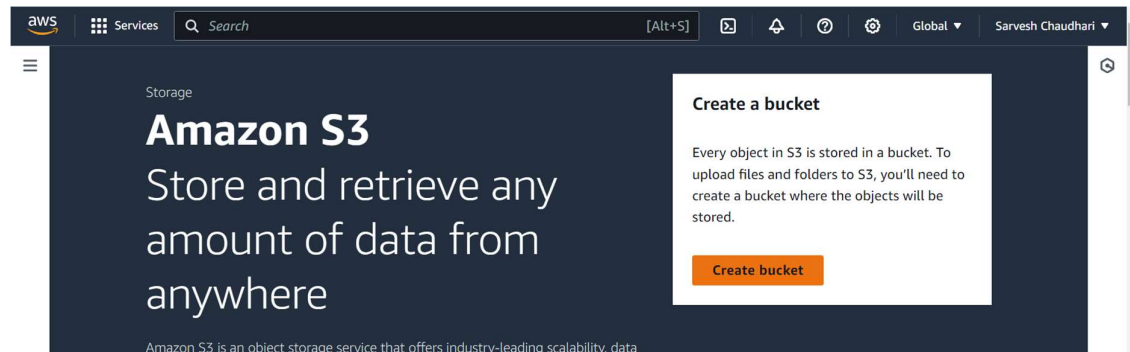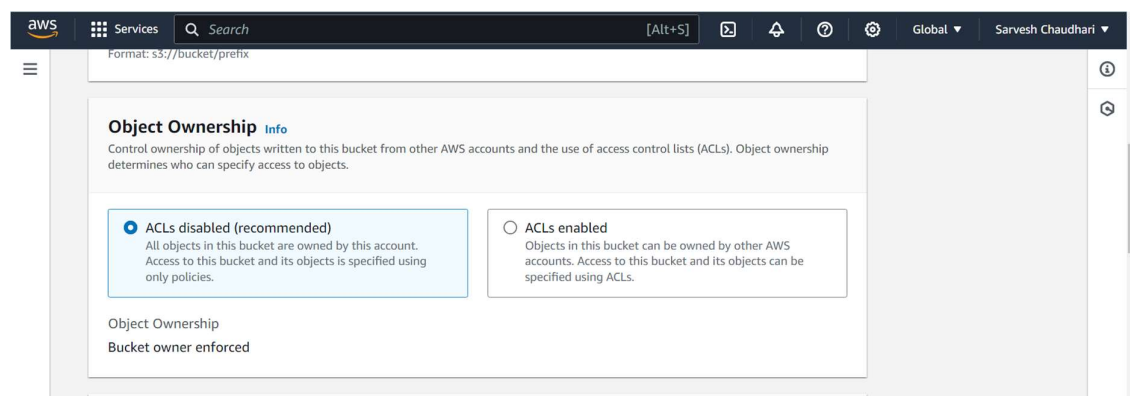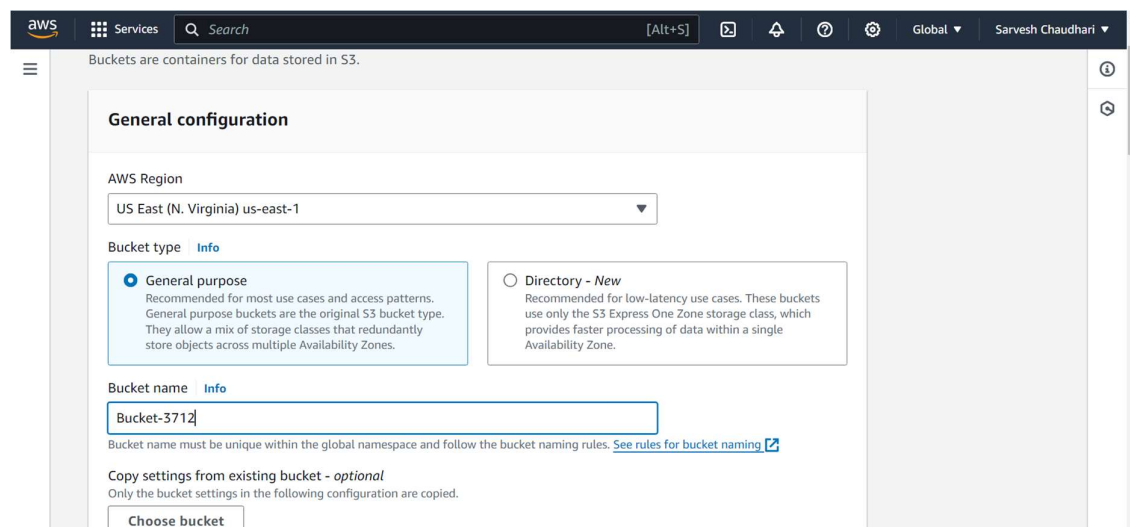# Objective :- Understanding S3 Buckets and its use

