**VIRTUAL PRIVATE CLOUD (VPC)**

A **VPC (Virtual Private Cloud)** in AWS is a **logically isolated** network within the AWS cloud where you can launch and manage AWS resources like **EC2 instances, RDS databases, and Lambda functions**. It allows you to control network settings such as **IP addressing, subnets, routing, and security**.

**VPC Components**

1. **CIDR Block** – Defines the IP range for the VPC (e.g., 10.0.0.0/16).
2. **Subnets** – Smaller networks within the VPC.
   * **Public Subnet** – Can access the internet.
   * **Private Subnet** – No direct internet access.
3. **Internet Gateway (IGW)** – Enables public internet access for public subnets.
4. **NAT Gateway** – Allows private subnets to access the internet **without being exposed**.
5. **Route Tables** – Define how traffic is routed between subnets and the internet.
6. **Security Groups** – Firewalls that control traffic for instances.
7. **Network ACLs (NACLs)** – Firewall rules at the **subnet level**.

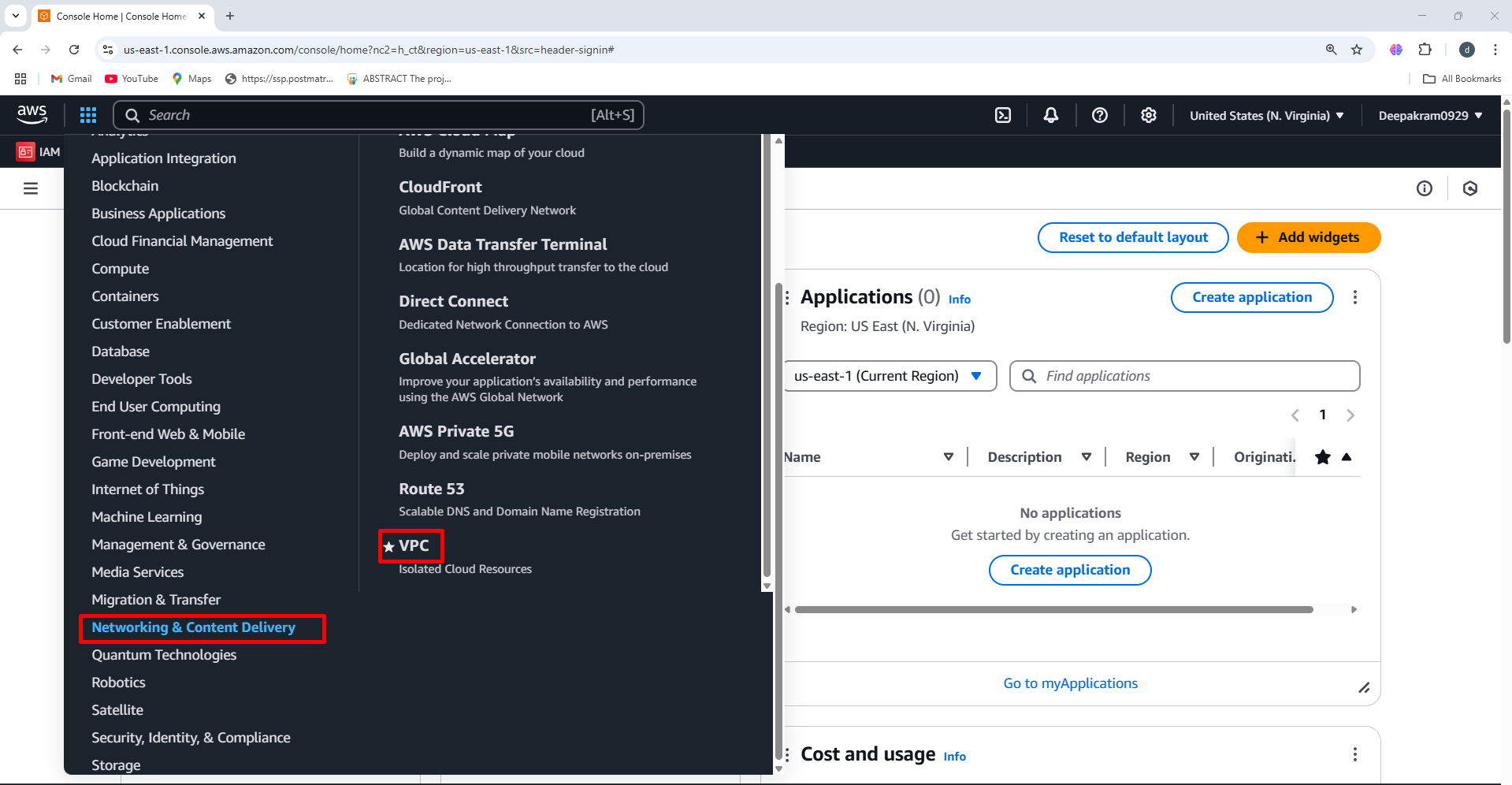
**Why Use a VPC?**

* **Custom Network Configuration** – Design your own network in AWS.
* **Security & Isolation** – Fully controlled and private.
* **Scalability** – Easily expand with multiple subnets.
* **Hybrid Cloud** – Connect with on-premises data centre’s via **VPN or Direct Connect**.

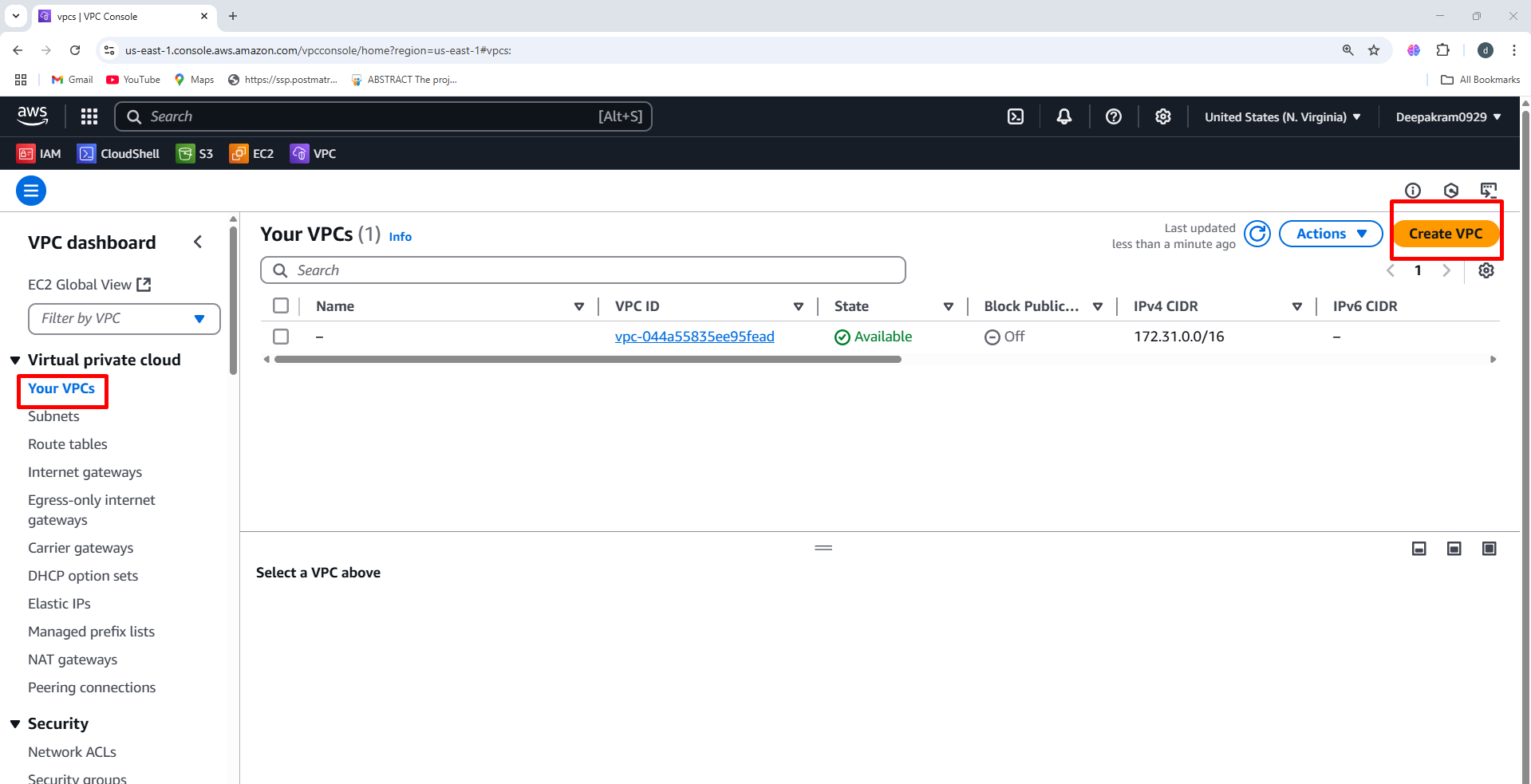
**To Create VPC**

Network content delivery 🡪 VPC 🡪 VPC’s 🡪 Create VPC 🡪 VPC and More 🡪 Name 🡪 Select number of availability zone 🡪 No of public subnets 🡪 No of private subnets 🡪 S3 end point 🡪 Create VPC

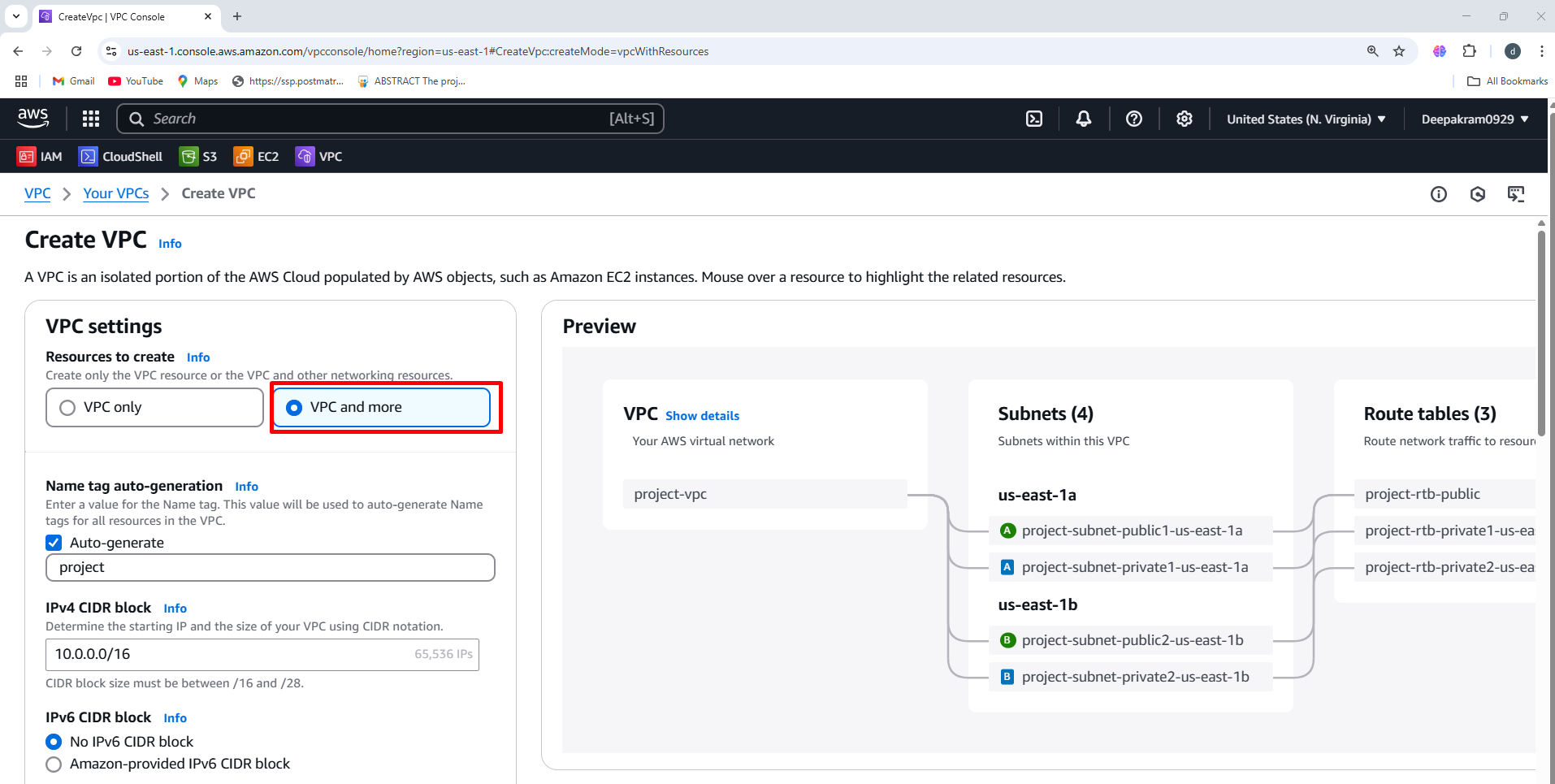
1. **AWS Management Console** 🡪 network content delivery 🡪 click on vpc



