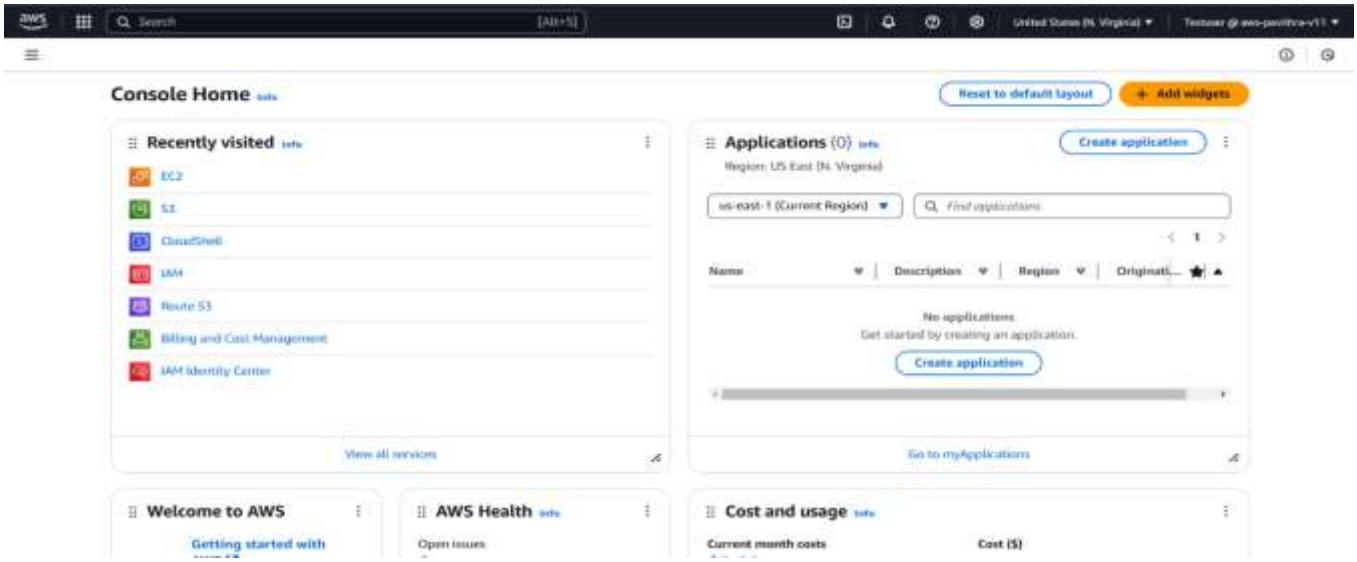
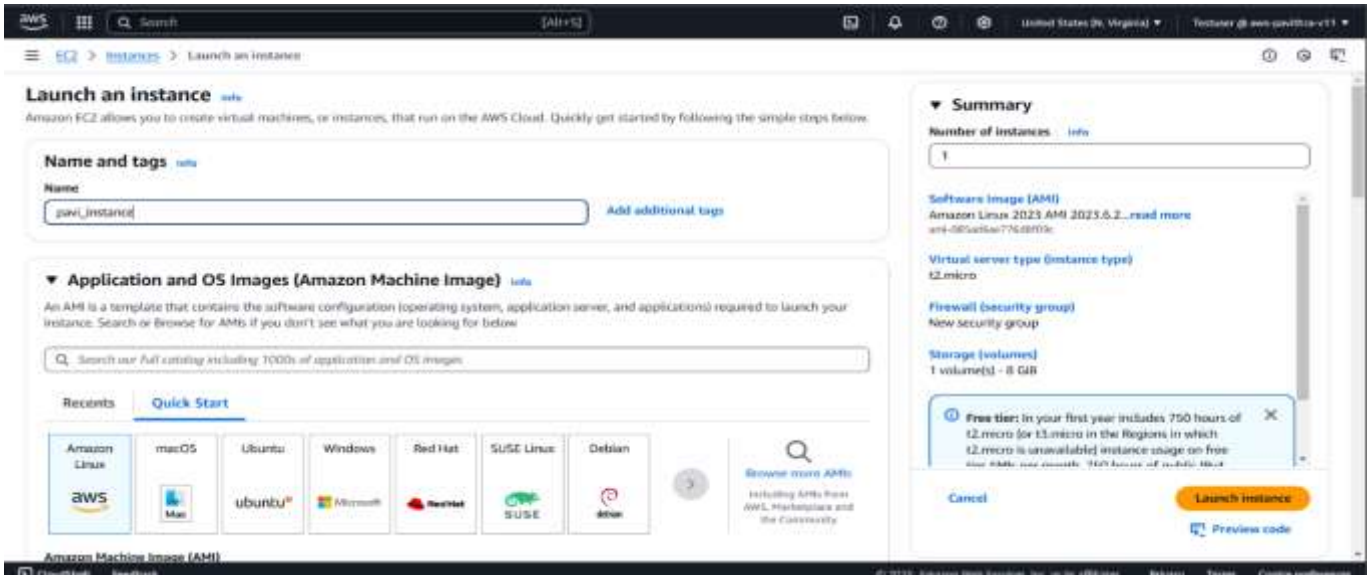
Creating a Linux EC2 Instance on AWS

