Securigeek

CTI Feed

Wazuh/AWS/Azure/MISP/Docker

Problem Statement

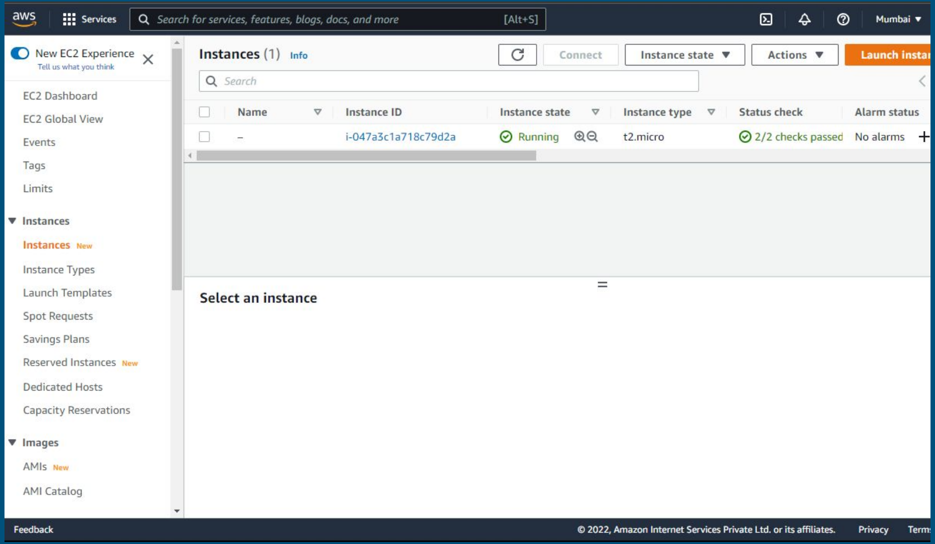
Create a small demo environment using wazuh.com . Integrate logs from end point and from AWS Cloud (take a free tier) and from O365 (use a trial account) .

Integrate the system with a setup of https://www.misp-project.org/ and show how we can use the CTI feed to detect and validate threats.

Working:

What I have done Until now!

1.Firstly I Created an Ubuntu Instance on AWS EC2 T2 Micro.



Instances (1) Info

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
□	–	i-047a3c1a718c79d2a	Running	t2.micro	2/2 checks passed	No alarms

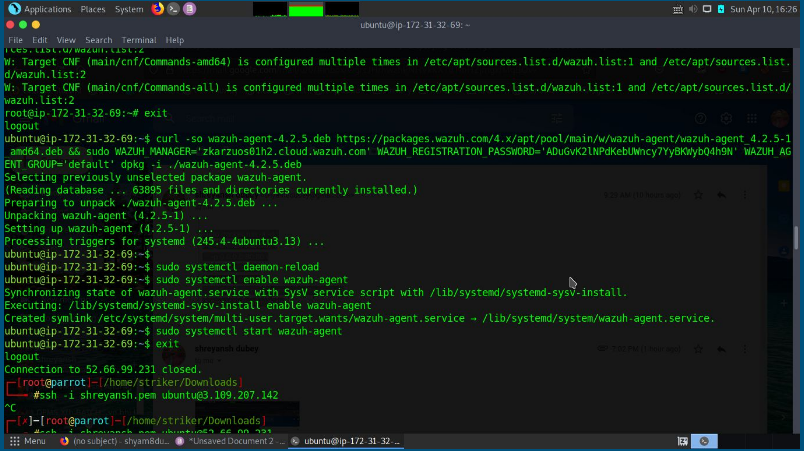
Select an instance

© 2022, Amazon Internet Services Private Ltd. or its affiliates.

