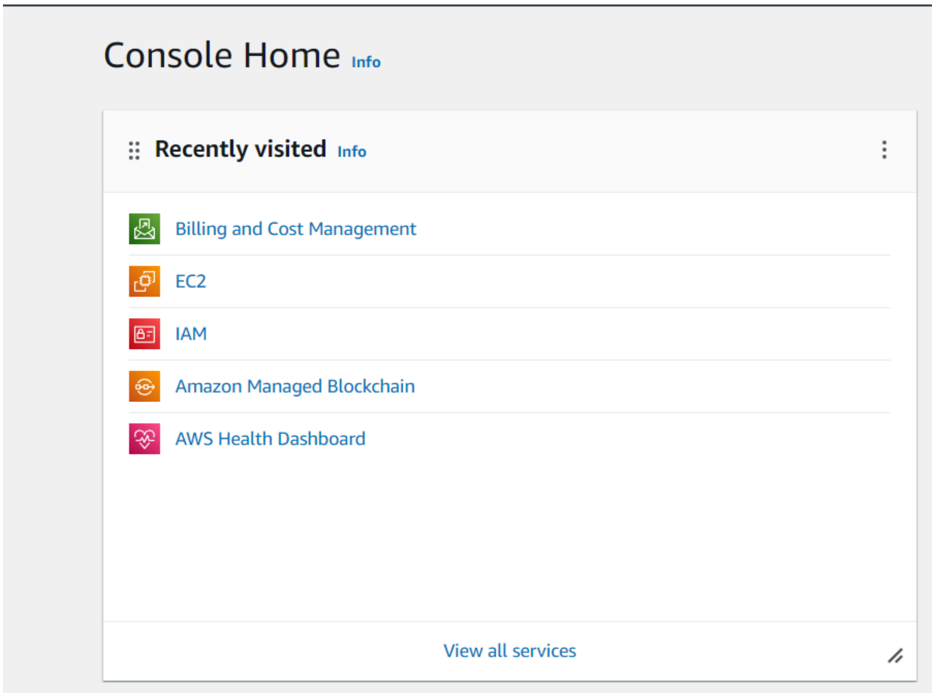
Practical No: - 06

Implementation of Storage as a Service using Google Docs/AWS

Login to your AWS account



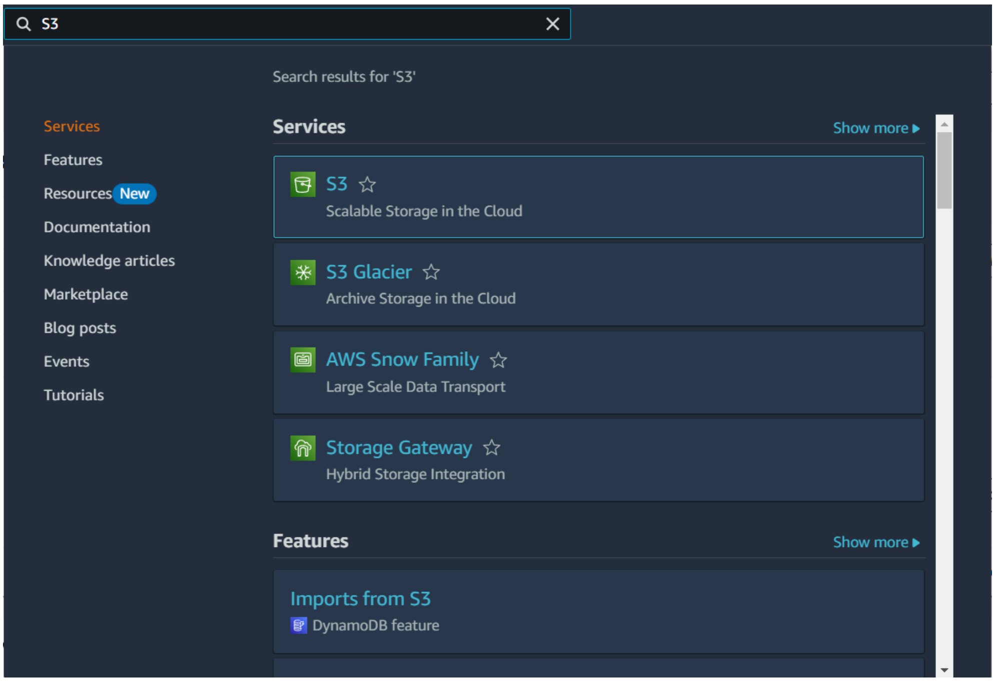
Console Home Info

Recently visited Info

- Billing and Cost Management
- EC2
- IAM
- Amazon Managed Blockchain
- AWS Health Dashboard