Step 1: Log In to AWS Management Console

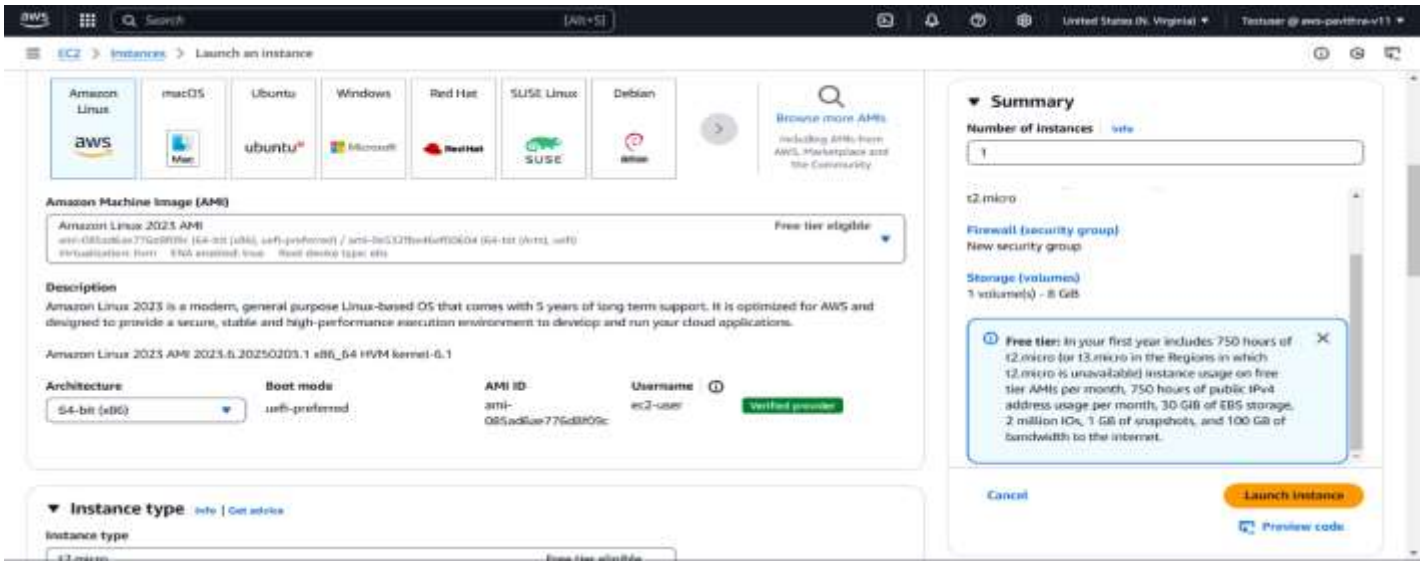


Step 2: Navigate to the EC2 Dashboard

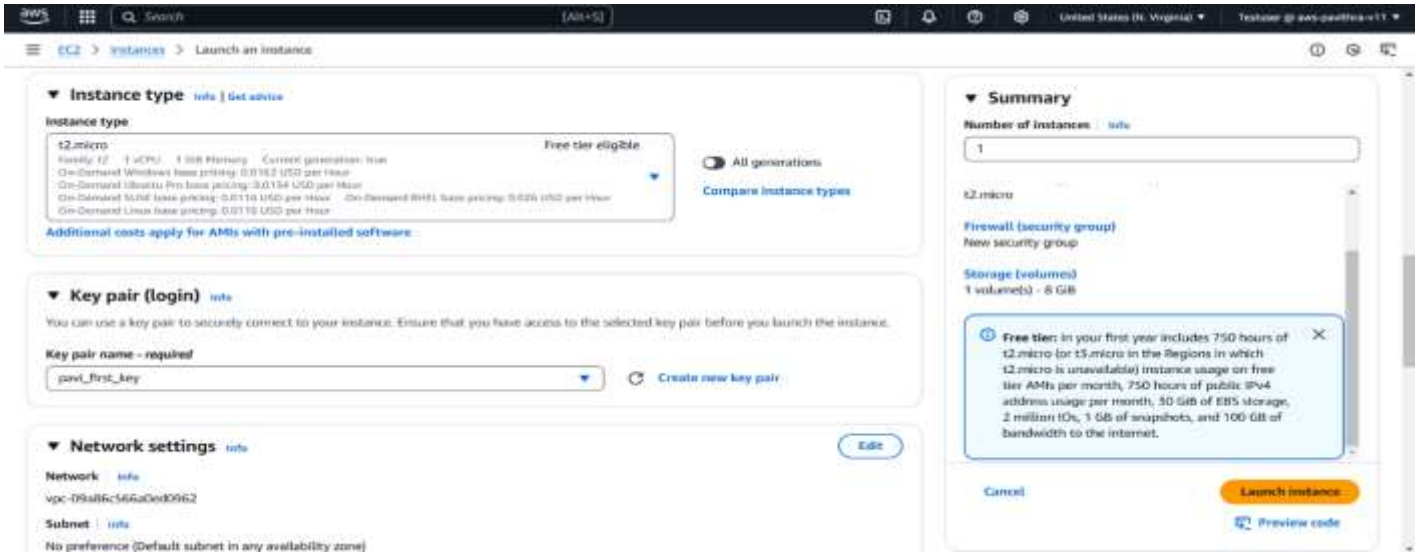


Step 3: Configure Instance Details

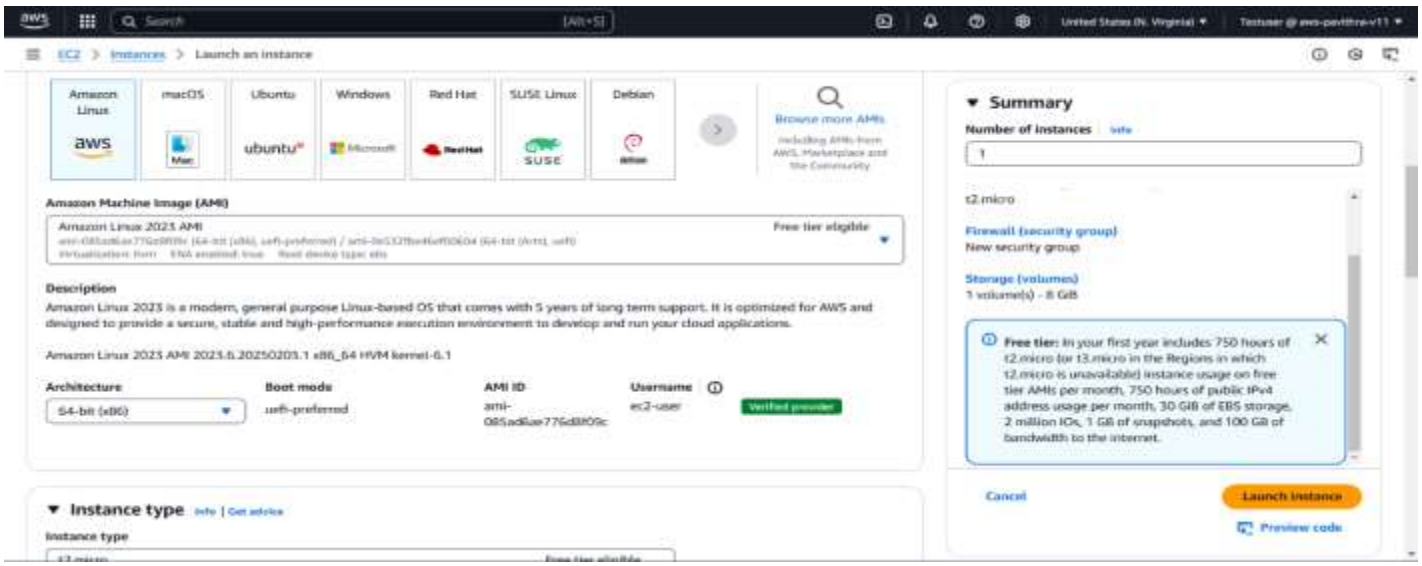
Step 3.1: Choose an Amazon Machine Image (AMI)



