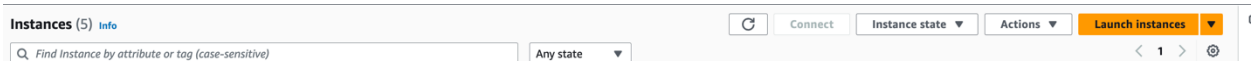
1. EC2 Basics Lab

Objective: To understand the process of setting up and managing an Amazon EC2 instance.

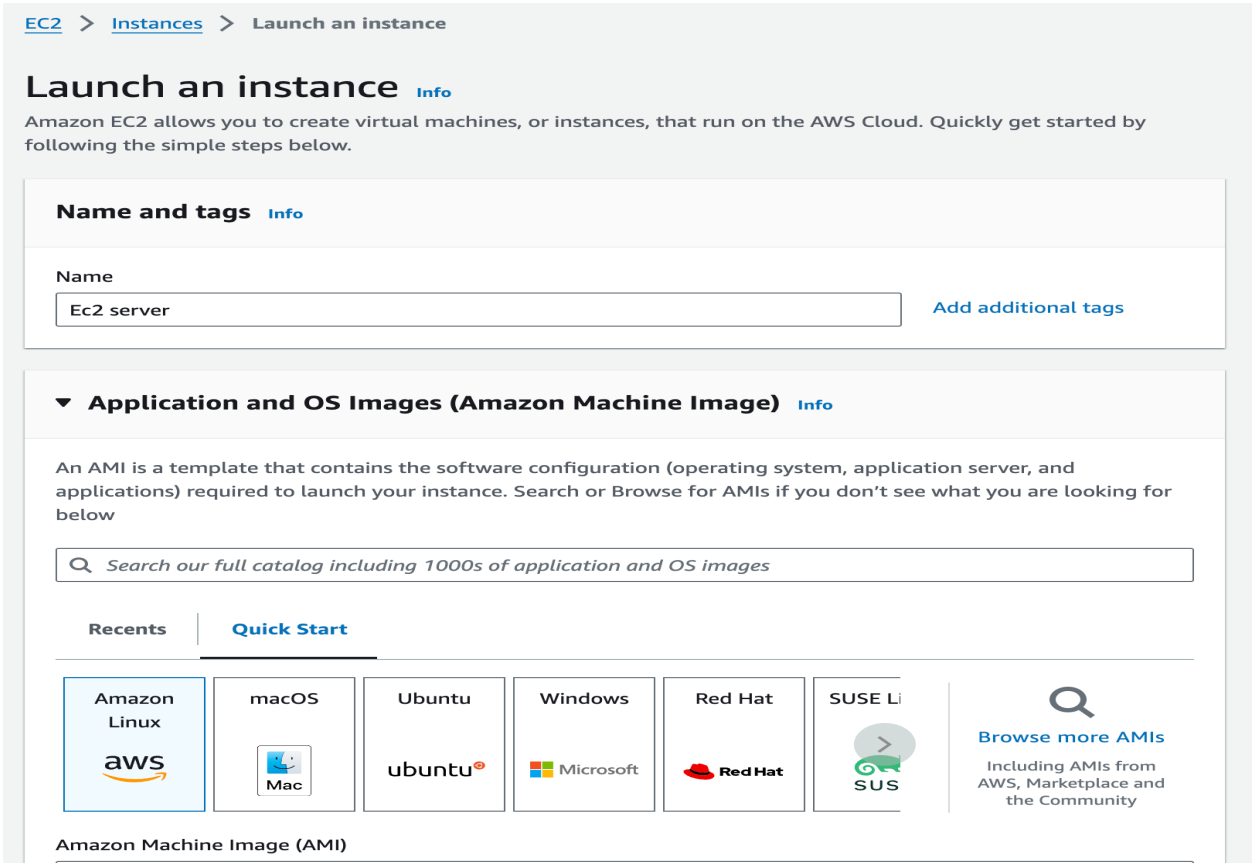
Approach: Students will start by launching a new EC2 instance, selecting an appropriate instance type and configuring the instance details. They will then create and configure a new Security Group, and allocate an Elastic IP address to the instance. The lab will also include connecting to the instance 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.

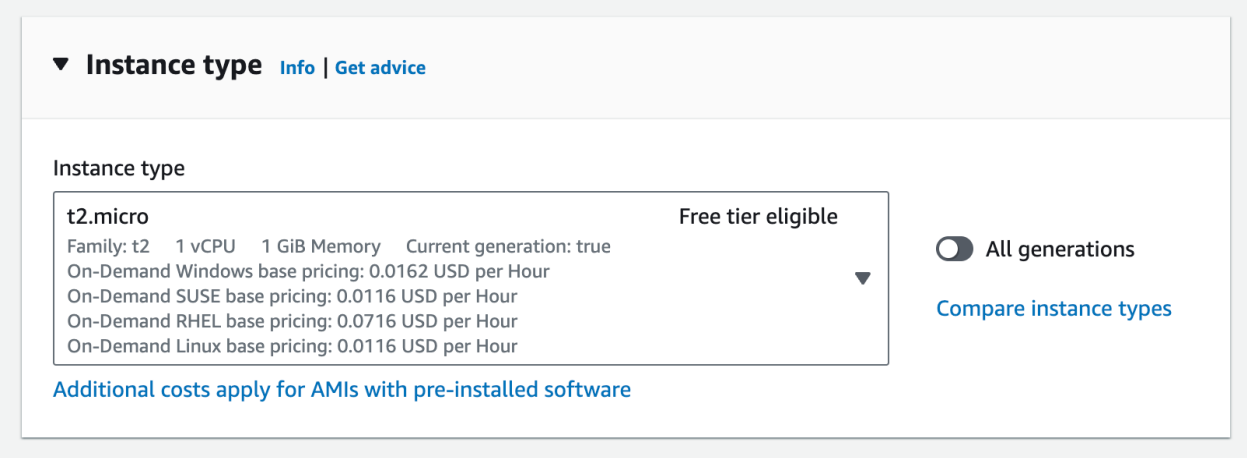
Start by launching a new EC2 instance



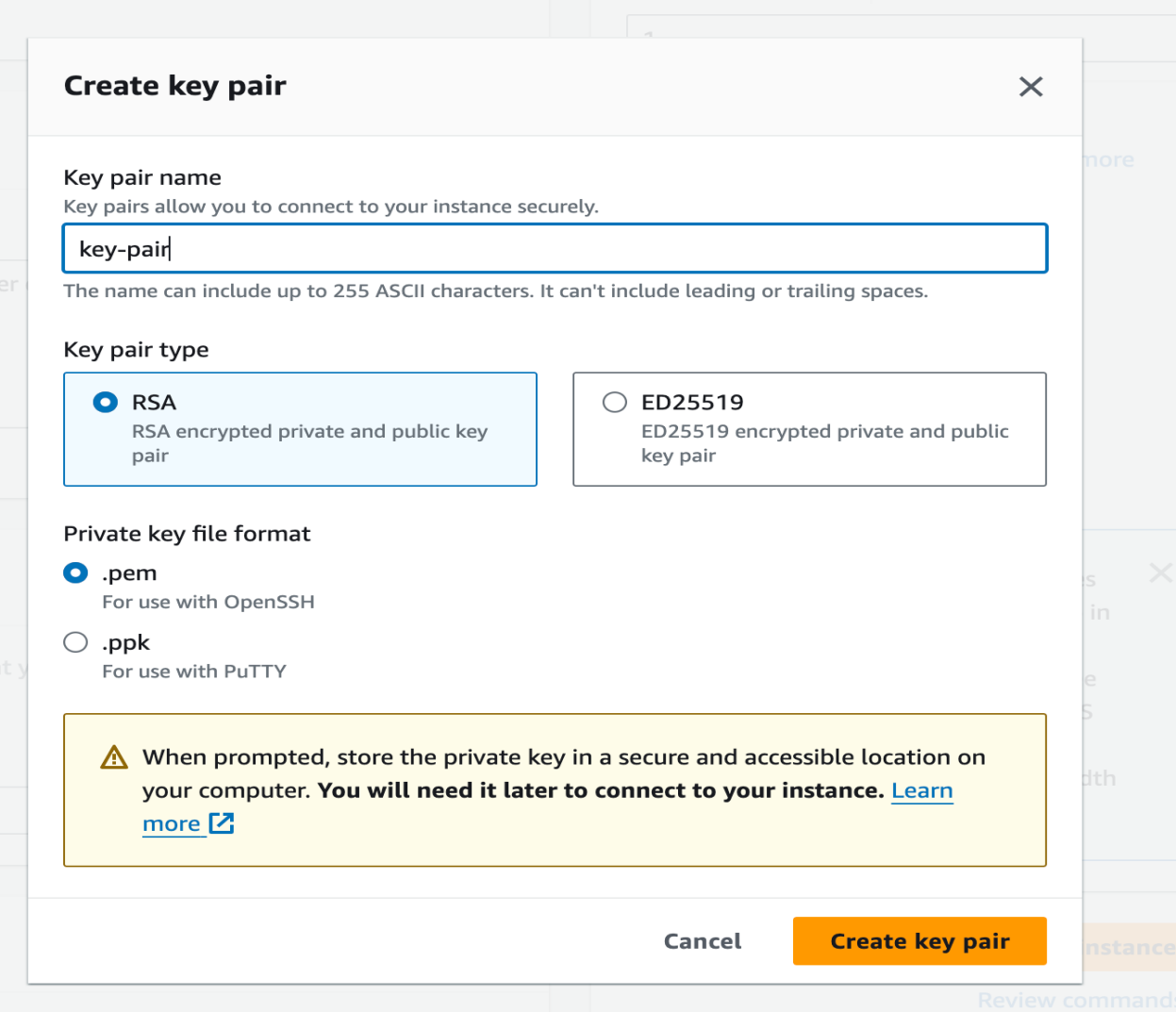
i. selecting an appropriate instance type and configuring the instance details.

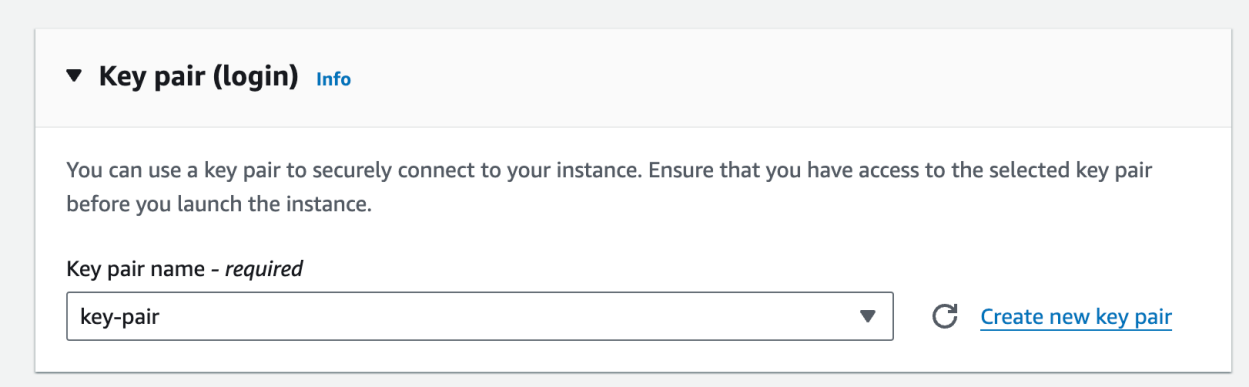


- Select instance type as t2.micro

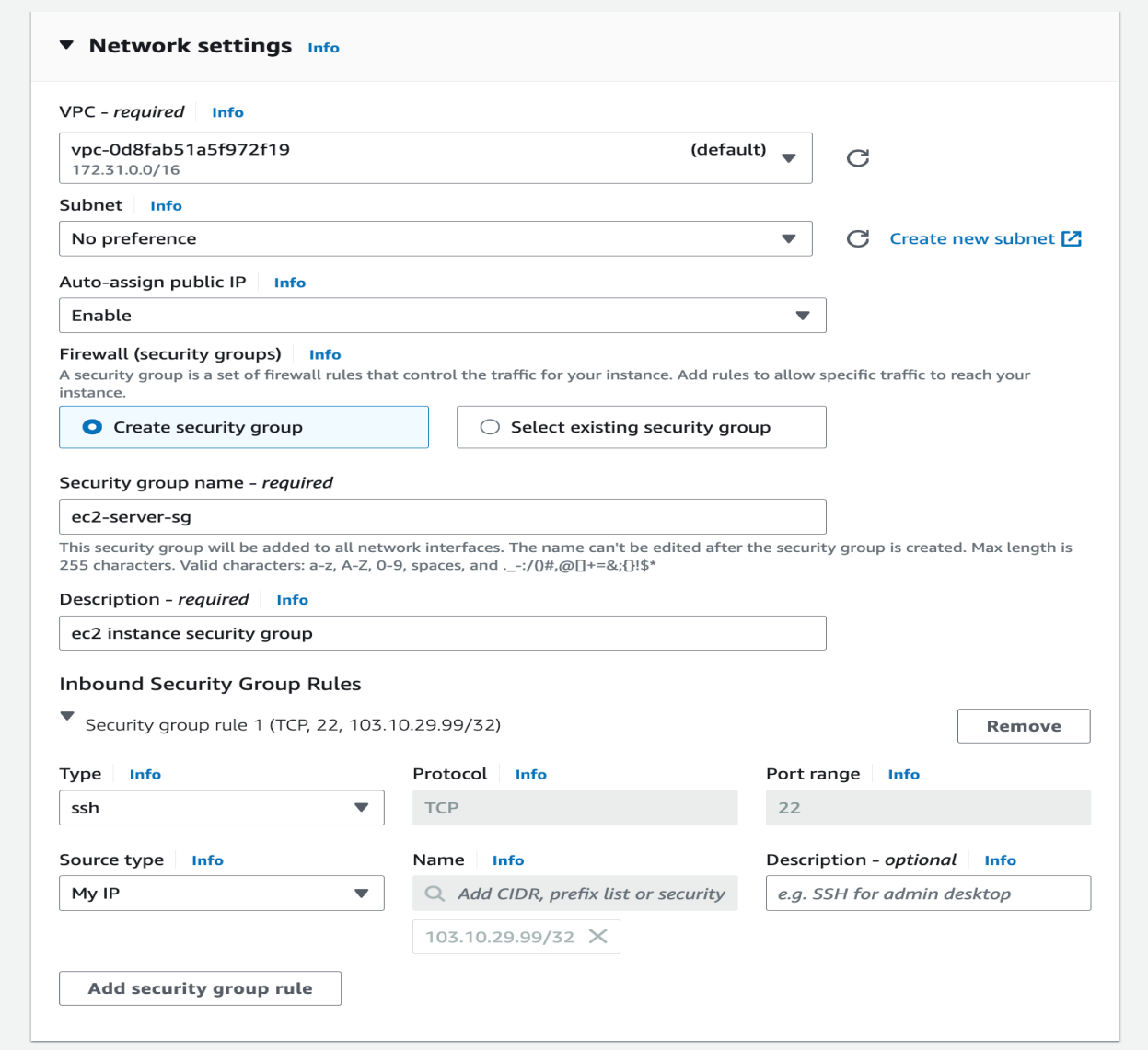


- Creating new Key pair





Create and configure a new Security Group



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

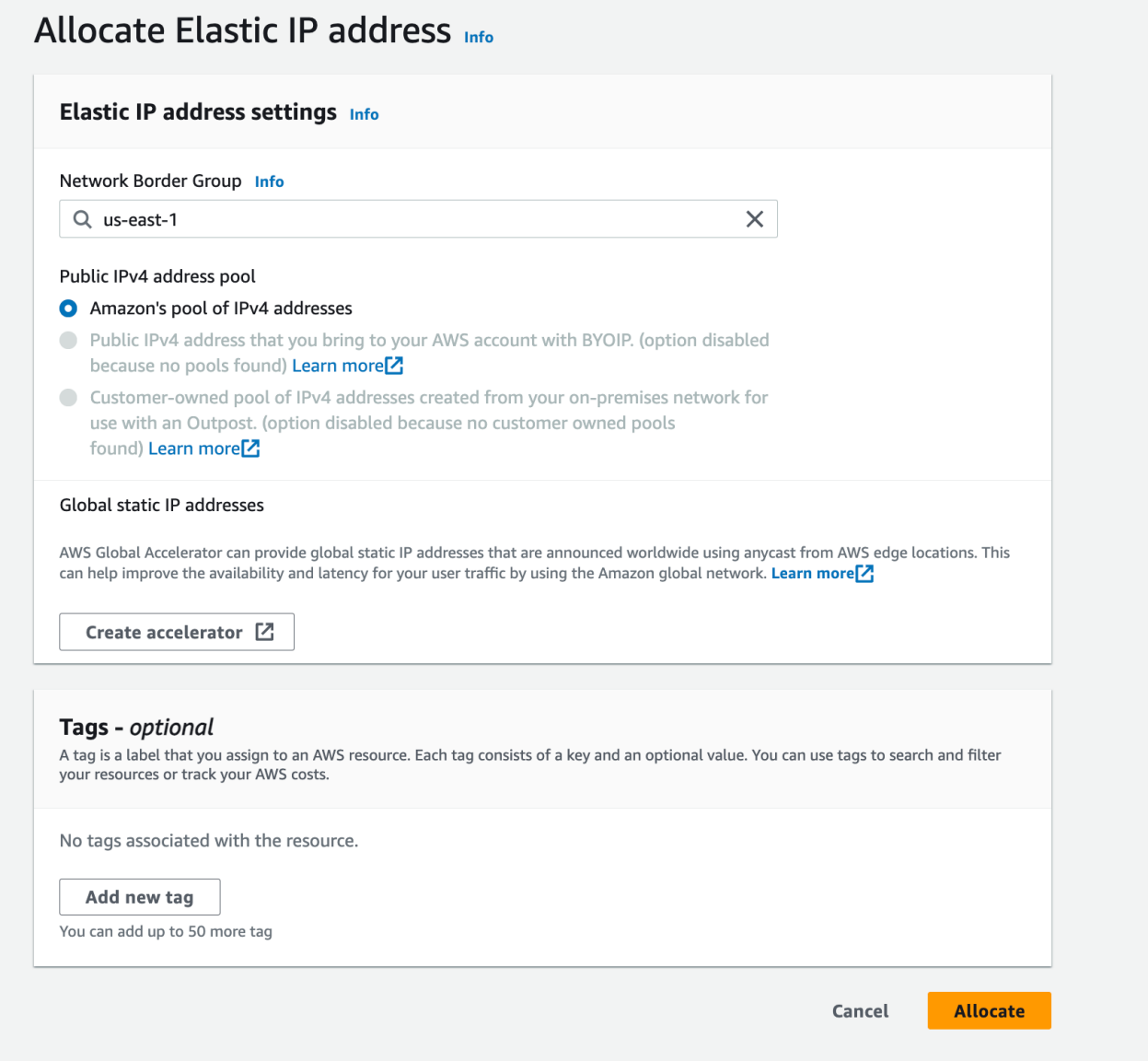
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

