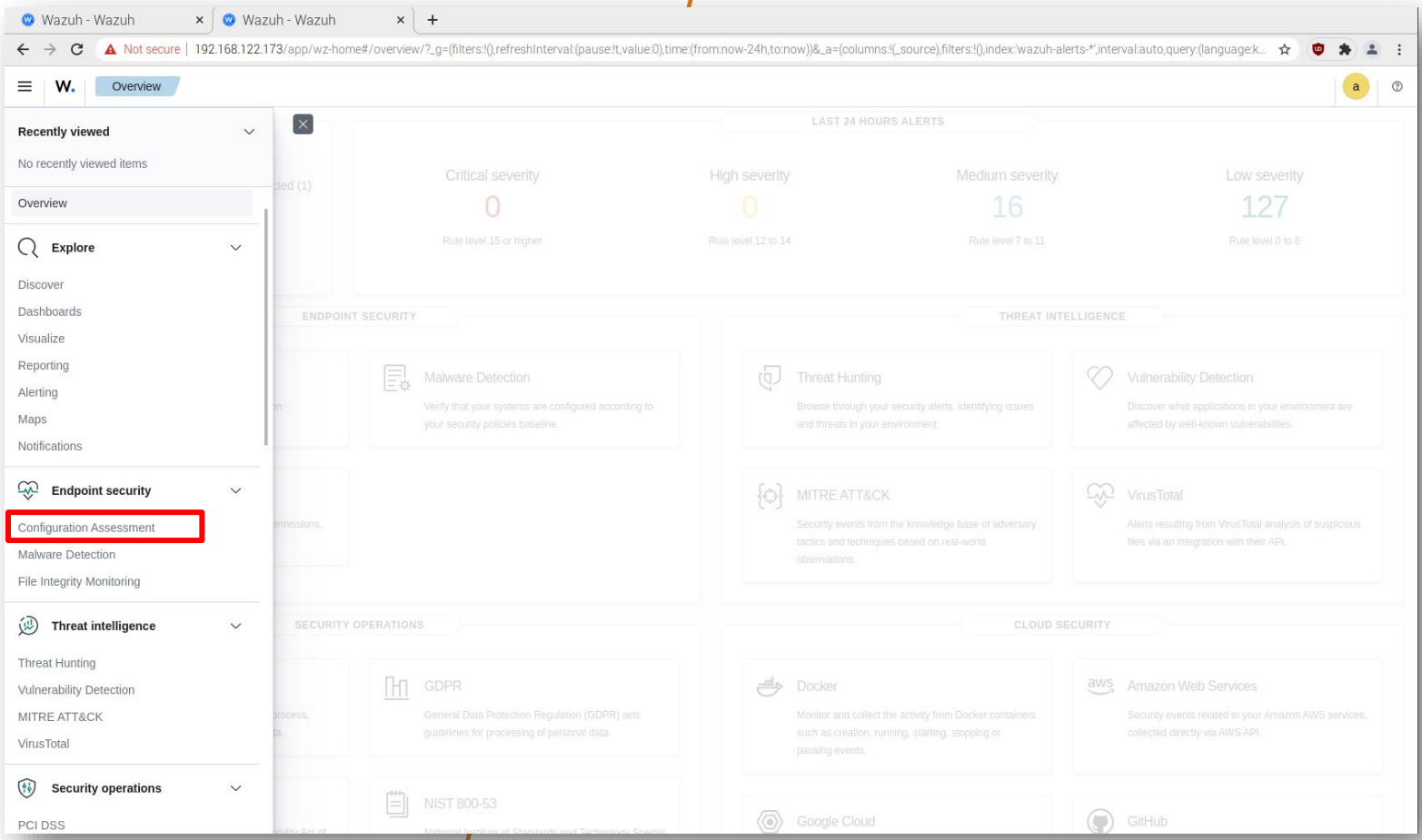
- In this example, we have **three active agents**.



Endpoint Security

Configuration Assessment

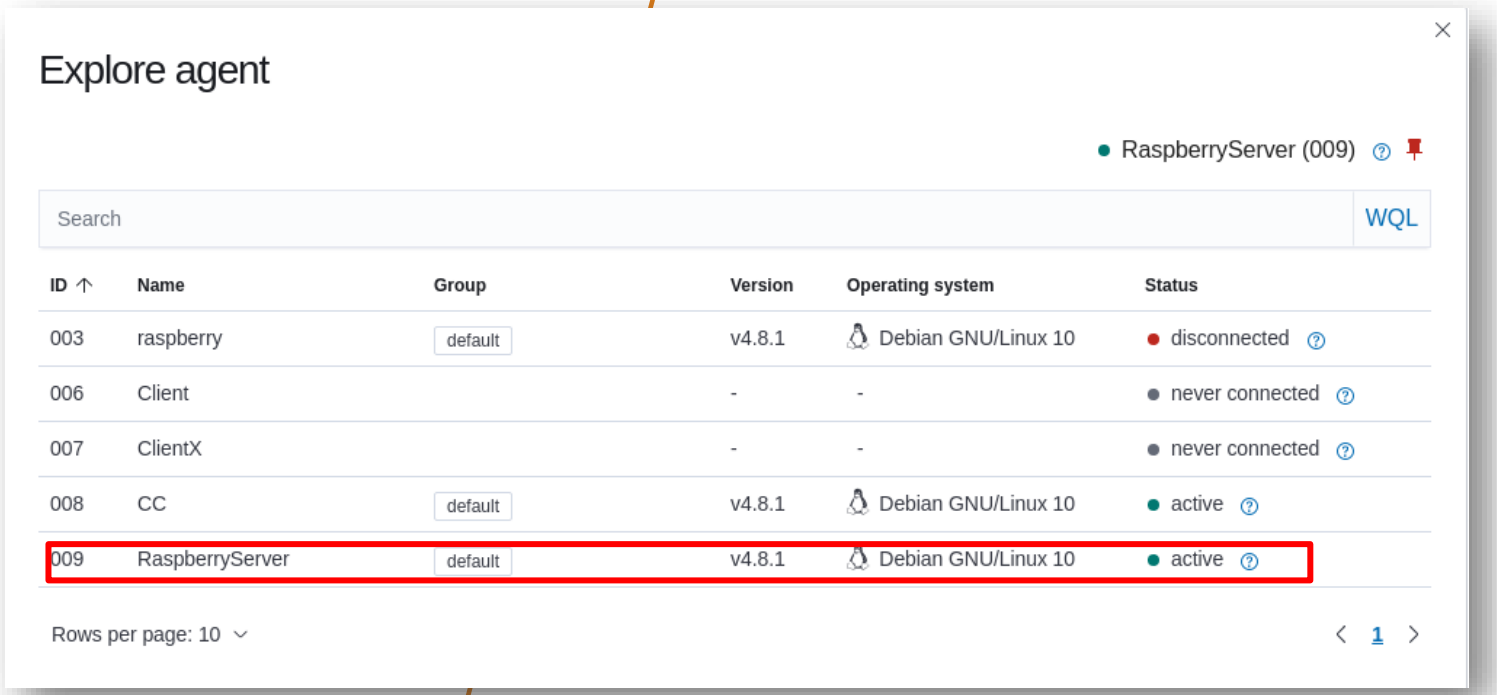
- This process **checks whether** your system **complies** with **established security standards** and **guidelines**.
- It **helps** you **track** the **compliance** status of all your **assets**, **ensuring** that they **follow** the **necessary** security **policies** and **controls**.