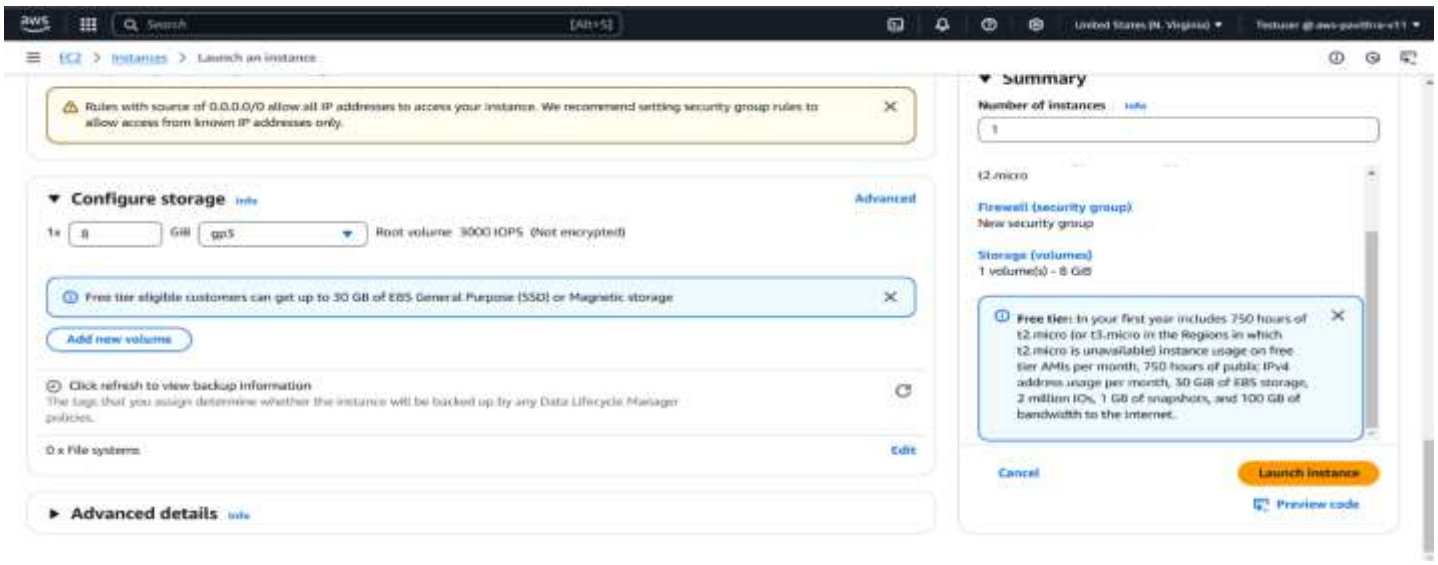
Step 3.2: Choose an Instance Type



Step 3.3: Configure Instance Details

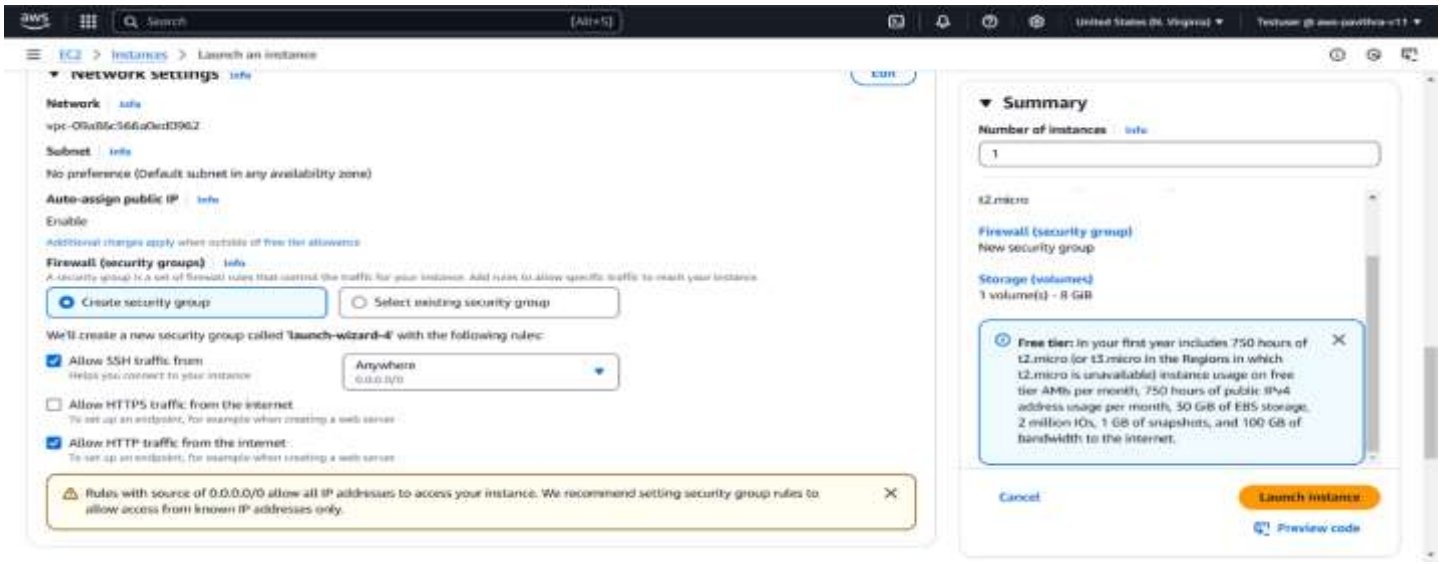


Step 4: Add Storage

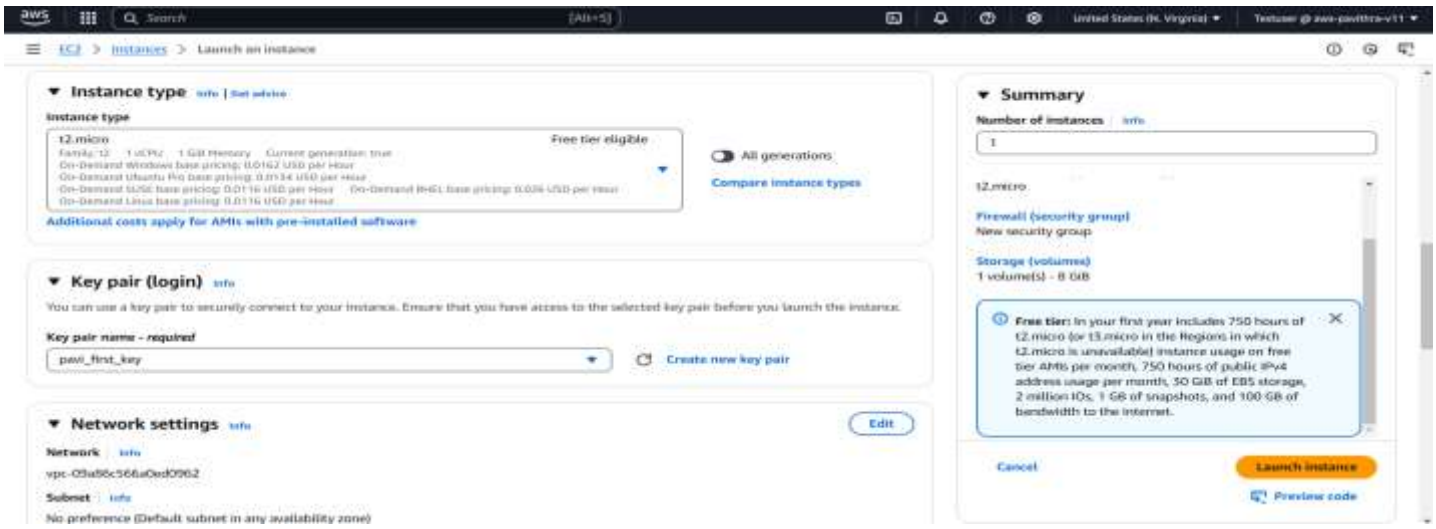


Step 5: Add Tags (Optional)

