



EDUCATION AND TRAINING

CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

Next level cybersecurity education and training



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

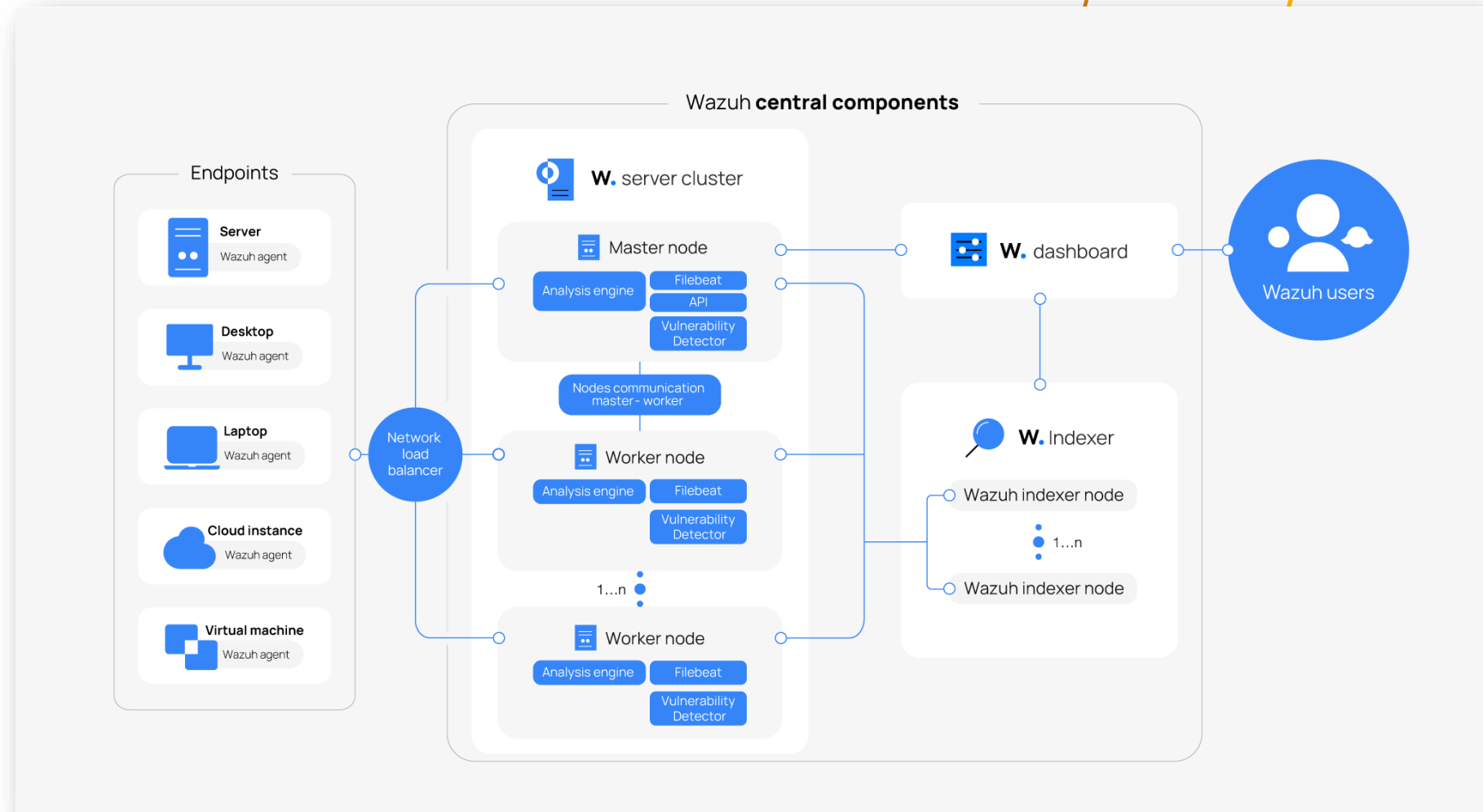
Containers Security

IT Hygiene

Regulatory Compliance

Incident Response

Wazuh: Central Components



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

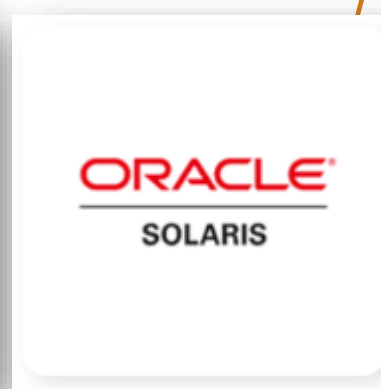
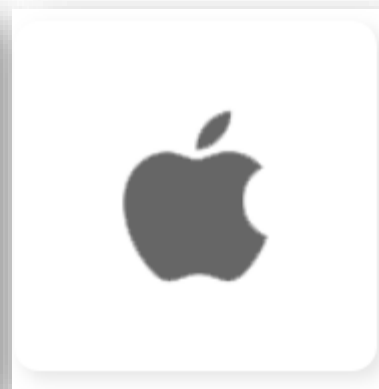
The Wazuh **dashboard** is the web **user interface** for data **visualization, analysis,** and management.

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

Wazuh Agents

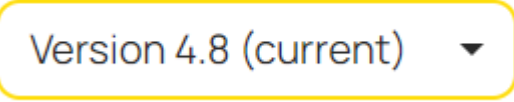
W.agent

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



Installing Wazuh Server

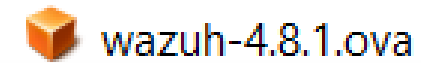
- Wazuh **provides** a pre-built **virtual machine image** in **Open Virtual Appliance (OVA)** format. This can be directly **imported** to **VirtualBox** or other **OVA-compatible virtualization systems**. Take into account that this **VM** only runs on **64-bit systems**. It does **not provide high 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.



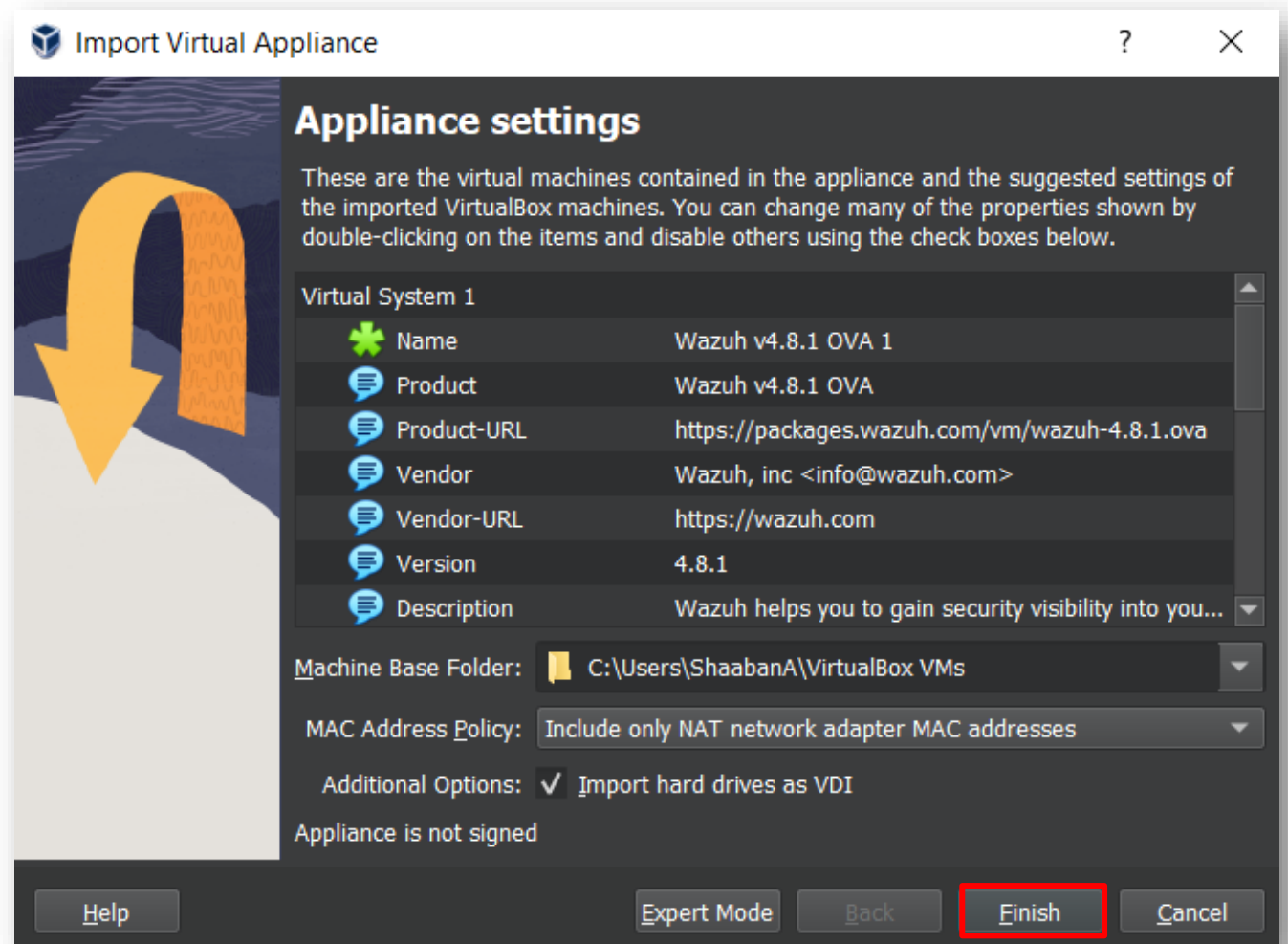
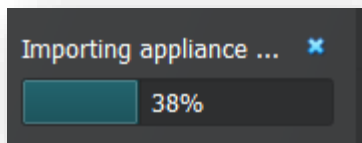
Version 4.8 (current) ▼

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.

