Document By:

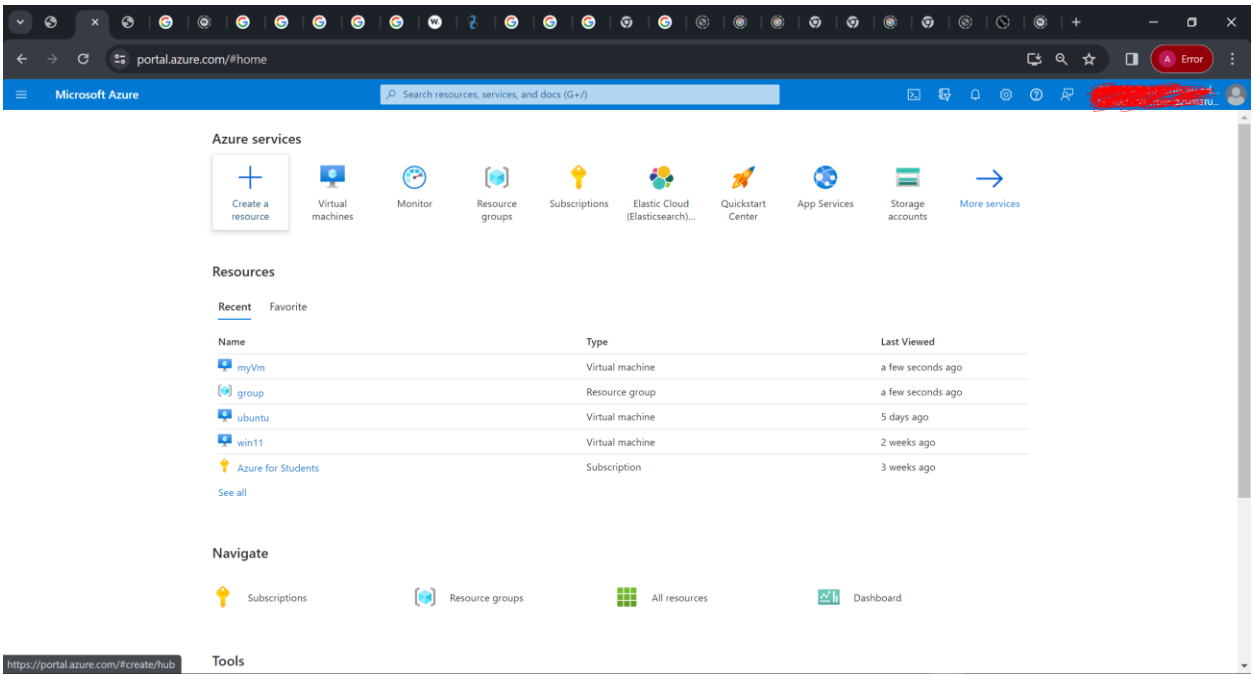
https://www.linkedin.com/in/ehtishamcyber/

Documentation Wazuh

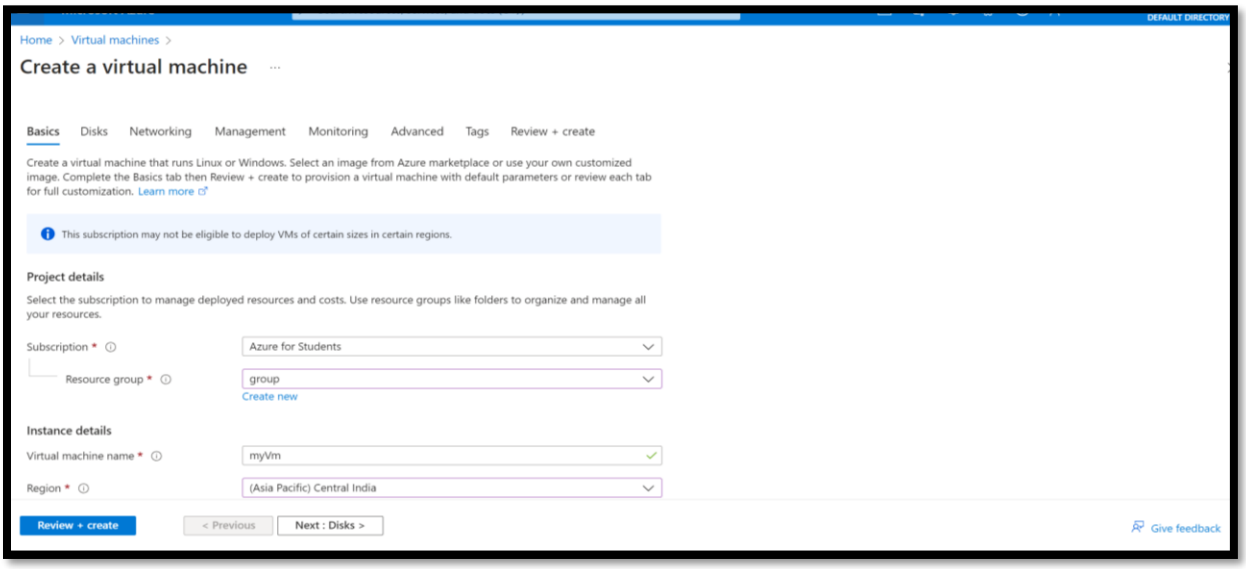
In this Documentation I will be Demonstrating the Wazuh Server on Cloud Platform such as Microsoft Azure.

Process will be like:

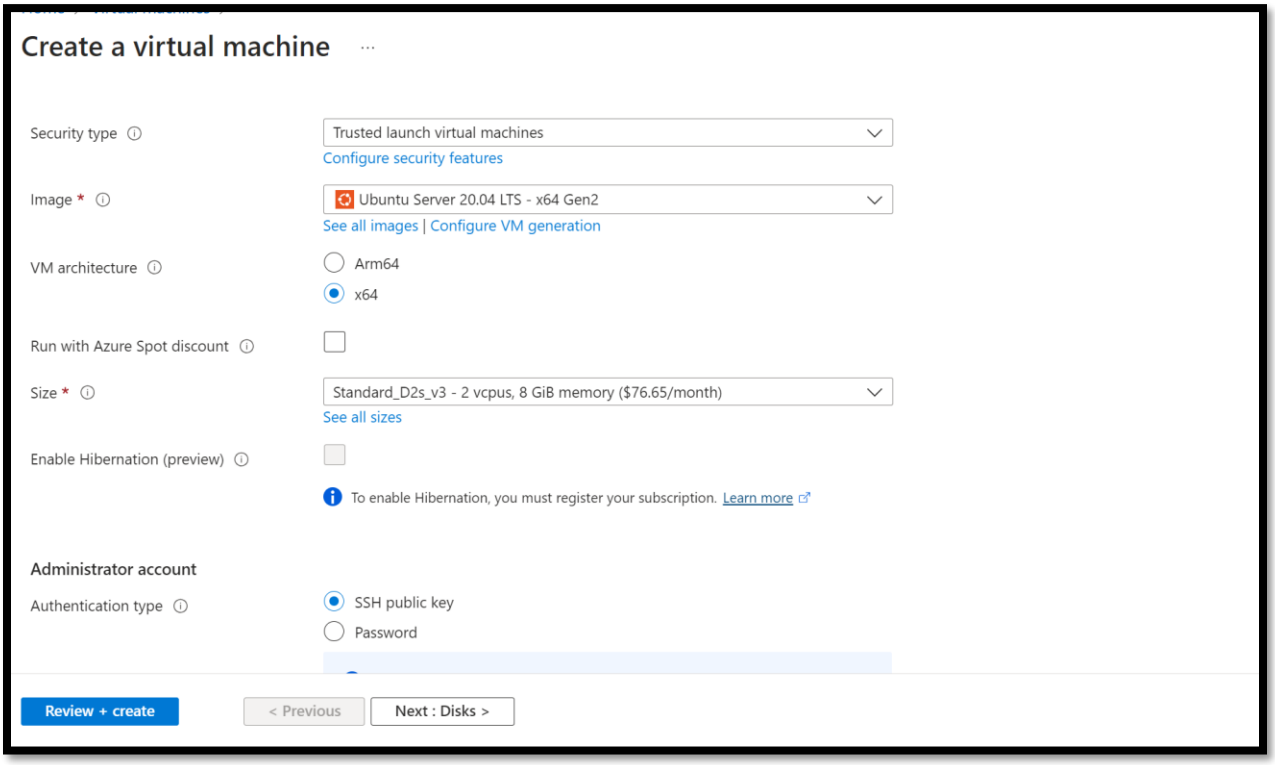
Login to your Azure Account and create a Virtual Machine of Ubuntu server.



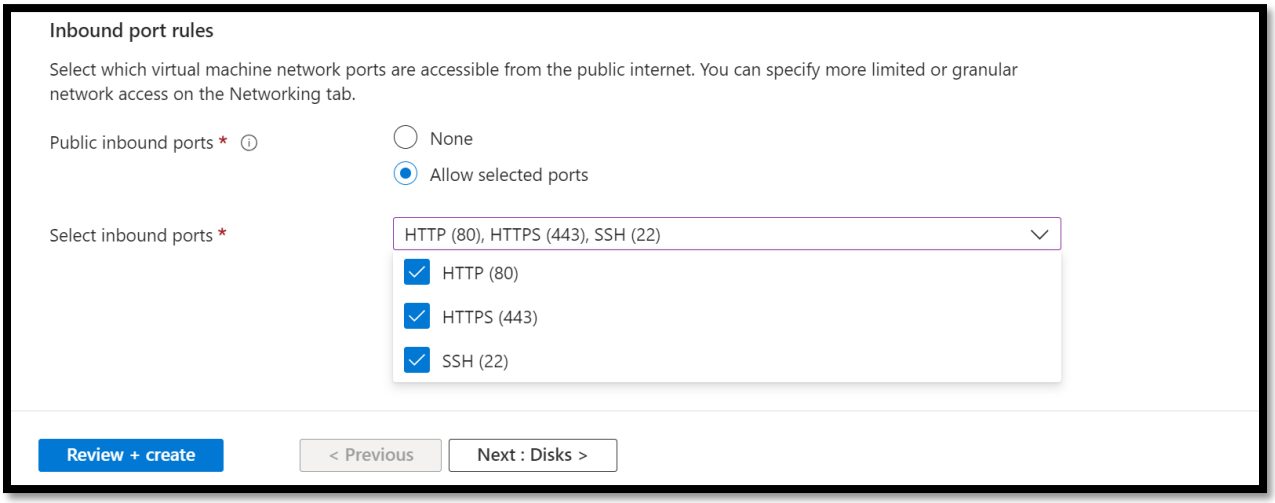
Create New Virtual Machine of Ubuntu Server.



