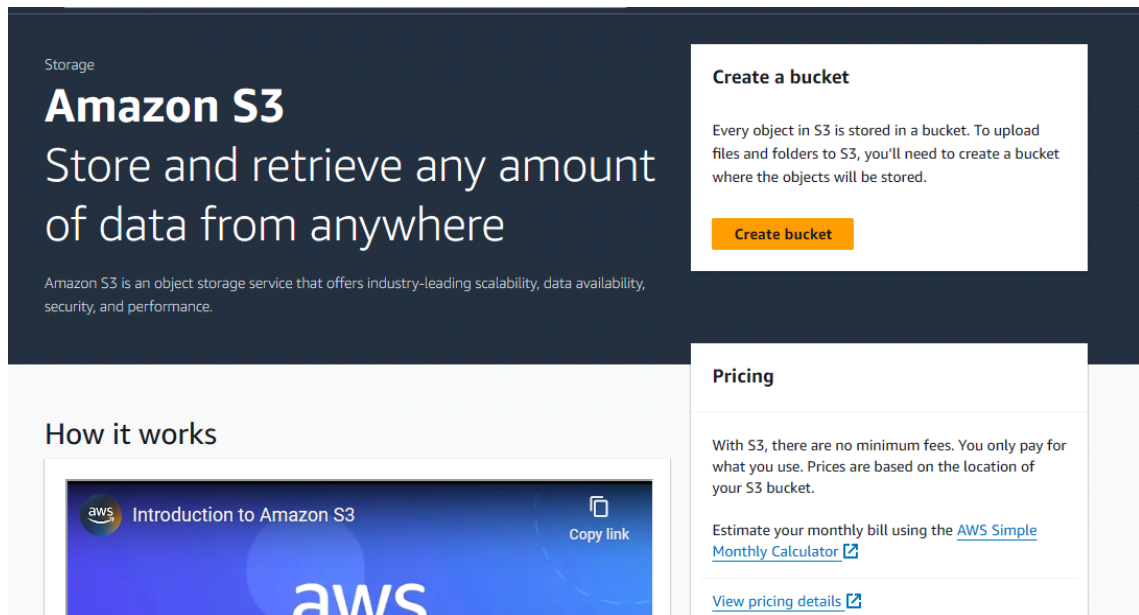


TASK 1: Create an S3 Bucket:

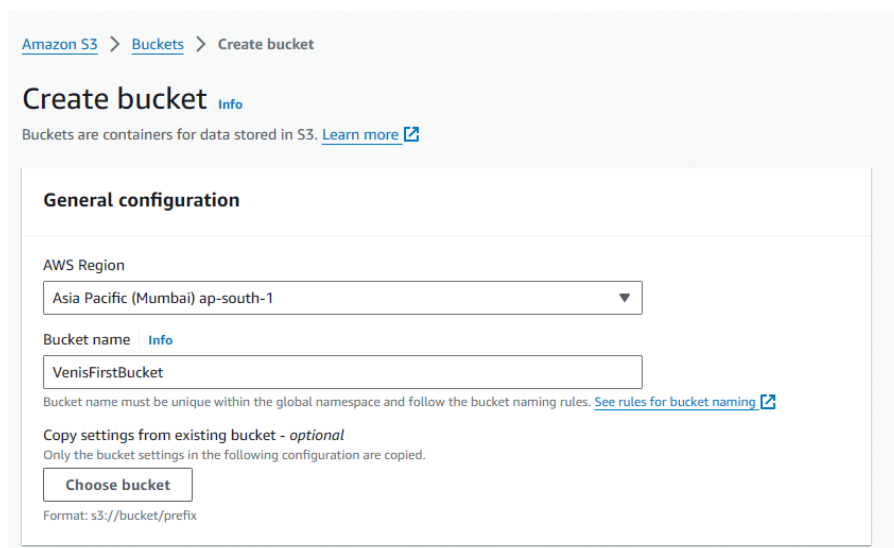
1.1 Steps to create S3 Bucket:

- In the Aws Cloud , search for S3 and select it .



The screenshot shows the Amazon S3 homepage. On the left, under the 'Storage' header, is the 'Amazon S3' logo and the text 'Store and retrieve any amount of data from anywhere'. Below this is a brief description of S3 as an object storage service. On the right, there is a 'Create a bucket' section with a description of buckets and a 'Create bucket' button. Below that is a 'Pricing' section explaining that there are no minimum fees and providing links to a monthly calculator and pricing details. At the bottom left, there is a 'How it works' section with a video player titled 'Introduction to Amazon S3' and a 'Copy link' button.