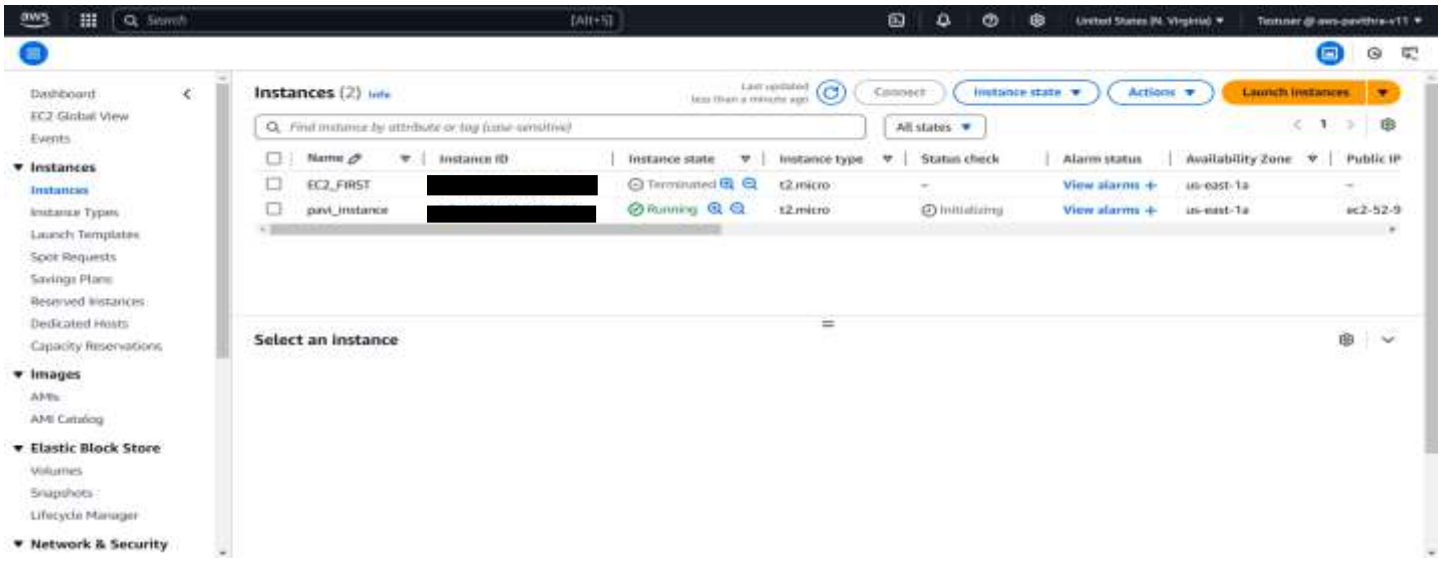
Step 6: Configure Security Group



Step 7: Launch Instance

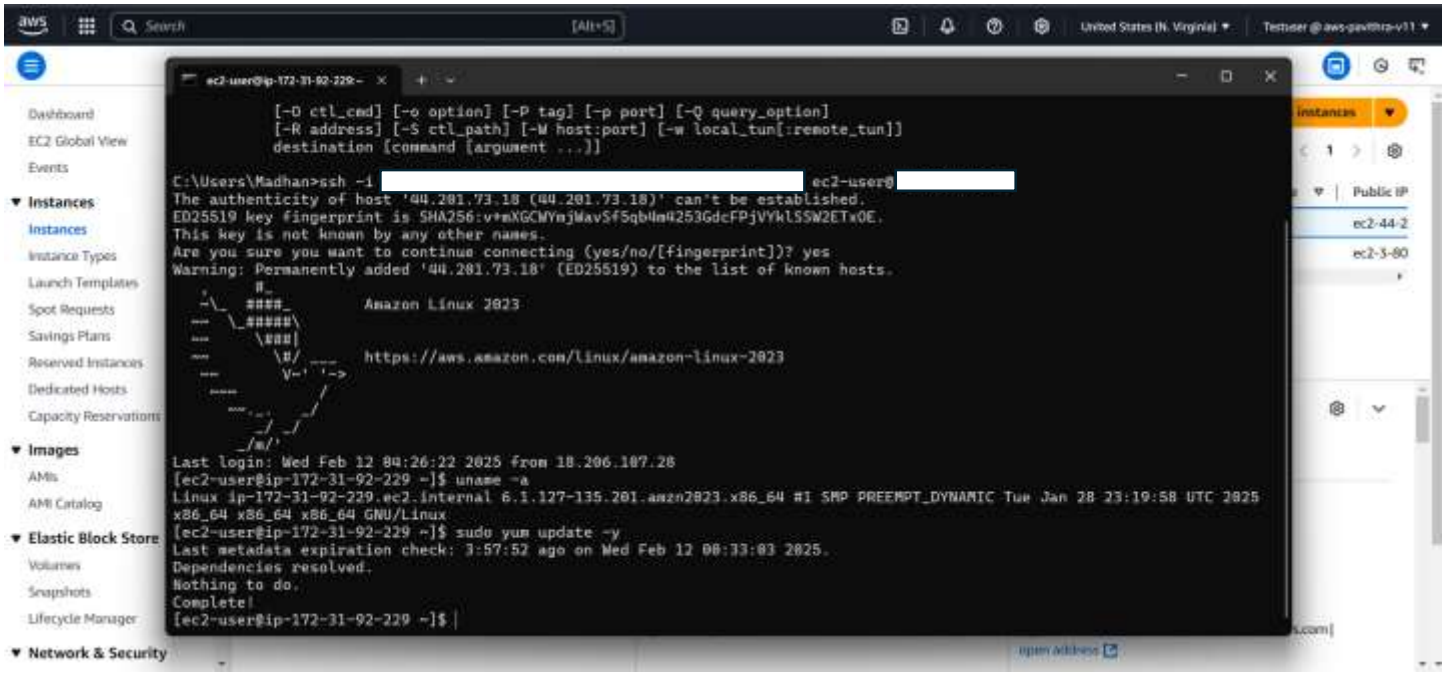


