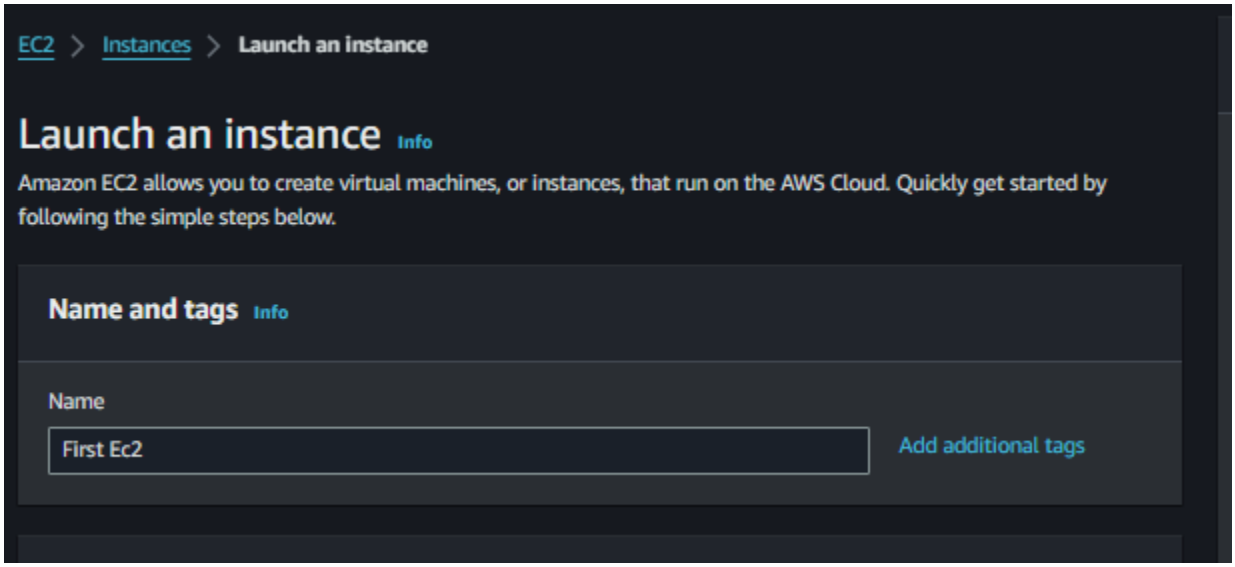
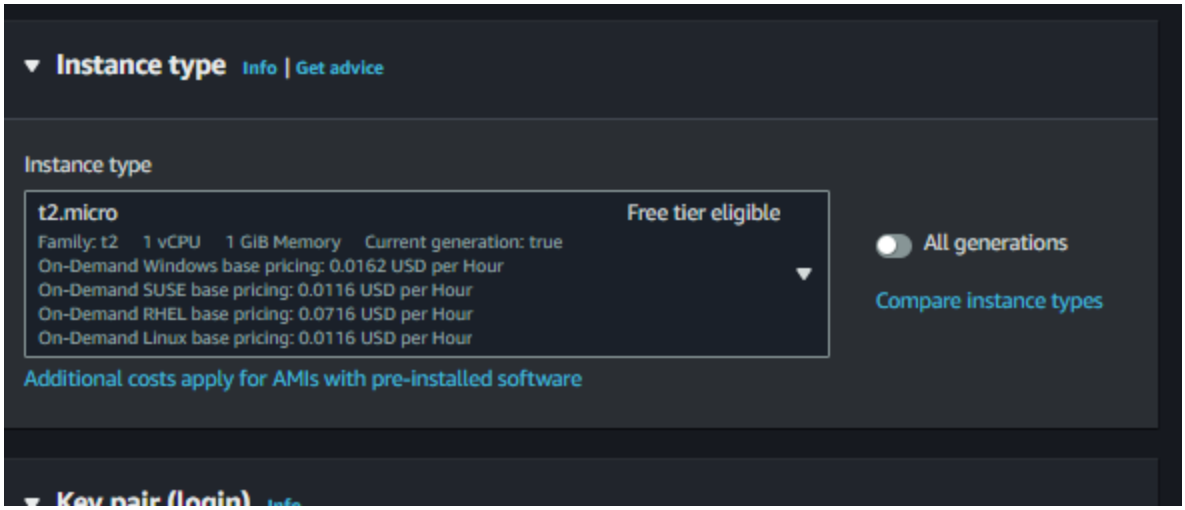
1.EC2 Basics Lab

- **Objective**: To understand the process of setting up and managing an Amazon EC2 instance.
- **Approach**: Students will start by launching a new EC2 instance, selecting an appropriate instance type and configuring the instance details. They will then create and configure a new Security Group, and allocate an Elastic IP address to the instance. The lab will also include connecting to the instance via SSH.
- **Goal**: By the end of this lab, students should be able to launch and manage an EC2 instance, understand instance types, security groups, and IP addressing in AWS.

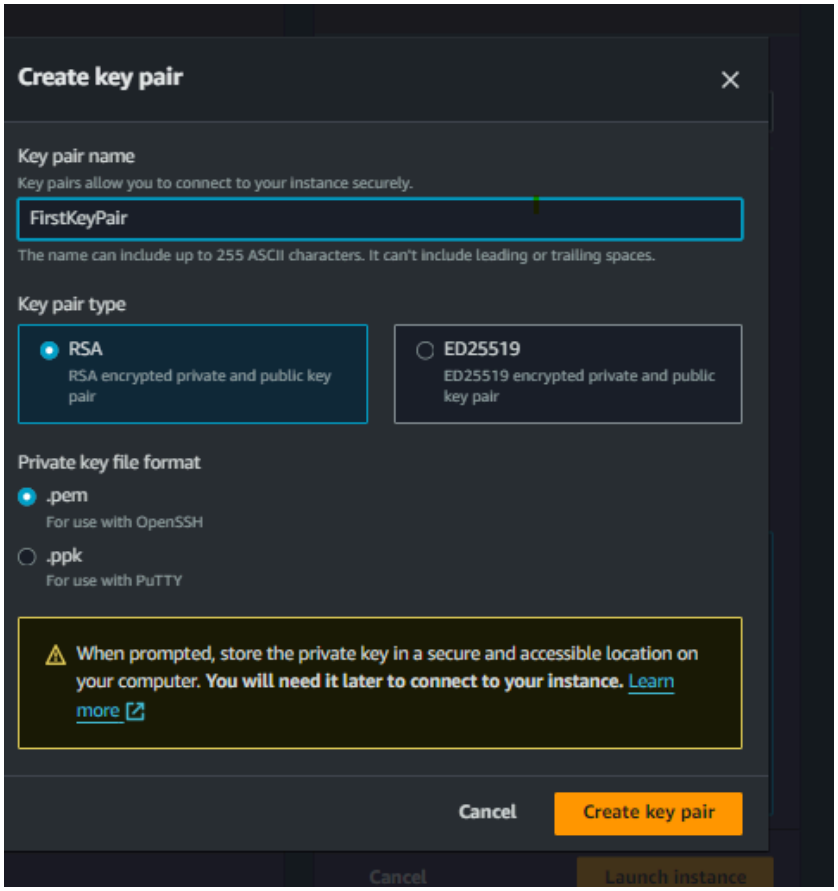
1. Open AWS Console ,select EC2 and Give the EC2 instance name
2. Select OS images and AMI



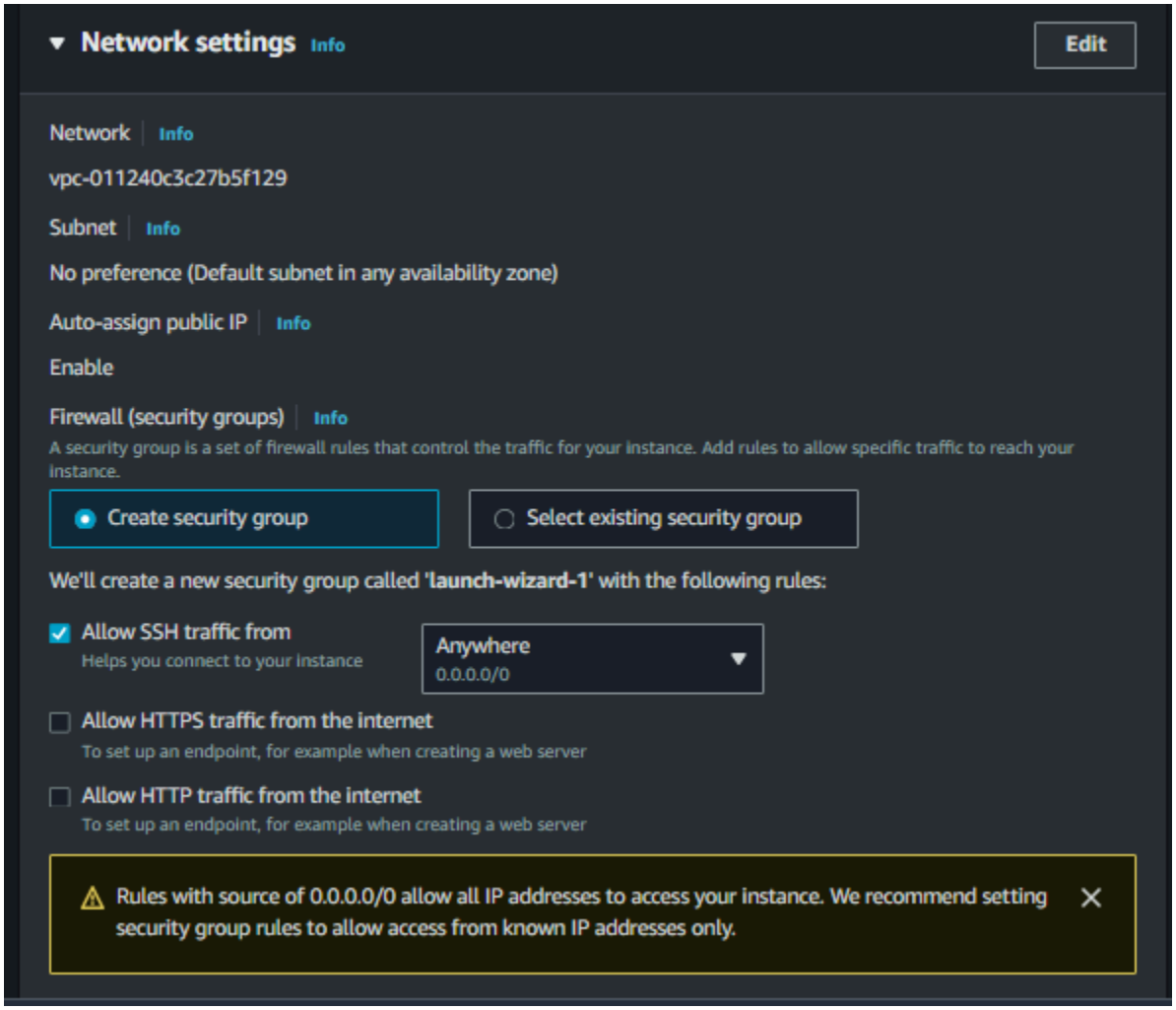
3.Select instance type as t2.micro



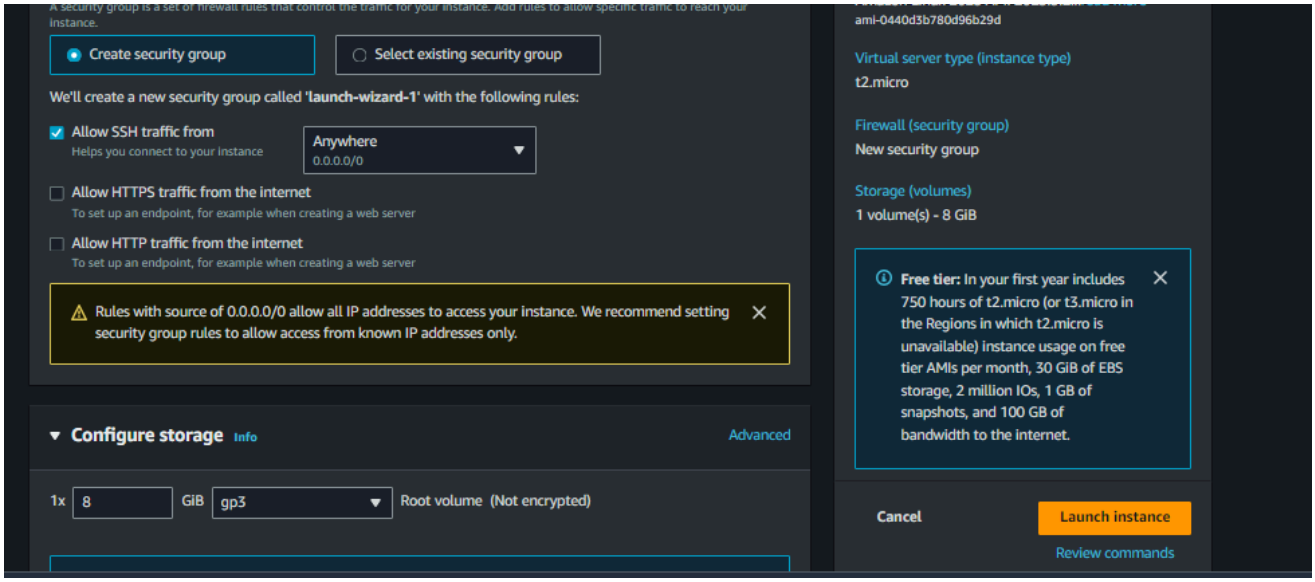
4. Create Key Pair:



