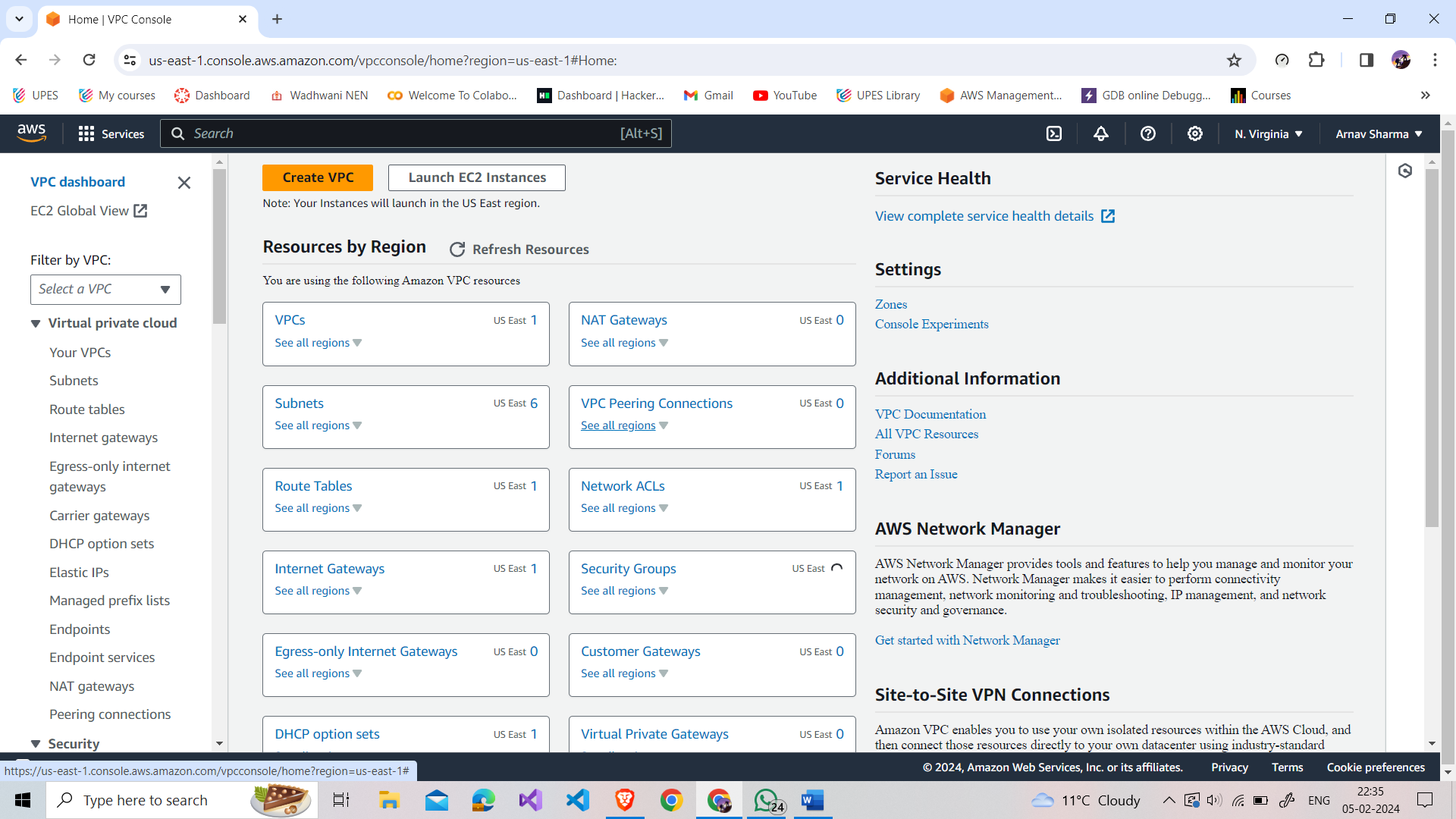
