**VPC SETUP AND CONFIGURATION SUMMARY**

**CIDR blocks used for VPC and Subnets**

In the VPC CIDR Block, I got to use 10.0.0.0/16 as the IP Address for the VPC which allows up to 65,536 addresses

**Public Subnets**

Got to use 10.1.0.0/24 IPv4 address

It is a smaller block within the VPC, dedicated to public-facing resources, providing 256 IP addresses

**Private Subnets**

Got to use 10.0.0.0/24 as my IPv4 address

Another subnet within the VPC that is intended for private resources without direct internet access, also with 256 IP addresses

**INTERNET GATEWAY AND NAT GATEWAY SETUP**

**Internet Gateway**

An internet gateway is attached to the VPC, enabling resources within the public subnet to communicate with the internet.

It is configured to allow outgoing and incoming traffic for the public, like EC2 instances that need internet access.

**NAT Gateway**

This is a setup in the public subnet to enable private subnet, instances to access the internet for outbound communication, for example, software updates without being directly accessible from the internet.

**SECURITY GROUP AND NETWORK ACL CONFIGURATION**

**Security Groups**

The public EC2 instance Security Group allows SSH port 22 access from a specific IP or range for secure administration, it also allows HTTP/HTTPS port 80/443 traffic web server access

In the Private EC2 instance security group, no inbound traffic is allowed except from the public subnet while its Outbound traffic is permitted for internet access via the NAT Gateway

**NETWORK ACL**

The public subnet NACL, Inbound allows HTTP, HTTPS, and SSH traffic while the Outbound allows all outbound traffic

The private subnet NACL, Inbound restricts external internet access, only allowing internal traffic, while Outbound enables all traffic to the NAT Gateway for internet access.

**EC2 INSTANCES LAUNCHED AND THEIR ROLES**

**Public EC2 Instance**

**Role:** It is a web server

**Location**: it is launched in the public subnet

**Access:** It is accessible via SSH and HTTP/HTTPS for external communication

**Purpose:** Provides direct internet access for hosting web applications

**Private EC2 instance**

**Role:** It is a backend service or application instance that does not need direct internet access

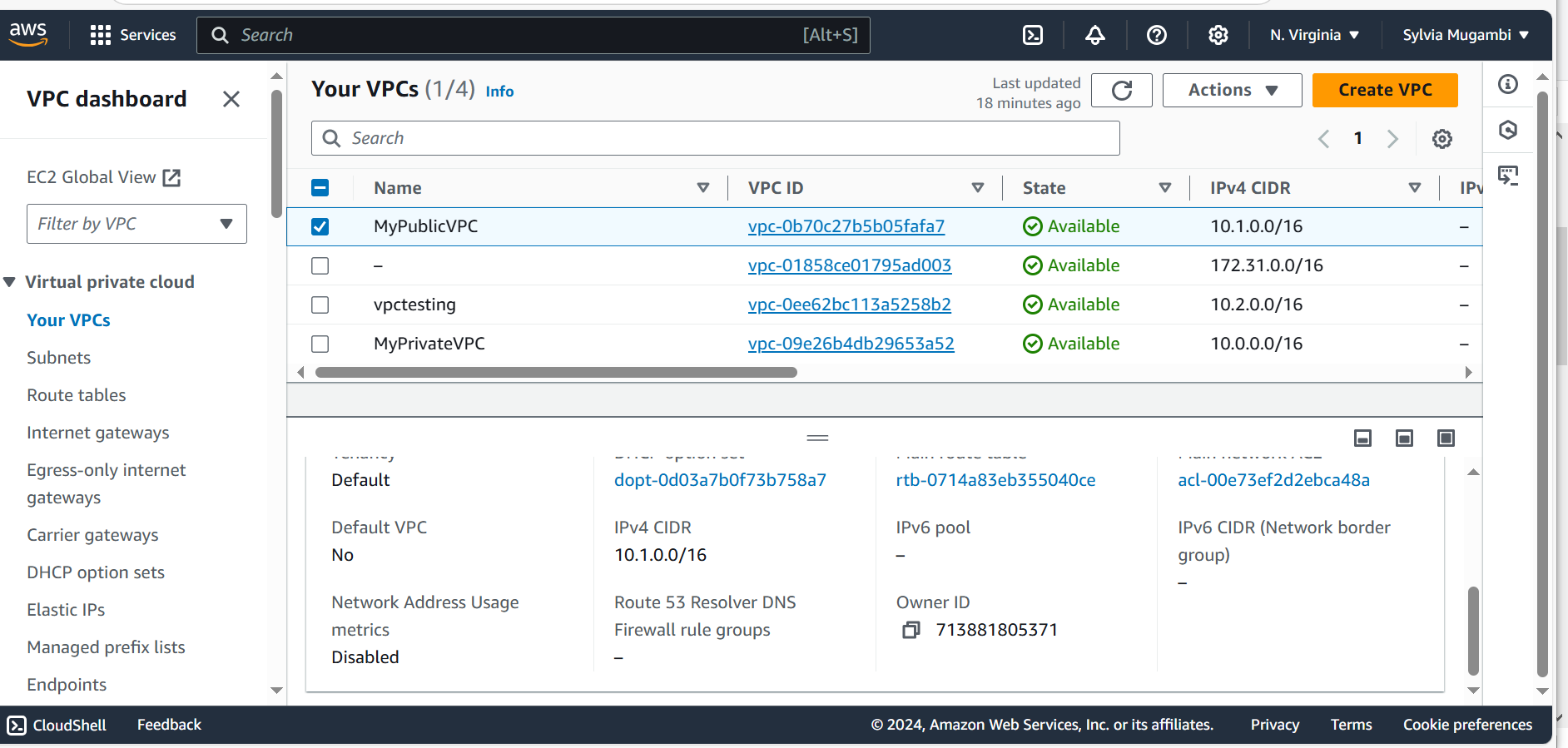
**Location:** Launched in the private subnet

