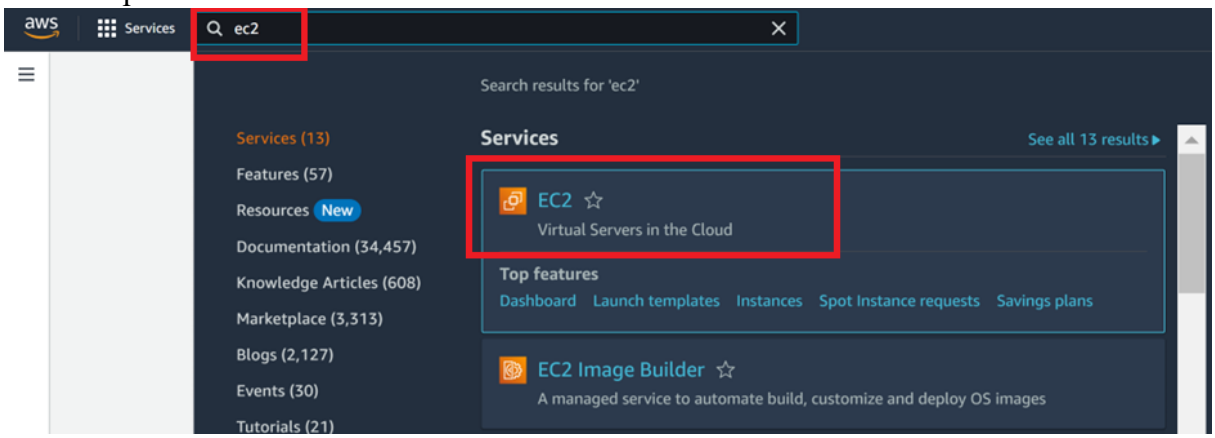
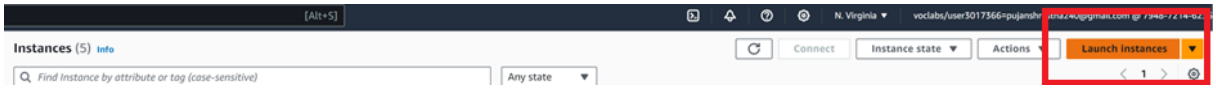
1. **EC2 Basics Lab**
    - **Objective**: To understand the process of setting up and managing an Amazon EC2 instance.
    - **Approach**: Students will start by launching a new EC2 instance, selecting an appropriate instance type and configuring the instance details. They will then create and configure 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 and select EC2





2. Prompts to a new page, follow the steps below:

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

bootcamp

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 Li

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible

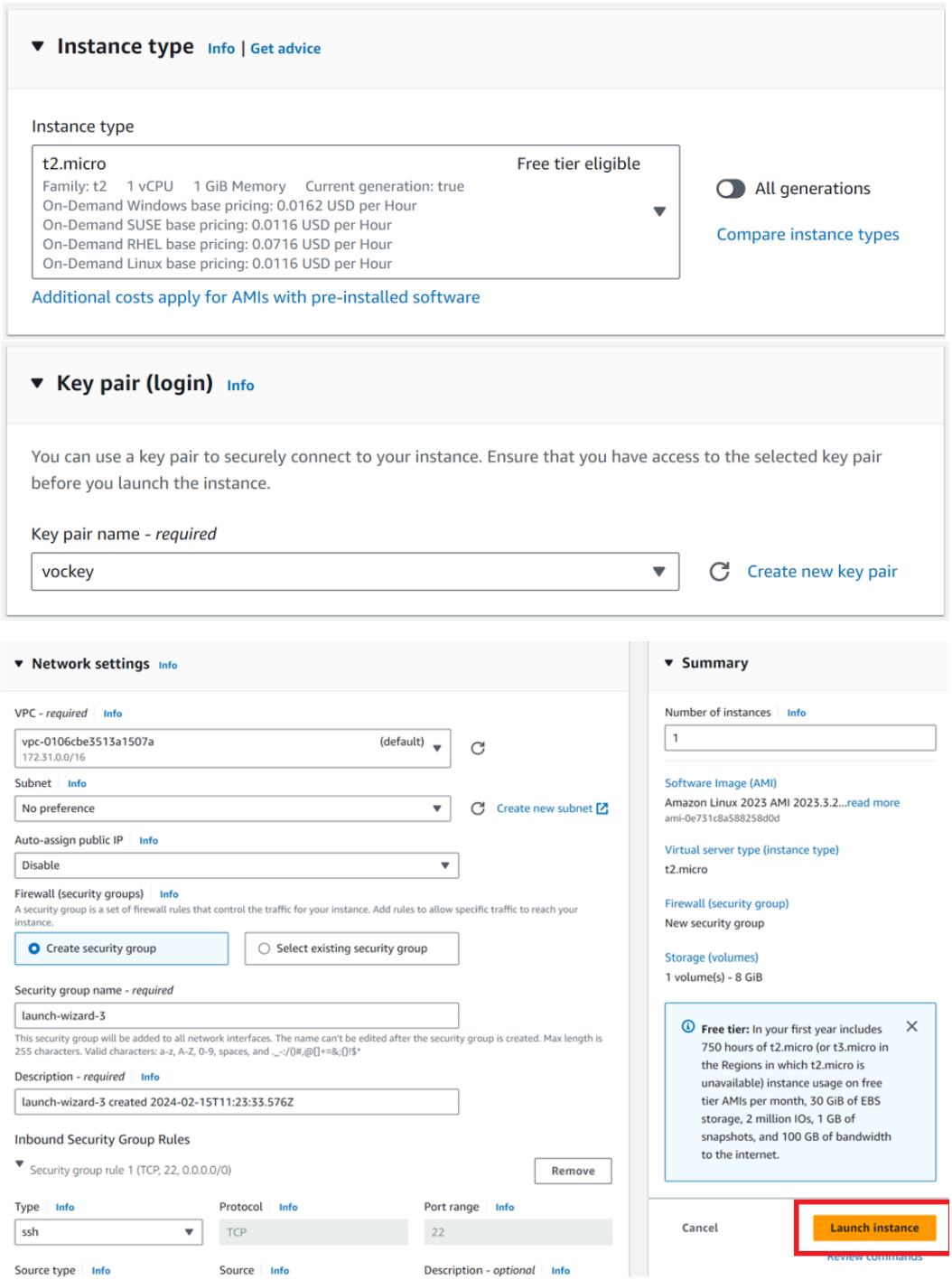
ami-0e731c8a588258d0d (64-bit (x86), uefi-preferred) / ami-0bbebc09f0a12d4d9 (64-bit (Arm), uefi)

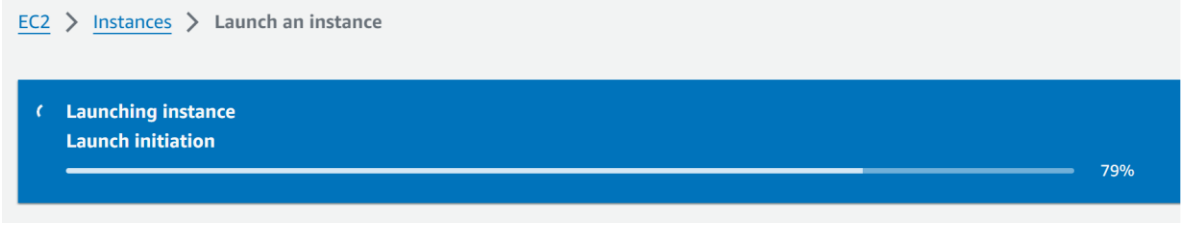
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

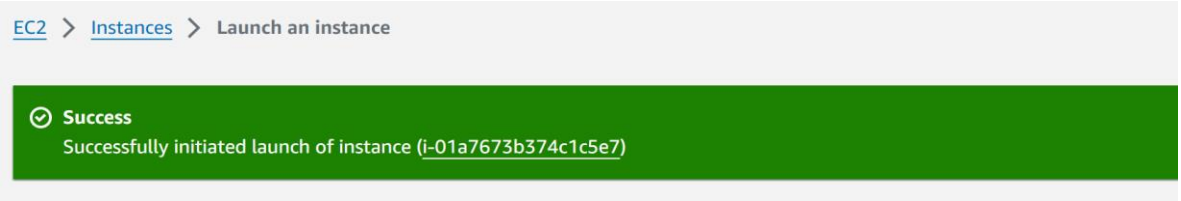
Amazon Linux 2023 AMI 2023.3.20240205.2 x86_64 HVM kernel-6.1

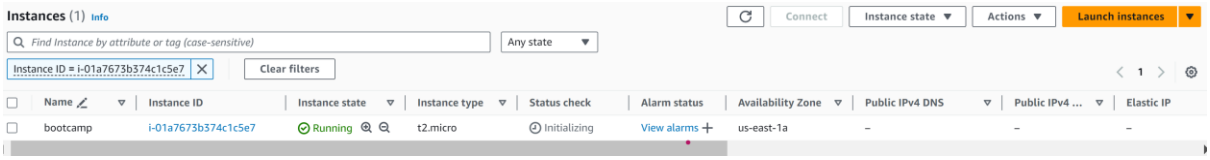
Architecture	Boot mode	AMI ID	
64-bit (x86)	uefi-preferred	ami-0e731c8a588258d0d	Verified provider


Instance type Info | Get advice
Instance type
t2.micro
Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.0716 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour
All generations
Compare instance types
Additional costs apply for AMIs with pre-installed software
Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
vockey
Create new key pair
Network settings Info
VPC - required Info
vpc-0106cbe3513a1507a (default)
172.31.0.0/16
Subnet Info
No preference
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-3
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
launch-wizard-3 created 2024-02-15T11:23:33.576Z
Inbound Security Group Rules
Security group rule 1 (TCP, 22, 0.0.0.0/0)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
Source Info
Description - optional Info
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-0e731c8a588258d0d
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Launch instance