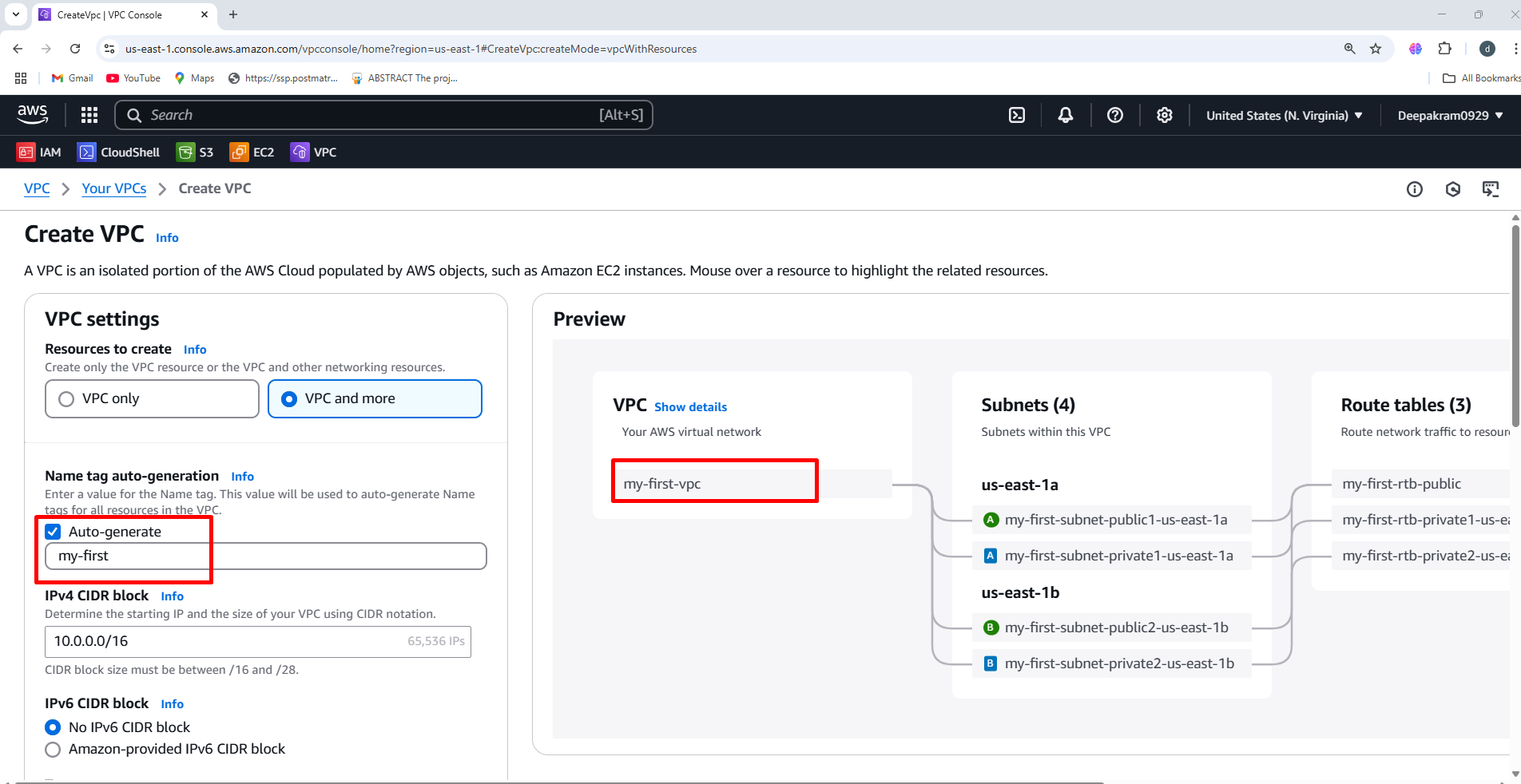
1. Your VPC’s 🡪 Create VPC



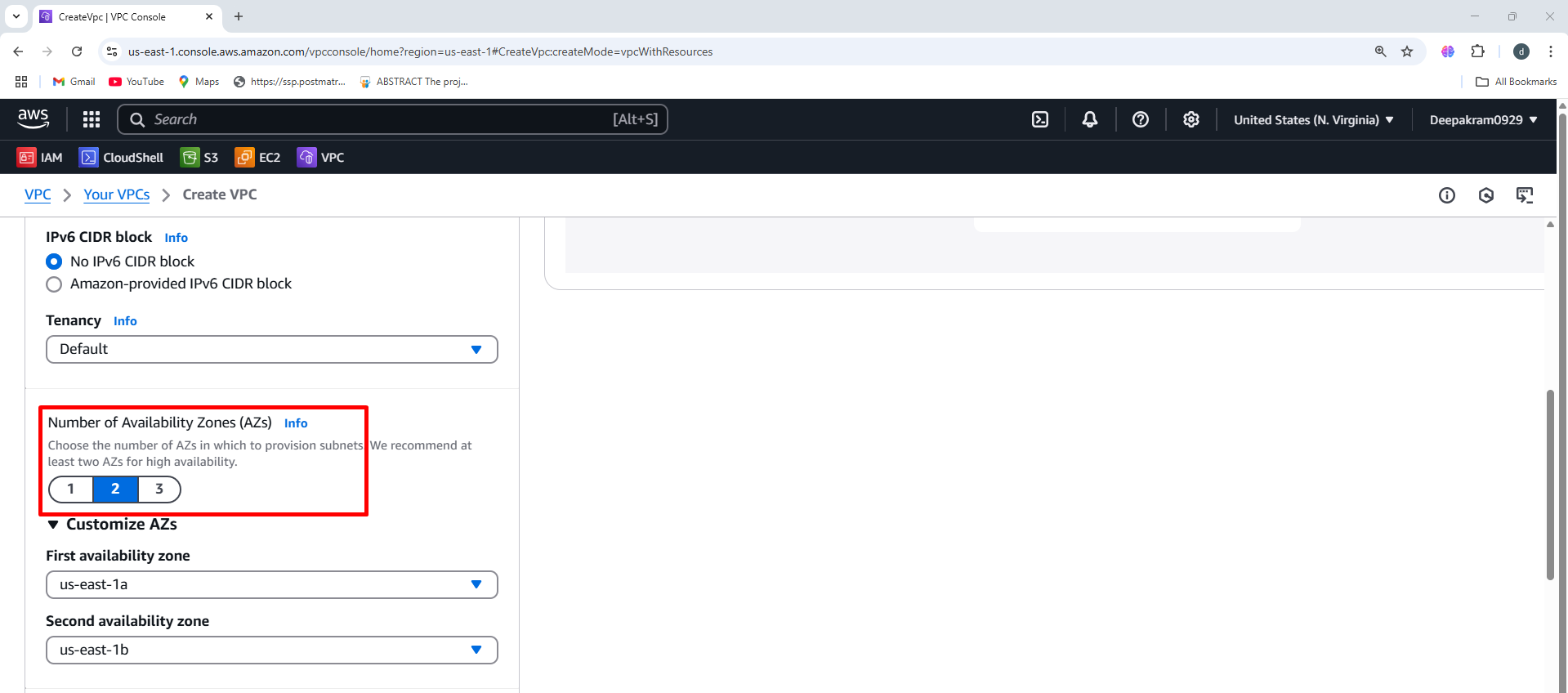
1. Choose **VPC and more** (VPC with subnets, gateways, etc.).



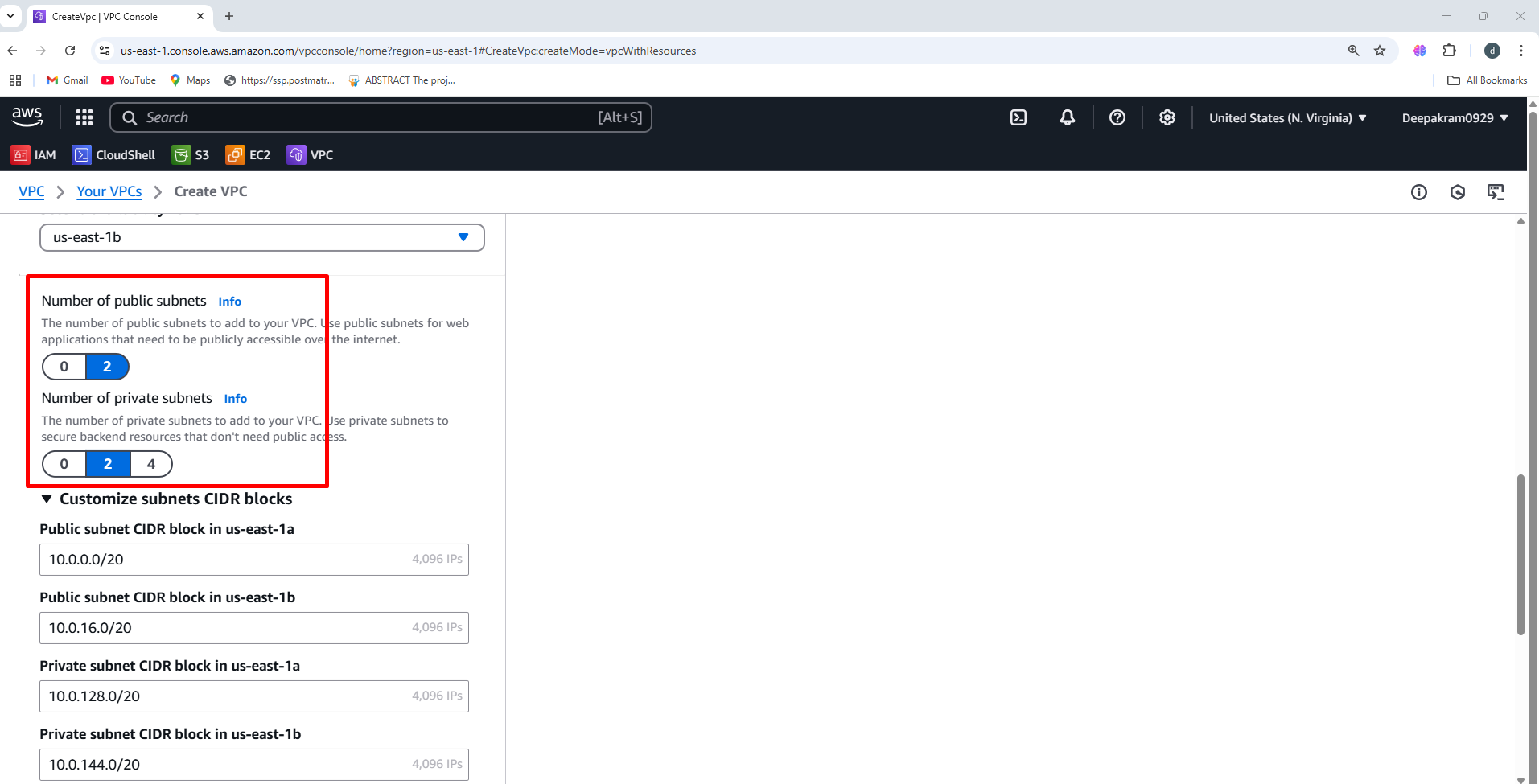
1. Provide the name for your VPC



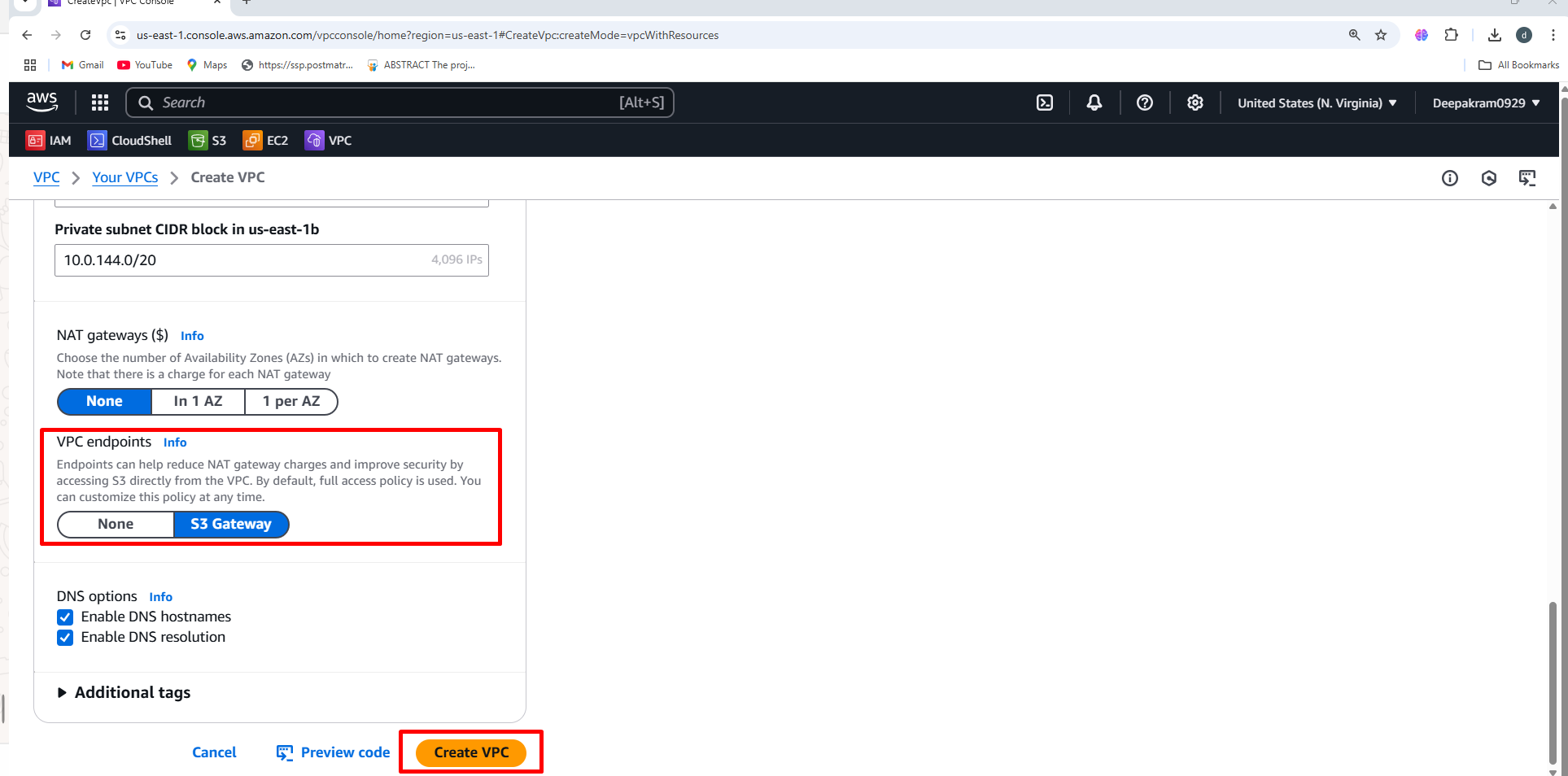
1. Select the number of availability zone