**Access:** It is not directly accessible from the internet but has outbound access

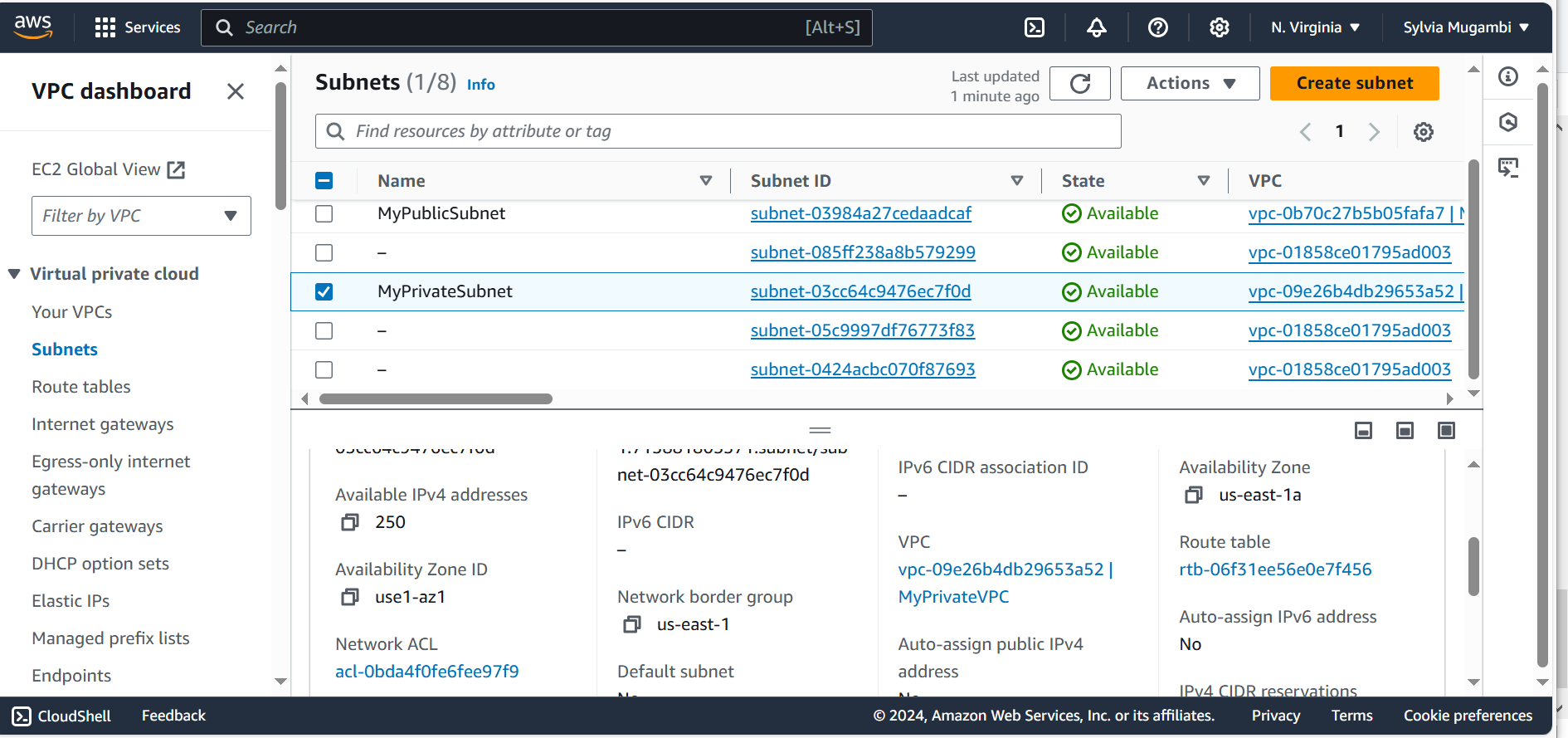
**Purpose:** It handles sensitive operations and stores data securely within the private network

