

INFOTRIXS TASK 1

Hosting a static website in AWS S3

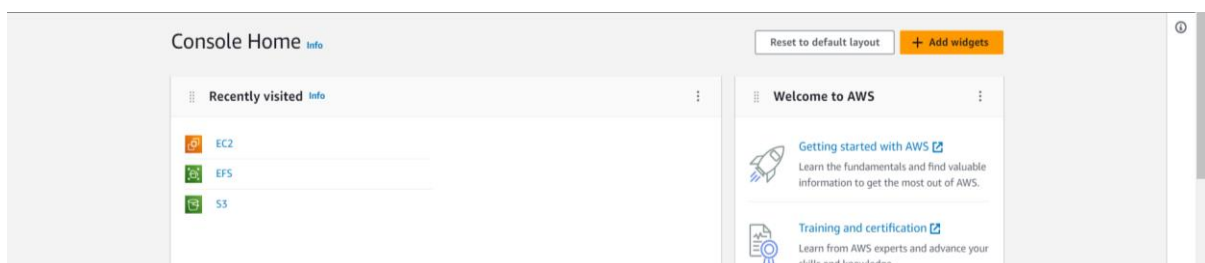
S3 service:

Amazon S3 (Simple Storage Service) is a highly scalable and durable cloud storage service offered by Amazon Web Services (AWS). It provides secure and reliable object storage for a wide range of data types, including documents, images, videos, and backups. S3 allows users to store and retrieve data from anywhere on the web, offering high availability, low latency, and seamless integration with other AWS services. With its simple and intuitive interface, users can easily create buckets to organize their data and set access controls to ensure data security. S3 also offers various storage classes, including Standard, Intelligent-Tiering, Glacier, and others, allowing users to optimize costs based on their specific data access patterns and requirements. Additionally, S3 provides features like versioning, lifecycle management, and event notifications to enable advanced data management and automation. Overall, Amazon S3 is a versatile and robust storage solution that allows businesses and developers to store, manage, and retrieve data at scale in a reliable and cost-effective manner.

Create a bucket:

In Amazon S3 (Simple Storage Service), we create a bucket to provide a unique namespace or container for storing and organizing our data. Buckets act as top-level folders within S3, allowing us to group related objects and manage their access permissions and lifecycle policies. By creating a bucket, we gain the ability to store, retrieve, and manage vast amounts of data securely and durably in the cloud. Buckets serve as a fundamental building block of S3, enabling scalability, high availability, and easy management of data for a wide range of applications and services.

To create a bucket in S3 select the **S3 service** in Amazon Web services.

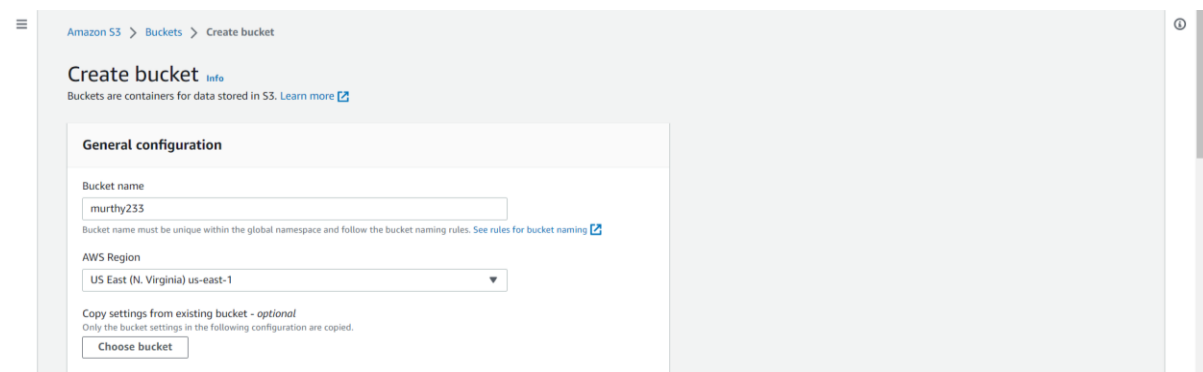


Now select create bucket option on the right side of the page.

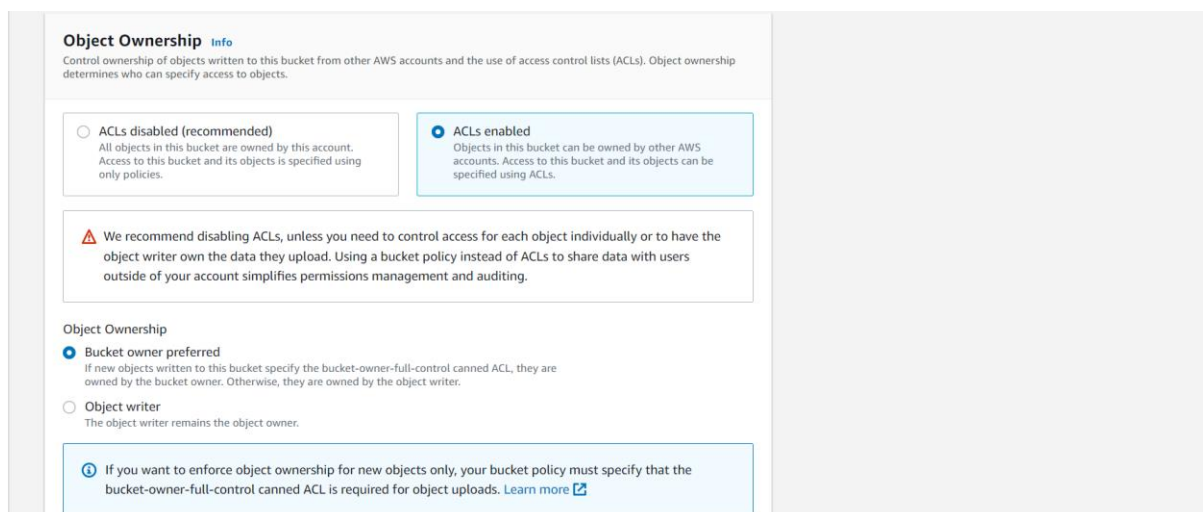


Enter the name of the bucket that should be globally unique.

Note: The bucket name can be between 3 to 63 characters long, and can contain only lower-case characters, numbers, periods, and dashes.



Select the object ownership as **ACLs enabled**. Then the objects in this bucket can be owned by other AWS accounts. Access to this bucket and its object can be specified using ACLs.



Now remove the **Block all public access** to 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. And accept all the policies that you turned off the public access option.

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 created 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

Versioning:

Versioning in Amazon S3 is a feature that allows you to keep multiple versions of an object within a bucket. Each time an object is updated or deleted, a new version is created, enabling easy retrieval of previous versions. This feature provides data protection and helps in recovering from both unintended user actions and application failures. Versioning can be managed programmatically or through the AWS Management Console, providing flexibility and control over object versioning in S3.

Enable the versioning option below.

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

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 Management & Insights](#) 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

Then click on the **create bucket** option to create the bucket .

▼ Advanced settings

Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. [Learn more](#)

☒ Disable

☐ Enable

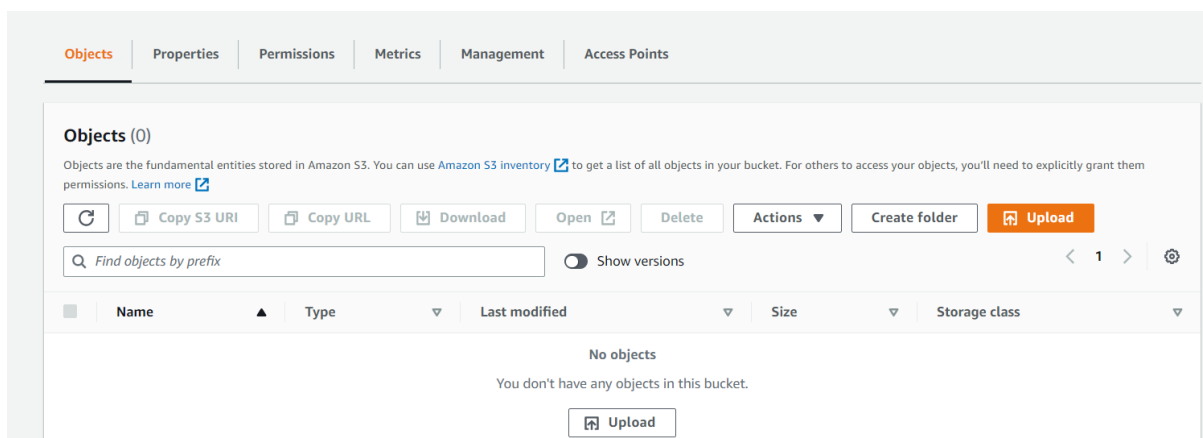
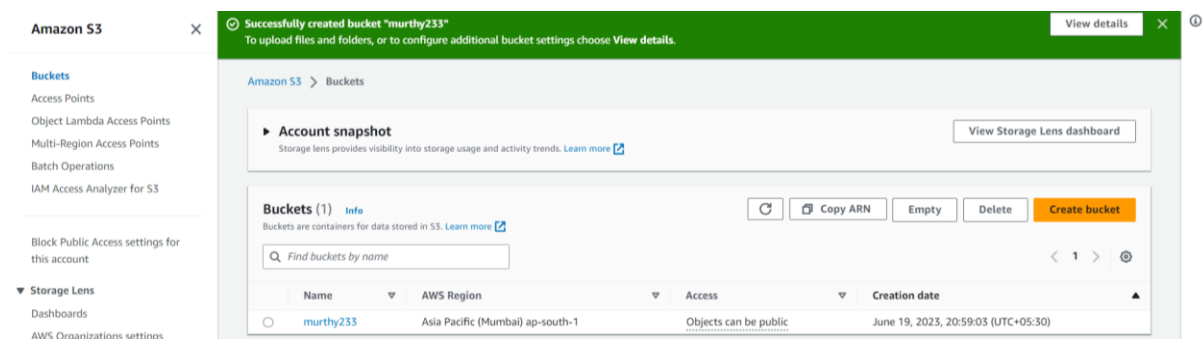
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

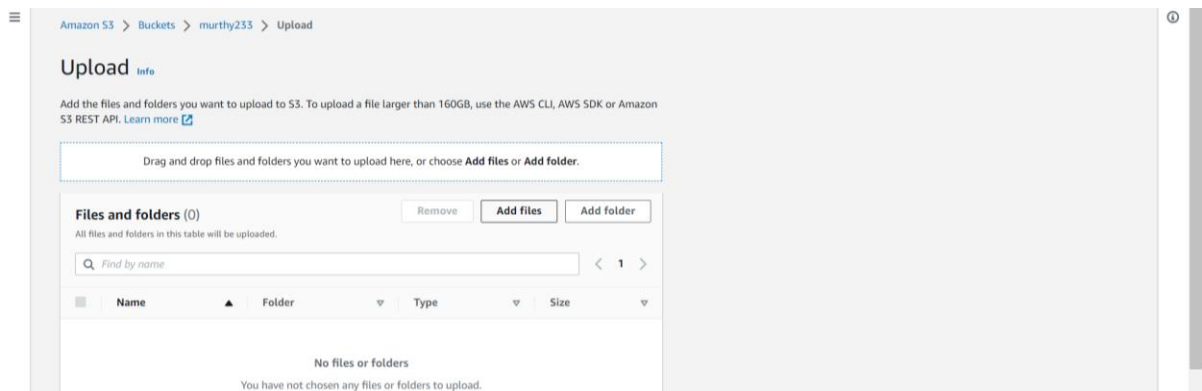
Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Bucket Versioning.

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

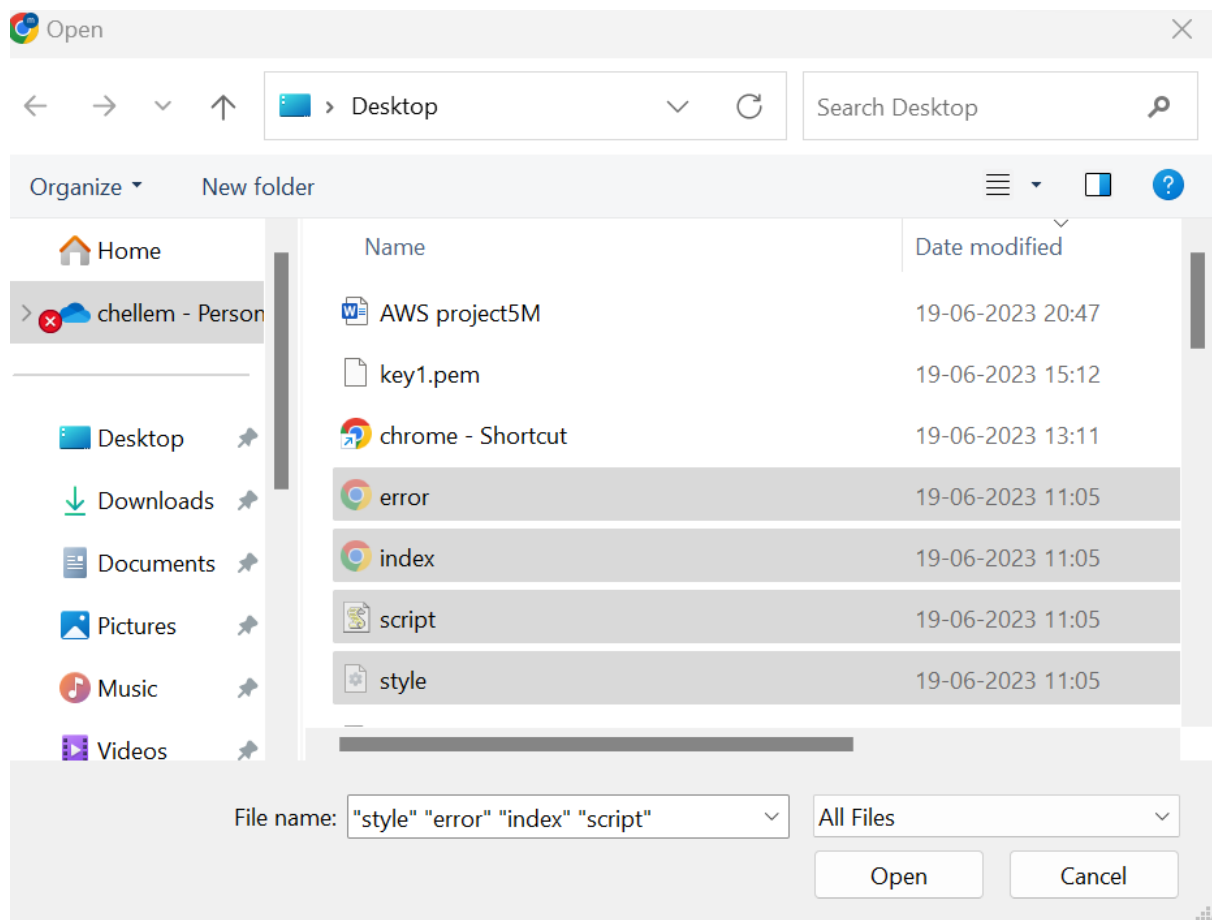
Cancel

Create bucket

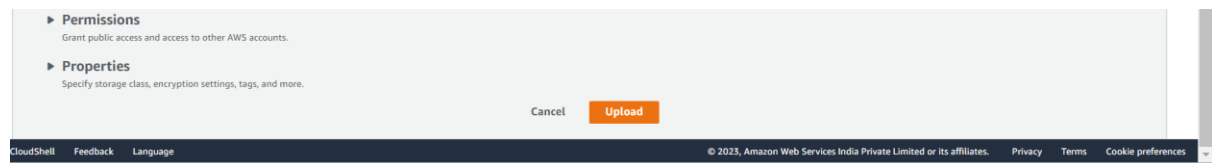




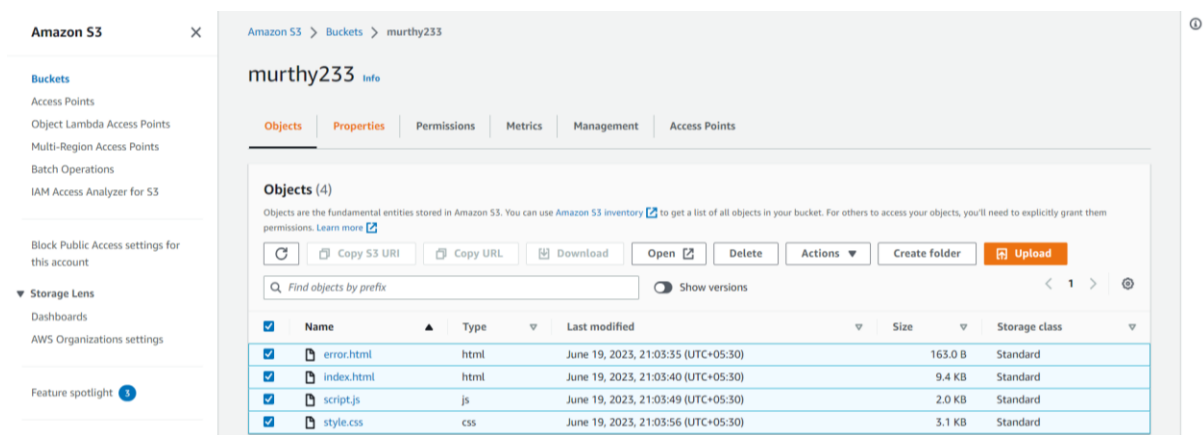
Now select the files from the File explorer that we want to add into the bucket and click on the **open**.



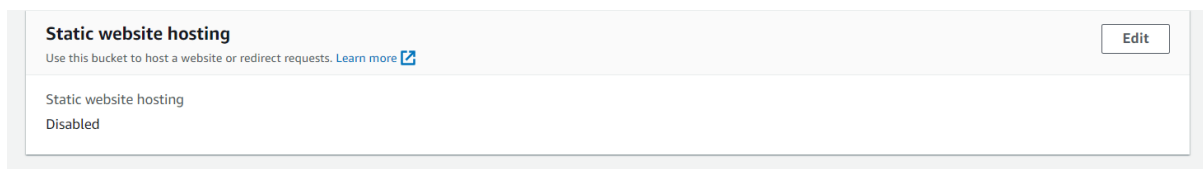
And then click on the **upload** button.



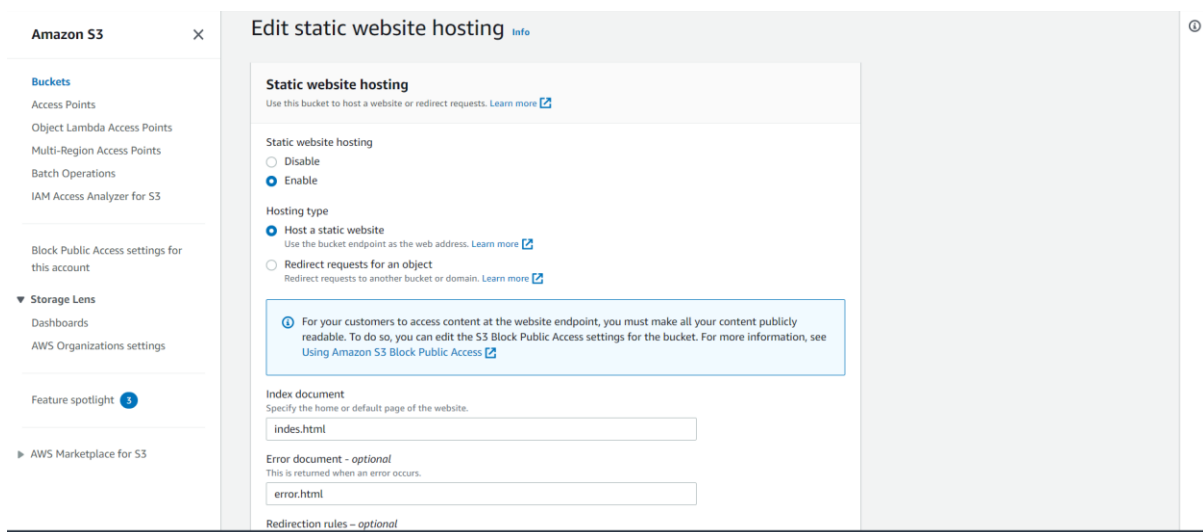
Enable Static website hosting: Now select the all files and click on the **properties** to enable the static website hosting.



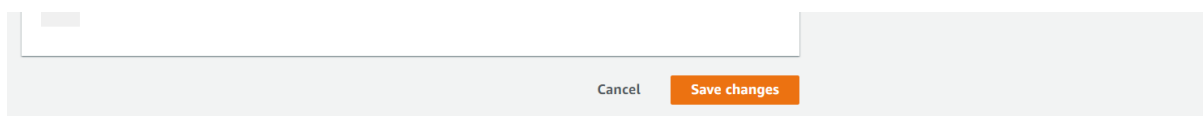
Click on **Edit option**.



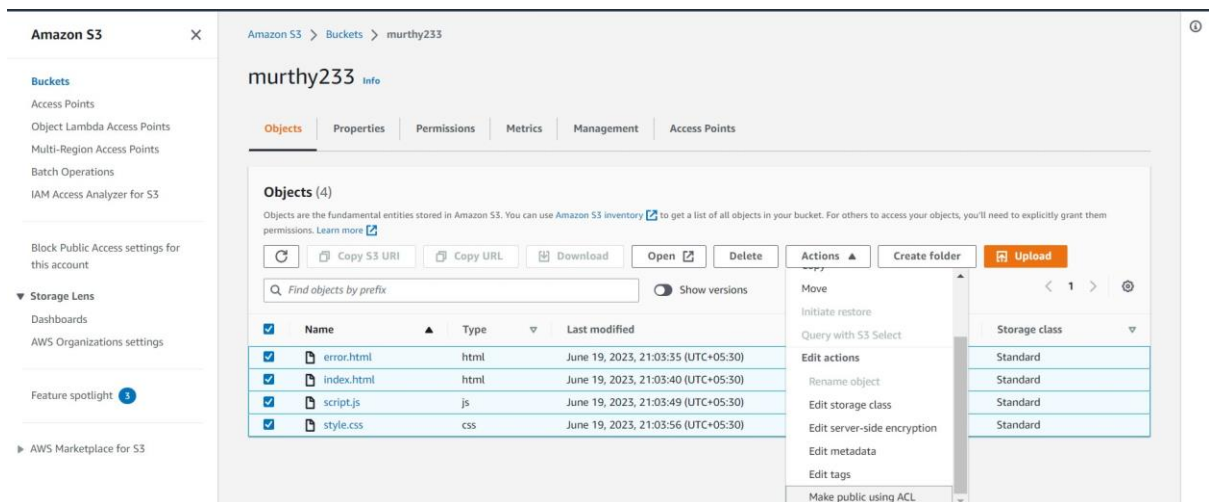
Enable the static website hosting and give the index document as **index.html** and error document as **error.html**.



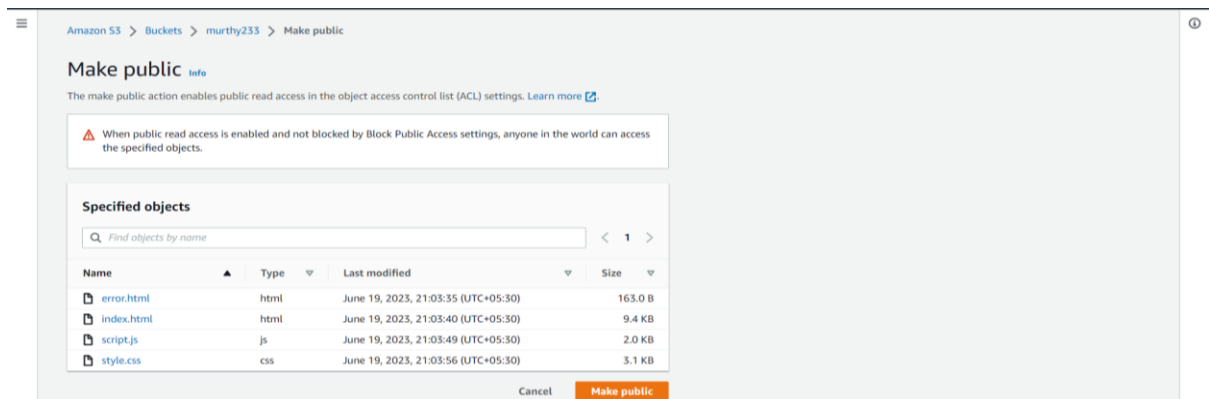
Now click on **save changes** to update the settings.



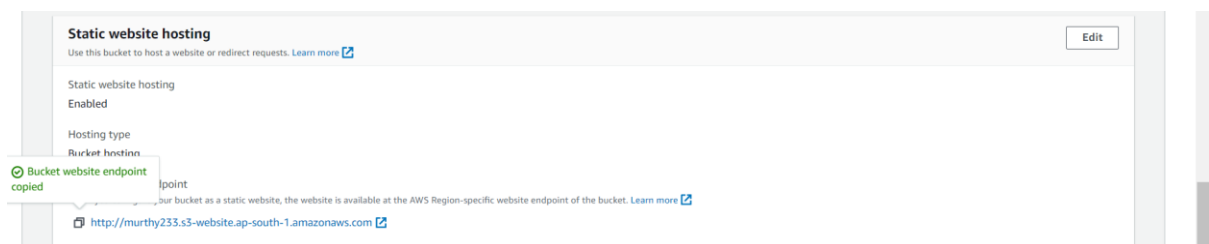
Now select all the objects in a bucket and go to **Actions** and select **Make public using ACL**.



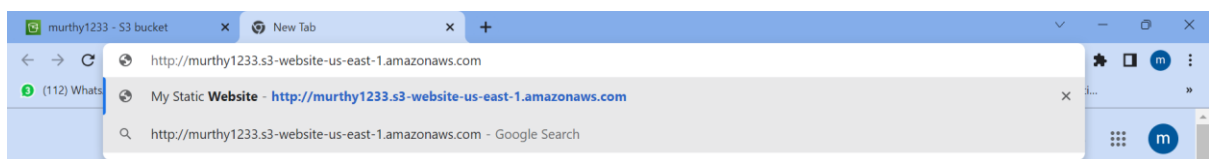
And click on the **Make public**.



Now again select all the objects in a bucket and go to **Properties** and go to **static website hosting**. And copy the **Bucket website endpoint**.



Now paste it on the another Tab in a Browser and click Enter.



Then the output will be as shown in below picture

Café



The Café offers an assortment of delicious and delectable pastries and coffees that will put a smile on your face. From cookies to croissants, tarts and cakes, each treat is specially prepared to excite your tastebuds and brighten your day!

Frank bakes a rich variety of cookies. Try them all!



Tea
Coffee
Latte
Hot
Chocolate
Yes, we
have it!



Our tarts are always a customer favorite!



About Us



Frank and Martha have been adding sweetness to their customers's lives since 2016. Both of them will personally greet you with a welcoming smile when you visit! Frank's recipes have been passed down from his mother and use simple and fresh ingredients to produce delightful flavors.

Contact Us

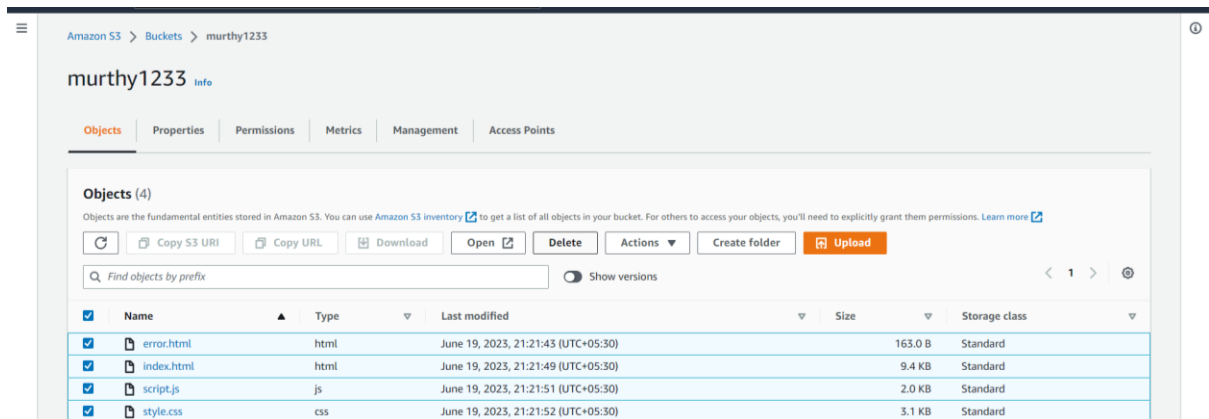


123 Sweet Tooth St.
London SW1A 0AA, UK
Tel: +44-12-12345678

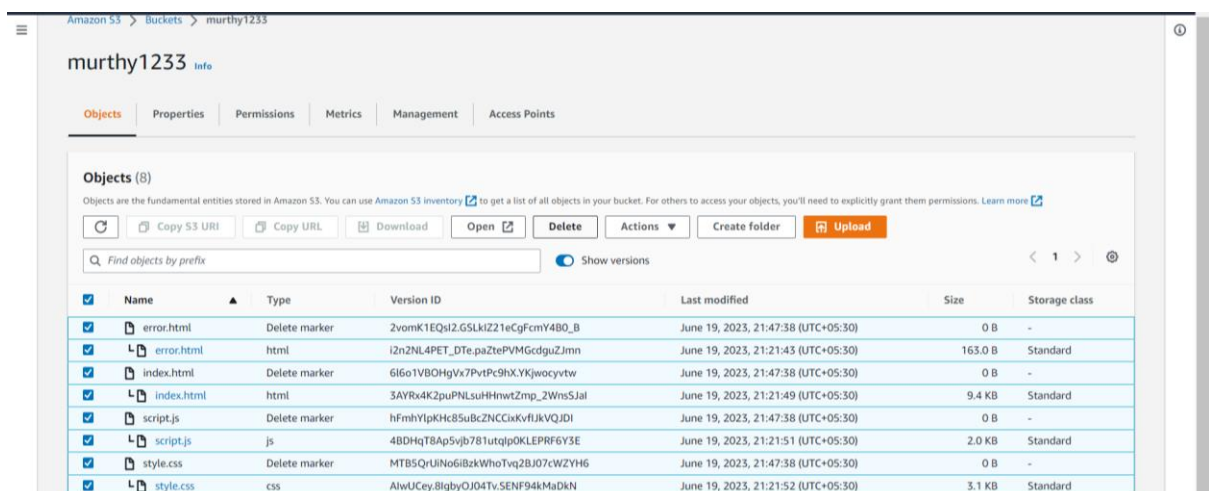
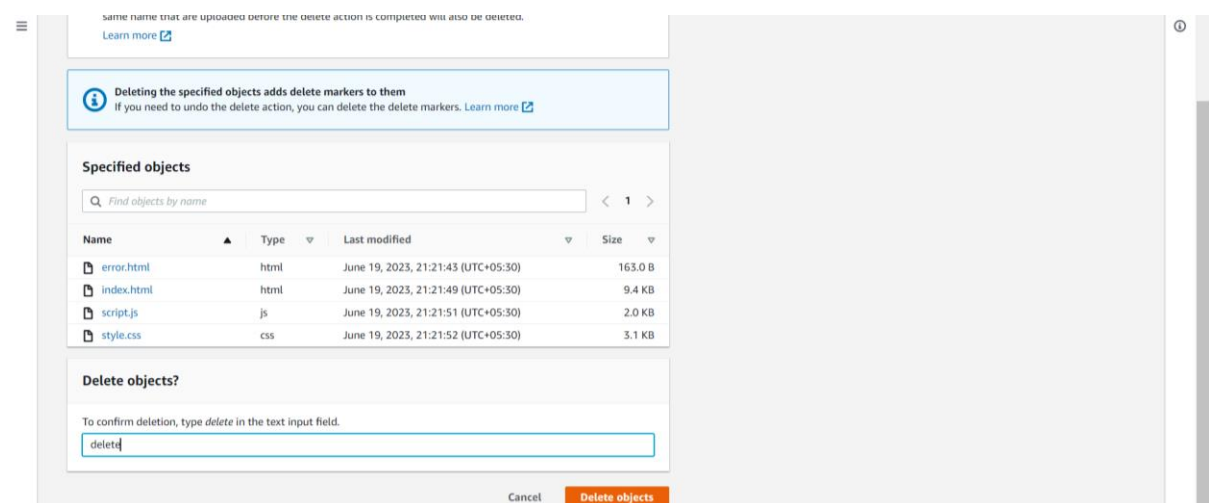
Hours

Clean up:

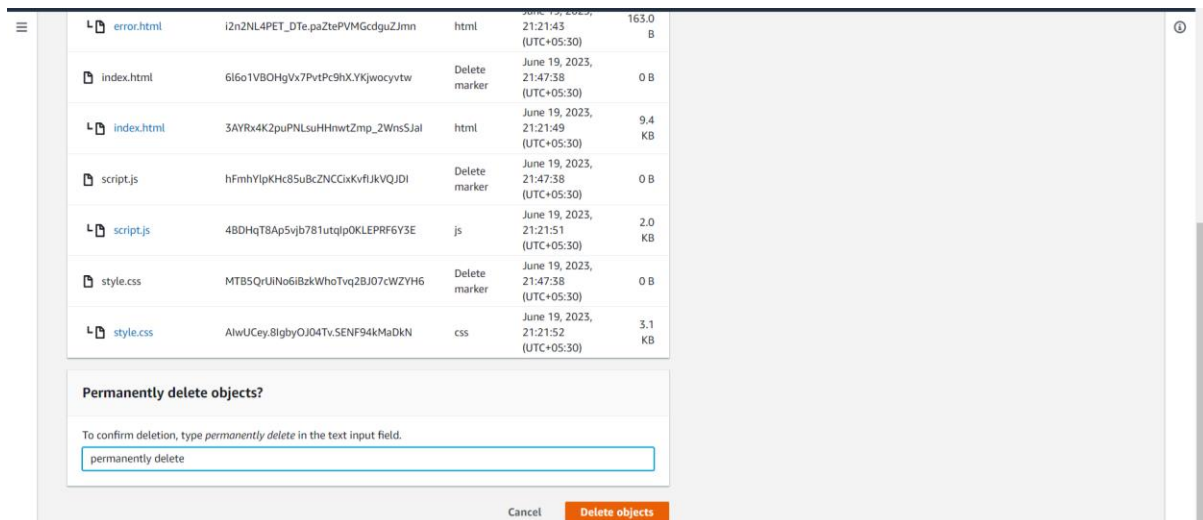
Object deletion: select the objects in the bucket and click on the **delete** button.



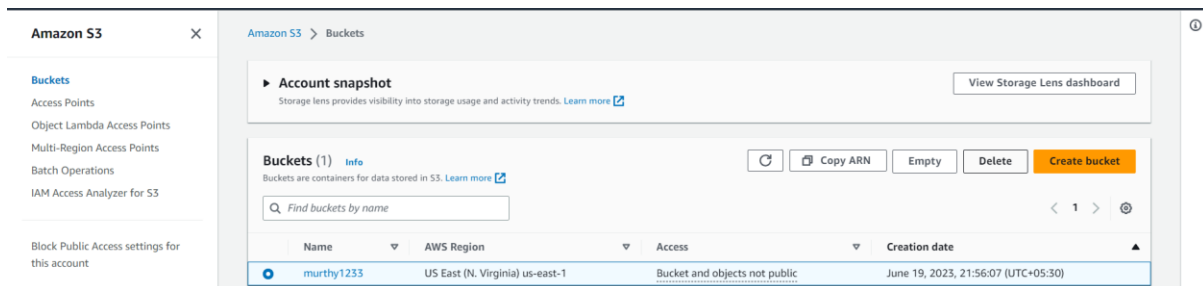
To conform deletion type **delete** in a given field. And click on the **Delete objects**.



If we delete the objects it only delete the objects without versioning to delete the versioning objects enable the **show versions** and select all the objects and click on the delete button and to conform type **permanently delete** in the given field and click on the **Delete objects**.



Bucket Deletion: To delete the bucket select the bucket and click on the **Delete** option.



To conform deletion Enter the bucket name in a given field and click on the **Delete bucket**.

