**Placement Empowerment Program**

***Cloud Computing and DevOps Centre***

**Secure Access with a Bastion Host**Set up a bastion host in a public subnet to securely access instances in a private subnet.

Name: SIVAKUMAR C Department: AML



**Introduction and Overview**

A **Bastion Host** is a secure server that provides controlled access to instances in a **private subnet**. This setup enhances security by restricting direct access to private instances while allowing SSH connections only through the **Bastion Host** in a public subnet. This guide outlines the steps to configure a **Bastion Host** in AWS to securely connect to instances in a private subnet.

**Objectives**

* Set up a **VPC** with public and private subnets.
* Deploy a **Bastion Host** in a public subnet.
* Deploy a **private instance** in a private subnet.
* Restrict direct SSH access to the private instance.
* Configure secure SSH access through the **Bastion Host**.

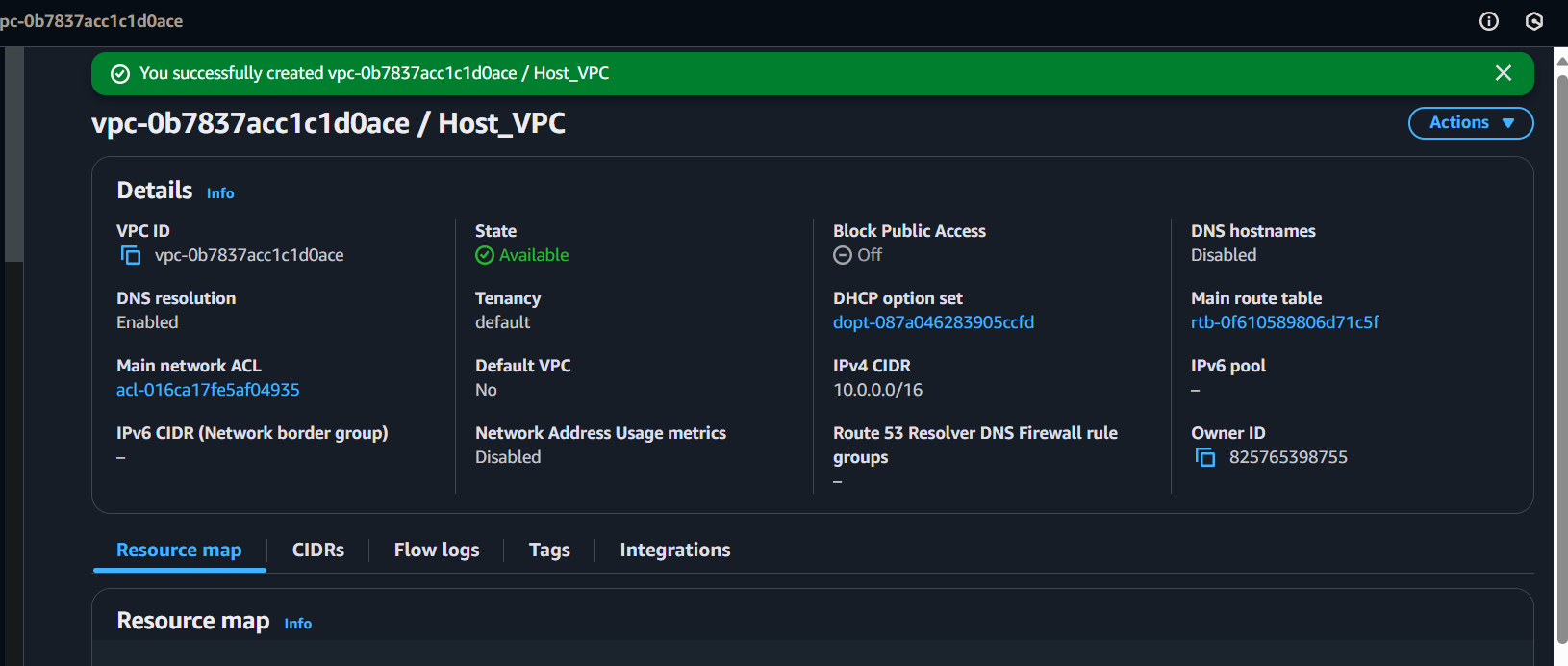
**Importance**

* **Enhanced Security**: Prevents direct access to private instances from the internet.
* **Controlled Access**: Only trusted users can connect via the Bastion Host.
* **Network Segmentation**: Isolates internal workloads for better security.
* **Compliance and Best Practices**: Follows AWS security guidelines.

