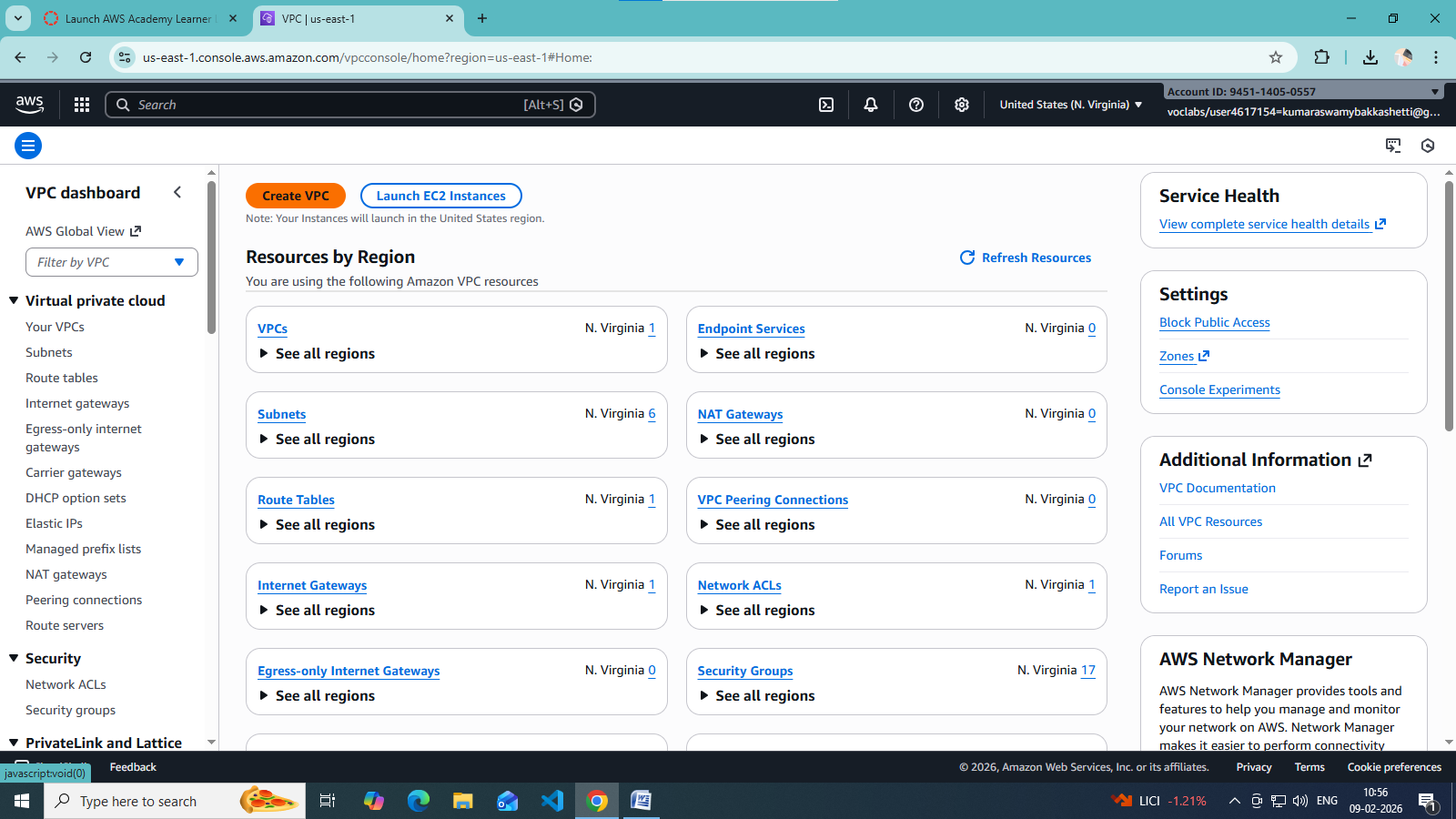
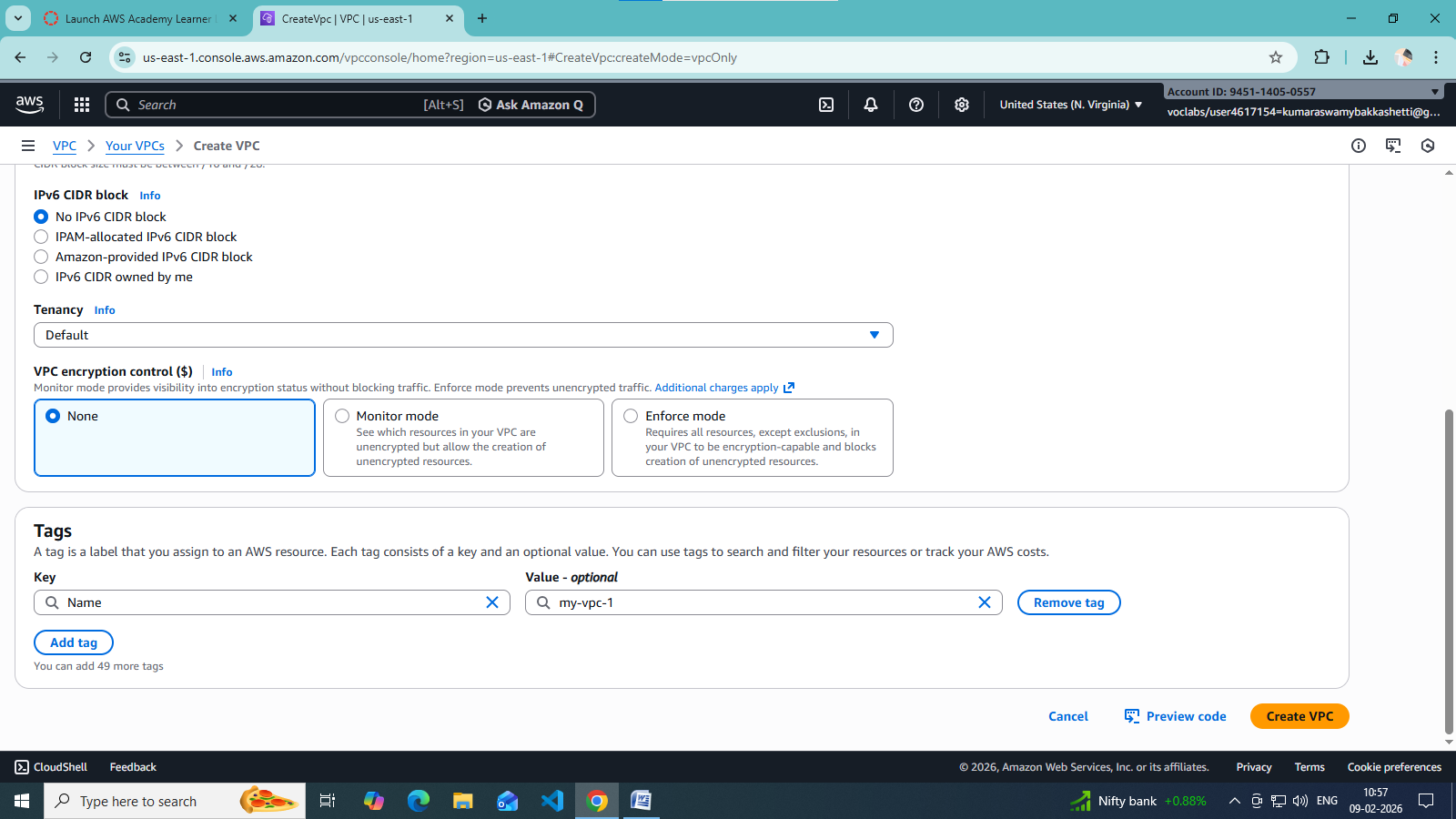
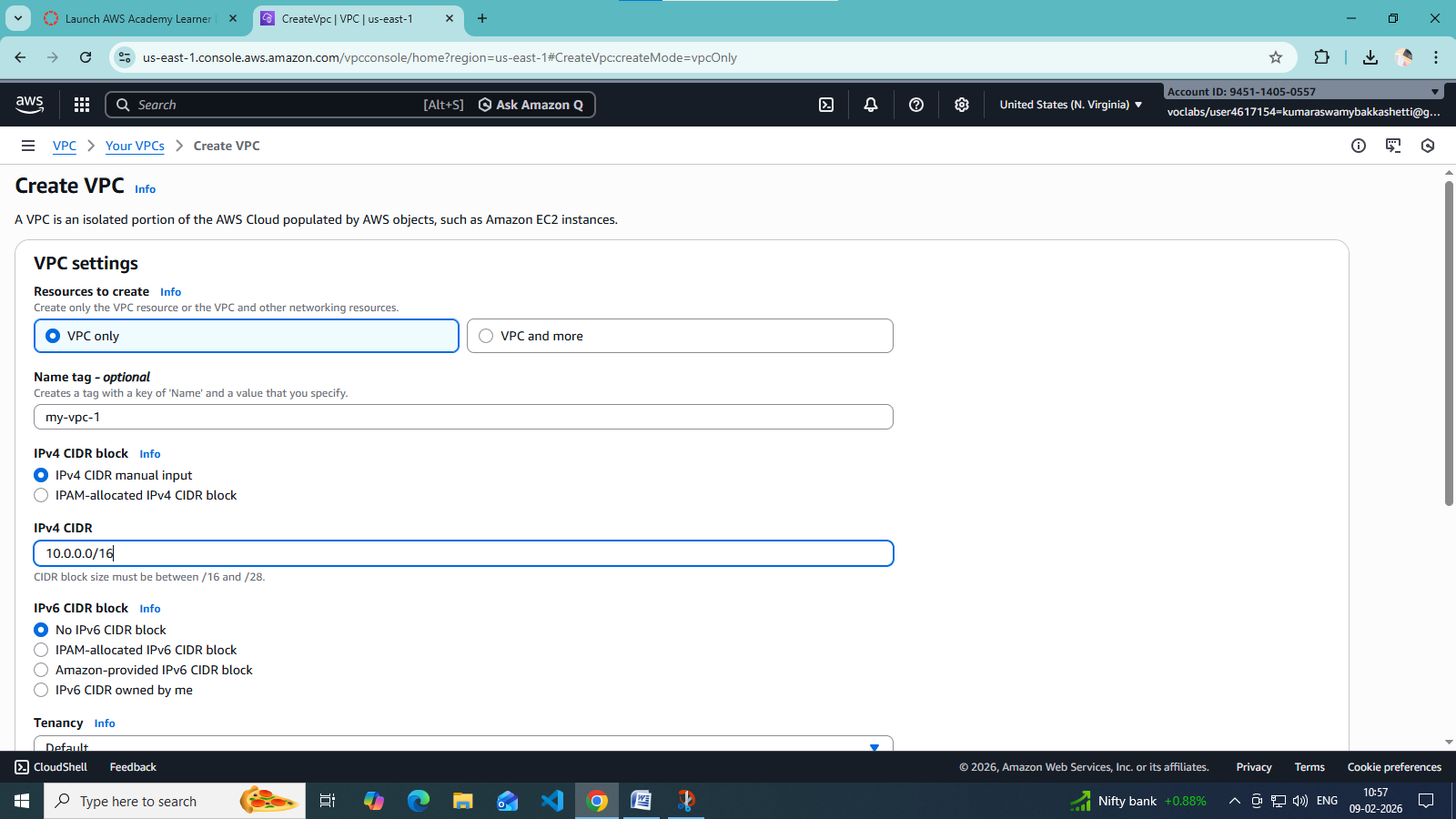
**Week 5: VPC Creation and Ec2 Instance Connection**

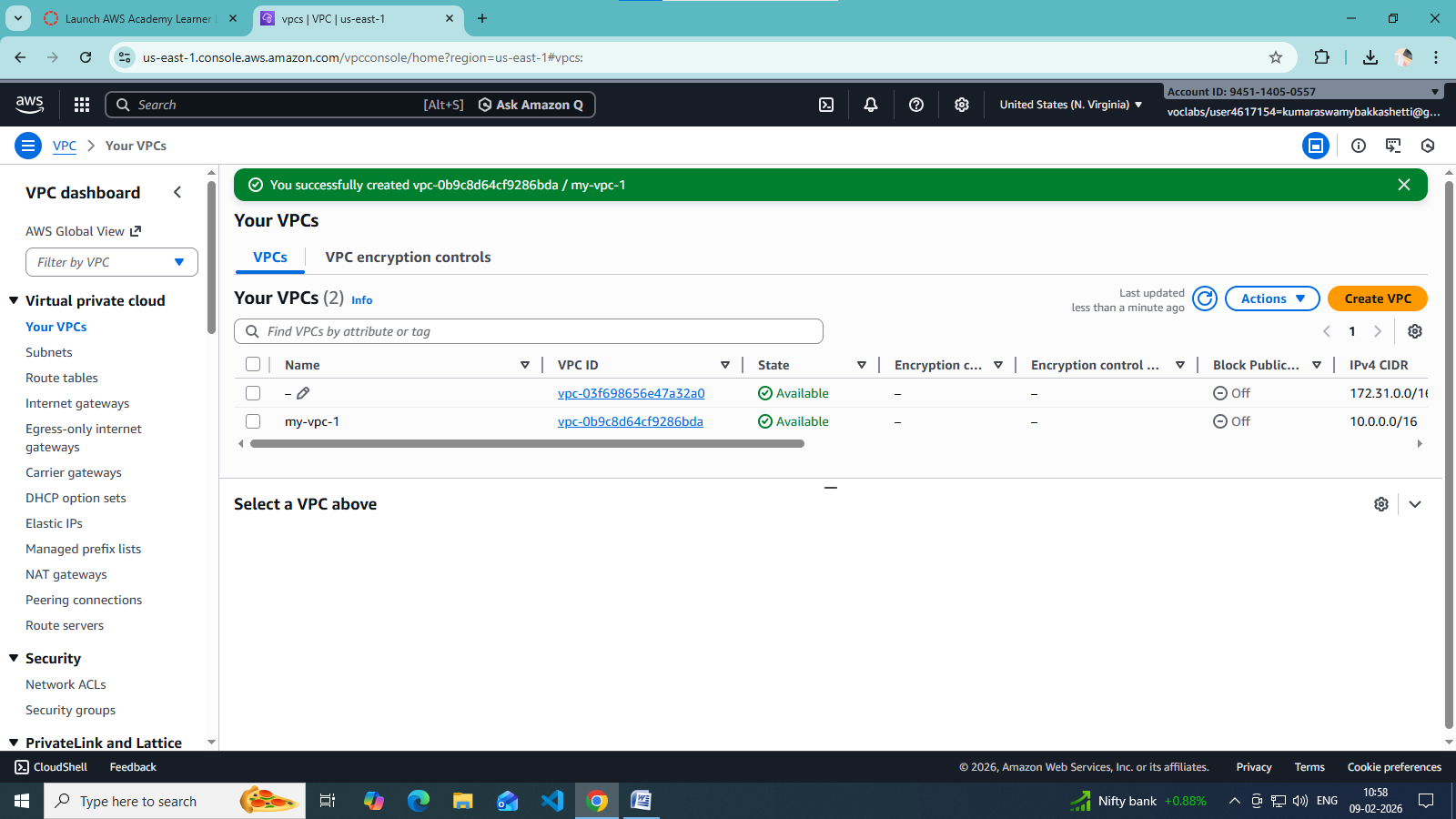
**🔹Step 1: Create the VPC**

1. Go to **AWS Management Console → VPC**
2. Click **Create VPC**
3. Choose **VPC only**
4. Enter:
   * **Name**: Custom-VPC
   * **IPv4 CIDR block**: e.g. 10.0.0.0/16
5. Click **Create VPC**









**🔹 Step 2: Create Subnets (Public & Private)**

Create subnets in same **Availability Zones** for high availability.