View all services

In the search bar, search for S3



S3

Search results for 'S3'

Services Show more ▸

S3 ☆
Scalable Storage in the Cloud

S3 Glacier ☆
Archive Storage in the Cloud

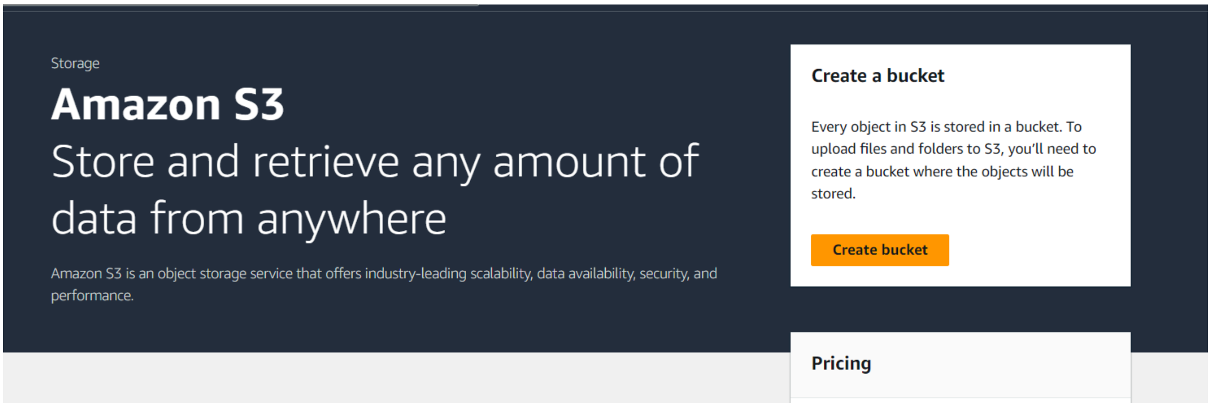
AWS Snow Family ☆
Large Scale Data Transport

Storage Gateway ☆
Hybrid Storage Integration

Features Show more ▸

Imports from S3
DynamoDB feature

Click on Create bucket



Storage

Amazon S3

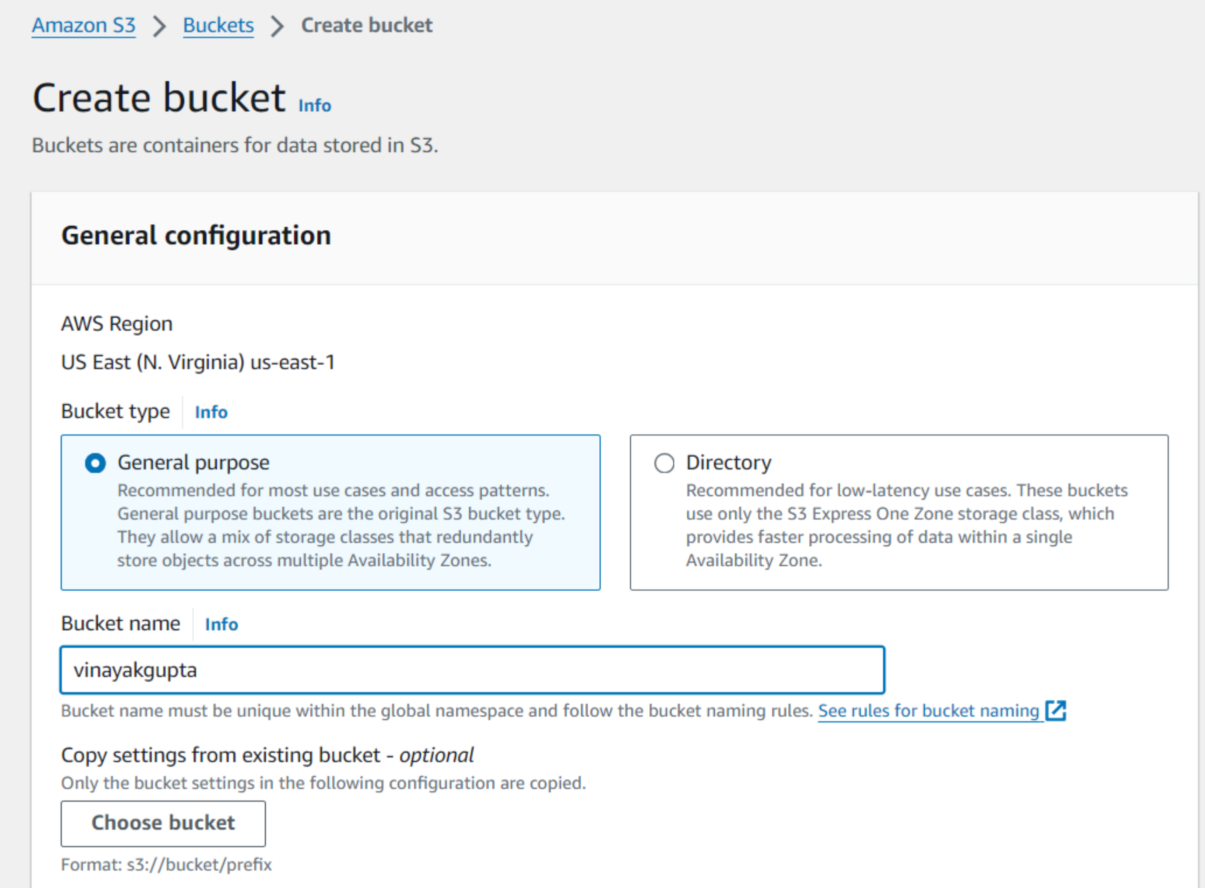
Store and retrieve any amount of data from anywhere