**STEPS:**

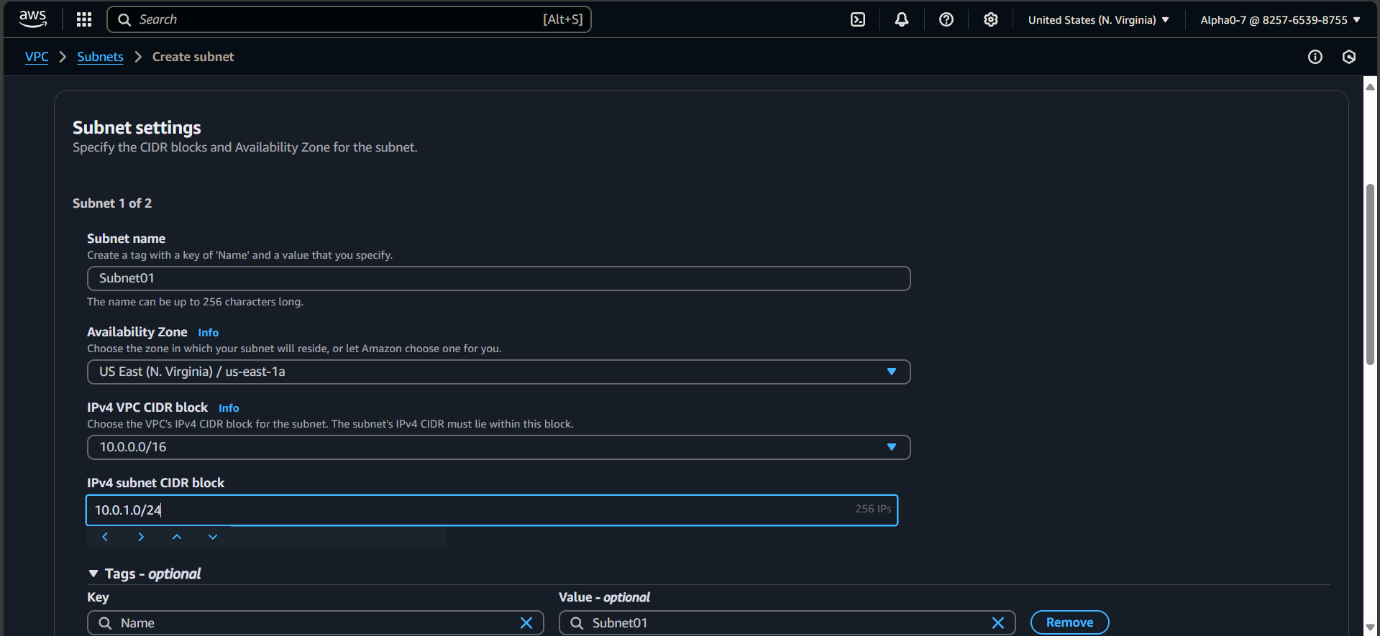
**STEP 1: Create a VPC**

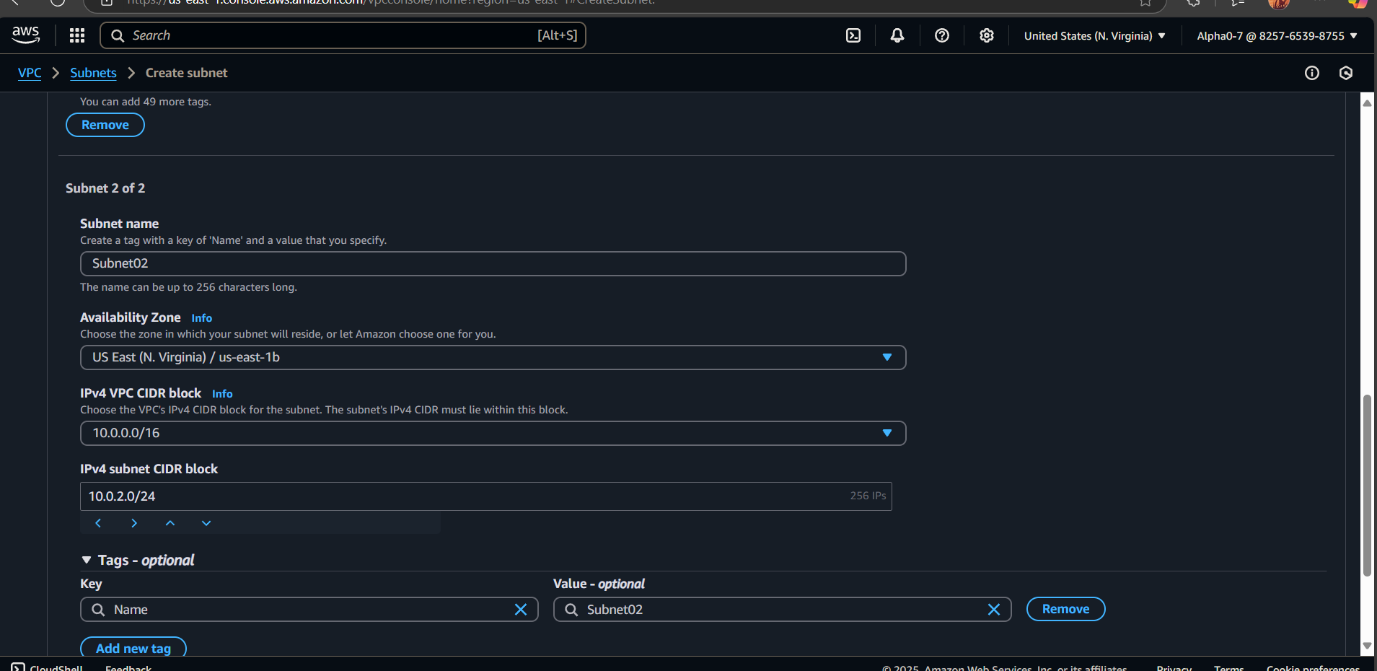
* Go to the AWS VPC Console.