Setting Up Wazuh-Agent

Wazuh-Agent

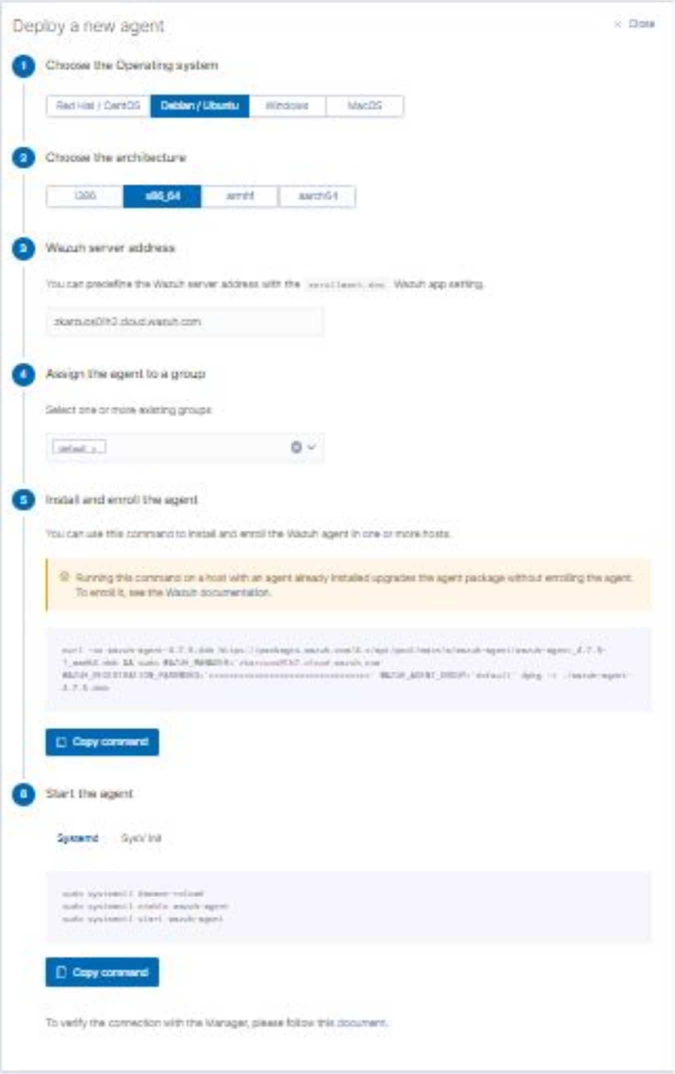
1. Add the Wazuh-Repo.
2. Deploying Wazuh-Agent.
3. Starting services.



```
rces.list.d/wazuh.list:2
W: Target CNF (main/cnf/Commands-amd64) is configured multiple times in /etc/apt/sources.list.d/wazuh.list:1 and /etc/apt/sources.list.
d/wazuh.list:2
W: Target CNF (main/cnf/Commands-all) is configured multiple times in /etc/apt/sources.list.d/wazuh.list:1 and /etc/apt/sources.list.d/
wazuh.list:2
root@ip-172-31-32-69:~# exit
logout
ubuntu@ip-172-31-32-69:~$ curl -so wazuh-agent-4.2.5.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.2.5-1
_amd64.deb && sudo WAZUH_MANAGER='zkarzuos01h2.cloud.wazuh.com' WAZUH_REGISTRATION_PASSWORD='ADuGvK2lNPdKebUWncy7YyBKWybQ4h9N' WAZUH_AG
ENT_GROUP='default' dpkg -i ./wazuh-agent-4.2.5.deb
Selecting previously unselected package wazuh-agent.
(Reading database ... 63895 files and directories currently installed.)
Preparing to unpack ./wazuh-agent-4.2.5.deb ...
Unpacking wazuh-agent (4.2.5-1) ...
Setting up wazuh-agent (4.2.5-1) ...
Processing triggers for systemd (245.4-4ubuntu3.13) ...
ubuntu@ip-172-31-32-69:~$
ubuntu@ip-172-31-32-69:~$ sudo systemctl daemon-reload
ubuntu@ip-172-31-32-69:~$ sudo systemctl enable wazuh-agent
Synchronizing state of wazuh-agent.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /lib/systemd/system/wazuh-agent.service.
ubuntu@ip-172-31-32-69:~$ sudo systemctl start wazuh-agent
ubuntu@ip-172-31-32-69:~$ exit
logout
Connection to 52.66.99.231 closed.
┌─[root@parrot]─[/home/striker/Downloads]
└──╼ #ssh -i shreyansh.pem ubuntu@3.109.207.142
^C
┌─[✗]─[root@parrot]─[/home/striker/Downloads]
└──╼ #ssh -i shreyansh.pem ubuntu@52.66.99.231
```

Adding Wazuh-Agent In Wazuh Cloud

1. Under Wazuh-Cloud .
2. Deploy New Agent
3. Select the os and architecture and enroll the agent .



Deploy a new agent

× Close

1 Choose the Operating system

2 Choose the architecture

3 Wazuh server address

You can predefine the Wazuh server address with the `enrollment.dns` Wazuh app setting.

[illegible].cloud.wazuh.com

4 Assign the agent to a group

Select one or more existing groups:

default

5 Install and enroll the agent

You can use this command to install and enroll the Wazuh agent in one or more hosts.

