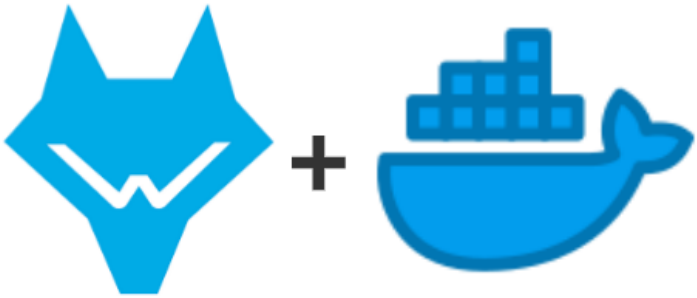
Build Open Source SIEM HA Using Wazuh + Docker Swarm *by : Ardita*

SUMMARY



Wazuh is a free and open source platform for threat detection, security monitoring, incident response and regulatory compliance. It can be used to monitor endpoints, cloud services and containers, and to aggregate and analyze data from external sources. *(source : wazuh docs)*

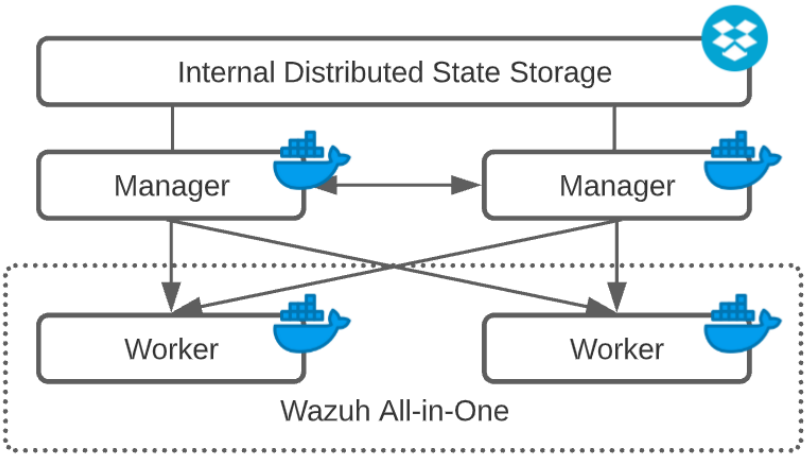
One of the wazuh functions can be used to detect brute-force attacks. Brute forcing SSH (on Linux) or RDP (on Windows) are common attack vectors. Wazuh provides out-of-the-box rules capable of identifying brute-force attacks by correlating multiple authentication failure events.

PREREQUISITES

For All-in-One Deployment :

1. **Operating system** (Amazon Linux 2, CentOS 7 and later, Debian 8 ELTS and later, Fedora Linux 31 and later, openSUSE Tumbleweed, Leap 15.2 and later, Oracle Linux 6 Extended and later, Red Hat Enterprise Linux 6 ELS and later, Ubuntu 14.04 ESM and later)
2. Min 4GB of **RAM**
3. Min 2 **CPU** cores
4. **Docker**
5. **Portainer** (Optional: for manage docker via dashboards)

DOCKER SWARM TOPOLOGY



ACTION

Note : Assuming docker and portainer have been installed !

Install Wazuh All-in-One

1. Clone wazuh repository to your system using git, current wazuh stable version on official documentation is v4.2.5.

```
git clone https://github.com/wazuh/wazuh-docker.git -b v4.2.5 --depth=1
```

