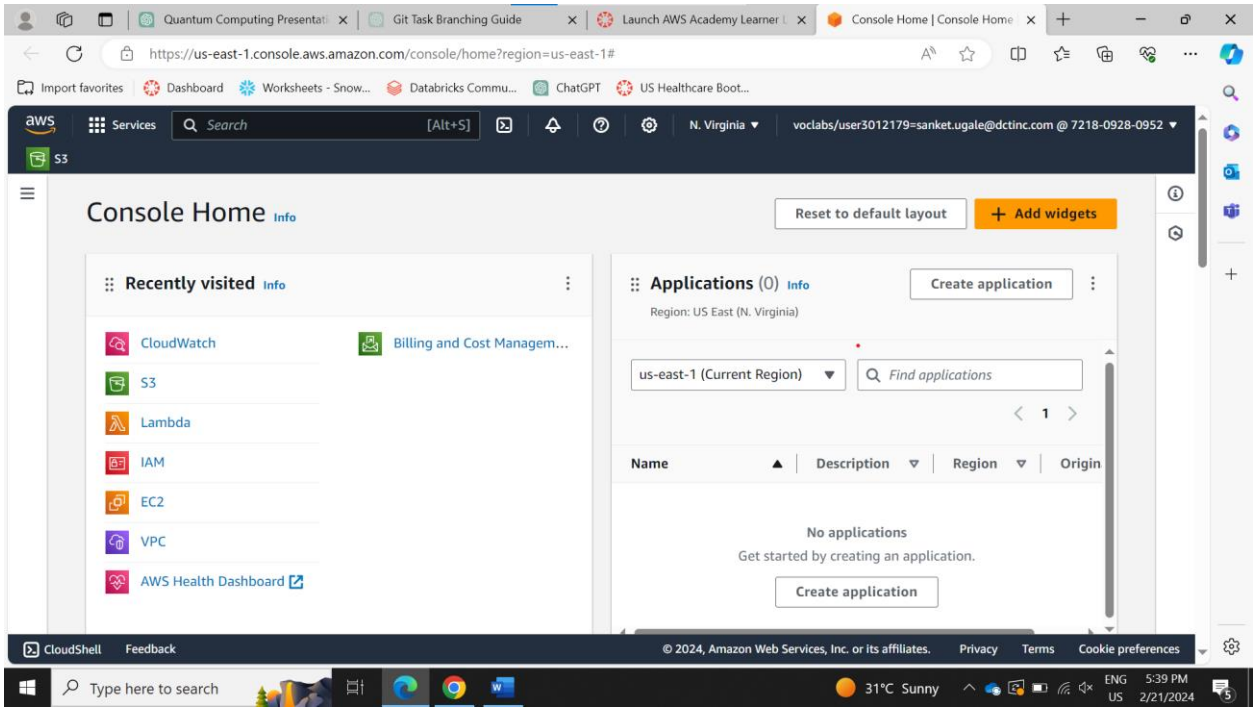
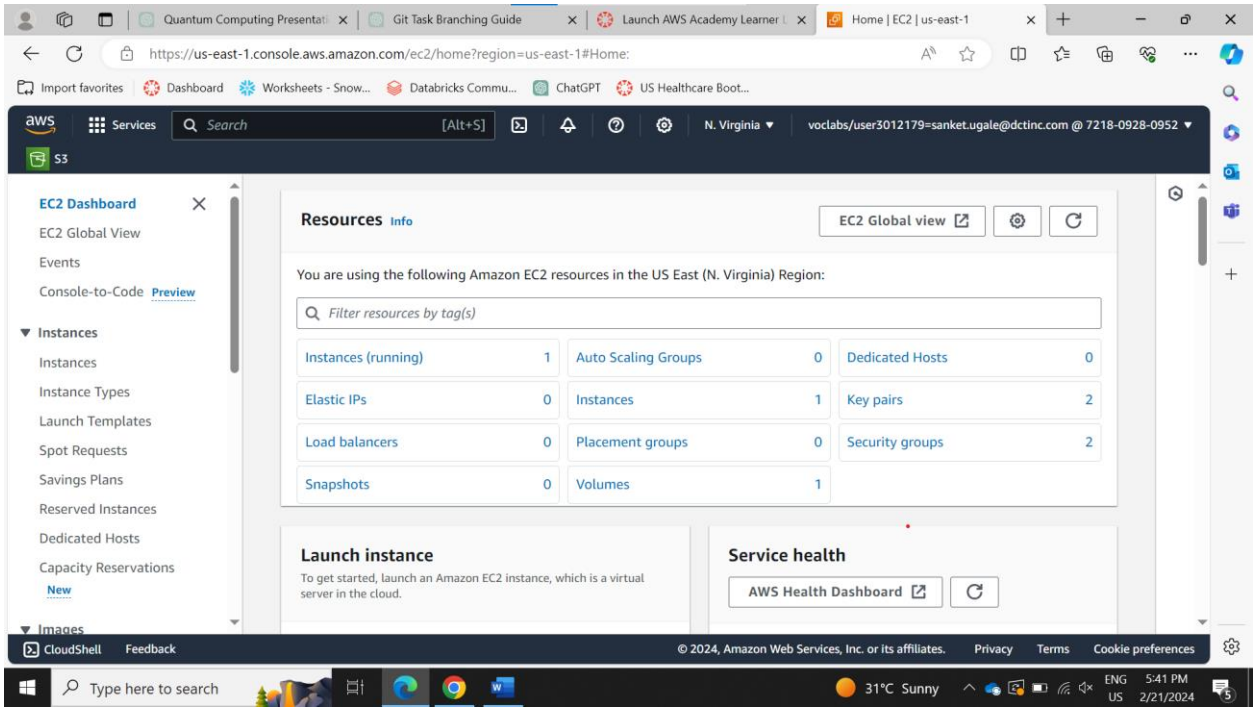
AWS EC2 (Elastic Compute Cloud) Task

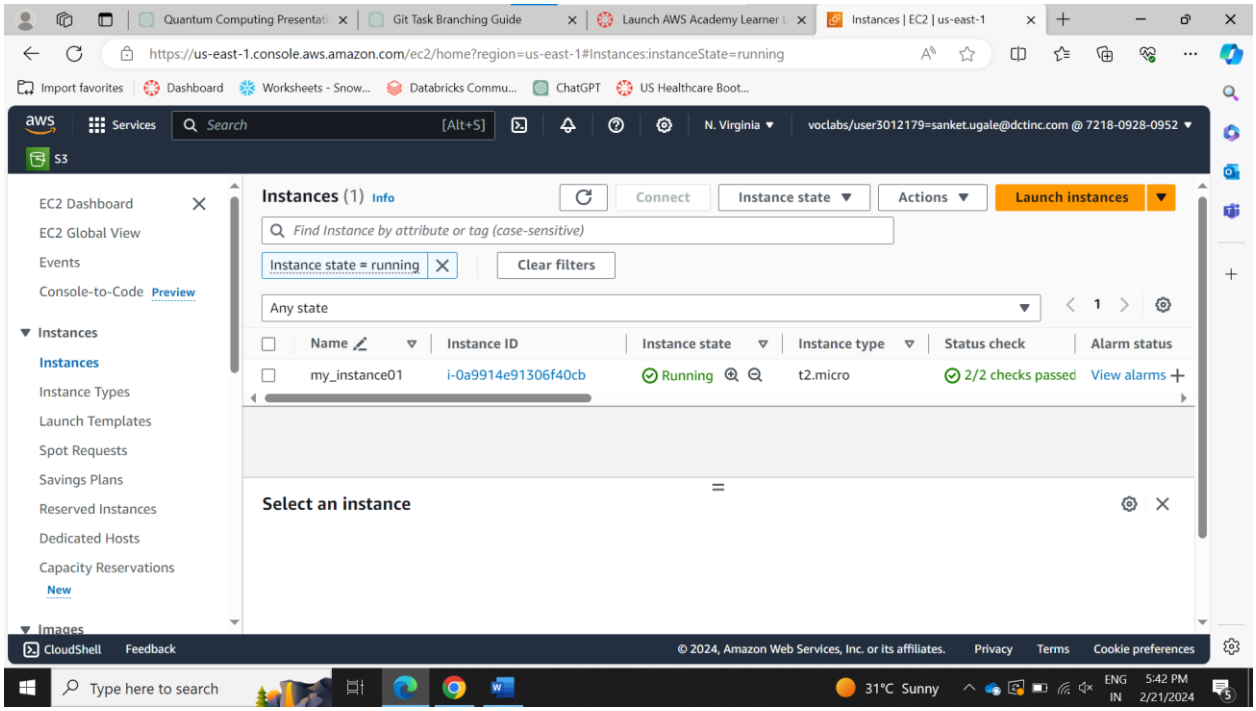
STEP : Open AWS console and go to EC2.



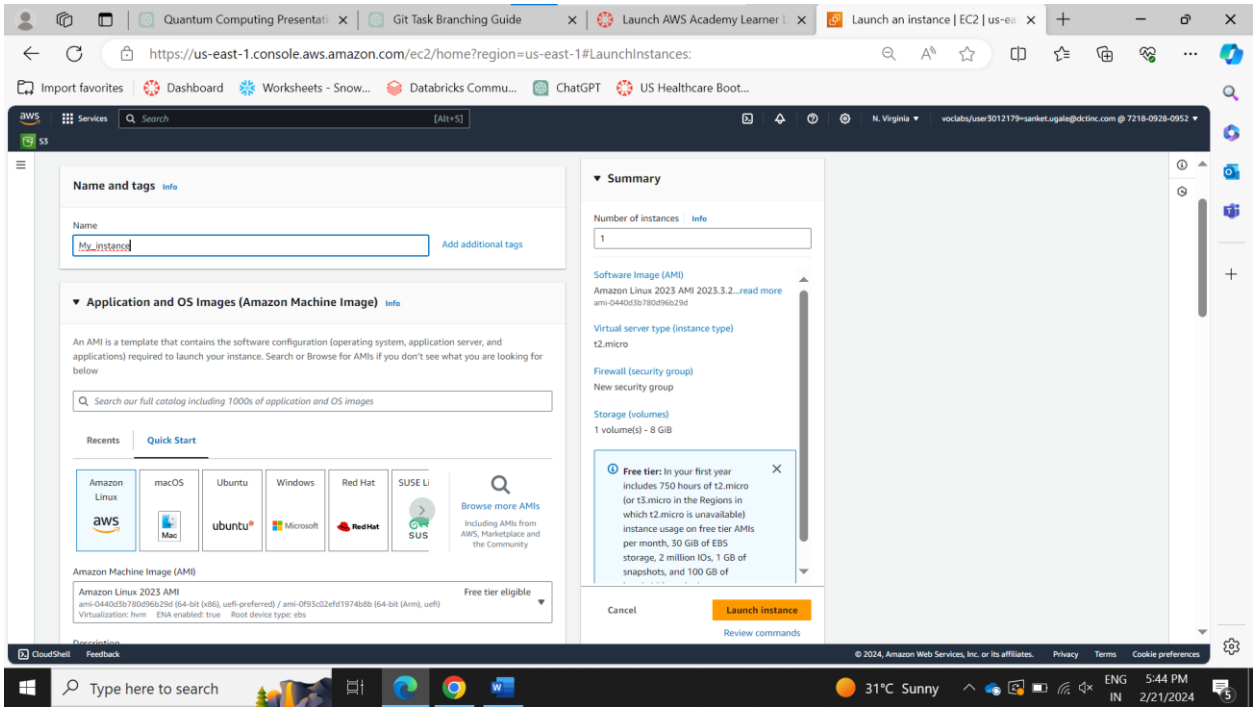
STEP : Click on Instance



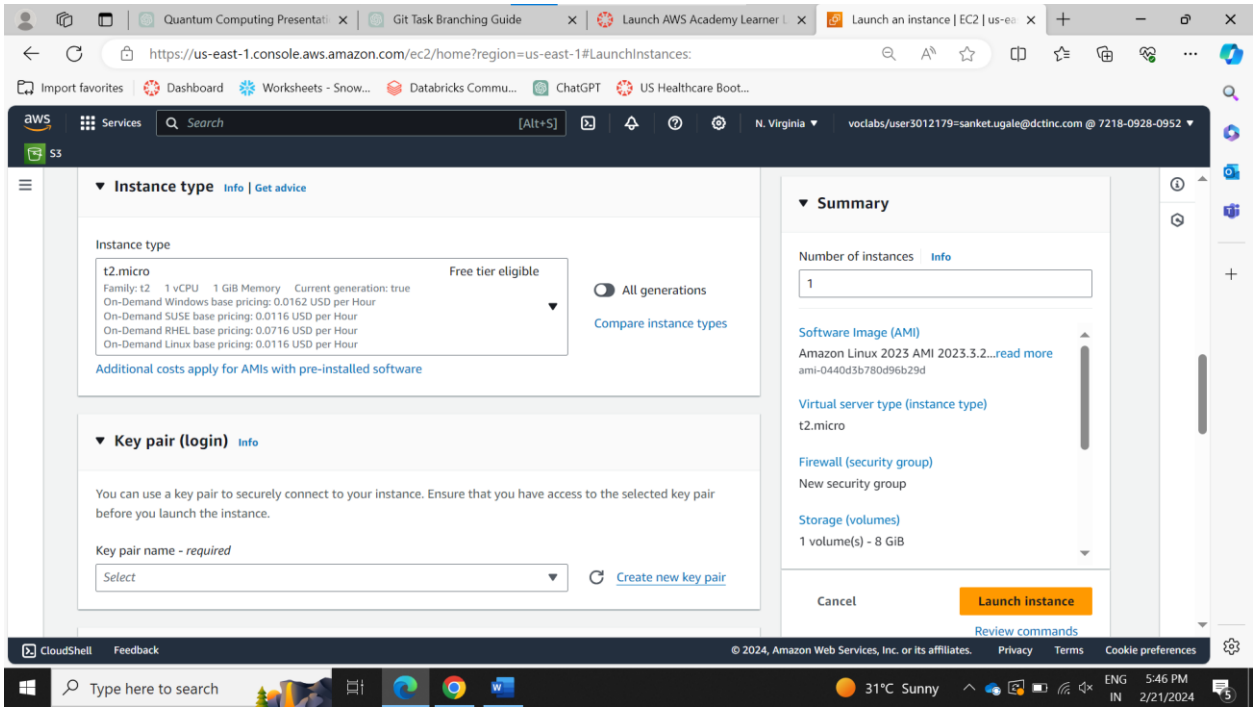
STEP : Click on Launch Instances



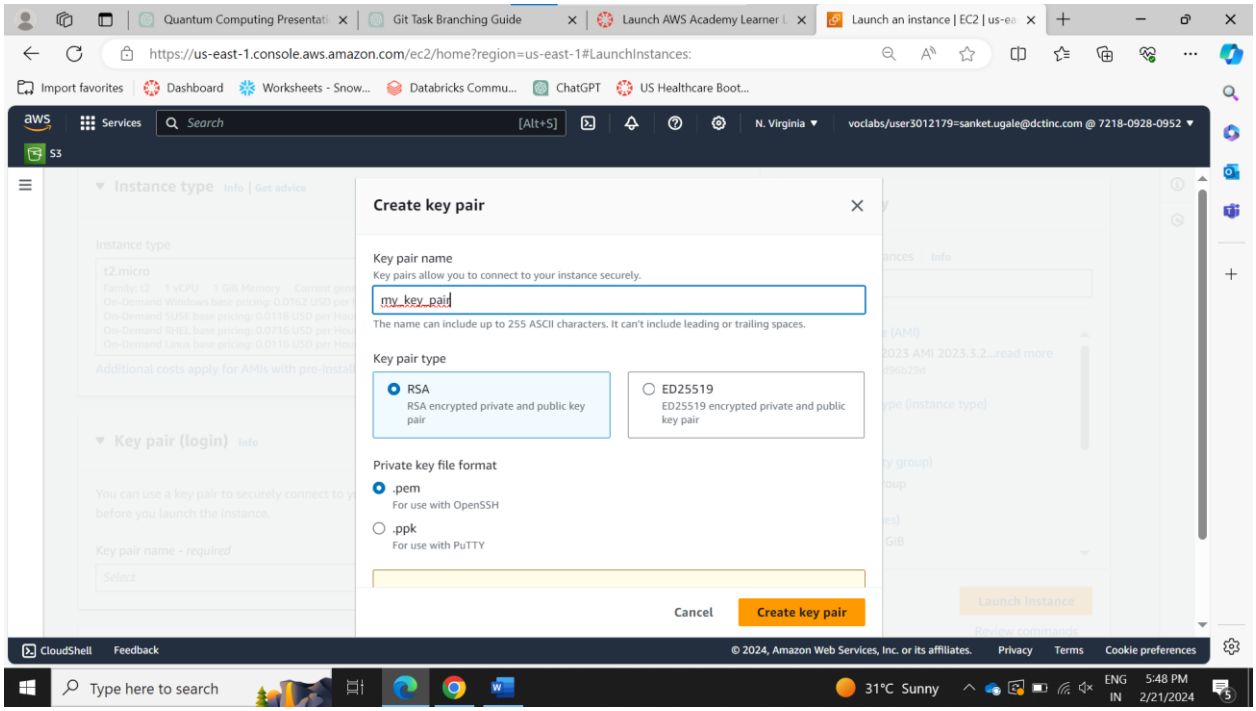
STEP : Give a name to your instance and select the AMI (Amazon Machine Image)