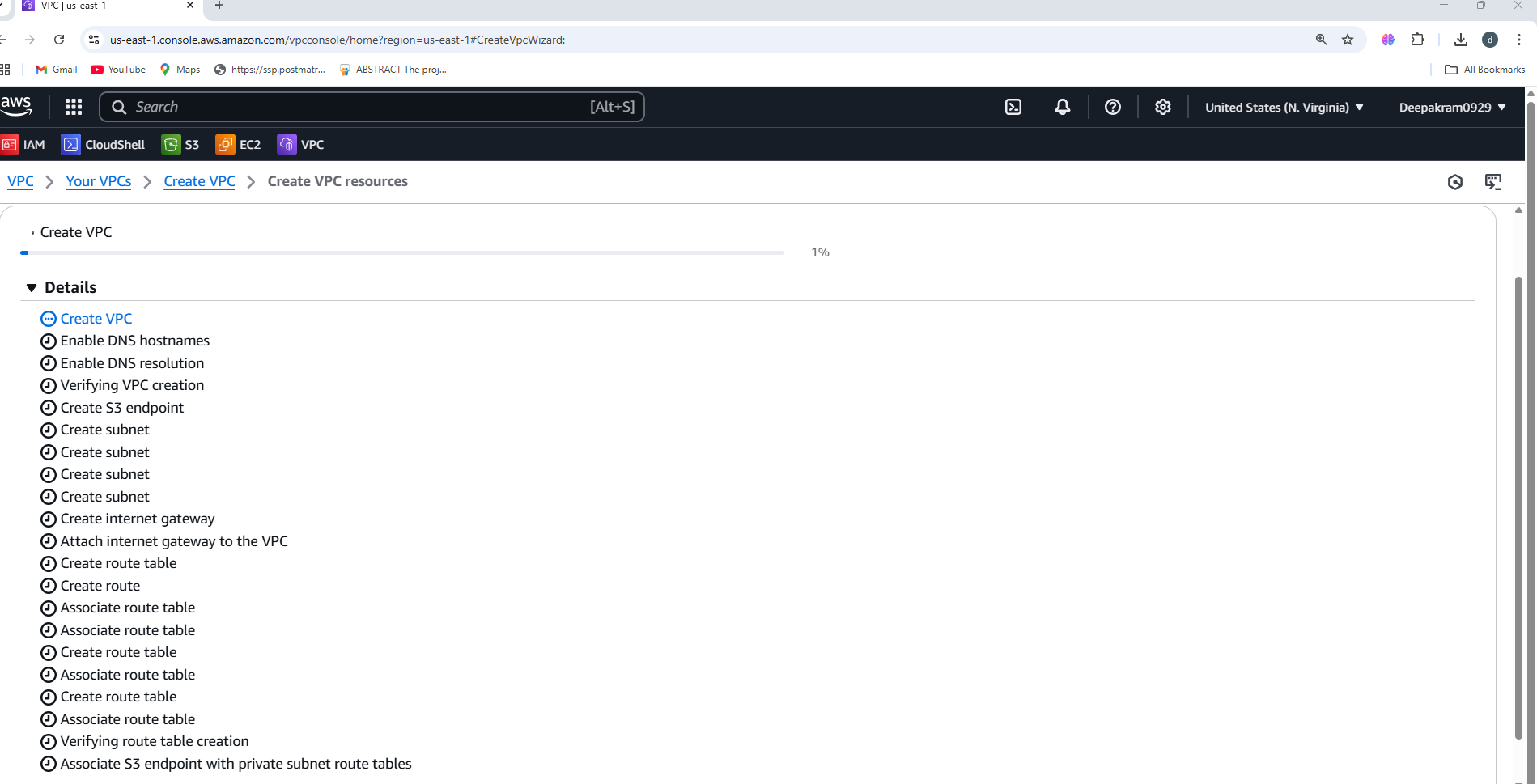


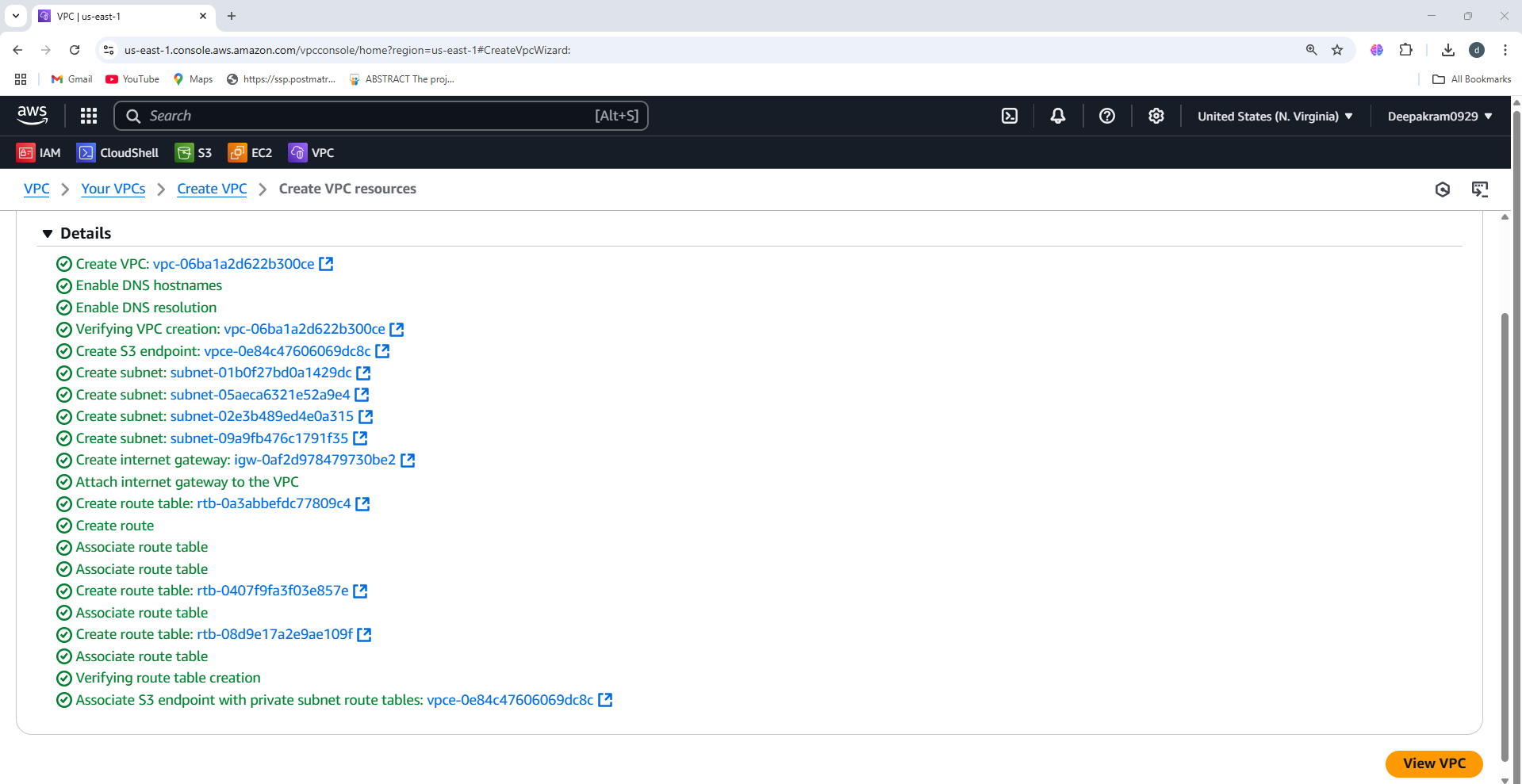
1. Select number of public subnets and private subnets

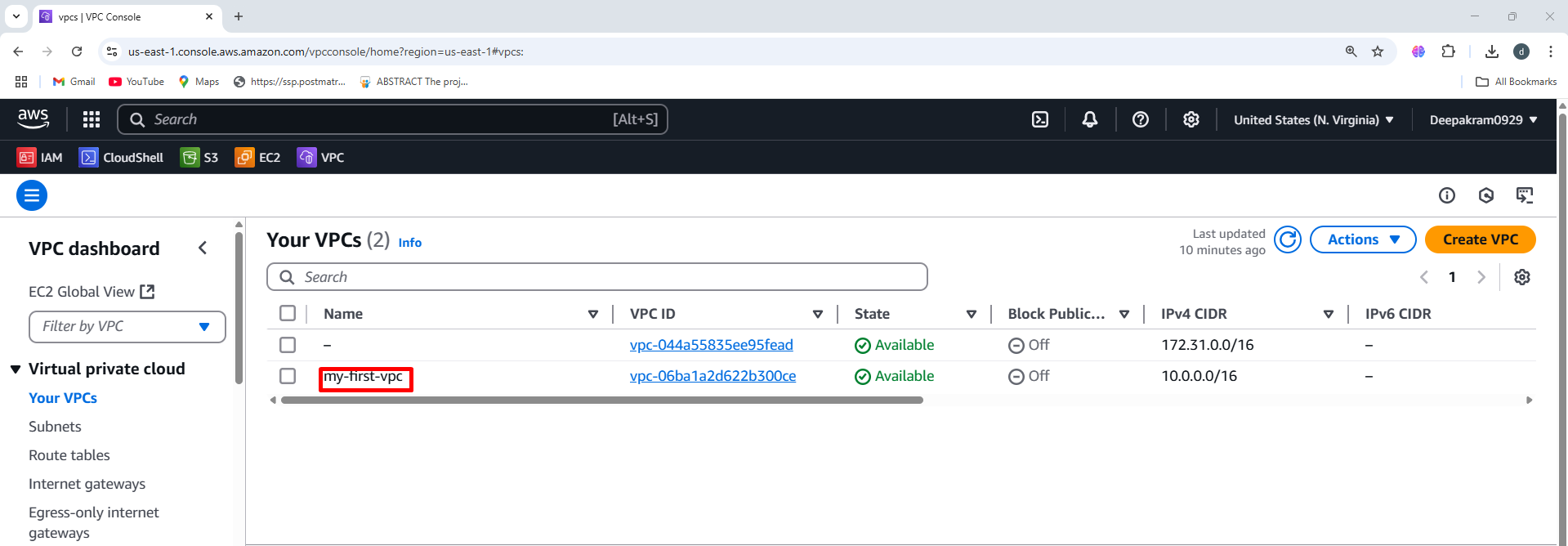


1. Nate gateway 🡪 none 🡪 S3 endpoint 🡪 create VPC

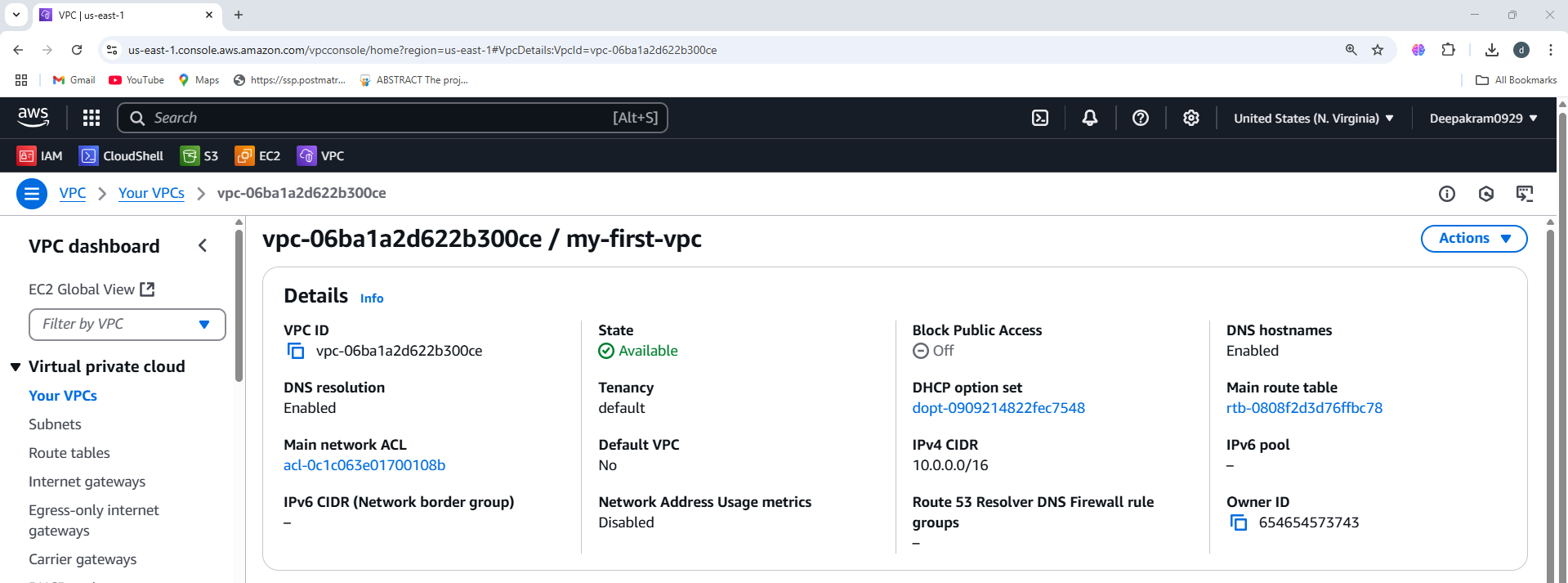








1. **VPC Dashboard - my-first-vpc 🡪** It shows details about a Virtual Private Cloud (VPC)



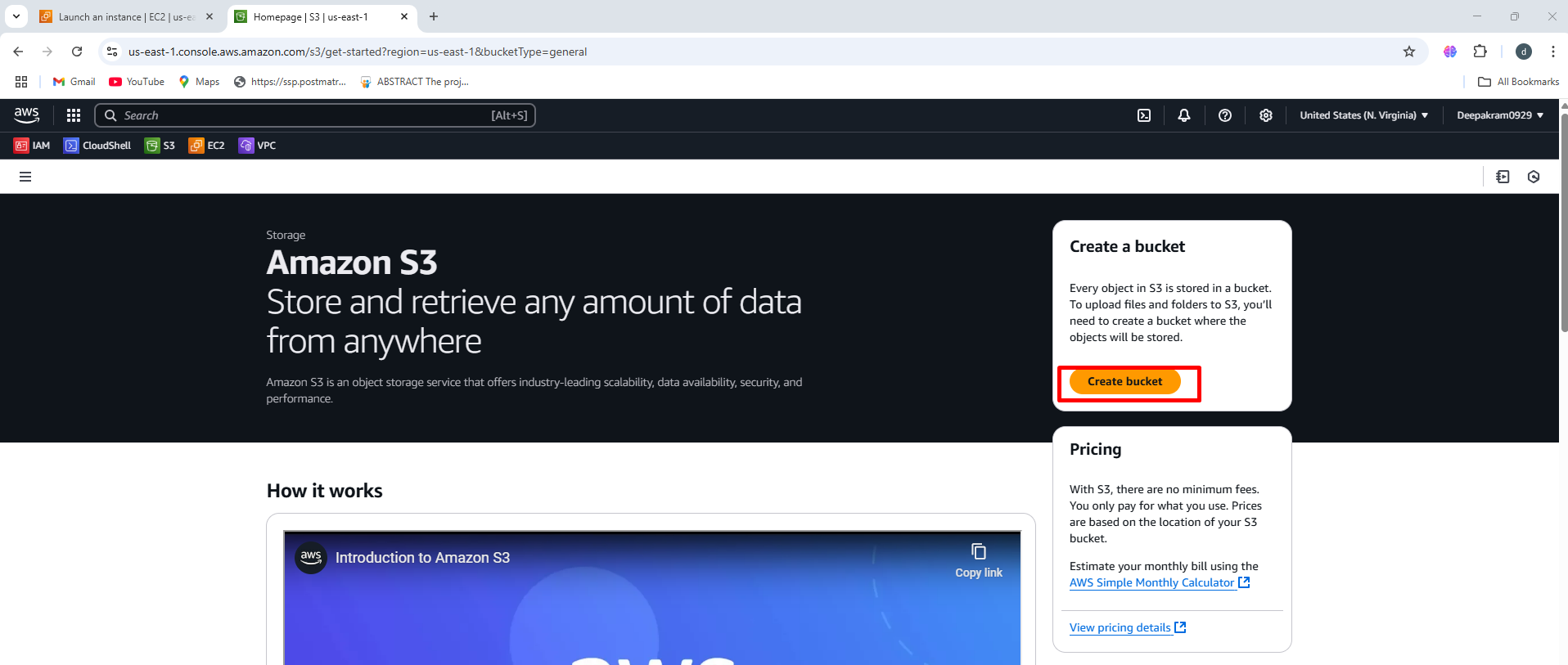
1. **AWS VPC Resource Map**, which provides a visual representation of the networking setup within a VPC.



