Basic Labs

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. AWS Landing Page

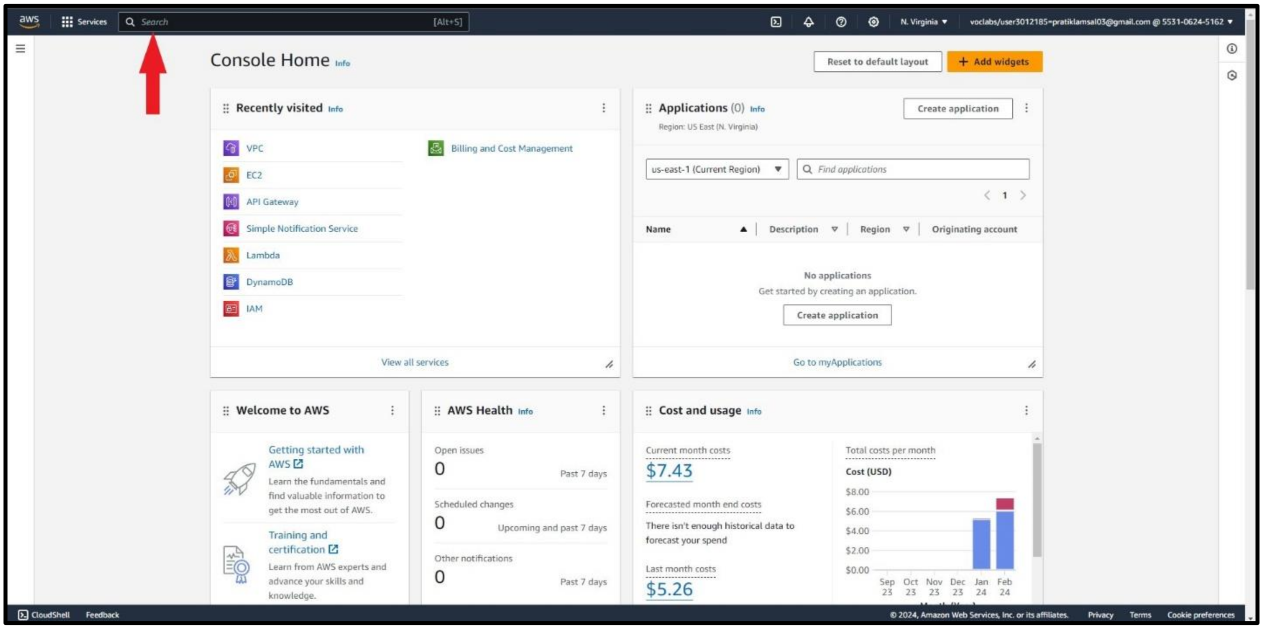


Figure 1 Landing Page

2. Searching for S3

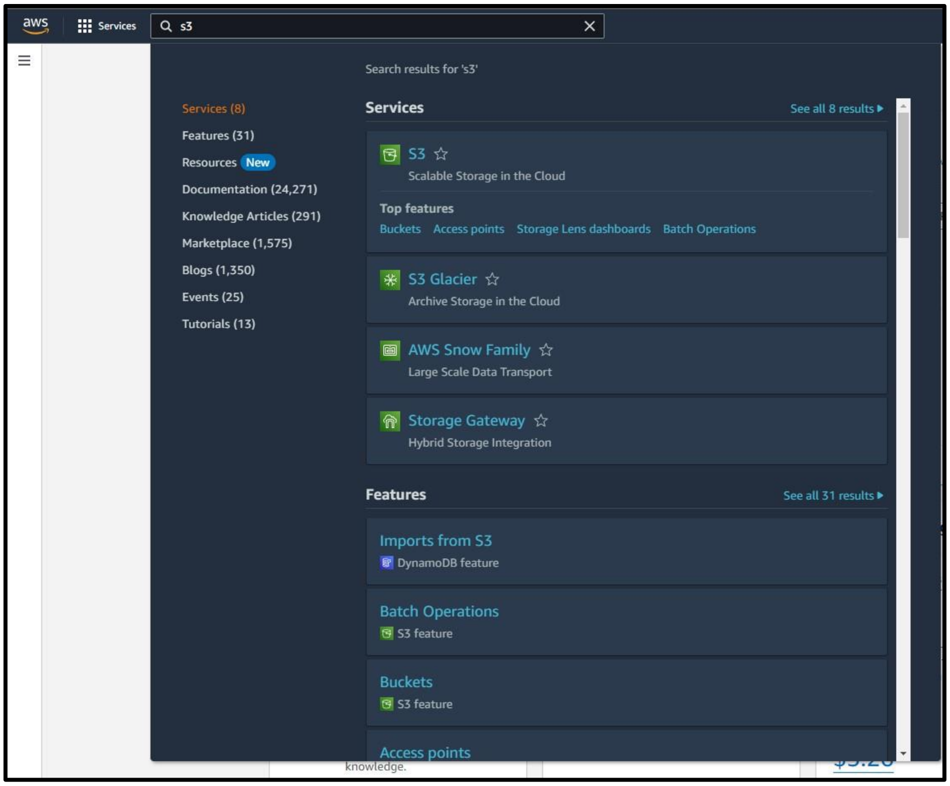
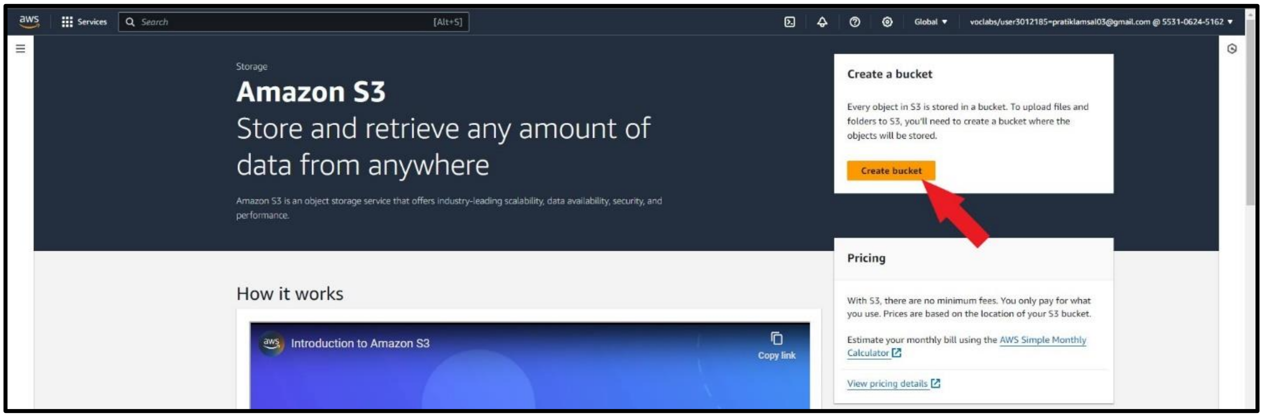