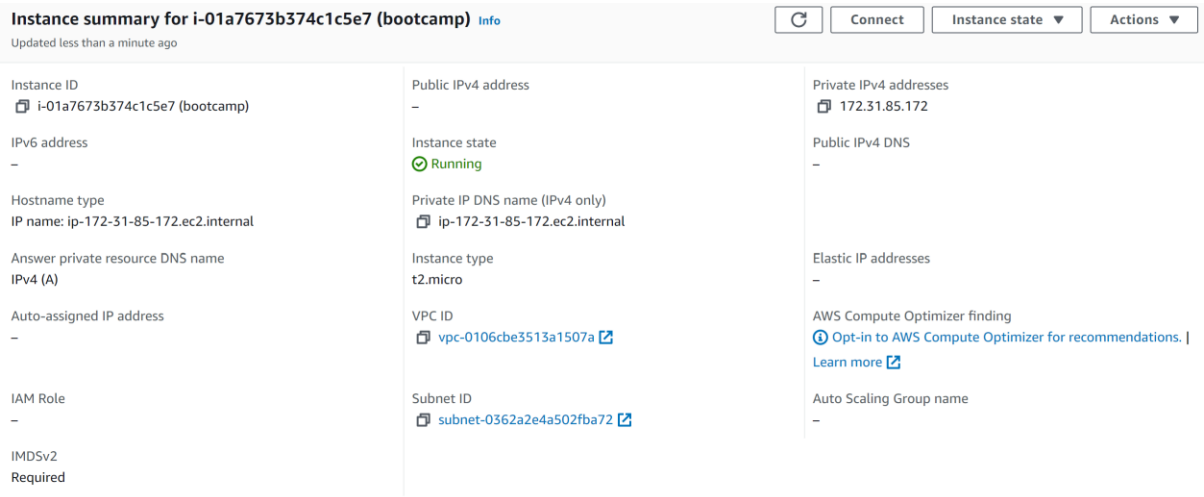

EC2 > Instances > Launch an instance
Launching instance
Launch initiation
79%

3. Now our Instance has been successfully created.



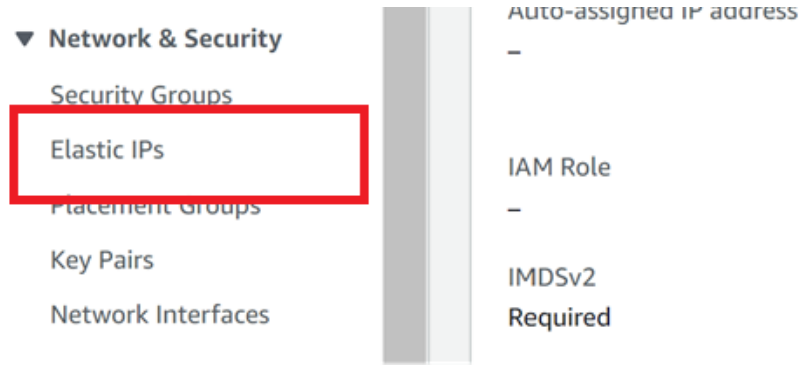


8. Not any assign IP for the EC2 instance



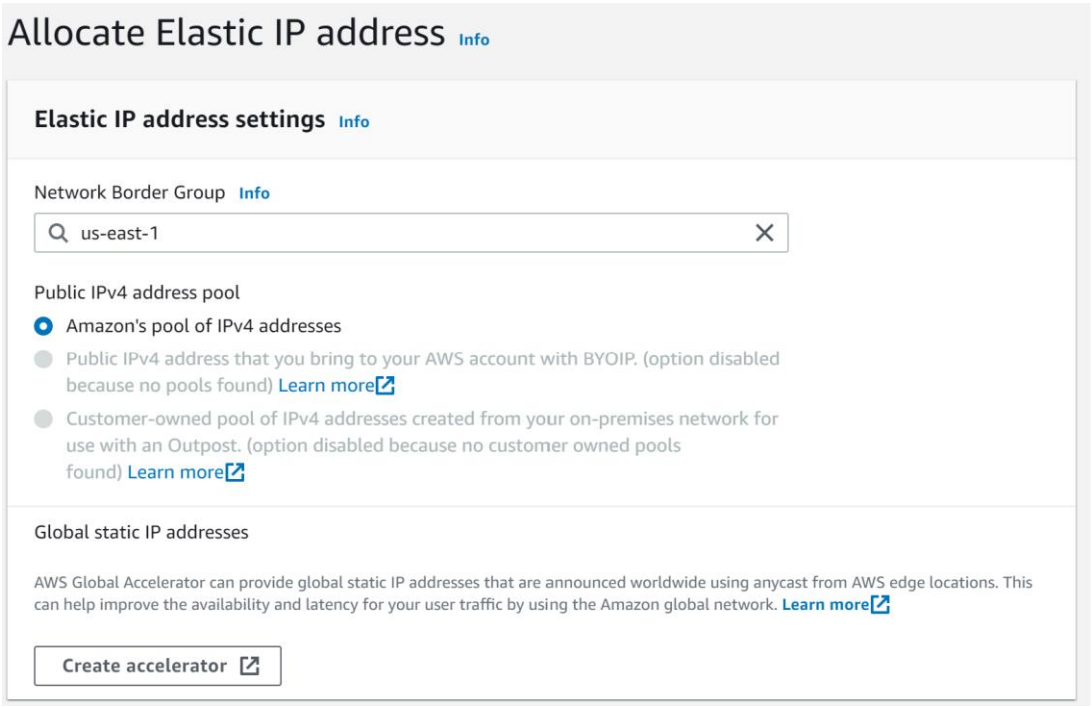
4. Now we adding the Elastic IP address

Select elastic IP

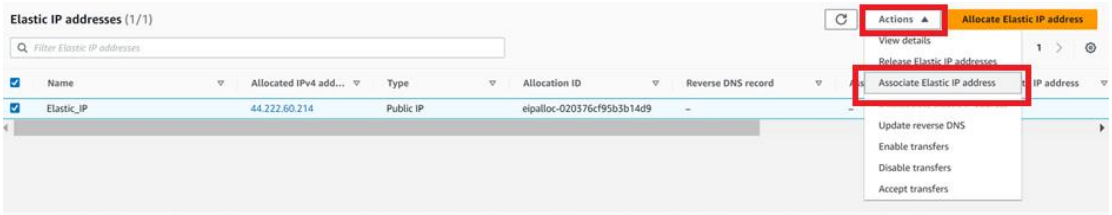


5. Select allocate Elastic IP Address

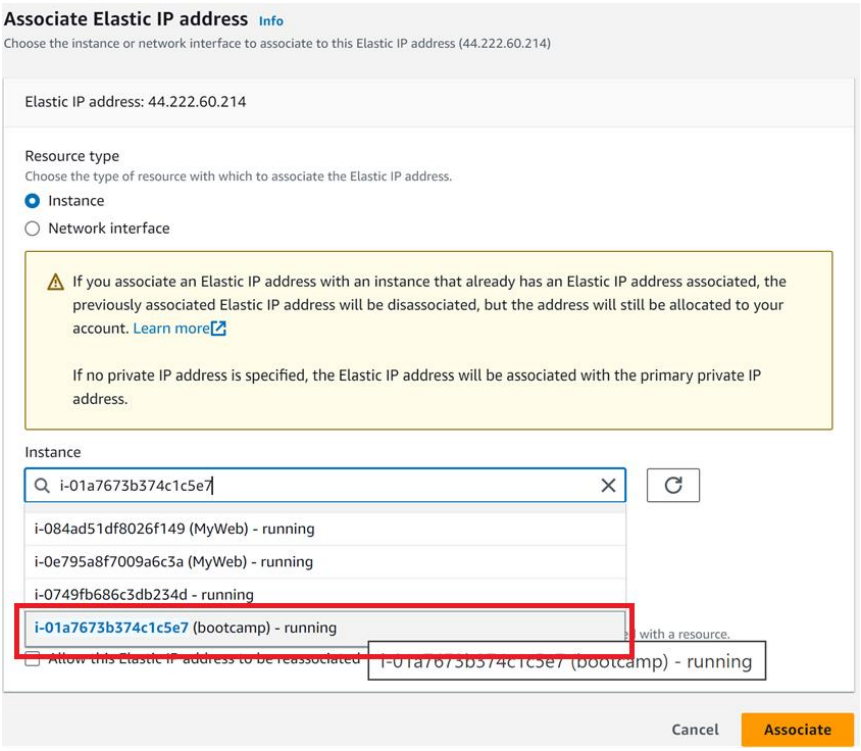
6. Select IPv4 to set IP Address



7. Keep the created IPv4 selected and click action and select associate elastic IP Address



8. Select the EC2 instance and click Associate

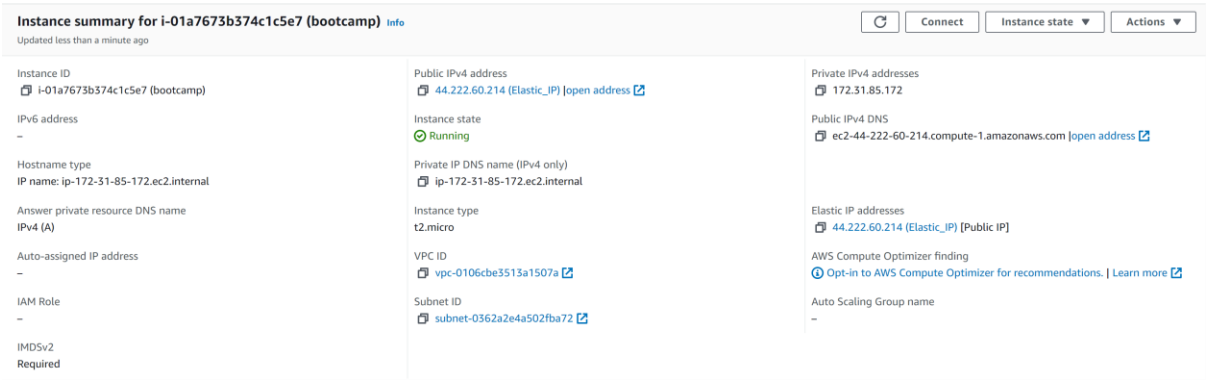


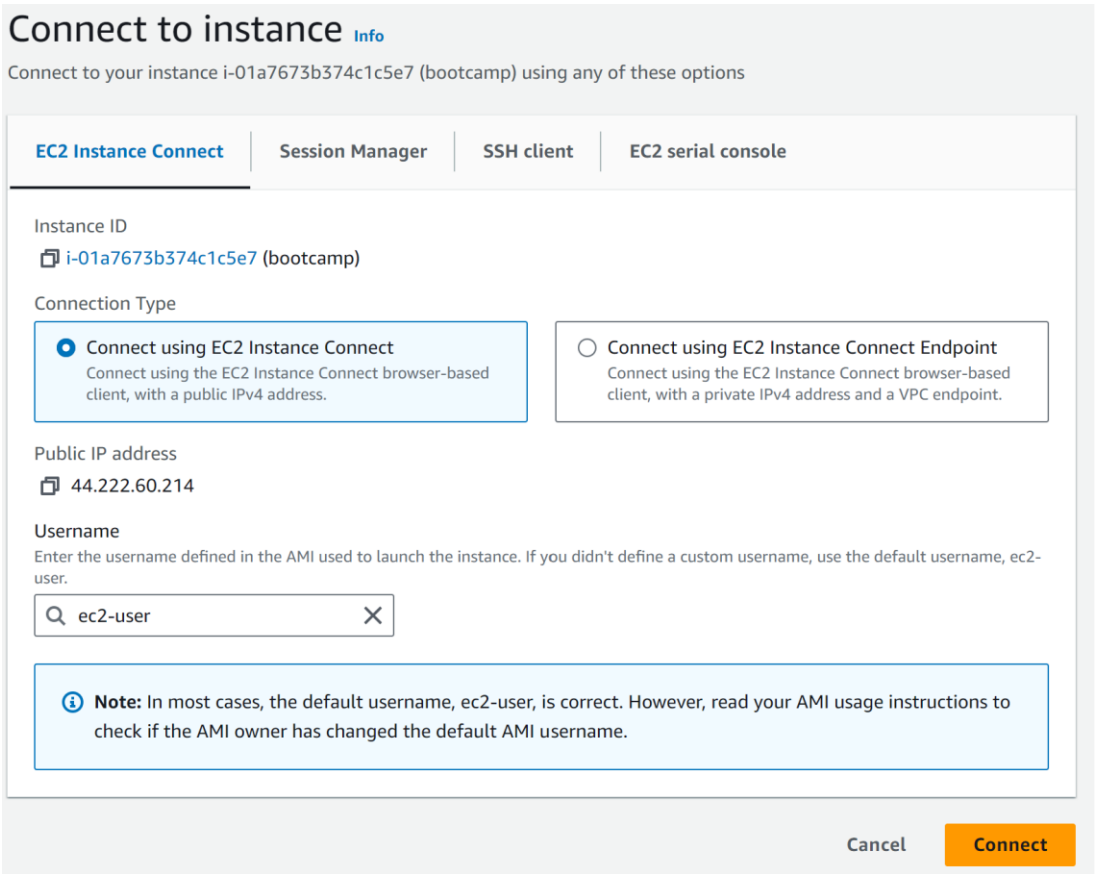
9. Now we can see the ec2 is assign in IP

Instance: i-01a7673b374c1c5e7 (bootcamp)

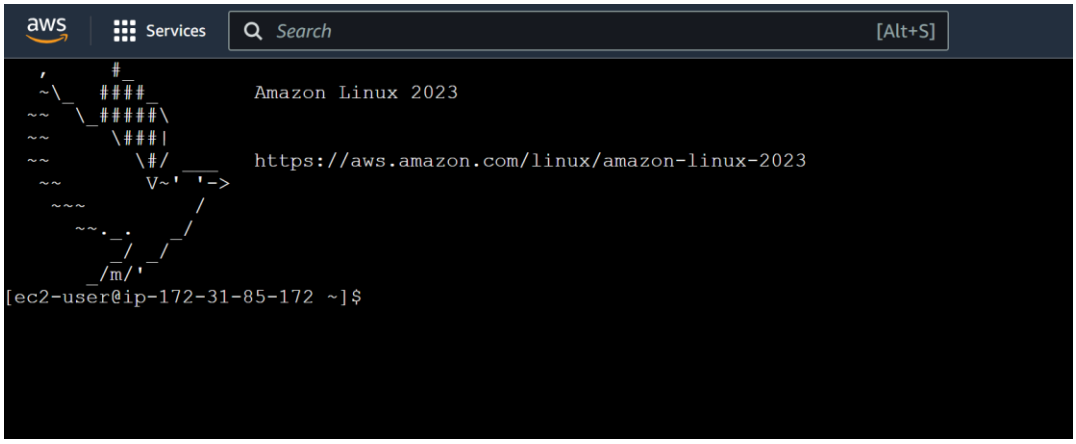
IPv6 address –	Instance state Running
Hostname type IP name: ip-172-31-85-172.ec2.internal	Private IP DNS name (IPv4 only) ip-172-31-85-172.ec2.internal
Answer private resource DNS name IPv4 (A)	Instance type t2.micro
Auto-assigned IP address –	VPC ID vpc-0106cbe3513a1507a
IAM Role –	Subnet ID subnet-0362a2e4a502fba72

10. To connect the EC2 instance via SSH, download the PEM file in AWS Details





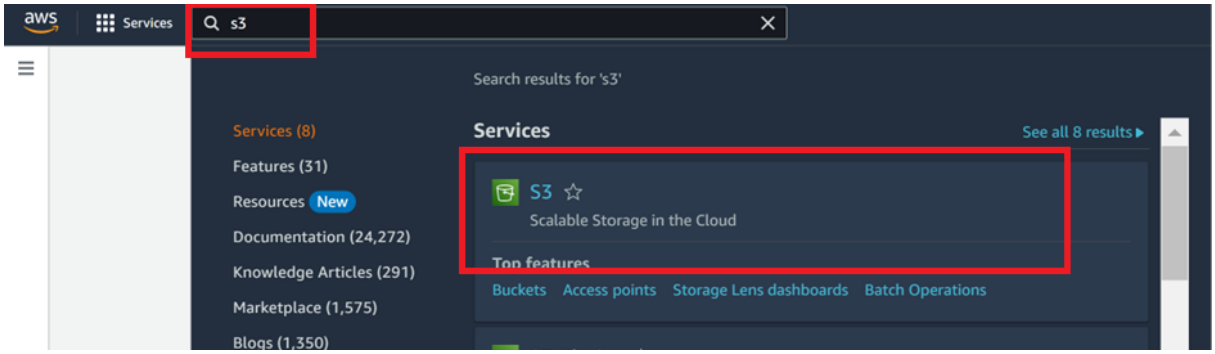
11. EC2 Instance Connect loads in a new page