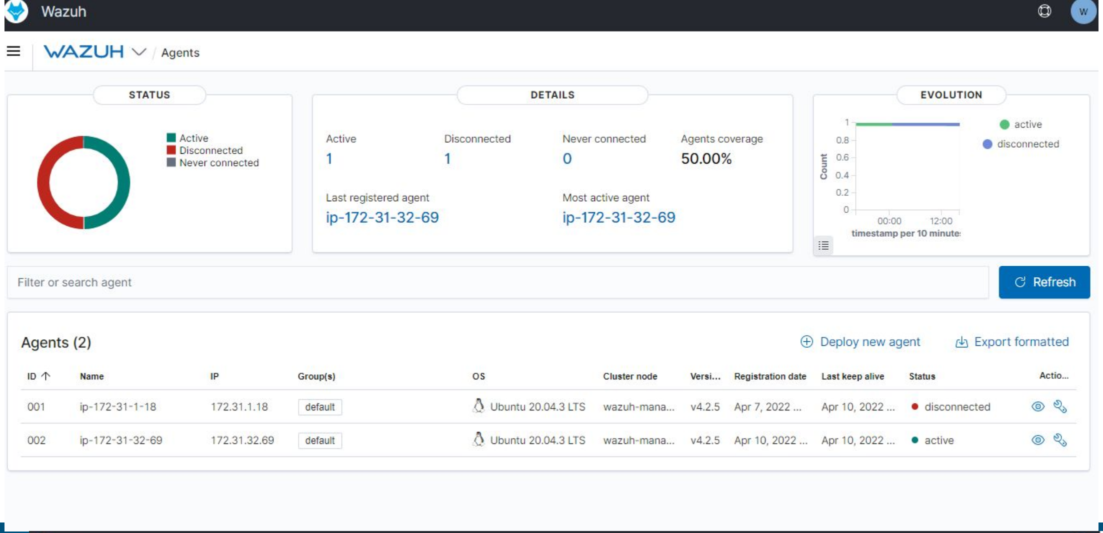
Running this command on a host with an agent already installed upgrades the agent package without enrolling the agent. To enroll it, see the Wazuh documentation.

```
curl -so wazuh-agent-4.7.5.deb https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.5-1_amd64.deb && sudo WAZUH_MANAGER='[illegible].cloud.wazuh.com' WAZUH_REGISTRATION_PASSWORD='[illegible]' WAZUH_AGENT_GROUP='default' dpkg -i ./wazuh-agent-4.7.5.deb
```

6 Start the agent

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

To verify the connection with the Manager, please follow this document.



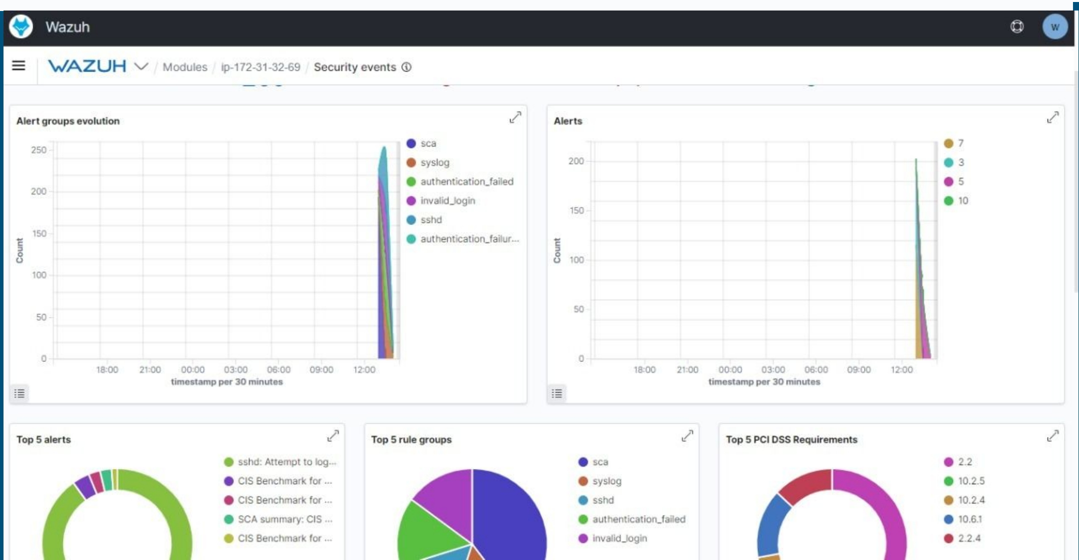
Active	Disconnected	Never connected	Agents coverage
1	1	0	50.00%

Last registered agent: ip-172-31-32-69

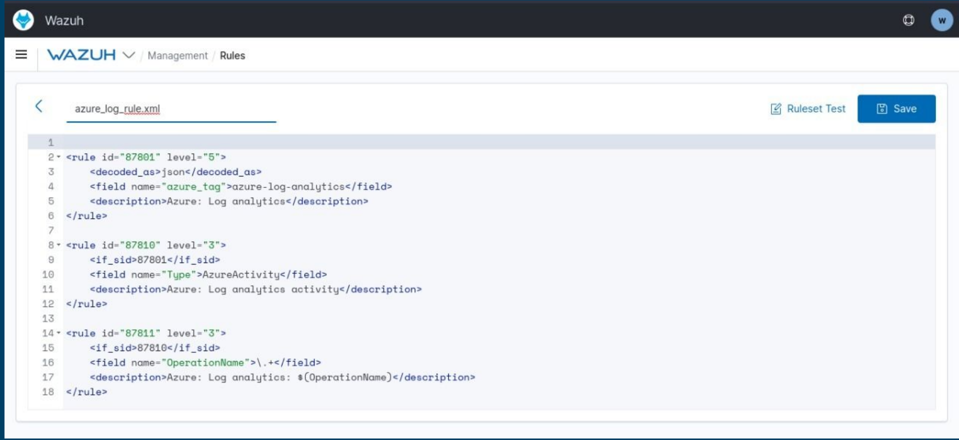
Most active agent: ip-172-31-32-69

Agents (2)