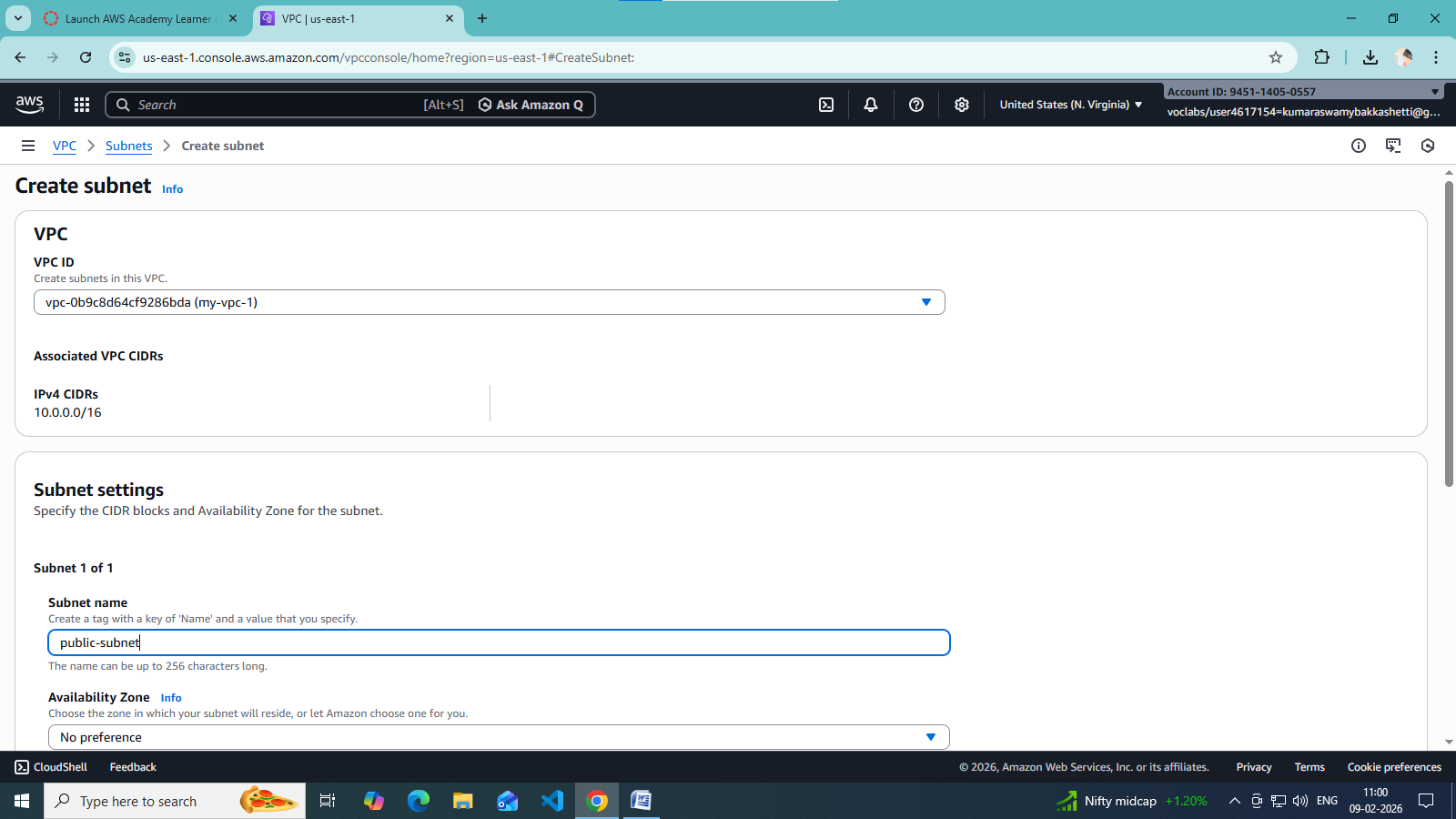
**Example:**

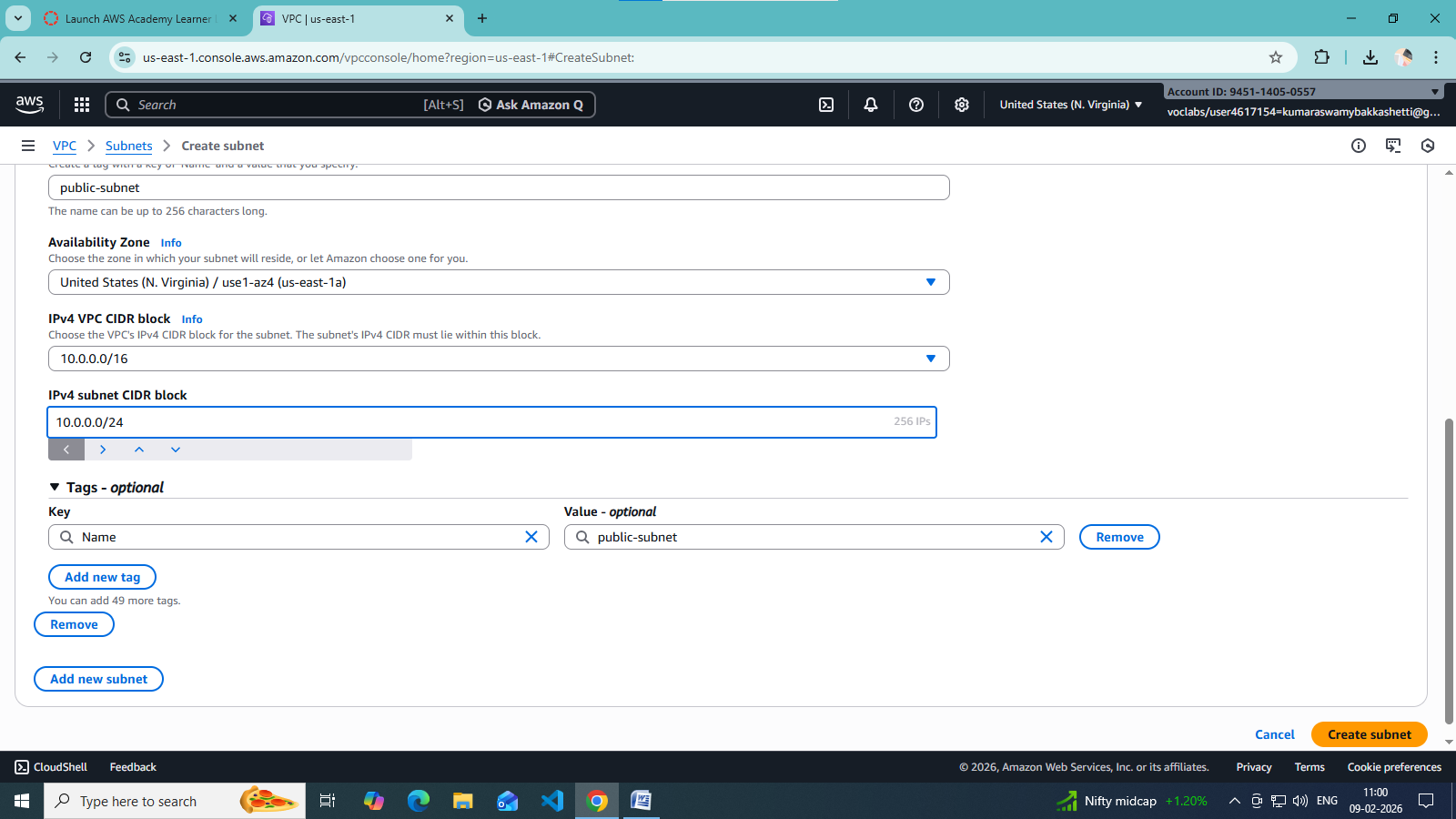
* **Public Subnet**: 10.0.1.0/24 (AZ-A)
* **Private Subnet**: 10.0.2.0/24 (AZ-A)

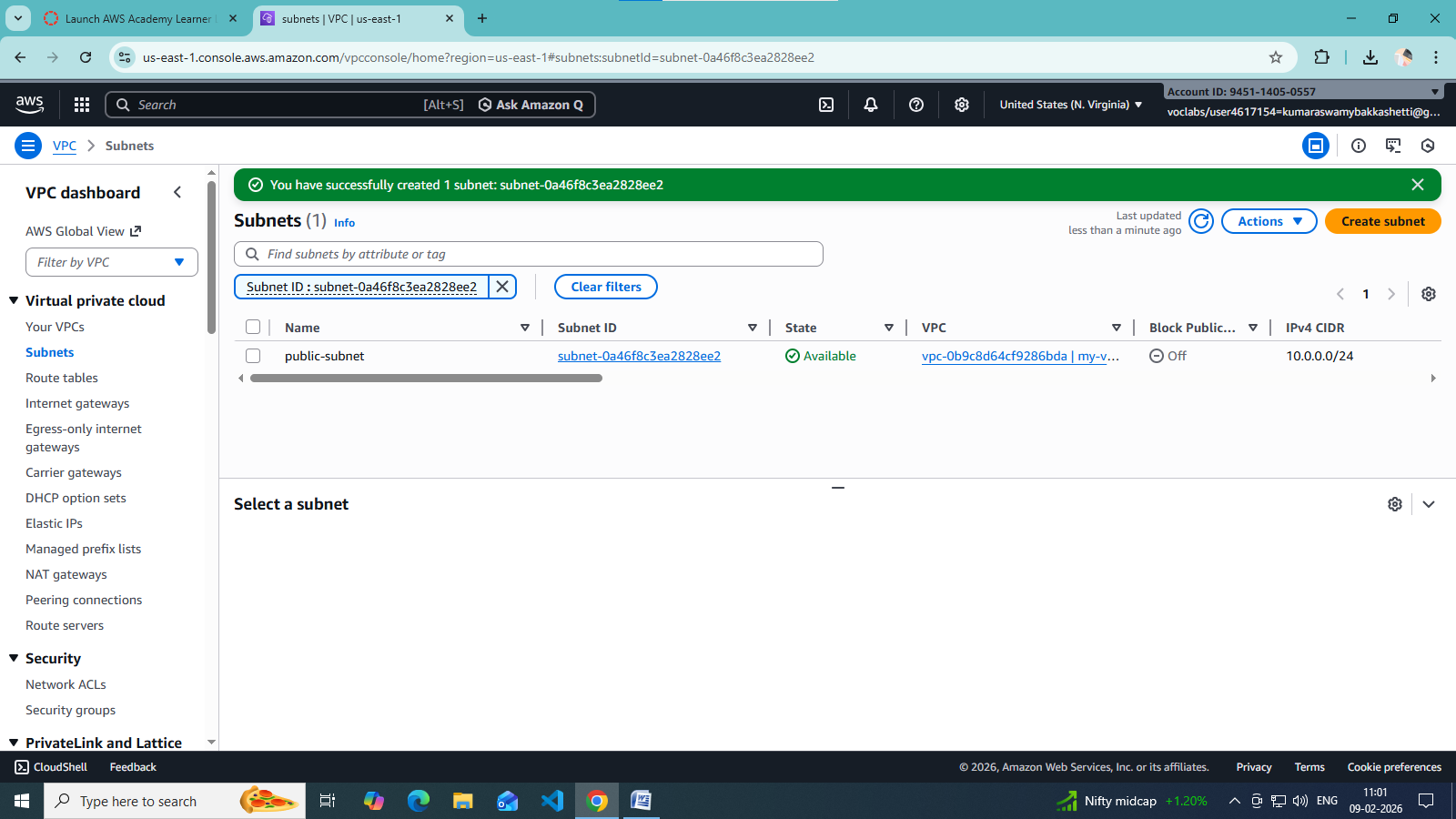
Steps:

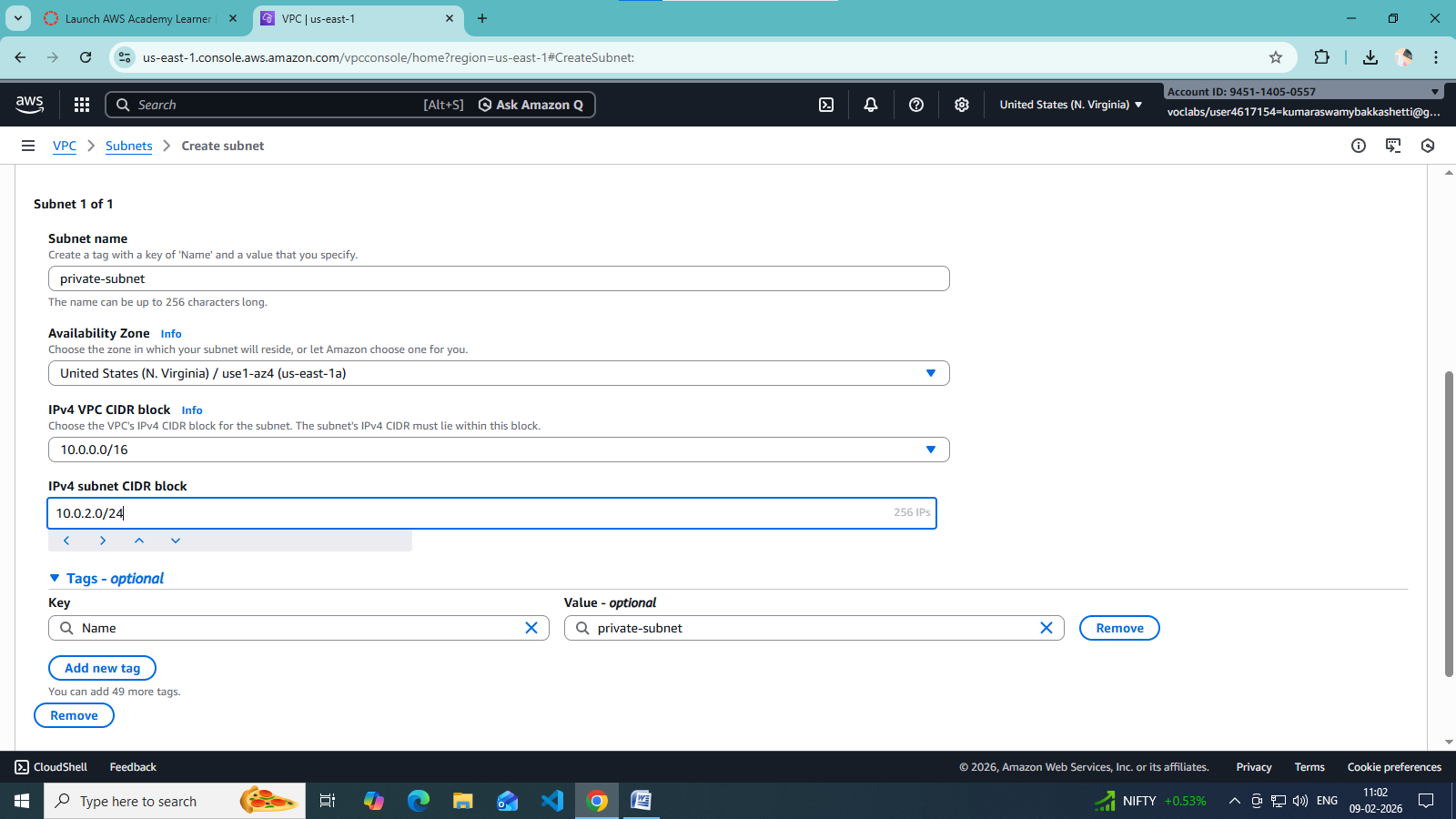
1. Go to **Subnets → Create subnet**
2. Select your VPC
3. Choose AZ
4. Enter CIDR
5. Create subnet