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

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.

Select "General Purpose" and give bucket name



Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region

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

Bucket type Info

● 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
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 Info

vinayakgupta

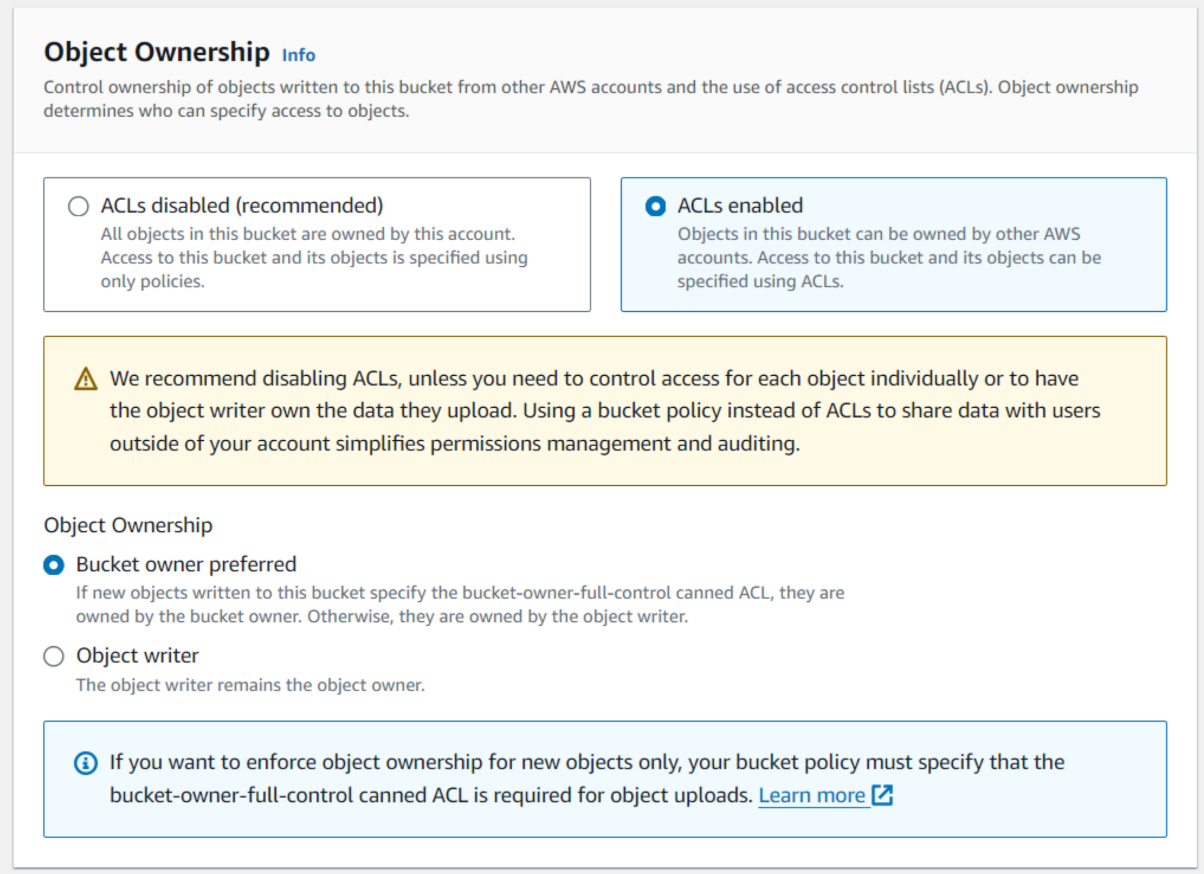
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

In Object Ownership, if ACLs is disabled, enable it



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.