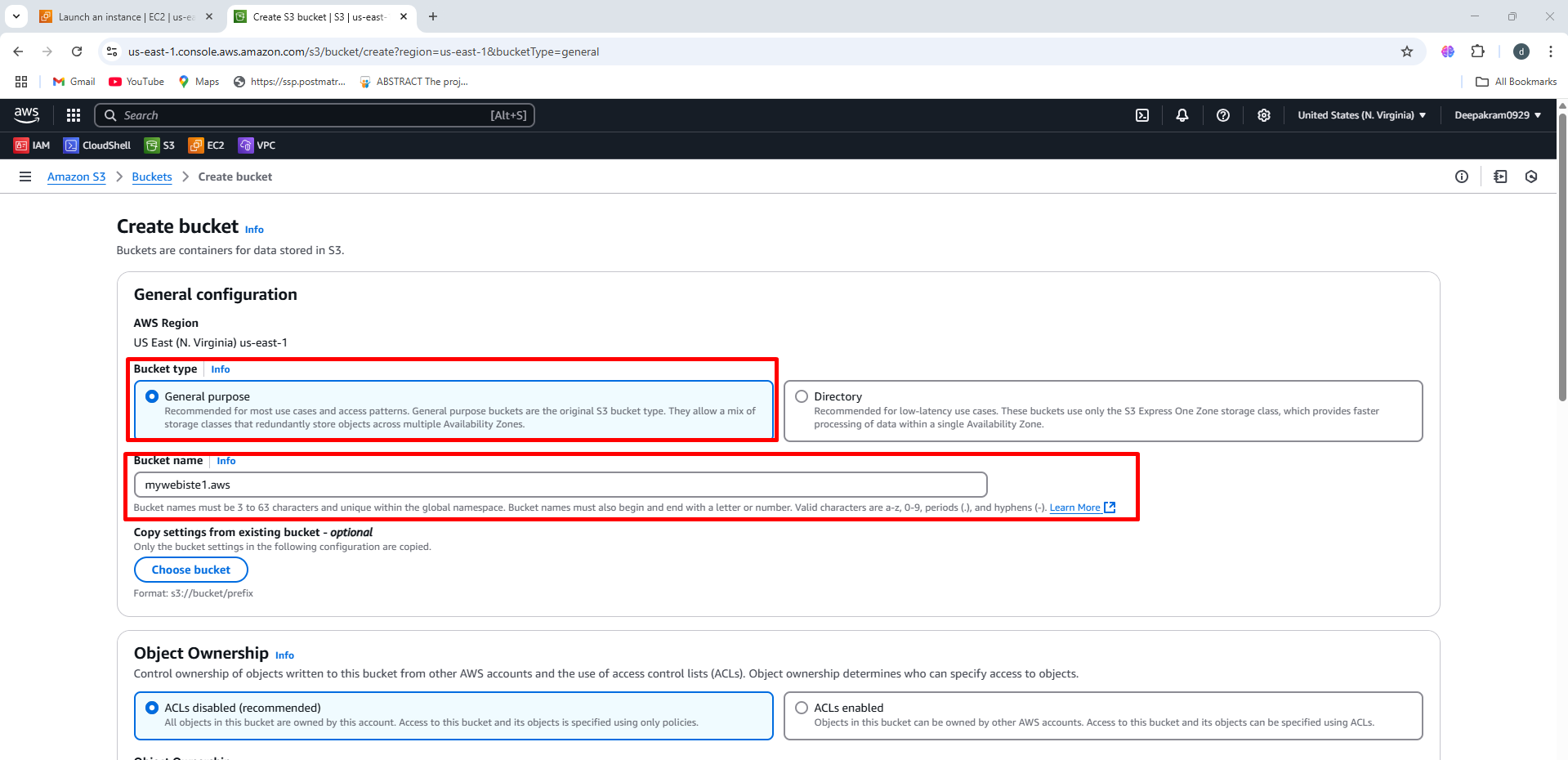
**S3 BUCKETS**

1. Click **Create bucket** 🡪 **General-Purpose**

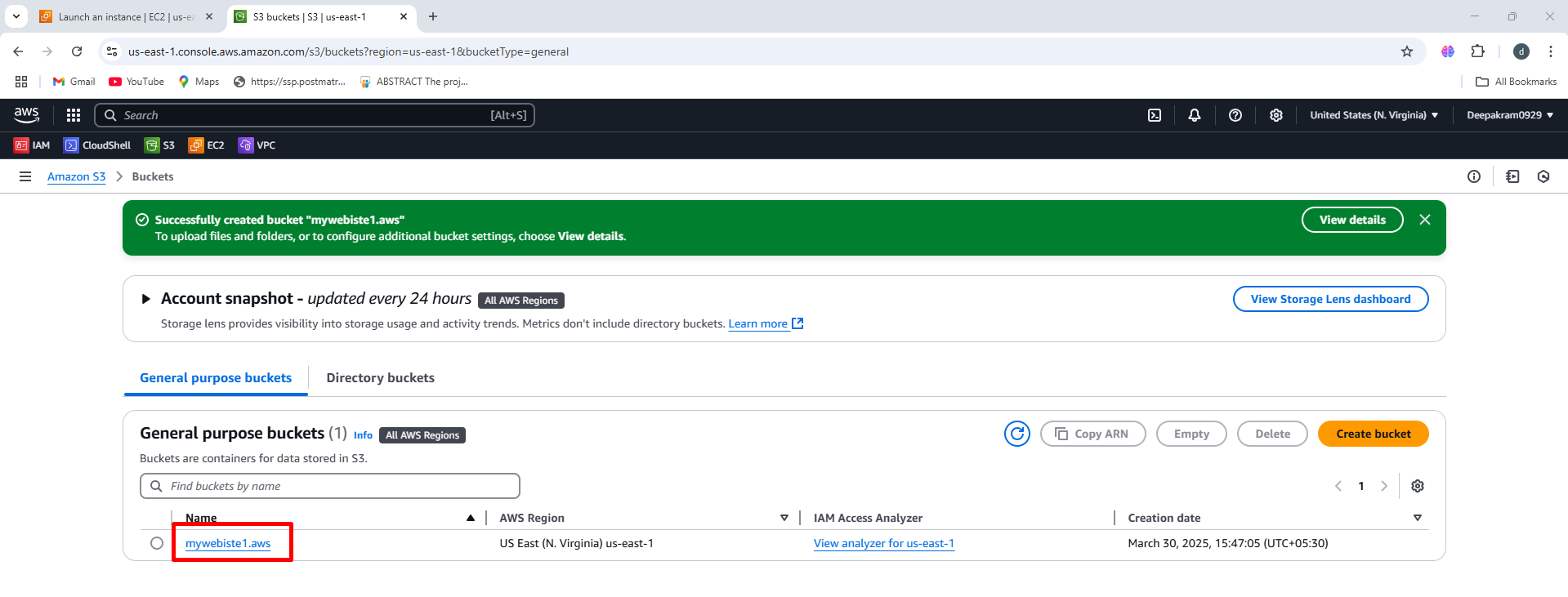
A **general-purpose S3 bucket** is typically used for storing files, images, backups, logs, or application data. It uses the **S3 Standard** storage class by default, providing high durability, availability, and low latency.



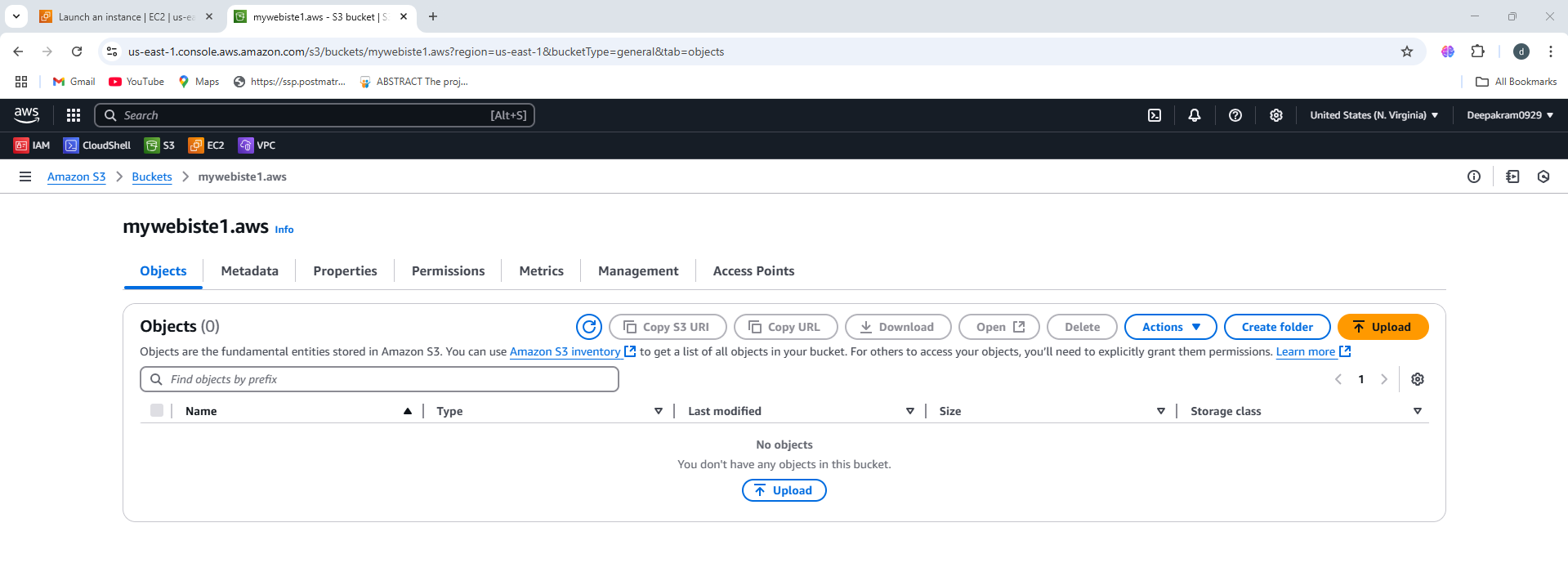
1. Enter a **unique bucket name**

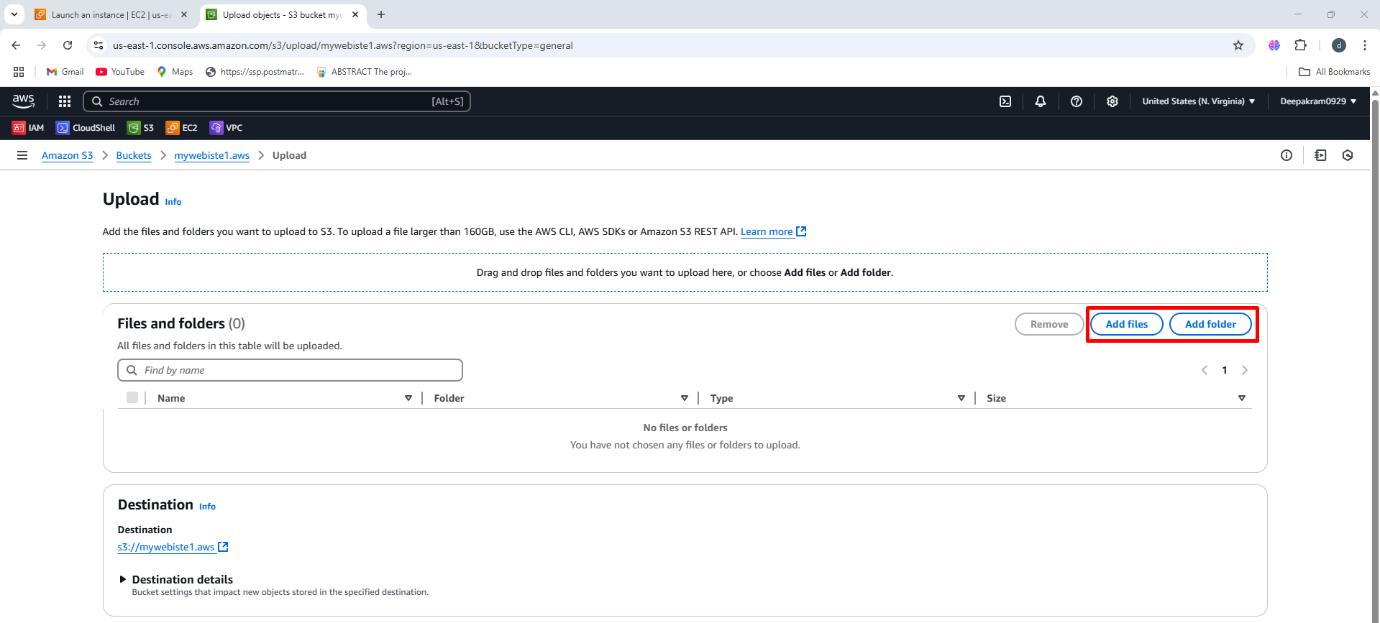


1. Mywebsite1.aws bucket as been created successfully

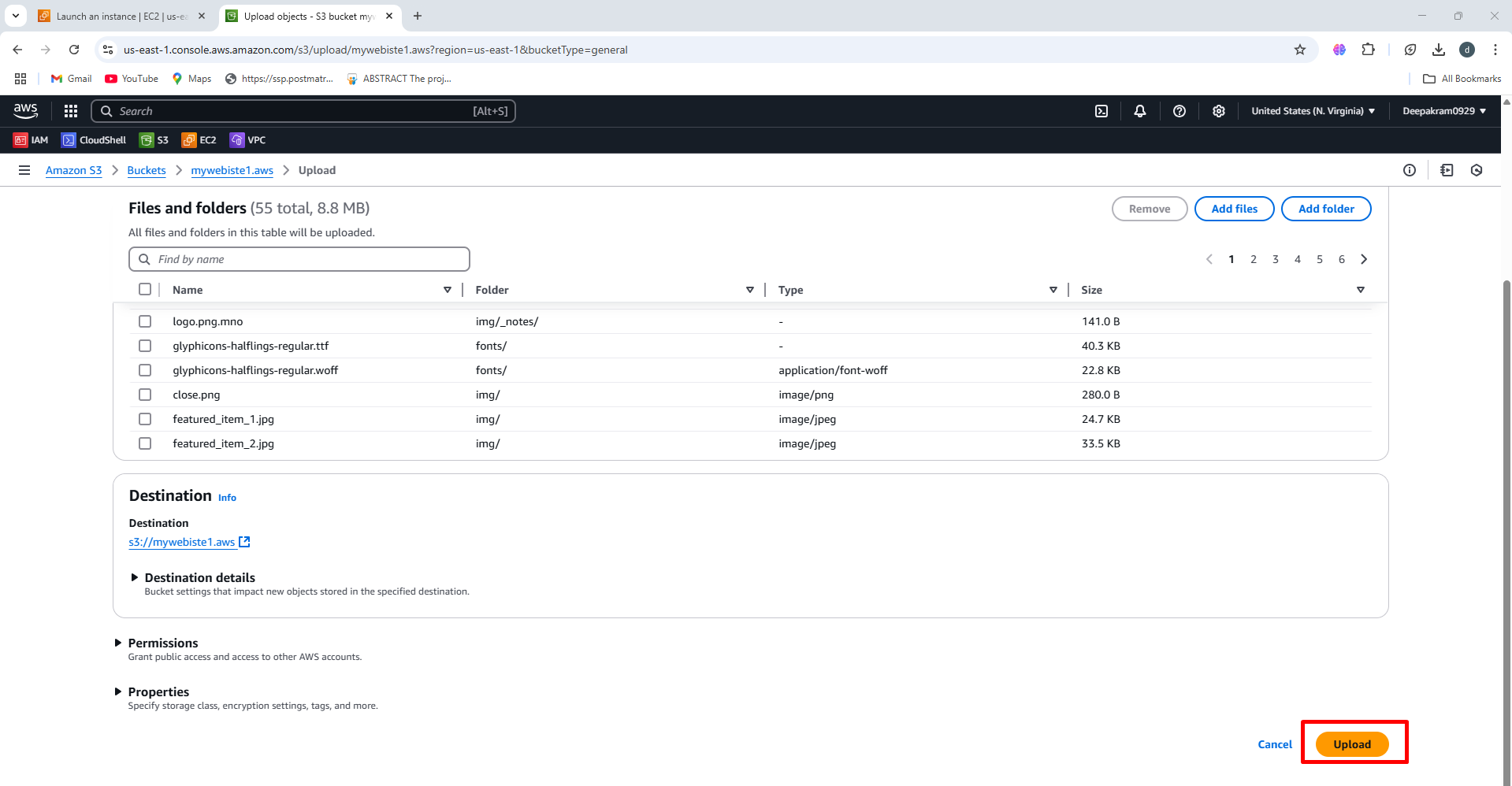


1. No Objects Present, The bucket is empty (no files uploaded yet) 🡪 Clicking **"Upload"** allows you to add files or folders to the S3 bucket.