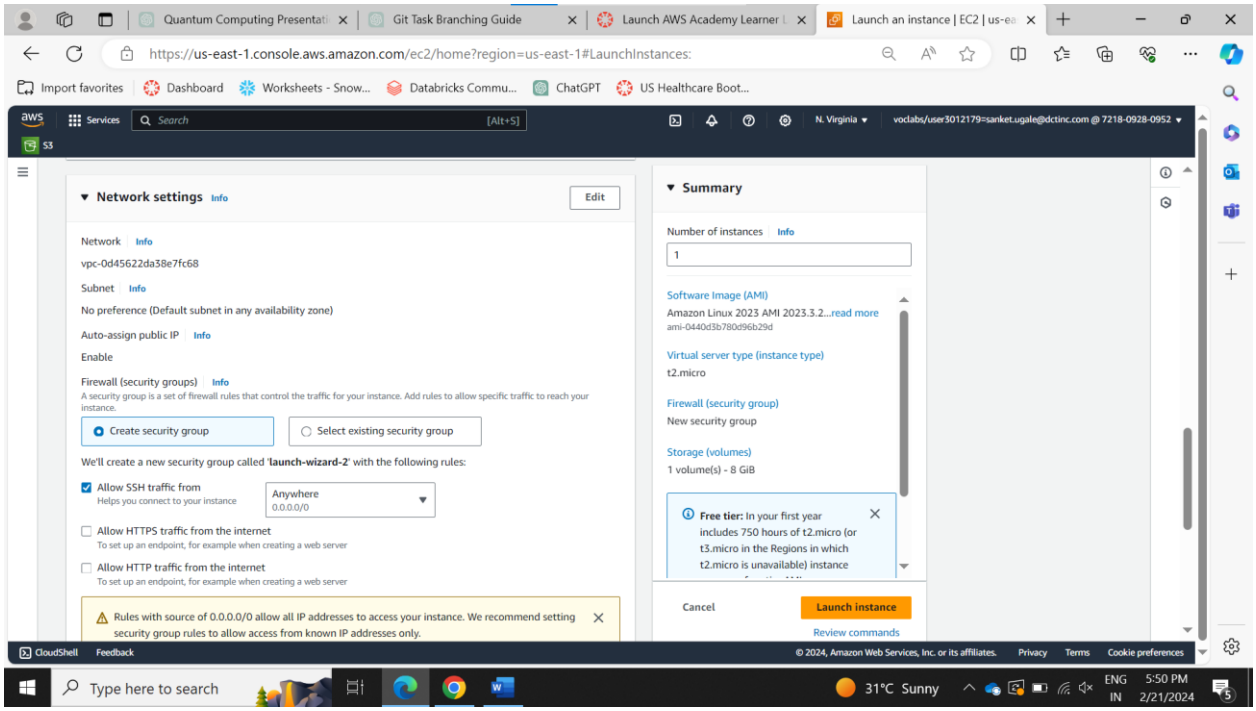
STEP : Select your instance type from the drop down menu and click on the create key pair.



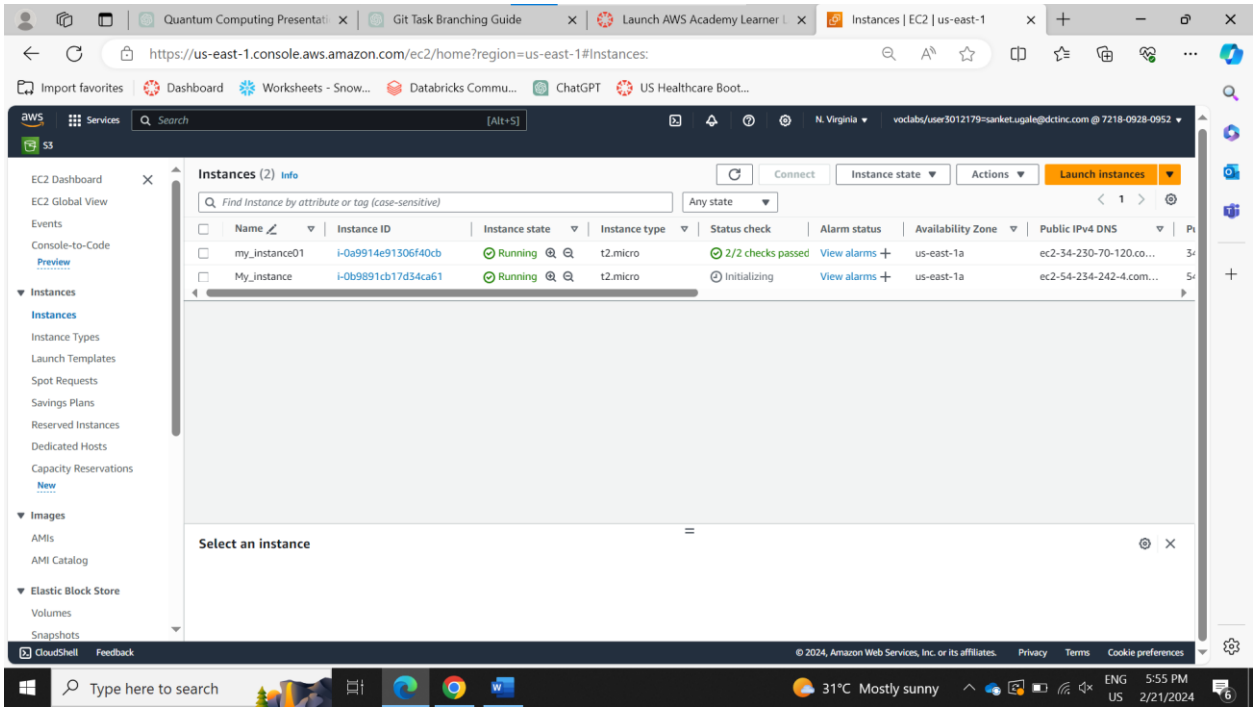
STEP : Name your key pair and select the .pem and click on create key pair and download the key pair.



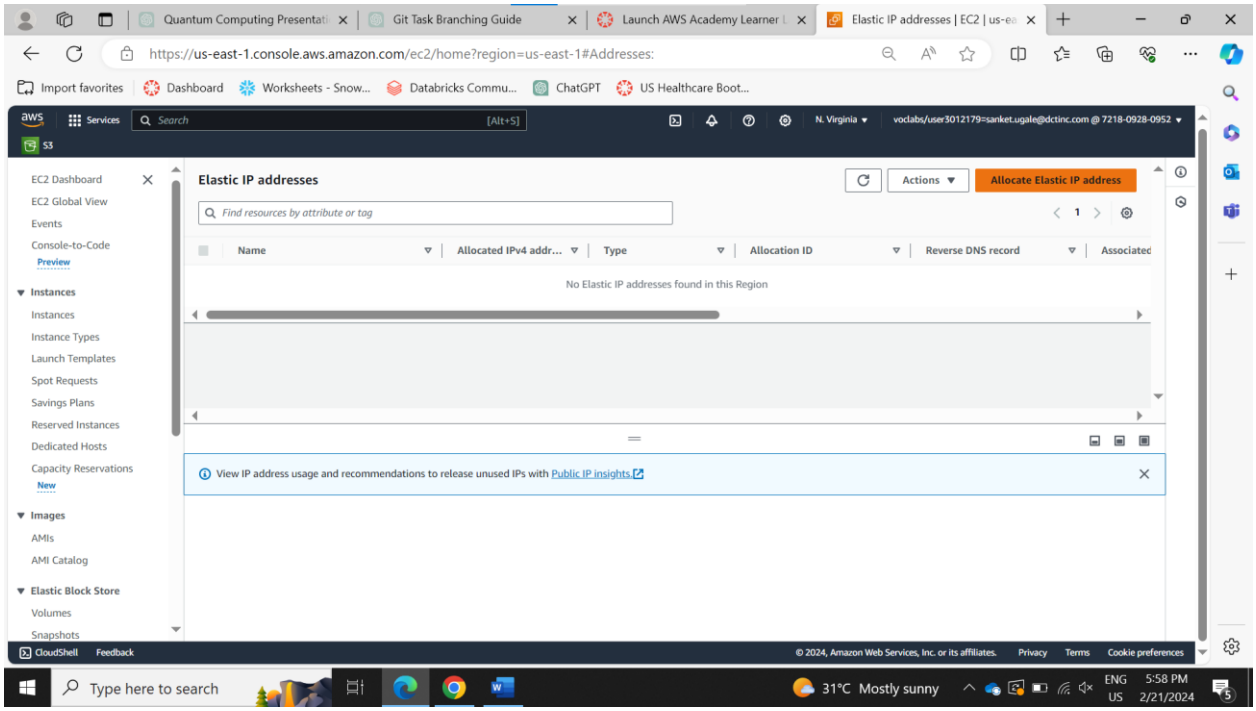
STEP : tick the create security group and create instance.



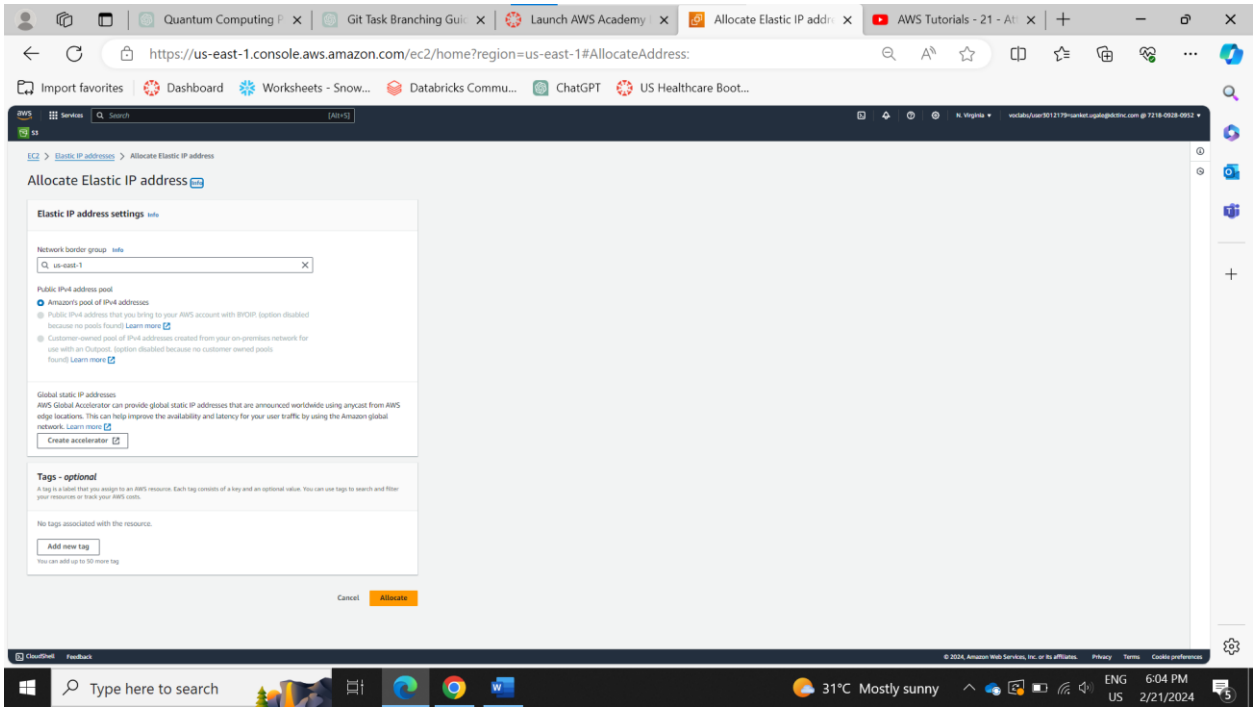
STEP : again go to instacnes and wait until you instance states comes to “Running”



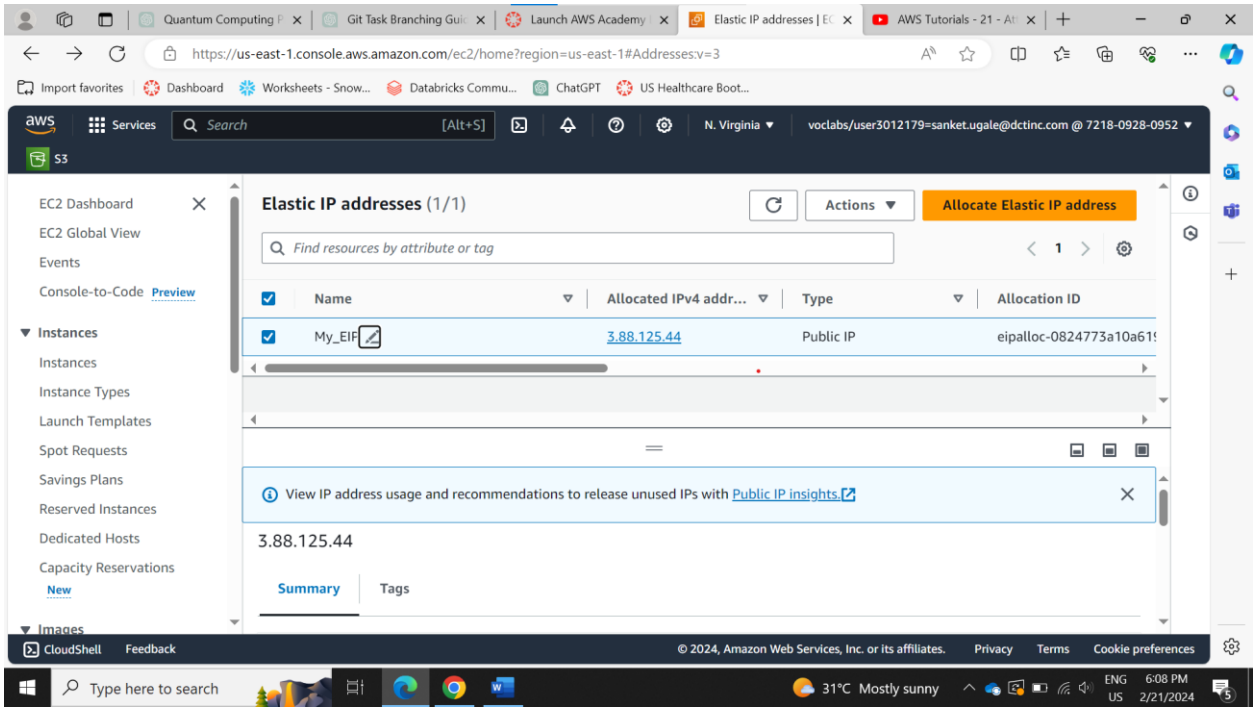
STEP : Go to Elastic IP in network and setting and click on allocate elastic IP.