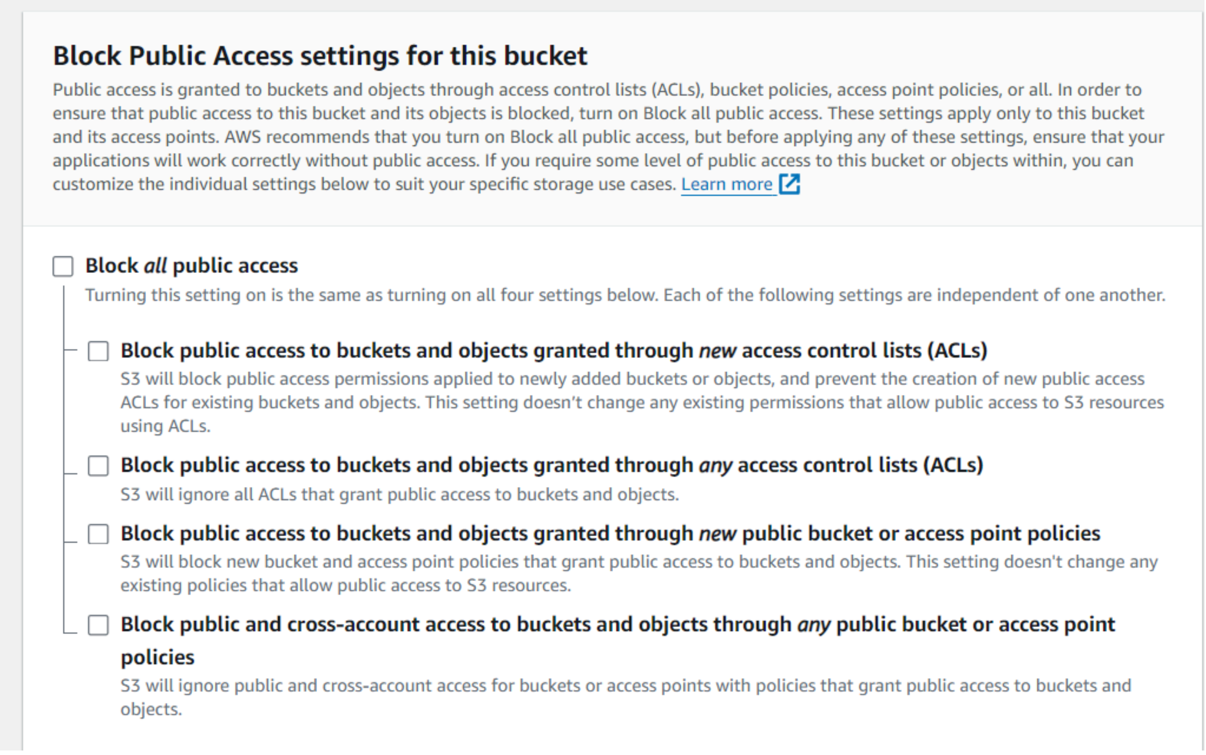
Object Ownership

● 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

In "Block Public Access settings for this bucket" section, if the "Block all public access" checkbox is checked, uncheck the box



