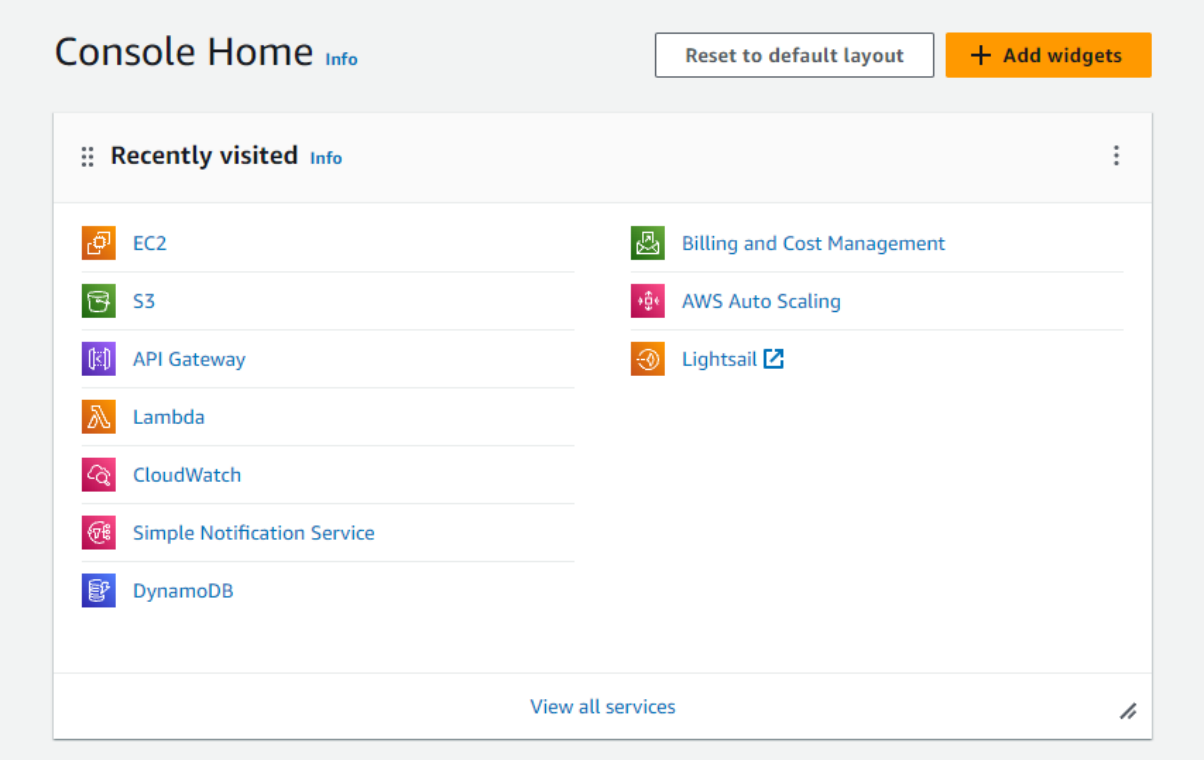
Basic Labs

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.
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.
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.

EC2 Basics Lab

Go to EC2 from AWS CONSOLE



Name and tags Info

Name

new-workshop

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 Linu

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)

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

Description

Amazon Linux 2023 AMI 2023.3.20240219.0 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	
64-bit (x86)	uefi-preferred	ami-0440d3b780d96b29d	Verified provider

Key pair (login) Info

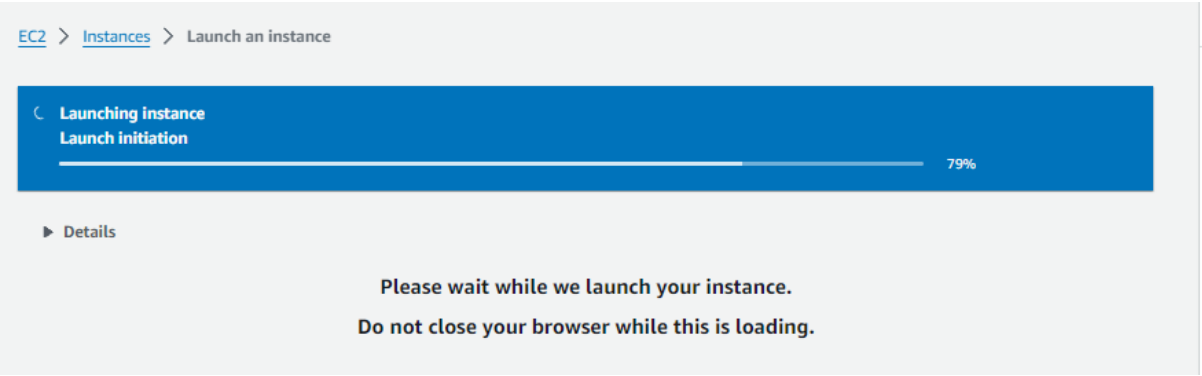
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