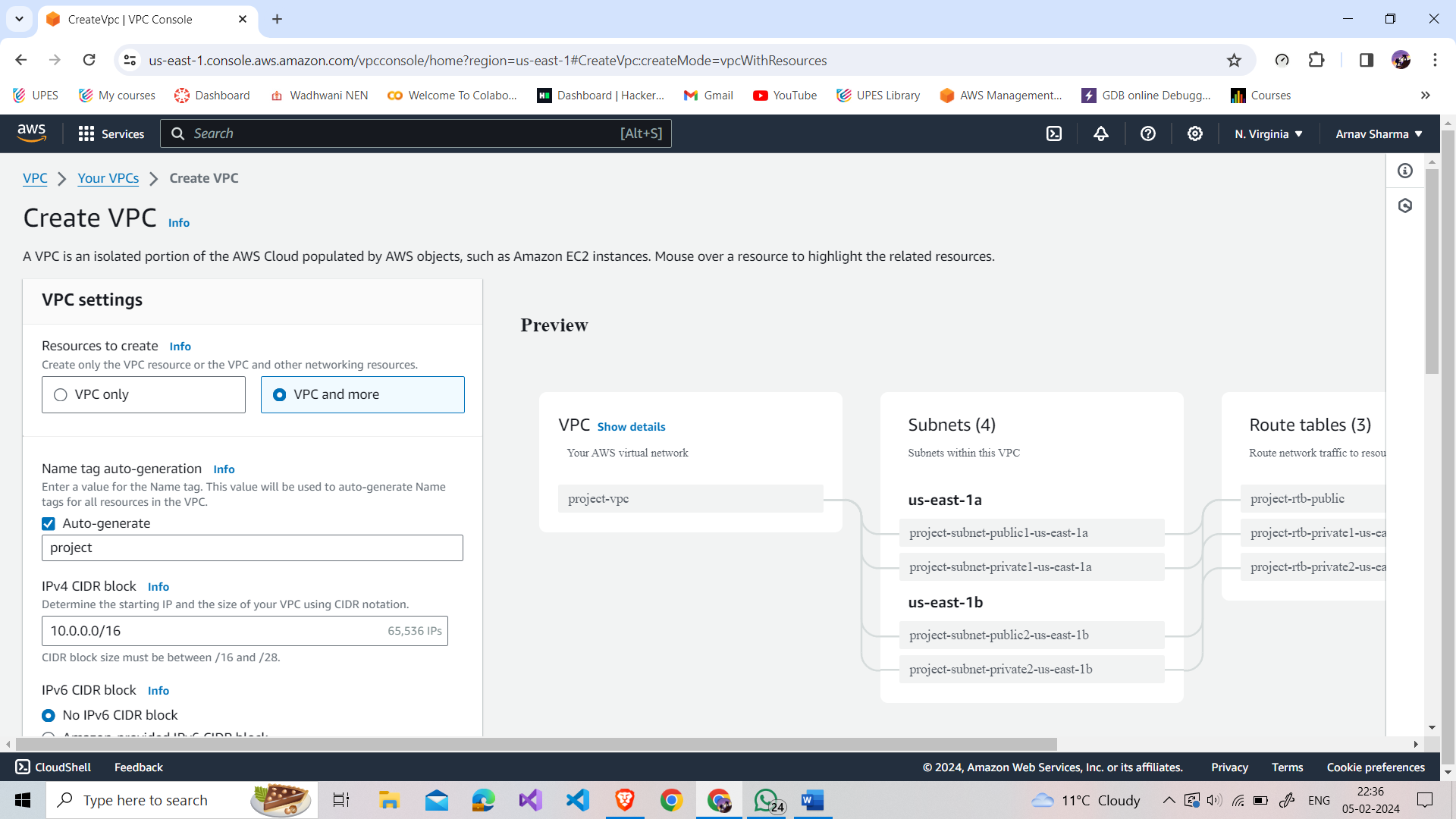