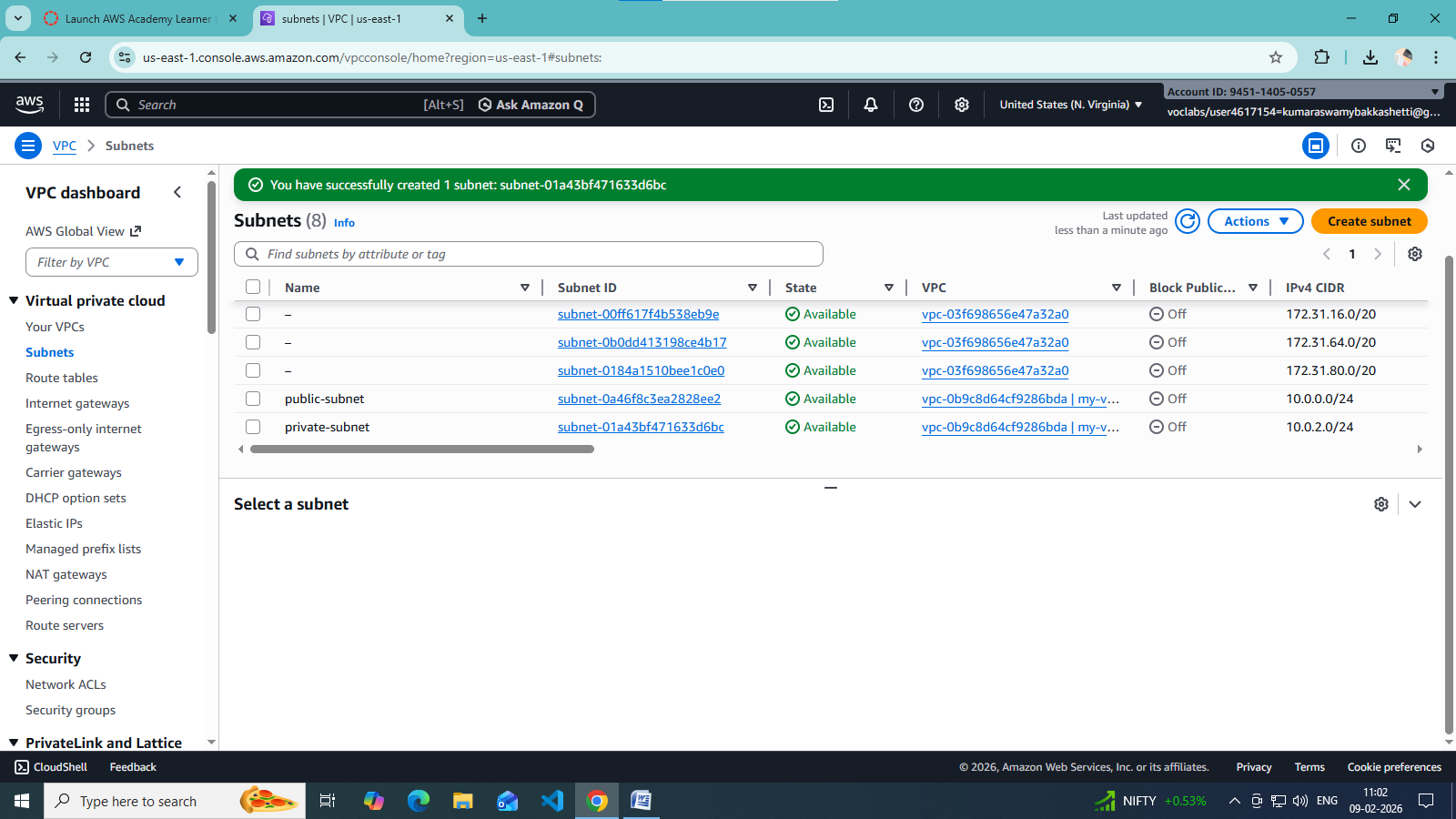






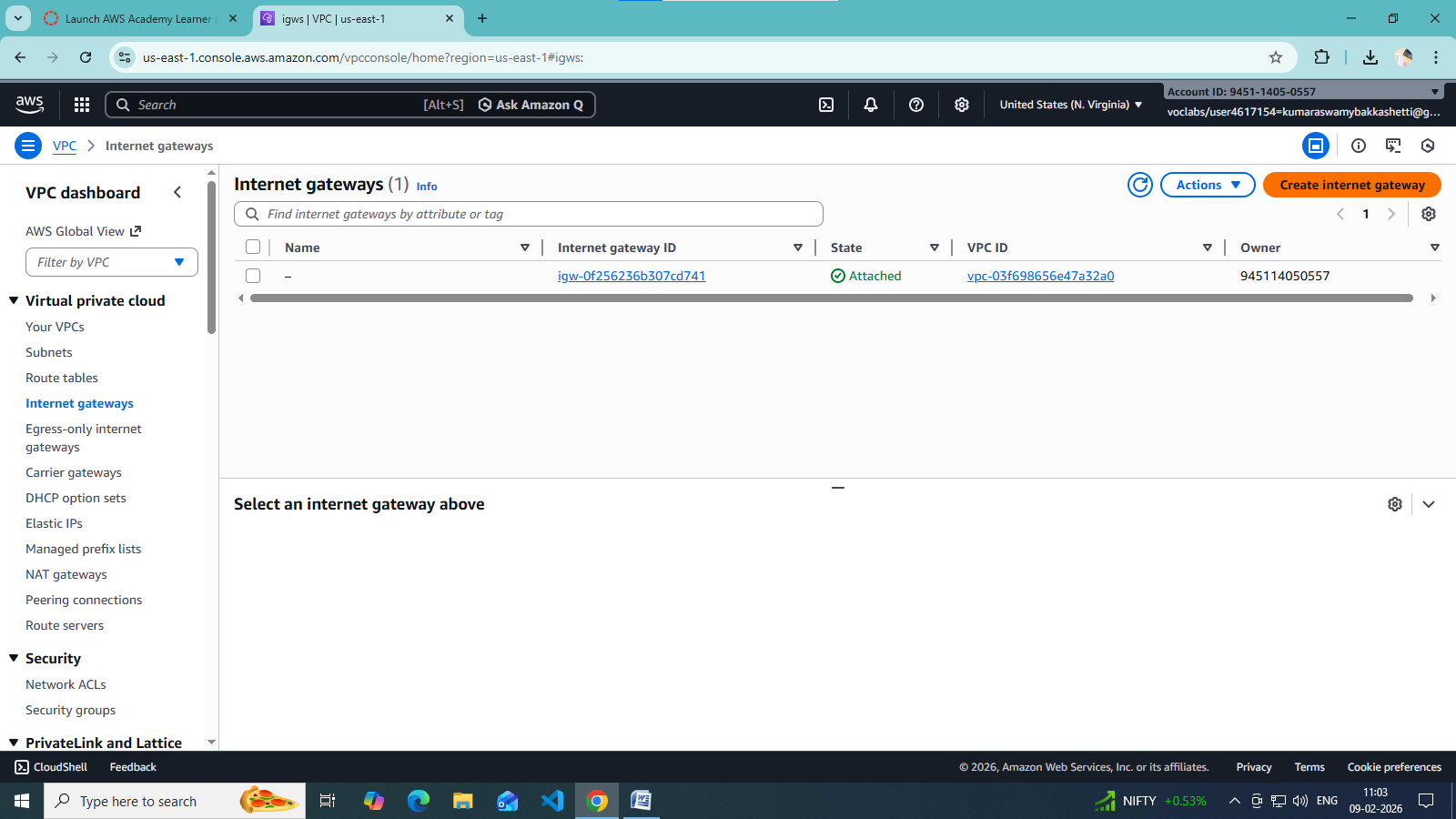


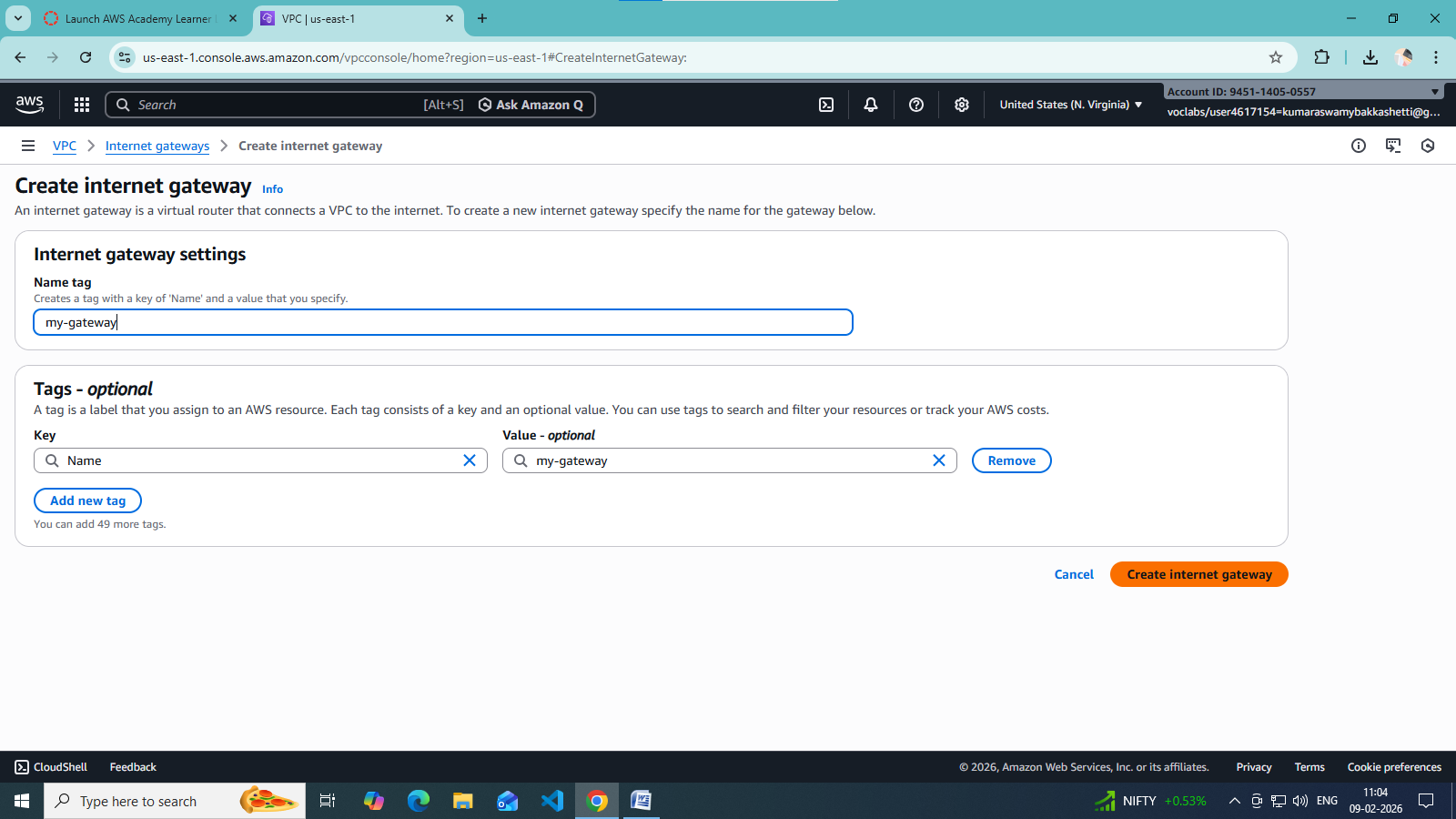


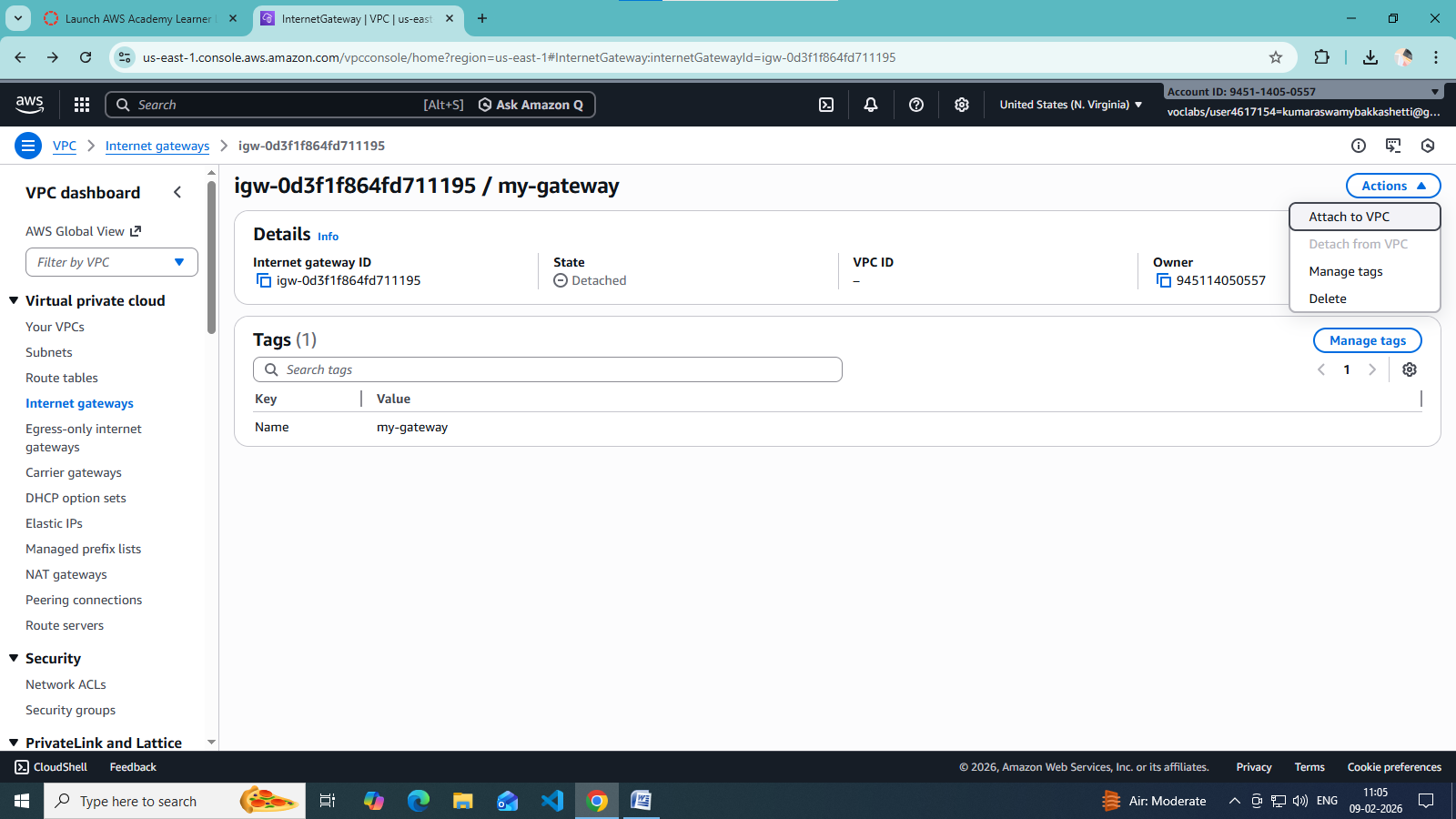


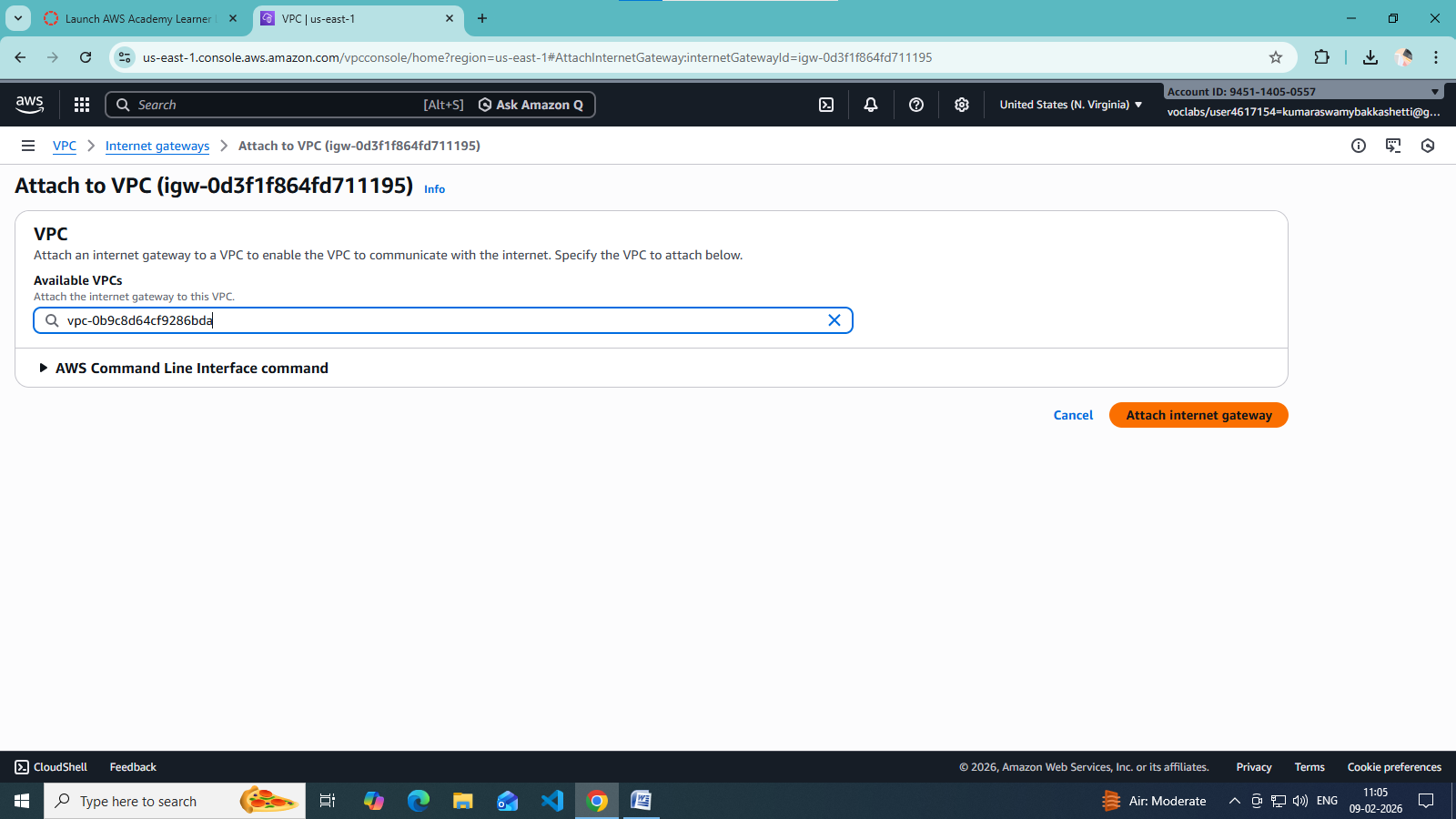
**🔹 Step 3: Create an Internet Gateway (IGW)**

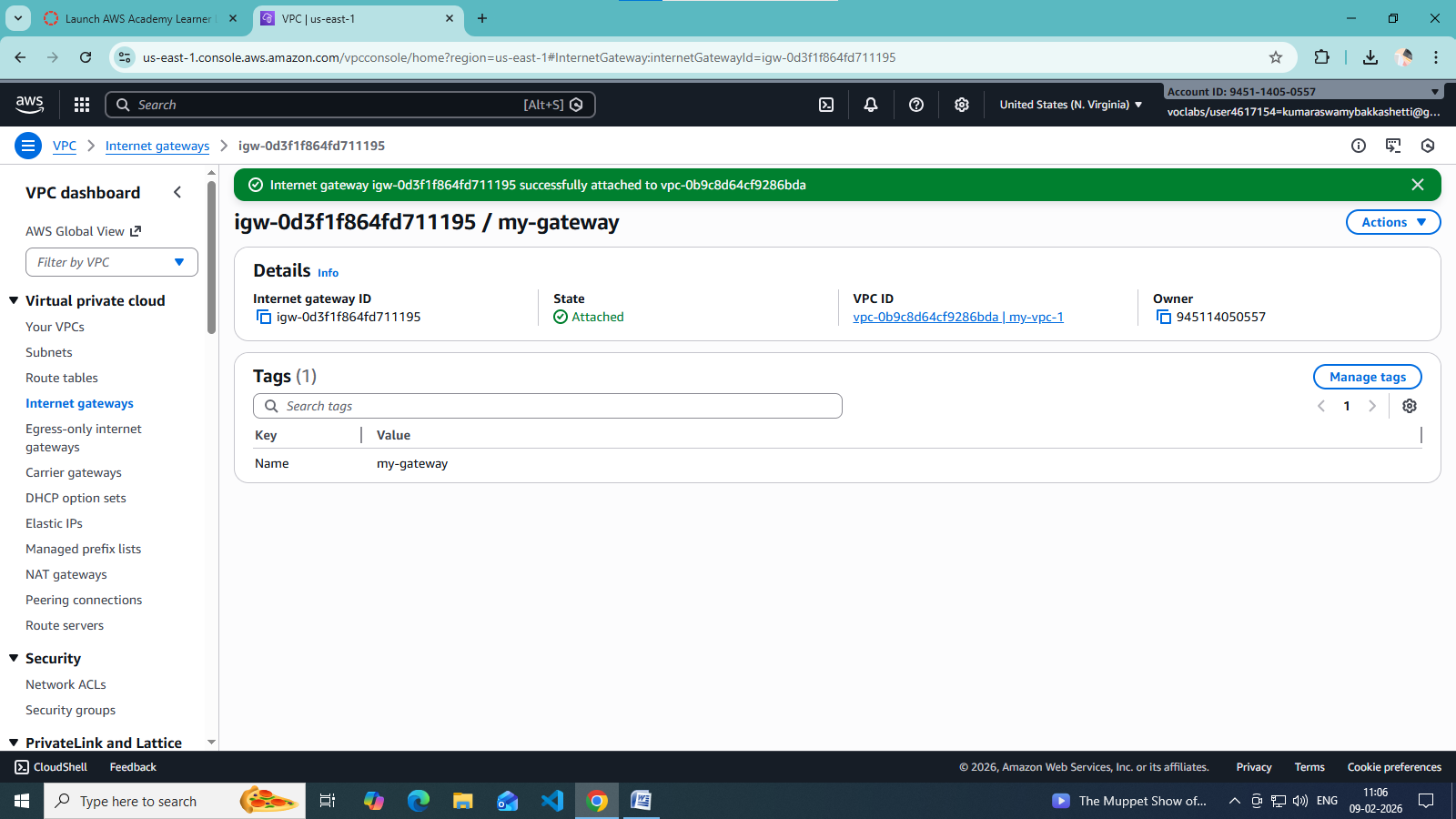
1. Go to **Internet Gateways**
