**Divya Dileep**

**DEPLOYING AND INTERACTING WITH A FREE VIRTUAL MACHINE IN AWS**

**CONTENTS**

**Overview** ........................................................................................................................ 2

**EC2 Instance Launch Process** ........................................................................................ 2

Accessing the EC2 Console .........................................................2

Launching the EC2 Instance......................................................... 3

Selecting the Amazon Machine Image (AMI) ...............................4

Choosing an Instance Type .............................................................4

Configuring Instance Details ..........................................................5

Setting Up Security Group Rules .................................................. 5

Final Review and Launch .............................................................. 6

**Connectivity Testing and Instance Access** .....................................................................7

Verifying Public IP Connectivity via Ping ..........................................7

Accessing the EC2 Instance via SSH ...................................................7

**Testing Public IP Connectivity from the Cloud** **VM** ..................................................... 8

Ping Test from the EC2 Instance ............................................................8

**Terminating the VM** ......................................................................................................... 9

**Summary of Results**................................................................................................10

**1.Overview**

The objective of this assignment is to conduct research and initiate a free Virtual Machine (VM) within a cloud computing environment, preferably Azure, although Amazon Web Services (AWS) or Google Cloud Platform (GCP) could also be utilized. The procedure encompasses configuring the VM, securing its IP address, confirming its connectivity through a ping test, and accessing the VM via Secure Shell (SSH). Furthermore, the tasks involve executing network tests, investigating the VM, and ensuring its proper shutdown upon completion of usage.

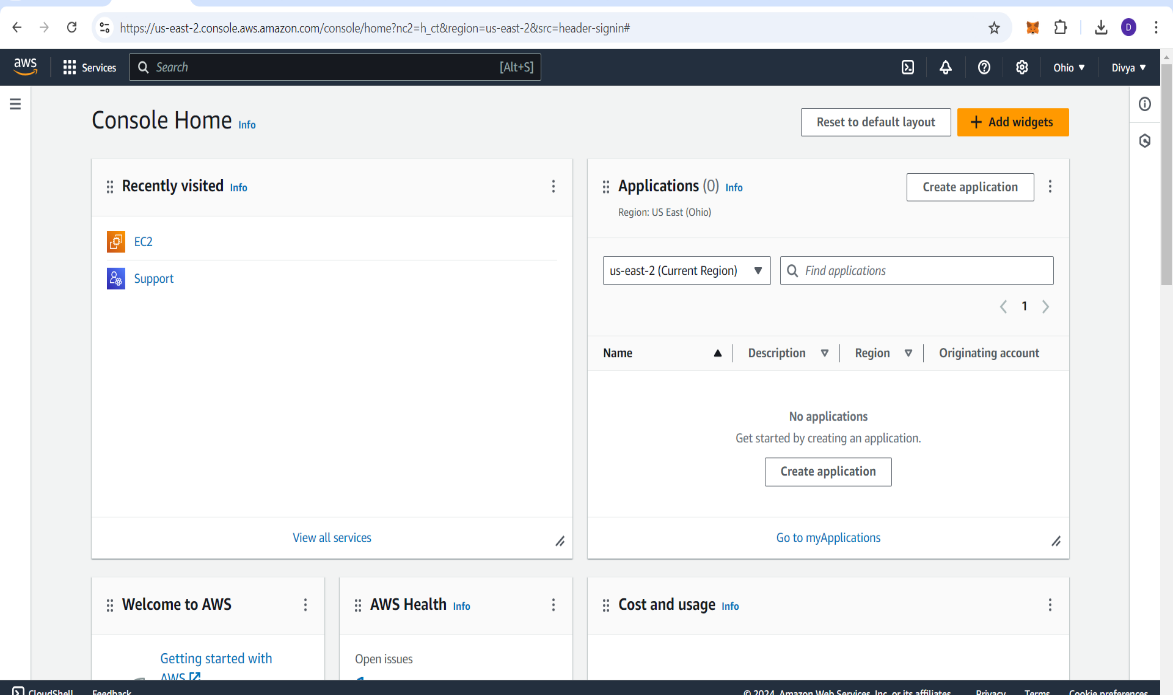
For the purpose of this report, Amazon Web Services (AWS) has been selected as the cloud provider.