Step 8: Verify Your Instance

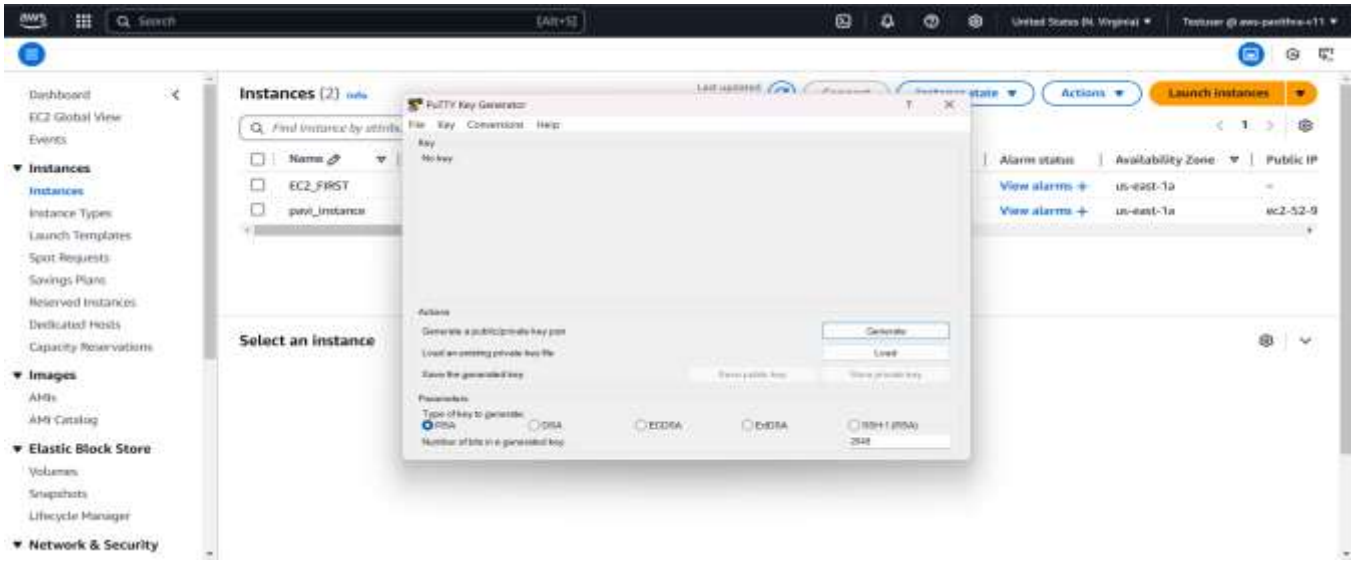


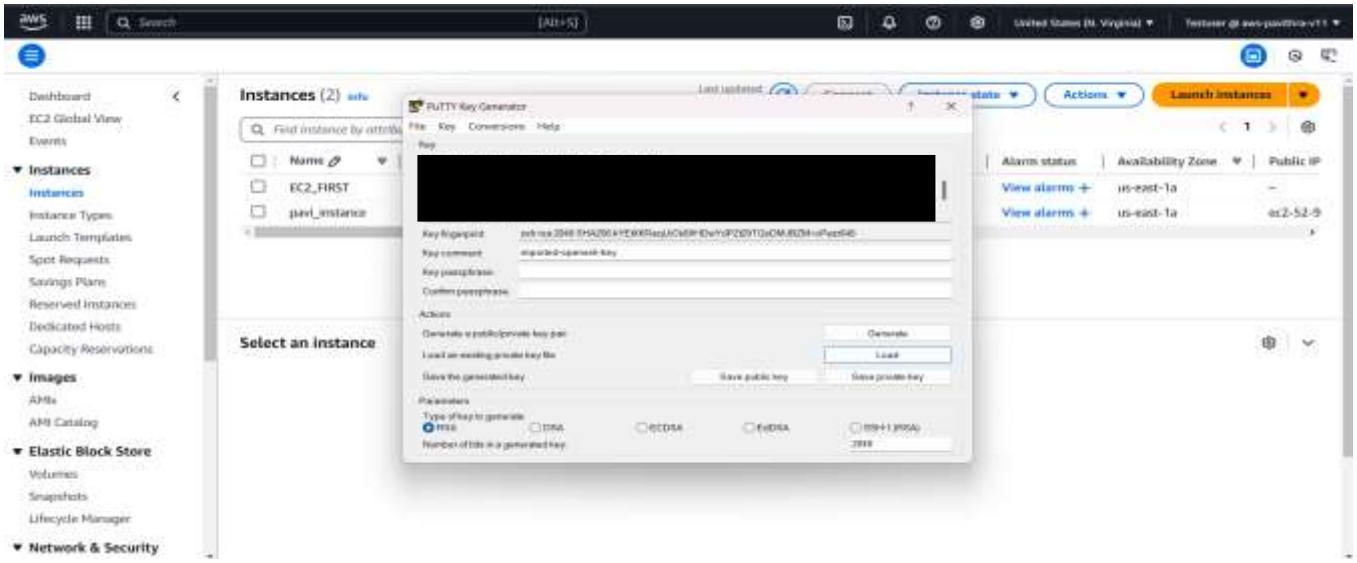
Step 9: Connect to the Instance