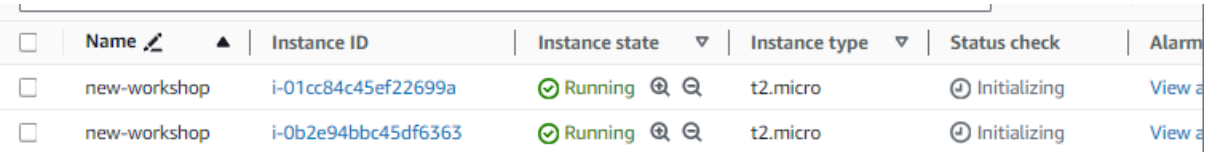
Test

Create new key pair

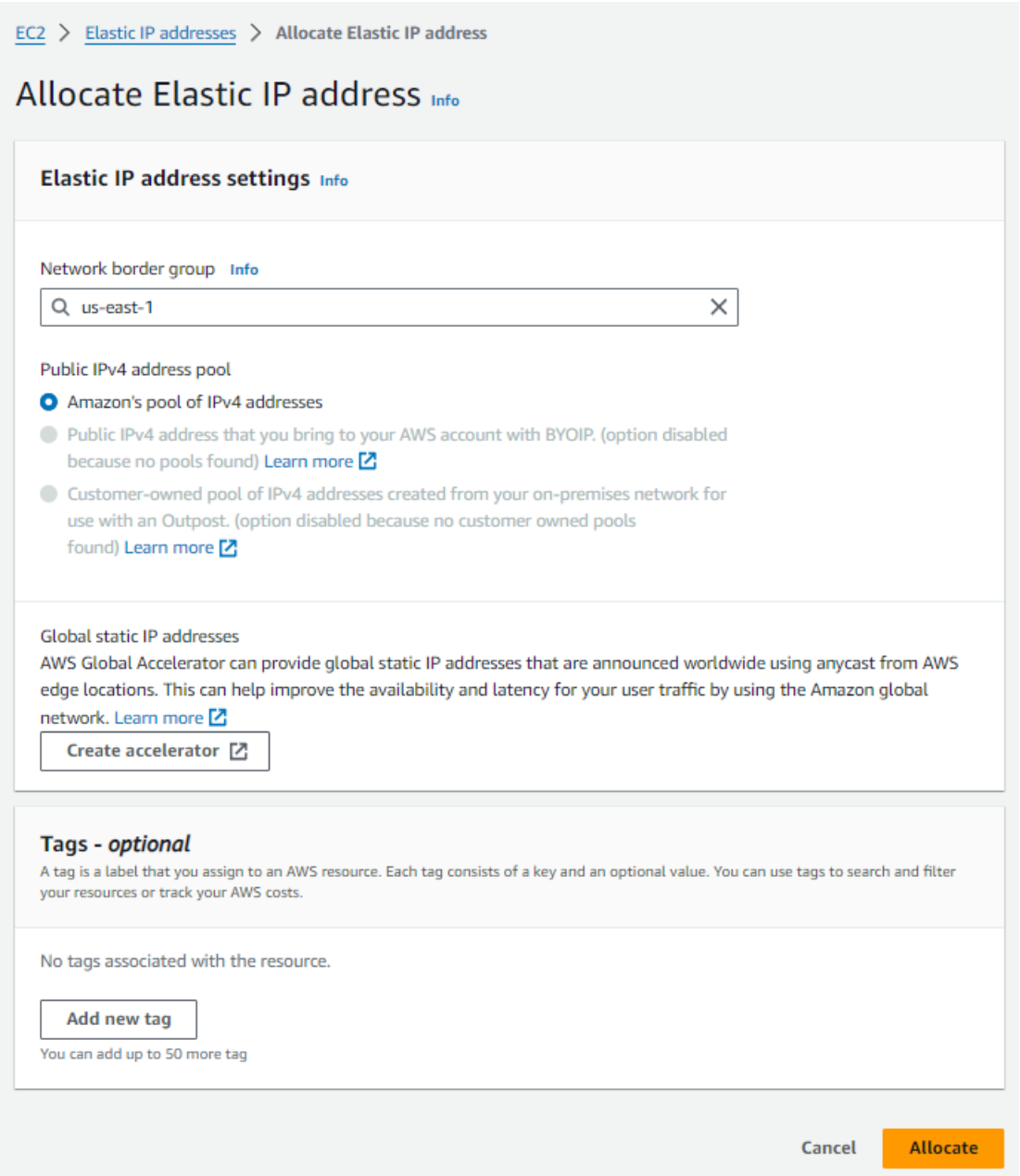
Create and launch Ec2 Instance

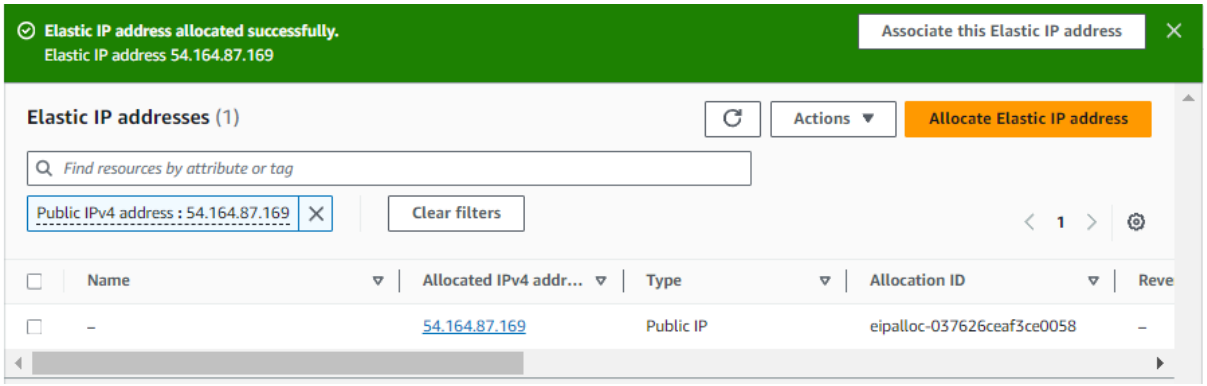


Click on Instances you can find the new created instances



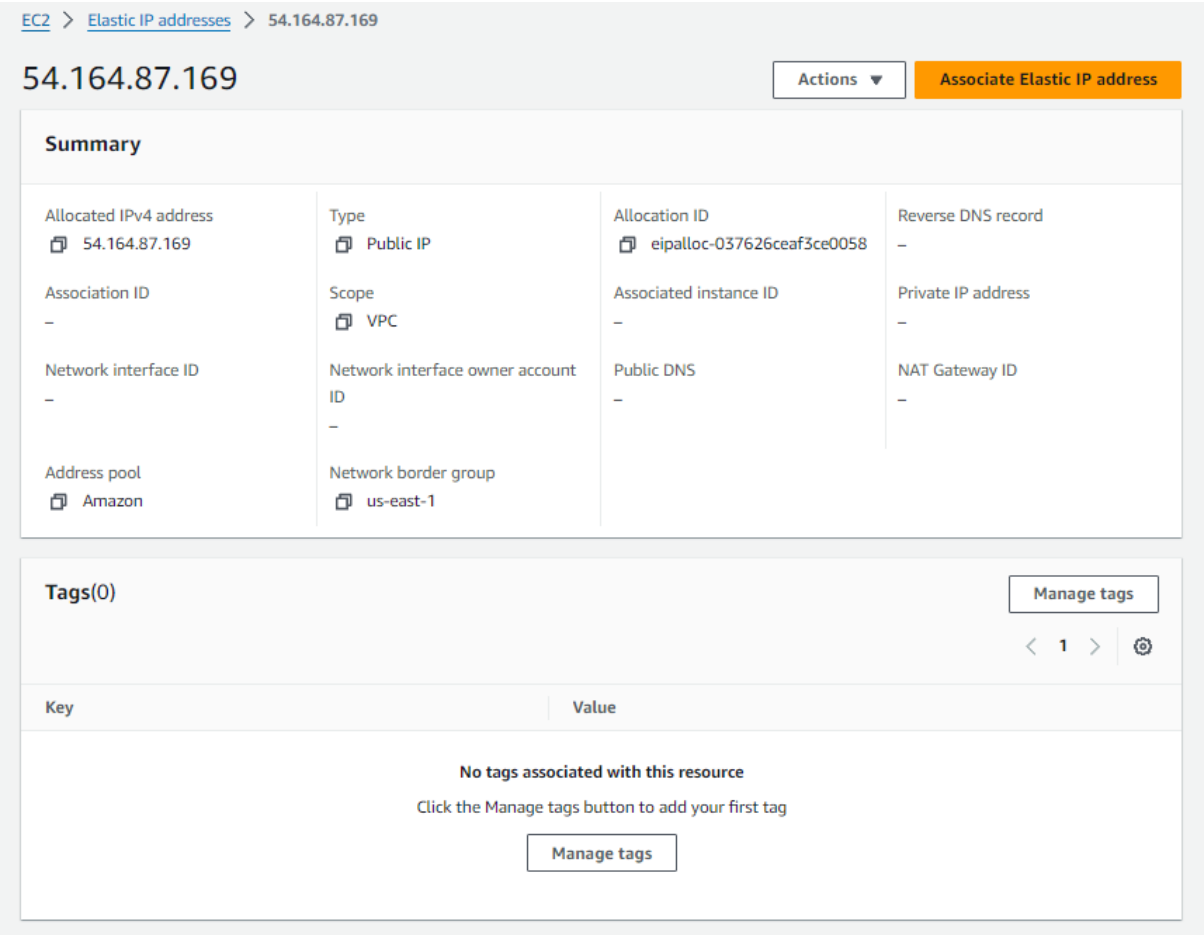
Now allocate an Elasic IP address to this instance





So that Elastic IP address has been allocated

Open the created IP Address.



Click on Associate Elasic IP Address

Associate Elastic IP address

Choose the instance or network interface to associate to this Elastic IP address (54.164.87.169)

Elastic IP address: 54.164.87.169

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

🔍 *Choose an instance* [↻]

Private IP address

The private IP address with which to associate the Elastic IP address.