Figure 2 S3 search

3. Creating a bucket


aws
Services
Search [Alt+S]
Global ▾
voclabs/user3012185=pratiklamsal03@gmail.com @ 5531-0624-5162 ▾
Create bucket
Introduction to Amazon S3
Copy link

Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

How it works

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Pricing

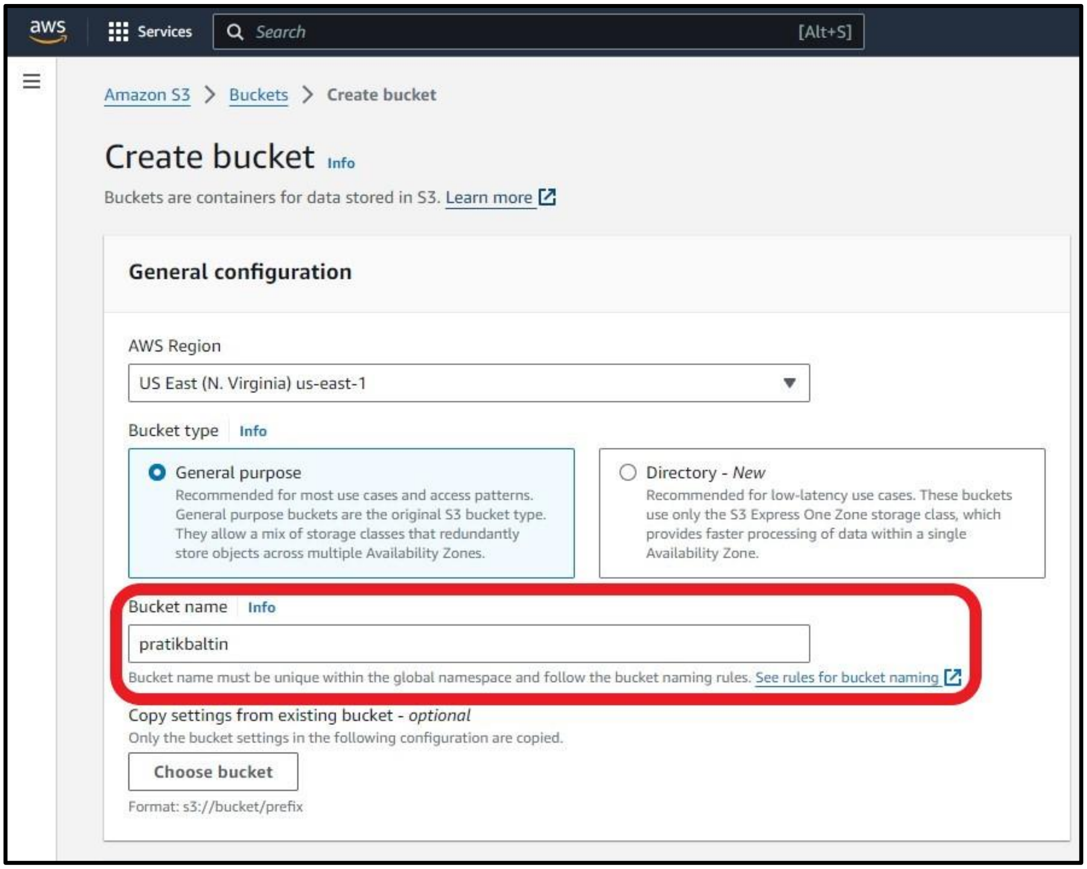
With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the AWS Simple Monthly Calculator

View pricing details

Figure 3 Bucket Creation

4. Naming the bucket


aws
Services
Search [Alt+S]
Amazon S3 > Buckets > Create bucket
Info
Learn more
Info
Info
See rules for bucket naming
Choose bucket

Create bucket

Buckets are containers for data stored in S3. Learn more

General configuration

AWS Region

US East (N. Virginia) us-east-1 ▾

Bucket type

● General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

○ Directory - *New*
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name

pratikbaltin

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - *optional*

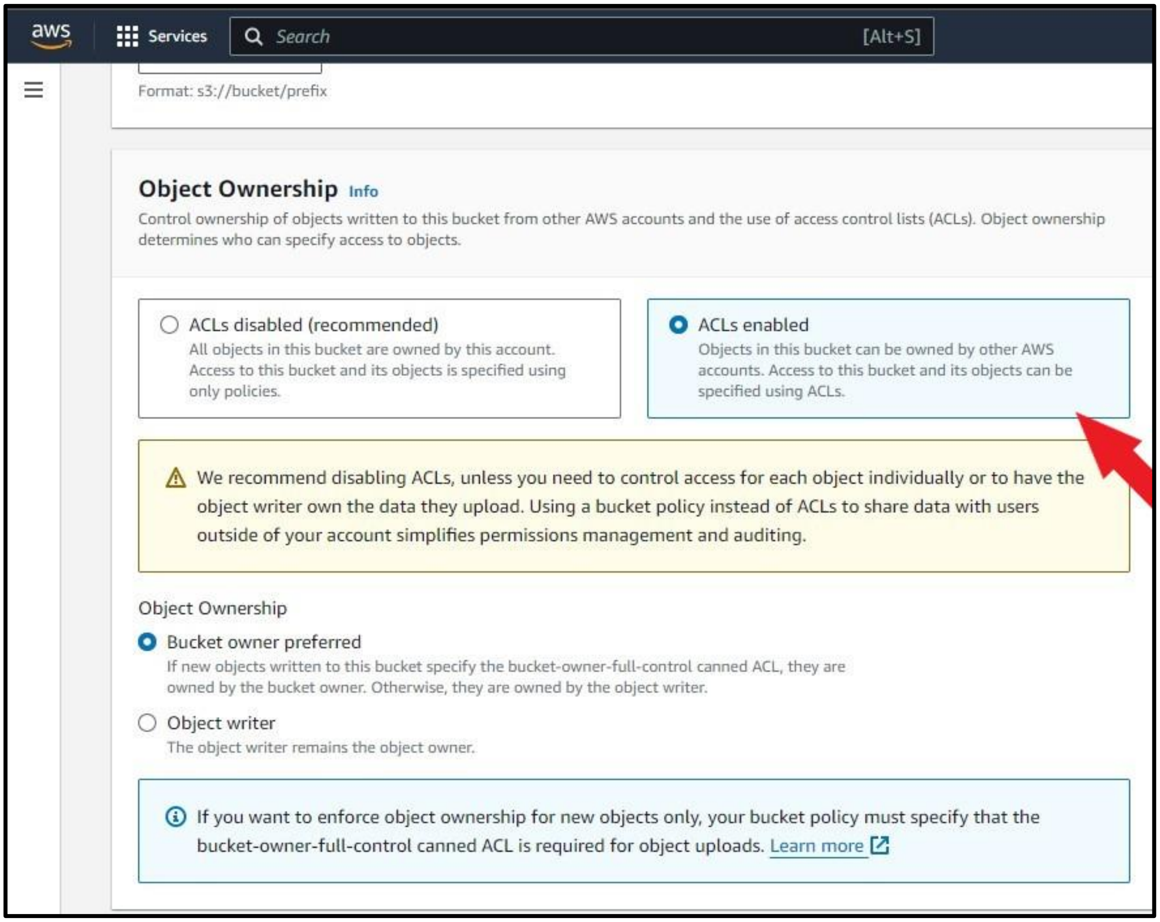
Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

Figure 4 Naming the Bucket

5. Object Ownership

ACL is enabled and Object Ownership is assigned.