* Click on Create VPC and select VPC only.
* Set the CIDR block as 10.0.0.0/16.
* Click Create VPC.



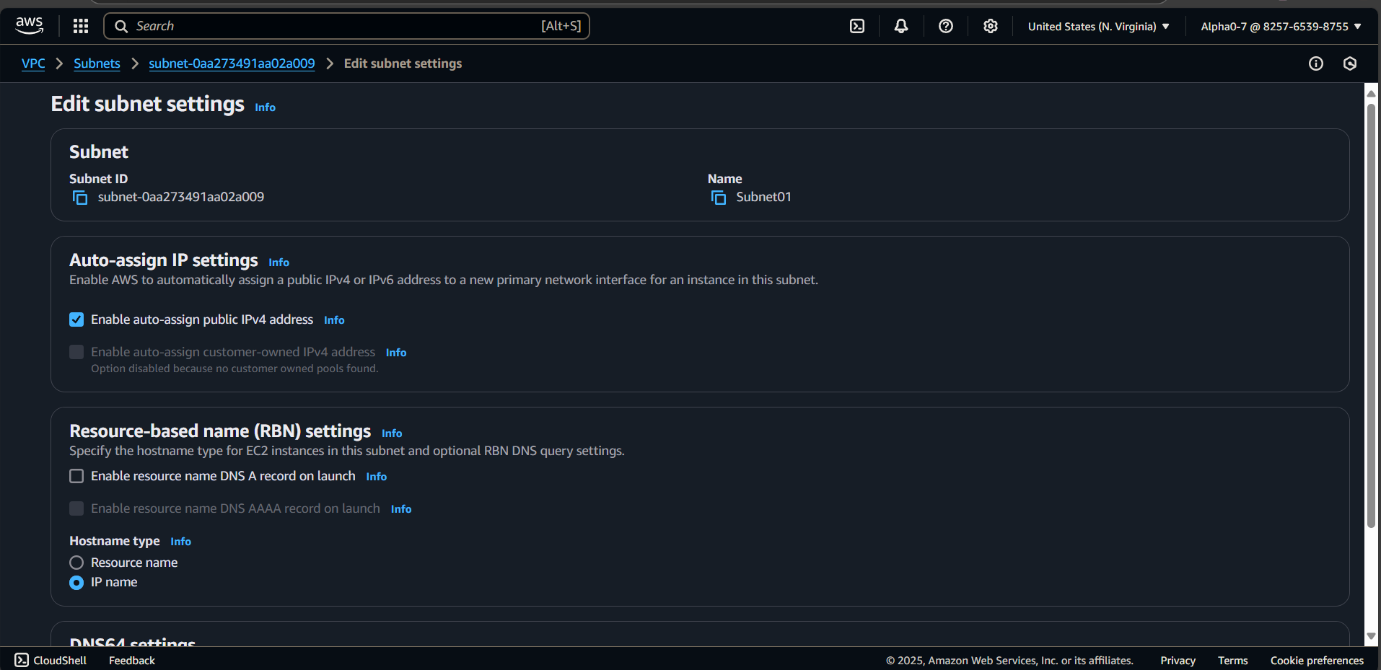
**STEP 2: Create Public and Private Subnets**

