

MODULE 1:AWS

Submitted by – ADESH ARUN ADHAV

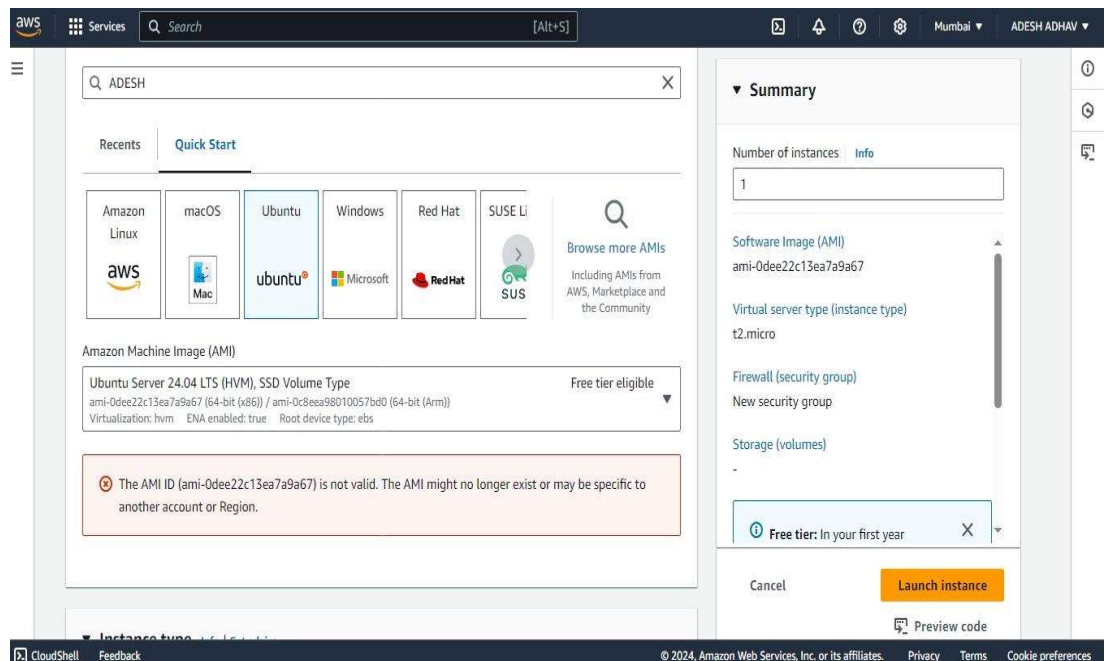
Submitted to – VIKUL SIR

L1 - Demonstrate the AWS EC2 Ubuntu Instance Creation steps and connect to EC2 Instance using putty agent.

➤ STEP 1- Launch an EC2 instance

- Login to AWS console
- Create an EC2 instance
 - 1.Search EC2 services
 - 2.Navigate to launch the instance
 - 3.Select ubuntu version
 4. Add key pair(used ppk file for putty)
 5. Add security group

LAUNCH INSTANCE



. Add key pair(used ppk file for putty)

The screenshot shows the AWS Management Console interface with the 'Create key pair' dialog box open. The dialog box has a title bar with 'Create key pair' and a close button. It contains the following sections:

- Key pair name:** A text input field containing 'AA'. Below it, a note states: 'The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.'
- Key pair type:** Two radio button options: 'RSA' (selected) and 'ED25519'. The 'RSA' option is described as 'RSA encrypted private and public key pair'. The 'ED25519' option is described as 'ED25519 encrypted private and public key pair'.
- Private key file format:** Two radio button options: '.pem' (selected) and '.ppk'. The '.pem' option is described as 'For use with OpenSSH'. The '.ppk' option is described as 'For use with PuTTY'.
- Warning:** A yellow warning box with a triangle icon stating: 'When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn](#)'.
- Buttons:** 'Cancel' and 'Create key pair' (highlighted in orange).

The background of the console shows the 'Instance type' section with 't2.micro' selected. The top navigation bar includes the AWS logo, 'Services', a search bar, and user information 'Mumbai' and 'ADESH ADHAV'.

.ADD SECURITY GROUP

Auto-assign public IP

Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups)

Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

We'll create a new security group called **launch-wizard-9** with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