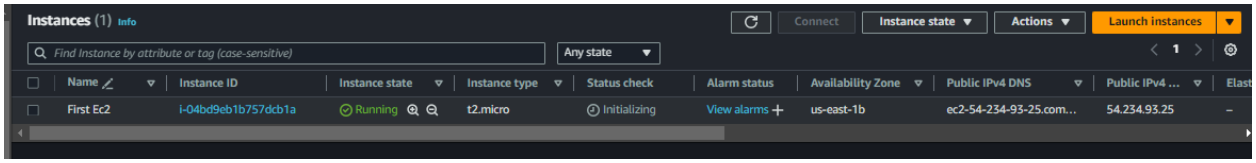
5. Select create security group and edit the rules



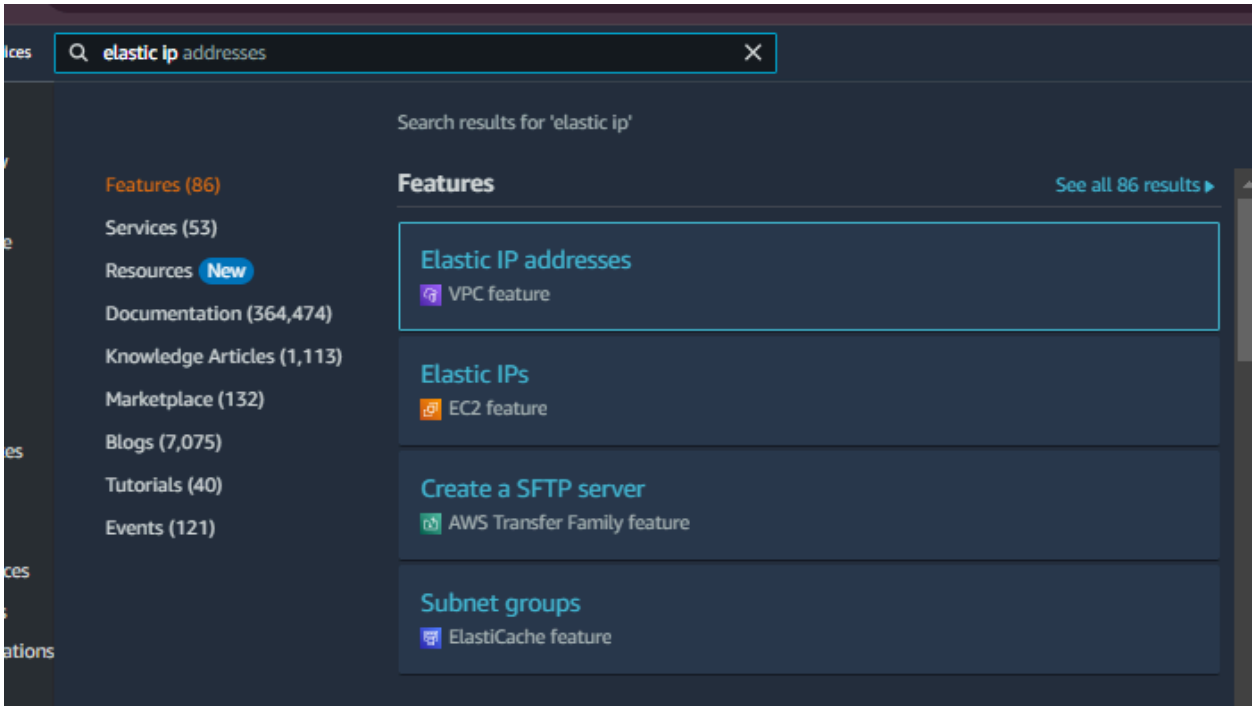
6.Lunch Instance:



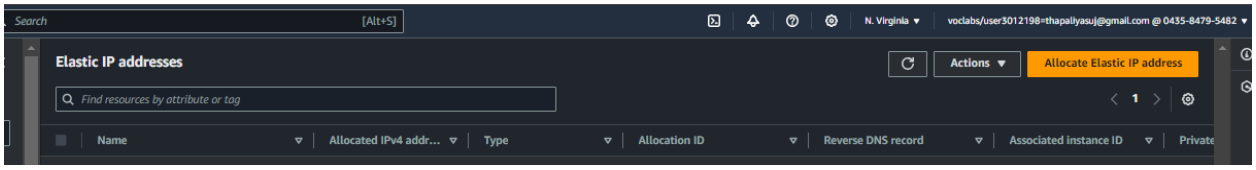
7.Now Instance has been successfully created.



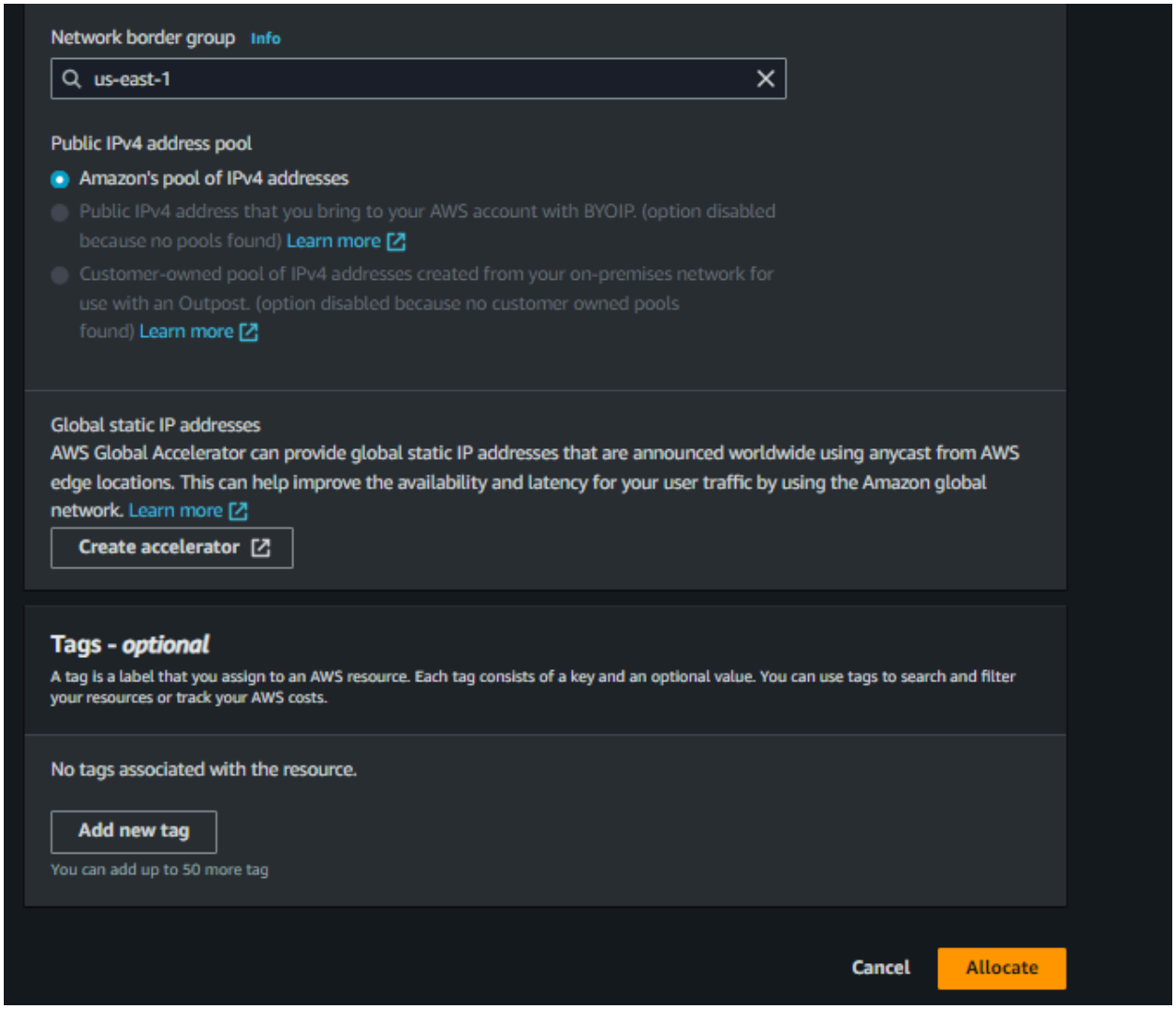
8.Now we adding the Elastic IP address:



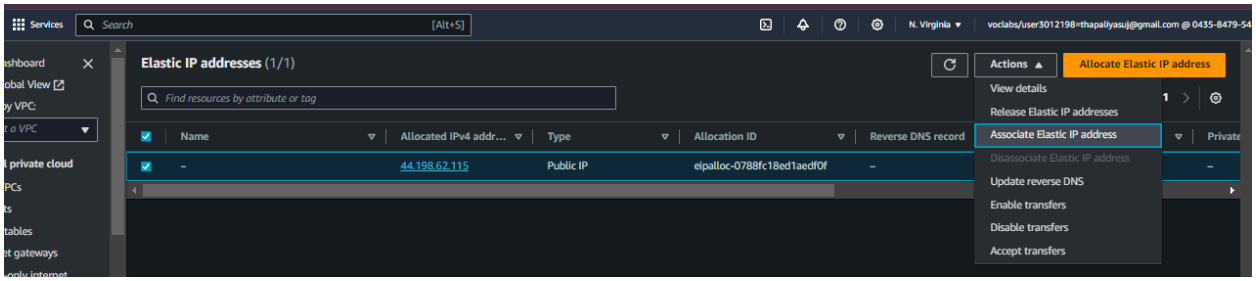
9.Allocate Elastic ip address



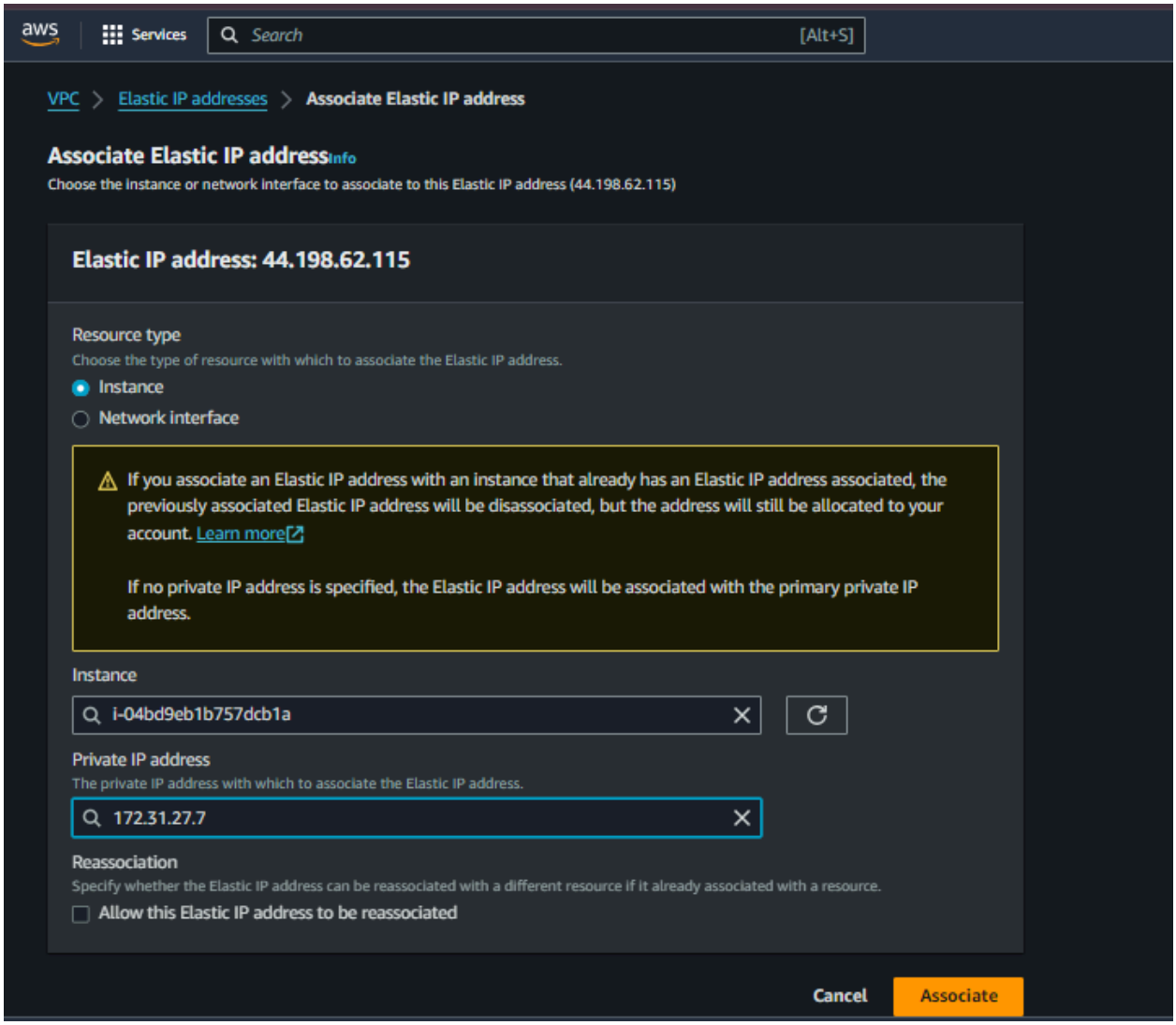
10.Select IPv4 to set IP address



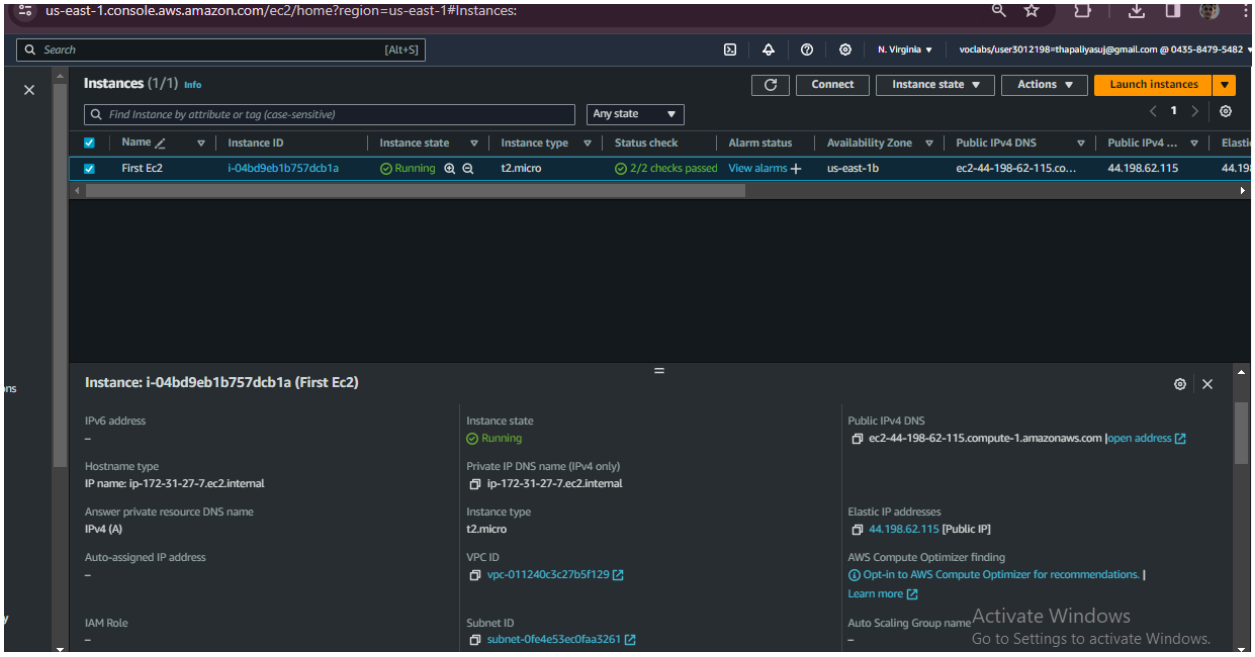
11.click action and select associate elastic ip address



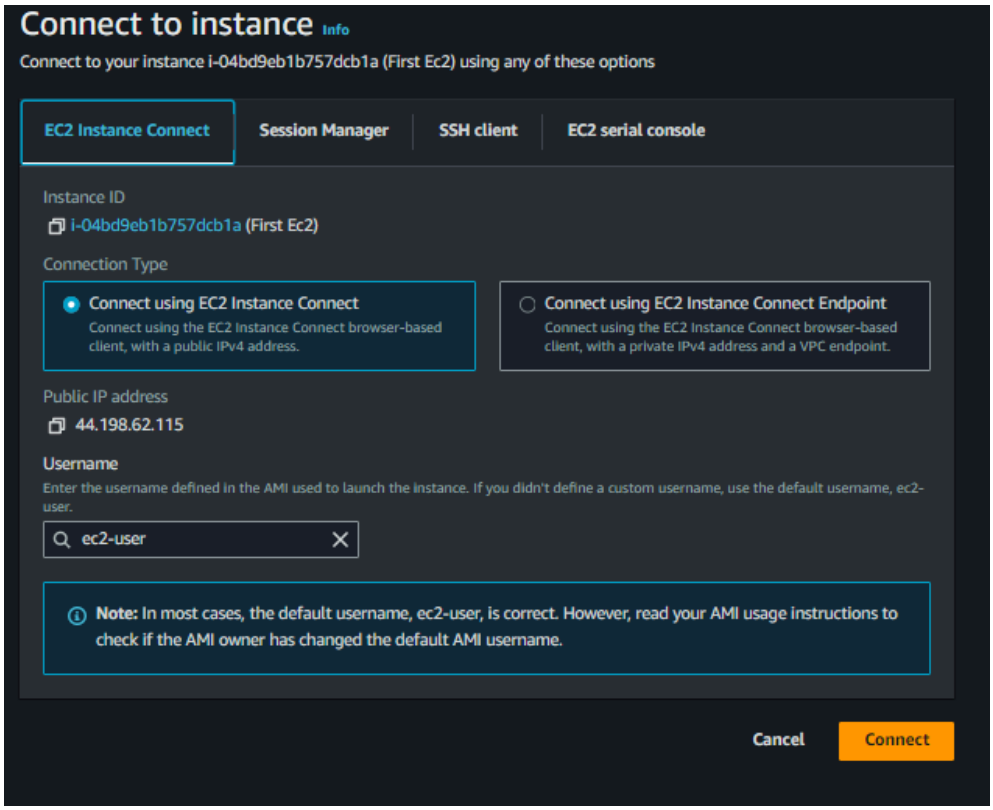
12.Select the EC2 instance and click associate