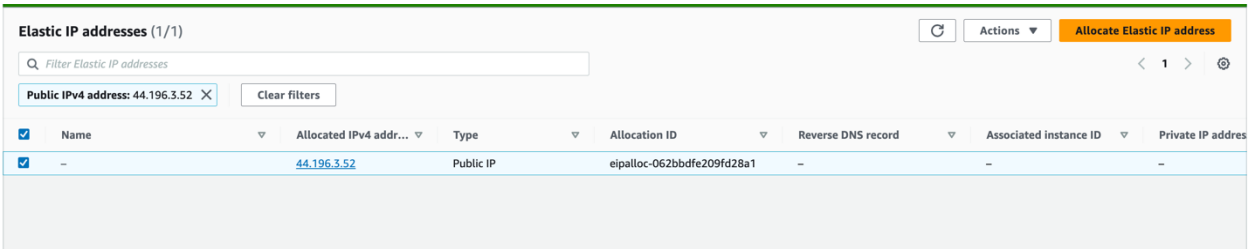
Cancel

Launch instance

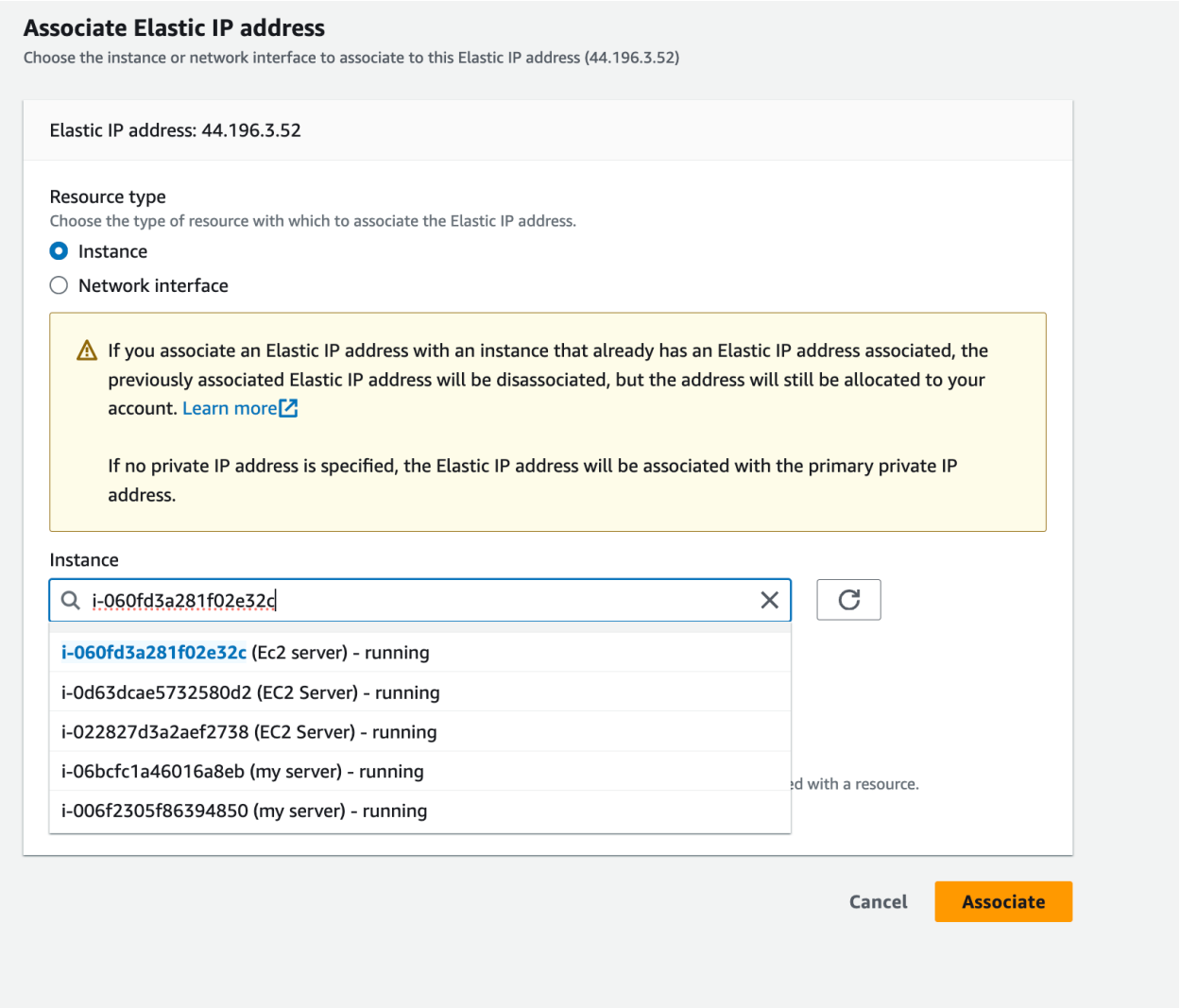
Review commands

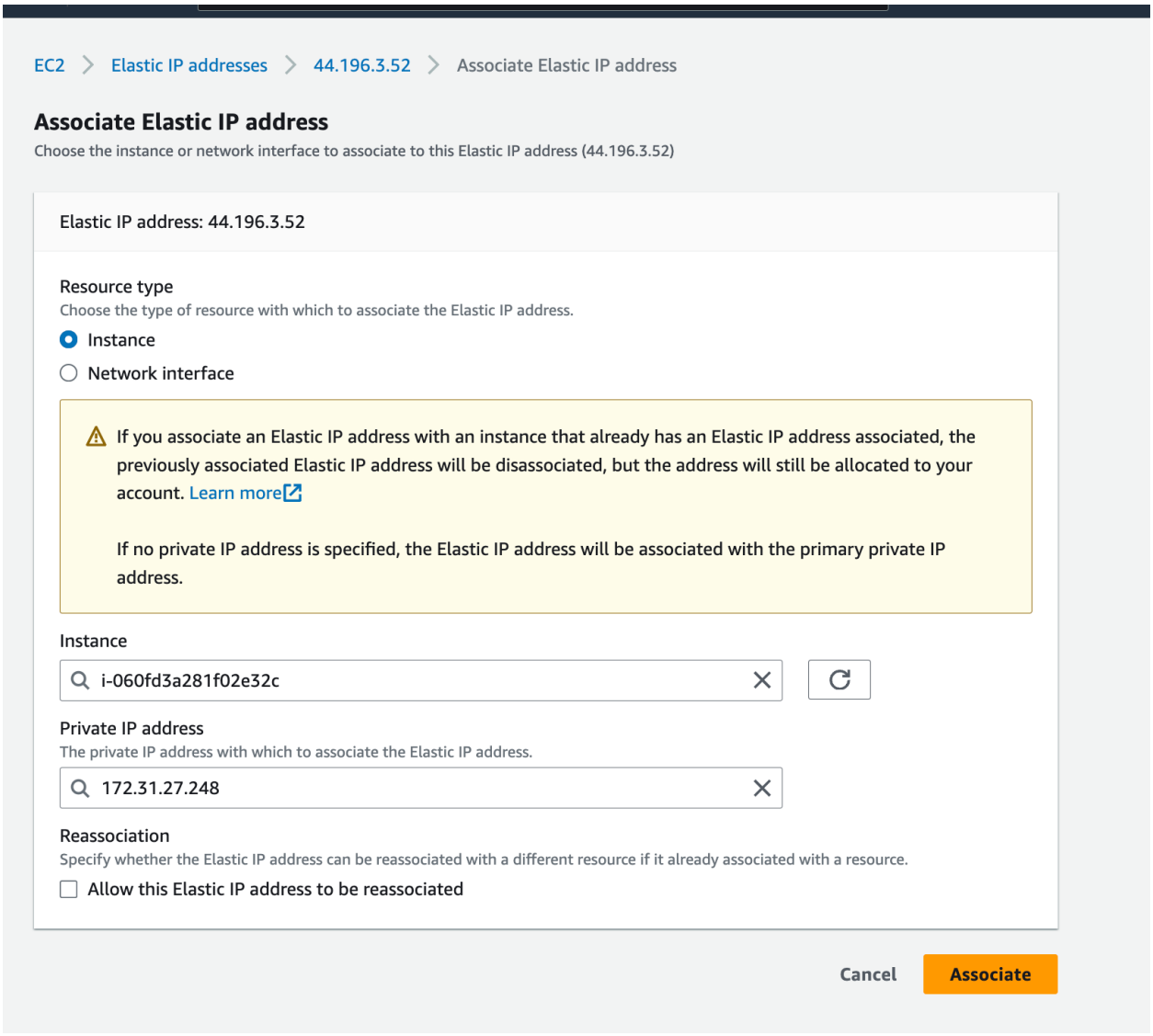
1.1. Allocate an Elastic IP address to the instance

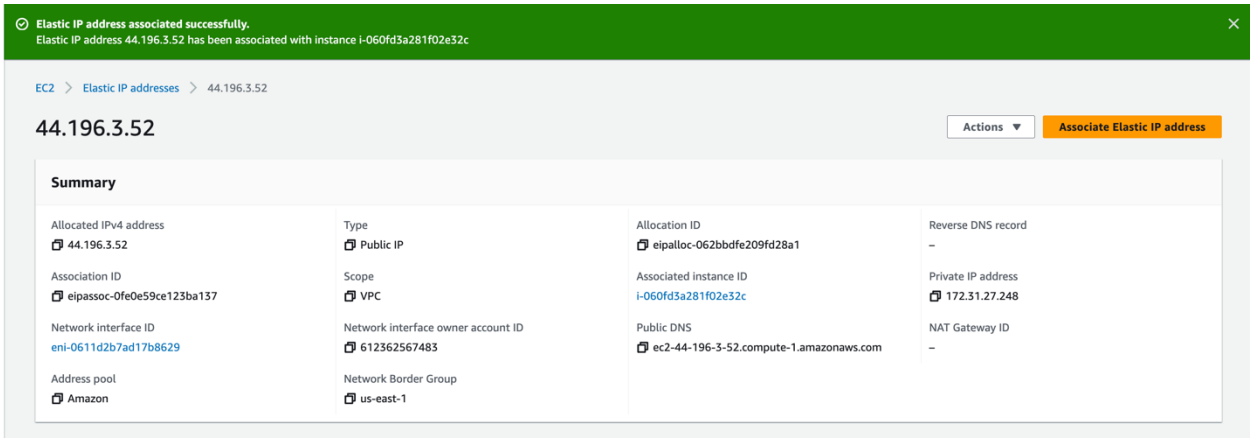


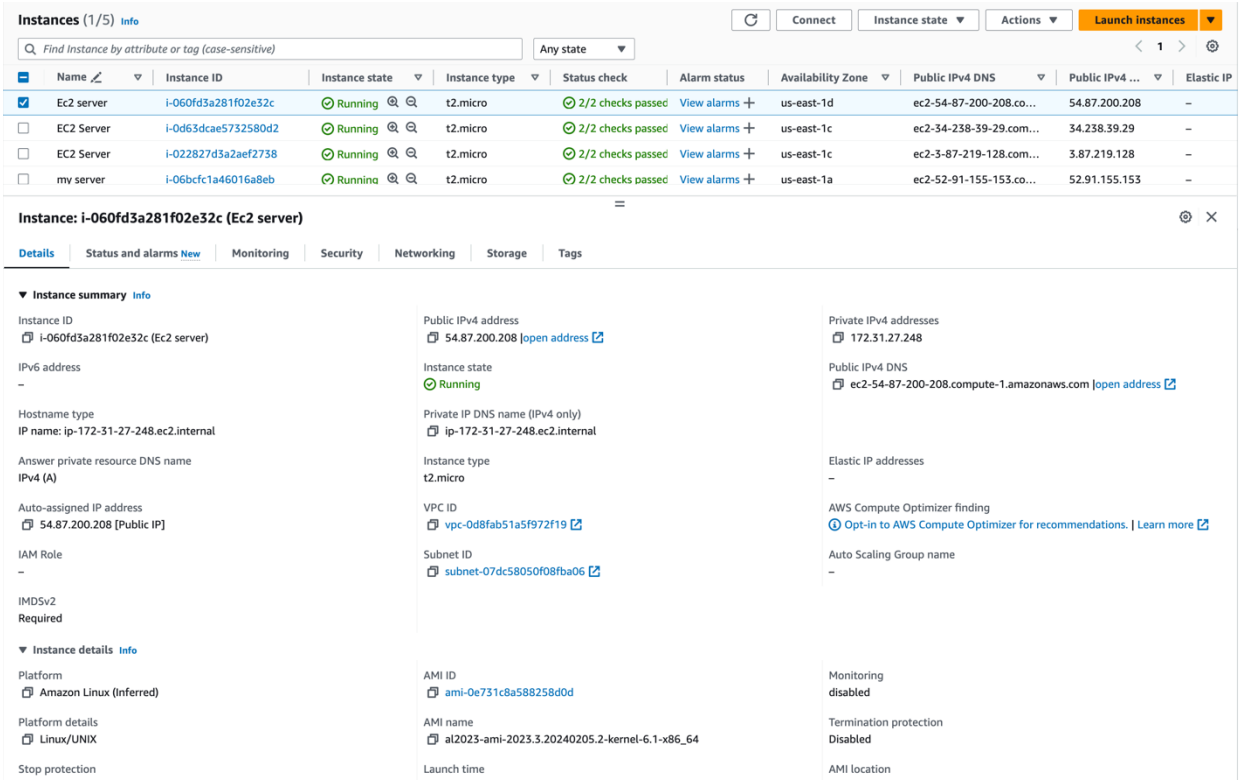


Opeining created elastic ip address

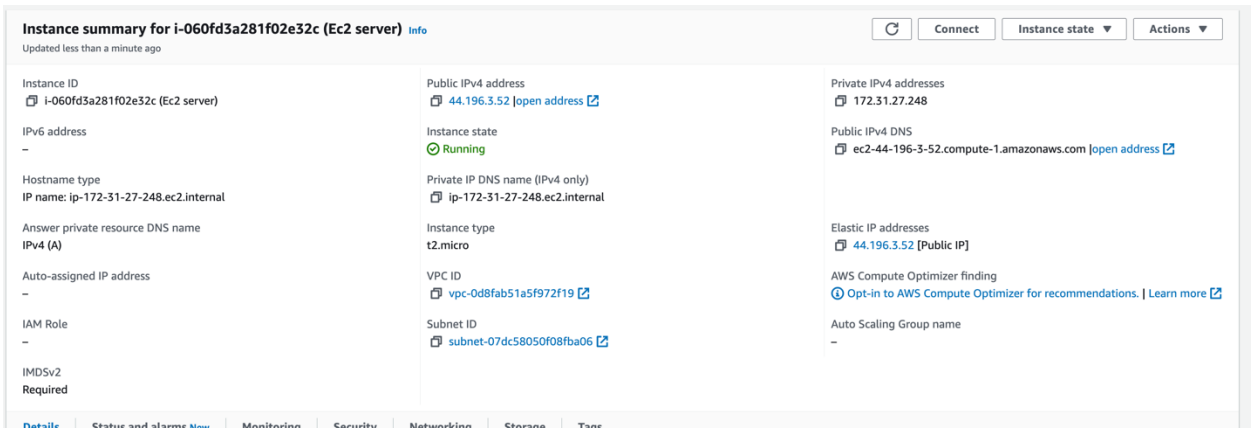



EC2 > Elastic IP addresses > 44.196.3.52 > Associate Elastic IP address
Associate Elastic IP address
Choose the instance or network interface to associate to this Elastic IP address (44.196.3.52)
Elastic IP address: 44.196.3.52
Resource type
Choose the type of resource with which to associate the Elastic IP address.
Instance
Network interface
If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. Learn more
If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.
Instance
i-060fd3a281f02e32c
Private IP address
The private IP address with which to associate the Elastic IP address.
172.31.27.248
Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.
Allow this Elastic IP address to be reassociated
Cancel
Associate


Elastic IP address associated successfully.
Elastic IP address 44.196.3.52 has been associated with instance i-060fd3a281f02e32c
EC2 > Elastic IP addresses > 44.196.3.52
44.196.3.52
Actions
Associate Elastic IP address
Summary
Allocated IPv4 address
44.196.3.52
Type
Public IP
Allocation ID
eipalloc-062bbdfe209fd28a1
Reverse DNS record
–
Association ID
eipassoc-0fe0e59ce123ba137
Scope
VPC
Associated instance ID
i-060fd3a281f02e32c
Private IP address
172.31.27.248
Network interface ID
eni-0611d2b7ad17b8629
Network interface owner account ID
612362567483
Public DNS
ec2-44-196-3-52.compute-1.amazonaws.com
NAT Gateway ID
–
Address pool
Amazon
Network Border Group
us-east-1

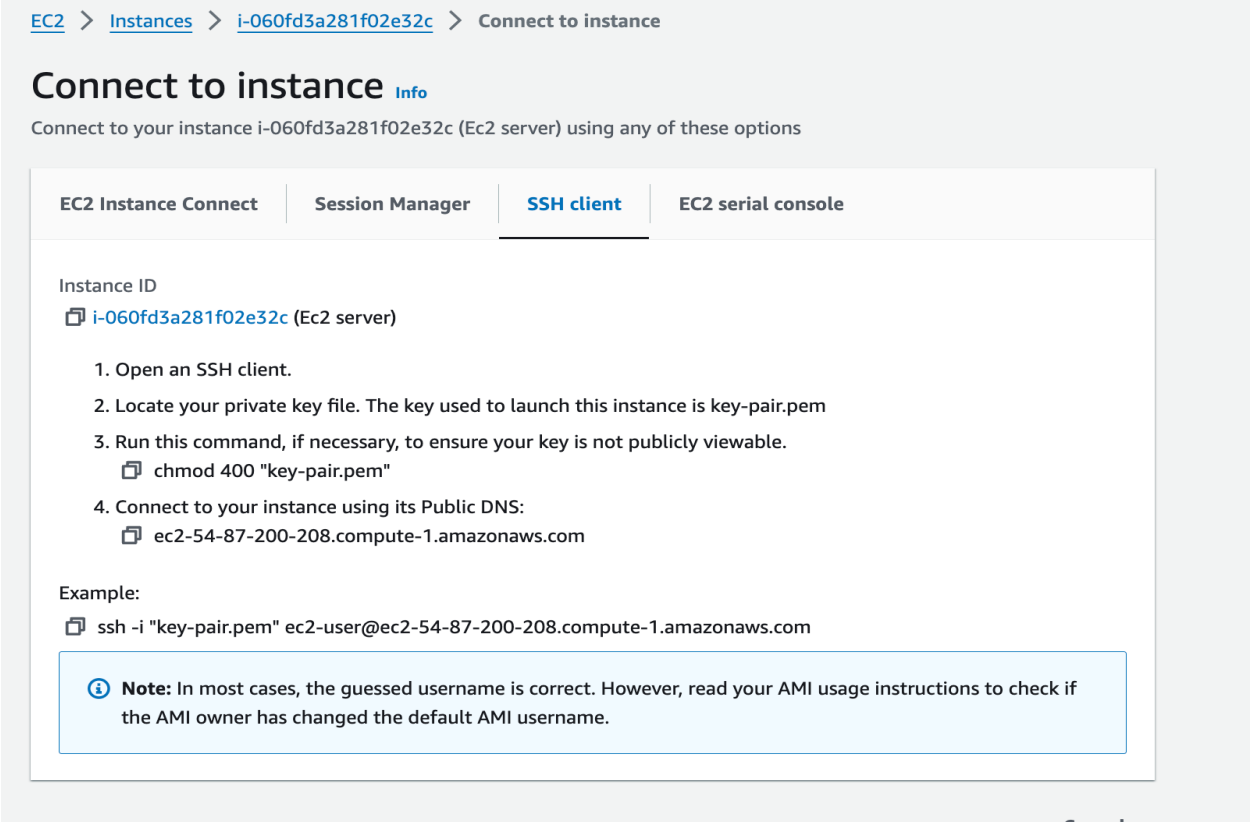


After allocation of elastic ip address in created ec2 instance



1.2. Connecting to the instance via SSH

Connecting to Ec2 instance



- the ipv4 addess of ec2 instance connected via ssh

```
Last login: Mon Feb 12 08:10:19 on console
utsha_mac@Utshas-MacBook-Pro Downloads % chmod 400 "key-pair.pem"
utsha_mac@Utshas-MacBook-Pro Downloads % ec2-54-87-200-208.compute-1.amazonaws.com
zsh: command not found: ec2-54-87-200-208.compute-1.amazonaws.com
utsha_mac@Utshas-MacBook-Pro Downloads % ssh -i "key-pair.pem" ec2-user@ec2-54-87-200-208.compute-1.amazonaws.com
The authenticity of host 'ec2-54-87-200-208.compute-1.amazonaws.com (54.87.200.208)' can't be established.
ED25519 key fingerprint is SHA256:c5k8iyTRsUwd+0J0bWYNw43fSEItnCfcmJ0mwZ/0mc0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-54-87-200-208.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-172-31-27-248 ~]$
```

1. S3 Storage Fundamental Lab

Objective: To gain hands-on experience with Amazon S3 by performing basic storage operations.