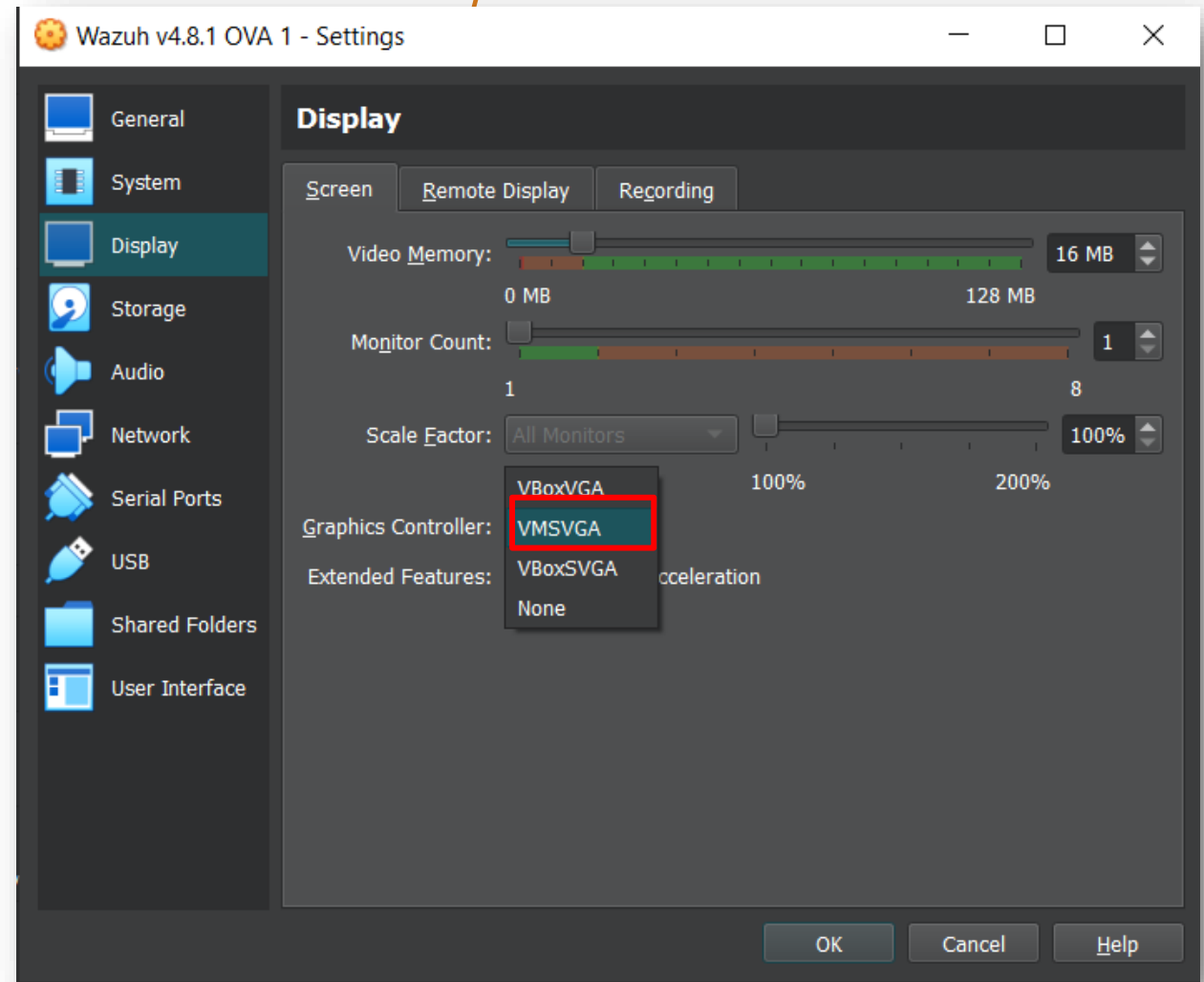


Installing Wazuh Server

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

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

- Press **ok**

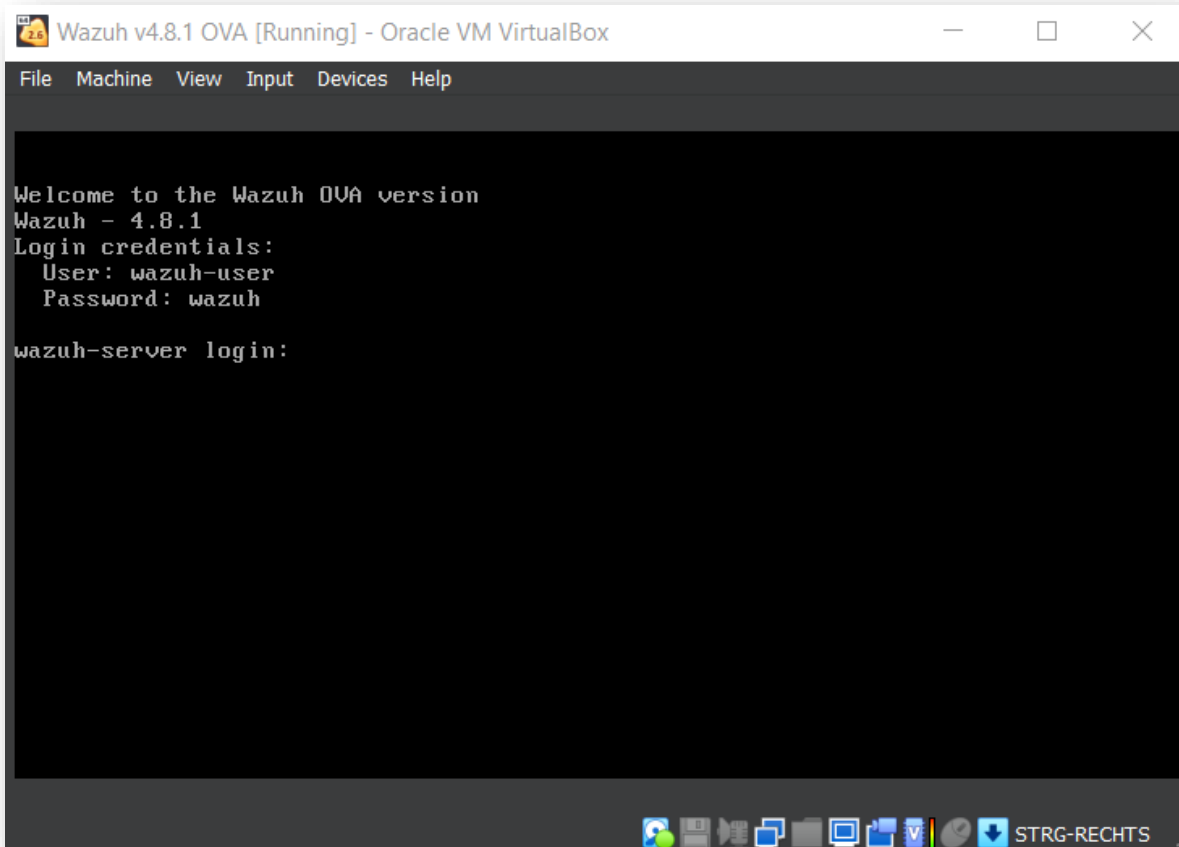


Launching Wazuh Server

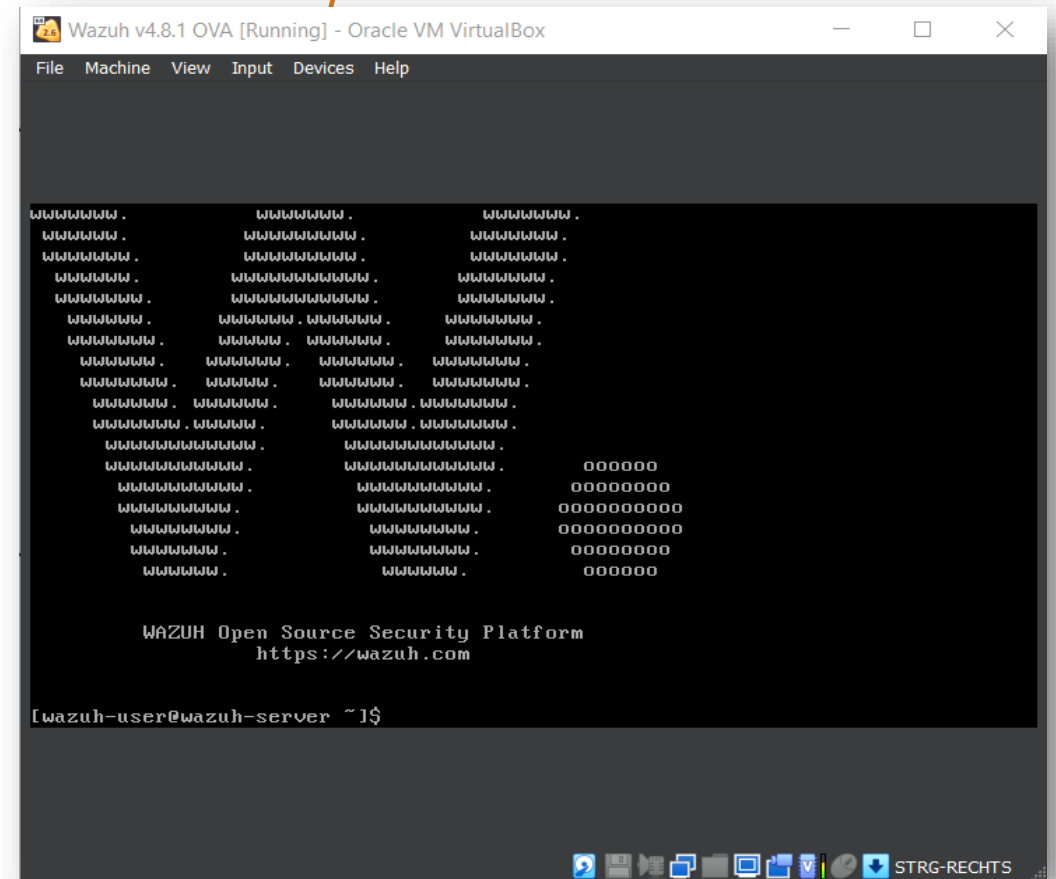
Press the **start button**.



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



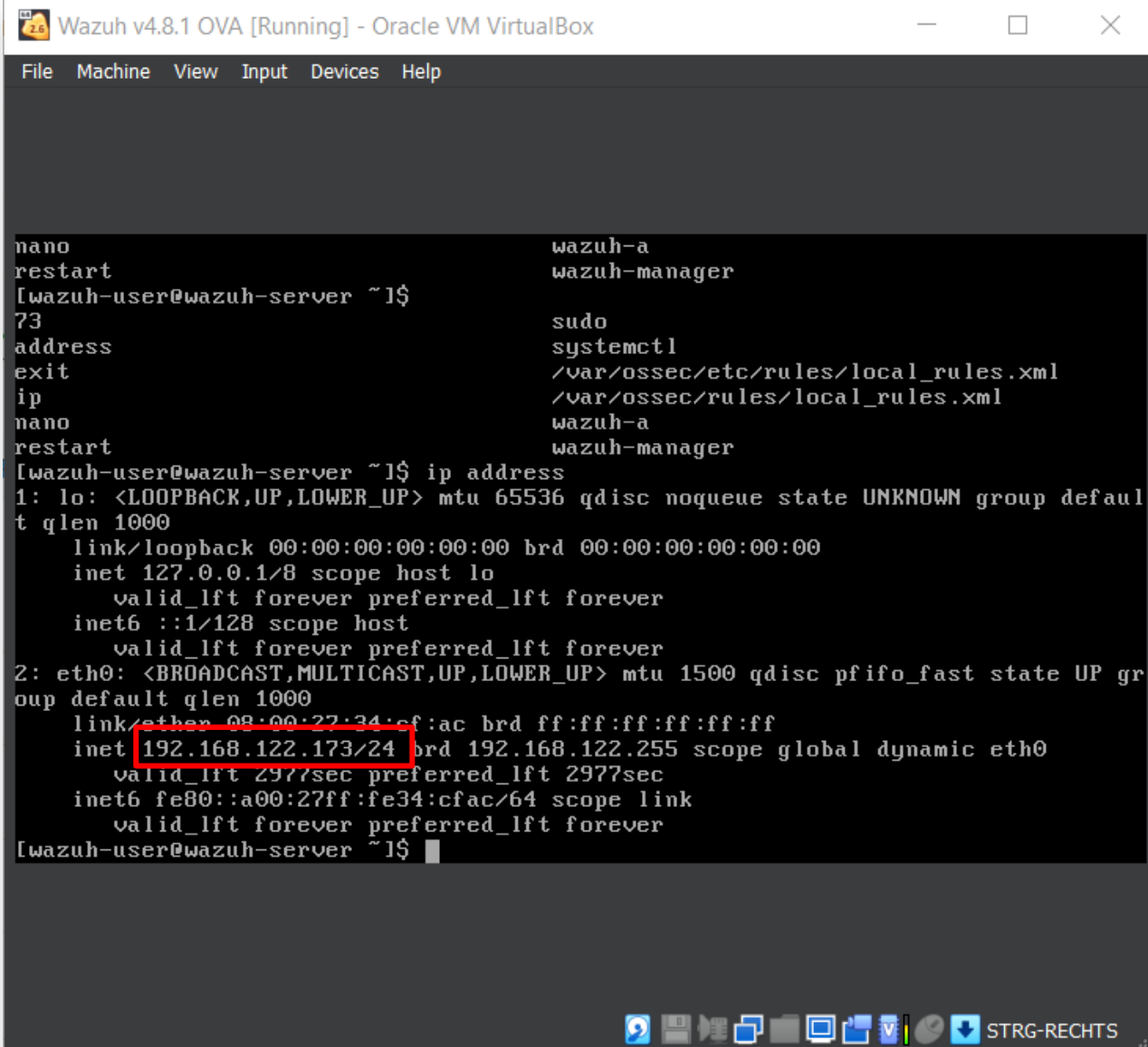
- Enter the **user** and **password**.
- **By default:**
 - **User:** wazuh-user
 - **Password:** wazuh