2. Move to wazuh-docker directory.

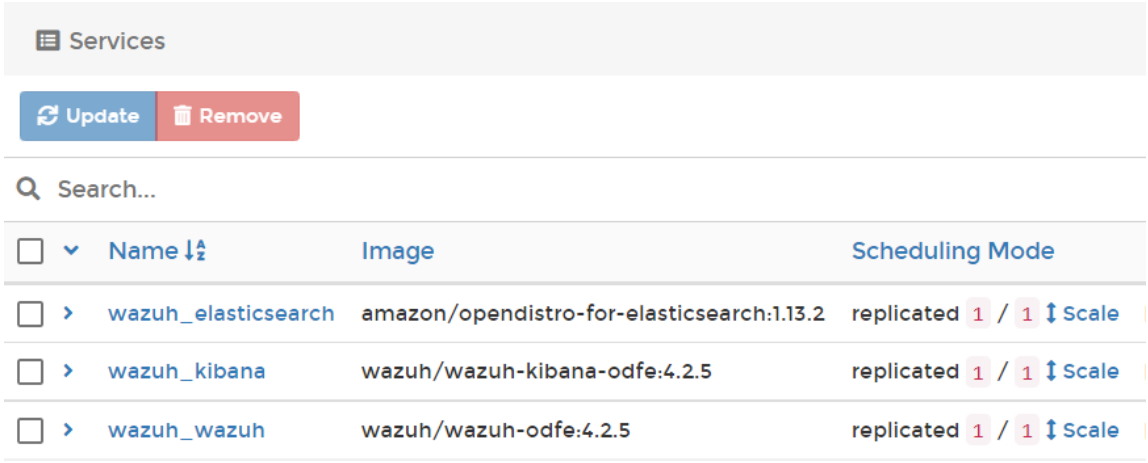
```
cd wazuh-docker/
```

3. Deploy wazuh All-in-One using Docker Swarm stack deploy, it will be distributed on all docker worker nodes.

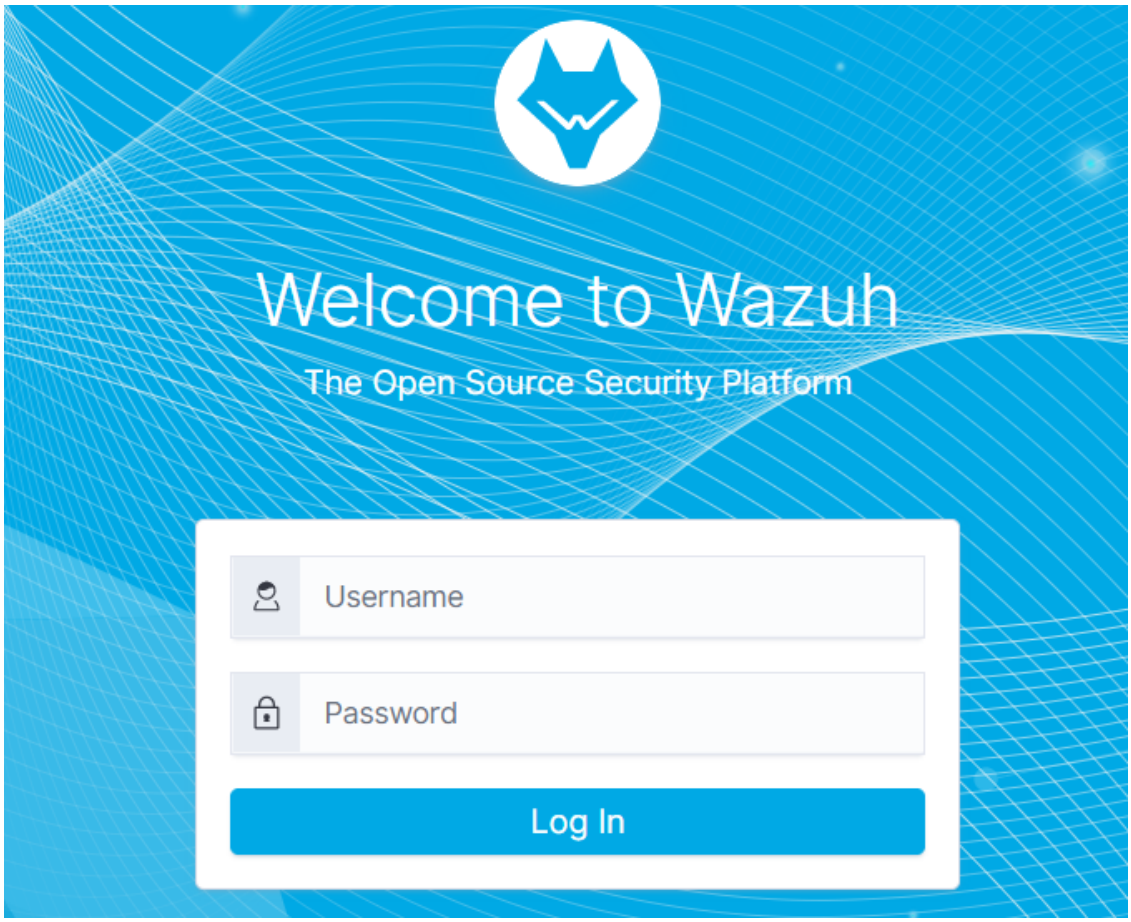
```
docker stack deploy -c docker-compose.yml Wazuh
```

