



wazuh.
The Open Source Security Platform



Document By:

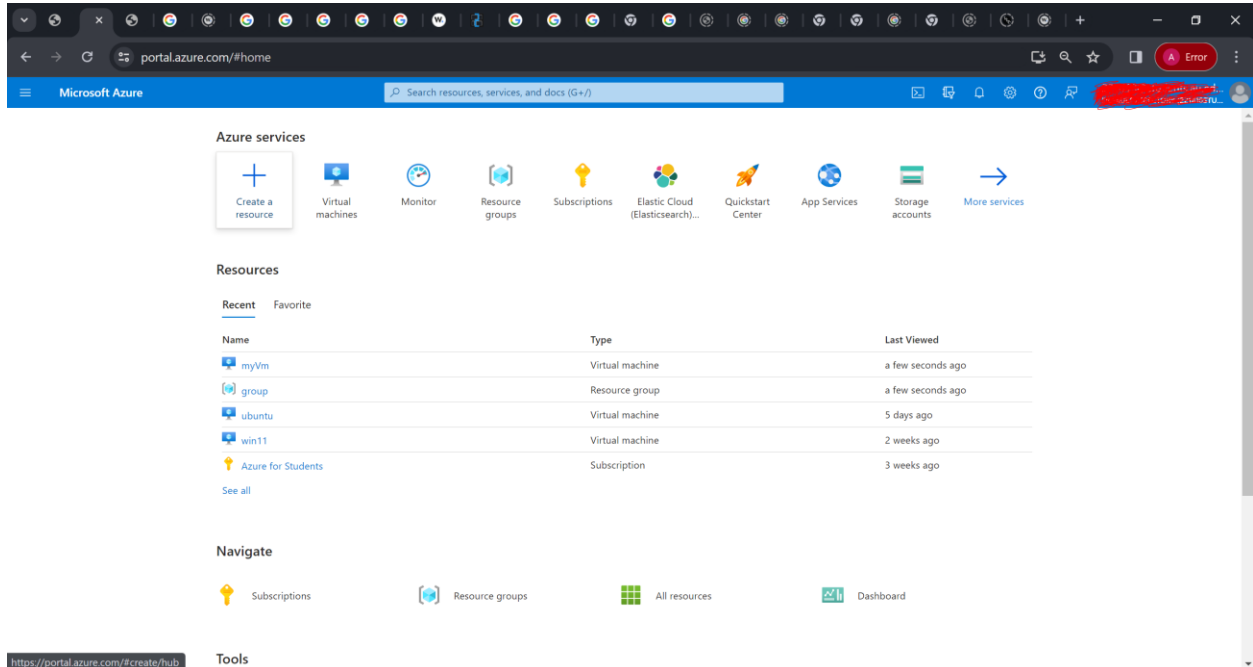
<https://www.linkedin.com/in/ehtishamcyber/>

Documentation Wazuh

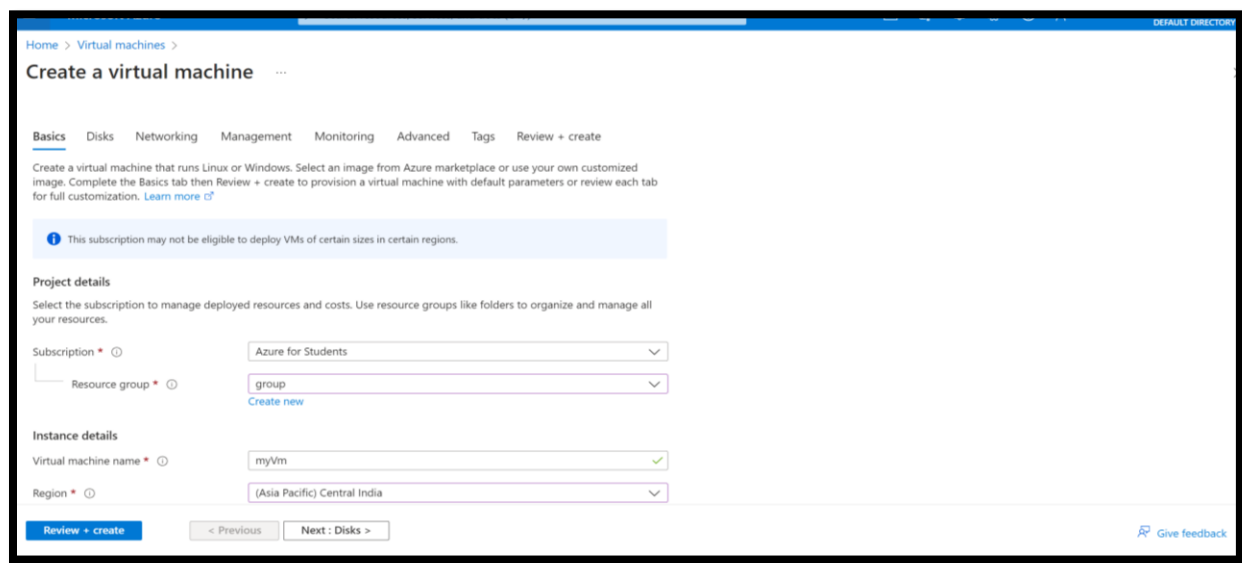
In this Documentation I will be Demonstrating the Wazuh Server on Cloud Platform such as Microsoft Azure.

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.

Create a virtual machine

Security type ⓘ Trusted launch virtual machines ▼
[Configure security features](#)

Image * ⓘ Ubuntu Server 20.04 LTS - x64 Gen2 ▼
[See all images](#) | [Configure VM generation](#)

VM architecture ⓘ ☐ Arm64
☒ x64

Run with Azure Spot discount ⓘ ☐

Size * ⓘ Standard_D2s_v3 - 2 vcpus, 8 GiB memory (\$76.65/month) ▼
[See all sizes](#)

Enable Hibernation (preview) ⓘ ☐
 ⓘ To enable Hibernation, you must register your subscription. [Learn more](#) ↗

Administrator account

Authentication type ⓘ ☒ SSH public key
☐ Password

Review + create < Previous Next : Disks >

Setting up ports

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ ☐ None
☒ Allow selected ports

Select inbound ports * HTTP (80), HTTPS (443), SSH (22) ▼

☒ HTTP (80)
☒ HTTPS (443)
☒ SSH (22)

Review + create < Previous Next : Disks >

Setting up Disk for storing Server related

Microsoft Azure

Search resources, services, and docs (G+/J)

[Home](#) > [Virtual machines](#) >

Create a virtual machine

Basics **Disks** Networking Management Monitoring Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host ☐

Encryption at host is not registered for the selected subscription. [Learn more about enabling this feature](#)

OS disk

OS disk size

OS disk type

Delete with VM ☒

Key management

Enable Ultra Disk compatibility ☐

Data disks for myVm

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM
-----	------	------------	-----------	--------------	----------------

[Create and attach a new disk](#) [Attach an existing disk](#)

Review + create

< Previous

Next : Networking >

Setting up Network for communication

Home

Virtual machines

Create a virtual machine

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network [Create new](#)

Subnet [Manage subnet configuration](#)

Public IP [Create new](#)

NIC network security group ☐ None ☒ Basic ☐ Advanced

Public inbound ports ☐ None ☒ Allow selected ports

Select inbound ports

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Delete public IP and NIC when VM is ☐

Review + create

< Previous

Next : Management >

Management

[Home](#) > [Virtual machines](#) >

Create a virtual machine

Basics Disks Networking **Management** Monitoring Advanced Tags Review + create

Configure management options for your VM.

Microsoft Defender for Cloud

Microsoft Defender for Cloud provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more](#)

✓ Your subscription is protected by Microsoft Defender for Cloud basic plan.

Identity

Enable system assigned managed identity ☐

i To enable system-assigned managed identity, change your orchestration mode to Uniform on the Basics tab

Azure AD

Login with Azure AD ☐

i RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Azure AD login. [Learn more](#)

i Azure AD login now uses SSH certificate-based authentication. You will need to use an SSH client that supports OpenSSH certificates. You can use Azure CLI or Cloud Shell from the Azure Portal. [Learn more](#)

Auto-shutdown

Enable auto-shutdown ☒

Shutdown time

[Review + create](#) [< Previous](#) [Next : Monitoring >](#)

Monitoring

Microsoft Azure [Search resources, services, and docs \(G+7\)](#)

[Home](#) > [Virtual machines](#) >

Create a virtual machine

Basics Disks Networking Management **Monitoring** Advanced Tags Review + create

Configure monitoring options for your VM.

Alerts

Enable recommended alert rules ☐

Diagnostics

Boot diagnostics ☒ Enable with managed storage account (recommended)
☐ Enable with custom storage account
☐ Disable

Enable OS guest diagnostics ☐

Health

Enable application health monitoring ☐

[Review + create](#) [< Previous](#) [Next : Advanced >](#)

Review and Create

Microsoft Azure

Search resources, services, and docs (G+)

[Home](#) > [Virtual machines](#) >

Create a virtual machine

Validation passed

Basics

Disks

Networking

Management

Monitoring

Advanced

Tags

Review + create

Cost given below is an estimate and not the final price. Please use [Pricing calculator](#) for all your pricing needs.