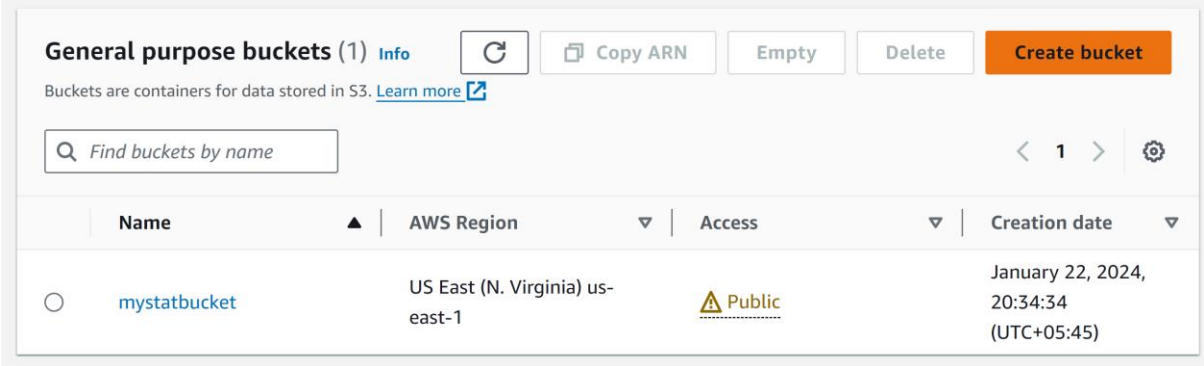


----------Next Task in new page----------

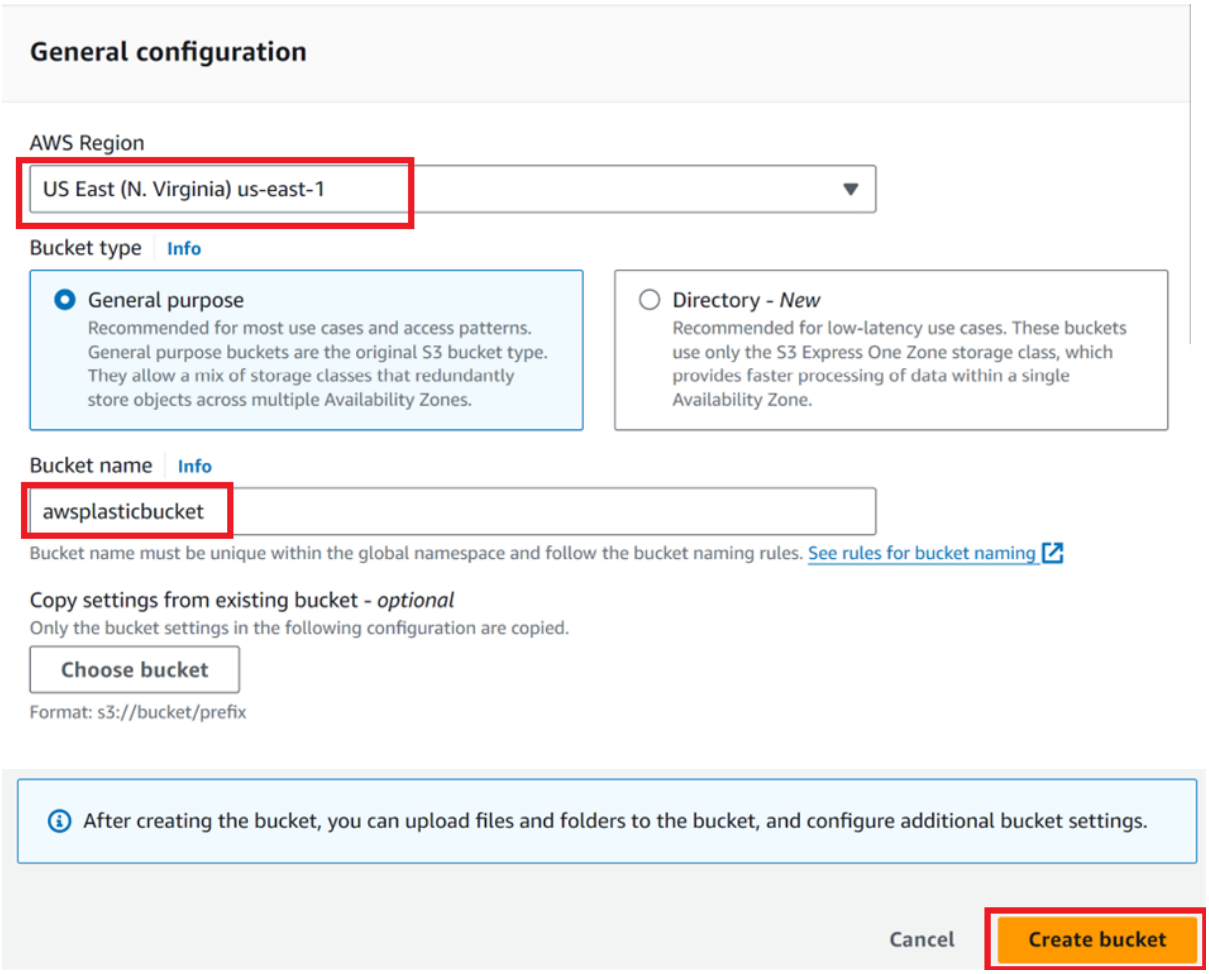
2. **S3 Storage Fundamentals Lab**
    - **Objective**: To gain hands-on experience with Amazon S3 by performing basic storage operations.
    - **Approach**: This lab involves creating an S3 bucket, uploading files to it, and setting up bucket policies for access control. Students will explore the S3 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.

i. Select S3 from Amazon Management Console and create an S3 Bucket

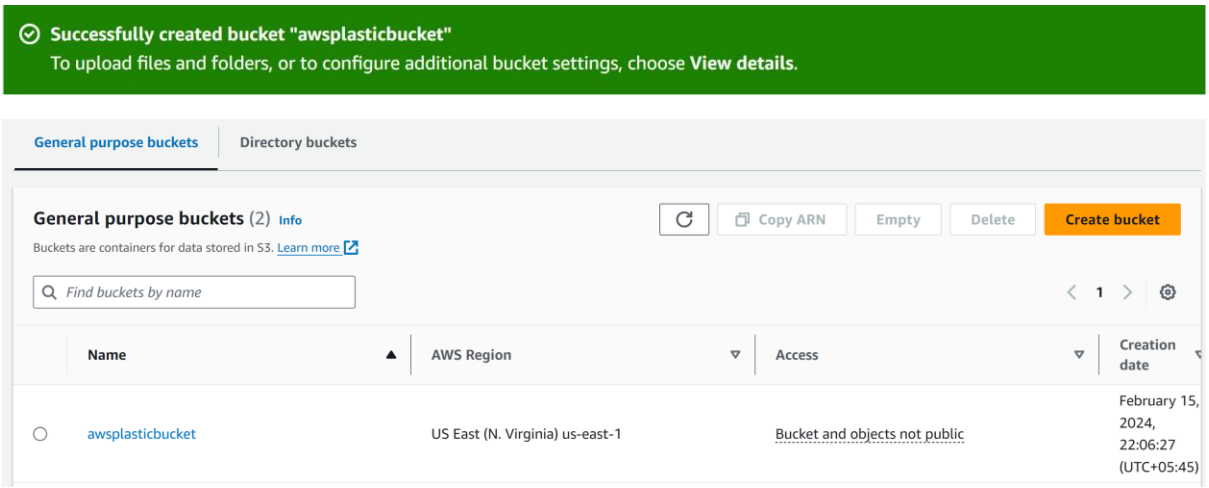




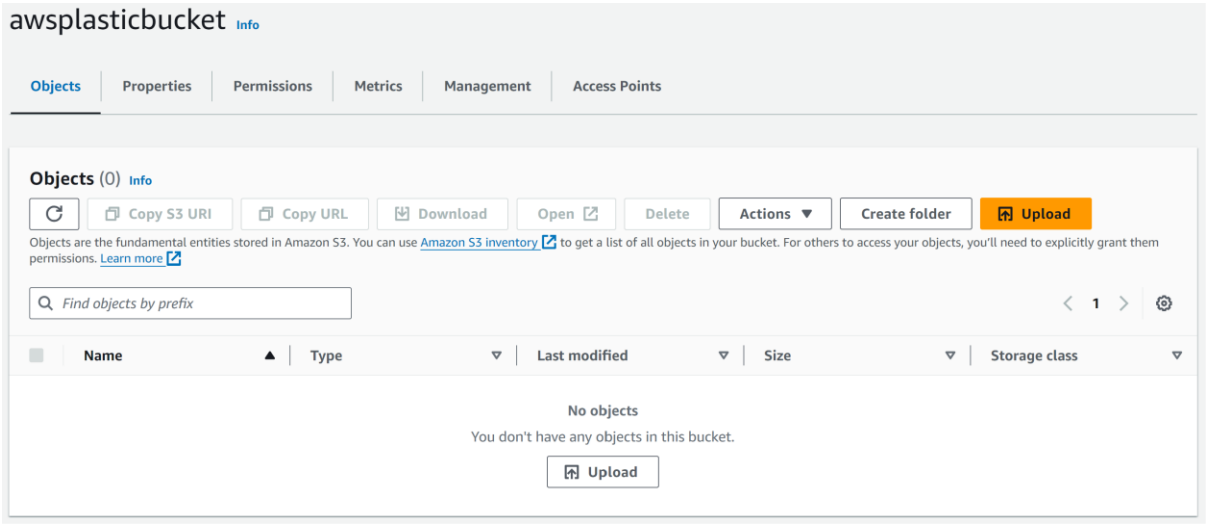
ii. Give a unique name to your bucket.

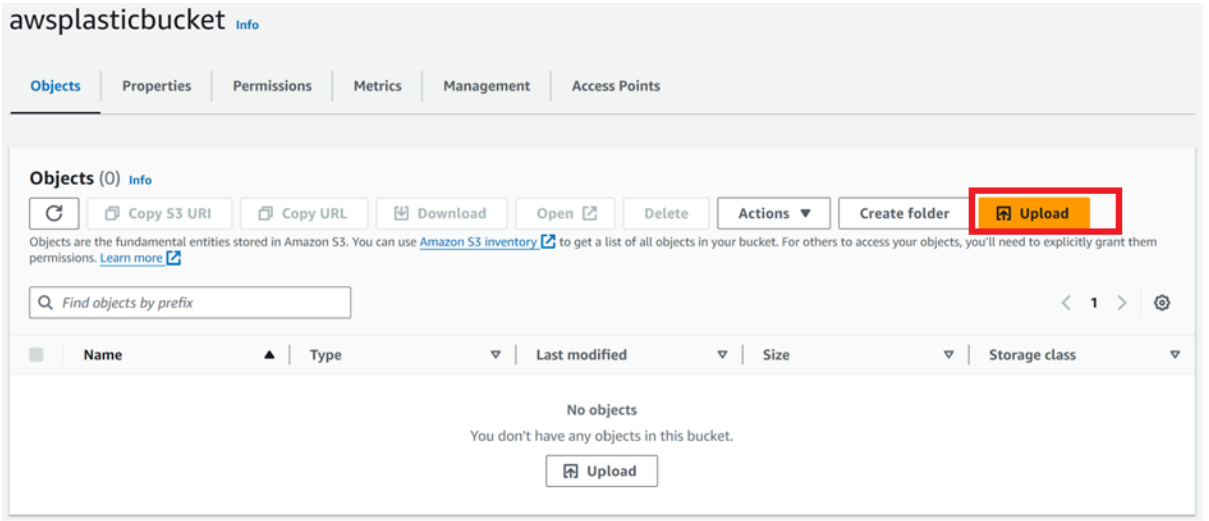


iii. Bucket Created

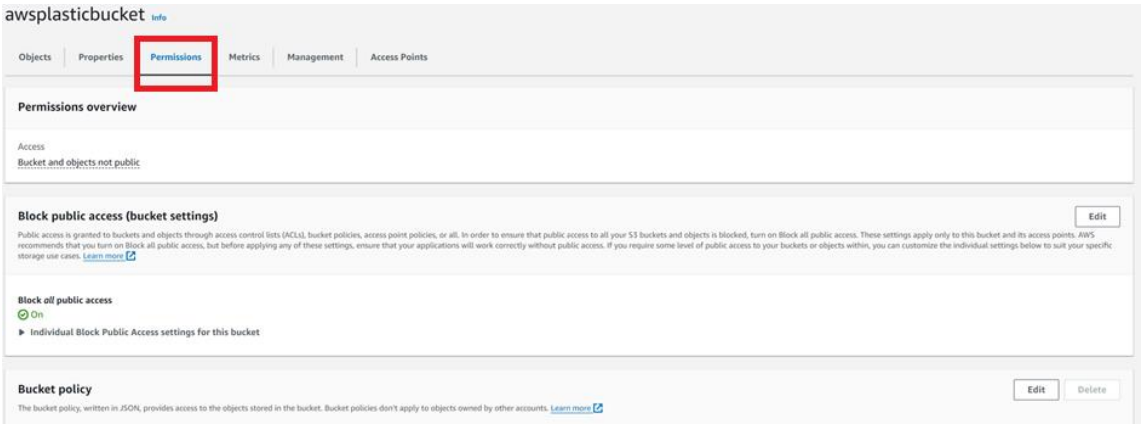


iv. Click **Upload** to upload file to the **bucket**.