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``.



```
Wazuh v4.8.1 OVA [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

nano wazuh-a
restart wazuh-manager
[wazuh-user@wazuh-server ~]#
73 sudo
address systemctl
exit /var/ossec/etc/rules/local_rules.xml
ip /var/ossec/rules/local_rules.xml
nano wazuh-a
restart wazuh-manager
[wazuh-user@wazuh-server ~]# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:34:cf:ac brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.173/24 brd 192.168.122.255 scope global dynamic eth0
        valid_lft 2977sec preferred_lft 2977sec
    inet6 fe80::a00:27ff:fe34:cfac/64 scope link
        valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]#
```

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:

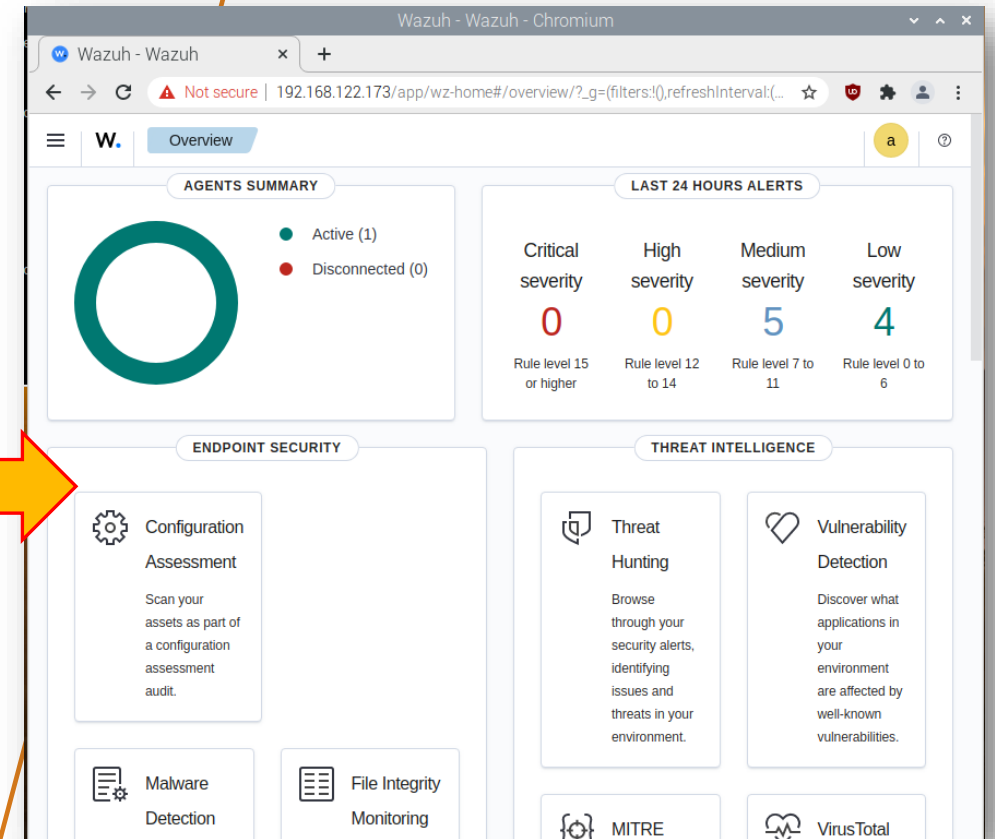
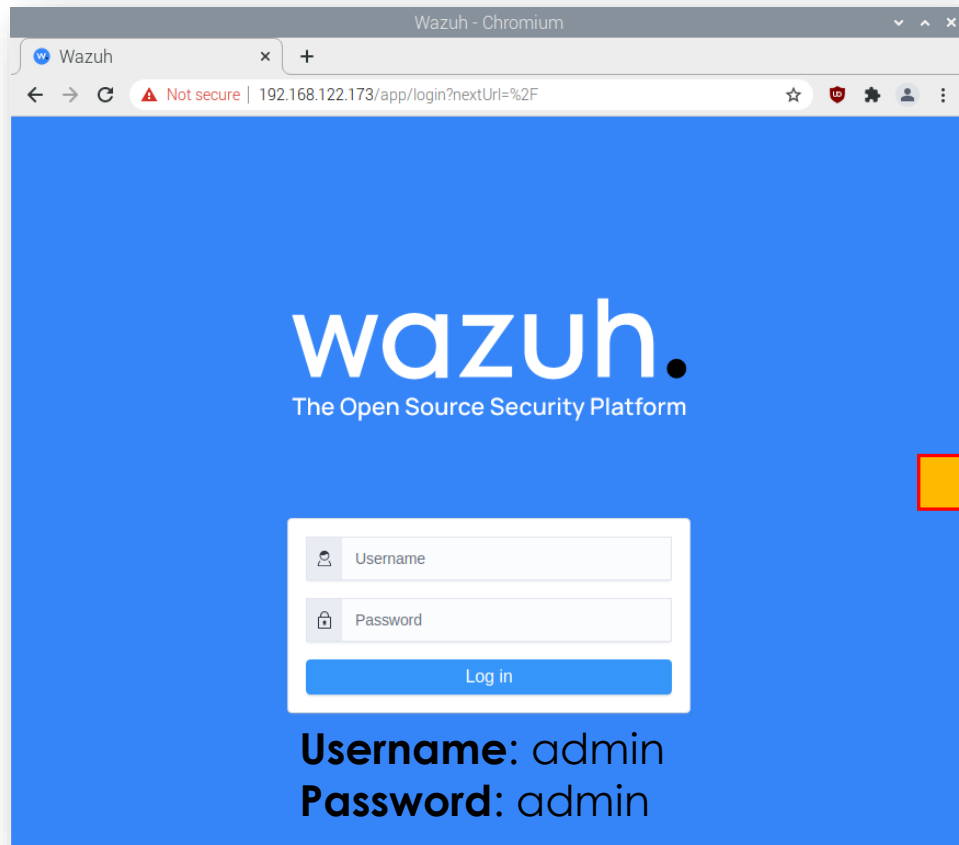
```
sudo systemctl restart wazuh-manager
```

```
[wazuh-user@wazuh-server ~]$ sudo systemctl status wazuh-manager
■ wazuh-manager.service - Wazuh manager
   Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2024-10-02 11:18:22 UTC; 7min ago
   Process: 19780 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/wazuh-manager.service
           └─ 5370 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr...
           └─ 5392 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr...
           └─ 5396 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr...
           └─ 5401 /var/ossec/framework/python/bin/python3 /var/ossec/api/scr...
           └─ 5466 /var/ossec/bin/wazuh-authd
           └─ 5529 /var/ossec/bin/wazuh-db
           └─ 5581 /var/ossec/bin/wazuh-execd
           └─ 5687 /var/ossec/bin/wazuh-analysisd
           └─ 5823 /var/ossec/bin/wazuh-syscheckd
           └─ 5959 /var/ossec/bin/wazuh-remoted
           └─ 6106 /var/ossec/bin/wazuh-logcollector
           └─ 6220 /var/ossec/bin/wazuh-monitord
           └─ 19909 /var/ossec/bin/wazuh-modulesd

Oct 02 11:18:18 wazuh-serve
```

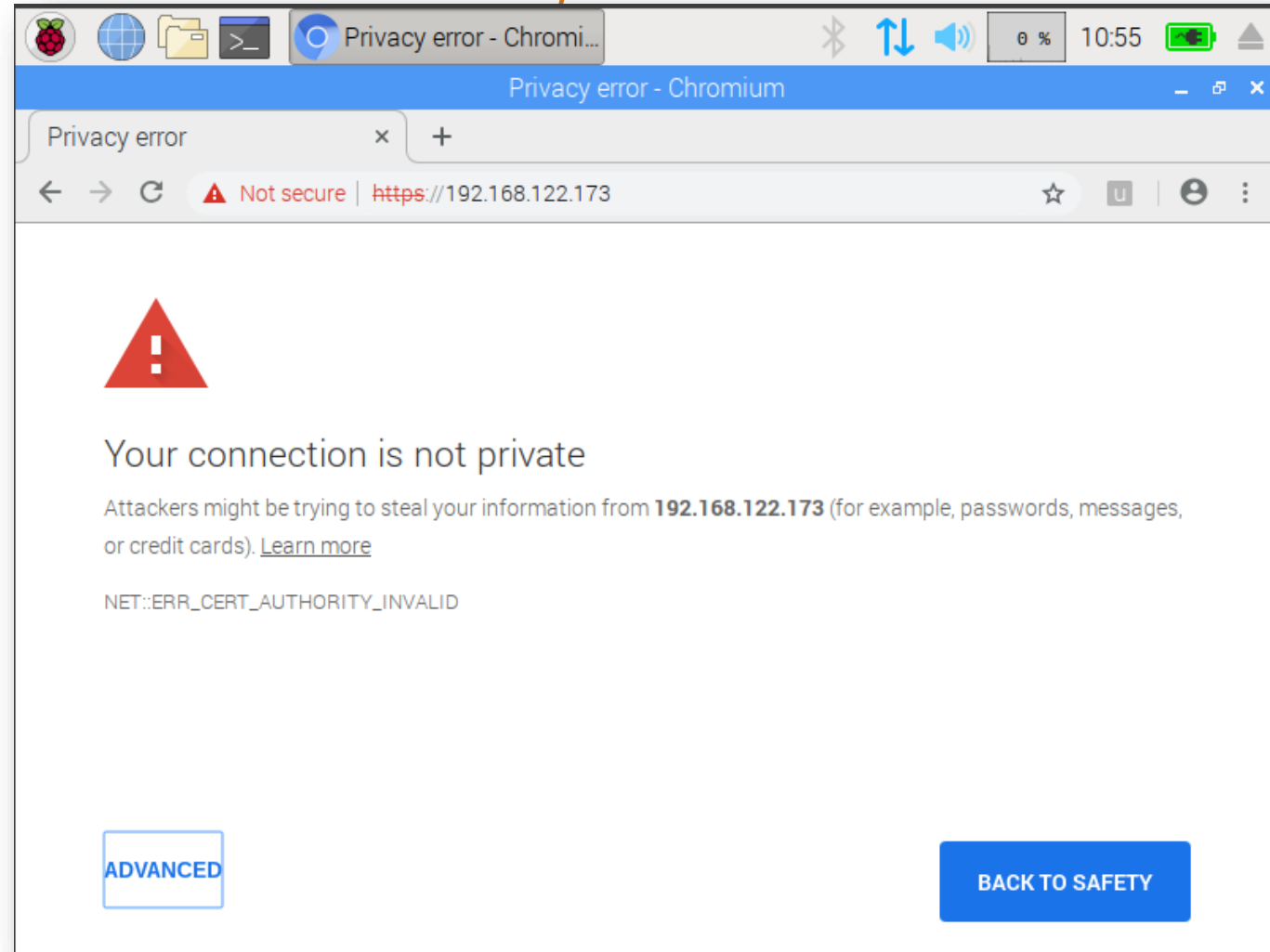
Installing Agent (Endpoint)