Price

1 X Standard D2s v3

by Microsoft

[Terms of use](#) | [Privacy policy](#)

Subscription credits apply

0.1050 USD/hr

[Pricing for other VM sizes](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Name

Abdul Aziz

Preferred e-mail address

221410@students.au.edu.pk

Preferred phone number

Create

< Previous

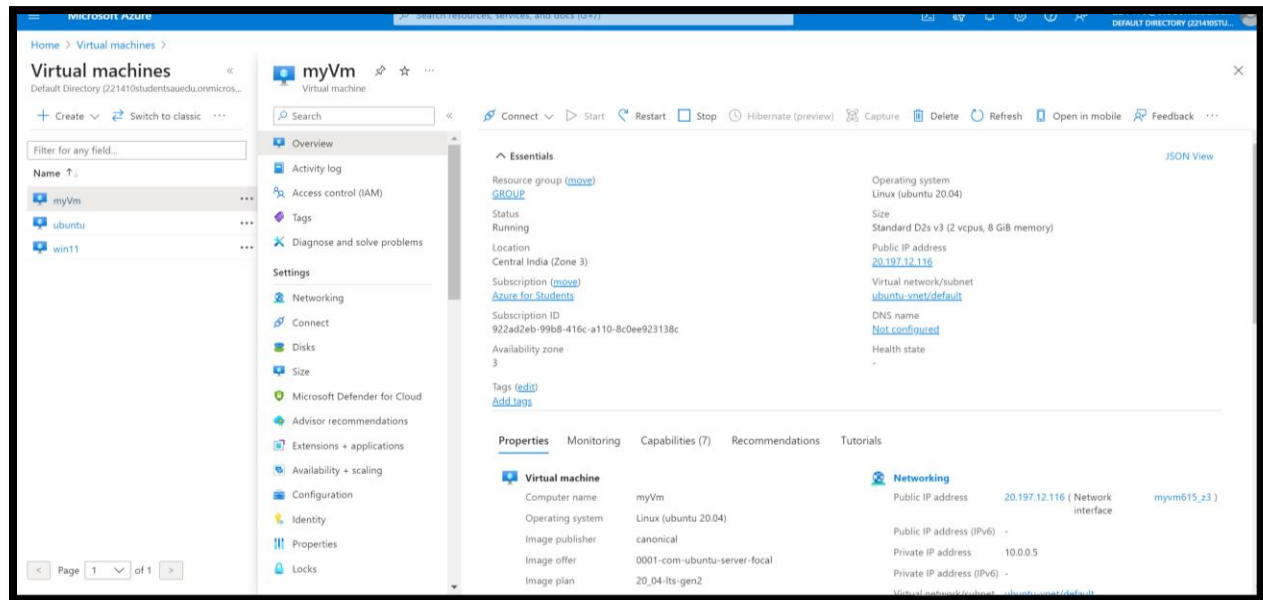
Next >

[Download a template for automation](#)

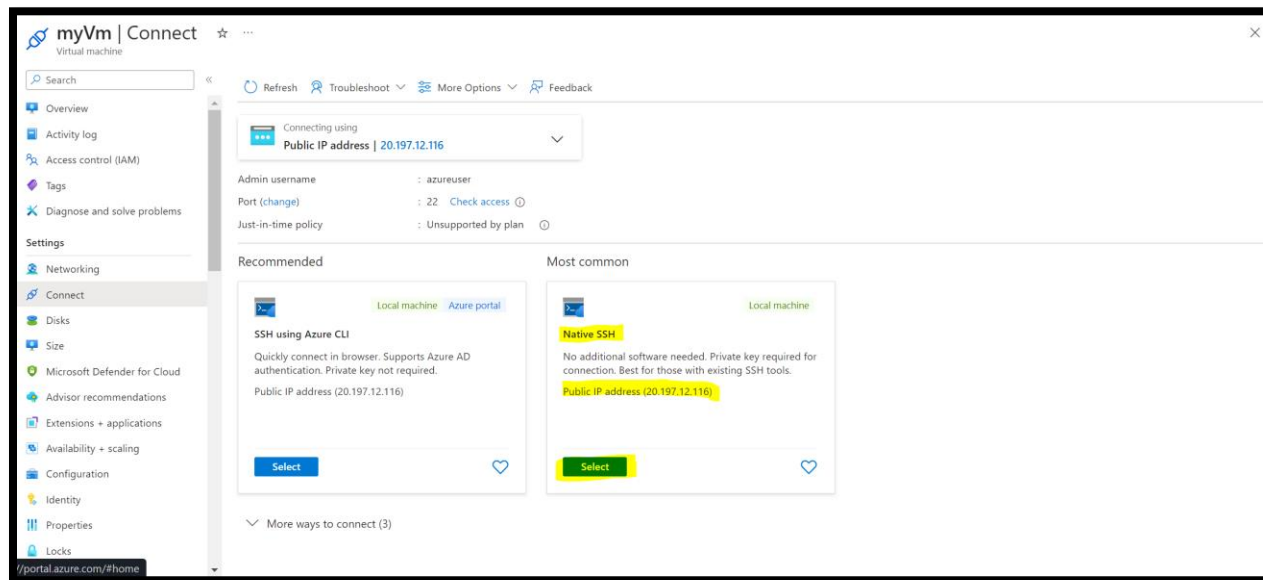
Download Key

A screenshot of the 'Generate new key pair' dialog box in the Azure portal. The dialog has a white background and a blue header bar with the title 'Generate new key pair'. Below the title, there is an information icon (a blue circle with a white 'i') followed by text: 'An SSH key pair contains both a public key and a private key. **Azure doesn't store the private key.** After the SSH key resource is created, you won't be able to download the private key again. [Learn more](#)'. Below this text are two buttons: a blue button labeled 'Download private key and create resource' and a white button with a black border labeled 'Return to create a virtual machine'.

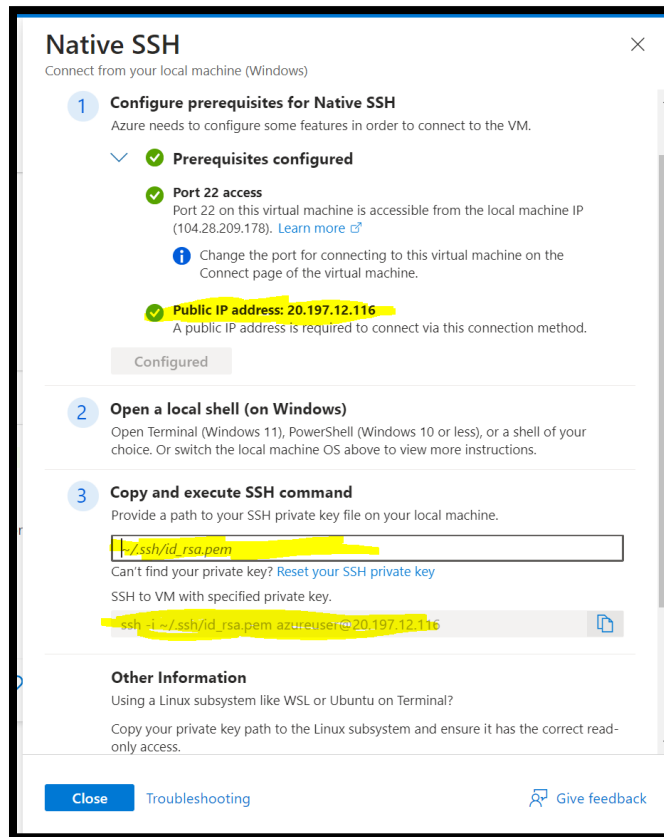
Created



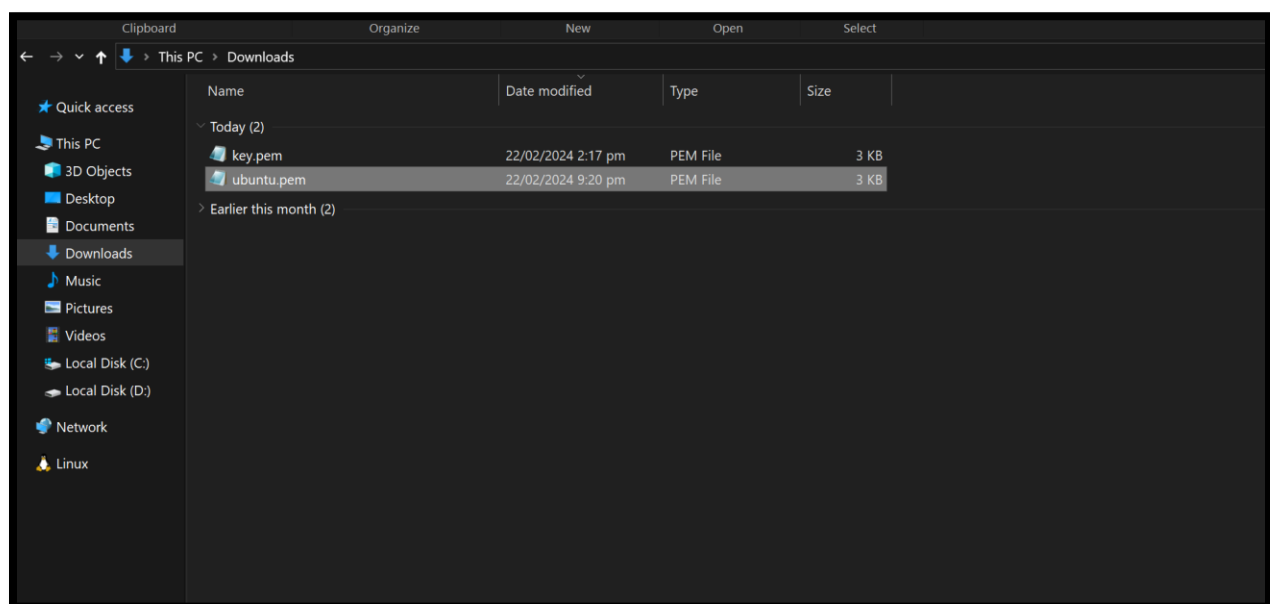
Now start and Connect the Ubuntu Server Virtual Machine to access the Terminal.