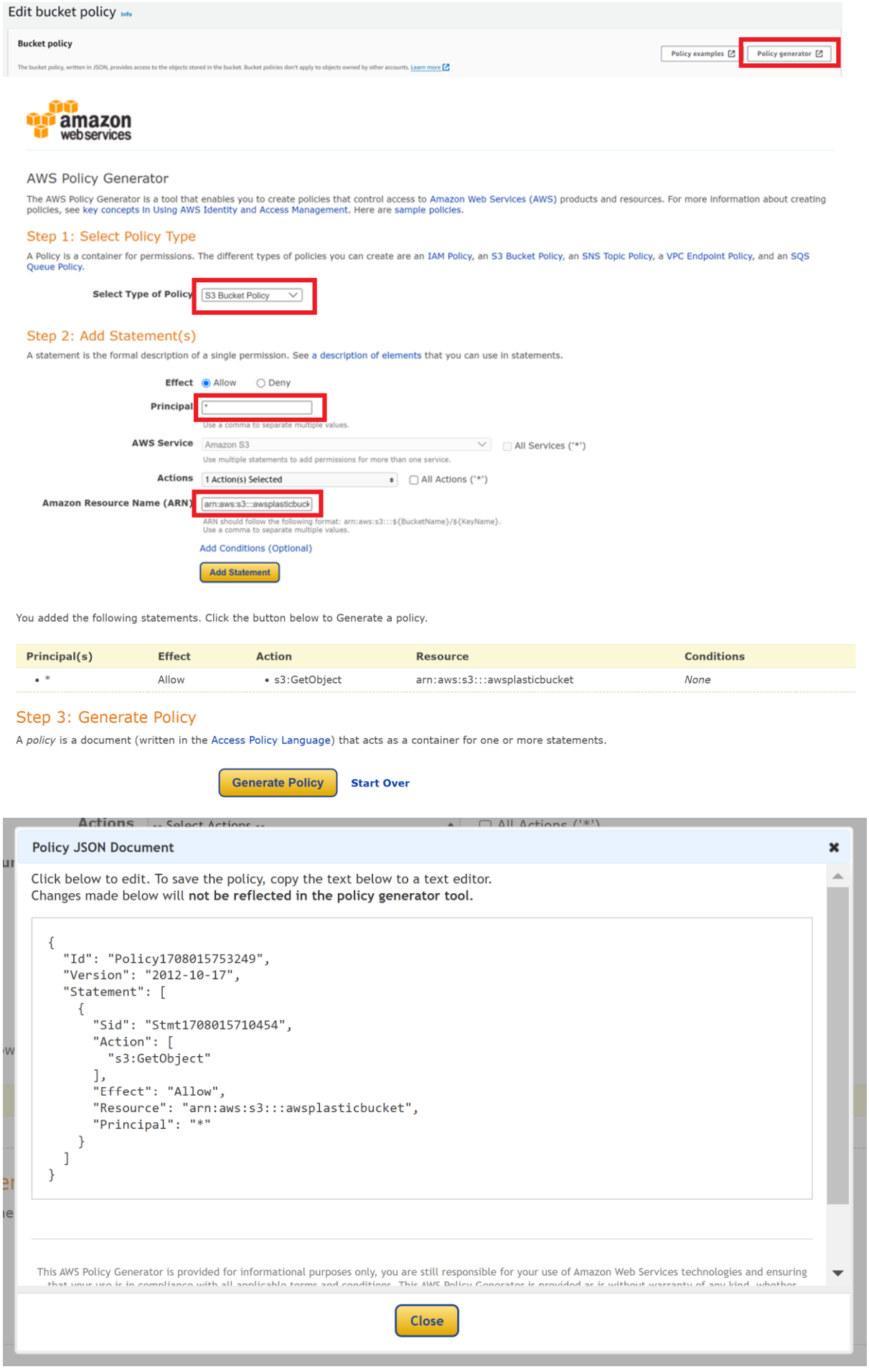




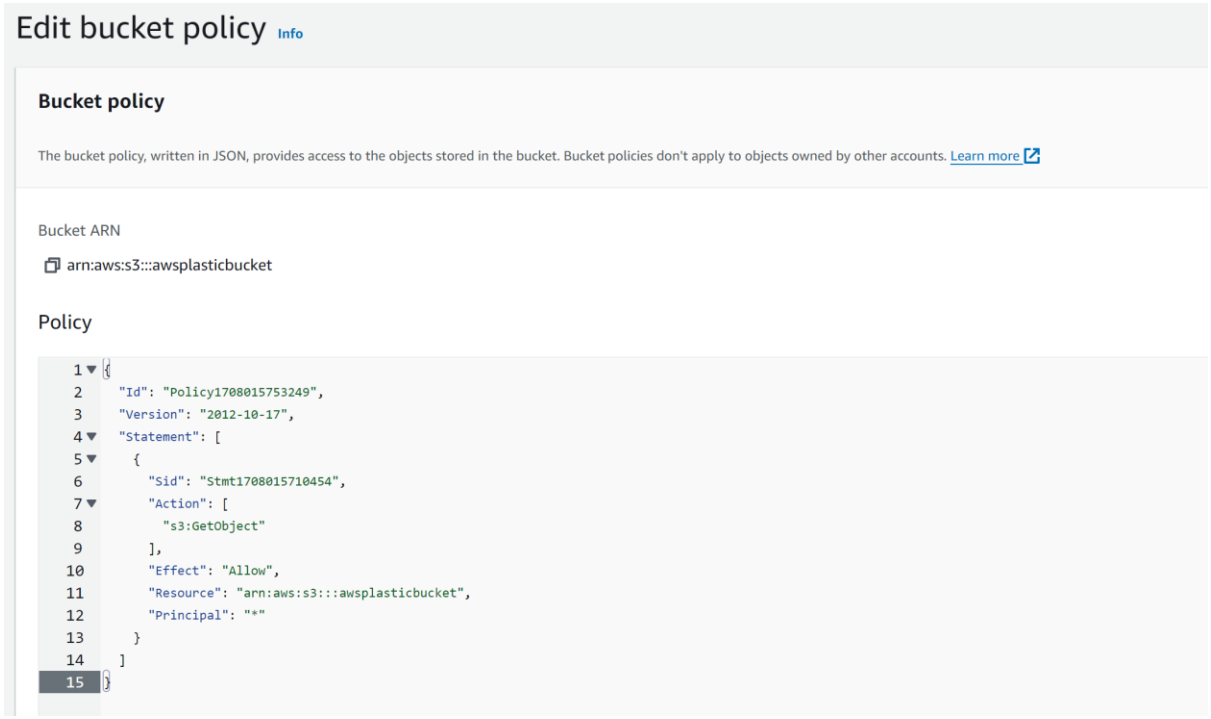
v. To set the policies, click the bucket name and select permission tab and you can see the bucket policy. Now click edit to set the policies.



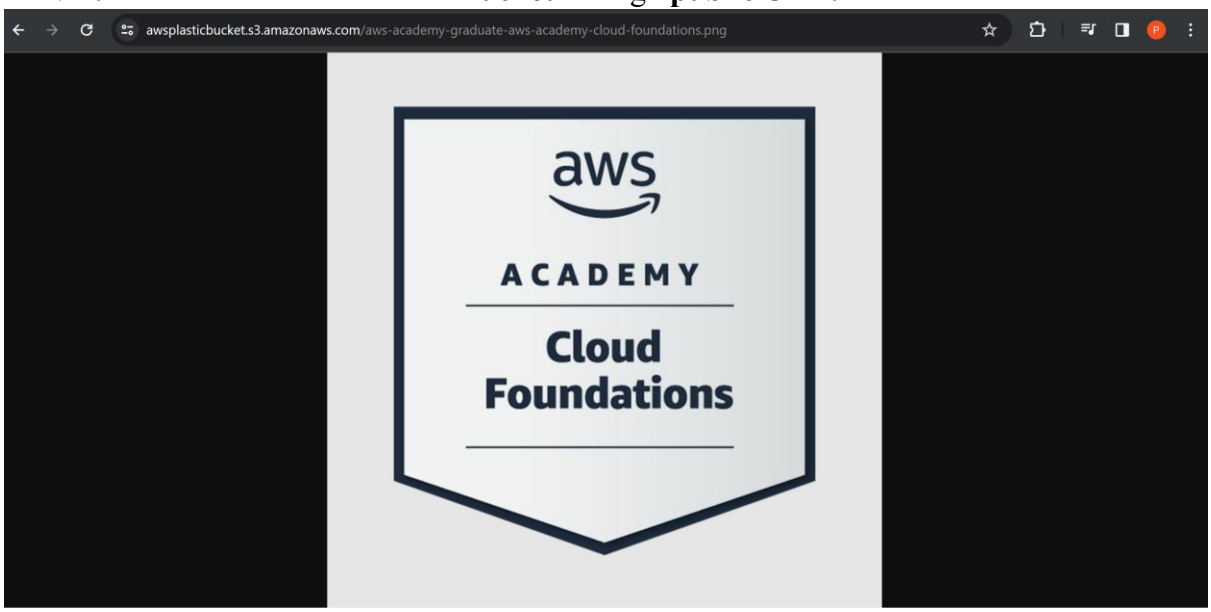
vi. Click policy generator to generate policy.



vii. Insert the generated JSON into **policy** and **save.**

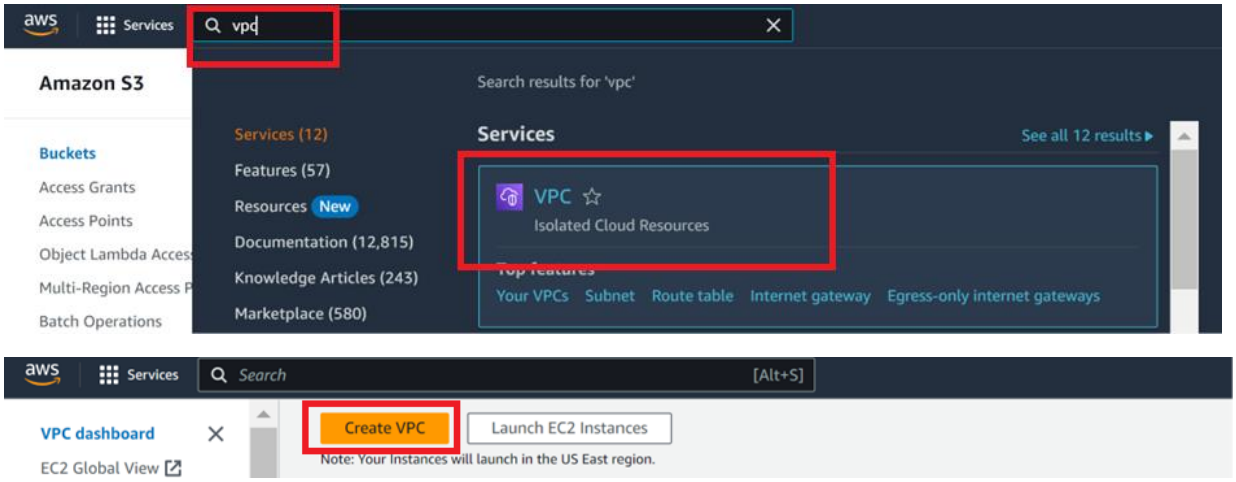


viii. Now we will access the **Bucket** through **public URL.**

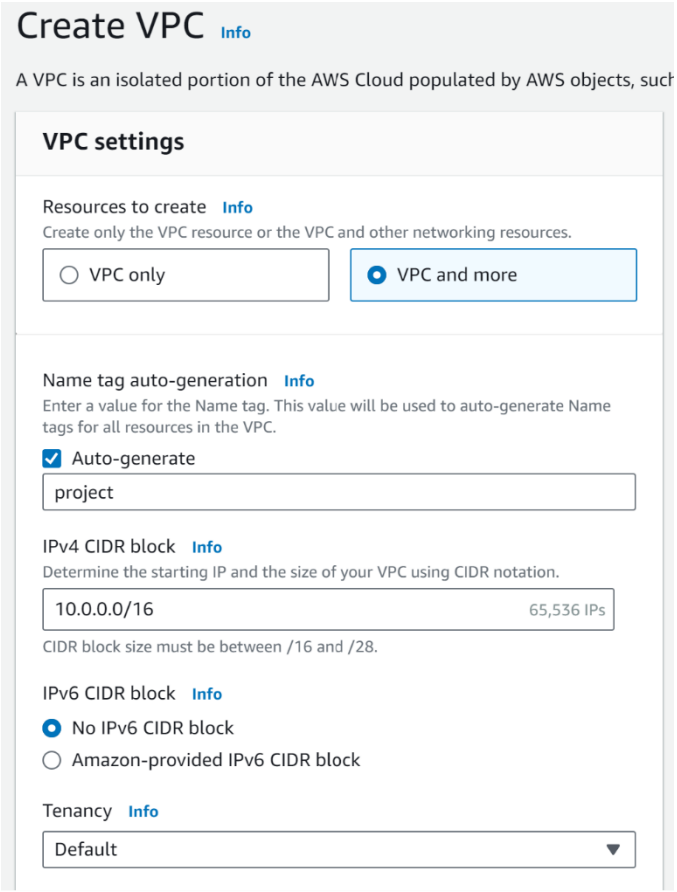


3. **VPC Configuration Lab**
   - **Objective**: To understand the fundamentals of AWS networking through the configuration of a Virtual Private Cloud (VPC).
   - **Approach**: Students will create a new VPC, add subnets, set up an Internet Gateway, and configure route tables. The lab might also include 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.

i. Open AWS console and look for VPC and create VPC



ii. Select the settings as per the steps.



