

## **S3** **SIMPLE STORAGE SERVICE**

- ▶ Amazon S3 is an object storage service that stores data as objects within buckets.
- ▶ An object is a file and any metadata that describes the file.
- ▶ A bucket is a container for objects. To store your data in Amazon S3, you first create a bucket and specify a bucket name and AWS Region.

- ❖ S3=Store+Process+Retrieve
- ❖ Free Tier Limit---->5GB

### **versioning**

S3 Object Versioning allows you to maintain multiple versions of an object. When you change the object, S3 creates a new version for you and stores it so you can revert to previous versions if required.

### **Delete marker**

Delete Markers are a feature of versioning-enabled S3 buckets.

When you delete an object in a versioning-enabled bucket, the object isn't deleted permanently. Instead, AWS creates a placeholder (or marker) for the object. This marker is referred to as the Delete Marker. This marker becomes the current version of the object. The Delete Marker makes AWS S3 behave as if the object has been deleted.

**Buckets---->root folder**

**Object ---->content**

## Bucket create:

Buckets--->create bucket--->bucket name(any)--->select region--->acl enabled

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight 3

AWS Marketplace for S3

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

seelanjaya23

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

Asia Pacific (Singapore) ap-southeast-1

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

Choose bucket

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.

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

Block Public Access settings for this bucket-----> remove tick block all public acces---->tick I acknowledge --->bucket versioning---->enable---->create bucket

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight 3

AWS Marketplace for S3

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.

 Turning off block all public access might result in this bucket and the objects within becoming public

AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Bucket Versioning

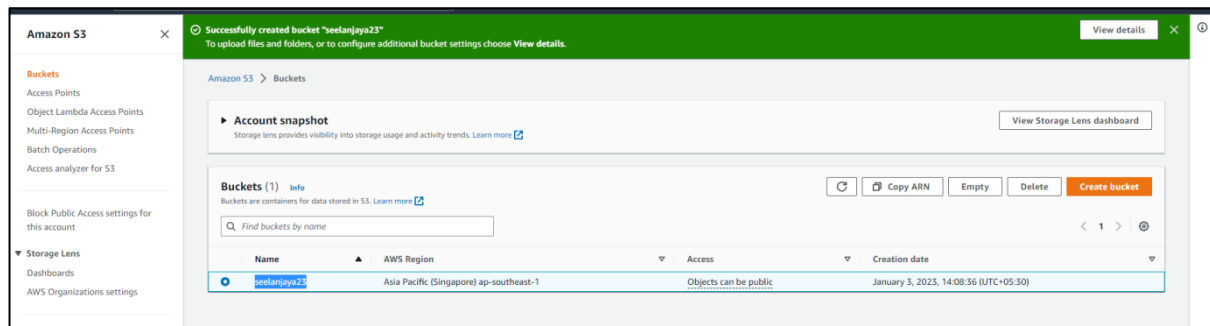
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures.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

Bucket Versioning

☐ Disable

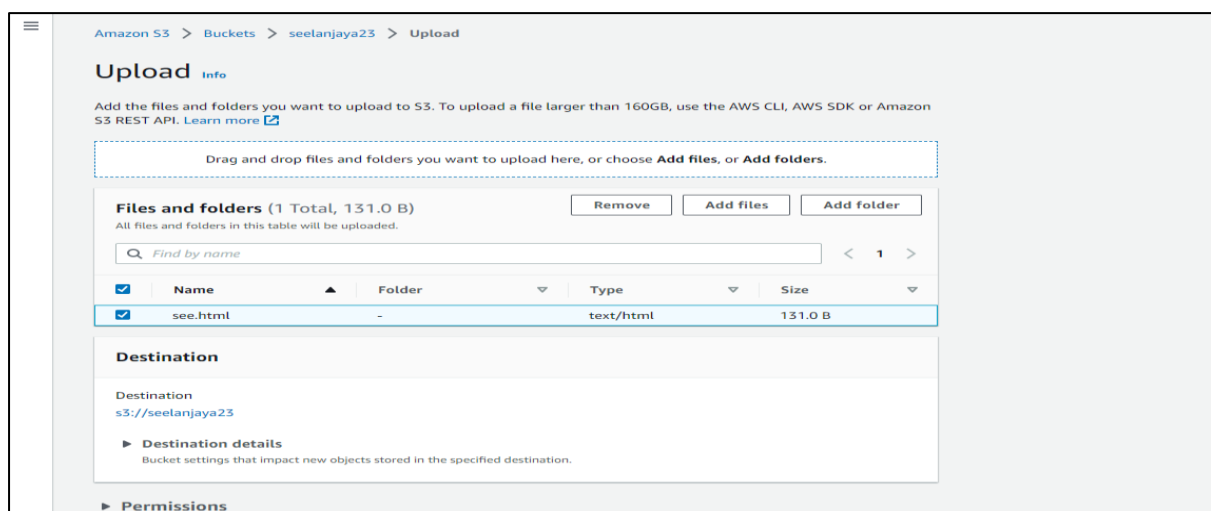
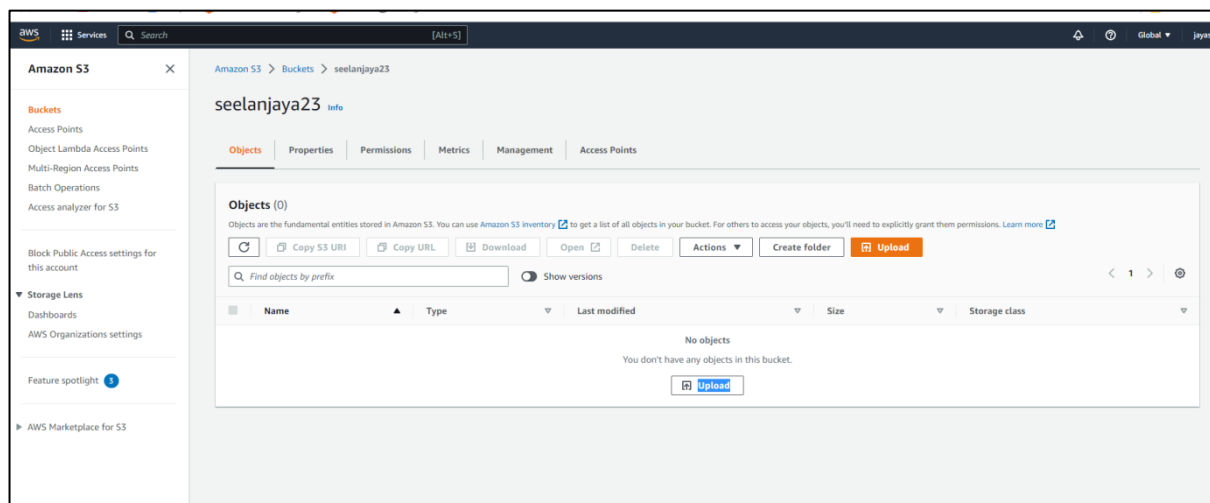
☒ Enable