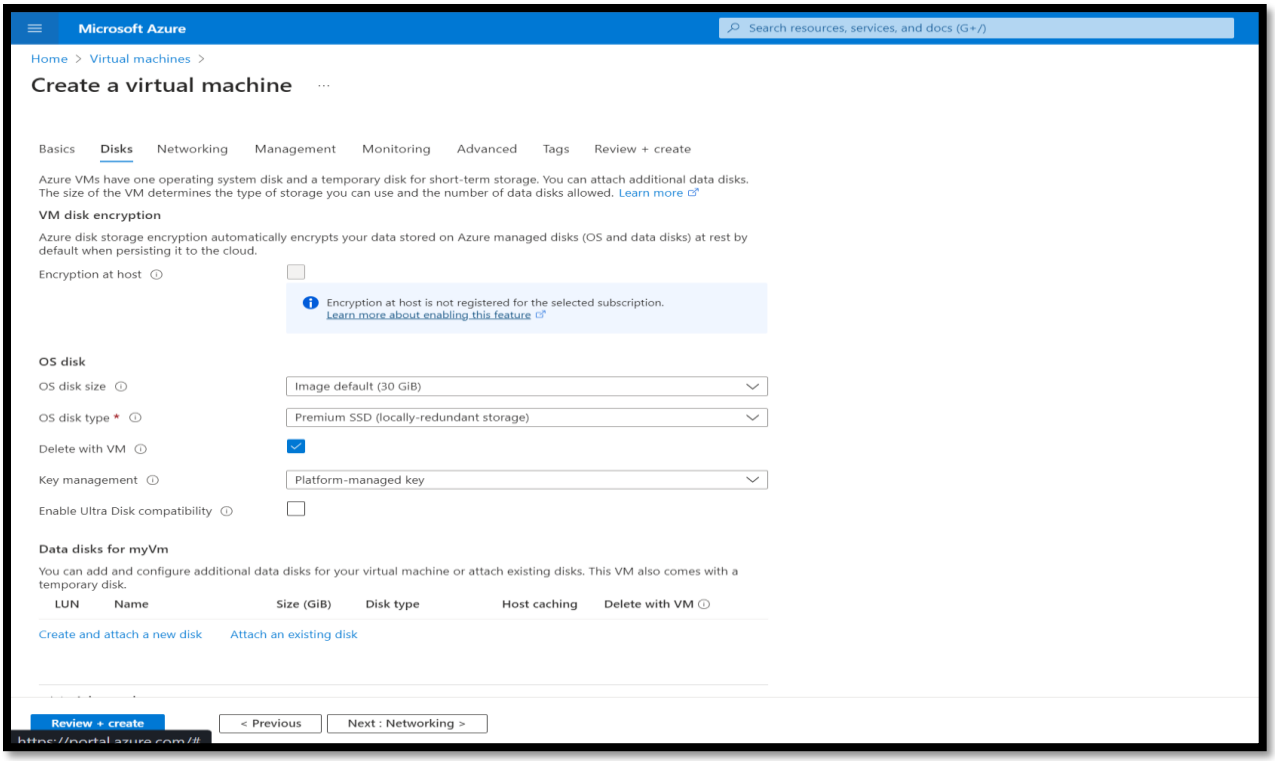
Setting up the basics.



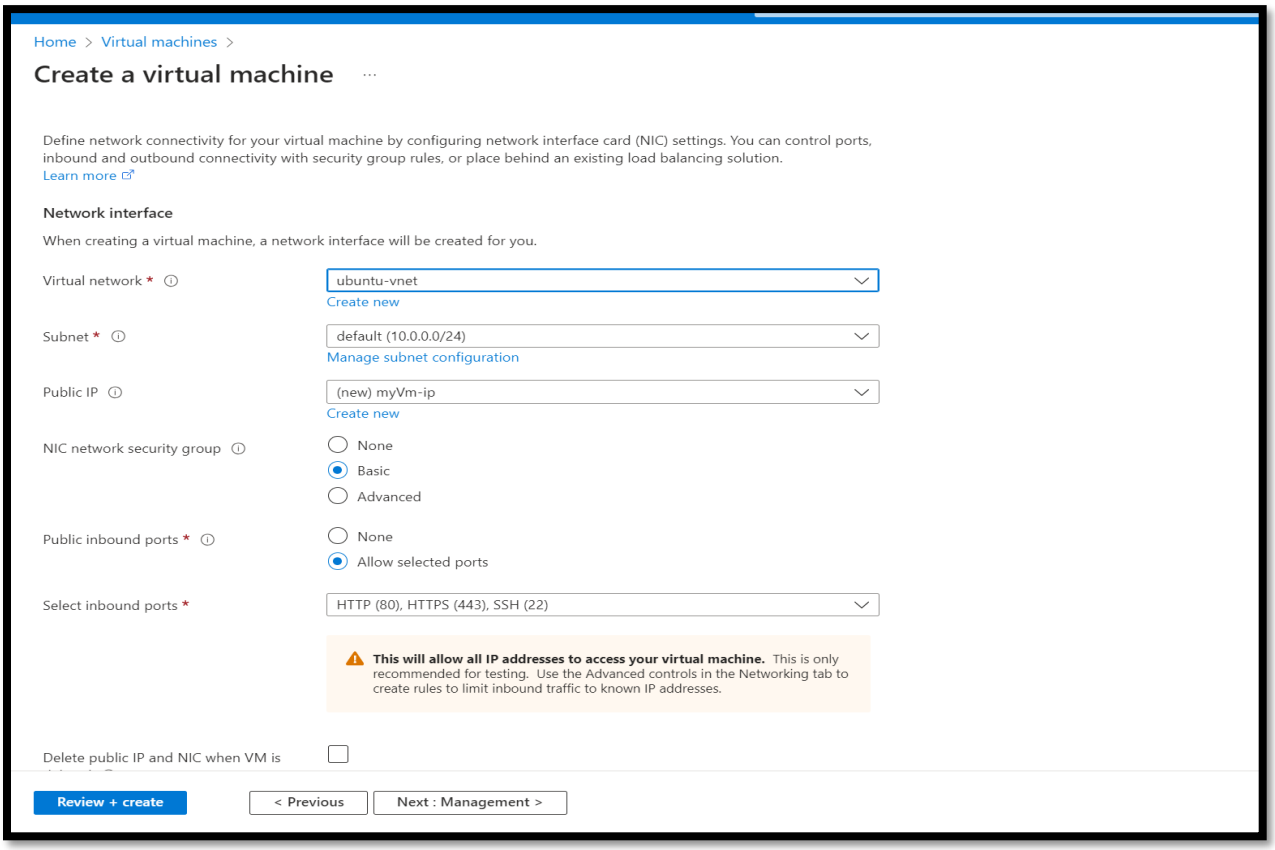
Setting up ports



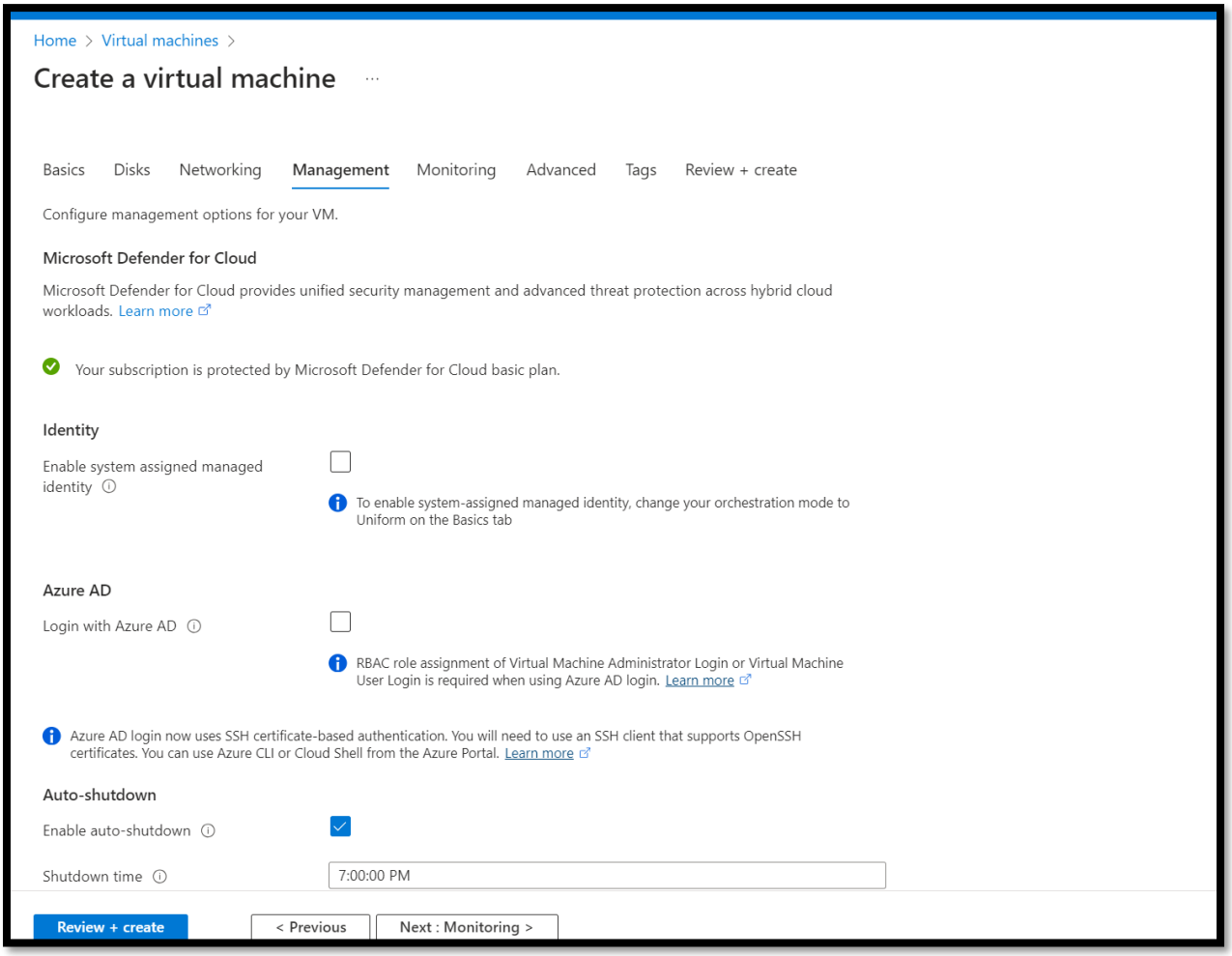
Setting up Disk for storing Server related