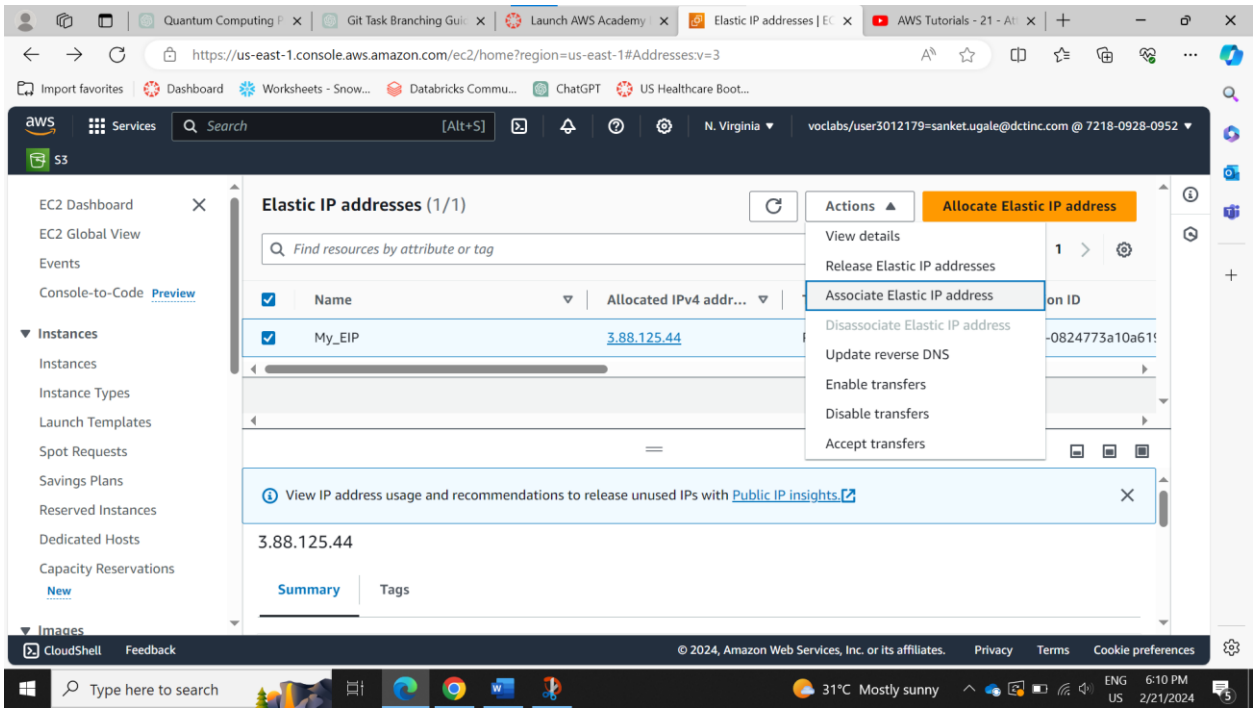
STEP : Click on allocate.



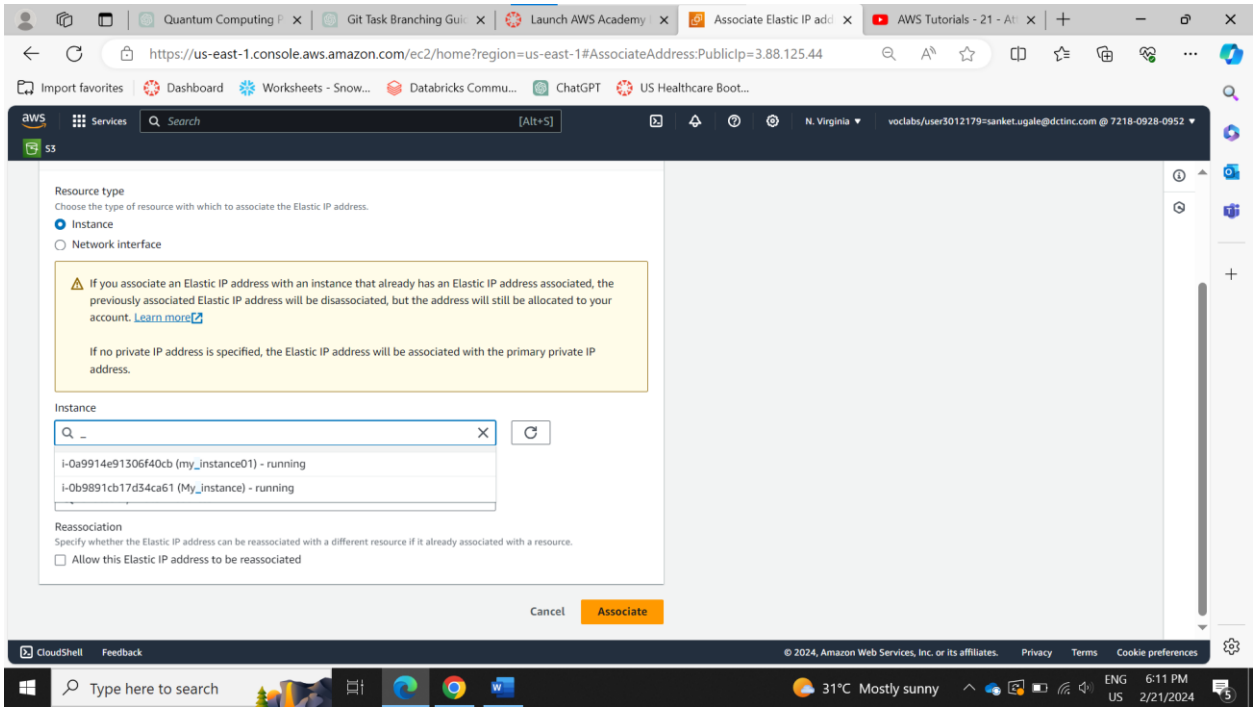
STEP : Your Elastic IP is generated rename it as per your need.



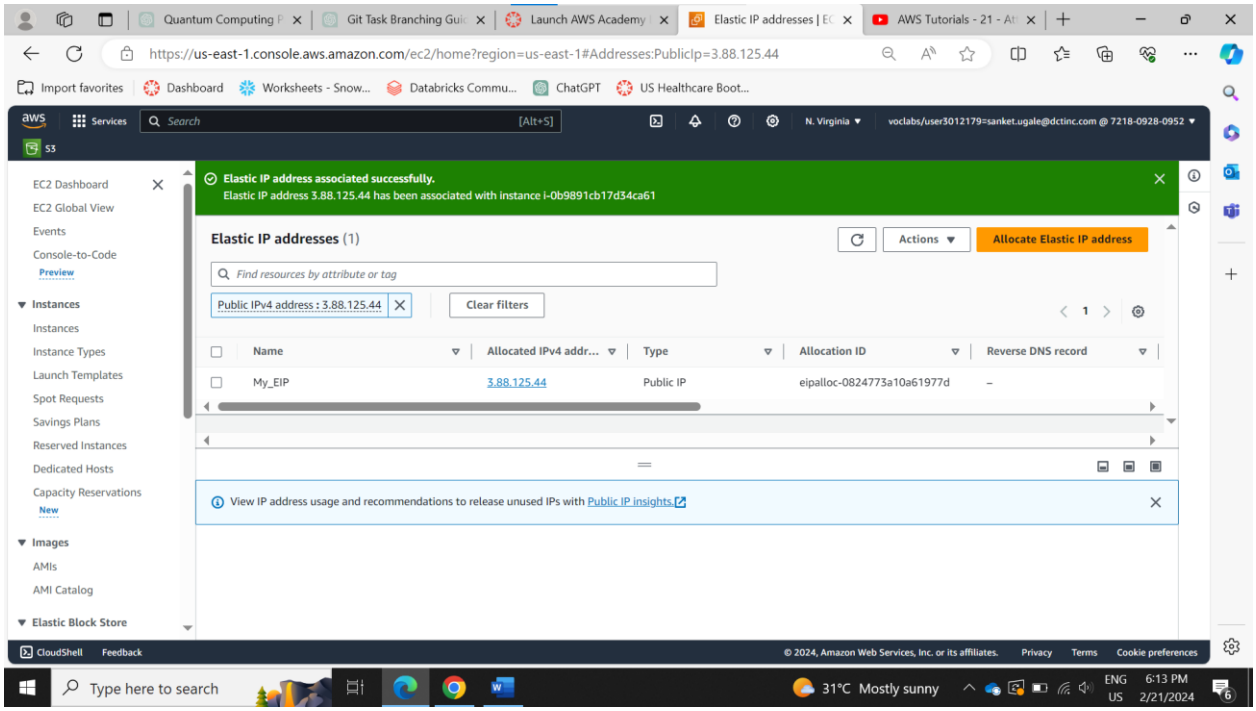
STEP : Select your Elastic IP and click on Actions and click on Associate Elastic IP Address.



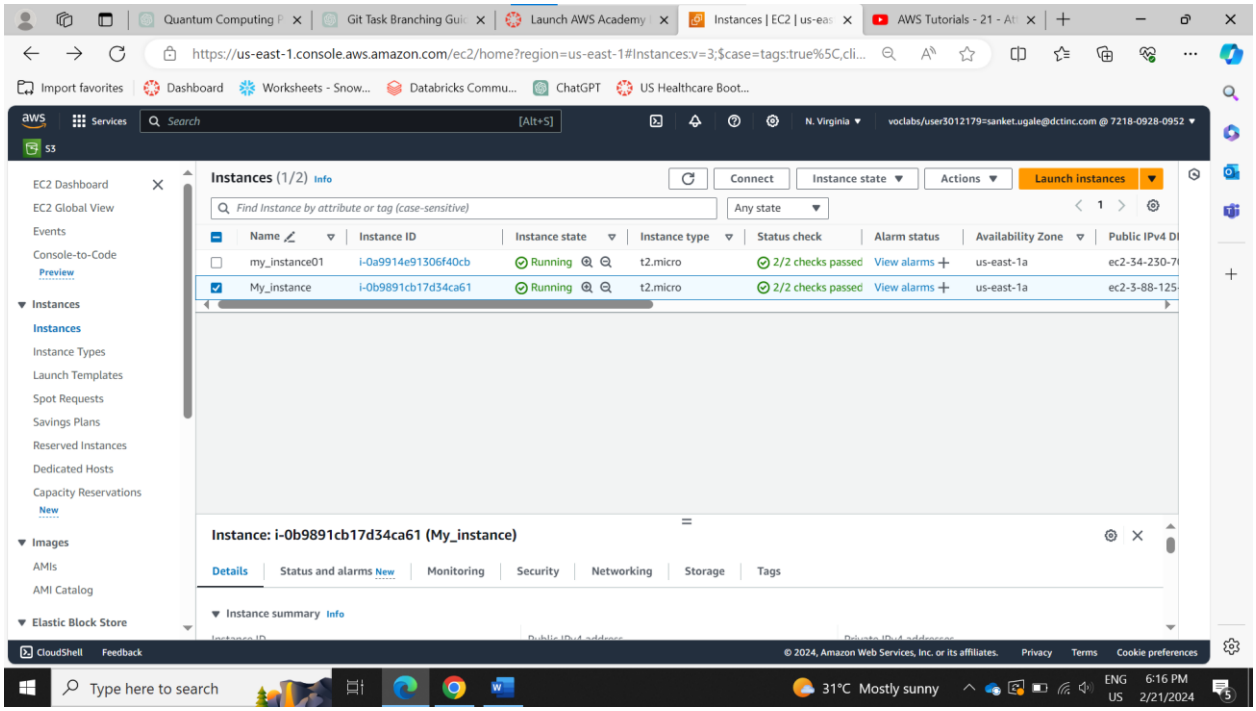
STEP : Tick the instance and select your instance from drop down menu and click on associate.



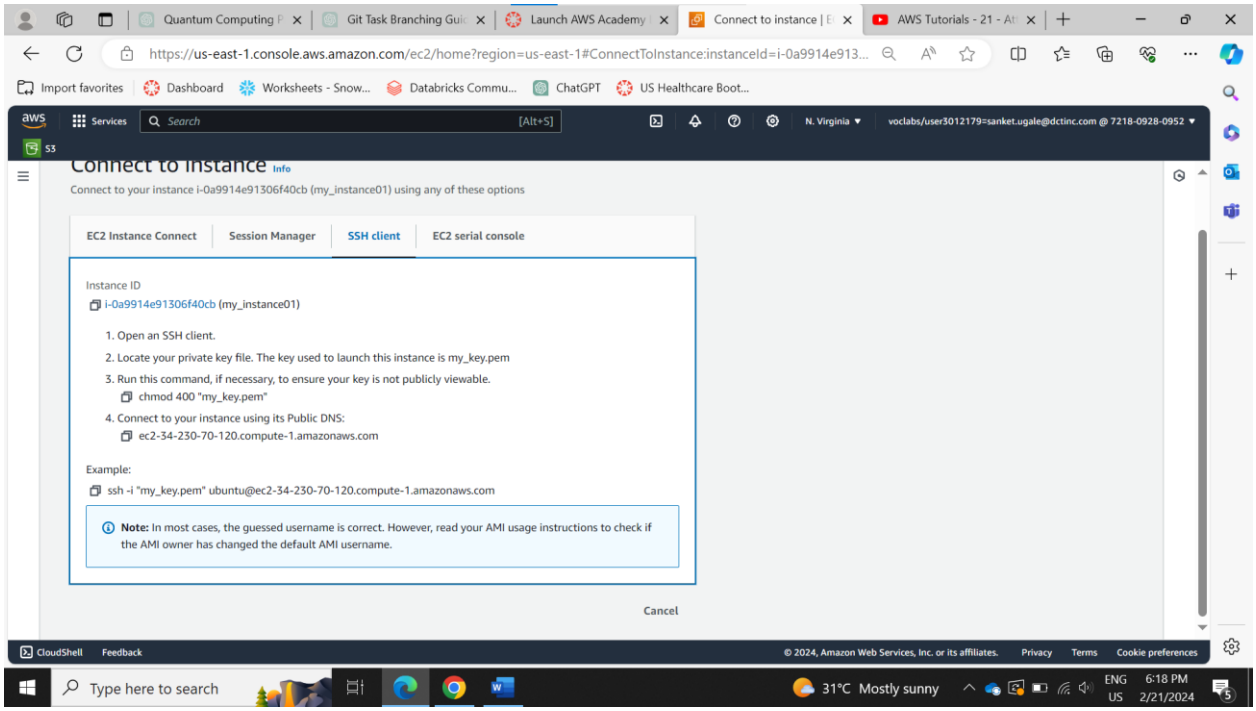
STEP : Congratulations your Elastic IP address is associated with your instance.



STEP : Now go to instances select your instance and click on connect.

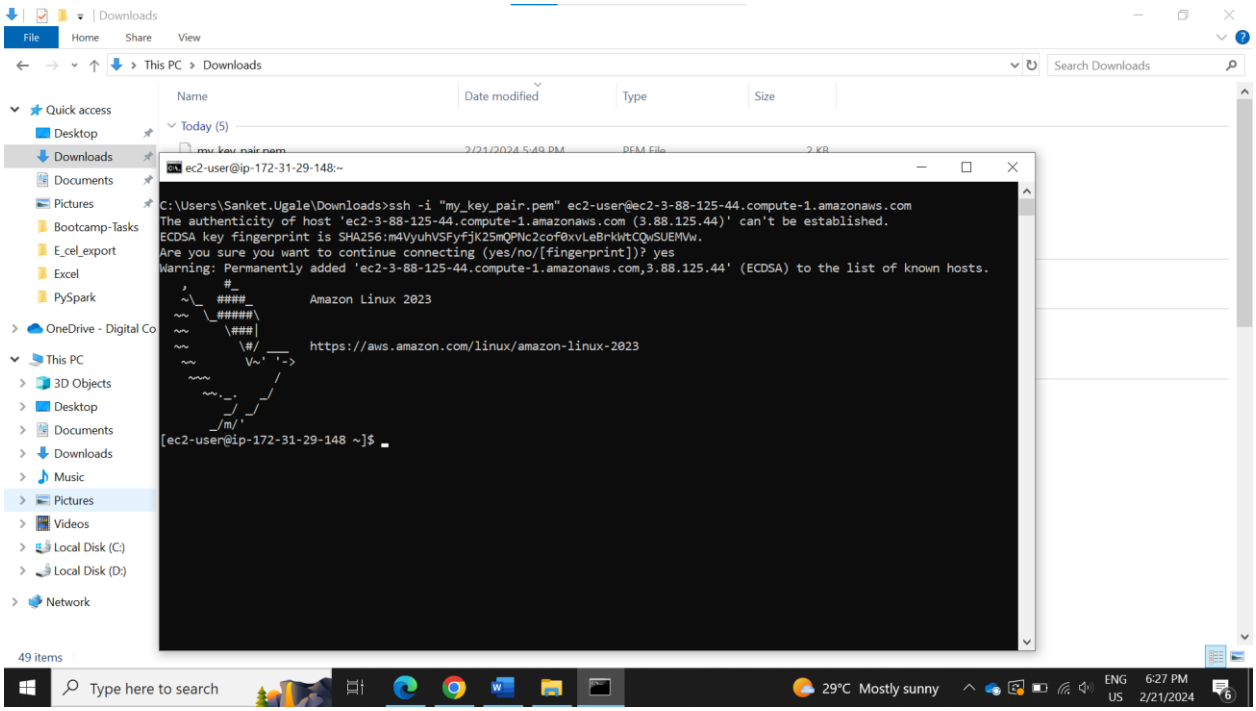


STEP : Go to SSH Client. And Copy your Public DNS.