- 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>



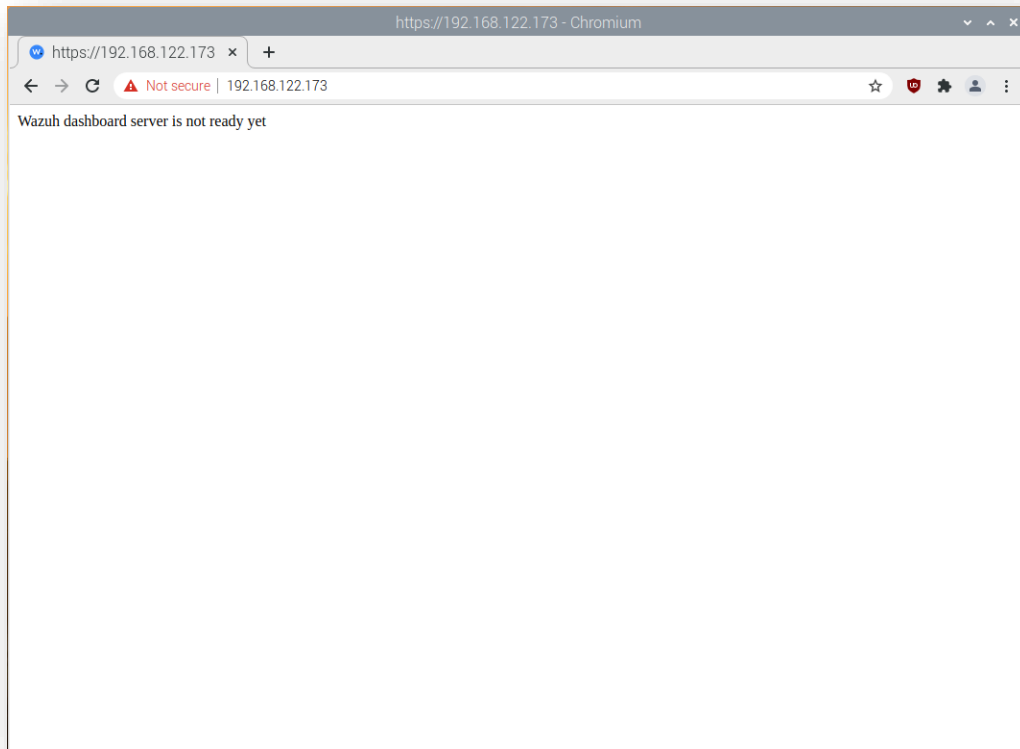
Installing Agent (Endpoint)

- 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; vendor 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; vendor 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**

The screenshot shows the Wazuh dashboard interface. At the top, there's a navigation bar with the Wazuh logo and a menu icon. Below that, the 'Endpoints' section is active. The main content area is divided into three panels: 'STATUS', 'DETAILS', and 'EVOLUTION'. The 'STATUS' panel shows a donut chart and a legend with 1 Active agent. The 'DETAILS' panel shows 1 Active agent, 0 Disconnected, 0 Pending, and 0 Never connected agents, with 100.00% coverage. The 'EVOLUTION' panel shows a line graph of agent status over time. Below these panels is the 'Agents (1)' table, which contains one entry for 'raspberry'. A red box highlights the '+ Deploy new agent' button in the top right of the agents table.

Wazuh - Wazuh - Chromium

Wazuh - Wazuh

Not secure | 192.168.122.173/app/endpoints-summary#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(colum...

Endpoints

STATUS

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

DETAILS

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

Last enrolled agent: raspberry, Most active agent: raspberry

EVOLUTION

Count vs timestamp per 10 min (18:00, 06:00). Legend: Last 24 hours disconnected (red), active (green).

Agents (1) **+ Deploy new agent** Refresh Export formatted

status=active WQL Refresh




ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
003	raspberry	192.168.122.109	default	Debian GNU/Linux 10	node01	v4.8.1	active	

Rows per page: 10

Installing Agent (Endpoint)

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

1 Select the package to download and install on your system:

 LINUX	 WINDOWS	 macOS
<input type="radio"/> RPM amd64 <input type="radio"/> RPM aarch64 <input checked="" type="radio"/> DEB amd64 <input type="radio"/> DEB aarch64	<input type="radio"/> MSI 32/64 bits	<input type="radio"/> Intel <input type="radio"/> Apple silicon

2 **Server address:**

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address ?

192.168.122.173

Remember server address

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

```
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
```

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
```

```
pi@raspberrypi: ~
File Edit Tabs Help
pi@raspberrypi:~ $ 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' WAZU
H_AGENT_NAME='Client' dpkg -i ./wazuh-agent_4.8.1-1_amd64.deb
--2024-08-27 13:10:10-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-ag
ent/wazuh-agent_4.8.1-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 13.32.110.36, 13.32.110.105
, 13.32.110.80, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|13.32.110.36|:443... conne
cted.
HTTP request sent, awaiting response... 200 OK
Length: 10270680 (9.8M) [binary/octet-stream]
Saving to: 'wazuh-agent_4.8.1-1_amd64.deb'

wazuh-agent_4.8.1-1 100%[=====] 9.79M 1.41MB/s in 7.0s

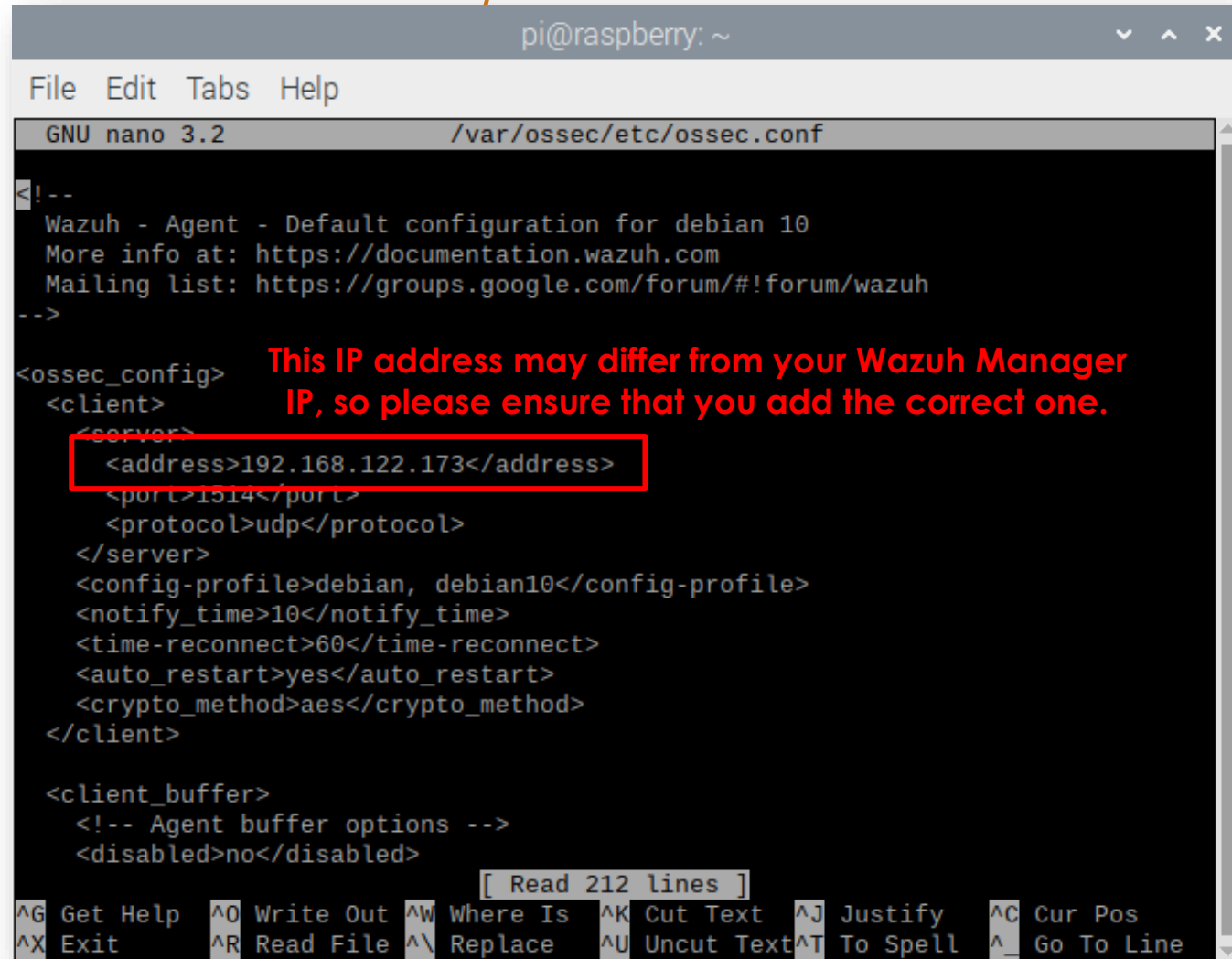
2024-08-27 13:10:17 (1.41 MB/s) - 'wazuh-agent_4.8.1-1_amd64.deb' saved [1027068
0/10270680]

(Reading database ... 145673 files and directories currently installed.)
Preparing to unpack ../wazuh-agent_4.8.1-1_amd64.deb ...
Unpacking wazuh-agent:amd64 (4.8.1-1) over (3.12.3-1) ...
Setting up wazuh-agent:amd64 (4.8.1-1) ...
Installing new version of config file /etc/systemd/system/wazuh-agent.service ..
.
Installing new version of config file /etc/init.d/wazuh-agent ...
Processing triggers for systemd (241-7~deb10u10) ...
pi@raspberrypi:~ $
```

Installing Agent (Endpoint)

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

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



```
pi@raspberrypi: ~
File Edit Tabs Help
GNU nano 3.2 /var/ossec/etc/ossec.conf
<!--
Wazuh - Agent - Default configuration for debian 10
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <client>
    <server>
      <address>192.168.122.173</address>
      <port>1514</port>
      <protocol>udp</protocol>
    </server>
    <config-profile>debian, debian10</config-profile>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
  </client>

  <client_buffer>
    <!-- Agent buffer options -->
    <disabled>no</disabled>

[ Read 212 lines ]
^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
```

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.