**2.EC2 Instance Launch Process**

**2.1Accessing the EC2 Console**

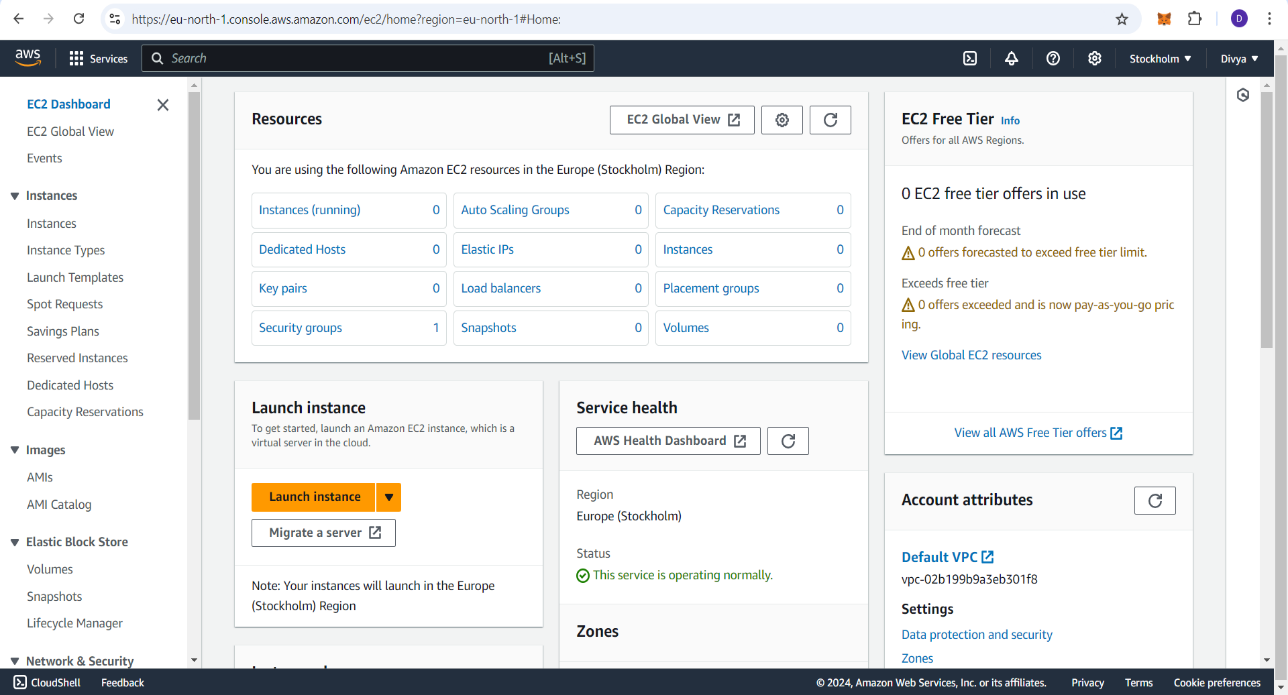
To initiate the setup process, I entered the EC2 Dashboard by doing the following actions:

1. I logged into the AWS Management Console and used the search bar to locate EC2.



Screenshot 1

1. Selecting EC2 from the results redirected me to the EC2 dashboard.

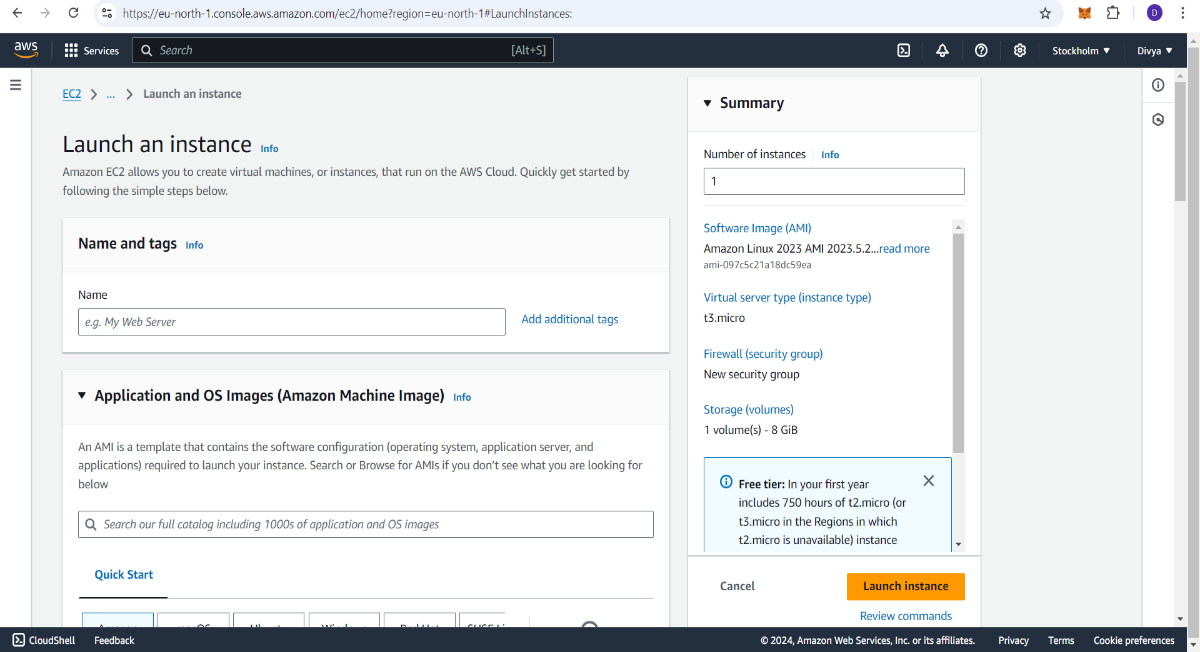


Screenshot 2

* 1. **Launching the EC2 Instance**

To start an EC2 instance creation process:

1. On the EC2 dashboard, I selected the Launch Instance option.   
2. This took me to the Launch an Instance page, where I could configure the settings for the virtual machine (VM).



Screenshot 3

* 1. **Selecting the Amazon Machine Image (AMI)**

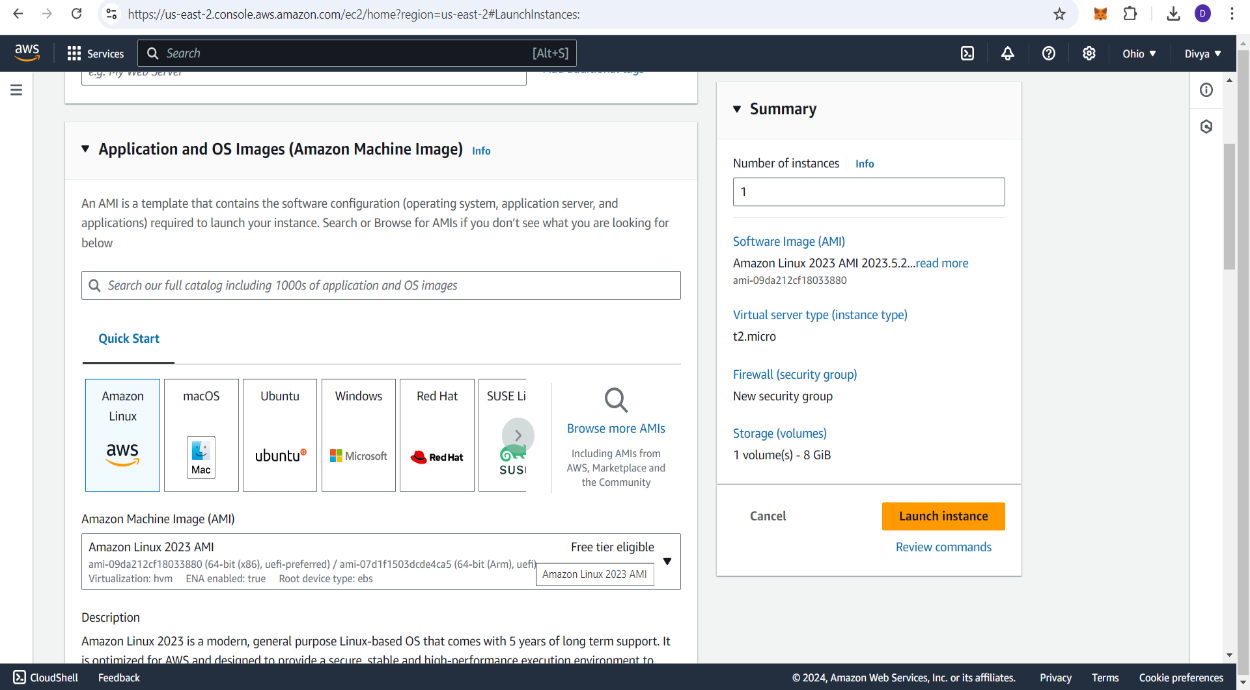
The Amazon Machine Image (AMI) determines the operating system for the EC2 instance:

1. I browsed through the available AMIs and chose Amazon Linux, which is free-tier

eligible.

2. Other options like macOS,Ubuntu or Windows Server are also available, but I

selected Amazon Linux for this setup



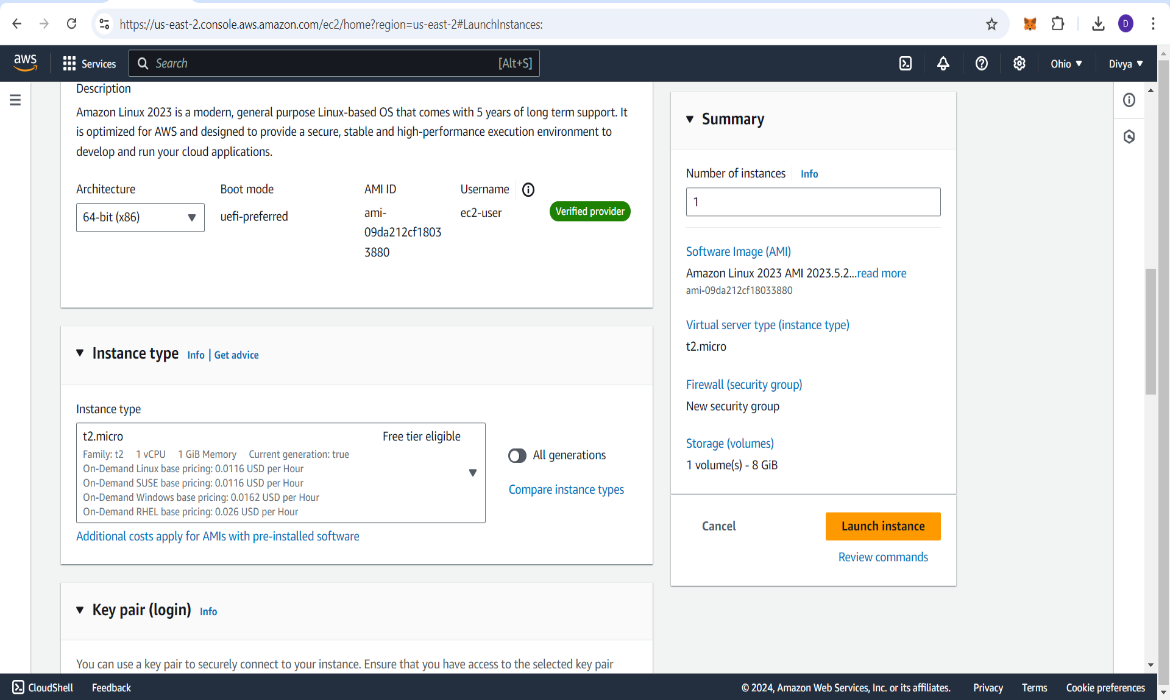
Screenshot 4

**2.4Choosing an Instance Type**

Instance types define the resource configuration (CPU, memory, etc.):

1. I selected the t2.micro instance type, which is suitable for light workloads and falls under the AWS free-tier offering.