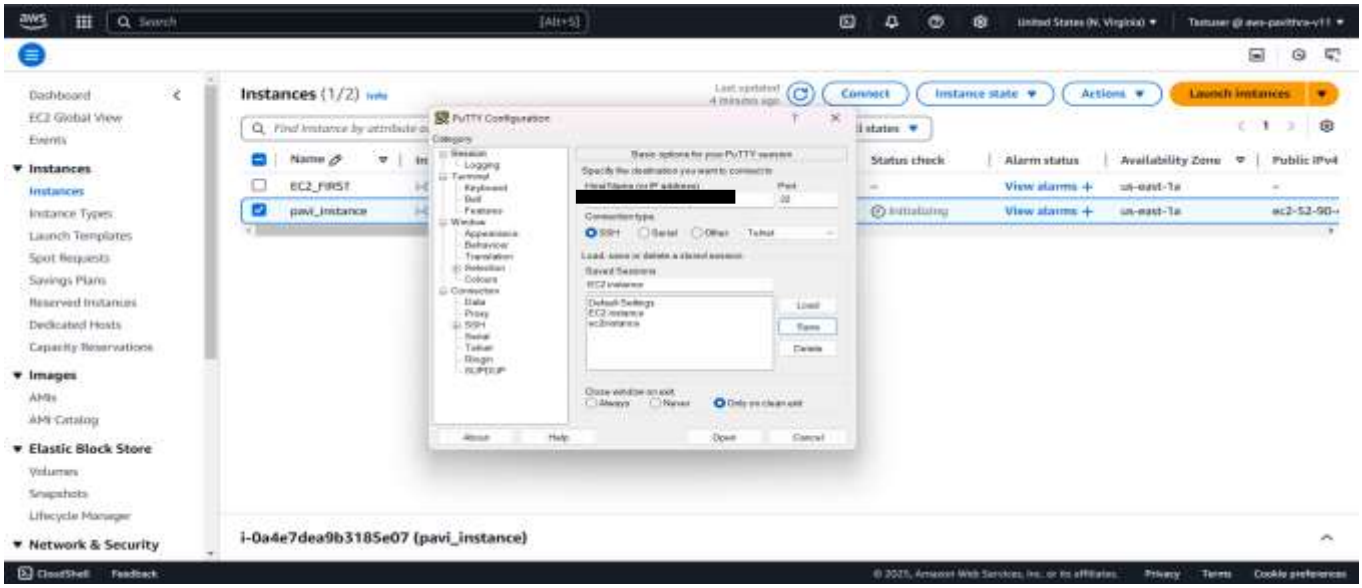
Step 9.1: Connect Using an SSH Client

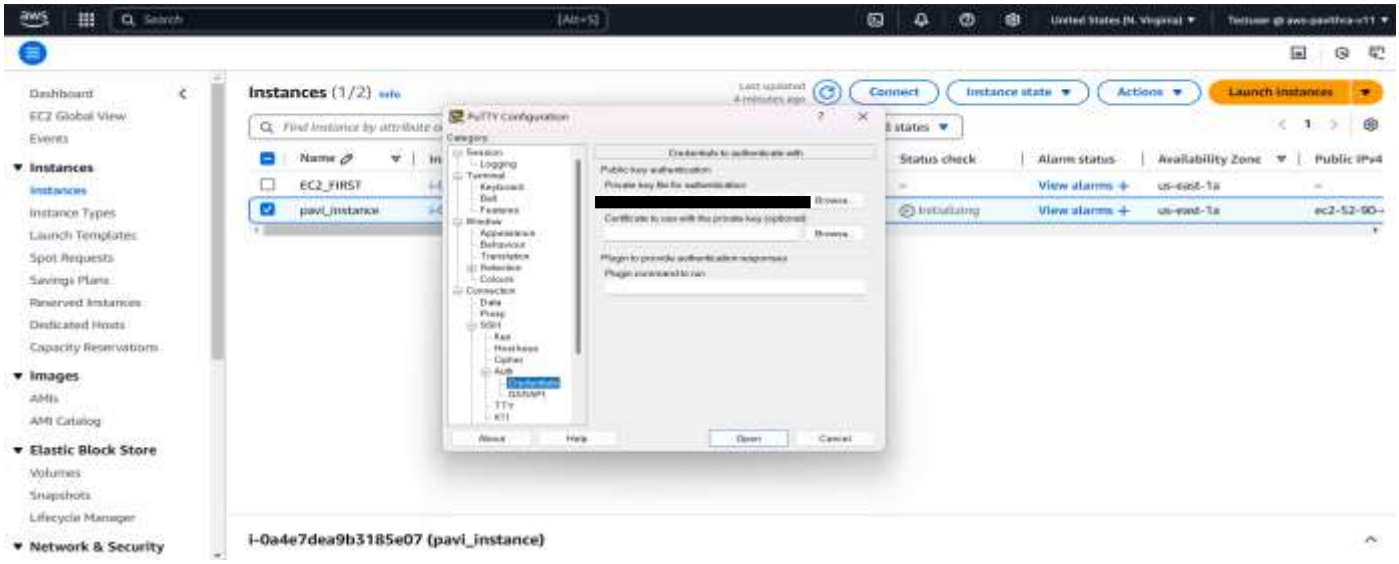


Step 9.2: Connect Using PuTTY (Windows)