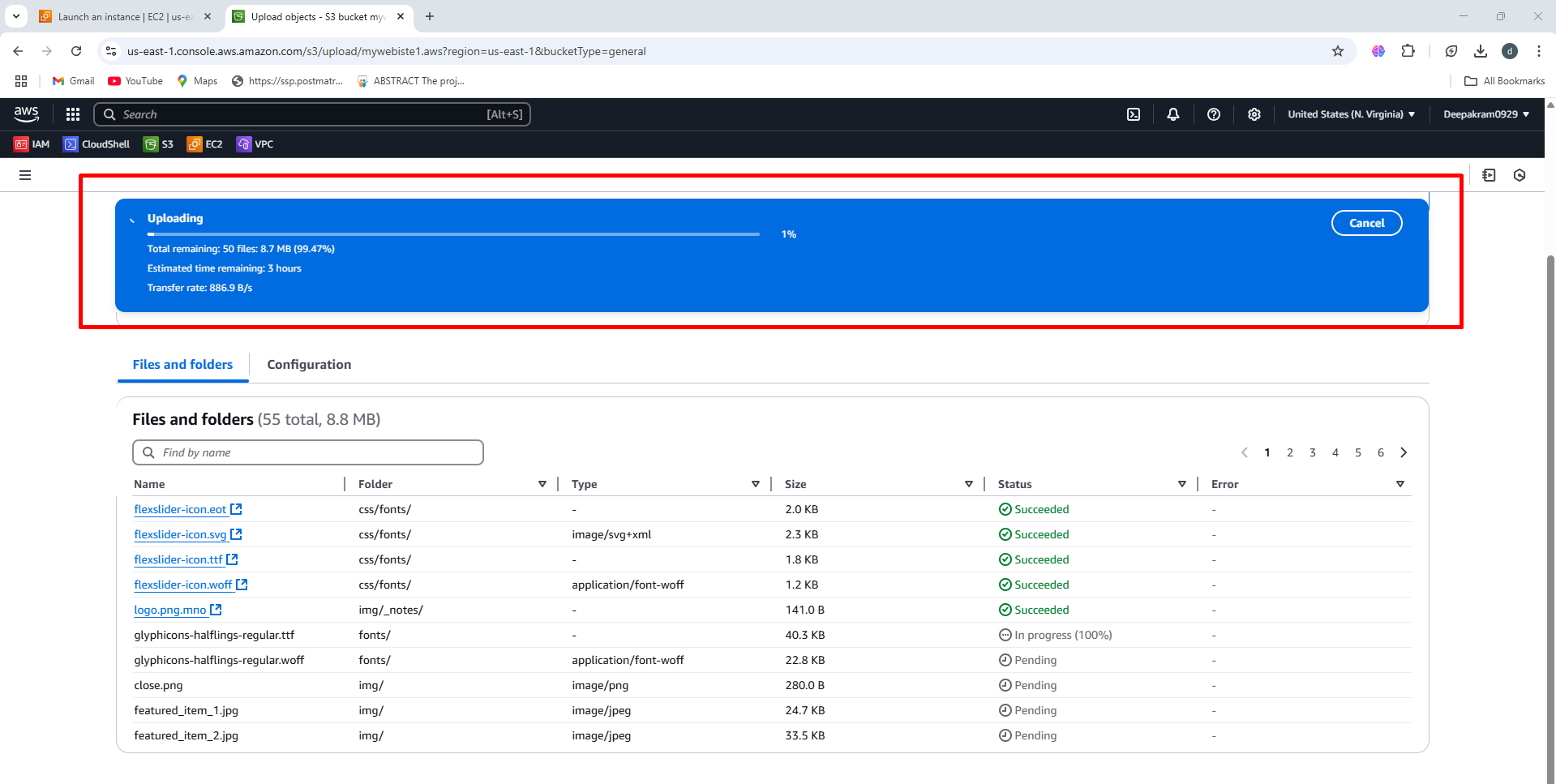




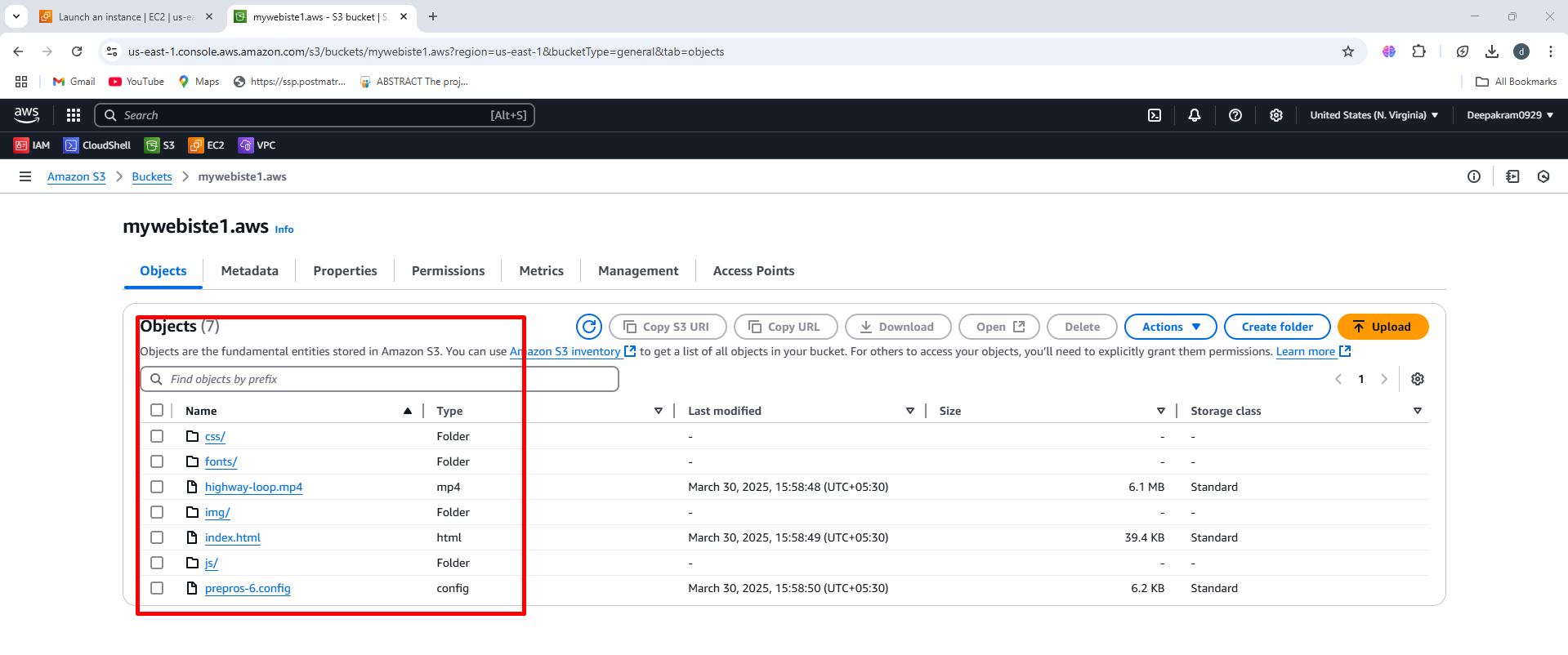
1. After adding files or folder click on upload



1. File as been uploading as shown in below figure



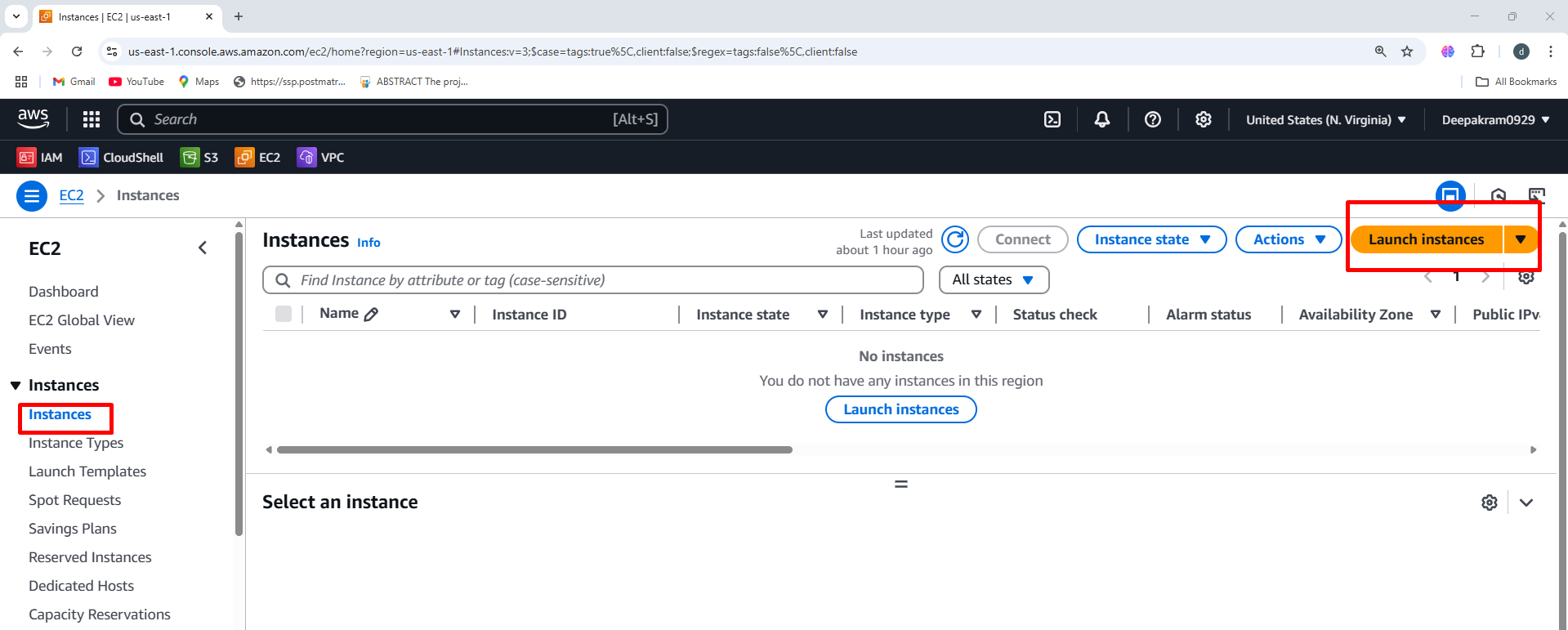
1. We can see the uploaded files in the bucket



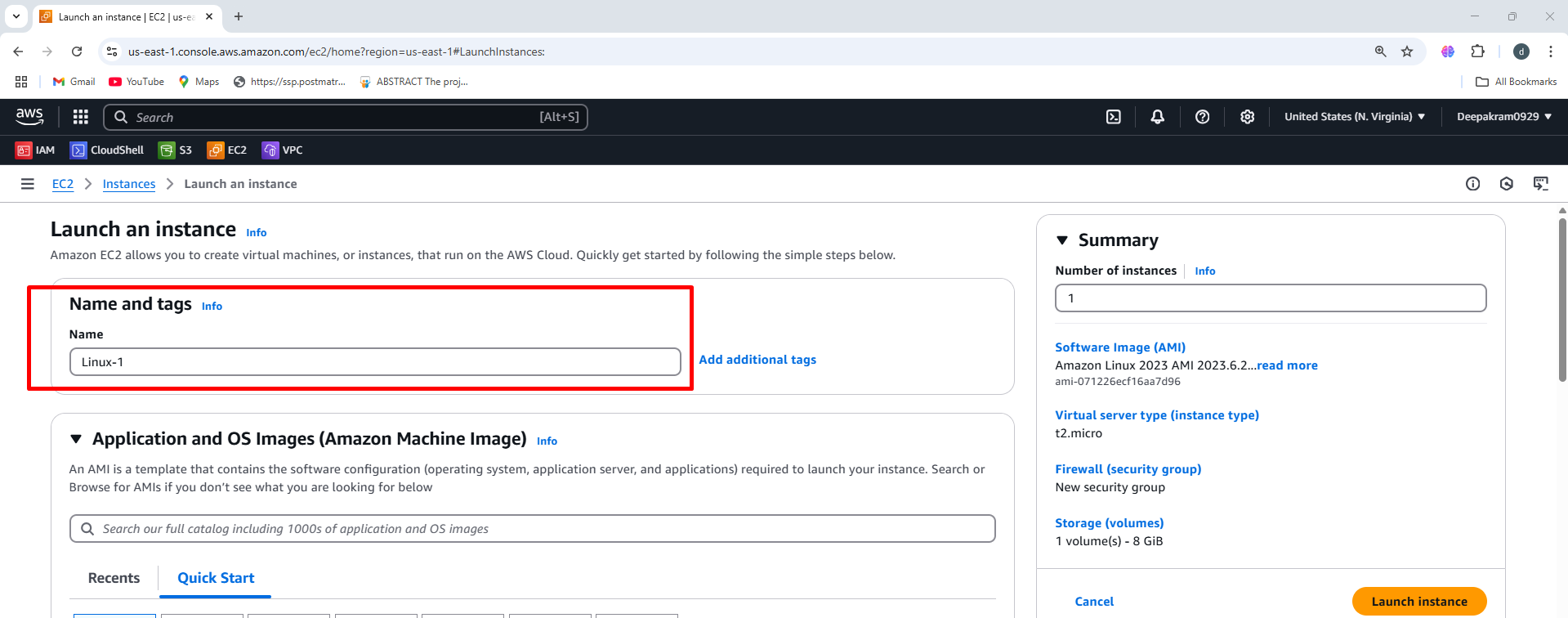
**Launch EC2 instance inside the created VPC**

Ec2 🡪 Launch ec2 🡪 Name 🡪 AMI 🡪 instance type 🡪 keypair 🡪 network setting (edit) 🡪 select VPC 🡪 Select VPC 🡪 Select subnet 🡪 enable auto assign public IP 🡪 create 🡪 security group 🡪 Launch EC2 instance