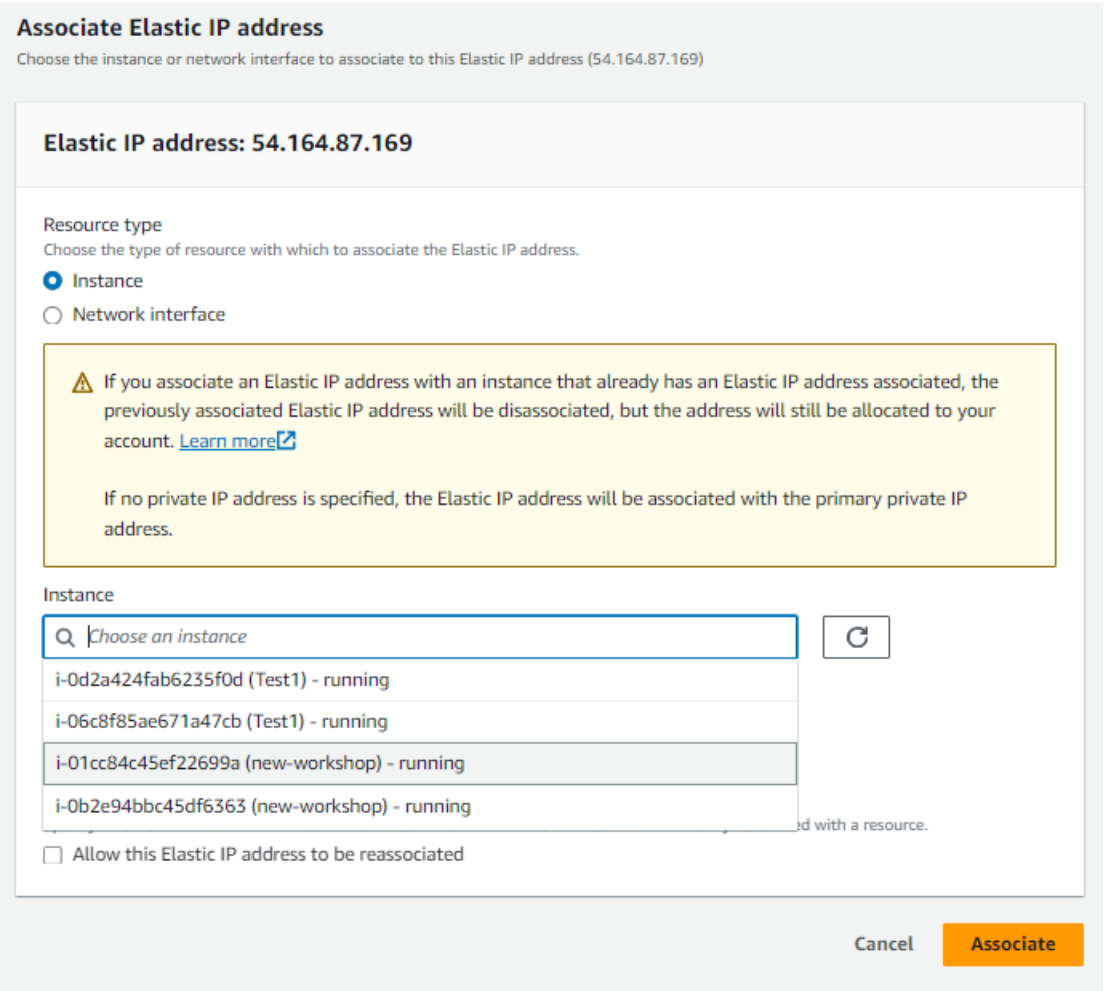
🔍 *Choose a private IP address*

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**



Now choose the Instance that we created previously .

EC2 > Elastic IP addresses > 54.164.87.169 > Associate Elastic IP address

Associate Elastic IP address

Choose the instance or network interface to associate to this Elastic IP address (54.164.87.169)

Elastic IP address: 54.164.87.169

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-01cc84c45ef22699a

Private IP address

The private IP address with which to associate the Elastic IP address.

172.31.17.17

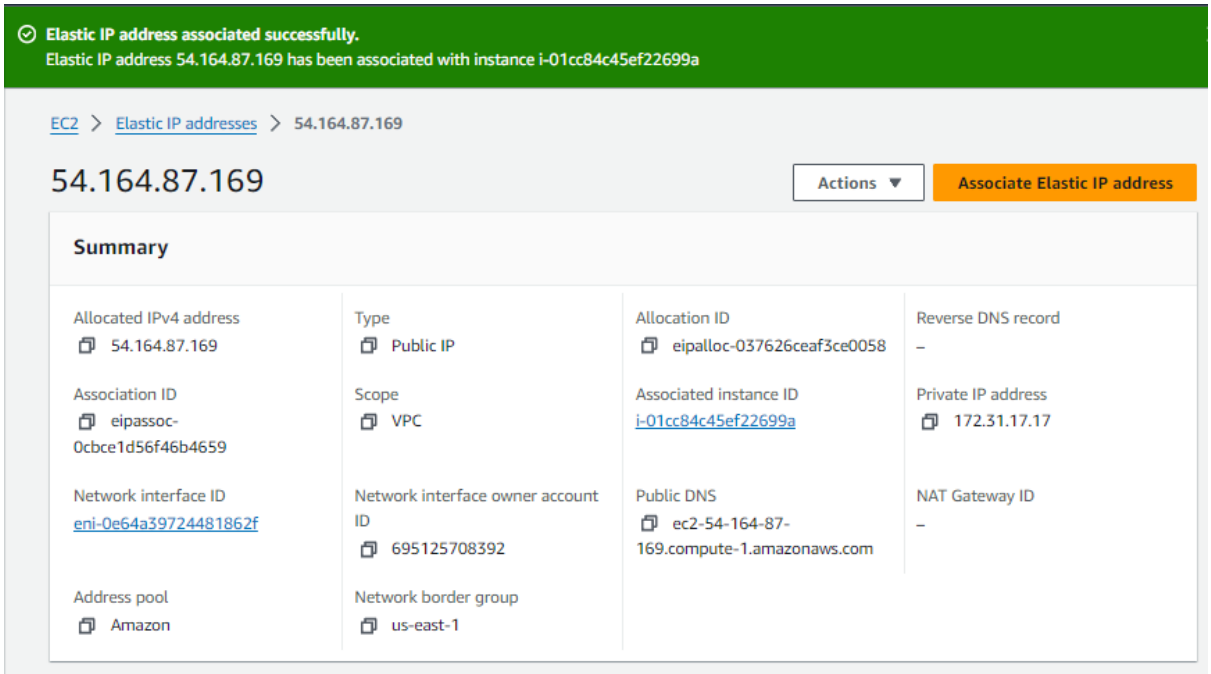
Reassociation

Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.