STEP : Open Command Prompt and Go to location where your key pair is downloaded.

And type the “ssh -i "my_key_pair.pem" ec2-user@ec2-3-88-125-44.compute-1.amazonaws.com” and click enter.

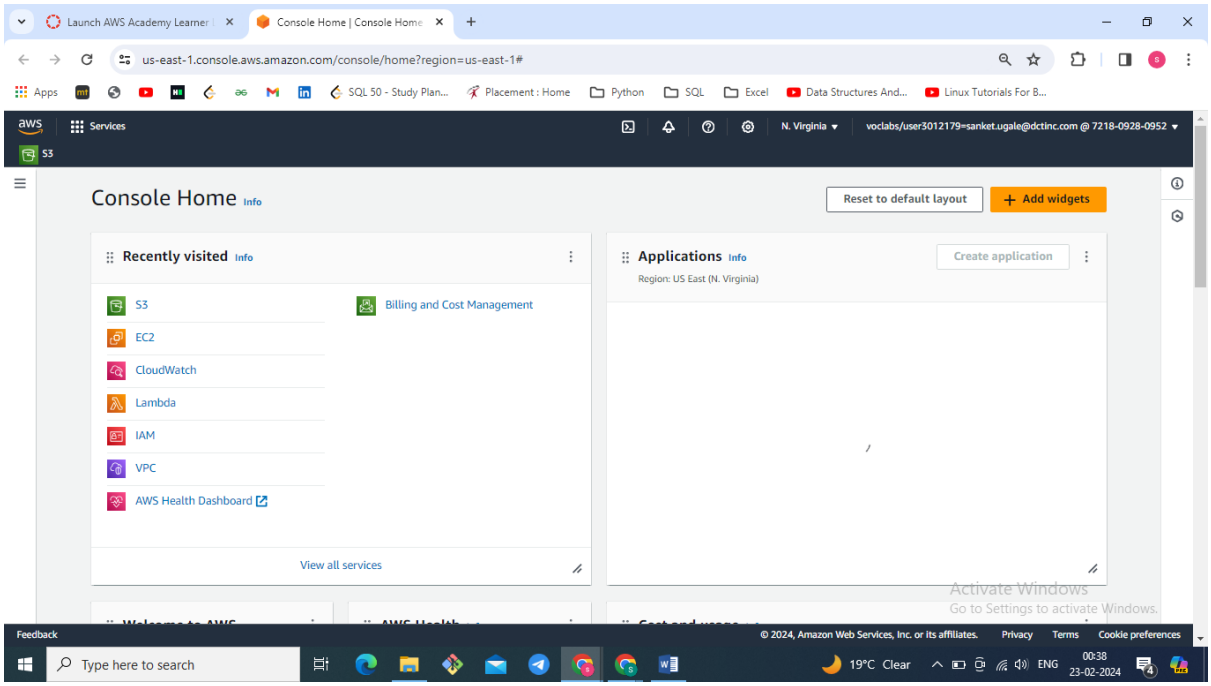


”

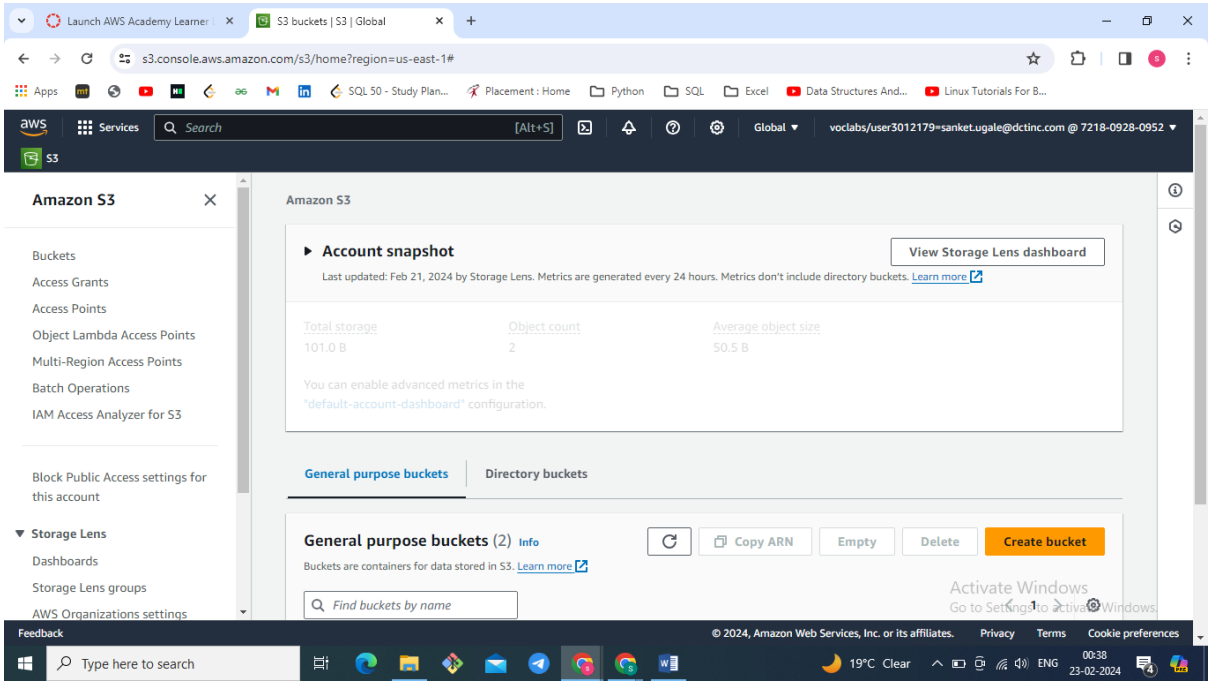
STEP : Congratulations you are connected to your EC2 instance by using ssh

AWS S3 Lab (Simple Storage Service)

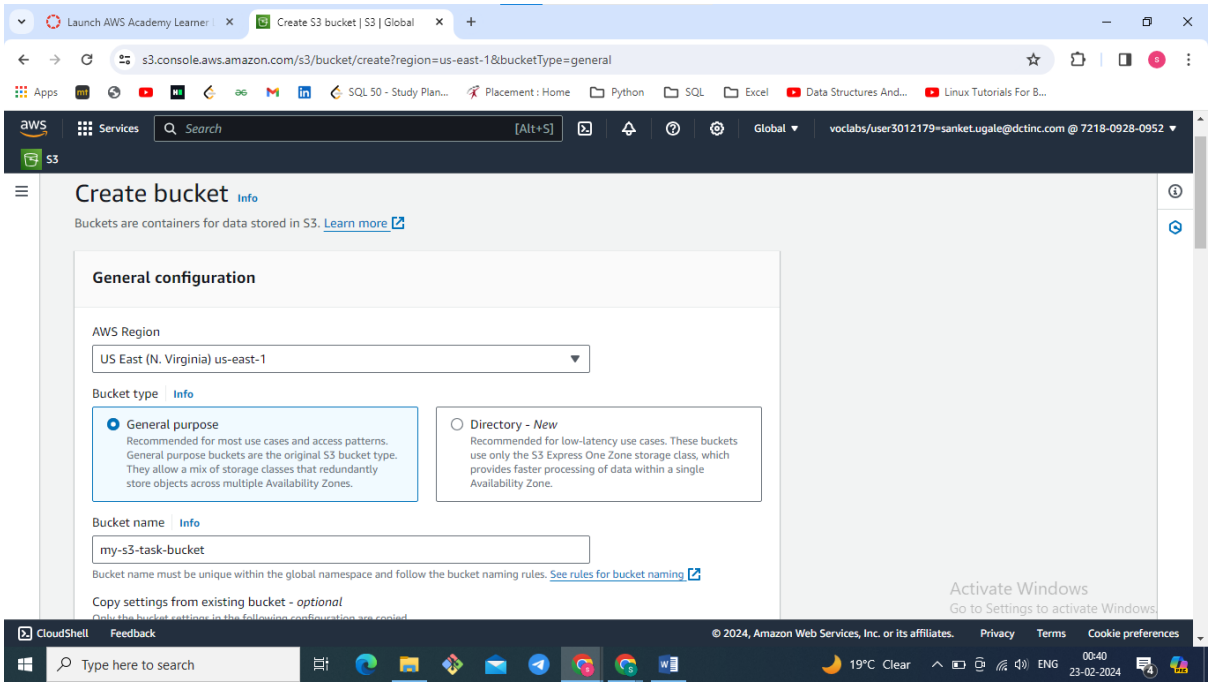
STEP 1 : Search S3 and go to s3 Console.



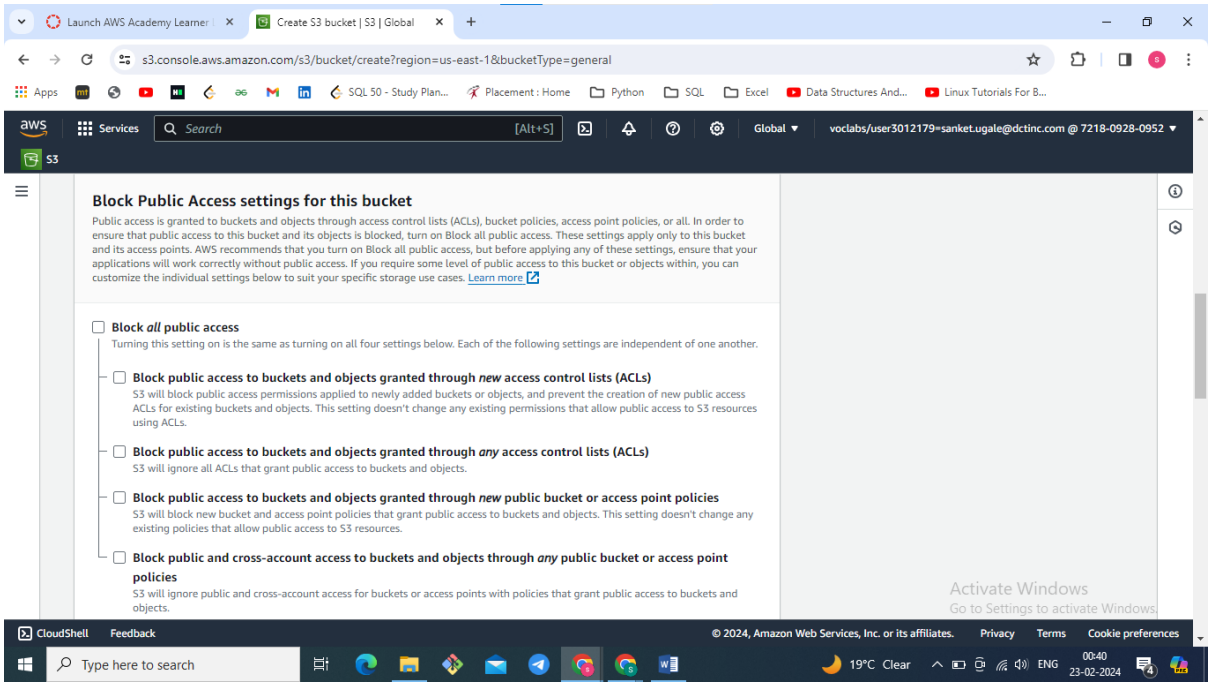
STEP 2 : Click on Create Bucket option.

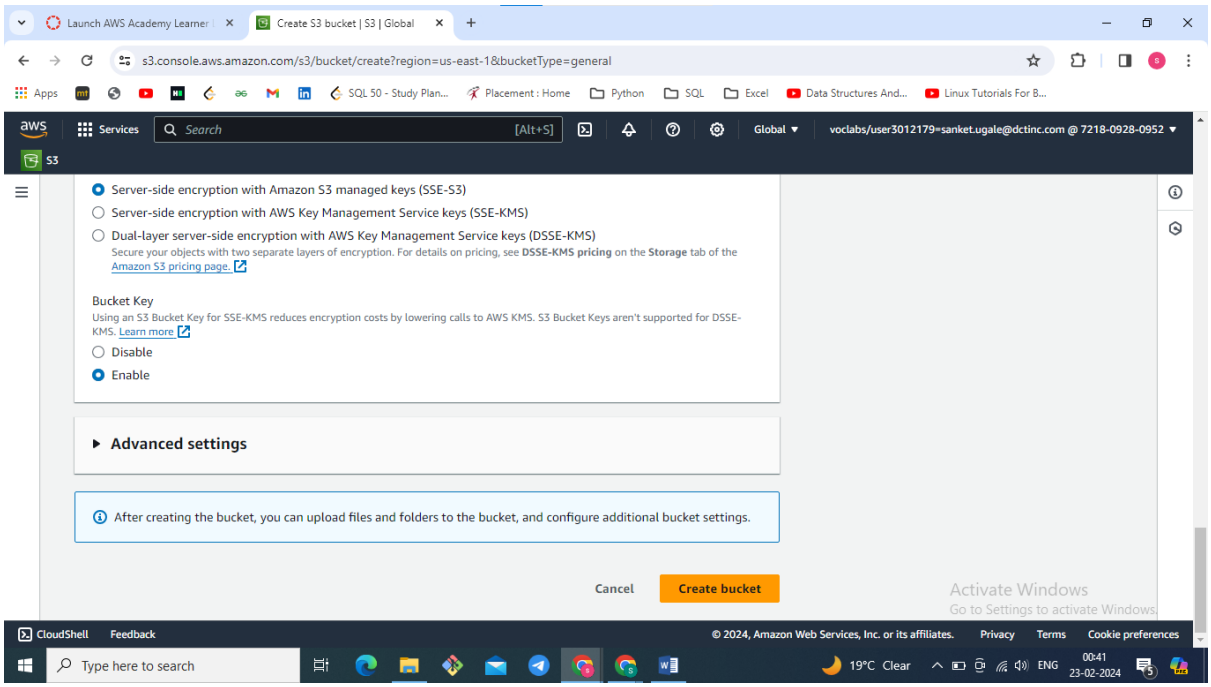


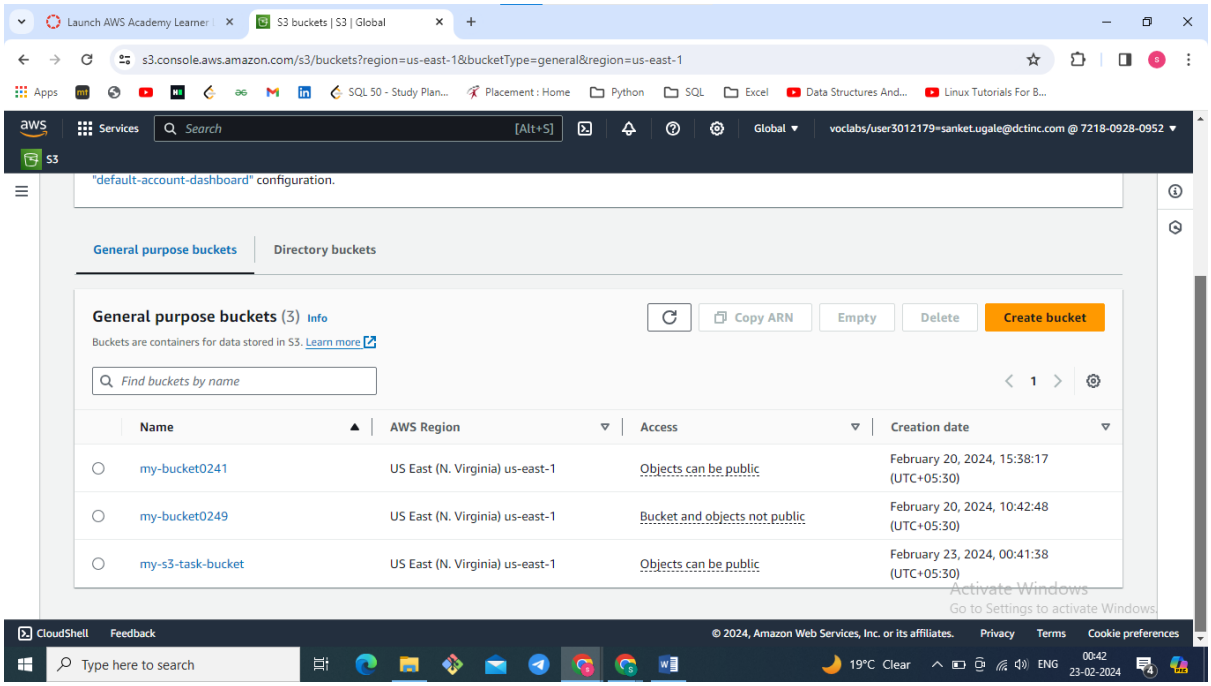
STEP 3 : Give a unique name to the bucket (Globally Unique) and Select a region where you want your bucket to be created.