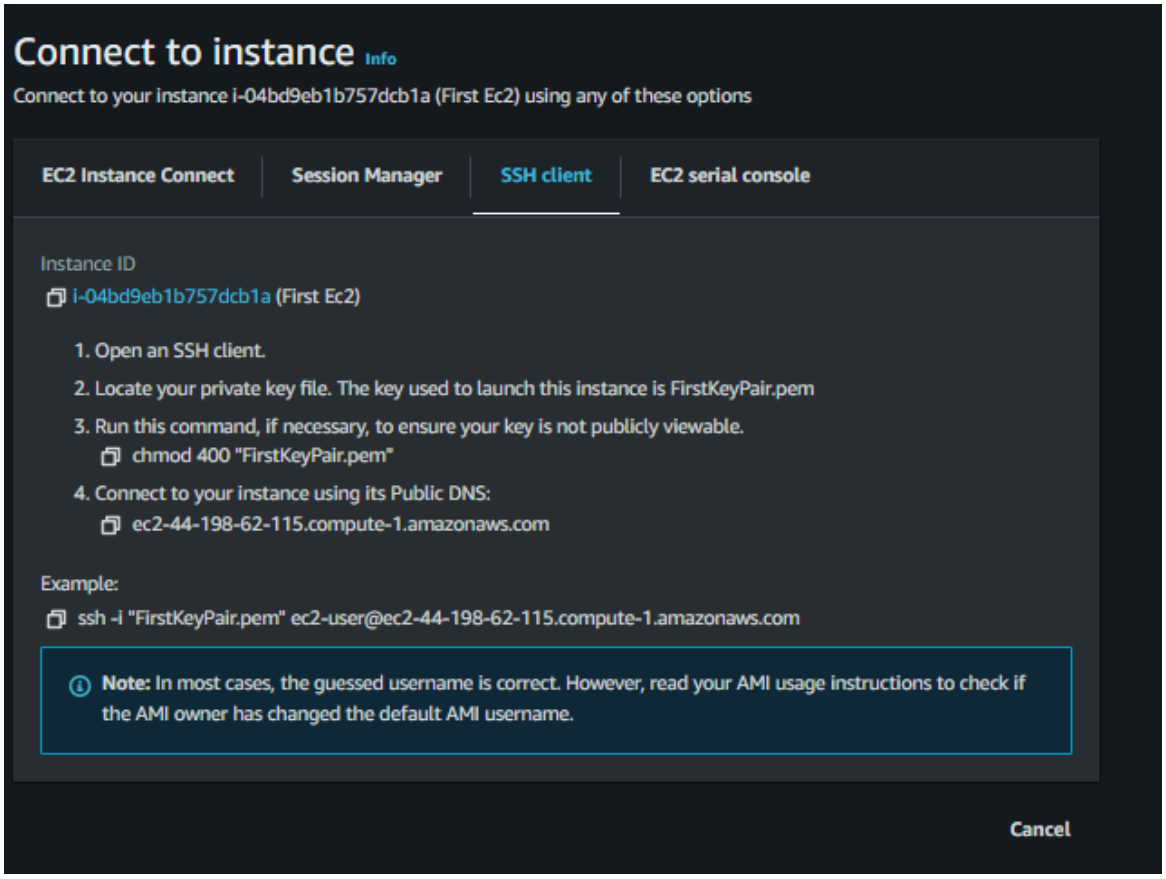


13.Now we can see the ec2 is assign in IP

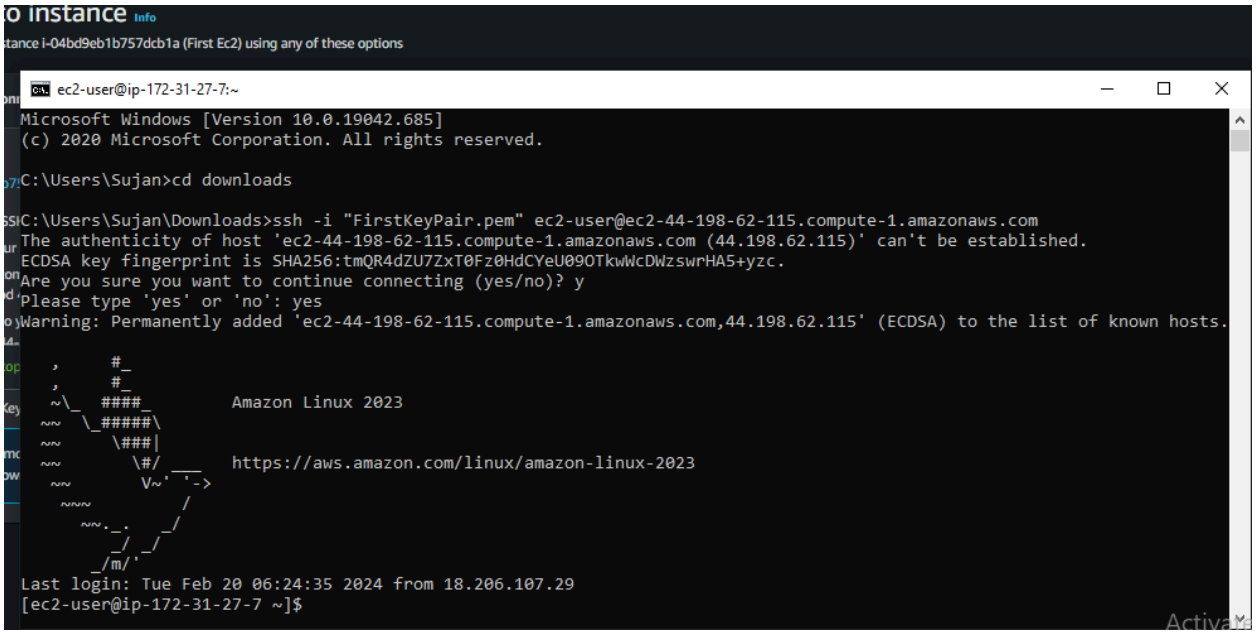


14. To connect to the ec2 instance via ssh with .pem file



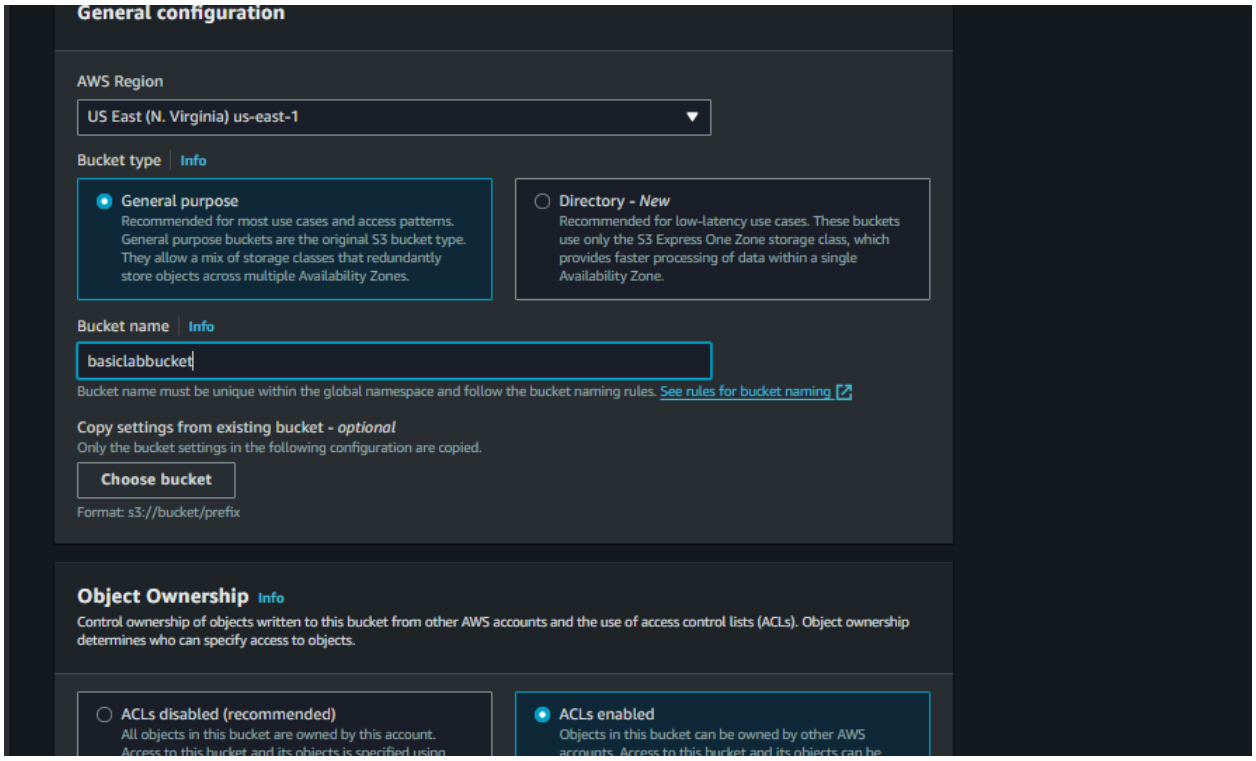


15.EC2 Instance Connect loads in a new page



2. **S3 Storage Fundamentals Lab**
    - **Objective**: To gain hands-on experience with Amazon S3 by performing basic storage operations.
    - **Approach**: This lab involves creating an S3 bucket, uploading files to it, and setting up bucket policies for access control. Students will explore the S3 management console, learn about object storage, and understand the concepts of buckets and objects.
    - **Goal**: Students will understand how to use S3 for storing and managing data, learn about S3 security and permissions, and become familiar with S3's user interface.

1.Go to the AWS Console and select S3 Click create bucket to create the S3 bucket and give unique bucket name:



Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

- ○ **ACLs disabled (recommended)**
  All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
- ◉ **ACLs enabled**
  Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

⚠ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

Object Ownership

- ◉ **Bucket owner preferred**
  If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.
- ○ **Object writer**
  The object writer remains the object owner.

ⓘ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more

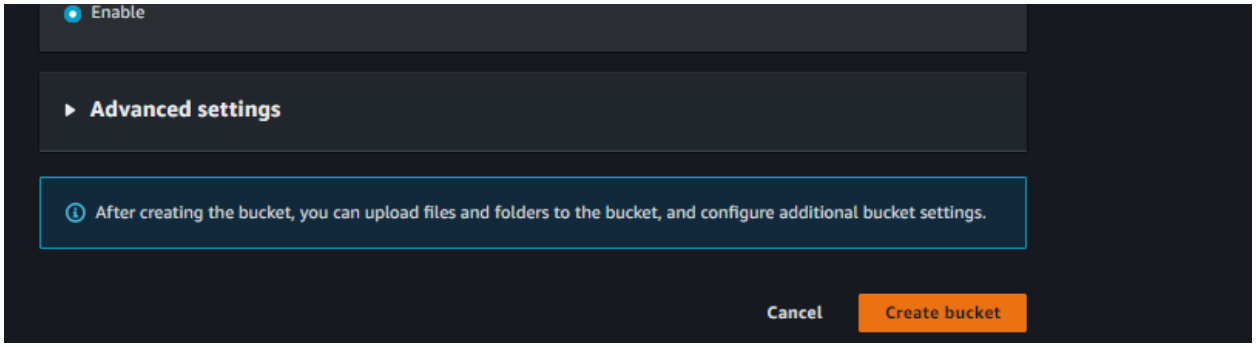
applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

- ☐ **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.

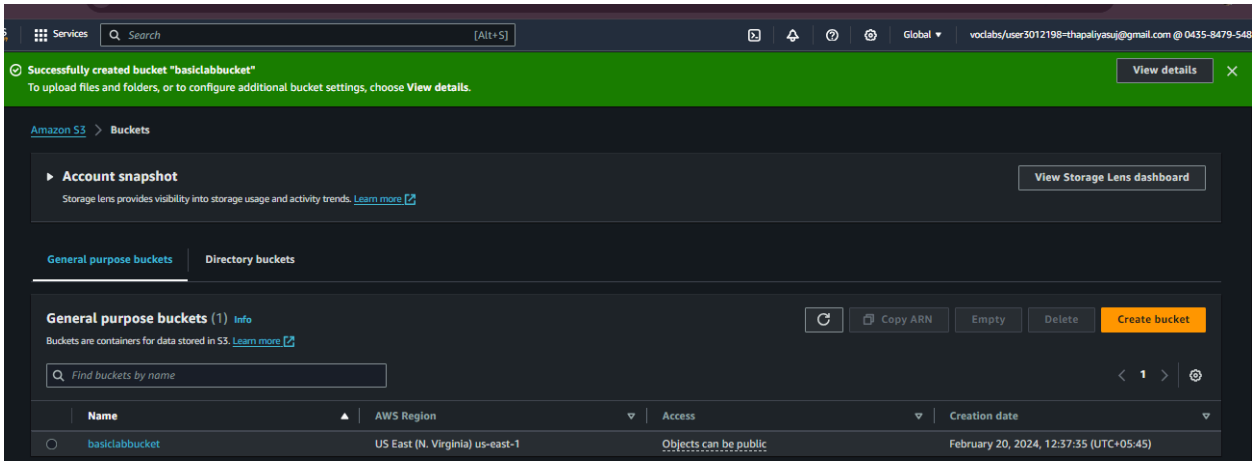
⚠ **Turning off block all public access might result in this bucket and the objects within becoming public**
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☑ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

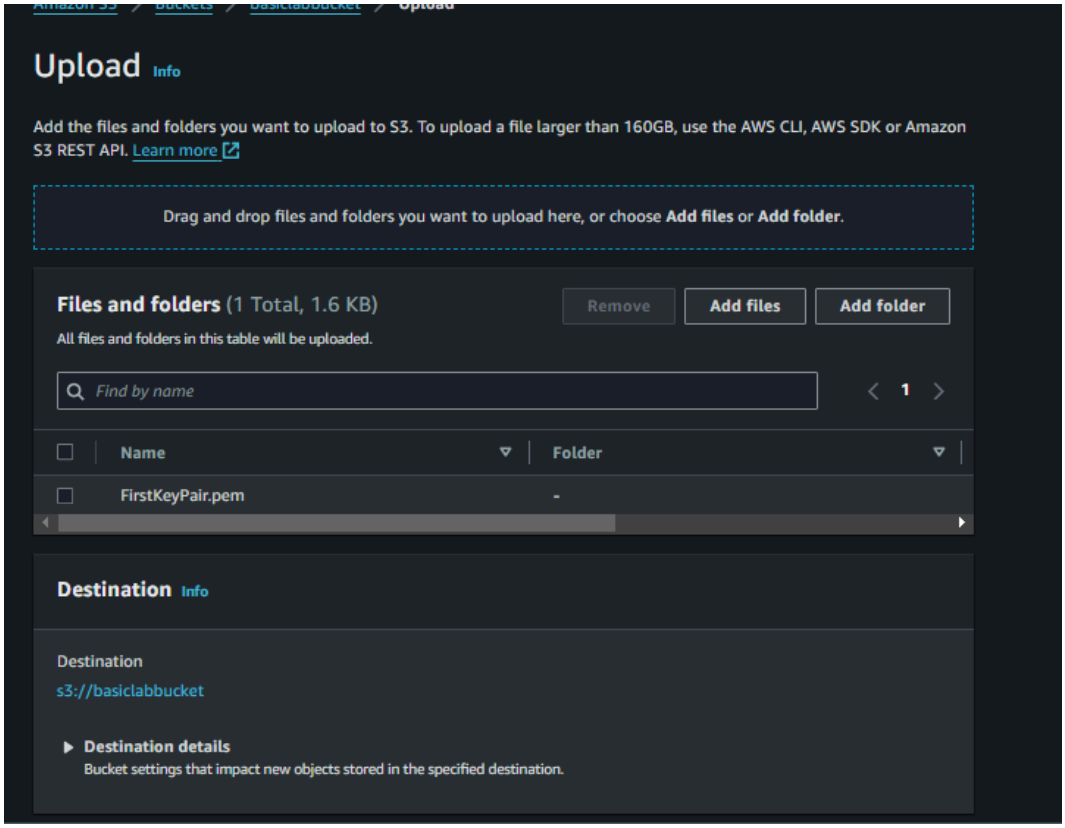
2. Click create bucket

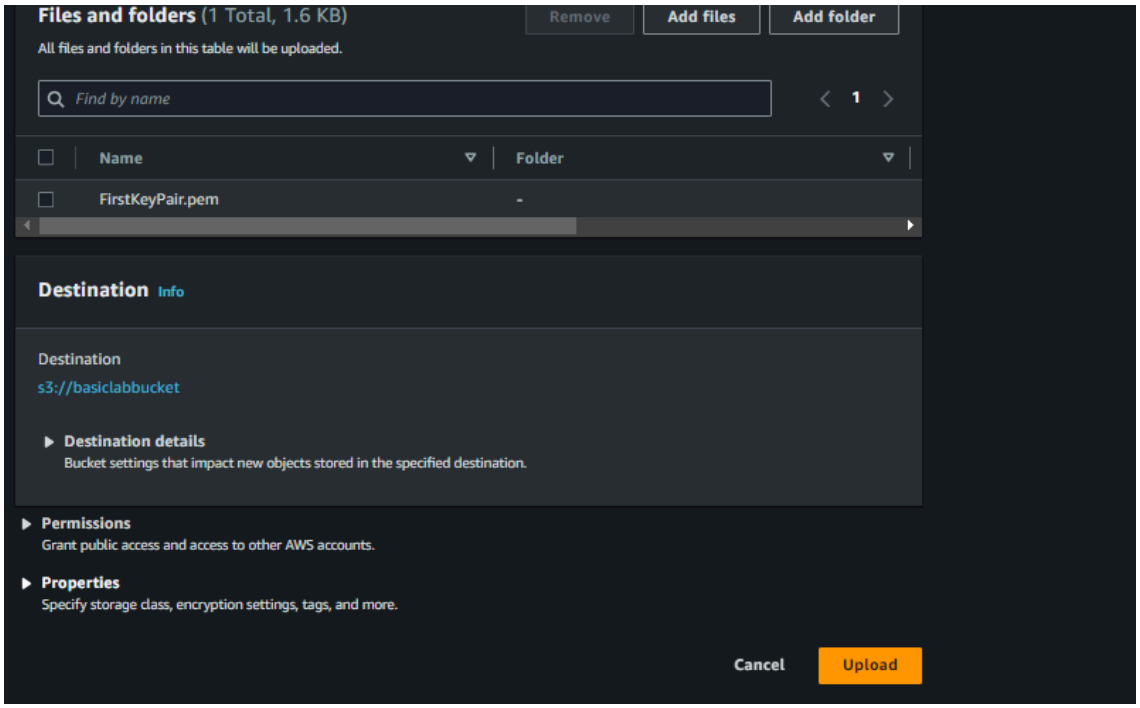


3.Bucket created successfully:

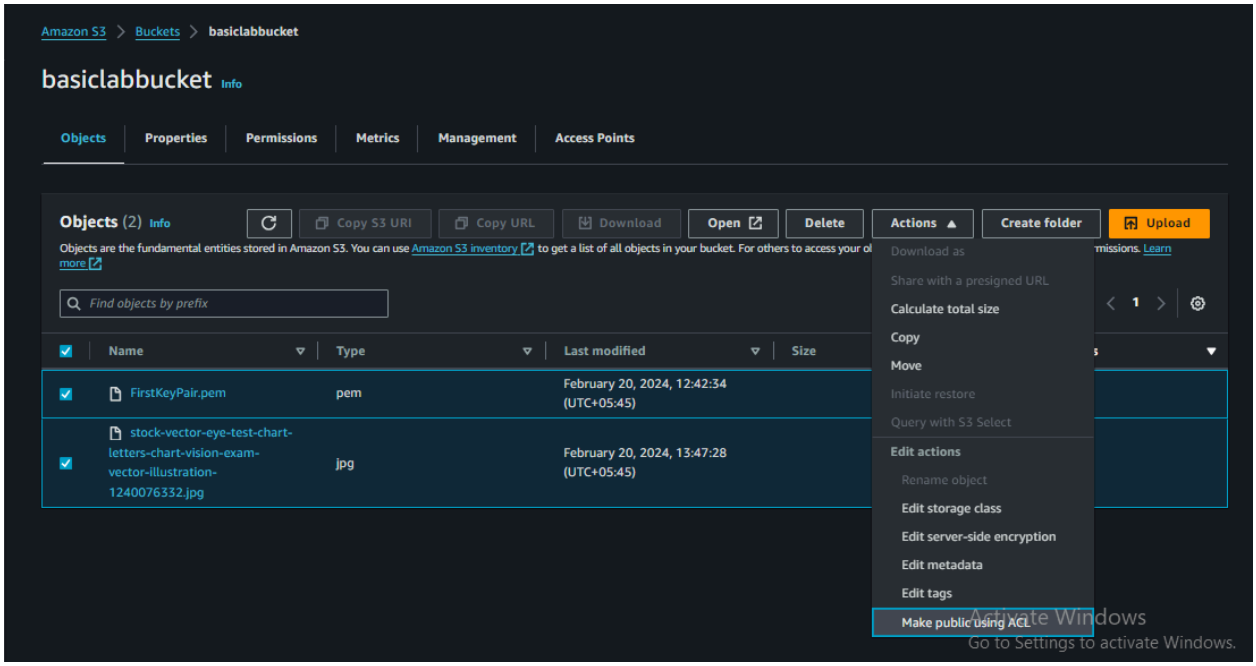


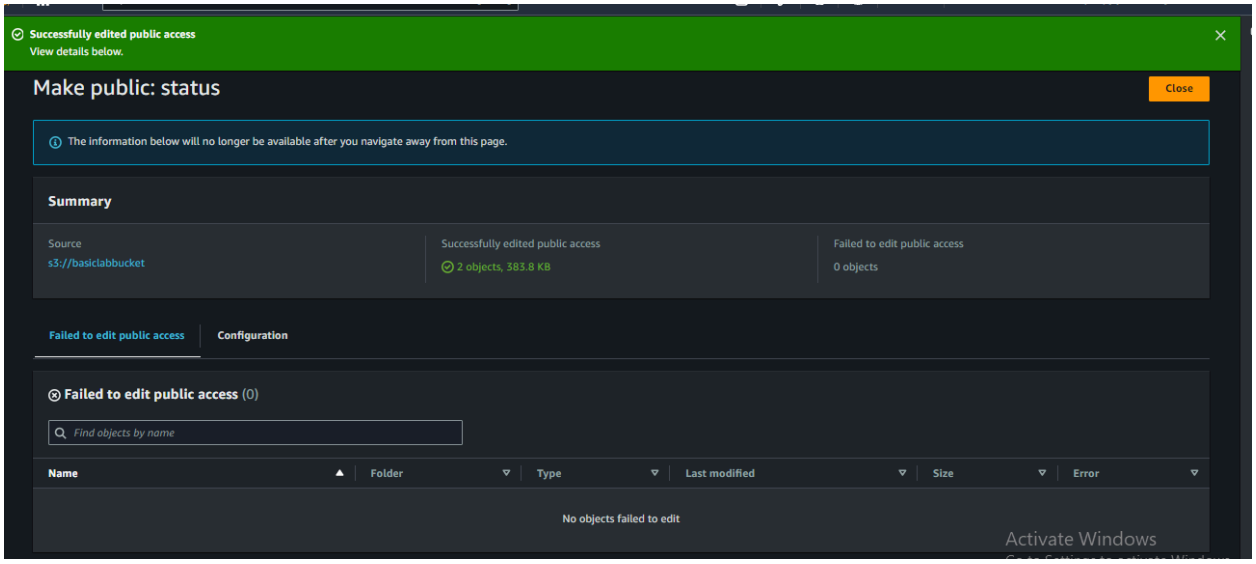
4. Click upload to upload the file





5.Make public using ACL:(Bucket Policy)





6. Now access the bucked through public URL

stock-vector-eye-test-chart-letters-chart-vision-exam-vector-illustration-1240076332.jpg Info

Copy S3 URI | Download | Open | Object actions

Properties | Permissions | Versions

Object overview

Owner
awslabsc0w6979356t1703207674

AWS Region
US East (N. Virginia) us-east-1

Last modified
February 20, 2024, 13:47:28 (UTC+05:45)

Size
382.2 KB

Type
jpg

Key
stock-vector-eye-test-chart-letters-chart-vision-exam-vector-illustration-1240076332.jpg

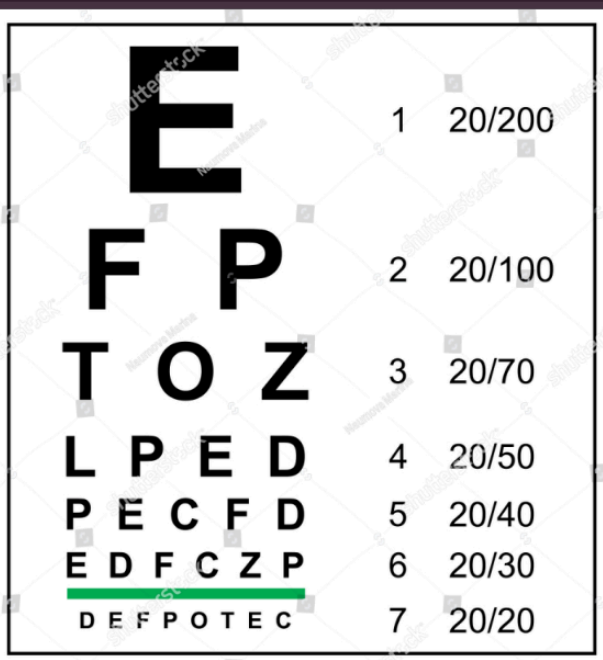
S3 URI
s3://basiclabbucket/stock-vector-eye-test-chart-letters-chart-vision-exam-vector-illustration-1240076332.jpg

Amazon Resource Name (ARN)
arn:aws:s3:::basiclabbucket/stock-vector-eye-test-chart-letters-chart-vision-exam-vector-illustration-1240076332.jpg

Entity tag (Etag)
6612fb586a986670e754640f5ad8818a

Object URL
https://basiclabbucket.s3.amazonaws.com/stock-vector-eye-test-chart-letters-chart-vision-exam-vector-illustration-1240076332.jpg

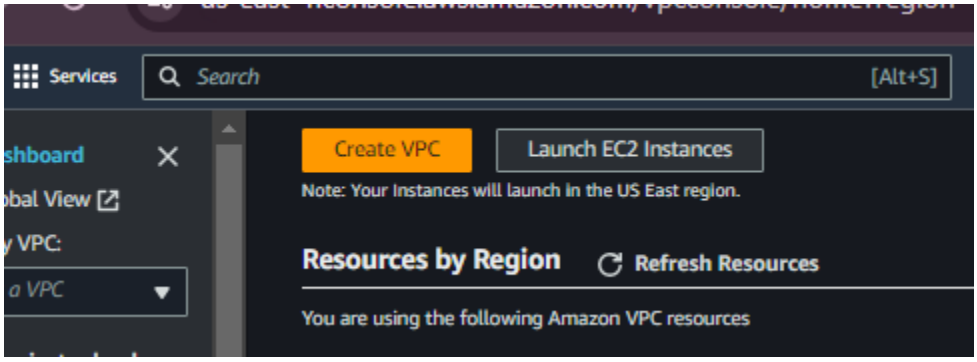
basiclabbucket.s3.amazonaws.com/stock-vector-eye-test-chart-letters-chart-vision-exam-vector-illustration-1240076332.jpg



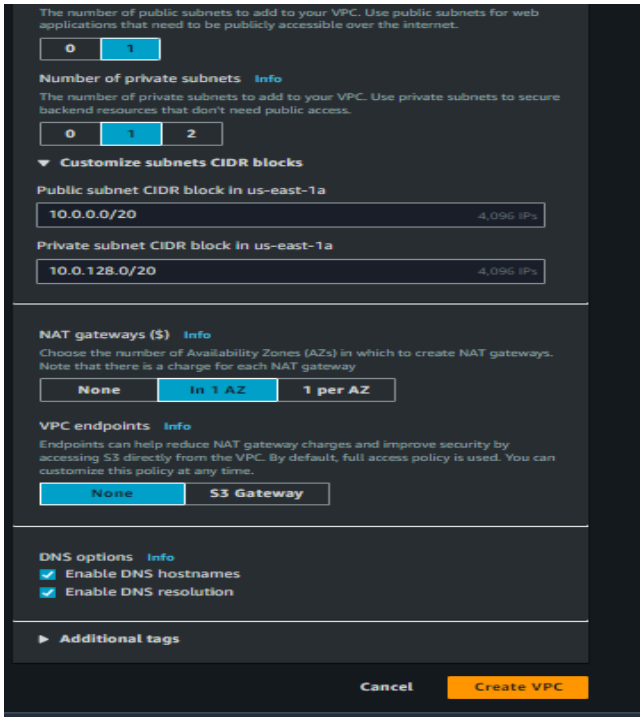
3. VPC Configuration Lab

- **Objective**: To understand the fundamentals of AWS networking through the configuration of a Virtual Private Cloud (VPC).
- **Approach**: Students will create a new VPC, add subnets, set up an Internet Gateway, and configure route tables. The lab might also include setting up a simple EC2 instance within this VPC to demonstrate how resources are deployed in a custom network environment.
- **Goal**: By the end of this lab, students should be able to create and configure a VPC, understand subnetting, and the role of route tables and internet gateways in AWS.