Bucket created...



## Object create:

Select bucket---->upload--->add files(upload any file In html formte)



Permission--->grand public –read acces---->tick acknowledgement--->upload

▼ Permissions

Grant public access and access to other AWS accounts.

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

ⓘ AWS recommends using S3 bucket policies or IAM policies for access control. [Learn more](#)

Access control list (ACL)

☒ Choose from predefined ACLs

☐ Specify individual ACL permissions

Predefined ACLs

☐ Private (recommended)

Only the object owner will have read and write access.

☒ Grant public-read access

Anyone in the world will be able to access the specified objects. The object owner will have read and write access. [Learn more](#)

⚠ Granting public-read access is not recommended

Anyone in the world will be able to access the specified objects. [Learn more](#)

☒ I understand the risk of granting public-read access to the specified objects.

► Properties

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

Cancel

Upload

Object created.

Amazon S3

×

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

▼ Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

► AWS Marketplace for S3

Amazon S3 > Buckets > seelanjaya23

seelanjaya23

Info

Objects Properties Permissions Metrics Management Access Points

Objects (1)

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](#)

🔄

📄 Copy S3 URI

📄 Copy URL

📄 Download

📄 Open

🗑 Delete

⌵ Actions

Create folder

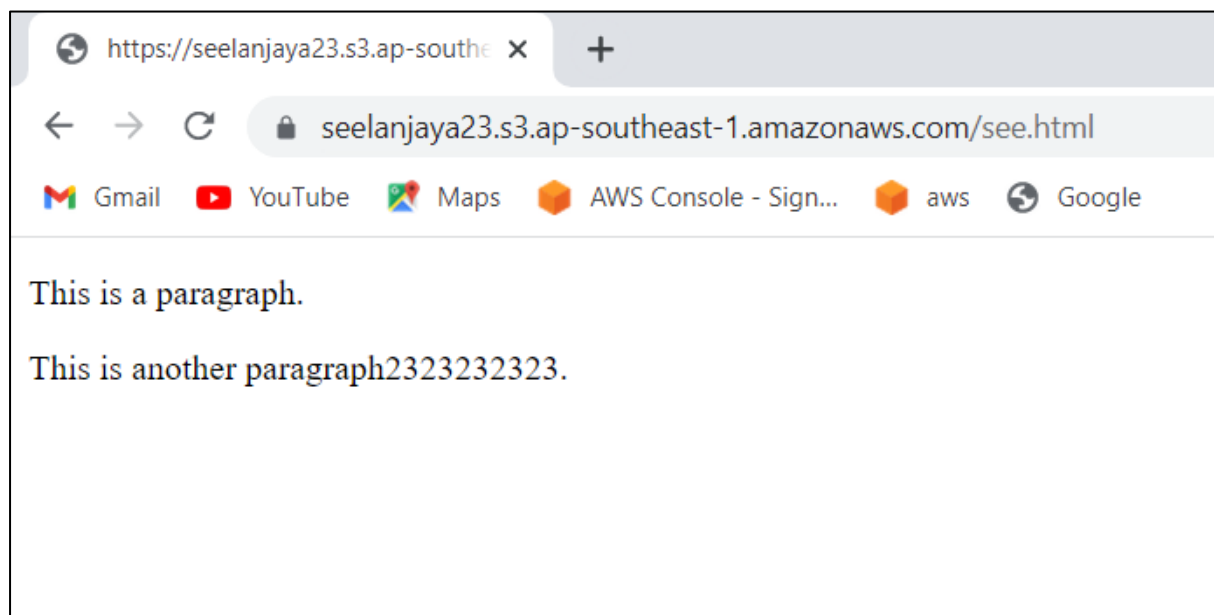
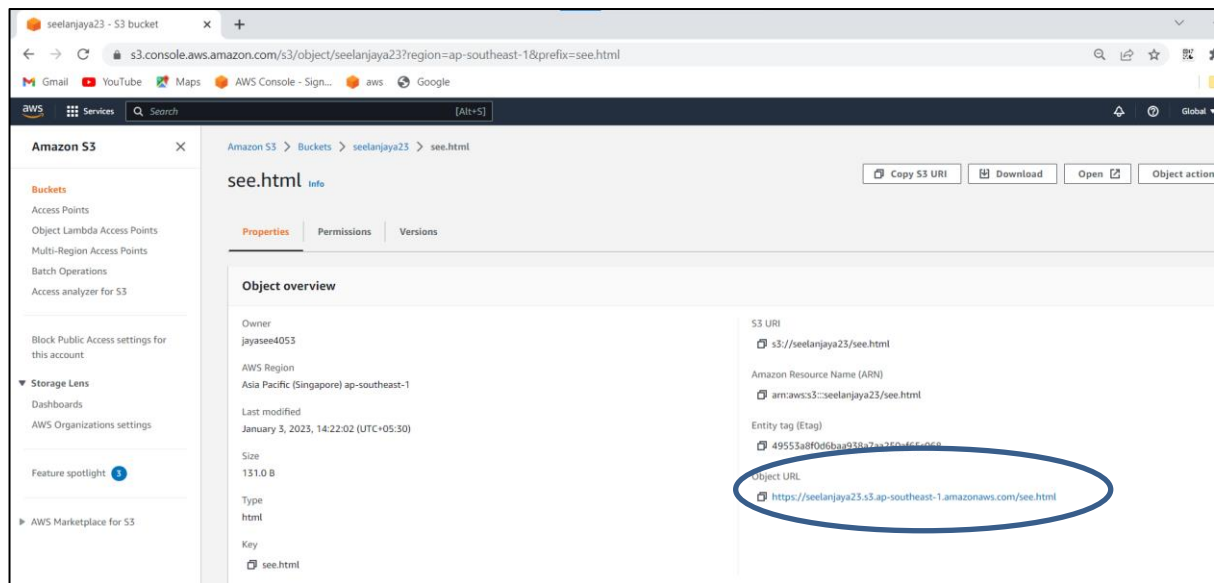
Upload