- Now click on “Create bucket”. Select the Nearest region so we'll select Mumbai(Asia pacific) , and give the bucket name as "VenisFirstBucket" .



The screenshot shows the 'Create bucket' form in the AWS console. The breadcrumb navigation at the top reads 'Amazon S3 > Buckets > Create bucket'. The main heading is 'Create bucket' with an 'Info' link. Below this is a sub-header 'General configuration'. The 'AWS Region' is set to 'Asia Pacific (Mumbai) ap-south-1'. The 'Bucket name' is 'VenisFirstBucket'. A note states that the bucket name must be unique and follows naming rules, with a link to 'See rules for bucket naming'. There is a section for 'Copy settings from existing bucket - optional' with a 'Choose bucket' button. At the bottom, the format 's3://bucket/prefix' is shown.

- Enable Bucket Versioning:

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.

Cancel

Create bucket

- Now we can see that our bucket has been created .

Successfully created bucket "venisassignments3bucket"

View details

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

Amazon S3 > Buckets

► Account snapshot

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

View Storage Lens dashboard

General purpose buckets

Directory buckets

General purpose buckets (1) [Info](#)

↻

Copy ARN

Empty

Delete

Create bucket

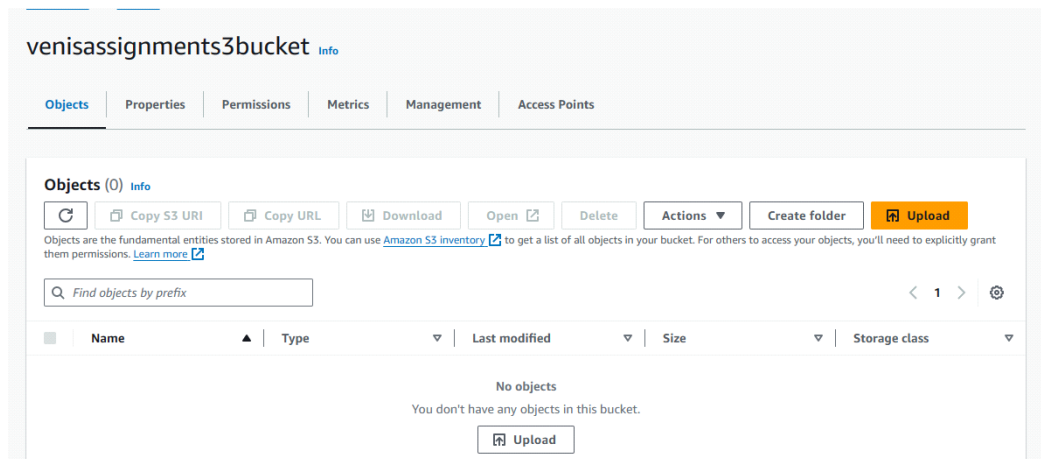
Find buckets by name

< 1 > ⓘ

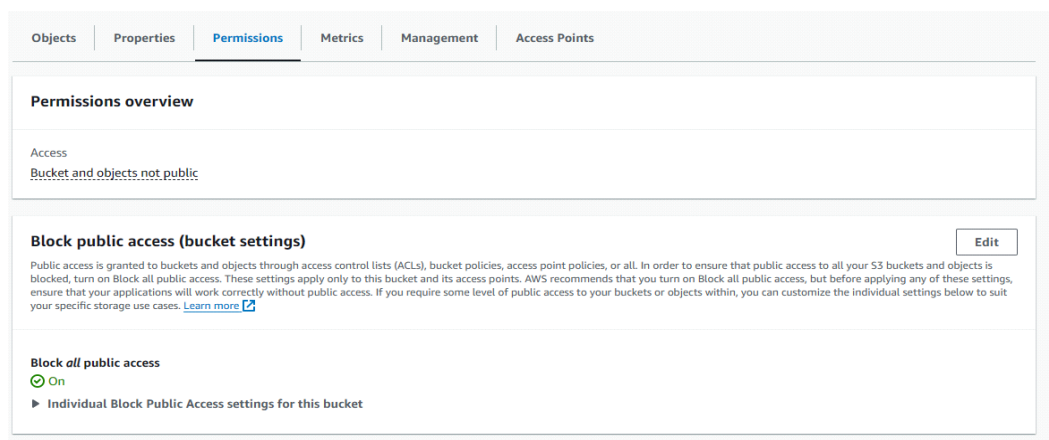
	Name	AWS Region	Access	Creation date
<input type="radio"/>	venisassignments3bucket	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	January 25, 2024, 17:05:50 (UTC+05:30)

Steps to edit public access :

- Select the venisassignments3bucket .