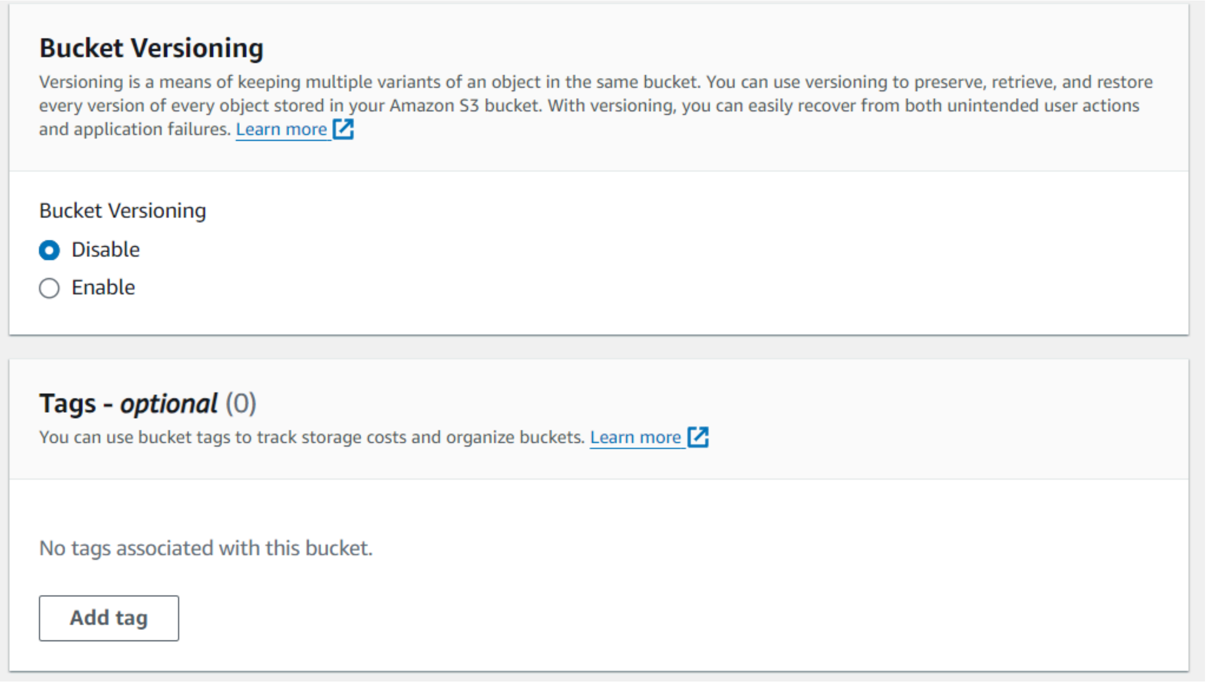
Block Public Access settings for this bucket

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.

In Bucket Versioning, select Disable



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

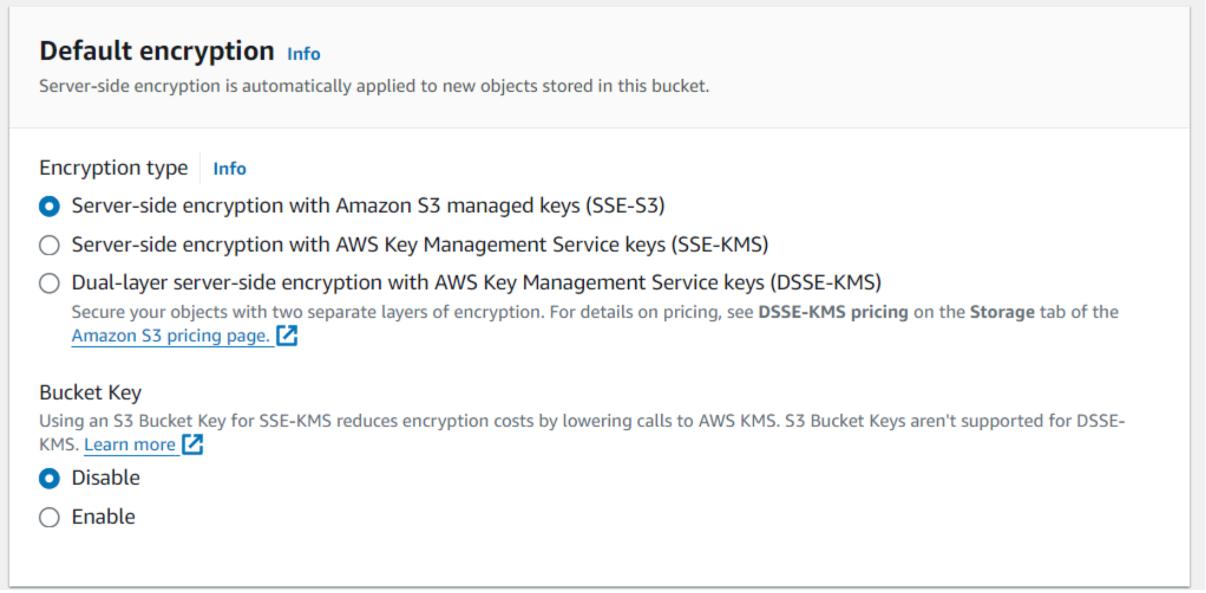
○ Enable

Tags - *optional* (0)

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

No tags associated with this bucket.

In Default encryption, select "Server-side encryption with Amazon S3 managed keys (SSE-S3)" and select bucket key as Disable



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.