```
(root@kali)~# /var/ossec/bin/agent-auth -m 192.168.122.173 -m MyAdminKali
2024/10/04 10:39:27 agent-auth: INFO: Started (pid: 127667).
2024/10/04 10:39:27 agent-auth: INFO: Requesting a key from server: MyAdminKali
2024/10/04 10:39:31 agent-auth: ERROR: Could not resolve hostname: MyAdminKali
```

Start the Agent (Endpoint)

Run the agent:

Sudo systemctl daemon-reload

Sudo systemctl enable wazuh-agent

Sudo systemctl start wazuh-agent

```
pi@raspberrypi: ~  
File Edit Tabs Help  
H_AGENT_NAME='Client' dpkg -i ./wazuh-agent_4.8.1-1_amd64.deb  
--2024-08-27 13:10:10-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.8.1-1_amd64.deb  
Resolving packages.wazuh.com (packages.wazuh.com)... 13.32.110.36, 13.32.110.105, 13.32.110.80, ...  
Connecting to packages.wazuh.com (packages.wazuh.com)|13.32.110.36|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 10270680 (9.8M) [binary/octet-stream]  
Saving to: 'wazuh-agent_4.8.1-1_amd64.deb'  
  
wazuh-agent_4.8.1-1 100%[=====] 9.79M 1.41MB/s in 7.0s  
  
2024-08-27 13:10:17 (1.41 MB/s) - 'wazuh-agent_4.8.1-1_amd64.deb' saved [10270680/10270680]  
  
(Reading database ... 145673 files and directories currently installed.)  
Preparing to unpack ../wazuh-agent_4.8.1-1_amd64.deb ...  
Unpacking wazuh-agent:amd64 (4.8.1-1) over (3.12.3-1) ...  
Setting up wazuh-agent:amd64 (4.8.1-1) ...  
Installing new version of config file /etc/systemd/system/wazuh-agent.service ...  
Installing new version of config file /etc/init.d/wazuh-agent ...  
Processing triggers for systemd (241-7~deb10u10) ...  
pi@raspberrypi:~$ sudo systemctl daemon-reload  
pi@raspberrypi:~$ sudo systemctl enable wazuh-agent  
Removed /etc/systemd/system/multi-user.target.wants/wazuh-agent.service.  
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /usr/lib/systemd/system/wazuh-agent.service.  
pi@raspberrypi:~$ sudo systemctl start wazuh-agent  
pi@raspberrypi:~$
```

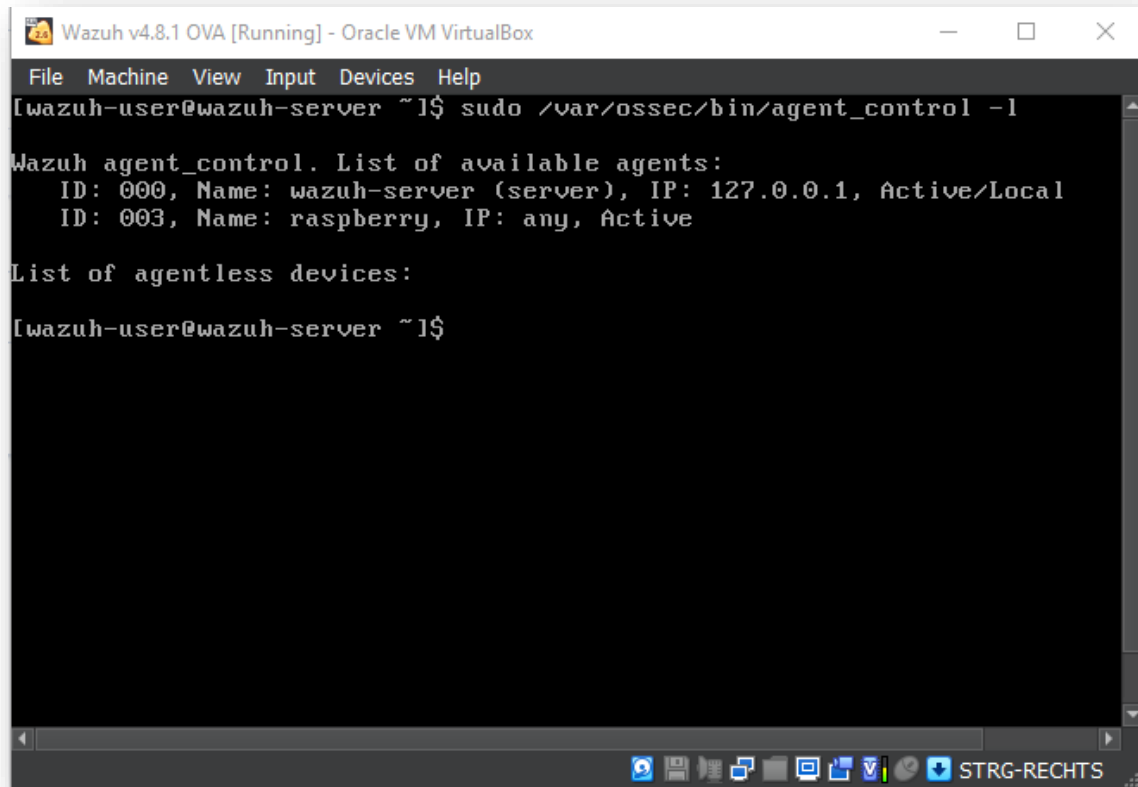
Check Agent List (Endpoint)

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.

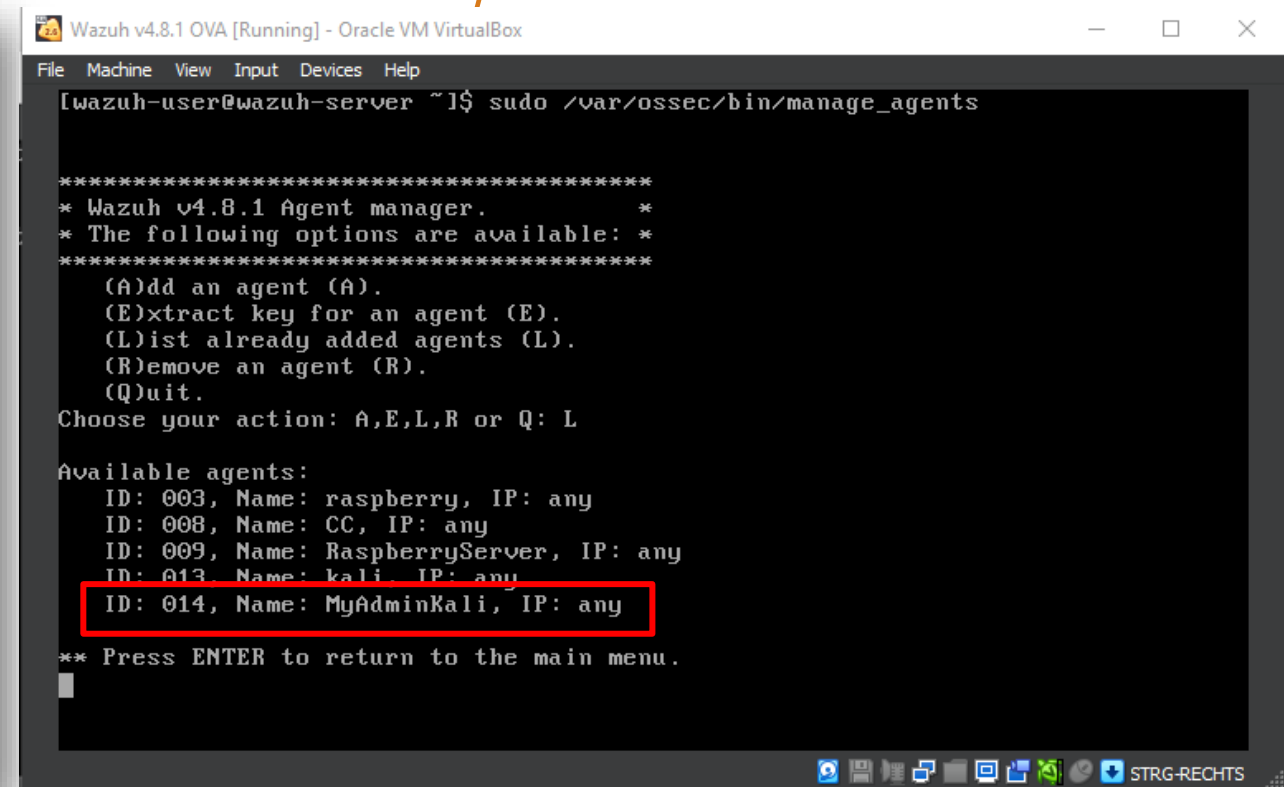


```
Wazuh v4.8.1 OVA [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[wazuh-user@wazuh-server ~]$ sudo /var/ossec/bin/agent_control -l

Wazuh agent_control. List of available agents:
  ID: 000, Name: wazuh-server (server), IP: 127.0.0.1, Active/Local
  ID: 003, Name: raspberry, IP: any, Active

List of agentless devices:

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



```
Wazuh v4.8.1 OVA [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[wazuh-user@wazuh-server ~]$ sudo /var/ossec/bin/manage_agents

*****
* Wazuh v4.8.1 Agent manager.
* The following options are available:
*****

(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.

Choose your action: A,E,L,R or Q: L

Available agents:
  ID: 003, Name: raspberry, IP: any
  ID: 008, Name: CC, IP: any
  ID: 009, Name: RaspberryServer, IP: any
  ID: 013, Name: kali, IP: any
  ID: 014, Name: MyAdminKali, IP: any

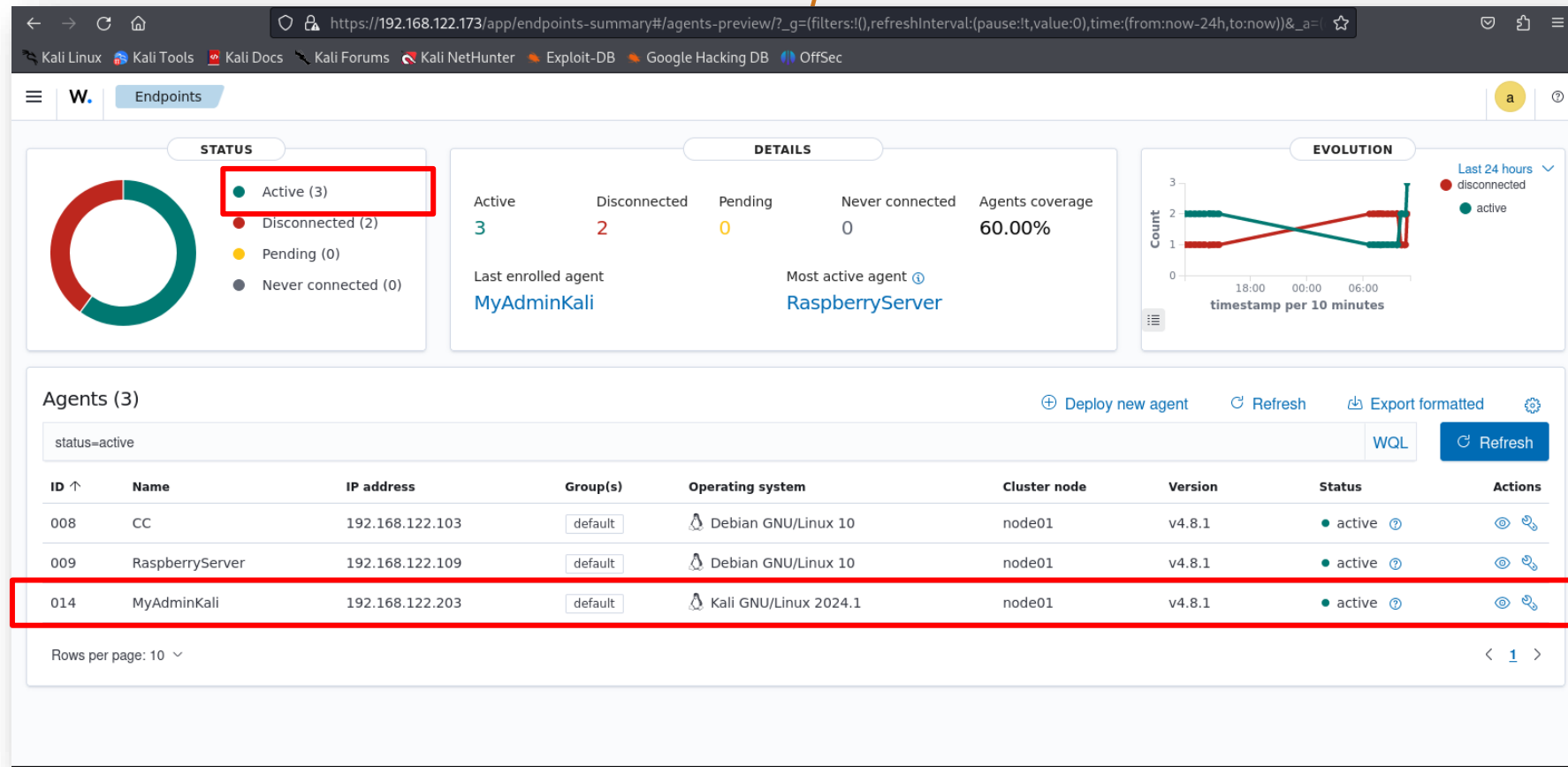
** Press ENTER to return to the main menu.
```