Endpoint Security

Configuration Assessment

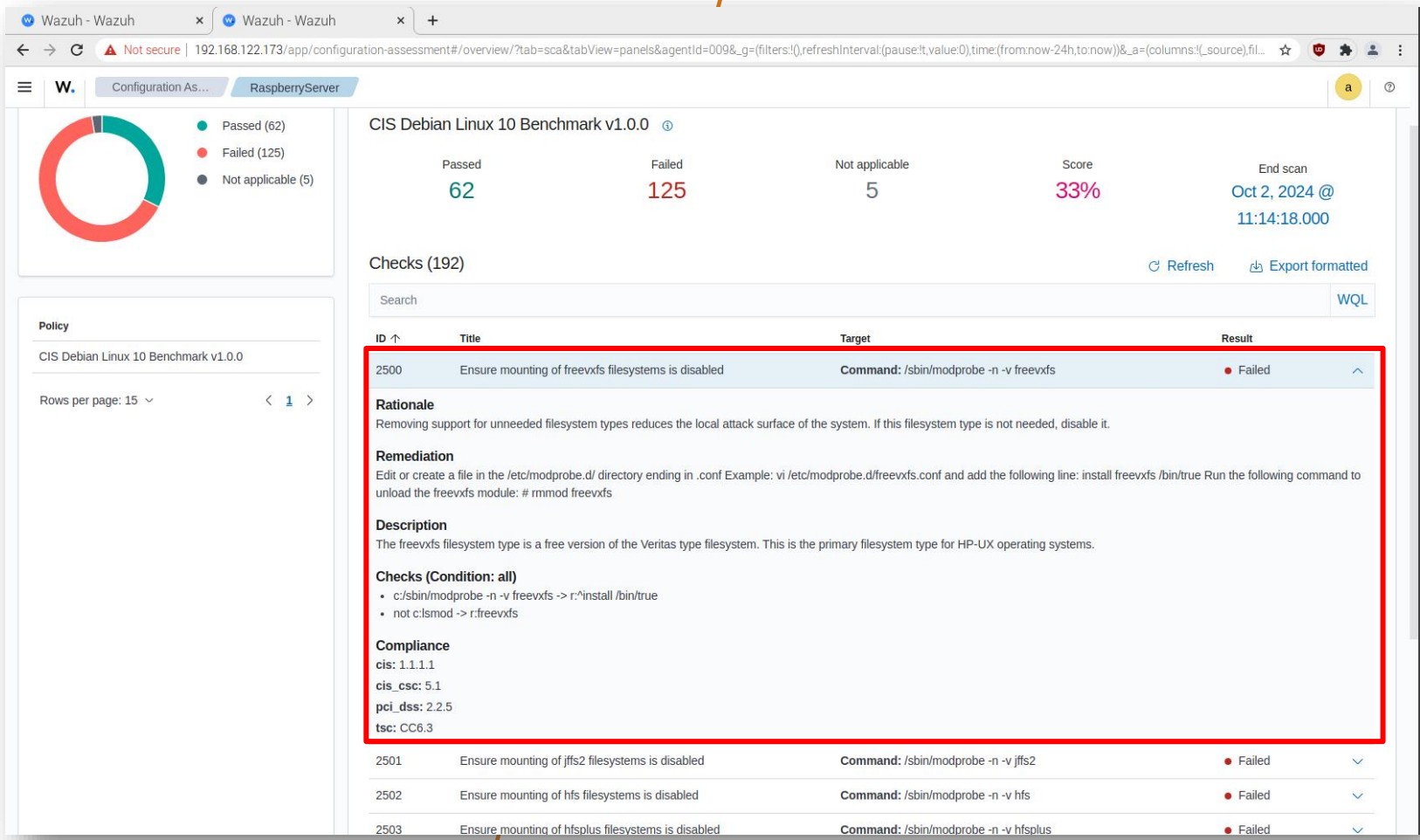
Select the agent you want to check



Endpoint Security

Configuration Assessment

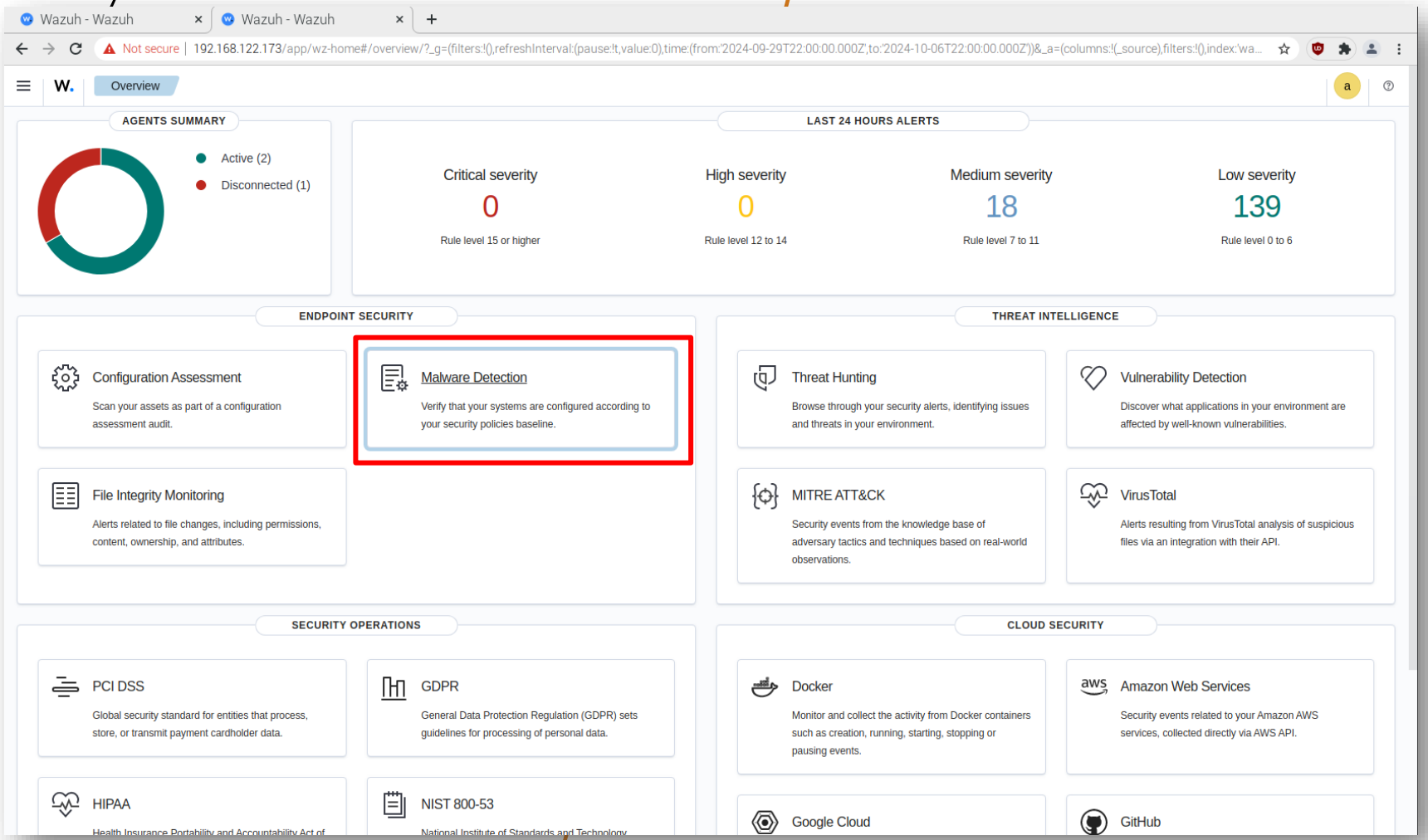
Here's a list of common **security alerts**, their **descriptions**, **recommendations** for **improvement**, and how they **map** to **regulatory compliance.**