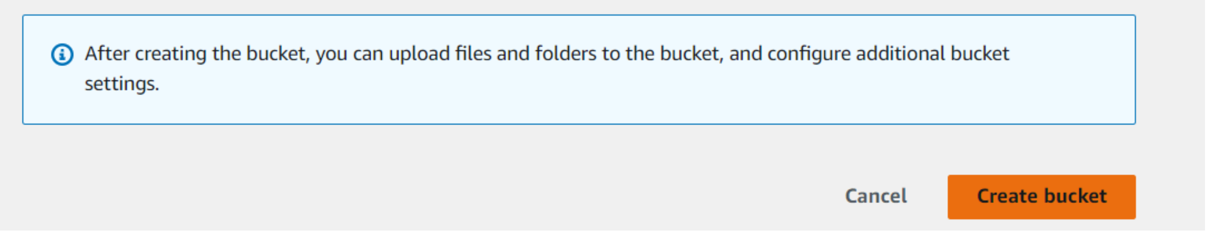
Bucket Key

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

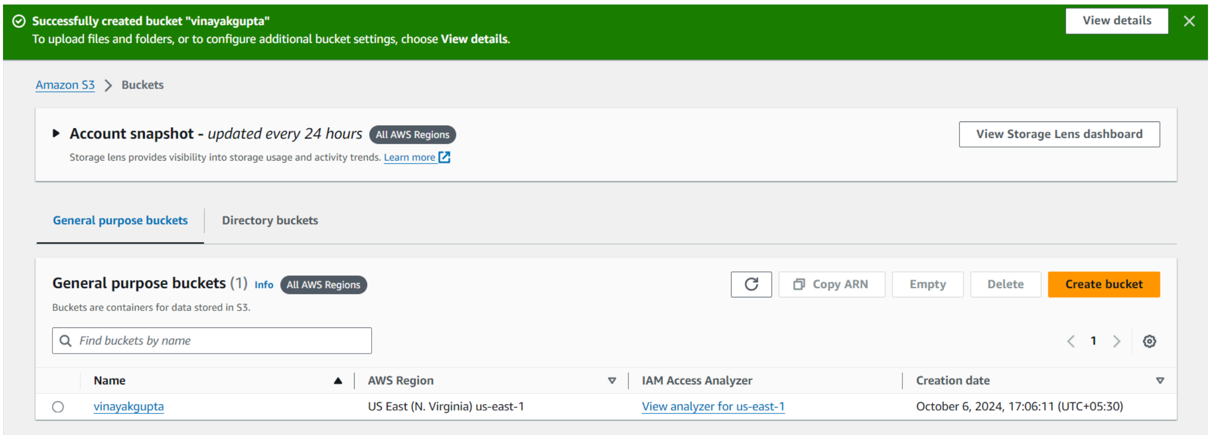
○ Enable

Click on create bucket



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

Your bucket will be created successfully



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

Amazon S3 > Buckets

Account snapshot - *updated every 24 hours* All AWS Regions

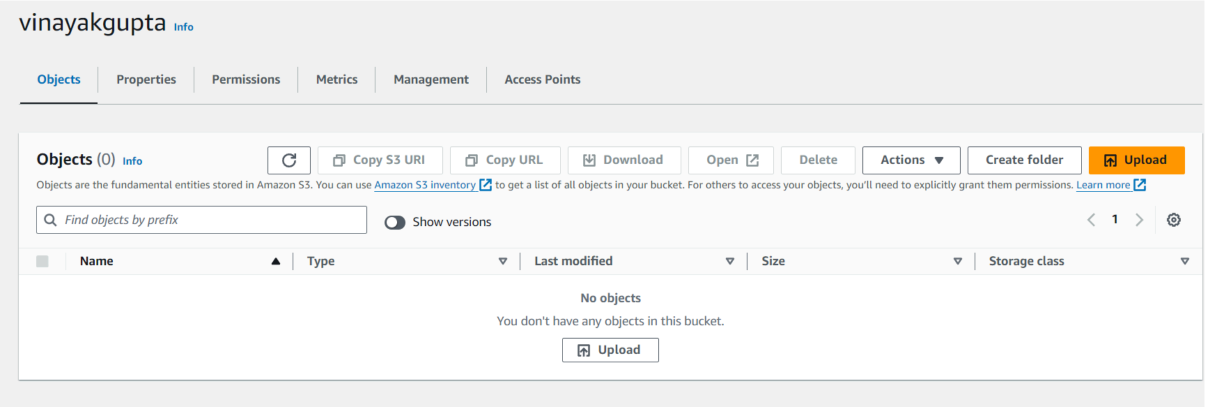
Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (1) Info All AWS Regions

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	vinayakgupta	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 6, 2024, 17:06:11 (UTC+05:30)