2. Click **Create internet gateway**
3. Name it Custom-IGW
4. **Attach** it to your VPC











**🔹 Step 4: Create Route Tables**

You need **separate route tables** for public and private subnets.

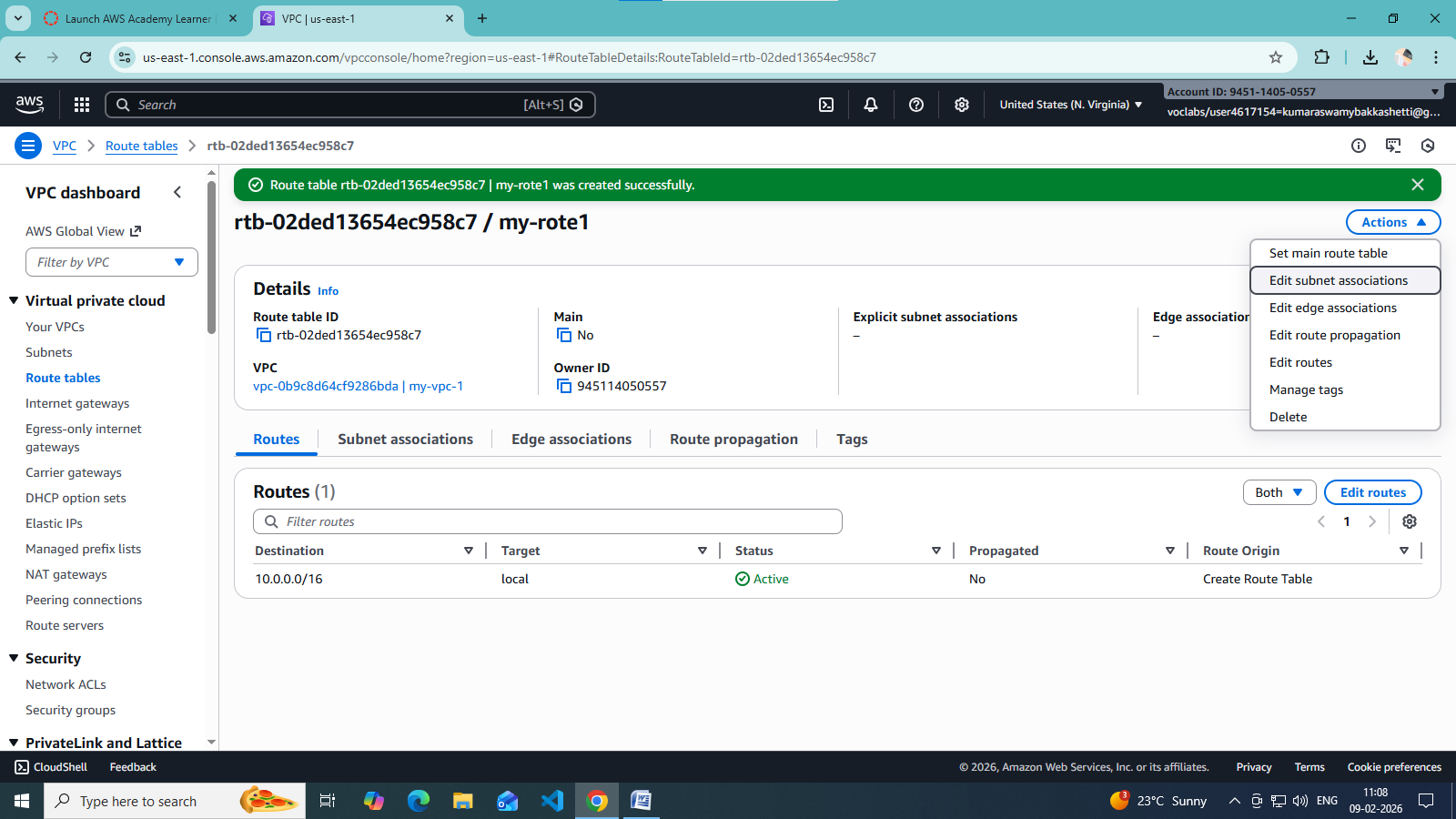
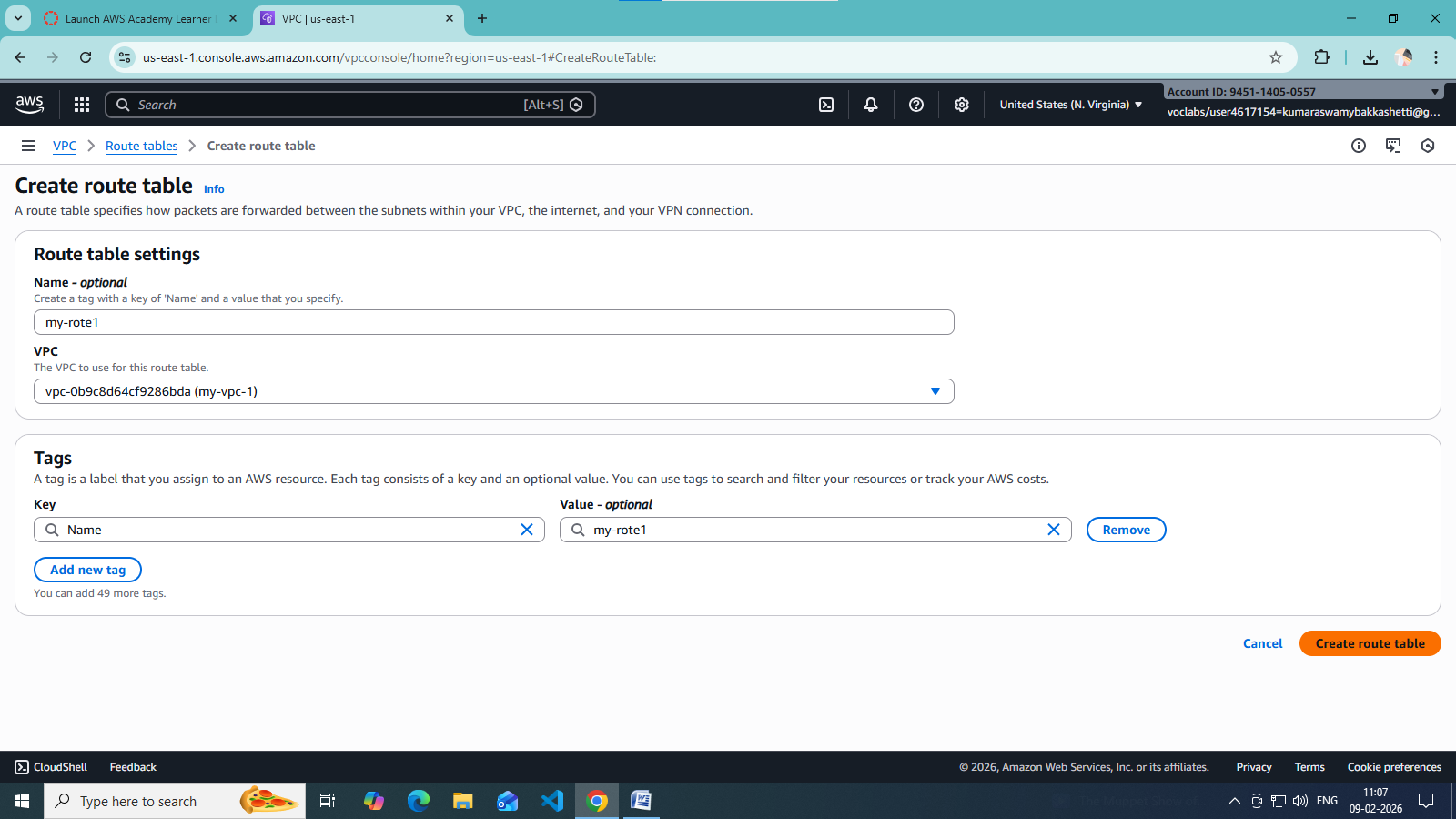
**Public Route Table**