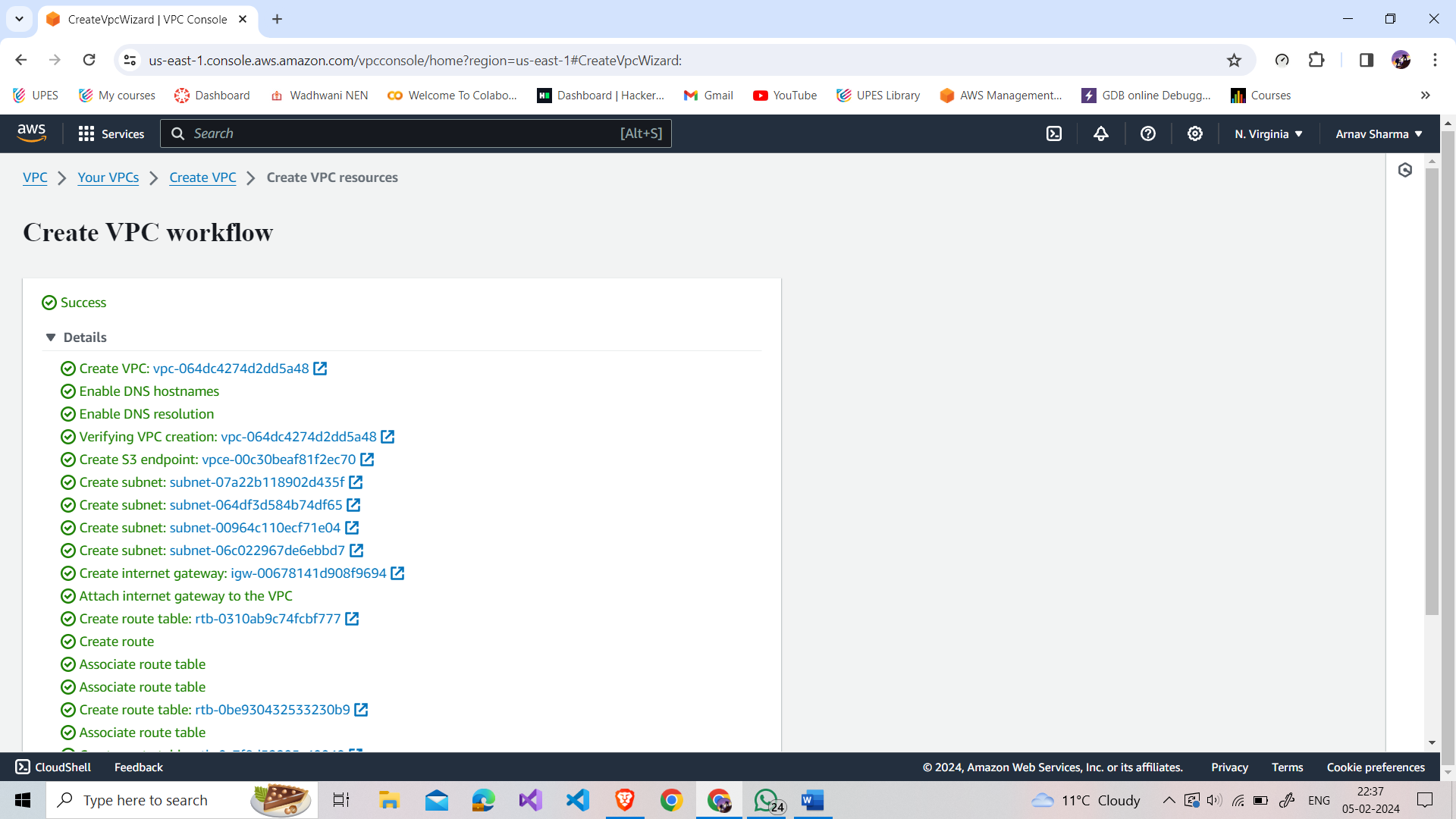