2. Selected key pair renamed to cyber[a key pair consists of a public key and a private key used for secure access to EC2 instances.]



Screenshot 4

* 1. **Configuring Instance Details**

At this stage, I configured additional settings for the instance:

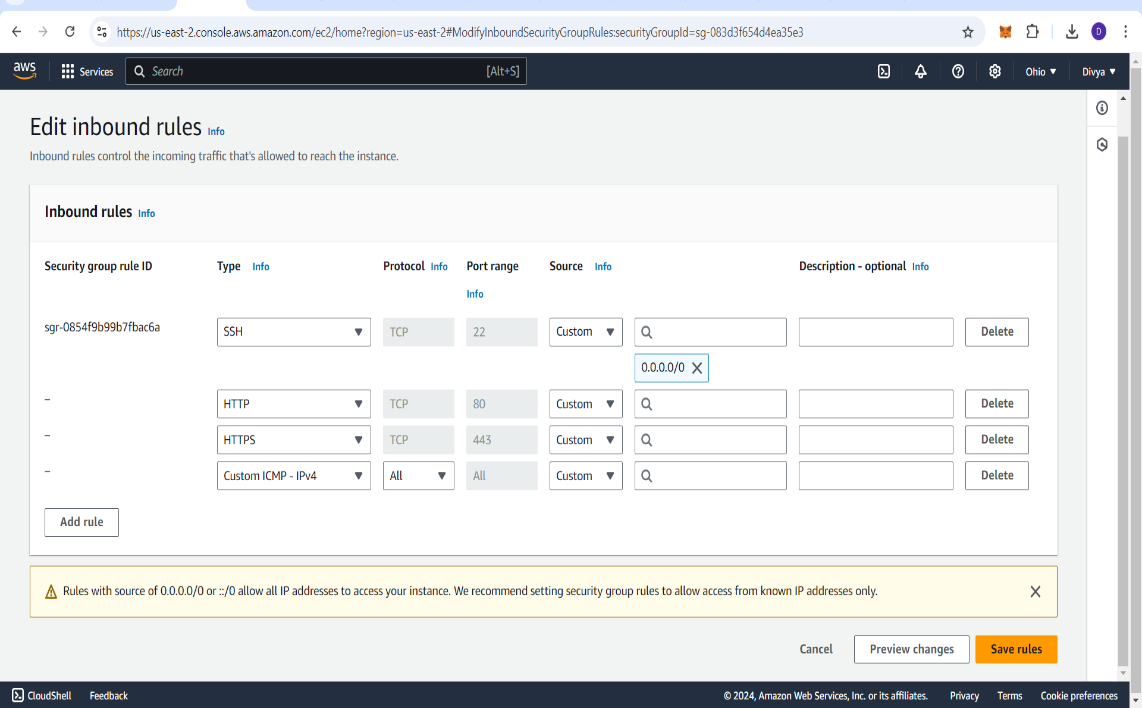
1. I used the default VPC (Virtual Private Cloud) for networking, leaving most of the default options unchanged.

2. This configuration was adequate for my needs, as I didn’t require any advanced networking configurations.

* 1. **Setting Up Security Group Rules**

The Security Group is a virtual firewall that controls the traffic to and from the instance:

1. For this instance, SSH (port 22) was pre-configured to allow remote access for Linux
2. I later made modifications to the inbound rules to enable specific traffic, such as allowing ICMP for ping tests. (refer screenshot 5)