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

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

⊘ **Successfully created bucket "bucket3712"**
To upload files and folders, or to configure additional bucket settings, choose **View details**.

[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   [⟳] [⧉ Copy ARN] [Empty] [Delete] [**Create bucket**]

Buckets are containers for data stored in S3.

[Q Find buckets by name]   ‹ 1 › ⚙

	Name ▲	AWS Region ▽	Access ▽	Creation date ▽
○	bucket3712	US East (N. Virginia) us-east-1	Bucket and objects not public	February 26, 2024, 11:12:57 (UTC+05:30)

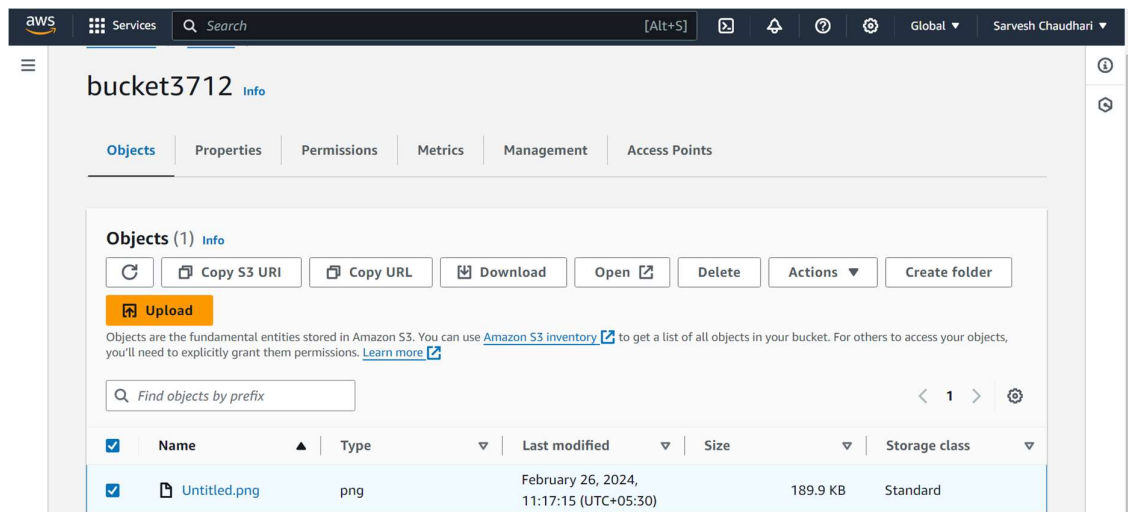Now click on bucket name to enter into bucket