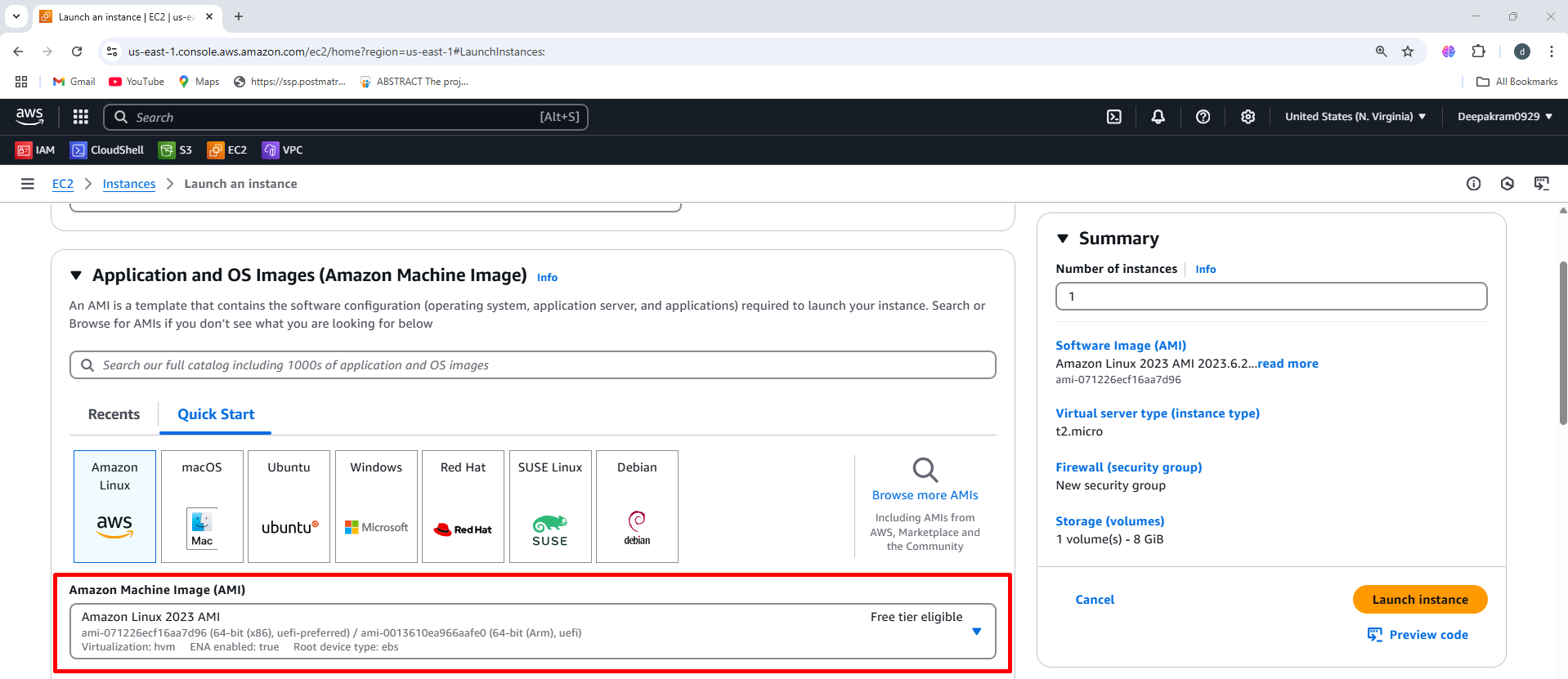
1. Instances 🡪 launch instances



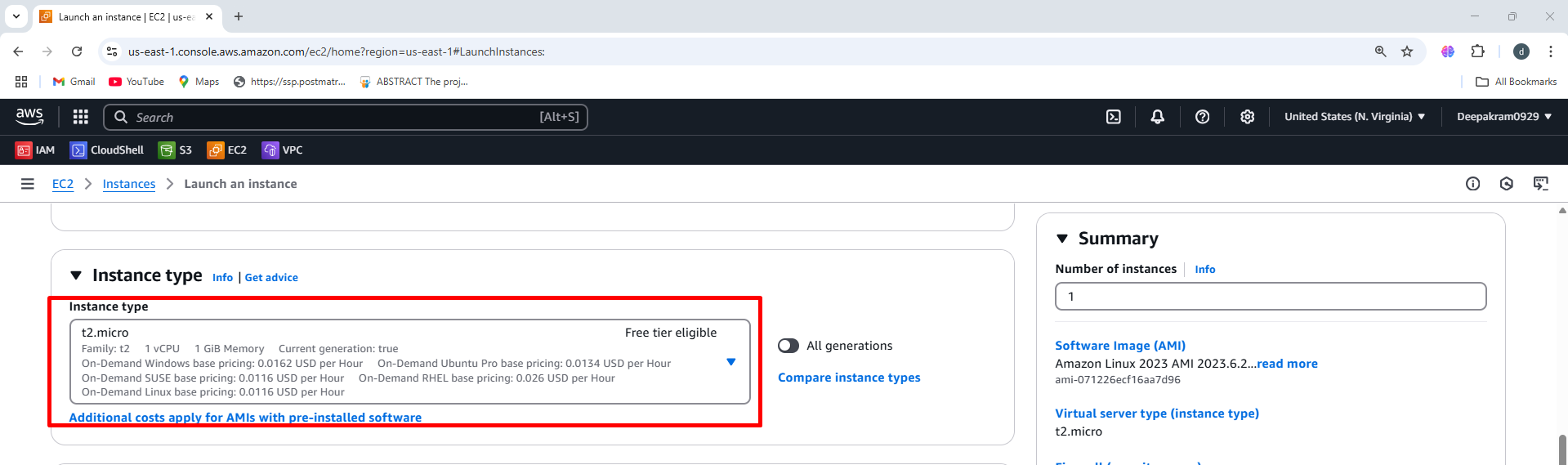
1. Enter instance name



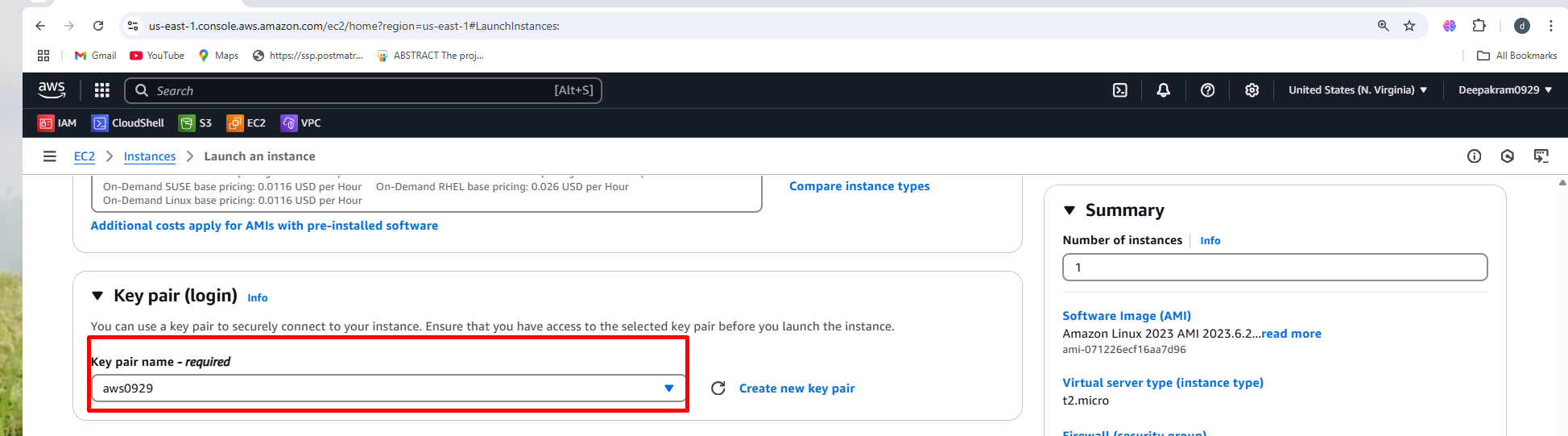
1. Choose the AMI



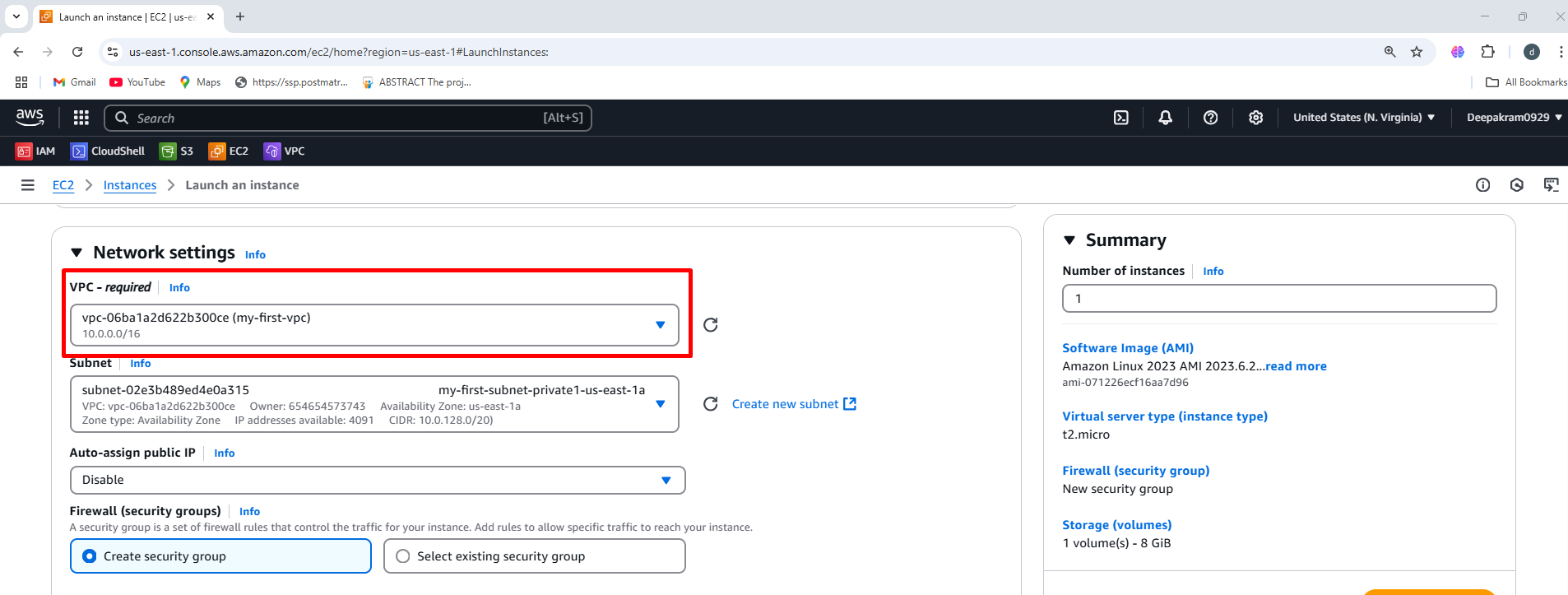
1. Select the instance type 🡪 t2.micro



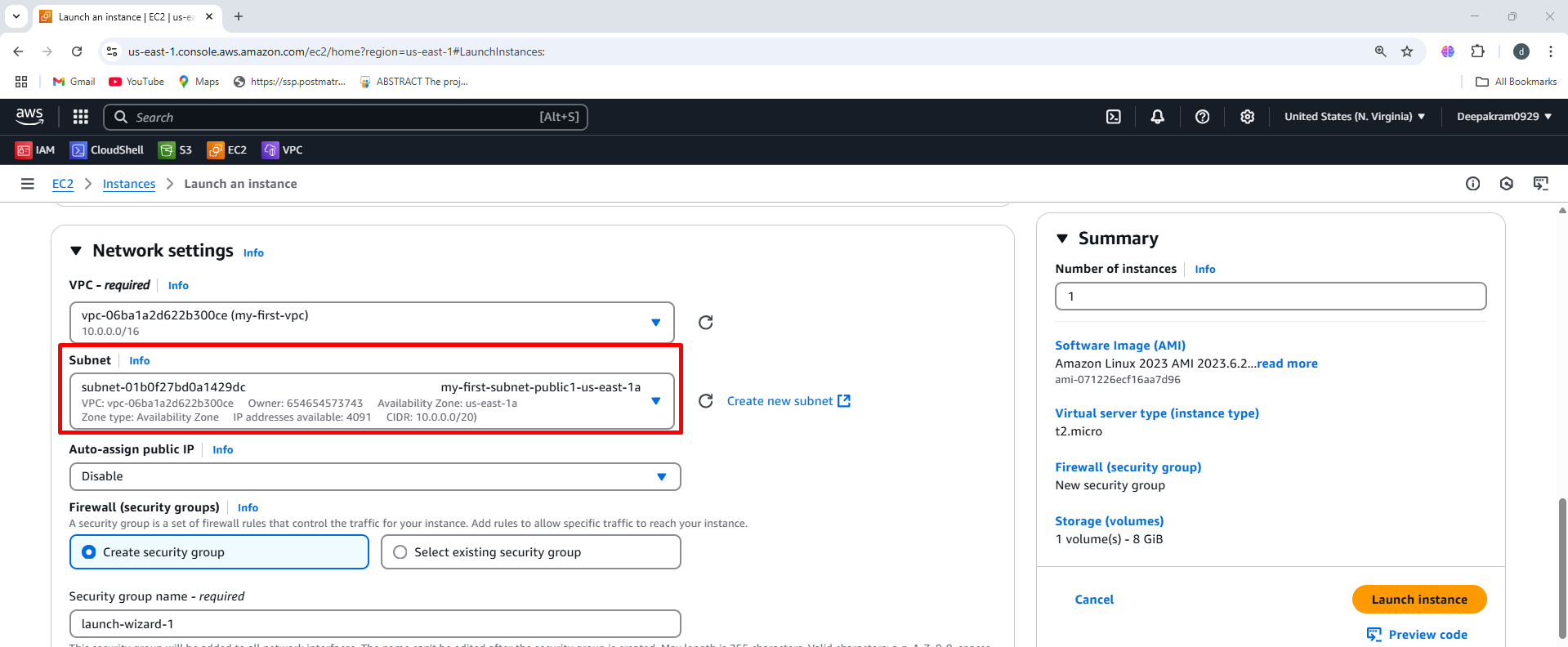
1. Select the keypair



1. Select custom VPC 🡪 my-first-vpc

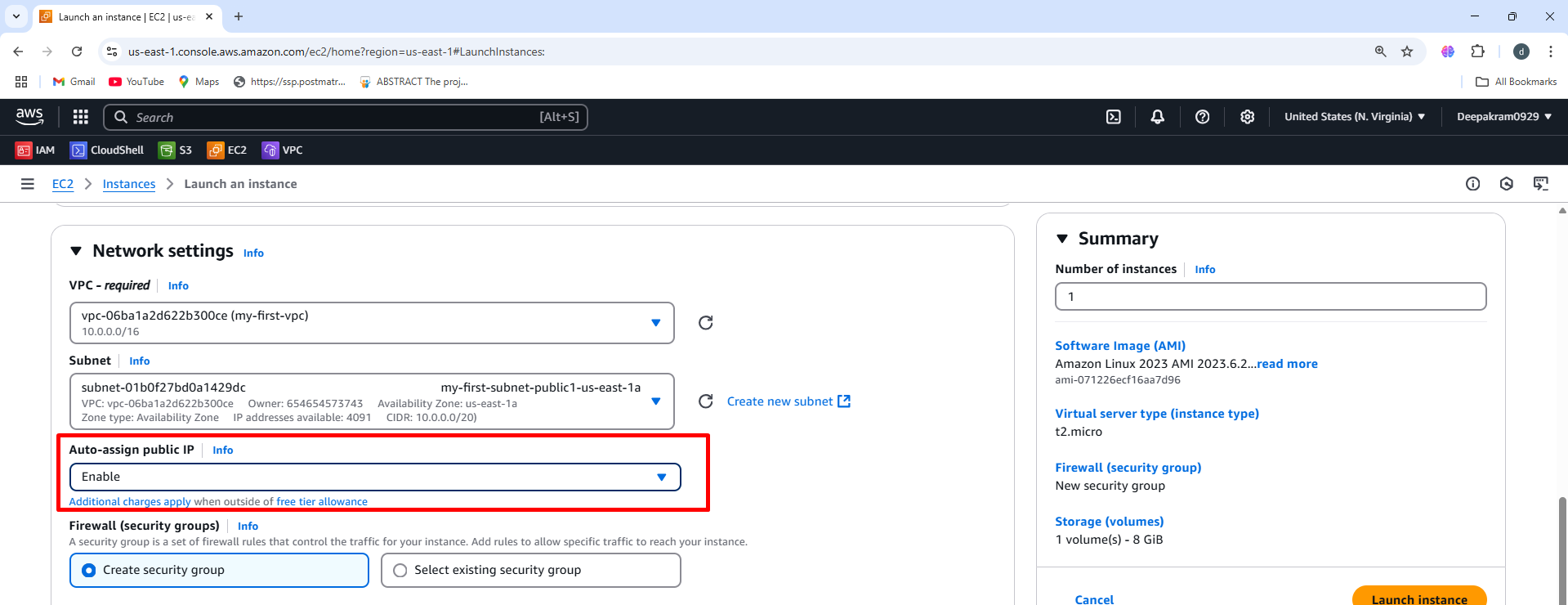