4. Check wazuh service is available on docker swarm via CLI or Portainer.

```
[root@docker01 wazuh-docker]# docker service ls
ID             NAME                MODE         REPLICAS
je73cnm5hf3s   jenkins             replicated   1/1
n93yld65vbe9   portainer_agent     global       2/2
ycdhorwvv3jd   portainer_portainer replicated   1/1
u2x3bol7pocj   wazuh_elasticsearch replicated   1/1
nrbdy3ioe90s   wazuh_kibana        replicated   1/1
u765wypkvcao   wazuh_wazuh         replicated   1/1
```

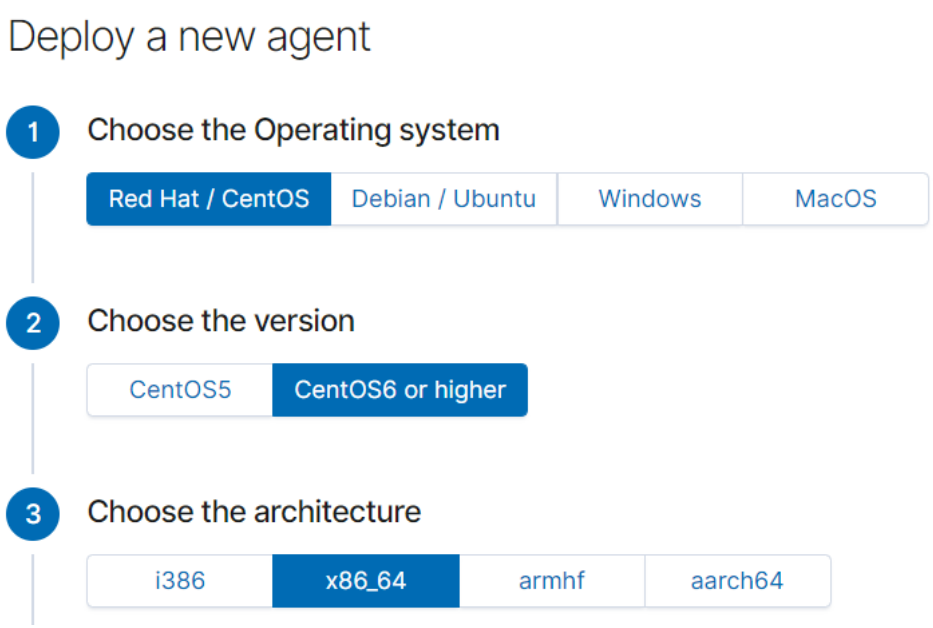


5. Access wazuh dashboards, the default **user** is **admin** and **password** is **admin**.

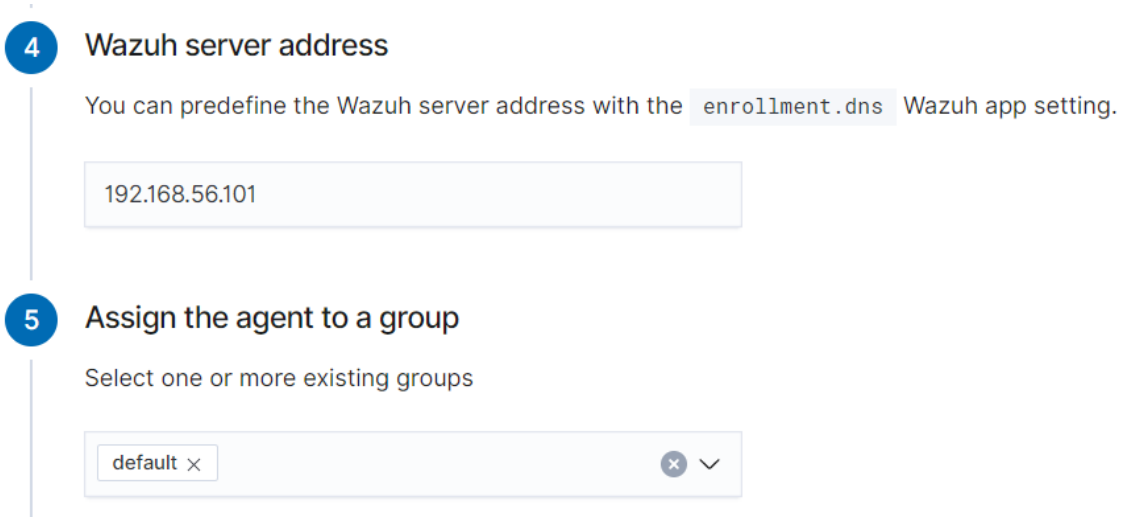


6. Install wazuh agent on an example Linux server using script on Wazuh > Agents > Deploy New Agent.