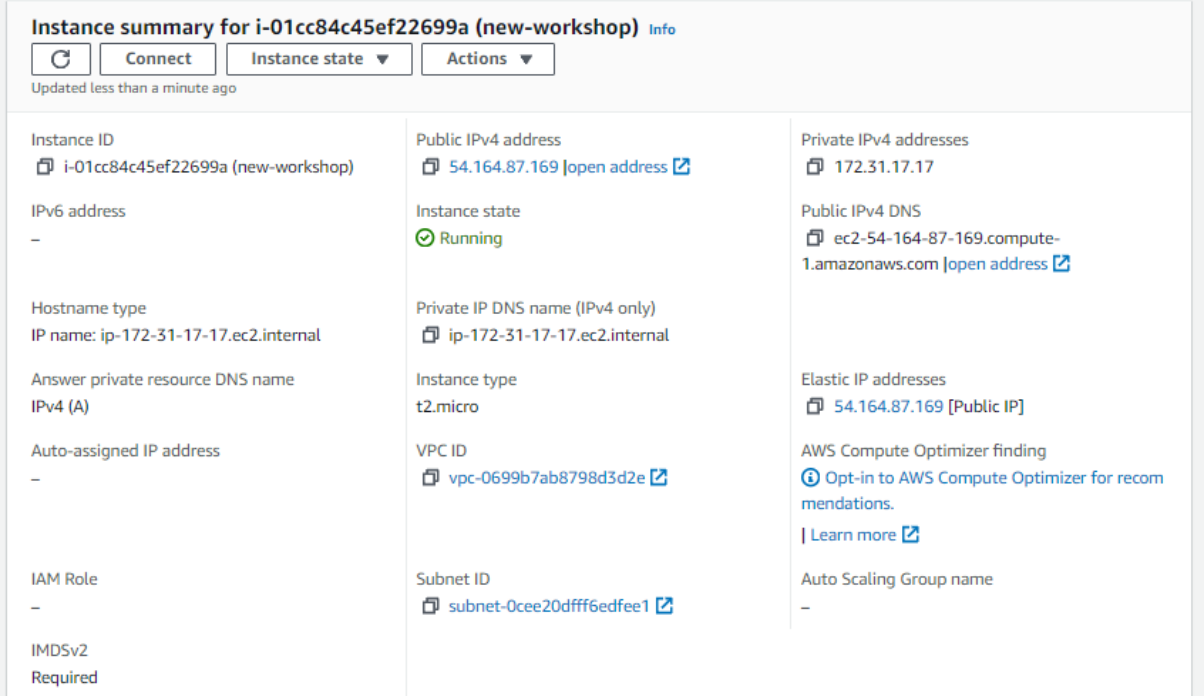
[ ] Allow this Elastic IP address to be reassociated

Cancel | Associate

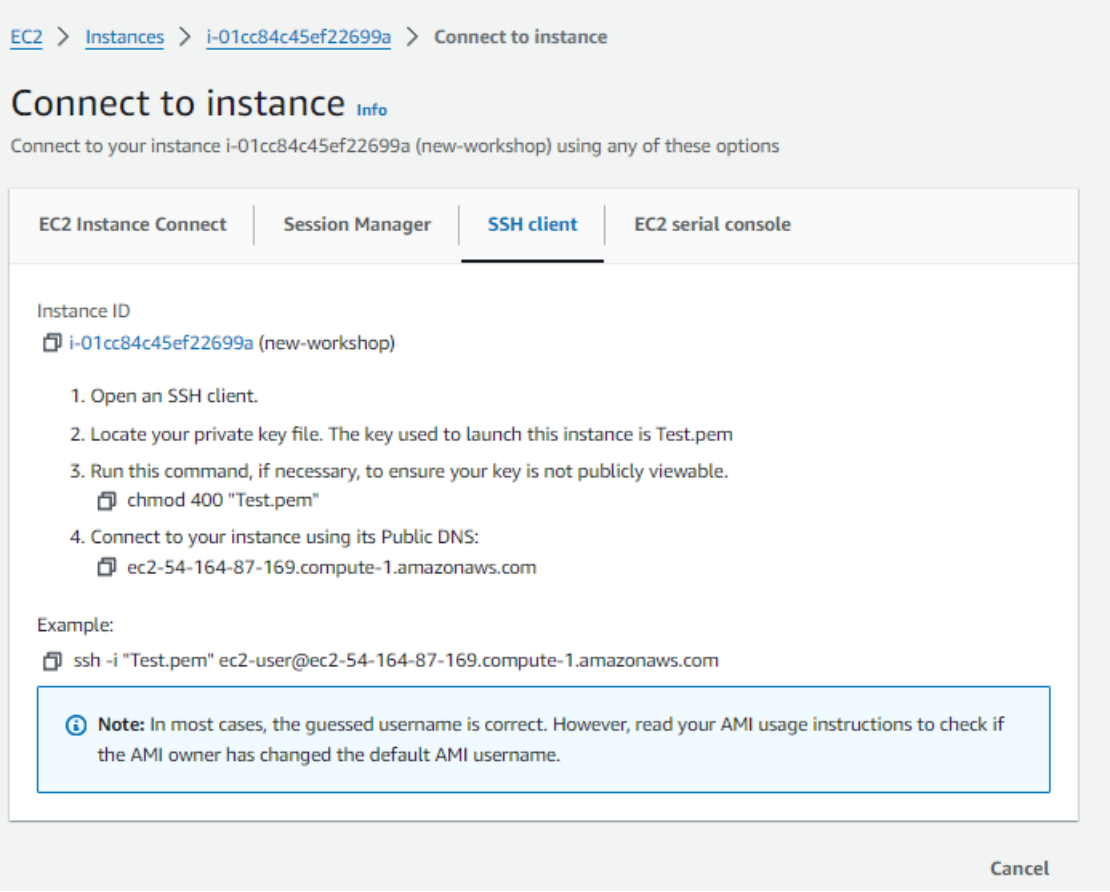
Now click on assosciate button after assigning private IP address



Now Elascitc IP is finally showing in our EC2 Instance



Now we have to connect the instance via SSH

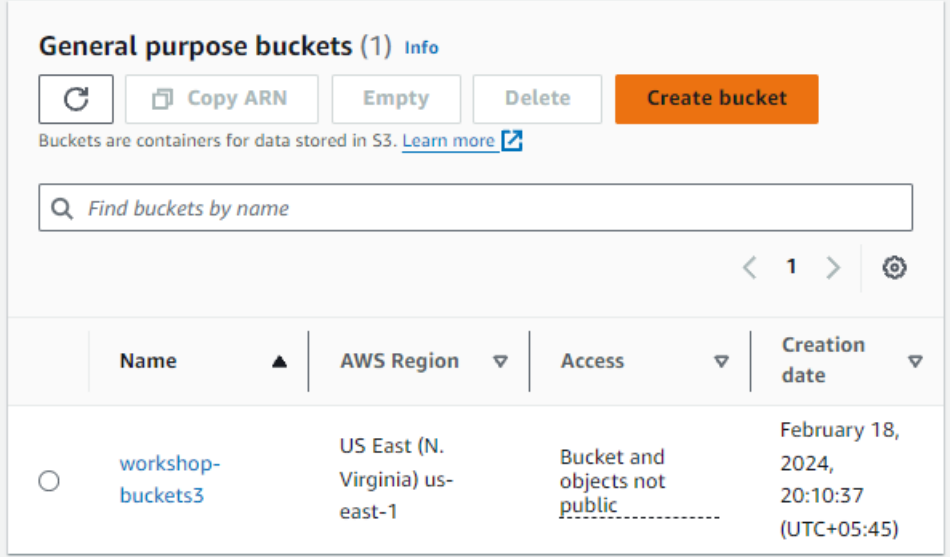


```
ec2-user@ip-172-31-17-17:~
Microsoft Windows [Version 10.0.22000.2777]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User\Downloads>chmod 400 "Test.pem"
'chmod' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\User\Downloads>ssh -i "Test.pem" ec2-user@54.164.87.169
The authenticity of host '54.164.87.169 (54.164.87.169)' can't be established.
ECDSA key fingerprint is SHA256:zTzvLcy/tpvaaPV2GWh0JVKpYxvhiMxgKkti3ETeG8Y.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '54.164.87.169' (ECDSA) to the list of known hosts.
       ,     #_
       ~\_  ####_        Amazon Linux 2023
      ~~  \_#####\
      ~~     \###|
      ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
       ~~       V~' '->
        ~~~         /
          ~~._.   _/
             _/ _/
           _/m/'
[ec2-user@ip-172-31-17-17 ~]$
```