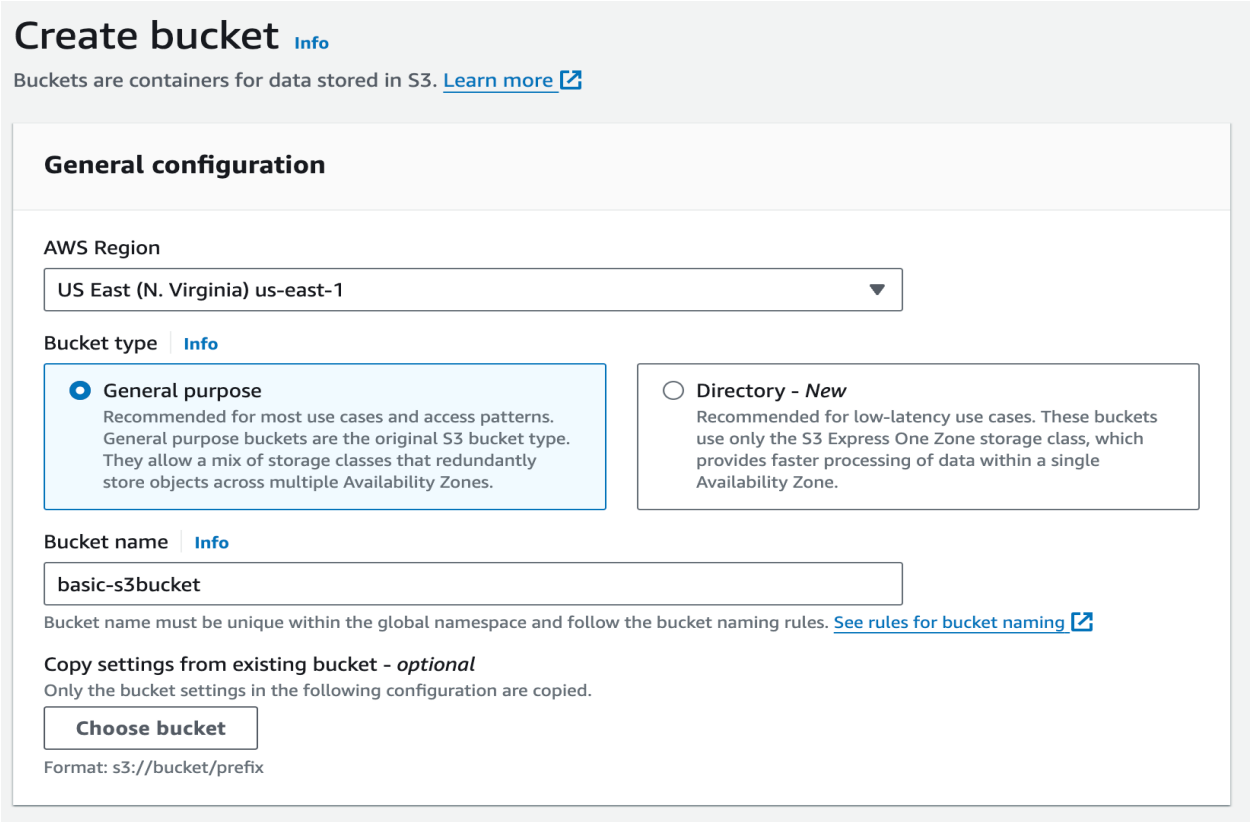
Approach: This lab involves creating an S3 bucket, uploading files to it, and setting up bucket policies for access control. Students will explore the S3 management console, learn about object storage, and understand the concepts of buckets and objects.

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.

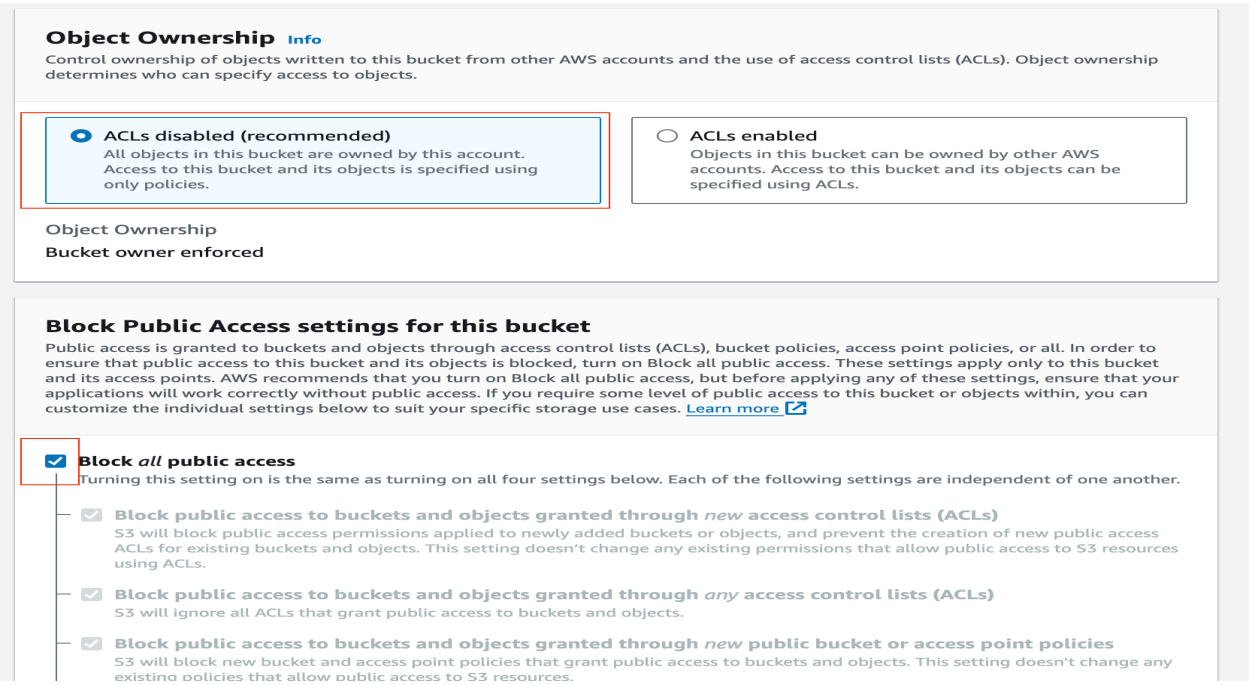
1.1. S3 bucket creation

Step-1: Create S3 bucket

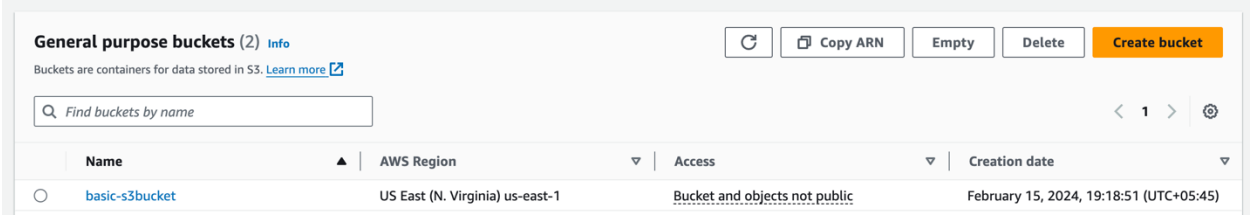
Step-2: Provide general configuration. Select nearest aws region and assigning a bucket name.



Step-3: Default configuration are kept as it is for rest.

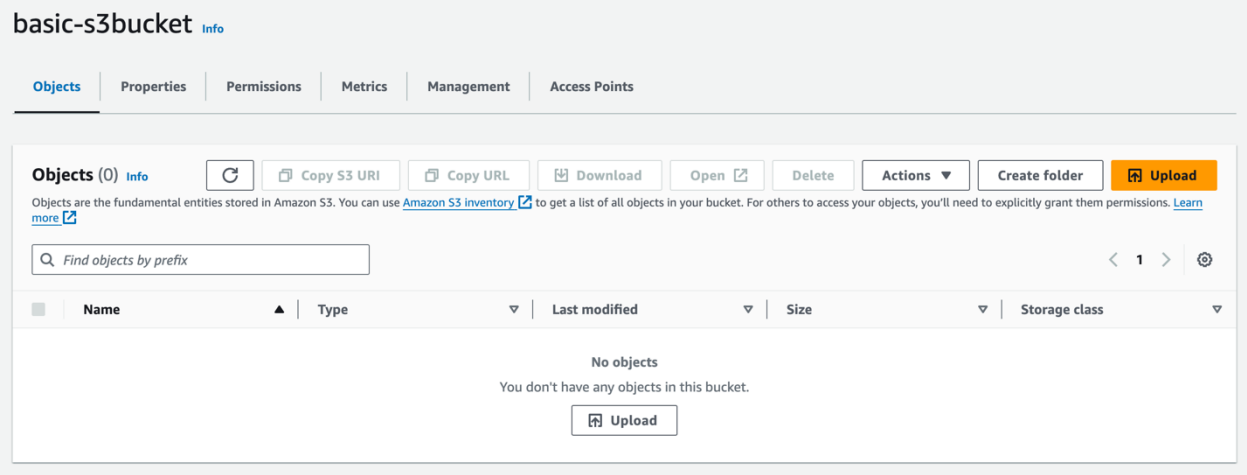


Then, click create bucket and new bucket is created

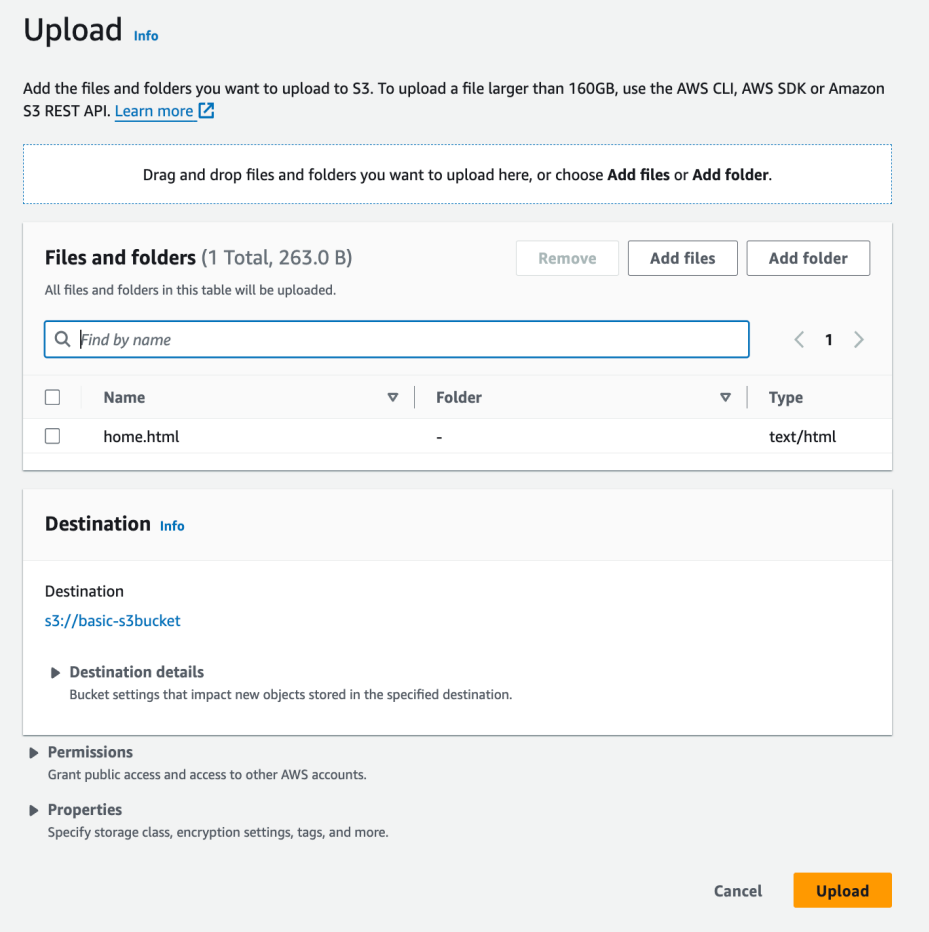


1.2. Upload files

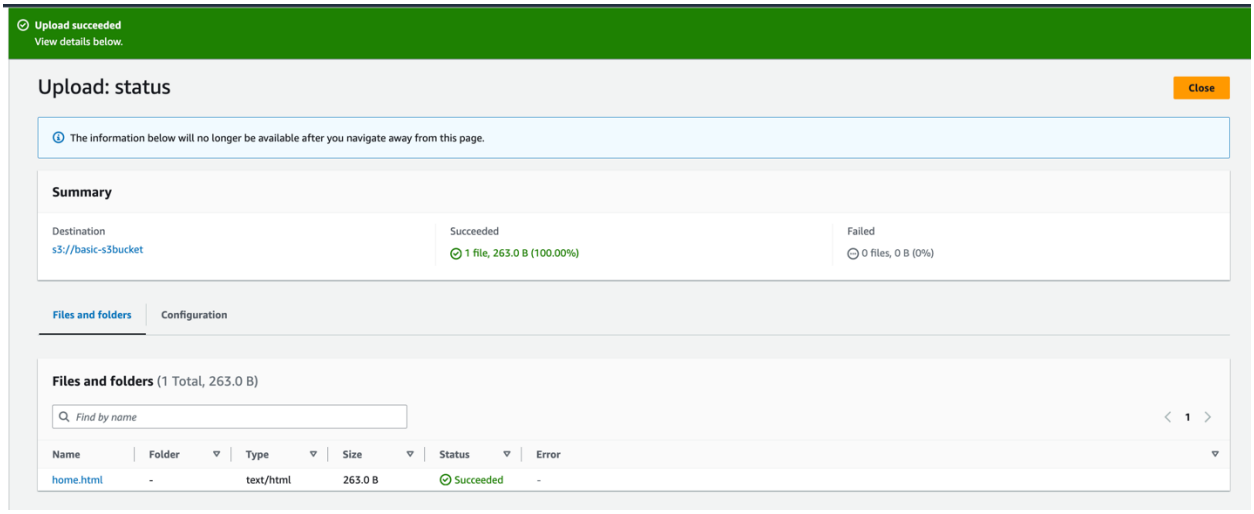
Step-1: Click Upload button to upload a files



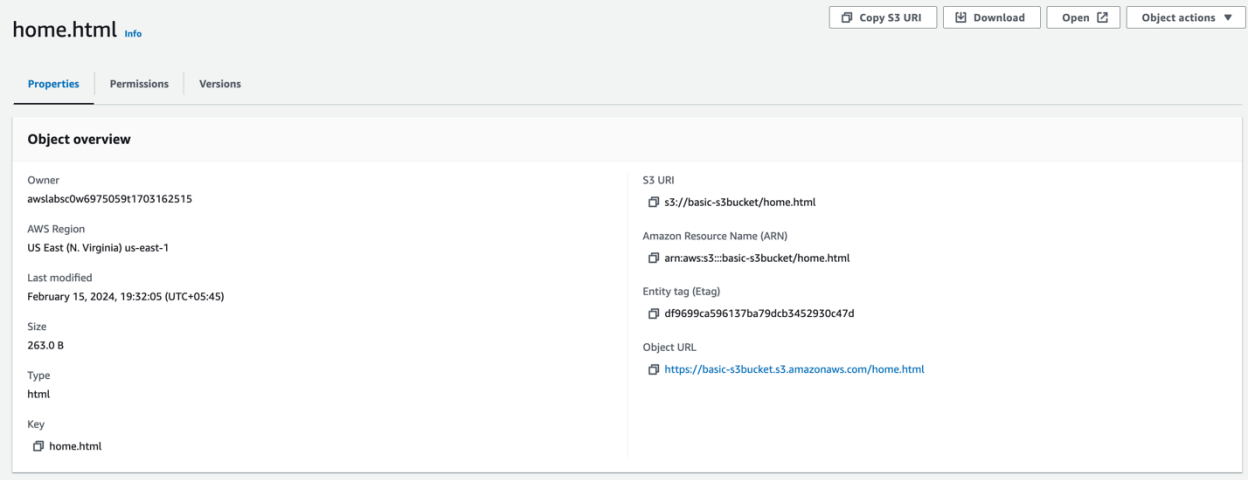
Step-2: Drag and drop the file that is to be uploaded and click upload. The remaining setting is set as default.