Endpoint Security

Malware Detection

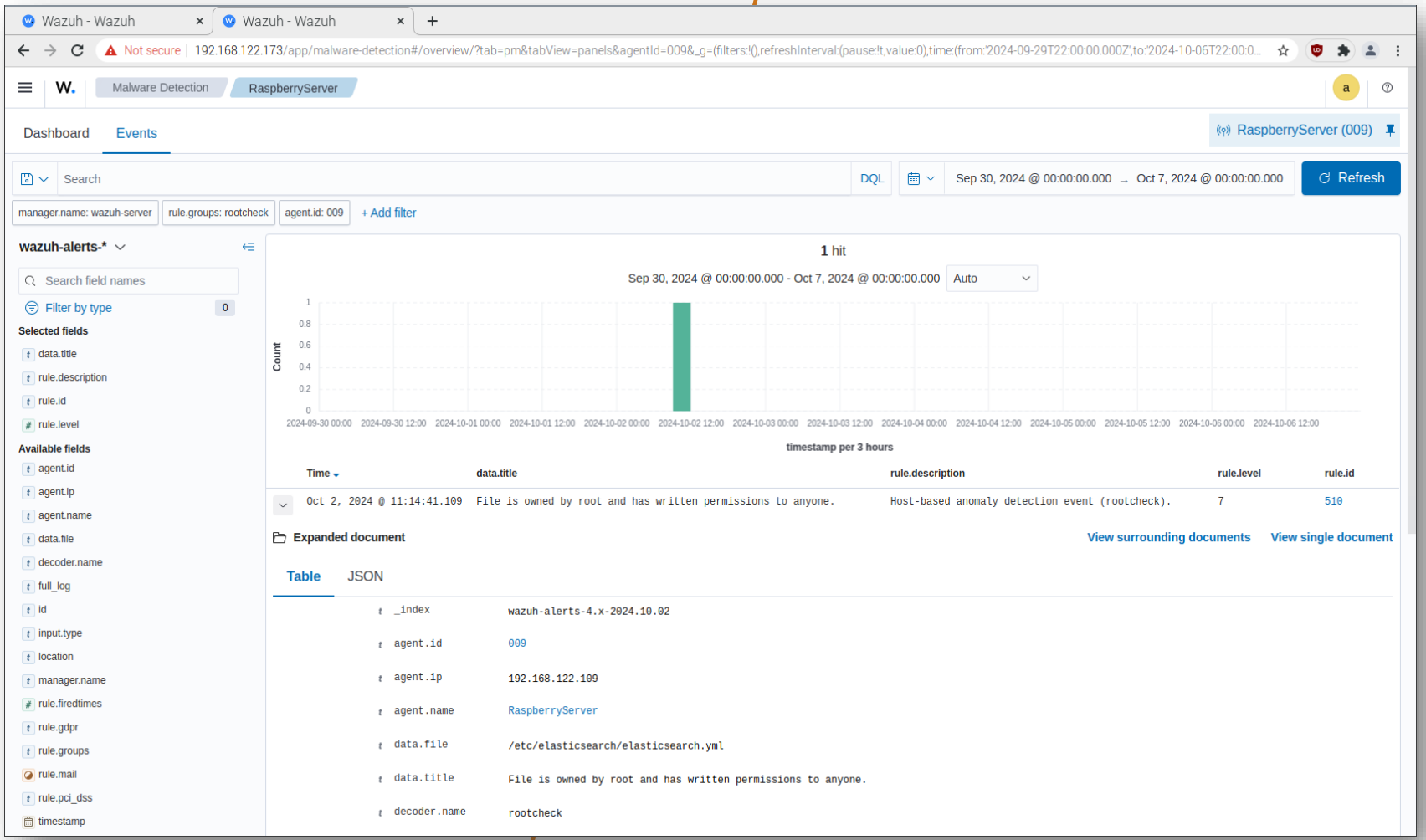
Make an **investigation** to check if any **suspicious files** have been **detected** on any **endpoints**.



Endpoint Security

Malware Detection

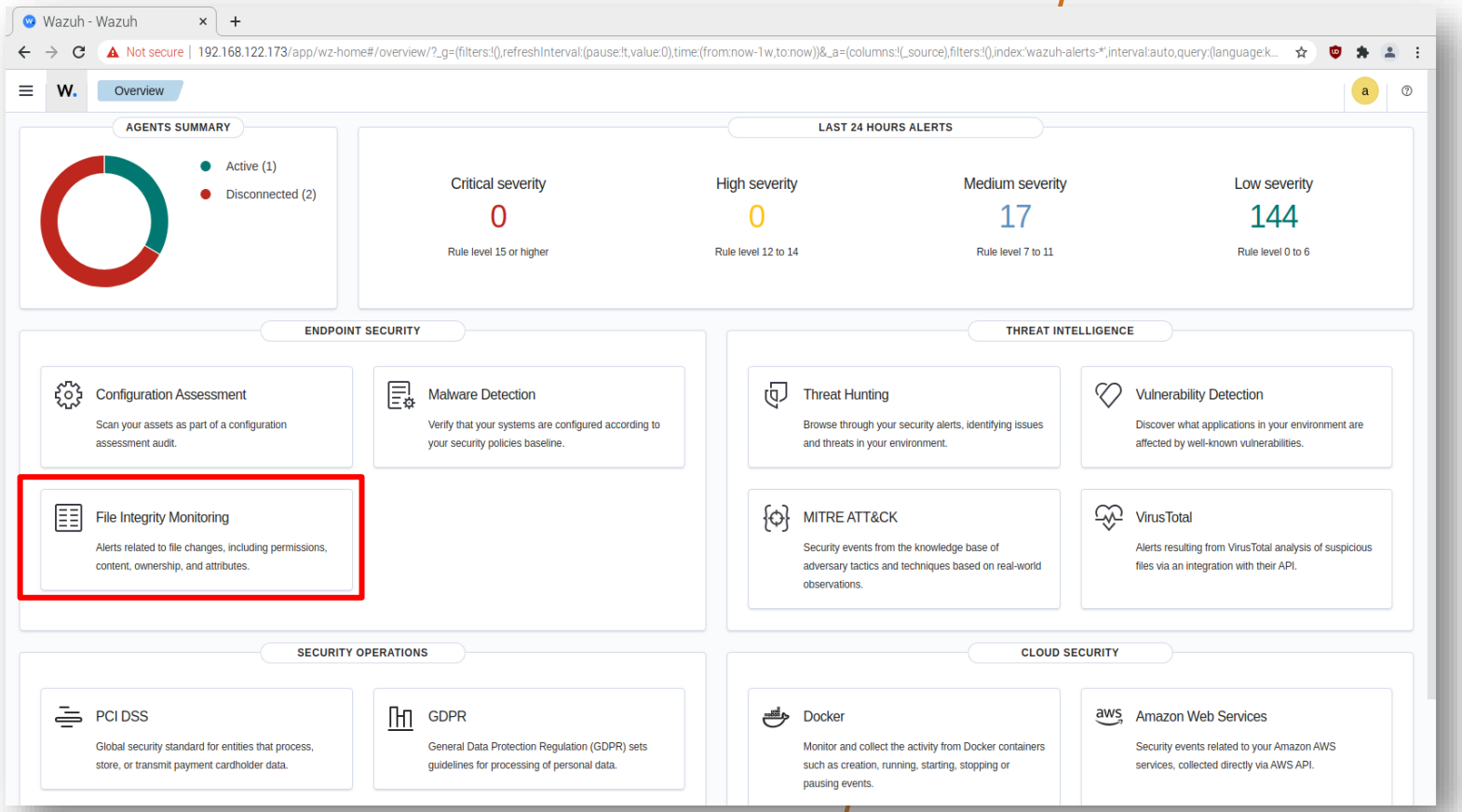
A **suspicious activity** was **detected**, which **referred** to a security risk because a **critical configuration** file (**elasticsearch.yml**) should not be **writable** by all **users**.