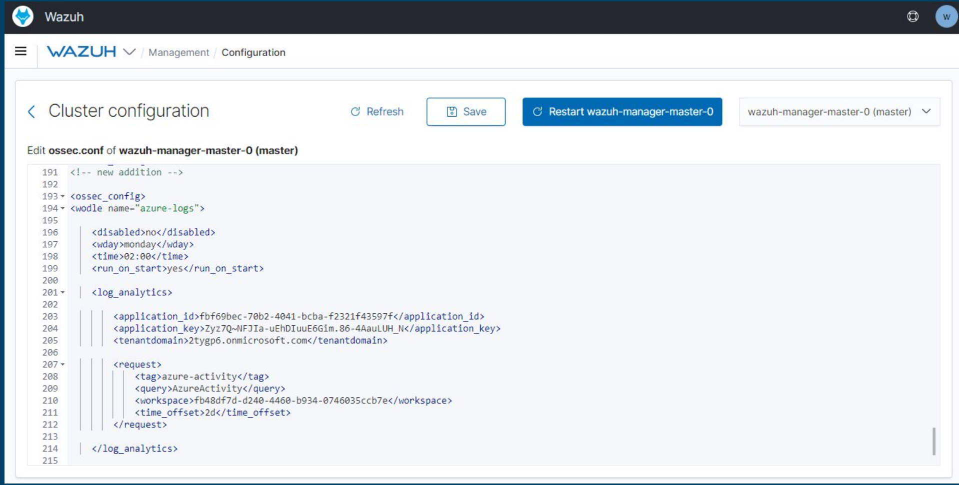
ID ↑	Name	IP	Group(s)	OS	Cluster node	Versi...	Registration date	Last keep alive	Status	Actio...
001	ip-172-31-1-18	172.31.1.18	default	Ubuntu 20.04.3 LTS	wazuh-mana...	v4.2.5	Apr 7, 2022 ...	Apr 10, 2022 ...	● disconnected	
002	ip-172-31-32-69	172.31.32.69	default	Ubuntu 20.04.3 LTS	wazuh-mana...	v4.2.5	Apr 10, 2022 ...	Apr 10, 2022 ...	● active	



Azure Logs Rule



```xml

<rule id="87801" level="5">
    <decoded_as>json</decoded_as>
    <field name="azure_tag">azure-log-analytics</field>
    <description>Azure: Log analytics</description>
</rule>

<rule id="87810" level="3">
    <if_sid>87801</if_sid>
    <field name="Type">AzureActivity</field>
    <description>Azure: Log analytics activity</description>
</rule>

<rule id="87811" level="3">
    <if_sid>87810</if_sid>
    <field name="OperationName">\.+</field>
    <description>Azure: Log analytics: $(OperationName)</description>
</rule>
```


Wazuh
w
WAZUH
Management / Configuration
Cluster configuration
Refresh
Save
Restart wazuh-manager-master-0
wazuh-manager-master-0 (master)

Edit **ossec.conf** of **wazuh-manager-master-0 (master)**

```xml
<!-- new addition -->

<ossec_config>
<wodle name="azure-logs">

    <disabled>no</disabled>
    <wday>monday</wday>
    <time>02:00</time>
    <run_on_start>yes</run_on_start>

    <log_analytics>

        <application_id>fbf69bec-70b2-4041-bcba-f2321f43597f</application_id>
        <application_key>Zyz7Q~NFJIa-uEhDIuuE6Gim.86-4AauLUH_N</application_key>
        <tenantdomain>2tygp6.onmicrosoft.com</tenantdomain>

        <request>
            <tag>azure-activity</tag>
            <query>AzureActivity</query>
            <workspace>fb48df7d-d240-4460-b934-0746035ccb7e</workspace>
            <time_offset>2d</time_offset>
        </request>

    </log_analytics>

```

Azure App Perms

https://wazuh.com/blog/monitor-office-365-with-wazuh/

(office_365.py Part Not properly Done - Rest OK)