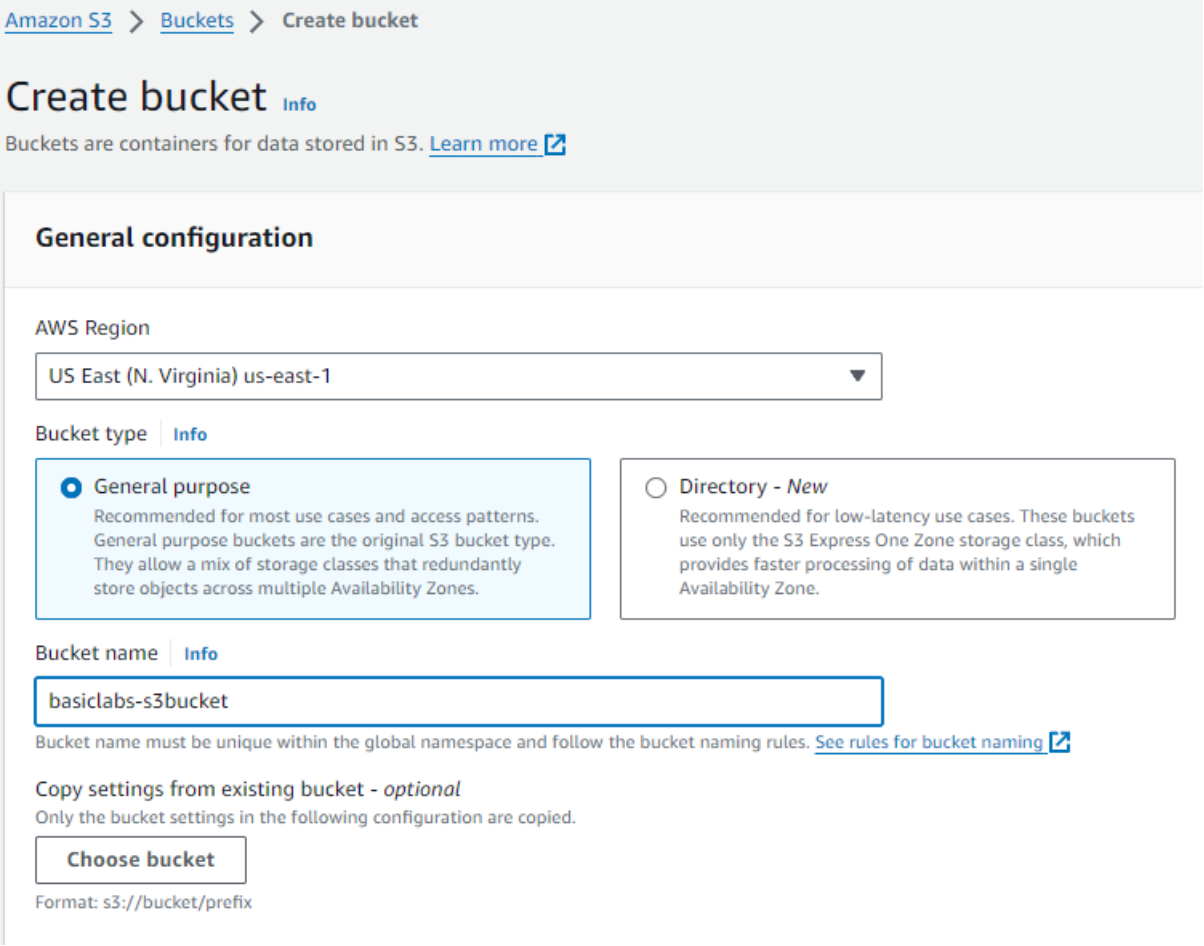
Connection Success of EC2 Instance via SSH Key.

S3 Storage Fundamentals Lab

First Create a S3 Bucket



Click on Create Bucket



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.