To upload file in bucket click on Upload files
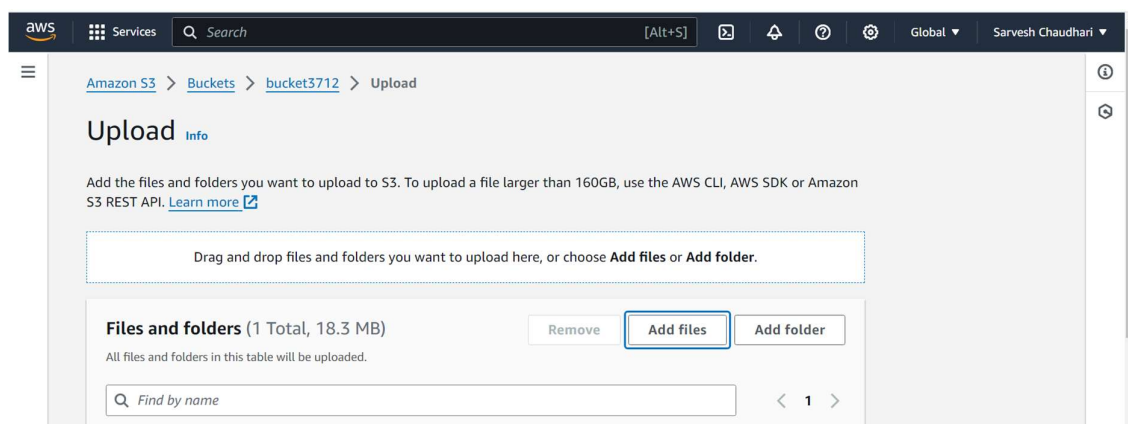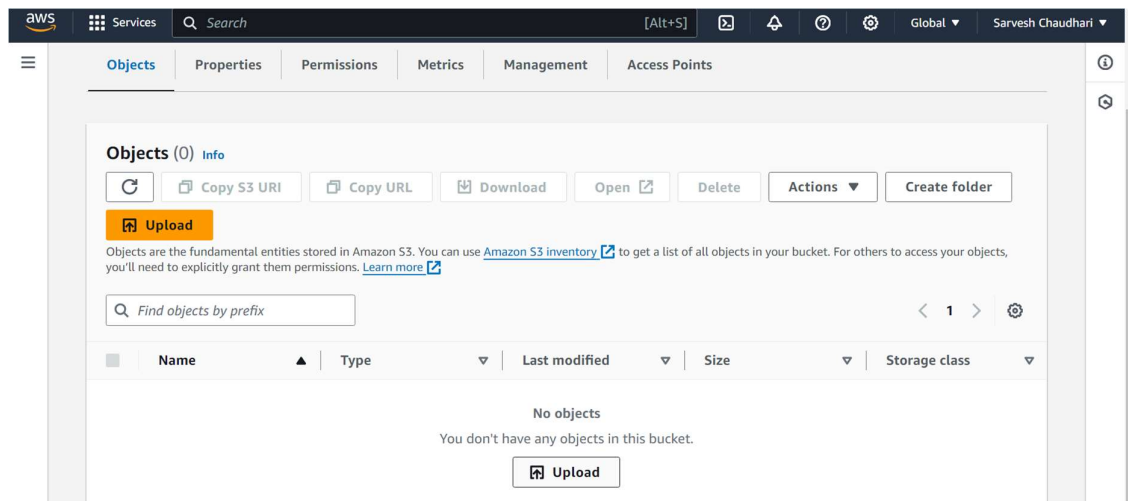
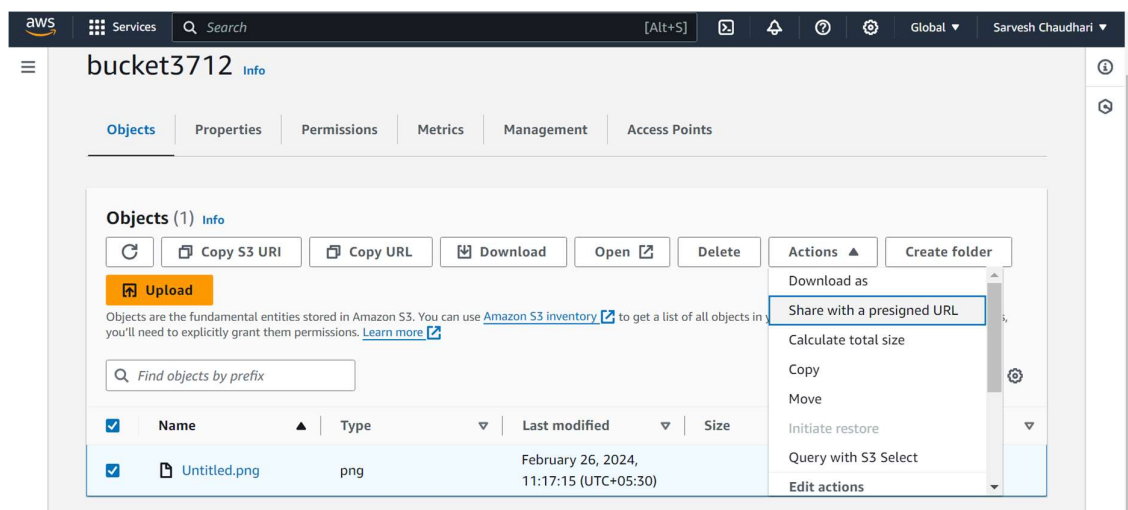Select file then Scroll down and click on upload
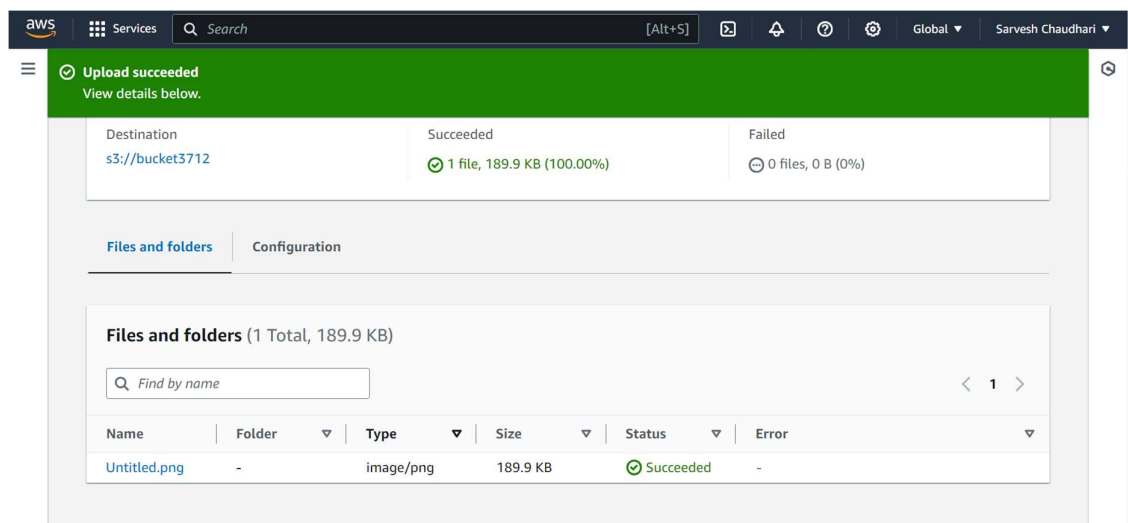