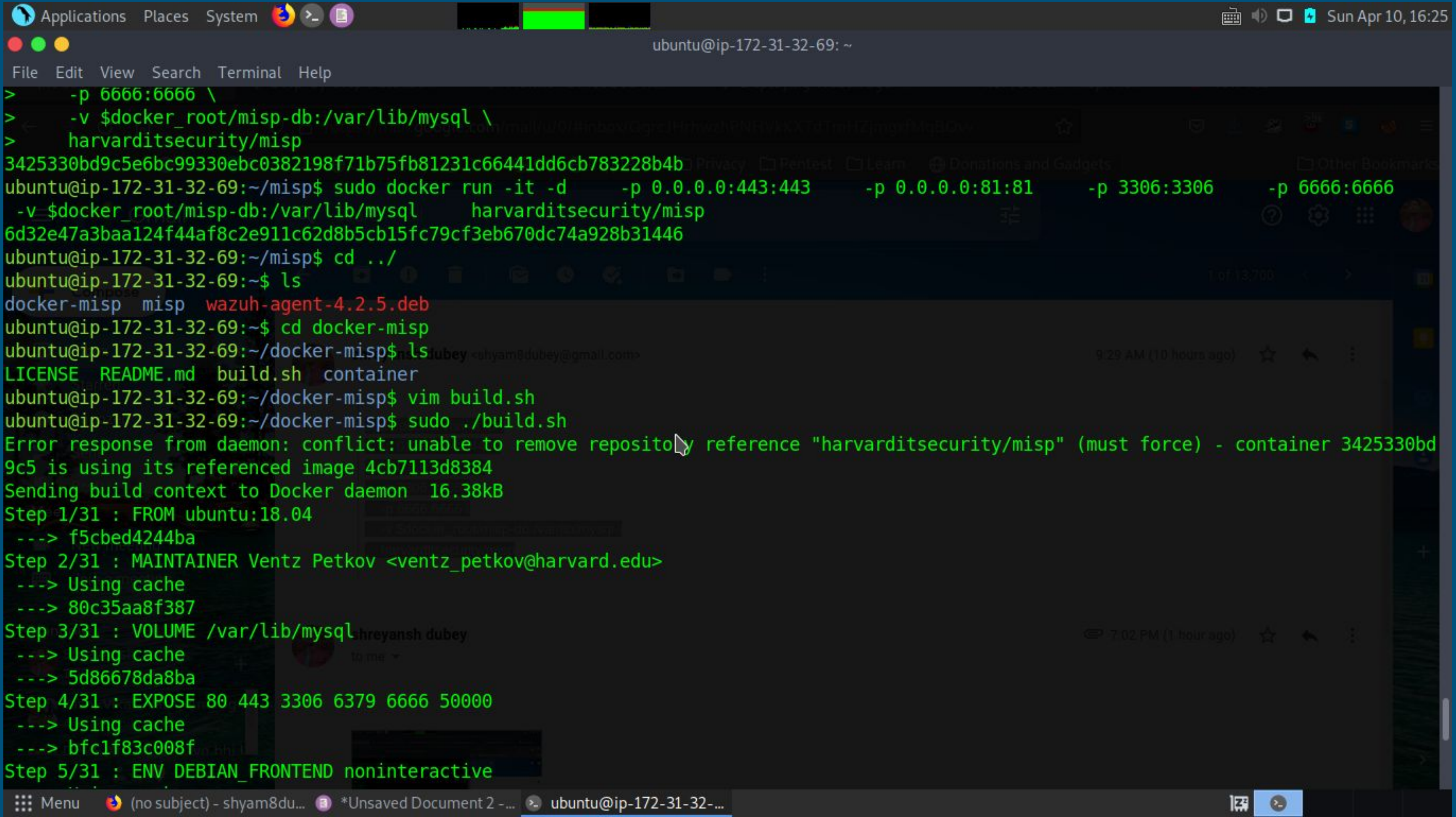
MISP Setup Using Docker

Reference:

https://github.com/MISP/docker-misp

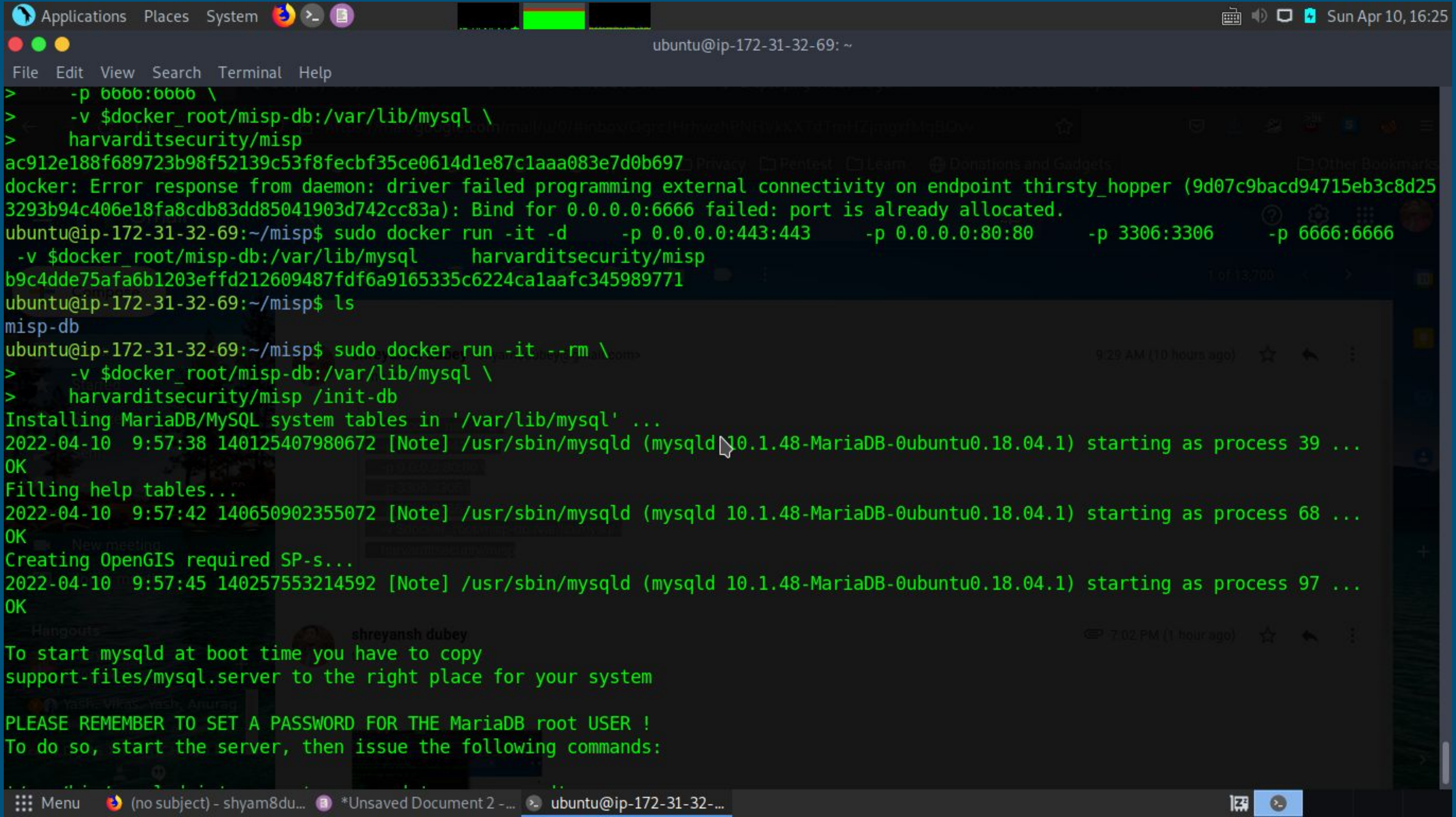
(Need IOC data for graph and monitoring)