Now click on your bucket and then click on "Upload"



vinayakgupta Info

Objects (0) Info

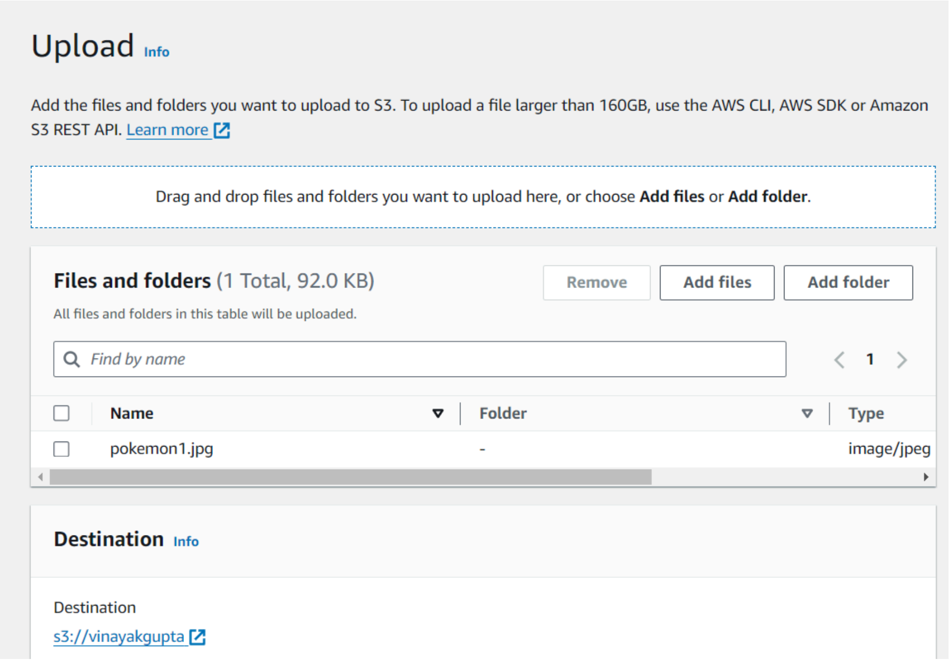
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

	Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.

In files and folders, click on Add files and select the file you want to upload(here I have select an image)



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, 92.0 KB)

All files and folders in this table will be uploaded.

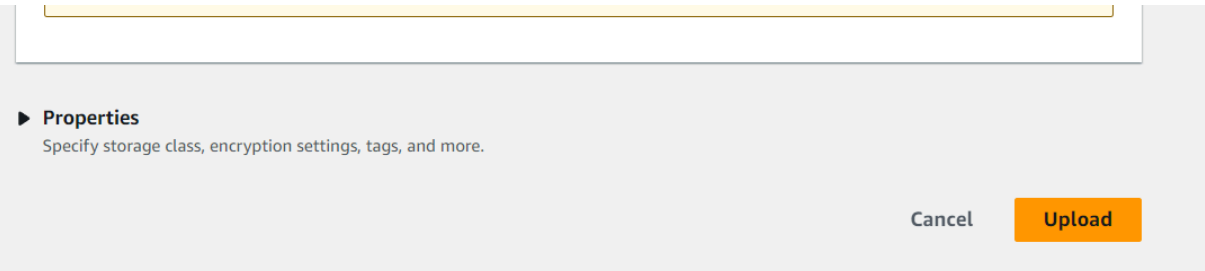
	Name	Folder	Type
□	pokemon1.jpg	-	image/jpeg