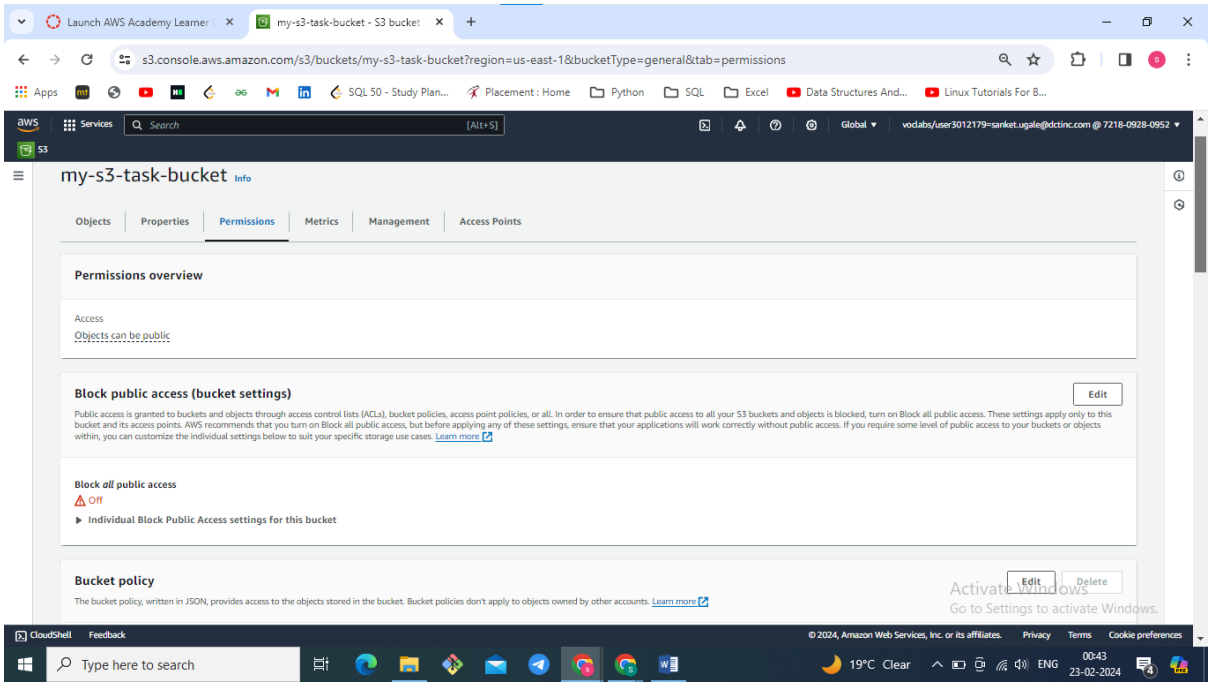
STEP : Untick the **“Block all Public access”** and Simpaly click on the create bucket option.


Launch AWS Academy Learner
Create S3 bucket | S3 | Global
s3.console.aws.amazon.com/s3/bucket/create?region=us-east-1&bucketType=general
Services
Search
[Alt+S]
Global
voclabs/user3012179=sanket.ugale@dctinc.com @ 7218-0928-0952
S3
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.
Activate Windows
Go to Settings to activate Windows.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
19°C Clear
ENG
00:40
23-02-2024


Launch AWS Academy Learner
Create S3 bucket | S3 | Global
s3.console.aws.amazon.com/s3/bucket/create?region=us-east-1&bucketType=general
Services
Search
[Alt+S]
Global
voclabs/user3012179=sanket.ugale@dctinc.com @ 7218-0928-0952
S3
Server-side encryption with Amazon S3 managed keys (SSE-S3)
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the Amazon S3 pricing page.
Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more
Disable
Enable
Advanced settings
After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.
Cancel
Create bucket
Activate Windows
Go to Settings to activate Windows.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
19°C Clear
ENG
00:41
23-02-2024

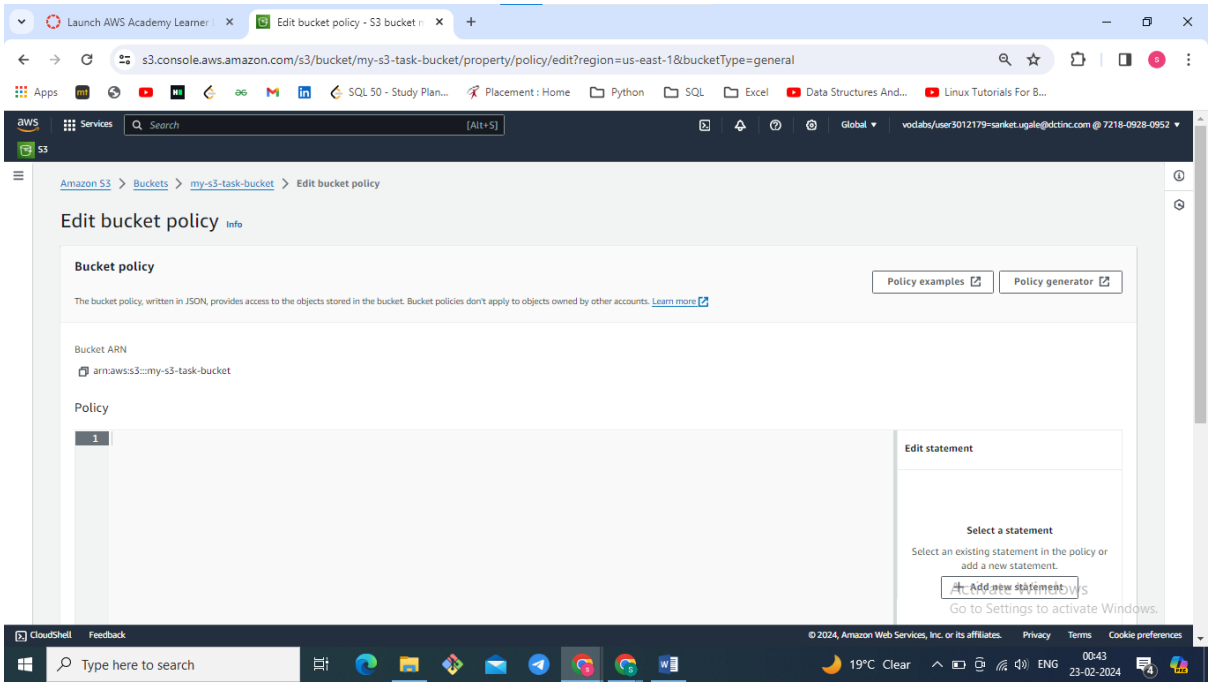


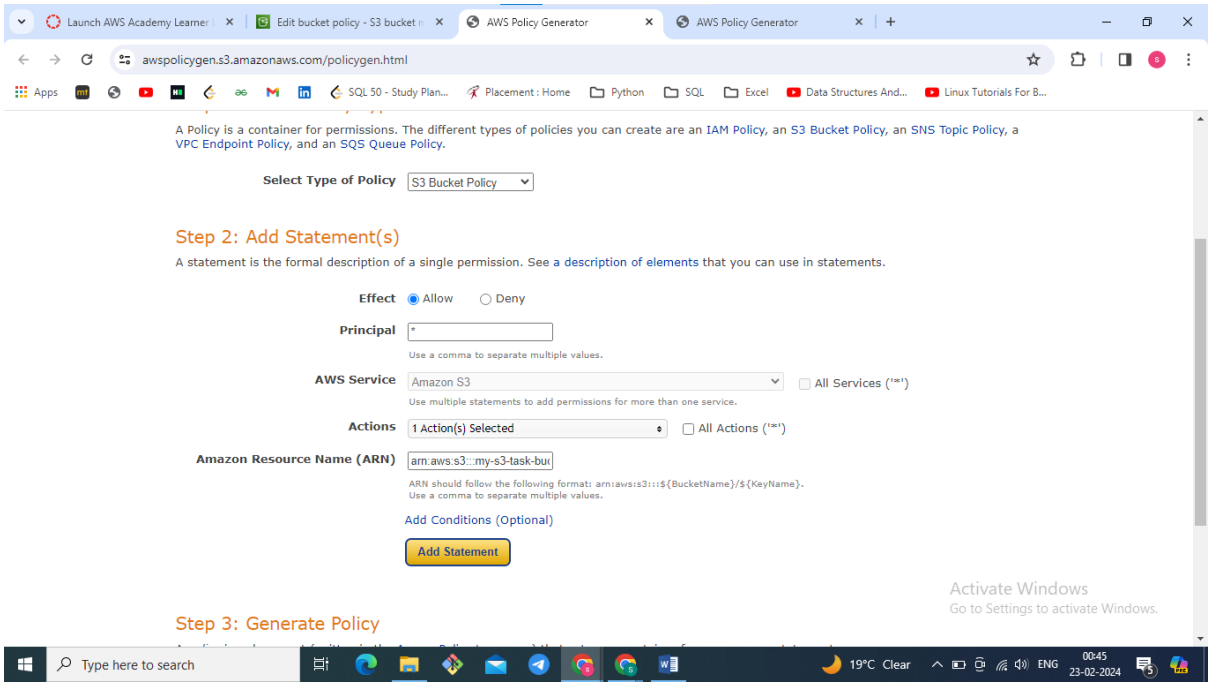
STEP : Go to Bucket permissions and edit bucket policy.

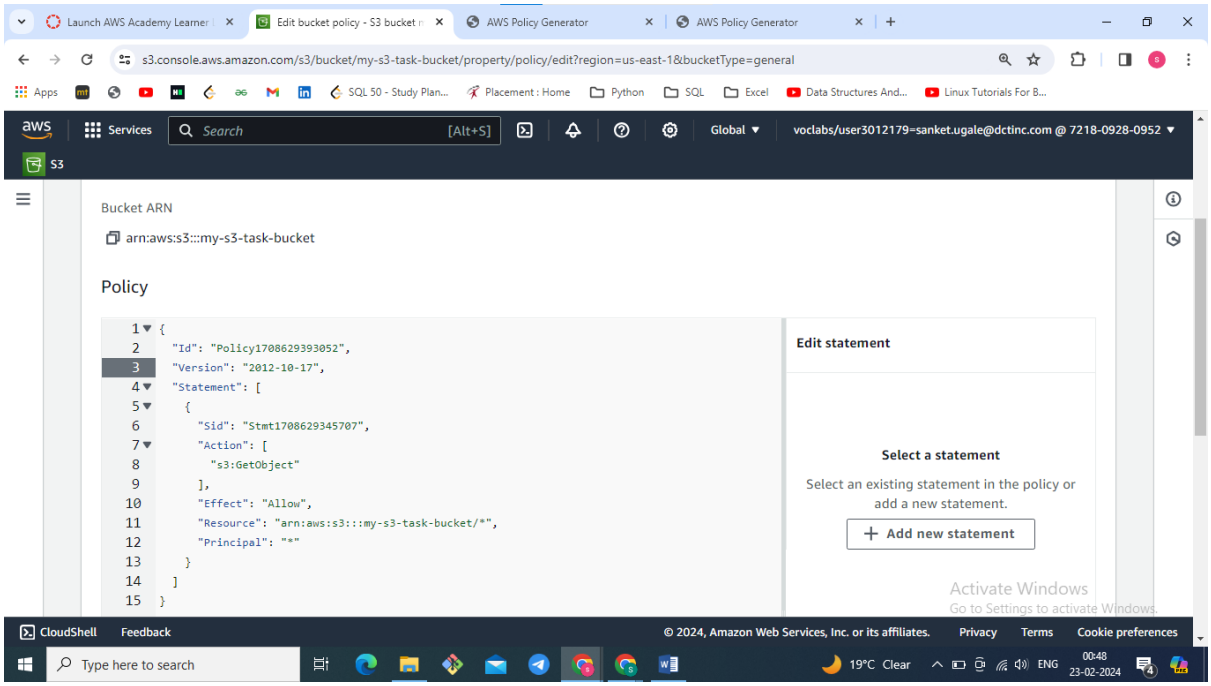


STEP : Click on policy generator.

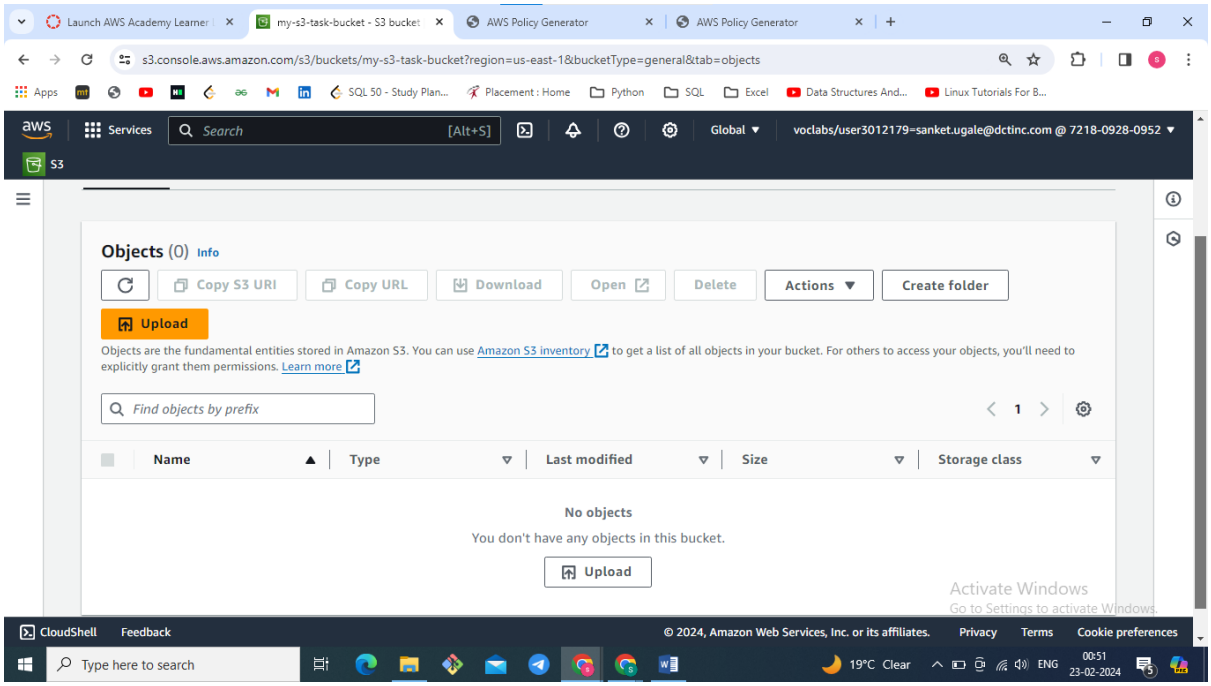
- Select the type of Polycy to **“s3 Bucket policy”**
- Allow it to everyone **”*”**
- Select action as **“get object”**
- Copy your bucket **ARN (Amazon Resource Name)** and Paste.
- Click on add statement and then generate Policy.
- Copy the generated policy and then paste in the bucket policy.
- And save the changes.

