



AARON JOSEPH-
KHAMA

ITS01ERA intern
SOC team beta

Linkdein Profile:

<http://www.linkedin.com/in/aaronjosephkhama/>

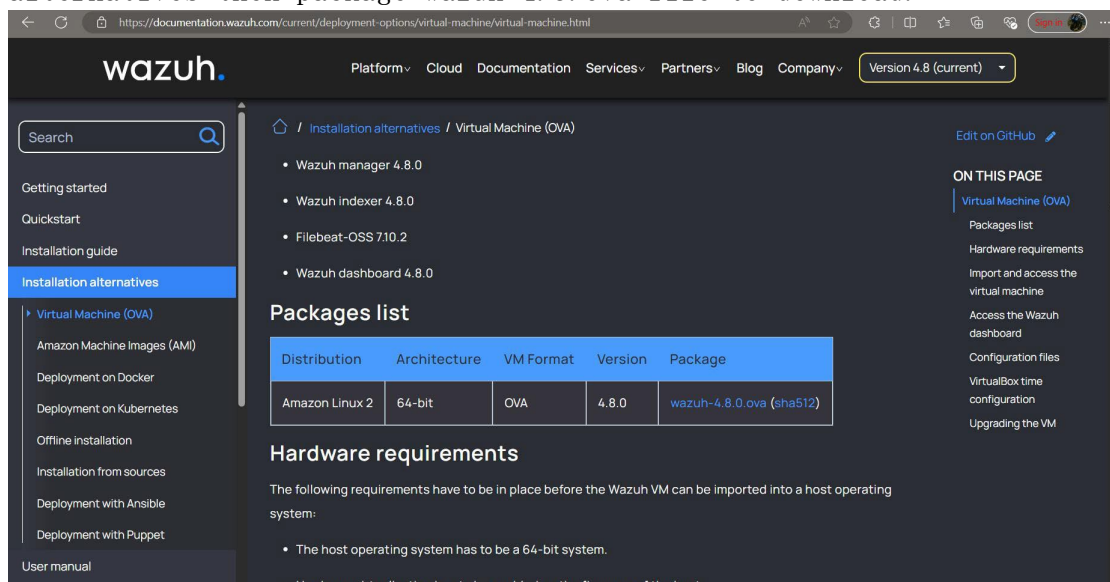
Lab Task Installation Process to Dashboard of Wazuh

1.) Download the virtualbox from official site. Click Windows Hosts for windows platform.






[Downloads - Oracle VM VirtualBox](#)

2.) After that go to wazuh official web page and click Installation alternatives then package wazuh-4.8.ova file to download.