Format: s3://bucket/prefix

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.

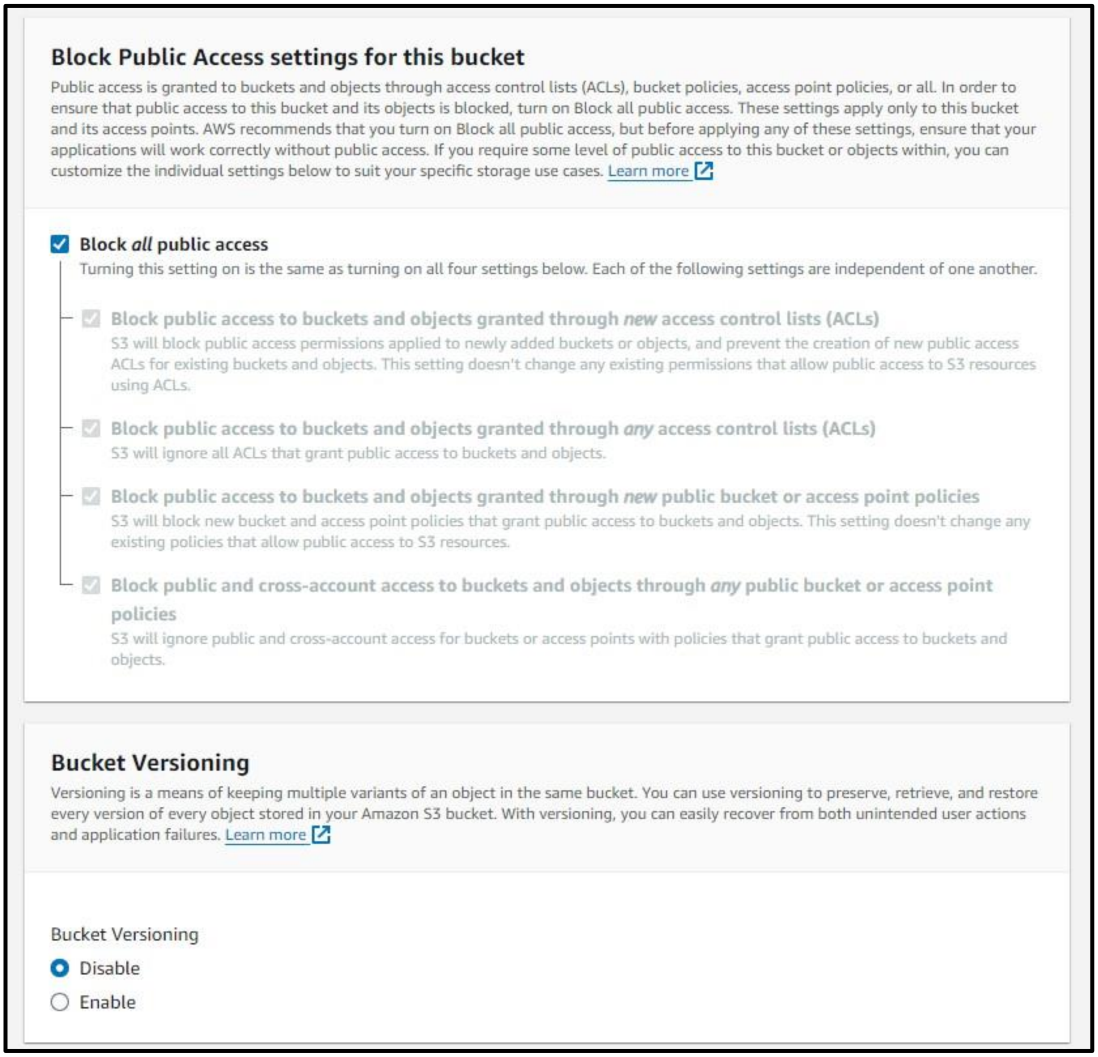
○ Object writer
The object writer remains the object owner.

ⓘ 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

Figure 5 Object Ownership

6. Public Access Settings

All public access is blocked for the bucket.



Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

☑ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☑ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☑ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  S3 will ignore all ACLs that grant public access to buckets and objects.
- ☑ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
  S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☑ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
  S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

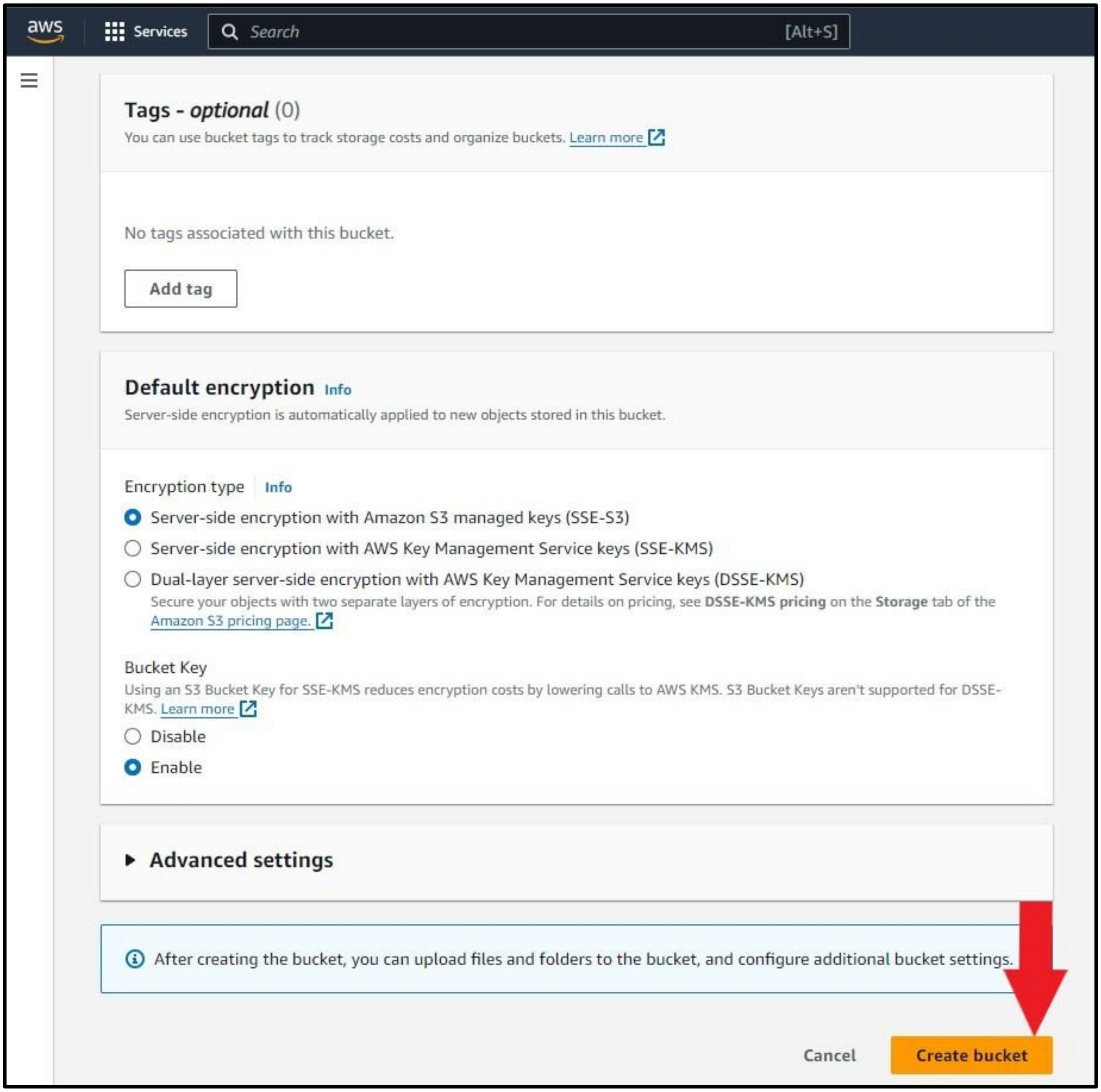
Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning
● Disable
○ Enable

