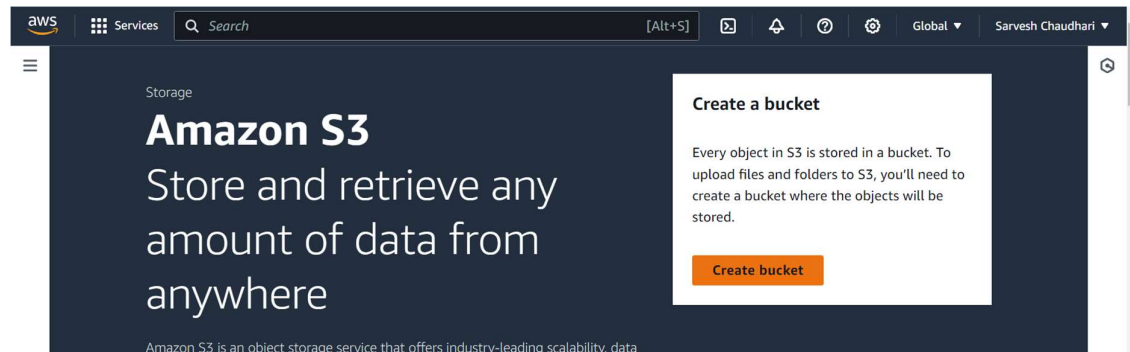


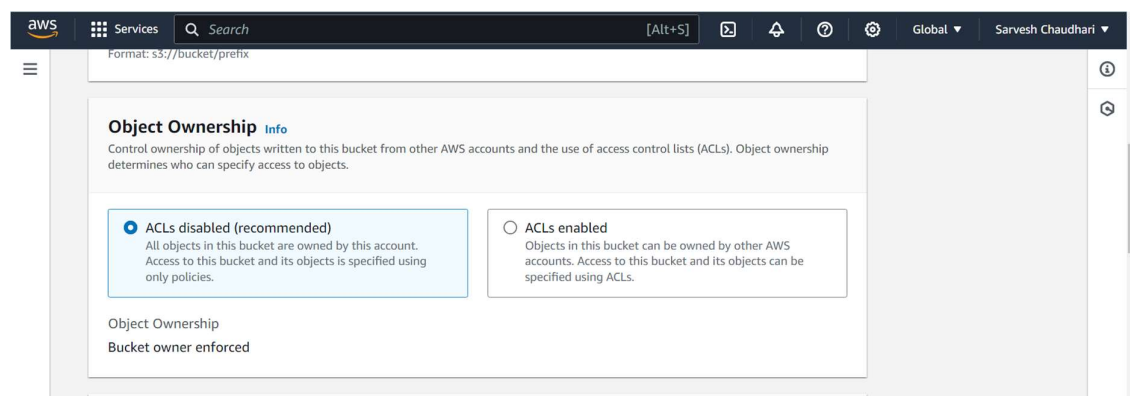
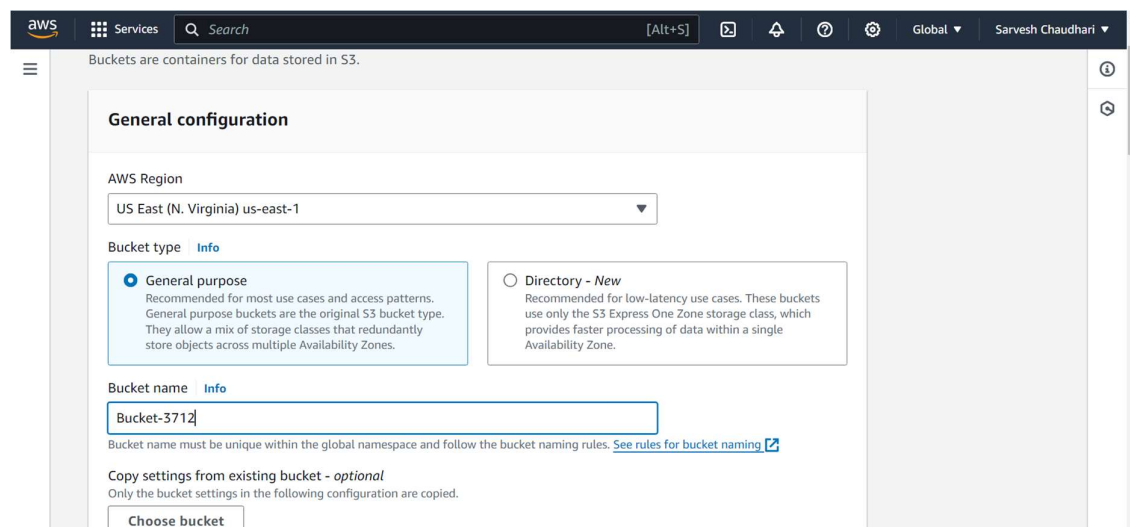
Objective :- Understanding S3 Buckets and its use