Endpoint Security

File Integrity Monitor

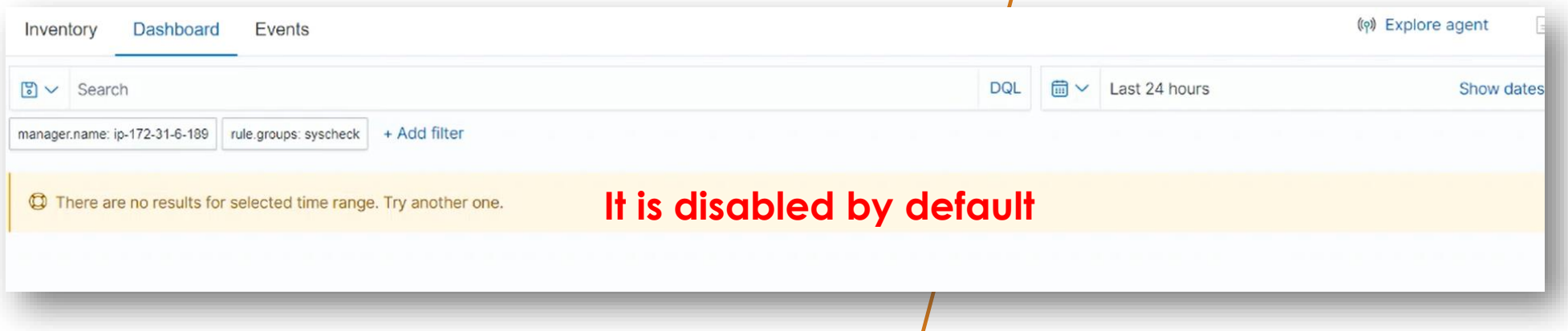
It is **designed** to **monitor** file **systems** and **detect** any **changes** in **content** or **permissions**, or any **related suspicious** activity that could **indicate** a potential **integrity breach**.



Endpoint Security

File Integrity Monitor

It is **designed** to **monitor** file **systems** and **detect** any **changes** in **content** or **permissions**, or any **related suspicious** activity that could **indicate** a potential **integrity breach**.



Lets enable this feature together ☺

Endpoint Security

On the Wazuh-Server Device

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

```
GNU nano 2.9.8                /var/ossec/etc/ossec.conf                Modified


  <!-- Generate alert when new file detected -->
  <alert_new_files>yes</alert_new_files>

  <!-- Don't ignore files that change more than 'frequency' times -->
  <auto_ignore frequency="10" timeframe="3600">no</auto_ignore>

  <!-- Directories to check  (perform all possible verifications) -->
  <directories>/etc,/usr/bin,/usr/sbin</directories>
  <directories>/bin,/sbin,/boot</directories>

  <!-- Files/directories to ignore -->
  <ignore>/etc/mtab</ignore>
  <ignore>/etc/hosts.deny</ignore>
  <ignore>/etc/mail/statistics</ignore>
  <ignore>/etc/random-seed</ignore>
  <ignore>/etc/random.seed</ignore>
  <ignore>/etc/adjtime</ignore>
  <ignore>/etc/httpd/logs</ignore>
  <ignore>/etc/utmpx</ignore>

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

```
GNU nano 2.9.8                /var/ossec/etc/ossec.conf

  <!-- File integrity monitoring -->
  <syscheck>
    <disabled>no</disabled>

    <!-- Frequency that syscheck is executed default every 12 hours -->
    <frequency>43200</frequency>

    <scan_on_start>yes</scan_on_start>

    <!-- Generate alert when new file detected -->
    <alert_new_files>yes</alert_new_files>

    <!-- Don't ignore files that change more than 'frequency' times -->
    <auto_ignore frequency="10" timeframe="3600">no</auto_ignore>

    <!-- Directories to check  (perform all possible verifications) -->
    <directories check_all="yes" whodata="yes">/etc,/usr/bin,/usr/sbin</directo$
    <directories check_all="yes" whodata="yes">/bin,/sbin,/boot</directories>

    <!-- Files/directories to ignore -->

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

Save the changes

Endpoint Security

```
  <!-- File integrity monitoring -->
  <syscheck>
    <disabled>no</disabled>

    <!-- Frequency that syscheck is executed default every 12 hours -->
    <frequency>43200</frequency>

    <scan_on_start>yes</scan_on_start>

    <!-- Generate alert when new file detected -->
    <alert_new_files>yes</alert_new_files>

    <!-- Don't ignore files that change more than 'frequency' times -->
    <auto_ignore frequency="10" timeframe="3600">no</auto_ignore>

    <!-- Directories to check  (perform all possible verifications) -->
    <directories check_all="yes" whodata="yes">/etc,/usr/bin,/usr/sbin</directo$
    <directories check_all="yes" whodata="yes">/bin,/sbin,/boot</directories>

    <!-- Files/directories to ignore -->
```

No errors ☺

```
[wazuh-user@wazuh-server ~]$ sudo systemctl restart wazuh-manager.service
[wazuh-user@wazuh-server ~]$
```