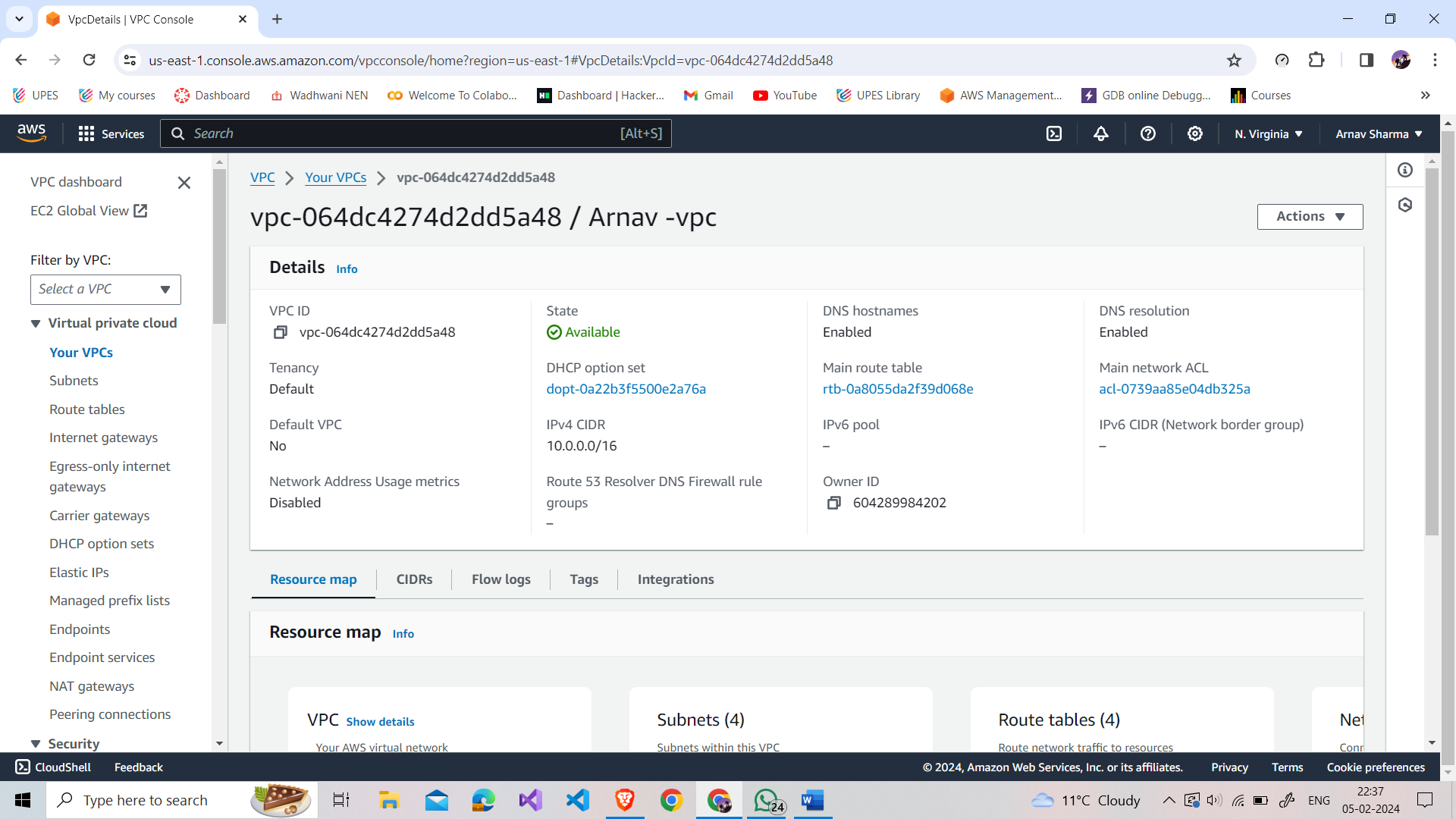
EXPERIMENT 3