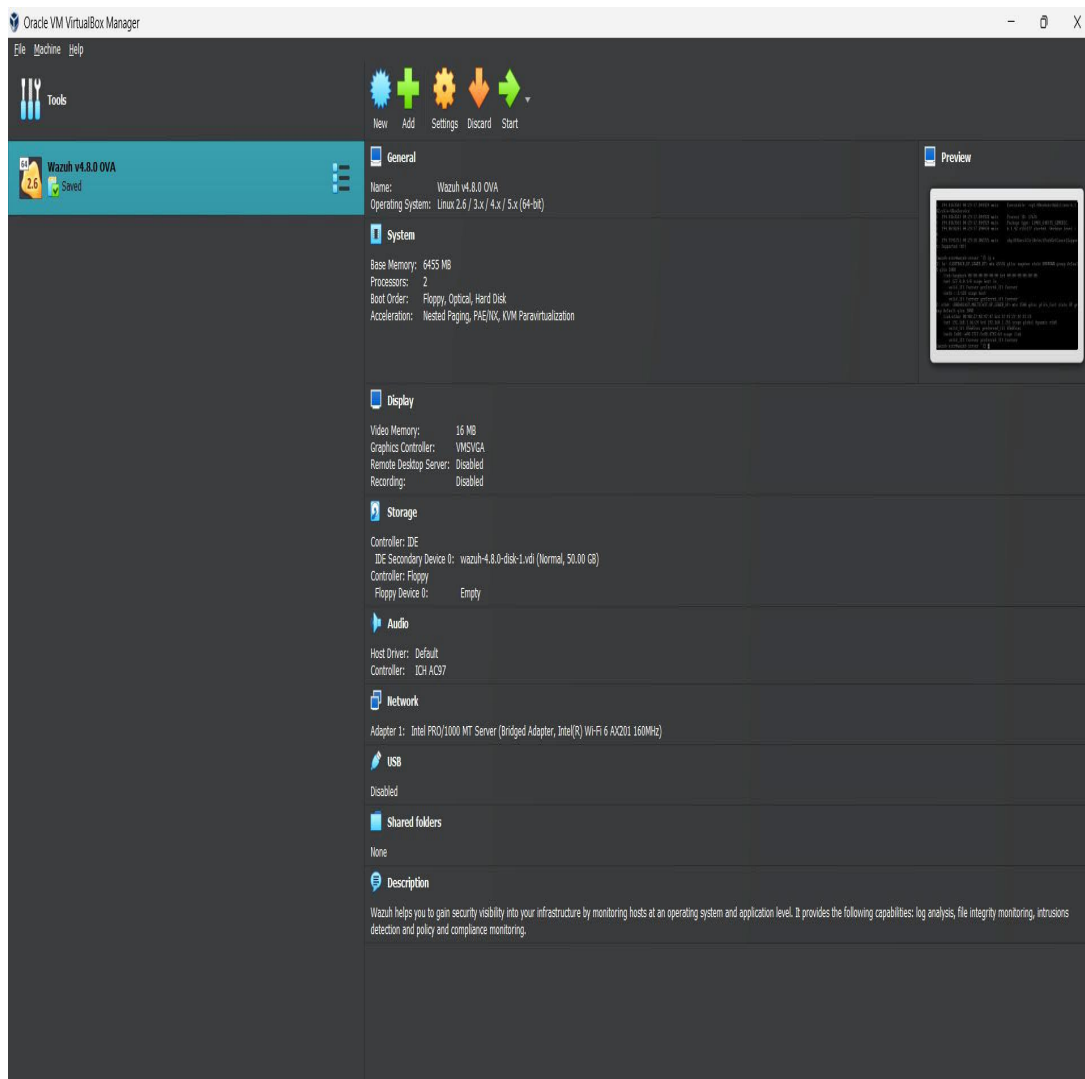


[Virtual Machine \(OVA\) - Installation alternatives \(wazuh.com\)](#)

3.) Wazuh-4.8.0 will be in download folder

	VirtualBox-7.0.18-162988-Win	6/29/2024 4:49 PM	Application	107,130
	wazuh-4.8.0	6/29/2024 12:24 PM	Open Virtualizatio...	4,131,51
	kali-linux-2024.2-installer-amd64 (1)	6/29/2024 11:57 AM	ISO File	4,212,05

4.) After installing virtualbox, import the ova file here and do all the setting as in the image. Change processor, physical memory if low storage and graphic controller.



5.) After that turn on virtual machine



6.) Booting up

```
early console in extract_kernel
input_data: 0x000000000313e3b4
input_len: 0x000000000062488d
output: 0x0000000001000000
output_len: 0x0000000001b3fa90
kernel_total_size: 0x0000000002787000

Decompressing Linux... Parsing ELF... done.
Booting the kernel.
```

7.) User name and password already mentioned when ova file is downloaded. In the documentation it is also mentioned.

```
Welcome to the Wazuh OVA version
Wazuh - 4.8.0
Login credentials:
  User: wazuh-user
  Password: wazuh

wazuh-server login:
```

[illegible]

WAZUH Open Source Security Platform
<https://wazuh.com>

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

8.) Note Inet IP for future.

```
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 77 bytes 4428 (4.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 77 bytes 4428 (4.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[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 08:00:27:48:47:47 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.66/24 brd 192.168.1.255 scope global dynamic eth0
        valid_lft 86344sec preferred_lft 86344sec
    inet6 fe80::a00:27ff:fe48:4747/64 scope link
        valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]#
```

9.) Check using nmap if ssh configuration is needed. If it is open and showing no configuration is further needed.

```
(alnewolf@kali)-[~]
└─$ sudo nmap -sV -p22 192.168.1.66
[sudo] password for alnewolf:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-30 00:30 EDT
Nmap scan report for 192.168.1.66
Host is up (0.0026s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.39 seconds

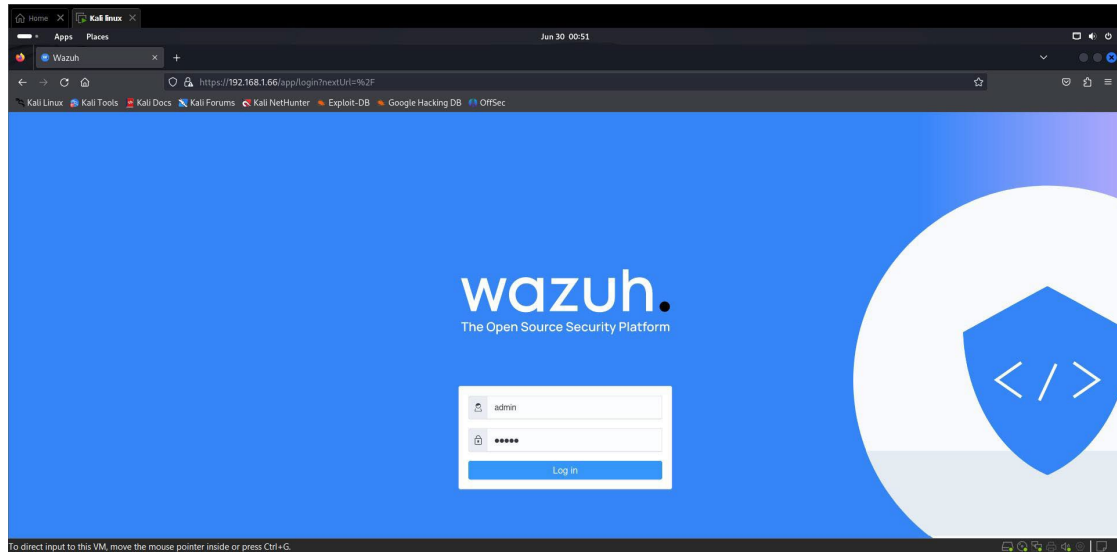
(alnewolf@kali)-[~]
└─$
```

[illegible]

```
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Sat 2024-06-29 05:40:06 EDT; 8s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 3959 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 3961 (sshd)
    Tasks: 1 (limit: 2229)
   Memory: 1.3M (peak: 1.6M)
      CPU: 91ms
   CGroup: /system.slice/ssh.service
           └─3961 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jun 29 05:40:06 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server:
Jun 29 05:40:06 kali sshd[3961]: Server listening on 0.0.0.0 port 22.
Jun 29 05:40:06 kali sshd[3961]: Server listening on :: port 22.
Jun 29 05:40:06 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server:
~
~
~
~
```


12.) Wazuh dashboard can be accessed by typing the IP in the browser. Username and password mentioned in documentation.



13.) DashBoard of Wazuh