Restart the wazuh-server using
sudo systemctl restart wazuh-manager.service

```
           ├─21768 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr...
           ├─21771 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr...
           ├─21774 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr...
           ├─21816 /var/ossec/bin/wazuh-authd
           ├─21830 /var/ossec/bin/wazuh-db
           ├─21857 /var/ossec/bin/wazuh-execd
           ├─21871 /var/ossec/bin/wazuh-analysisd
           ├─21881 /var/ossec/bin/wazuh-syscheckd
           ├─21901 /var/ossec/bin/wazuh-remoted
           ├─21987 /var/ossec/bin/wazuh-logcollector
           ├─22028 /var/ossec/bin/wazuh-monitord
           └─22075 /var/ossec/bin/wazuh-modulesd

Oct 03 10:30:58 wazuh-server env[21707]: Started wazuh-execd...
Oct 03 10:30:58 wazuh-server env[21707]: Started wazuh-analysisd...
Oct 03 10:30:59 wazuh-server env[21707]: Started wazuh-syscheckd...
Oct 03 10:31:00 wazuh-server env[21707]: Started wazuh-remoted...
Oct 03 10:31:02 wazuh-server env[21707]: Started wazuh-logcollector...
Oct 03 10:31:03 wazuh-server env[21707]: Started wazuh-monitord...
Oct 03 10:31:03 wazuh-server env[21707]: 2024/10/03 10:31:03 wazuh-modulesd:....
Oct 03 10:31:03 wazuh-server env[21707]: 2024/10/03 10:31:03 wazuh-modulesd:....
Oct 03 10:31:04 wazuh-server env[21707]: Started wazuh-modulesd...
Oct 03 10:31:06 wazuh-server env[21707]: Completed.
Hint: Some lines were ellipsized, use -l to show in full.
[wazuh-user@wazuh-server ~]$
```

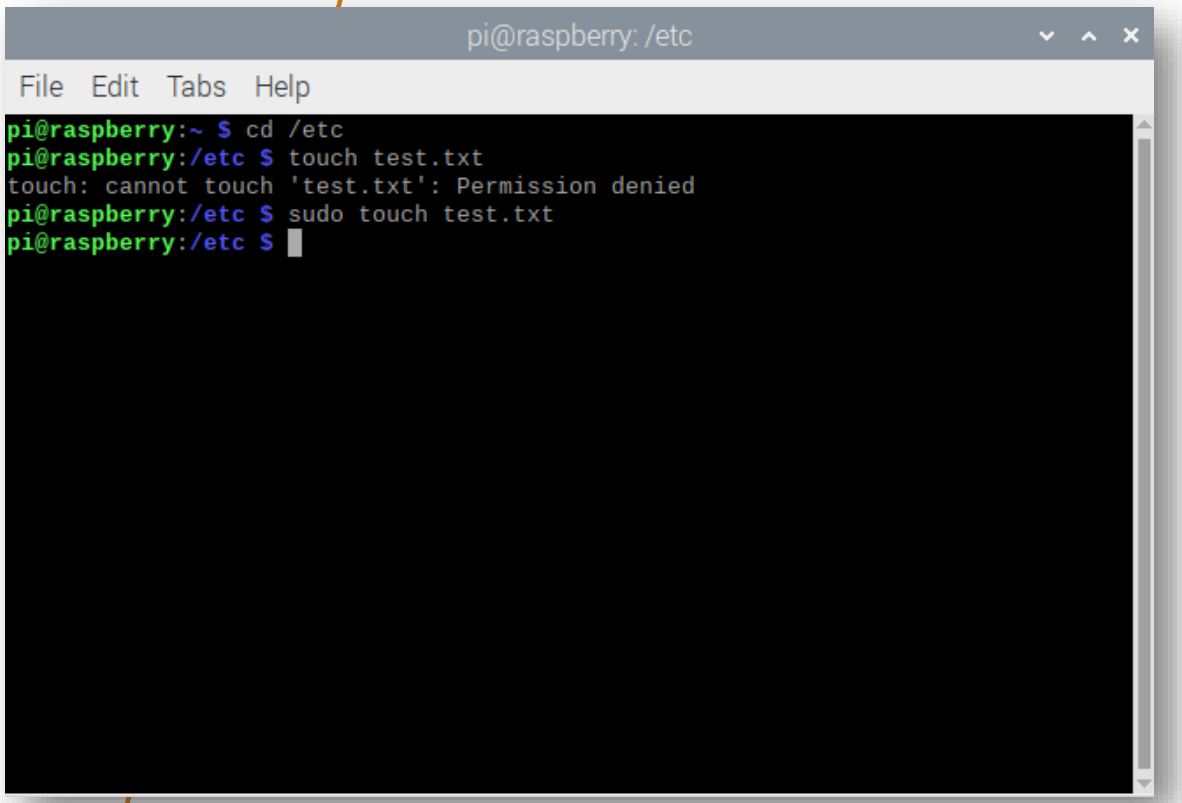
Check the status of the server using
sudo systemctl status wazuh-manager.service

Endpoint Security

Let's create a file named "**test.txt**" in the **`/etc` directory** to see if **Wazuh's File Integrity Monitoring** will detect it.

On the agent side, navigate to the `/etc` directory by typing: **cd /etc**

Then, create the file using the `**touch**` command: **touch test.txt**



Wazuh should now be able to **monitor** for **unauthorized changes** or **file creations** in critical system **directories**.