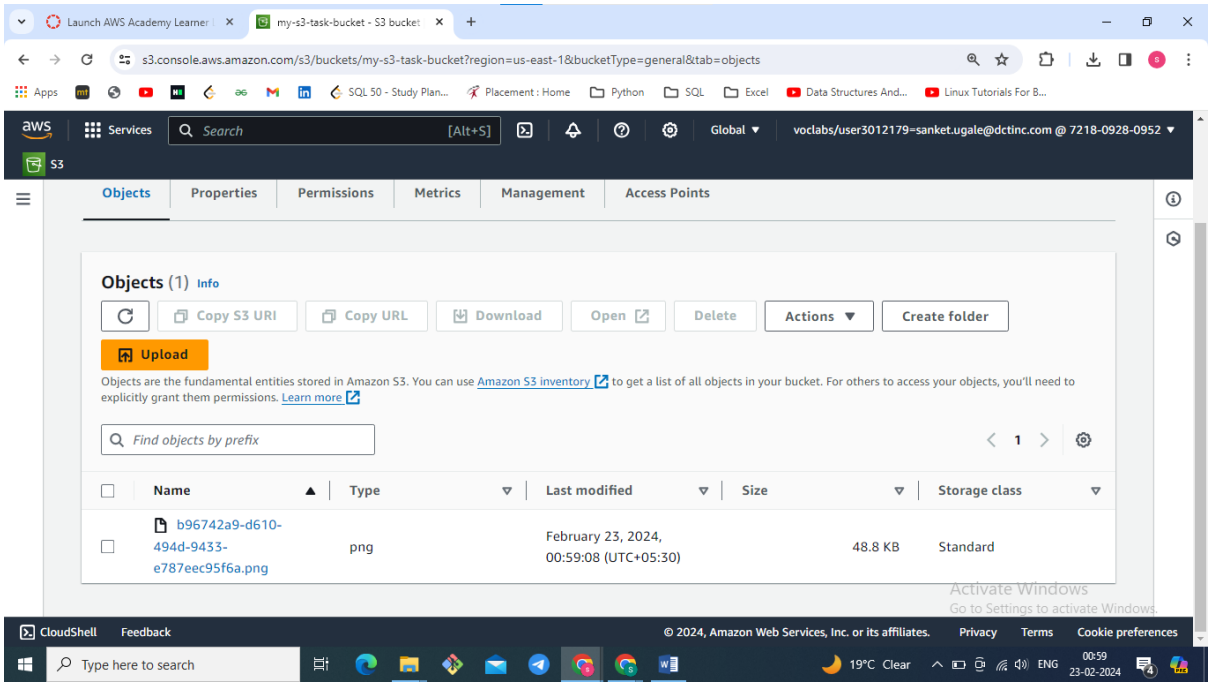

Launch AWS Academy Learner
Edit bucket policy - S3 bucket
s3.console.aws.amazon.com/s3/bucket/my-s3-task-bucket/property/policy/edit?region=us-east-1&bucketType=general
Amazon S3 > Buckets > my-s3-task-bucket > Edit bucket policy
Edit bucket policy Info
Bucket policy
Policy examples
Policy generator
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more
Bucket ARN
arn:aws:s3:::my-s3-task-bucket
Policy
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
19°C Clear
ENG
00:43
23-02-2024


Launch AWS Academy Learner
Edit bucket policy - S3 bucket
AWS Policy Generator
AWS Policy Generator
awspolicygen.s3.amazonaws.com/policygen.html
A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.
Select Type of Policy
S3 Bucket Policy
Step 2: Add Statement(s)
A statement is the formal description of a single permission. See a description of elements that you can use in statements.
Effect
Allow
Deny
Principal
*
Use a comma to separate multiple values.
AWS Service
Amazon S3
All Services ('*')
Use multiple statements to add permissions for more than one service.
Actions
1 Action(s) Selected
All Actions ('*')
Amazon Resource Name (ARN)
arn:aws:s3:::my-s3-task-buc
ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.
Add Conditions (Optional)
Add Statement
Step 3: Generate Policy
Type here to search
19°C Clear
ENG
00:45
23-02-2024

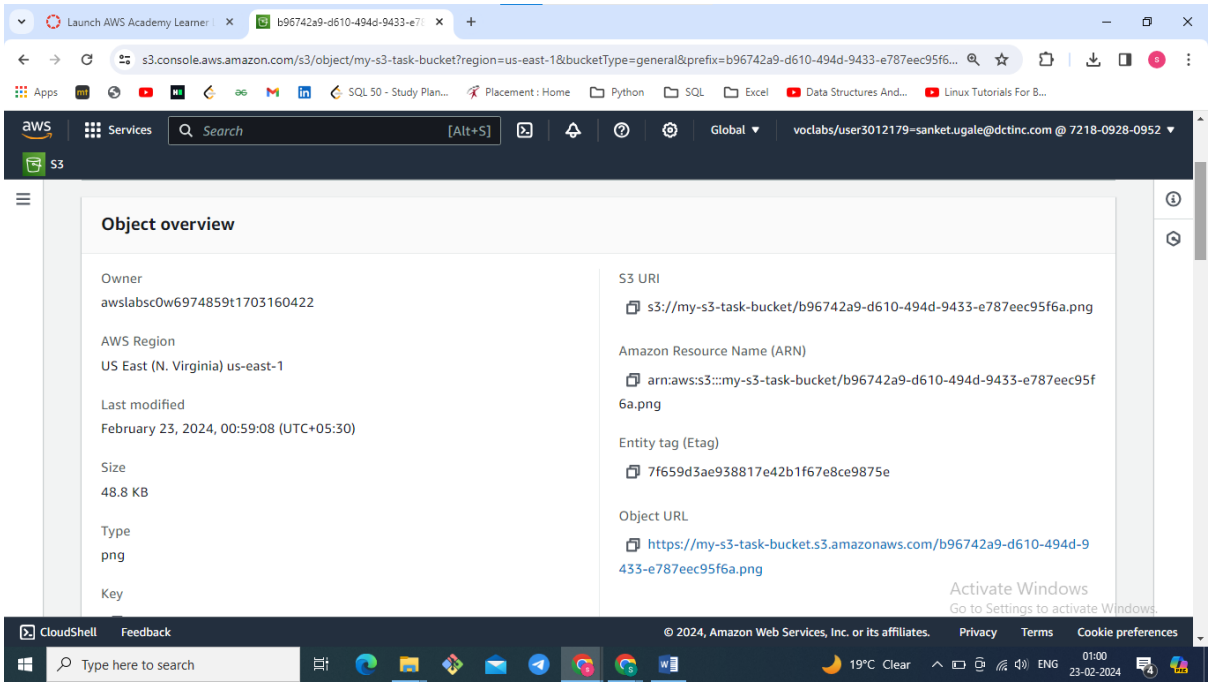


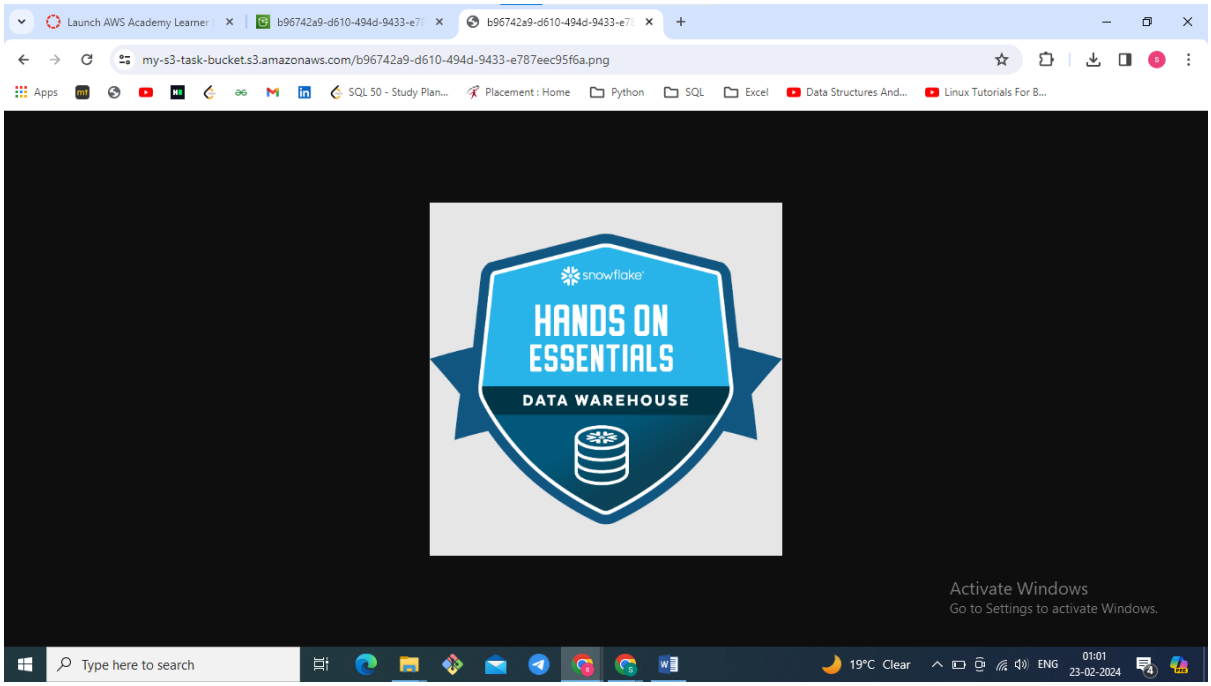
STEP : Go to bucket and upload some file.





STEP : Go to object properties and copy the Object URL and paste it in the new tab.

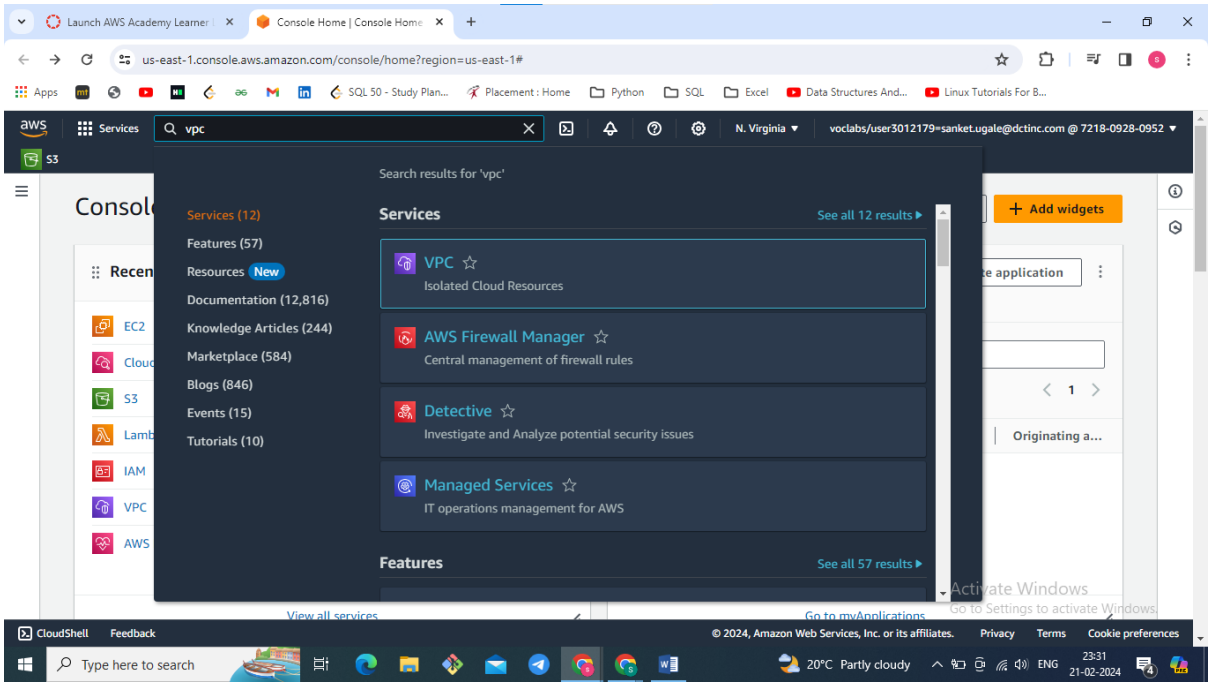




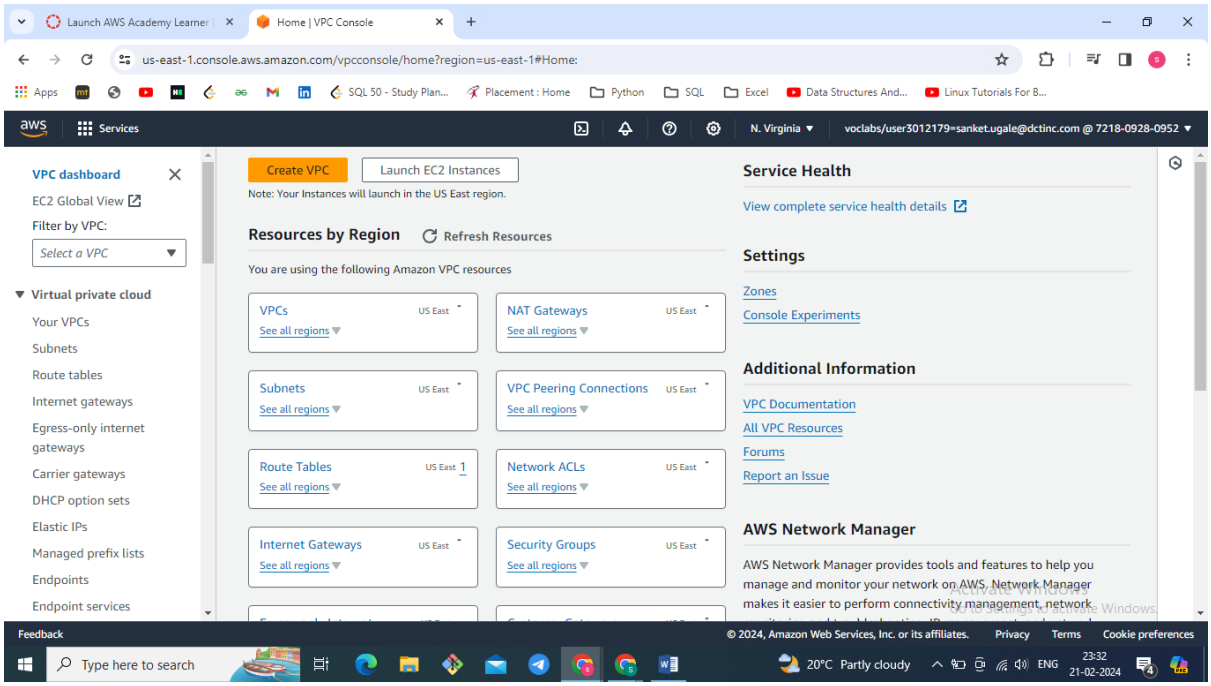
Congratulations now you can access the objects in your buckets Publically

AWS VPC Lab (Virtual Private Cloud)

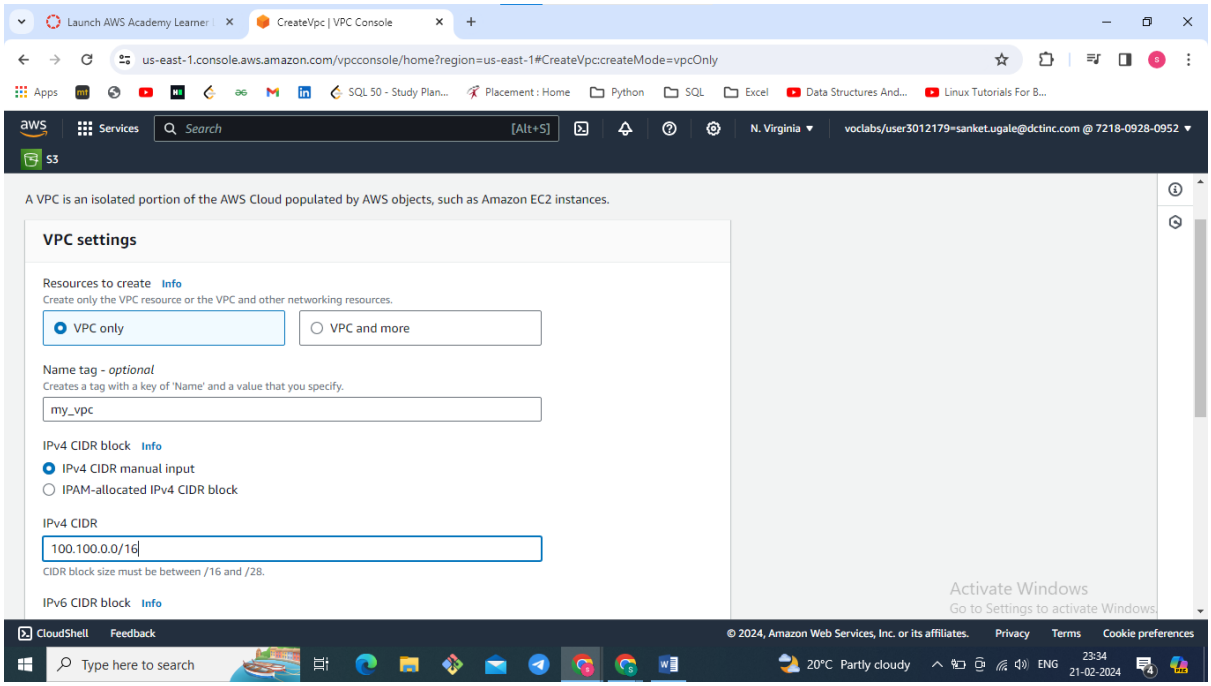
STEP 1 : Open AWS and search and select VPC