- Now we can see the Permissions section . So Now click on Edit .



- Now untick all the checkboxes and write confirm to confirm the changes .

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.

Cancel

Save changes

Edit Block public access (bucket settings) ×



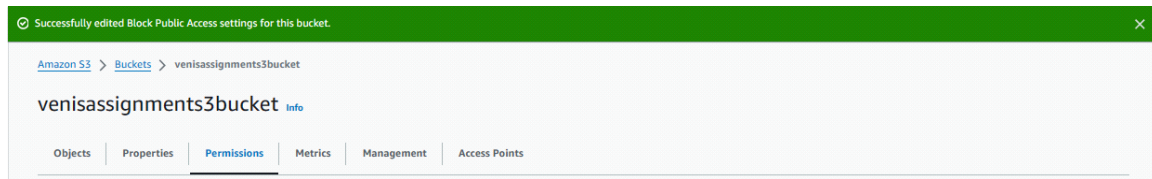
Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, enter *confirm* in the field.

Cancel

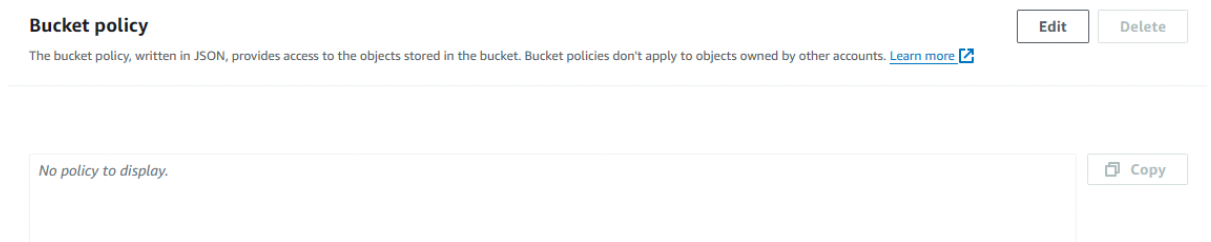
Confirm

- Now we can see the confirmation of the saved changes .

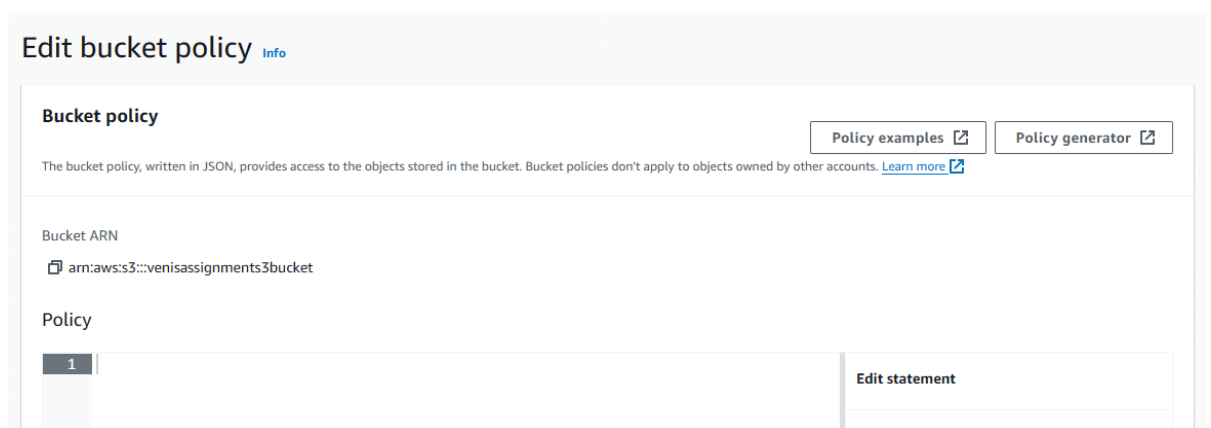


2.1 To configure bucket policies to control permissions:

- Click on edit inside Bucket policy tab.