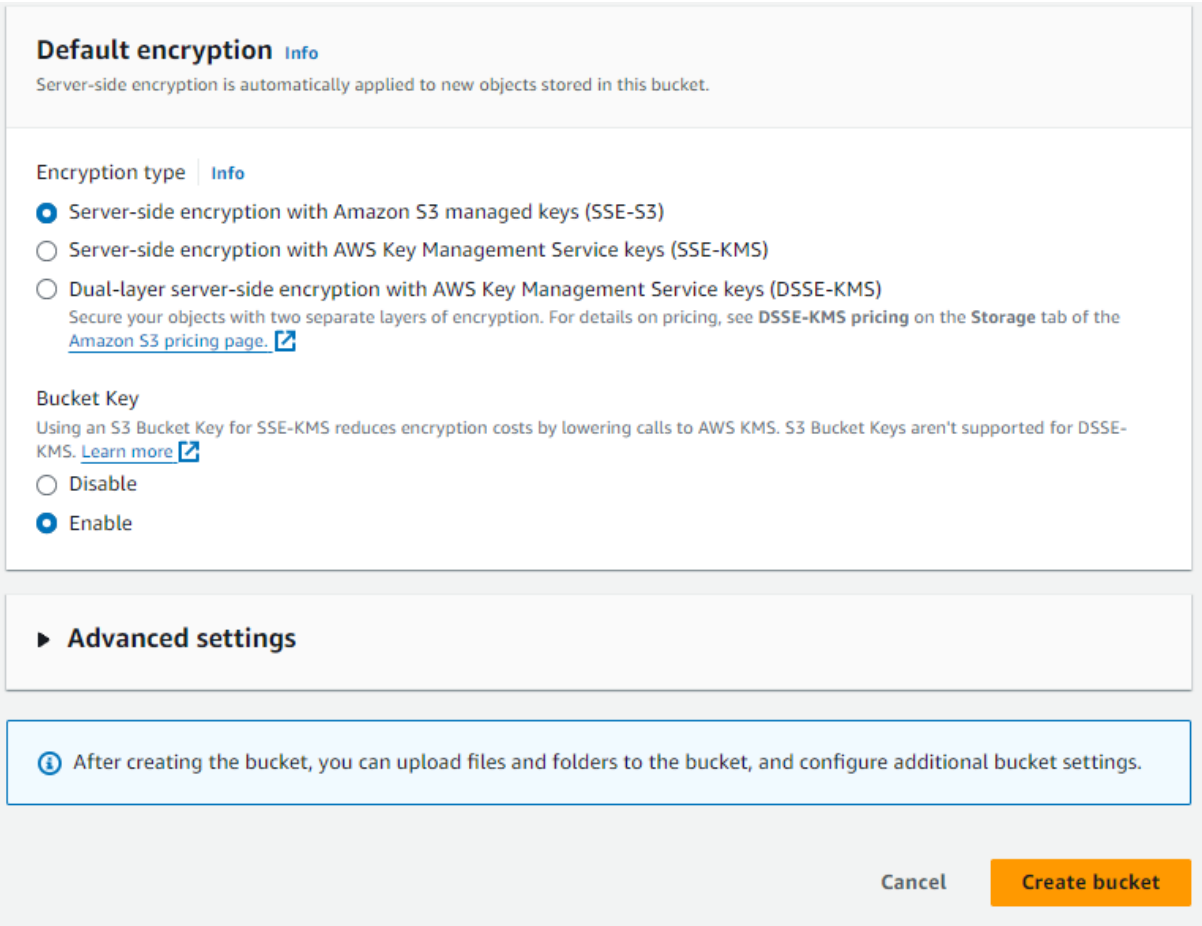
Object Ownership

Bucket owner enforced

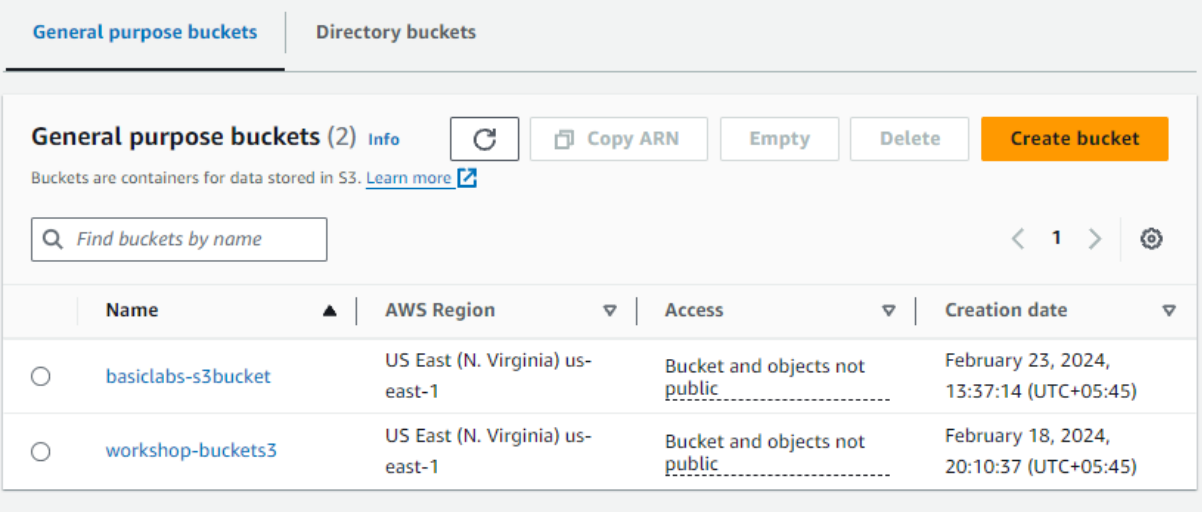
Block Public Access settings for this bucket

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

- [x] **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.
  - [x] **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.
  - [x] **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.
  - [x] **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.
  - [x] **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.



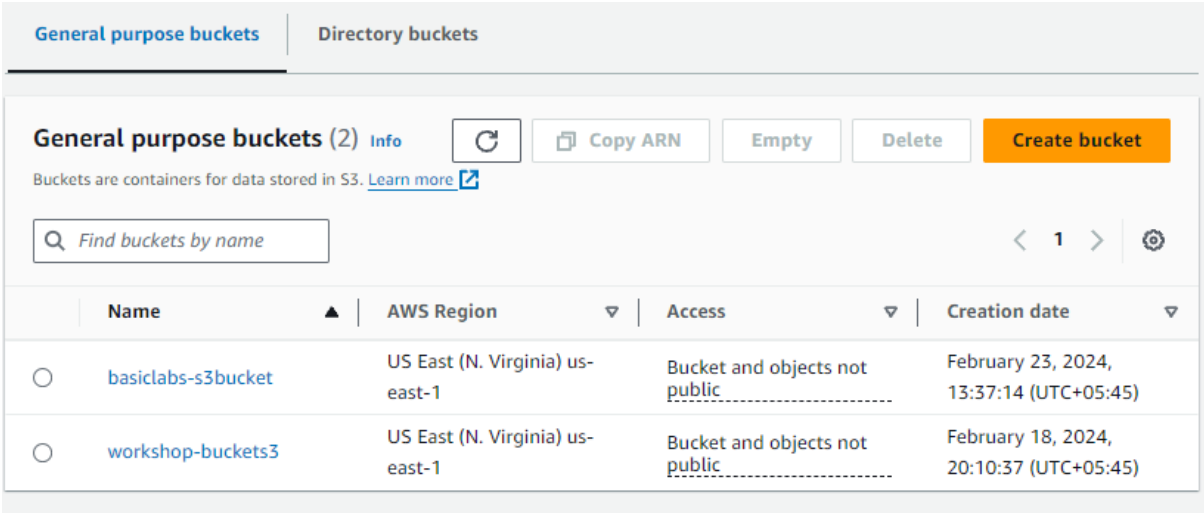
Set bucket name and leave the rest as it is and click on Create Bucket