* Navigate to the Subnets section in the VPC console.
* Click Create Subnet and configure:
  1. Public Subnet: 10.0.1.0/24
  2. Private Subnet: 10.0.2.0/24



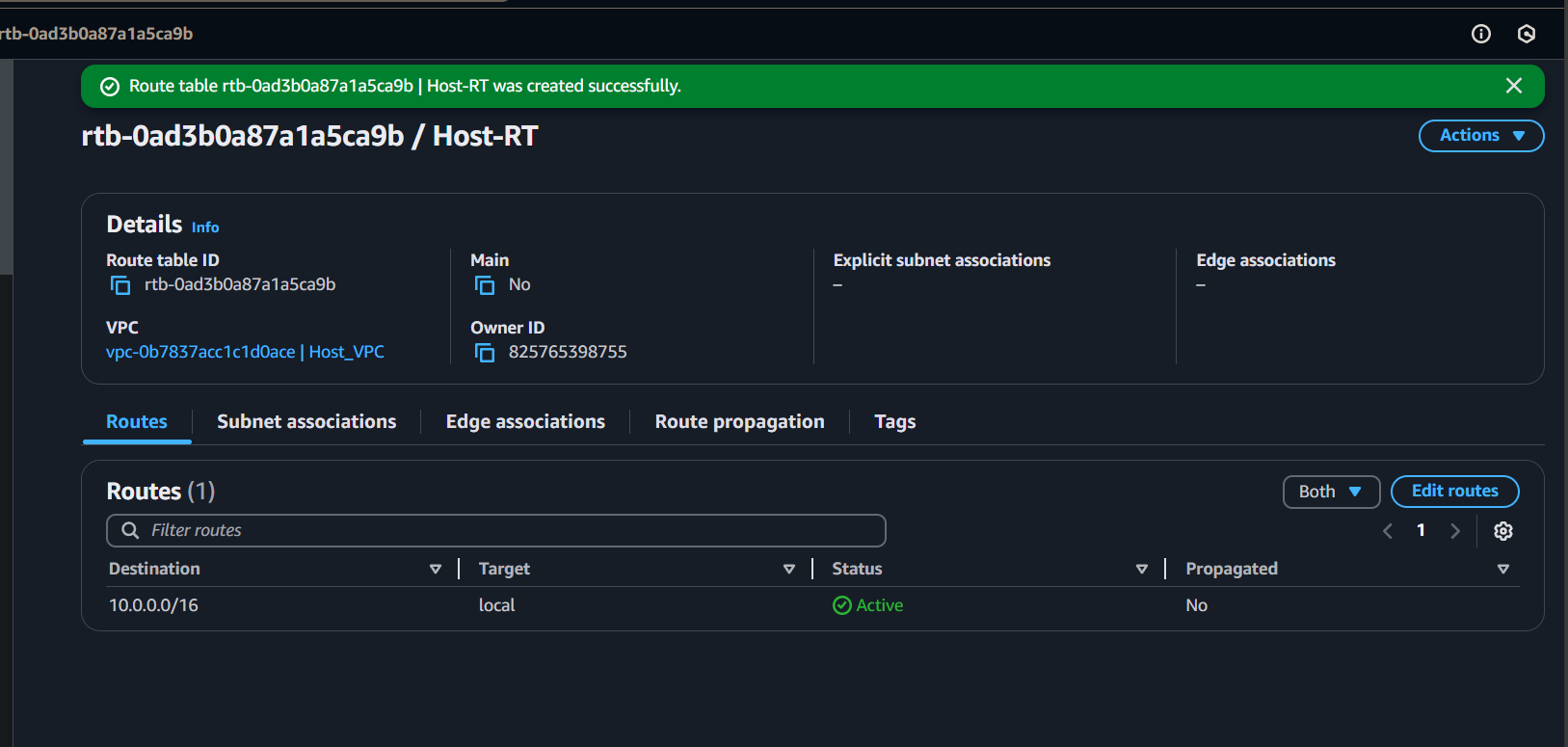


* Enable Auto-assign Public IPv4 for the public subnet.