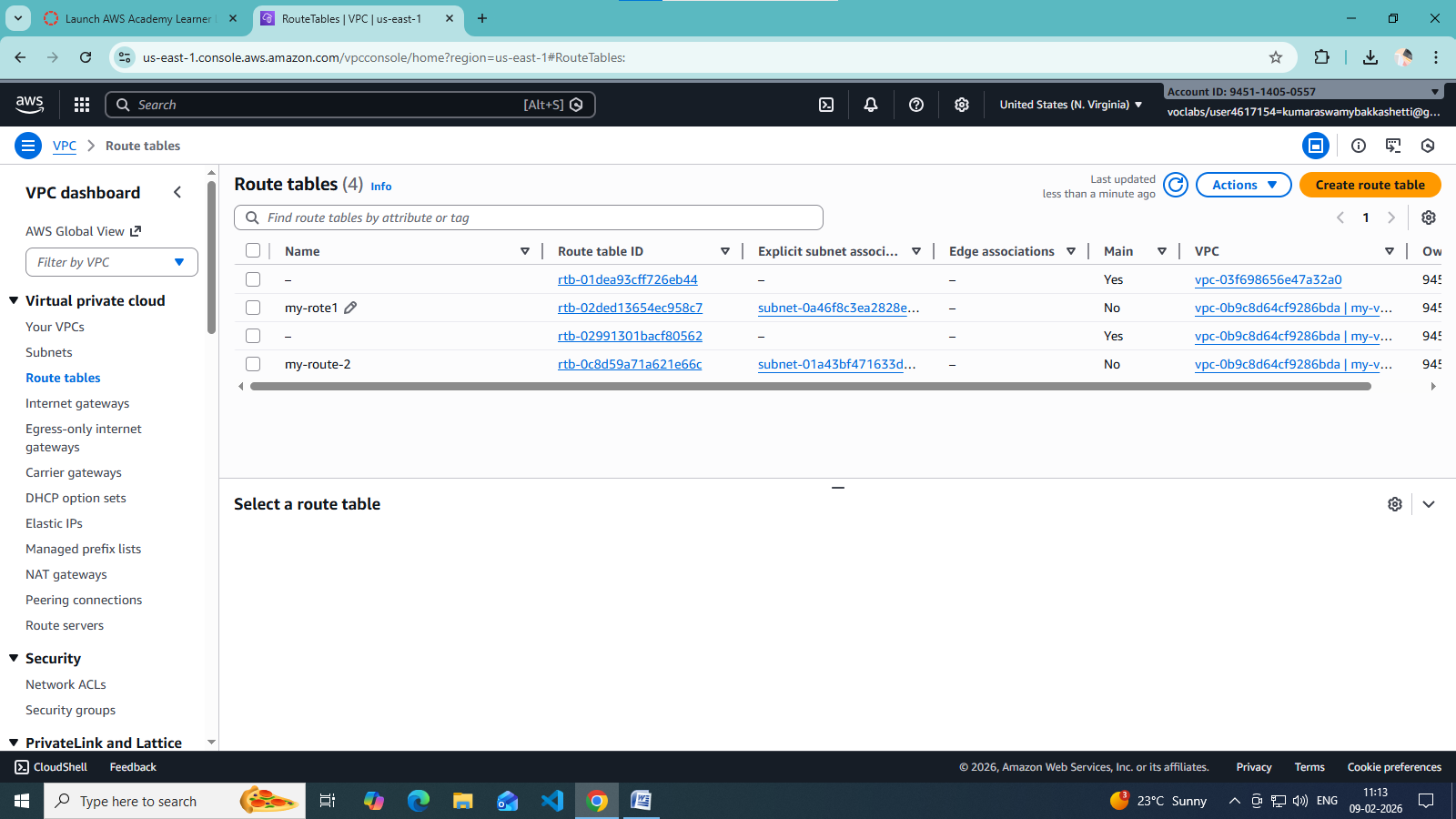
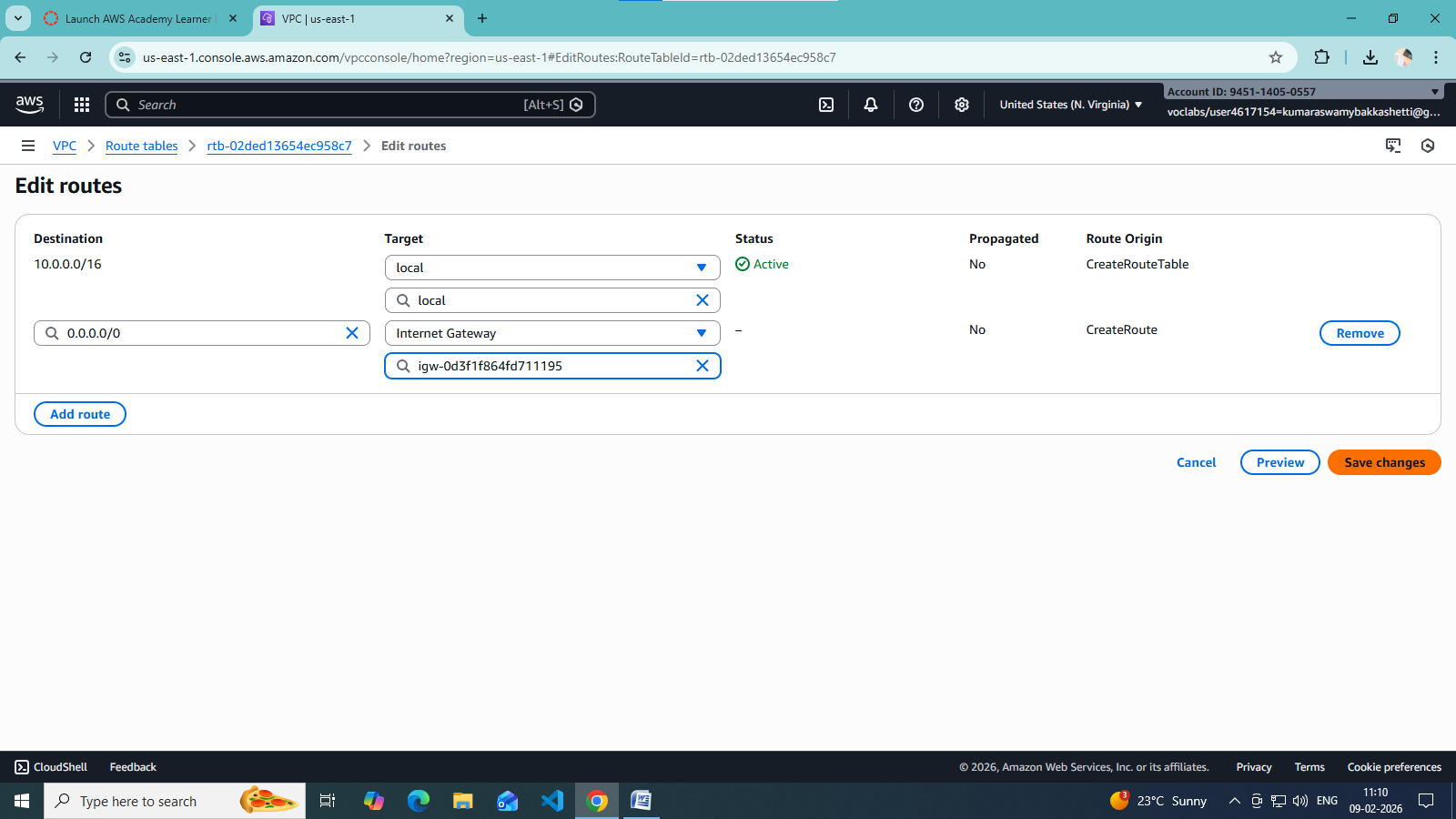
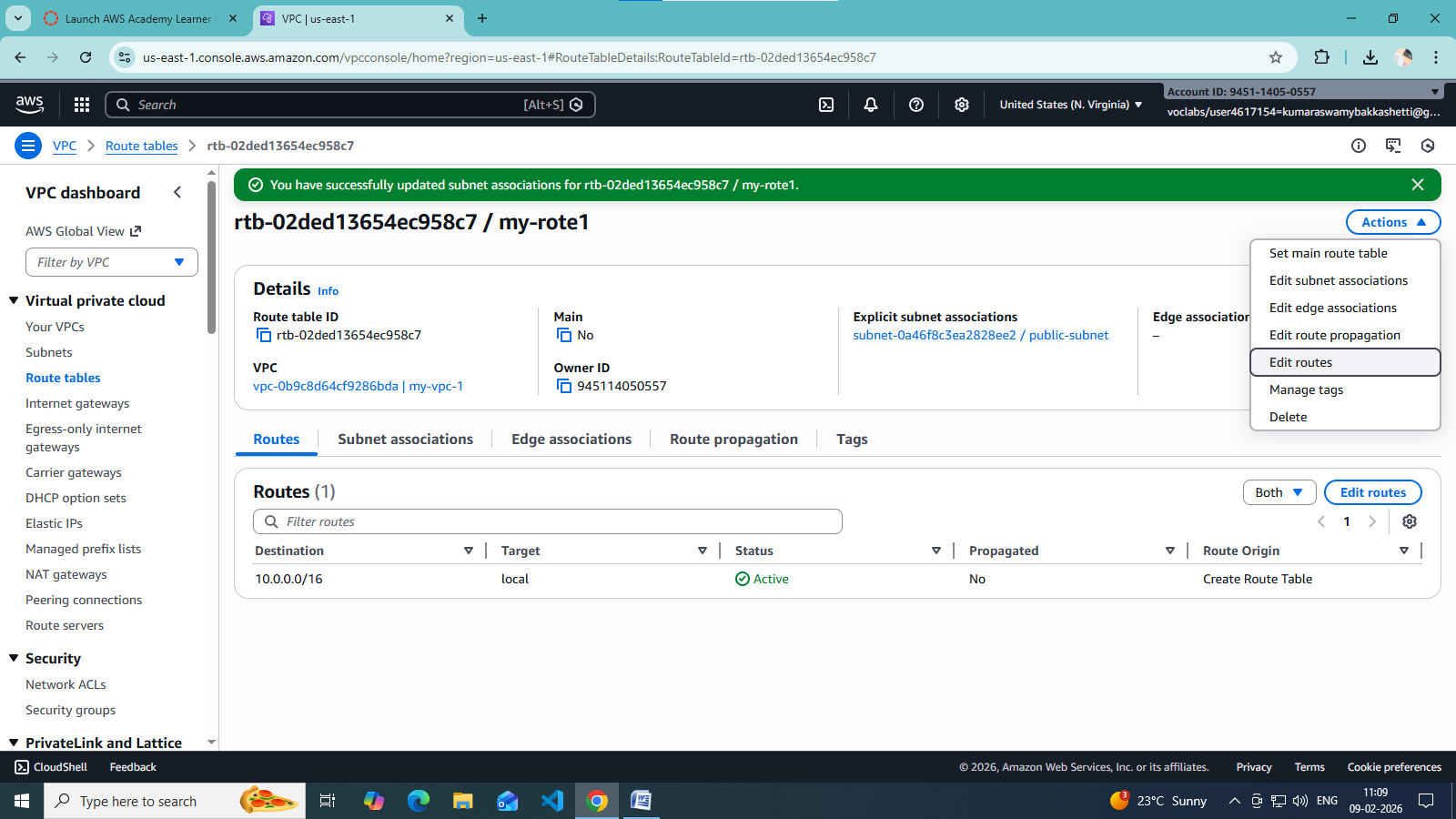
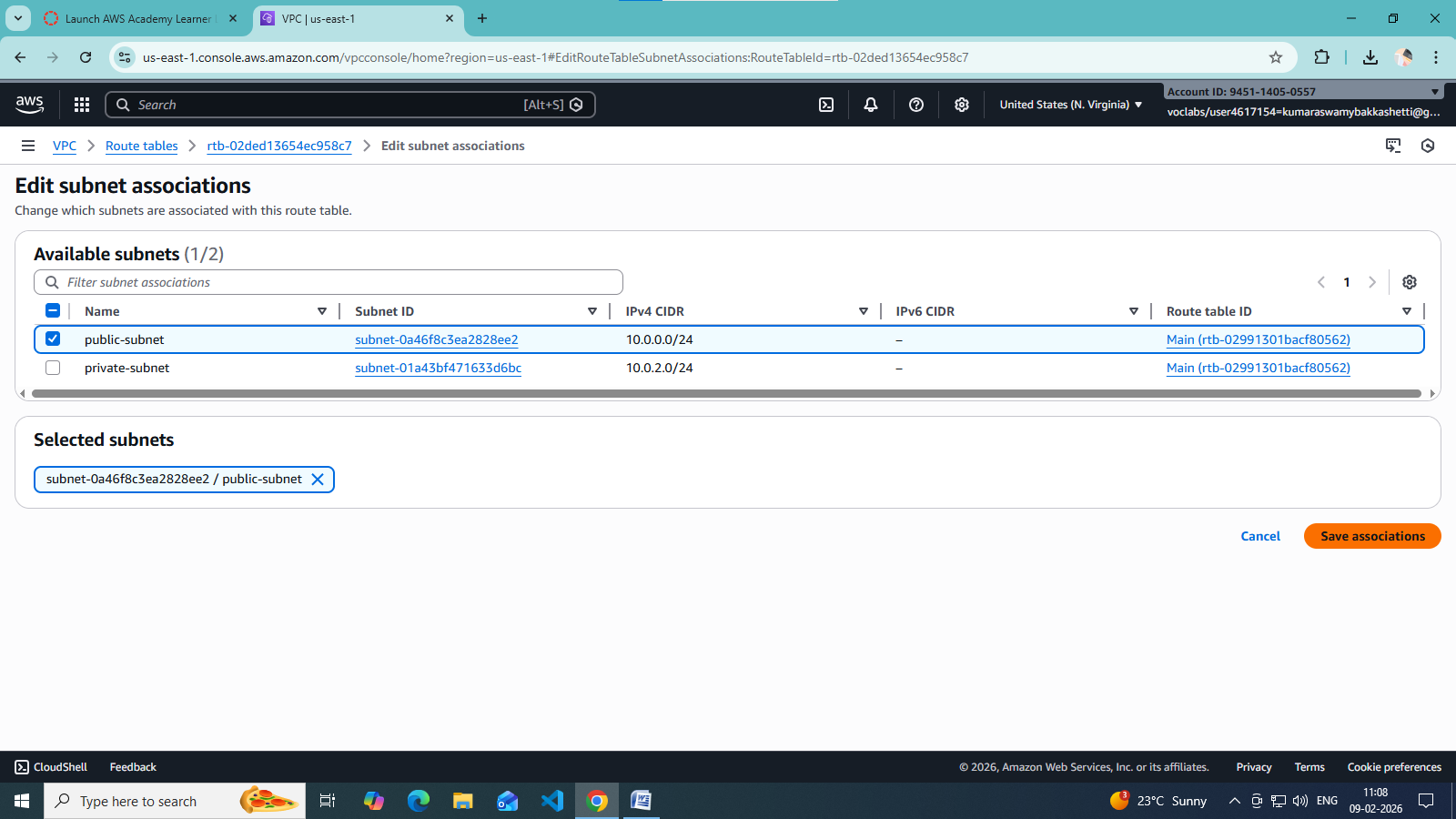
1. Go to **Route Tables → Create route table**
2. Select VPC
3. Add route:
   * Destination: 0.0.0.0/0
   * Target: **Internet Gateway**
4. Associate with **public subnet**