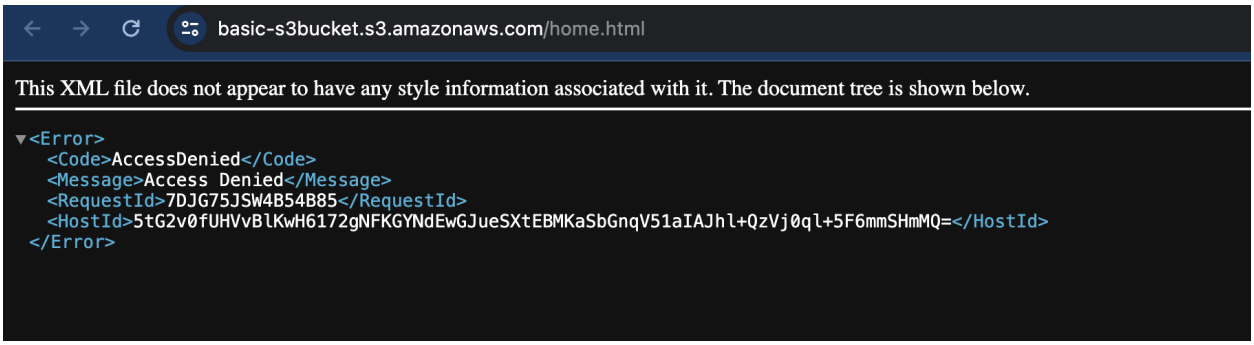
Then, files is uploaded sucessfully in assigned destination.



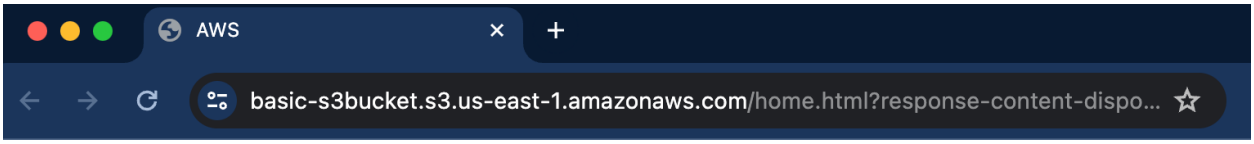
The details of uploaded files can be viewed



When the file is viewed from object url link, the permission accessed denied is shown, as the “Block all public access” setting was checked during file upload.



But, the uploaded file can be accessed from the open button located at top right section of object detail page.

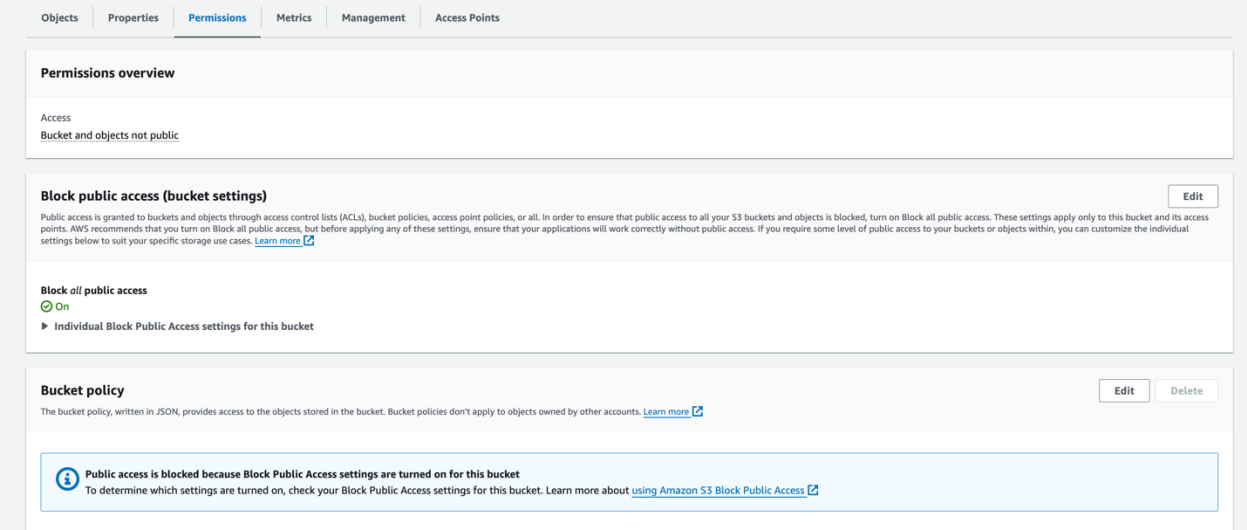


Amazon Web Services

Get started with AWS

1.3. Setting up bucket policies for access control

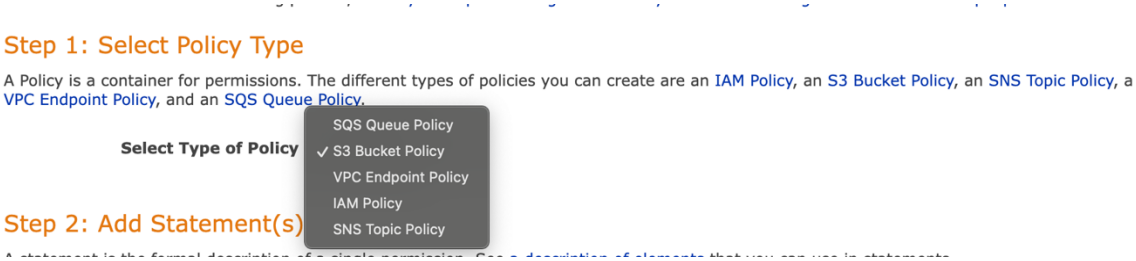
Step-1: Select “permissions” tab and “edit” button of “Bucket policy” section to edit the policies of the bucket, which will take to new screen pf buclet policy.



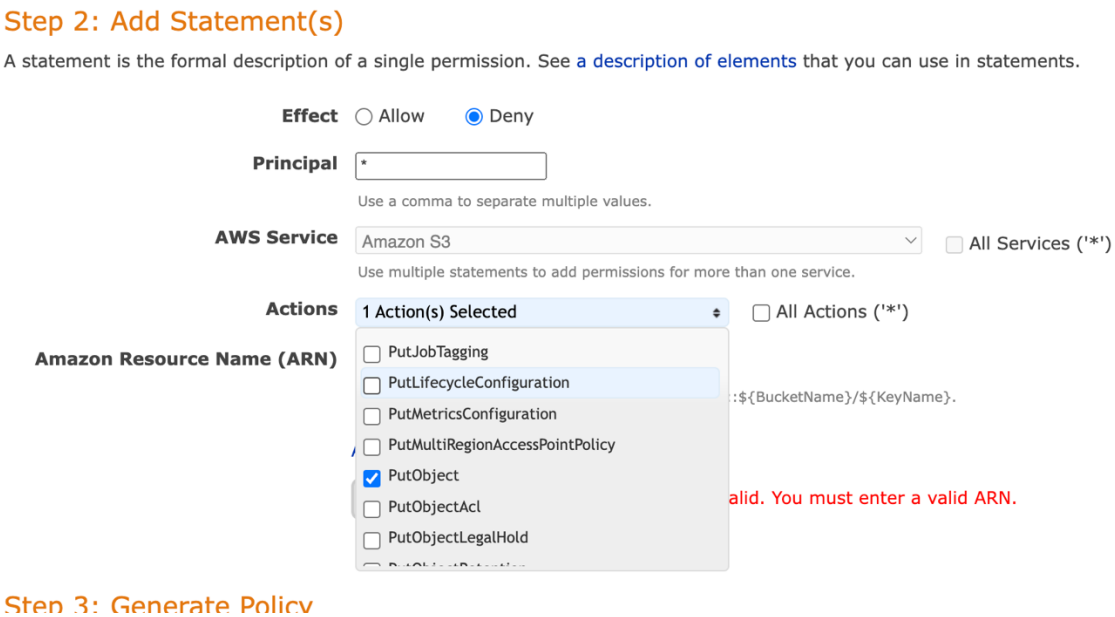
Step-2: Select “Policy generator” to generate the policy.

This navigated to new tab of policy generator. Here, policies are defines for access control.

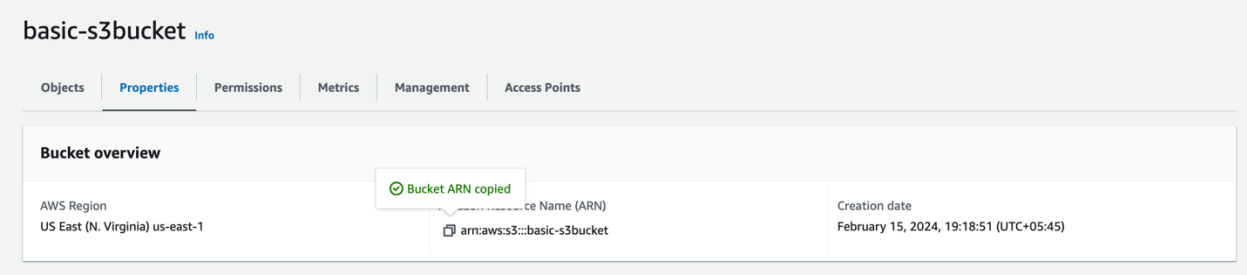
Step-3: Select policy type as “S3 Bucket Policy”



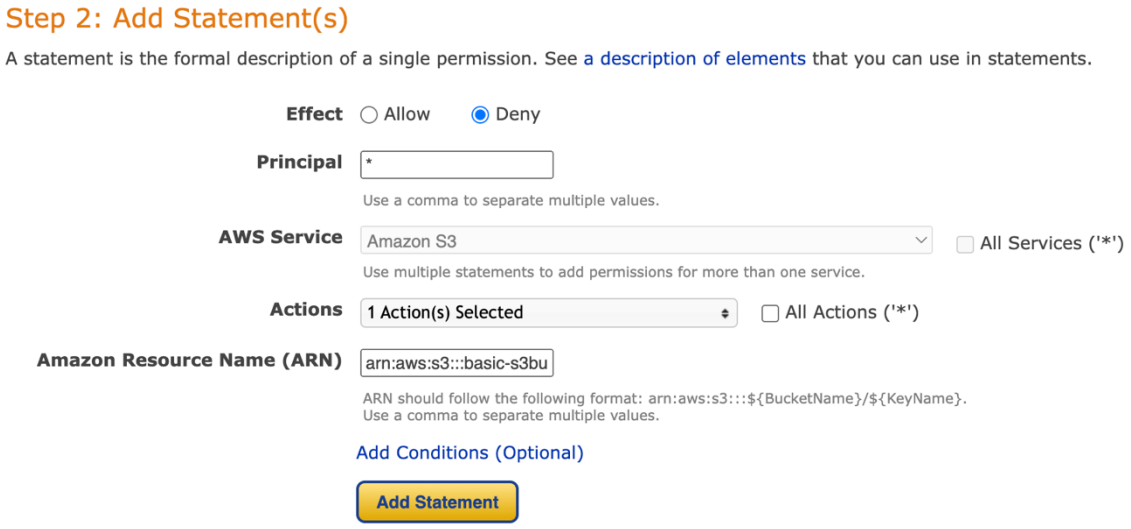
Step-4: Fill the form as required. In effect “deny” and in action “PutPbject” is selected.



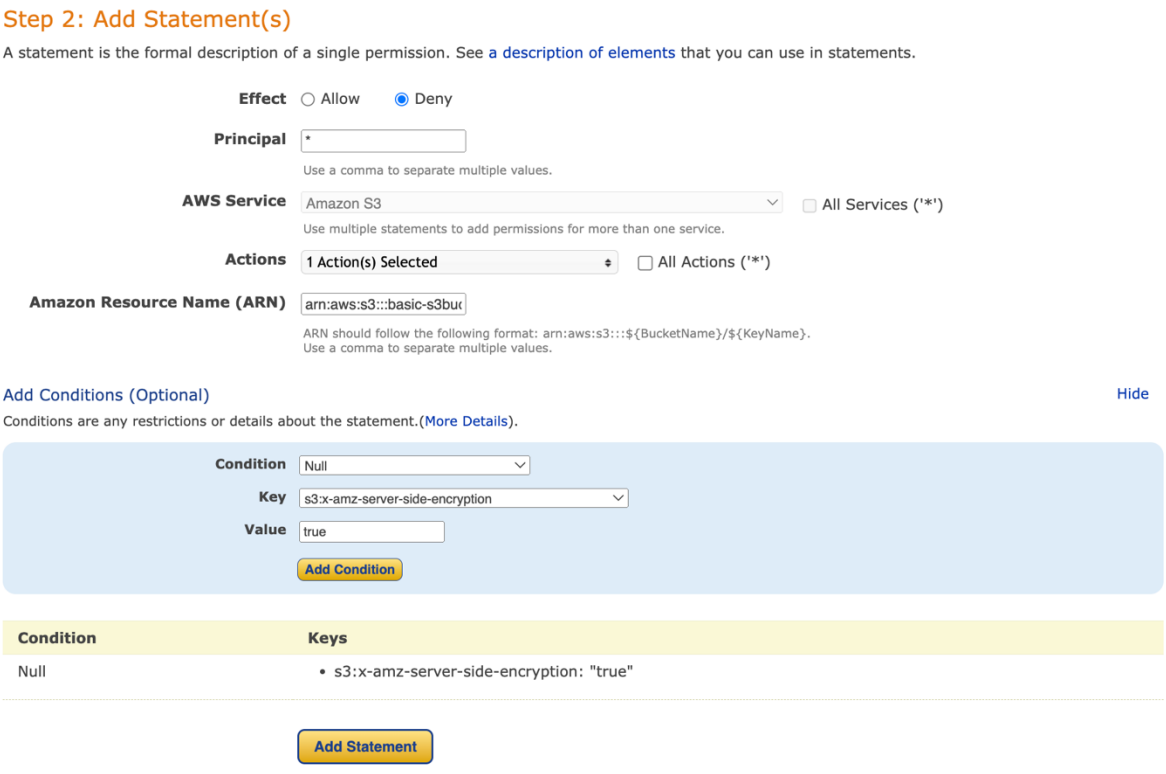
ARN value of created s3 bucket is assigned in ARN section, this can be found in bucket properties section



/* is added after bucket ARN value.



Then, conditions for denying specific object to be uploaded. Here, we are denying any objects with Key s3:x-amz-server-side-encryption set to Null.



Click “Add Statement” and then json document of s3 bucket policy is generated with “Generate Policy”

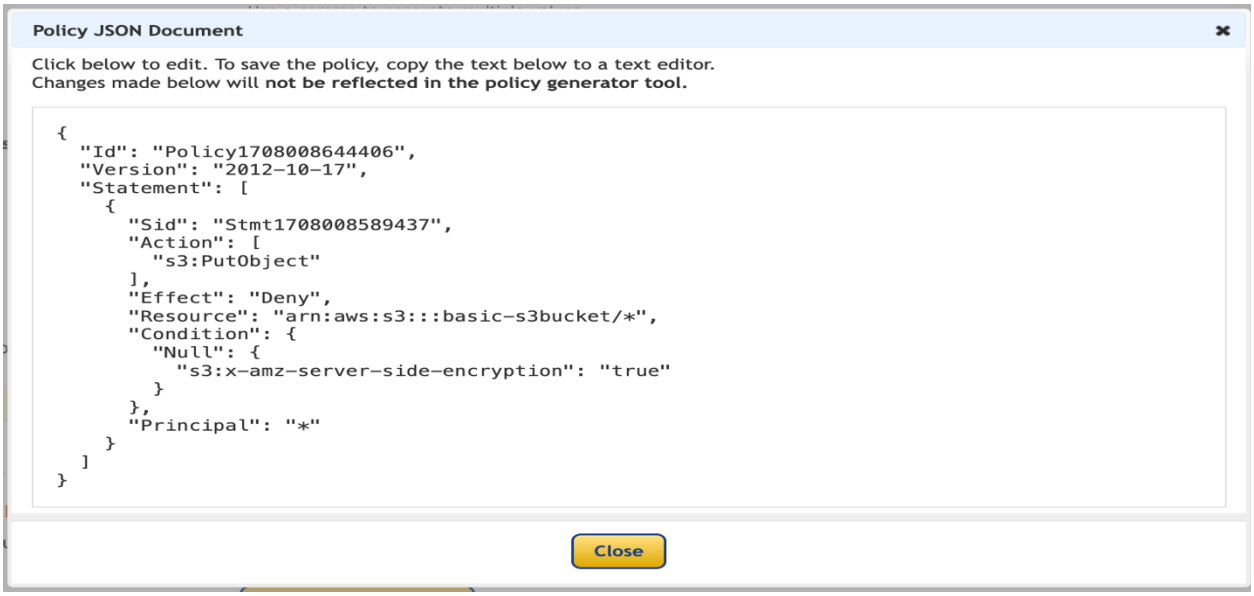
You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• *	Deny	• s3:PutObject	arn:aws:s3:::basic-s3bucket/*	• Null ◦ s3:x-amz-server-side-encryption: "true"

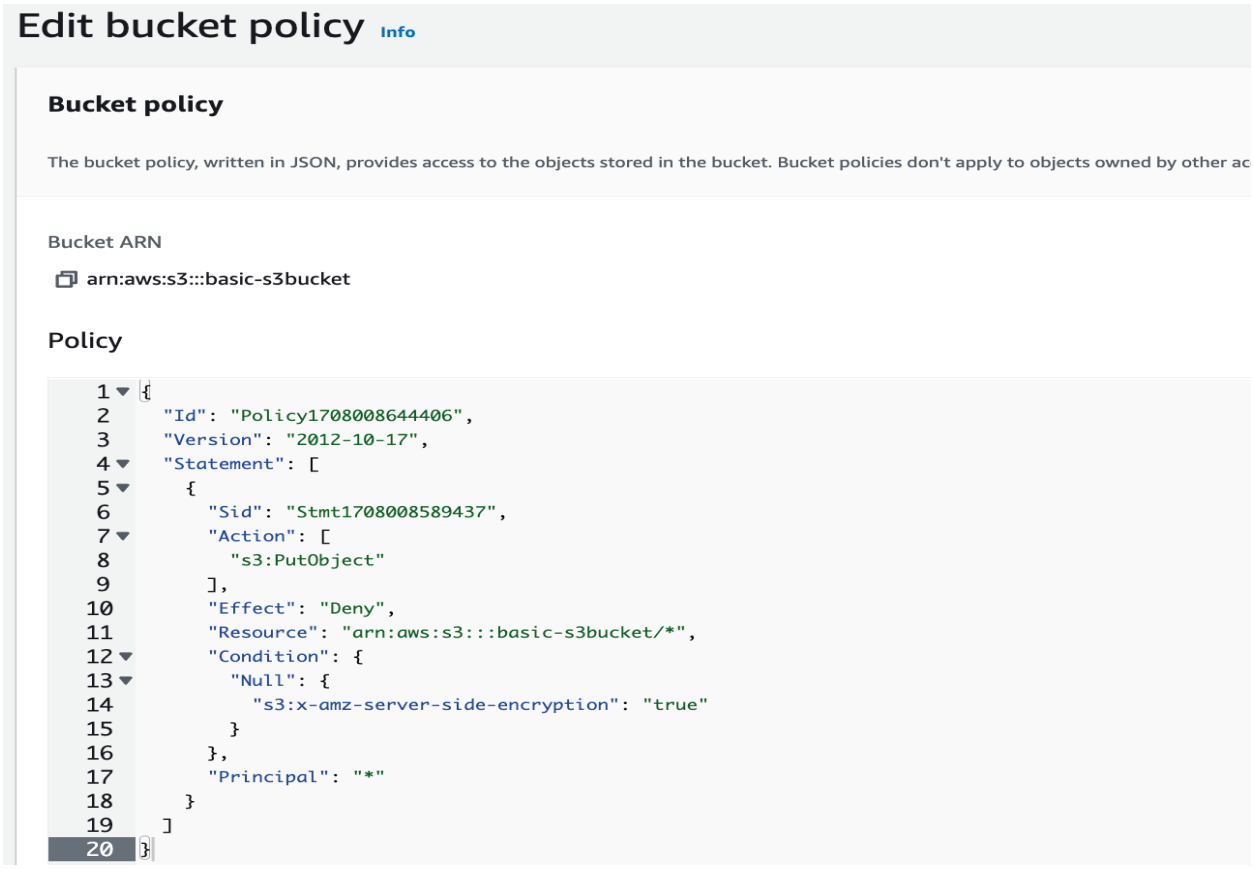
Step 3: Generate Policy

A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more statements.