**HERE ARE A FEW SCREENSHOTS SHOWING THE SUCCESSFUL CREATION AND TESTING OF VPC AND EC2 INSTANCES**

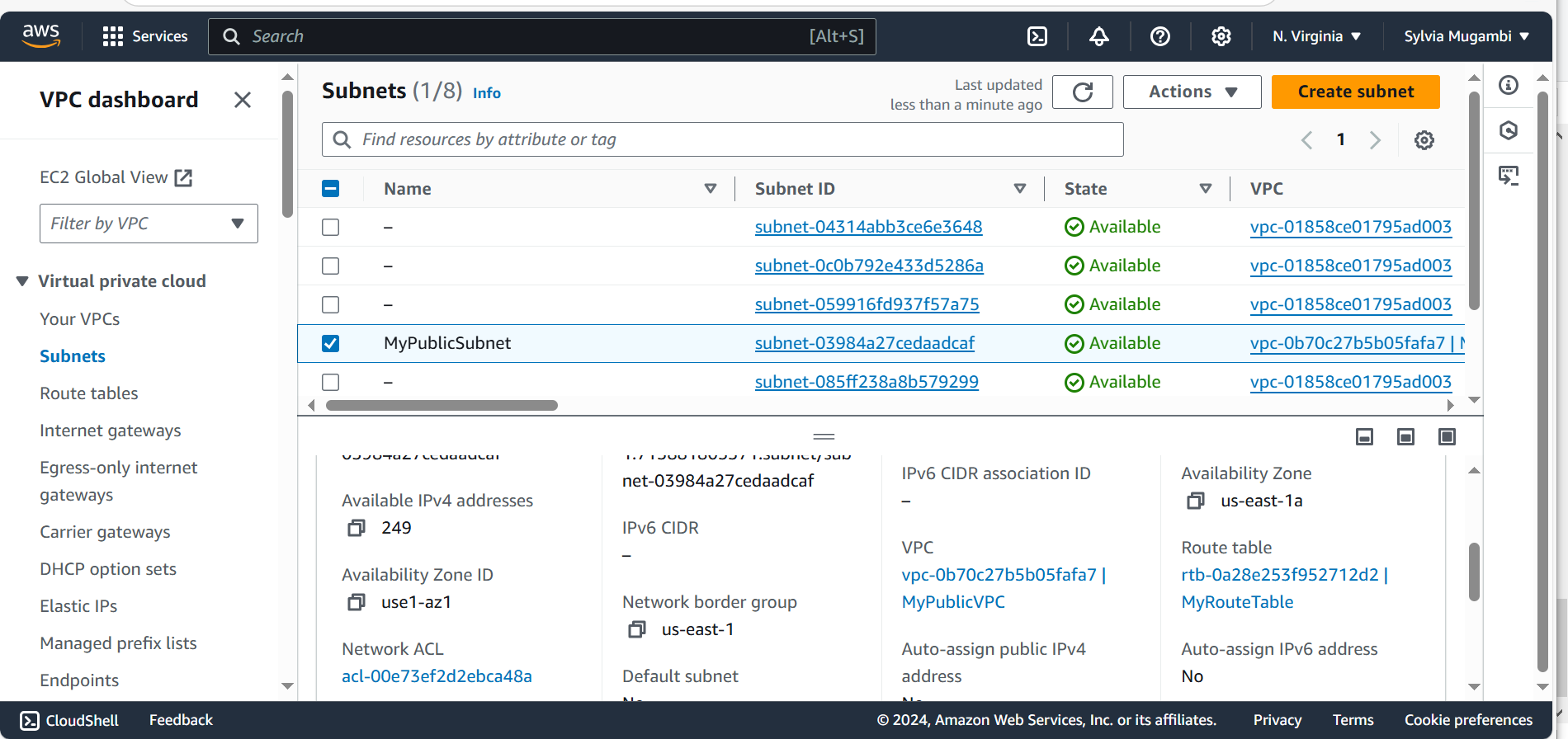
**Below is Public VPC Screenshot**



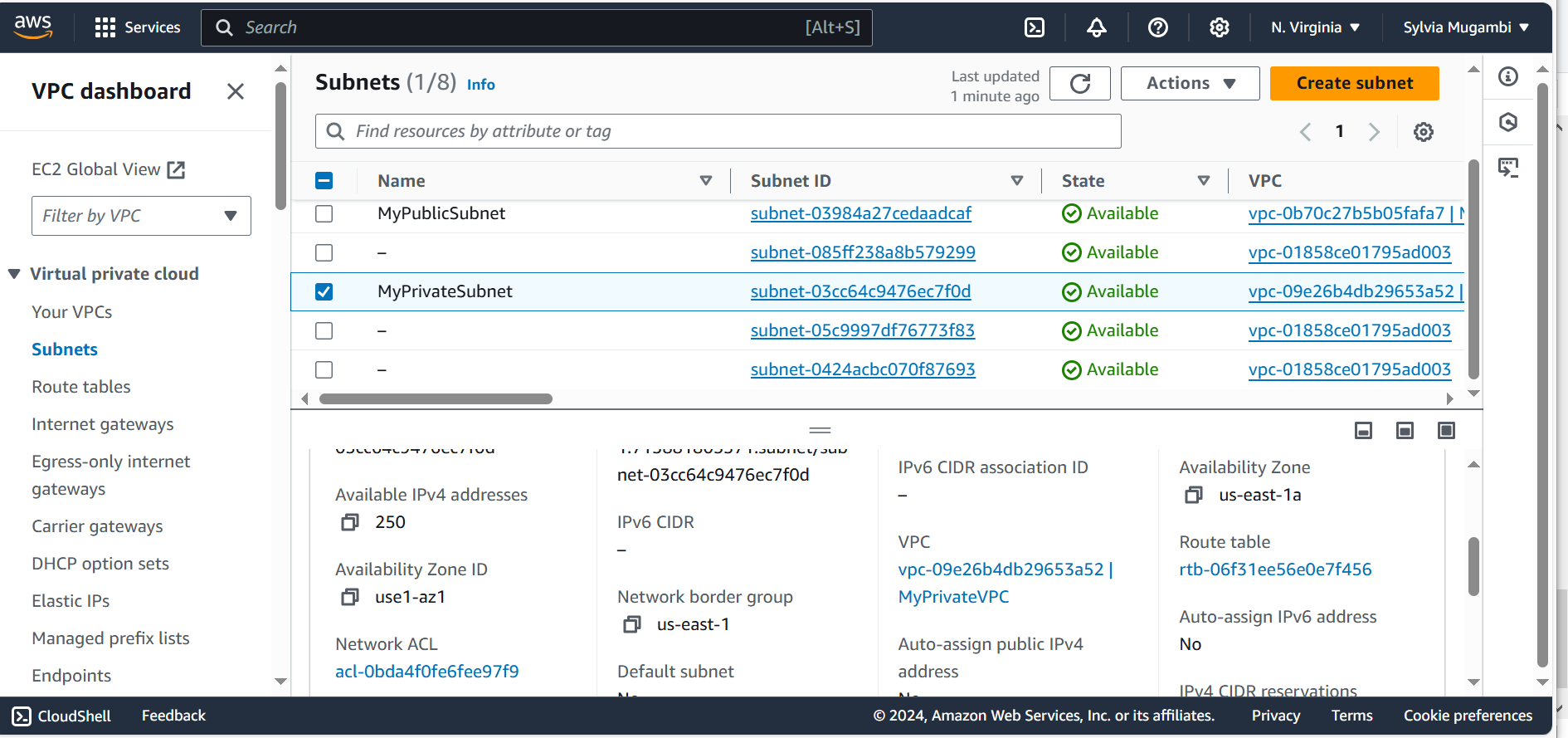
**Below is Private