Steps:-

Now create Storage S3



Name should be unique in global



Bucket versioning allows us to preserve, retrieve and restore 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

Keep all by-default

Services

Search

[Alt+S]

Global

Sarvesh Chaudhari

Add tag

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

Services

Search

[Alt+S]

Global

Sarvesh Chaudhari

Successfully created bucket "bucket3712"

View details

To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Account snapshot

View Storage Lens dashboard

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

General purpose buckets

Directory buckets

General purpose buckets (1)

Info

Buckets are containers for data stored in S3.

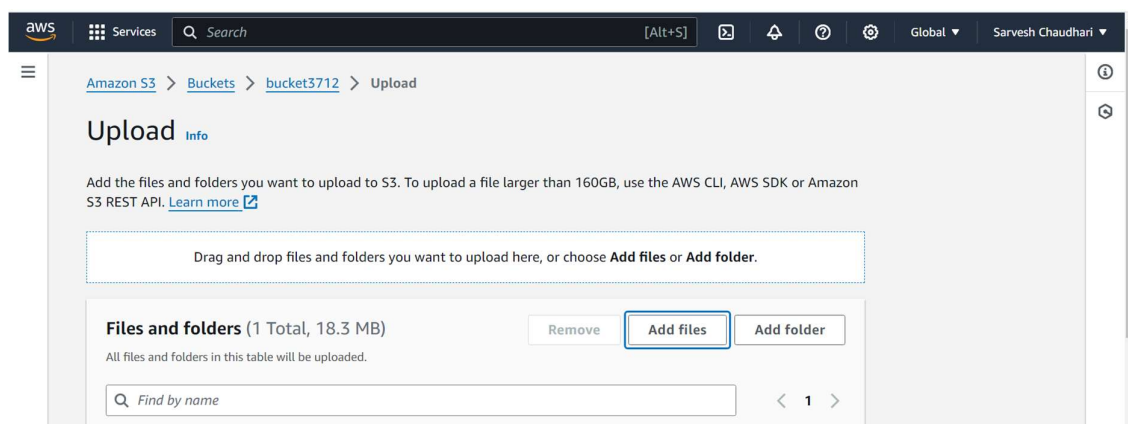
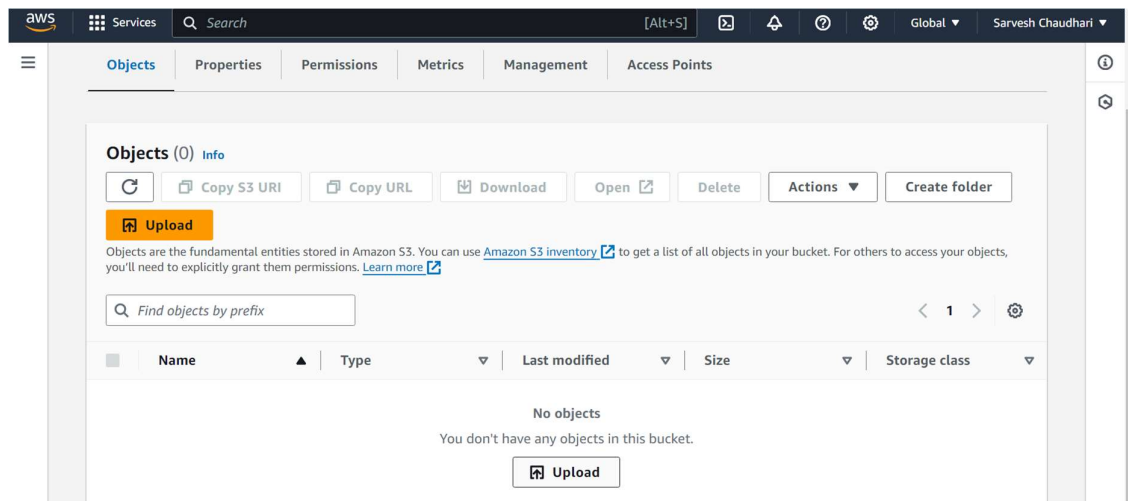
Find buckets by name