🔍 Find objects by prefix

Show versions

Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/> <a href="#">see.html</a>	html	January 3, 2023, 14:22:02 (UTC+05:30)	131.0 B	Standard

Click the object--->properties--->select url ---->put chrome(shown html page)



## Storage class types

Storage class	Designed for	Availability Zones	Min storage duration	Min billable object size	Monitoring and auto-tiering fees	Retrieval fees
Standard	Frequently accessed data (more than once a month) with milliseconds access	≥ 3	-	-	-	-
Intelligent-Tiering	Data with changing or unknown access patterns	≥ 3	-	-	Per-object fees apply for objects >= 128 KB	-
Standard-IA	Infrequently accessed data (once a month) with milliseconds access	≥ 3	30 days	128 KB	-	Per-GB fees apply
One Zone-IA	Recreateable, infrequently accessed data (once a month) stored in a single Availability Zone with milliseconds access	1	30 days	128 KB	-	Per-GB fees apply
Glacier Instant Retrieval	Long-lived archive data accessed once a quarter with instant retrieval in milliseconds	≥ 3	90 days	128 KB	-	Per-GB fees apply
Glacier Flexible Retrieval (formerly Glacier)	Long-lived archive data accessed once a year with retrieval of minutes to hours	≥ 3	90 days	-	-	Per-GB fees apply
Glacier Deep Archive	Long-lived archive data accessed less than once a year with retrieval of hours	≥ 3	180 days	-	-	Per-GB fees apply
Reduced redundancy	Noncritical, frequently accessed data with milliseconds access (not recommended as S3 Standard is more cost effective)	≥ 3	-	-	-	Per-GB

## versioning

Same html file select and edit content--->upload

Upload succeeded  
View details below.

Upload: status

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

Summary

Destination  
s3://seelanjaya23

Succeeded  
✔ 1 file, 121.0 B (100.00%)

Failed  
✖ 0 files, 0 B (0%)

Files and folders

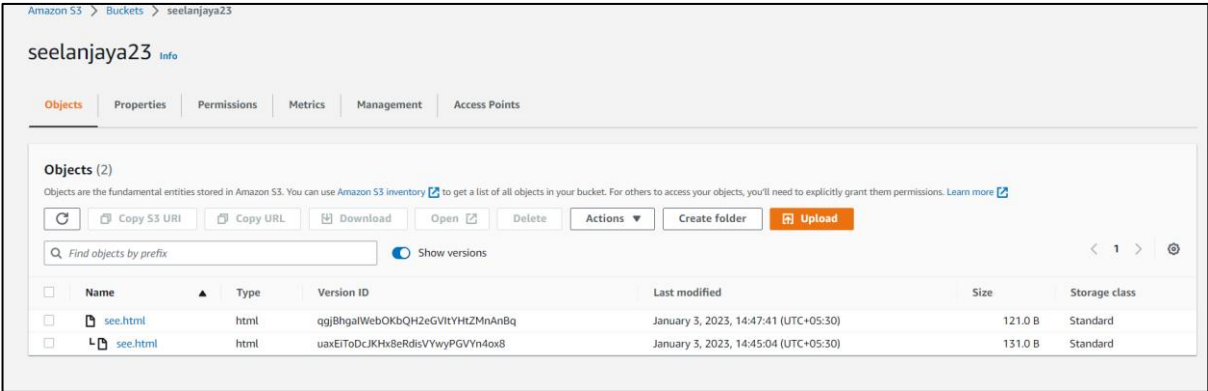
Configuration

Files and folders (1 Total, 121.0 B)