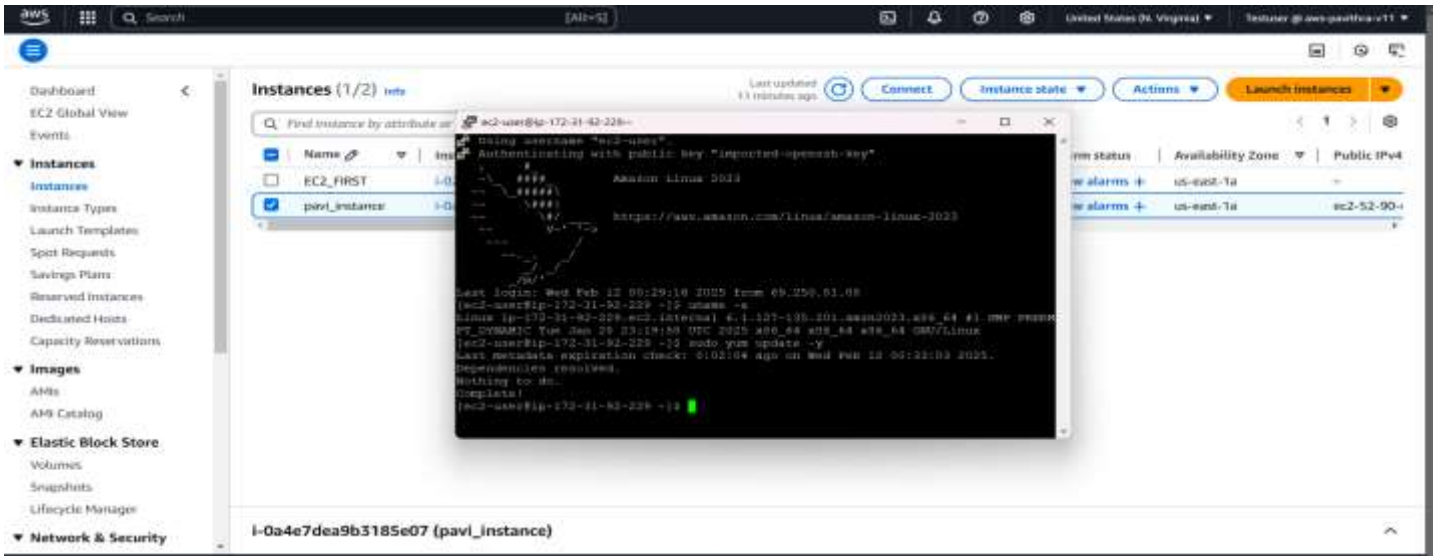


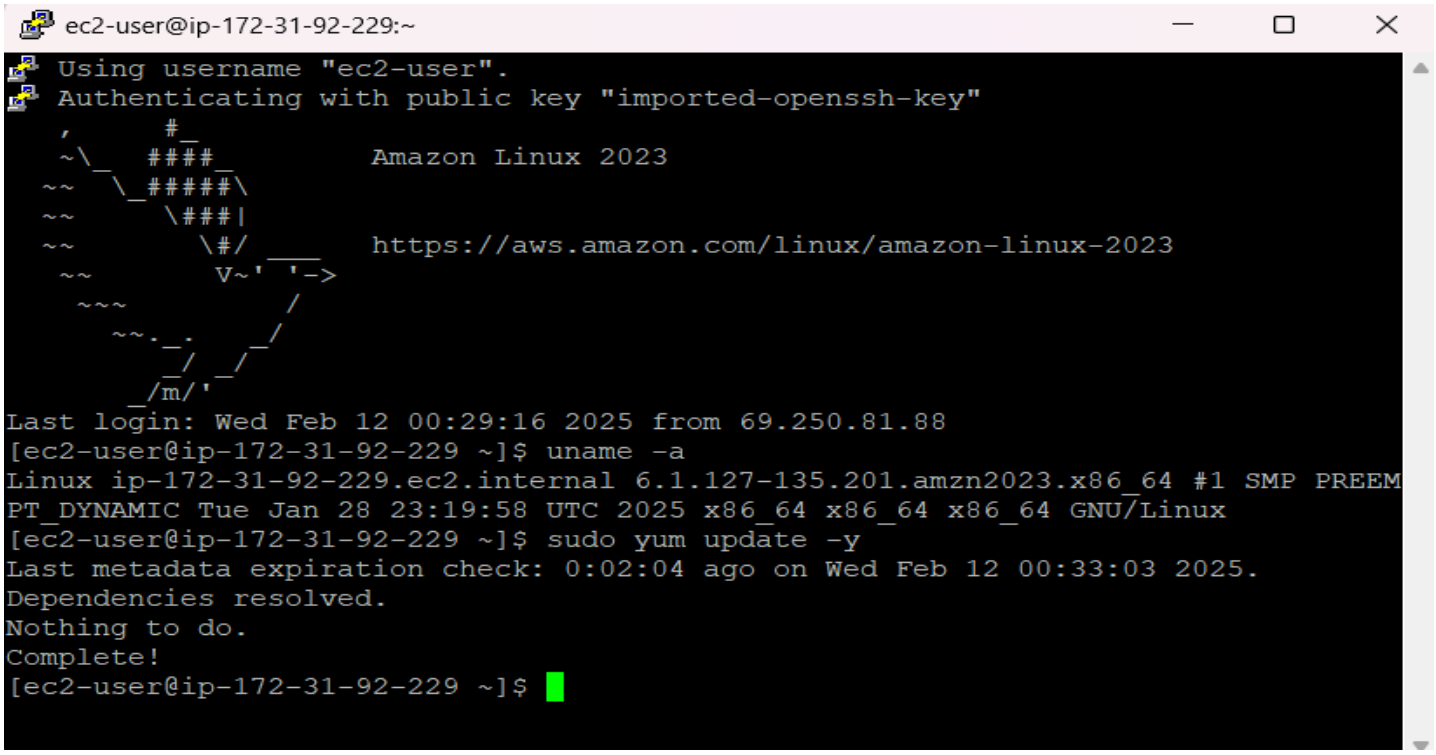

Instances (2)
PuTTY Key Generator
Select an instance


Instances (1/2)
PuTTY Configuration
i-0a4e7dea9b3185e07 (pavi_instance)