< 1 >

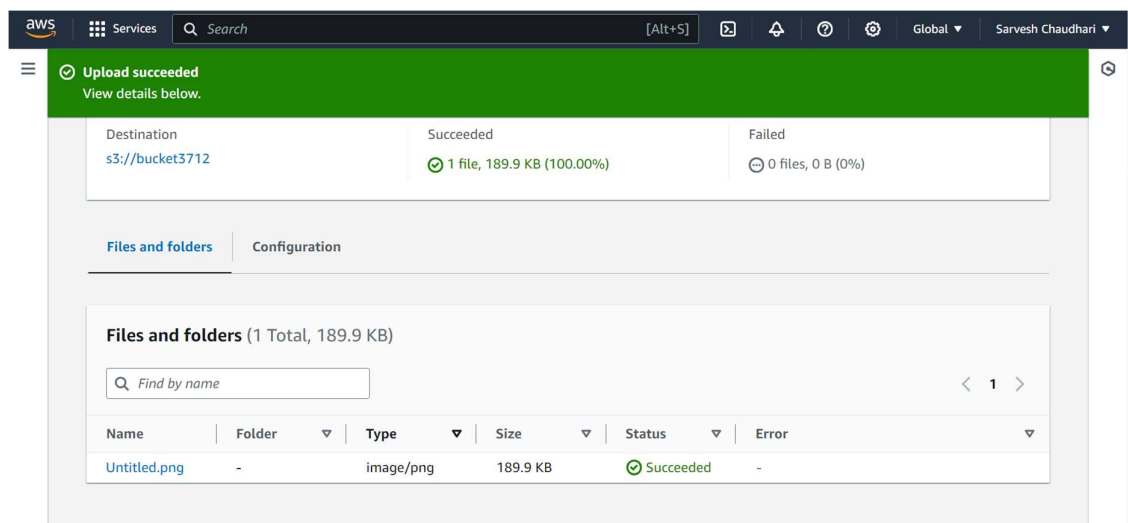
Name	AWS Region	Access	Creation date
<input type="radio"/> bucket3712	US East (N. Virginia) us-east-1	Bucket and objects not public	February 26, 2024, 11:12:57 (UTC+05:30)

Now click on bucket name to enter into bucket

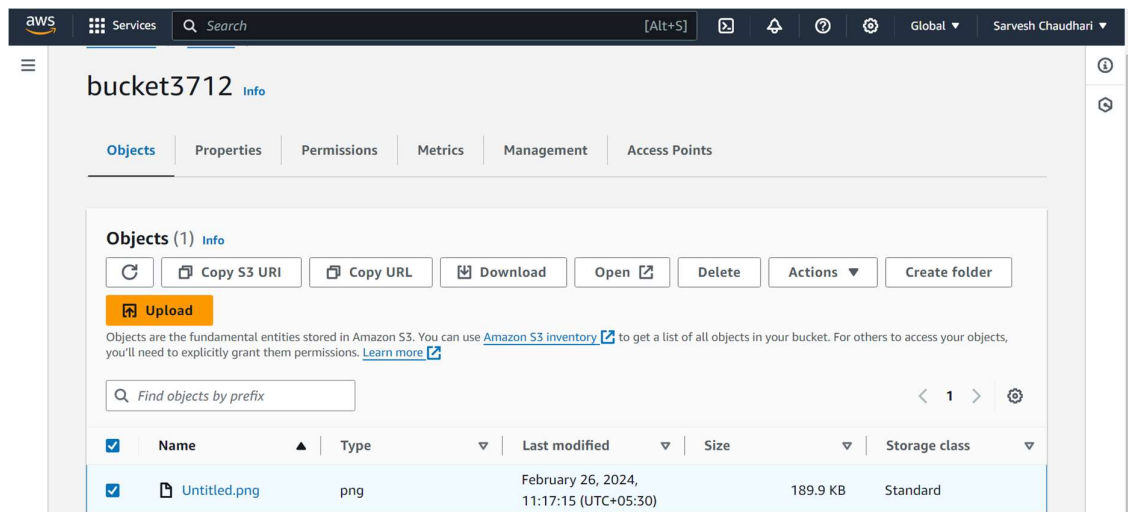
To upload file in bucket click on Upload files



