

## Introduction to Wazuh

**Wazuh** is an open-source security monitoring platform that provides comprehensive threat detection, visibility, and compliance monitoring capabilities. It is designed to help organizations detect and respond to security incidents in real-time, ensuring the integrity and security of their IT infrastructure.

### Key Features of Wazuh:

#### 1. Threat Detection and Response:

- **Real-time Monitoring:** Wazuh continuously monitors the security events generated by systems, applications, and network devices to detect suspicious activity and potential threats.
- **Intrusion Detection:** The platform includes Host Intrusion Detection System (HIDS) capabilities, using rules and anomaly detection methods to identify malicious behaviour.

#### 2. Log Data Analysis:

- **Log Collection:** Wazuh agents collect log data from various sources, including operating systems, applications, and cloud services.
- **Log Parsing and Analysis:** Collected logs are parsed, normalized, and analyzed to identify security incidents and compliance issues.

#### 3. File Integrity Monitoring (FIM):

- **Change Detection:** Wazuh monitors critical system files, directories, and configurations for unauthorized changes, alerting administrators of potential security breaches.

#### 4. Vulnerability Detection:

- **Vulnerability Assessment:** The platform scans systems for known vulnerabilities, providing detailed reports to help prioritize and remediate security risks.

#### 5. Configuration Assessment:

- **Security Policies:** Wazuh can enforce and validate security policies and configurations, ensuring systems comply with organizational and regulatory standards.

#### 6. Compliance Management:

- **Regulatory Compliance:** Wazuh helps organizations meet regulatory requirements such as GDPR, HIPAA, PCI DSS, and more by providing tools for continuous monitoring, reporting, and auditing.

#### 7. Integration and Extensibility:

- **SIEM Integration:** Wazuh integrates with Security Information and Event Management (SIEM) solutions like Elasticsearch and Kibana for advanced visualization and analysis.

- **API and Customization:** The platform offers APIs and customization options to extend its functionality and integrate with other security tools and workflows.

## Architecture of Wazuh:

### 1. Wazuh Agents:

- Installed on monitored endpoints (e.g., servers, workstations, cloud instances), agents collect and forward security data to the Wazuh server.

### 2. Wazuh Server:

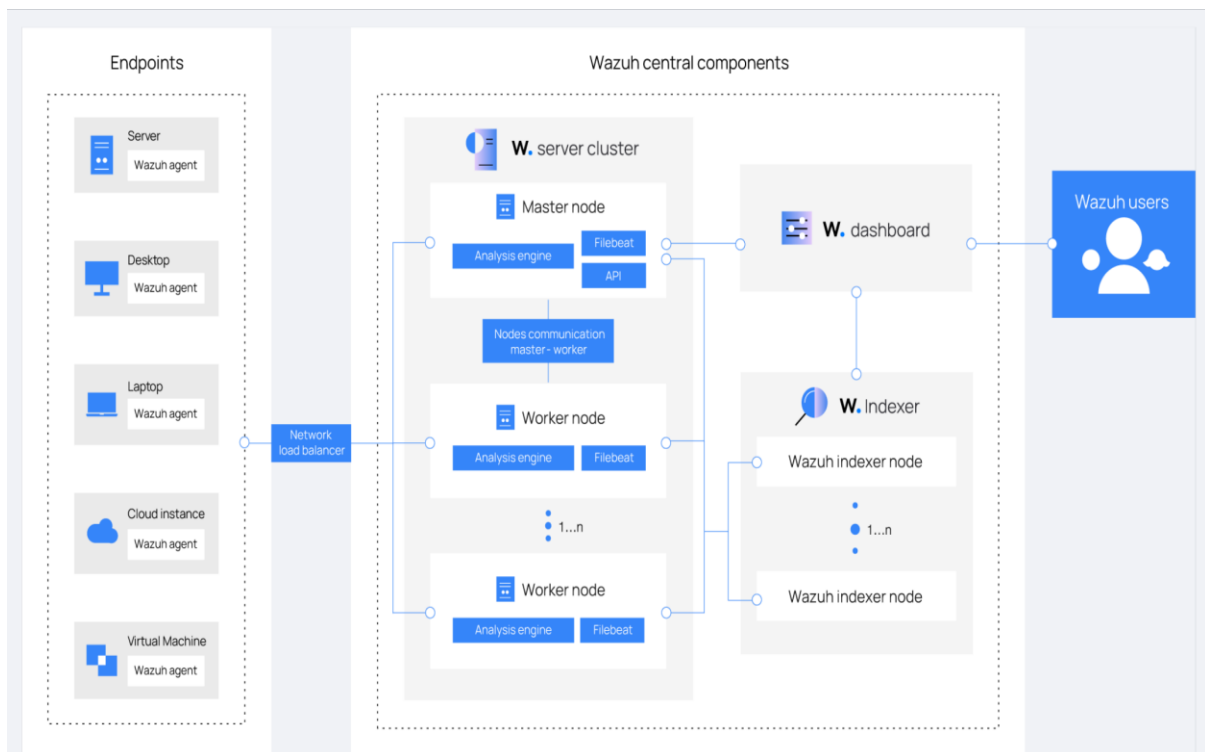
- The central component that processes data from agents, applying rules, performing analysis, and generating alerts.