- Inside edit mode click on policy generator.



- Policy generator provides gui for creating policies. Now select type of policy “S3 Bucket Policy”.

choose effect: “allow”, Principal: “*”, Actions: “GetObject”, Amazon Resource Name (ARN): “arn:aws:s3:::venisassignments3bucket/*”. Then click on Add Statement and click on generate 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}/{Key*}.

Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement

Activate Window:
Go to Settings to activate

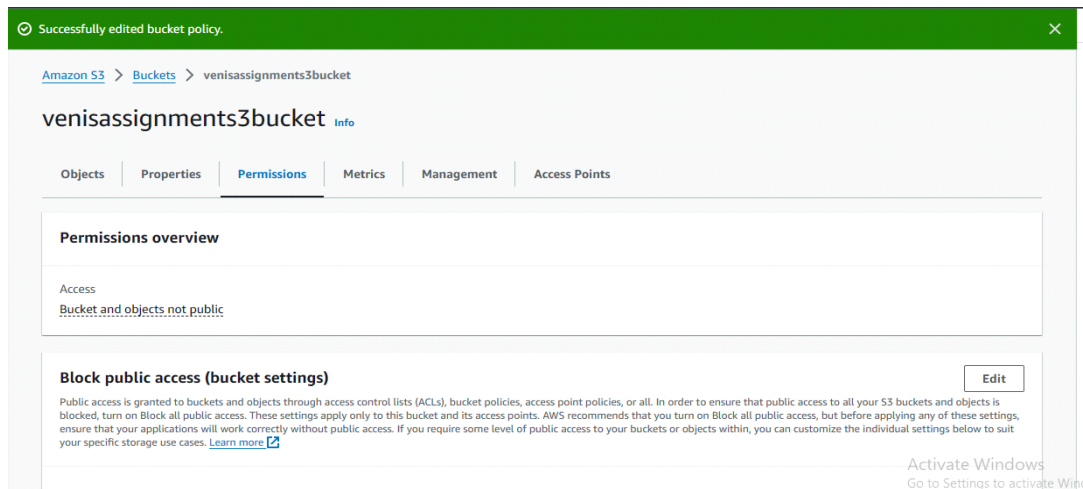
- Now Copy the json text and paste it in the Edit bucket policy page, then click on Save Changes.

Policy

```

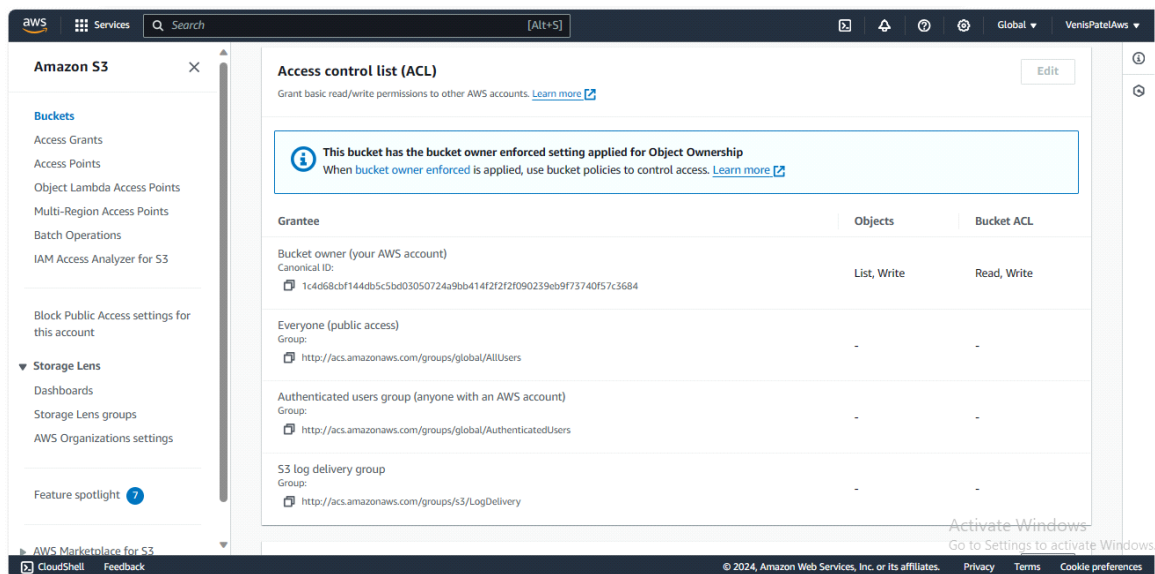
1  {
2    "Id": "Policy1706183752668",
3    "Version": "2012-10-17",
4    "Statement": [
5      {
6        "Sid": "Stmt1706183719037",
7        "Action": [
8          "s3:GetObject"
9        ],
10       "Effect": "Allow",
11       "Resource": "arn:aws:s3:::venisassignments3bucket/*",
12       "Principal": "*"
13     }
14   ]
15 }
```