Select file then Scroll down and click on upload

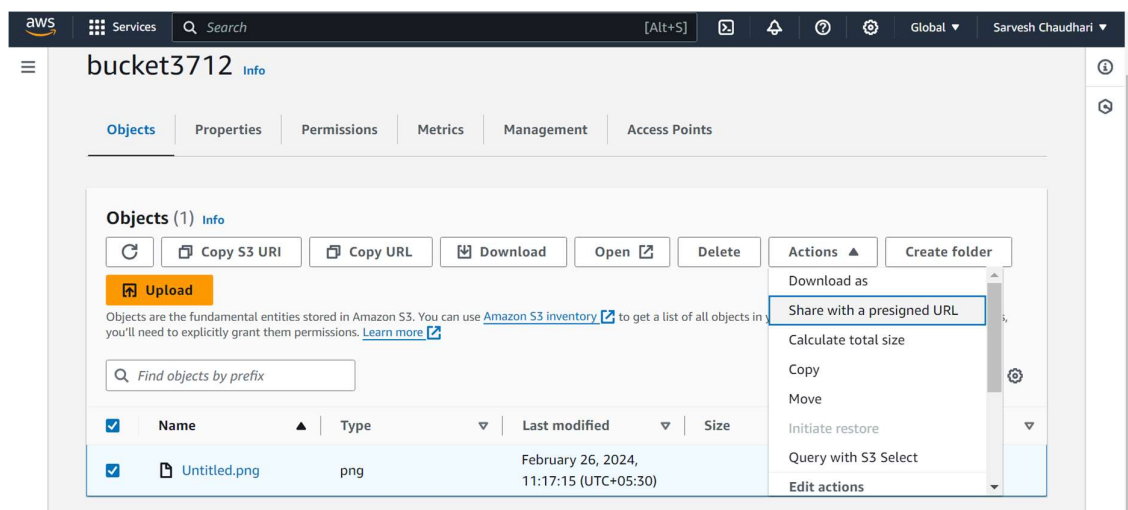


File uploaded successfully



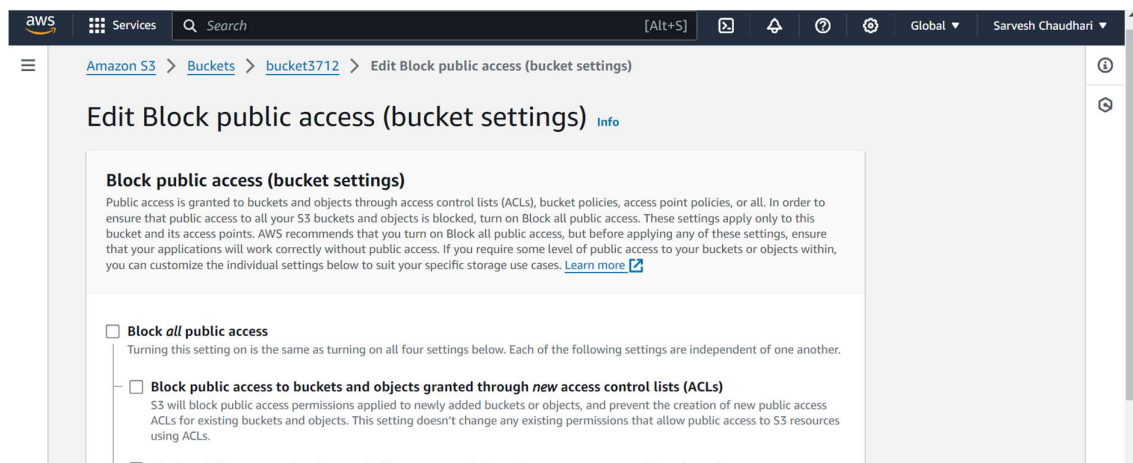
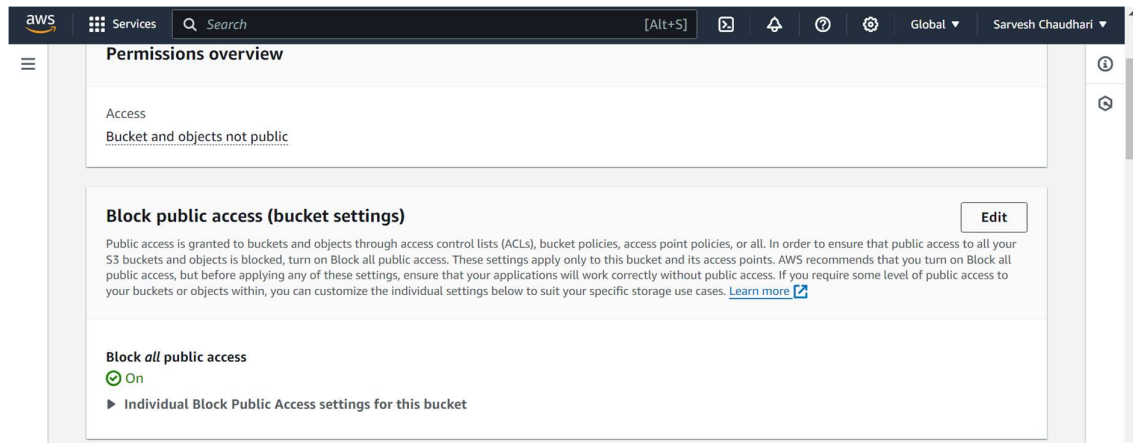
This file can not be directly accessible as we kept bucket private.