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**.

The screenshot displays a web dashboard for managing agents. The top navigation bar includes a search bar and several utility links. The main content area is divided into three sections: STATUS, DETAILS, and EVOLUTION.

STATUS: A donut chart shows the distribution of agent statuses: Active (3), Disconnected (2), Pending (0), and Never connected (0).

DETAILS: A summary of agent counts and coverage. Active agents: 3, Disconnected: 2, Pending: 0, Never connected: 0. Agents coverage: 60.00%. The last enrolled agent is MyAdminKali, and the most active agent is RaspberryServer.

EVOLUTION: A line graph showing the count of active and disconnected agents over time (timestamp per 10 minutes).

Agents (3): A table listing the active agents. The IP addresses 192.168.122.103 and 192.168.122.109 are highlighted with a red box.

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
008	CC	192.168.122.103	default	Debian GNU/Linux 10	node01	v4.8.1	active	
009	RaspberryServer	192.168.122.109	default	Debian GNU/Linux 10	node01	v4.8.1	active	
014	MyAdminKali	192.168.122.203	default	Kali GNU/Linux 2024.1	node01	v4.8.1	active	

Rows per page: 10 **Raspberry pi client, server, and my Admin Kali device**

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**.

The screenshot displays the Wazuh dashboard interface. The left sidebar contains a navigation menu with the following sections:

- Recently viewed (No items)
- Overview
- Explore
 - Discover
 - Dashboards
 - Visualize
 - Reporting
 - Alerting
 - Maps
 - Notifications
- Endpoint security
 - Configuration Assessment** (highlighted with a red box)
 - Malware Detection
 - File Integrity Monitoring
- Threat intelligence
 - Threat Hunting
 - Vulnerability Detection
 - MITRE ATT&CK
 - VirusTotal
- Security operations
 - PCI DSS

The main dashboard area shows a 'LAST 24 HOURS ALERTS' summary with four severity levels:

Severity	Count	Rule Level
Critical severity	0	15 or higher
High severity	0	12 to 14
Medium severity	16	7 to 11
Low severity	127	0 to 6

Below the alerts, the dashboard is organized into several functional areas:

- ENDPOINT SECURITY:** Includes Malware Detection (Verify that your systems are configured according to your security policies baseline).
- THREAT INTELLIGENCE:** Includes 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 (Security events from the knowledge base of adversary tactics and techniques based on real-world observations), and VirusTotal (Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API).
- SECURITY OPERATIONS:** Includes GDPR (General Data Protection Regulation (GDPR) sets guidelines for processing of personal data) and NIST 800-53 (National Institute of Standards and Technology Special).
- CLOUD SECURITY:** Includes Docker (Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events), Amazon Web Services (Security events related to your Amazon AWS services, collected directly via AWS API), Google Cloud, and GitHub.

Endpoint Security

Configuration Assessment

Select the agent you want to check

Explore agent ● RaspberryServer (009) ? 📌

Search WQL

ID ↑	Name	Group	Version	Operating system	Status
003	raspberry	default	v4.8.1	Debian GNU/Linux 10	● disconnected ?
006	Client		-	-	● never connected ?
007	ClientX		-	-	● never connected ?
008	CC	default	v4.8.1	Debian GNU/Linux 10	● active ?
009	RaspberryServer	default	v4.8.1	Debian GNU/Linux 10	● active ?

Rows per page: 10 ▾ < 1 >

Endpoint Security

Configuration Assessment

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

Wazuh - Wazuh

Configuration Assessment - RaspberryServer

Passed (62)
Failed (125)
Not applicable (5)

CIS Debian Linux 10 Benchmark v1.0.0

Passed 62 Failed 125 Not applicable 5 Score 33% End scan Oct 2, 2024 @ 11:14:18.000

Checks (192) Refresh Export formatted

ID	Title	Target	Result
2500	Ensure mounting of freevxfs filesystems is disabled	Command: /sbin/modprobe -n -v freevxfs	Failed
Rationale Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.			
Remediation Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vi /etc/modprobe.d/freevxfs.conf and add the following line: install freevxfs /bin/true Run the following command to unload the freevxfs module: # rmmod freevxfs			
Description The freevxfs filesystem type is a free version of the Veritas type filesystem. This is the primary filesystem type for HP-UX operating systems.			
Checks (Condition: all) <ul style="list-style-type: none">c:/sbin/modprobe -n -v freevxfs -> r:^install /bin/truenot c:/sbin/modprobe -> r:freevxfs			
Compliance cis: 1.1.1.1 cis_csc: 5.1 pci_dss: 2.2.5 tsc: CC6.3			
2501	Ensure mounting of jffs2 filesystems is disabled	Command: /sbin/modprobe -n -v jffs2	Failed
2502	Ensure mounting of hfs filesystems is disabled	Command: /sbin/modprobe -n -v hfs	Failed
2503	Ensure mounting of hfsplus filesystems is disabled	Command: /sbin/modprobe -n -v hfsplus	Failed

Endpoint Security

Malware Detection

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

The screenshot displays the Wazuh dashboard interface. At the top, there are browser tabs for 'Wazuh - Wazuh' and a navigation bar with a 'W.' logo and an 'Overview' tab. Below the navigation bar, the dashboard is divided into several sections:

- AGENTS SUMMARY:** A donut chart showing 2 Active agents (green) and 1 Disconnected agent (red).
- LAST 24 HOURS ALERTS:** A summary of alerts by severity: Critical (0), High (0), Medium (18), and Low (139).
- ENDPOINT SECURITY:** A section containing four cards: Configuration Assessment, **Malware Detection** (highlighted with a red box), File Integrity Monitoring, and Security Operations. The Malware Detection card includes a description: 'Verify that your systems are configured according to your security policies baseline.'
- THREAT INTELLIGENCE:** A section containing four cards: Threat Hunting, Vulnerability Detection, MITRE ATT&CK, and VirusTotal.
- CLOUD SECURITY:** A section containing four cards: Docker, Amazon Web Services, Google Cloud, and GitHub.

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**.

The screenshot displays the Wazuh Malware Detection interface for the agent 'RaspberryServer'. The 'Events' tab is active, showing a search for 'wazuh-alerts-*' with filters for 'manager.name: wazuh-server', 'rule.groups: rootcheck', and 'agent.id: 009'. A bar chart shows a single hit on October 2, 2024, at 11:14:41.109. Below the chart, a table lists the alert details:

Time	data.title	rule.description	rule.level	rule.id
Oct 2, 2024 @ 11:14:41.109	File is owned by root and has written permissions to anyone.	Host-based anomaly detection event (rootcheck).	7	510

The 'Expanded document' section shows the following JSON data:

```
{  "_index": "wazuh-alerts-4.x-2024.10.02",  "agent.id": "009",  "agent.ip": "192.168.122.109",  "agent.name": "RaspberryServer",  "data.file": "/etc/elasticsearch/elasticsearch.yml",  "data.title": "File is owned by root and has written permissions to anyone.",  "decoder.name": "rootcheck"}
```

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**.

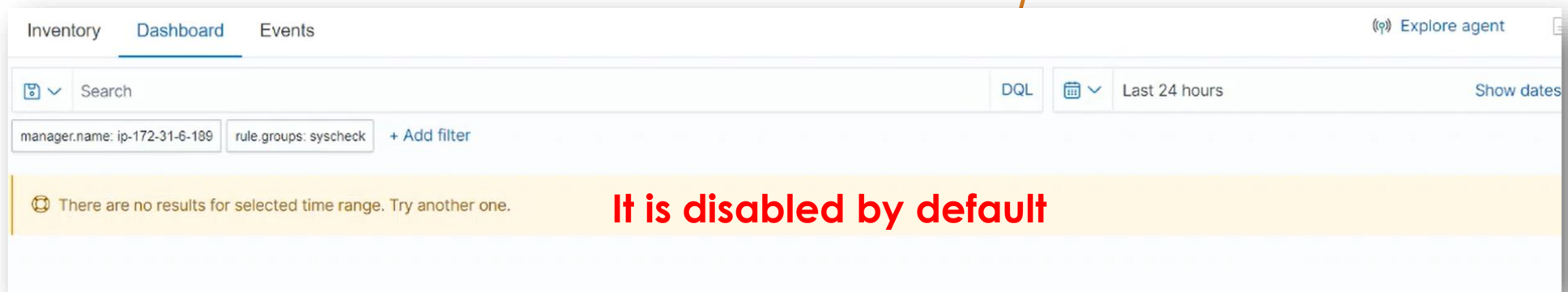
The screenshot displays the Wazuh dashboard interface. The top navigation bar includes the Wazuh logo and the 'Overview' tab. The main content area is divided into several sections:

- AGENTS SUMMARY:** A donut chart showing 1 Active agent (green) and 2 Disconnected agents (red).
- LAST 24 HOURS ALERTS:** A summary of alerts by severity: Critical (0), High (0), Medium (17), and Low (144).
- ENDPOINT SECURITY:** A section containing four sub-modules:
 - Configuration Assessment:** Scan your assets as part of a configuration assessment audit.
 - Malware Detection:** Verify that your systems are configured according to your security policies baseline.
 - File Integrity Monitoring:** Alerts related to file changes, including permissions, content, ownership, and attributes. This section is highlighted with a red border.
 - Threat Intelligence:** A section containing four sub-modules:
 - 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:** Security events from the knowledge base of adversary tactics and techniques based on real-world observations.
 - VirusTotal:** Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.
- SECURITY OPERATIONS:** A section containing two sub-modules:
 - PCI DSS:** Global security standard for entities that process, store, or transmit payment cardholder data.
 - GDPR:** General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.
- CLOUD SECURITY:** A section containing two sub-modules:
 - Docker:** Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.
 - Amazon Web Services:** Security events related to your Amazon AWS services, collected directly via AWS API.