Build:



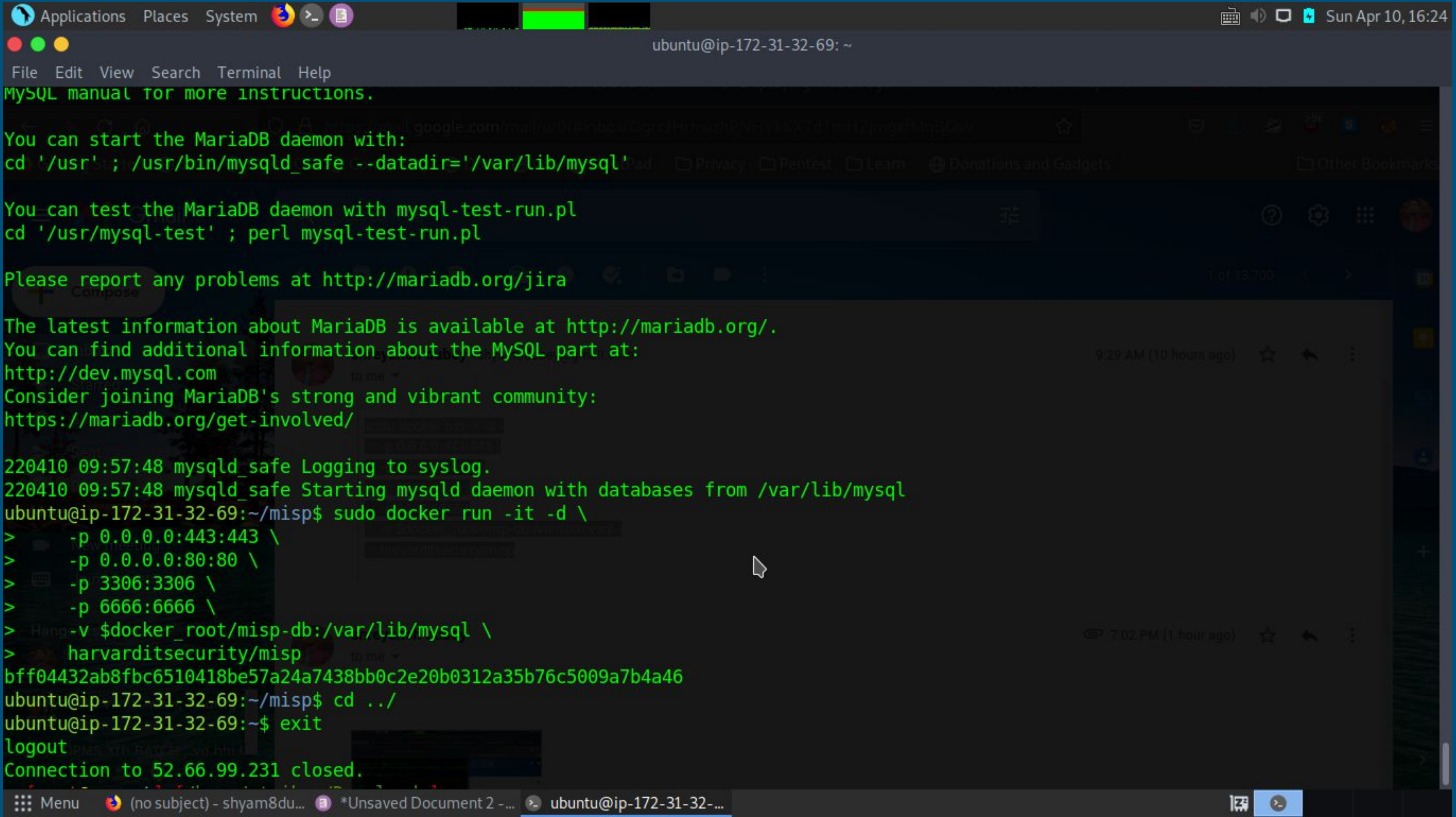
```
>     -p 6666:6666 \
>     -v $docker_root/misp-db:/var/lib/mysql \
>     harvarditsecurity/misp
3425330bd9c5e6bc99330ebc0382198f71b75fb81231c66441dd6cb783228b4b
ubuntu@ip-172-31-32-69:~/misp$ sudo docker run -it -d     -p 0.0.0.0:443:443     -p 0.0.0.0:81:81     -p 3306:3306     -p 6666:6666
 -v $docker_root/misp-db:/var/lib/mysql     harvarditsecurity/misp
6d32e47a3baa124f44af8c2e911c62d8b5cb15fc79cf3eb670dc74a928b31446
ubuntu@ip-172-31-32-69:~/misp$ cd ../
ubuntu@ip-172-31-32-69:~$ ls
docker-misp  misp  wazuh-agent-4.2.5.deb
ubuntu@ip-172-31-32-69:~$ cd docker-misp
ubuntu@ip-172-31-32-69:~/docker-misp$ ls
LICENSE  README.md  build.sh  container
ubuntu@ip-172-31-32-69:~/docker-misp$ vim build.sh
ubuntu@ip-172-31-32-69:~/docker-misp$ sudo ./build.sh
Error response from daemon: conflict: unable to remove repository reference "harvarditsecurity/misp" (must force) - container 3425330bd
9c5 is using its referenced image 4cb7113d8384
Sending build context to Docker daemon  16.38kB
Step 1/31 : FROM ubuntu:18.04
 ---> f5cbed4244ba
Step 2/31 : MAINTAINER Ventz Petkov <ventz_petkov@harvard.edu>
 ---> Using cache
 ---> 80c35aa8f387
Step 3/31 : VOLUME /var/lib/mysql
 ---> Using cache
 ---> 5d86678da8ba
Step 4/31 : EXPOSE 80 443 3306 6379 6666 50000
 ---> Using cache
 ---> bfc1f83c008f
Step 5/31 : ENV DEBIAN_FRONTEND noninteractive
```