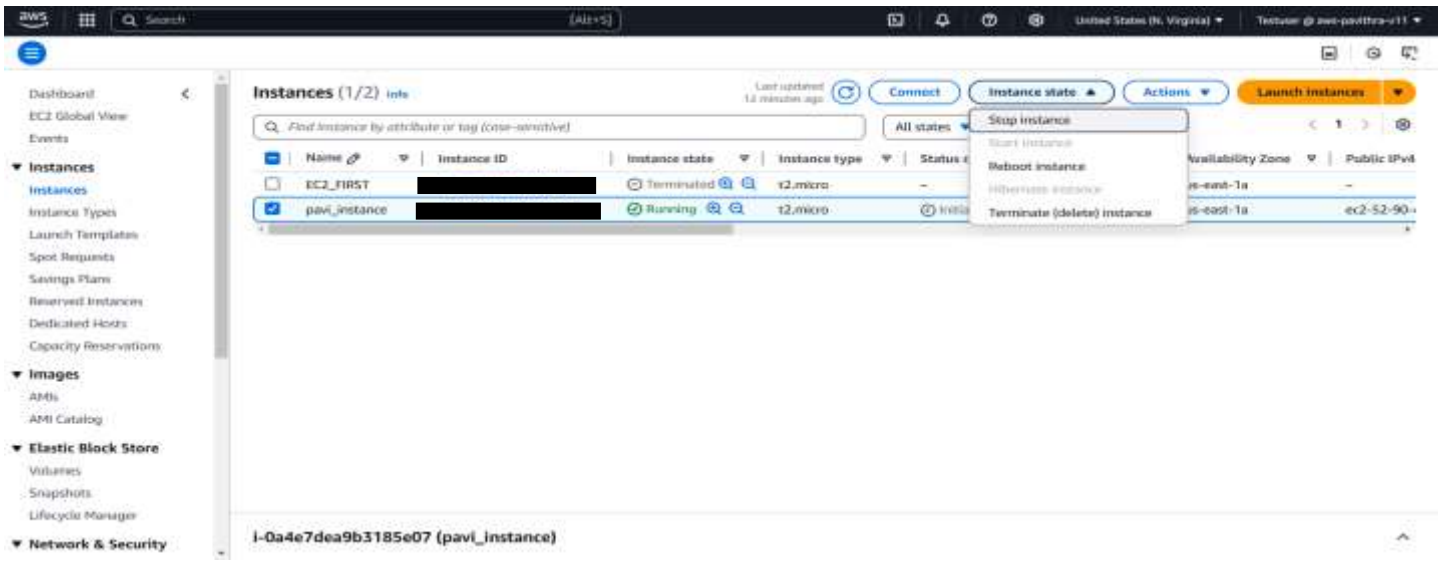

Instances (1/2)
PuTTY Configuration
i-0a4e7dea9b3185e07 (pavi_instance)

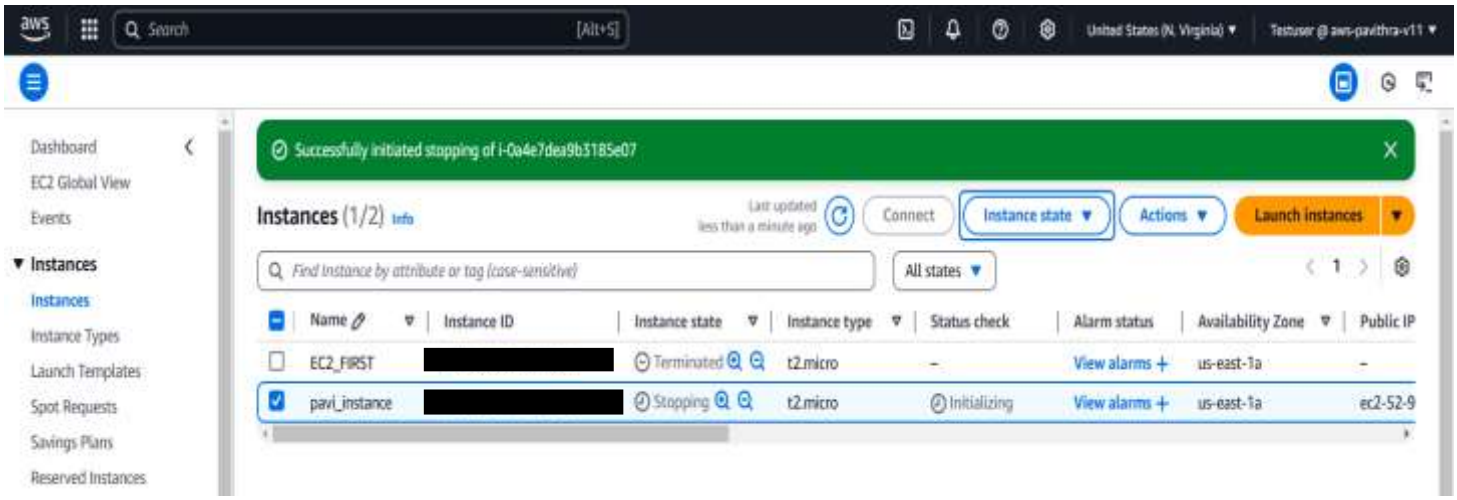
Step 10: Verify Connection





Step 11: Clean Up (Optional)





A brief report summarizing

Step 1: Log In to AWS Management Console

- Access the **AWS Management Console** and sign in.
- Navigate to the **EC2 Dashboard**.

Step 2: Configure EC2 Instance

- **Choose Amazon Machine Image (AMI):** Selected **Amazon Linux** as the operating system.
- **Select Instance Type:** Chose an instance type based on performance needs.
- **Configure Instance Details:** Ensured the instance is properly set up with networking options.

Step 3: Add Storage & Tags

- **Define Storage:** Kept the default storage settings.
- **Add Tags (Optional):** Assigned a tag to easily identify the instance.

Step 4: Configure Security Group

- Configured **security rules** to allow access for:
    - **SSH (Port 22)** – Enabled secure remote login.

- **HTTP (Port 80)** – Allowed web traffic access.

Step 5: Launch and Verify Instance

- Reviewed configurations and **launched the instance**.
- Created and downloaded a **key pair (.pem file)** for secure SSH access.
- Verified that the instance **changed to Running status** in the EC2 dashboard.

Step 6: Connect to the Instance

Option 1: SSH Client (Linux/Mac/Windows Terminal)

1. Open a terminal and navigate to the directory containing the .pem file.
2. Connect using the following command:
3. ssh -i <your-key.pem> ec2-user@<public-ip>
4. Accepted the host key fingerprint and successfully logged in.

Option 2: PuTTY (Windows Users)

1. Converted the .pem file to. ppk format using PuTTYgen.
2. Opened **PuTTY**, entered the **Public IP** of the instance like ec2-user@<public-ip>
3. Under **Connection → SSH → Auth->credintials**, loaded the. ppk key and connected.

Step 7: Verify the Connection

- After logging in, ran system verification commands:
- uname -a
- lsb_release -a
- sudo yum update -y
- Ensured connectivity and verified that **Amazon Linux** was running correctly.

Step 8: Clean Up (Optional)

- If the instance is no longer needed, it can be **terminated** from the AWS EC2 dashboard to prevent additional charges.