Find by name

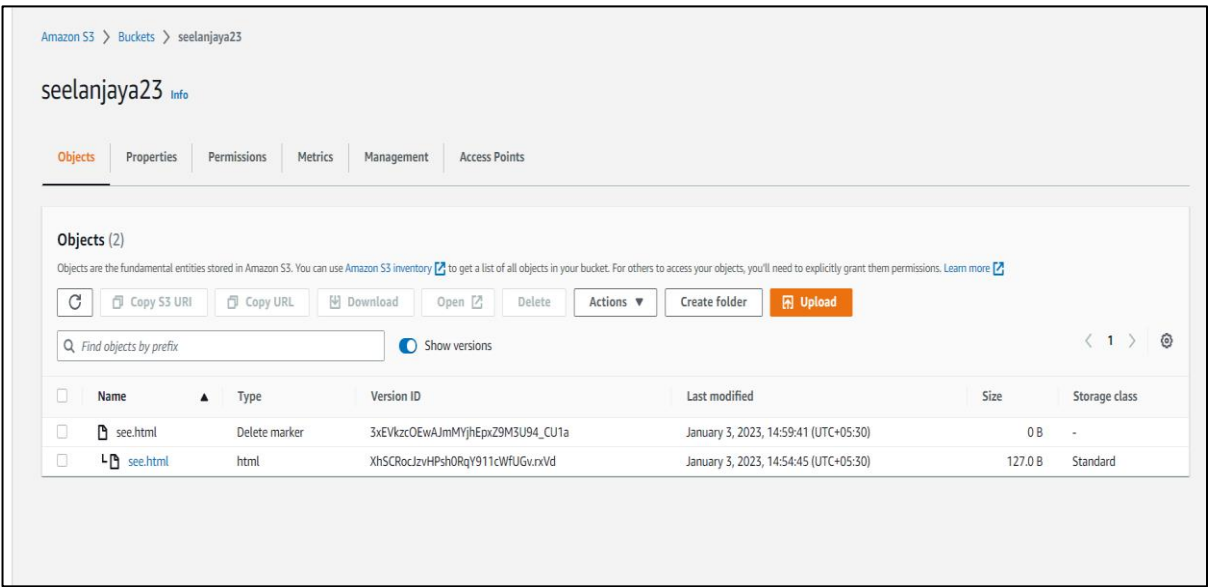
Name	Folder	Type	Size	Status	Error
see.html	-	text/html	121.0 B	✔ Succeeded	-

Now enable version click--->it will shown update file frst & old file down



**Delete marker**

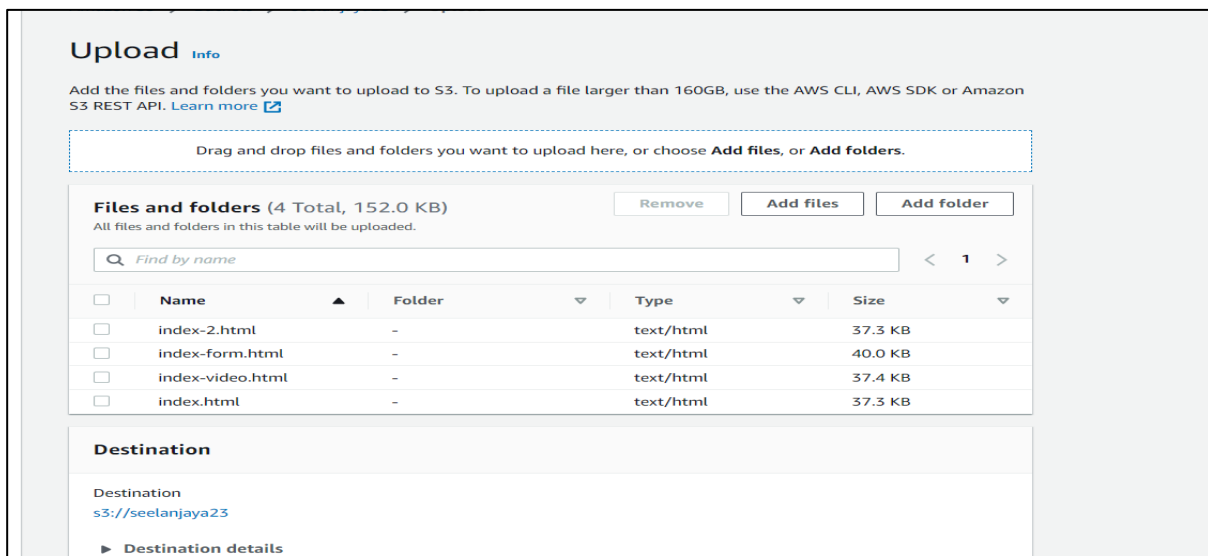
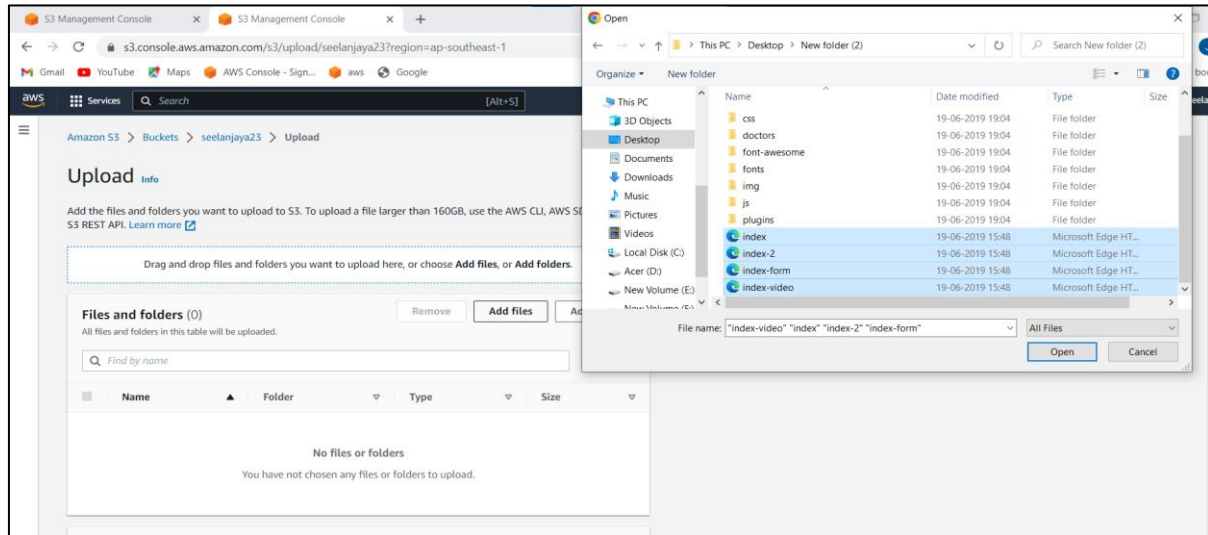
Two files delete---->object(show versions)---->deleted files show(source)---->(one file type show delete marker that file click and upload )---->it will backup