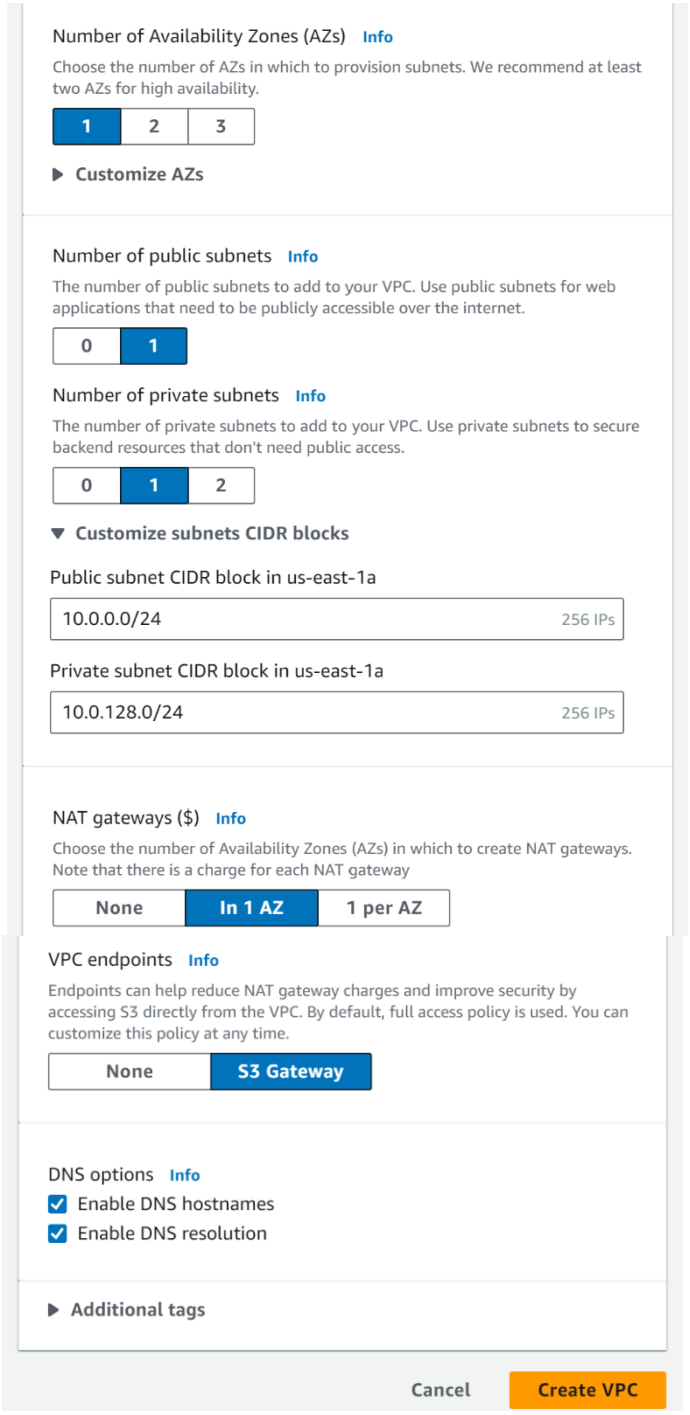
Set up the VPC specifics within the VPC settings section located on the left-hand panel:

Select "VPC and more." Opt for "VPC and more."

Ensure "Auto-generate" remains selected under "Name tag auto-generation," but modify the entry from "project" to "lab."

Maintain the IPv4 CIDR block as 10.0.0.0/16. Opt for 1 for the Number of Availability Zones.

Retain the setting of 1 for both the Number of public subnets and the Number of private subnets.



Broaden the section for customizing CIDR blocks of subnets.

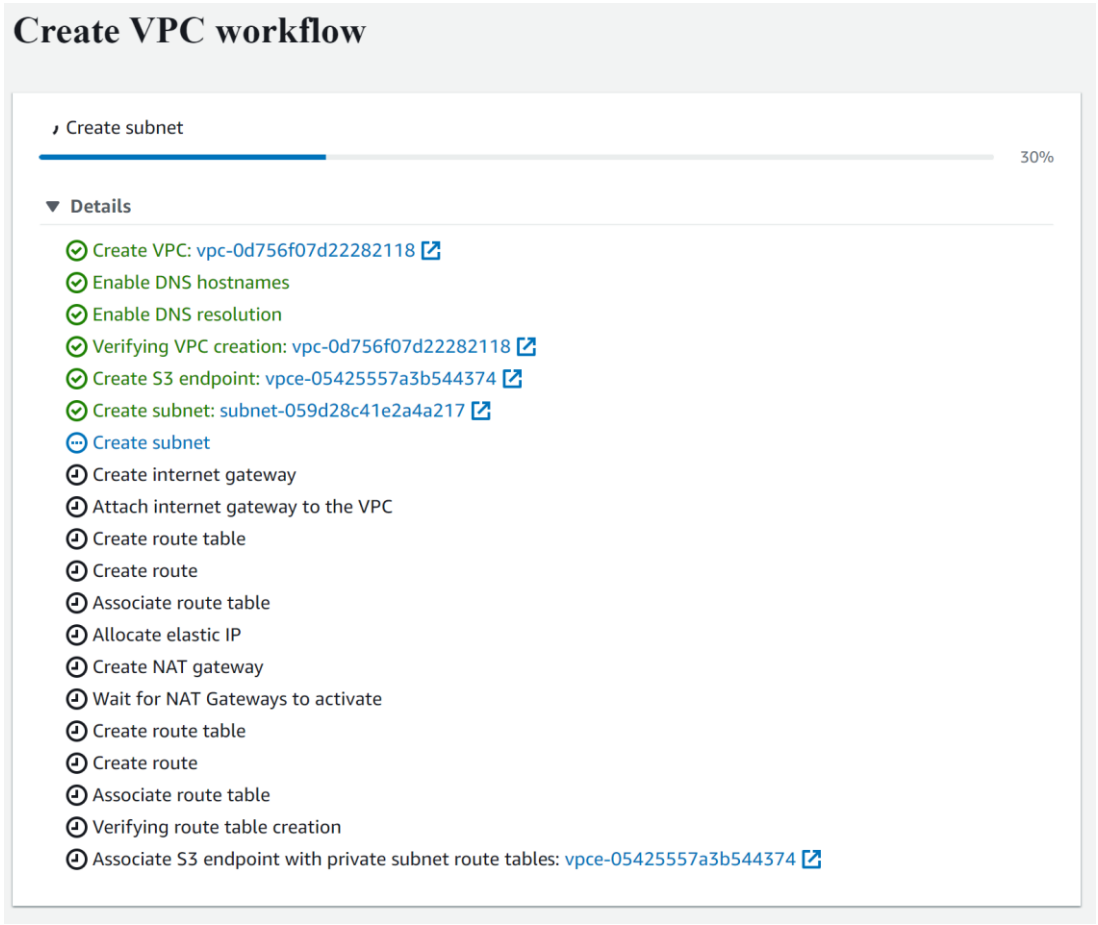
Adjust the Public subnet CIDR block to 10.0.0.0/24 within us-east-1a.

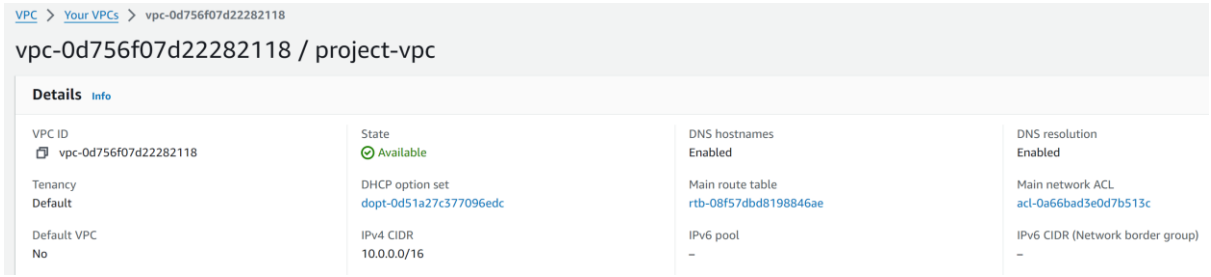
Modify the Private subnet CIDR block to 10.0.1.0/24 within us-east-1a.

Configure NAT gateways for availability within a single AZ.

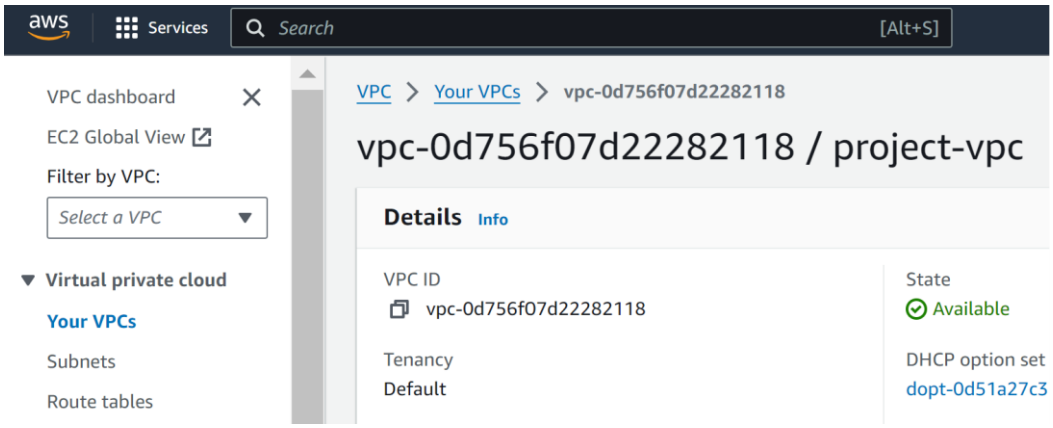
Opt not to use VPC endpoints. Ensure that both DNS hostnames and DNS resolution remain enabled.

