



DEPLOYING WAZUH ON THE VIRTUAL MACHINE

Redback Operations

Document Owner: Cyber Security Team

Deployed By: Devika Sivakumar

Last Modified By: Mehak

Last Modified on: 12 May 2024



Contents

1. Prerequisites	3
2. Deploying Wazuh on the Virtual Machine.....	3
3. Conclusion:	8
Figure 1 switching to the root user.	3
Figure 2 Update the system.	3
Figure 3 Configuring the system parameter.....	4
Figure 4 First command.....	4
Figure 5 Installing Docker and Docker Compose.....	4
Figure 6 Cloning Docker Github	5
Figure 7 Changing directory and generating indexer certificates.	5
Figure 8 Starting Wazuh.	6
Figure 9 Wazuh running successfully.	6
Figure 10 Wazuh Dashboard	7
Figure 11 Wazuh Dashboard.	7



Name	Team	Role	Position
Devika Sivakumar	Purple Team	Deployed Wazuh on the Virtual Machine	Junior
Mehak	Secure Coding Team	Guided with the Implementation and Documentation	Senior

1. Prerequisites

Before deploying Wazuh on the VM, ensure the following prerequisites are met:

- Access to the VM with root permissions.
- Basic understanding of SSH for connecting to the VM.
- Internet connectivity on the VM for downloading necessary packages.
- A web browser installed on your local machine for accessing the Wazuh dashboard.
- If accessing the VM from outside the university network, ensure VPN access is set up as per the instructions provided in the [Implementation Guide](#).

2. Deploying Wazuh on the Virtual Machine

Step 1: Log in via SSH

- Use SSH to connect to the VM. If you are unsure how to do this, refer to the [Wazuh Implementation Guide](#).

Step 2: Preparing the System

- Switch to the root user:

```
sudo su
```

```
devika@redback1:~$ sudo su  
[sudo] password for devika:
```

Figure 1 switching to the root user.

- Update the system and install necessary upgrades:

```
apt update && apt upgrade -y
```

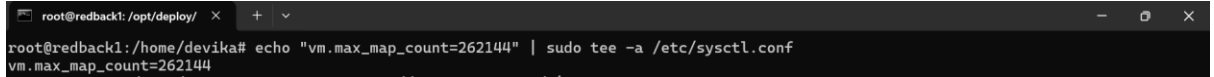
```
root@redback1:/home/devika# apt update && apt upgrade -y  
Hit:1 https://download.docker.com/linux/ubuntu focal InRelease  
Hit:2 http://archive.ubuntu.com/ubuntu focal InRelease  
Hit:3 http://ppa.launchpad.net/oisf/suricata-stable/ubuntu focal InRelease  
Hit:4 http://archive.ubuntu.com/ubuntu focal-updates InRelease  
Hit:5 http://archive.ubuntu.com/ubuntu focal-backports InRelease  
Hit:6 http://archive.ubuntu.com/ubuntu focal-security InRelease  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
All packages are up to date.  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
Calculating upgrade... Done  
Get more security updates through Ubuntu Pro with 'esm-apps' enabled:  
node-hosted-git-info mosquitto node-tar libmosquitto1 node-ip  
mosquitto-clients  
Learn more about Ubuntu Pro at https://ubuntu.com/pro  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Figure 2 Update the system.

Note: This process may take a few minutes.

- Configure required system parameter for Docker:

```
echo "vm.max_map_count=262144" | sudo tee -a /etc/sysctl.conf
```



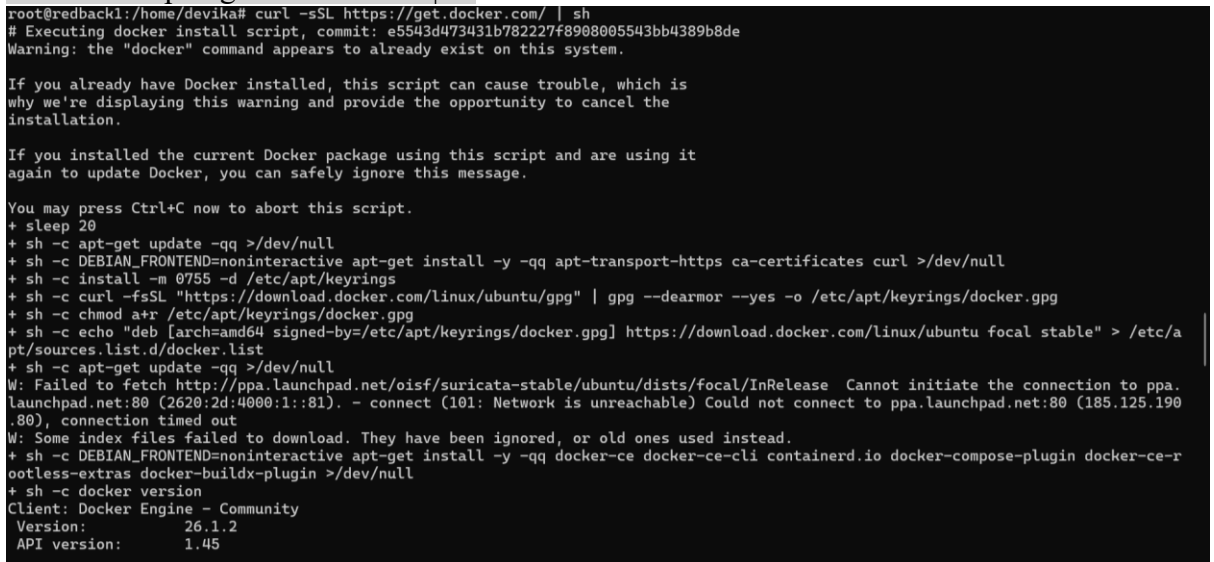
```
root@redback1: /opt/deploy/ x + v
root@redback1: /home/devika# echo "vm.max_map_count=262144" | sudo tee -a /etc/sysctl.conf
vm.max_map_count=262144
```

Figure 3 Configuring the system parameter.

Step 3: Installing Docker and Docker Compose

- Install Docker and Docker Compose

```
curl -sSL https://get.docker.com/ | sh
```



```
root@redback1: /home/devika# curl -sSL https://get.docker.com/ | sh
# Executing docker install script, commit: e5543d473431b782227f8908005543bb4389b8de
Warning: the "docker" command appears to already exist on this system.

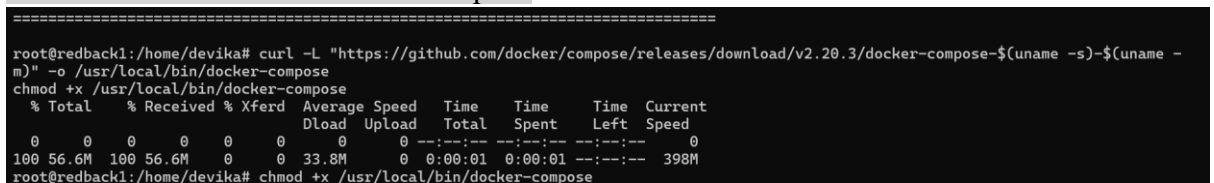
If you already have Docker installed, this script can cause trouble, which is
why we're displaying this warning and provide the opportunity to cancel the
installation.

If you installed the current Docker package using this script and are using it
again to update Docker, you can safely ignore this message.

You may press Ctrl+C now to abort this script.
+ sleep 20
+ sh -c apt-get update -qq >/dev/null
+ sh -c DEBIAN_FRONTEND=noninteractive apt-get install -y -qq apt-transport-https ca-certificates curl >/dev/null
+ sh -c install -m 0755 -d /etc/apt/keyrings
+ sh -c curl -fsSL "https://download.docker.com/linux/ubuntu/gpg" | gpg --dearmor --yes -o /etc/apt/keyrings/docker.gpg
+ sh -c chmod a+r /etc/apt/keyrings/docker.gpg
+ sh -c echo "deb [arch=amd64 signed-by=/etc/apt/keyrings/docker.gpg] https://download.docker.com/linux/ubuntu focal stable" > /etc/a
pt/sources.list.d/docker.list
+ sh -c apt-get update -qq >/dev/null
W: Failed to fetch http://ppa.launchpad.net/oisf/suricata-stable/ubuntu/dists/focal/InRelease Cannot initiate the connection to ppa.
launchpad.net:80 (2620:2d:4000:1::81). - connect (101: Network is unreachable) Could not connect to ppa.launchpad.net:80 (185.125.190
.80), connection timed out
W: Some index files failed to download. They have been ignored, or old ones used instead.
+ sh -c DEBIAN_FRONTEND=noninteractive apt-get install -y -qq docker-ce docker-ce-cli containerd.io docker-compose-plugin docker-ce-r
ootless-extras docker-buildx-plugin >/dev/null
+ sh -c docker version
Client: Docker Engine - Community
Version: 26.1.2
API version: 1.45
```

Figure 4 First command.