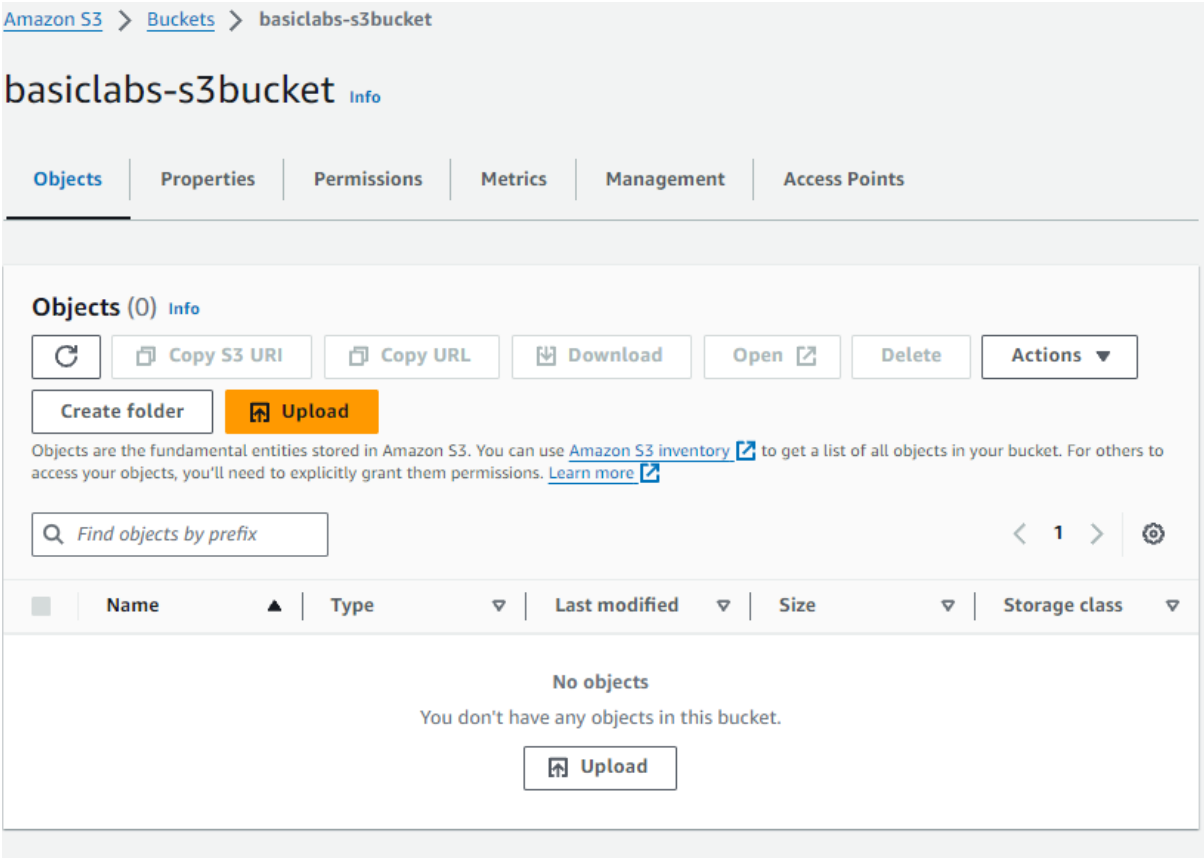


So the New bucket has been created with the name basiclabs-s3bucket

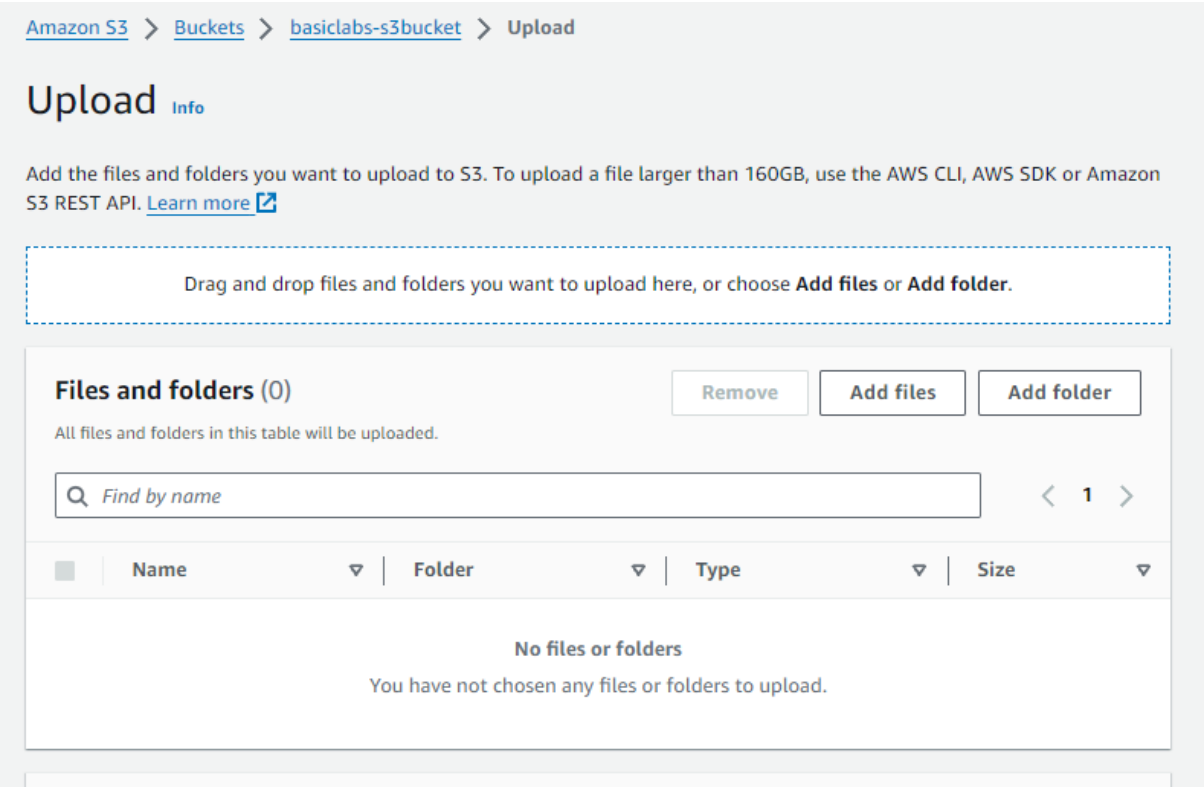
Now the next task will be to Upload files

To upload files click on the new bucket that we just created.

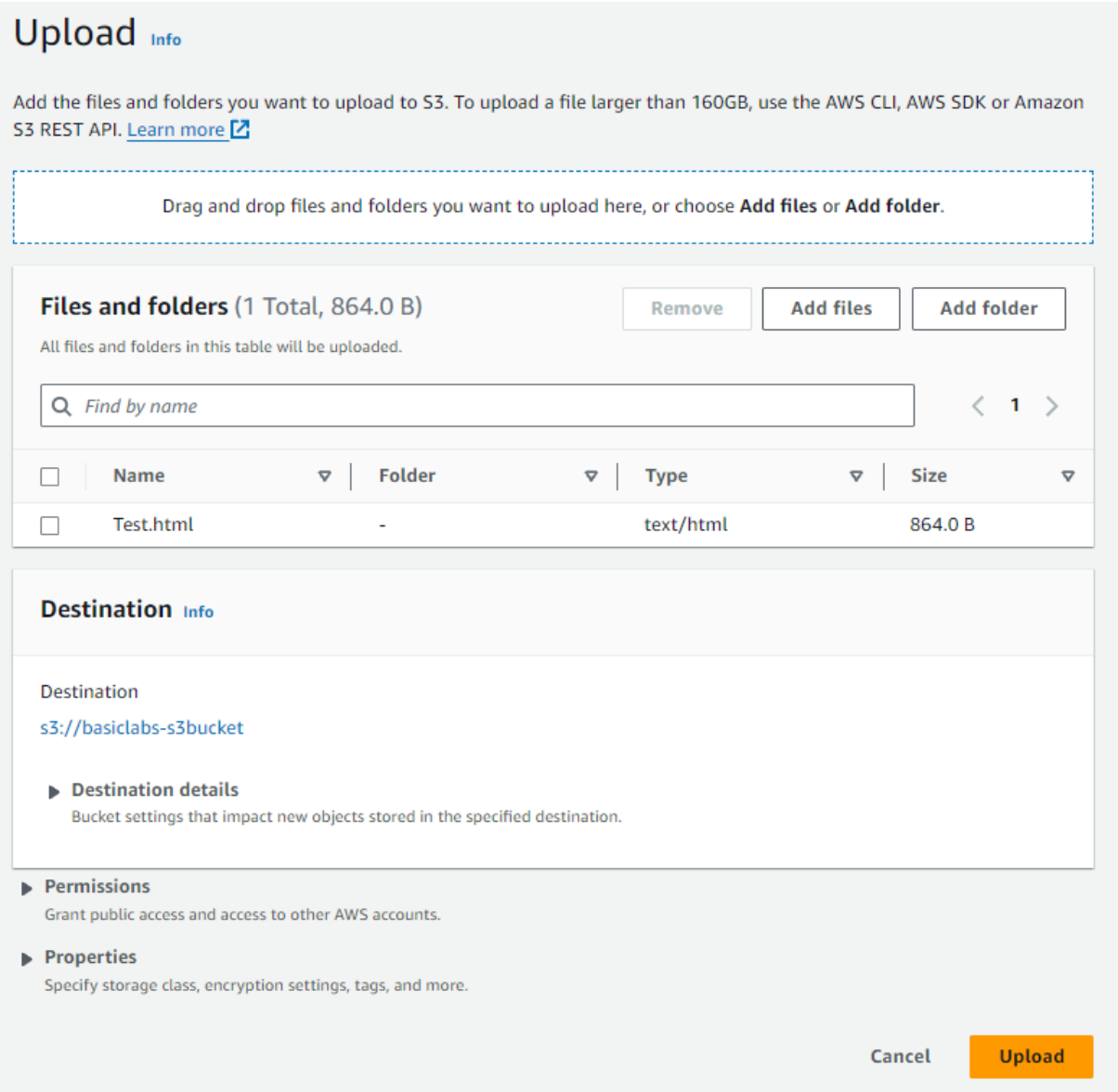




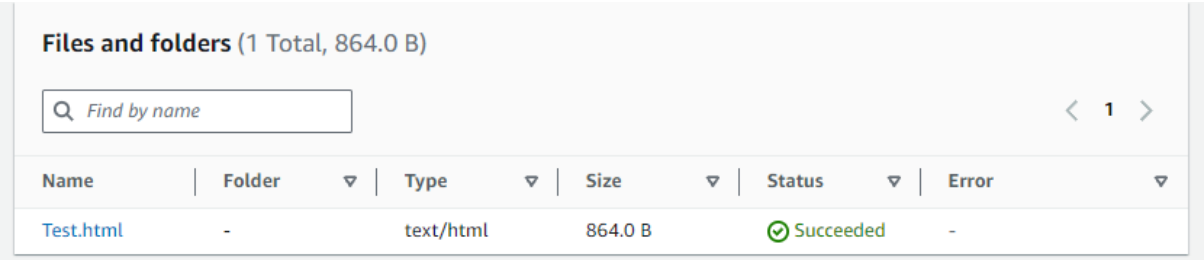
Then click on upload button



Then drag and drop file to be uploaded



Now upload the file .