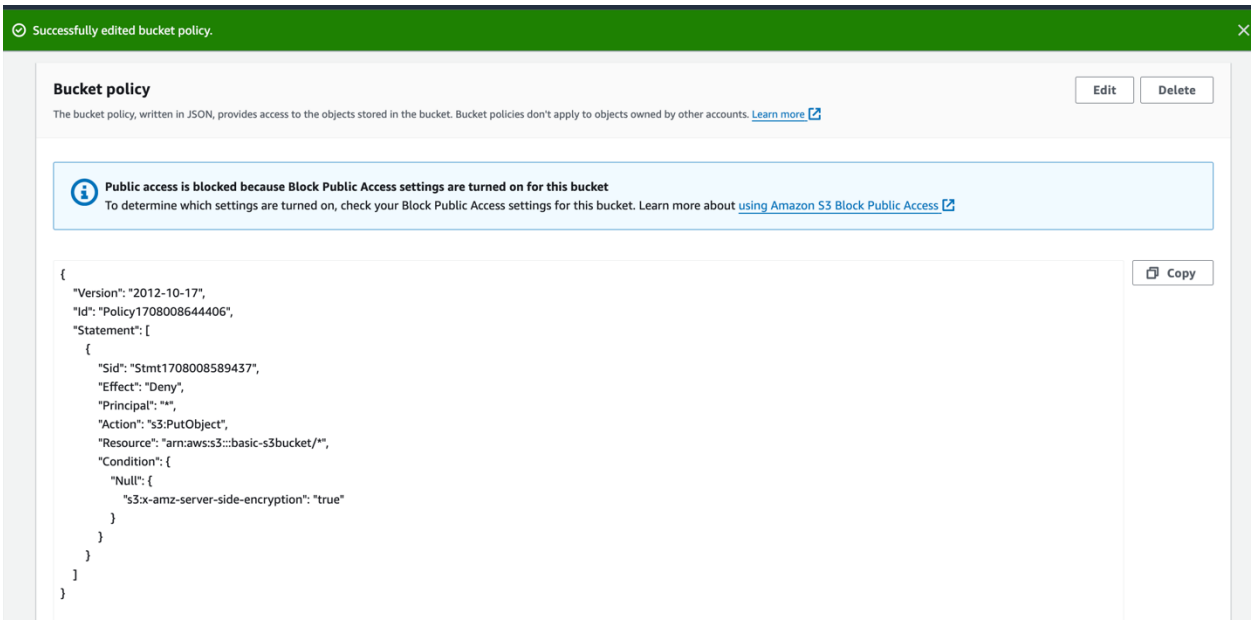
Generate Policy Start Over



The generated policy is copied and paste to bucket policy.

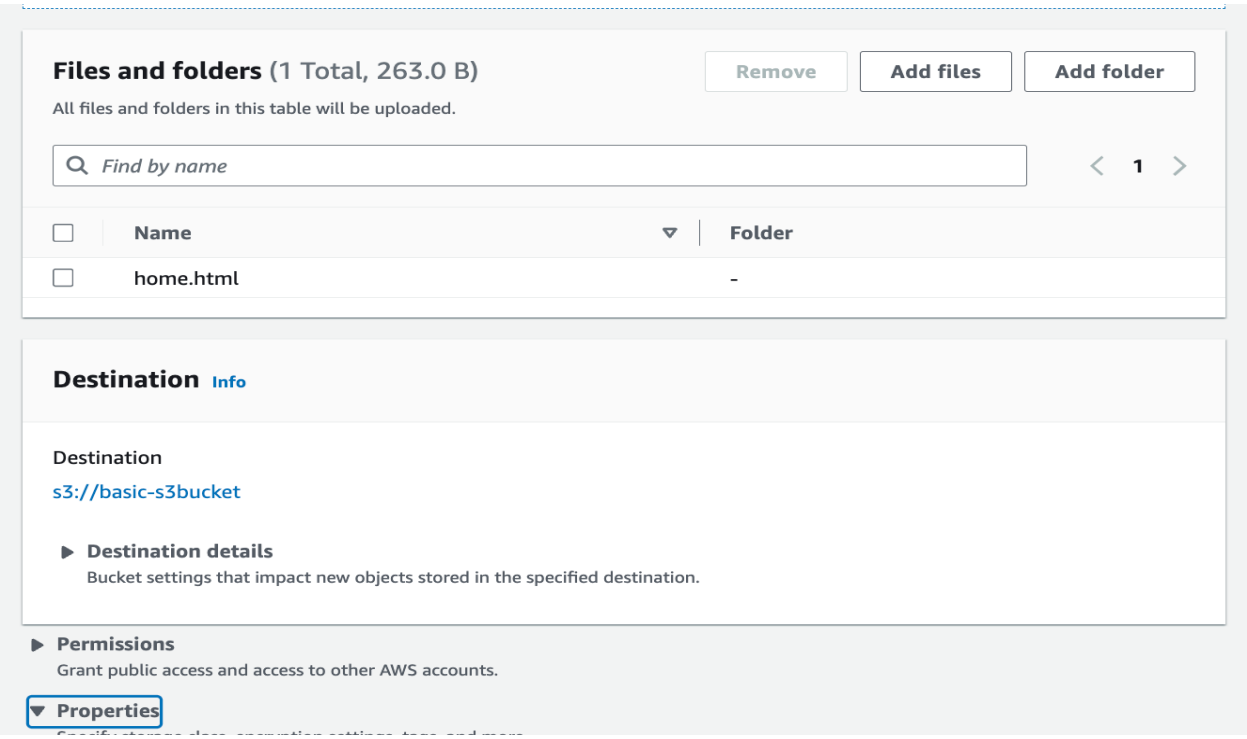


Then the changes is saved clicking “Save Changes” button.

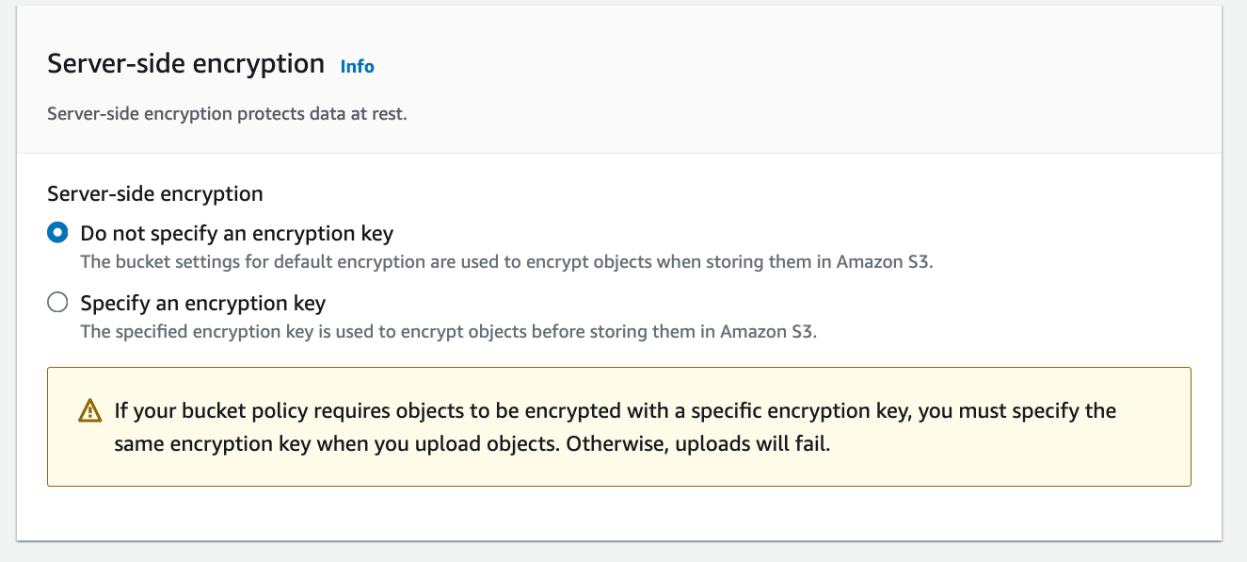


2.4. Testing the policy

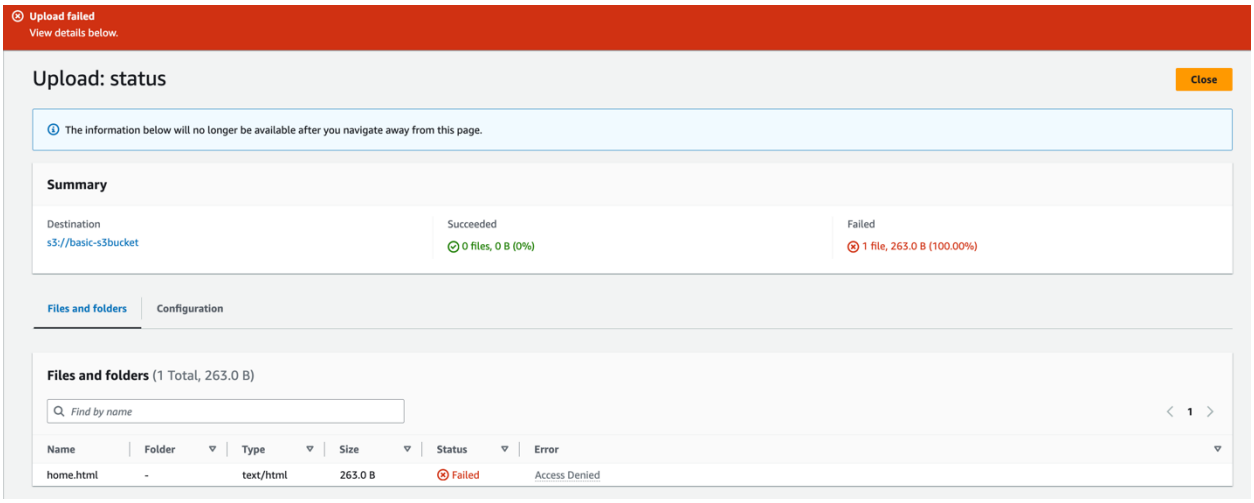
Uploading the same html file without specifying any encryption key



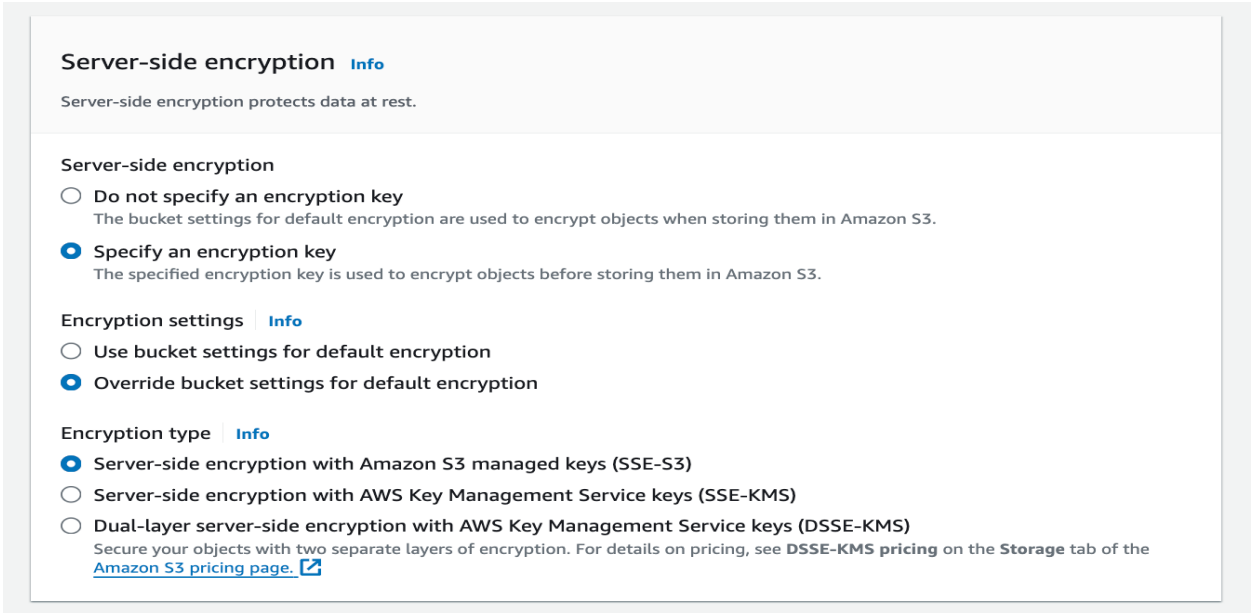
Server side encryption can be updated from “Properties” section



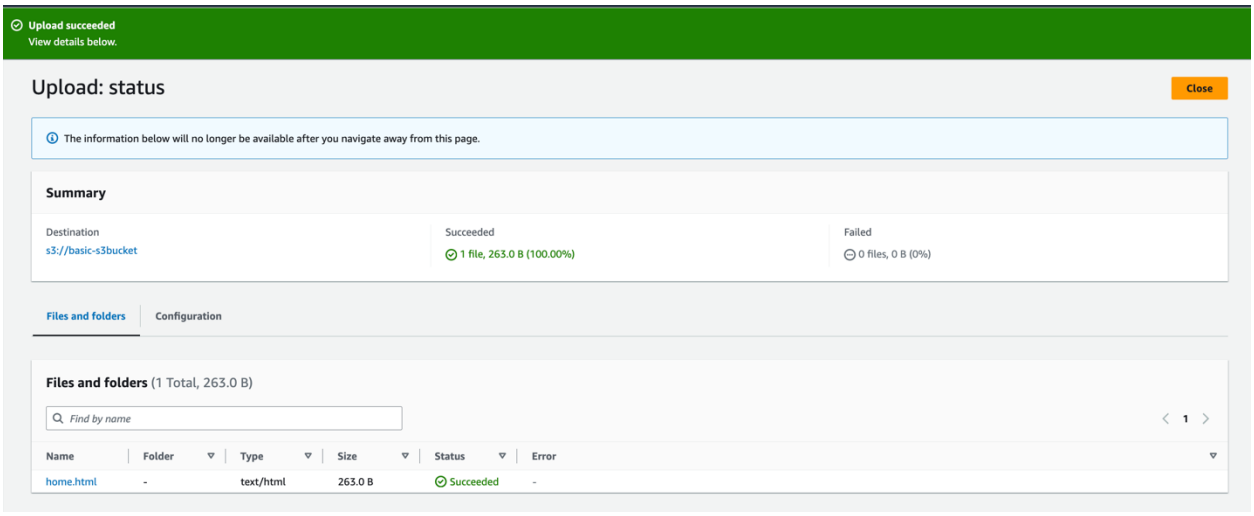
The access is denied as the encryption key is not specifed while uploading the file.



Now, for uploading the file, below setup is configured



Now, the file is uploaded successfully after adding encryption key.