Anywhere

0.0.0.0/0

☐ Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

▼ Configure storage

Info

Advanced

▼ Summary

Number of instances

Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.6.2...read more

ami-04a37924ffe27da53

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel

Launch instance

Preview code

CloudShell

Feedback

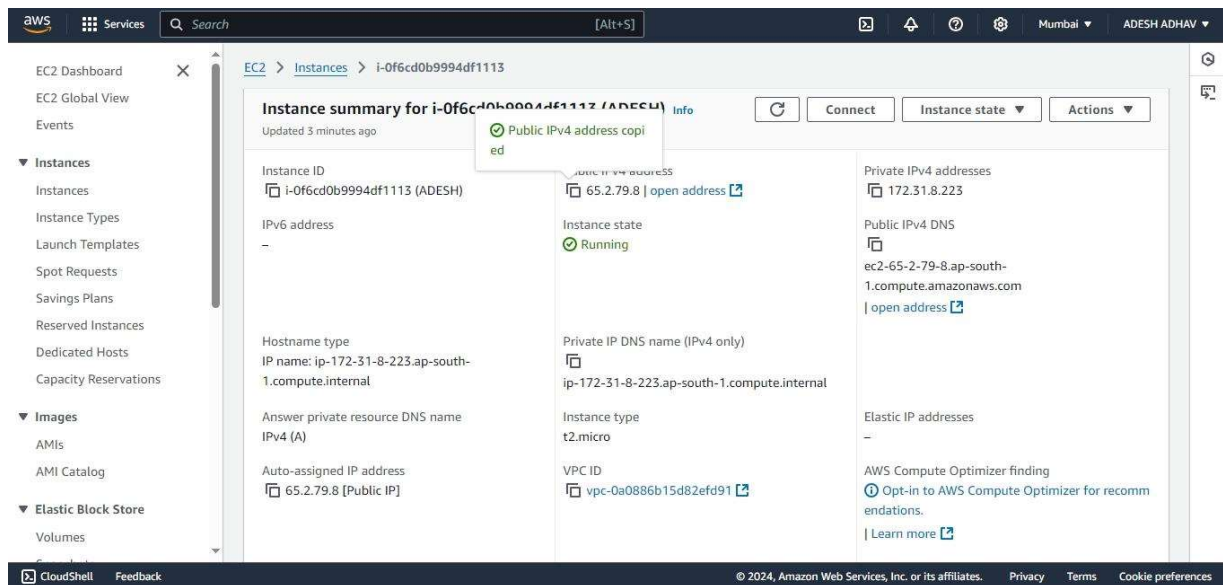
© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

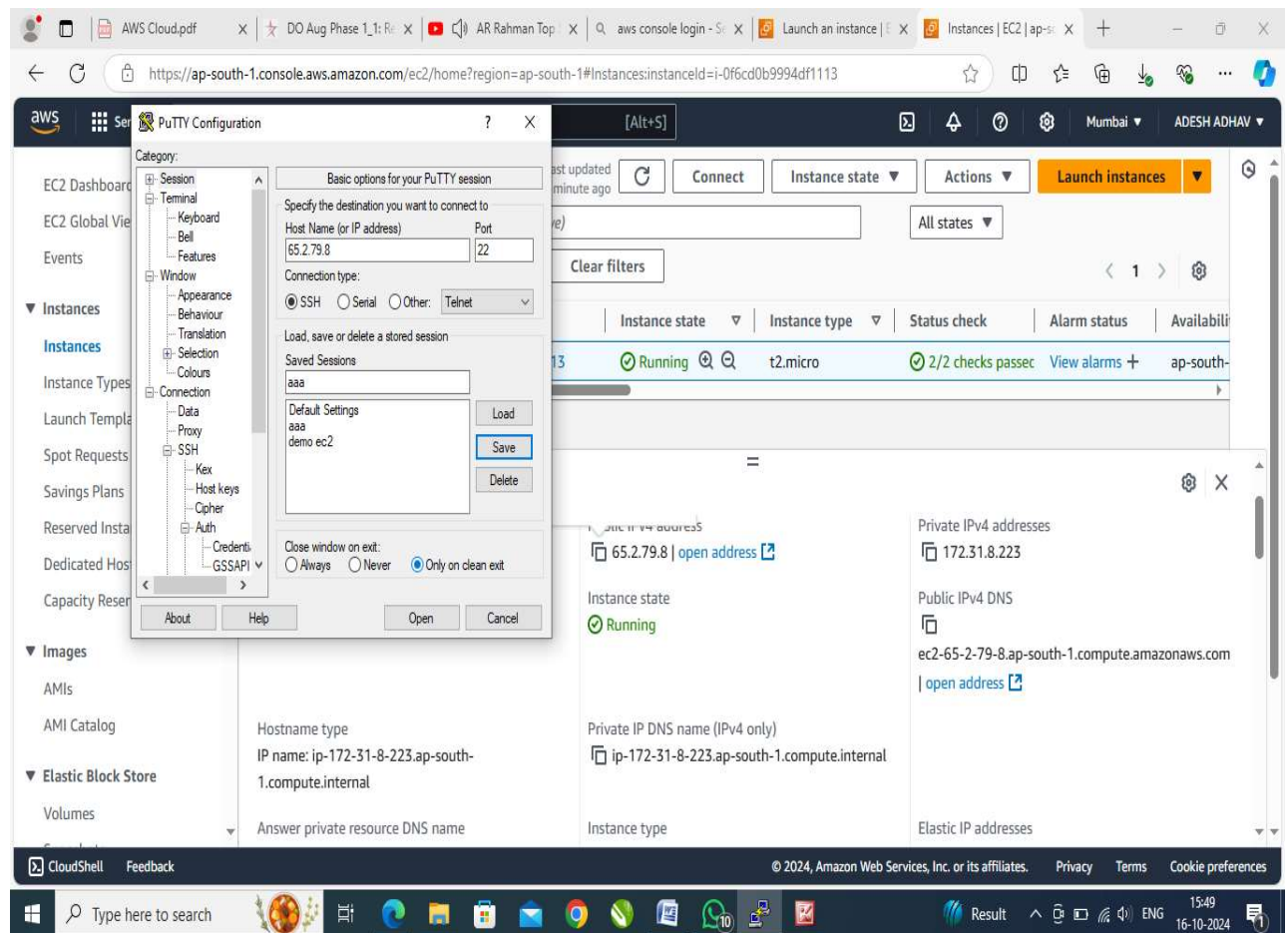
CONNECTION :