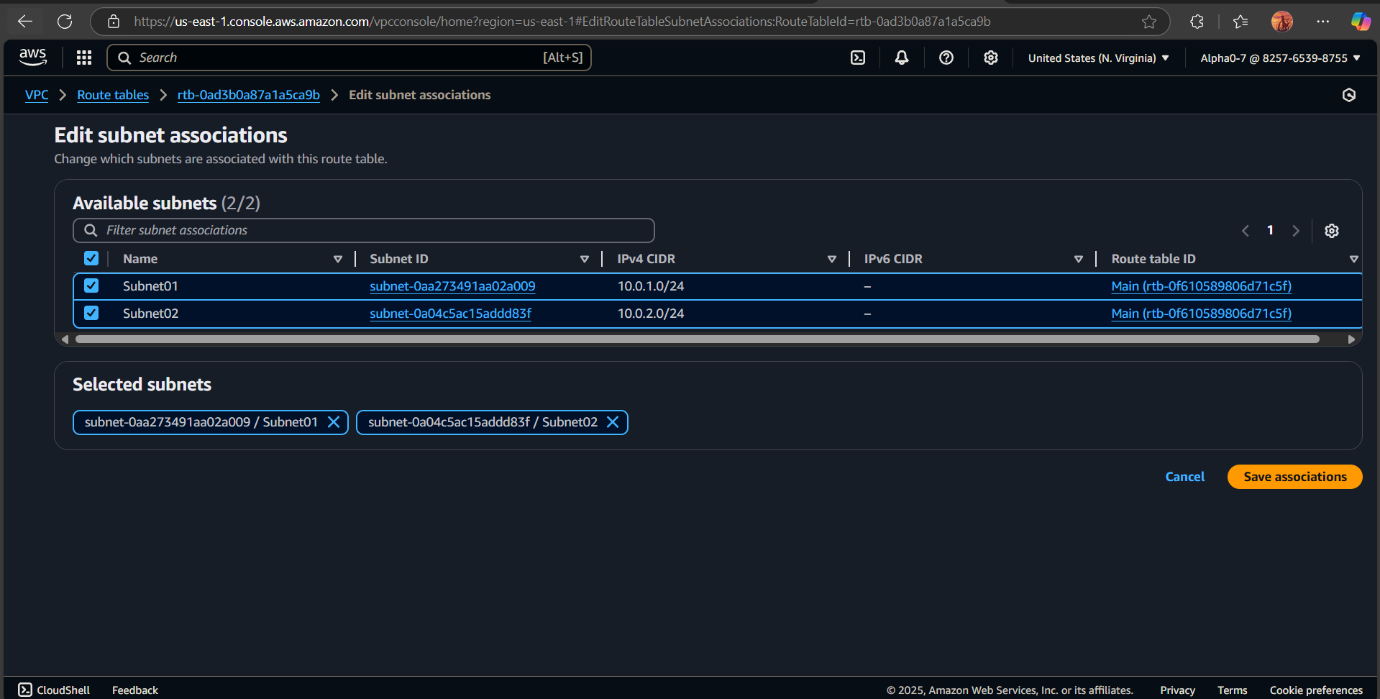


**STEP 3: Create a Route Table and Associate Subnets**

* Go to Route Tables and click Create Route Table.