Detail of the uploaded file can be viewed by clicking on It.

Amazon S3 > Buckets > basiclabs-s3bucket > Test.html

Test.html Info

Copy S3 URI | Download | Open | Object actions

Properties | Permissions | Versions

Object overview

Owner
awslabsc0w6974879t1703160632

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

Last modified
February 23, 2024, 13:52:06 (UTC+05:45)

Size
864.0 B

Type
html

Key
Test.html

S3 URI
s3://basiclabs-s3bucket/Test.html

Amazon Resource Name (ARN)
arn:aws:s3:::basiclabs-s3bucket/Test.html

Entity tag (Etag)
b362130ef50dd00bd226d0a37e4c340f

Object URL
https://basiclabs-s3bucket.s3.amazonaws.com/Test.html

basiclabs-s3buck...

Welcome to My AWS Website

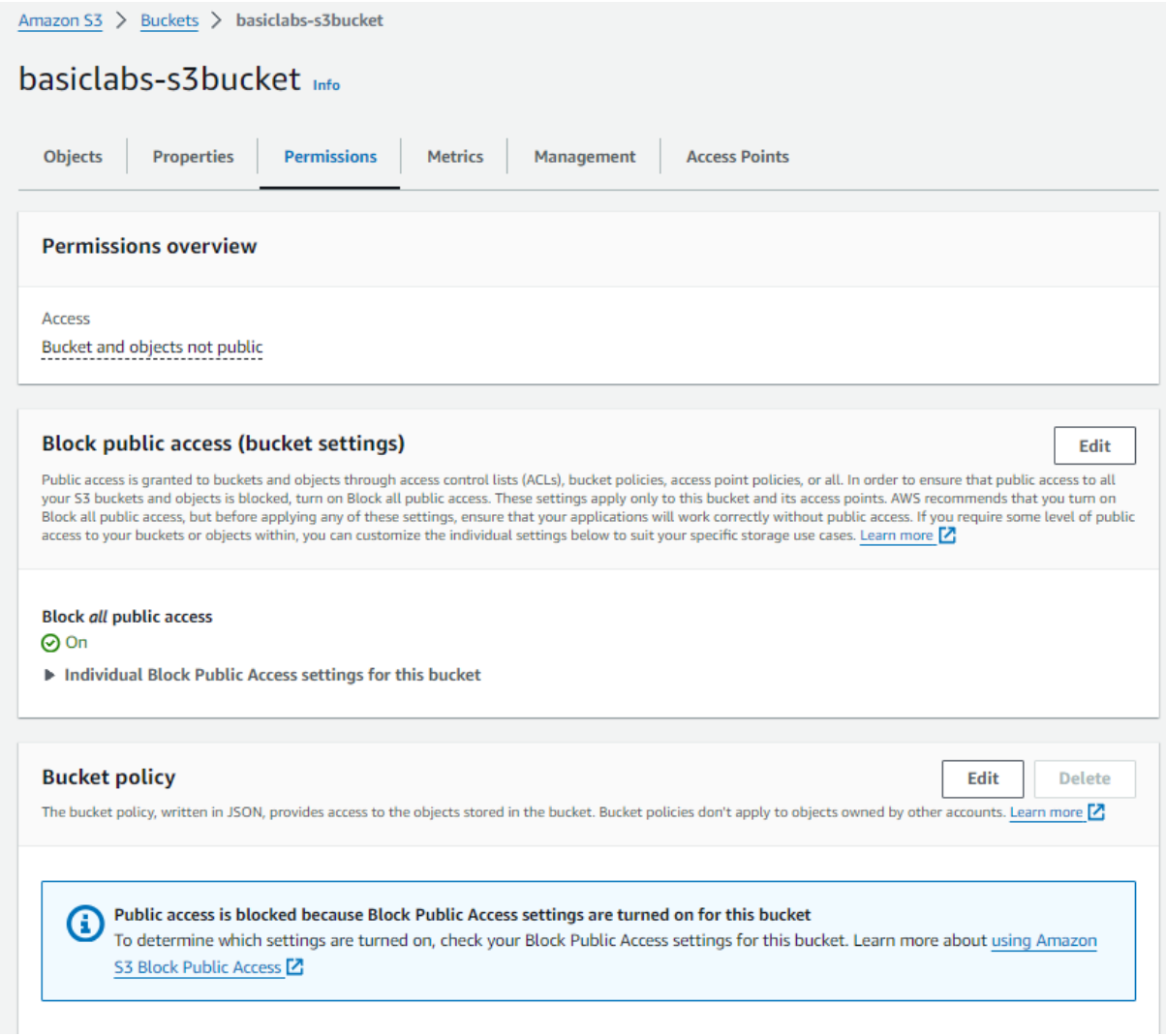
AWS Logo

Amazon Web Services (AWS) is a cloud computing platform that provides a wide range of services, including compute, storage, databases, machine learning, and more. It's widely used by businesses and developers to build scalable and reliable applications.

Uploaded file can be accessed by clicking on the open button on the object overview page.

Setting up bucket policies for Access Control

Click on Permissions of the bucket we created.



Click on Edit Bucket and then policy Generator which will redirect you to the new page.

Amazon S3 > Buckets > basiclabs-s3bucket > 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:::basiclabs-s3bucket

Policy

1

+ Add new statement

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

amazon web services

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

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

- SQS Queue Policy
- S3 Bucket Policy
- VPC Endpoint Policy
- IAM Policy
- SNS Topic Policy

Step 2: Add Statement(s)

A statement is the formal description of [illegible] ee 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 -- Select Actions -- ☐ All Actions ('*')

Amazon Resource Name (ARN)

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

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

Add one or more statements above to generate a policy.

AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies.

Step 1: Select Policy Type

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 -- Select Actions -- ☐ All Actions ('*')

Amazon Resource Name (ARN)

ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement

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:::basiclabs-s3bucket/*	• Null ◦ s3:x-amz-server-side-encryption: "true"

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.

Amazon

You added t

Principal

- *

Step 3:

A *policy* is a

Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will **not be reflected in the policy generator tool.**

```
{
  "Id": "Policy1708676898825",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1708676897441",
      "Action": [
        "s3:PutObject"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::basiclabs-s3bucket/*",
      "Condition": {
        "Null": {
          "s3:x-amz-server-side-encryption": "true"
        }
      },
      "Principal": "*"
    }
  ]
}
```

Close

Generate Policy Start Over

Amazon S3 > Buckets > basiclabs-s3bucket > 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:::basiclabs-s3bucket

Policy

```
1  {
2    "Id": "Policy1708676950435",
3    "Version": "2012-10-17",
4    "Statement": [
5      {
6        "Sid": "Stmt1708676897441",
7        "Action": [
8          "s3:PutObject"
9        ],
10       "Effect": "Deny",
11       "Resource": "arn:aws:s3:::basiclabs-s3bucket/*",
12       "Condition": {
13         "Null": {
14           "s3:x-amz-server-side-encryption": "true"
15         }
16       },
17       "Principal": "*"
18     }
19   ]
20 }
```

+ Add new statement

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

JSON Ln 20, Col 1

Amazon S3 > Buckets > basiclabs-s3bucket > 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:::basiclabs-s3bucket

Policy

1

+ Add new statement

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement