

Experiment 05 - Cloud Computing

December 21, 2022

Aim

Create S3 bucket and store objects in the bucket. Implement Version Control and Static Website hosting.

Theory

- **S3** : Amazon S3 or Amazon Simple Storage Service is a service offered by Amazon Web Services that provides object storage through a web service interface. Amazon S3 uses the same scalable storage infrastructure that Amazon.com uses to run its e-commerce network. Some important features of S3 are Storage management and monitoring, Storage analytics and insights, Storage classes, Access management and security, Data processing, Query in place, Data transfer and Performance consistency.
- **Versioning** : The versioning in Amazon S3 is a means of keeping multiple variants of an object in the same bucket. You can use the S3 Versioning feature to preserve, retrieve, and restore every version of every object stored in your buckets.
- **Cloudfront** : Amazon CloudFront is a content delivery network operated by Amazon Web Services. Content delivery networks provide a globally-distributed network of proxy servers that cache content, such as web videos or other bulky media, more locally to consumers, thus improving access speed for downloading the content.

Results

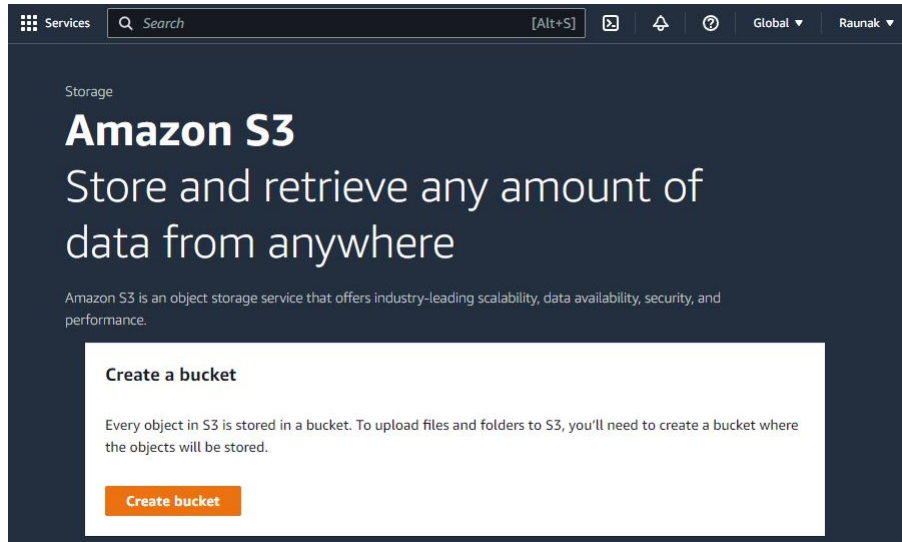


Figure 1: Start by creating a bucket by searching for S3 from the search bar

A screenshot of the 'Create bucket' form in the AWS console. The title is 'Create bucket' with an 'Info' link. Below it, a note says 'Buckets are containers for data stored in S3. [Learn more](#)'. The form is divided into a 'General configuration' section. It has a 'Bucket name' field with 'generics3bucket' entered and highlighted in yellow. Below the field is a note: 'Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)'. There is an 'AWS Region' dropdown menu currently set to 'US East (N. Virginia) us-east-1'. At the bottom, there's a section for 'Copy settings from existing bucket - optional' with a note: 'Only the bucket settings in the following configuration are copied.' and a 'Choose bucket' button.

Figure 2: Give you bucket the name you want

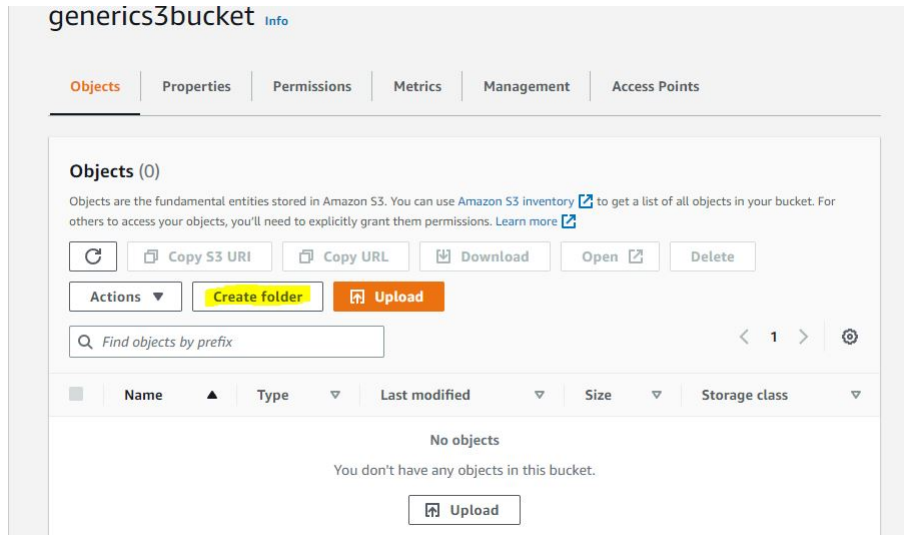


Figure 3: Create a folder after directing to created bucket

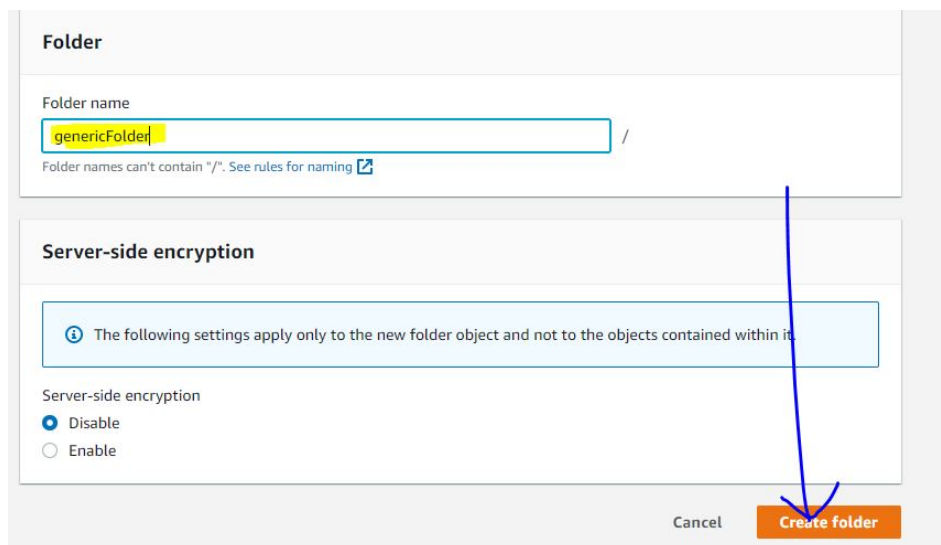


Figure 4: Name the folder whatever you prefer and select the create option

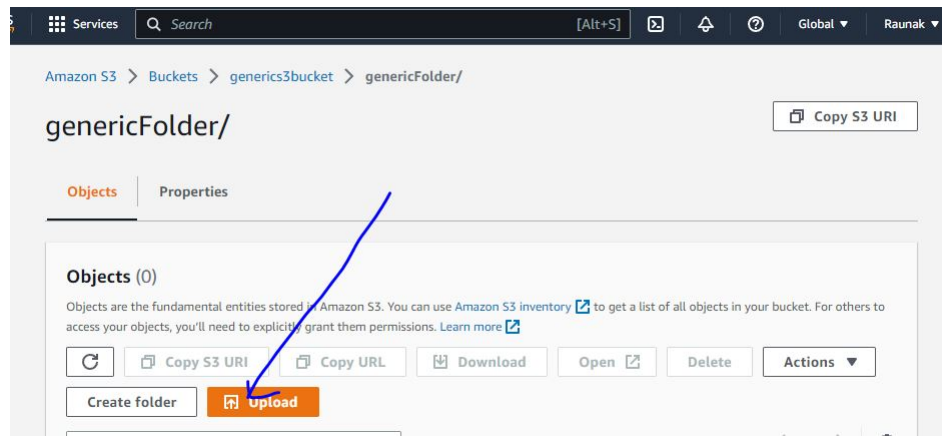


Figure 5: After directing to folder select on upload to upload files

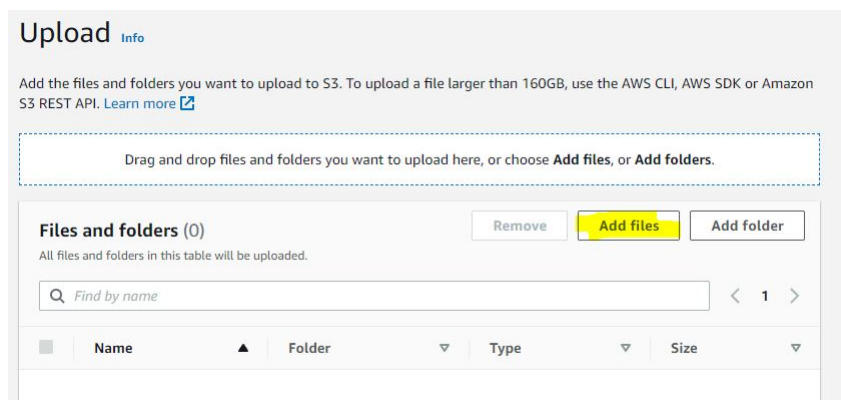


Figure 6: Select add files option

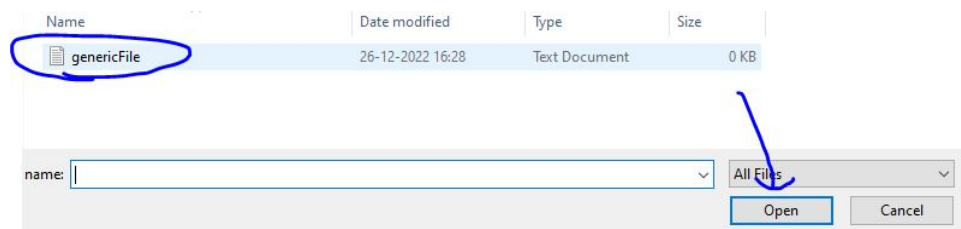