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

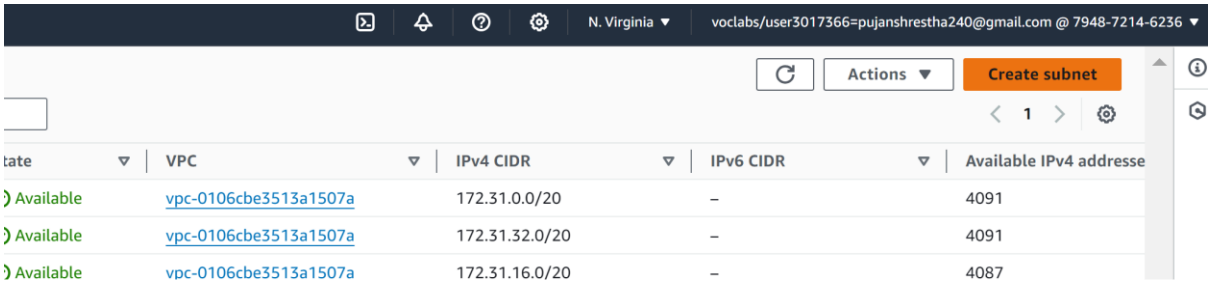




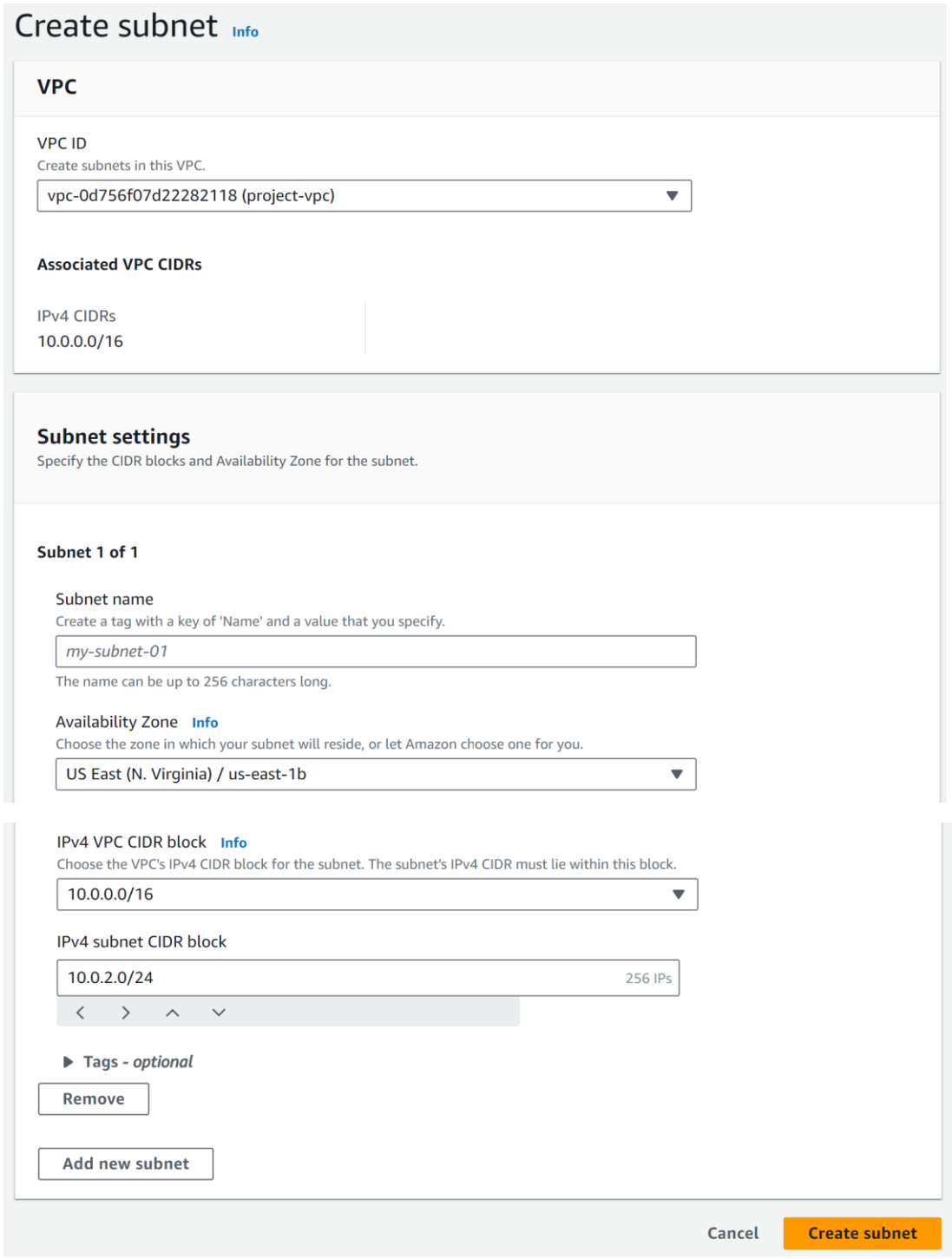
iv. To add Subnet, click **Subnet** in left-hand side of the panel. It is situated just below *Your VPC*

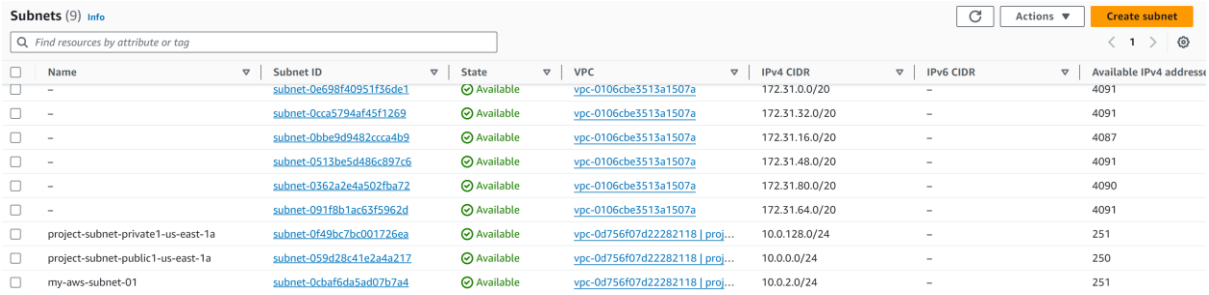


v. Select Create SubNet

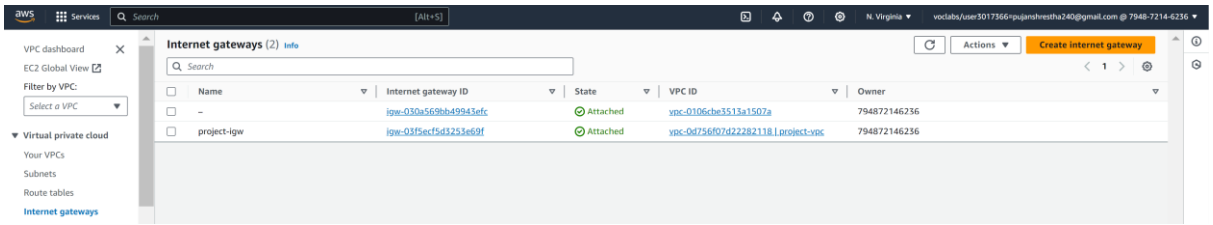


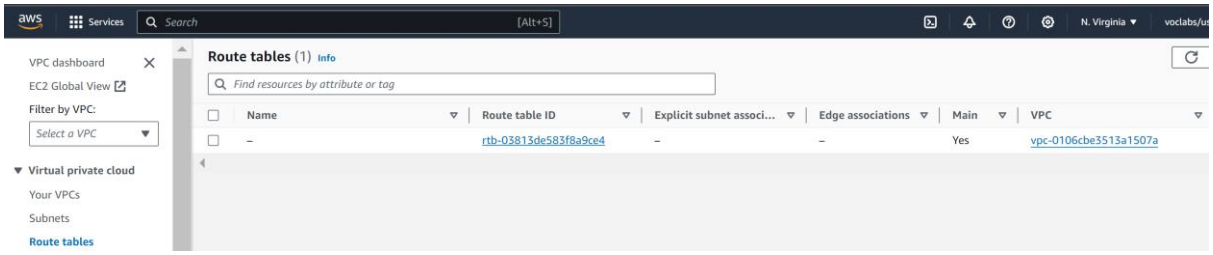
vi. Set subset name, availability zone, and add the IPv4-CIDR Subnet



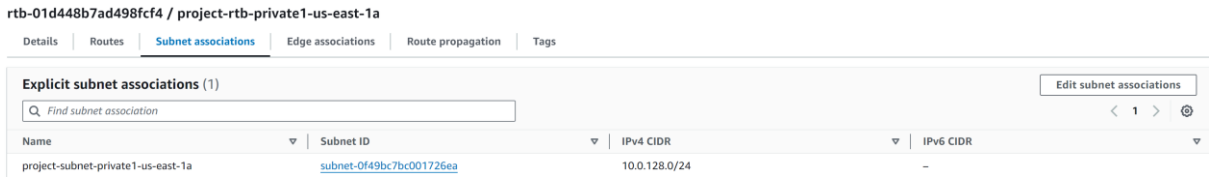


vii. To set up the Internet Gateway, select Internet gateway from left-bar and select Create internet gateway.

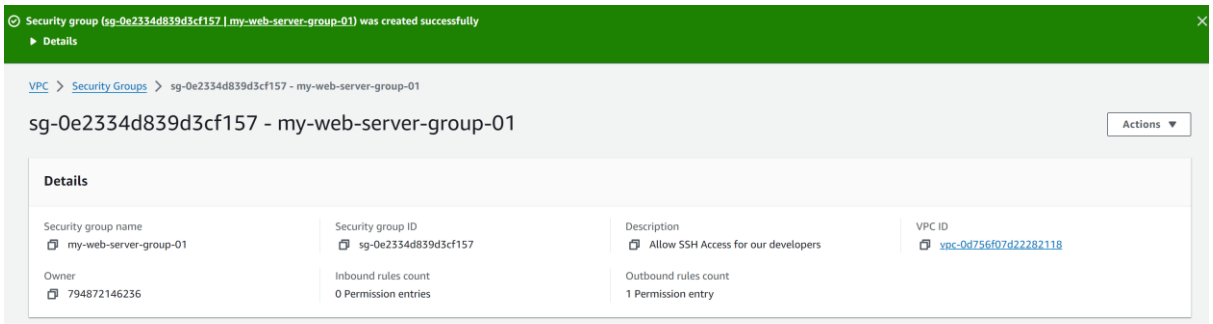




viii. Configure the Route table by clicking on the Route Table and select the lab session.

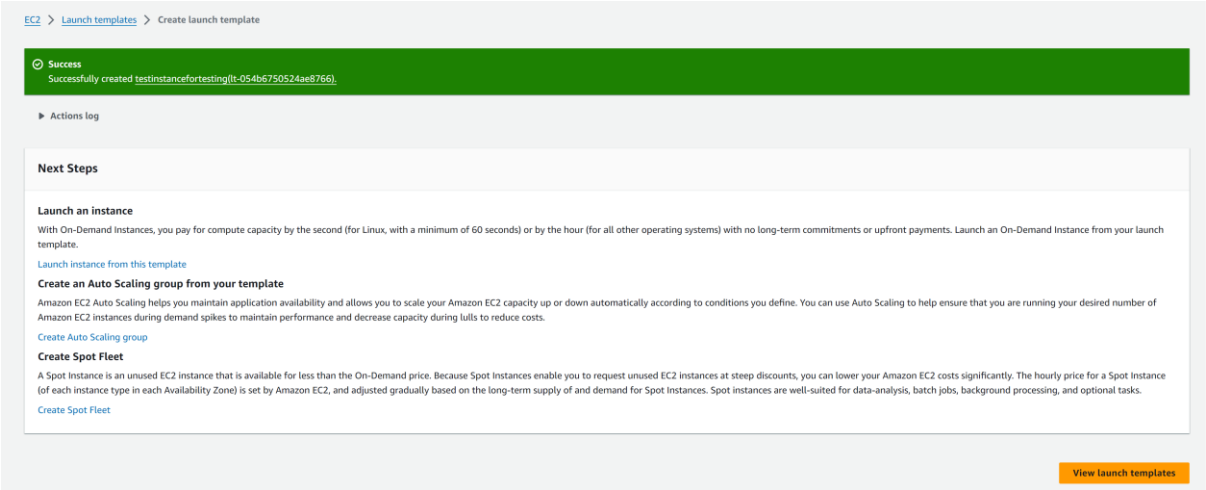


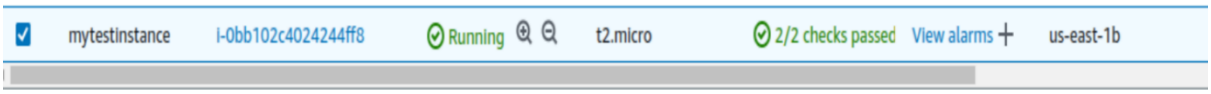
ix. Create Security Group with necessary rule for the VPC



x. Instantiate an EC2 instance utilizing the previously established security group and VPC. Embed a code within the user data box for execution upon launch. Return to the newly created instance once its status indicates "2 checks passed." Identify and retrieve the

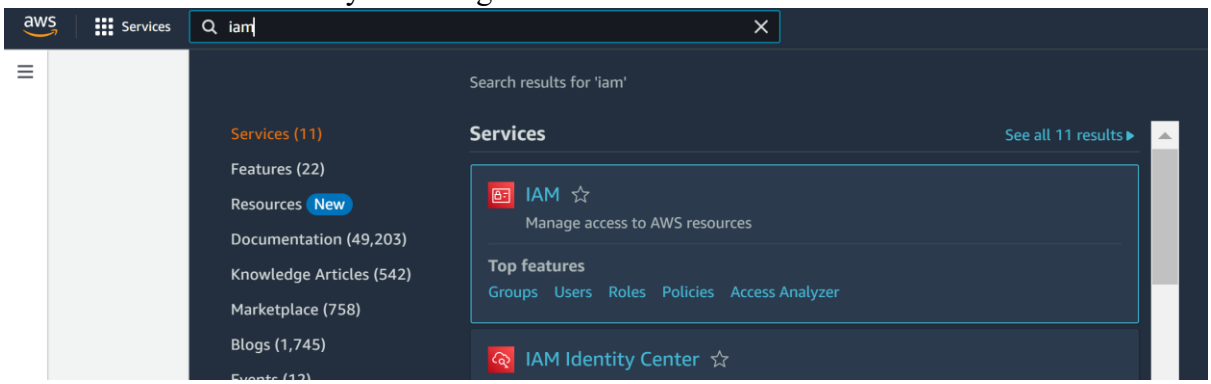
public IP address associated with the instance.