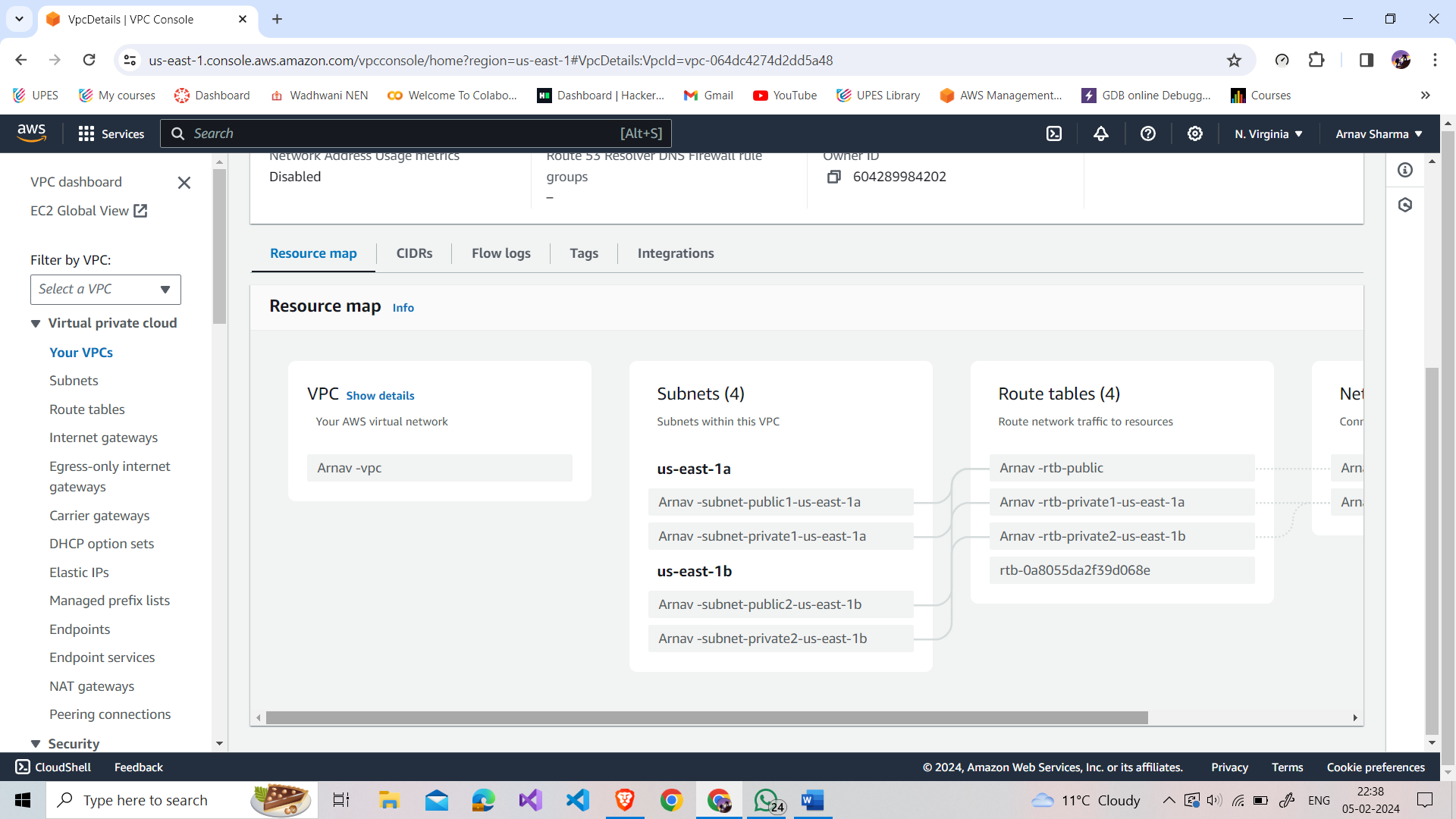
Create a Virtual Private cloud within AWS infrastructure.