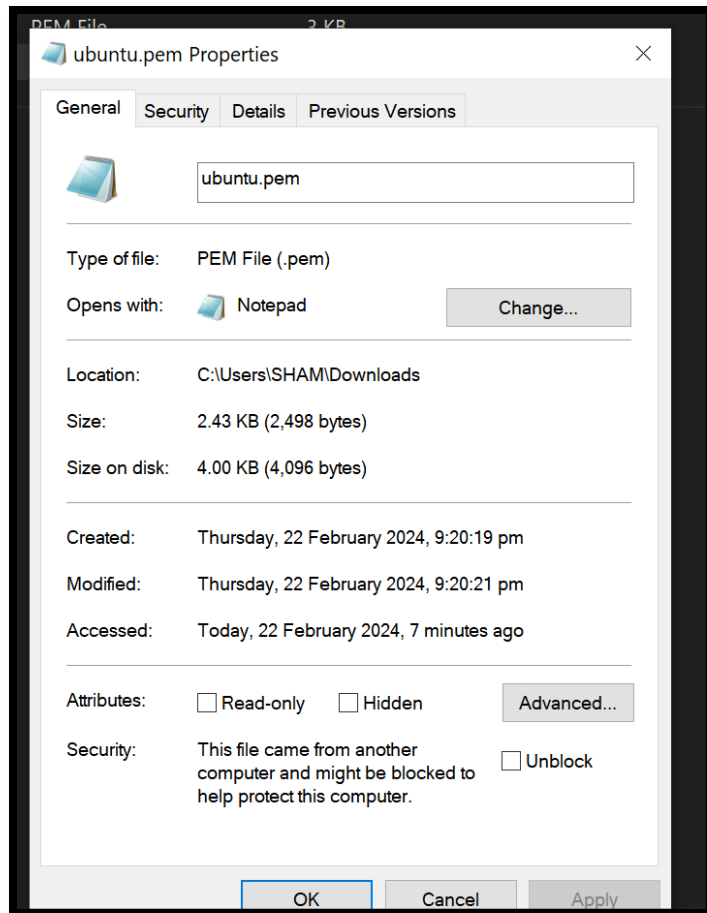


Open Native SSH

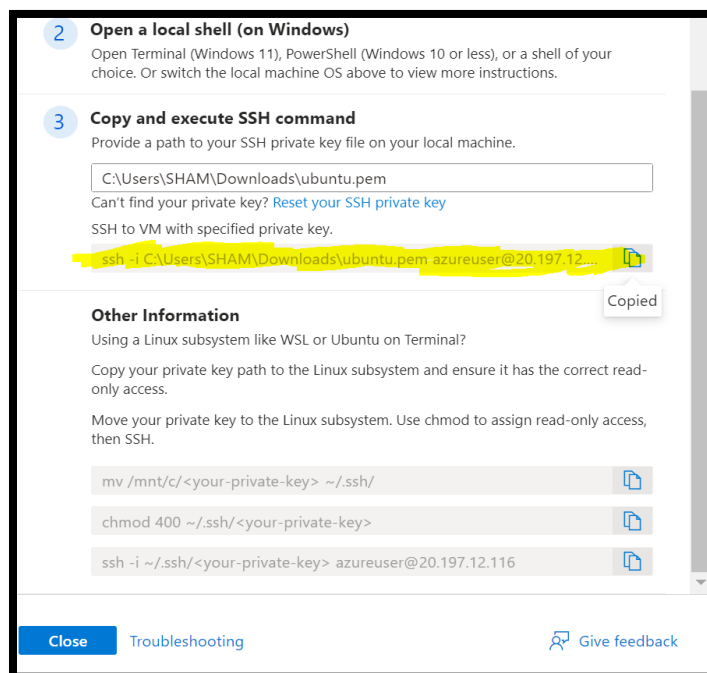


Open properties of pem file



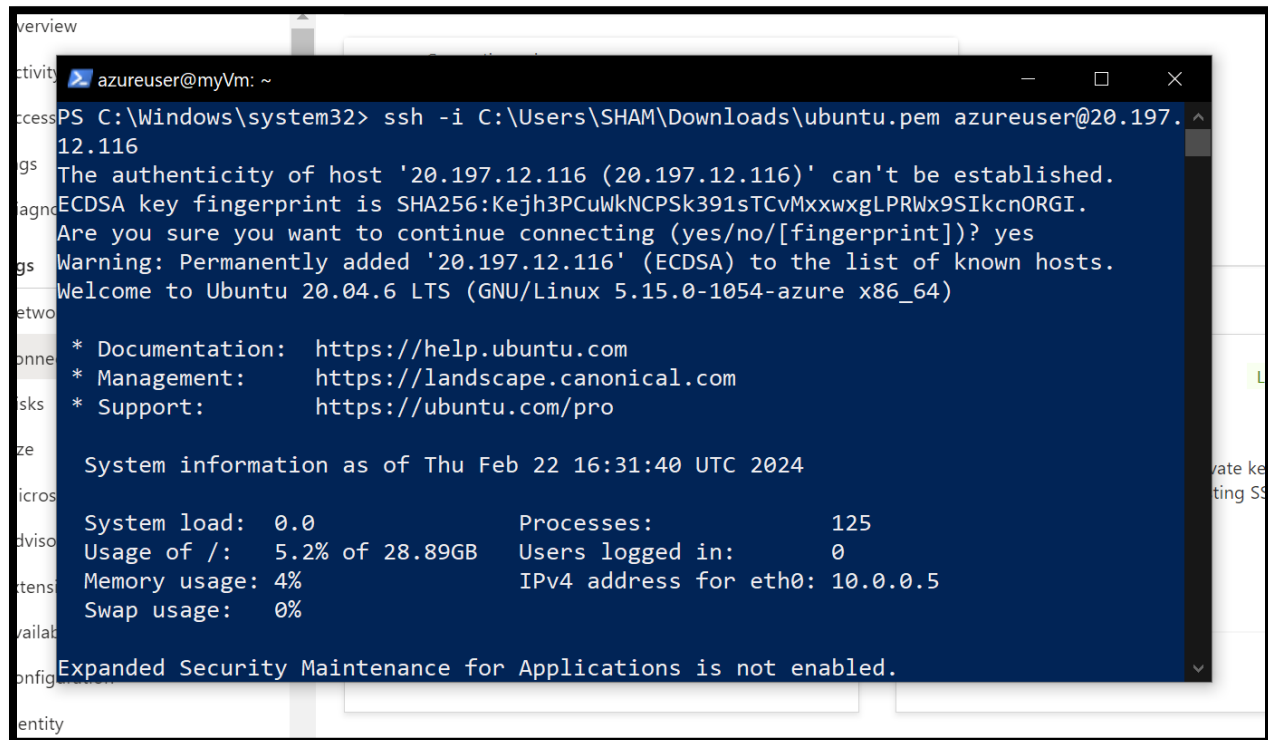


Copy the path of file and paste in ssh command.



Copy the command and run this in PowerShell as Administrator mode

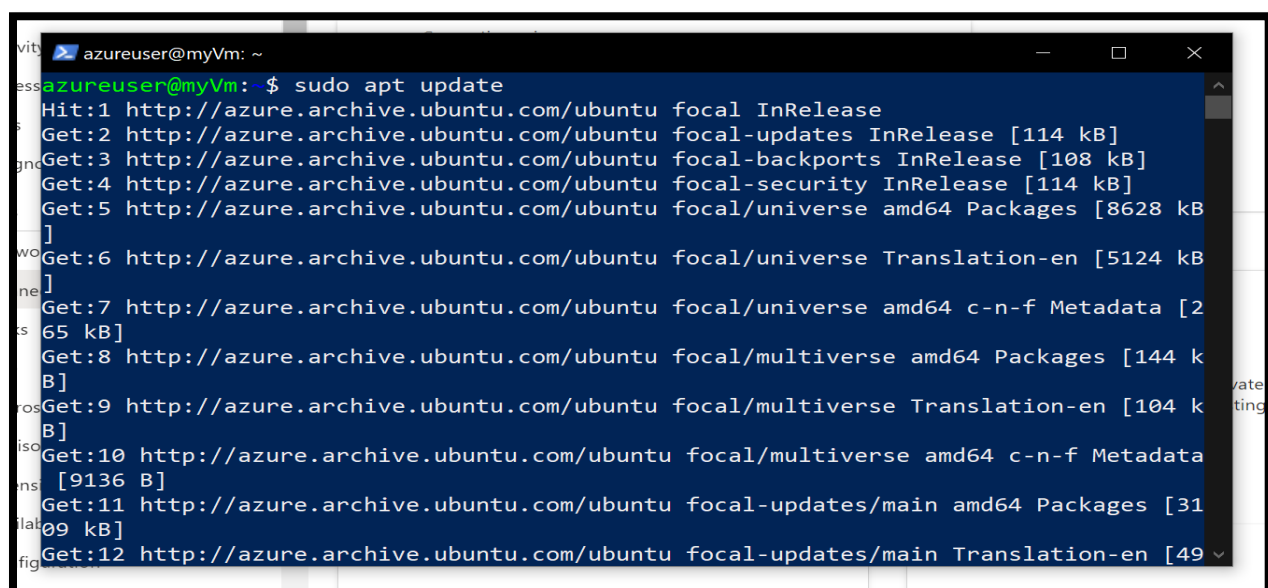
`ssh -i C:\Users\SHAM\Downloads\ubuntu.pem azureuser@20.197.12.116`



A terminal window titled 'azureuser@myVm: ~' showing the execution of an SSH command. The command is `ssh -i C:\Users\SHAM\Downloads\ubuntu.pem azureuser@20.197.12.116`. The output shows a warning about the host's authenticity, a confirmation to continue, and a warning that the host has been permanently added to the known hosts list. The terminal then displays the Ubuntu 20.04.6 LTS welcome message and system information.

```
azureuser@myVm: ~  
PS C:\Windows\system32> ssh -i C:\Users\SHAM\Downloads\ubuntu.pem azureuser@20.197.12.116  
The authenticity of host '20.197.12.116 (20.197.12.116)' can't be established.  
ECDSA key fingerprint is SHA256:Kejh3PCuWkNCPSk391sTCvMxxwxgLPRWx9SIkcNORGI.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '20.197.12.116' (ECDSA) to the list of known hosts.  
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1054-azure x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/pro  
  
System information as of Thu Feb 22 16:31:40 UTC 2024  
  
System load:  0.0      Processes:      125  
Usage of /:   5.2% of 28.89GB  Users logged in:  0  
Memory usage: 4%      IPv4 address for eth0: 10.0.0.5  
Swap usage:   0%  
  
Expanded Security Maintenance for Applications is not enabled.
```