Figure 7: Select the file from upload option the file you wish to upload

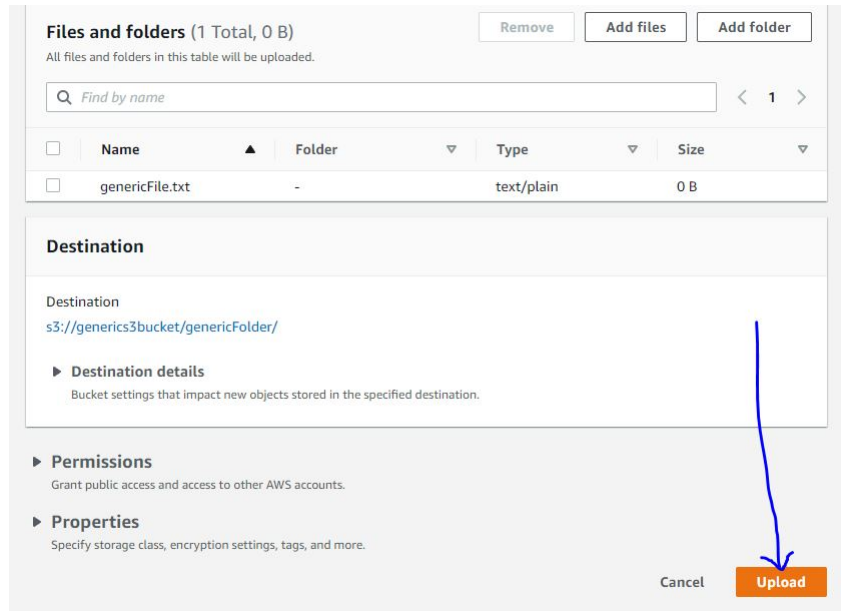


Figure 8: Upload button uploads the selected files from add files option

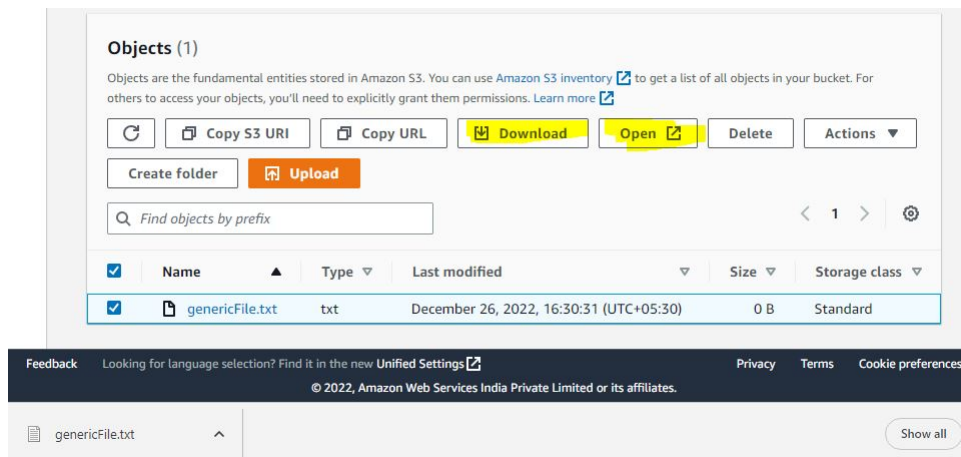


Figure 9: One can either open or download the file once upload is successful

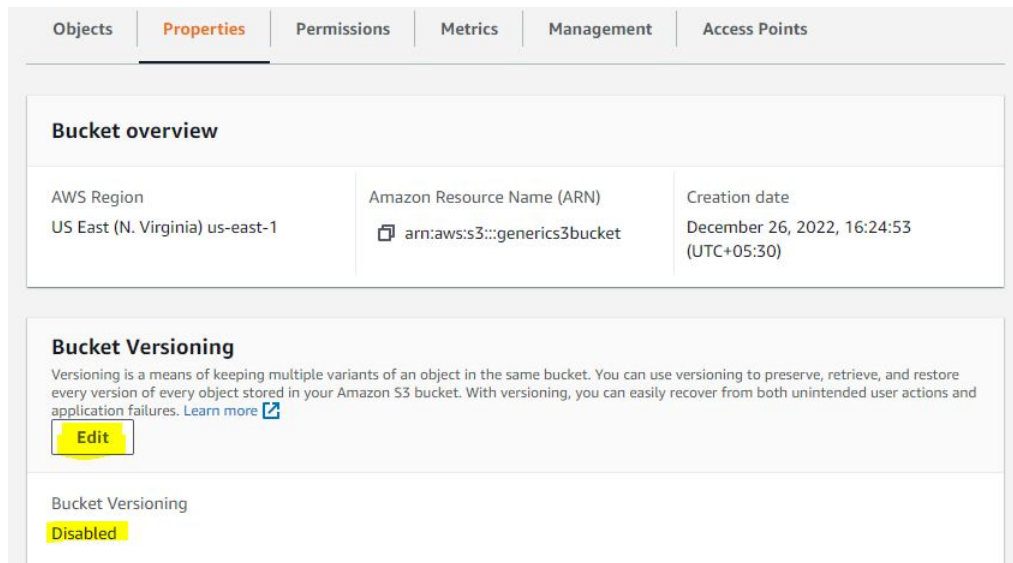


Figure 10: Versioning can be enabled with selecting the properties tab of the created bucket. Select the bucket versioning edit option

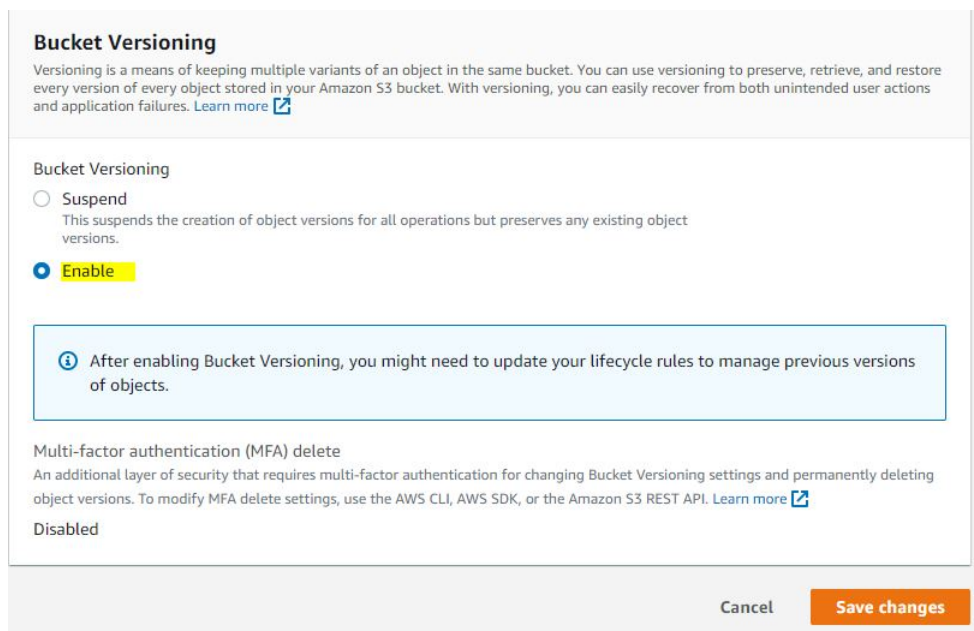


Figure 11: Select the enable radio button to make the versioning changes and save the changes for effect

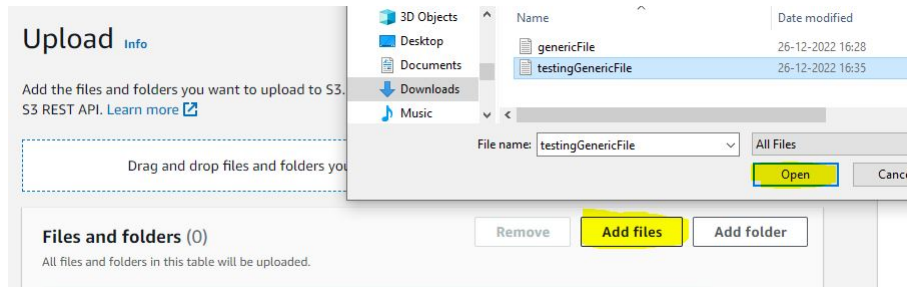


Figure 12: Upload a new file

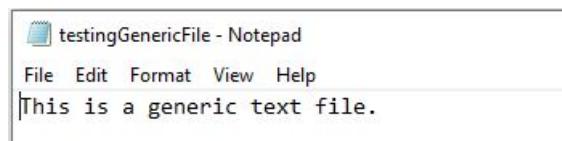


Figure 13: The basic text is available in the file to get started

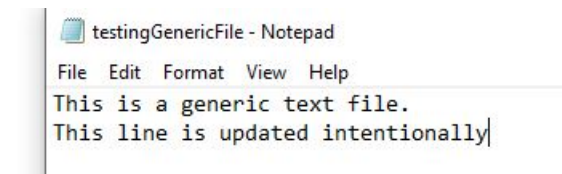


Figure 14: Try to add and edit some text

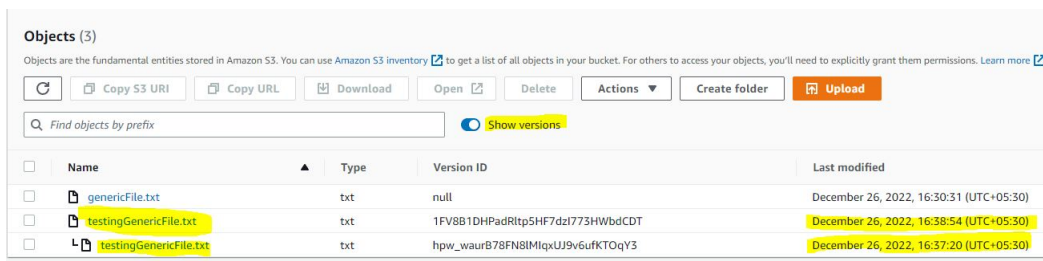


Figure 15: Upload the edited file and select the **Show versions** option to display the versions

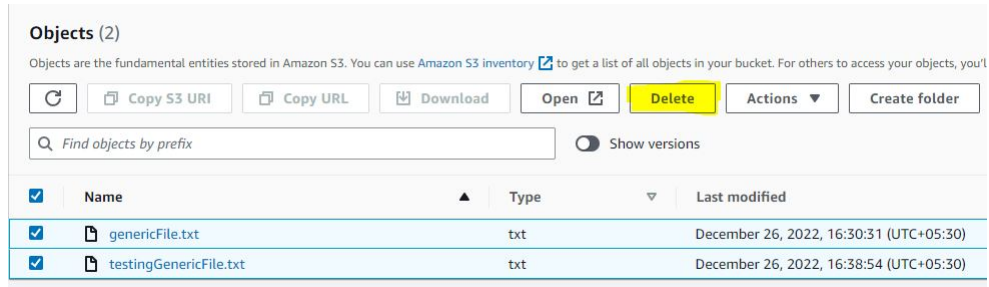


Figure 16: Delete the file by selecting the files

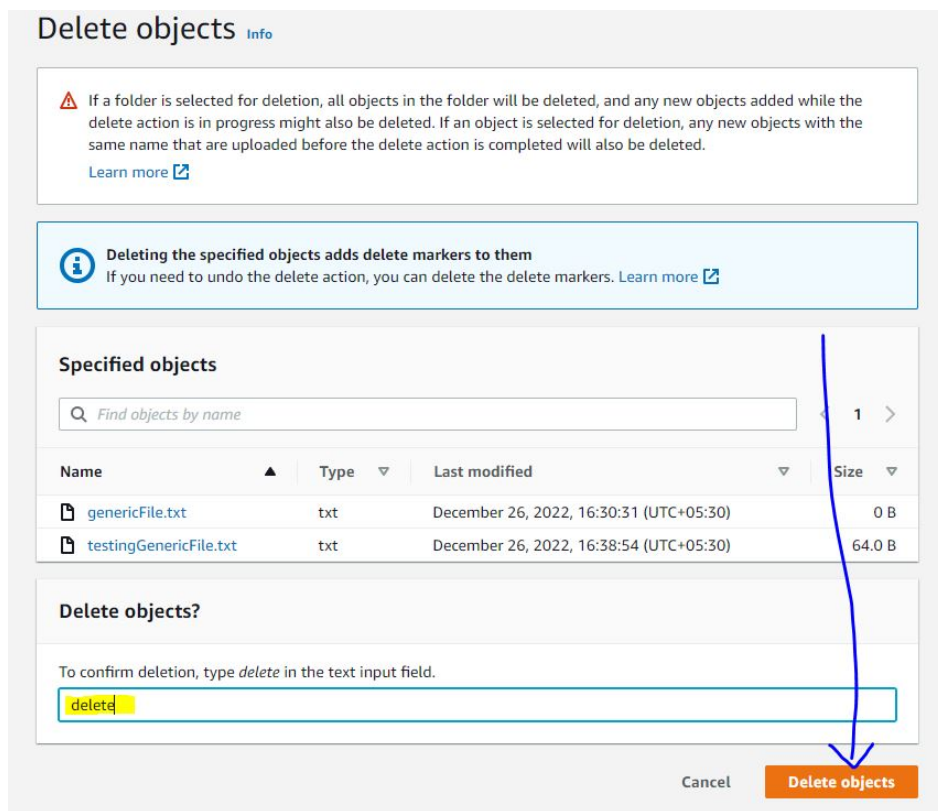


Figure 17: Command `delete` should be typed to delete the objects

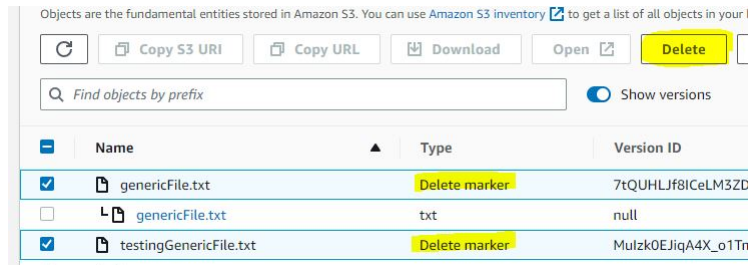


Figure 18: Looking at show versions one can see the delete marker which can be deleted to restore the files

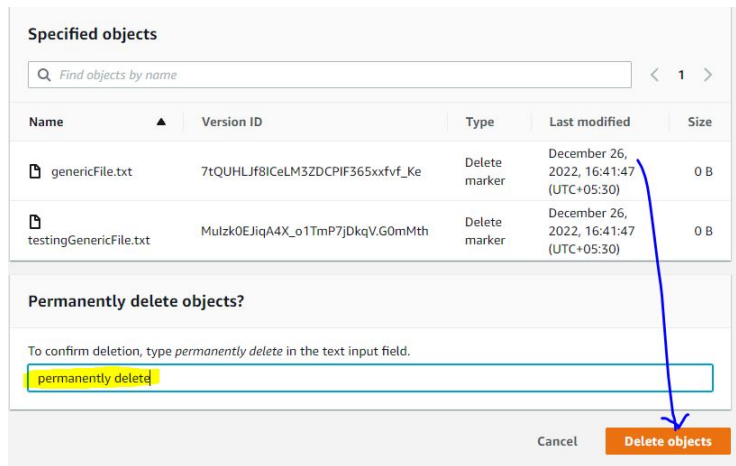


Figure 19: To execute the command successfully permanently delete is necessary

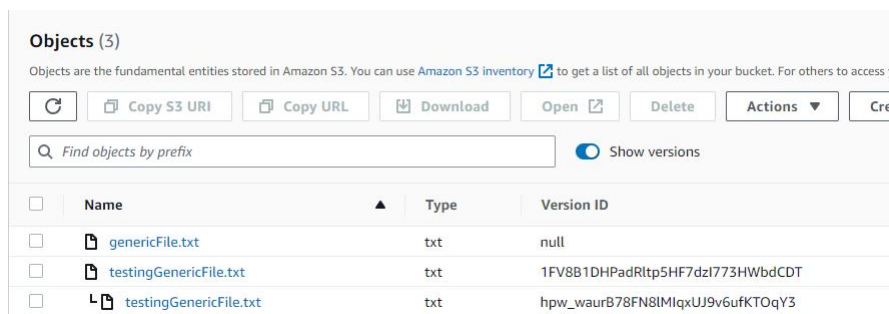


Figure 20: The files are restored in pristine order

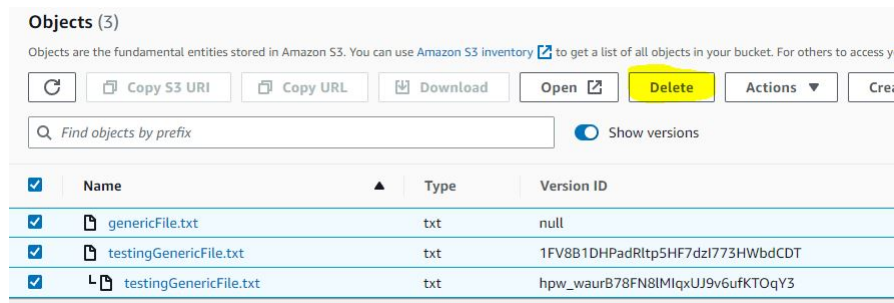


Figure 21: While all versions are displayed select all the files to delete them permanently

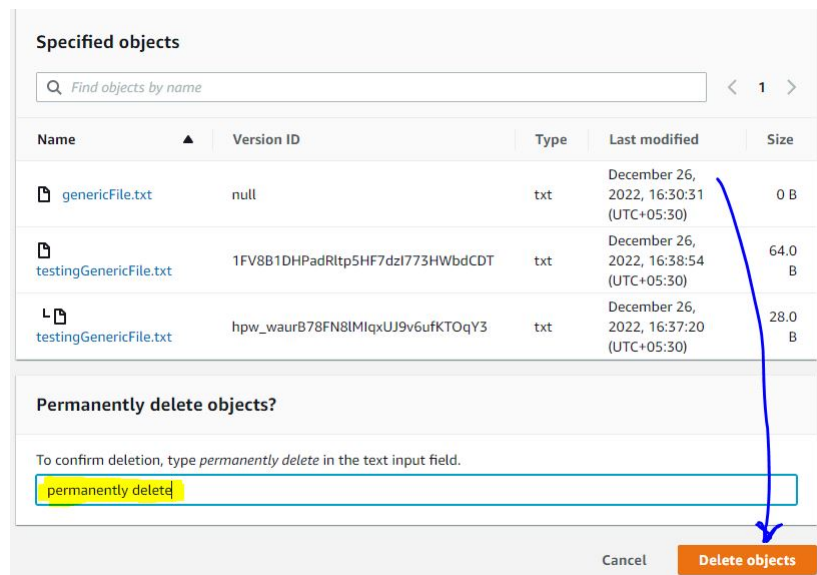


Figure 22: The execution requires permanently delete option to successfully finish the process

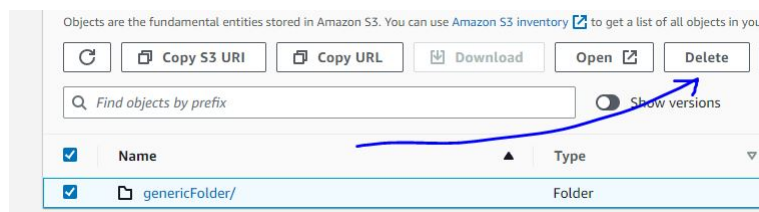


Figure 23: Deletion of folder is a very straight-forward process

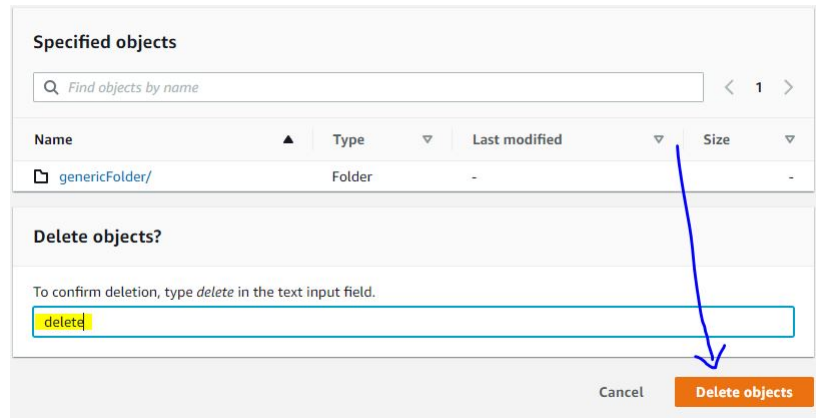


Figure 24: The folder can be deleted with `delete` command to finish the process

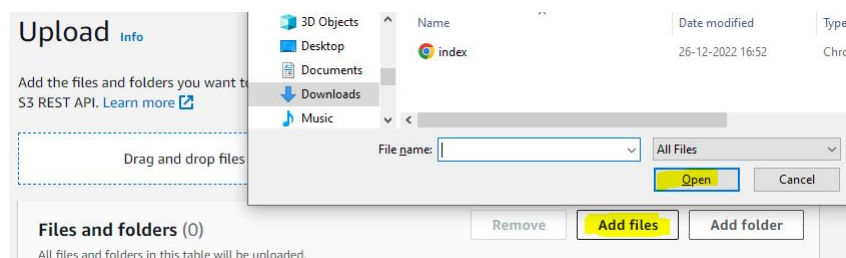


Figure 25: Static website hosting can be done on S3. This can be done by uploading the website files. Here I upload one single generic HTML file

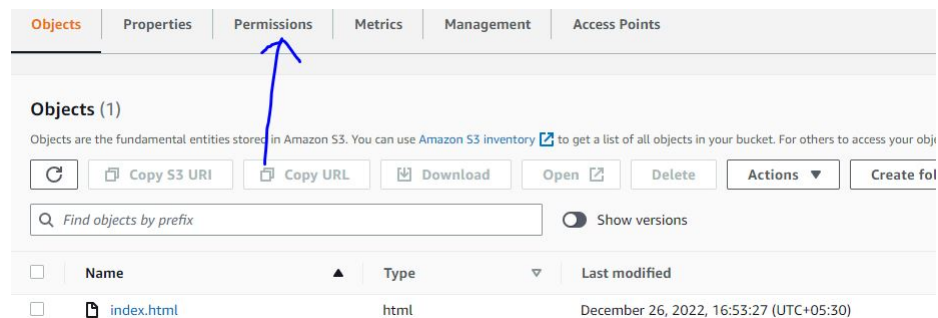


Figure 26: Selecting the permissions for the bucket, the setup for static website can be done

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**

Figure 27: Uncheck the block all public access option and save the 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**

