

Wazuh- SIEM Tool

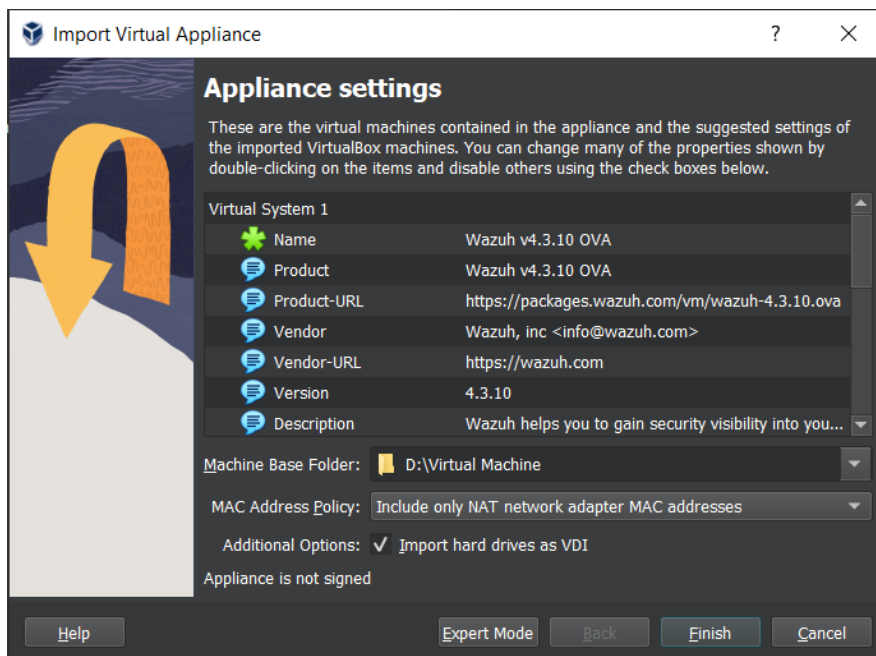
Security Information and Event Management (SIEM) is a comprehensive cybersecurity solution that combines two key aspects: Security Information Management (SIM) and Security Event Management (SEM). SIEM systems are designed to provide real-time analysis of security alerts generated by applications and network hardware, allowing organizations to detect, analyze, and respond to potential security threats swiftly. By collecting and aggregating data from various sources, such as network devices, servers, and applications, SIEM systems enable the identification of unusual or suspicious activities. Advanced SIEM tools often incorporate machine learning and behavioral analytics to enhance threat detection capabilities. They also facilitate compliance with regulatory requirements by providing detailed reporting and audit trails. Overall, SIEM is an essential component of a robust cybersecurity strategy, offering visibility, intelligence, and automated responses to safeguard an organization's digital assets.

Wazuh is an open-source security monitoring and threat detection platform that provides comprehensive visibility into an organization's security posture. It integrates log analysis, intrusion detection, vulnerability detection, configuration assessment, and incident response capabilities into a unified solution. Wazuh collects and

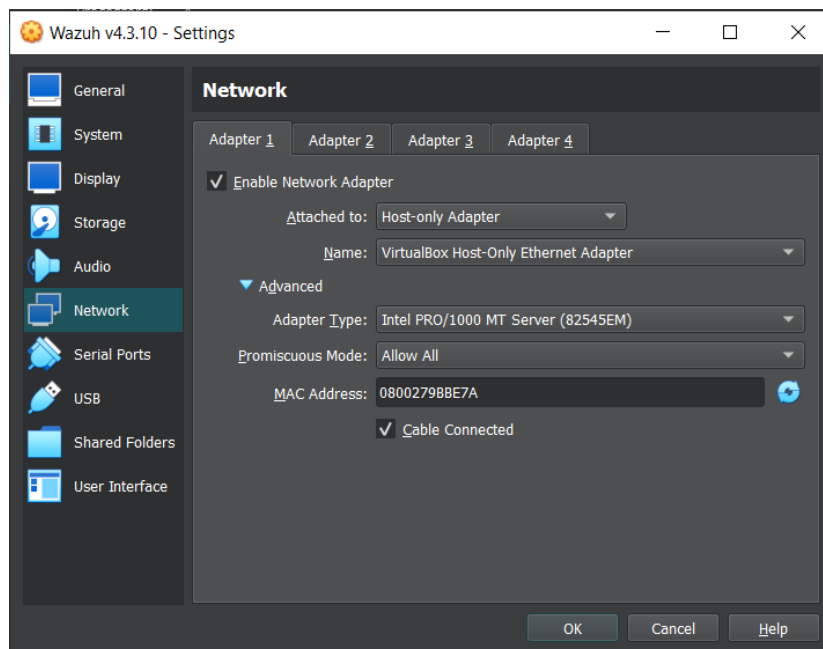
analyzes data from various sources, including endpoints, servers, and network devices, enabling real-time detection of security events and anomalies. With its scalable architecture, Wazuh can be deployed in large, distributed environments, offering centralized management and monitoring. It also features a rich set of integrations with other security tools and platforms, enhancing its flexibility and effectiveness. By leveraging Wazuh, organizations can improve their security operations, achieve compliance with regulatory standards, and protect their digital assets from evolving cyber threats.