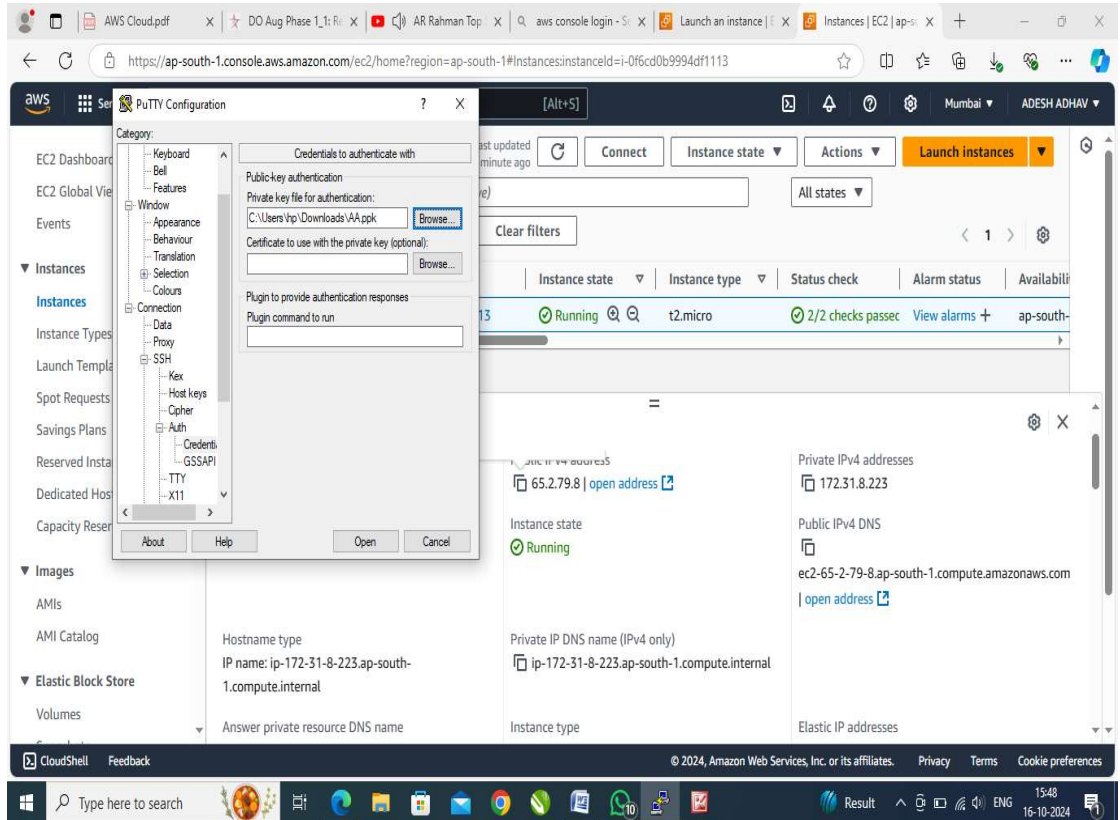
Step 2: Connect to Your Instance Using Putty

- INSTALL PUTTY
- Open putty
- 1.In the Host Name field, enter the public IP address of your instance.
 Configure SSH Authentication
 Connection > SSH > Auth
- 2.Browse and select your .ppk file.
- 3.Connect to instance by allowing open command

HOST NAME



BROWSE A KEY PAIR



```
ubuntu@ip-172-31-8-223: ~  
* Using username "ubuntu".  
* Authenticating with public key "AA"  
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-aws x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/pro  
  
System information as of Wed Oct 16 10:19:12 UTC 2024  
  
System load:  0.0          Processes:           106  
Usage of /:   23.0% of 6.71GB Users logged in:       0  
Memory usage: 20%         IPv4 address for enX0: 172.31.8.223  
Swap usage:   0%  
  
Expanded Security Maintenance for Applications is not enabled.  
  
0 updates can be applied immediately.  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
Last login: Wed Oct 16 09:57:26 2024 from 103.249.241.61  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
ubuntu@ip-172-31-8-223:~$
```