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</directories>
  <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</directories>
  <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-monitor
-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-monitor...
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 ~]$
```

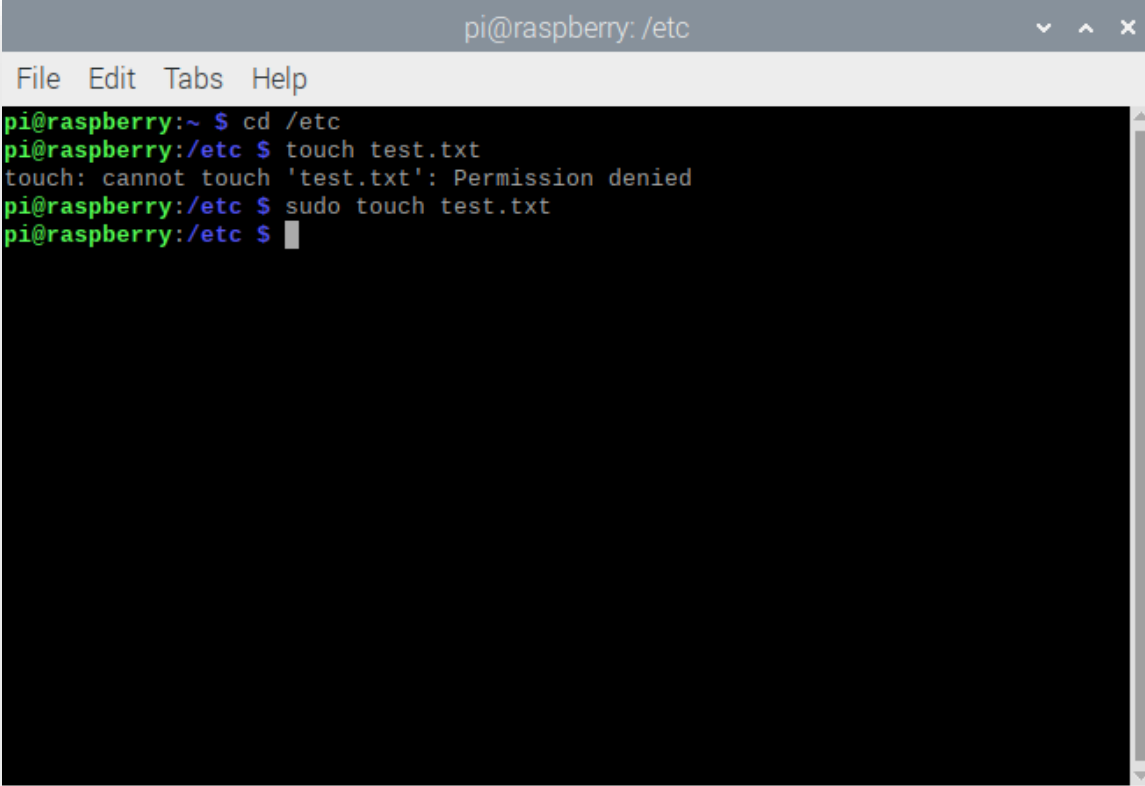
Check the status of the server using
sudo systemctl status wazuh-manager.service

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**

A terminal window titled "pi@raspberrypi: /etc" with a menu bar (File, Edit, Tabs, Help). The terminal shows the following commands and output:

```
pi@raspberrypi:~ $ cd /etc
pi@raspberrypi:/etc $ touch test.txt
touch: cannot touch 'test.txt': Permission denied
pi@raspberrypi:/etc $ sudo touch test.txt
pi@raspberrypi:/etc $
```

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

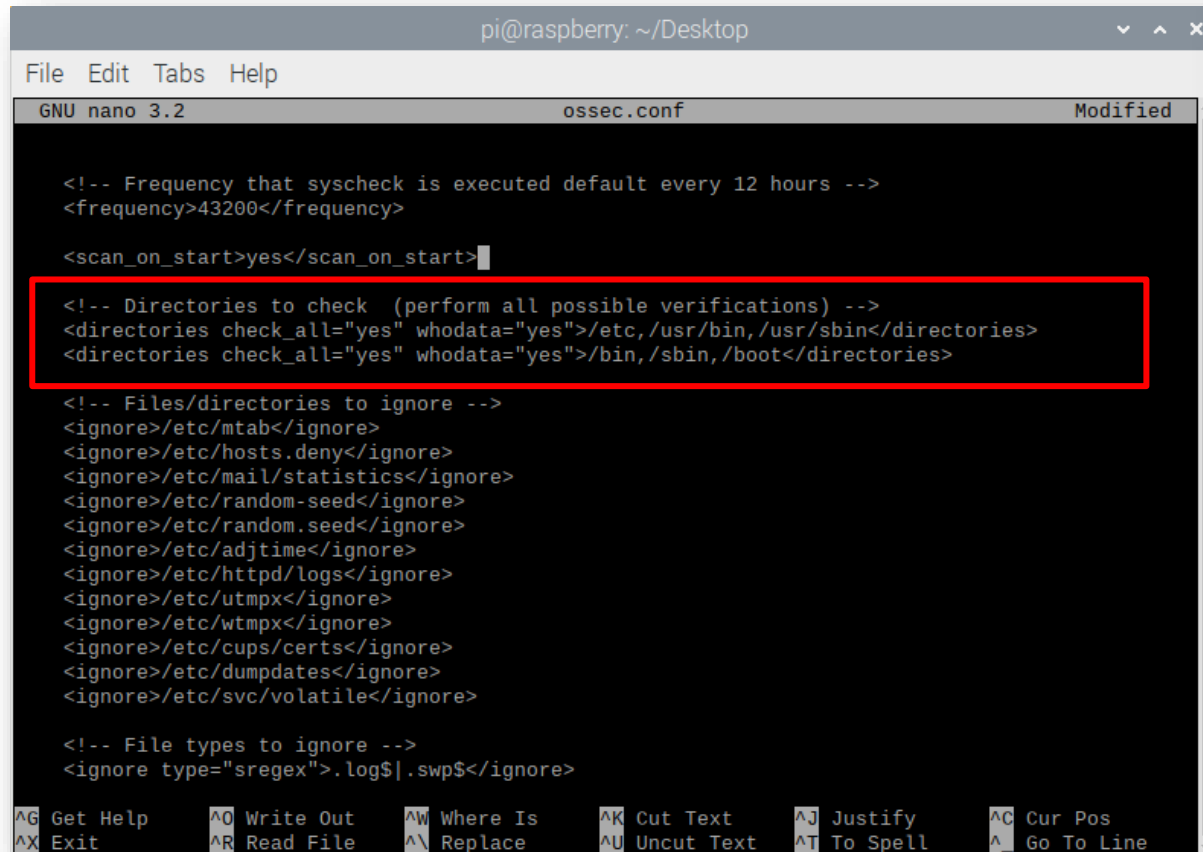
Endpoint Security

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



```
pi@raspberrypi: ~/Desktop
File Edit Tabs Help
GNU nano 3.2 ossec.conf Modified
<!-- Frequency that syscheck is executed default every 12 hours -->
<frequency>43200</frequency>

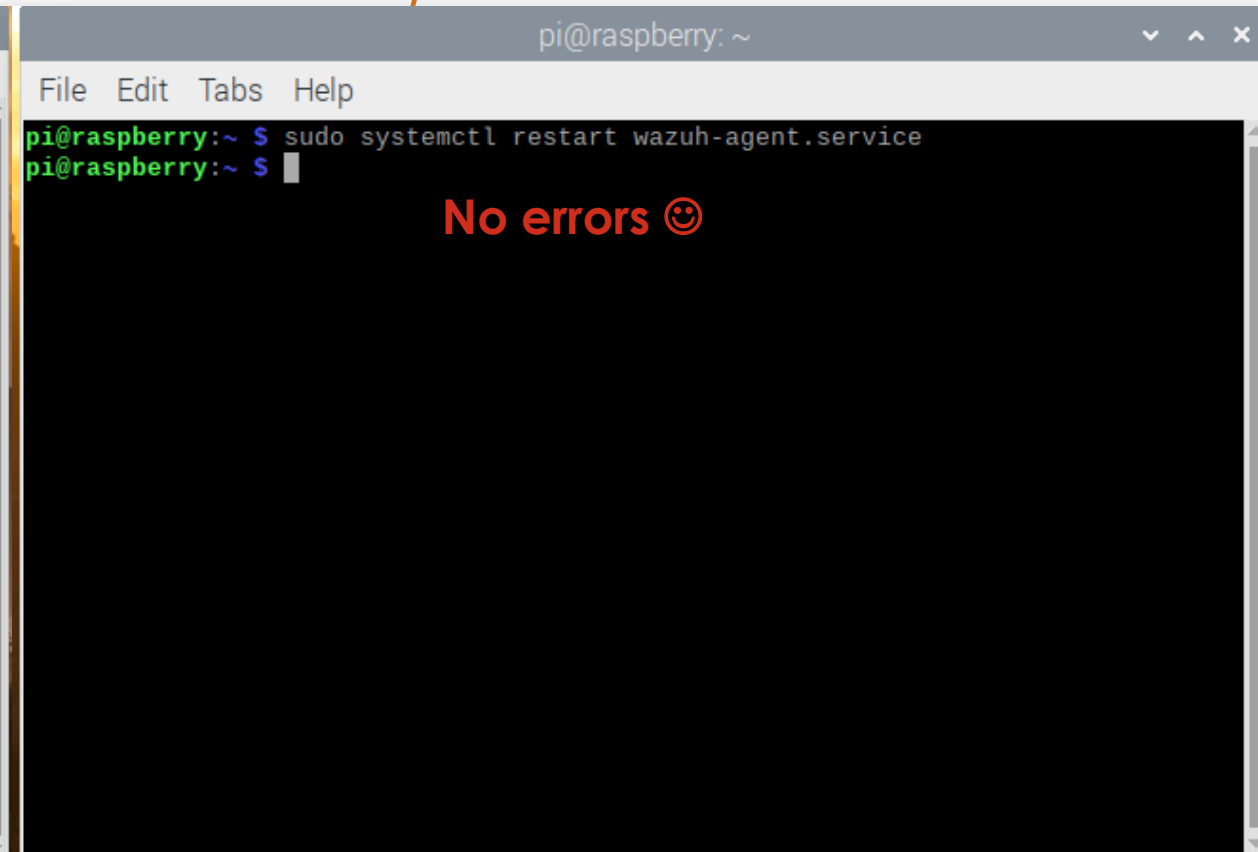
<scan_on_start>yes</scan_on_start>

<!-- Directories to check (perform all possible verifications) -->
<directories check_all="yes" whodata="yes">/etc,/usr/bin,/usr/sbin</directories>
<directories check_all="yes" whodata="yes">/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>
<ignore>/etc/wtmpx</ignore>
<ignore>/etc/cups/certs</ignore>
<ignore>/etc/dumpdates</ignore>
<ignore>/etc/svc/volatile</ignore>