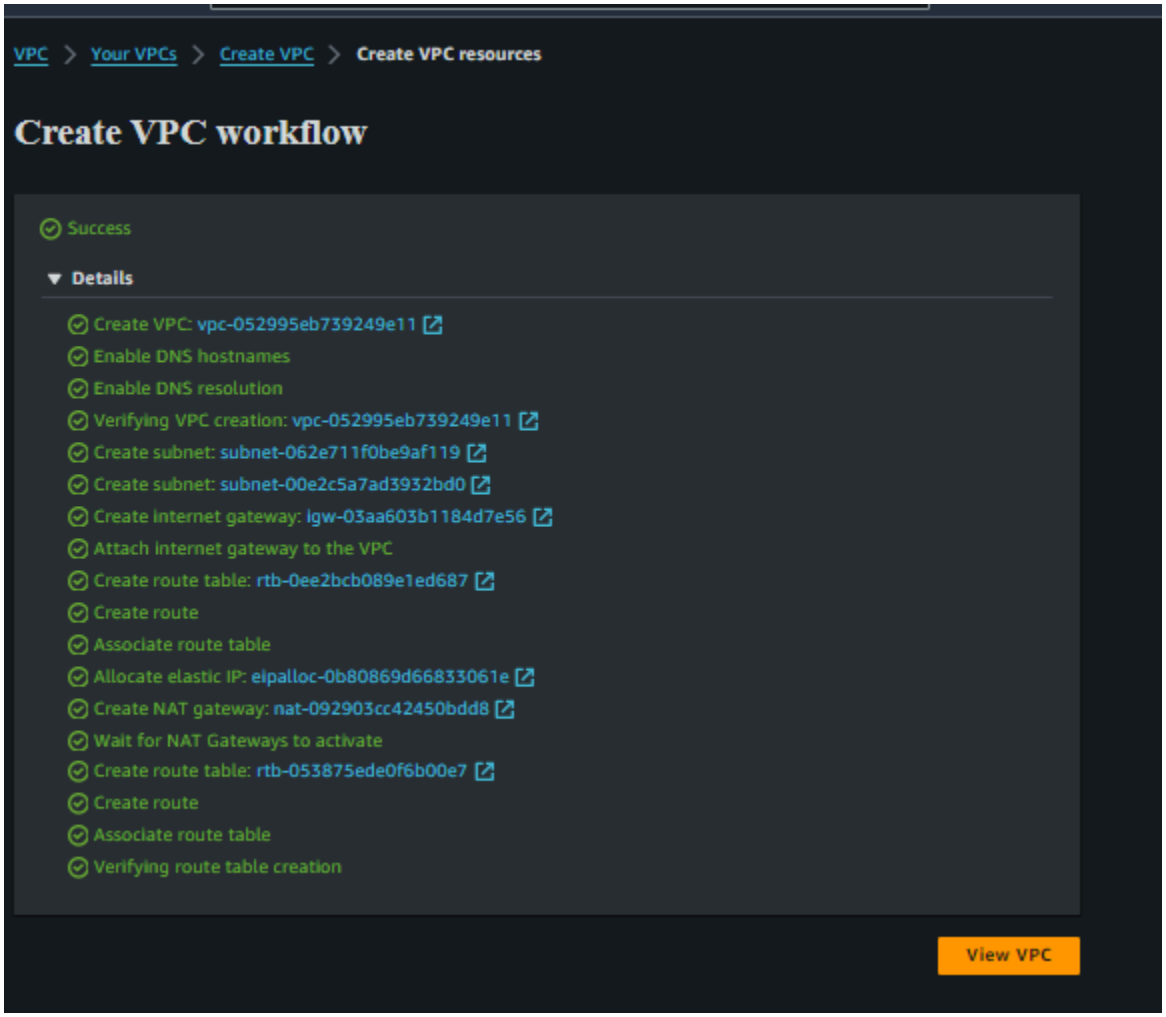
1.Open AWS Console and search for VPC and click create VPC

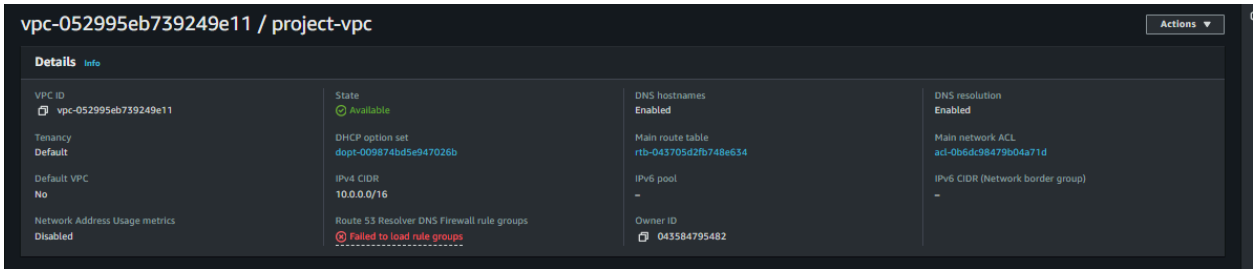



Create VPC Info
VPC is an isolated portion of the AWS Cloud populated by AWS objects, such
VPC settings
Resources to create Info
Create only the VPC resource or the VPC and other networking resources.
VPC only
VPC and more
Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.
Auto-generate
lab
IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
10.0.0.0/16
65,536 IPs
CIDR block size must be between /16 and /28.
IPv6 CIDR block Info
No IPv6 CIDR block
Amazon-provided IPv6 CIDR block
Tenancy Info
Default

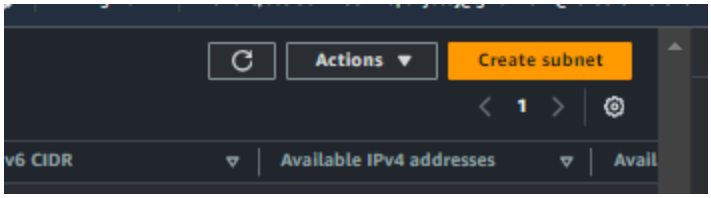

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.
0
1
Number of private subnets Info
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.
0
1
2
Customize subnets CIDR blocks
Public subnet CIDR block in us-east-1a
10.0.0.0/20
4,096 IPs
Private subnet CIDR block in us-east-1a
10.0.128.0/20
4,096 IPs
NAT gateways ($) Info
Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway
None
In 1 AZ
1 per AZ
VPC endpoints Info
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.
None
S3 Gateway
DNS options Info
Enable DNS hostnames
Enable DNS resolution
Additional tags
Cancel
Create VPC

2.Click create VPC and the VPC will be created in a while

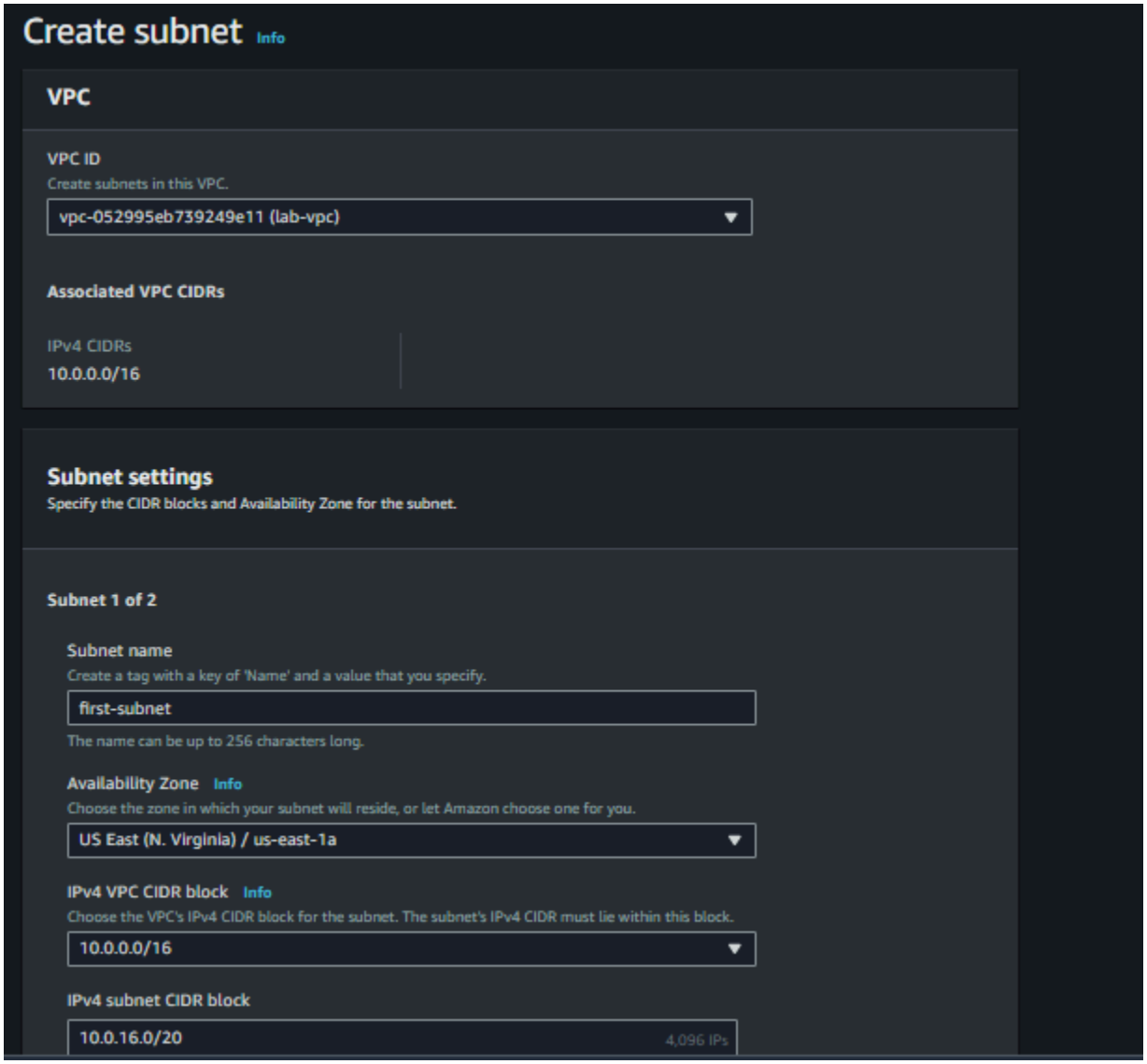


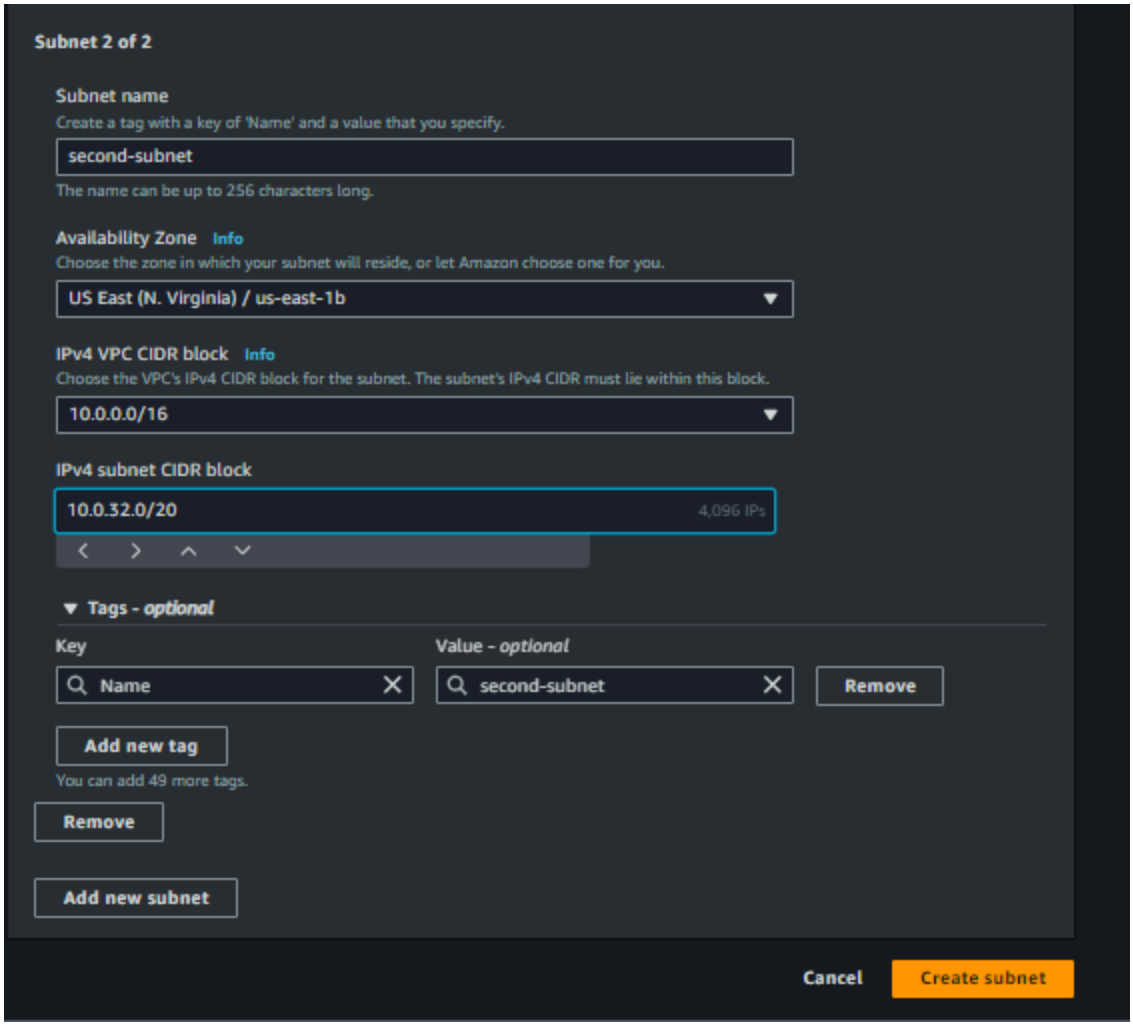


3.To add Subnets, click Subnet and create :