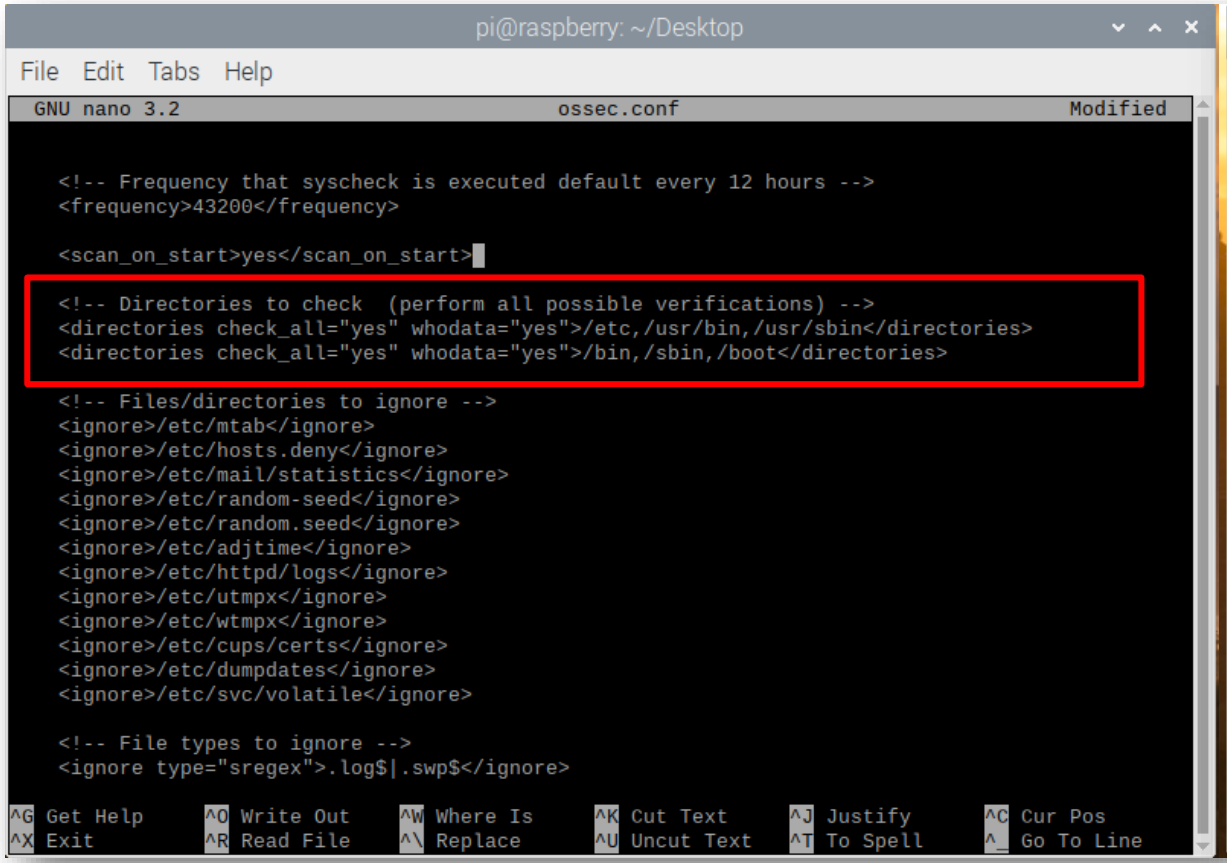
Endpoint Security

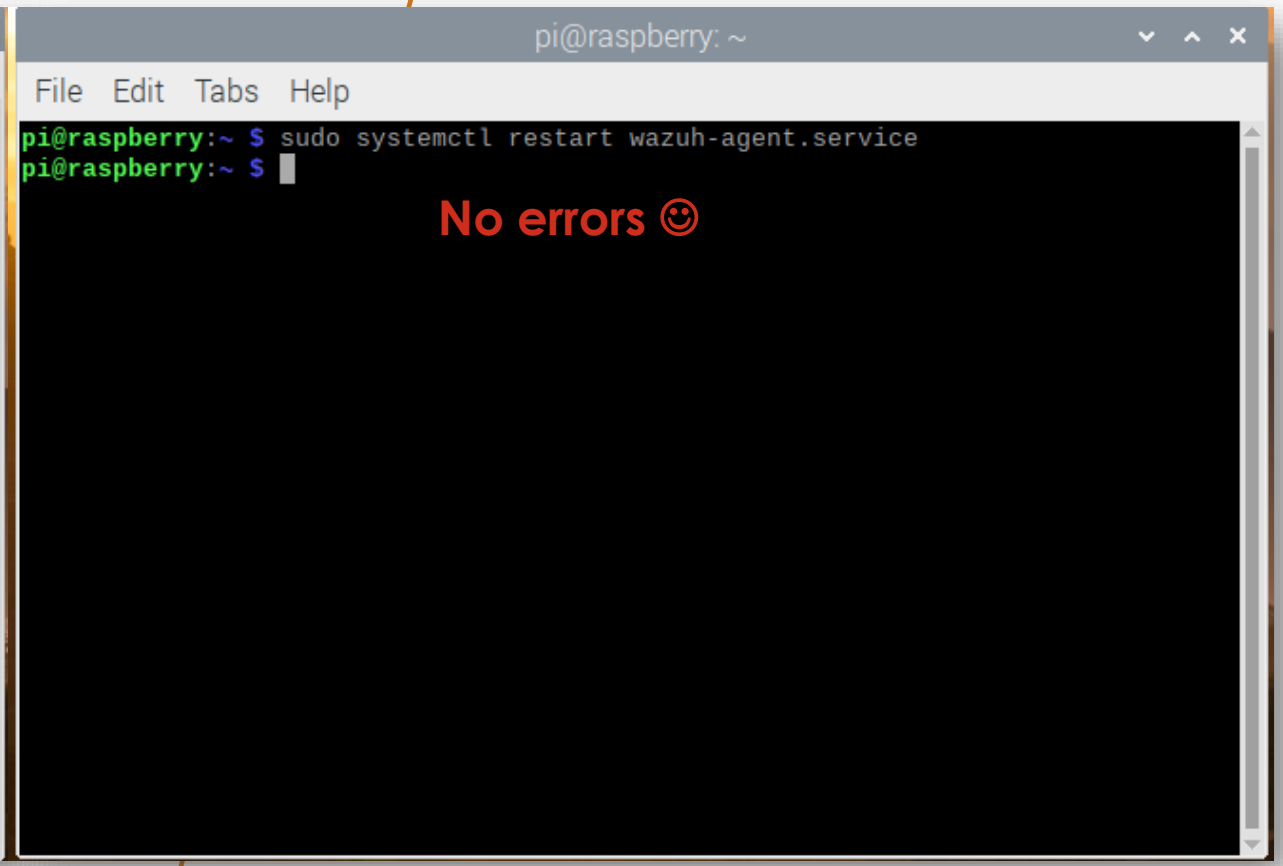
Check the File **Integrity Monitoring** page on the **agent** side; it should be working now.

However, if **no changes** are **detected due to creating the file (text.txt), we** may need to **update the ossec.conf** file on the **agent** to ensure proper **monitoring** and **detection** of file **changes**.