Using copy url option we can not see the file content to view this file we can select file then in action select 'Share with Presigned URL'

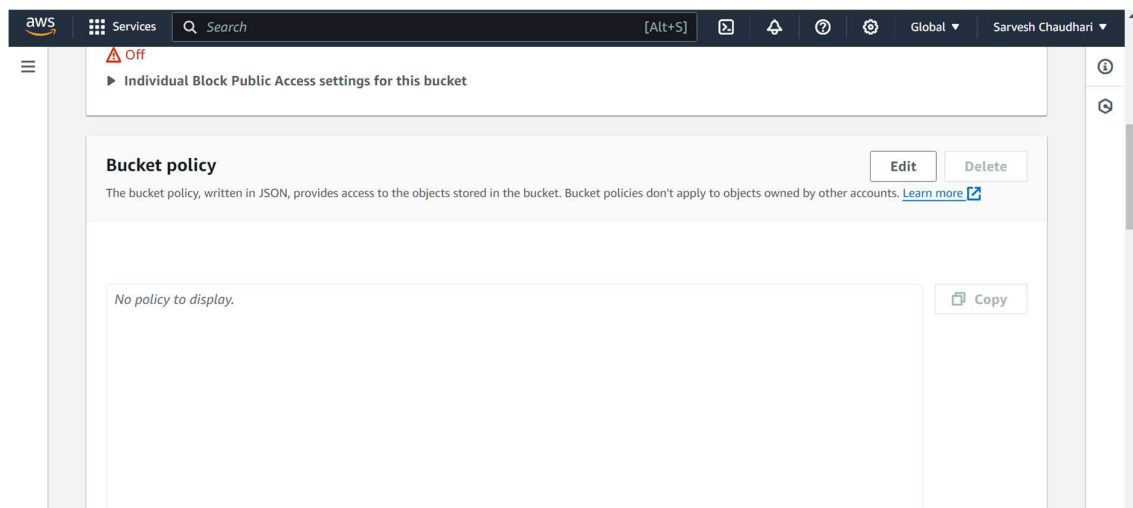


Select the time for this link is active then click on create

- Now to allow the public access permission go to permission > Block Public access > edit > Untick the box



Now we have allowed public access but our policies are not assigned to access publicly. Now scroll down and go to Bucket Policy > edit



Now create policy using Policy Genrator

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 1 Action(s) Selected ☐ All Actions ("*")