File uploaded successfully

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'
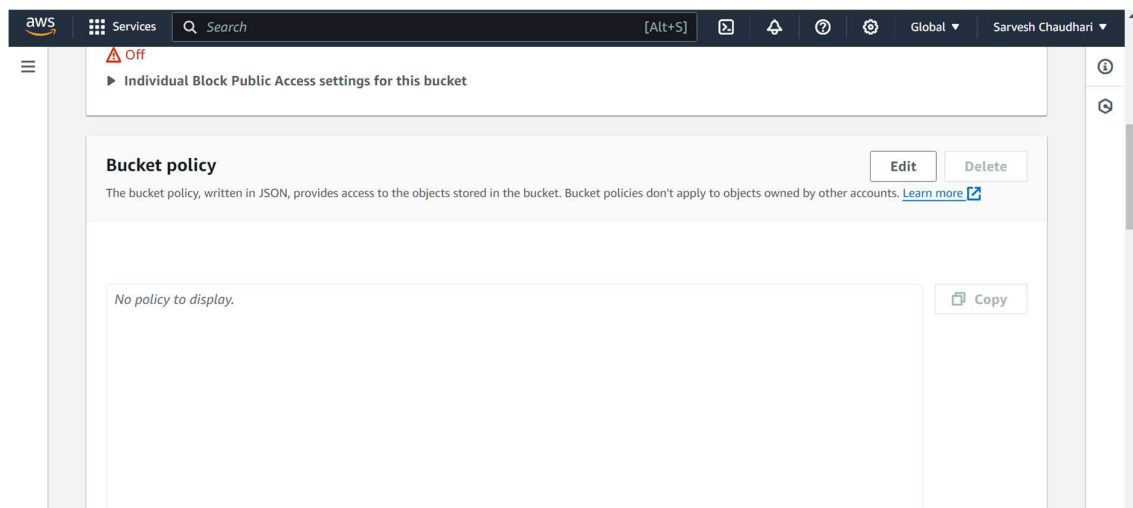