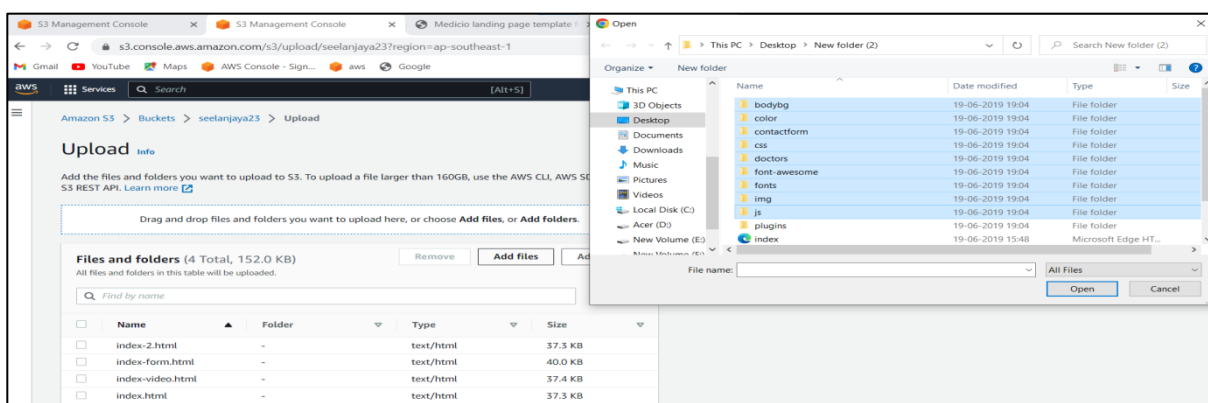
## Application host

**Step1:** create bucket

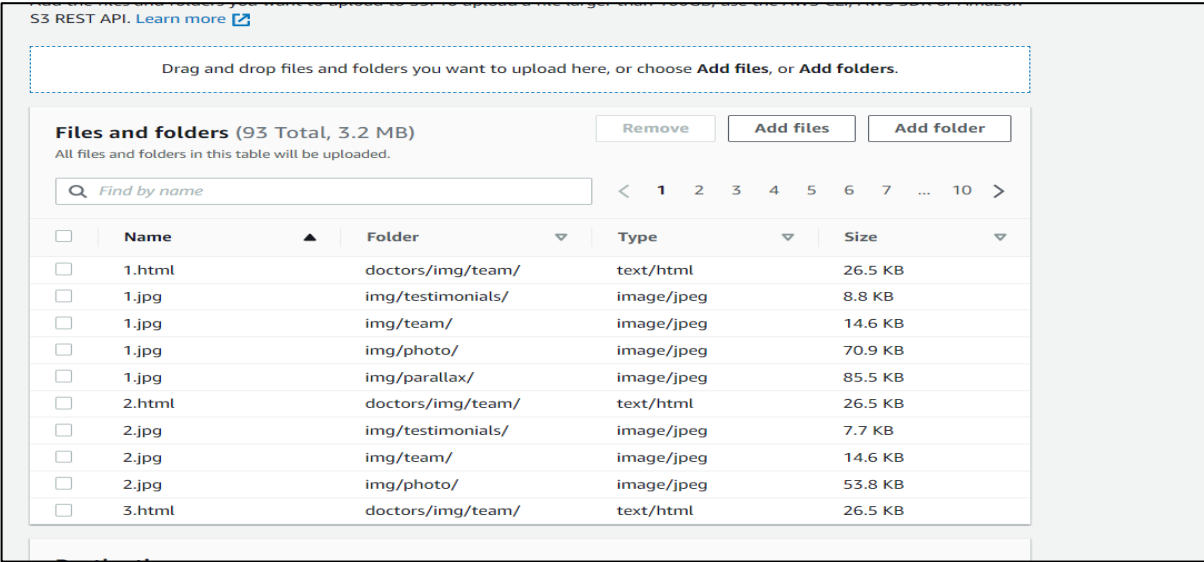
**Step2:** create object ---->upload content for app host--->add files---> select first html file---->open --->upload