Amazon Resource Name (ARN) arn:aws:s3:::bucket3712/*

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

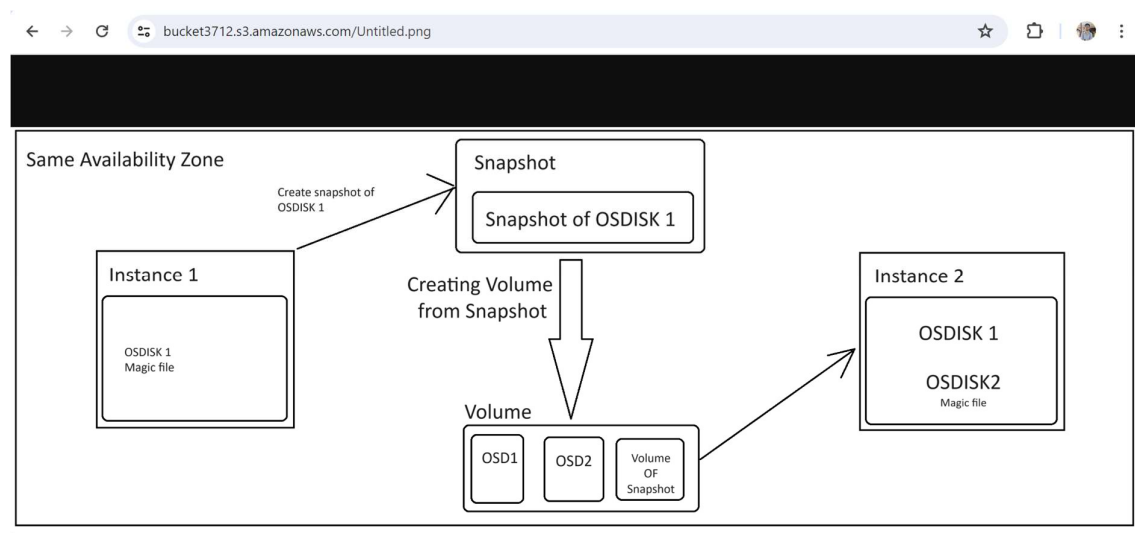
[Add Conditions \(Optional\)](#)

[Add Statement](#)

Now add Statement > Generate Policy

The screenshot shows the AWS IAM console interface. At the top, there's a navigation bar with the AWS logo, 'Services', a search bar, and user information 'Global Sarvesh Chaudhari'. Below the navigation bar, the breadcrumb trail shows 'arn:aws:s3:::bucket3712'. The main content area is titled 'Policy' and displays a JSON policy document. The policy has an ID 'Policy1708927247982', version '2012-10-17', and a single statement with Sid 'Stet1708927246294', Action 's3:GetObject', Effect 'Allow', Resource 'arn:aws:s3:::bucket3712/*', and Principal '*'. To the right of the JSON editor is a panel titled 'Edit statement' with the text 'Select a statement' and 'Select an existing statement in the policy or add a new statement.', along with a '+ Add new statement' button.

Now save changes.

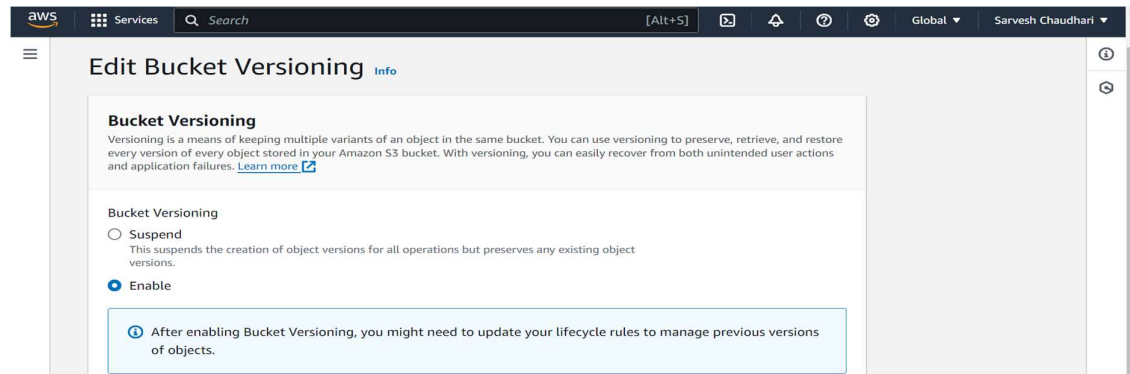


As we give permission here we can see that within the link we can access content.