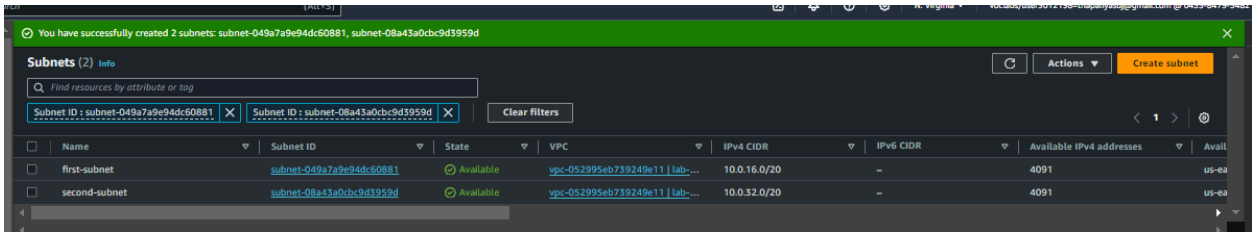


8. Select the created VPC .Now give subnet name, availability zone, and add the IPv4-CIDR subnet

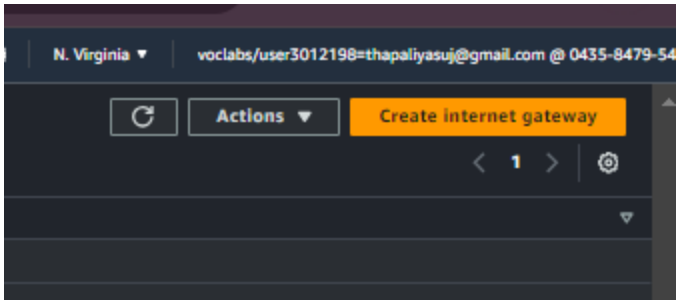


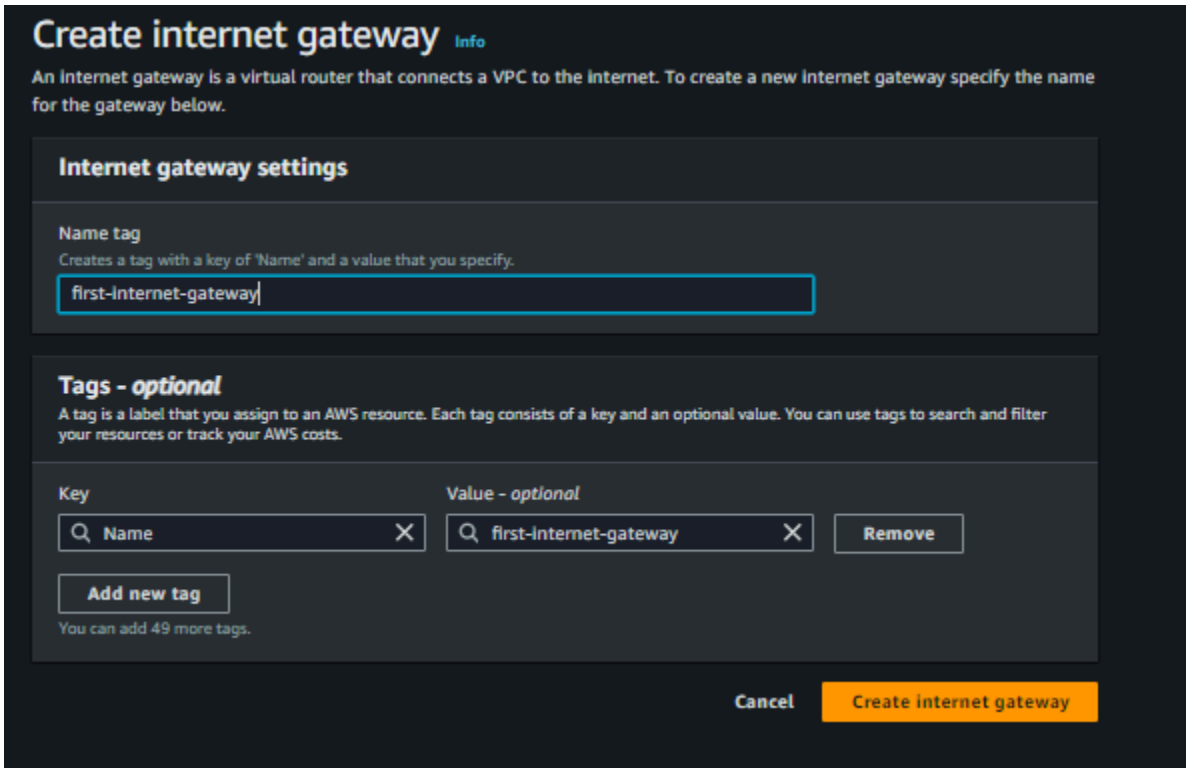


9.Subnets created:

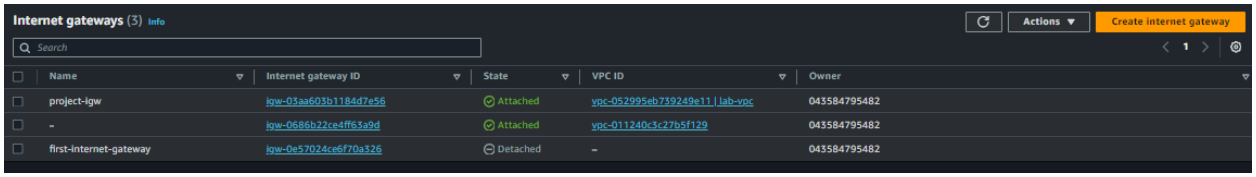


10.To set up the Internet Gateway, select Internet gateway from left-bar and select Create internet gateway

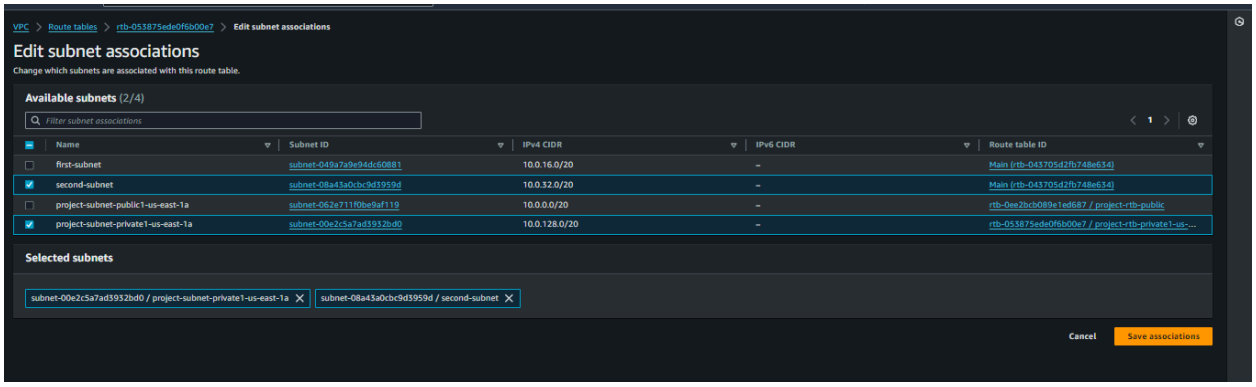


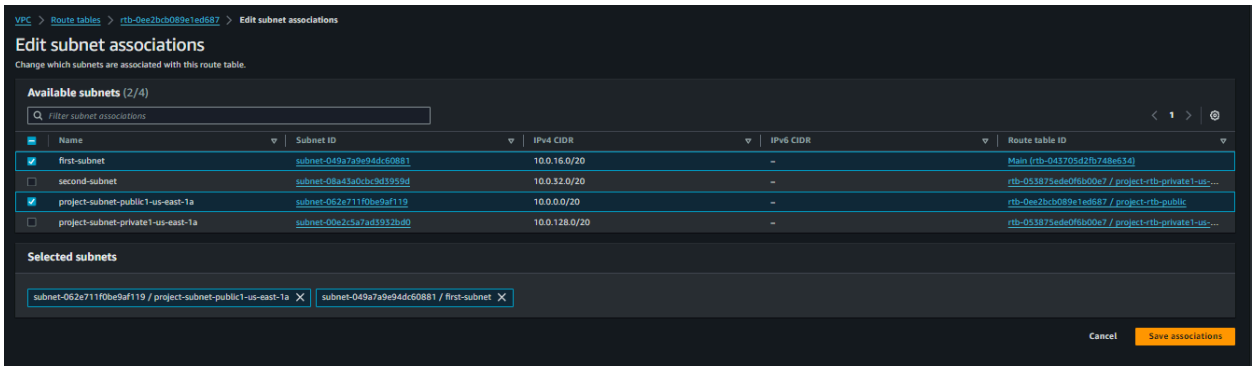


11.Internet gateway created:

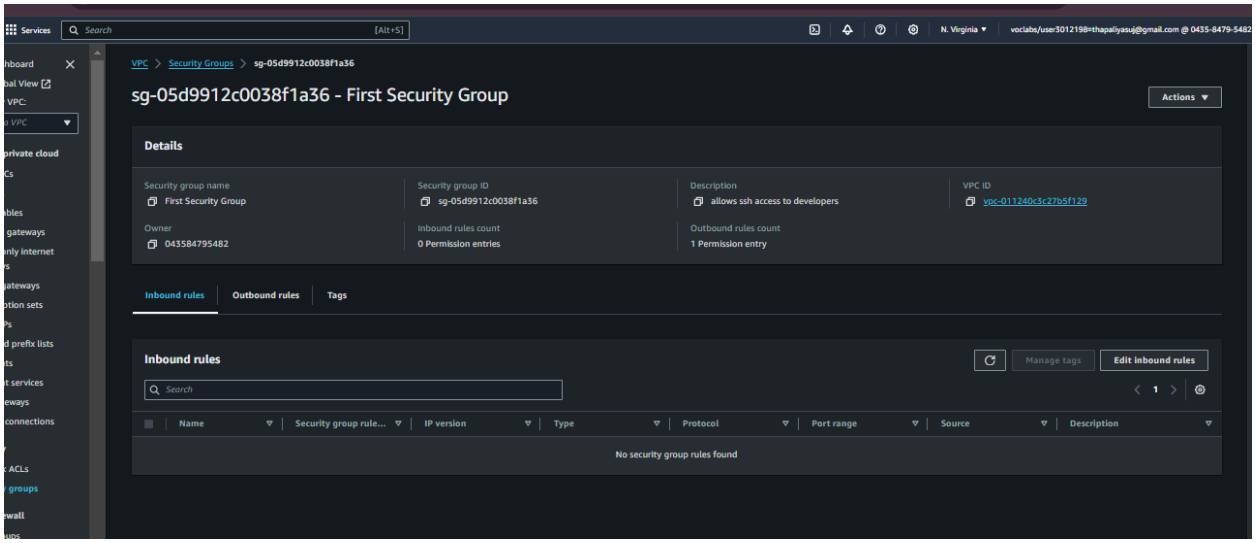


12.Configure the Route table by clicking on the Route Table and select the lab session.