Figure 6 Bucket Public Access Settings

7. Bucket Creation



Tags - *optional* (0)

You can use bucket tags to track storage costs and organize buckets. Learn more

No tags associated with this bucket.

Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info

● Server-side encryption with Amazon S3 managed keys (SSE-S3)

○ Server-side encryption with AWS Key Management Service keys (SSE-KMS)

○ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see **DSSE-KMS pricing** on the **Storage** tab of the Amazon S3 pricing page.

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more

○ Disable

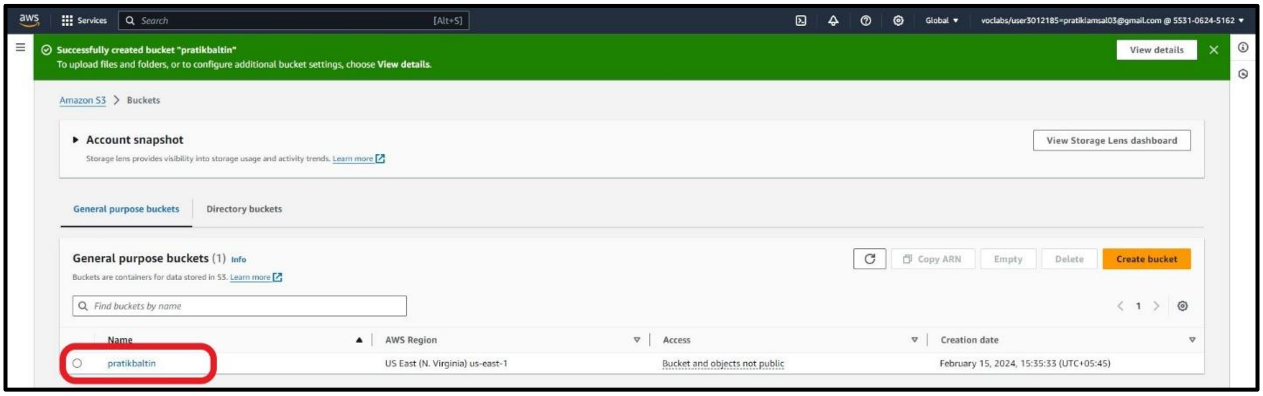
● Enable

▸ **Advanced settings**

ⓘ After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Figure 7 Bucket Creation

8. Successful Bucket Creation



Successfully created bucket "pratikbaltin"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

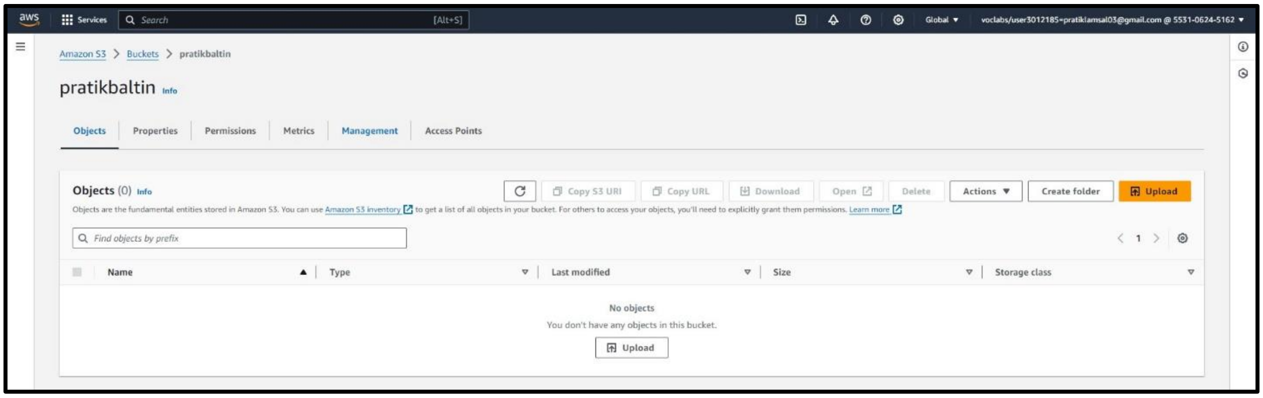
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (1)
Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	pratikbaltin	US East (N. Virginia) us-east-1	Bucket and objects not public	February 15, 2024, 15:35:33 (UTC+05:45)