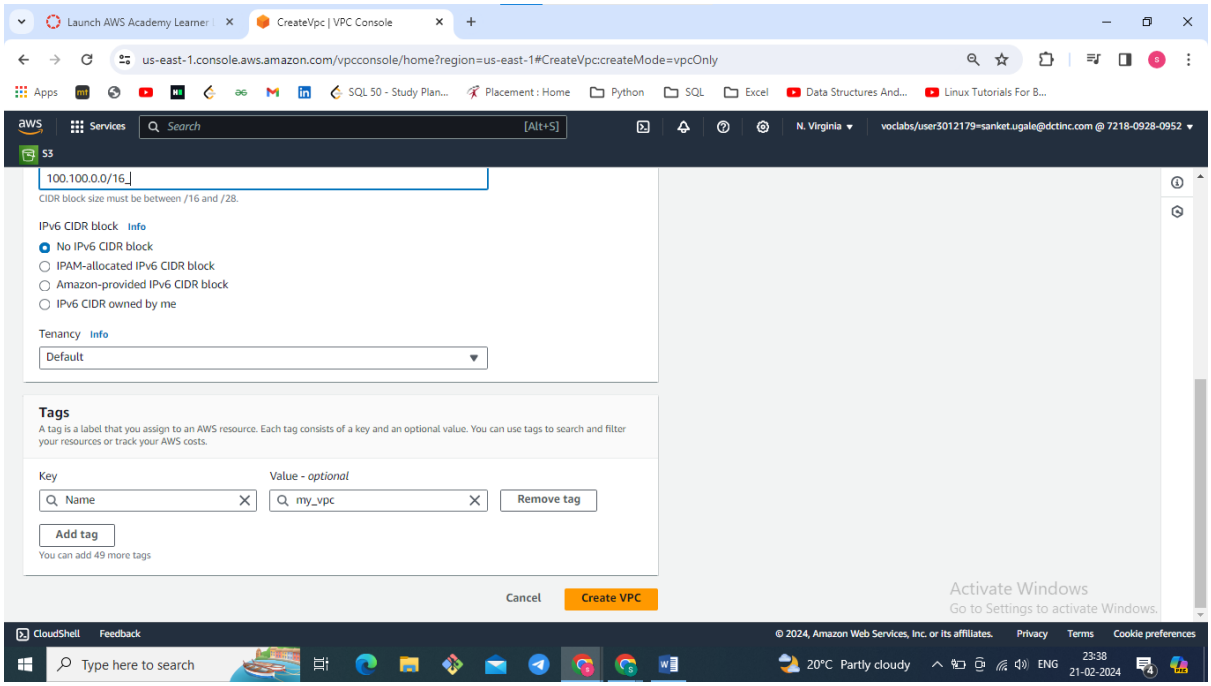


STEP 2 : Go to VPC and Click on Create VPC (Region Specific)

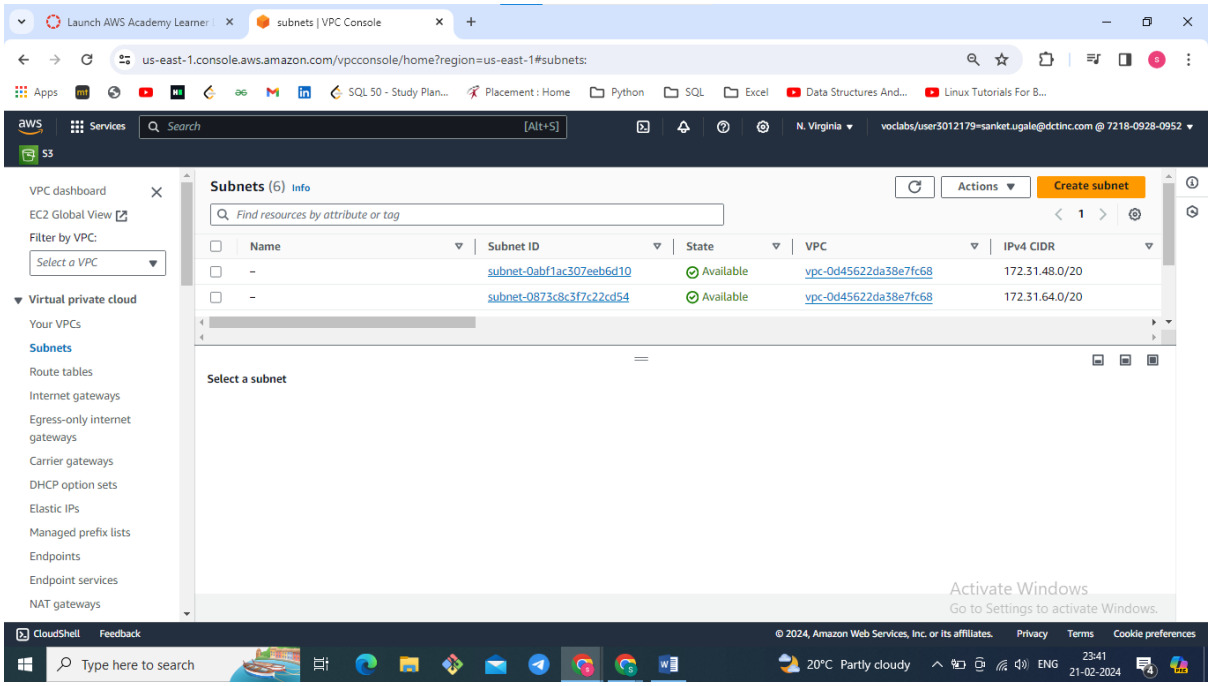


STEP 3 : Give a name of VPC and Provide IPv4 CIDR **(100.100.0.0/16)** and click on create VPC.

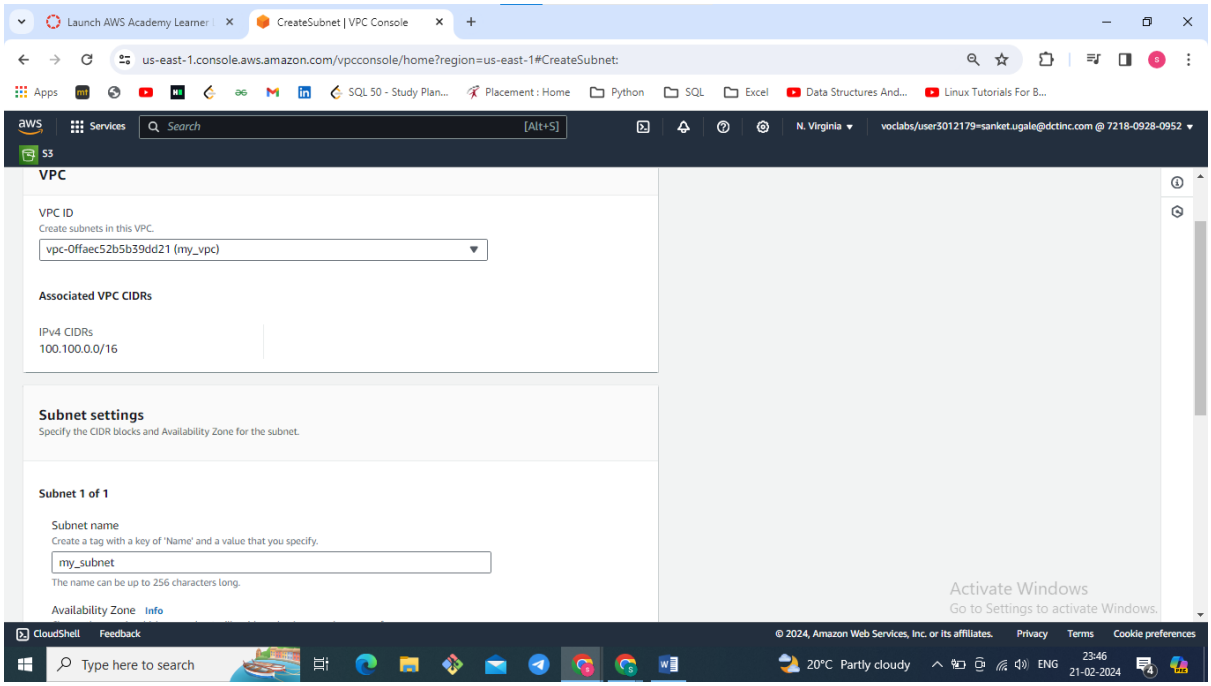




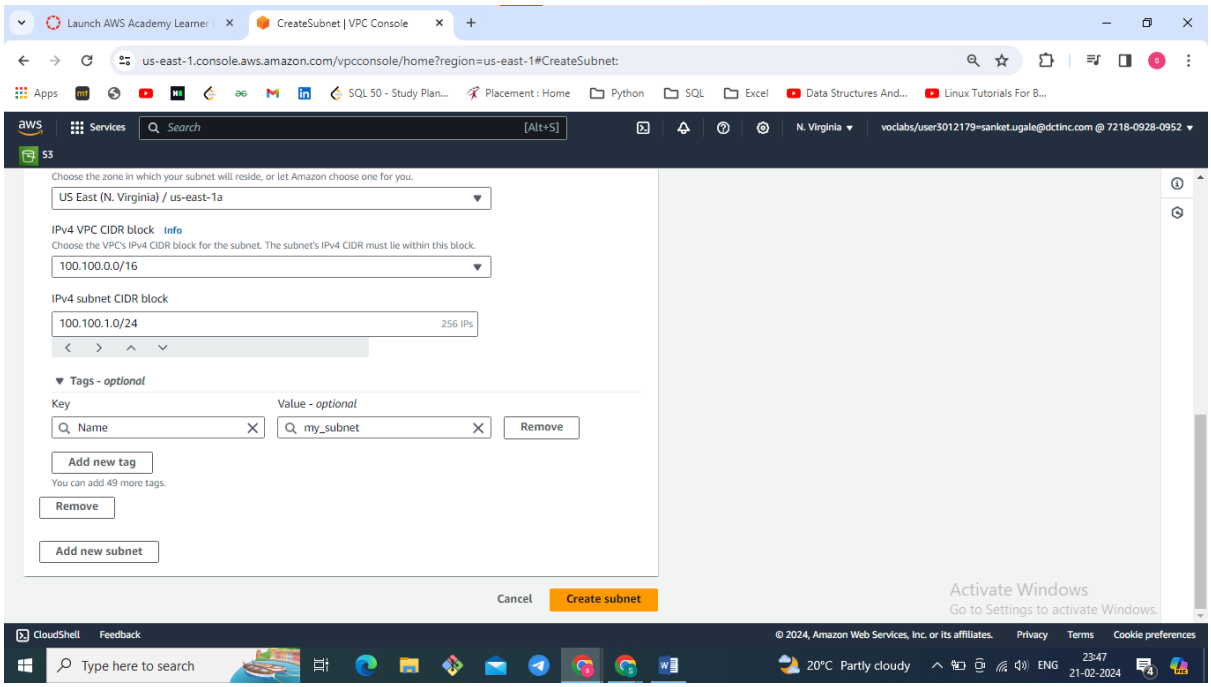
STEP ： Go to Subnets and click on Create subnets (Availibility Zone Specific)



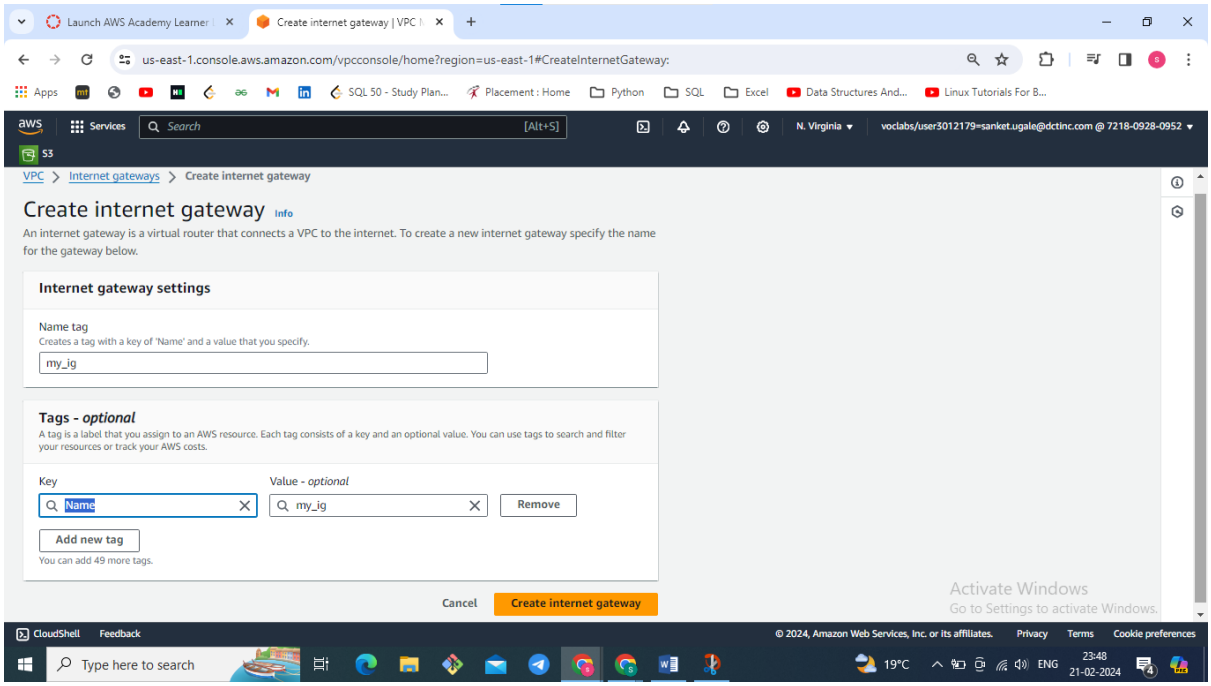
STEP : Selct your vpc (Which you have already created) and name your subnet



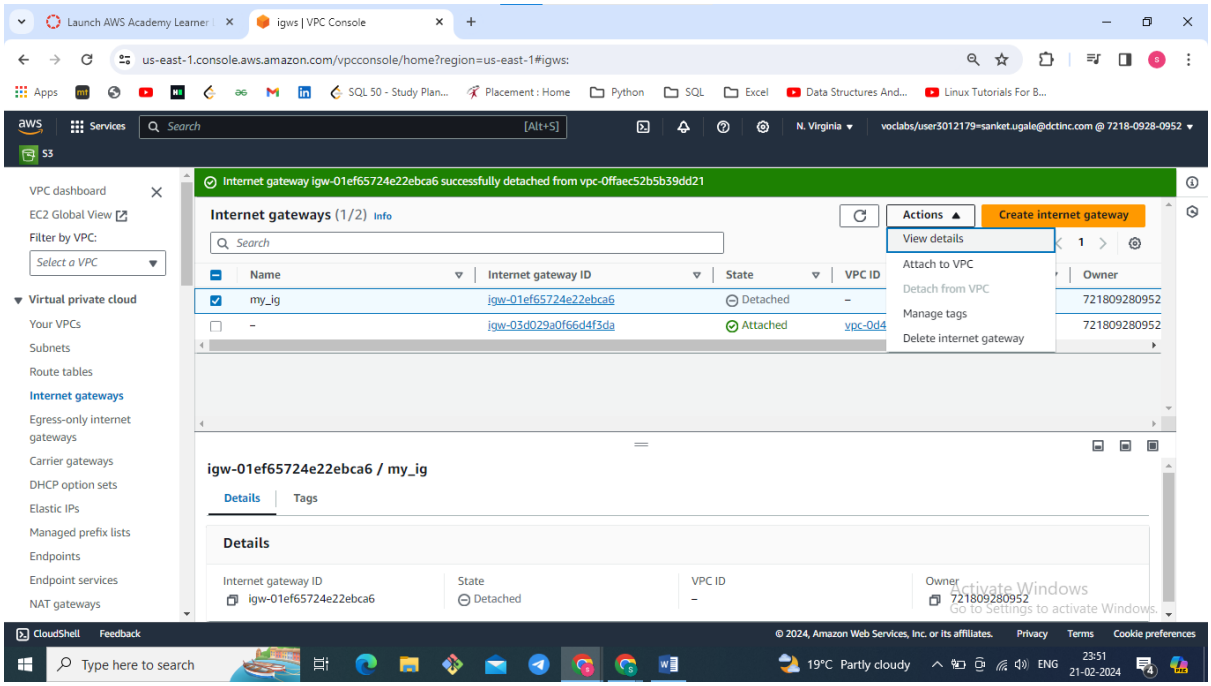
STEP : Select your AZ and Provide IPv4 CIDR **(100.100.1.0/24)/ (100.100.2.0/24)** and click on create 2 Subnets.