### 3. Wazuh Manager:

- Manages configuration, policies, and coordination of agents, ensuring consistent monitoring and response across the environment.

### 4. Data Storage and Analysis:

- Wazuh typically integrates with Elasticsearch for storing and searching collected data, and with Kibana for visualizing and analysing security information.



## Installation Guide and Configuration in VMware Workstation 17 Player :

**Step 01:** Download Wazuh (.ova) file

Resource: <https://packages.wazuh.com/4.x/vm/wazuh-4.7.5.ova>

### **Difference between .iso and .ova**

An `.iso` file is an optical disc image file that contains the complete contents of a CD, DVD, or Blu-ray disc. It is a single file that represents the entire contents and structure of the disc.

(or)

An `.iso` file is like a digital copy of a CD, DVD, or Blu-ray disc

An `.ova` file (Open Virtualization Archive) is a package that contains a complete virtual machine (VM) in a single file. It is a tar archive file that typically contains an OVF (Open Virtualization Format) descriptor file, one or more disk images, and optional resource files.

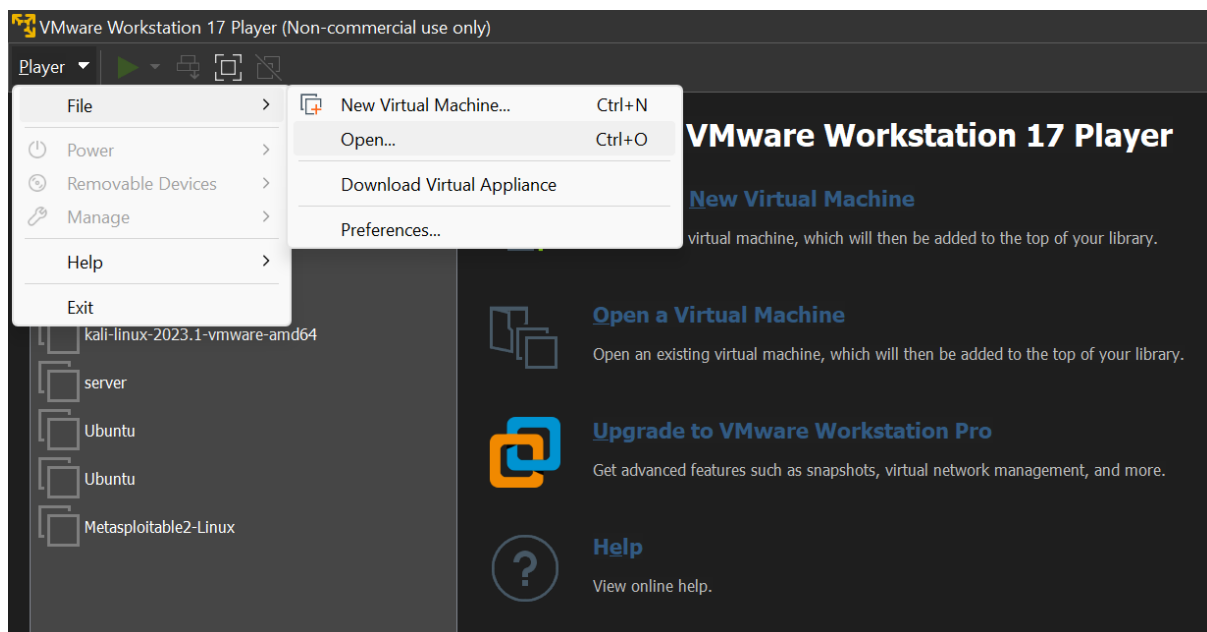
(or)