Figure 8 Successful Bucket Creation

9. Empty Bucket



pratikbaltin

Objects (0)
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

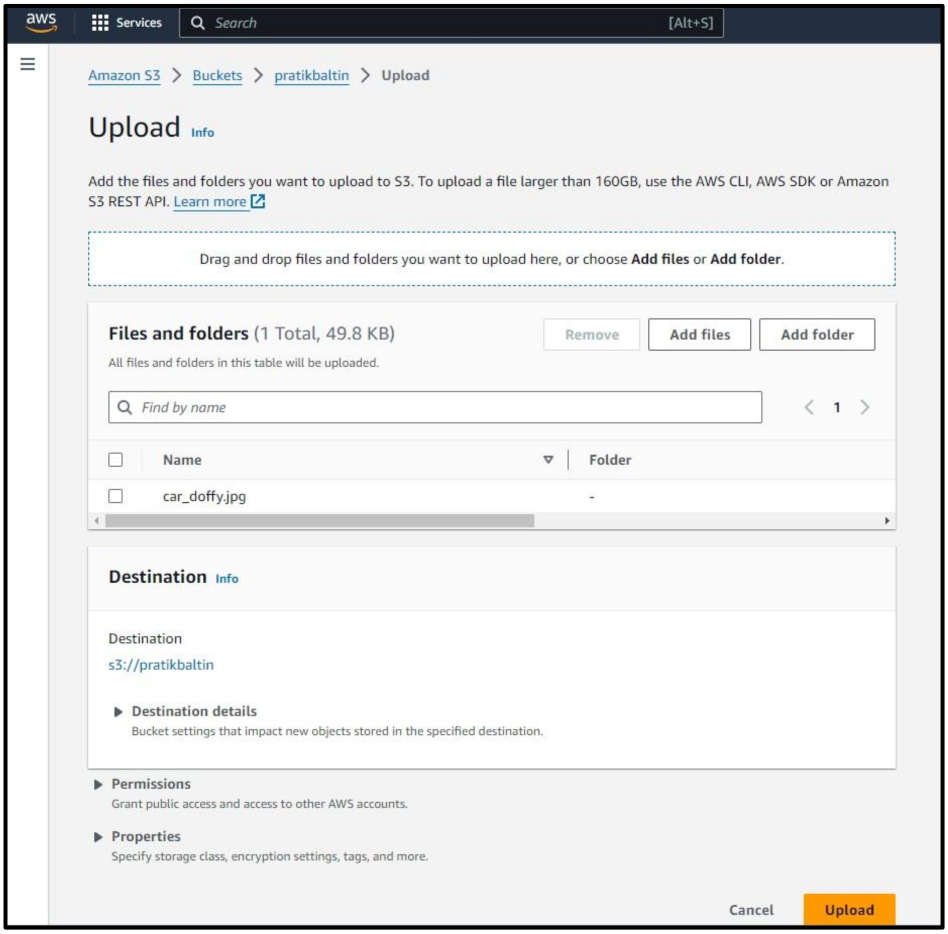
Name	Type	Last modified	Size	Storage class

No objects
You don't have any objects in this bucket.

Figure 9 Empty Bucket

10. File Upload

A file is uploaded to the empty bucket



Amazon S3 > Buckets > pratikbaltin > Upload

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (1 Total, 49.8 KB)

All files and folders in this table will be uploaded.

□	Name	Folder
□	car_doffy.jpg	-

Destination Info

Destination

s3://pratikbaltin

▶ Destination details

Bucket settings that impact new objects stored in the specified destination.

▶ Permissions

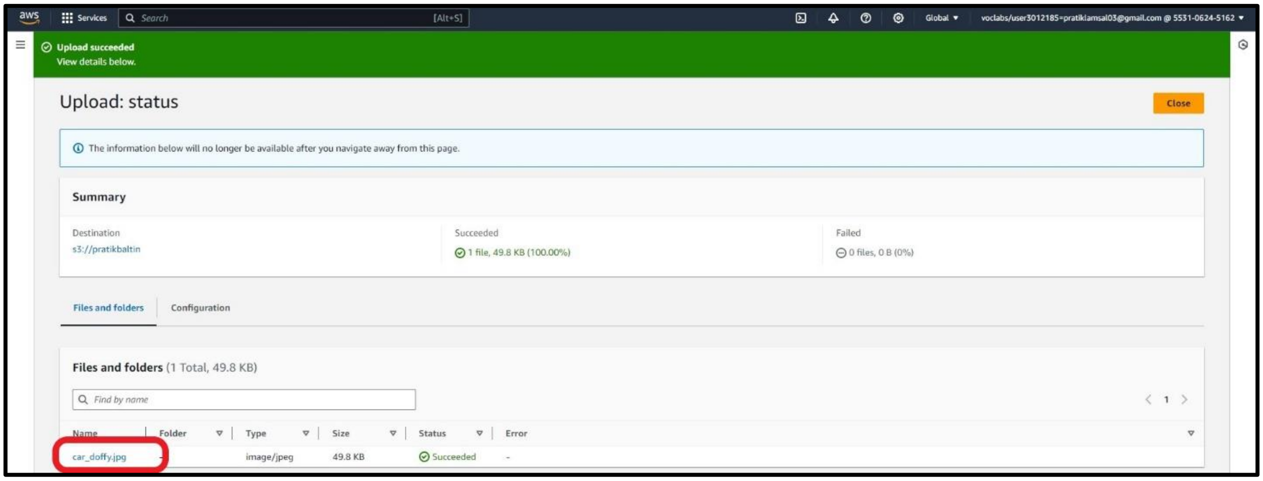
Grant public access and access to other AWS accounts.

▶ Properties

Specify storage class, encryption settings, tags, and more.

Figure 10 File Upload to Empty Bucket

11. File Successfully Uploaded



Upload succeeded
View details below.

Upload: status

The information below will no longer be available after you navigate away from this page.

Summary

Destination	Succeeded	Failed
s3://pratikbaltin	1 file, 49.8 KB (100.00%)	0 files, 0 B (0%)

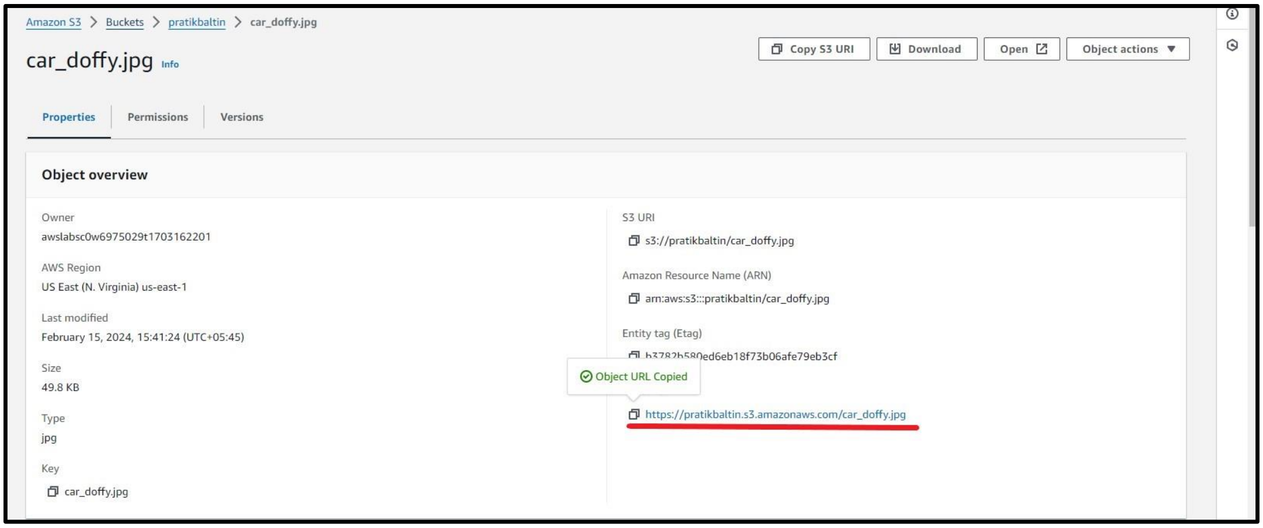
Files and folders (1 Total, 49.8 KB)

Name	Folder	Type	Size	Status	Error
car_doffy.jpg	-	image/jpeg	49.8 KB	Succeeded	-