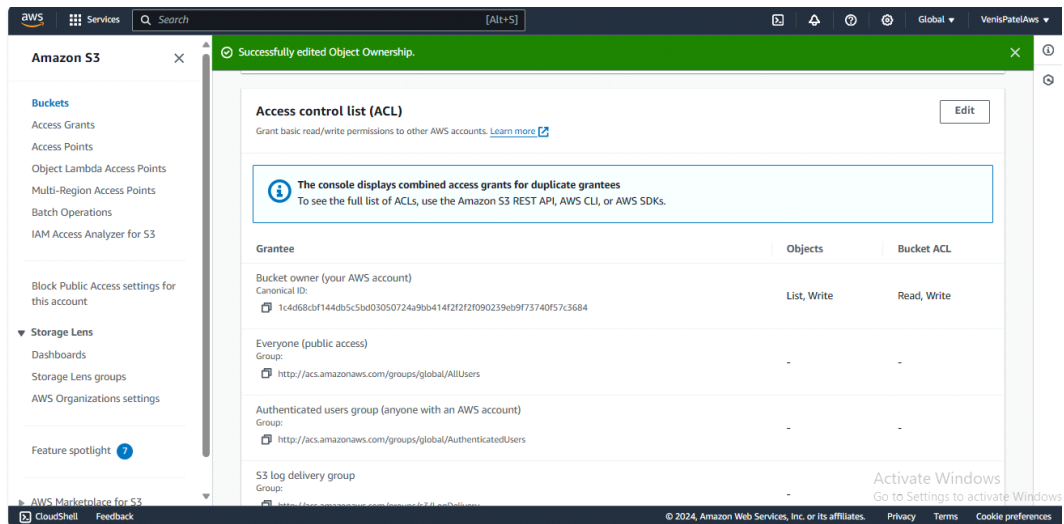
- Now we can see the changes here



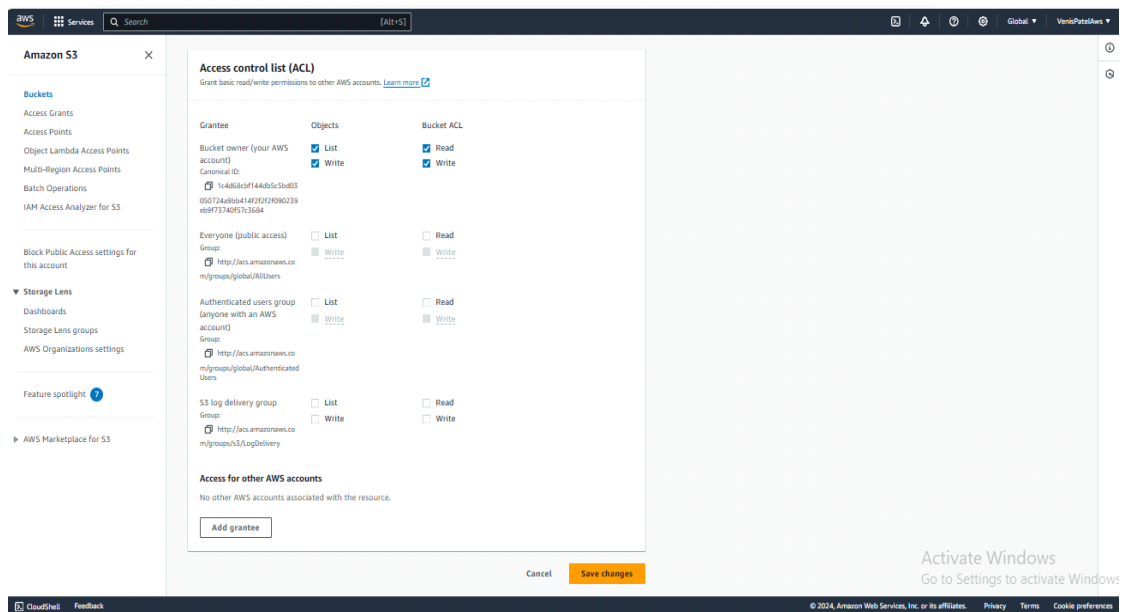
2.2 To configure access control lists (ACLs) to control permissions:

- Scroll Down in Permission of s3 bucket find Access Control List and click on edit.





- Now configure access control list to control list, read, write permission about objects and Bucket ACL. After configuring ACL click on “Save changes”.



3.Enable the versioning of your S3 bucket .

- Go to bucket versioning and then Enable bucket versioning and then save that changes and we can see those changes .

Bucket Versioning Edit

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
Disabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

Edit Bucket Versioning Info

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

☐ Suspend
This suspends the creation of object versions for all operations but preserves any existing object versions.

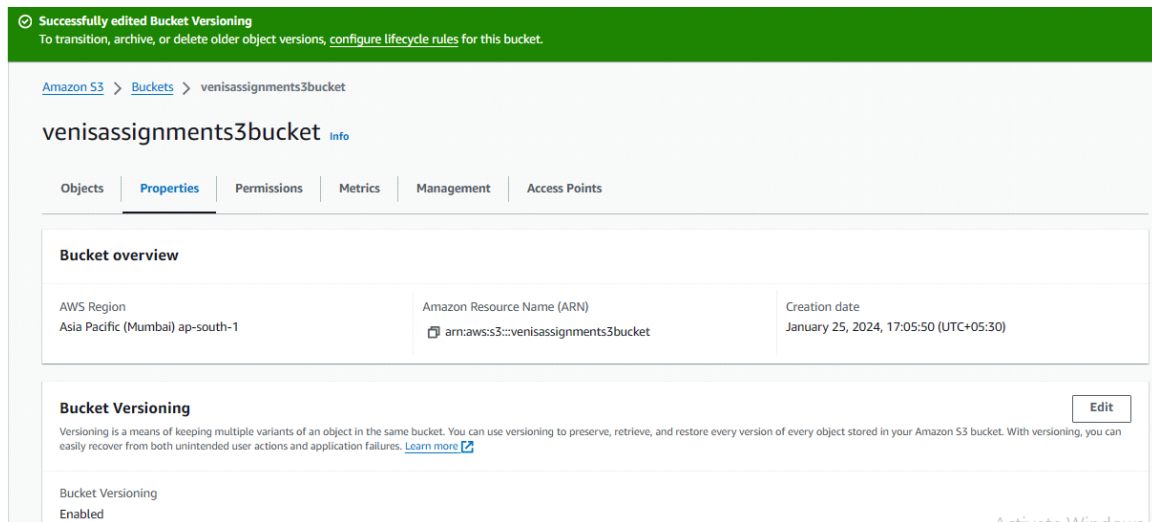
☒ **Enable**

i After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.