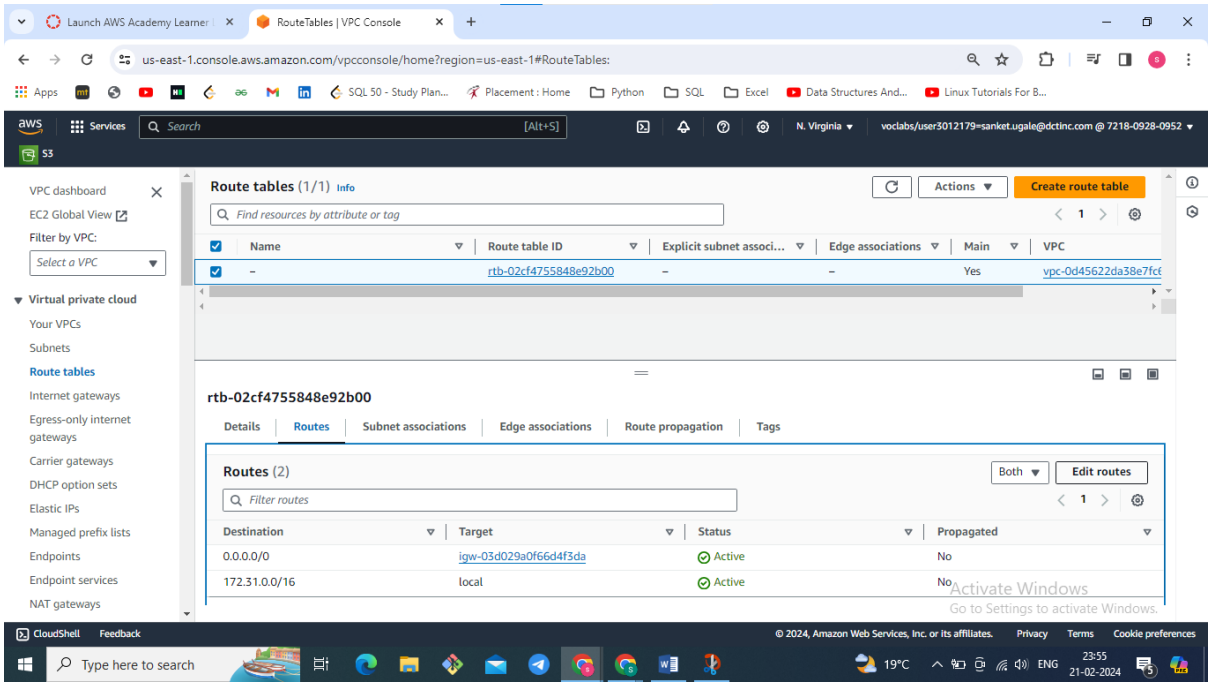
STEP : Go to internet gateway and give the name to IG and click on Create.

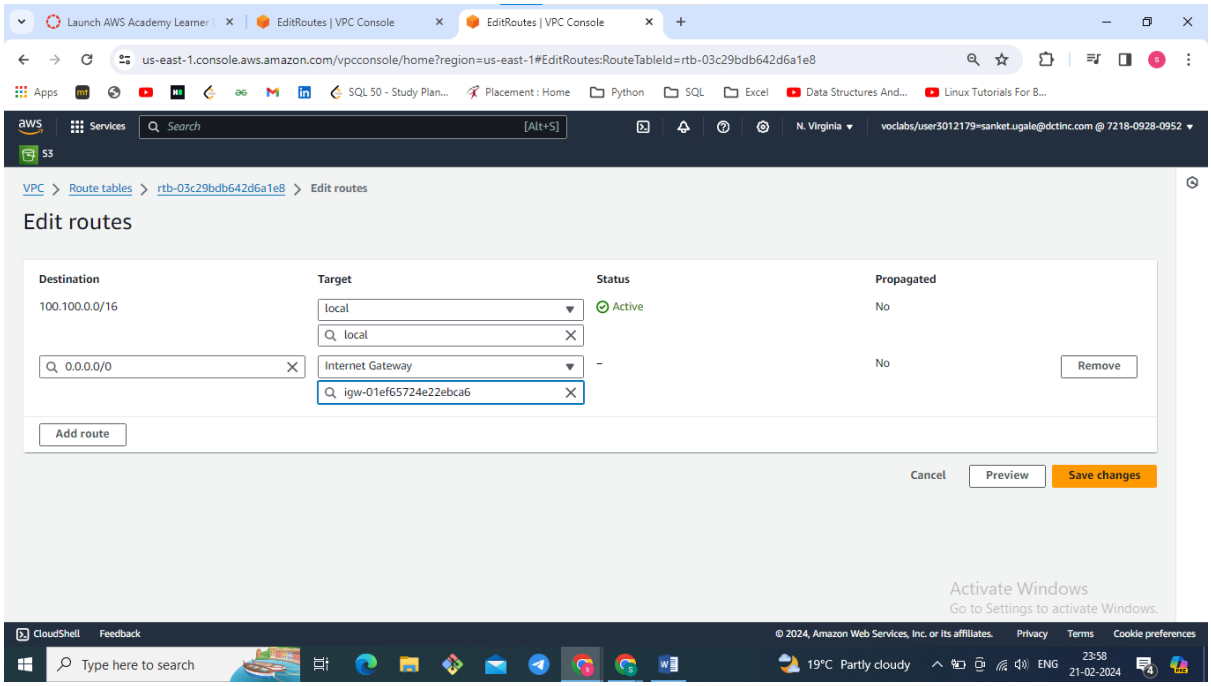


STEP : Select your created IG and go to action and attach it to your VPC.

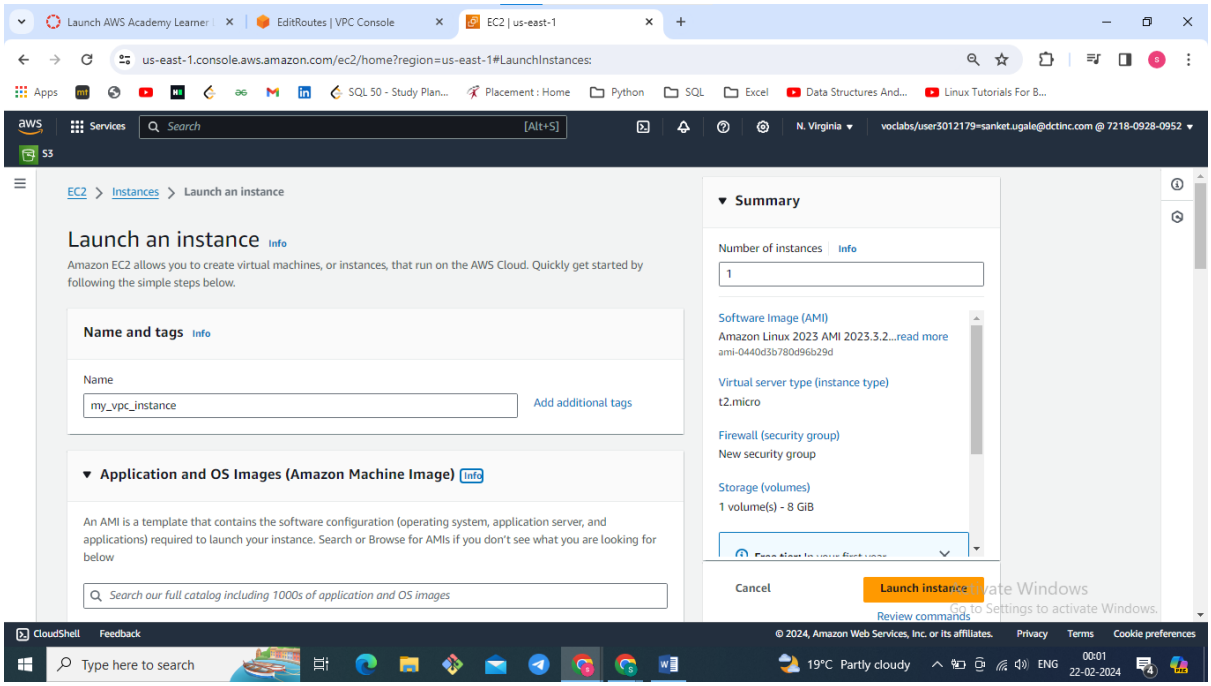


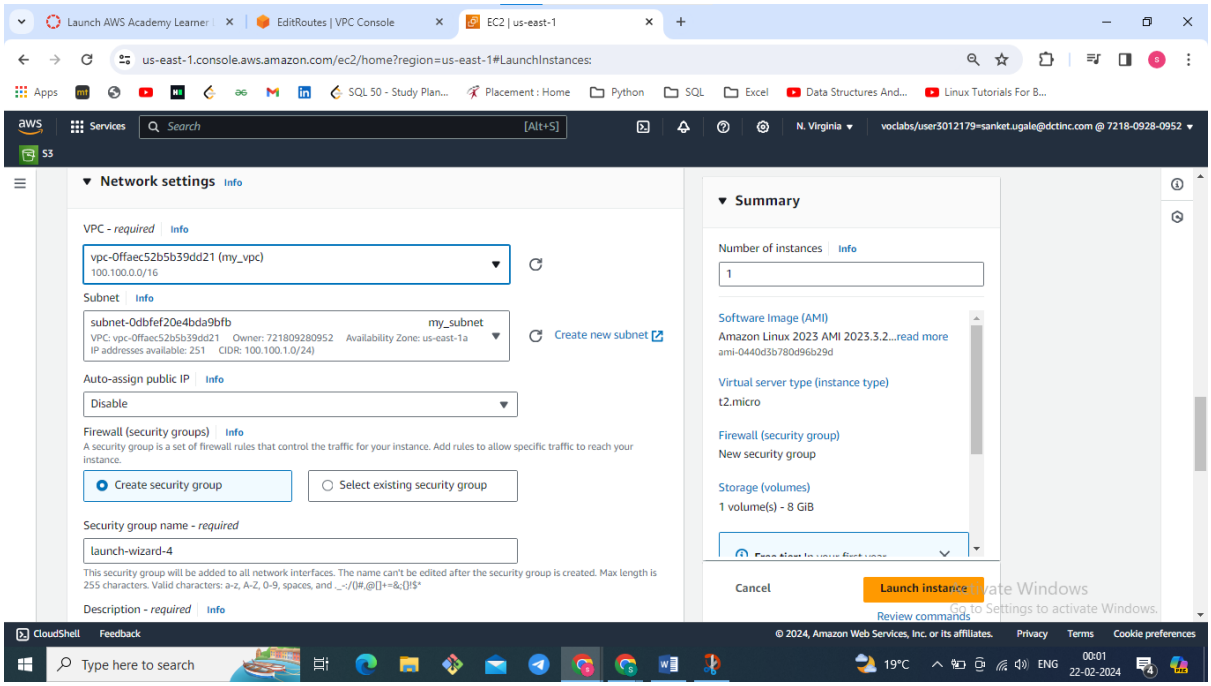
STEP : Go to route table and select your route table > route > Edit route > add route >
Destination : 0.0.0.0/0 → my created IG save changes.

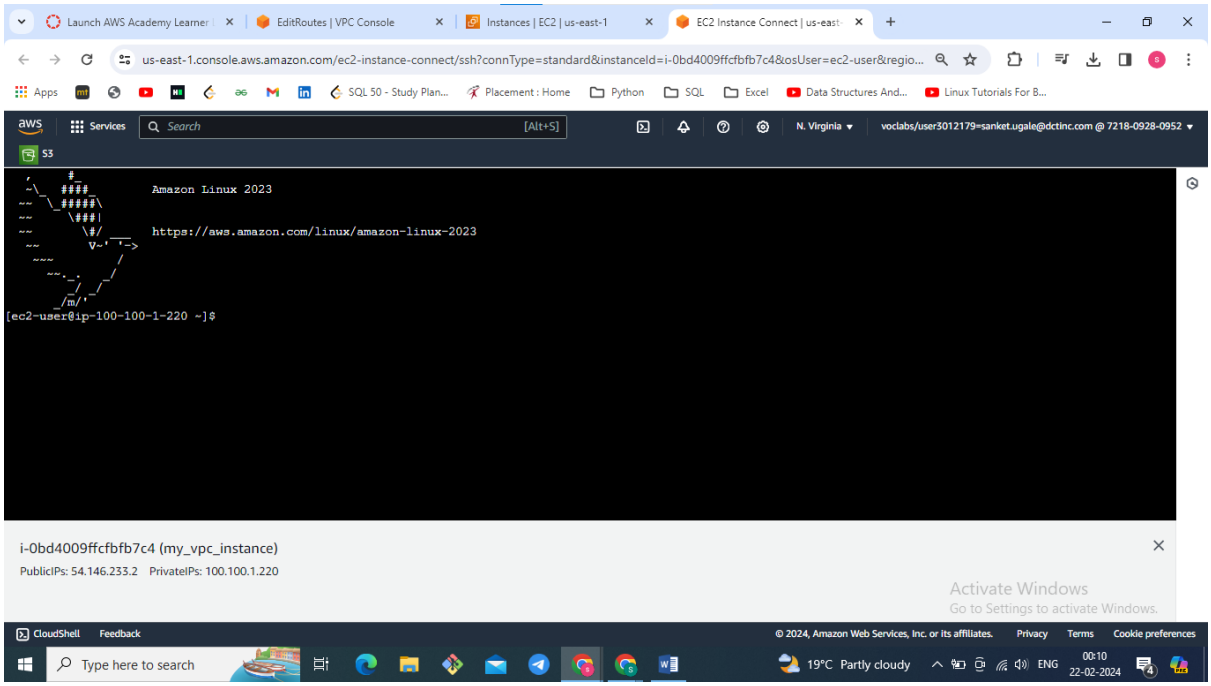




STEP : Create a instance with the above VPC attached.


Launch AWS Academy Learner
EditRoutes | VPC Console
EC2 | us-east-1
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
Services
Search
[Alt+S]
N. Virginia
voclabs/user3012179=sanket.ugale@dctinc.com @ 7218-0928-0952
EC2 > Instances > Launch an instance
Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
my_vpc_instance
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below
Search our full catalog including 1000s of application and OS images
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-0440d3b780d96b29d
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
19°C Partly cloudy
ENG
00:01
22-02-2024


Launch AWS Academy Learner
EditRoutes | VPC Console
EC2 | us-east-1
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
Services
Search
[Alt+S]
N. Virginia
voclabs/user3012179=sanket.ugale@dctinc.com @ 7218-0928-0952
Network settings Info
VPC - required Info
vpc-0ffaec52b5b39dd21 (my_vpc)
100.100.0.0/16
Subnet Info
subnet-0dbfef20e4bda9bfb my_subnet
VPC: vpc-0ffaec52b5b39dd21 Owner: 721809280952 Availability Zone: us-east-1a
IP addresses available: 251 CIDR: 100.100.1.0/24)
Create new subnet
Auto-assign public IP Info
Disable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Security group name - required
launch-wizard-4
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*
Description - required Info
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-0440d3b780d96b29d
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Review commands
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
19°C
ENG
00:01
22-02-2024



Congratulations now you have created a VPC by which your instance cn access the internet.

AWS IAM Lab (Identity and Access Management)

Amazon Web Services Identity and Access Management (AWS IAM) is a web service that enables secure control and management of access to AWS resources. IAM allows you to create and manage users and their permissions within your AWS account, helping you control who can access specific resources and what actions they can perform.

Key features of AWS IAM include:

1. **Users and Groups:** IAM allows you to create individual IAM users for people accessing your AWS account and organize them into groups for easier management.

2. **Policies:** IAM policies define permissions and specify what actions are allowed or denied on AWS resources. These policies can be attached to users, groups, or roles.

3. **Roles:** IAM roles are similar to users but are meant to be assumed by other AWS entities, such as EC2 instances or Lambda functions. Roles define a set of permissions, and AWS services or users assume these roles to perform specific tasks.

4. **Multi-Factor Authentication (MFA):** IAM supports the use of MFA to add an extra layer of security by requiring users to provide a second form of authentication, in addition to their password, when accessing AWS resources.

5. **Identity Federation:** IAM allows you to integrate with external identity providers, enabling users to sign in using credentials from sources like Active Directory or social identity providers.

6. **Access Advisor:** IAM provides an Access Advisor that helps you identify unused or underutilized permissions within your IAM policies, helping you adhere to the principle of least privilege.

7. **Audit Trail:** IAM maintains an audit trail by logging all API calls made on your account. These logs can be analyzed to track user activity, changes to policies, and other security-relevant events.

By effectively using AWS IAM, organizations can implement strong security practices, ensure least privilege access, and manage access to their AWS resources in a scalable and controlled manner.