1. Choose subnets 🡪 subnet-public1- us-east-1a

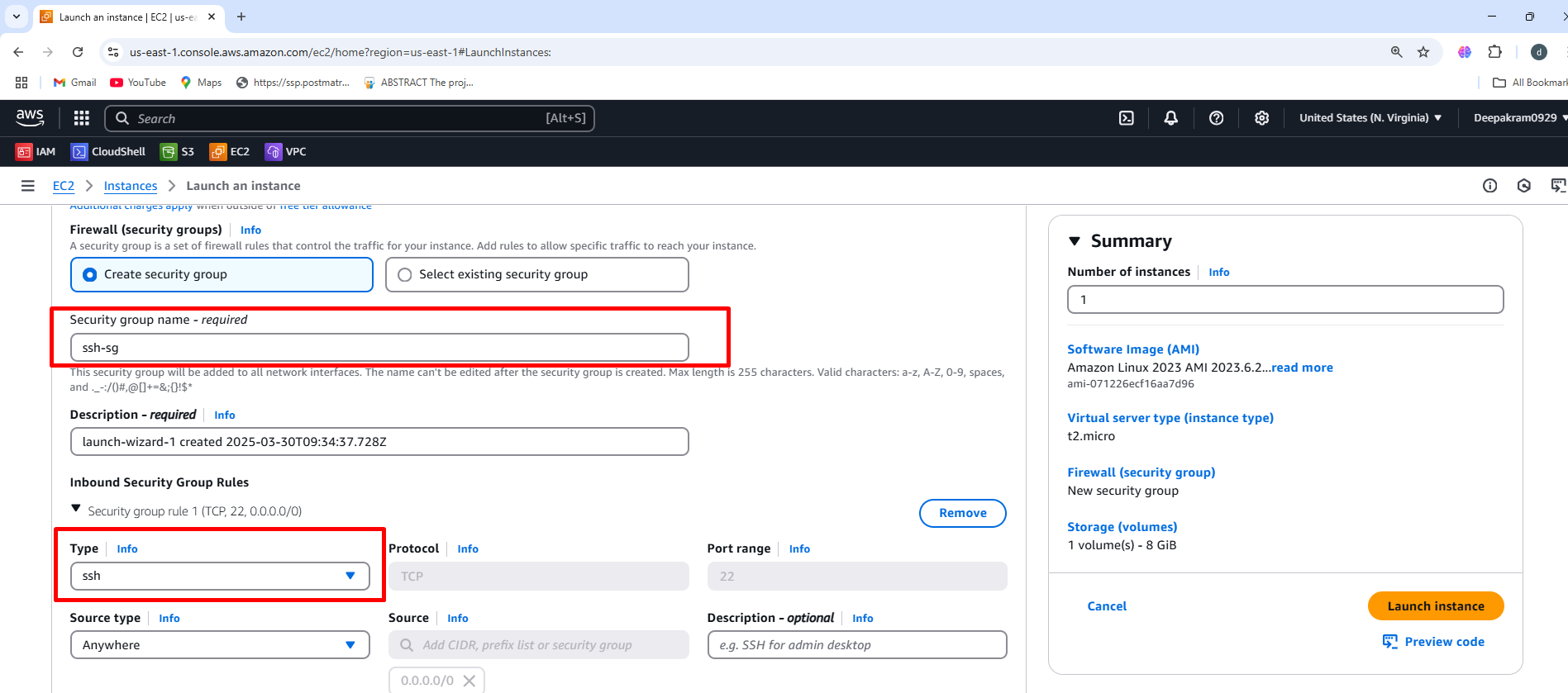


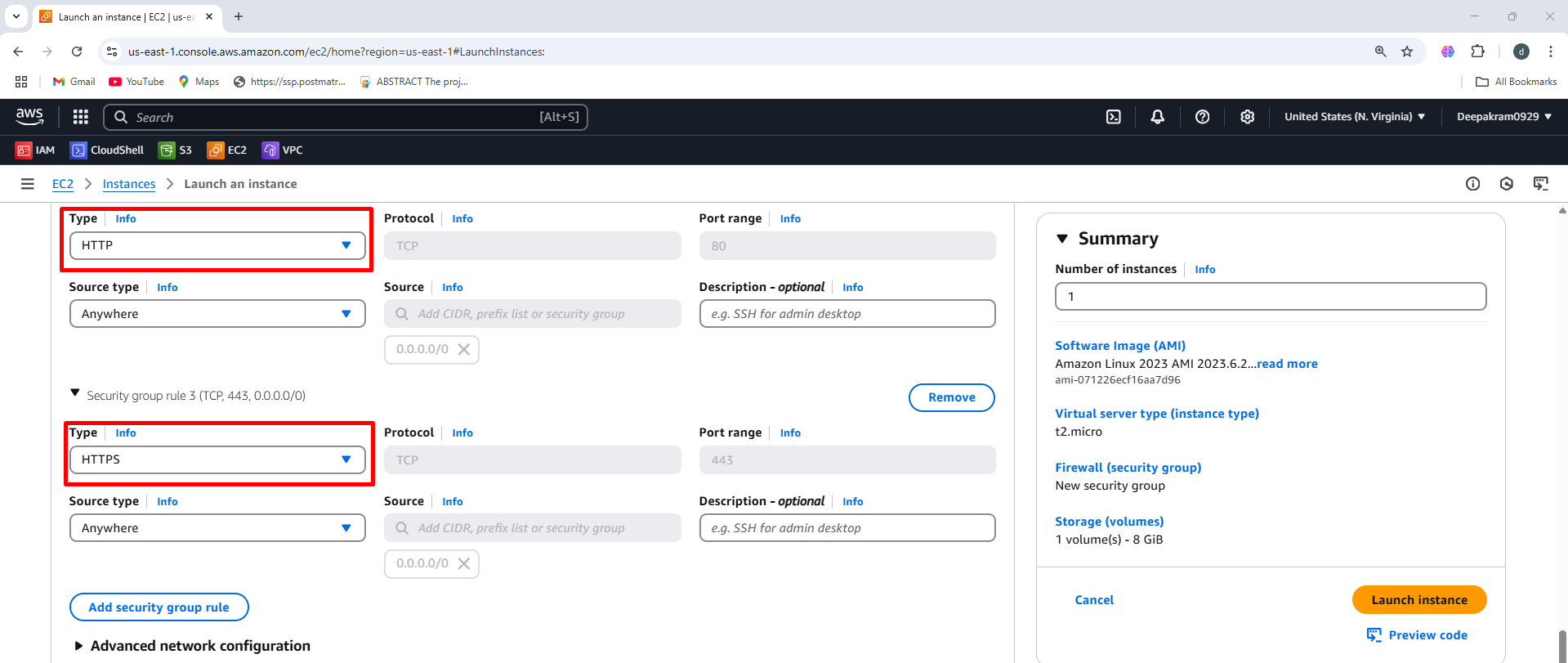
1. Enable public IP

when an instance needs direct internet access for updates, APIs, or public-facing applications for security and persistence, use Elastic IPs or NAT Gateways when necessary. Always secure access with Security Groups and prefer AWS Session Manager over SSH.