<!-- File types to ignore -->
<ignore type="sregex">.log$.swp$</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
```

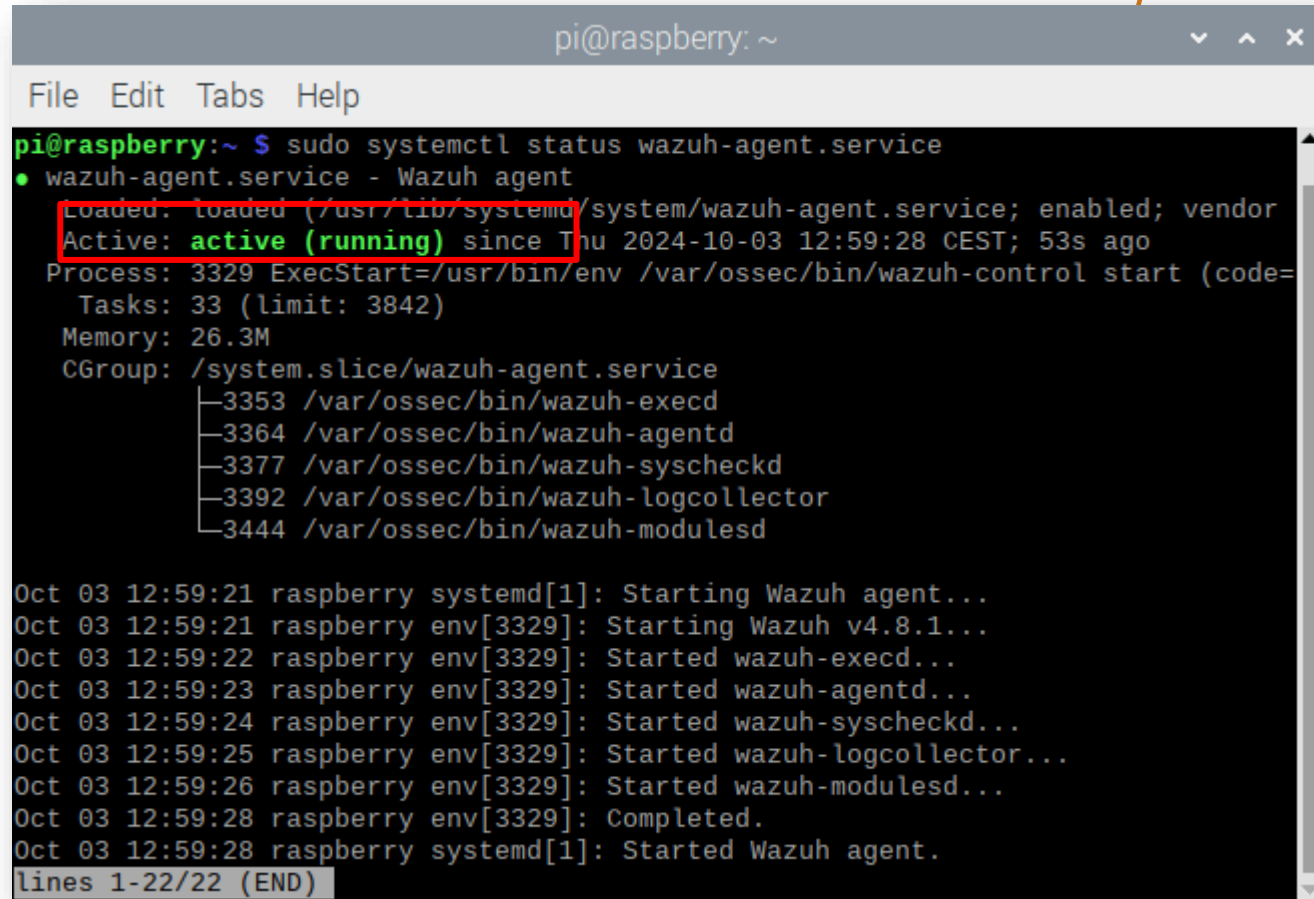


```
pi@raspberrypi: ~
File Edit Tabs Help
pi@raspberrypi:~ $ sudo systemctl restart wazuh-agent.service
pi@raspberrypi:~ $

No errors 😊
```

Endpoint Security

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



```
pi@raspberrypi: ~  
File Edit Tabs Help  
pi@raspberrypi:~ $ sudo systemctl status wazuh-agent.service  
● wazuh-agent.service - Wazuh agent  
Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; enabled; vendor  
Active: active (running) since Thu 2024-10-03 12:59:28 CEST; 53s ago  
Process: 3329 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=  
Tasks: 33 (limit: 3842)  
Memory: 26.3M  
CGroup: /system.slice/wazuh-agent.service  
├─3353 /var/ossec/bin/wazuh-execd  
├─3364 /var/ossec/bin/wazuh-agentd  
├─3377 /var/ossec/bin/wazuh-syscheckd  
├─3392 /var/ossec/bin/wazuh-logcollector  
└─3444 /var/ossec/bin/wazuh-modulesd  
  
Oct 03 12:59:21 raspberrypi systemd[1]: Starting Wazuh agent...  
Oct 03 12:59:21 raspberrypi env[3329]: Starting Wazuh v4.8.1...  
Oct 03 12:59:22 raspberrypi env[3329]: Started wazuh-execd...  
Oct 03 12:59:23 raspberrypi env[3329]: Started wazuh-agentd...  
Oct 03 12:59:24 raspberrypi env[3329]: Started wazuh-syscheckd...  
Oct 03 12:59:25 raspberrypi env[3329]: Started wazuh-logcollector...  
Oct 03 12:59:26 raspberrypi env[3329]: Started wazuh-modulesd...  
Oct 03 12:59:28 raspberrypi env[3329]: Completed.  
Oct 03 12:59:28 raspberrypi systemd[1]: Started Wazuh agent.  
lines 1-22/22 (END)
```

Endpoint Security

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

The screenshot displays the Wazuh File Integrity Monitoring dashboard. The interface includes a search bar, filters for 'manager.name: wazuh-server' and 'rule.groups: syscheck', and a time range of 'Last 24 hours'. A bar chart shows a single data point at 13:07 on Oct 3, 2024. Below the chart is a table with the following data:

Time	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Oct 3, 2024 @ 13:05:56.760	RaspberryServer	/etc/test.txt	added	File added to the system.	5	554

Below the table, an 'Expanded document' section shows the following JSON data:

```
Table JSON
{
  "_index": "wazuh-alerts-4.x-2024.10.03",
  "agent.id": "009",
  "agent.ip": "192.168.122.109",
  "agent.name": "RaspberryServer",
  "decoder.name": "syscheck_new_entry",
  "full_log": "File '/etc/test.txt' added\nMode: realtime",
  "id": "1727953556.124731"
}
```

Endpoint Security

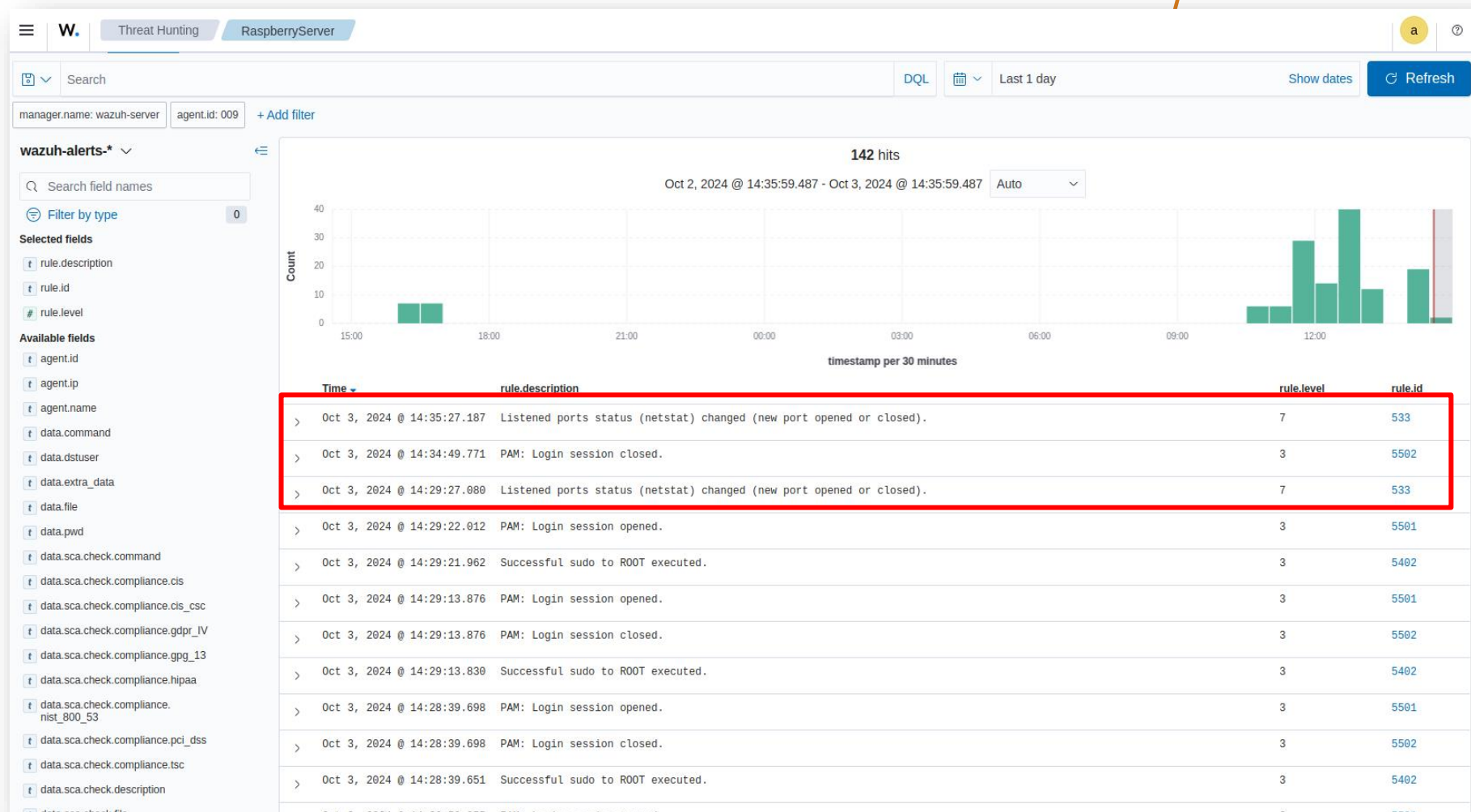
Threat Hunting: detect any **potential** cyber **threats** on the active **agents**

The screenshot displays the Wazuh dashboard interface. At the top, there's a navigation bar with a menu icon, the Wazuh logo, and an 'Overview' tab. The main content area is divided into several sections:

- AGENTS SUMMARY:** A donut chart showing 2 Active agents (green) and 1 Disconnected agent (red).
- LAST 24 HOURS ALERTS:** A summary of alerts by severity: Critical (0), High (0), Medium (44), and Low (233).
- ENDPOINT SECURITY:** Includes Configuration Assessment, Malware Detection, and File Integrity Monitoring.
- THREAT INTELLIGENCE:** Includes Threat Hunting (highlighted with a red box), Vulnerability Detection, MITRE ATT&CK, and VirusTotal.
- SECURITY OPERATIONS:** Includes PCI DSS, GDPR, HIPAA, and NIST 800-53.
- CLOUD SECURITY:** Includes Docker, Amazon Web Services, Google Cloud, and GitHub.

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