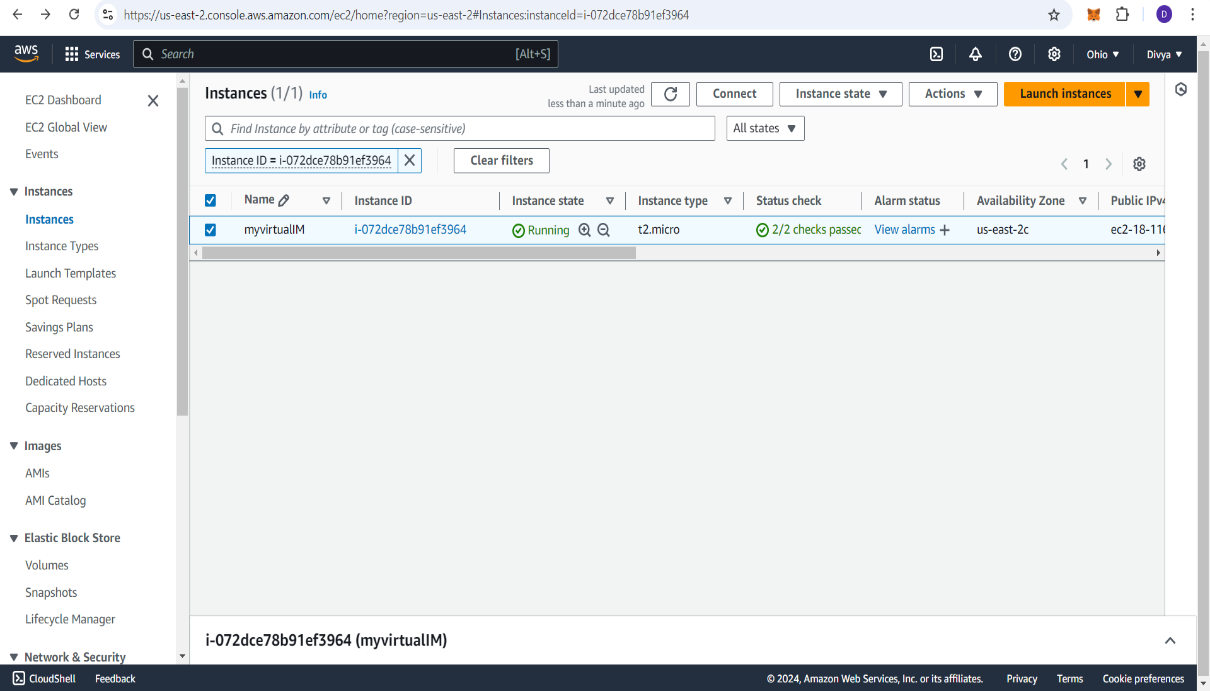


Screenshot 5

* 1. **Final Review and Launch**

1. I reviewed the configuration settings and confirmed they were correct.

2. After verifying the setup, I clicked Launch Instance, which successfully created and deployed the EC2 instance



Screenshot 6

**3.Connectivity Testing and Instance Access**

**3.1 Verifying Public IP Connectivity via Ping**

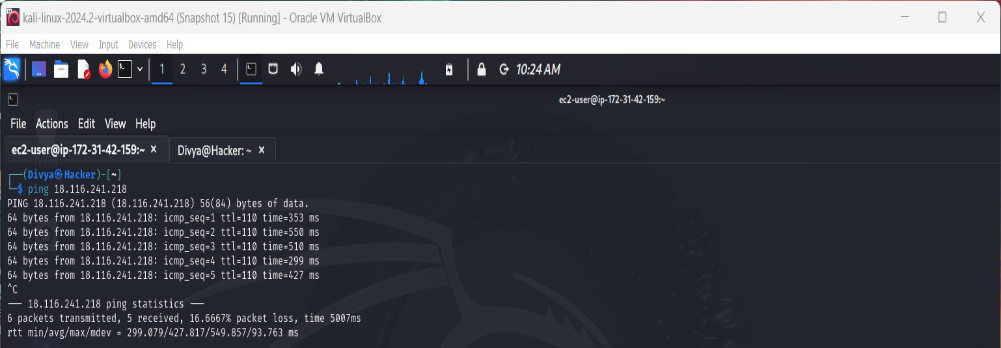
Once the instance was up and running, I tested the public IP connectivity:

1. The public IP assigned to my EC2 instance was:

Public ip : 18.116.241.218

1. Initially, I was unable to ping the instance from outside.
2. However, after modifying the inbound rules in the security group to allow ICMP traffic.