An `.ova` file is like a zip file that contains a whole virtual computer (virtual machine or VM).

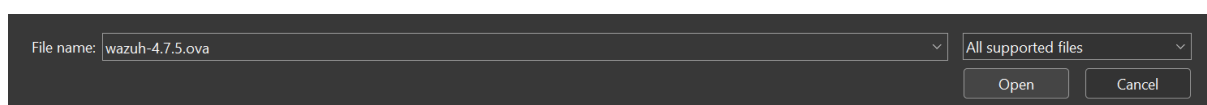
### **Step 02:**

In my case, I am using VMware Workstation 17 player.

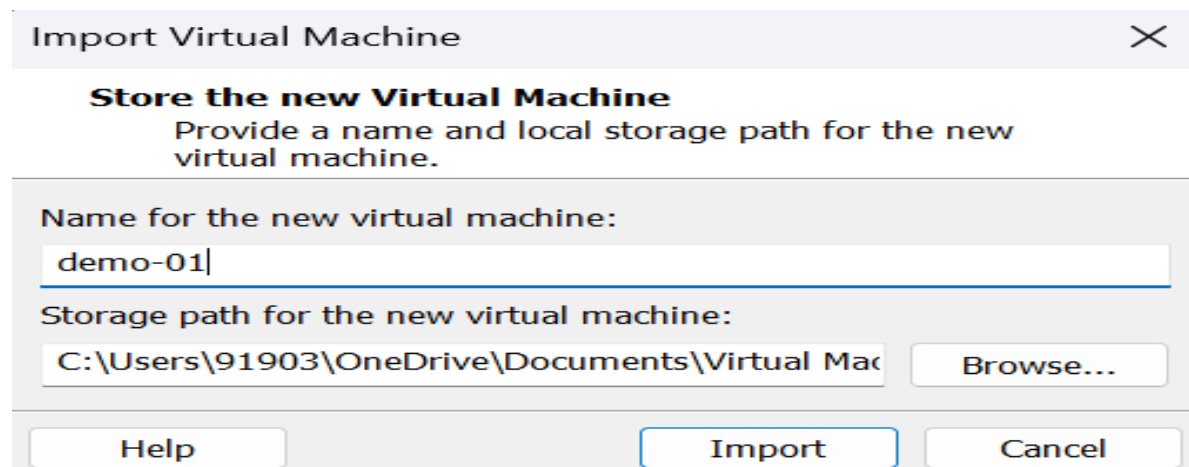
Click on Player → File → open → then locate and attach the .ova file



Attach the file and then click on open



Next, give any name to your virtual machine(in my case its demo-01 ) and then specify the path to download all its dependencies.