VPC screenshot**

****

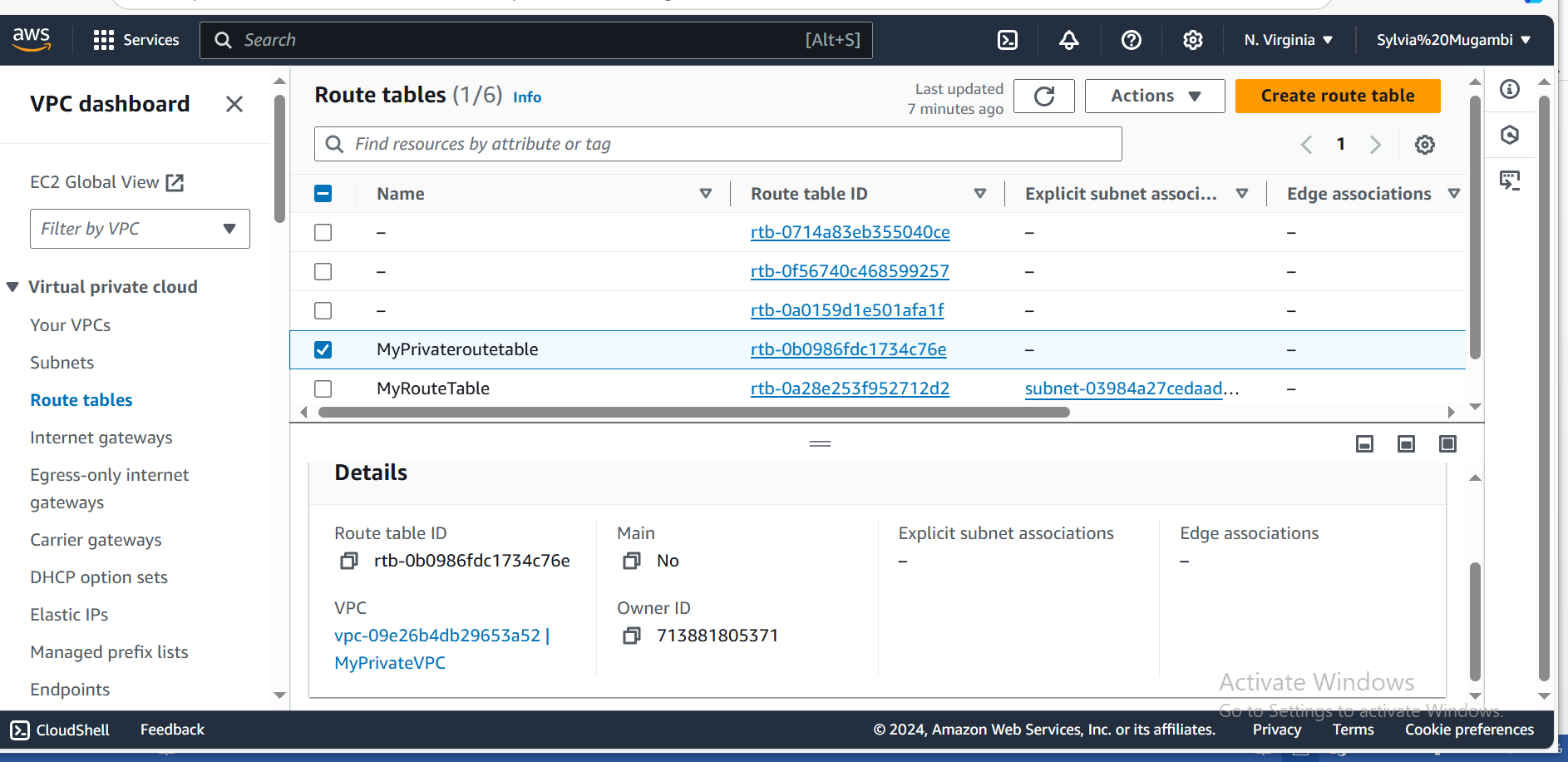
**Below is Public subnet screenshot**

