

Wazuh: A SEIM, SOC,XDR Solution

Wazuh is a free, open source and lightweight security monitoring platform for threat detection, integrity monitoring and incident response



Key Components of Wazuh

1. Wazuh Manager

Role: The Wazuh Manager is the core component of the Wazuh platform. It collects, normalizes, and analyzes security data generated by agents installed on monitored systems.

Importance: The Manager is responsible for real-time threat detection, log analysis, and incident response. It centralizes security event data from multiple sources and provides a unified view for monitoring and alerting.

2. Wazuh API:

Role: The Wazuh API provides a RESTful interface to interact with the Wazuh Manager. It enables you to query and retrieve security data, manage agents, and configure the Wazuh system programmatically.

Importance: The API allows integration with external tools and dashboards, making it easier to build custom security solutions and automate incident response processes.

3. Elasticsearch:

Role: Elasticsearch is a powerful and scalable search and analytics engine. In a Wazuh deployment, it stores and indexes the security data collected by the Wazuh Manager, making it searchable and accessible.

importance: Elasticsearch enables you to efficiently store, search, and visualize security data. It forms the foundation for historical data analysis, log correlation, and threat hunting.

4. Kibana:

Role: Kibana is a web-based data visualization and exploration tool that works seamlessly with Elasticsearch. It provides a user-friendly interface for querying and visualizing data stored in Elasticsearch.

Importance: Kibana is crucial for security analysts and administrators to create custom dashboards, view real-time alerts, and perform ad-hoc queries. It simplifies the process of monitoring and responding to security events.

5. Logstash:

Role: Logstash is an open-source data processing pipeline. While not explicitly mentioned in the provided installation guide, it is often used in conjunction with Elasticsearch and Kibana to ingest, transform, and enrich log data before it's indexed in Elasticsearch.

Importance: Logstash can be helpful for data preprocessing, especially when you need to parse and normalize logs from various sources before they are stored in Elasticsearch.

6. Agents:

Role: Agents are installed on monitored systems (servers, workstations, etc.) and collect security-related data such as logs, system events, and configurations. They send this data to the Wazuh Manager for analysis.

Importance: Agents are distributed across your network to provide comprehensive coverage of your IT infrastructure. They ensure that security events from all systems are centrally monitored and analyzed.

7. Wazuh App for Kibana:

Role: This is a plugin or app specifically designed for Kibana. It provides pre-built dashboards, visualizations, and search queries tailored for Wazuh data, making it easier to monitor and investigate security incidents.

Importance: The Wazuh app simplifies the process of creating security-focused dashboards and visualizations in Kibana. It allows security teams to quickly identify and respond to threats.

To sum up, each component in a Wazuh all-in-one deployment plays a crucial role in the overall security monitoring and analysis process. The combination of Wazuh, Elasticsearch, Kibana, and optional components like Logstash forms a powerful platform for threat detection, incident response, and security data analysis. This integrated approach helps organizations better protect their systems and data from security threats.

Features

1. SIEM

As a SIEM solution, Wazuh provides the following features:

- i. Security event collection from endpoints and cloud workloads
- ii. Log data analysis using rules and decoders
- iii. Threat hunting using dashboards and reports
- iv. Incident response tools like active responses and remote commands
- v. Compliance reporting to meet regulations like PCI DSS, GDPR, etc.

2. XDR

Wazuh's XDR capabilities include:

- i. Endpoint detection and response
- ii. File integrity monitoring
- iii. Vulnerability assessment
- iv. Malware detection using signatures and behavior analytics
- v. Threat intelligence integration

The Wazuh agent runs on endpoints and provides real-time prevention, detection, and response. The Wazuh server correlates data from all agents and uses threat intelligence to detect threats.

3. SOC

For Security Operations Centers, Wazuh offers:

- i. Automated alerts for security incidents
- ii. Dashboards and reports for threat visualization and analysis
- iii. Active responses to contain threats like IP blocking and file quarantining
- iv. Incident tracking and ticketing integration

4. New features

Some of Wazuh's latest features include:

- i. Wazuh Cloud: A managed cloud SIEM and XDR offering
- ii. Container security: Monitoring Docker hosts and containers
- iii. Cloud security: Monitoring of AWS, Azure, and GCP
- iv. On-demand API: To trigger agent scans and responses programmatically
- v. AI-based anomaly detection: Using machine learning models

Wazuh installation Guide:

1. Using virtualization (OVM file) :

Wazuh provides an Open Virtual Appliance (OVA) file that contains a pre-configured virtual machine. This makes it easy to install and run Wazuh on a virtual machine.