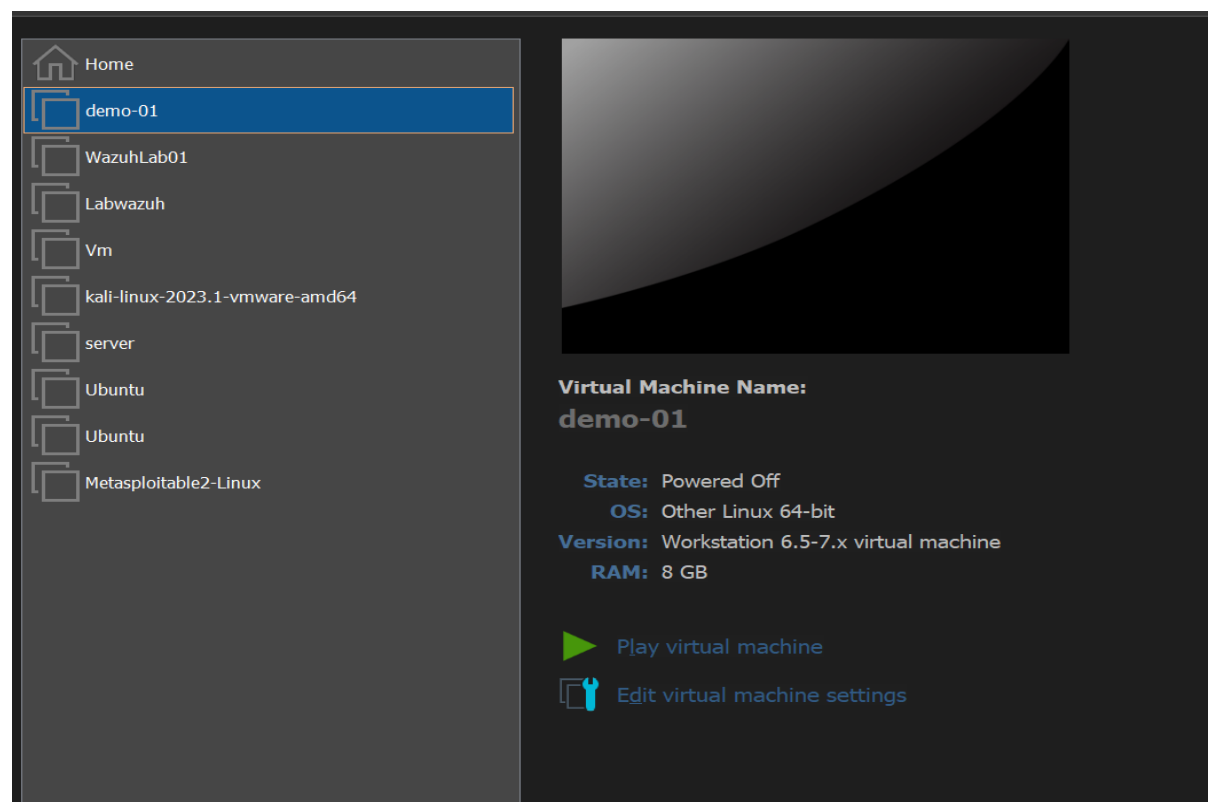


The screenshot shows the 'Import Virtual Machine' dialog box. At the top, it says 'Store the new Virtual Machine' and 'Provide a name and local storage path for the new virtual machine.' Below this, there are two input fields. The first is 'Name for the new virtual machine:' with the text 'demo-01' entered. The second is 'Storage path for the new virtual machine:' with the path 'C:\Users\91903\OneDrive\Documents\Virtual Mac' entered. To the right of the storage path field is a 'Browse...' button. At the bottom of the dialog are three buttons: 'Help', 'Import', and 'Cancel'.