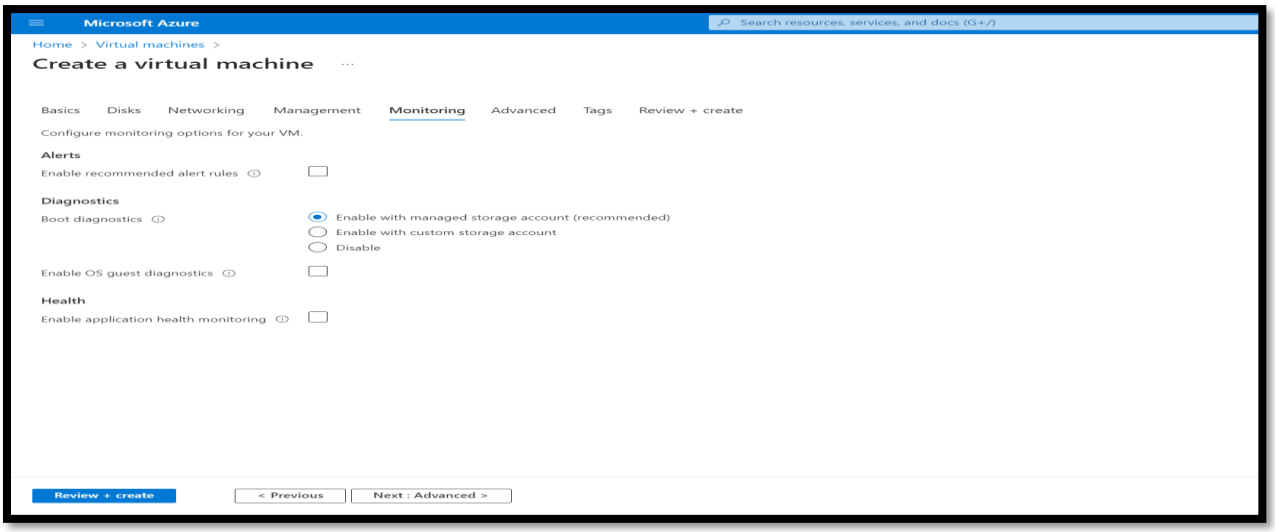
Setting up Network for communication



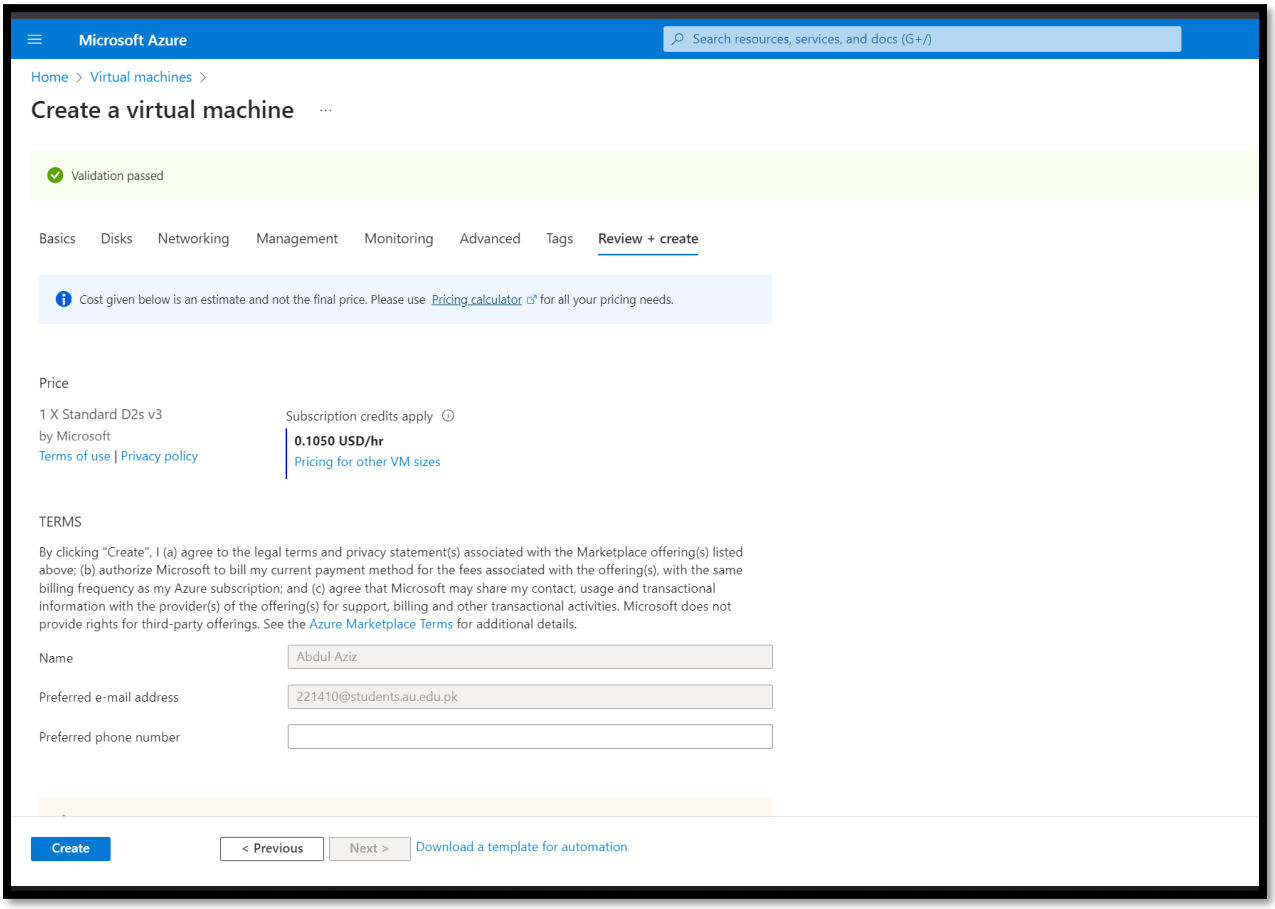
Management



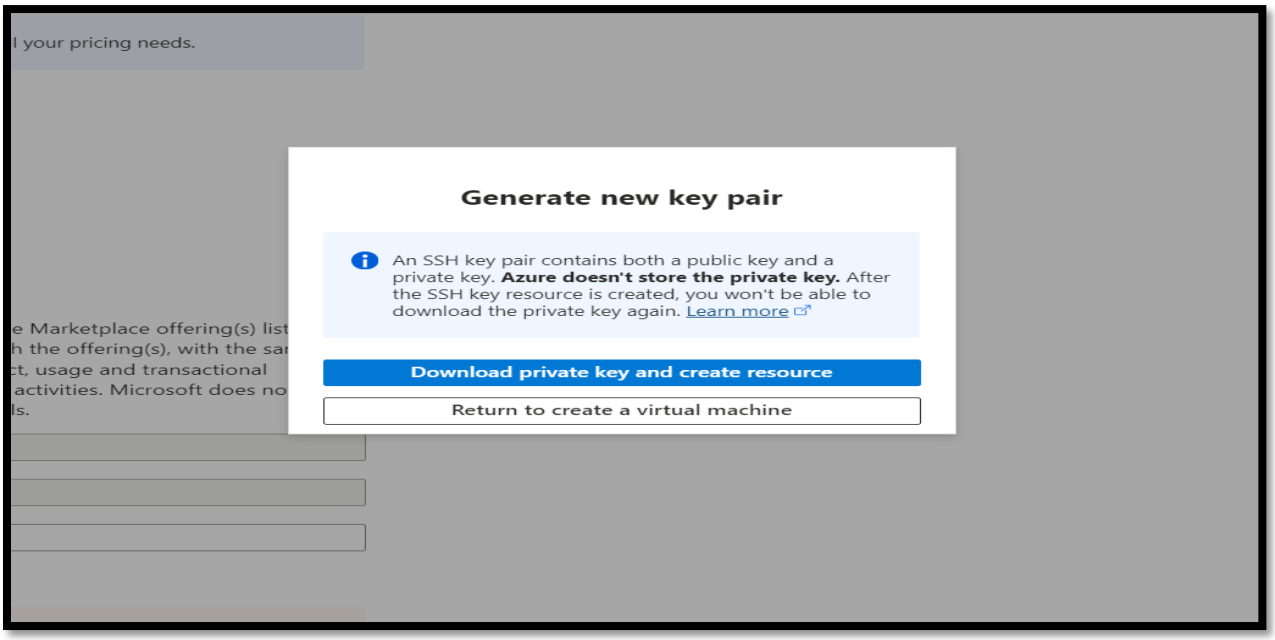
Monitoring



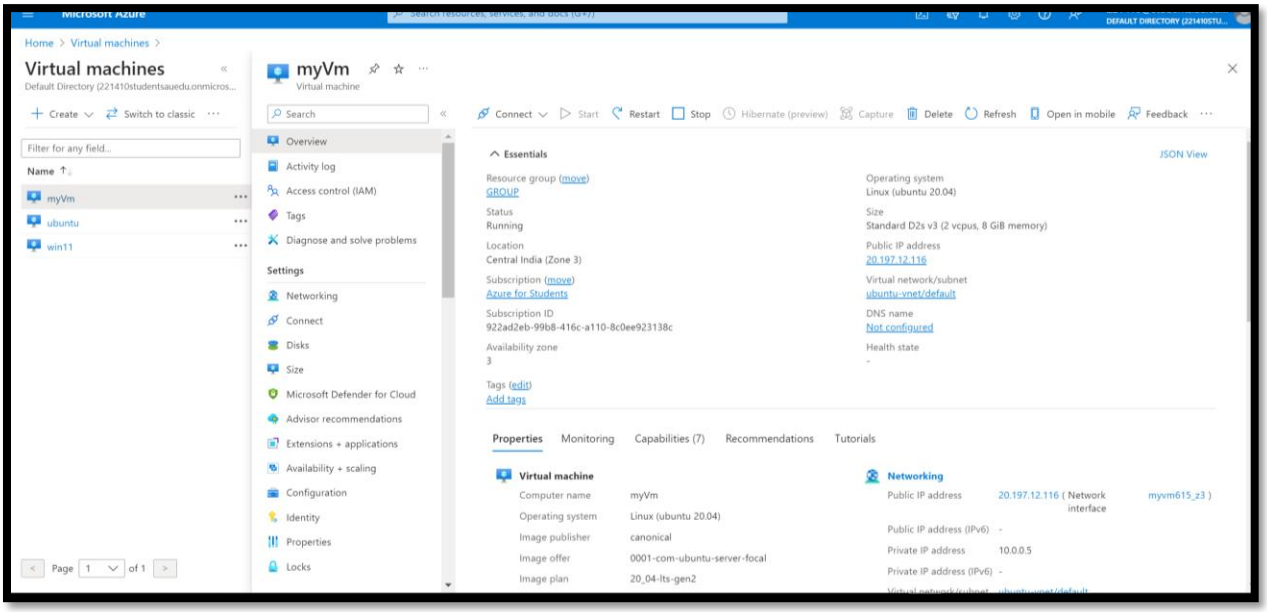
Review and Create



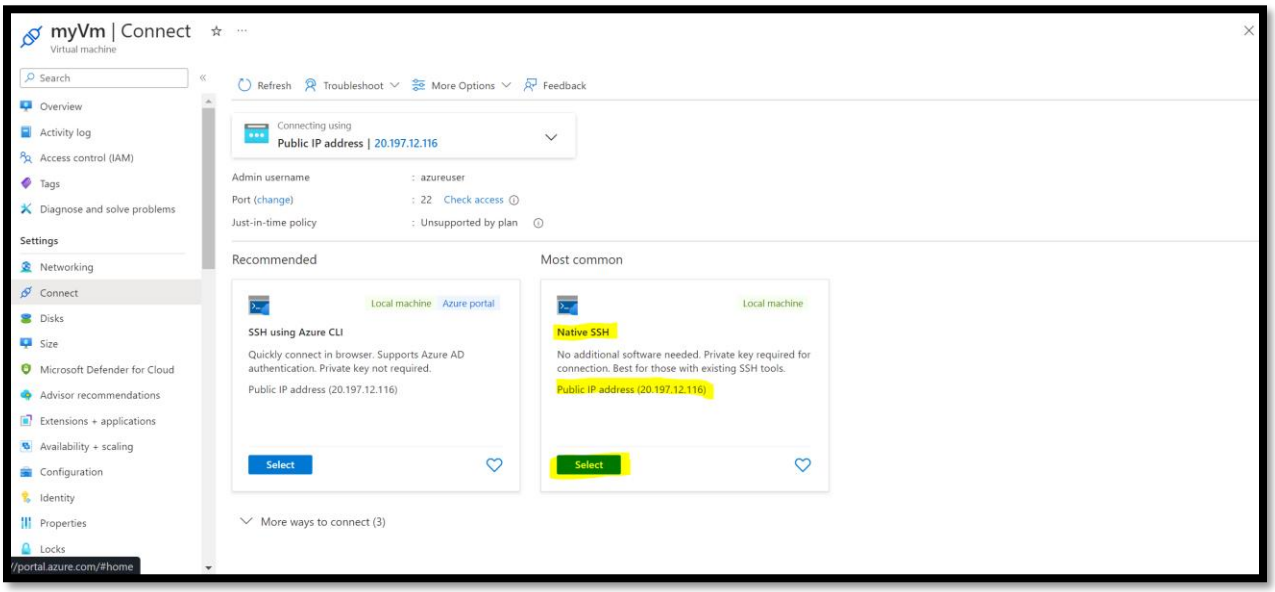
Download Key



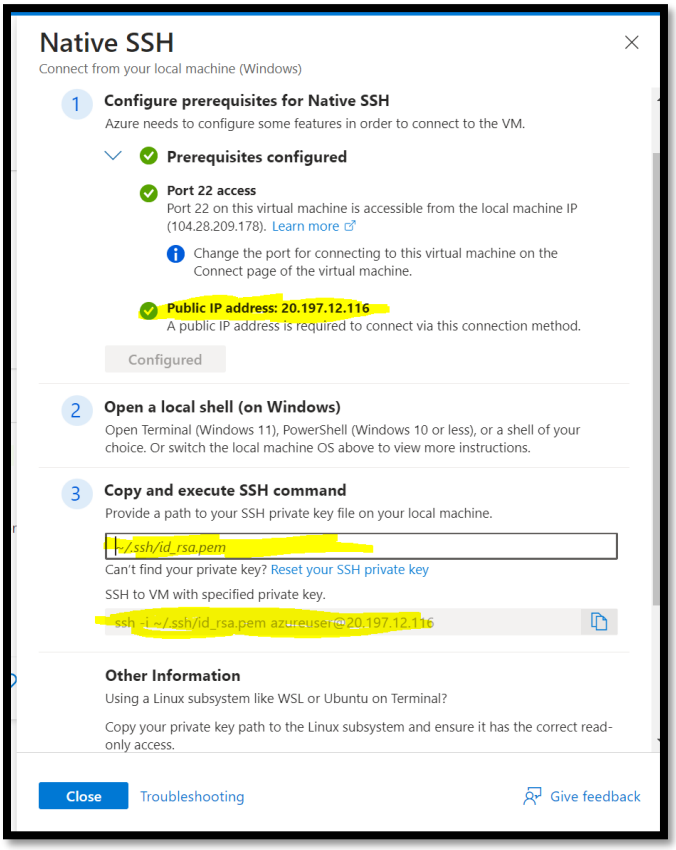