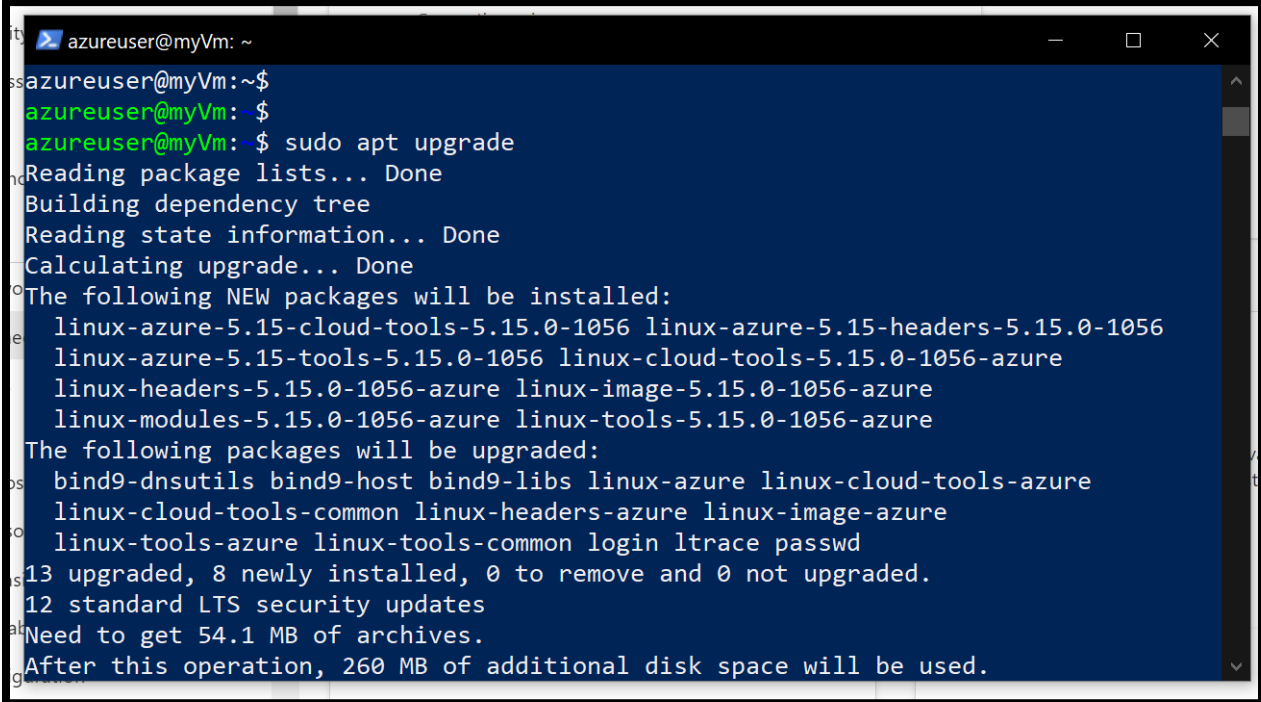
And you have accessed the Ubuntu server.



A terminal window titled 'azureuser@myVm: ~' showing the execution of the command `sudo apt update`. The output lists 12 packages to be updated, including focal InRelease, focal-updates InRelease, focal-backports InRelease, focal-security InRelease, focal/universe amd64 Packages, focal/universe Translation-en, focal/universe amd64 c-n-f Metadata, focal/multiverse amd64 Packages, focal/multiverse Translation-en, focal/multiverse amd64 c-n-f Metadata, focal-updates/main amd64 Packages, and focal-updates/main Translation-en.

```
azureuser@myVm: ~  
$ sudo apt update  
Hit:1 http://azure.archive.ubuntu.com/ubuntu focal InRelease  
Get:2 http://azure.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]  
Get:3 http://azure.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]  
Get:4 http://azure.archive.ubuntu.com/ubuntu focal-security InRelease [114 kB]  
Get:5 http://azure.archive.ubuntu.com/ubuntu focal/universe amd64 Packages [8628 kB]  
Get:6 http://azure.archive.ubuntu.com/ubuntu focal/universe Translation-en [5124 kB]  
Get:7 http://azure.archive.ubuntu.com/ubuntu focal/universe amd64 c-n-f Metadata [265 kB]  
Get:8 http://azure.archive.ubuntu.com/ubuntu focal/multiverse amd64 Packages [144 kB]  
Get:9 http://azure.archive.ubuntu.com/ubuntu focal/multiverse Translation-en [104 kB]  
Get:10 http://azure.archive.ubuntu.com/ubuntu focal/multiverse amd64 c-n-f Metadata [9136 B]  
Get:11 http://azure.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [3109 kB]  
Get:12 http://azure.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [49
```

First Update and upgrade machine.

A terminal window titled 'azureuser@myVm: ~' with a dark blue background and white text. The window shows the execution of the 'sudo apt upgrade' command. The output indicates that 13 packages will be upgraded, 8 new packages will be installed, and 0 packages will be removed or not upgraded. The packages to be installed include various linux-azure and linux-cloud-tools packages. The packages to be upgraded include bind9-dnsutils, bind9-host, bind9-libs, linux-azure, linux-cloud-tools-azure, linux-cloud-tools-common, linux-headers-azure, linux-image-azure, linux-tools-azure, linux-tools-common, login, ltrace, and passwd. The terminal also shows the disk space requirements: 54.1 MB of archives need to be downloaded, and 260 MB of additional disk space will be used after the operation.

```
it azureuser@myVm: ~
ss azureuser@myVm:~$
azureuser@myVm:~$
azureuser@myVm:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following NEW packages will be installed:
  linux-azure-5.15-cloud-tools-5.15.0-1056 linux-azure-5.15-headers-5.15.0-1056
  linux-azure-5.15-tools-5.15.0-1056 linux-cloud-tools-5.15.0-1056-azure
  linux-headers-5.15.0-1056-azure linux-image-5.15.0-1056-azure
  linux-modules-5.15.0-1056-azure linux-tools-5.15.0-1056-azure
The following packages will be upgraded:
  bind9-dnsutils bind9-host bind9-libs linux-azure linux-cloud-tools-azure
  linux-cloud-tools-common linux-headers-azure linux-image-azure
  linux-tools-azure linux-tools-common login ltrace passwd
13 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
12 standard LTS security updates
Need to get 54.1 MB of archives.
After this operation, 260 MB of additional disk space will be used.
```

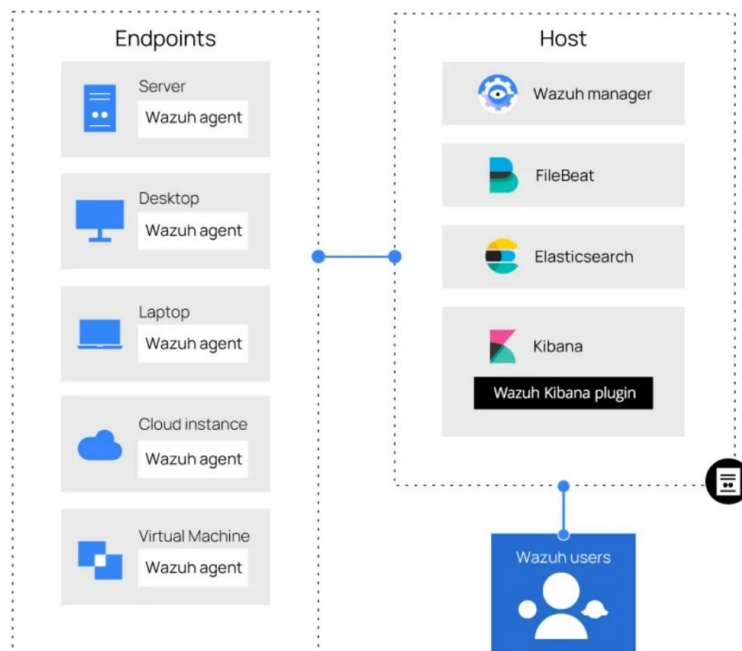
Installing initial packages

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:

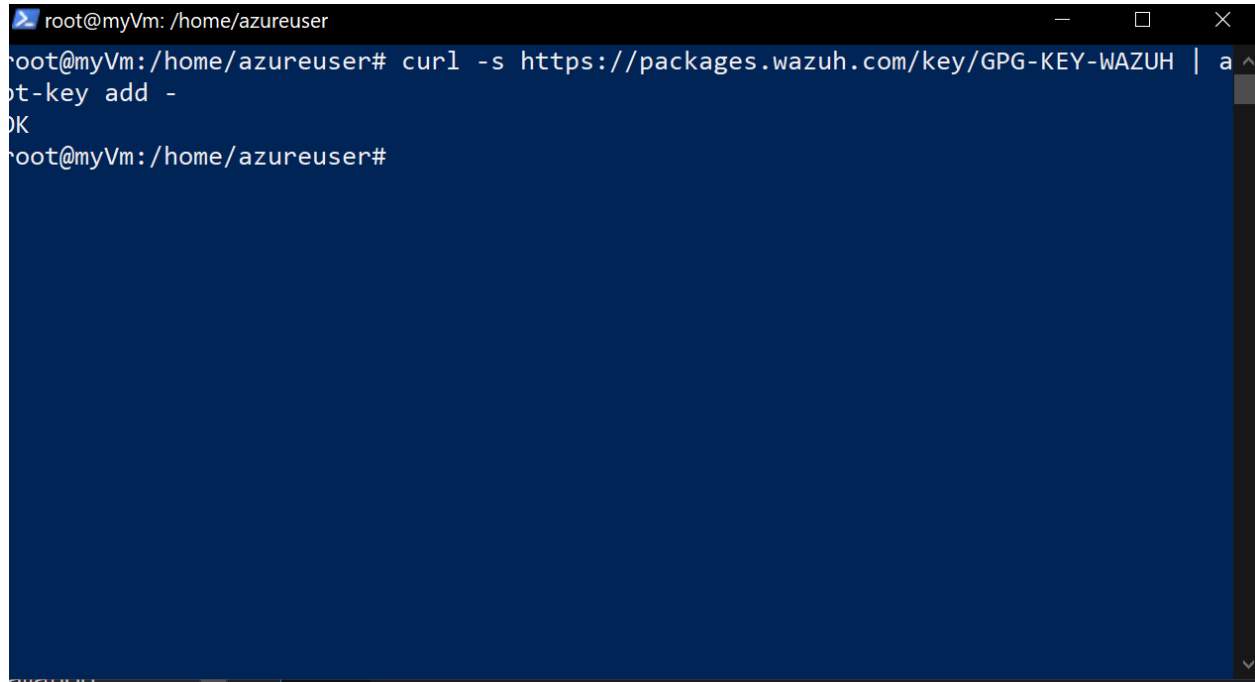
- 1- Install the necessary packages for the installation:

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

```
azureuser@myVm: ~  
azureuser@myVm: $ sudo apt install curl apt-transport-https unzip wget libcap2-bin  
software-properties-common lsb-release gnupg  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
lsb-release is already the newest version (11.1.0ubuntu2).  
lsb-release set to manually installed.  
curl is already the newest version (7.68.0-1ubuntu2.21).  
curl set to manually installed.  
gnupg is already the newest version (2.2.19-3ubuntu2.2).  
gnupg set to manually installed.  
libcap2-bin is already the newest version (1:2.32-1ubuntu0.1).  
libcap2-bin set to manually installed.  
software-properties-common is already the newest version (0.99.9.12).  
software-properties-common set to manually installed.  
wget is already the newest version (1.20.3-1ubuntu2).  
wget set to manually installed.  
Suggested packages:  
  zip  
The following NEW packages will be installed:
```

2- Install the GPG key:

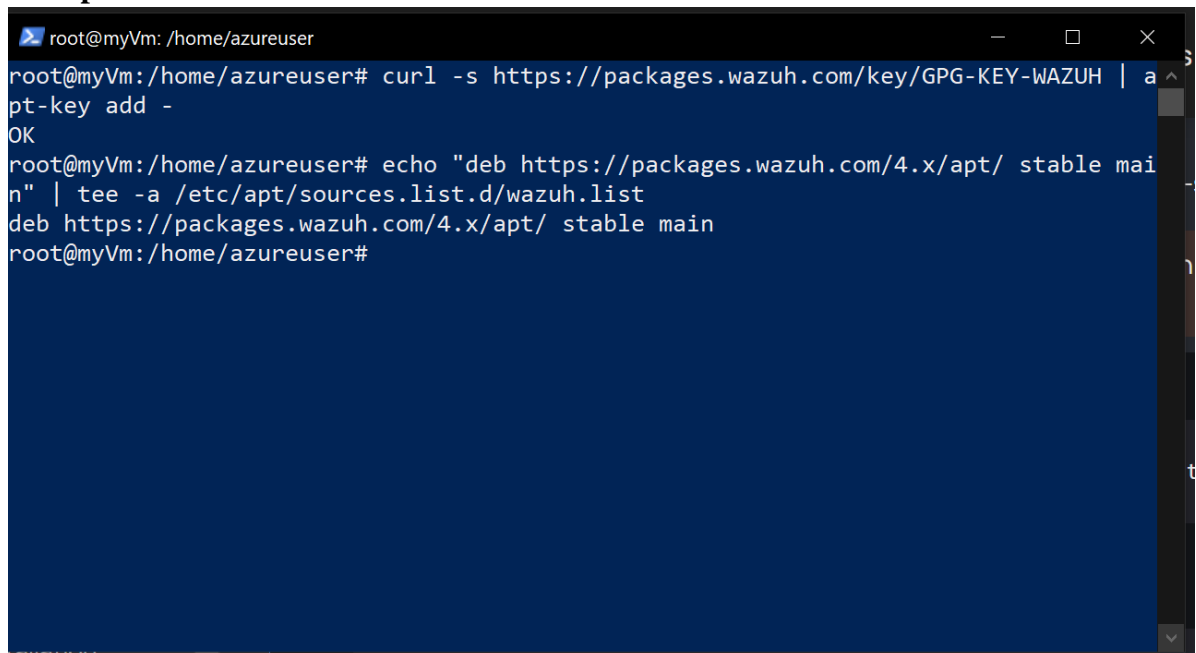
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -

A terminal window with a dark blue background and white text. The prompt is 'root@myVm: /home/azureuser'. The command 'curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -' is entered and executed. The output is 'OK'.

```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -
OK
root@myVm:/home/azureuser#
```

3- Add the repository:

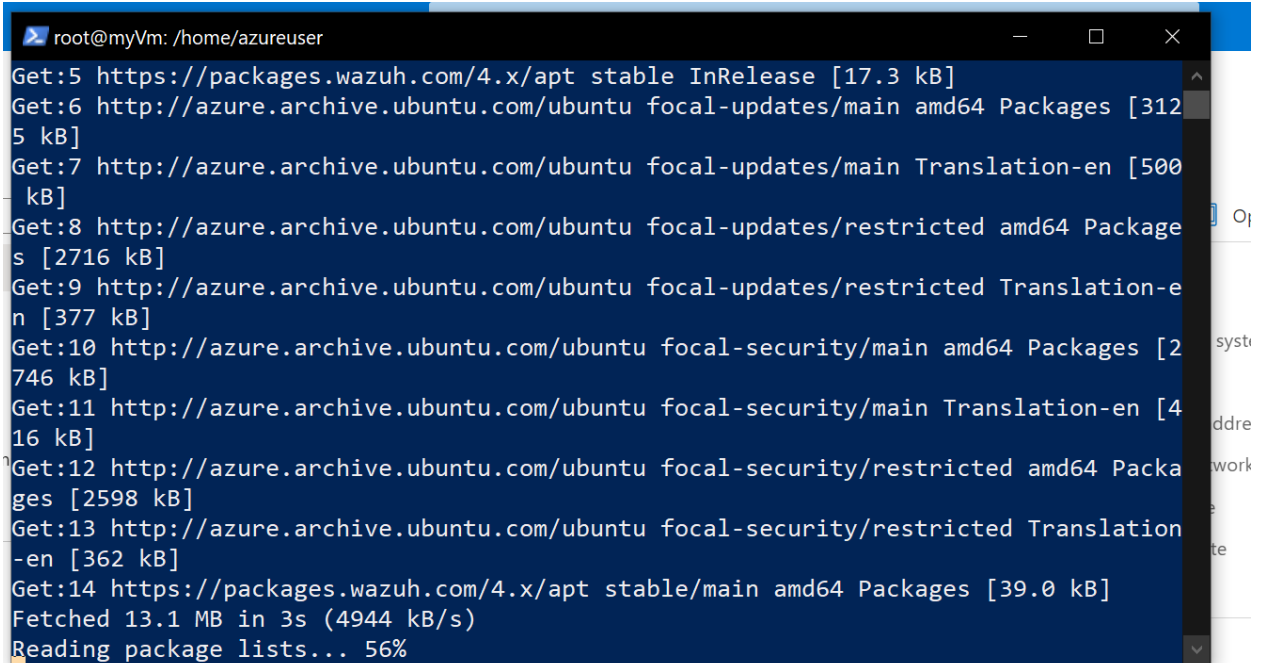
echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list

A terminal window with a dark blue background and white text. The prompt is 'root@myVm: /home/azureuser'. The command 'curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -' is entered and executed, resulting in 'OK'. Then, the command 'echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list' is entered and executed, resulting in 'deb https://packages.wazuh.com/4.x/apt/ stable main' being printed to the terminal.

```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -
OK
root@myVm:/home/azureuser# echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
deb https://packages.wazuh.com/4.x/apt/ stable main
root@myVm:/home/azureuser#
```

- 4- Update the package information:

apt-get update

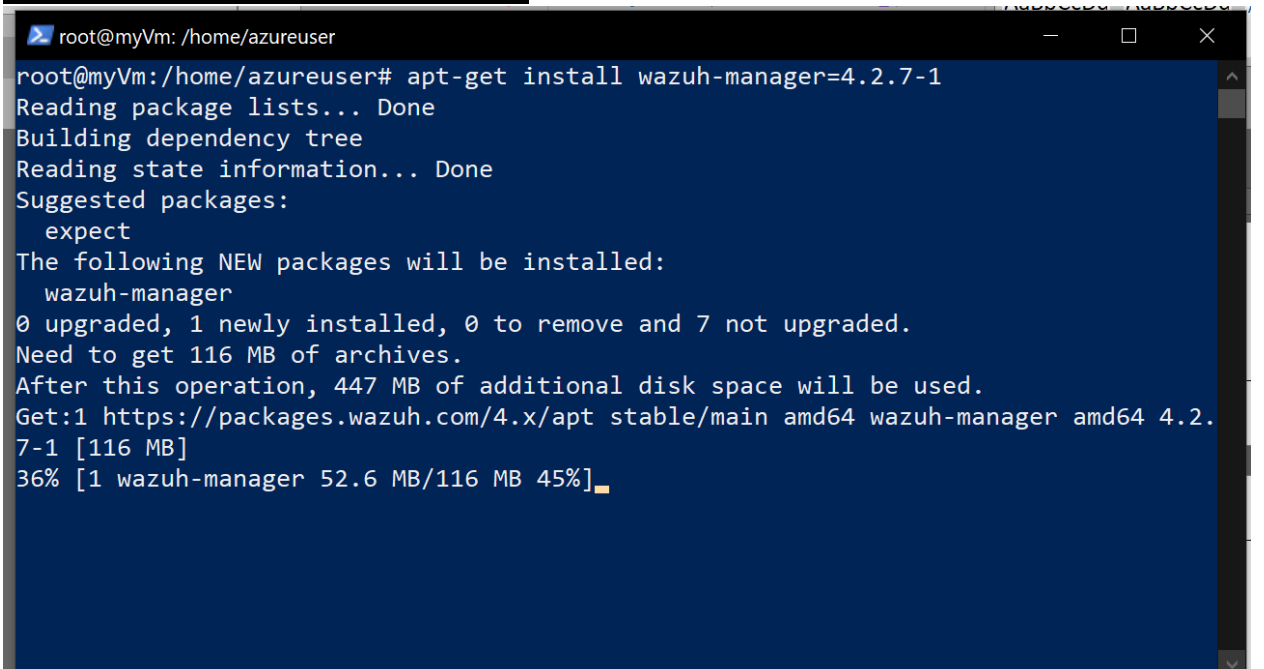
A terminal window titled 'root@myVm: /home/azureuser' showing the output of the 'apt-get update' command. The output lists updates from various sources including wazuh.com and azure.archive.ubuntu.com for focal-updates and focal-security repositories. It shows the size of the packages being fetched and the total amount of data downloaded (13.1 MB) over a 3-second period.

```
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

A terminal window titled 'root@myVm: /home/azureuser' showing the output of the 'apt-get install wazuh-manager=4.2.7-1' command. The output displays the package list, dependency tree, and state information. It suggests installing 'expect' and shows that 'wazuh-manager' will be newly installed. It also indicates the disk space requirements and the progress of the download (36% complete).