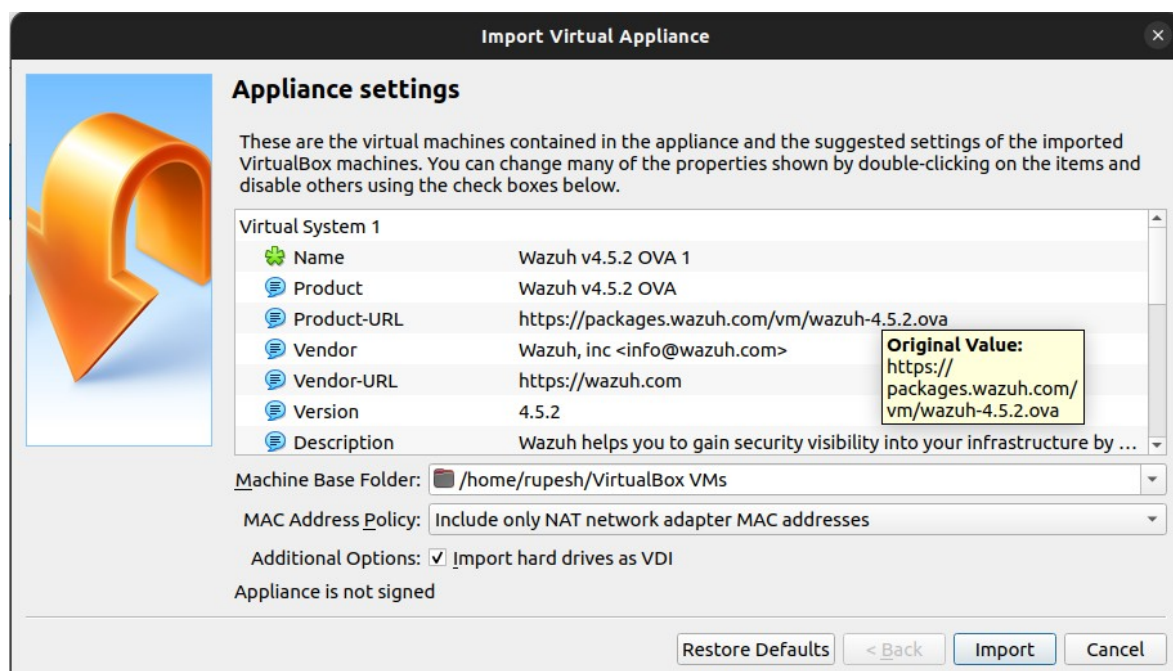
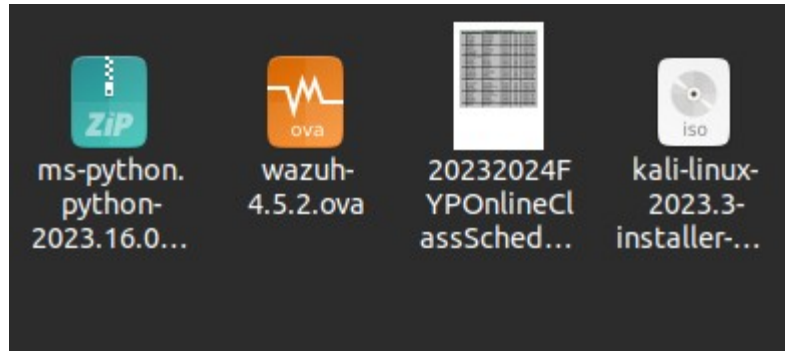
Here are the step-by-step instructions to install Wazuh OVA on a virtual machine:

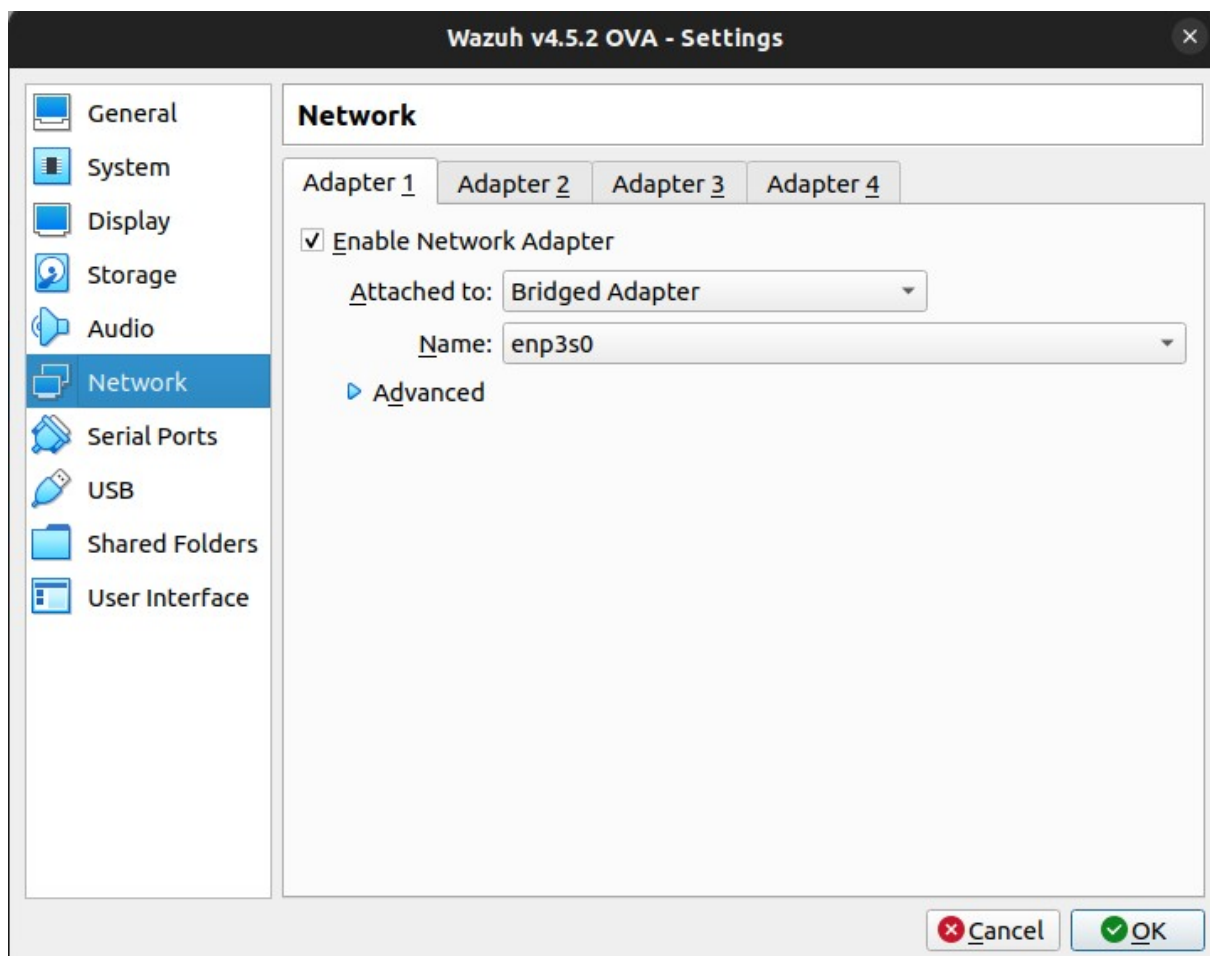
Step 1: Download the Wazuh OVA file from the official website. It contains:

- ◆ Amazon Linux 2
- ◆ Wazuh manager
- ◆ Wazuh indexer
- ◆ Filebeat
- ◆ Wazuh dashboard

Step 2: Import the OVA file into your virtualization software like VirtualBox.

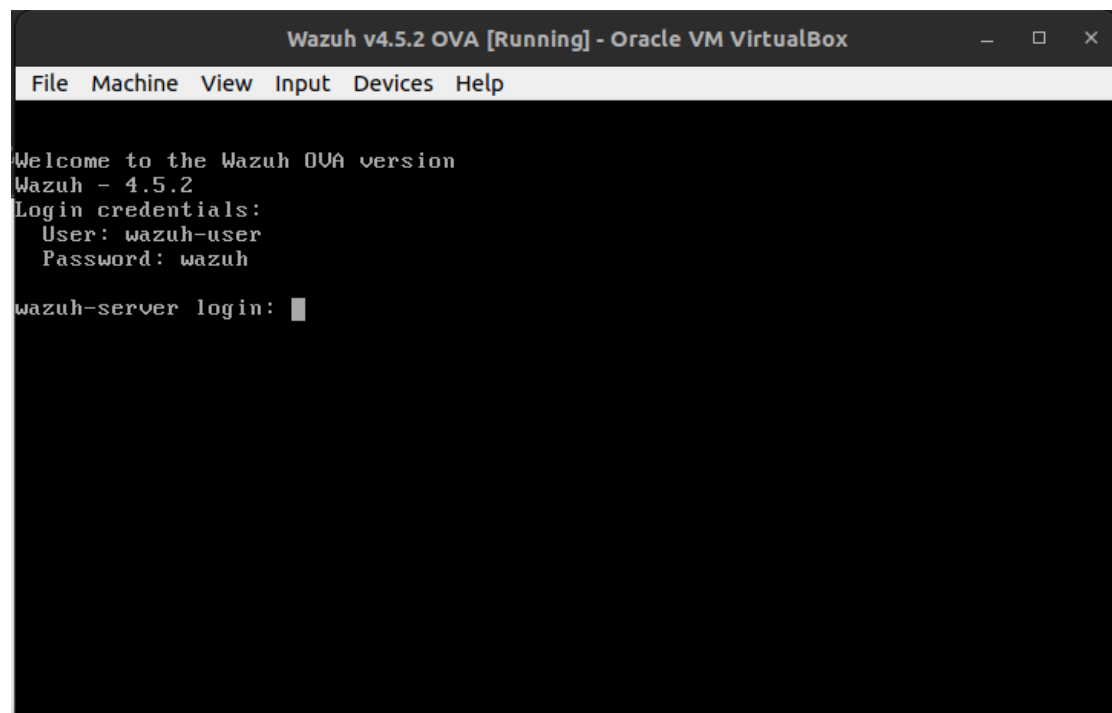
- Double click on the OVA file that you have downloaded. After that you will have option to import. Click on Import button. After few minutes vm will be ready. You can configure some of the configuration according to your need. Some of the configuration image is shown below:





Step 3: Start the virtual machine and log in using:

Username: wazuh-user



Password:
wazuh

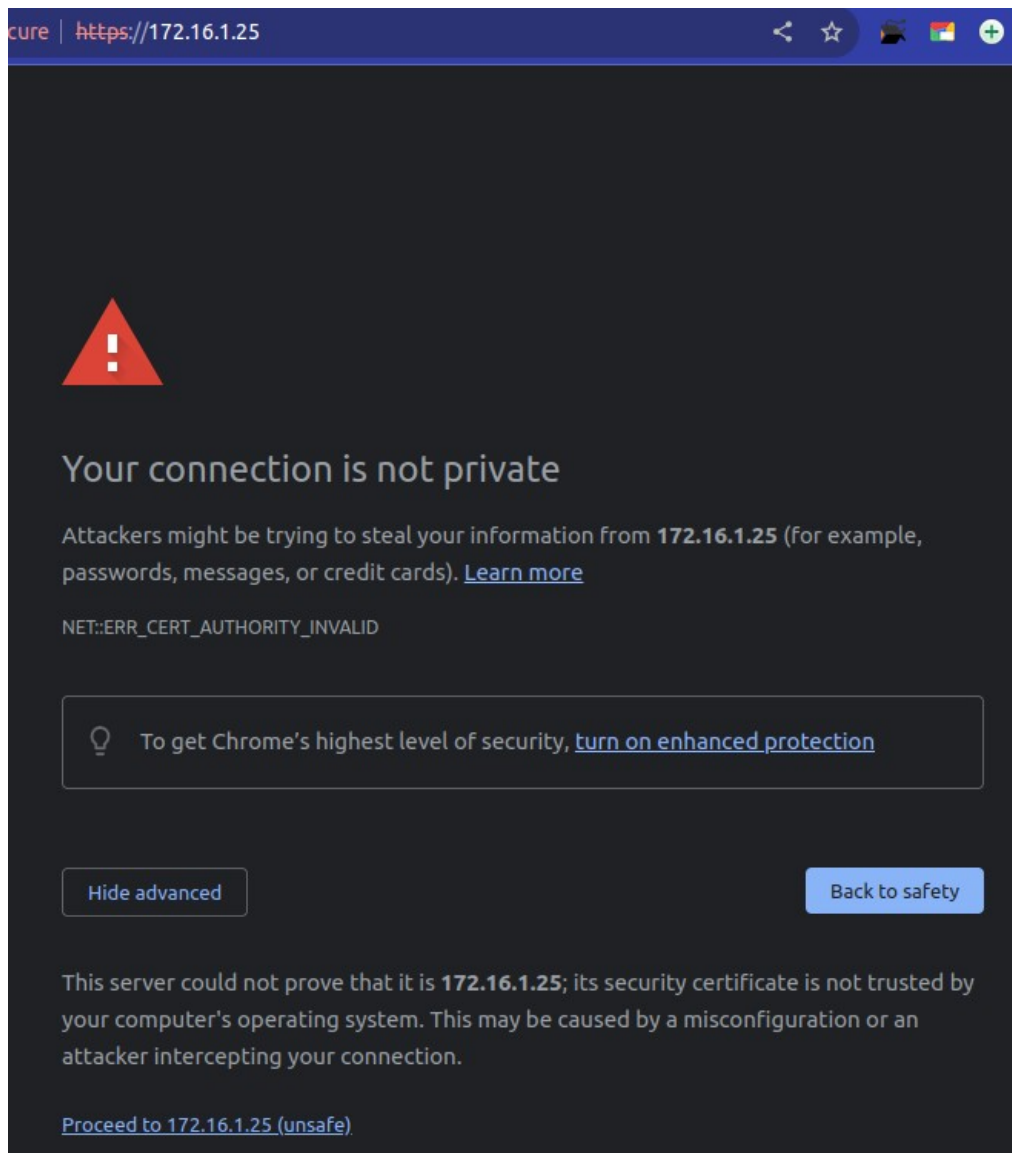
Step 4: In the terminal of Wazuh type: **ifconfig** to find the IP of your wazuh manager.

```
32 package(s) needed for security, out of 60 available
Run "sudo yum update" to apply all updates.
[wazuh-user@wazuh-server ~]$
[wazuh-user@wazuh-server ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.1.25 netmask 255.255.255.0 broadcast 172.16.1.255
    inet6 fe80::a00:27ff:fe1b:5adb prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:1b:5a:db txqueuelen 1000 (Ethernet)
    RX packets 2397 bytes 3452263 (3.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1694 bytes 130129 (127.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 569 bytes 130927 (127.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 569 bytes 130927 (127.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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

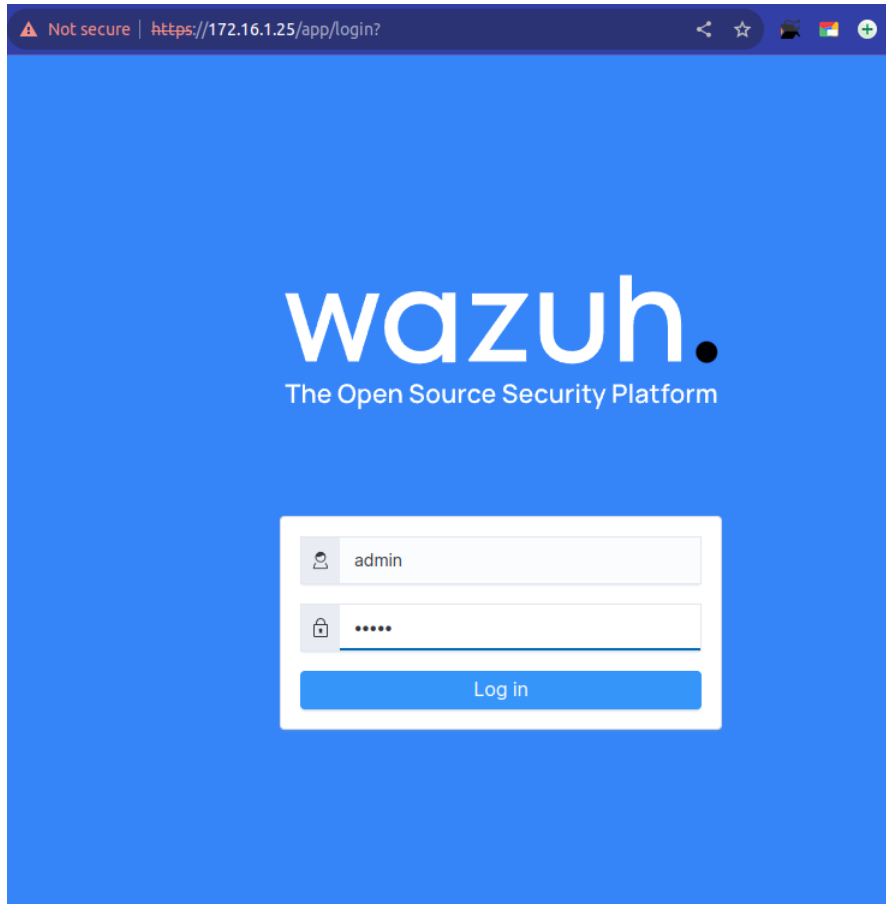