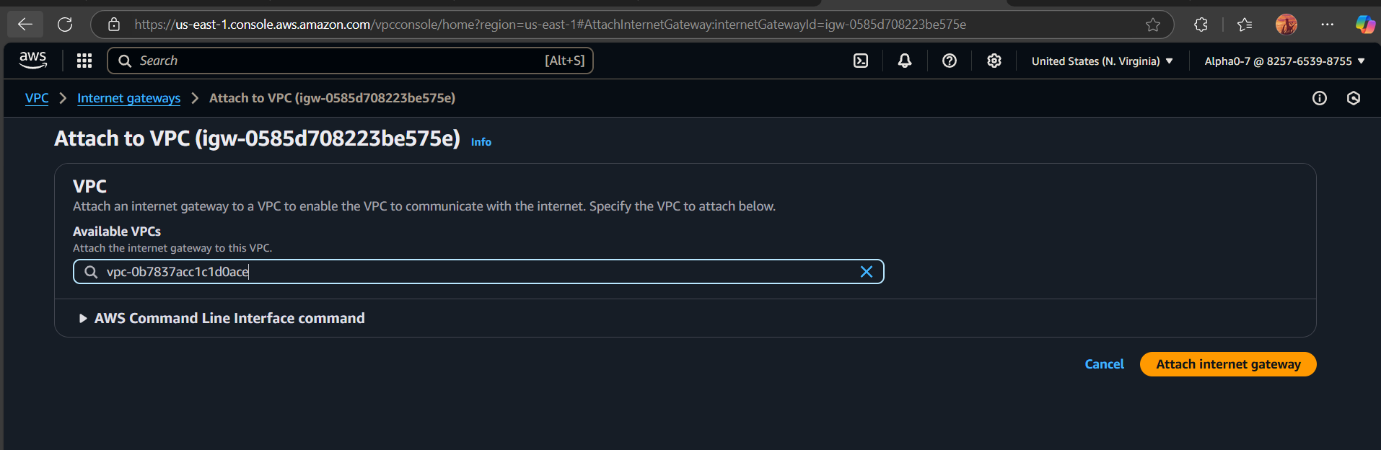


* Associate the VPC you created.
* Explicitly associate both public and private subnets with this route table.