```
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- Enable and start the Wazuh manager service:

```
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/systemd/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- Run the following command to check if the Wazuh manager is active:

```
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 pre>
   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

```
root@myVm: /home/azureuser
Unpacking opendistro-knn (1.13.0.0-1) ...
Selecting previously unselected package opendistro-performance-analyzer.
Preparing to unpack .../08-opendistro-performance-analyzer_1.13.0.0-1_all.deb ...
Unpacking opendistro-performance-analyzer (1.13.0.0-1) ...
Selecting previously unselected package opendistro-reports-scheduler.
Preparing to unpack .../09-opendistro-reports-scheduler_1.13.0.0-1_all.deb ...
Unpacking opendistro-reports-scheduler (1.13.0.0-1) ...
Selecting previously unselected package opendistro-security.
Preparing to unpack .../10-opendistro-security_1.13.1.0-1_all.deb ...
Unpacking opendistro-security (1.13.1.0-1) ...
Selecting previously unselected package opendistro-sql.
Preparing to unpack .../11-opendistro-sql_1.13.2.0-1_all.deb ...
Unpacking opendistro-sql (1.13.2.0-1) ...
Selecting previously unselected package opendistroforelasticsearch.
Preparing to unpack .../12-opendistroforelasticsearch_1.13.2-1_amd64.deb ...
Unpacking opendistroforelasticsearch (1.13.2-1) ...
Setting up opendistro-knnlib (1.13.0.0) ...
Setting up elasticsearch-oss (7.10.2) ...
Progress: [ 55%] [#####.....]
```

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

```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# curl -so /etc/elasticsearch/elasticsearch.yml https://packages.wazuh.com/resources/4.2/open-distro/elasticsearch/7.x/elasticsearch_all_in_one.yml
root@myVm:/home/azureuser#
```

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-](https://packages.wazuh.com/resources/4.2/open-distro/elasticsearch/roles/roles.yml)

distro/elasticsearch/roles/roles.yml

curl -so

/usr/share/elasticsearch/plugins/opendistro_security/securityconfig/roles_mapping

g.yml [https://packages.wazuh.com/resources/4.2/open-](https://packages.wazuh.com/resources/4.2/open-distro/elasticsearch/roles/roles_mapping.yml)

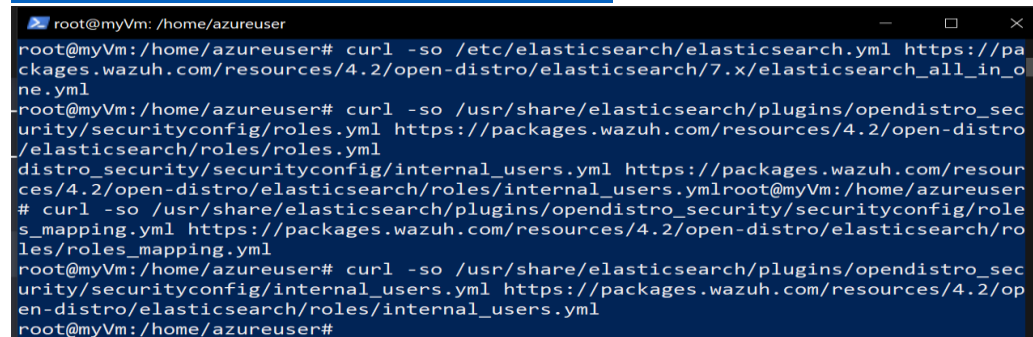
distro/elasticsearch/roles/roles_mapping.yml

curl -so

/usr/share/elasticsearch/plugins/opendistro_security/securityconfig/internal_user

s.yml [https://packages.wazuh.com/resources/4.2/open-](https://packages.wazuh.com/resources/4.2/open-distro/elasticsearch/roles/internal_users.yml)

distro/elasticsearch/roles/internal_users.yml



```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# curl -so /etc/elasticsearch/elasticsearch.yml https://pa
ckages.wazuh.com/resources/4.2/open-distro/elasticsearch/7.x/elasticsearch_all_in_o
ne.yml
root@myVm:/home/azureuser# curl -so /usr/share/elasticsearch/plugins/opendistro_sec
urity/securityconfig/roles.yml https://packages.wazuh.com/resources/4.2/open-distro
/elasticsearch/roles/roles.yml
root@myVm:/home/azureuser# curl -so /usr/share/elasticsearch/plugins/opendistro_sec
urity/securityconfig/internal_users.yml https://packages.wazuh.com/resour
ces/4.2/open-distro/elasticsearch/roles/internal_users.yml
root@myVm:/home/azureuser# curl -so /usr/share/elasticsearch/plugins/opendistro_sec
urity/securityconfig/roles_mapping.yml https://packages.wazuh.com/resources/4.2/open-distro/elasticsearch/ro
les/roles_mapping.yml
root@myVm:/home/azureuser# curl -so /usr/share/elasticsearch/plugins/opendistro_sec
urity/securityconfig/internal_users.yml https://packages.wazuh.com/resources/4.2/op
en-distro/elasticsearch/roles/internal_users.yml
root@myVm:/home/azureuser#
```

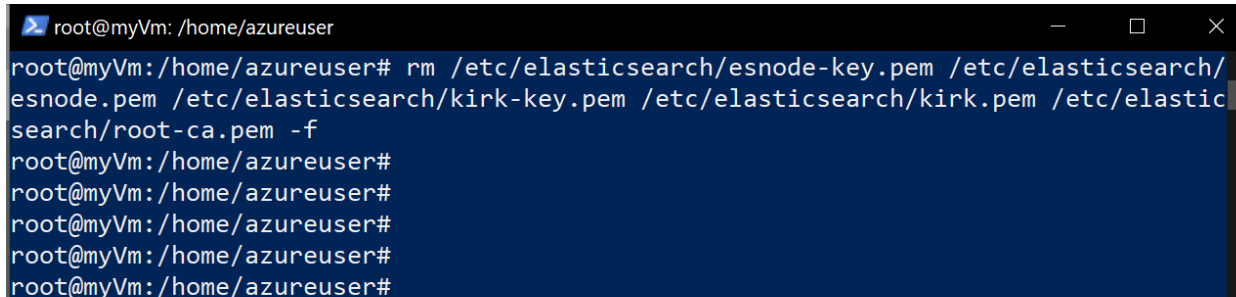
Certificates creation

- 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



```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# rm /etc/elasticsearch/esnode-key.pem /etc/elasticsearch/
esnode.pem /etc/elasticsearch/kirk-key.pem /etc/elasticsearch/kirk.pem /etc/elastic
search/root-ca.pem -f
root@myVm:/home/azureuser#
root@myVm:/home/azureuser#
root@myVm:/home/azureuser#
root@myVm:/home/azureuser#
root@myVm:/home/azureuser#
```

2- Generate and deploy the certificates:

- **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/

```
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# mkdir /etc/elasticsearch/certs/
root@myVm:/home/azureuser# mv ~/certs/elasticsearch* /etc/elasticsearch/certs/
root@myVm:/home/azureuser# mv ~/certs/admin* /etc/elasticsearch/certs/
root@myVm:/home/azureuser# cp ~/certs/root-ca* /etc/elasticsearch/certs/
root@myVm:/home/azureuser#
```

- 3- Enable and start the Elasticsearch service:

Warning

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/elasticsearch/jvm.options.d/disabledlog4j.options
root@myVm:/home/azureuser# chmod 2750 /etc/elasticsearch/jvm.options.d/disabledlog4j.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/systemd/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/systemd/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/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
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 replicas)
Populate config from /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/
```

6- Run the following command to ensure that the installation is successful:

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#
```