Update the ossec.conf from this path
/var/ossec/etc/ossec.conf

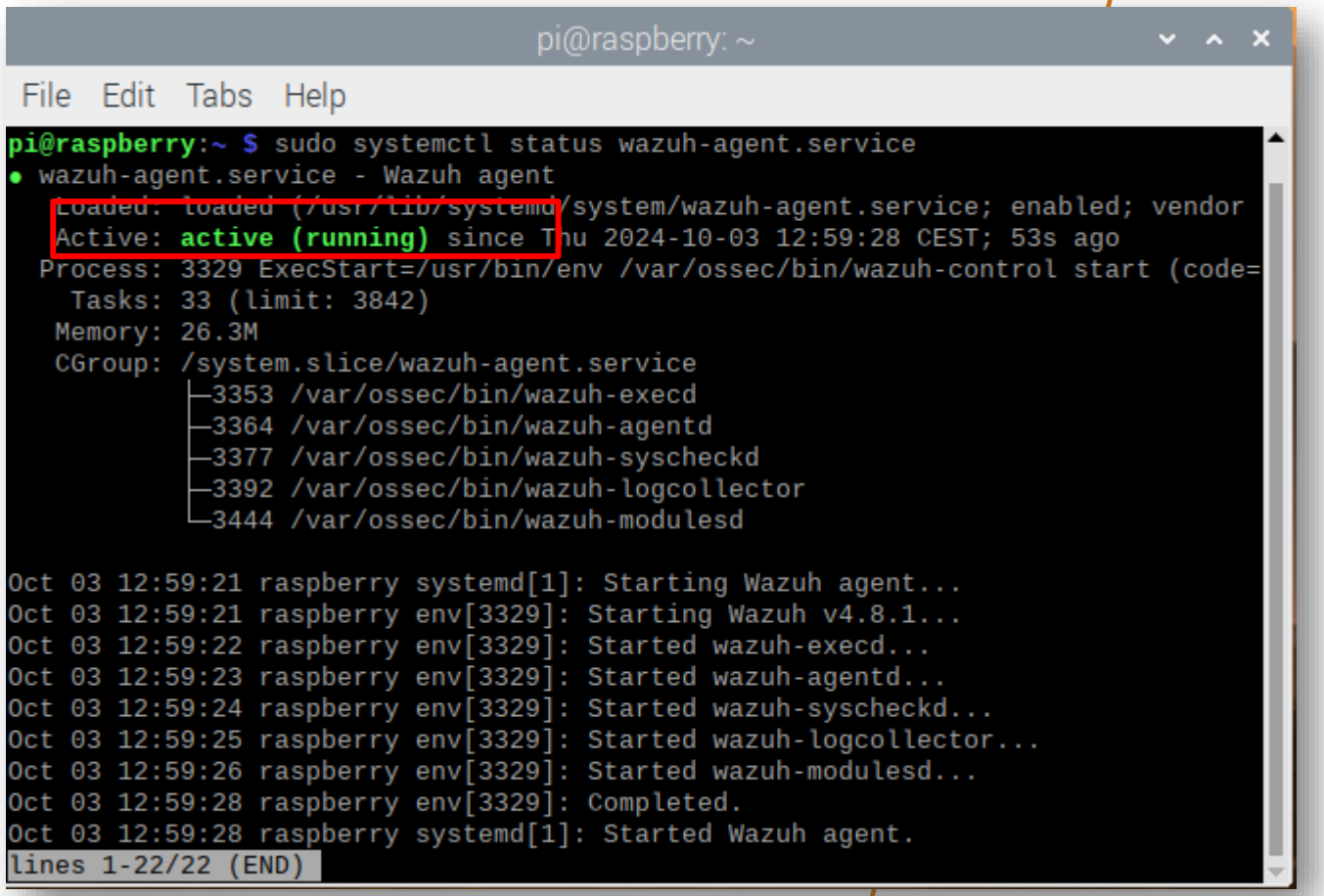
Then restart the agent using the following command:
sudo systemctl restart wazuh-agent.service