Next, you'll get a pop up



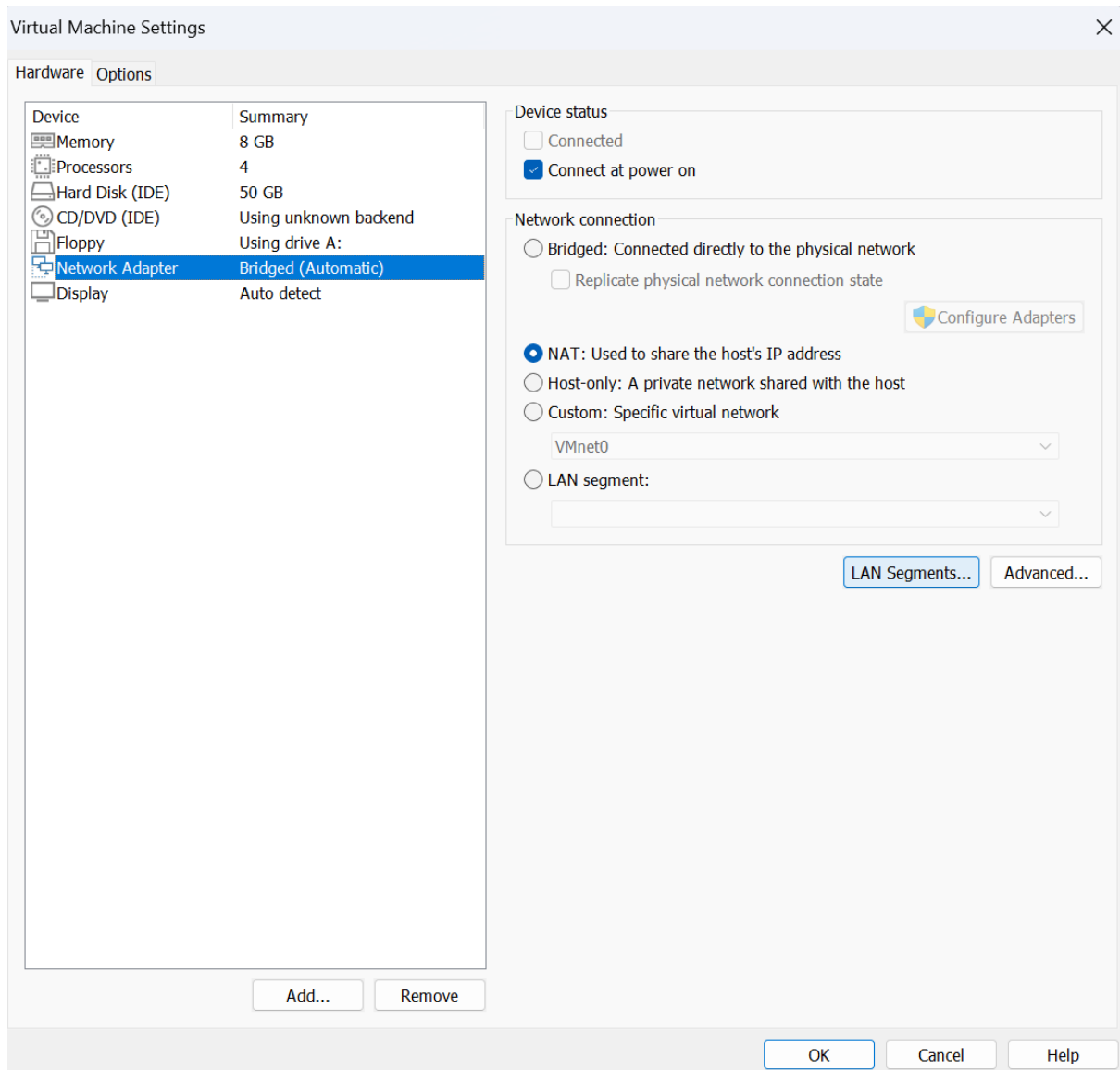
Next, you can see the virtual machine ready



Click on, edit virtual Machine settings and customize based on your requirements.

Next, click on network adapter and under network connections,

change from **Bridged network** type to NAT and then click on “ Ok ”



After modifying the settings, click on “play virtual machine”, then your virtual machine starts booting up.

After booting up, you will be prompted with authentication to login as shown

```

Welcome to the Wazuh OVA version
Wazuh - 4.7.5
Login credentials:
  User: wazuh-user
  Password: wazuh

wazuh-server login:

```

**Note:**

The default username and password for login are:

Username : wazuh-user

Password : wazuh

After successful authentication, you will get this interface

[illegible]

Now, check for your ipv4 address, by typing command "ifconfig"

```
[wazuh-user@wazuh-server ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.198.130 netmask 255.255.255.0 broadcast 192.168.198.255
    inet6 fe80::20c:29ff:fea8:8cf6 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:a8:8c:f6 txqueuelen 1000 (Ethernet)
    RX packets 13354 bytes 15301658 (14.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 15806 bytes 20067082 (19.1 MiB)
    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 47194 bytes 4460925 (4.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 47194 bytes 4460925 (4.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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

Now, Check if SSH is running on Wazuh,

Here I have taken another kali vm to check SSH is running on Wazuh (you can use any flavour of your choice)

Type the command:

Sudo nmap -p22 -sV 192.168.198.130 {in kali linux}.

After typing this cmd, you can see the host is up and running

```
(kali㉿kali)-[~]
$ sudo nmap -p22 -sV 192.168.198.130
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-07 13:38 EDT
Nmap scan report for 192.168.198.130
Host is up (0.0019s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
MAC Address: 00:0C:29:A8:8C:F6 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.32 seconds
```

← → ↺ Not secure https://192.168.198.130/app/login? ☆ 📄 🔄 ⌚

# wazuh.

The Open Source Security Platform

Username
  Password

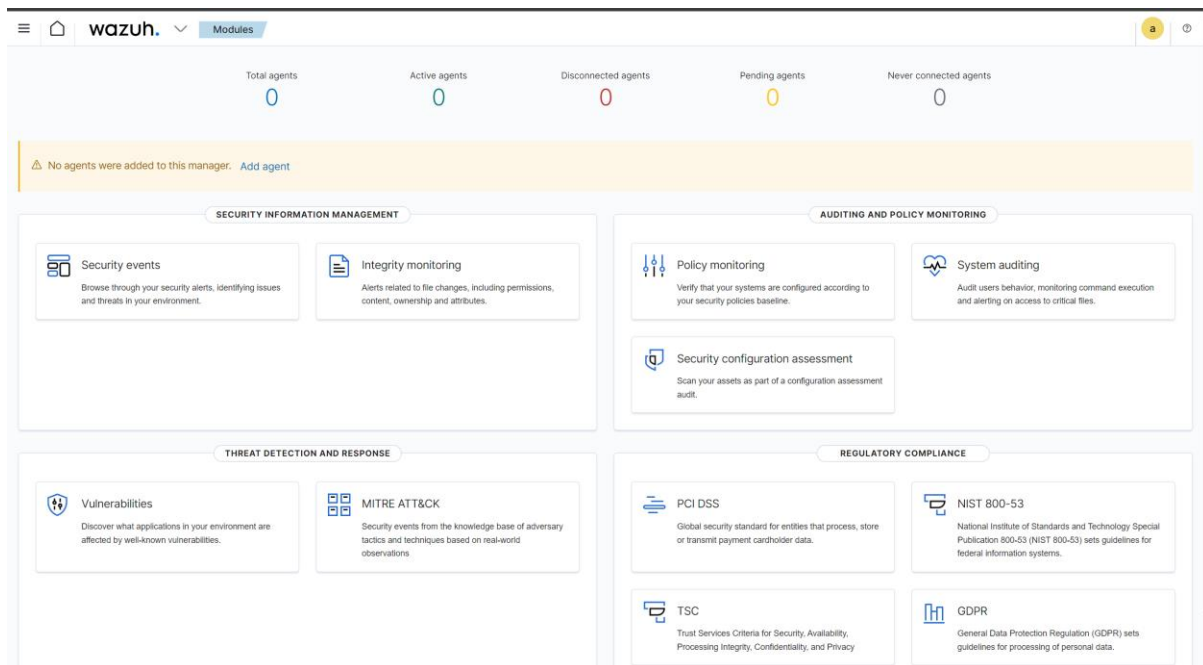


Default login credentials are

Username : admin

Password : admin

After authentication, it redirects to your Wazuh dashboard



Additionally, if you want to assign static IP Address to your Wazuh Server

Step 01: Check your current IP address by typing the command “ **ifconfig** ”

```
[wazuh-user@wazuh-server ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.198.132 netmask 255.255.255.0 broadcast 192.168.198.255
    inet6 fe80::20c:29ff:fe5:3eac prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f5:3e:ac txqueuelen 1000 (Ethernet)
    RX packets 575 bytes 670077 (654.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 302 bytes 22497 (21.9 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 1056 bytes 147420 (143.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1056 bytes 147420 (143.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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

You can see, my current IPv4 address is **192.168.198.132**

Now access the configuration file “ ifcfg-eth0 ”

```
[wazuh-user@wazuh-server ~]$ sudo -i
[root@wazuh-server ~]# cd /
[root@wazuh-server /]# cd etc
[root@wazuh-server etc]# cd sysconfig
[root@wazuh-server sysconfig]# cd network-scripts/
[root@wazuh-server network-scripts]# nano ifcfg-eth0
```

This is the default configuration

```
GNU nano 2.9.8 ifcfg-eth0
# Automatically generated by the VM import process
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
NM_CONTROLLED=no

[ Read 6 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
```

Now, check for the routing information

```
[root@wazuh-server network-scripts]# route -n
Kernel IP routing table

```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.198.2	0.0.0.0	UG	0	0	0	eth0
169.254.0.0	0.0.0.0	255.255.0.0	U	1002	0	0	eth0
192.168.198.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0

```
[root@wazuh-server network-scripts]#
```

As you can see my routing info as

Gateway : 192.168.198.2

Genmask : 255.255.255.0

Now, add these like in the configuration file

```
GNU nano 2.9.8 ifcfg-eth0 Modified
# Automatically generated by the vm import process
#DEVICE=eth0
#ONBOOT=yes
#BOOTPROTO=dhcp
#TYPE=Ethernet
#NM_CONTROLLED=no

DEVICE=eth0
ONBOOT=yes
BOOTPROTO=none
TYPE=Ethernet
NM_CONTROLLED=no
PREFIX=24
IPADDR=192.168.198.126
GATEWAY=198.168.198.2
DNS1=192.168.198.2
DNS2=192.168.198.2

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

In, IPADDR → you can give any IP address that you want.

Now, save the file (ctrl+O,)save the changes → enter(save the file name) → ctrl+y (exit)

Now, try to restart the network

Command: `sudo systemctl restart network`

```
[root@wazuh-server network-scripts]# sudo systemctl restart network
[ 1210.001417] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[ 1210.006342] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: N
one
[ 1210.010296] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[root@wazuh-server network-scripts]#
```

After, successful restart.

Type command: “ `ifconfig` ” and check, the assigned IP Address will get updated

```
[root@wazuh-server network-scripts]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.198.126 netmask 255.255.255.0 broadcast 192.168.198.255
    inet6 fe80::20c:29ff:fe5:3eac prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f5:3e:ac txqueuelen 1000 (Ethernet)
    RX packets 779 bytes 684279 (668.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 581 bytes 41435 (40.4 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 8155 bytes 816917 (797.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8155 bytes 816917 (797.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@wazuh-server network-scripts]#
```

Now, access the dashboard with any browser by typing IP Address in the URL

<https://192.168.198.126>