Installing Filebeat

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 [22.1 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.wazuh.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.githubusercontent.com/wazuh/wazuh/4.2/extensions/elasticsearch/7.x/wazuh-template.json
root@myVm:/home/azureuser# chmod go+r /etc/filebeat/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.githubusercontent.com/wazuh/wazuh/4.2/extensions/elasticsearch/7.x/wazuh-template.json
root@myVm:/home/azureuser# chmod go+r /etc/filebeat/wazuh-template.json
root@myVm:/home/azureuser# curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-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/
```

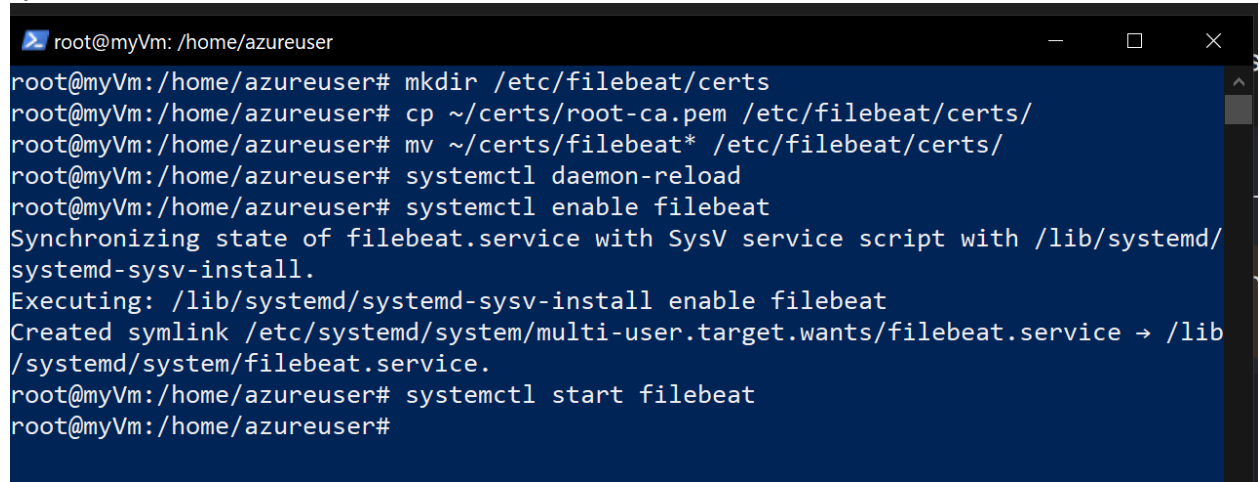
```
root@myVm: /home/azureuser
root@myVm:/home/azureuser# mkdir /etc/filebeat/certs
root@myVm:/home/azureuser# cp ~/certs/root-ca.pem /etc/filebeat/certs/
root@myVm:/home/azureuser# mv ~/certs/filebeat* /etc/filebeat/certs/
root@myVm:/home/azureuser#
```


- 5- Enable and start the Filebeat service:

systemctl daemon-reload

systemctl enable filebeat

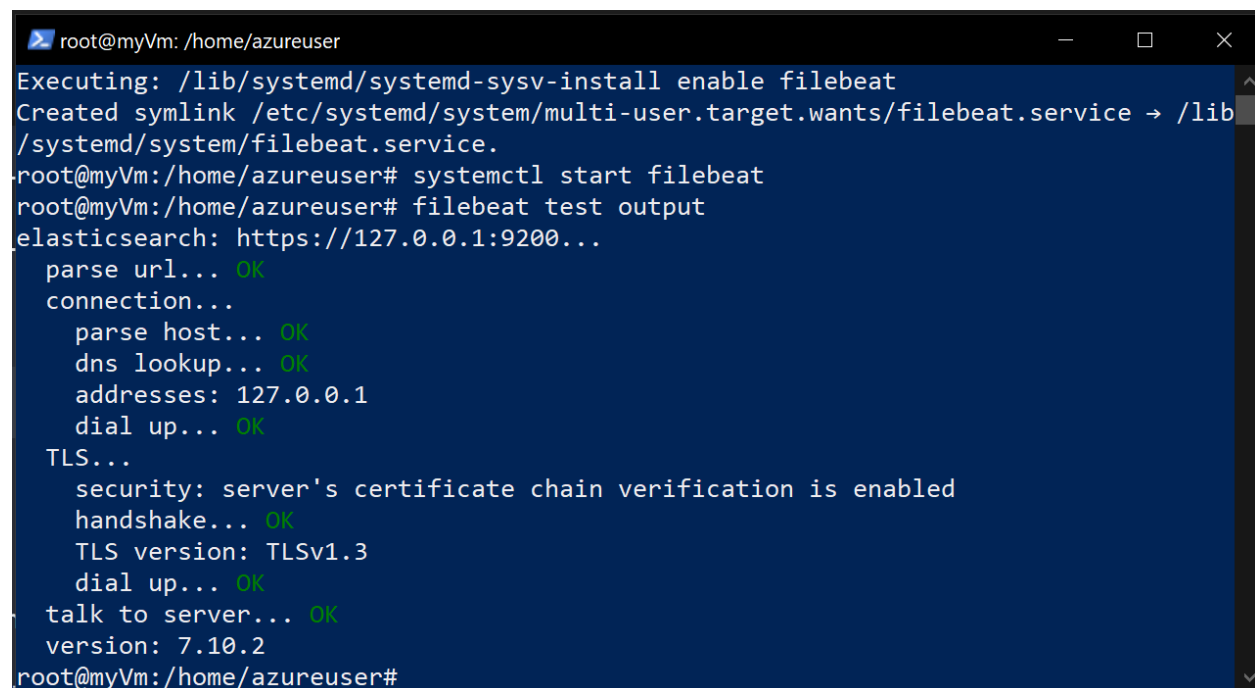
systemctl start filebeat



```
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



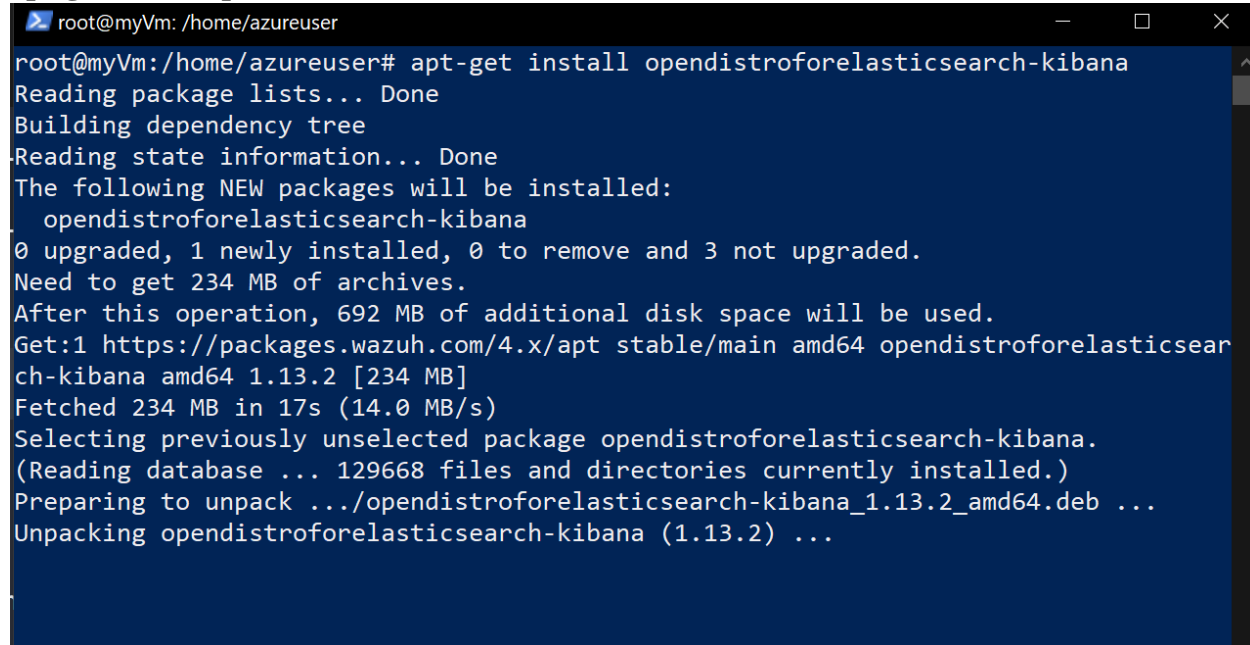
```
root@myVm: /home/azureuser
Executing: /lib/systemd/systemd-sysv-install enable filebeat
Created symlink /etc/systemd/system/multi-user.target.wants/filebeat.service → /lib
/systemd/system/filebeat.service.
root@myVm:/home/azureuser# systemctl start filebeat
root@myVm:/home/azureuser# filebeat test 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:

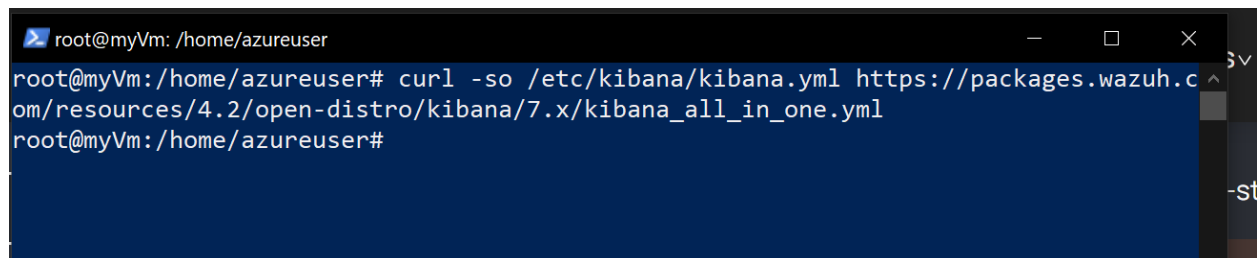
apt-get install opendistroforelasticsearch-kibana

A terminal window with a dark blue background and white text. The prompt is 'root@myVm: /home/azureuser'. The command 'apt-get install opendistroforelasticsearch-kibana' has been executed. The output shows the package list being read, the dependency tree being built, and state information being read. It lists the new packages to be installed, the disk space requirements (234 MB for archives, 692 MB additional space), and the source of the package (wazuh.com). It shows the package being fetched and then unpacked.

```
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 opendistroforelasticsearch-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

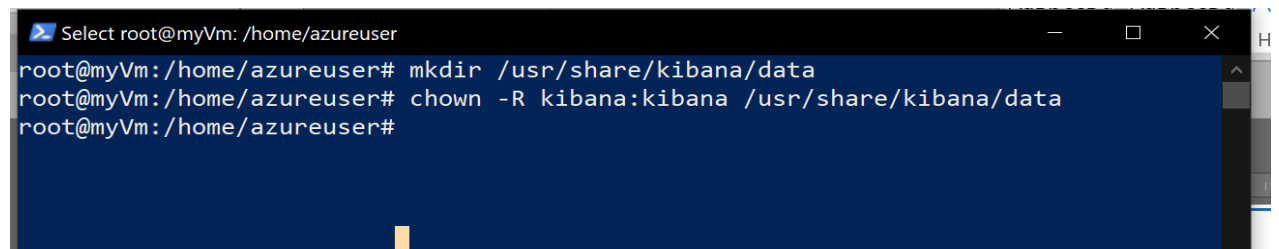
A terminal window with a dark blue background and white text. The prompt is 'root@myVm: /home/azureuser'. The command 'curl -so /etc/kibana/kibana.yml https://packages.wazuh.com/resources/4.2/open-distro/kibana/7.x/kibana_all_in_one.yml' has been executed. The output shows the file being downloaded and saved to the specified location.

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

- 3- Create the /usr/share/kibana/data directory:

mkdir /usr/share/kibana/data

chown -R kibana:kibana /usr/share/kibana/data

A terminal window with a dark blue background and white text. The prompt is 'root@myVm: /home/azureuser'. The commands 'mkdir /usr/share/kibana/data' and 'chown -R kibana:kibana /usr/share/kibana/data' have been executed. The output shows the directory being created and the permissions being set.