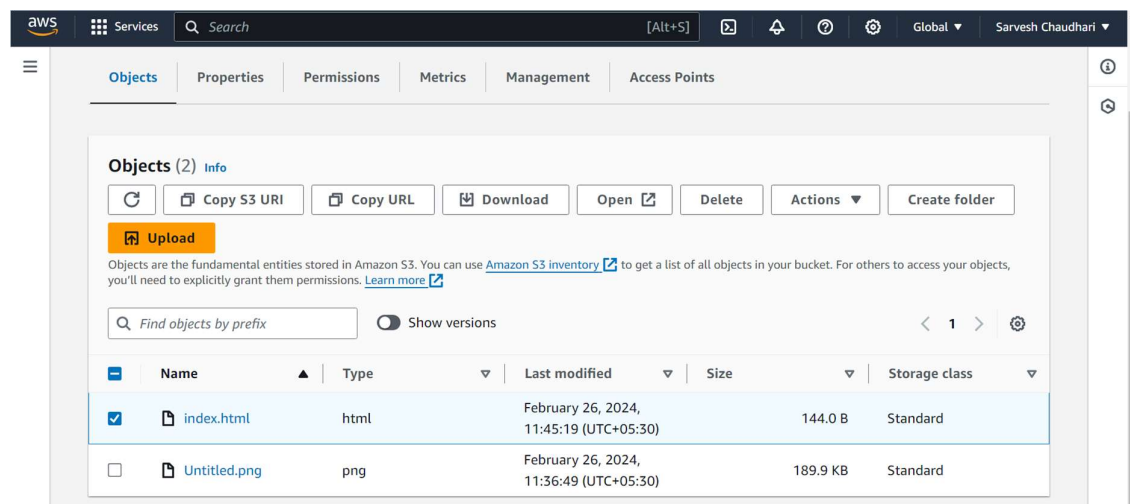
- Now let's see how versioning works

Now go to properties > Bucket Versioning >

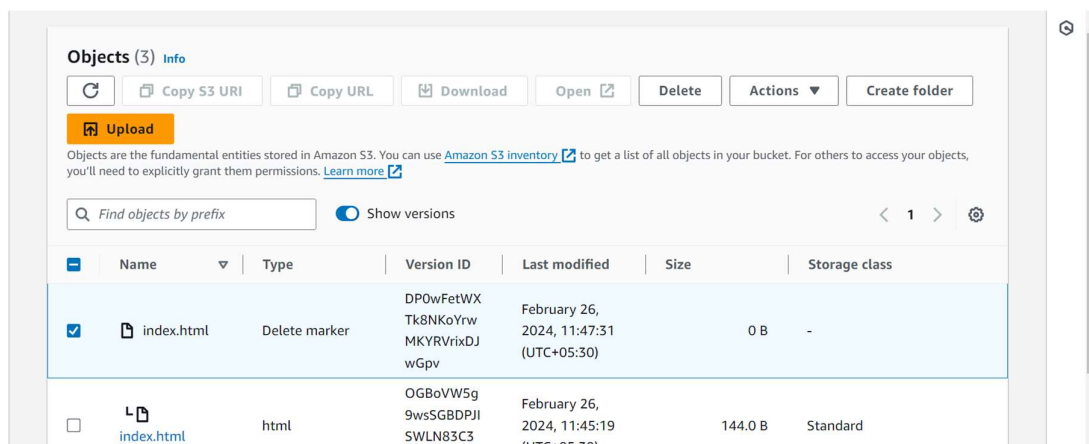
Now select the file go to permissions scroll down and edit Static Website Hosting.



Now upload Hello World file Index.html



Now delete file. The deleted file is visible in show versions as Delete Marker



When we delete this delete marker type file we will retrieve this document from the versions

- Website hosting

The screenshot shows the 'Edit static website hosting' page in the AWS Management Console. The page has a dark header with the AWS logo, 'Services' menu, a search bar, and user information 'Sarvesh Chaudhari'. The main content area is titled 'Edit static website hosting' with an 'Info' link. Below the title, there's a section 'Static website hosting' with a description and a 'Learn more' link. The 'Static website hosting' section has two radio buttons: 'Disable' and 'Enable', with 'Enable' selected. The 'Hosting type' section has two radio buttons: 'Host a static website' (selected) and 'Redirect requests for an object'. Below these, there's a blue information box stating: 'For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access'. The bottom section is 'Index document', where 'index.html' is entered in a text field. Below that is 'Error document - optional' with 'error.html' entered. The 'Redirection rules - optional' section is partially visible at the bottom.