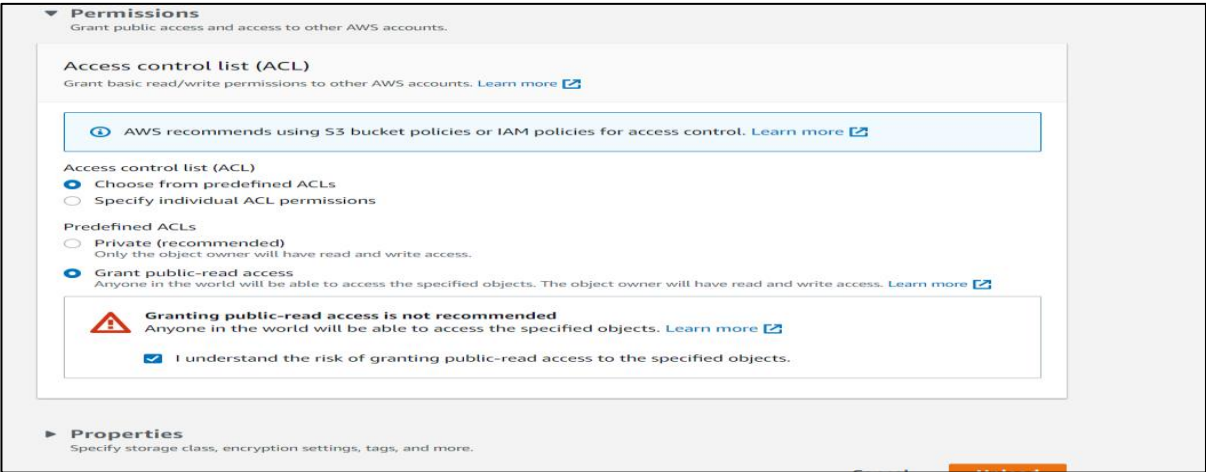
**Step3:**upload app host content folder --->upload folder--->one one folder upload separately



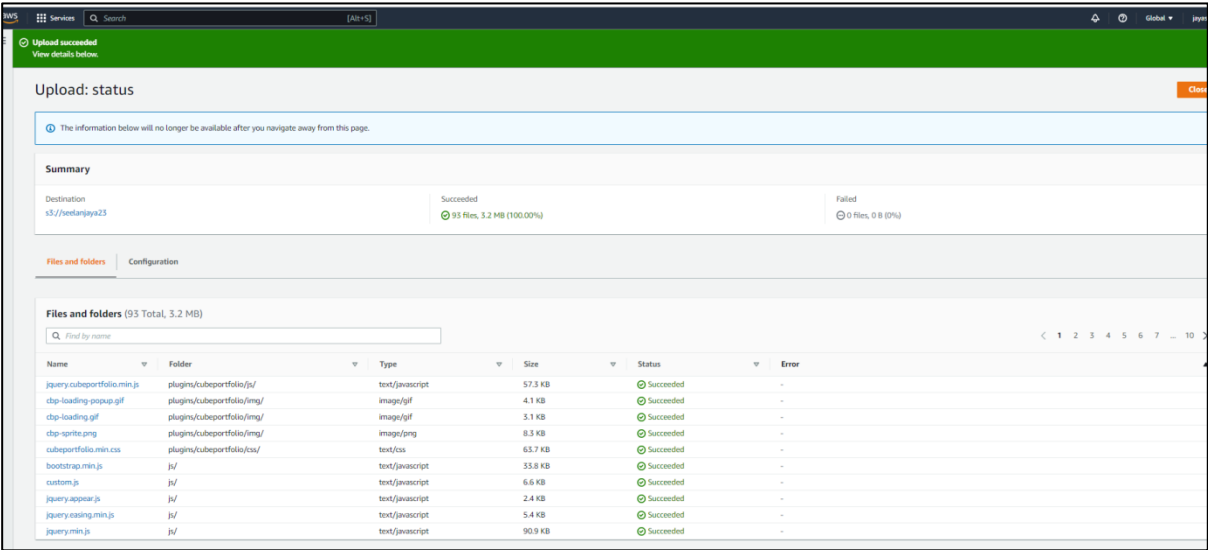




Permission--->grand public –read access---->click acknowledgement ----->upload



upload success



## Elastic Website Hosting

Bucket--->properties--->static webhosting

Amazon S3 > Buckets > seelanjaya23 > Edit static website hosting

### Edit static website hosting [Info](#)

**Static website hosting**  
Use this bucket to host a website or redirect requests. [Learn more](#)

**Static website hosting**  
☒ Disable  
☐ Enable

[Cancel](#) [Save changes](#)