Select the time for this link is active then click on create

- Now to allow the public access permission go to permission > Block Public access > edit > Untick the box
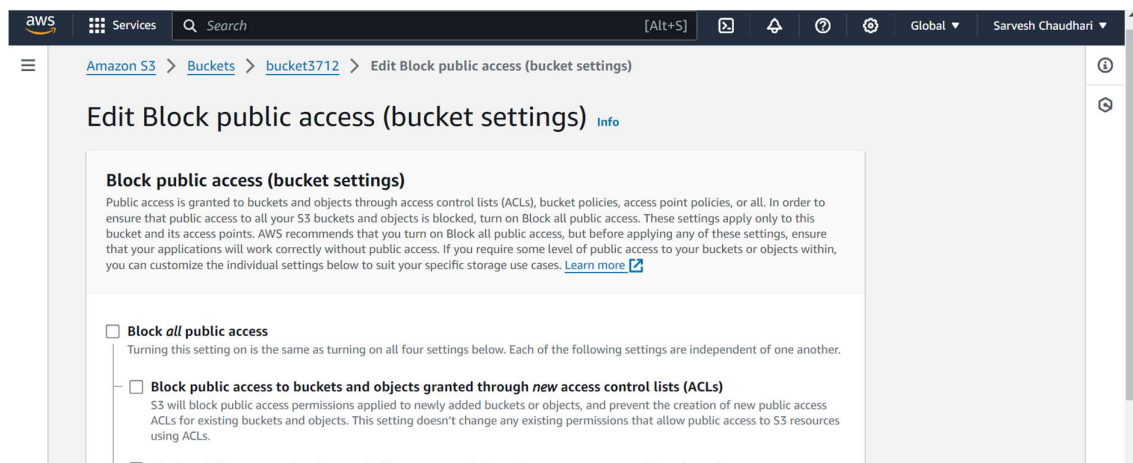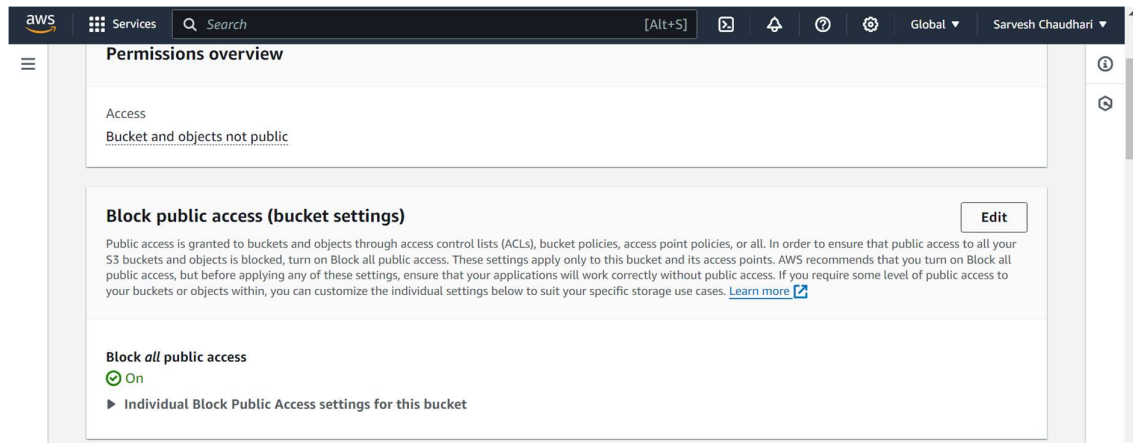
Now we have allowed public access but our policies are not assigned to access publicaly. Now scroll down and go to Bucket Policy > edit