Figure 28: The `confirm` command is required to complete the execution

generics3bucket Info

Objects **Properties** Permissions Metrics Management Access Points

Bucket overview

Figure 29: Now head to properties for further hosting options

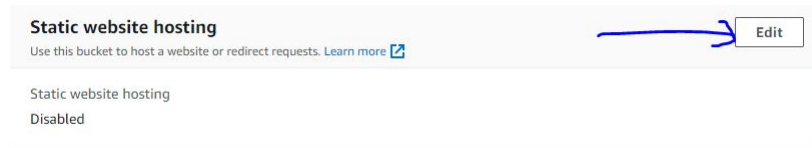


Figure 30: Scroll down and reach to static website hosting option and select Edit

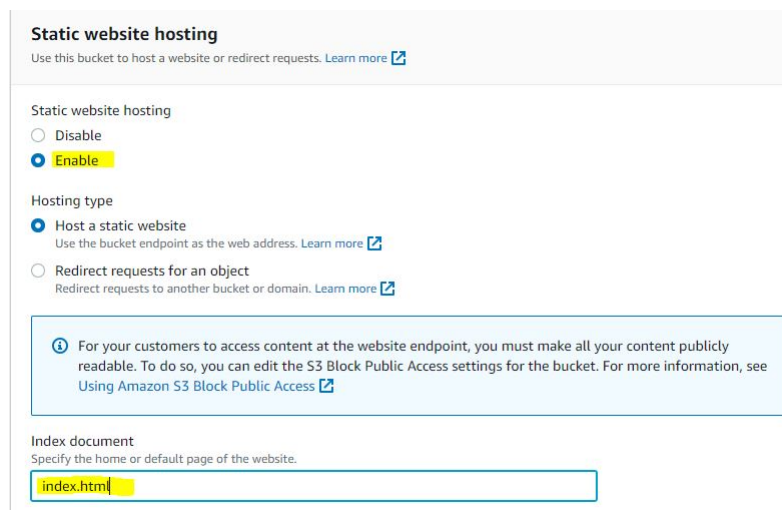


Figure 31: Enable the website hosting and type the name of main file of system and save

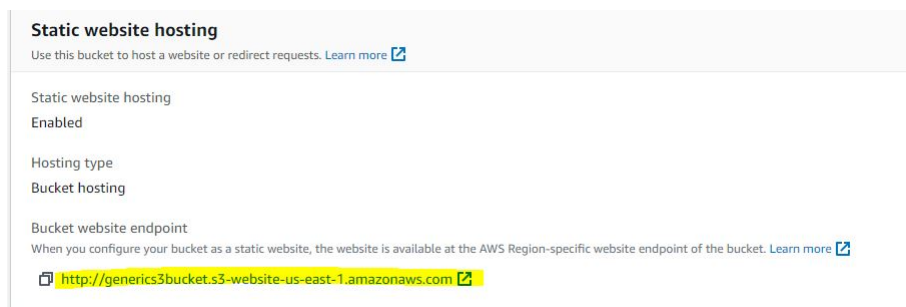


Figure 32: The link can be followed for viewing the page

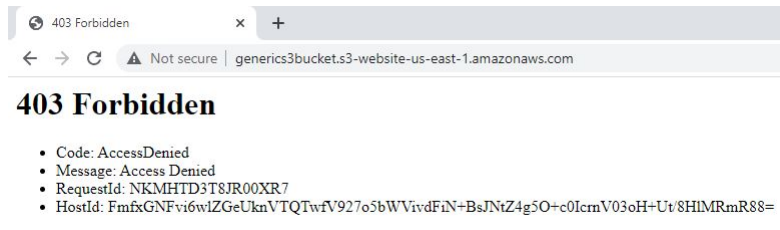


Figure 33: Page rams into a 403 Forbidden error which can be tackled by making some changes

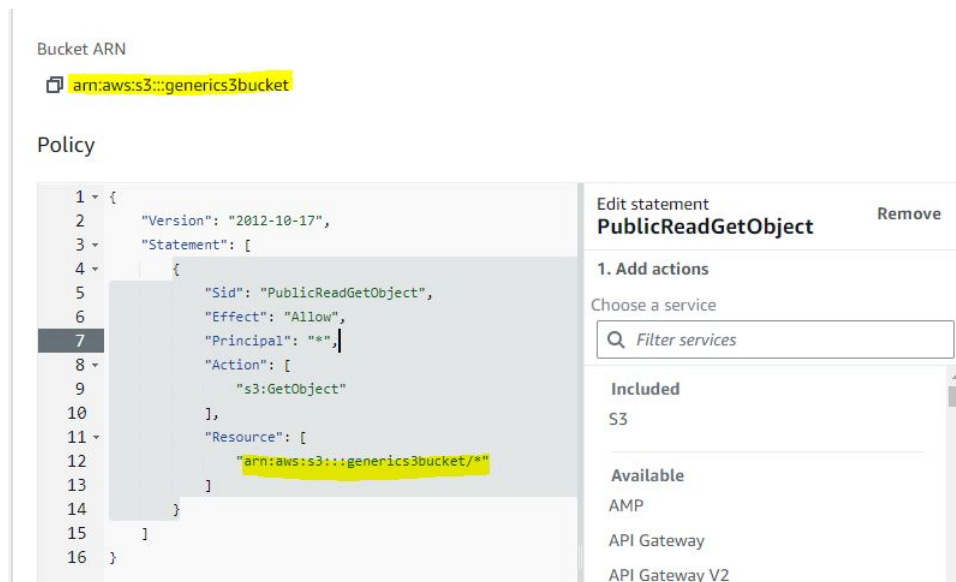


Figure 34: Type the bucket policy and mention the ARN provided by the bucket

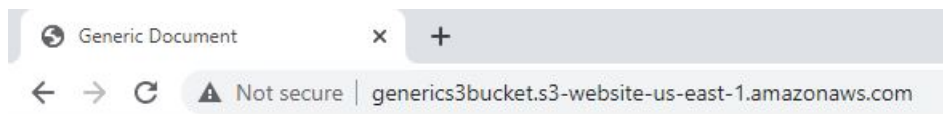


Figure 35: The link is now accessible to host the static page

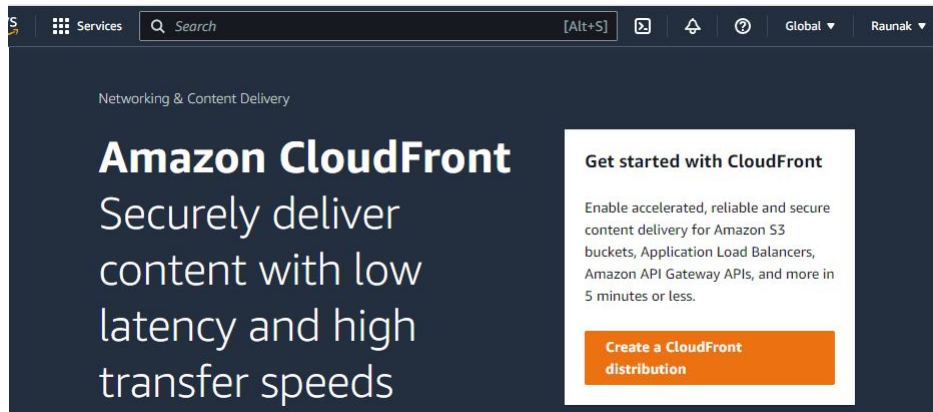


Figure 36: Using cloudfront to safe-gaurd the direct access to S3. Before starting this delete the bucket policy and disable the public sharing access to bucket directly

Origin

Origin domain
Choose an AWS origin, or enter your origin's domain name.

Origin path - optional [Info](#)
Enter a URL path to append to the origin domain name for origin requests.

Name
Enter a name for this origin.

Origin access [Info](#)

☐ Public
Bucket must allow public access.

☐ Origin access control settings (recommended)
Bucket can restrict access to only CloudFront.

☒ **Legacy access identities**
Use a CloudFront origin access identity (OAI) to access the S3 bucket.

Origin access identity
Select an existing origin access identity (recommended) or create a new identity.

[Create new OAI](#)

Bucket policy
Update the S3 bucket policy to allow read access to the OAI.

☐ No, I will update the bucket policy

☒ **Yes, update the bucket policy**

Figure 37: Select all the highlighted options from the image and follow accordingly. This is initial creation process of cloudfront. Do not change anything apart from given options in the image

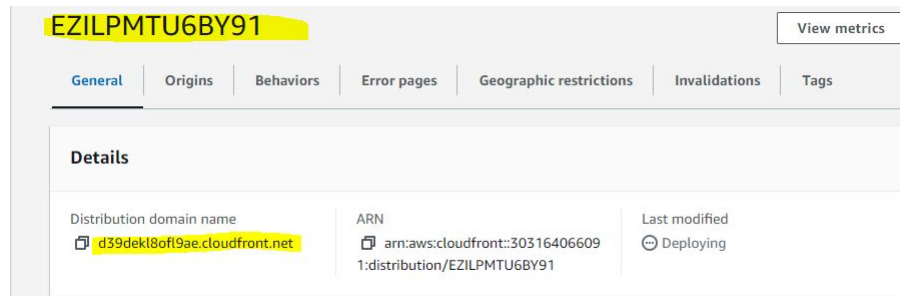
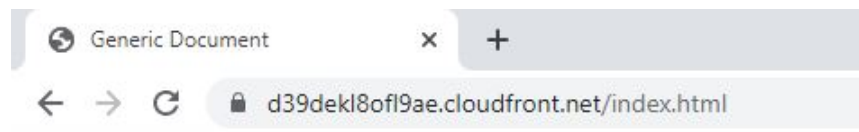


Figure 38: The distribution is available on the cloudfront access link with its own domain



A generic document created by Raunak

Figure 39: Successful hosting of the website using CloudFront

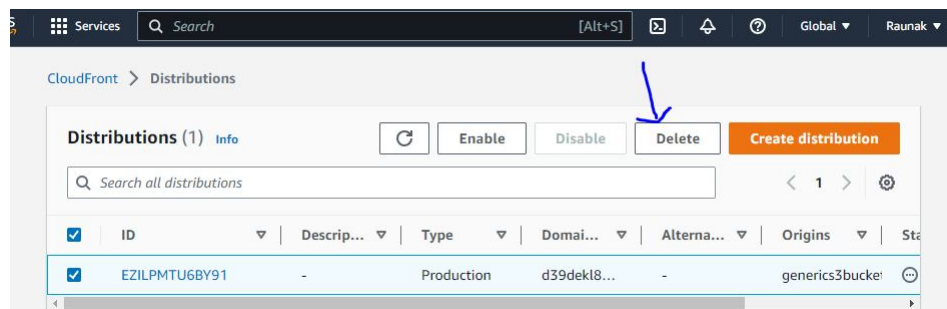


Figure 40: Disable the distribution service and delete the created distribution once experiment performed effectively

Conclusion

This experiment is successful demonstration of many facets associated with Amazon S3 Bucket. The S3 can be used to upload the files as well leverage the versioning abilities of it to keep track of the files. The deletion process can be done along with restoration and permanent deletion. The latter can be used to host a static website. Although the process is seamless but not recommended, the cloud front is another service provided by Amazon and can be used to create a distinguish hosting platform of the website hosted on S3. The service acts as a barrier between the basic files of the S3 and the public users. The cloud front provides its domain for distribution of the site. The execution of the all the process has been successfully shown in the results section of this experiment respectively.