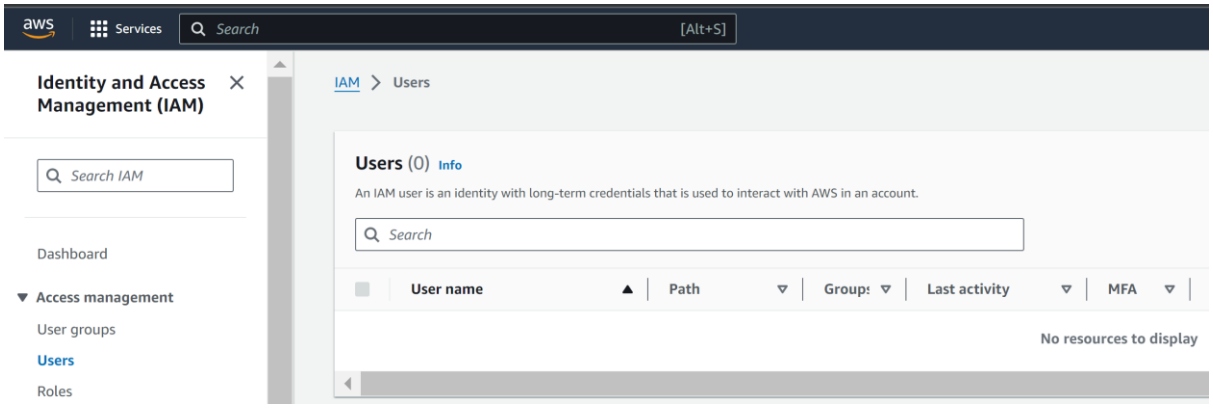


4. **IAM Users and Roles Lab**
    - **Objective**: To understand AWS Identity and Access Management (IAM) by creating and managing users, groups, and roles.
    - **Approach**: Students will create new IAM users, assign them to groups, and apply policies to manage permissions. The lab will also involve 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.

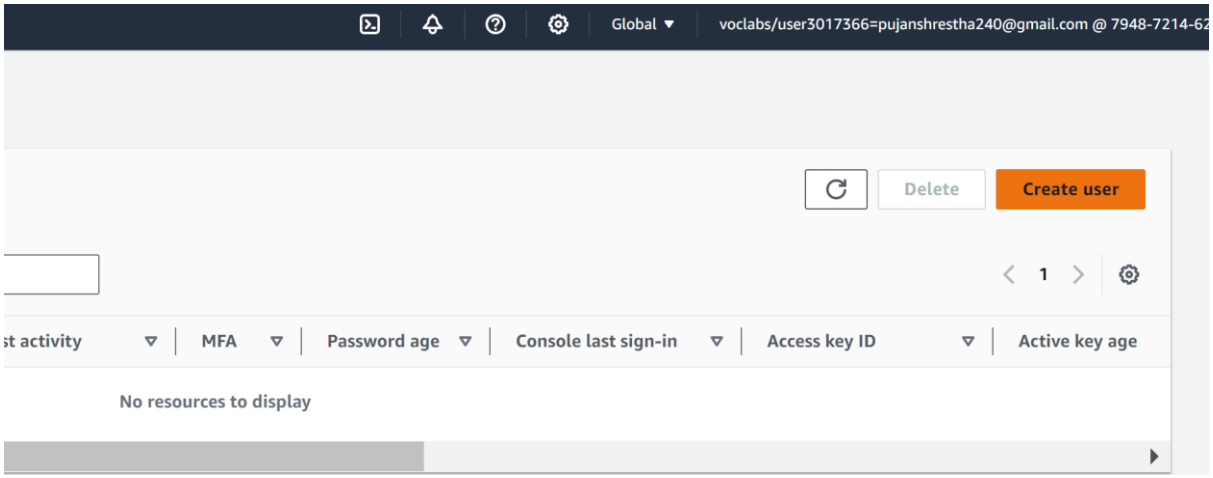
i. First we start by searching IAM in AWS Console and we create a IAM User.

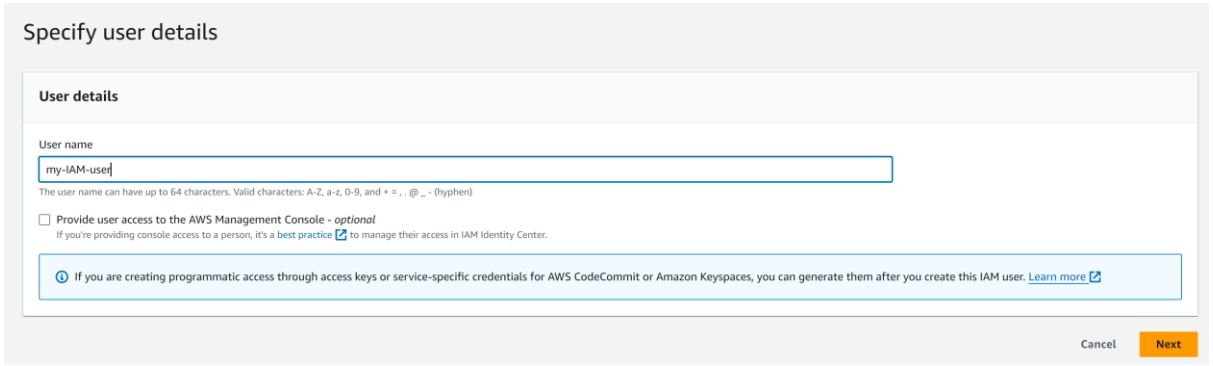


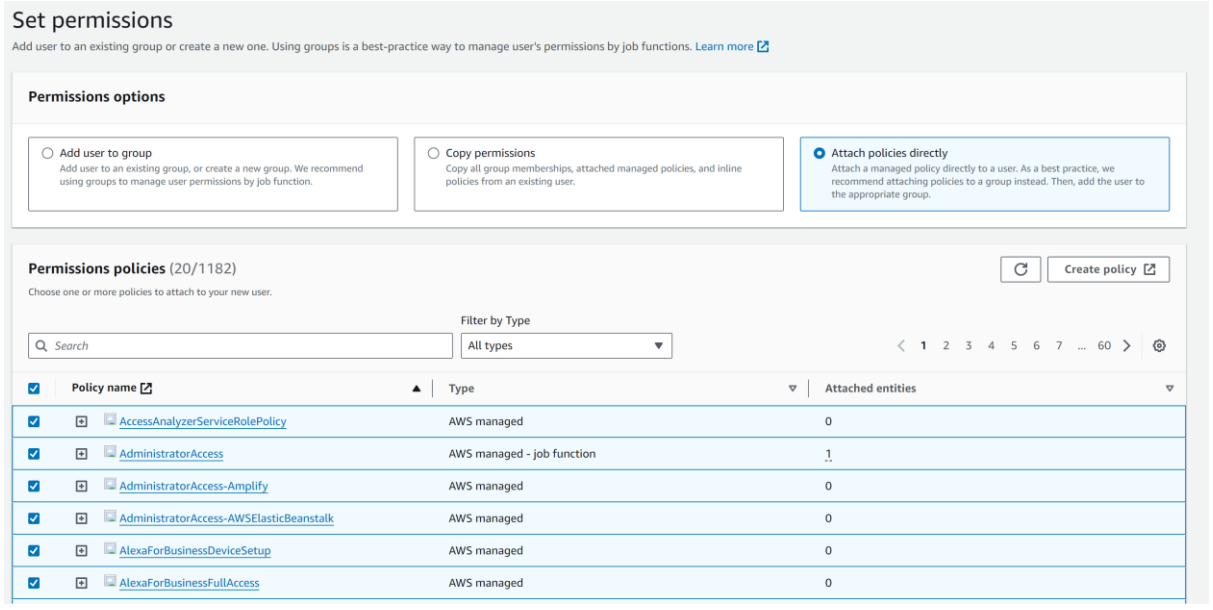
ii. Select User from the left side of the screen