1.Index document--->index.html 2.error document---->error.html--->save changes

**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](#)**

**Index document**  
Specify the home or default page of the website.

index.html

**Error document - optional**  
This is returned when an error occurs.

error.html

**Redirection rules - optional**  
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

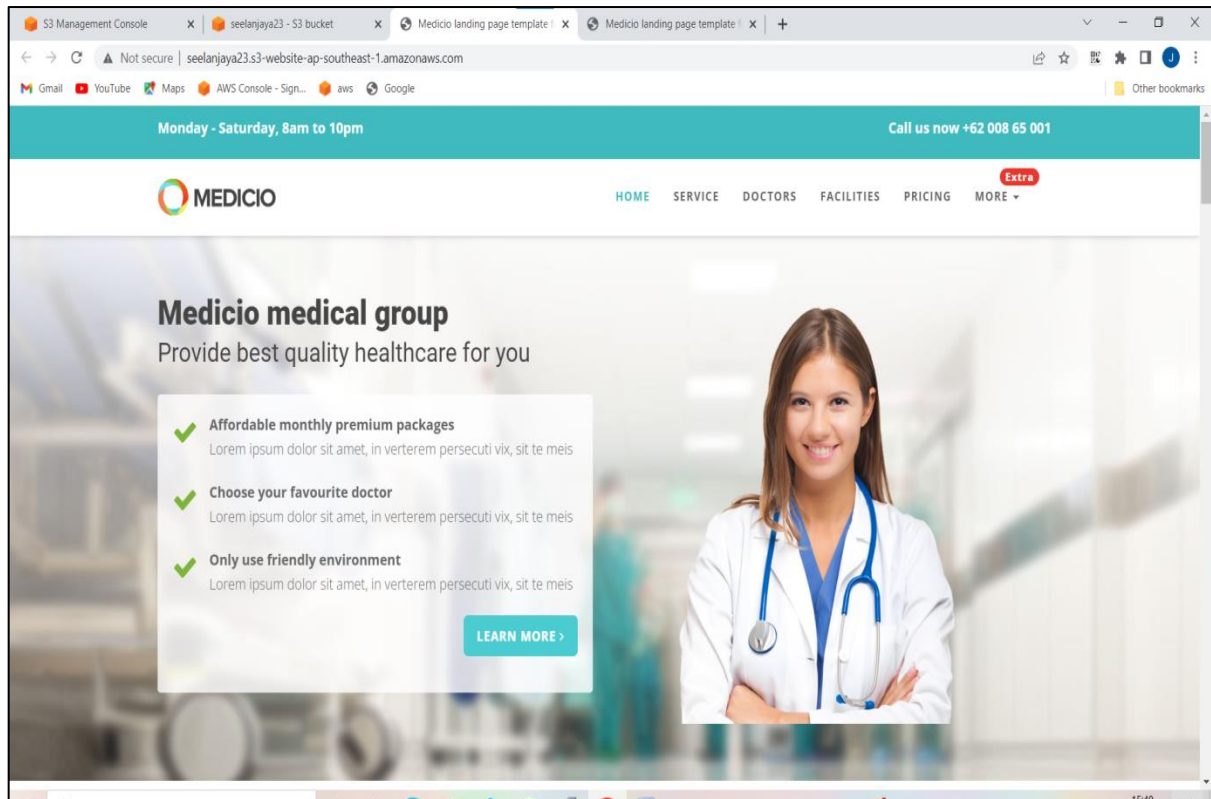
1

Static webhostig link created

**Requester pays**  
When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)  
Requester pays  
Disabled

**Static website hosting**  
Use this bucket to host a website or redirect requests. [Learn more](#)  
Static website hosting  
Enabled  
Hosting type  
Bucket hosting  
Bucket website endpoint  
When you configure your bucket as a static website, the website is available at the [Amazon S3 website endpoint](#) of the bucket. [Learn more](#)  
<http://seelanjaya23.s3-website-ap-southeast-1.amazonaws.com>

click static webhost link it will show original content page.



## Acl Disable:

### BUCKET CREATE:

Create bucket--->bucket name--->object ownership(**ACL DISABLED**)----> Block Public  
Access settings for this bucket-----> remove tick block all public acces---->tick I acknowledge  
--->bucket versioning----->enable----->create bucket

Amazon S3 > Buckets > Create bucket

### Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

#### General configuration

Bucket name

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

Copy settings from existing bucket - *optional*  
Only the bucket settings in the following configuration are copied.

#### 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.

Object Ownership  
Bucket owner enforced

#### Block Public Access settings for this bucket

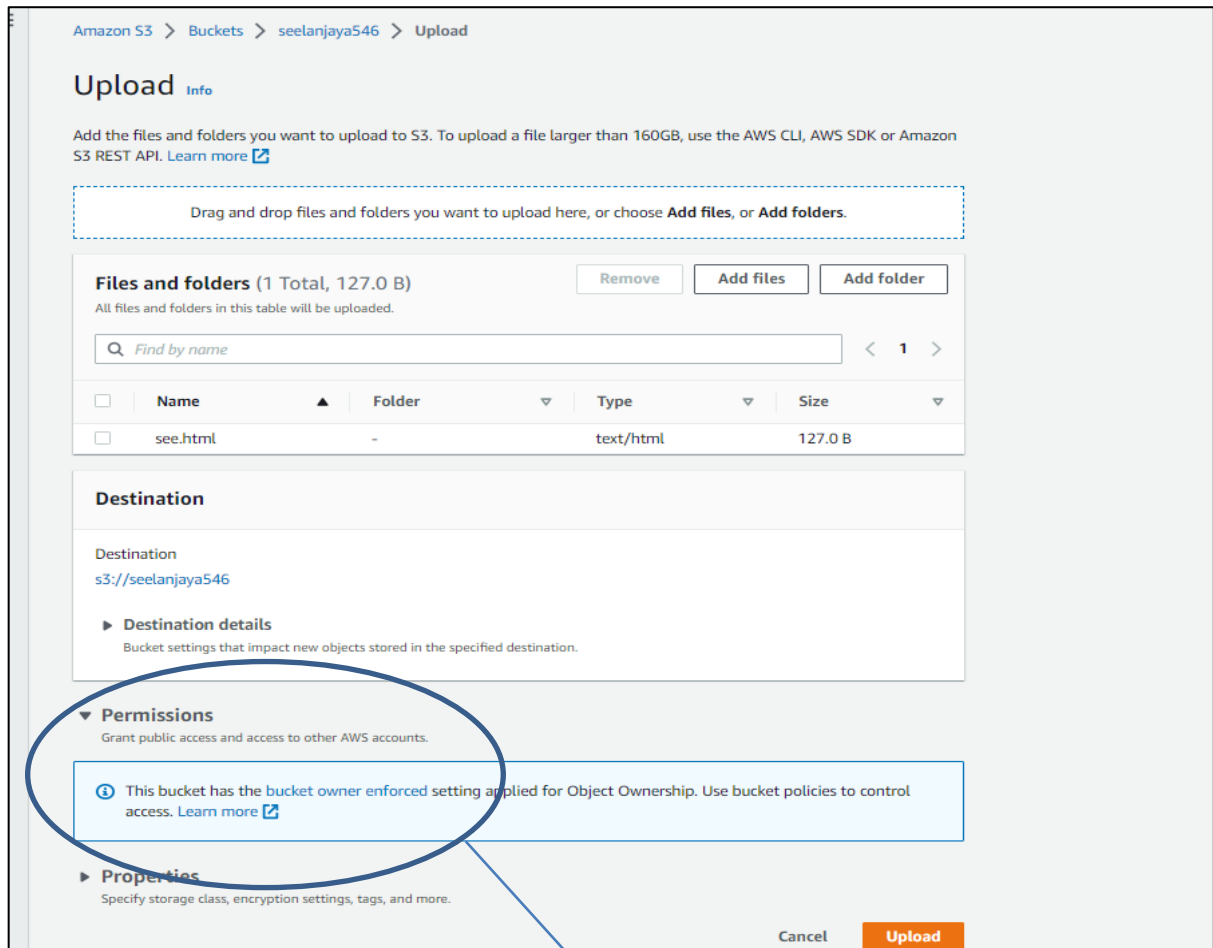
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access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