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}.
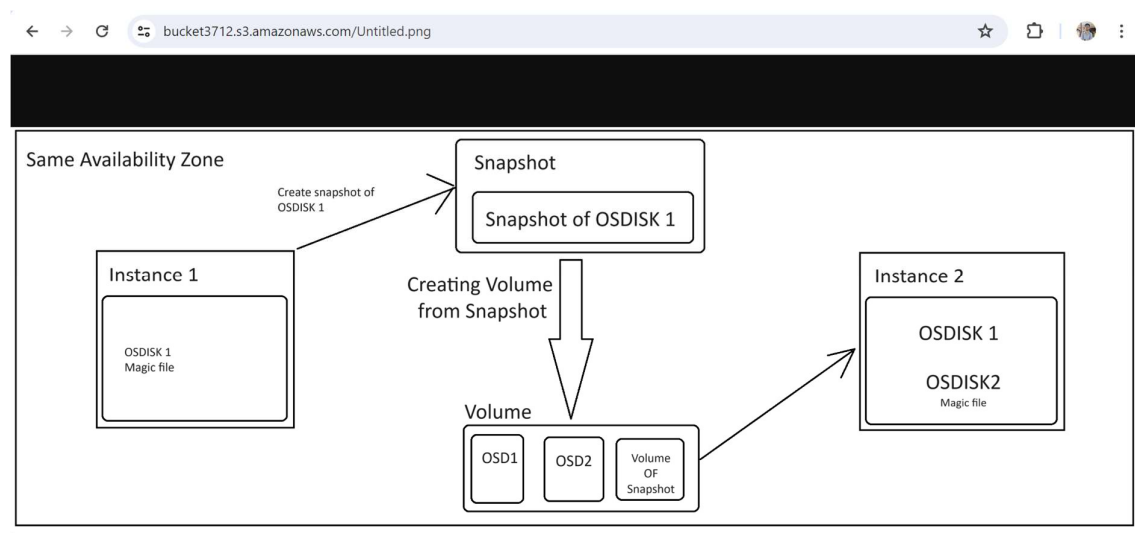Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement
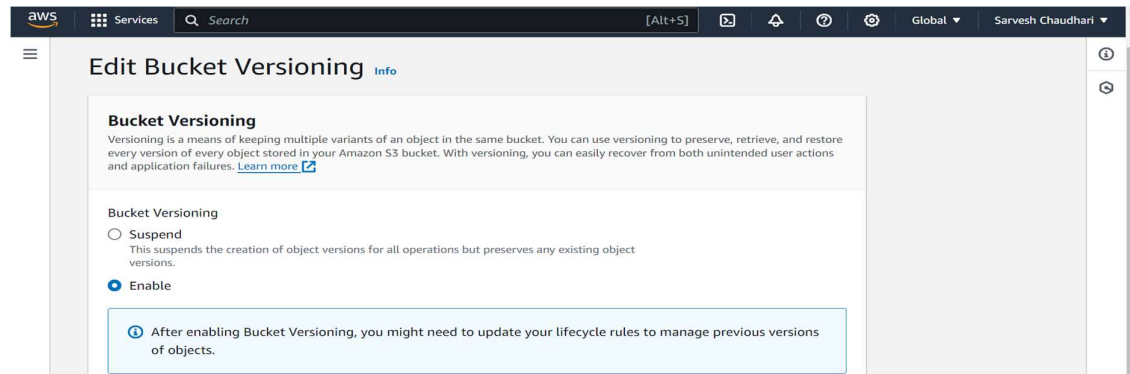
Now add Statement > Generate Policy

Now save changes.