13.Create Security Group with necessary rule for the VPC



14.Now create a EC2 instance with the created security group and the VPC And launch

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

ec2 for vpc

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

Recents | Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | SUSE I

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible

ami-0440d3b780d96b29d (64-bit (x86), uefi-preferred) / ami-0f93c02efd1974b8b (64-bit (Arm), uefi)

Network settings Info

Edit

Network Info

vpc-011240c3c27b5f129

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

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

Common security groups Info

Select security groups

First Security Group sg-05d9912c0038f1a36

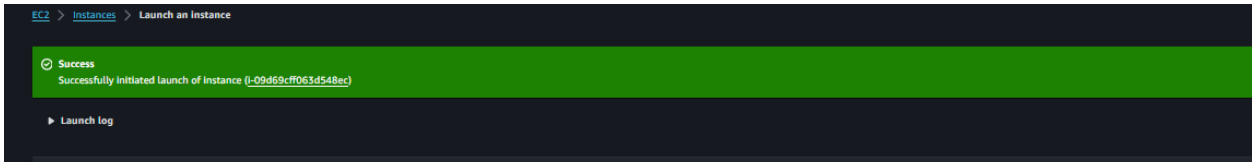
VPC: vpc-011240c3c27b5f129

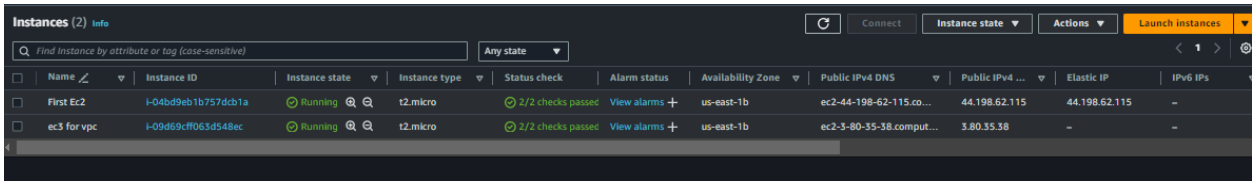
Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

Configure storage Info

Advanced

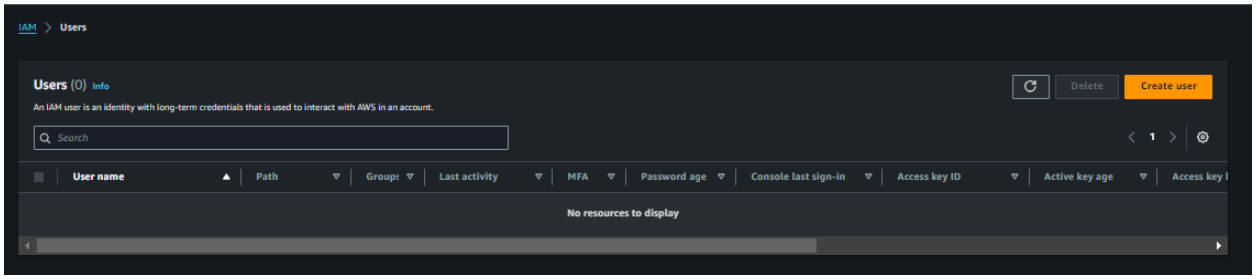


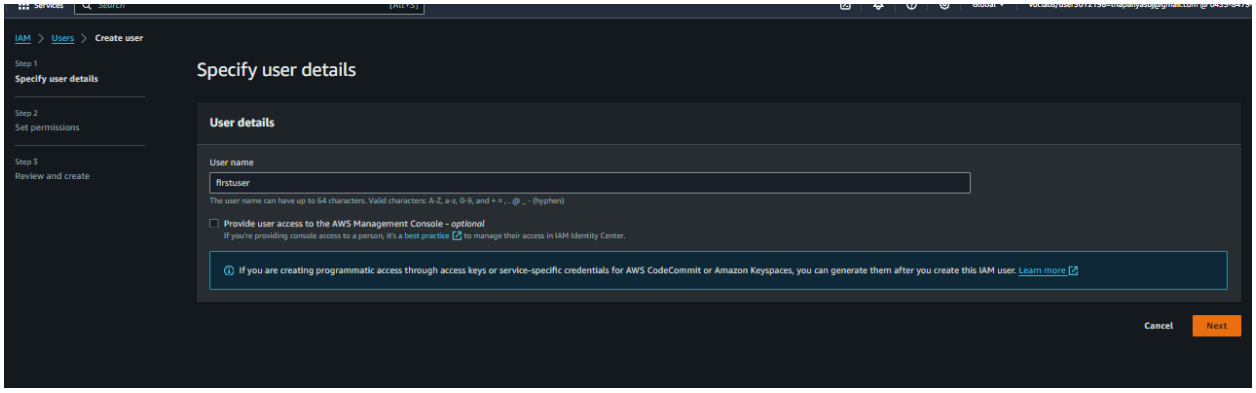


4. **IAM Users and Roles Lab**

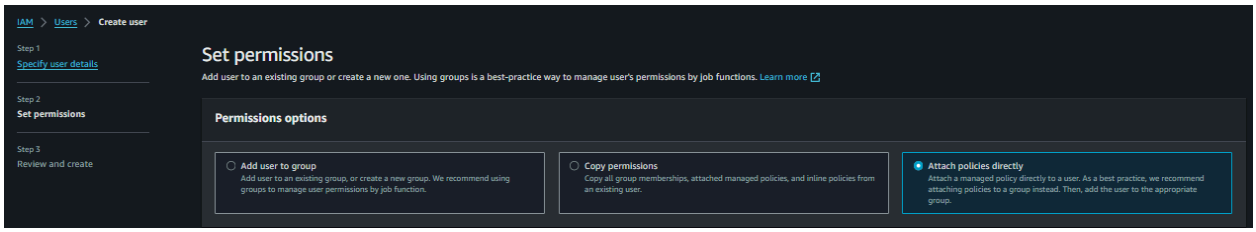
- **Objective**: To understand AWS Identity and Access Management (IAM) by creating and managing users, groups, and roles.
- **Approach**: Students will create new IAM users, assign them to groups, and apply policies to manage permissions. The lab will also involve creating roles for AWS services and understanding the use of IAM roles for cross-service access.
- **Goal**: Students will learn about user and permission management in AWS, the importance of roles for security and best practices for IAM.

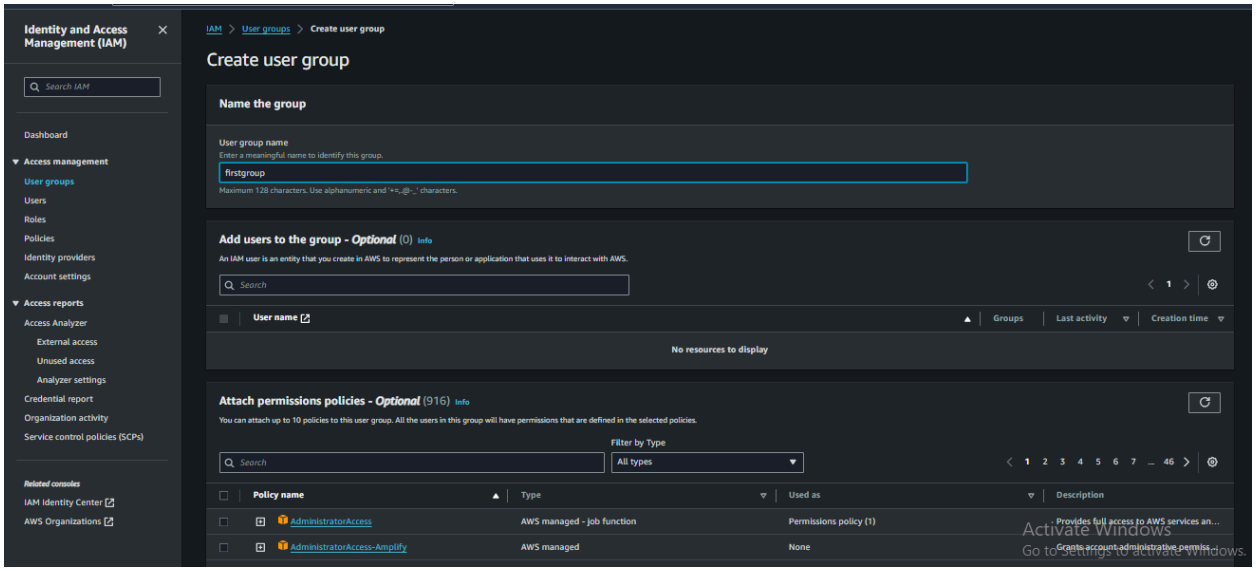
1. Create a IAM User first, to create this, open the AWS Console Management tab and search for IAM. Click the User on the left side and create IAM user with necessary attribute

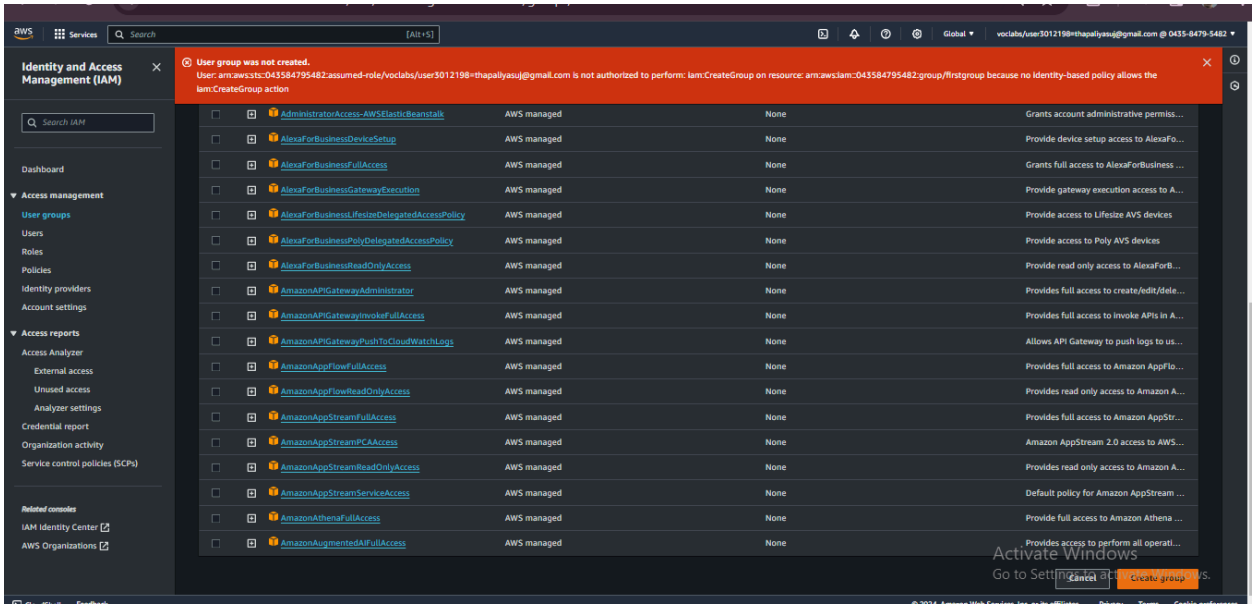




2. Attach the policy for that user, you have to select attach policies directly radio button to do so






Identity and Access Management (IAM)
User group was not created.
User: arn:aws:sts::043584795482:assumed-role/voclabs/user3012198=thapaliyasuj@gmail.com is not authorized to perform: iam:CreateGroup on resource: arn:aws:iam::043584795482:group/firstgroup because no identity-based policy allows the iam:CreateGroup action
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies (SCPs)
Related consoles
IAM Identity Center
AWS Organizations
AdministratorAccess-AWSElasticBeanstalk
AlexaForBusinessDeviceSetup
AlexaForBusinessFullAccess
AlexaForBusinessGatewayExecution
AlexaForBusinessLifesizeDelegatedAccessPolicy
AlexaForBusinessPolyDelegatedAccessPolicy
AlexaForBusinessReadOnlyAccess
AmazonAPIGatewayAdministrator
AmazonAPIGatewayInvokeFullAccess
AmazonAPIGatewayPushToCloudWatchLogs
AmazonAppFlowFullAccess
AmazonAppFlowReadOnlyAccess
AmazonAppStreamFullAccess
AmazonAppStreamPCAAccess
AmazonAppStreamReadOnlyAccess
AmazonAppStreamServiceAccess
AmazonAthenaFullAccess
AmazonAugmentedAIFullAccess
Cancel
Create group