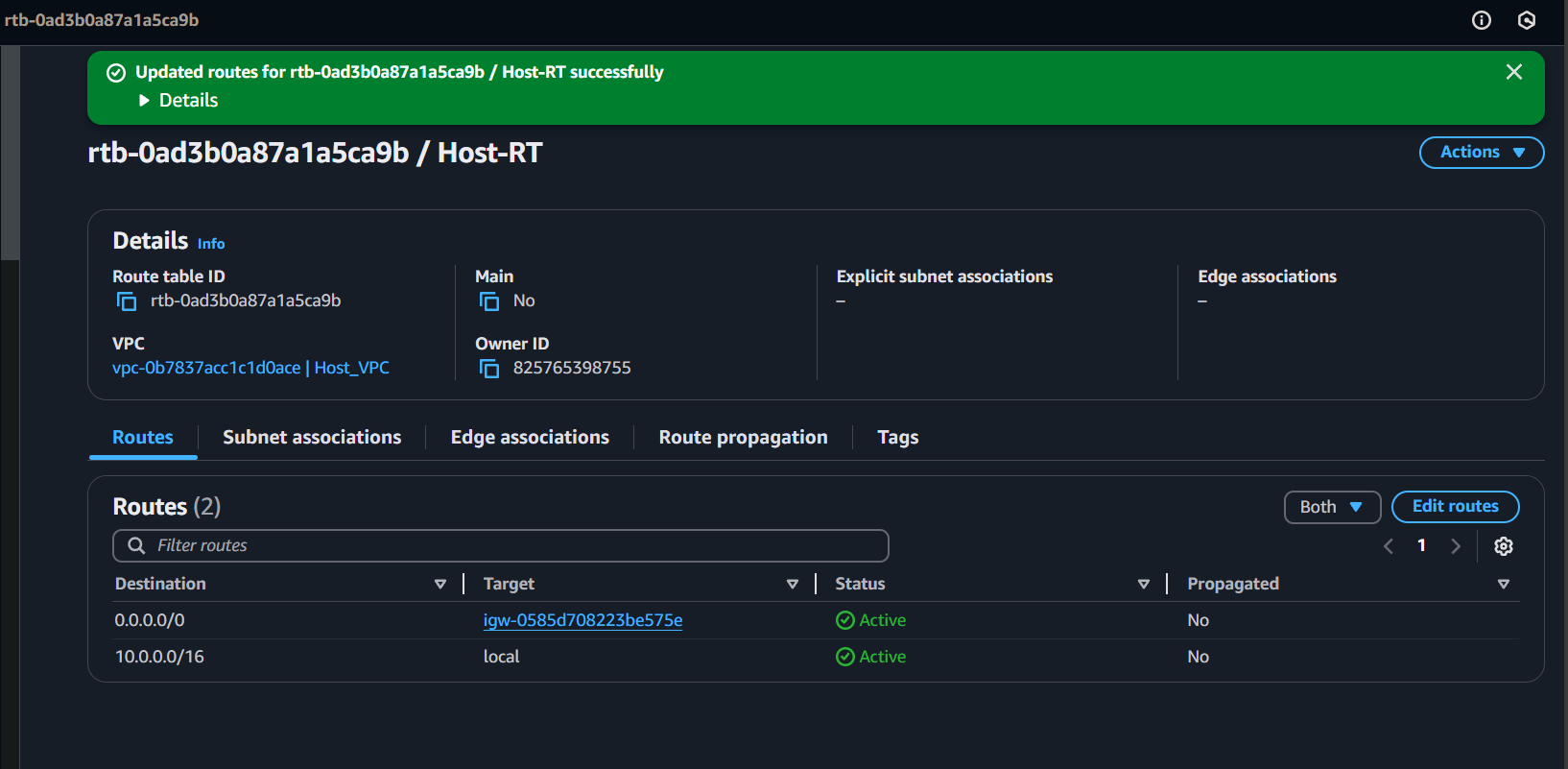


**STEP 4: Create and Attach an Internet Gateway**

* Navigate to Internet Gateways and click Create Internet Gateway.
* Attach it to your VPC.



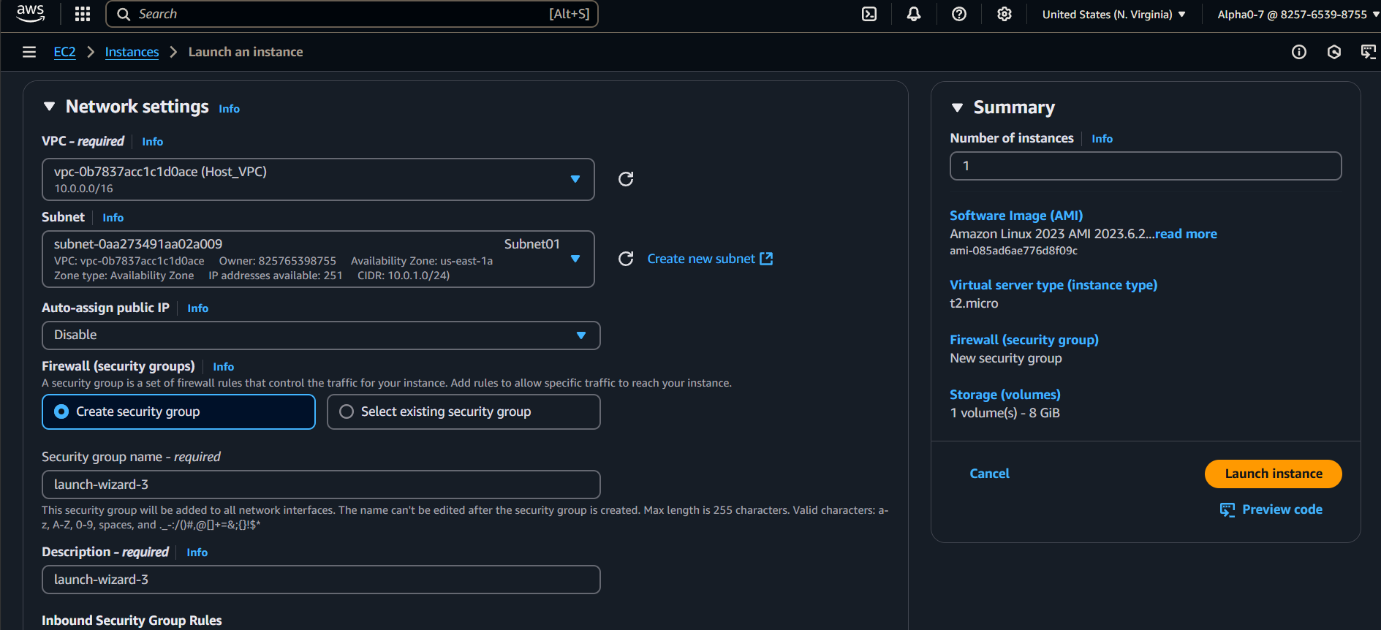
* Add a default route (0.0.0.0/0) in the Route Table to the Internet Gateway (for public internet access).



**STEP 5: Launch EC2 Instances**

Bastion Host (Public Subnet)

* Go to EC2 Console and click Launch Instance.
* Select an AMI (Amazon Linux/Ubuntu).
* Choose the public subnet.
* Ensure Auto-assign Public IP is enabled.
* Attach a Security Group that allows SSH (Port 22) from your IP.