Created



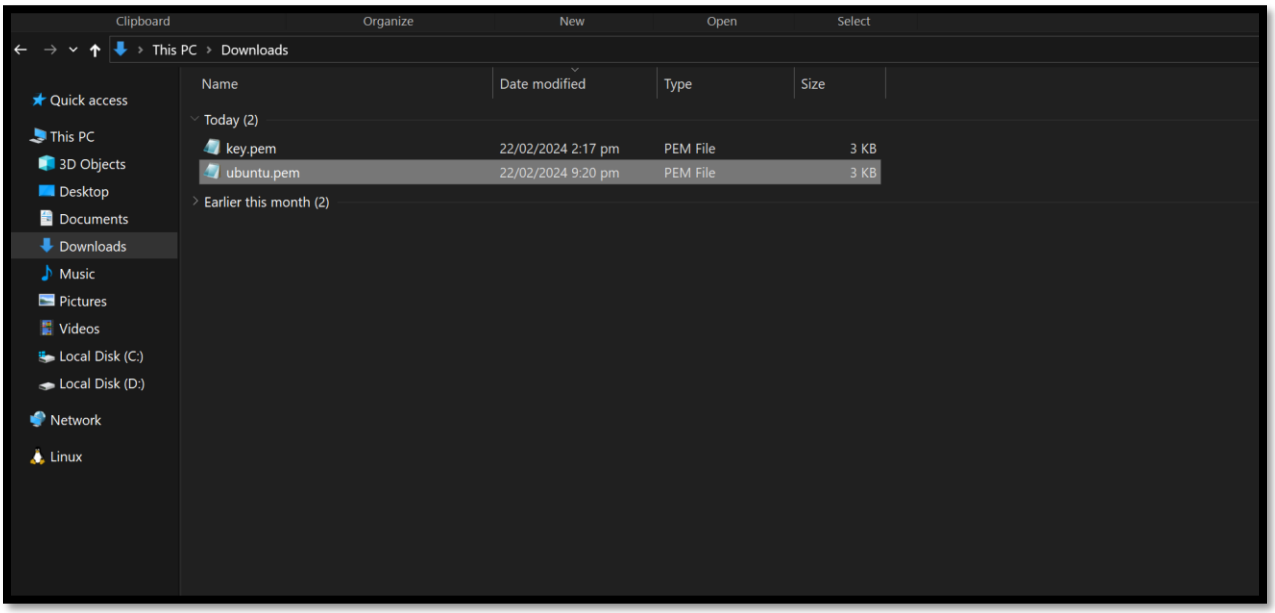
Now start and Connect the Ubuntu Server Virtual Machine to access the Terminal.

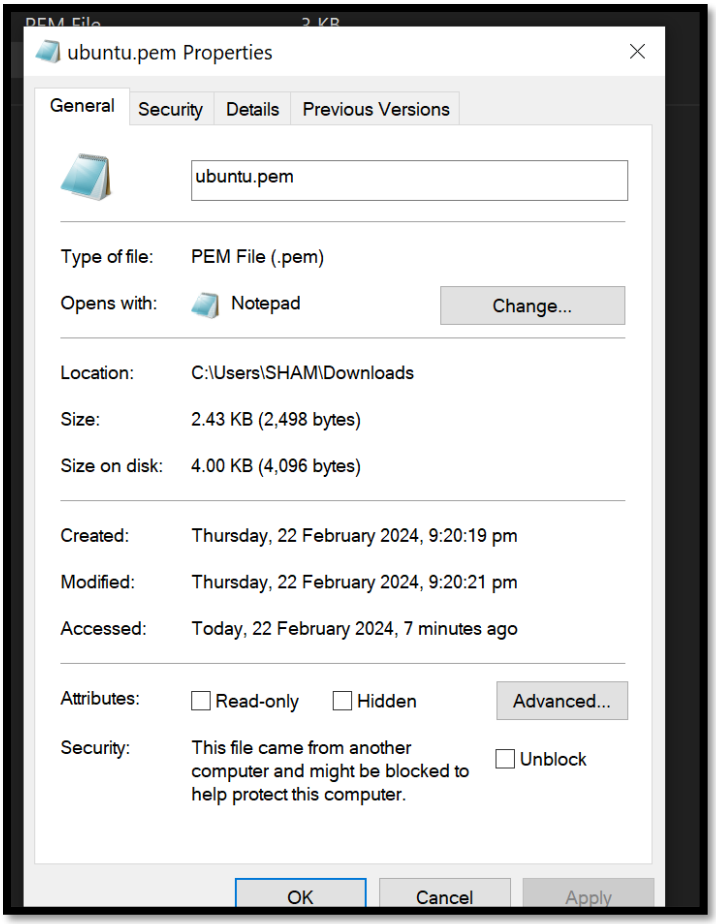


Open Native SSH

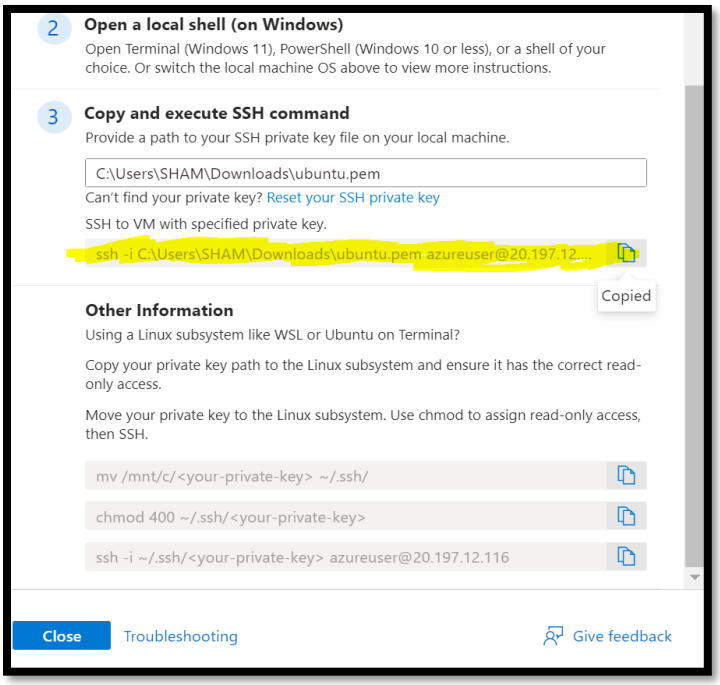


Open properties of pem file



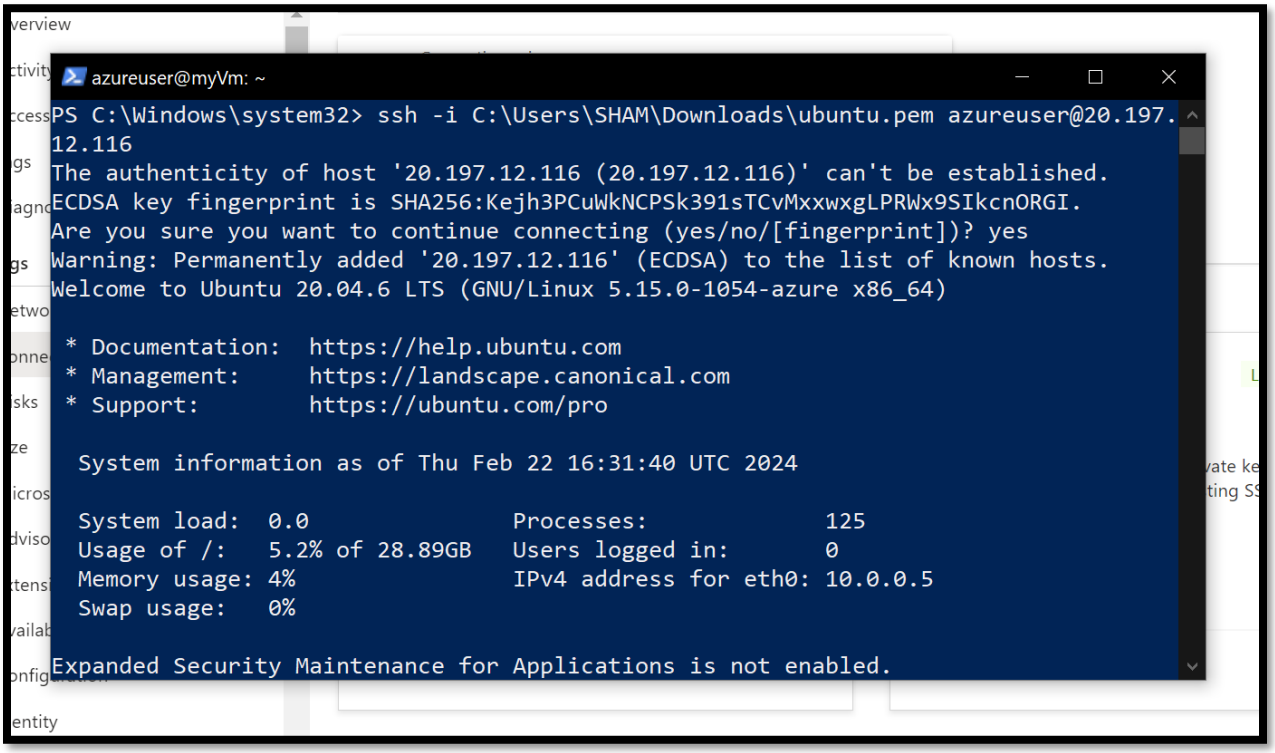


Copy the path of file and paste in ssh command.