7. Choose the operating system, version, and architecture based on the server that will be monitoring.



8. Define wazuh server address (can be predefined on setting) and assign the agent to a group (the default group is default).

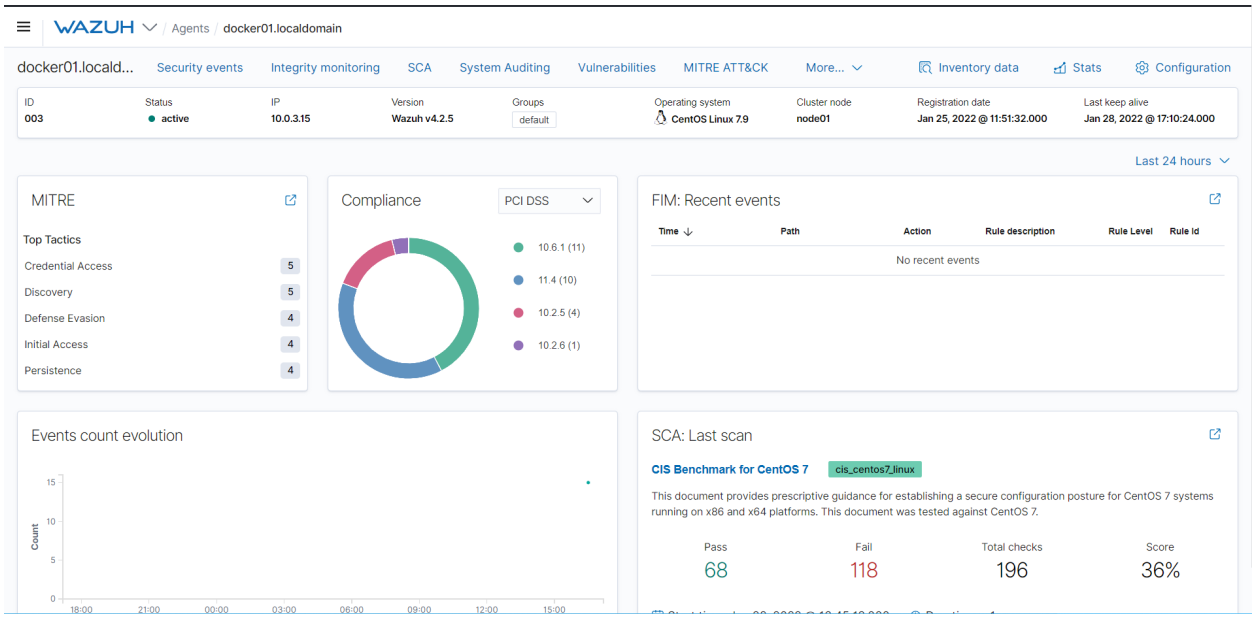


9. Wazuh will be create a simple script, run on the server that will be monitoring and reload the service.
10. Check on dashboards.

RESULTS

Wazuh Dashboards

Wazuh has very complex dashboards, we can use benchmark functions, security events, inventory data and others to create monitoring on the server. One of the functions is to detect brute force attacks.



How to detect a brute-force ?

We can use brute-force attack tools such as hydra for a demo.