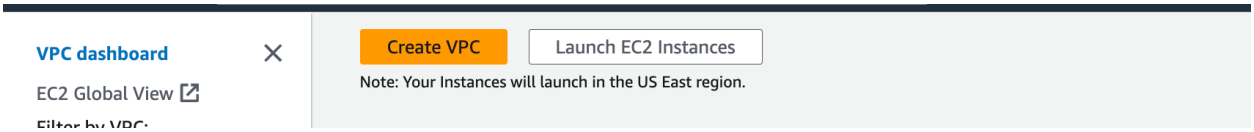


2. VPC Configuration

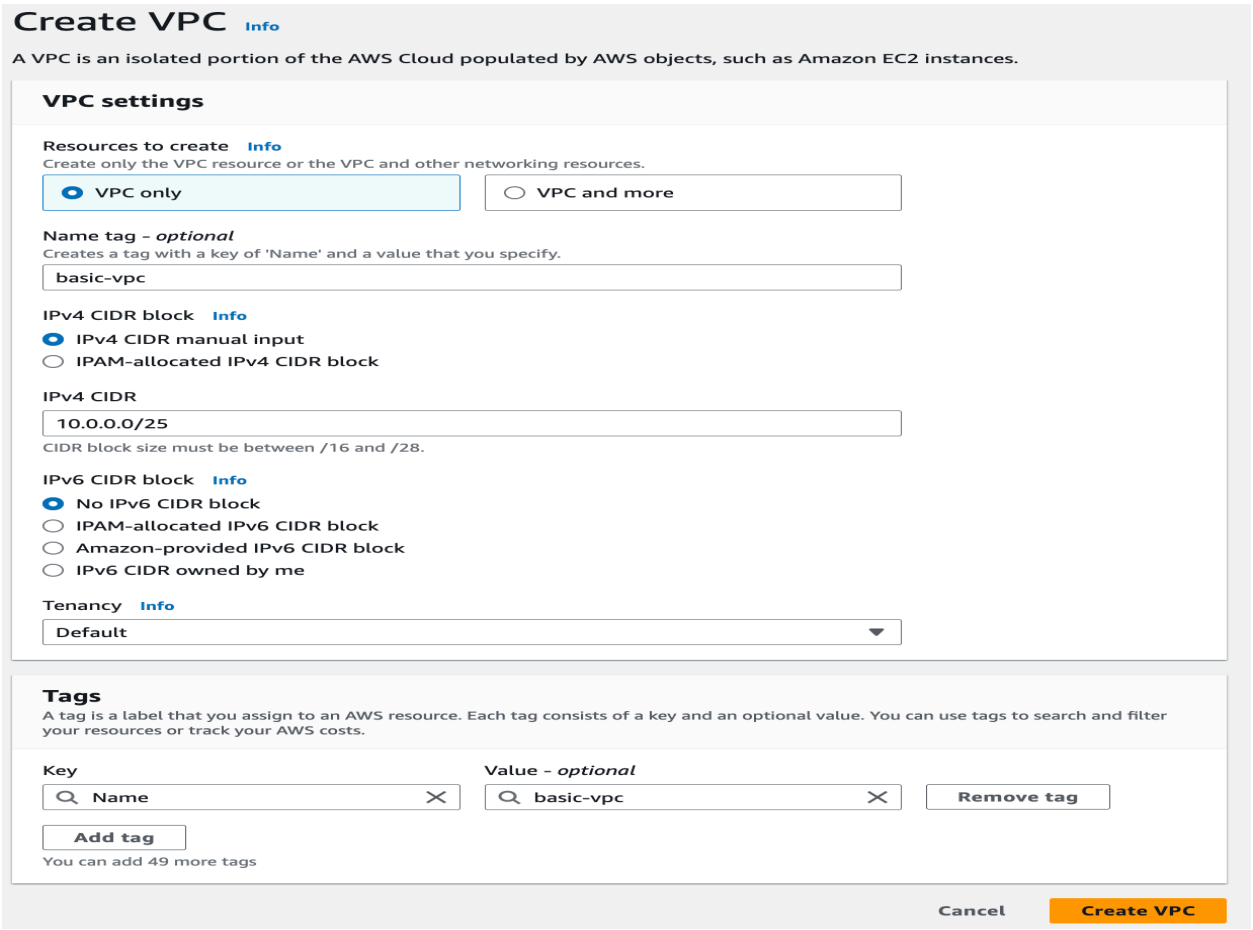
- **Objective**: To understand the fundamentals of AWS networking through the configuration of a Virtual Private Cloud (VPC).
- **Approach**: Students will create a new VPC, add subnets, set up an Internet Gateway, and configure route tables. The lab might also include setting up a simple EC2 instance 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.

2.1. Create VPC

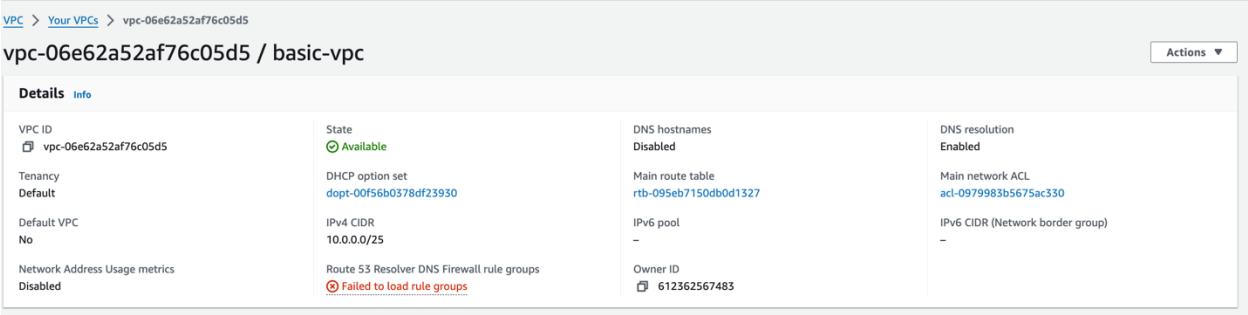
Navigate to VPC dashboard and click “Create VPC” button to create a new VPC



Configure the VPC form and assign the requested values



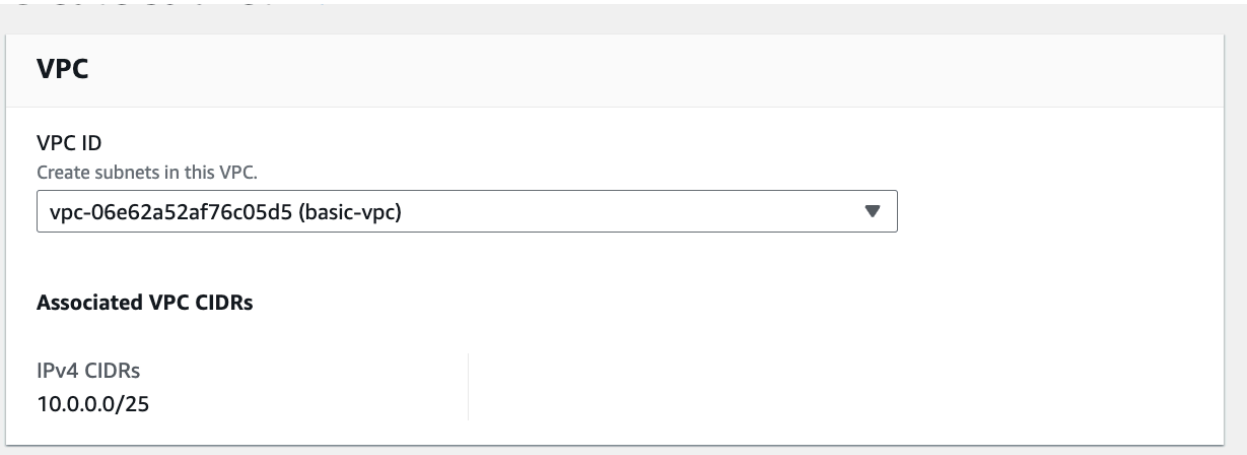
Then, a new VPC is created



2.2. Add Subnets

Step-1: Navigate to subnet section of VPC dashboard and configure subnet.

Step:-2: Select created VPC ID



Step-3: Assign subnet name and select nearest possible availabilty zone and then create subnet

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

vpc-subnet-01

The name can be up to 256 characters long.

Availability Zone Info

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1a

IPv4 VPC CIDR block Info

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

10.0.0.0/25

IPv4 subnet CIDR block

10.0.0.0/26 64 IPs

▼ Tags - *optional*

Key: Name

Value - *optional*: vpc-subnet-01

Remove

Add new tag

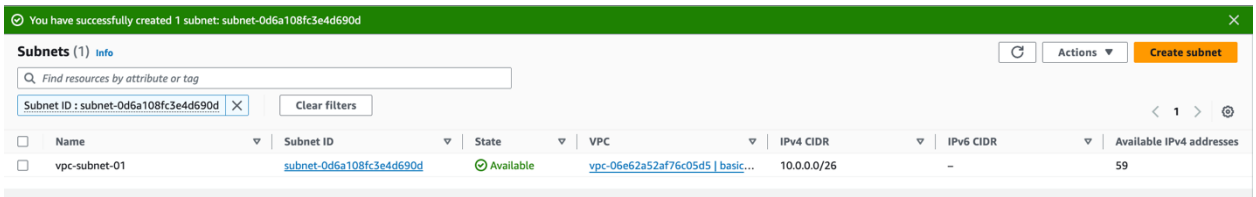
You can add 49 more tags.

Remove

Add new subnet

Cancel Create subnet

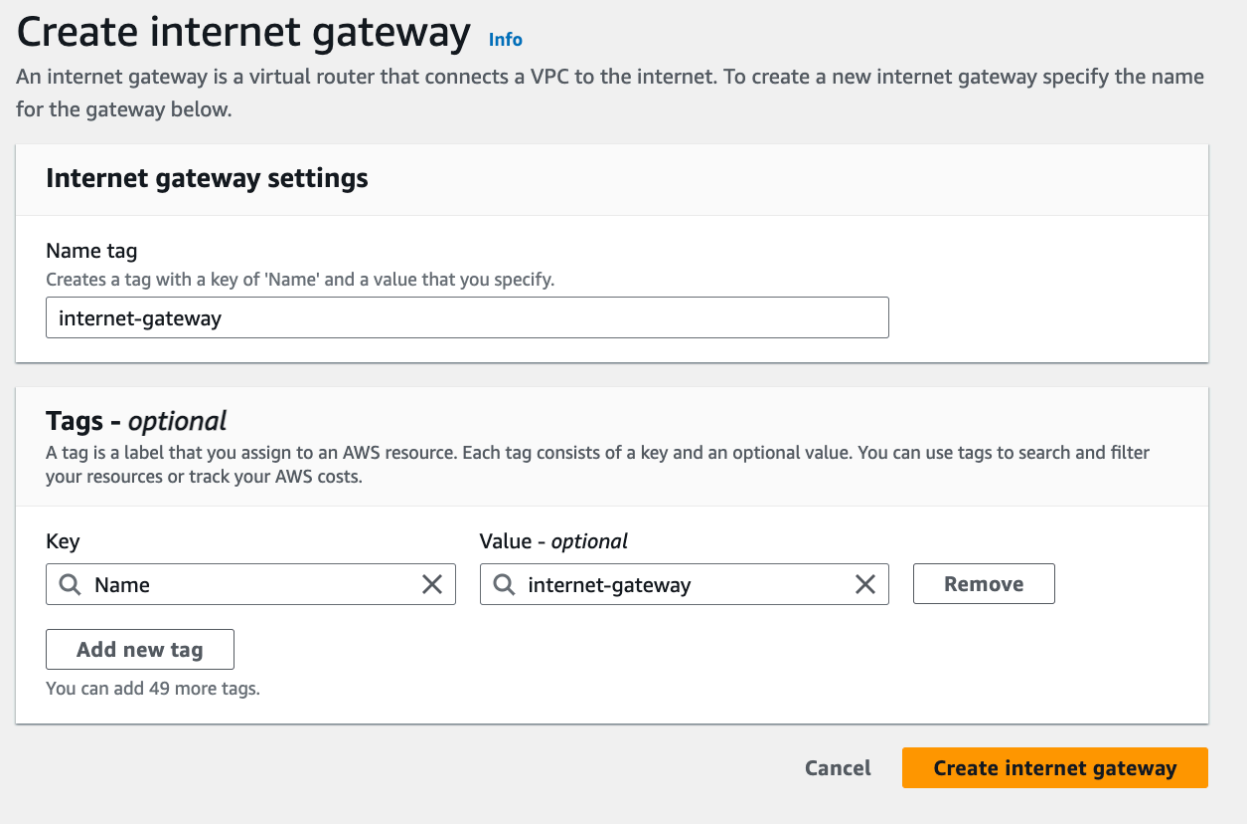
Then, the subnet is created successfully.

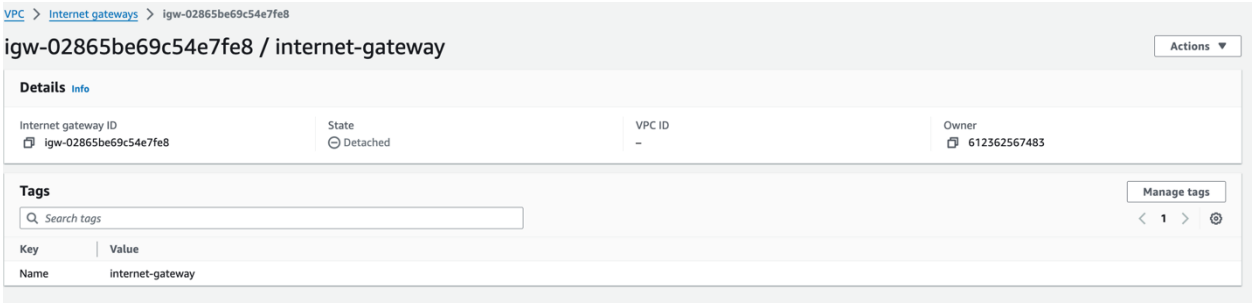


2.3. Setup Internet Gateway

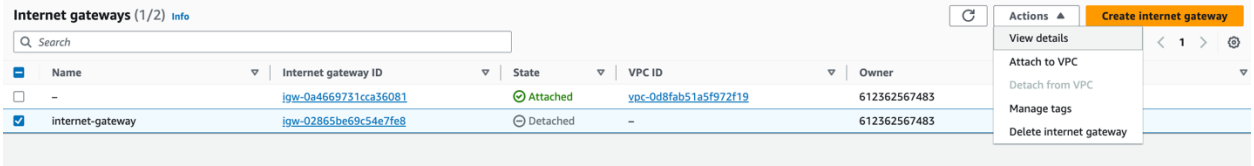
Step-1: Navigate to “Internet gateways” and select “Create internet gateway”.

Step-2: Assign gateway name and then create

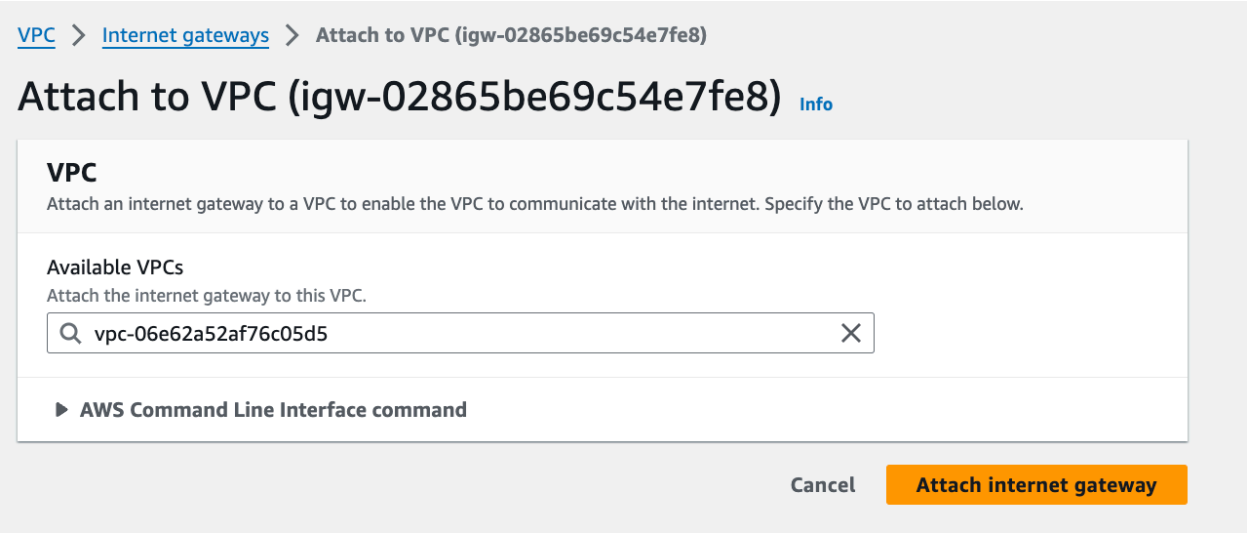


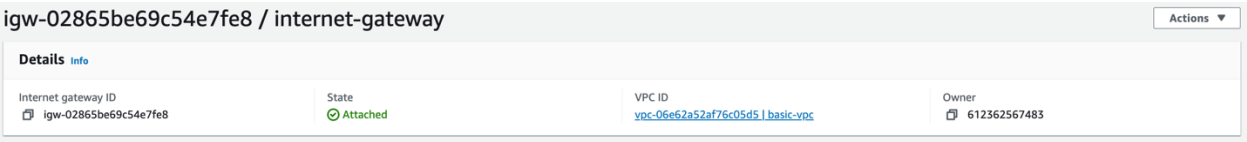


Step-3: Attach the gateway to vpc by selecting created internet gateway. Click on actions and then select “Attach VPC”. This navigates to “Attach to VPC” page.

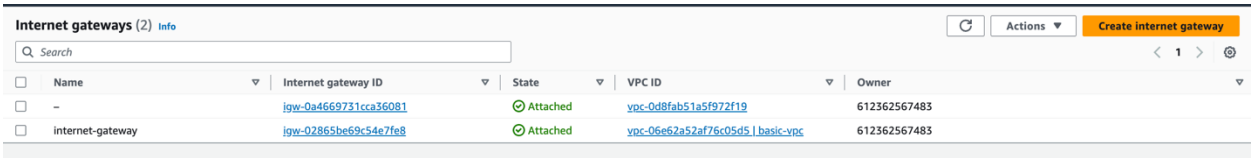


Step-4: Select the created VPC and then click “Attach internet gateway”