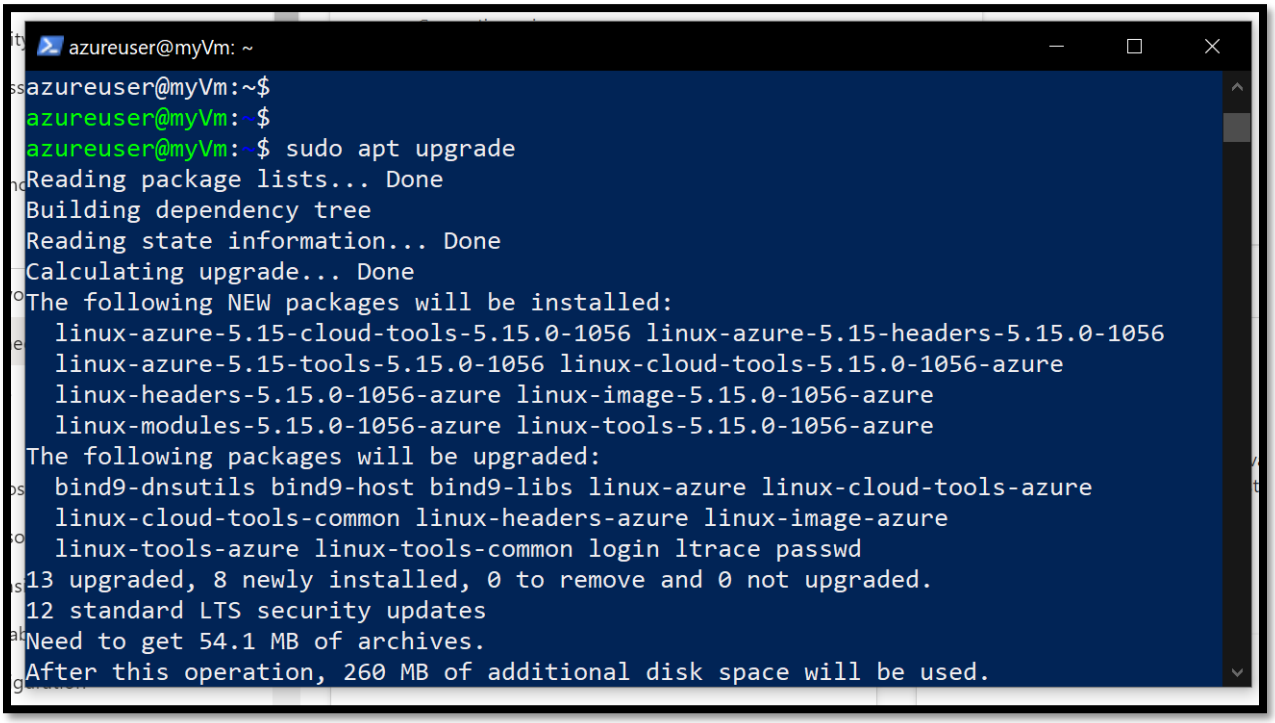
Copy the command and run this in PowerShell as Administrator mode

ssh -i C:\Users\SHAM\Downloads\ubuntu.pem azureuser@20.197.12.116



And you have accessed the Ubuntu server.

First Update and upgrade machine.



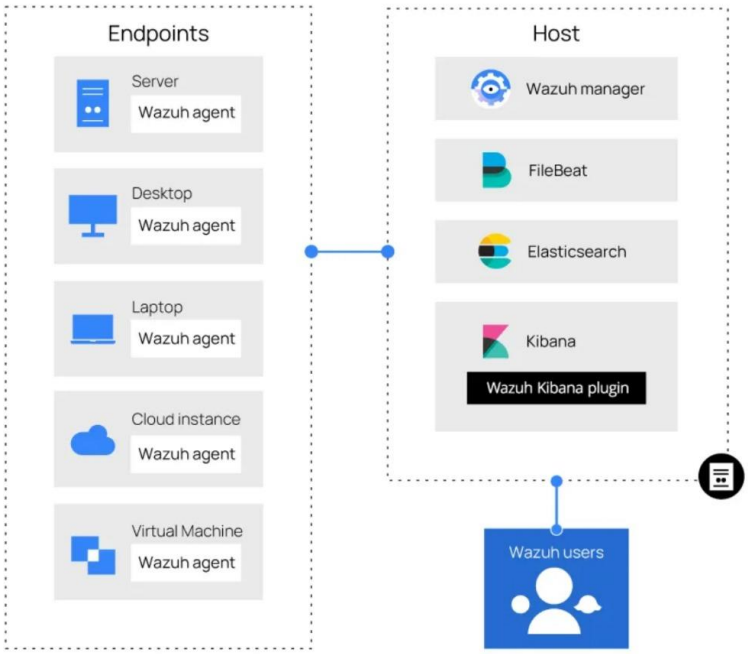
Installing initial packages

Installing Wazuh Server on Ubuntu server.

Step-by-step installation:

Installing Wazuh

The Wazuh server collects and analyzes data from the deployed Wazuh agents. It runs the Wazuh manager, the Wazuh API and Filebeat.

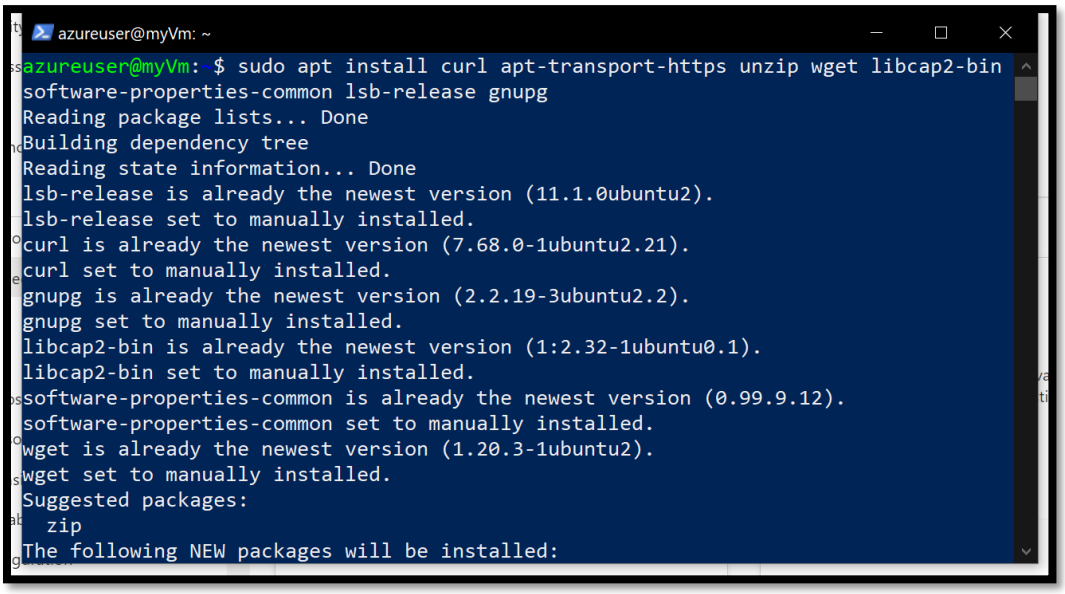


To start setting up Wazuh, add the Wazuh repository to the server.

Command:

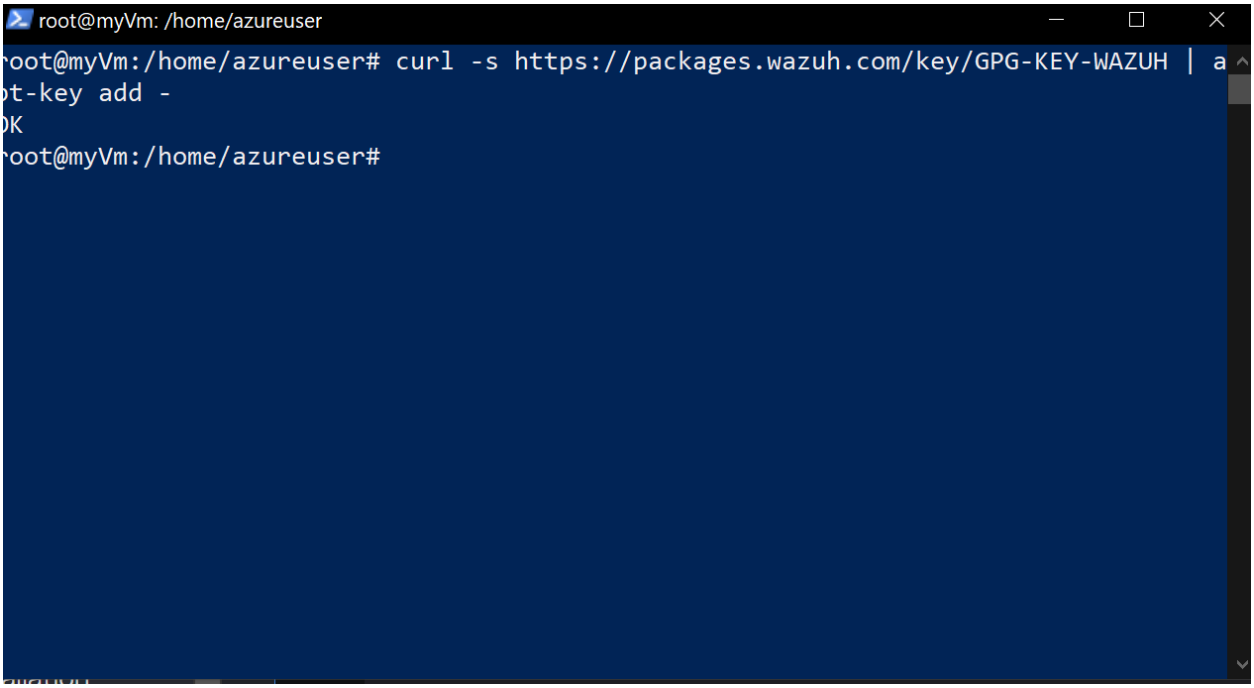
1- <u>Install the necessary packages for the installation:</u>

sudo apt install curl apt-transport-https unzip wget libcap2-bin software-properties-common lsb-release gnupg

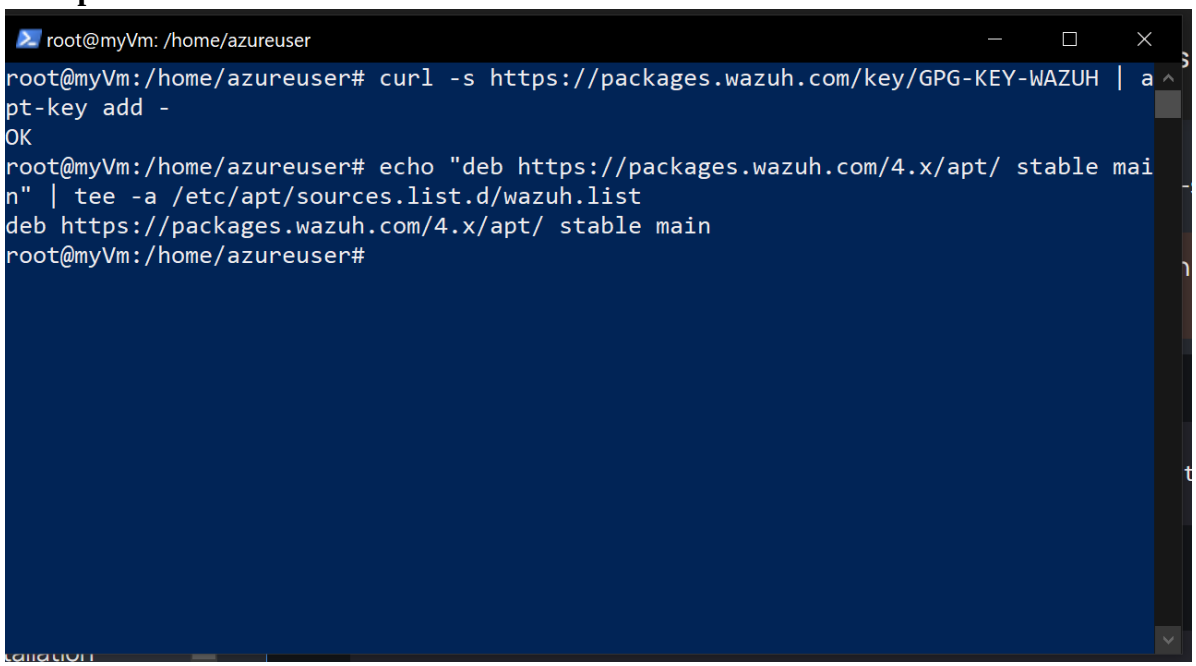


2- <u>Install the GPG key:</u>

curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -



3- Add the repository:
echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list