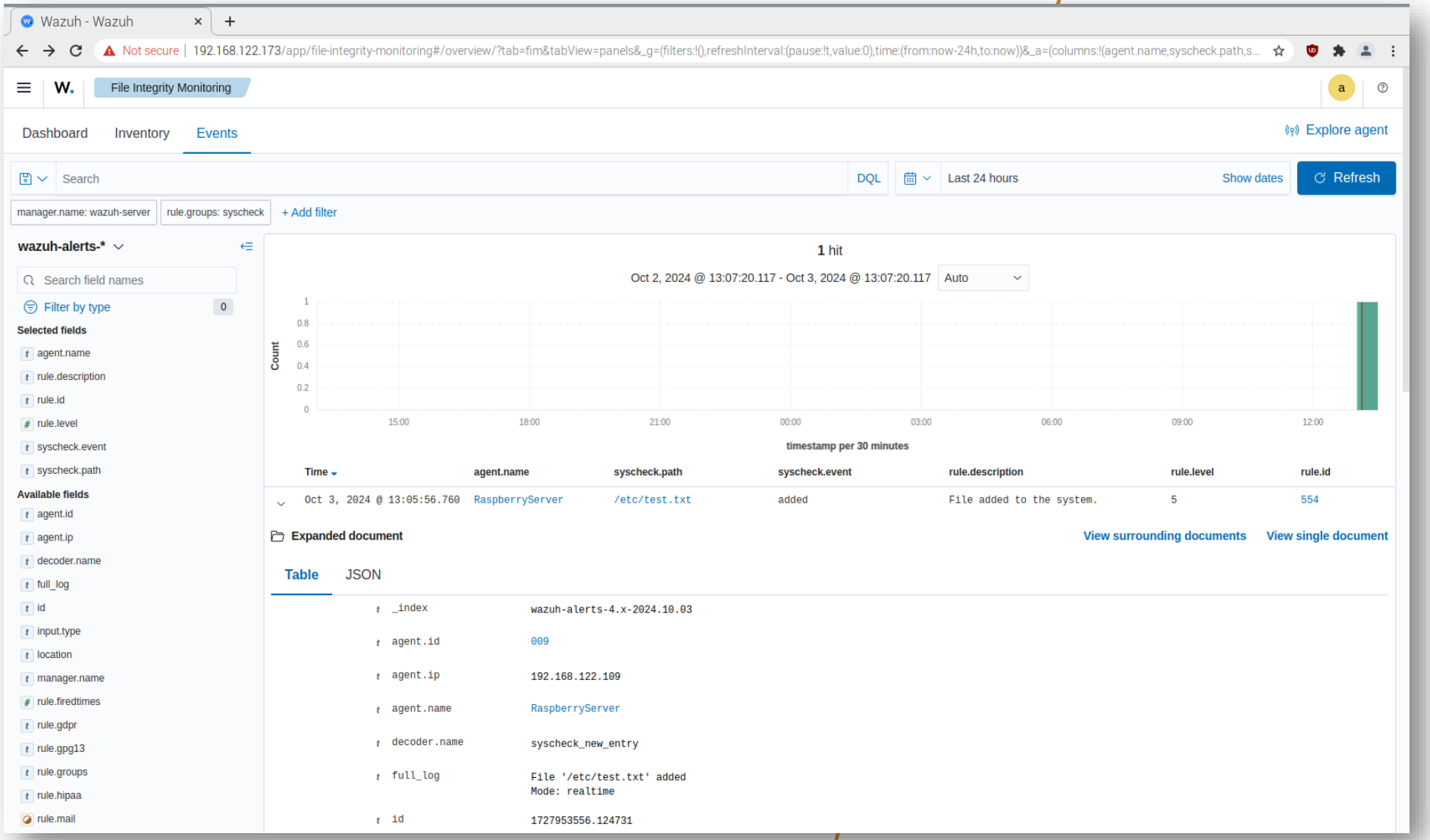
Endpoint Security

Chek the agent status using
Sudo systemctl status wazuh-agent.service



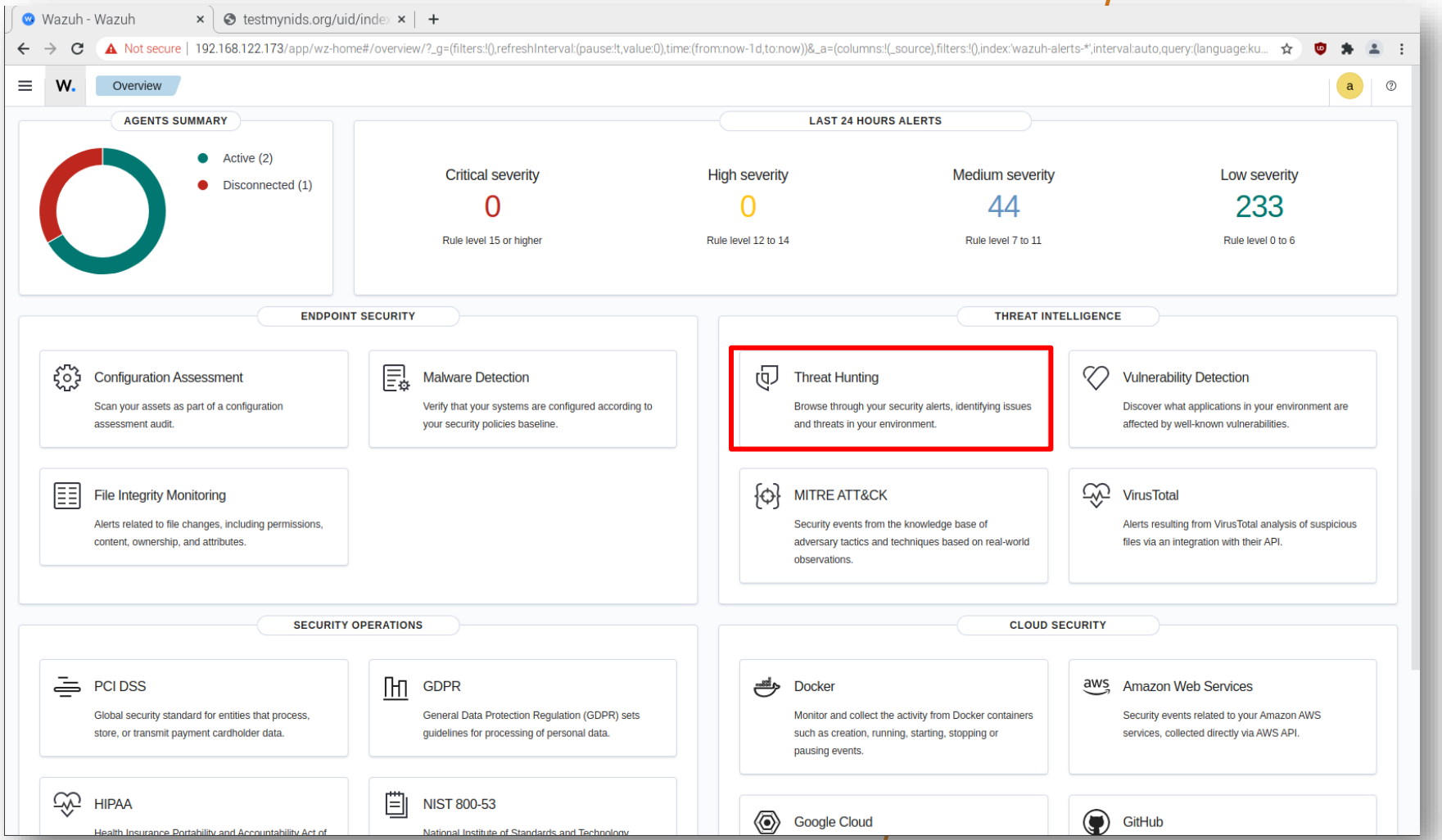
Endpoint Security

Check again the File **Integrity Monitoring** page on the **agent** side



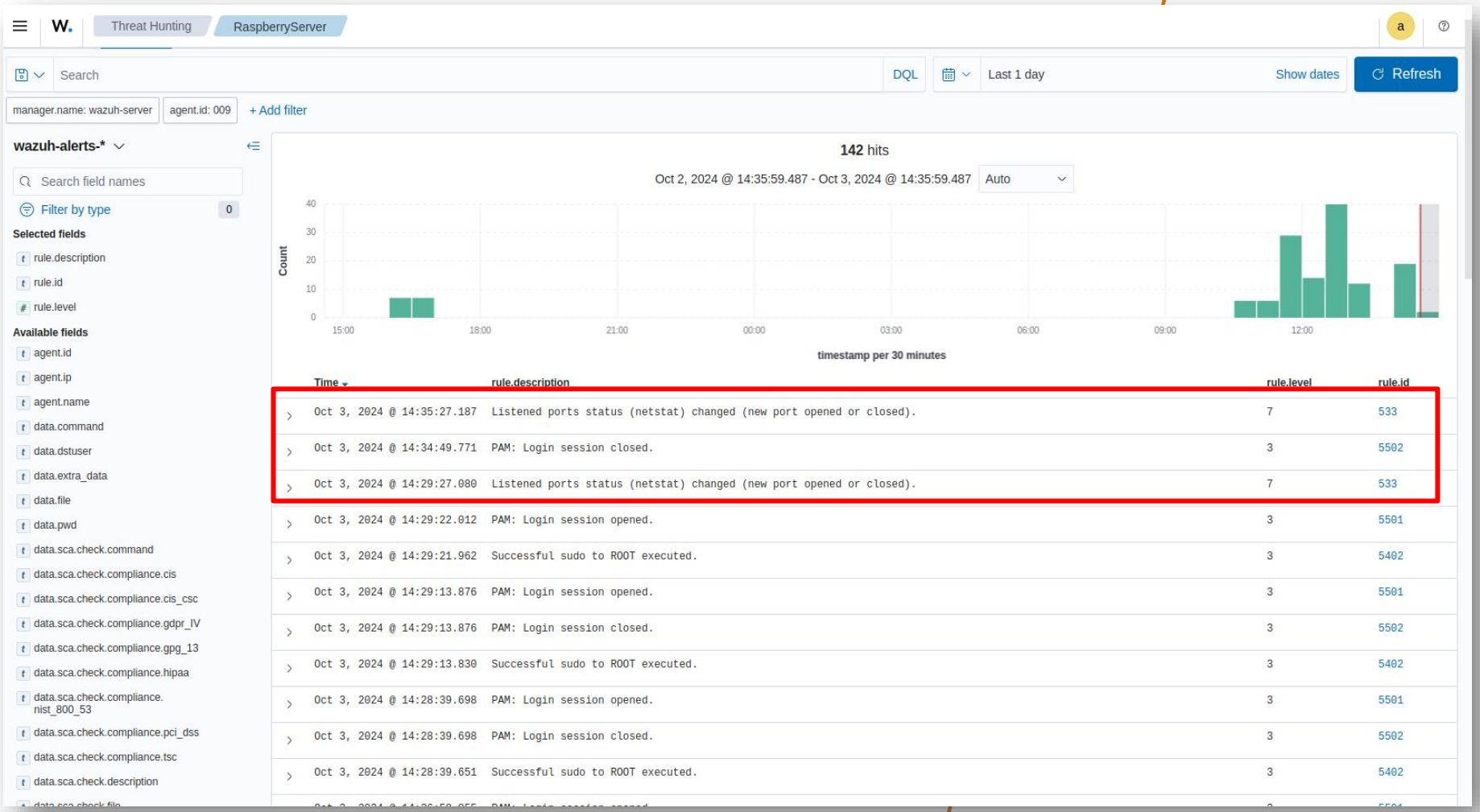
Endpoint Security

Threat Hunting: detect any **potential** cyber **threats** on the active **agents**



Endpoint Security

Threat Hunting: detect any **potential** cyber **threats** on the active **agents**



Threats have been **detected** due to the **open** and **closed status of port 502 (i.e., Modbus TCP client-server scheme**).

Thank you

Please send all questions to:
Abdelkader Shaaban,
abdelkader.Shaaban@ait.ac.at
Stefan Schauer
Stefan.Schauer@ait.ac.at