Destination Info

Destination

s3://vinayakgupta

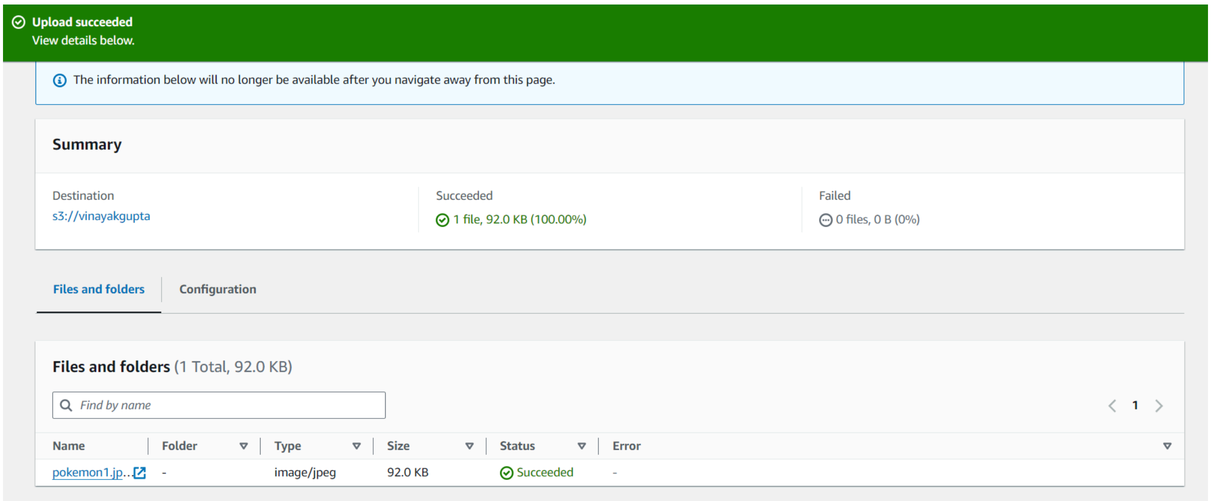
Click on upload



▶ Properties

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

Your file will be uploaded successfully



✓ Upload succeeded
View details below.

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

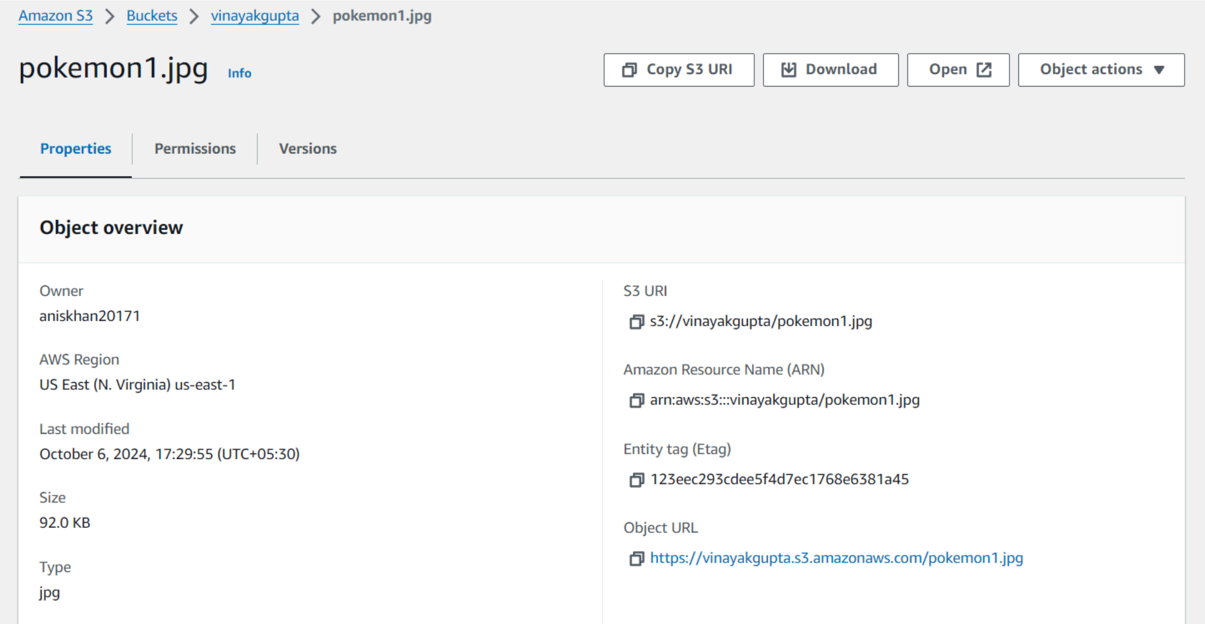
Summary

Destination	Succeeded	Failed
s3://vinayakgupta	✓ 1 file, 92.0 KB (100.00%)	⊖ 0 files, 0 B (0%)

Files and folders (1 Total, 92.0 KB)

Name	Folder	Type	Size	Status	Error
pokemon1.jp..	-	image/jpeg	92.0 KB	✓ Succeeded	-

Click on the file



Amazon S3 > Buckets > vinayakgupta > pokemon1.jpg

pokemon1.jpg Info

Object overview

Owner
aniskhan20171

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

Last modified
October 6, 2024, 17:29:55 (UTC+05:30)

Size
92.0 KB

Type
jpg

S3 URI
s3://vinayakgupta/pokemon1.jpg

Amazon Resource Name (ARN)
arn:aws:s3:::vinayakgupta/pokemon1.jpg

Entity tag (Etag)
123eec293cdee5f4d7ec1768e6381a45

Object URL
https://vinayakgupta.s3.amazonaws.com/pokemon1.jpg

Now to see if the file is uploaded, click on the object url link, it will open the uploaded image.
(my Object URL: https://vinayakgupta.s3.amazonaws.com/pokemon1.jpg)