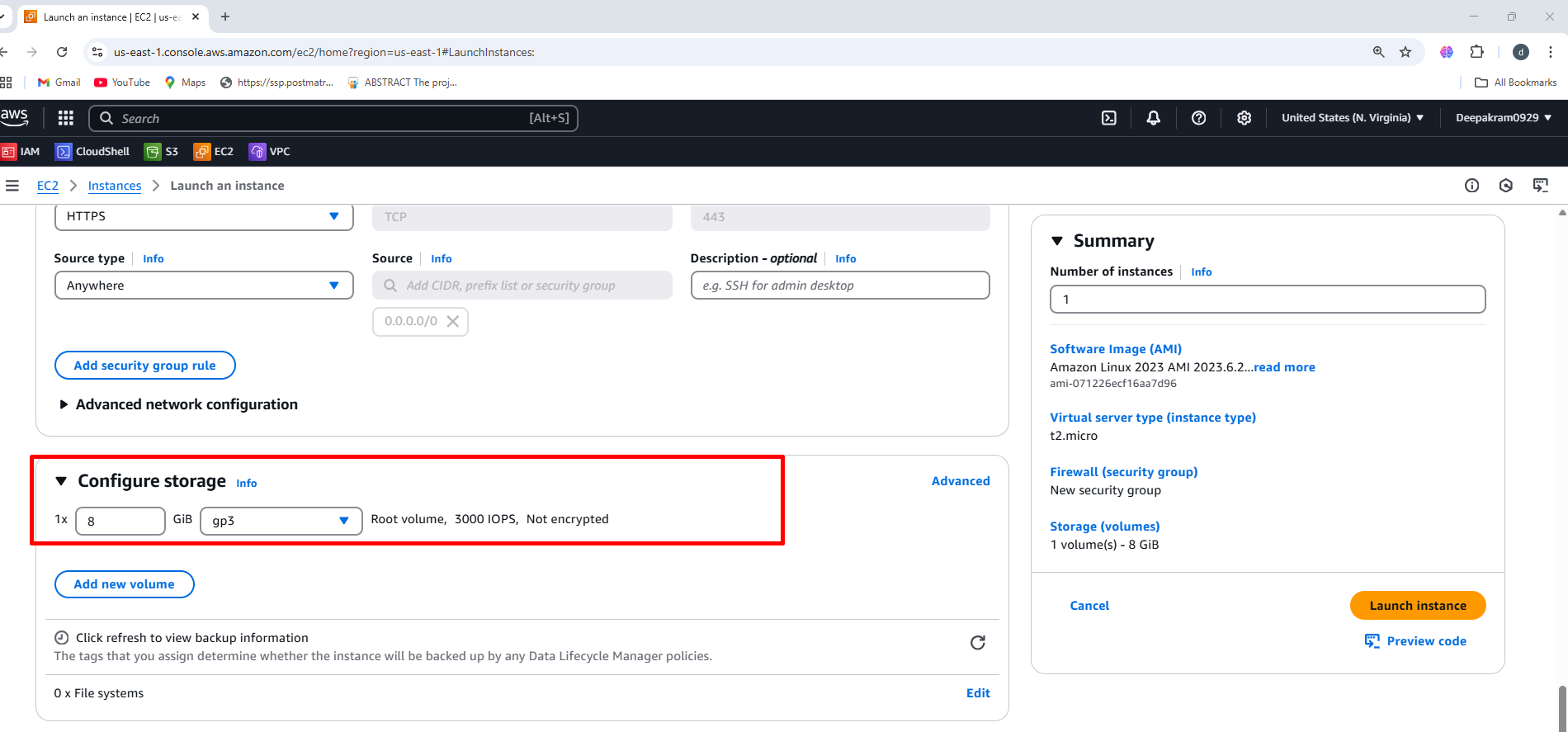


1. Create security group 🡪 Name 🡪 Inbound rules

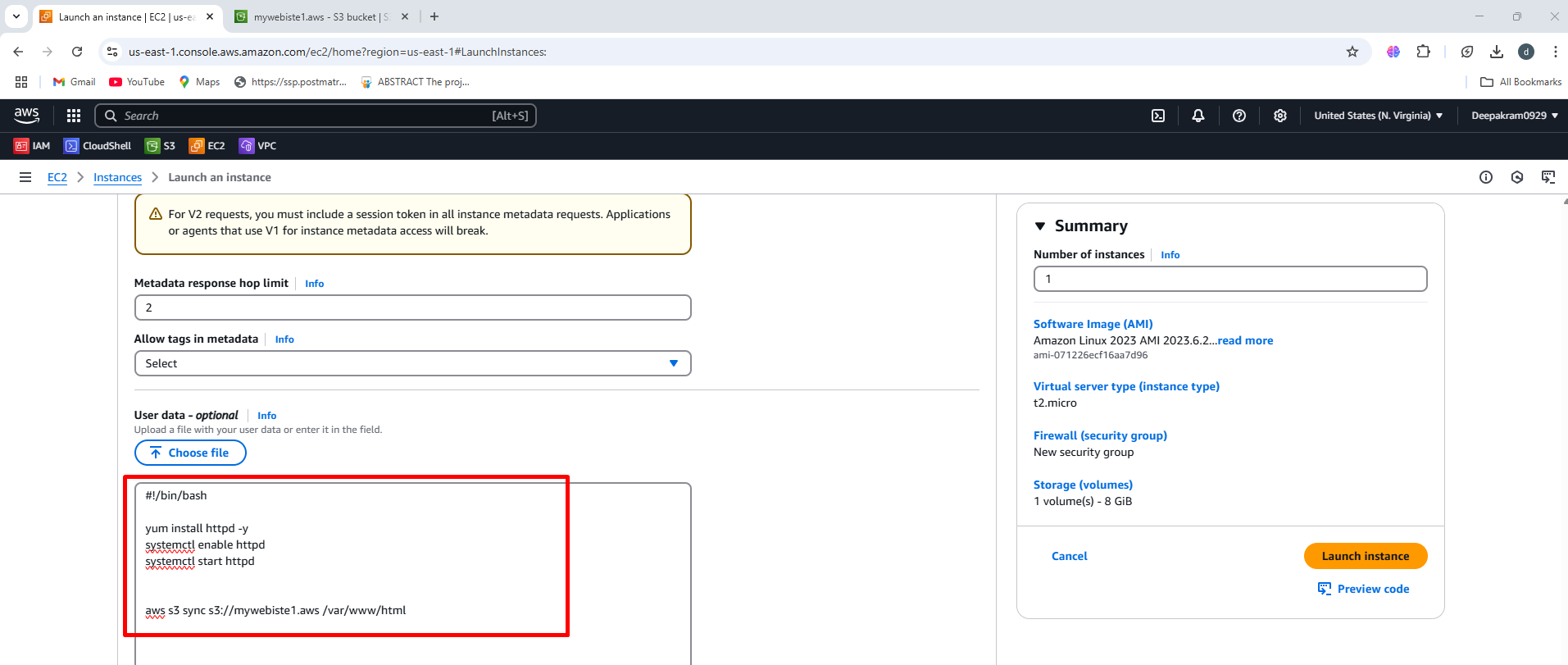


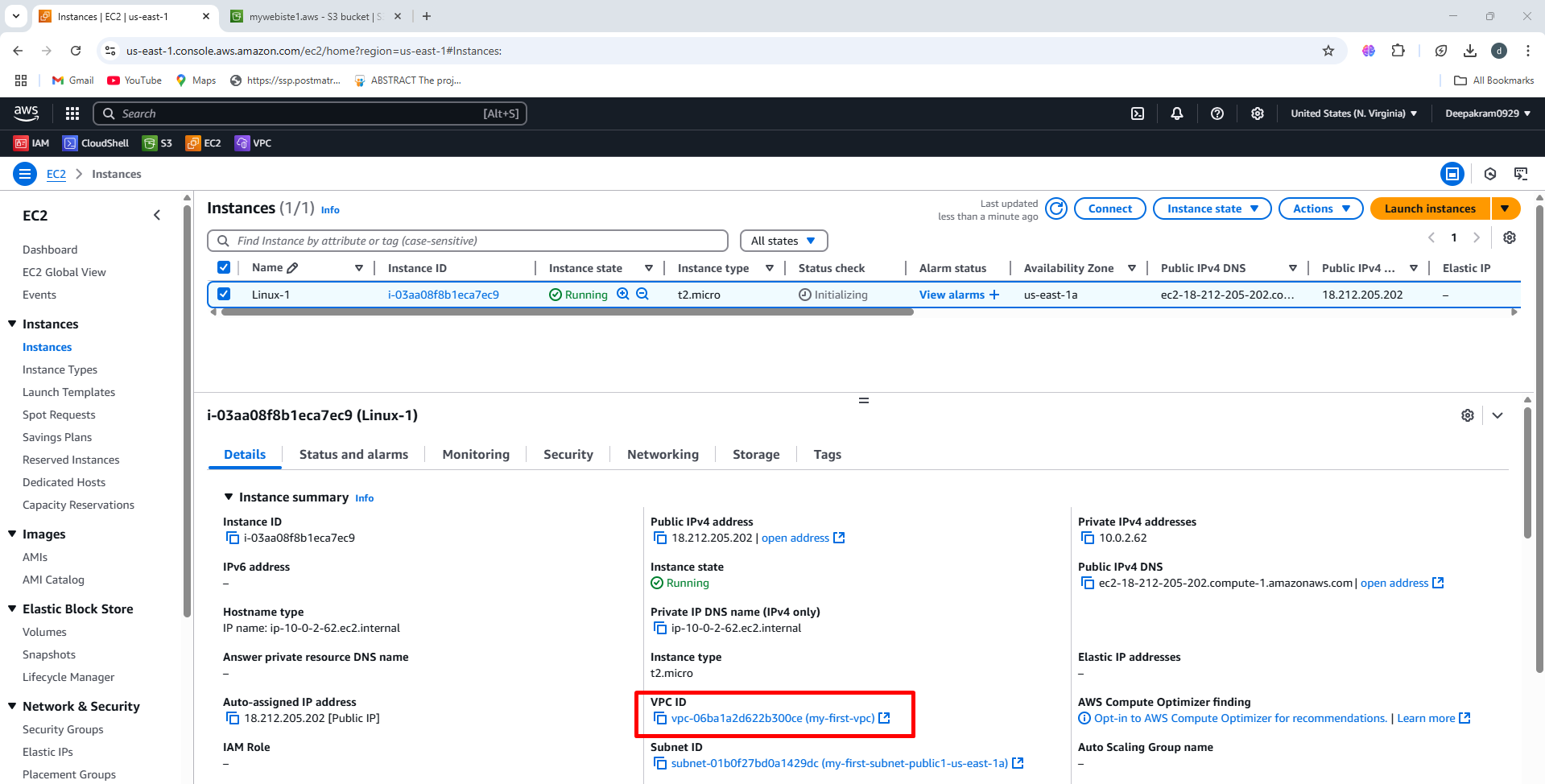


1. Select the volume size



1. Launching EC2 instance using user data to the existing S3 bucket

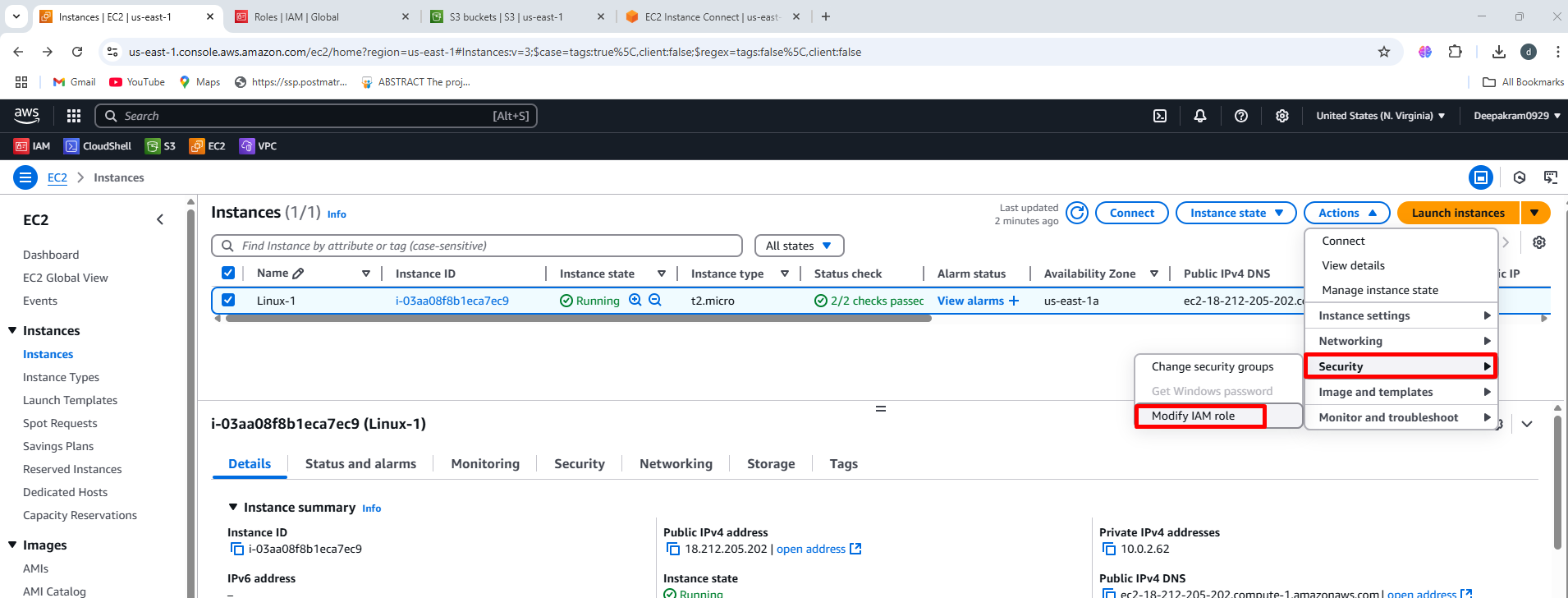




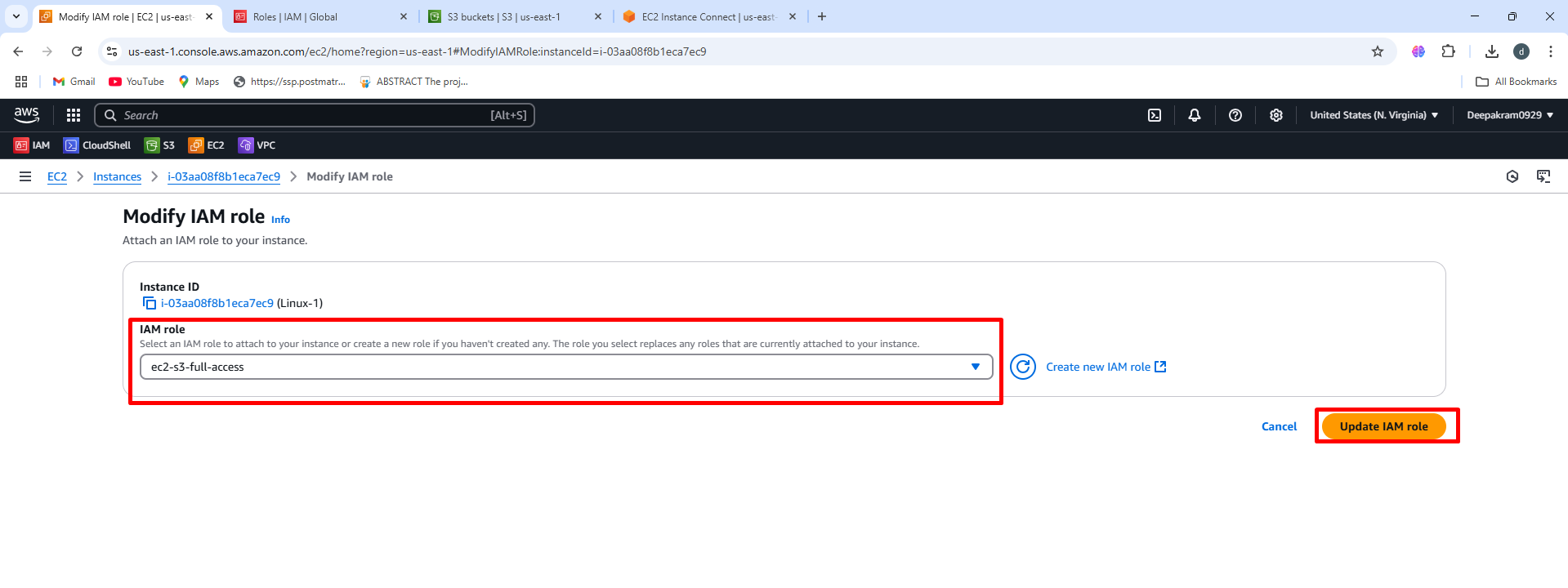
**TO ADD IAM ROLES AND POLICY**

Attaching Existing IAM role

1. Select the instance 🡪 Action 🡪 Security 🡪 Modify IAM role



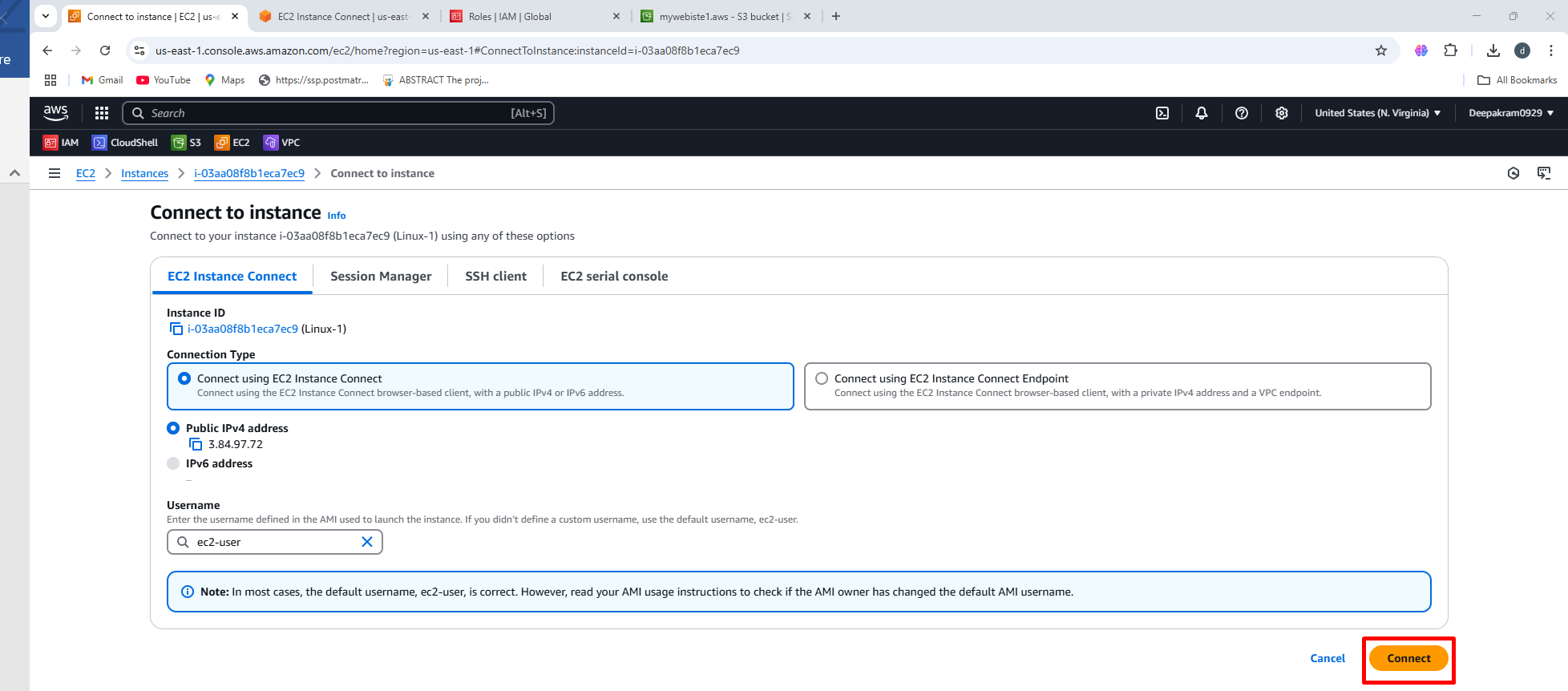
1. Select the IAM role previously created ec2-s2-full-access 🡪 Update IAM



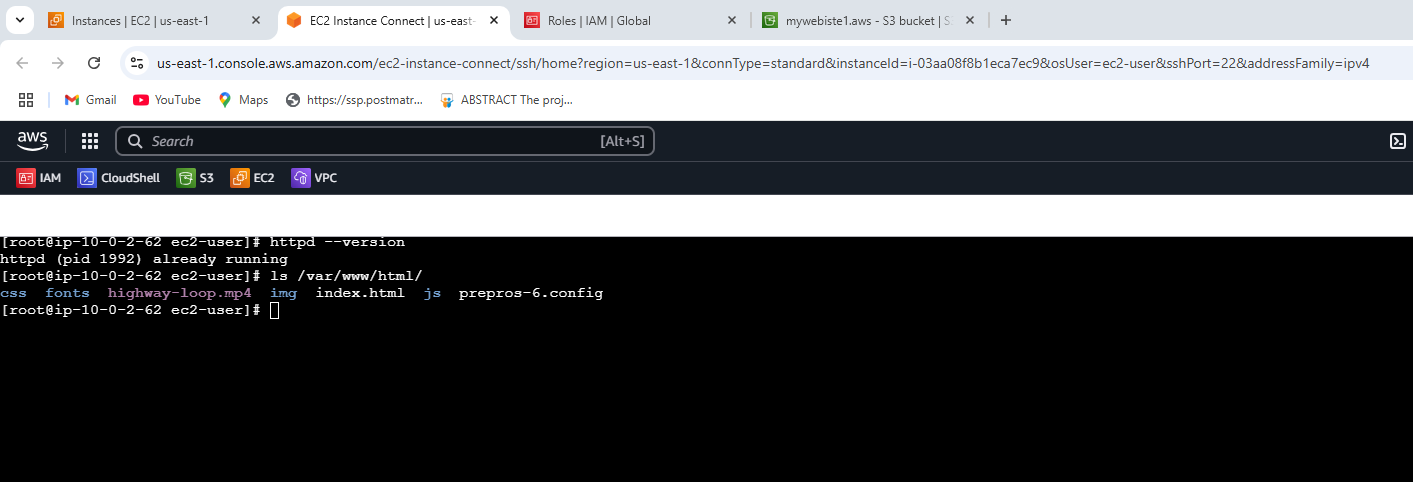
**OUTPUT**

1. To check user data and httpd status

Connect to the EC2 console



1. Check httpd packages are install or not 🡪 Check the file present inside html location



1. Paste public IP 🡪 Output of static webite