```
curl -L "https://github.com/docker/compose/releases/download/v2.20.3/docker-
compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose
chmod +x /usr/local/bin/docker-compose
```



```
root@redback1: /home/devika# curl -L "https://github.com/docker/compose/releases/download/v2.20.3/docker-compose-$(uname -s)-$(uname -
m)" -o /usr/local/bin/docker-compose
chmod +x /usr/local/bin/docker-compose
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
100 56.6M 100 56.6M 0 0 33.8M 0 0:00:01 0:00:01 --:-- 398M
root@redback1: /home/devika# chmod +x /usr/local/bin/docker-compose
```

Figure 5 Installing Docker and Docker Compose

Step 4: Deploying Wazuh

- Change to the deployment directory and clone the Wazuh Docker repository:

```
cd /opt/ && mkdir deploy && cd deploy
```

```
git clone https://github.com/wazuh/wazuh-docker.git -b v4.5.0
```

```
root@redback1:/home/devika# cd /opt/ && mkdir deploy && cd deploy
root@redback1:/opt/deploy# git clone https://github.com/wazuh/wazuh-docker.git -b v4.5.0
Cloning into 'wazuh-docker'...
remote: Enumerating objects: 12829, done.
remote: Counting objects: 100% (149/149), done.
remote: Compressing objects: 100% (90/90), done.
remote: Total 12829 (delta 57), reused 141 (delta 52), pack-reused 12680
Receiving objects: 100% (12829/12829), 314.39 MiB | 13.38 MiB/s, done.
Resolving deltas: 100% (6684/6684), done.
Note: switching to 'e01d39e13834b5ebb86baf3ffb5805afa24ec435'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

    git switch -c <new-branch-name>

Or undo this operation with:
```

Figure 6 Cloning Docker Github

```
cd wazuh-docker/single-node/
```

- Generate indexer certificates

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

```
root@redback1:/opt/deploy# cd wazuh-docker/single-node/
root@redback1:/opt/deploy/wazuh-docker/single-node# docker-compose -f generate-indexer-certs.yml run --rm generator
[+] Creating 1/0
  ✓ Network single-node_default Created 0.0s
[+] Running 5/5
  ✓ generator 4 layers [#####] 0B/0B Pulled 5.7s
  ✓ edaadc954fb5 Pull complete 1.0s
  ✓ 573f4d11a520 Pull complete 1.1s
  ✓ 8f200922197d Pull complete 0.7s
  ✓ 55a86de68c5c Pull complete 1.4s
The tool to create the certificates exists in the in Packages bucket
11/05/2024 02:13:16 INFO: Admin certificates created.
11/05/2024 02:13:16 INFO: Wazuh indexer certificates created.
11/05/2024 02:13:16 INFO: Wazuh server certificates created.
11/05/2024 02:13:16 INFO: Wazuh dashboard certificates created.
Moving created certificates to the destination directory
Changing certificate permissions
Setting UID indexer and dashboard
Setting UID for wazuh manager and worker
root@redback1:/opt/deploy/wazuh-docker/single-node# |
```

Figure 7 Changing directory and generating indexer certificates.

- Start Wazuh using Docker Compose:

```
docker-compose up -d
```

```

root@redback1: /opt/deploy/wazuh-docker/single-node# docker-compose up -d
[+] Running 43/20
✓wazuh.indexer 13 layers [#####] 0B/0B Pulled 44.4s
✓wazuh.dashboard 10 layers [#####] 0B/0B Pulled 52.7s
✓wazuh.manager 17 layers [#####] 0B/0B Pulled 31.3s