I was able to successfully ping the public IP



Screenshot 7

* 1. **Accessing the EC2 Instance via SSH**

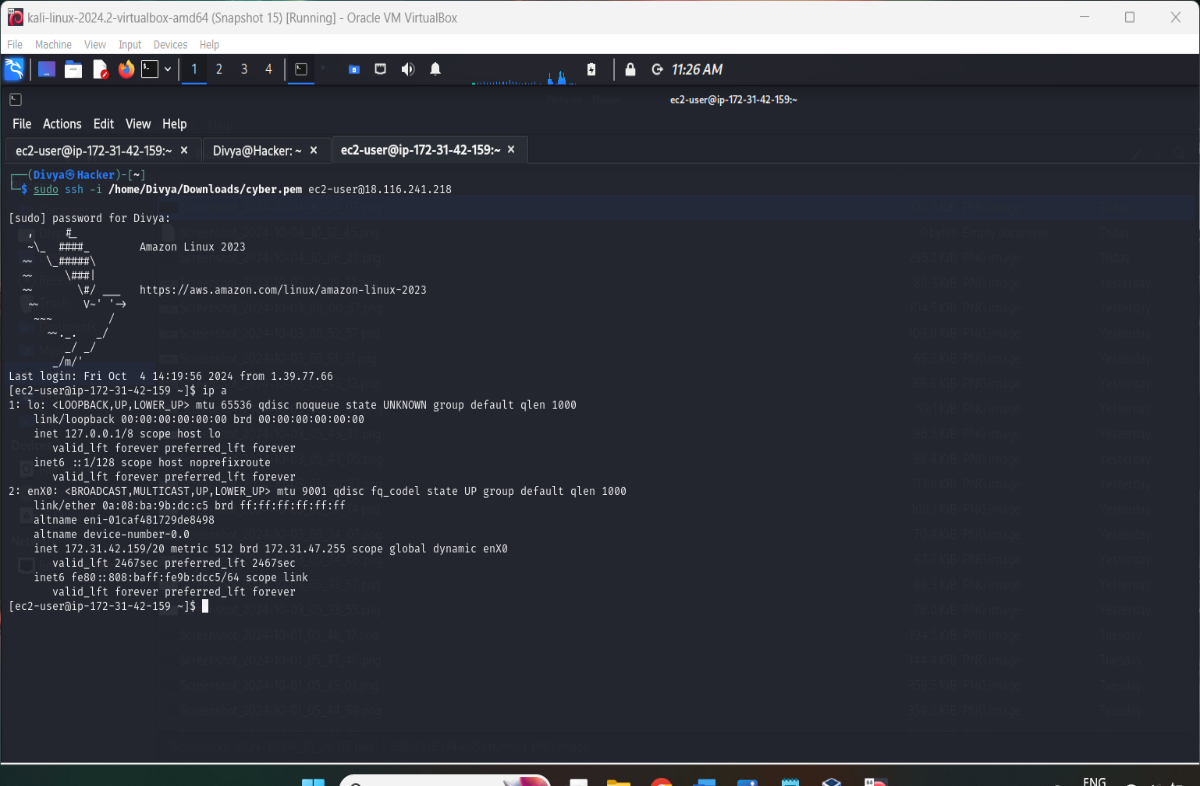
To access the EC2 instance remotely, I used SSH with the following steps:

1. I used the security key [cloudkey] (generated during the instance setup) to securely log in to the instance from my local machine.