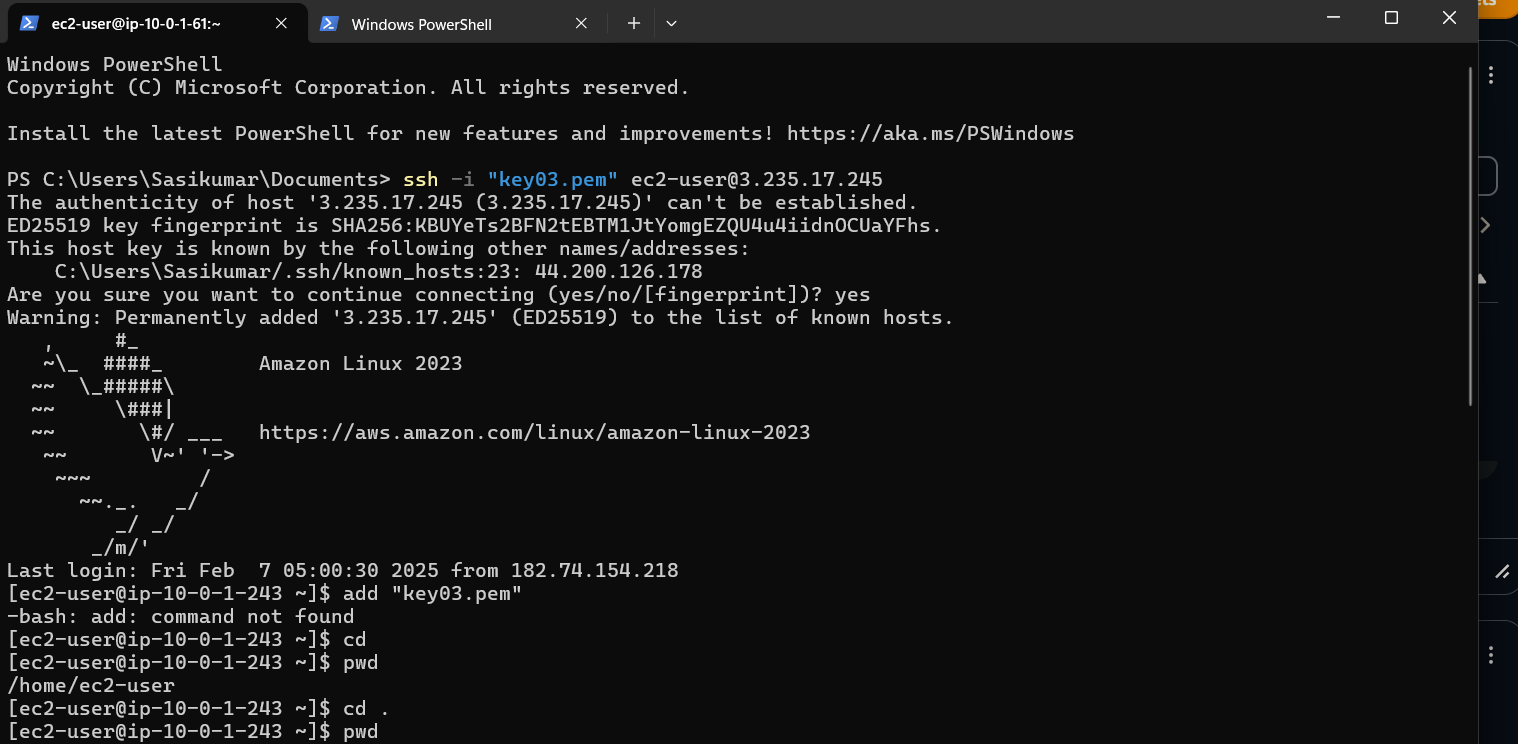
Private Instance (Private Subnet)

* Launch another EC2 instance.
* Select the private subnet.
* Do not enable Auto-assign Public IP.
* Attach a Security Group that allows SSH access only from the Bastion Host’s Security Group.

**STEP 6: SSH into the Bastion Host**

* Open a terminal on your local machine.
* Connect to the Bastion Host using SSH:

ssh -i your-key.pem ec2-user@<Bastion\_Host\_Public\_IP>



**STEP 7: Transfer Key to Bastion Host**

* Open a new terminal window and use scp to transfer the private key to the Bastion Host:

scp -i your-key.pem your-key.pem ec2-user@<Bastion\_Host\_Public\_IP>:~/



* Secure the Key File on the Bastion Host:

chmod 400 your-key.pem

**STEP 8: SSH into the Private Instance from the Bastion Host**

* From the Bastion Host, connect to the private instance:

ssh -i your-key.pem ec2-user@<Private\_Instance\_Private\_IP>

* You should now have secure access to the private instance.