Figure 11 Successful File Upload

12. Object URL

Object URL is copied to check if the task performed is successful



car_doffy.jpg

Object overview

Owner
awslabsc0w6975029t1703162201

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

Last modified
February 15, 2024, 15:41:24 (UTC+05:45)

Size
49.8 KB

Type
jpg

Key
car_doffy.jpg

S3 URI
s3://pratikbaltin/car_doffy.jpg

Amazon Resource Name (ARN)
arn:aws:s3:::pratikbaltin/car_doffy.jpg

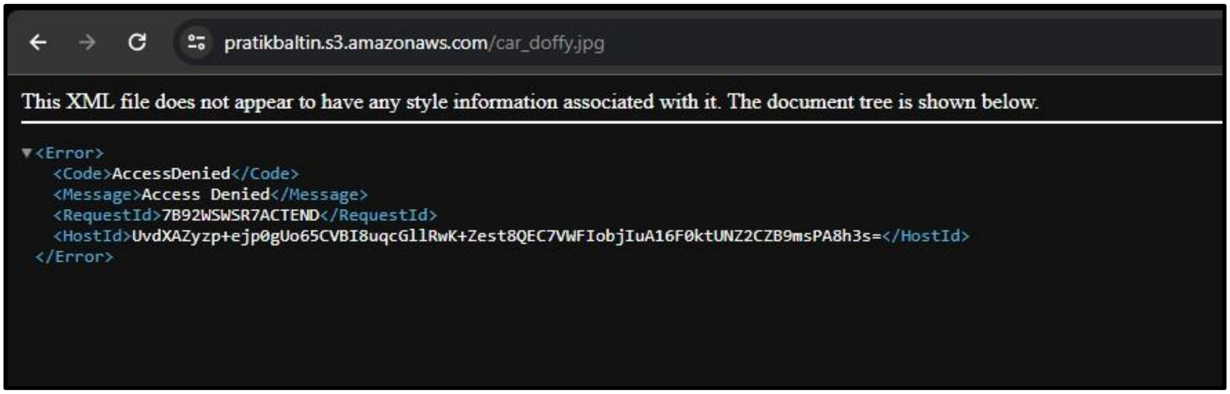
Entity tag (Etag)
b3782b580ed6eb18f73b06afe79eb3cf