Now, the newly created VPC state status is attached

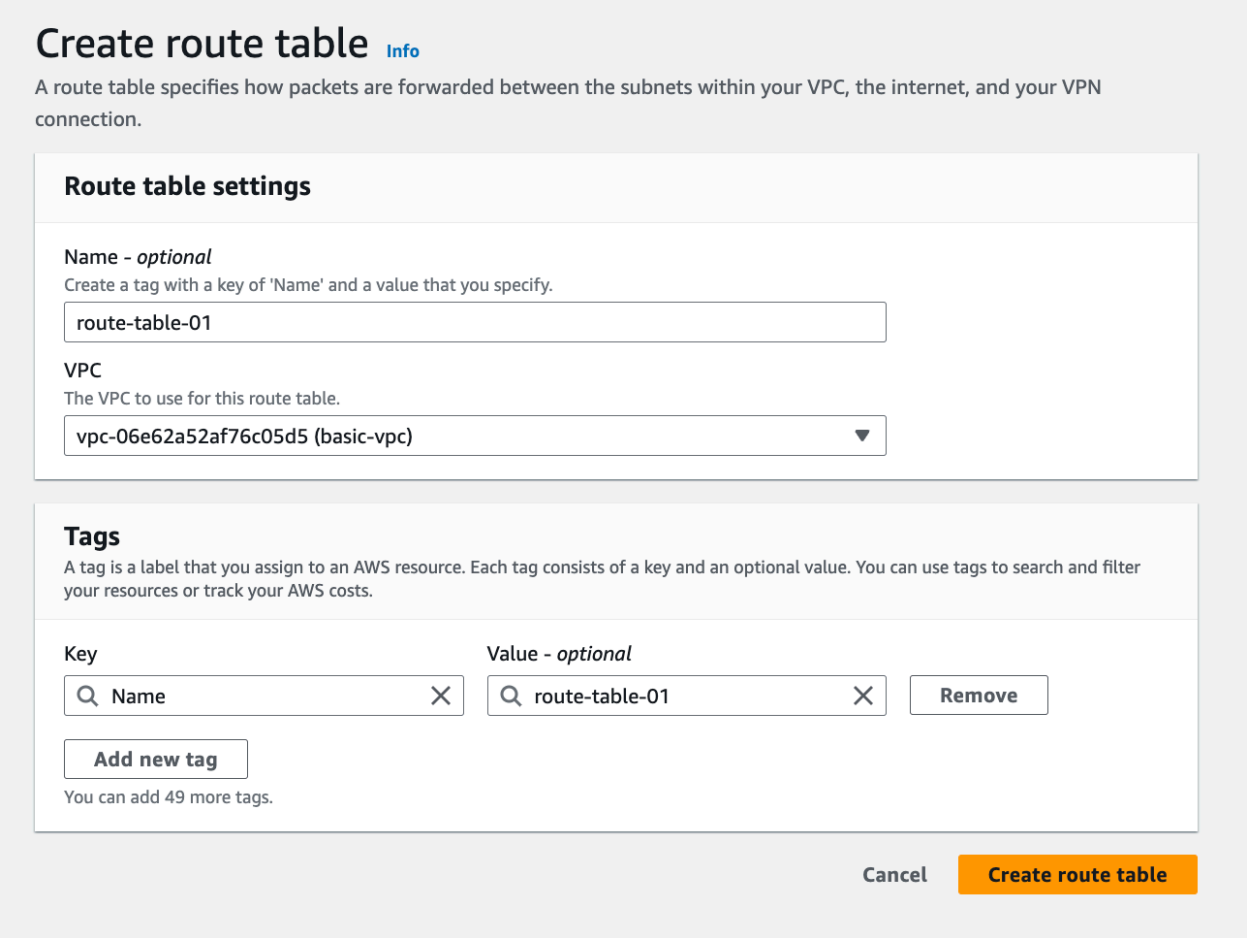


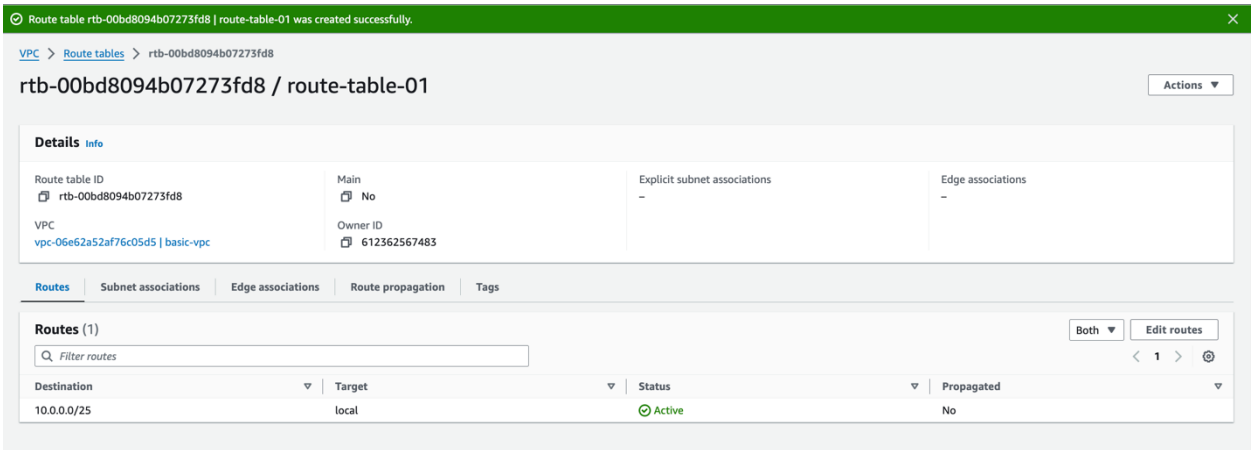
2.4. Configure route table

Navigate to “Route Tables” and click “Create route table” to create a new route table. This navigates to “Create route table” page.

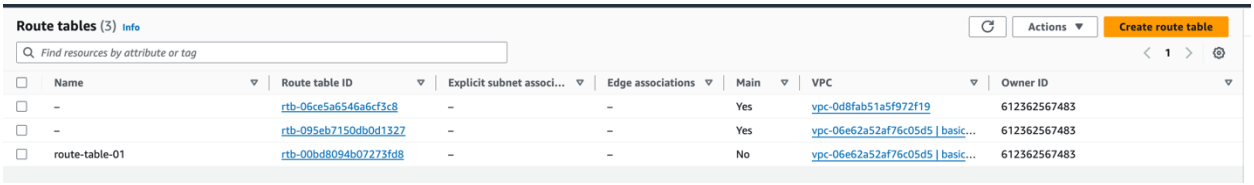
Step-1: Assign route table name

Step-2: Select VPC



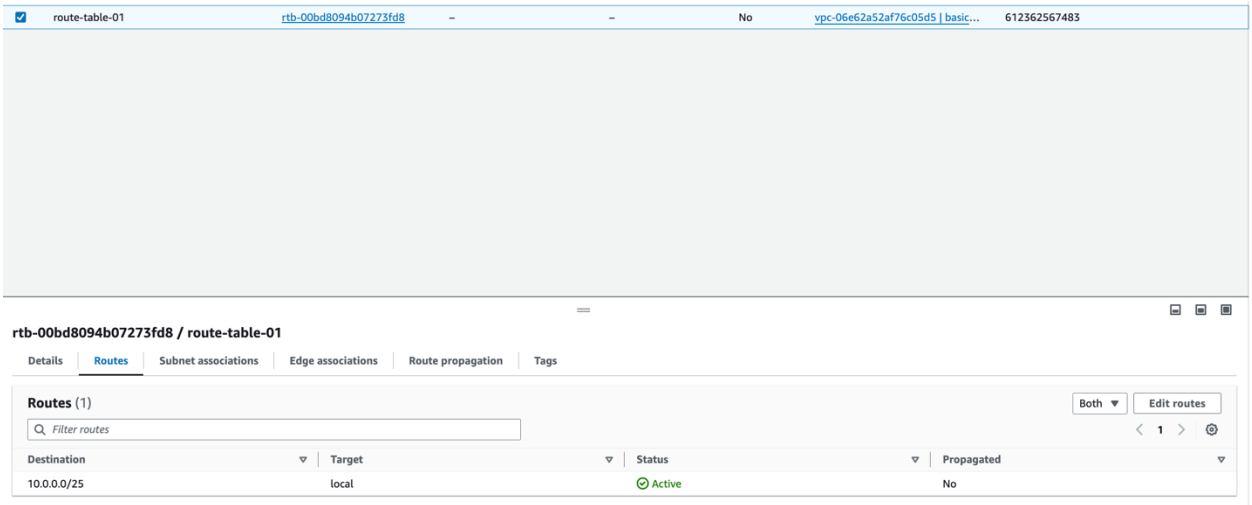


Now, the route table is created.



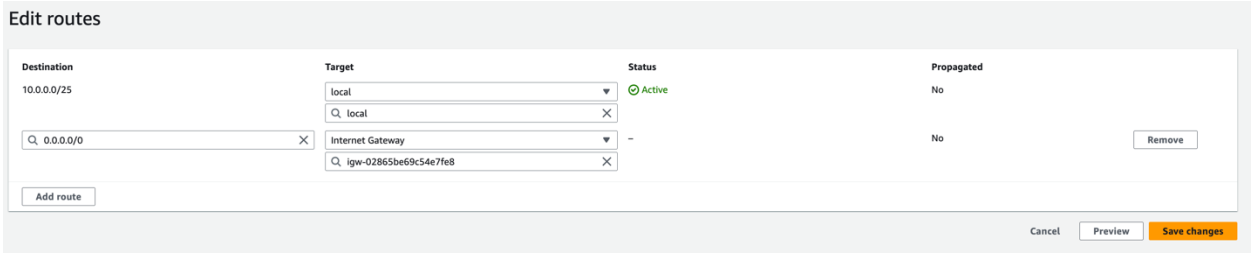
2.5. Attaching internet gateway to the route table

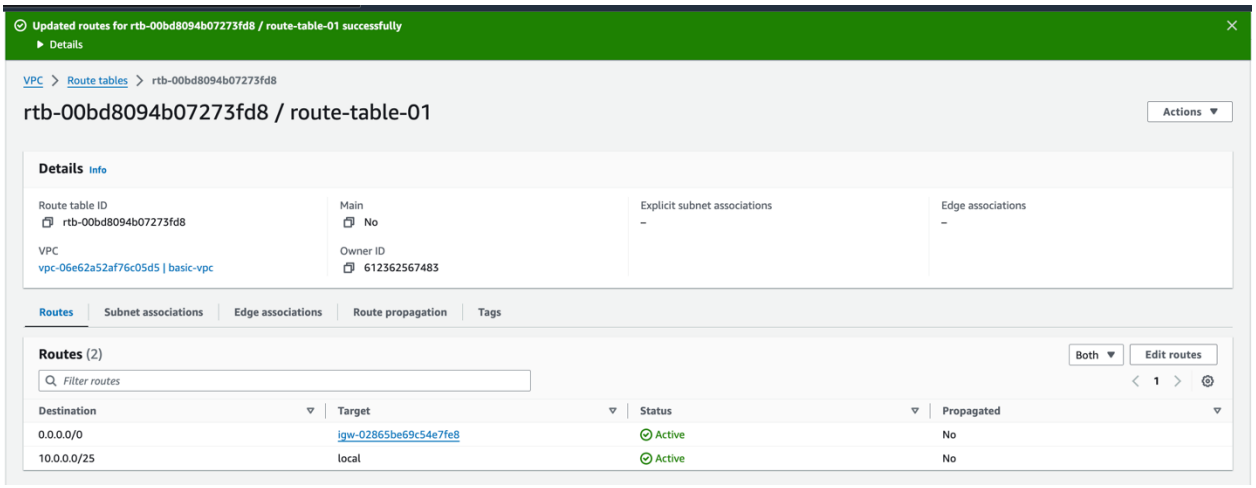
Step-1: Select the route table and click edit routes



Step-2: Configure the edit route form

Select Internet Gateway and then newly created internet gateway

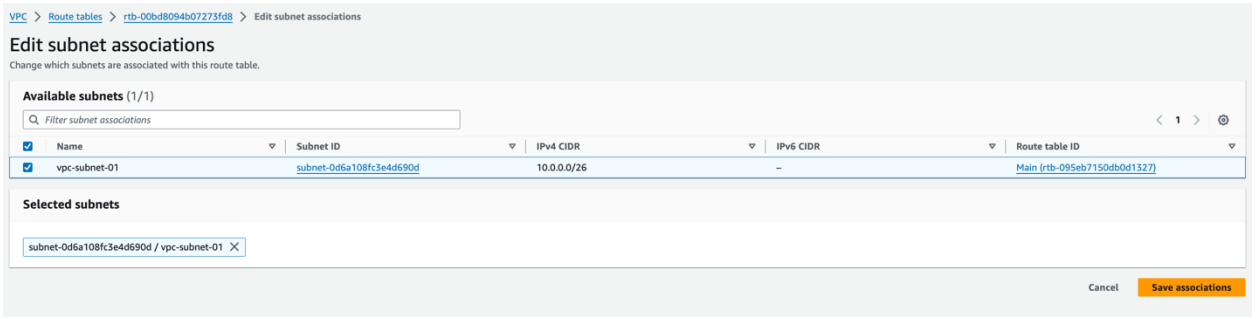




2.6. Subnet associations

Step-1: Navigate to “Subnet associations” tab

Step-2: Select the created subnet and save the associations



2.7. Setting up a simple EC2 instance

Create a new EC2 instance and in network setting select the creted VPC and subnet and set “Auto-assign public IP” as enable. Create new ssh group

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

vpc-ec2-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

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

Network settings Info

VPC - *required* Info

vpc-06e62a52af76c05d5 (basic-vpc)
10.0.0.0/25

Subnet Info

subnet-0d6a108fc3e4d690d vpc-subnet-01
VPC: vpc-06e62a52af76c05d5 Owner: 612362567483 Availability Zone: us-east-1a
IP addresses available: 59 CIDR: 10.0.0.0/26)

Create new subnet

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

Security group name - *required*

new-ssh-group

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

security group

Inbound Security Group Rules

Security group rule 1 (TCP, 22, 0.0.0.0/0) Remove

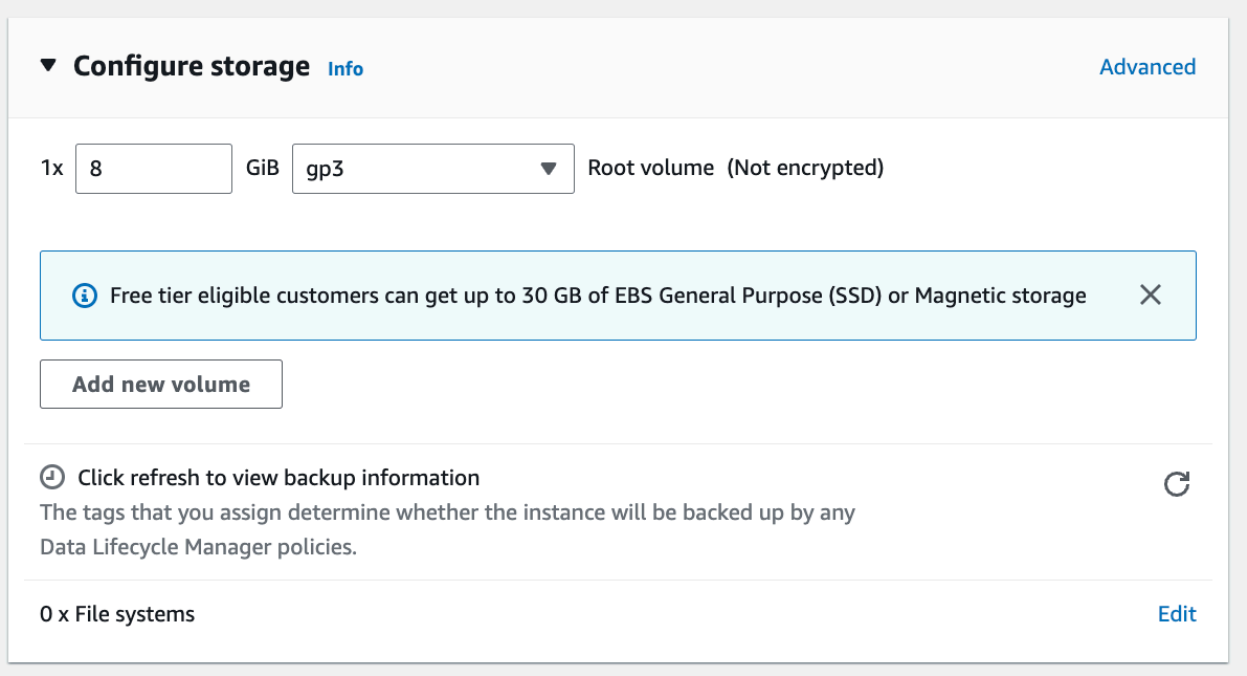
Type Info	Protocol Info	Port range Info
ssh	TCP	22

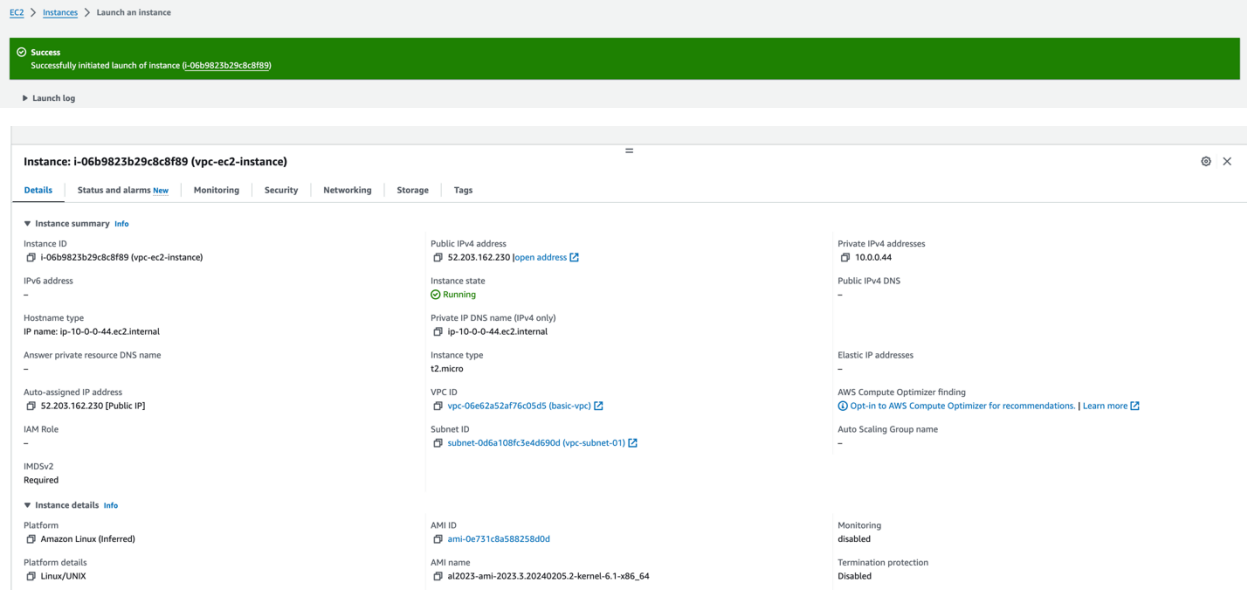
Source type Info	Source Info	Description - *optional* Info
Anywhere	Add CIDR, prefix list or security	e.g. SSH for admin desktop
	0.0.0.0/0	

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Add security group rule

▶ Advanced network configuration


Configure storage Info
Advanced
1x
8
GiB
gp3
Root volume (Not encrypted)
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage
Add new volume
Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.
0 x File systems
Edit


EC2 > Instances > Launch an instance
Success
Successfully initiated launch of instance (i-06b9823b29c8c8f89)
Launch log
Instance: i-06b9823b29c8c8f89 (vpc-ec2-instance)
Details
Status and alarms New
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-06b9823b29c8c8f89 (vpc-ec2-instance)
Public IPv4 address
52.203.162.230 |open address
Private IPv4 addresses
10.0.0.44
IPv6 address
–
Instance state
Running
Public IPv4 DNS
–
Hostname type
IP name: ip-10-0-0-44.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-0-0-44.ec2.internal
Answer private resource DNS name
–
Instance type
t2.micro
Elastic IP addresses
–
Auto-assigned IP address
52.203.162.230 [Public IP]
VPC ID
vpc-06e62a52af76c05d5 (basic-vpc)
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more
IAM Role
–
Subnet ID
subnet-0d6a108fc3e4d690d (vpc-subnet-01)
Auto Scaling Group name
–
IMDSv2
Required
Instance details Info
Platform
Amazon Linux (Inferred)
AMI ID
ami-0e731c8a588258d0d
Monitoring
disabled
Platform details
Linux/UNIX
AMI name
al2023-ami-2023.3.20240205.2-kernel-6.1-x86_64
Termination protection
Disabled

```
utsha_mac@Utshas-MacBook-Pro Downloads % chmod 400 "key-pair.pem"
utsha_mac@Utshas-MacBook-Pro Downloads % ssh -i "key-pair.pem" ec2-user@52.203.162.230
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
```

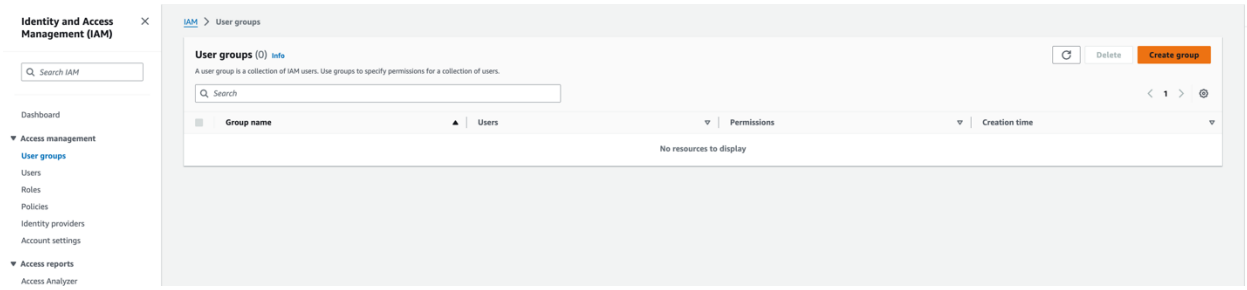
3. IAM Users and Roles Lab

- **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.

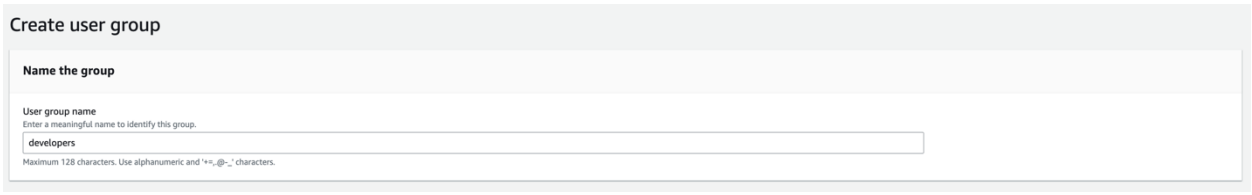
3.1. Create new IAM user group

Step-1: Search from IAM in and navigate to IAM dashboard

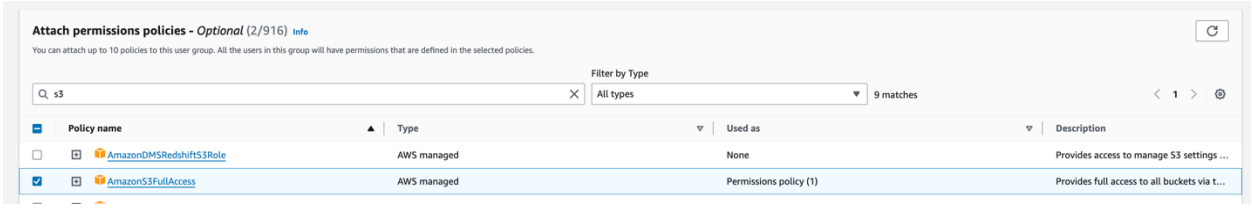
Step-2: From left navigation bar select “User group”

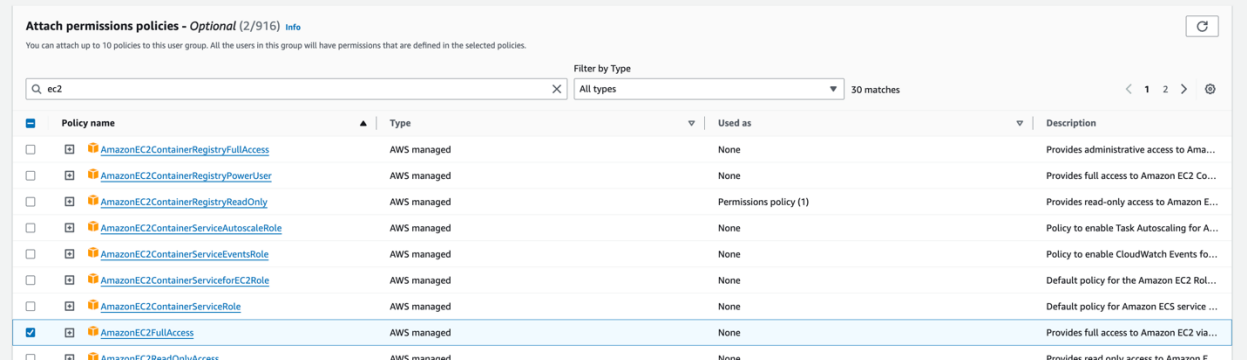


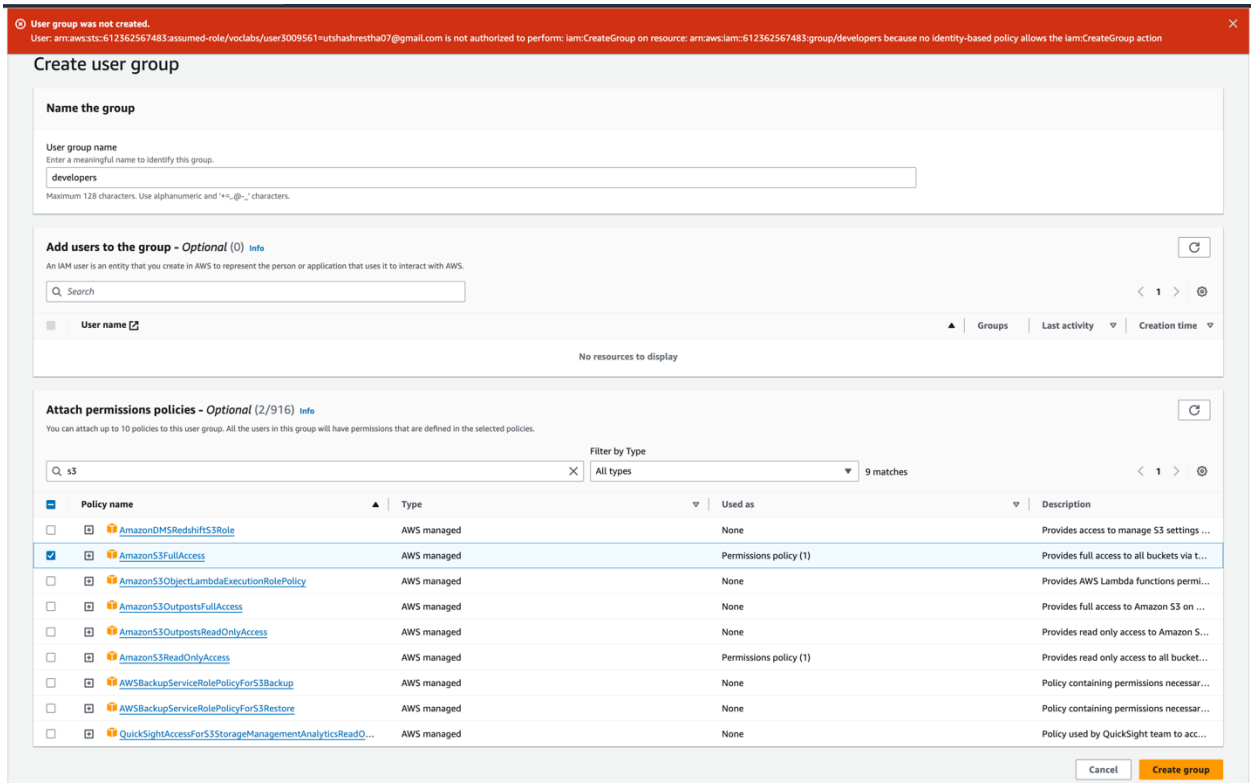
Step-3: Select “Create group” and provide required configuration



Step-4: Apply policies to manage permission. Here, “AmazonS3FullAccess” and “AmazonEc2FullAccess” policies is attached.





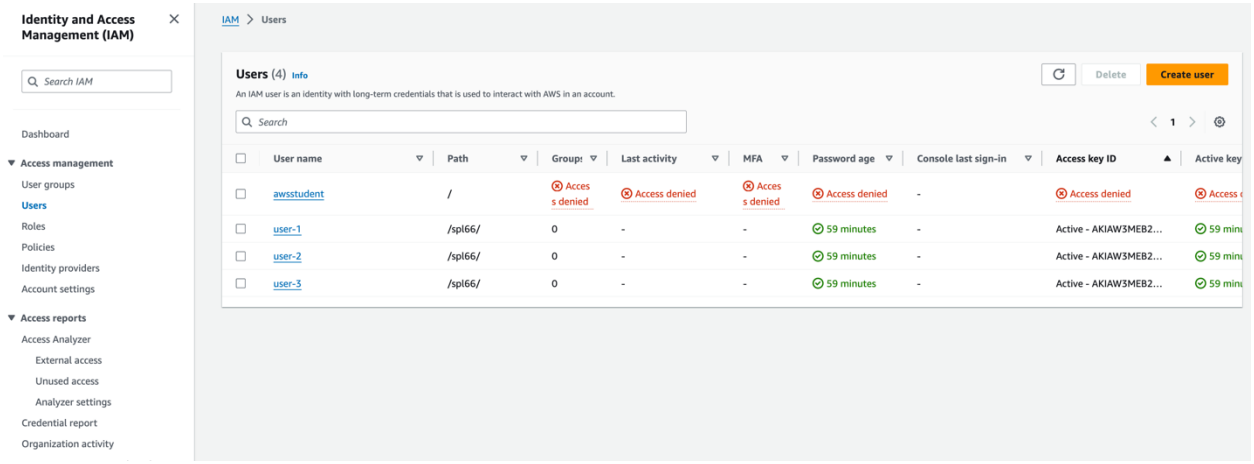


As we have not access to create group in provided lab “AWS learner Lab” above error message is displayed.

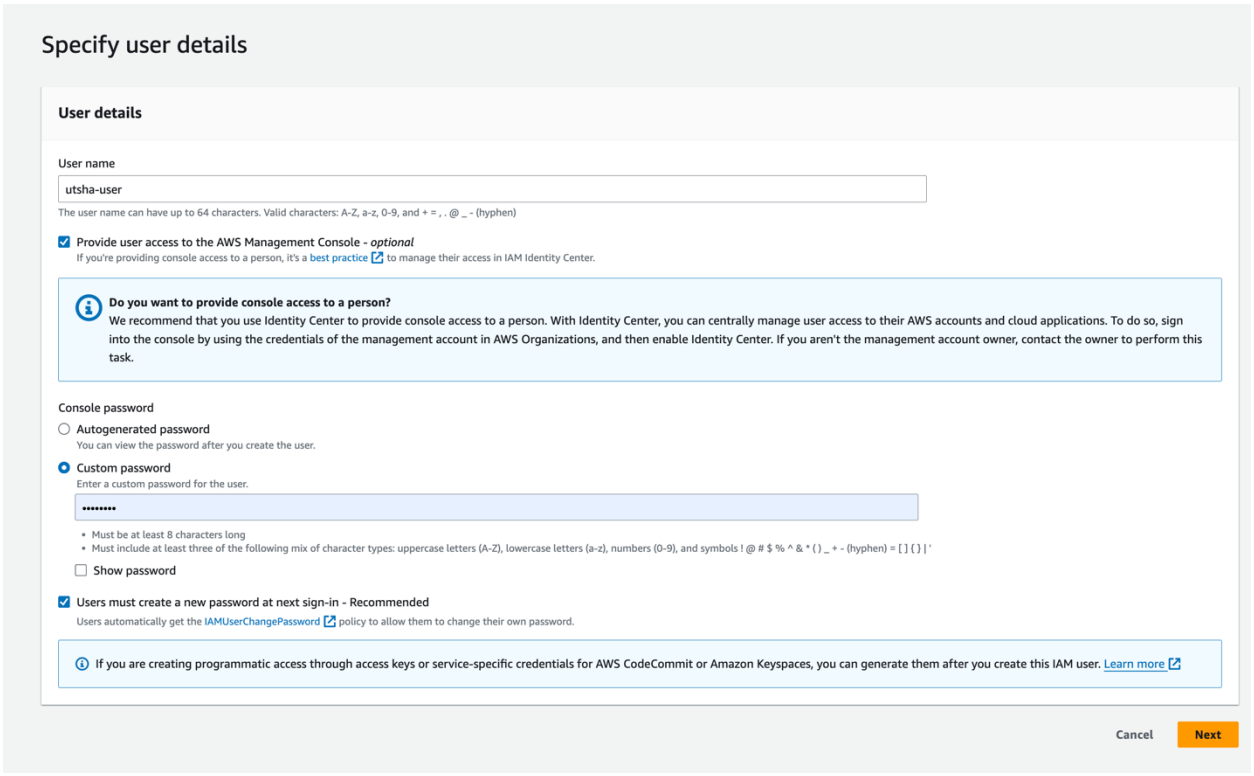
3.2. Create new user

This part is implemented in “AWS Cloud Foundations” Lab and the steps involved for this is listed below.

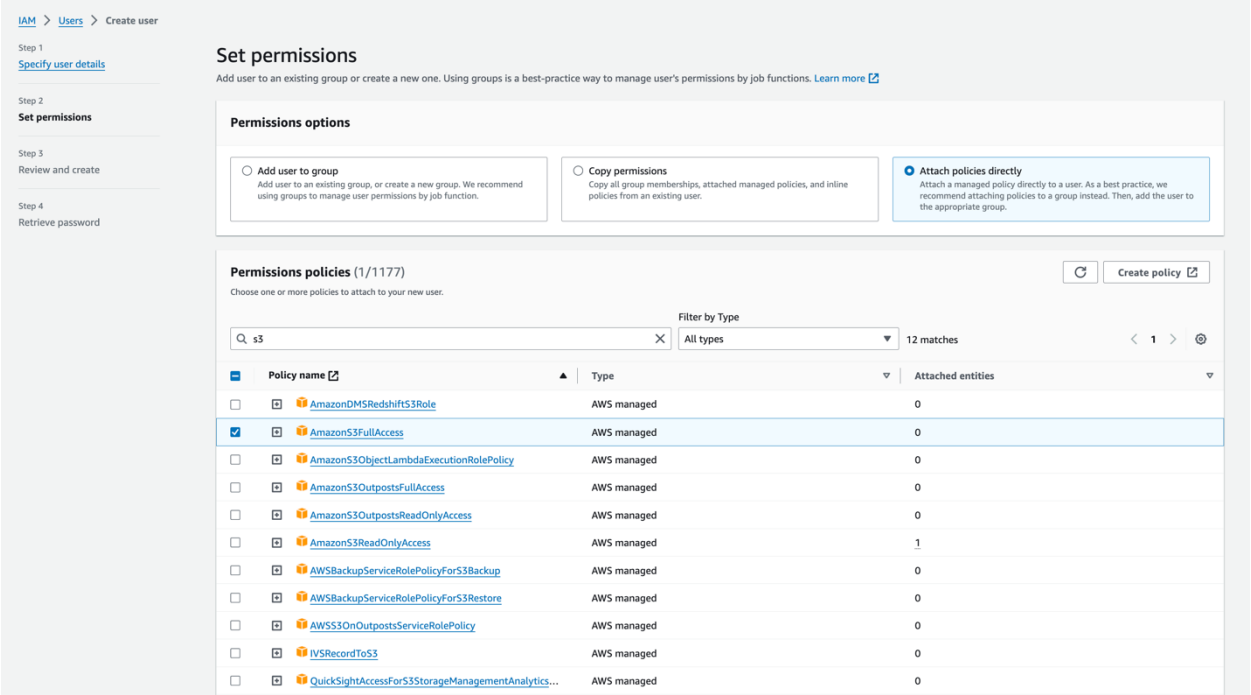
Step-1: Navigate to IAM dashboard

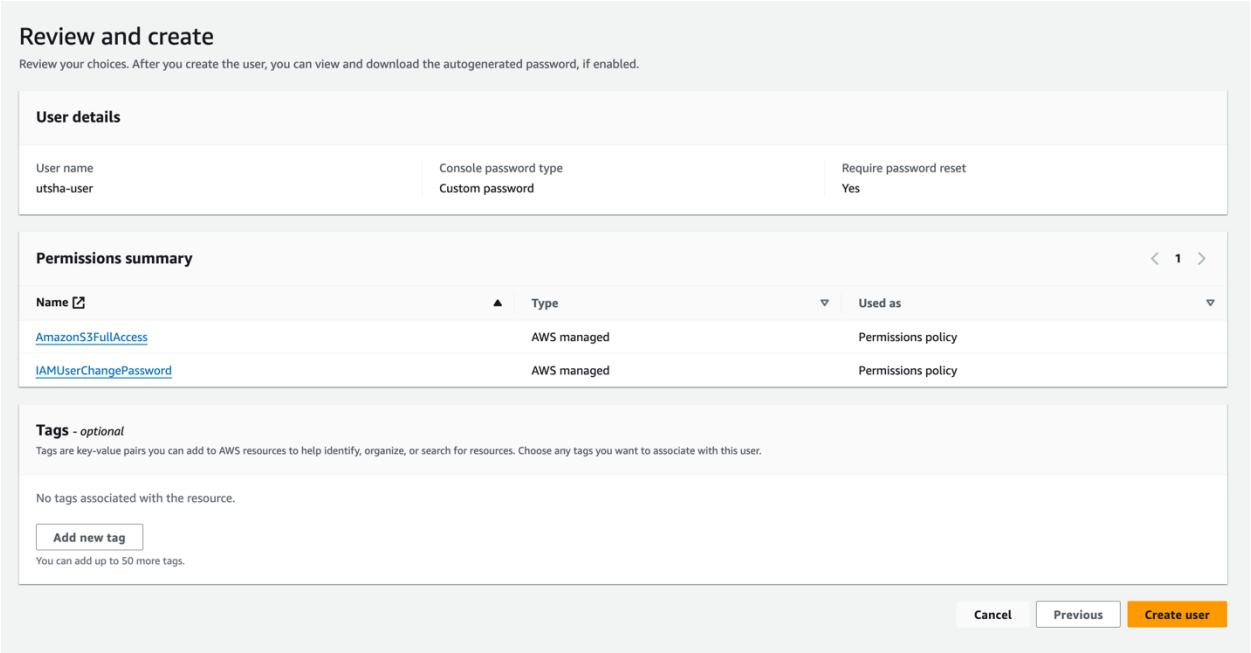


Step-2: Click create user and then this will navigate to create user page. Required configuration is provided.



Step-3: After that, select attach policies directly and give permission to the newly created user.





In this way new user can be created.