### OBJECT CREATE:

Select bucket---->upload--->add files(upload any file In html formte)

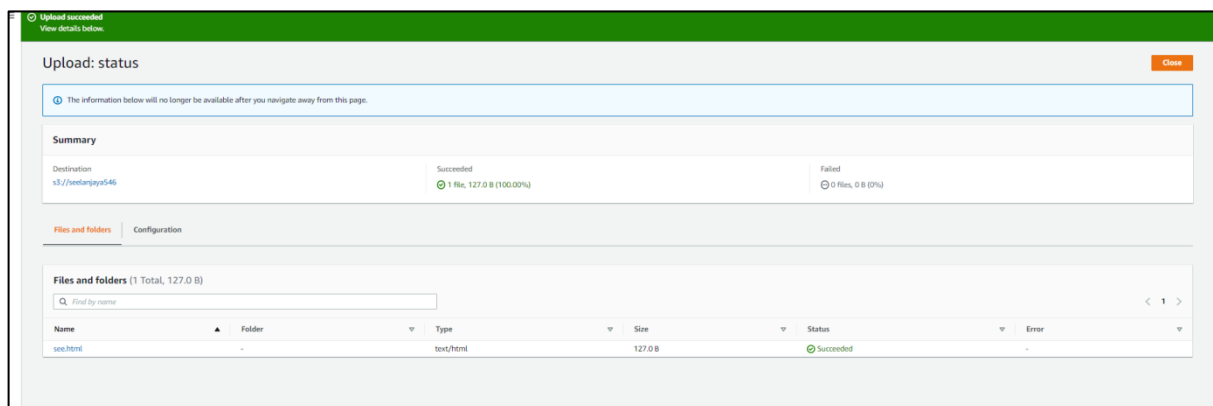
Permission--->grand public –read acces---->tick acknowledgement--->upload

↘ Can't show because **acl is disabled..**

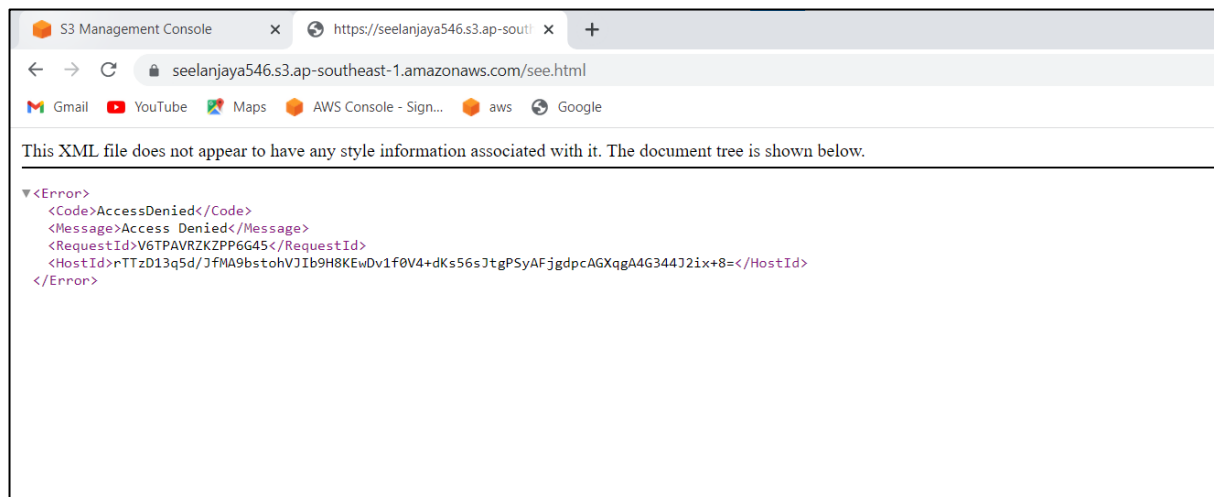


Can't show

But upload file



Now check object url



Can't show original file content because **acl was disabled..**

## ACLs disabled

- ACLs are disabled, and the bucket owner automatically owns and has full control over every object in the bucket. ACLs no longer affect permissions to data in the S3 bucket. The bucket uses policies to define access control.

## ACLs enabled

- The bucket owner owns and has full control over new objects that other accounts write to the bucket with the bucket-owner-full-control canned ACL.