Object URL Copied

https://pratikbaltin.s3.amazonaws.com/car_doffy.jpg

Figure 12 Copying Object URL

13. Access Denied



pratikbaltin.s3.amazonaws.com/car_doffy.jpg

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>7B92WSWSR7ACTEND</RequestId>
   <HostId>UvdXAZyzp+ejp0gUo65CVBI8uqcGllRwK+Zest8QEC7VWFIobjIuA16F0ktUNZ2CZB9msPA8h3s=</HostId>
 </Error>
```

Figure 13 Access Denied

14. Changing Object ACL

Object ACL is changed to check if it can be accessed.

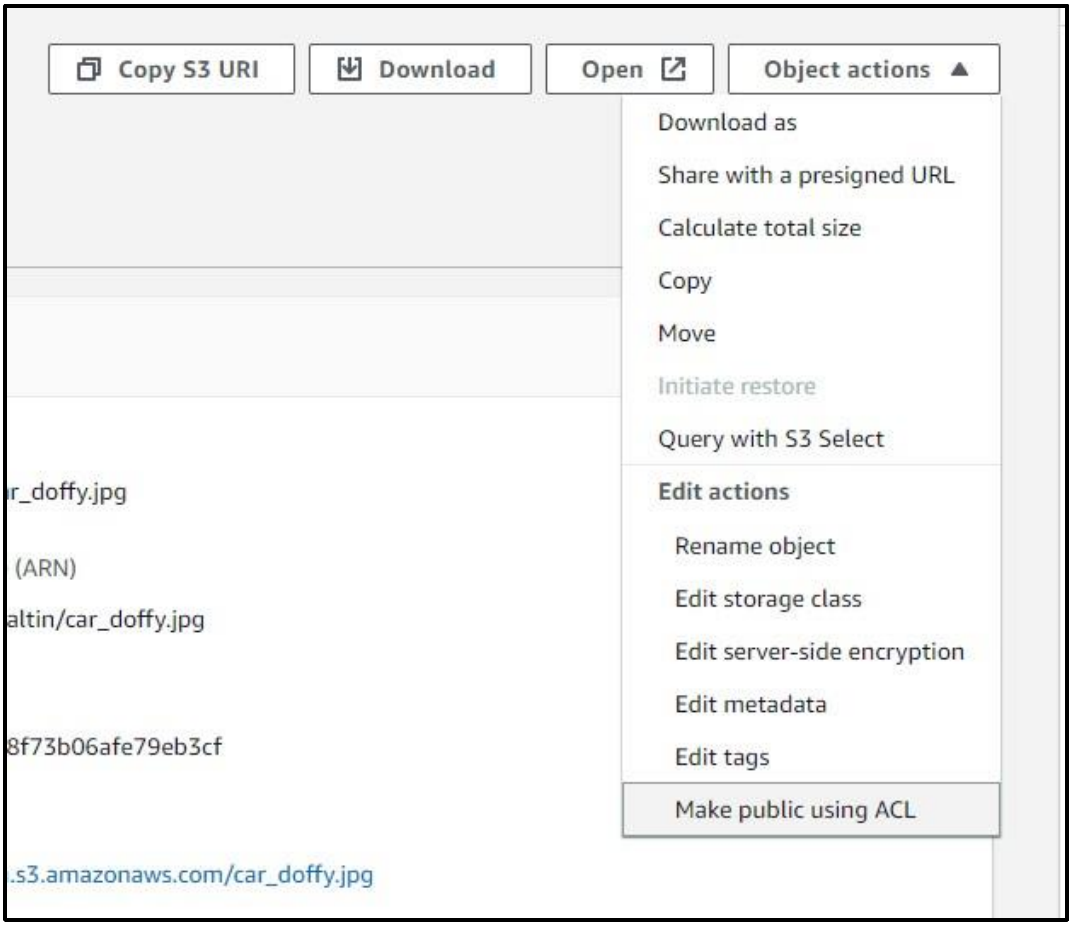
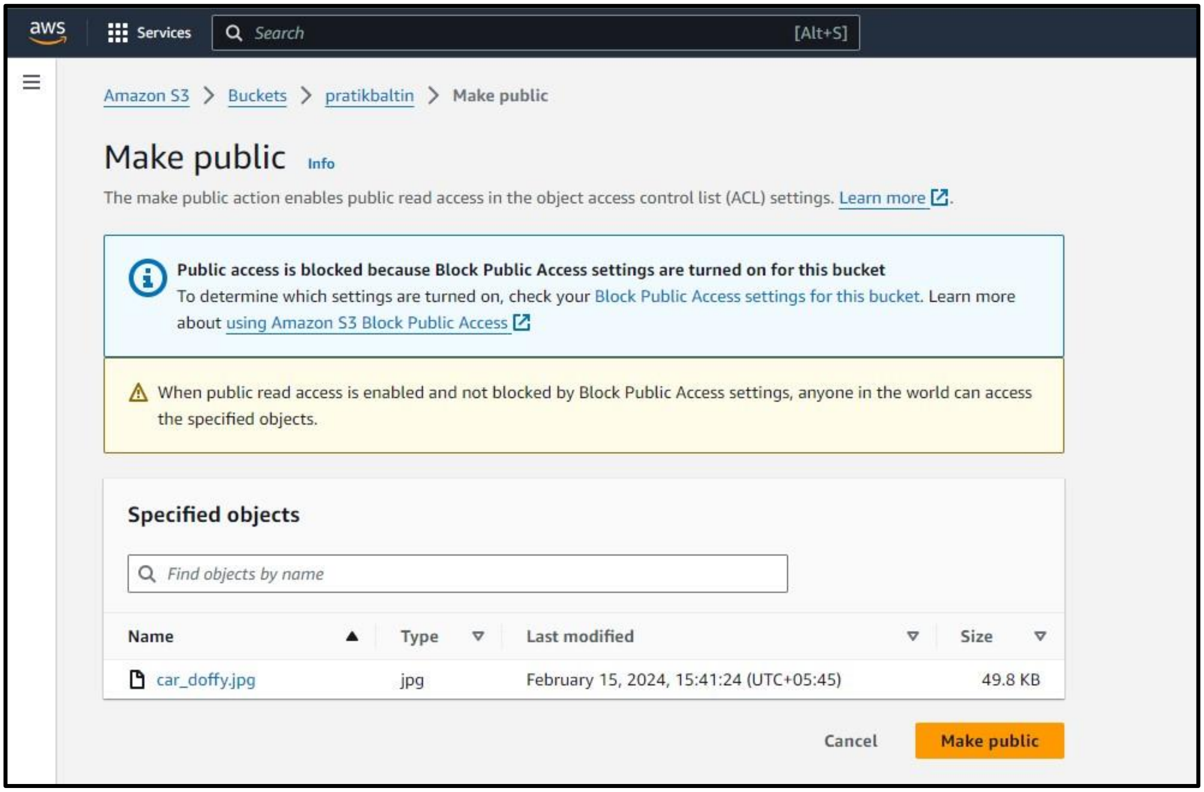


Figure 14 Changing Object ACL

15. Making Object Public



Amazon S3 > Buckets > pratikbaltin > Make public

Make public Info

The make public action enables public read access in the object access control list (ACL) settings. Learn more.

Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access

When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.

Specified objects

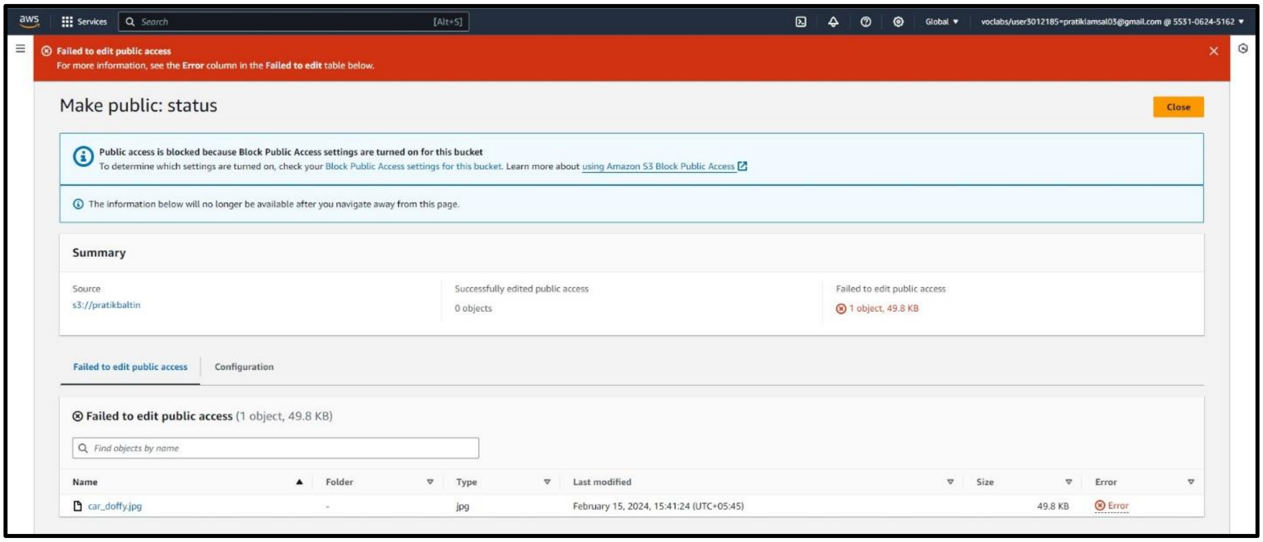
Find objects by name

Name	Type	Last modified	Size
car_doffy.jpg	jpg	February 15, 2024, 15:41:24 (UTC+05:45)	49.8 KB

Figure 15 Making Object Public

16. Failed to Make Public

Public Access for object failed as the bucket itself has no access to public.


aws
Services
Search [Alt+S]
Global
voclabs/user3012185=pratiklamsal03@gmail.com @ 5531-0624-5162

Failed to edit public access
For more information, see the **Error** column in the **Failed to edit** table below.

Make public: status

Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access

The information below will no longer be available after you navigate away from this page.

Summary