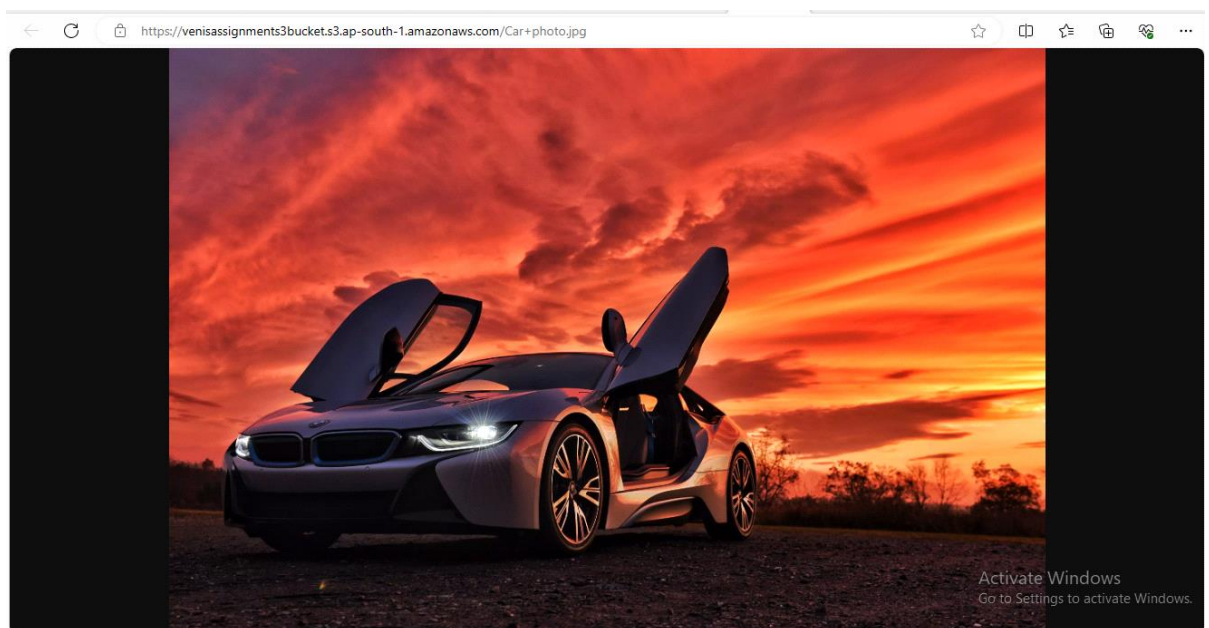
Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

Cancel Save changes



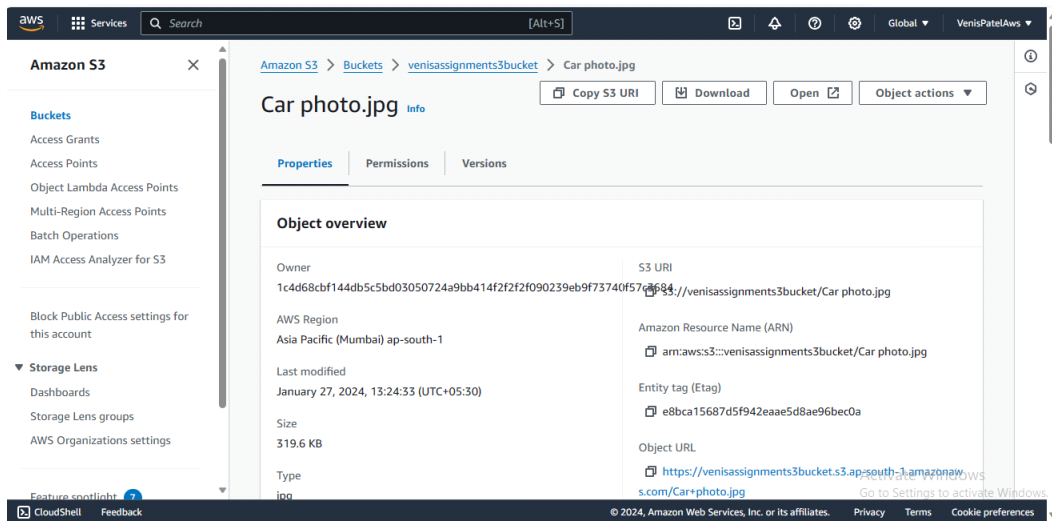
Check if s3 object is accessible:



4. Upload, modify, and delete objects to observe versioning in action:

Uploading Image:

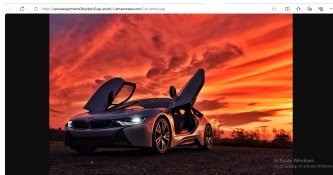
In venisassignments3bucket click on upload and then click on add file and select Car photo.jpg to upload it to s3 bucket. This created a new version id which is visible in the image.