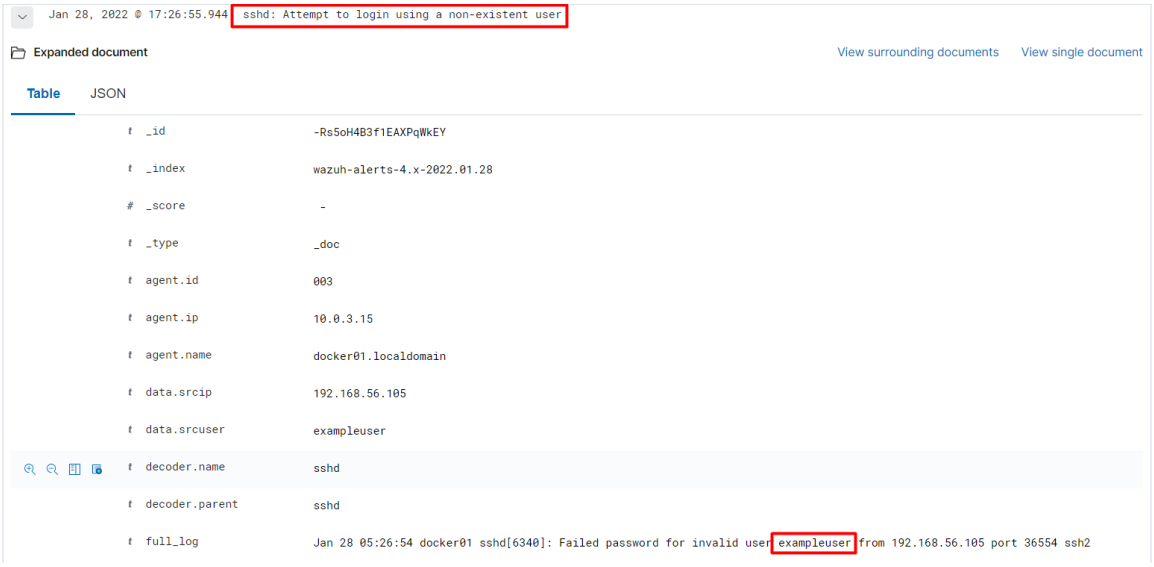
1. Install hydra tools or use pentest operating systems such as Kali Linux.

```
yum install -y hydra
```

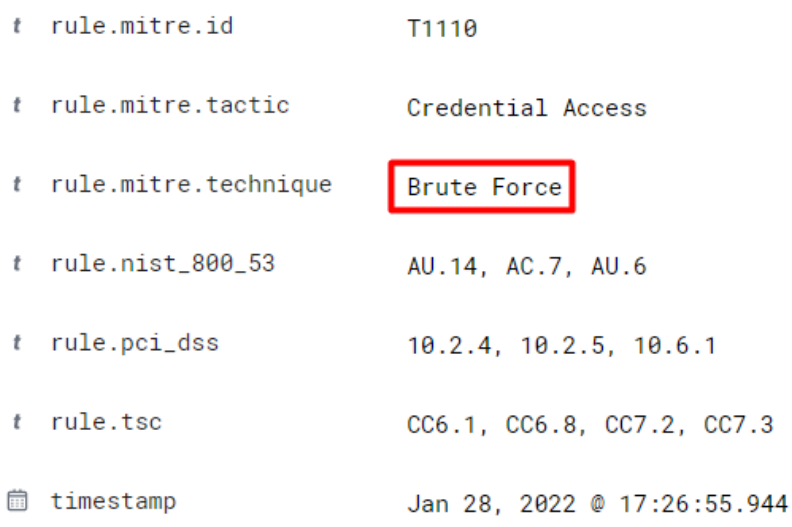
2. Run hydra command for brute-force attack.

```
hydra -l exampleuser -p wrong_password 192.168.56.101 ssh
```

3. Check on wazuh dashboards > discover, user exampleuser will try to login and wazuh create log for this action.



4. In the next section, wazuh defines this action based on MITRE RULE as a brute-force attack.



5. Next step we will try to make a reporting dashboard, See You...

NOTES

https://docs.docker.com/engine/swarm/

https://documentation.wazuh.com/current/getting-started/index.html

https://documentation.wazuh.com/current/proof-of-concept-guide/detect-brute-force-attack.html