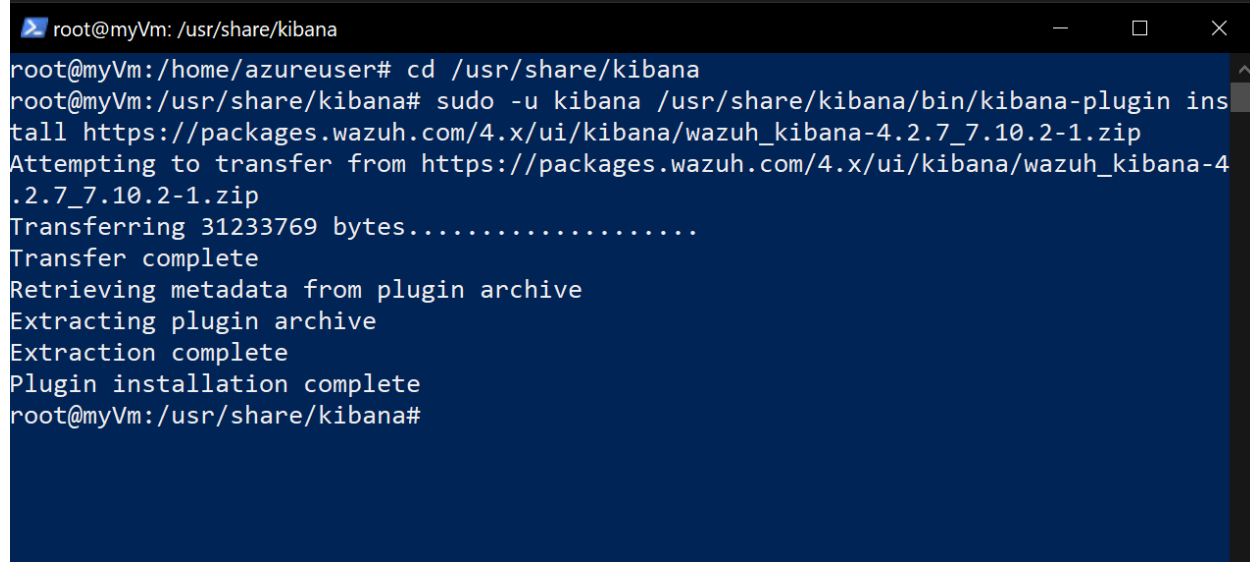
```
root@myVm: /home/azureuser# mkdir /usr/share/kibana/data
root@myVm: /home/azureuser# chown -R kibana:kibana /usr/share/kibana/data
root@myVm: /home/azureuser#
```

- 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

A terminal window titled 'root@myVm: /usr/share/kibana' showing the execution of the 'kibana-plugin install' command. The output shows the file being transferred from a URL, the transfer completion, and the successful installation of the plugin.

```
root@myVm:/home/azureuser# cd /usr/share/kibana
root@myVm:/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
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#
```

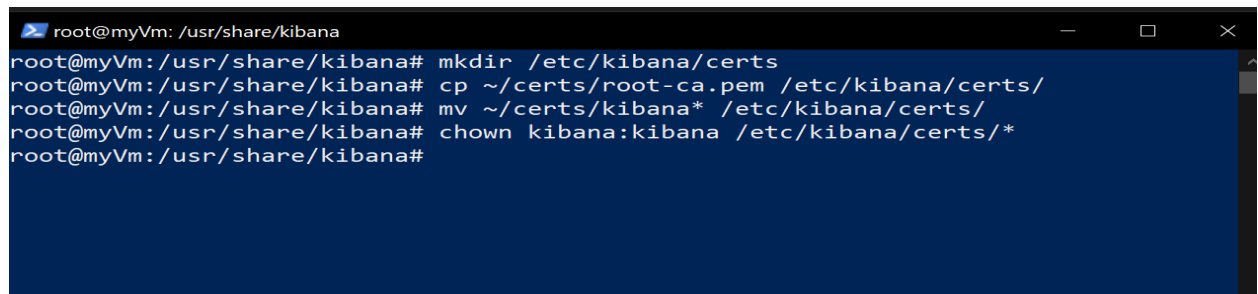
- 5- Copy the Elasticsearch certificates into /etc/kibana/certs:

mkdir /etc/kibana/certs

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

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

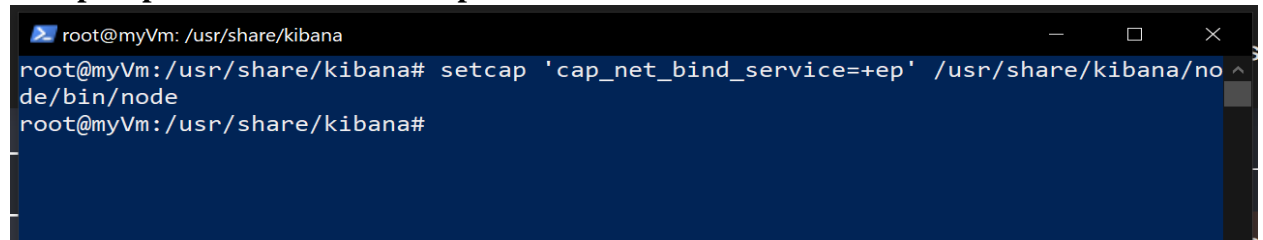
chown kibana:kibana /etc/kibana/certs/*

A terminal window titled 'root@myVm: /usr/share/kibana' showing the execution of 'mkdir', 'cp', 'mv', and 'chown' commands to set up the certificate directory and permissions.

```
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

A terminal window titled 'root@myVm: /usr/share/kibana' showing the execution of the 'setcap' command to set the 'cap_net_bind_service' capability on the node binary.

```
root@myVm:/usr/share/kibana# setcap 'cap_net_bind_service=+ep' /usr/share/kibana/node/bin/node
root@myVm:/usr/share/kibana#
```

7- Enable and start the Kibana service:

systemctl daemon-reload

systemctl enable kibana

systemctl start kibana

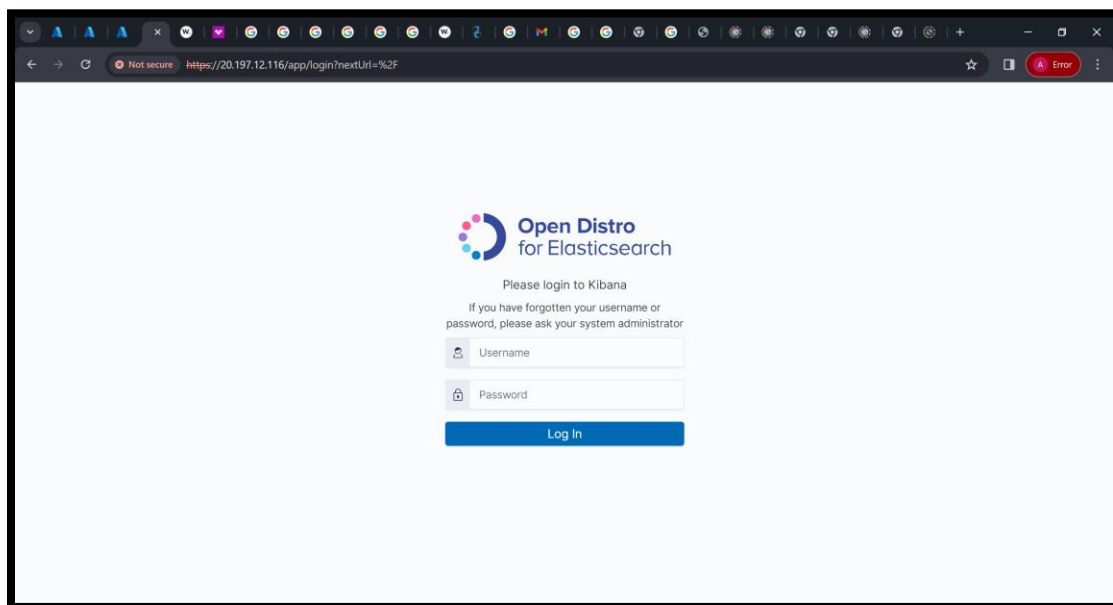
```
root@myVm: /usr/share/kibana
root@myVm:/usr/share/kibana# systemctl daemon-reload
root@myVm:/usr/share/kibana# systemctl enable kibana
Synchronizing state of kibana.service with SysV service script with /lib/systemd/sy
stemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable kibana
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- Access the web interface:

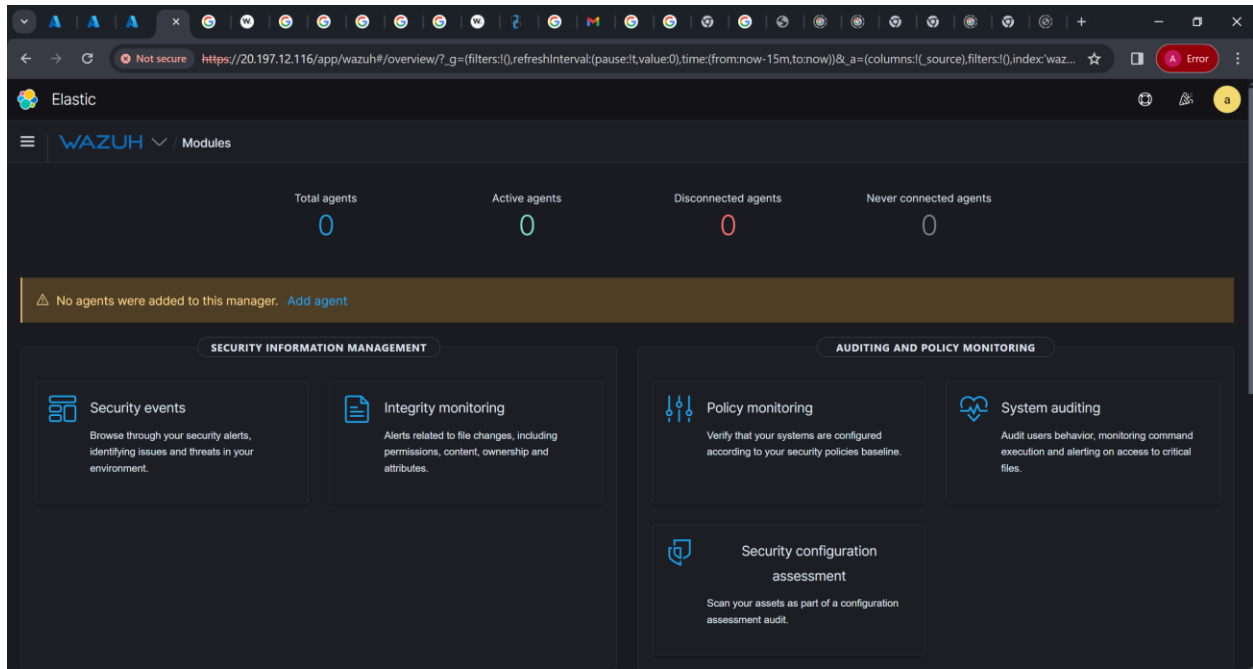
URL: https://<wazuh_server_ip>

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.