**Private Route Table**

* Keep default local route only (no IGW)
* Associate with **private subnet**

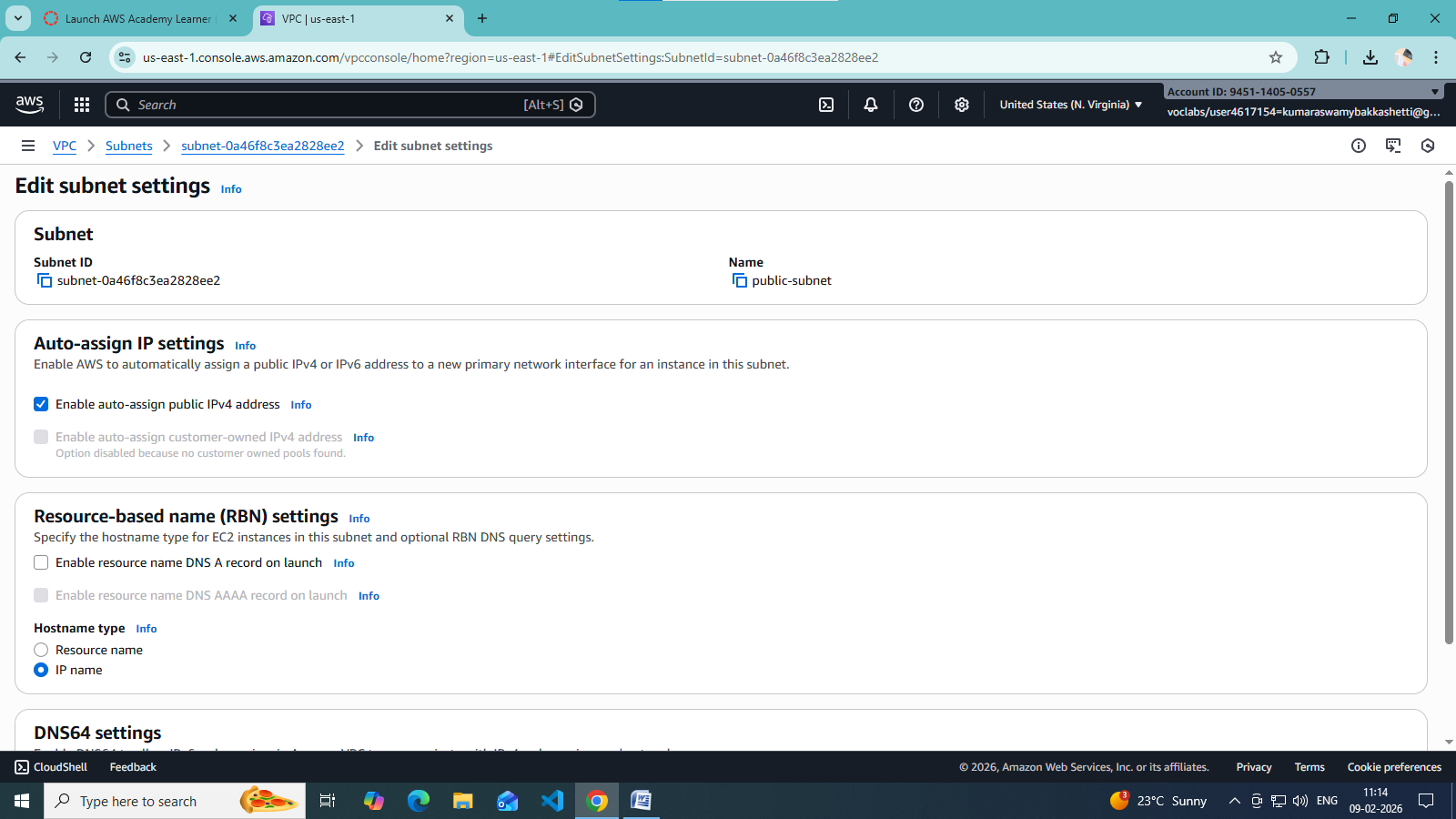
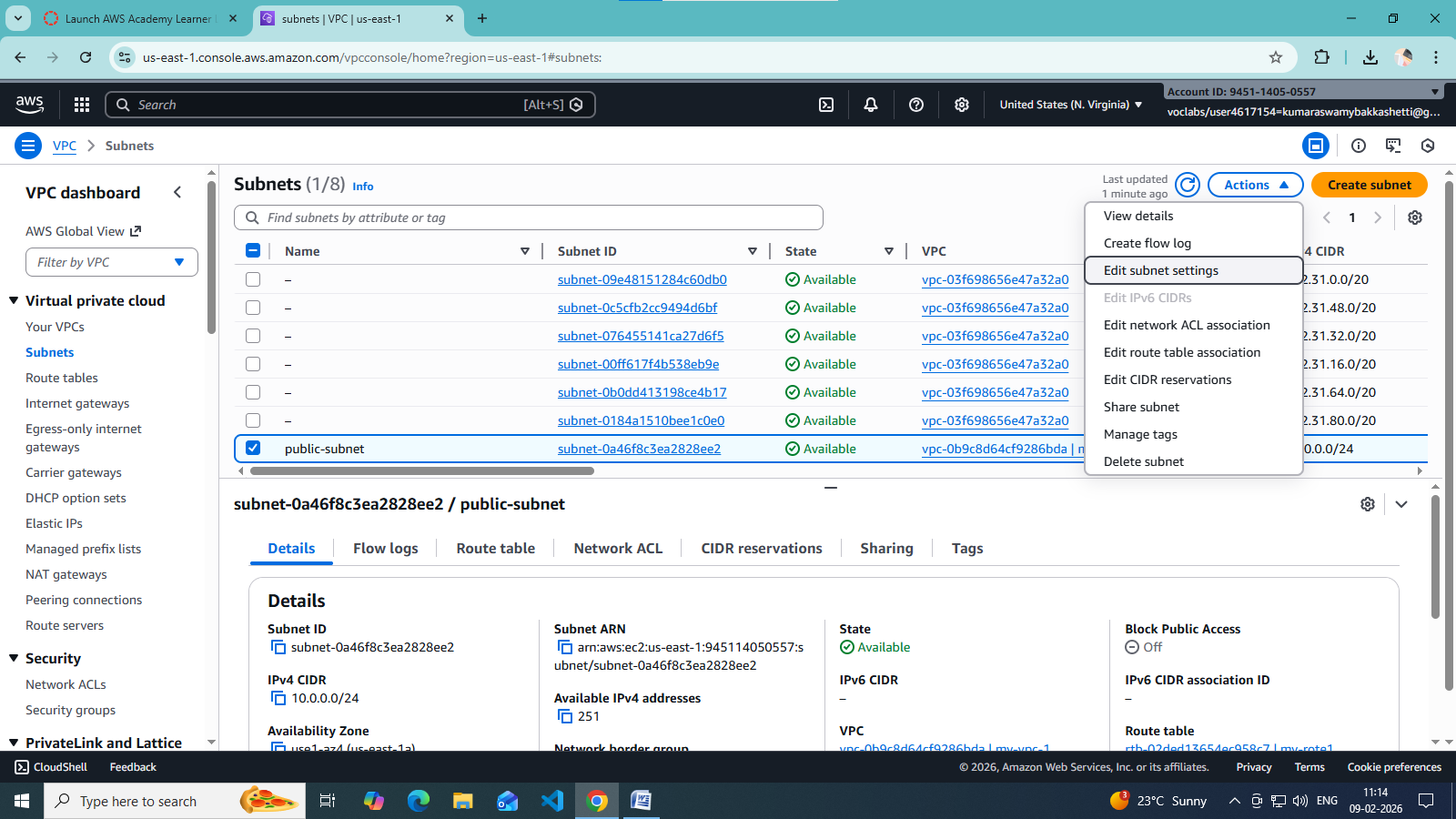






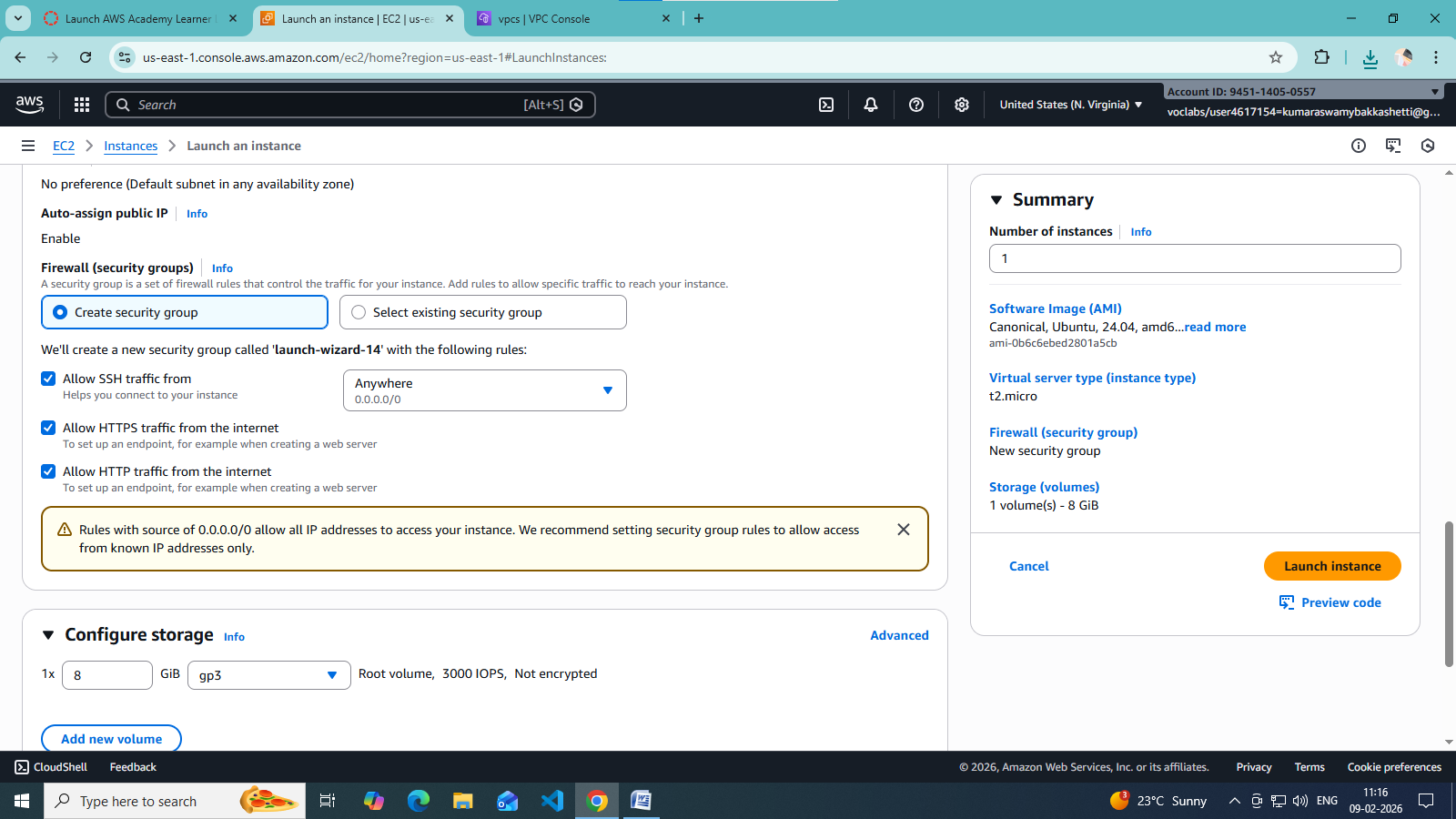
**🔹 Step 5: Enable Auto-Assign Public IP (Public Subnet)**

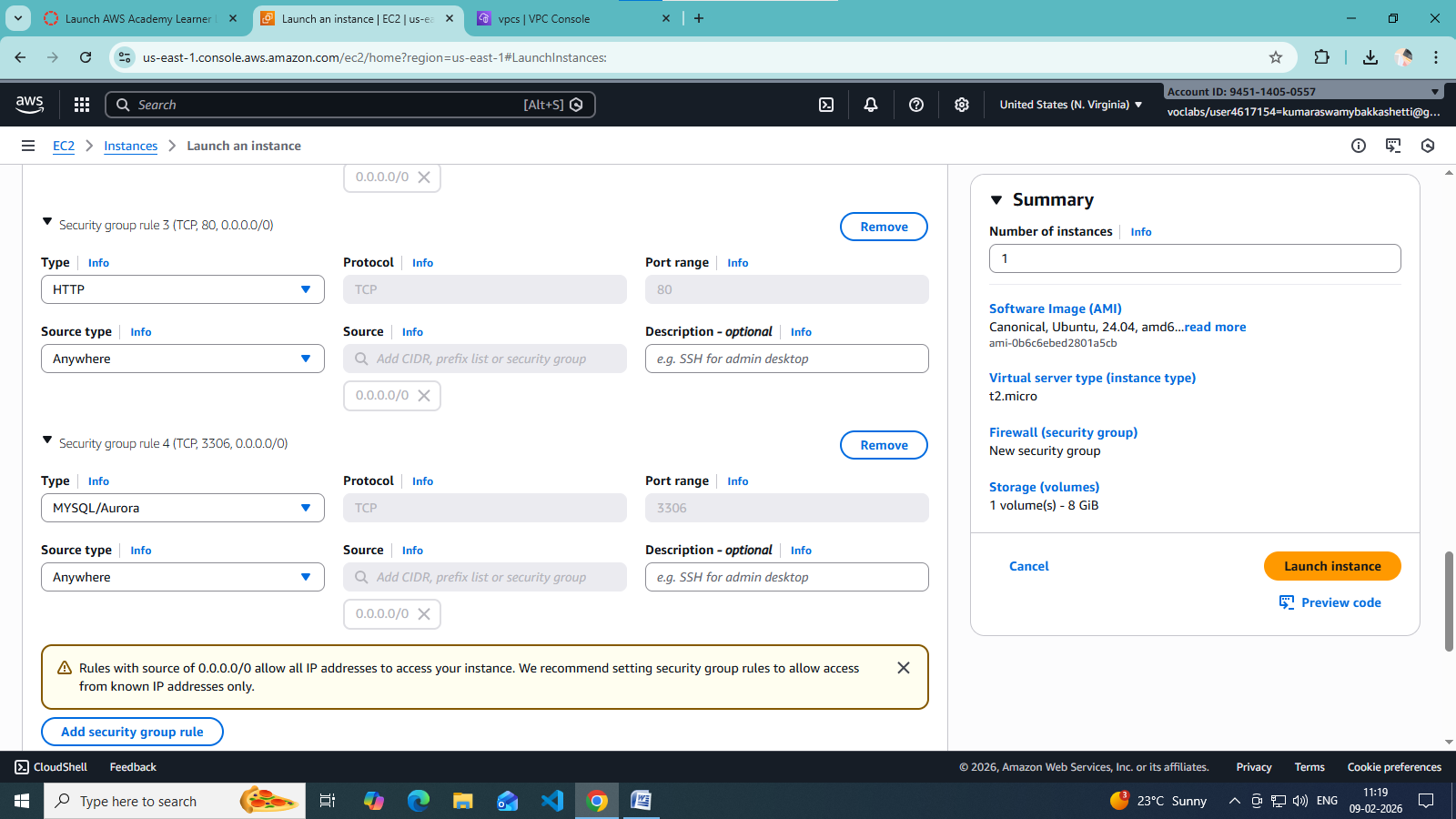
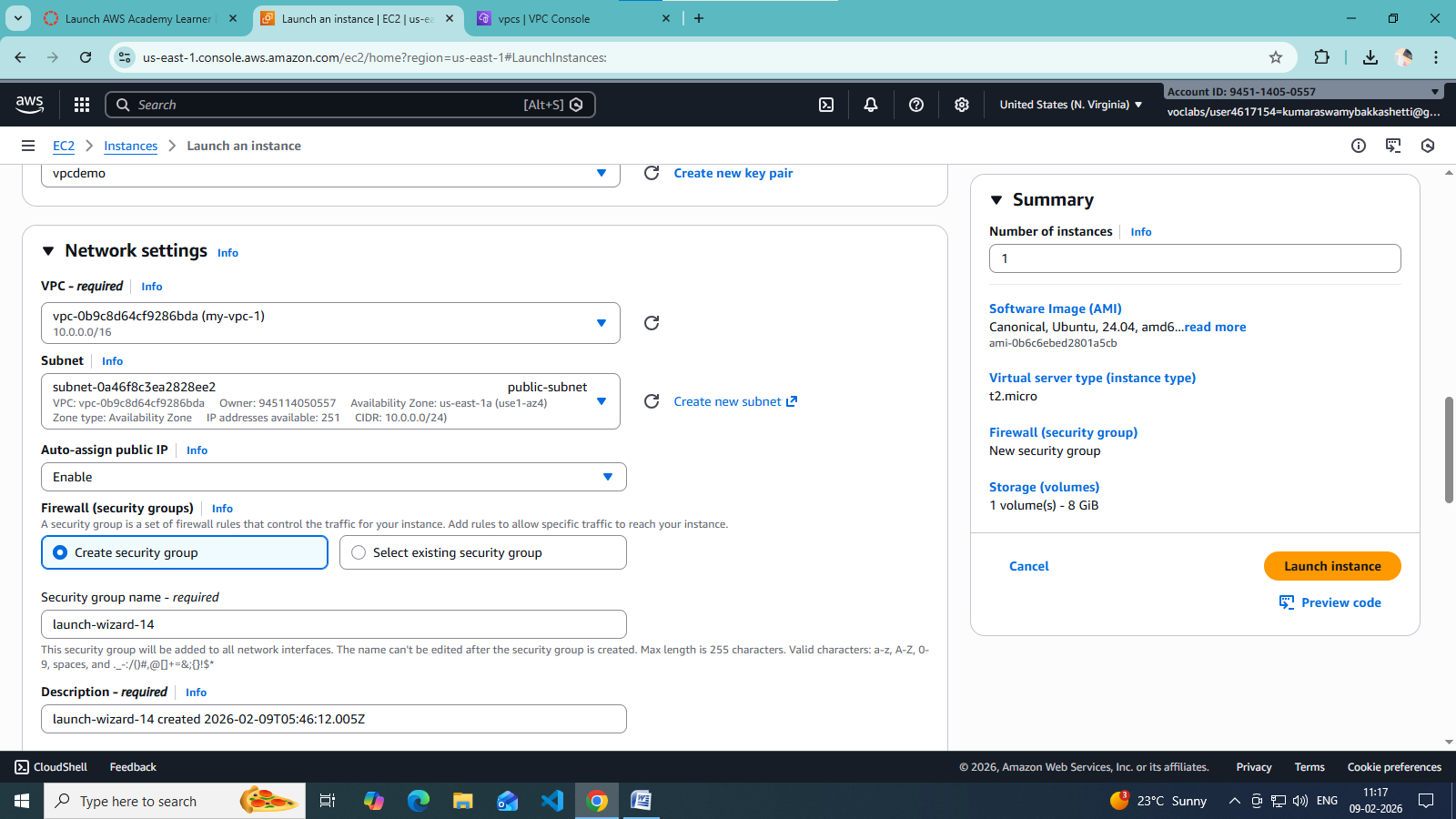
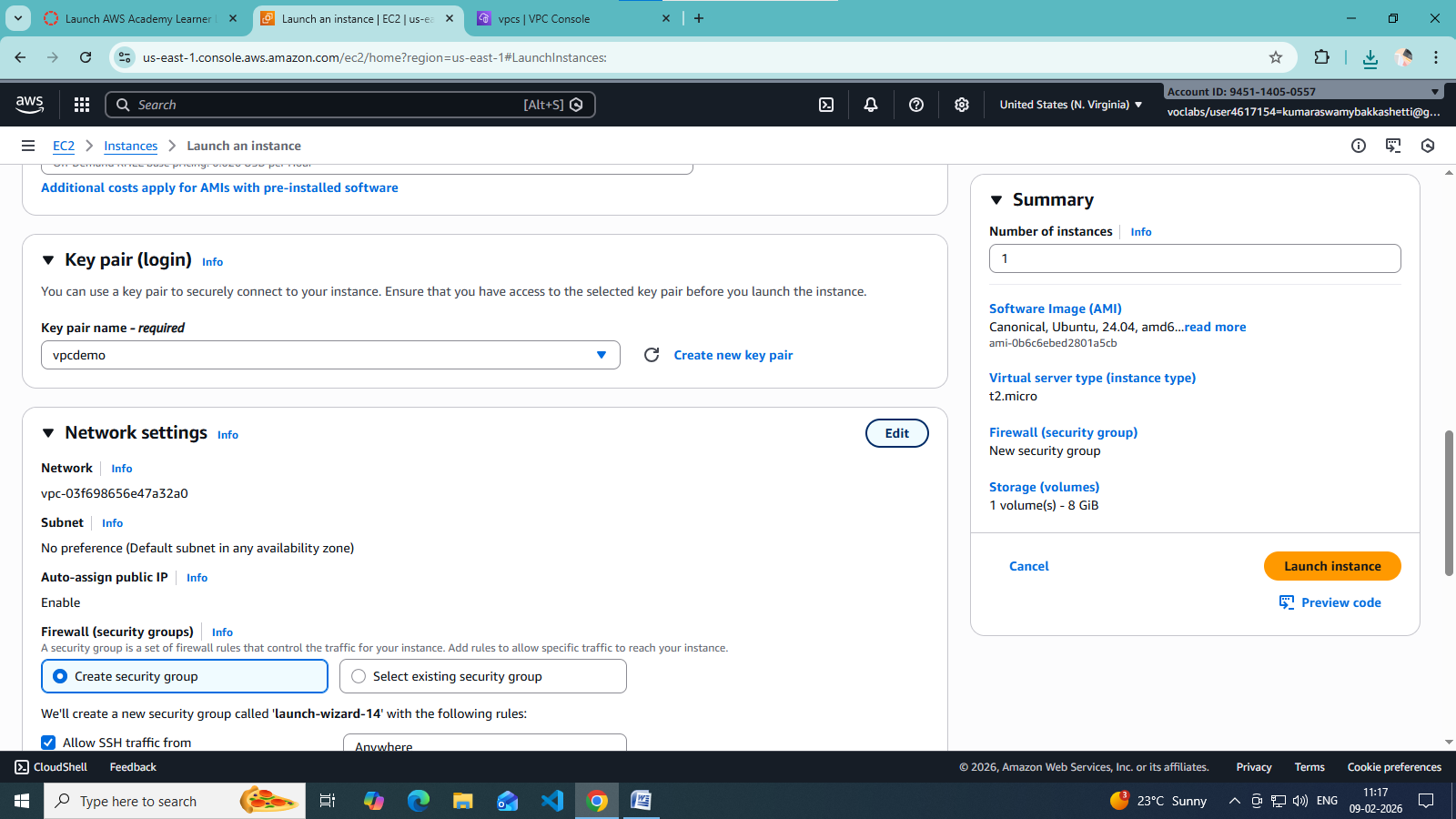
1. Select **Public Subnet**
2. Go to **Edit subnet settings**
3. Enable **Auto-assign public IPv4 address**



**🔹 Step 6: Configure Security Groups**

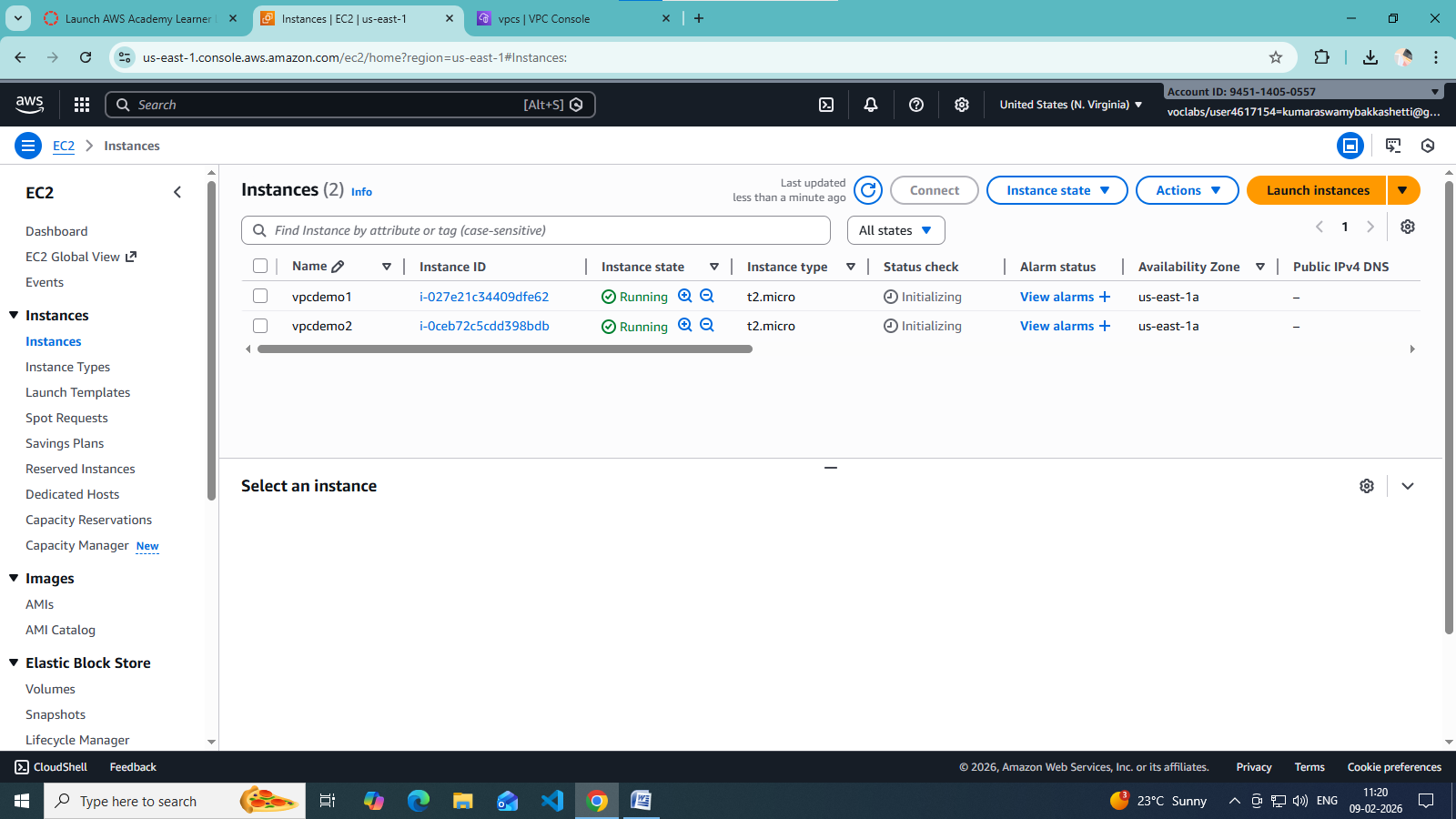
1. Create a **Security Group**
2. Add inbound rules:
   * HTTP (80) / HTTPS (443)
   * SSH (22) from trusted IP
3. Attach to EC2 instances