Source
s3://pratikbaltin

Successfully edited public access
0 objects

Failed to edit public access
1 object, 49.8 KB

Failed to edit public access (1 object, 49.8 KB)

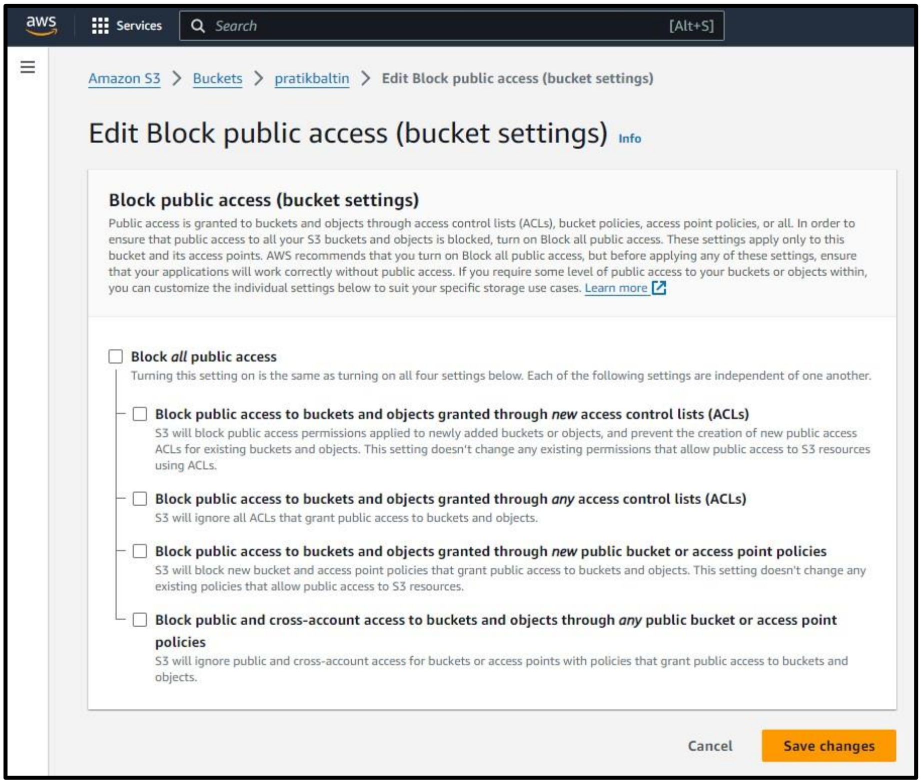
Find objects by name

Name	Folder	Type	Last modified	Size	Error
car_doffy.jpg	-	jpg	February 15, 2024, 15:41:24 (UTC+05:45)	49.8 KB	Error

Figure 16 Failed Object Public Access

17. Bucket Public Access

Bucket Public Access is changed to allow public access.



Amazon S3 > Buckets > pratikbaltin > Edit Block public access (bucket settings)

Edit Block public access (bucket settings) Info

Block public access (bucket settings)

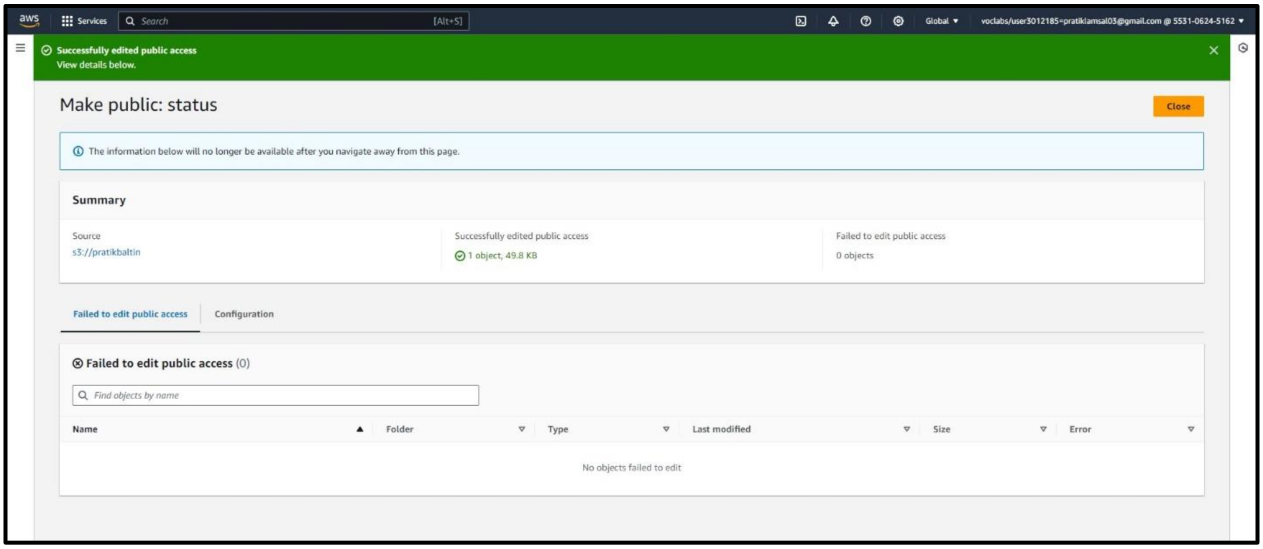
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access 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 your buckets 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.

Figure 17 Bucket Public Access

18. Public Access Settings Changed



aws
Services
Search
[Alt+S]
Global ▾
voclabs/user3012185=pratiklamsal03@gmail.com @ 5531-0624-5162 ▾

Successfully edited public access
View details below.

Make public: status

The information below will no longer be available after you navigate away from this page.

Summary

Source	Successfully edited public access	Failed to edit public access
s3://pratikbaltin	1 object, 49.8 KB	0 objects

Failed to edit public access
Configuration

Failed to edit public access (0)

Name	Folder	Type	Last modified	Size	Error

No objects failed to edit

Figure 18 Successful Public Access Changed

19. Successful Upload to Bucket

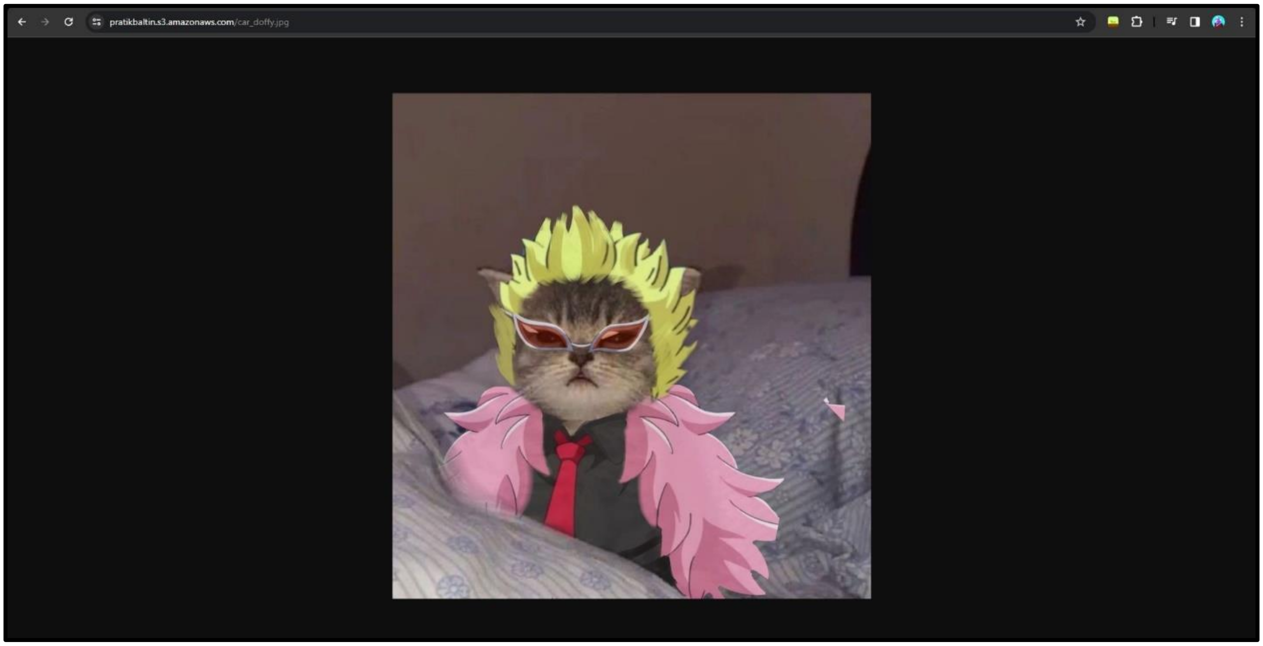


Figure 19 Successful Image Upload