Examples: -

1. Download wazuh .ova file from wazuh documentation.



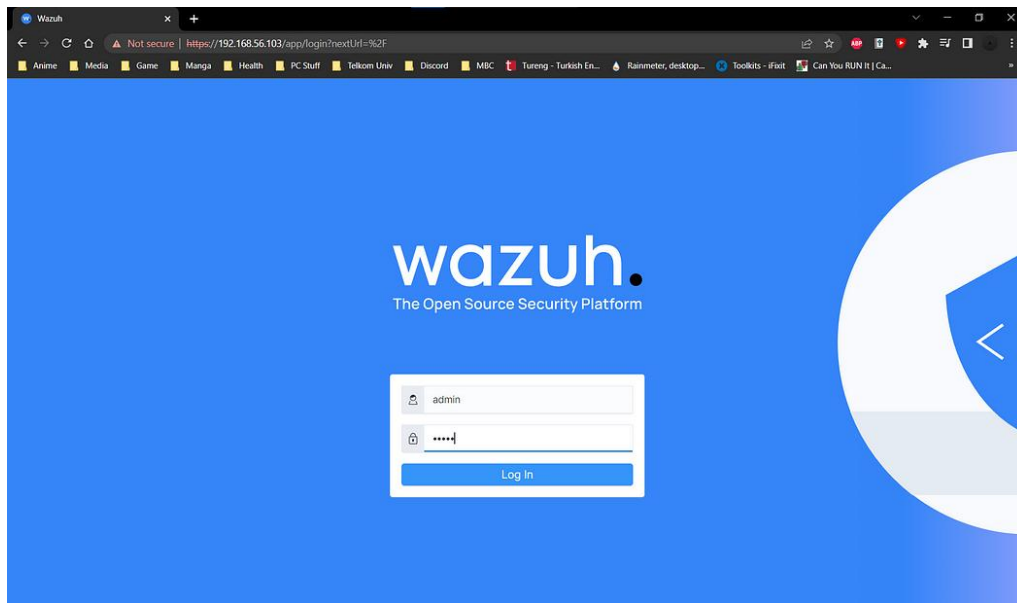
2. After the machine has finished installing, go to the machine settings and change the network adapter to 'host-only Adapter'.



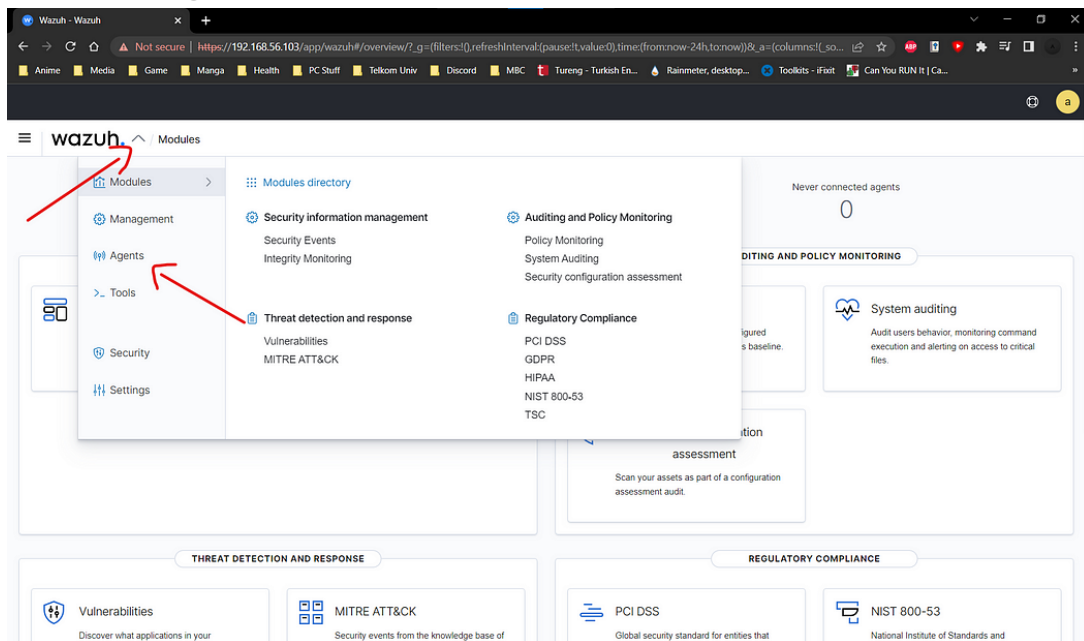
3. Now we can fire up wazuh virtual machine and login as wazuh-user with password wazuh and type ip a to display the IP of your wazuh virtual machine.

```
[wazuh-user@wazuh-server ~]$ ip a
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 08:00:27:9b:be:7a brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.103/24 brd 192.168.56.255 scope global dynamic eth0
        valid_lft 588sec preferred_lft 588sec
    inet6 fe80::a00:27ff:fe9b:be7a/64 scope link
        valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]$
```

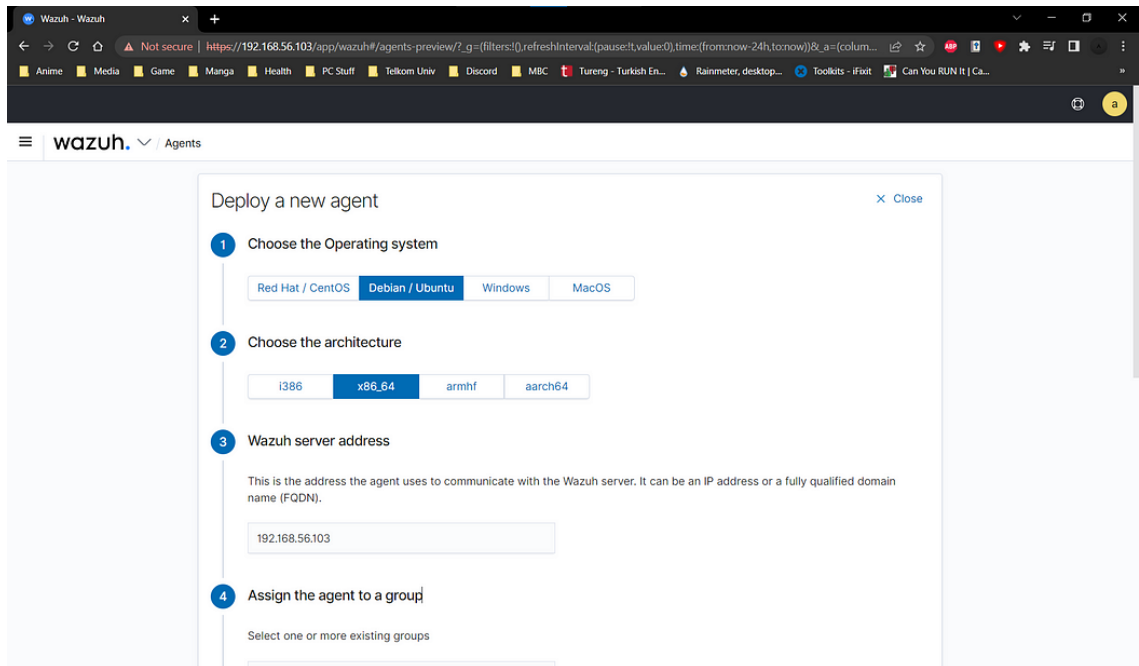
4. Type in your local browser the IP on to your browser.



5. When you got inside of your wazuh dashboard, you will be greeted with a lot of button and function that you don't know, but you can learn about all of it from the documentation, for now you can click on total agent or click on agent inside the arrow.



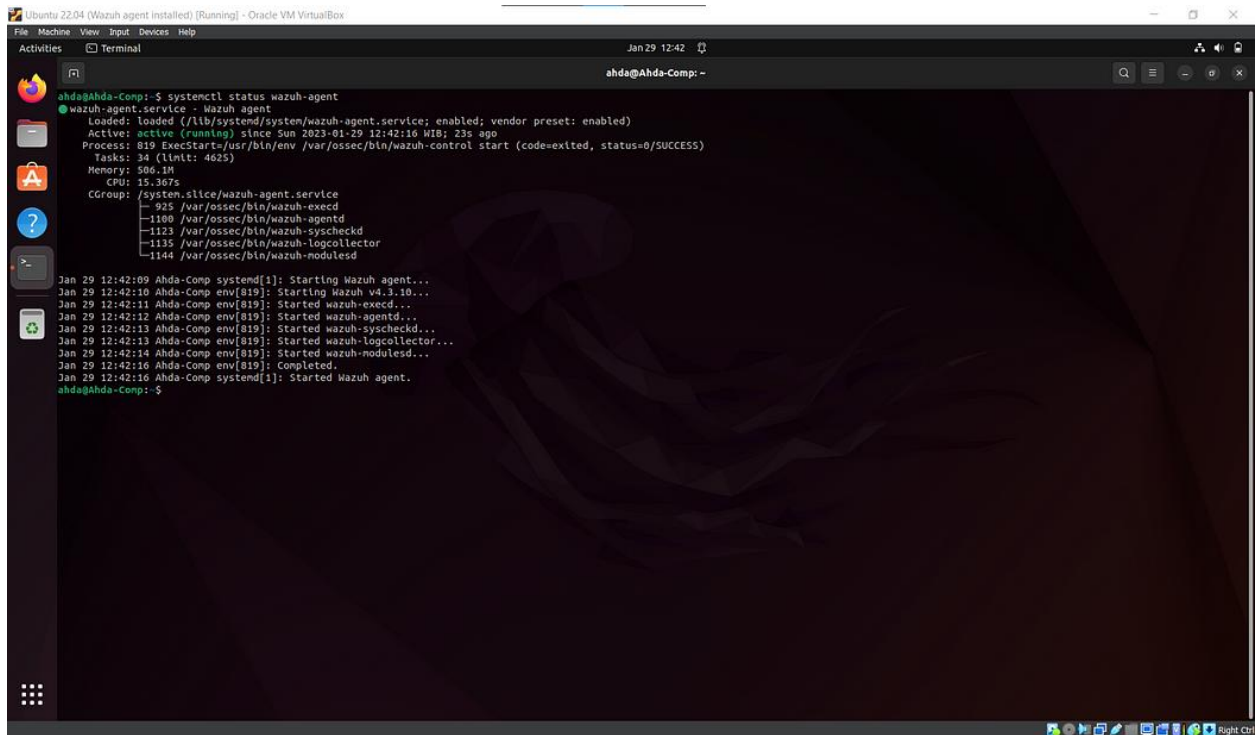
6. You will need to choose the operating system to deploy your wazuh agent and insert the IP for your WAZUH MANAGER.



The screenshot shows a web browser window with the Wazuh web interface. The browser's address bar shows a URL starting with `https://192.168.56.103/app/wazuh#/agents-preview/?_g=(filters:[]&refreshInterval:(pause:0,value:0)&time:(from:now-24h,to:now))&a=(column...`. The Wazuh logo and 'Agents' tab are visible in the top navigation bar. A modal window titled 'Deploy a new agent' is open, featuring a close button in the top right corner. The modal contains four steps:

- 1 Choose the Operating system**: A horizontal selection bar with four options: 'Red Hat / CentOS', 'Debian / Ubuntu' (which is selected and highlighted in blue), 'Windows', and 'MacOS'.
- 2 Choose the architecture**: A horizontal selection bar with four options: 'i386', 'x86_64' (which is selected and highlighted in blue), 'armhf', and 'aarch64'.
- 3 Wazuh server address**: A text input field containing the IP address '192.168.56.103'. Below the input field, a small text note states: '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).'.
- 4 Assign the agent to a group**: A text input field with the placeholder text 'Select one or more existing groups'.

7. On the 5th option there are Install and enroll agent option, copy and paste the command onto your desire machine, in this case it's Ubuntu 22.04. Follow the next instruction and you should see that the agent already online.



```
ahda@Ahda-Comp:~$ systemctl status wazuh-agent
wazuh-agent.service - Wazuh agent
Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor preset: enabled)
Active: active (running) since Sun 2023-01-29 12:42:16 M18; 23s ago
Process: 819 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
Tasks: 34 (limit: 4625)
Memory: 506.1M
CPU: 15.367s
CGroup: /system.slice/wazuh-agent.service
├─ 925 /var/ossec/bin/wazuh-execd
├─ 1180 /var/ossec/bin/wazuh-agentd
├─ 1123 /var/ossec/bin/wazuh-syscheckd
├─ 1135 /var/ossec/bin/wazuh-logcollector
└─ 1144 /var/ossec/bin/wazuh-modulesd

Jan 29 12:42:09 Ahda-Comp systemd[1]: Starting Wazuh agent...
Jan 29 12:42:10 Ahda-Comp env[819]: Starting Wazuh v4.3.10...
Jan 29 12:42:11 Ahda-Comp env[819]: Started wazuh-execd...
Jan 29 12:42:12 Ahda-Comp env[819]: Started wazuh-agentd...
Jan 29 12:42:13 Ahda-Comp env[819]: Started wazuh-syscheckd...
Jan 29 12:42:13 Ahda-Comp env[819]: Started wazuh-logcollector...
Jan 29 12:42:14 Ahda-Comp env[819]: Started wazuh-modulesd...
Jan 29 12:42:16 Ahda-Comp env[819]: Completed.
Jan 29 12:42:16 Ahda-Comp systemd[1]: Started Wazuh agent.
ahda@Ahda-Comp:~$
```