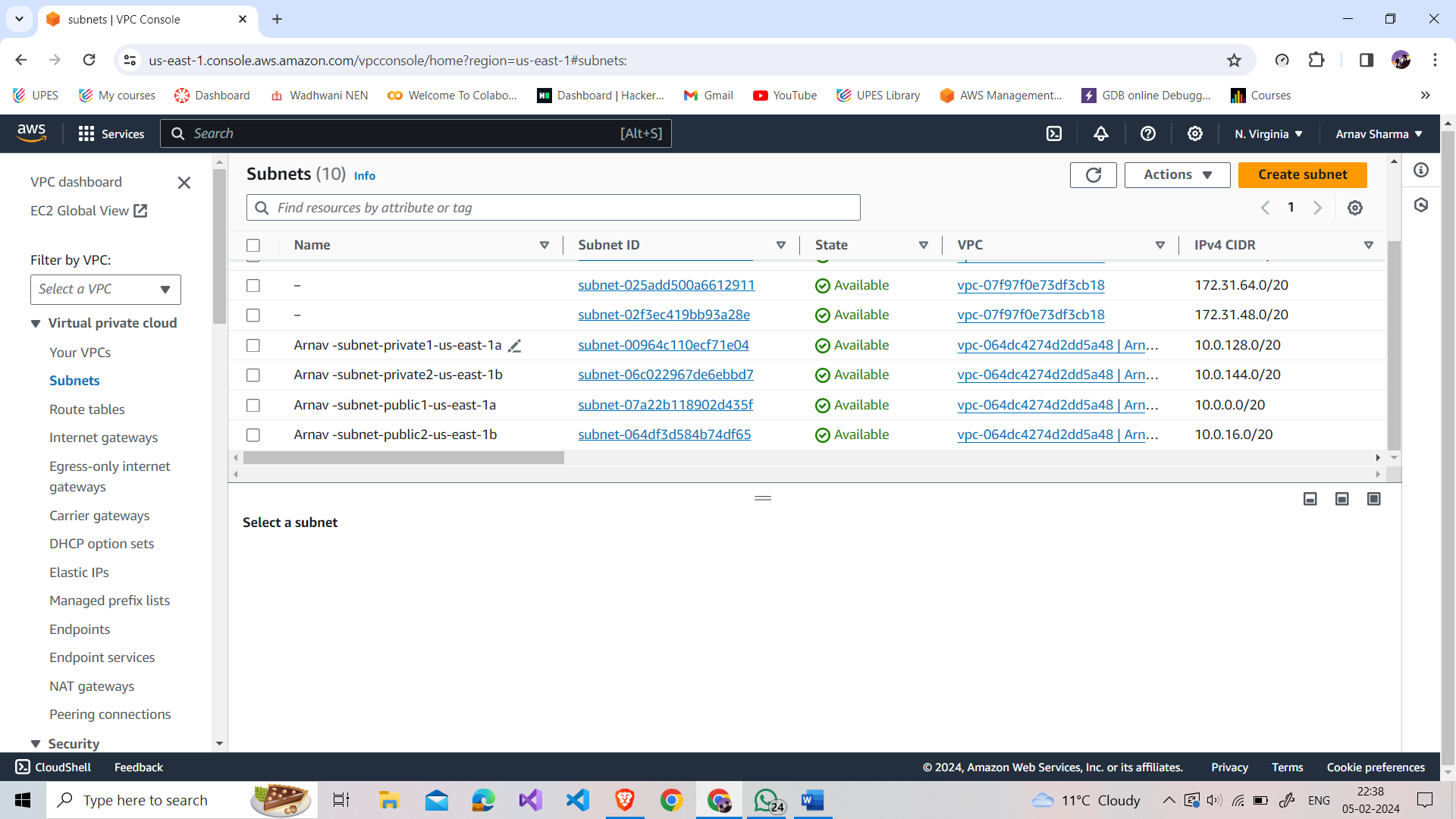


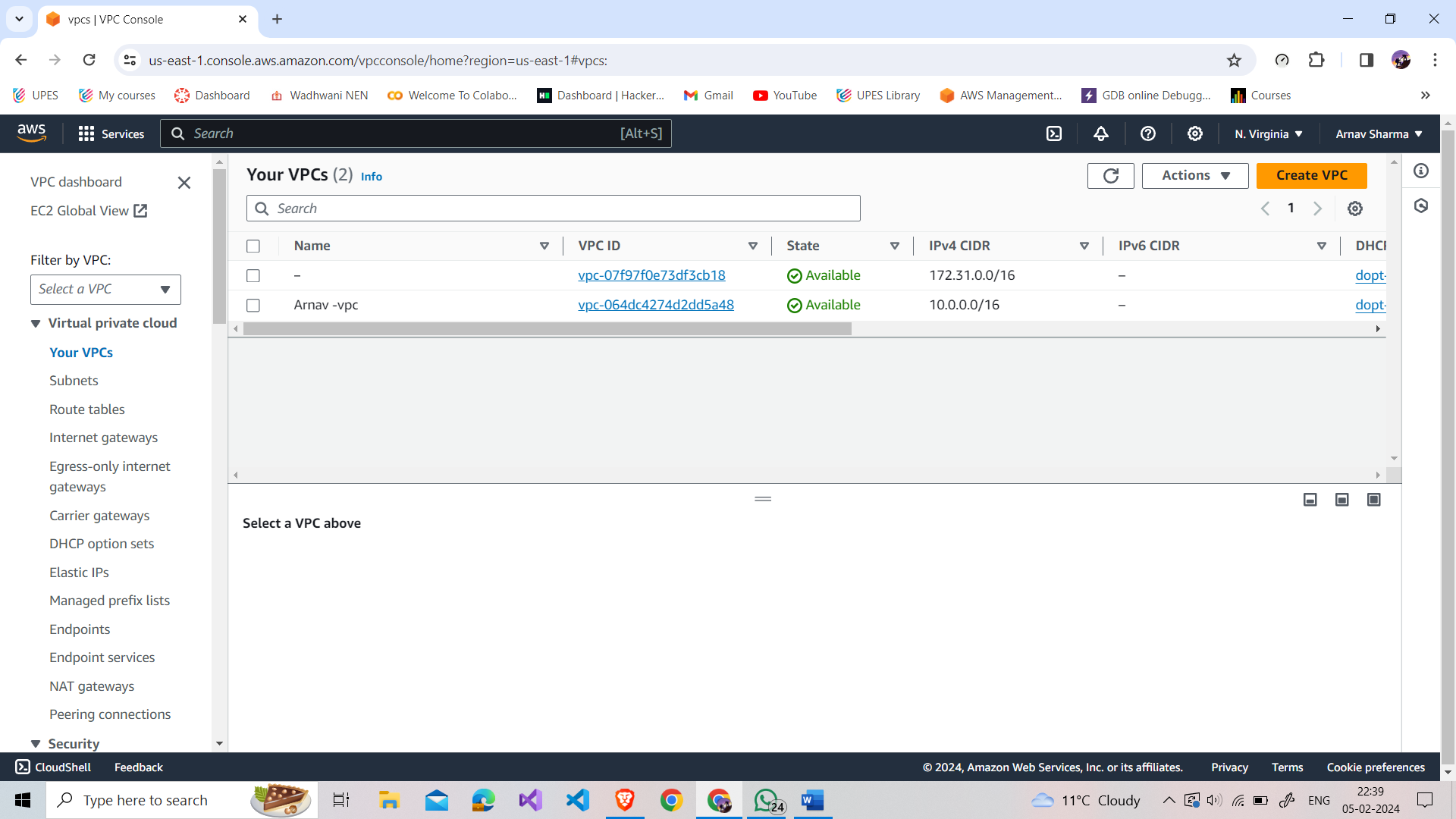












Q1. What is EC2 in AWS. What are key features of EC2.

Ans: Amazon Elastic Compute Cloud (EC2) is a service in AWS that lets you rent virtual servers (instances) on-demand.

Key features include scalability for adjusting computing capacity, various instance types, pre-configured machine images, flexible pricing models, security features like security groups and Virtual Private Cloud (VPC), Elastic Load Balancing (ELB) for distributing traffic, Elastic Block Store (EBS) for scalable block storage, monitoring with Amazon CloudWatch, identity management with IAM, and auto-scaling to adjust the number of instances based on demand. It provides a scalable, flexible, and cost-effective solution for running virtual servers in the cloud.

Q2. What does VPC stands in AWS. Why is VPC is important in AWS.