4- Update the package information:
apt-get update

```
root@myVm: /home/azureuser
Get:5 https://packages.wazuh.com/4.x/apt stable InRelease [17.3 kB]
Get:6 http://azure.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [312
5 kB]
Get:7 http://azure.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [500
 kB]
Get:8 http://azure.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Package
s [2716 kB]
Get:9 http://azure.archive.ubuntu.com/ubuntu focal-updates/restricted Translation-e
n [377 kB]
Get:10 http://azure.archive.ubuntu.com/ubuntu focal-security/main amd64 Packages [2
746 kB]
Get:11 http://azure.archive.ubuntu.com/ubuntu focal-security/main Translation-en [4
16 kB]
Get:12 http://azure.archive.ubuntu.com/ubuntu focal-security/restricted amd64 Packa
ges [2598 kB]
Get:13 http://azure.archive.ubuntu.com/ubuntu focal-security/restricted Translation
-en [362 kB]
Get:14 https://packages.wazuh.com/4.x/apt stable/main amd64 Packages [39.0 kB]
Fetched 13.1 MB in 3s (4944 kB/s)
Reading package lists... 56%
```

Installing the Wazuh manager

1- Install the Wazuh manager package:
apt-get install wazuh-manager=4.2.7-1

```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# apt-get install wazuh-manager=4.2.7-1
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  expect
The following NEW packages will be installed:
  wazuh-manager
0 upgraded, 1 newly installed, 0 to remove and 7 not upgraded.
Need to get 116 MB of archives.
After this operation, 447 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-manager amd64 4.2.
7-1 [116 MB]
36% [1 wazuh-manager 52.6 MB/116 MB 45%]
```

2- <u>Enable and start the Wazuh manager service:</u>

systemctl daemon-reload
systemctl enable wazuh-manager
systemctl start wazuh-manager

```
root@myVm: /home/azureuser
Need to get 116 MB of archives.
After this operation, 447 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-manager amd64 4.2.
7-1 [116 MB]
Fetched 116 MB in 10s (12.2 MB/s)
Selecting previously unselected package wazuh-manager.
(Reading database ... 84319 files and directories currently installed.)
Preparing to unpack .../wazuh-manager_4.2.7-1_amd64.deb ...
Unpacking wazuh-manager (4.2.7-1) ...
Setting up wazuh-manager (4.2.7-1) ...
Processing triggers for systemd (245.4-4ubuntu3.23) ...
root@myVm:/home/azureuser# systemctl daemon-reload
root@myVm:/home/azureuser# systemctl enable wazuh-manager
Synchronizing state of wazuh-manager.service with SysV service script with /lib/sys
temd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable wazuh-manager
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-manager.service →
 /lib/systemd/system/wazuh-manager.service.
root@myVm:/home/azureuser# systemctl start wazuh-manager
```

3- <u>Run the following command to check if the Wazuh manager is active:</u>

systemctl status wazuh-manager

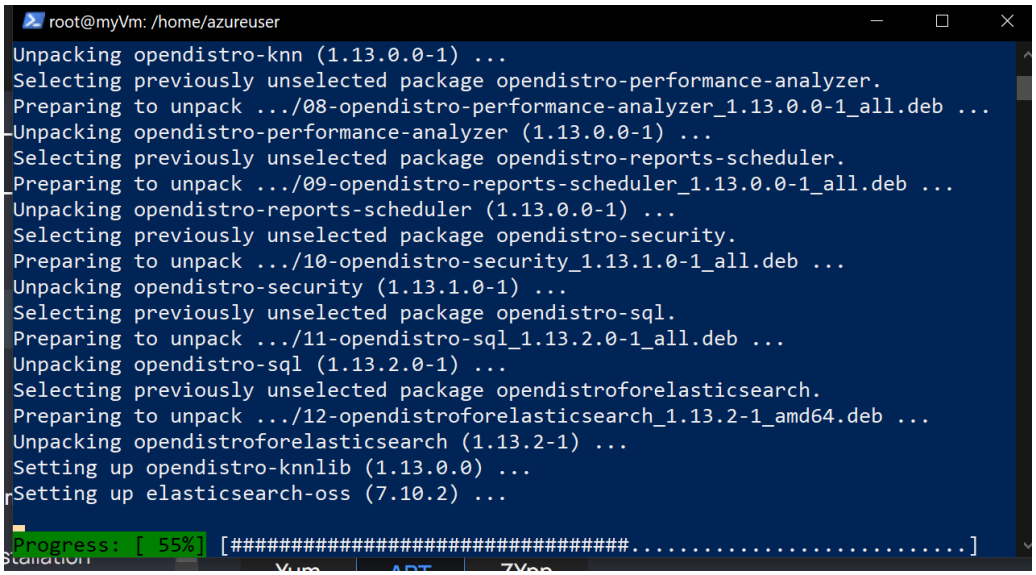
```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor pr>
     Active: active (running) since Sun 2024-02-25 09:51:24 UTC; 1min 46s ago
    Process: 39817 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code>
      Tasks: 108 (limit: 9456)
     Memory: 390.5M
     CGroup: /system.slice/wazuh-manager.service
             ├─39969 /var/ossec/framework/python/bin/python3 /var/ossec/api/script>
             ├─40009 /var/ossec/bin/wazuh-authd
             ├─40025 /var/ossec/bin/wazuh-db
             ├─40056 /var/ossec/bin/wazuh-execd
             ├─40078 /var/ossec/bin/wazuh-analysisd
             ├─40132 /var/ossec/bin/wazuh-syscheckd
             ├─40195 /var/ossec/bin/wazuh-remoted
             ├─40231 /var/ossec/bin/wazuh-logcollector
             ├─40248 /var/ossec/bin/wazuh-monitord
             └─40342 /var/ossec/bin/wazuh-modulesd

Feb 25 09:51:15 myVm env[39817]: Started wazuh-db...
```

Installing Elasticsearch

1- Open Distro for Elasticsearch is an open source distribution of Elasticsearch, a highly scalable full-text search engine. It offers advanced security, alerting, index management, deep performance analysis, and several other additional features.

Install Elasticsearch OSS and Open Distro for Elasticsearch:

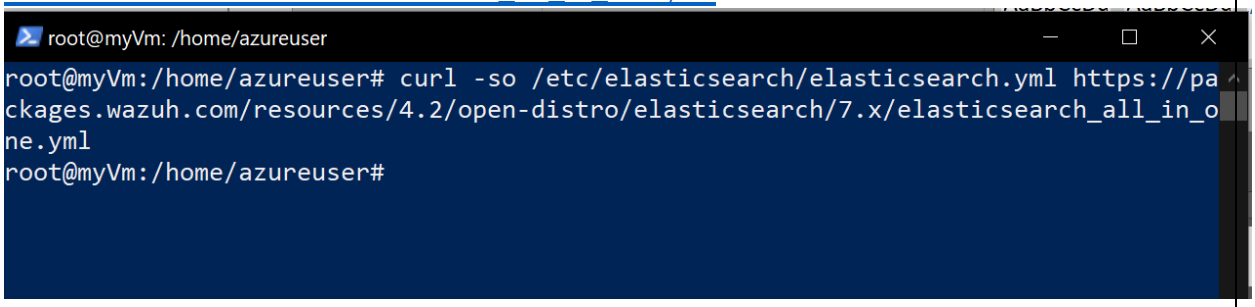
apt install elasticsearch-oss opendistroforelasticsearch



Configuring Elasticsearch

Run the following command to download the configuration file /etc/elasticsearch/elasticsearch.yml:

curl -so /etc/elasticsearch/elasticsearch.yml
https://packages.wazuh.com/resources/4.2/open-distro/elasticsearch/7.x/elasticsearch_all_in_one.yml



Elasticsearch users and roles

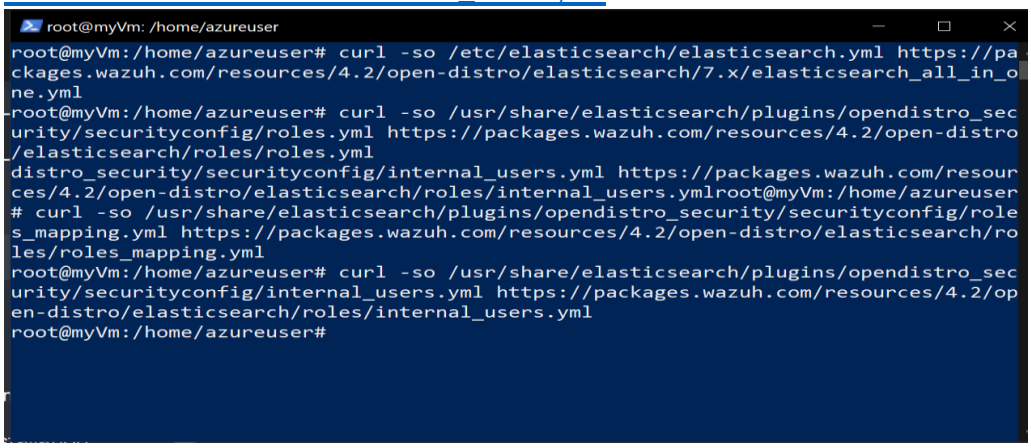
You need to add users and roles in order to use the Wazuh Kibana properly.

Run the following commands to add the Wazuh users and additional roles in Kibana:

curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/roles.yml https://packages.wazuh.com/resources/4.2/open-distro/elasticsearch/roles/roles.yml

curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/roles_mapping.yml https://packages.wazuh.com/resources/4.2/open-distro/elasticsearch/roles/roles_mapping.yml

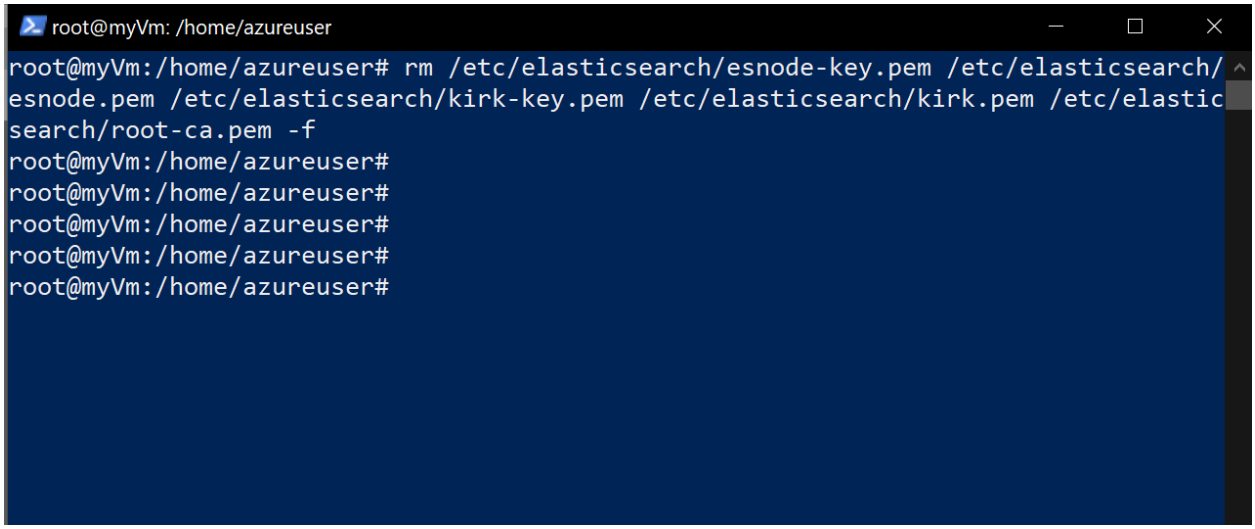
curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/internal_users.yml https://packages.wazuh.com/resources/4.2/open-distro/elasticsearch/roles/internal_users.yml



Certificates creation

1- Remove the demo certificates:

rm /etc/elasticsearch/esnode-key.pem /etc/elasticsearch/esnode.pem /etc/elasticsearch/kirk-key.pem /etc/elasticsearch/kirk.pem /etc/elasticsearch/root-ca.pem –f