iii. Create a new user



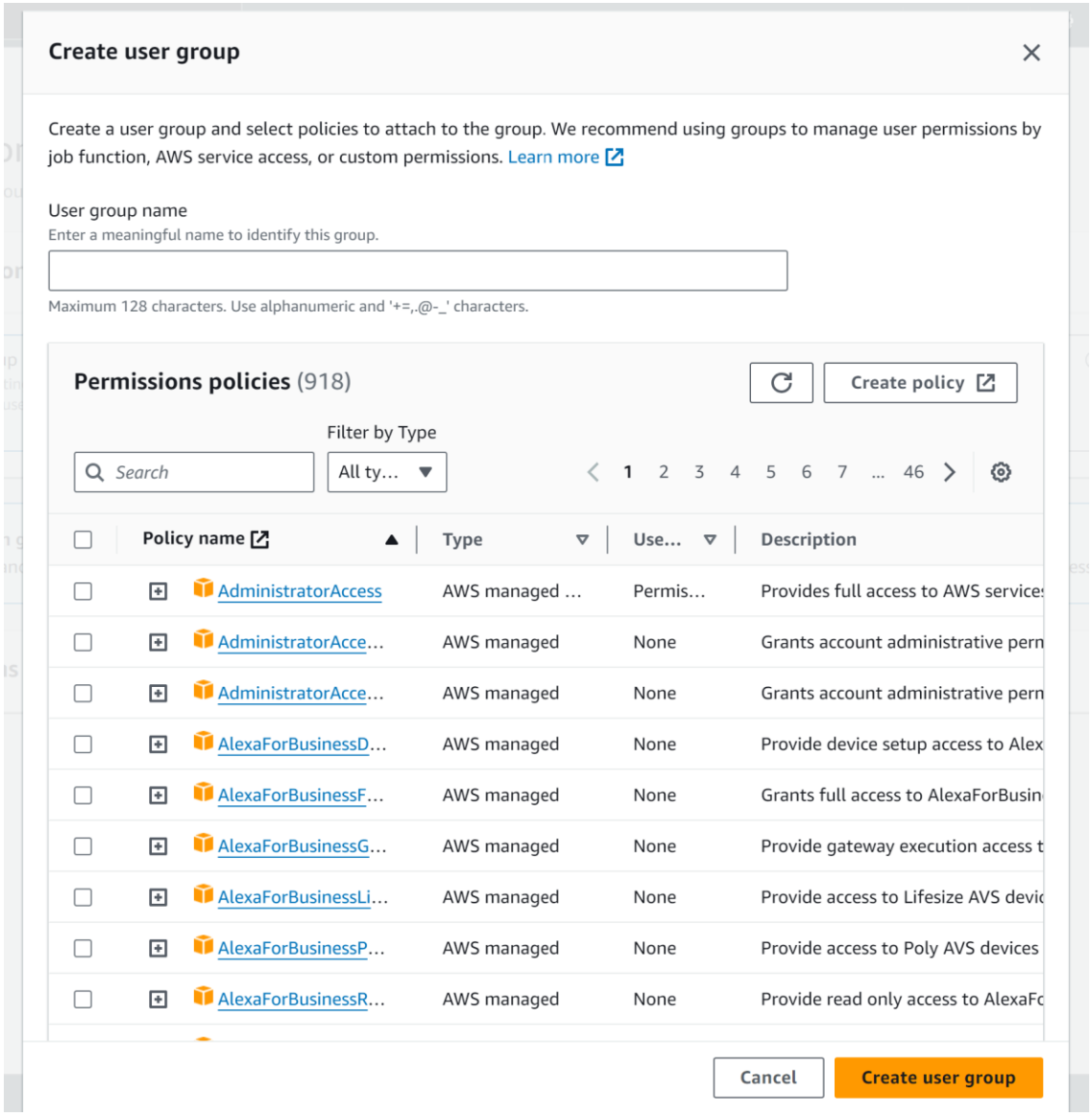


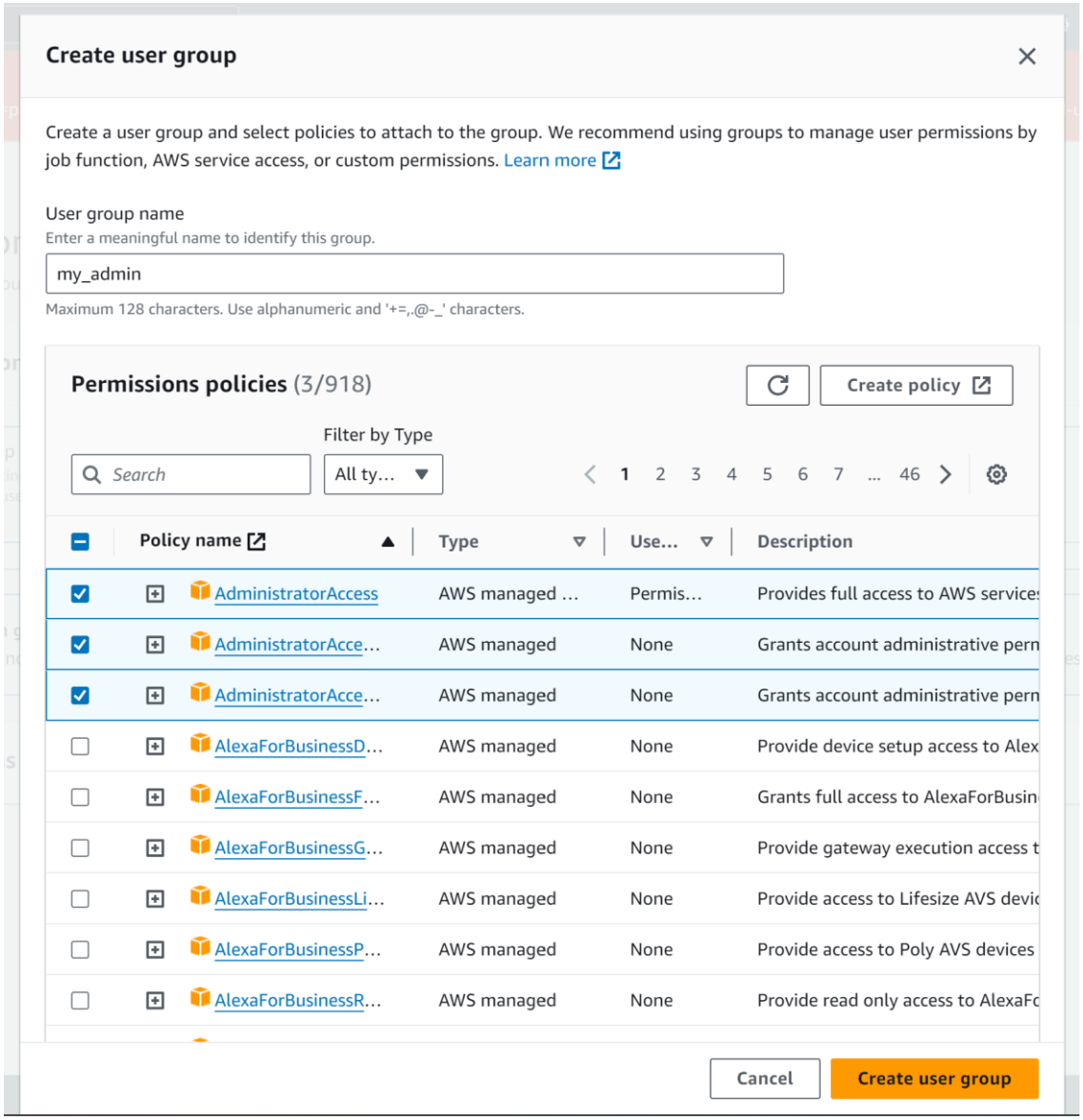


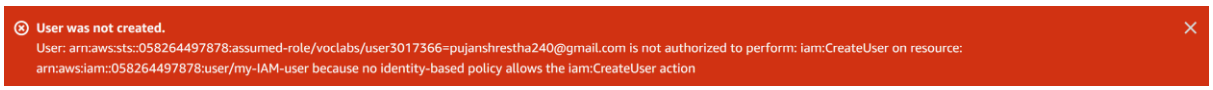
AlexaForBusinessFullAccess	AWS managed	0
AlexaForBusinessGatewayExecution	AWS managed	0
AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS managed	0
AlexaForBusinessNetworkProfileServicePolicy	AWS managed	0
AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	0
AlexaForBusinessReadOnlyAccess	AWS managed	0
AmazonAPIGatewayAdministrator	AWS managed	0
AmazonAPIGatewayInvokeFullAccess	AWS managed	0
AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	0
AmazonAppFlowFullAccess	AWS managed	0
AmazonAppFlowReadOnlyAccess	AWS managed	0
AmazonAppStreamFullAccess	AWS managed	0
AmazonAppStreamPCAAccess	AWS managed	0
AmazonAppStreamReadOnlyAccess	AWS managed	0
AmazonAppStreamServiceAccess	AWS managed	0

▸ **Set permissions boundary - *optional***

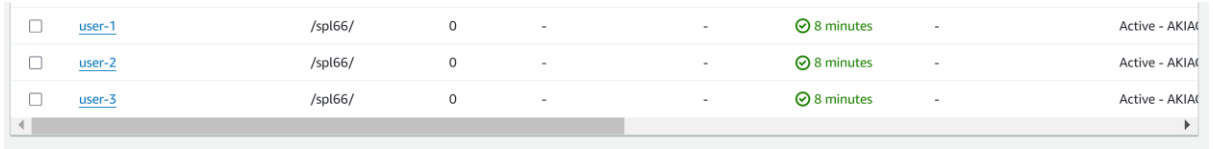
Cancel Previous Next


Create user group
Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more
User group name
Enter a meaningful name to identify this group.
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions policies (918)
Create policy
Filter by Type
Search
All ty...
1 2 3 4 5 6 7 ... 46
Policy name
Type
Use...
Description
AdministratorAccess
AWS managed ...
Permis...
Provides full access to AWS service
AdministratorAcce...
AWS managed
None
Grants account administrative pern
AdministratorAcce...
AWS managed
None
Grants account administrative pern
AlexaForBusinessD...
AWS managed
None
Provide device setup access to Alex
AlexaForBusinessF...
AWS managed
None
Grants full access to AlexaForBusin
AlexaForBusinessG...
AWS managed
None
Provide gateway execution access t
AlexaForBusinessLi...
AWS managed
None
Provide access to Lifesize AVS devi
AlexaForBusinessP...
AWS managed
None
Provide access to Poly AVS devices
AlexaForBusinessR...
AWS managed
None
Provide read only access to AlexaFo
Cancel
Create user group

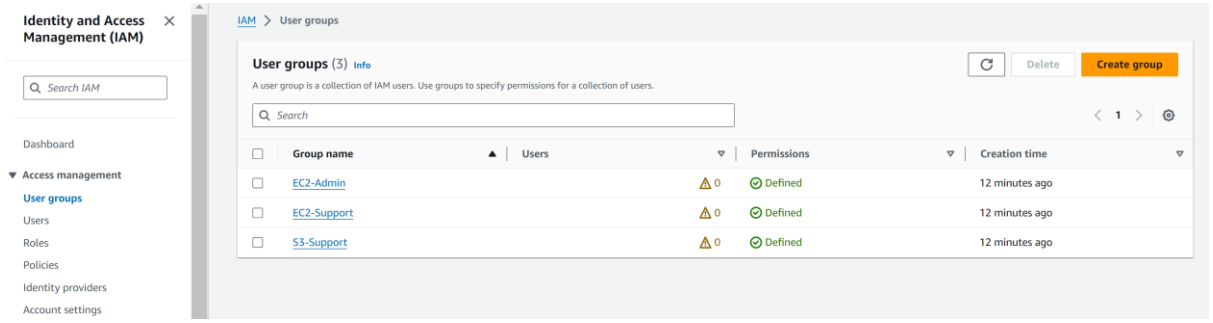




We don't have access to create user and group with the provided account so, I am referring to the foundation course to assign group to the users (pre-created users and groups).

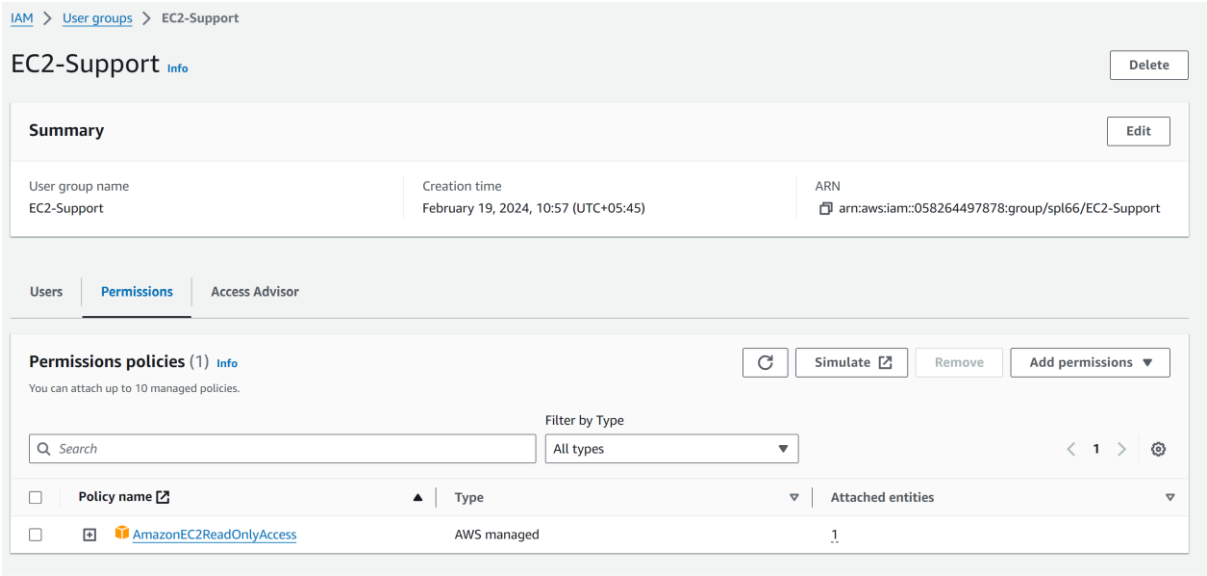


Now select User groups from the left side-bar and select **Create Group.**



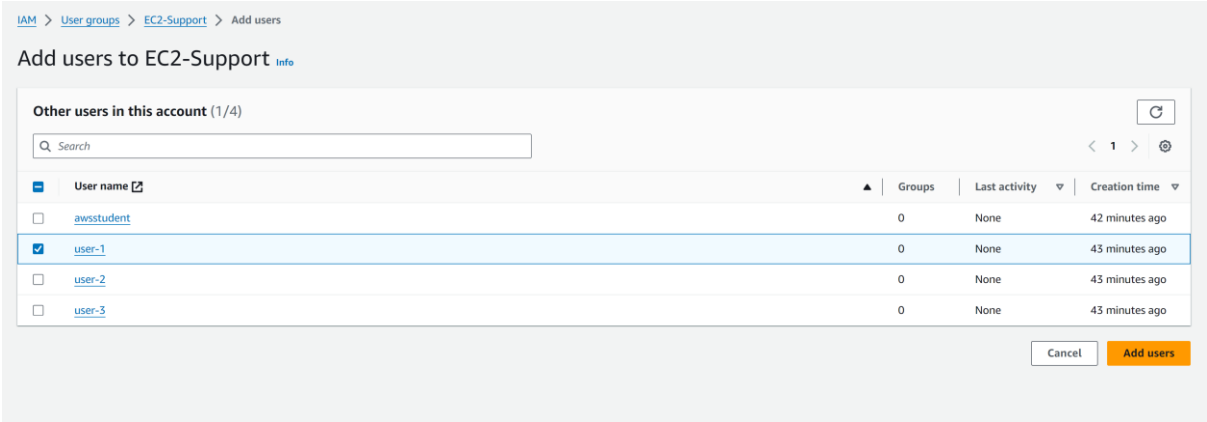
Go to the user group which is under the users in the left panel, click the group

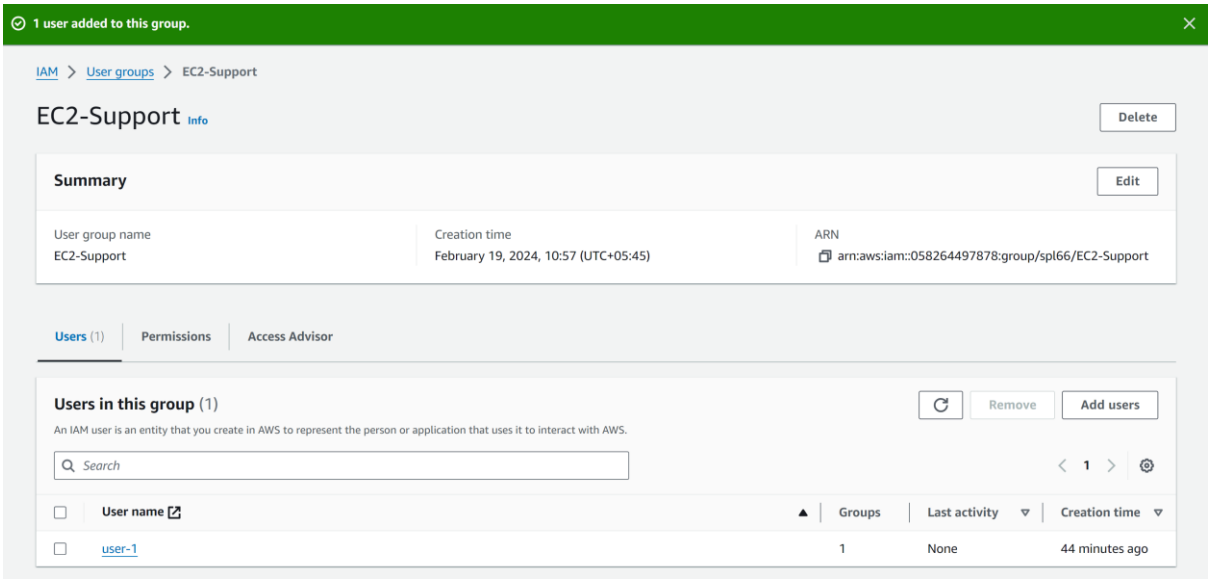
Name



Here, we have selected EC2-Support which is a pre-created group. Upon selecting Permissions, we can see that there is one permission on the policy i.e., **AmazonEC2ReadOnlyAccess.**

Now click on the users tab and add users.





Now we can create new user, create password or use generated password and login with the assigned roles within the group.