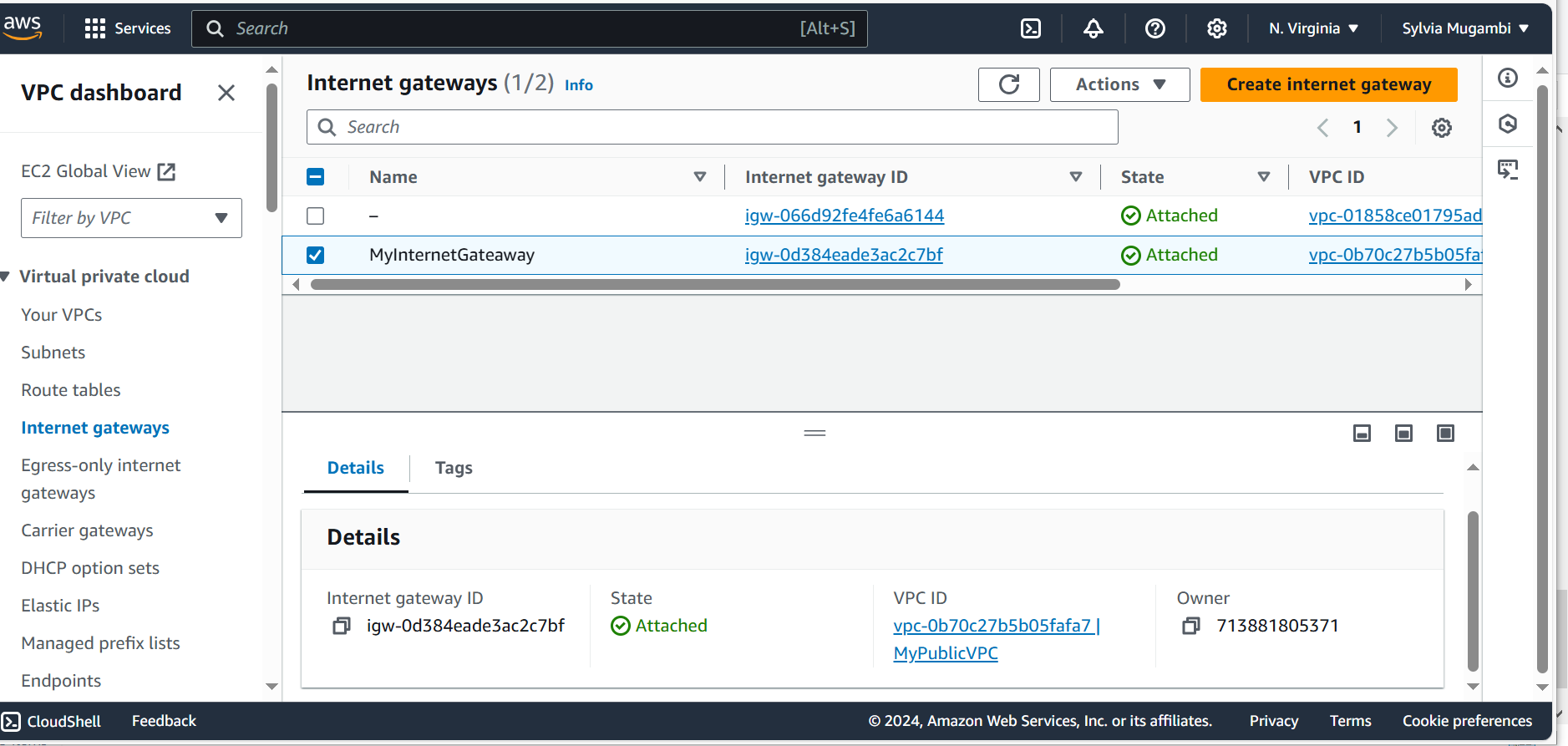
****

**Below is Private subnet screenshot**

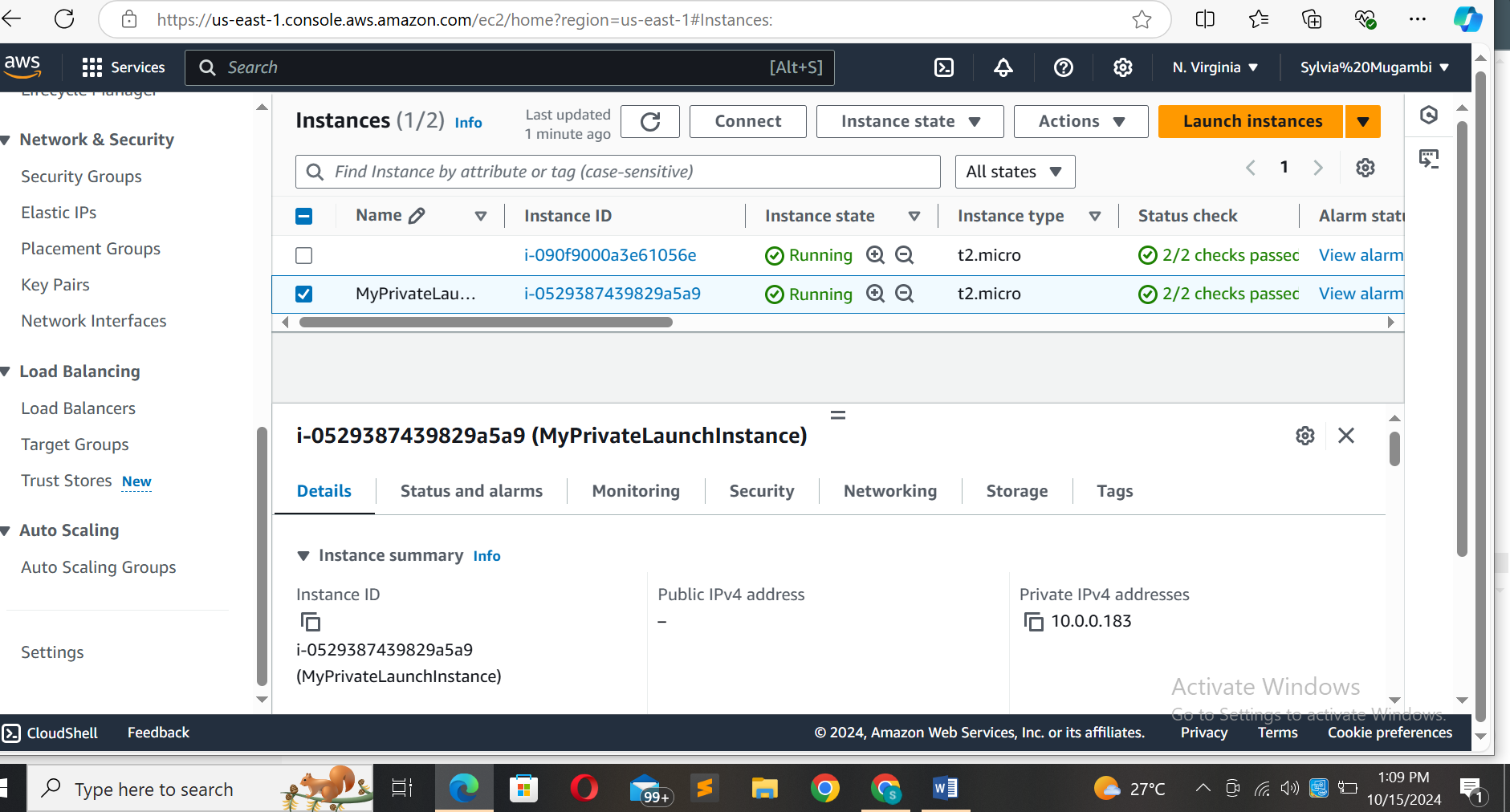