- Bucket replication

Create another bucket

The screenshot shows the 'Create bucket' page in the AWS Management Console. The page has a dark header with the AWS logo, 'Services' menu, a search bar, and user information 'Sarvesh Chaudhari'. The main content area is titled 'Create bucket' with an 'Info' link. Below the title, there's a section 'General configuration'. The 'AWS Region' is set to 'US East (N. Virginia) us-east-1'. The 'Bucket type' section has two radio buttons: 'General purpose' (selected) and 'Directory - New'. The 'General purpose' option is highlighted with a blue box and contains the text: '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.' The 'Directory - New' option is highlighted with a blue box and contains the text: '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.' The 'Bucket name' field is filled with 'bucket1109'.

aws

Services

Search

[Alt+S]

Global

Sarvesh Chaudhari

Amazon S3 > Buckets > bucket372119

bucket372119

Objects | Properties | Permissions | Metrics | Management | Access Points

Lifecycle rules

View details | Edit | Delete | Actions | Create lifecycle rule

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. [Learn more](#)

Lifecycle ru...

Status

Scope

Current ver...

Noncurrent ...

Expired obj...

Incomplete ...

No lifecycle rules

There are no lifecycle rules for this bucket.

Create lifecycle rule

Replication rules (0)

View details | Edit rule | Delete | Actions | Create replication rule

Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more. [Learn more](#)

Replication rule name

Status

Destination bucket

Destination Region

Priority

Scope

Storage class

Replica owner

Replication Time Control

No replication rules

You don't have any rules in the replication configuration.

Create replication rule

aws

Services

Search

[Alt+S]

Global

Sarvesh Chaudhari

Amazon S3 > Buckets > bucket372119 > Replication rules > Create replication rule

Create replication rule

Replication rule configuration

Replication rule name

Replication1

Up to 255 characters. In order to be able to use CloudWatch metrics to monitor the progress of your replication rule, the replication rule name must only contain English characters.

Status

Choose whether the rule will be enabled or disabled when created.

☒ Enabled

☐ Disabled

Priority

The priority value resolves conflicts that occur when an object is eligible for replication under multiple rules to the same destination. The rule is added to the configuration at the highest priority and the priority can be changed on the replication rules table.

aws Services Search [Alt+S] Global Sarvesh Chaudhari

Source bucket

Source bucket name
bucket372119

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

Choose a rule scope

- ☐ Limit the scope of this rule using one or more filters
- ☒ Apply to all objects in the bucket

Destination

Destination

You can replicate objects across buckets in different AWS Regions (Cross-Region Replication) or you can replicate objects across buckets in the same AWS Region (Same-Region Replication). You can also specify a different bucket for each rule in the configuration. [Learn more](#) or see [Amazon S3 pricing](#)

Choose a bucket in this account

- ☒ Choose a bucket in this account
- ☐ Specify a bucket in another account

Bucket name

Choose the bucket that will receive replicated objects.

bucket3702 Browse S3

IAM role

Choose a role

- ☒ Create new role
- ☐ Choose from existing IAM roles
- ☐ Enter IAM role ARN

Then save

ation aren't displayed, choose the refresh button. Changes apply only to new objects. To
with this configuration, choose **Create replication job**.

Replicate existing objects?

You can enable a one-time Batch Operations job from this replication configuration to replicate objects that already exist in the bucket and to synchronize the source and destination buckets. [Learn more](#) or [see pricing](#)

Existing objects

- ☒ No, do not replicate existing objects.
- ☐ Yes, replicate existing objects.

Cancel Submit

Now upload file to bucket 3702 it will appear in bucket372119

aws

Services

Search

[Alt+S]

Global

Sarvesh Chaudhari

bucket372119

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (1)

Info

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

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](#)

Find objects by prefix

Show versions

< 1 >

	Name	Type	Last modified	Size	Storage class
	b12.pem	pem	February 27, 2024, 12:07:16 (UTC+05:30)	1.6 KB	Standard