2. On my Kali Linux system, I used the following command to establish the SSH connection:

sudo ssh -i <path>/cyber.pem ec2-user@ 18.116.241.218

1. I successfully logged into the instance and gained shell access to the EC2 virtual machine



Screenshot 8

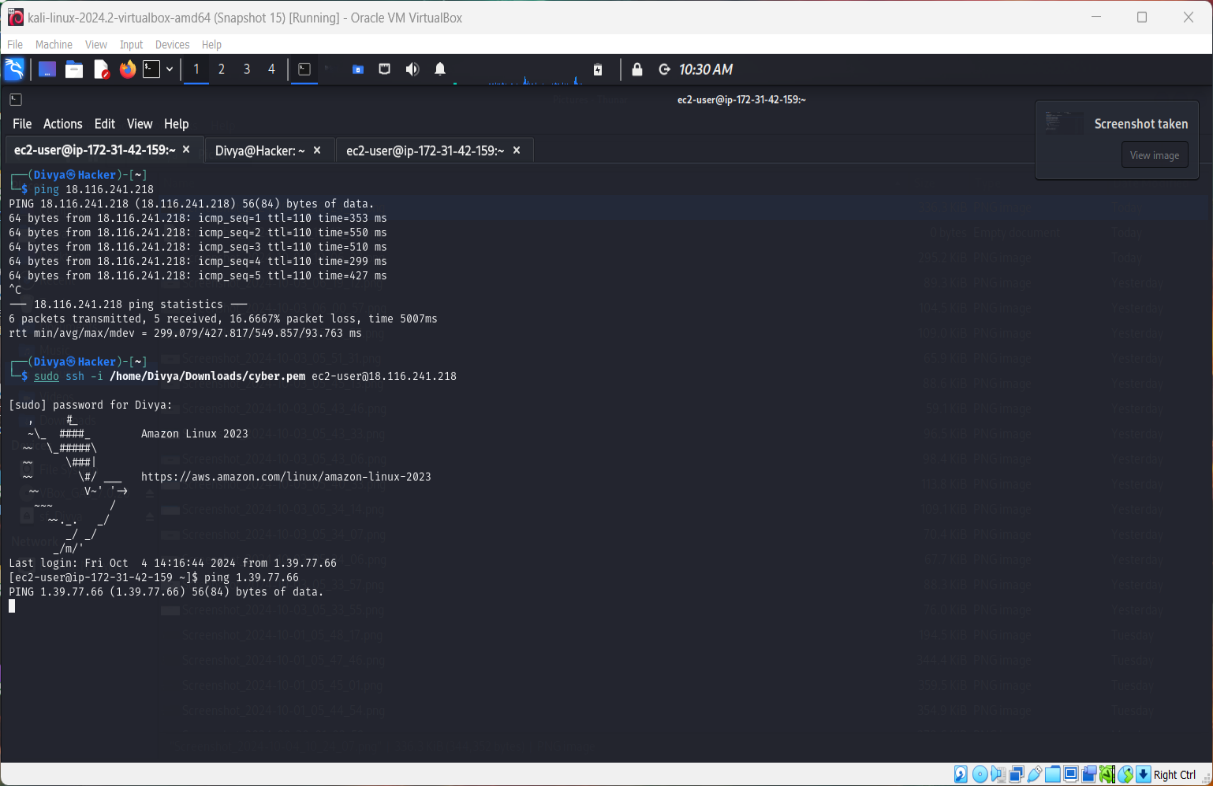
**4. Testing Public IP Connectivity from the Cloud VM**

**4.1 Ping Test from the EC2 Instance**

I attempted to verify the public IP connectivity by pinging my public IP from within the EC2 instance itself:

1. However, I was unable to ping the public IP due to restrictions imposed by the ISP blocking ICMP (ping) packets.

2. This is a common limitation where Internet Service Providers prevent ICMP traffic for security or network performance reasons.



Screenshot 9

1. **Terminating the VM**

Finally, I returned to the AWS EC2 dashboard and terminated the VM to ensure it no longer incurs any charges or resources

**SUMMARY OF RESULTS**

1. I successfully started a free-tier VM on AWS and obtained the public IP.
2. After adjusting the security settings, I was able to ping the VM from my Kali Linux machine.
3. I logged into the VM via SSH, ran the ip a command, and captured the screenshot.
4. I attempted to ping the public IP from within the cloud VM, but the request was blocked by ISP restrictions.
5. After completing the tasks, I shut down and terminated the VM as required.