2- <u>Generate and deploy the certificates:</u>

- **Download the wazuh-cert-tool.sh:**
  curl -so ~/wazuh-cert-tool.sh https://packages.wazuh.com/resources/4.2/open-distro/tools/certificate-utility/wazuh-cert-tool.sh
  curl -so ~/instances.yml https://packages.wazuh.com/resources/4.2/open-distro/tools/certificate-utility/instances_aio.yml

```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# curl -so ~/wazuh-cert-tool.sh https://packages.wazuh.com
/resources/4.2/open-distro/tools/certificate-utility/wazuh-cert-tool.sh
yml https://packages.wazuh.com/resources/4.2/open-distro/tools/certificate-utility/
-instances_aio.ymlroot@myVm:/home/azureuser# curl -so ~/instances.yml https://packag
es.wazuh.com/resources/4.2/open-distro/tools/certificate-utility/instances_aio.yml
root@myVm:/home/azureuser#
```

- **Run the wazuh-cert-tool.sh to create the certificates:**
  bash ~/wazuh-cert-tool.sh

```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# curl -so ~/wazuh-cert-tool.sh https://packages.wazuh.com
/resources/4.2/open-distro/tools/certificate-utility/wazuh-cert-tool.sh
yml https://packages.wazuh.com/resources/4.2/open-distro/tools/certificate-utility/
instances_aio.ymlroot@myVm:/home/azureuser# curl -so ~/instances.yml https://packag
es.wazuh.com/resources/4.2/open-distro/tools/certificate-utility/instances_aio.yml
root@myVm:/home/azureuser# bash ~/wazuh-cert-tool.sh
02/25/2024 10:11:42 INFO: Configuration file found. Creating certificates...
02/25/2024 10:11:42 INFO: Creating the Elasticsearch certificates...

02/25/2024 10:11:42 INFO: Creating Wazuh server certificates...
02/25/2024 10:11:42 INFO: Creating Kibana certificate...
02/25/2024 10:11:42 INFO: Certificates creation finished. They can be found in ~/ce
rts.
root@myVm:/home/azureuser#
root@myVm:/home/azureuser#
```

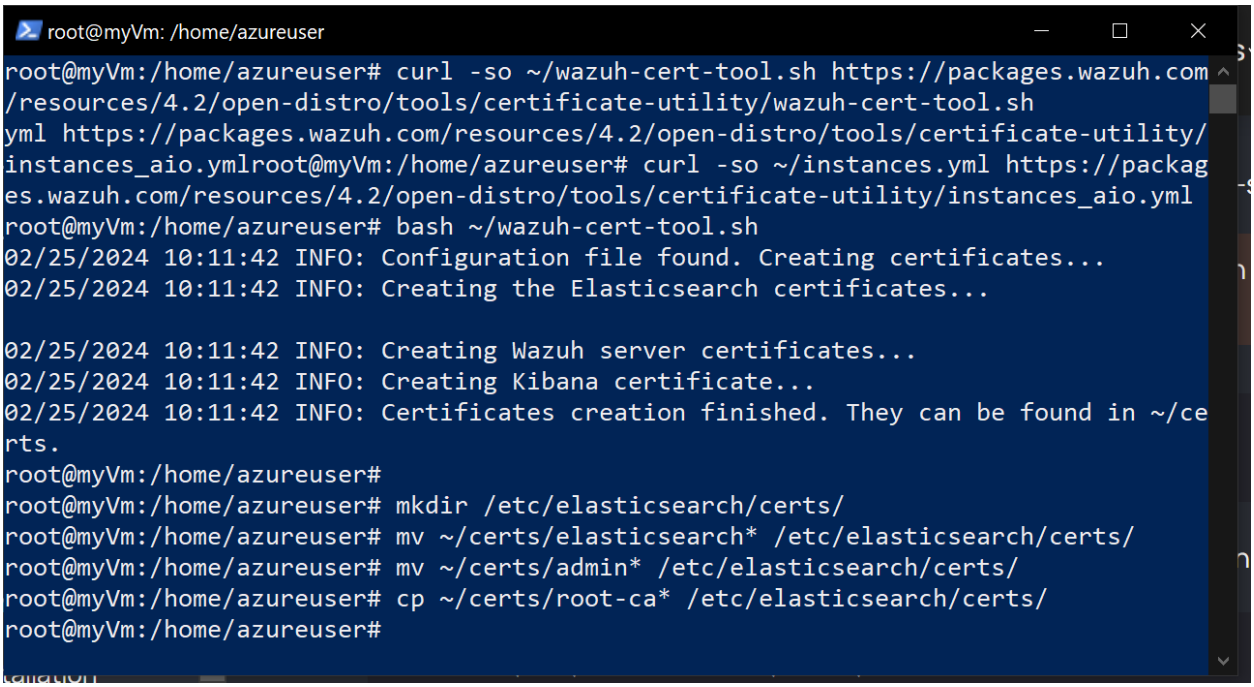
- **Move the Elasticsearch certificates to their corresponding location:**

mkdir /etc/elasticsearch/certs/

mv ~/certs/elasticsearch* /etc/elasticsearch/certs/

mv ~/certs/admin* /etc/elasticsearch/certs/

cp ~/certs/root-ca* /etc/elasticsearch/certs/



3- <u>Enable and start the Elasticsearch service:</u>

<u>Warning</u>
Add the following configuration to mitigate Apache Log4j2 Remote Code Execution (RCE) vulnerability - CVE-2021-44228 - ESA-2021-31.
mkdir -p /etc/elasticsearch/jvm.options.d
echo '-Dlog4j2.formatMsgNoLookups=true' > /etc/elasticsearch/jvm.options.d/disabledlog4j.options
chmod 2750 /etc/elasticsearch/jvm.options.d/disabledlog4j.options
chown root:elasticsearch /etc/elasticsearch/jvm.options.d/disabledlog4j.options

```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# mkdir -p /etc/elasticsearch/jvm.options.d
root@myVm:/home/azureuser# echo '-Dlog4j2.formatMsgNoLookups=true' > /etc/elasticse
arch/jvm.options.d/disabledlog4j.options
root@myVm:/home/azureuser# chmod 2750 /etc/elasticsearch/jvm.options.d/disabledlog4
j.options
root@myVm:/home/azureuser# chown root:elasticsearch /etc/elasticsearch/jvm.options.
d/disabledlog4j.options
root@myVm:/home/azureuser#
```

4- Run the Following commands to start elastic search

systemctl daemon-reload

systemctl enable elasticsearch

systemctl start elasticsearch

```
root@myVm: /home/azureuser
Synchronizing state of elasticsearch.service with SysV service script with /lib/sys
temd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service →
 /lib/systemd/system/elasticsearch.service.
root@myVm:/home/azureuser# systemctl start elastic
Failed to start elastic.service: Unit elastic.service not found.
root@myVm:/home/azureuser# systemctl daemon-reload
root@myVm:/home/azureuser# systemctl enable elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /lib/sys
temd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
root@myVm:/home/azureuser# systemctl start elasticsearch

root@myVm:/home/azureuser#
root@myVm:/home/azureuser#
```

5- Run the Elasticsearch securityadmin script to load the new certificates information and start the cluster:

export JAVA_HOME=/usr/share/elasticsearch/jdk/ && /usr/share/elasticsearch/plugins/opendistro_security/tools/securityadmin.sh -cd /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/ -nhnv -cacert /etc/elasticsearch/certs/root-ca.pem -cert /etc/elasticsearch/certs/admin.pem -key /etc/elasticsearch/certs/admin-key.pem

```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# export JAVA_HOME=/usr/share/elasticsearch/jdk/ && /usr/s
hare/elasticsearch/plugins/opendistro_security/tools/securityadmin.sh -cd /usr/shar
e/elasticsearch/plugins/opendistro_security/securityconfig/ -nhnv -cacert /etc/elas
ticsearch/certs/root-ca.pem -cert /etc/elasticsearch/certs/admin.pem -key /etc/elas
ticsearch/certs/admin-key.pem
Open Distro Security Admin v7
Will connect to localhost:9300 ... done
Connected as CN=admin,OU=Docu,O=Wazuh,L=California,C=US
Elasticsearch Version: 7.10.2
Open Distro Security Version: 1.13.1.0
Contacting elasticsearch cluster 'elasticsearch' and wait for YELLOW clusterstate .
..
Clustername: elasticsearch
Clusterstate: GREEN
Number of nodes: 1
Number of data nodes: 1
.opendistro_security index does not exists, attempt to create it ... done (0-all re
plicas)
Populate config from /usr/share/elasticsearch/plugins/opendistro_security/securityc
onfig/
```

6- <u>Run the following command to ensure that the installation is successful:</u>

curl -XGET https://localhost:9200 -u admin:admin –k

```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# curl -XGET https://localhost:9200 -u admin:admin -k
{
  "name" : "node-1",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "Z-BN1371TTGKjmsvSGLYvA",
  "version" : {
    "number" : "7.10.2",
    "build_flavor" : "oss",
    "build_type" : "deb",
    "build_hash" : "747e1cc71def077253878a59143c1f785afa92b9",
    "build_date" : "2021-01-13T00:42:12.435326Z",
    "build_snapshot" : false,
    "lucene_version" : "8.7.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
root@myVm:/home/azureuser#
```

<u>Installing Filebeat</u>

Filebeat is the tool on the Wazuh server that securely forwards alerts and archived events to Elasticsearch.

1- Install the Filebeat package:
   apt-get install filebeat

```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# apt-get install filebeat
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  filebeat
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 22.1 MB of archives.
After this operation, 73.6 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 filebeat amd64 7.10.2 [2
2.1 MB]
Fetched 22.1 MB in 0s (66.7 MB/s)
Selecting previously unselected package filebeat.
(Reading database ... 129349 files and directories currently installed.)
Preparing to unpack .../filebeat_7.10.2_amd64.deb ...
Unpacking filebeat (7.10.2) ...
Setting up filebeat (7.10.2) ...
Processing triggers for systemd (245.4-4ubuntu3.23) ...
root@myVm:/home/azureuser#
```

2- Download the preconfigured Filebeat configuration file used to forward the Wazuh alerts to Elasticsearch:

curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/resources/4.2/open-distro/filebeat/7.x/filebeat_all_in_one.yml

```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# curl -so /etc/filebeat/filebeat.yml https://packages.waz
uh.com/resources/4.2/open-distro/filebeat/7.x/filebeat_all_in_one.yml
root@myVm:/home/azureuser#
```

3- Download the alerts template for Elasticsearch:

curl -so /etc/filebeat/wazuh-template.json https://raw.githubusercontent.com/wazuh/wazuh/4.2/extensions/elasticsearch/7.x/wazuh-template.json

chmod go+r /etc/filebeat/wazuh-template.json

```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# curl -so /etc/filebeat/wazuh-template.json https://raw.g
ithubusercontent.com/wazuh/wazuh/4.2/extensions/elasticsearch/7.x/wazuh-template.js
on
r /etc/filebeat/wazuh-template.jsonroot@myVm:/home/azureuser# chmod go+r /etc/fileb
eat/wazuh-template.json
root@myVm:/home/azureuser#
```

4- Download the Wazuh module for Filebeat:

curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.1.tar.gz | tar -xvz -C /usr/share/filebeat/module

```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# curl -so /etc/filebeat/wazuh-template.json https://raw.g
ithubusercontent.com/wazuh/wazuh/4.2/extensions/elasticsearch/7.x/wazuh-template.js
on
r /etc/filebeat/wazuh-template.jsonroot@myVm:/home/azureuser# chmod go+r /etc/fileb
eat/wazuh-template.json
root@myVm:/home/azureuser# curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-fi
lebeat-0.1.tar.gz | tar -xvz -C /usr/share/filebeat/module
wazuh/
wazuh/module.yml
wazuh/archives/
wazuh/archives/config/
wazuh/archives/config/archives.yml
wazuh/archives/ingest/
wazuh/archives/ingest/pipeline.json
wazuh/archives/manifest.yml
wazuh/alerts/
wazuh/alerts/config/
wazuh/alerts/config/alerts.yml
wazuh/alerts/ingest/
wazuh/alerts/ingest/pipeline.json
```