Step 5: Access the Wazuh dashboard by going to **https://Ip-of-wazuh-manager** in your browser. The default credentials are:

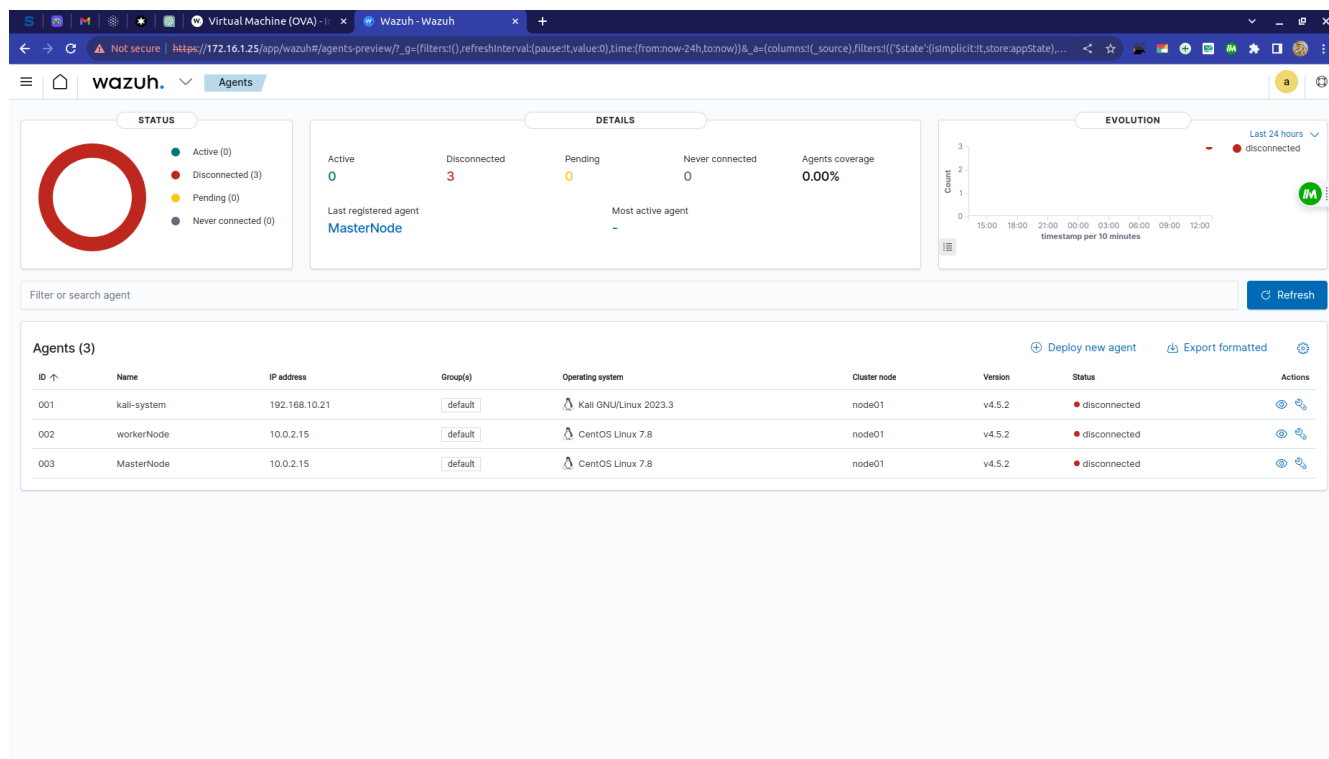


Step 6: Click on proceed to unsafe after few seconds you will see wazuh login page. Use the below credential to authenticate.

Username: admin

Password: admin





NOTE: At first you won't have any agents you have to add the agents to the wazuh manager.

NOTE: All the Wazuh components are pre-configured and ready to use out of the box. However, you can customize the configuration files located at:

`/var/ossec/etc/ossec.conf` for the Wazuh manager

`/etc/wazuh-indexer/opensearch.yml` for the Wazuh indexer

`/etc/filebeat/filebeat.yml` for Filebeat

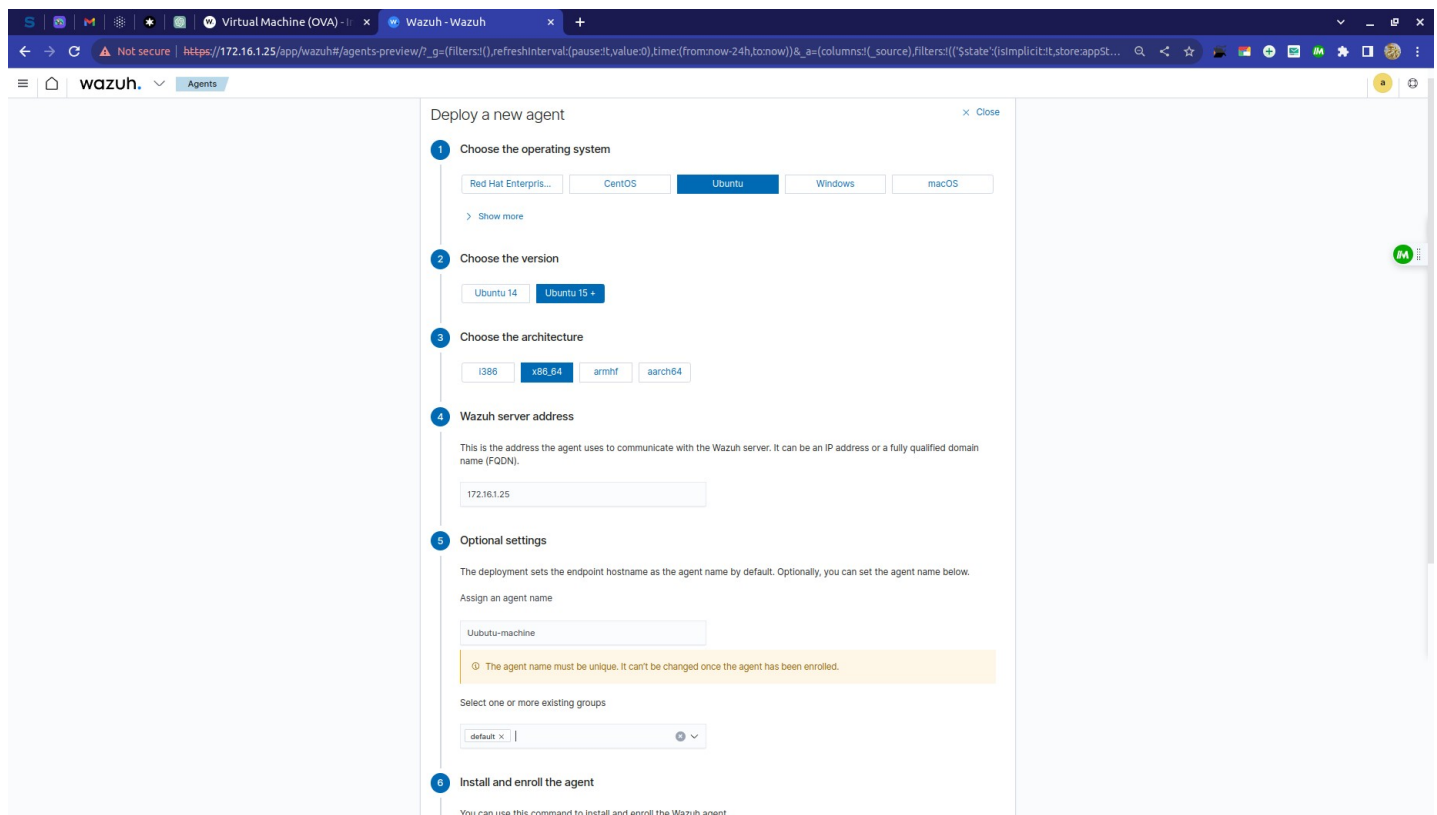
`/etc/wazuh-dashboard/opensearch_dashboards.yml`

and

`/usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml` for the Wazuh dashboard

ADDING AGENTS TO THE WAZUH SERVER

Click on agent to add the agents and select the appropriate machine you want to add. The images below show the steps:



The screenshot shows a web browser window with the Wazuh web interface. The browser's address bar displays the URL `https://172.16.1.25/app/wazuh#agents-preview/?_g=(filters:{},refreshInterval:(pause:{value:0},time:(from:now-24h,to:now)))&_a=(columns:{_source},filters:{('$state':{implicit:it.store.appSt...`. The Wazuh logo is visible in the top left corner, and the 'Agents' tab is selected. The main content area is titled 'Deploy a new agent' and contains a multi-step form:

- 1 Choose the operating system**
Buttons: Red Hat Enterpris..., CentOS, **Ubuntu**, Windows, macOS
Link: > Show more
- 2 Choose the version**
Buttons: Ubuntu 14, **Ubuntu 15**
- 3 Choose the architecture**
Buttons: i386, **x86_64**, armhf, aarch64
- 4 Wazuh server address**
Text: This is the address the agent uses to communicate with the Wazuh server. It can be an IP address or a fully qualified domain name (FQDN).
Input field: 172.16.1.25
- 5 Optional settings**
Text: The deployment sets the endpoint hostname as the agent name by default. Optionally, you can set the agent name below.
Text: Assign an agent name
Input field: Ubuntu-machine
Warning: ⚠ The agent name must be unique. It can't be changed once the agent has been enrolled.
Text: Select one or more existing groups
Dropdown menu: default x | v
- 6 Install and enroll the agent**
Text: You can use this command to install and enroll the Wazuh agent.

Virtual Machine (OVA) - Wazuh - Wazuh

Not secure | [https://172.16.1.25/app/wazuh#/agents-preview?_g=\[filters:\(\),refreshInterval:\(pause:0,value:0\),time:\(from:now-24h,to:now\)\]&_a=\(columns:\(_source\),filters:!\(\(\\$state?\)\[simplicit:it.store.appState\],...](https://172.16.1.25/app/wazuh#/agents-preview?_g=[filters:(),refreshInterval:(pause:0,value:0),time:(from:now-24h,to:now)]&_a=(columns:(_source),filters:!(($state?)[simplicit:it.store.appState],...)

wazuh. Agents

The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups

default x |

6 Install and enroll the agent

You can use this command to install and enroll the Wazuh agent.

If the installer finds another Wazuh agent in the system, it will upgrade it preserving the configuration.