[+] Running 15/15
✓Volume "single-node-wazuh-indexer-data" Created 0.0s
✓Volume "single-node-wazuh-agentless" Created 0.0s
✓Volume "single-node-filebeat_etc" Created 0.0s
✓Volume "single-node-wazuh_active_response" Created 0.0s
✓Volume "single-node-wazuh_wodles" Created 0.0s
✓Volume "single-node-wazuh_var_multigroups" Created 0.0s
✓Volume "single-node-filebeat_var" Created 0.0s
✓Volume "single-node-wazuh_etc" Created 0.0s
✓Volume "single-node-wazuh_logs" Created 0.0s
✓Volume "single-node-wazuh_integrations" Created 0.0s
✓Volume "single-node-wazuh_api_configuration" Created 0.0s
✓Volume "single-node-wazuh_queue" Created 0.0s
✓Container single-node-wazuh.indexer-1 Started 8.2s
✓Container single-node-wazuh.manager-1 Started 8.2s
✓Container single-node-wazuh.dashboard-1 Started 0.0s
root@redback1: /opt/deploy/wazuh-docker/single-node#

```

Figure 8 Starting Wazuh.

Step 5: Accessing Wazuh Web Interface

1. The Wazuh dashboard is currently running on the server with the following Docker services which can be seen by running the below command:

```
docker-compose ps
```

```

devika@redback1: /opt/deploy/wazuh-docker$ cd
devika@redback1:~$ sudo su
[sudo] password for devika:
root@redback1: /opt/deploy/wazuh-docker/single-node# docker-compose ps
NAME                IMAGE                COMMAND                  SERVICE    CREATED        STATUS        PORTS
single-node-wazuh.dashboard-1  wazuh/wazuh-dashboard:4.5.0  "/entrypoint.sh"        wazuh.dashboard    2 hours ago    Up 2 hours    443/tcp, 0.0.0.0:443->5601/tcp, ::443->5601/tcp
single-node-wazuh.indexer-1    wazuh/wazuh-indexer:4.5.0    "/entrypoint.sh open_"  wazuh.indexer      2 hours ago    Up 2 hours    0.0.0.0:9200->9200/tcp, ::9200->9200/tcp
single-node-wazuh.manager-1    wazuh/wazuh-manager:4.5.0    "/init"                 wazuh.manager      2 hours ago    Up 2 hours    0.0.0.0:1514-1515->1514-1515/tcp, ::1514-1515->1514-1515/tcp, 0.0.0.0:55000->55000/tcp, ::55000->55000/tcp, 1516/tcp
root@redback1: /opt/deploy/wazuh-docker/single-node#

```

Figure 9 Wazuh running successfully.

2. Accessing the Wazuh dashboard interface is achieved by following the provided URL which can only be accessed if you are connected to the Deakin VPN: <https://redback.it.deakin.edu.au/app/login?>
3. Upon reaching this interface, enter the following credentials:
 - Username: kibanaserver
 - Password: kibanaserver

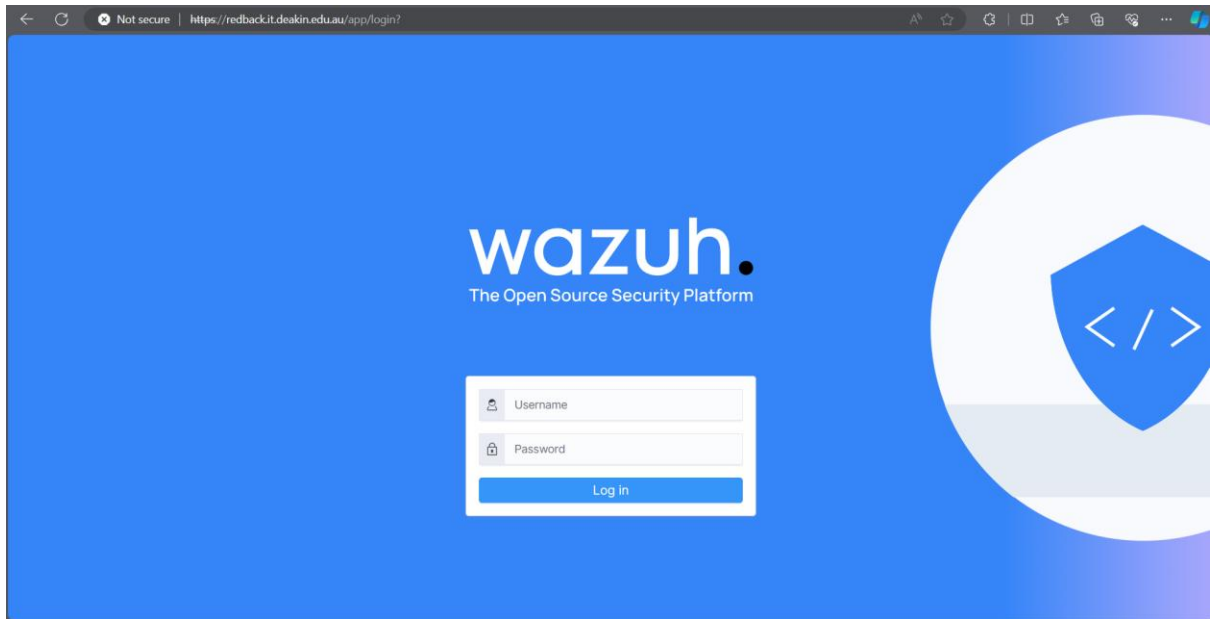


Figure 10 Wazuh Dashboard

4. After successful authentication, users are redirected to the Wazuh dashboard interface, where they can utilize various features, including monitoring security events, analysing logs, configuring alerts, and more.

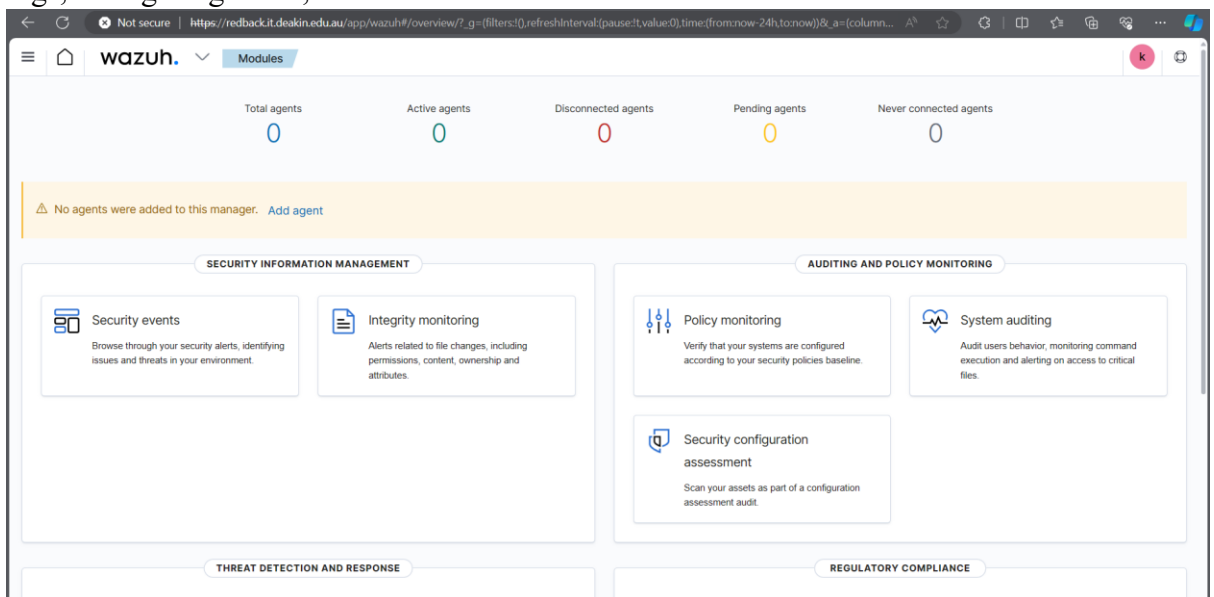


Figure 11 Wazuh Dashboard.

3. Conclusion:

Now Wazuh has been successfully deployed on the company's VM, enhancing security. In the next trimester, this deployment can be leveraged for upcoming projects on the VM. Here are some benefits of Wazuh for the company:

- Real-time threat detection and response.
- Centralized monitoring and management of security events.
- Compliance with industry regulations and standards.
- Improved incident response capabilities.
- Enhanced visibility into network and system activities.
- Scalability to accommodate future growth and project expansions.

This deployment sets a strong foundation for bolstering the company's security posture and ensuring proactive threat mitigation.