Ans: AWS VPC, or Virtual Private Cloud, is a secure and isolated section within AWS where you can launch resources. It provides control over networking, security, and connectivity, allowing you to create a tailored environment for your applications. VPC is crucial for security, compliance, resource deployment, and cost management in AWS.

Q3. What is the primary purpose of creating subnets with it a VPC.

Ans: The primary purpose of creating subnets within a VPC is to logically partition and organize the IP address space, allowing for better network management, improved security, and more efficient resource utilization within the AWS Virtual Private Cloud.

Q4. Can a VPC span multiple AWS region.

Ans: No, a VPC cannot span multiple AWS regions. Each VPC is confined to a single AWS region.

Q5. How does the concept the availability zone relate to VPC, can resources in one availability zones communicate with another resources in another availability zones with in the VPC.

Ans: Availability Zones (AZs) in AWS are separate data centers within a region. When you create a VPC, you can spread it across multiple AZs for high availability. Resources in one AZ can communicate with resources in another AZ within the same VPC. This enhances fault tolerance, and AWS ensures low-latency connectivity between AZs. For communication between resources in different VPCs, additional configurations like VPC peering are required.

Q6. How is internet connectivity achieved with in the VPC.  
Ans: Internet connectivity within an AWS VPC is achieved through an Internet Gateway (IGW), route tables, and public subnets. Attach an IGW to the VPC, configure route tables to direct traffic to the IGW, and place instances that need internet access in public subnets. Assign Elastic IP addresses as needed for public access.

Q7. What is the significant of route table in a VPC  
Ans: In an AWS VPC (Virtual Private Cloud), a route table is a fundamental component that plays a crucial role in determining how network traffic is directed. Here are the key significances of a route table in a VPC:

* Traffic Routing: The primary purpose of a route table is to define the routes for network traffic within the VPC. It specifies the paths that traffic takes when traveling between subnets, to and from the internet, and to other network destinations.
* Association with Subnets: Each subnet in a VPC must be associated with a specific route table. This association determines how the traffic in that subnet is routed. A subnet's route table dictates the destinations for local traffic (within the VPC) and remote traffic (outside the VPC).
* Internet Connectivity: For instances in a public subnet to access the internet, the associated route table typically includes a route to the Internet Gateway (IGW). This allows traffic destined for the internet to be directed through the IGW.
* Customization: Route tables offer a high degree of customization. You can create multiple route tables and associate different subnets with different route tables. This flexibility allows you to design complex network architectures and control the flow of traffic based on your requirements.
* Traffic Isolation: By associating subnets with specific route tables, you can isolate traffic and control the communication between different parts of your network. This is essential for creating secure and segmented environments within a VPC.
* Multi-Region and VPC Peering: In more advanced scenarios, route tables are crucial for configuring multi-region communication or VPC peering. They define the routes for traffic going between VPCs or across different AWS regions.
* Default Route: Each route table typically includes a default route, often pointing to the local VPC CIDR block. This ensures that local traffic within the VPC is handled efficiently.

Q8. What is the difference between public, private and elastic IP addresses  
Ans:

* Public IP Address: Used for resources directly accessible over the internet. Instances in public subnets often have public IPs. Not persistent.
* Private IP Address: Used for internal communication within a VPC. Instances in private subnets typically have private IPs. More stable and not directly reachable from the internet.
* Elastic IP Address: Static IP for dynamic cloud computing. Provides a persistent public IP, can be associated with instances, and is remappable. Public and reachable from the internet.

Q9. How can one securely access resources with IP address with in a VPC.  
Ans: Securely accessing resources within a VPC involves:

* Use Network Security Groups and Security Groups to control traffic.
* Differentiate between public and private subnets.
* Implement bastion hosts or jump boxes for secure access.
* Set up VPN or Direct Connect for secure connectivity.
* Use Elastic IP addresses or DNS for addressing.
* Utilize IAM roles and policies for access control.
* Enable auditing and monitoring with CloudTrail and CloudWatch.
* Implement encryption for data at rest and in transit.
* Conduct regular security audits and stay informed about best practices.