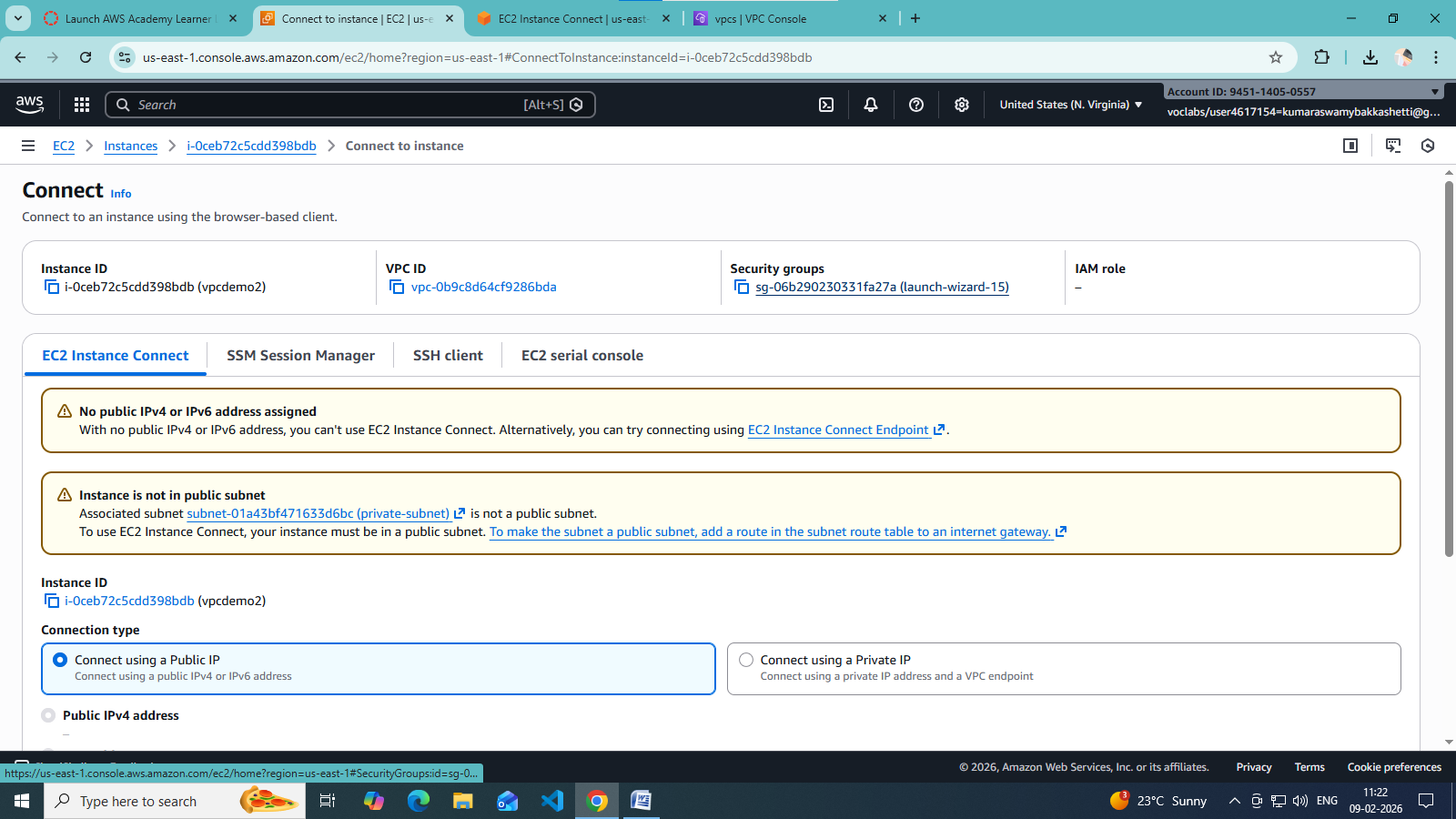
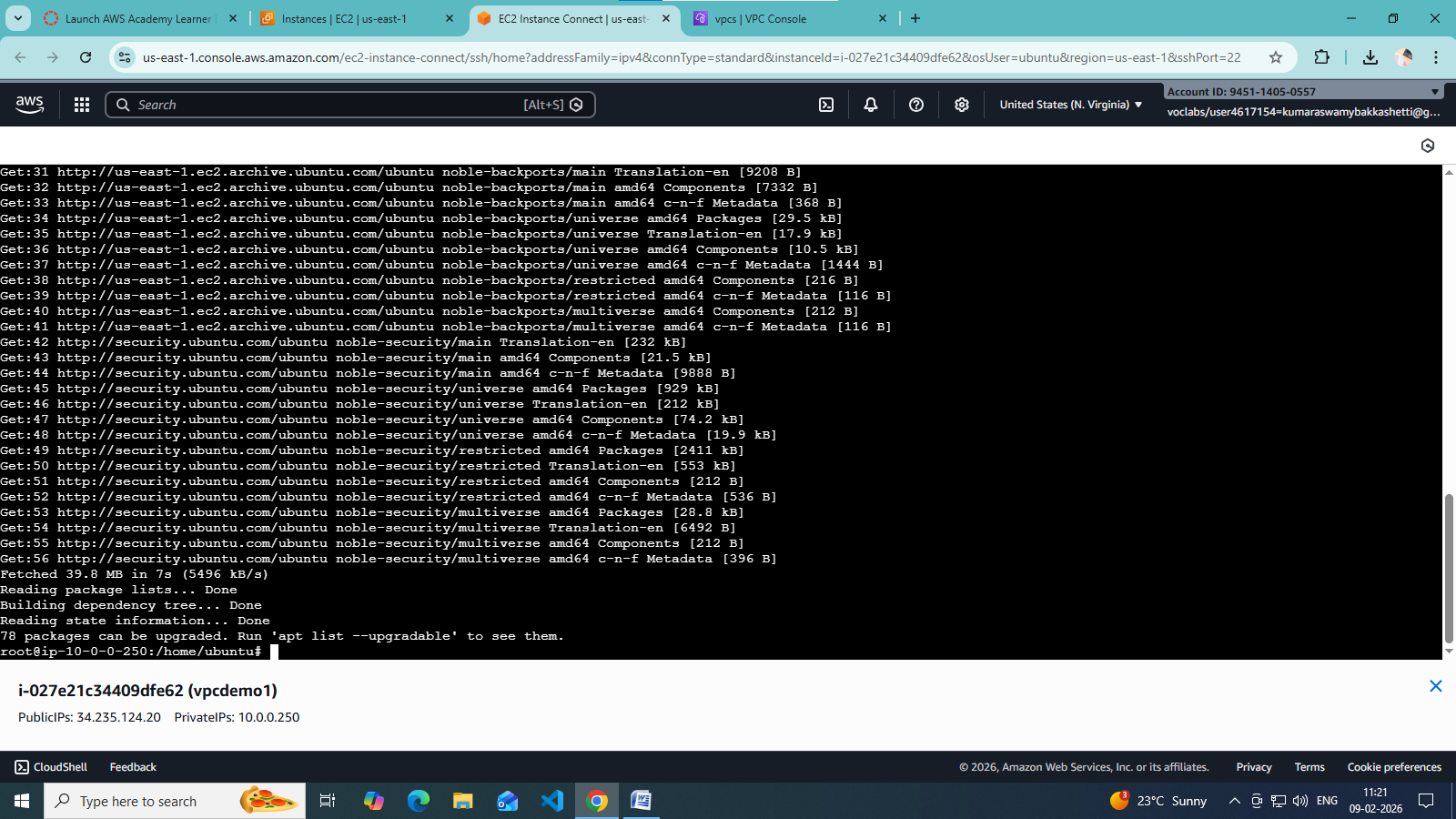
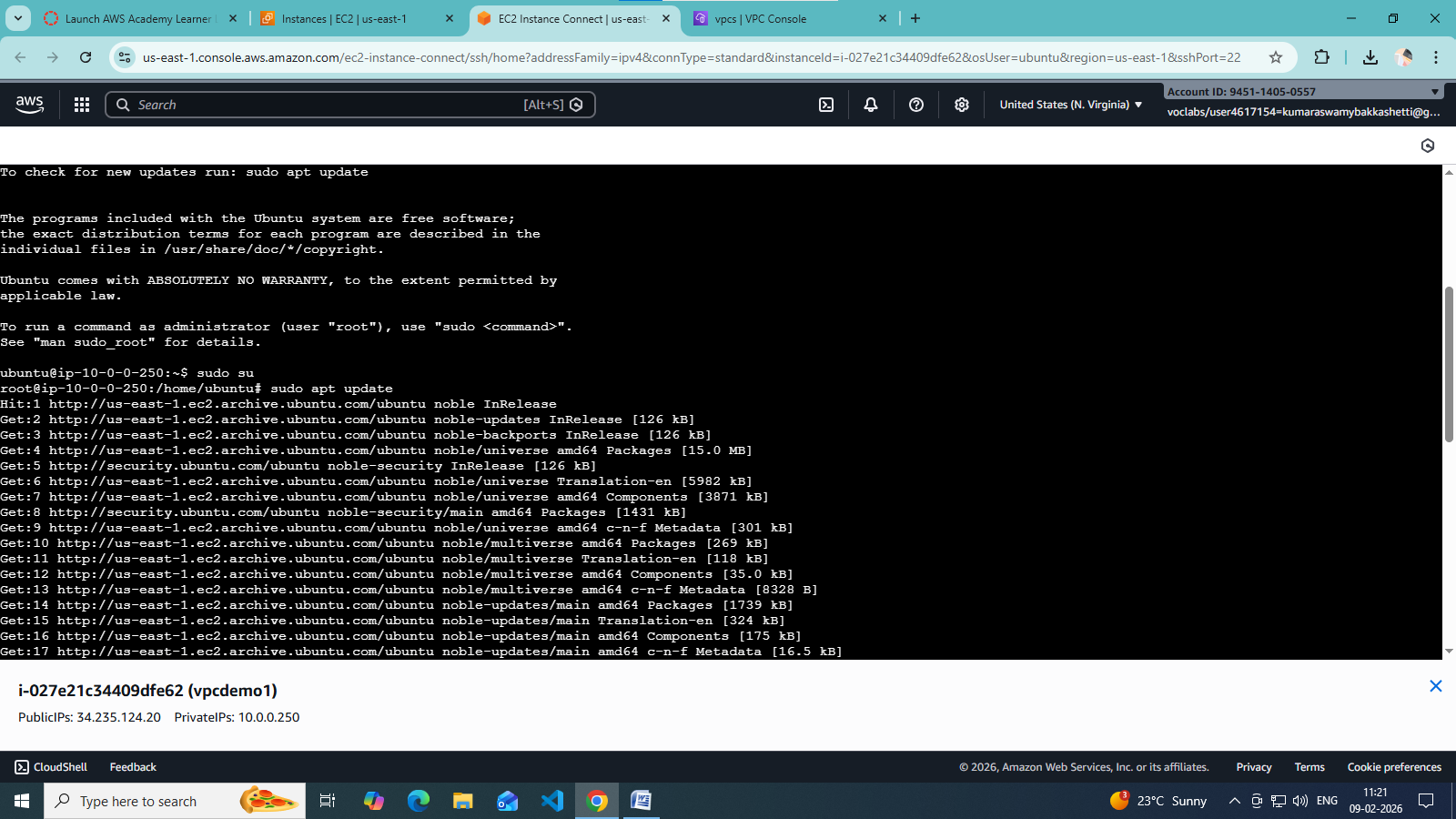
**🔹 Step 7: Launch EC2 Instances**

* Public EC2 → Public subnet
* Private EC2 → Private subnet  
  Attach correct security groups.



**🔹 Step 8: Test the Setup**

* Public EC2 → Internet access ✔
* Private EC2 → Internet via NAT ✔
* Private EC2 → No direct inbound access ✔



Scenario Based Questions:

1. You have a web application where users access a website, but the database should not be exposed to the internet. How would you design the VPC? Which resources go into public and private subnets?

**Public Subnet: Web servers + Internet Gateway  
Private Subnet: Application servers + Database (RDS)  
Users access web servers in public subnet. App and DB remain private for security.**

1. An EC2 instance in a public subnet cannot access the internet. What VPC components would you check and why?

**Check if Internet Gateway is attached to VPC  
Check route table has 0.0.0.0/0 → IGW  
Check instance has a public IP  
Check security group outbound rules  
Check NACL inbound and outbound rules**

1. Your application server needs to connect to an RDS database securely. How would you configure security groups and subnets?

**Place RDS in private subnet  
App server in private or public subnet  
Allow DB port only from App Server Security Group  
Do not allow public access to RDS**

1. You are asked to design a VPC for 500 servers today, but it should scale to 2,000 servers in the future. How would you choose the CIDR block?

**Choose a large CIDR block like /16 (example: 10.0.0.0/16)  
This provides enough IPs for future scaling across subnets and AZs**

1. A company wants secure connectivity between its on-premises data center and AWS VPC. Which AWS services would you choose and why (VPN vs Direct Connect)?

**Site-to-Site VPN: Quick, cost-effective, encrypted over internet  
Direct Connect: Dedicated private line, high bandwidth, low latency  
Use VPN for short-term or low traffic, Direct Connect for long-term or high traffic**

1. You need to connect two VPCs, but both use the same CIDR range. How would you solve this problem?

**Use VPC Peering is NOT possible  
Use AWS Transit Gateway with NAT  
Or redesign one VPC CIDR  
Or use application-level proxy**

1. Multiple microservices running in different subnets need to communicate securely. How would you design routing and security groups?

**Use same VPC local routing  
Create separate security groups per service  
Allow inbound traffic only from required service SGs  
Avoid using wide CIDR ranges**

1. Design a VPC for a 3-tier application (Web, App, DB) with high security and scalability. Explain subnets, route tables, gateways, and security groups.

**Public Subnet: Web tier + IGW  
Private Subnet 1: App tier + NAT Gateway access  
Private Subnet 2: DB tier (no internet access)  
Route tables configured separately  
Security groups allow tier-to-tier access only**

1. You suspect unusual traffic inside your VPC. How would you monitor and analyze network traffic?

**Enable VPC Flow Logs  
Use CloudWatch Logs and metrics  
Analyze using Athena or CloudWatch Insights  
Use GuardDuty for threat detection**

1. Why can’t a private subnet have an Internet Gateway directly attached?

**Internet Gateway attaches only to VPC, not subnet  
Private subnet does not route traffic to IGW  
It uses NAT Gateway for outbound internet access**

1. What happens if route tables are misconfigured in a VPC?

**Instances may lose internet access  
Private resources may become public  
Traffic may be dropped or misrouted**

1. What happens if a route table has no local route?

**VPC communication breaks  
Subnets cannot communicate internally  
AWS always adds local route automatically; removing it breaks networking**

1. An EC2 instance allows traffic on port 80 in the security group, but traffic is still blocked. What could be the reason?

**Network ACL blocking traffic  
Instance firewall blocking traffic  
Route table misconfiguration  
No public IP or IGW missing**

1. You need to create a VPC that will host 1,000+ EC2 instances across multiple AZs. How do you decide the CIDR block?

**Estimate future IP usage  
Choose /16 or /17 CIDR  
Split into multiple subnets per AZ  
Avoid overlapping CIDRs**

1. Only a company’s corporate IP should be able to SSH into EC2 instances. How would you implement this securely in AWS VPC?

**Allow port 22 only from corporate public IP in security group  
Use private subnets + Bastion Host  
Prefer AWS Systems Manager Session Manager**

1. An EC2 instance can send traffic out but cannot receive responses. Which VPC component might be misconfigured and why?

**Security group inbound rules missing  
Network ACL inbound rules blocking traffic  
Route table missing return route  
Source/Destination check enabled incorrectly**