```
curl -so wazuh-agent.deb https://packages.wazuh.com/deb/main/w/wazuh-agent/wazuh-agent_4.5.2-1_amd64.deb
&& sudo WAZUH_MANAGER=172.16.1.25 WAZUH_AGENT= Copy command WAZUH_AGENT_NAME=ubuntu-machine dpkg -i ./wazuh-agent.deb
```

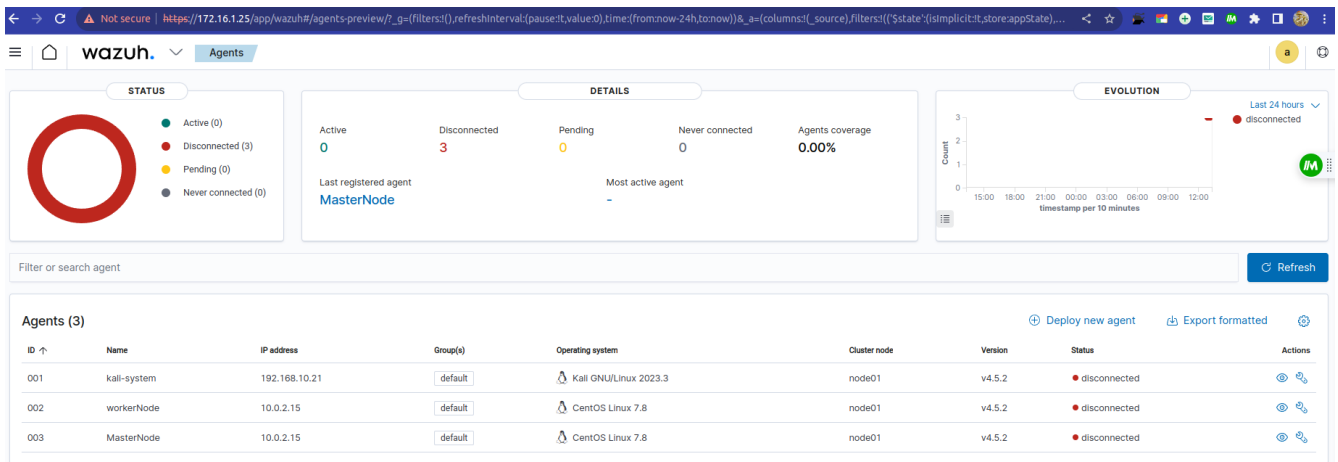
7 Start the agent

Systemd

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

To verify the connection with the Wazuh server, please follow this [document](#).

Copy paste the command and refresh the the wazuh dashboard. You will see the agent added.



Now you can monitor and find what are the vulnerabilities and much more with wazuh.

2. Wazuh deployment using Docker and Docker-compose

Docker and Docker compose can be used to install wazuh manger for SEIM

The below are the steps to use docker to install wazuh

Step1: Install docker and docker-compose using terminal:

sudo apt install docker.io docker-compose -y && sudo apt update

Note: If you are using rpm based linux use yum instead of apt.

Step 2: clone the wazuh from github

git clone <https://github.com/wazuh/wazuh-docker.git> -b v4.5.2

Step 3: Download the certificates

docker-compose -f generate-indexer-certs.yml run --rm generator

Step 4: Use docker-compose to download and install wazuh.

docker-compose up -d

Step 5: Find the IP of docker interface or host machine ip also works.

Ifconfig

ip a

Step 5: In the Browser type <https://ip-of-docker>

The default username is admin and password is SecretPassword use this to login to the wazuh dashboard.

Wazuh compliance:

Wazuh is a cybersecurity monitoring and intrusion detection system. It helps organizations keep an eye on their computer systems and networks to make sure they're safe from cyber threats. In the context of Wazuh:

1. HIPAA Compliance: Wazuh can be configured to monitor access to electronic health records and alert if there are any unauthorized attempts to access patient data, helping healthcare organizations meet HIPAA requirements.

2. PCI DSS: Wazuh can be set up to watch over the systems that handle credit card data, making sure they follow the PCI DSS rules and reporting any suspicious activities that could lead to a data breach.

3. NIST 800-53: Wazuh can implement security controls and checks based on the NIST guidelines, ensuring that the organization's systems comply with these high standards.

4. GPG13: If an organization needs to align with the GPG13 policy, Wazuh can be customized to enforce the necessary security measures to protect sensitive government information.

5. TSC (Threat and Security Controls): Wazuh is all about detecting and responding to threats, making it a valuable tool for implementing and monitoring various security controls to protect against cyber threats.

In addition to that, Wazuh is a versatile tool that can be used to meet the specific security and compliance needs of different organizations, including those related to HIPAA, PCI DSS, NIST 800-53, GPG13, and general threat and security controls.