DB Intialisation:



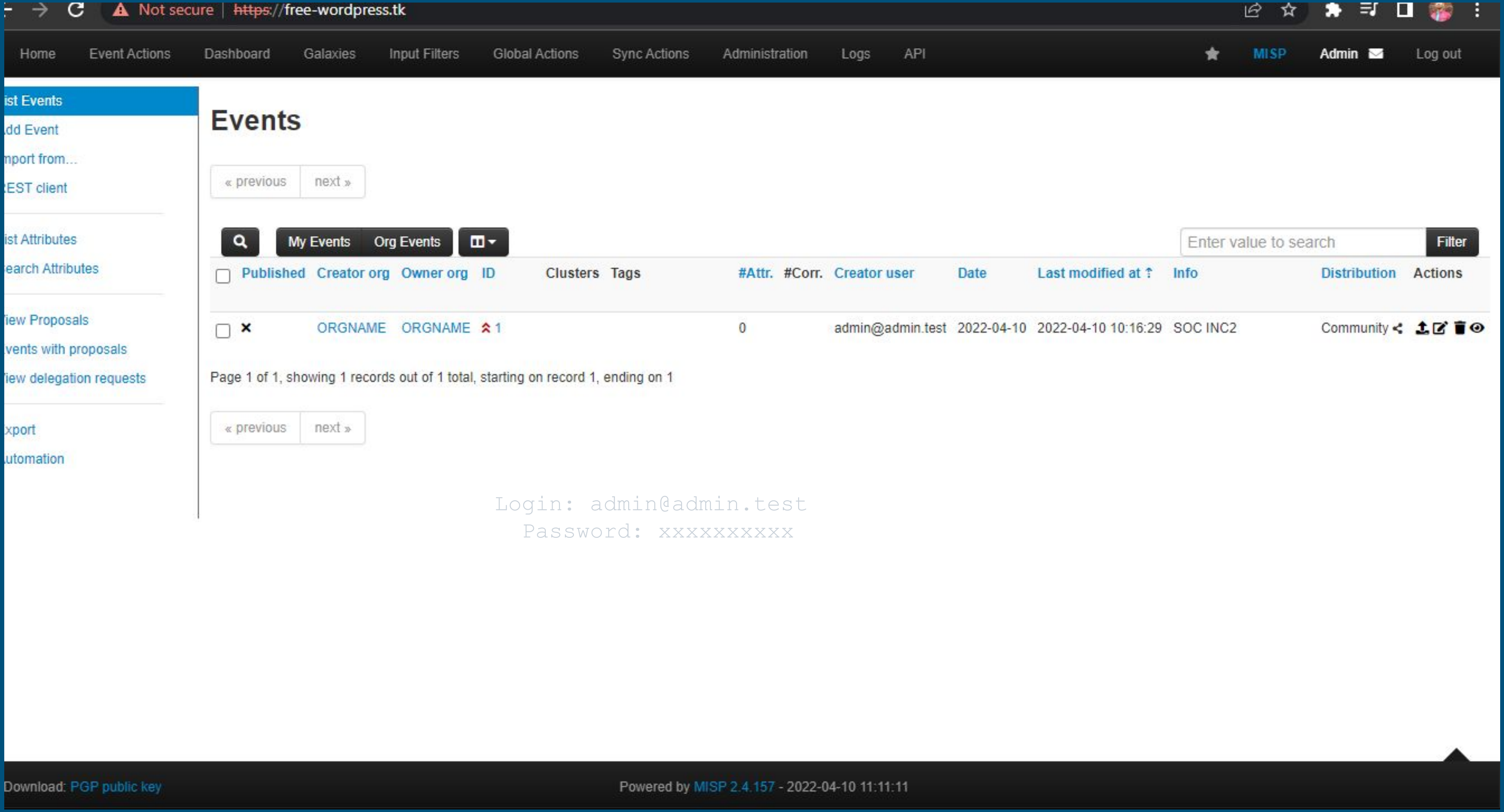
```
>     -p 6666:6666 \
>     -v $docker_root/misp-db:/var/lib/mysql \
>     harvarditsecurity/misp
ac912e188f689723b98f52139c53f8fecbf35ce0614d1e87c1aaa083e7d0b697
docker: Error response from daemon: driver failed programming external connectivity on endpoint thirsty_hopper (9d07c9bacd94715eb3c8d25
3293b94c406e18fa8cdb83dd85041903d742cc83a): Bind for 0.0.0.0:6666 failed: port is already allocated.
ubuntu@ip-172-31-32-69:~/misp$ sudo docker run -it -d     -p 0.0.0.0:443:443     -p 0.0.0.0:80:80     -p 3306:3306     -p 6666:6666
 -v $docker_root/misp-db:/var/lib/mysql     harvarditsecurity/misp
b9c4dde75afa6b1203effd212609487fdf6a9165335c6224ca1aafc345989771
ubuntu@ip-172-31-32-69:~/misp$ ls
misp-db
ubuntu@ip-172-31-32-69:~/misp$ sudo docker run -it --rm \
>     -v $docker_root/misp-db:/var/lib/mysql \
>     harvarditsecurity/misp /init-db
Installing MariaDB/MySQL system tables in '/var/lib/mysql' ...
2022-04-10  9:57:38 140125407980672 [Note] /usr/sbin/mysqld (mysqld 10.1.48-MariaDB-0ubuntu0.18.04.1) starting as process 39 ...
OK
Filling help tables...
2022-04-10  9:57:42 140650902355072 [Note] /usr/sbin/mysqld (mysqld 10.1.48-MariaDB-0ubuntu0.18.04.1) starting as process 68 ...
OK
Creating OpenGIS required SP-s...
2022-04-10  9:57:45 140257553214592 [Note] /usr/sbin/mysqld (mysqld 10.1.48-MariaDB-0ubuntu0.18.04.1) starting as process 97 ...
OK

To start mysqld at boot time you have to copy
support-files/mysql.server to the right place for your system

PLEASE REMEMBER TO SET A PASSWORD FOR THE MariaDB root USER !