****

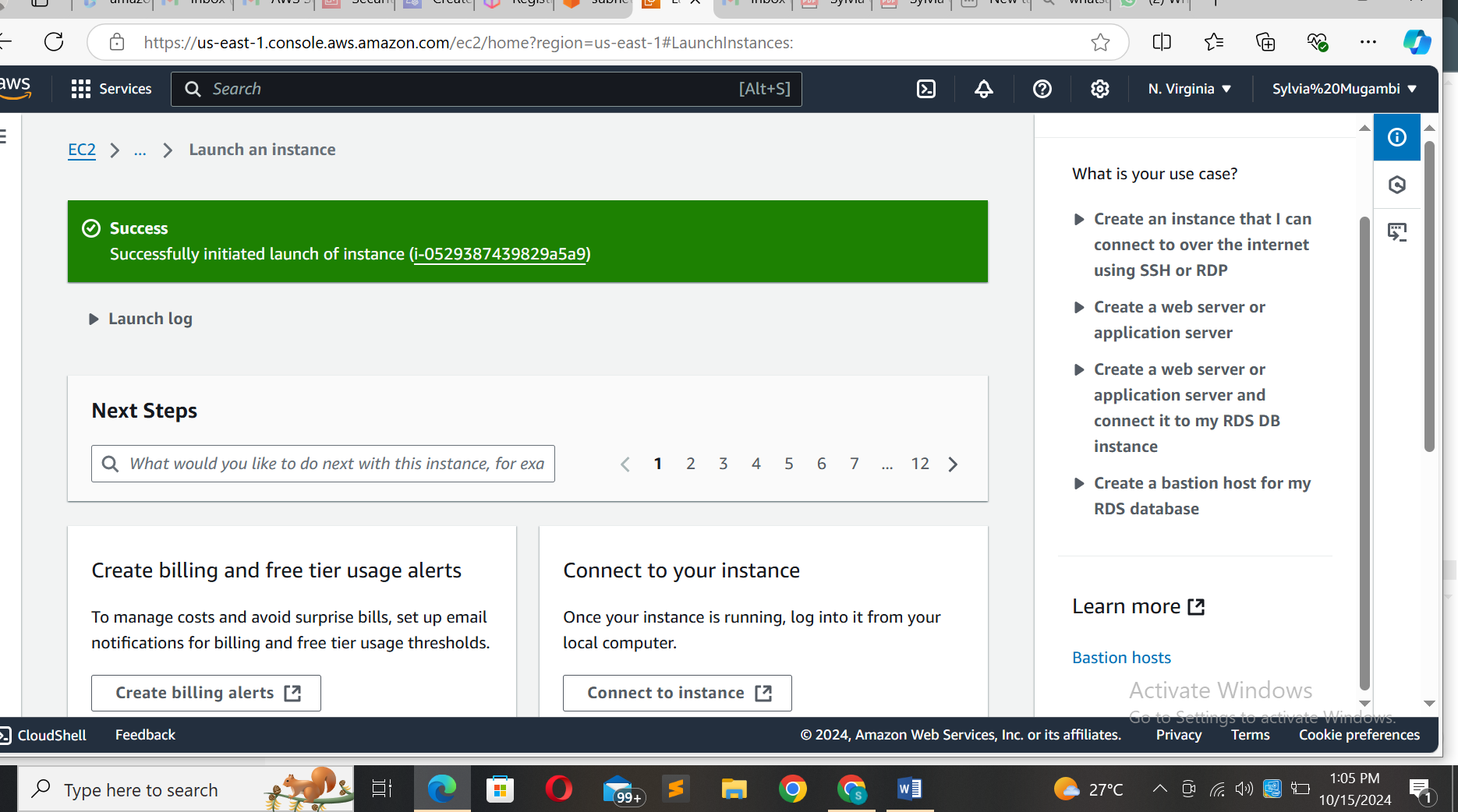
**Below is the Myroutetable configuration screenshot**

****

**Below is myinternet Gateway**

**Below is EC2 instance screenshot**

****

**Below is a screenshot of a successful instance launch on EC2**