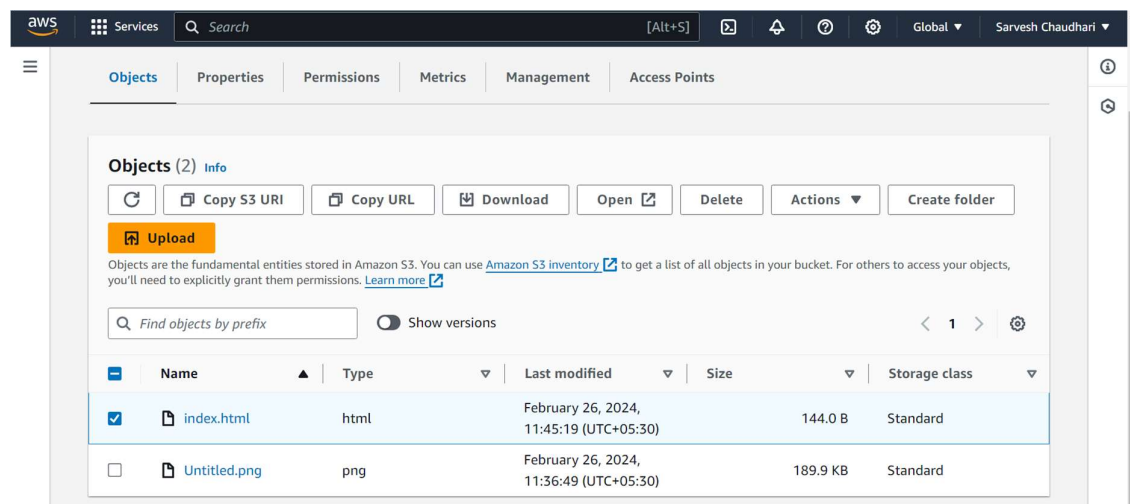As we give permission here we can see that within the link we can access content.

- Now lets see how versioning work
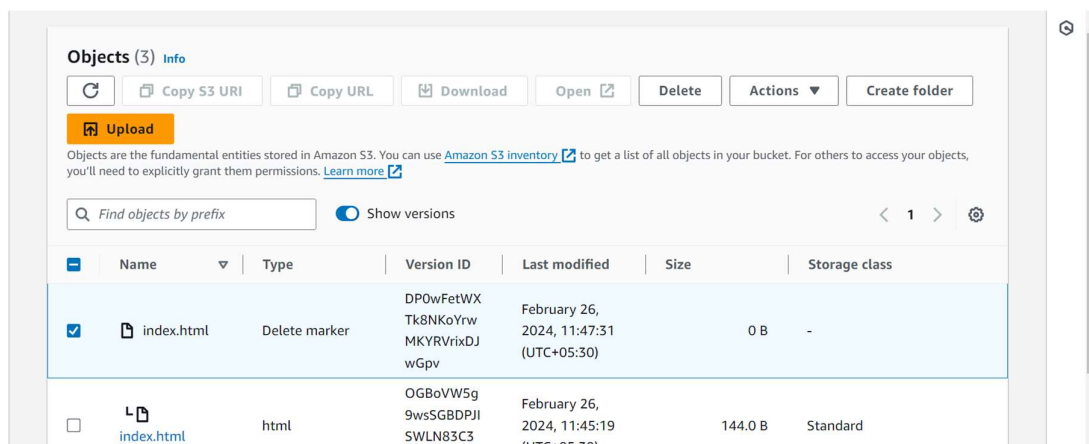
Now go to properties > Bucket Versioning >

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

- Bucket replication

Create another bucket

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

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

Create replication rule   Info

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.

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
○ Specify a bucket in another account

Bucket name
Choose the bucket that will receive replicated objects.

| bucket3702 | | Browse S3 |

IAM role

● Create new role
○ Choose from existing IAM roles
○ Enter IAM role ARN

Then save

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