5- Copy the Elasticsearch certificates into /etc/filebeat/certs:

mkdir /etc/filebeat/certs

cp ~/certs/root-ca.pem /etc/filebeat/certs/

mv ~/certs/filebeat* /etc/filebeat/certs/

```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# mkdir /etc/filebeat/certs
root@myVm:/home/azureuser# cp ~/certs/root-ca.pem /etc/filebeat/certs/
root@myVm:/home/azureuser# mv ~/certs/filebeat* /etc/filebeat/certs/
root@myVm:/home/azureuser#
```

5- Enable and start the Filebeat service:

systemctl daemon-reload
systemctl enable filebeat
systemctl start filebeat

```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# mkdir /etc/filebeat/certs
root@myVm:/home/azureuser# cp ~/certs/root-ca.pem /etc/filebeat/certs/
root@myVm:/home/azureuser# mv ~/certs/filebeat* /etc/filebeat/certs/
root@myVm:/home/azureuser# systemctl daemon-reload
root@myVm:/home/azureuser# systemctl enable filebeat
Synchronizing state of filebeat.service with SysV service script with /lib/systemd/
systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable filebeat
Created symlink /etc/systemd/system/multi-user.target.wants/filebeat.service → /lib
/systemd/system/filebeat.service.
root@myVm:/home/azureuser# systemctl start filebeat
root@myVm:/home/azureuser#
```

6- To ensure that Filebeat is successfully installed, run the following command:

filebeat test output

```
root@myVm: /home/azureuser
Executing: /lib/systemd/systemd-sysv-install enable filebeat
Created symlink /etc/systemd/system/multi-user.target.wants/filebeat.service → /lib
/systemd/system/filebeat.service.
root@myVm:/home/azureuser# systemctl start filebeat
root@myVm:/home/azureuser# filebeat test output
elasticsearch: https://127.0.0.1:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 127.0.0.1
    dial up... OK
  TLS...
    security: server's certificate chain verification is enabled
    handshake... OK
    TLS version: TLSv1.3
    dial up... OK
  talk to server... OK
  version: 7.10.2
root@myVm:/home/azureuser#
```

Installing Kibana

Kibana is a flexible and intuitive web interface for mining and visualizing the events and archives stored in Elasticsearch.

1- Install the Kibana package:
apt-get install opendistroforelasticsearch-kibana

```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# apt-get install opendistroforelasticsearch-kibana
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  opendistroforelasticsearch-kibana
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 234 MB of archives.
After this operation, 692 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 opendistroforelasticsear
ch-kibana amd64 1.13.2 [234 MB]
Fetched 234 MB in 17s (14.0 MB/s)
Selecting previously unselected package opendistroforelasticsearch-kibana.
(Reading database ... 129668 files and directories currently installed.)
Preparing to unpack .../opendistroforelasticsearch-kibana_1.13.2_amd64.deb ...
Unpacking opendistroforelasticsearch-kibana (1.13.2) ...
```

2- Download the Kibana configuration file:

curl -so /etc/kibana/kibana.yml https://packages.wazuh.com/resources/4.2/open-distro/kibana/7.x/kibana_all_in_one.yml

```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# curl -so /etc/kibana/kibana.yml https://packages.wazuh.c
om/resources/4.2/open-distro/kibana/7.x/kibana_all_in_one.yml
root@myVm:/home/azureuser#
```

3- Create the /usr/share/kibana/data directory:
mkdir /usr/share/kibana/data
chown -R kibana:kibana /usr/share/kibana/data

```
Select root@myVm: /home/azureuser
root@myVm:/home/azureuser# mkdir /usr/share/kibana/data
root@myVm:/home/azureuser# chown -R kibana:kibana /usr/share/kibana/data
root@myVm:/home/azureuser#
```

4- Install the Wazuh Kibana plugin. The installation of the plugin must be done from the Kibana home directory as follows:

cd /usr/share/kibana

sudo -u kibana /usr/share/kibana/bin/kibana-plugin install

https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana-4.2.7_7.10.2-1.zip

```
root@myVm: /usr/share/kibana
root@myVm:/home/azureuser# cd /usr/share/kibana
root@myVm:/usr/share/kibana# sudo -u kibana /usr/share/kibana/bin/kibana-plugin ins
tall https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana-4.2.7_7.10.2-1.zip
Attempting to transfer from https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana-4
.2.7_7.10.2-1.zip
Transferring 31233769 bytes....................
Transfer complete
Retrieving metadata from plugin archive
Extracting plugin archive
Extraction complete
Plugin installation complete
root@myVm:/usr/share/kibana#
```

5- Copy the Elasticsearch certificates into /etc/kibana/certs:

mkdir /etc/kibana/certs

cp ~/certs/root-ca.pem /etc/kibana/certs/

mv ~/certs/kibana* /etc/kibana/certs/

chown kibana:kibana /etc/kibana/certs/*

```
root@myVm: /usr/share/kibana
root@myVm:/usr/share/kibana# mkdir /etc/kibana/certs
root@myVm:/usr/share/kibana# cp ~/certs/root-ca.pem /etc/kibana/certs/
root@myVm:/usr/share/kibana# mv ~/certs/kibana* /etc/kibana/certs/
root@myVm:/usr/share/kibana# chown kibana:kibana /etc/kibana/certs/*
root@myVm:/usr/share/kibana#
```

6- Link Kibana socket to privileged port 443:

setcap 'cap_net_bind_service=+ep' /usr/share/kibana/node/bin/node

```
root@myVm: /usr/share/kibana
root@myVm:/usr/share/kibana# setcap 'cap_net_bind_service=+ep' /usr/share/kibana/no
de/bin/node
root@myVm:/usr/share/kibana#
```

7- <u>Enable and start the Kibana service:</u>

systemctl daemon-reload
systemctl enable kibana
systemctl start kibana

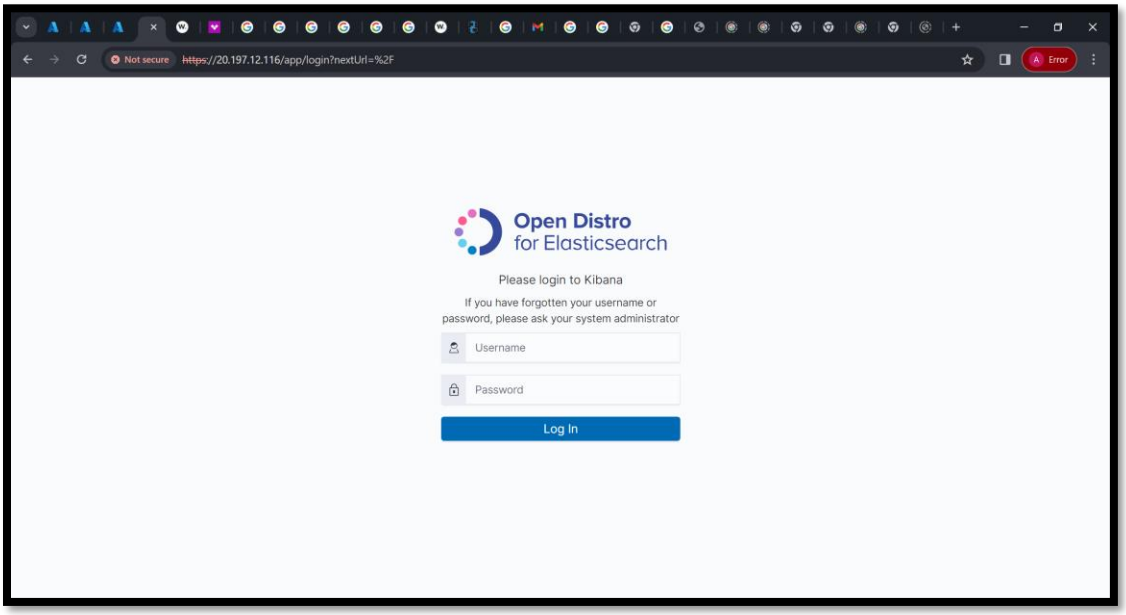
```
root@myVm: /usr/share/kibana
root@myVm:/usr/share/kibana# systemctl daemon-reload
root@myVm:/usr/share/kibana# systemctl enable kibana
Synchronizing state of kibana.service with SysV service script with /lib/systemd/sy
stemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /etc/s
ystemd/system/kibana.service.
root@myVm:/usr/share/kibana# systemctl start kibana
root@myVm:/usr/share/kibana#
```

8- <u>Access the web interface:</u>

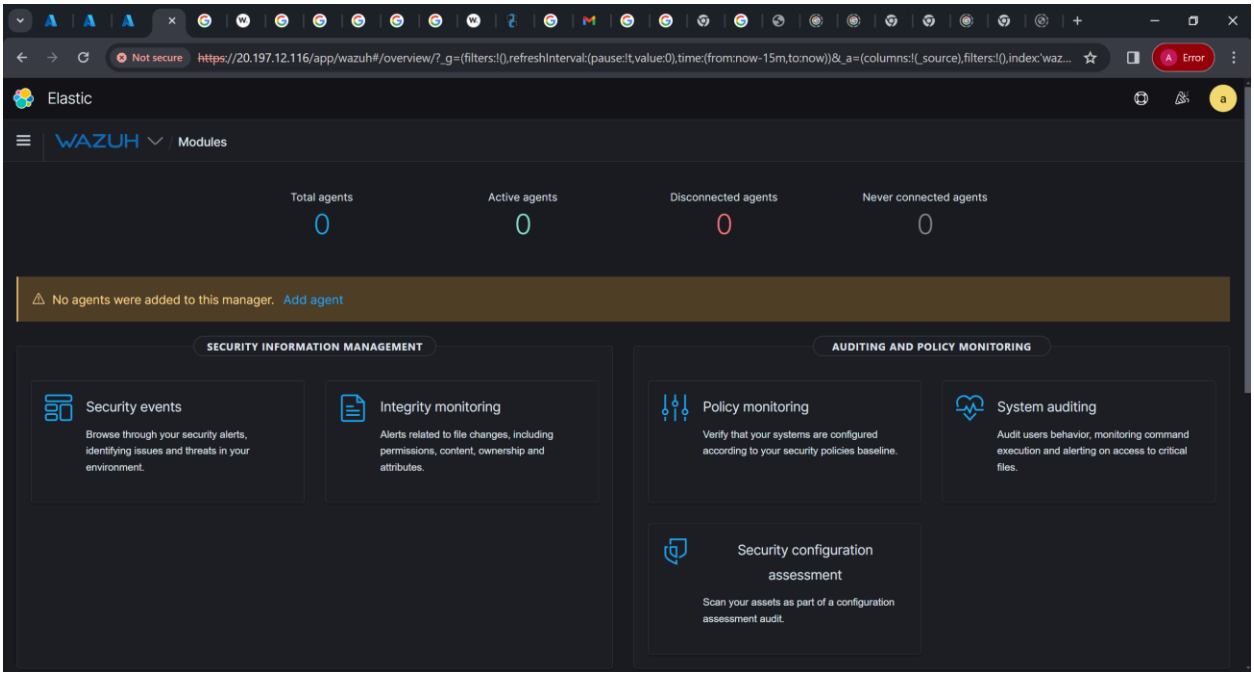
URL: https://<wazuh_server_ip>

user: admin

password: admin



And Finally we got the DashBoard



Conclusions:

This documentation outlines the deployment of Wazuh Server on a cloud platform, covering setup, configuration, and integration with Elasticsearch, Filebeat, and Kibana for effective security monitoring and management. The step-by-step guide enables users to establish a comprehensive security infrastructure, leveraging Elasticsearch's scalability and Kibana's visualization capabilities to create a functional security dashboard.