Modifying Image:

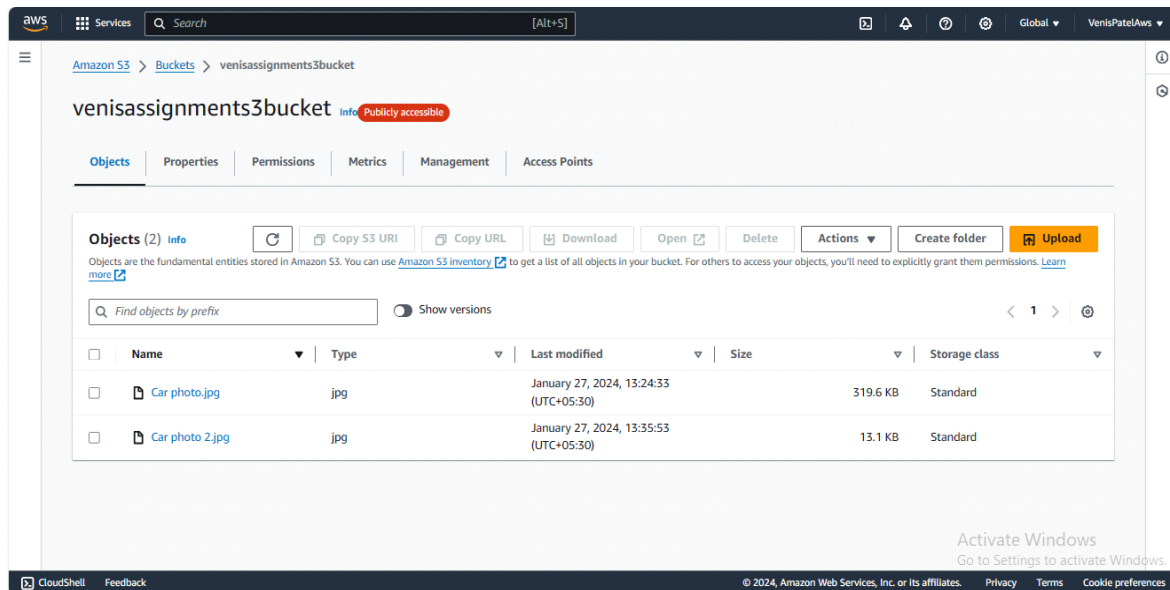
Click on upload in assignment-s3-bucket-jainil and click on add file then select another digital_camera.jpg to replace existing image.

Existing Image:



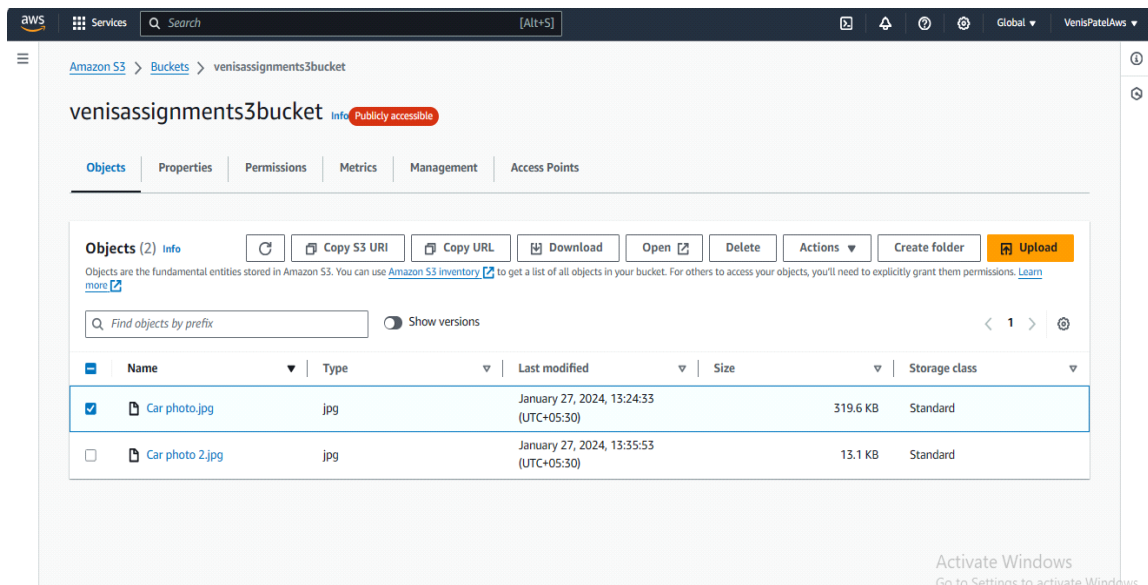
Modified Image:





Delete:

To delete a s3 object select that object and click on delete. Now confirm the deletion by writing delete and click on Delete object.



Here we can see that after deleting the image , we still have the older version .