To do so, start the server, then issue the following commands:
```

Container-Run:



```
MySQL manual for more instructions.

You can start the MariaDB daemon with:
cd '/usr' ; /usr/bin/mysqld_safe --datadir='/var/lib/mysql'

You can test the MariaDB daemon with mysql-test-run.pl
cd '/usr/mysql-test' ; perl mysql-test-run.pl

Please report any problems at http://mariadb.org/jira

The latest information about MariaDB is available at http://mariadb.org/.
You can find additional information about the MySQL part at:
http://dev.mysql.com
Consider joining MariaDB's strong and vibrant community:
https://mariadb.org/get-involved/

220410 09:57:48 mysqld_safe Logging to syslog.
220410 09:57:48 mysqld_safe Starting mysqld daemon with databases from /var/lib/mysql
ubuntu@ip-172-31-32-69:~/misp$ sudo docker run -it -d \
>     -p 0.0.0.0:443:443 \
>     -p 0.0.0.0:80:80 \
>     -p 3306:3306 \
>     -p 6666:6666 \
>     -v $docker_root/misp-db:/var/lib/mysql \
>     harvarditsecurity/misp
bff04432ab8fbc6510418be57a24a7438bb0c2e20b0312a35b76c5009a7b4a46
ubuntu@ip-172-31-32-69:~/misp$ cd ../
ubuntu@ip-172-31-32-69:~$ exit
logout
Connection to 52.66.99.231 closed.
```

MISP Interface:https://free-wordpress.tk/



Events

☐	Published	Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Last modified at ↑	Info	Distribution	Actions
☐	✕	ORGNAME	ORGNAME	1			0		admin@admin.test	2022-04-10	2022-04-10 10:16:29	SOC INC2	Community	

Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1

Login: admin@admin.test
Password: xxxxxxxxxx

Download: PGP public key

Powered by MISP 2.4.157 - 2022-04-10 11:11:11

Thankyou