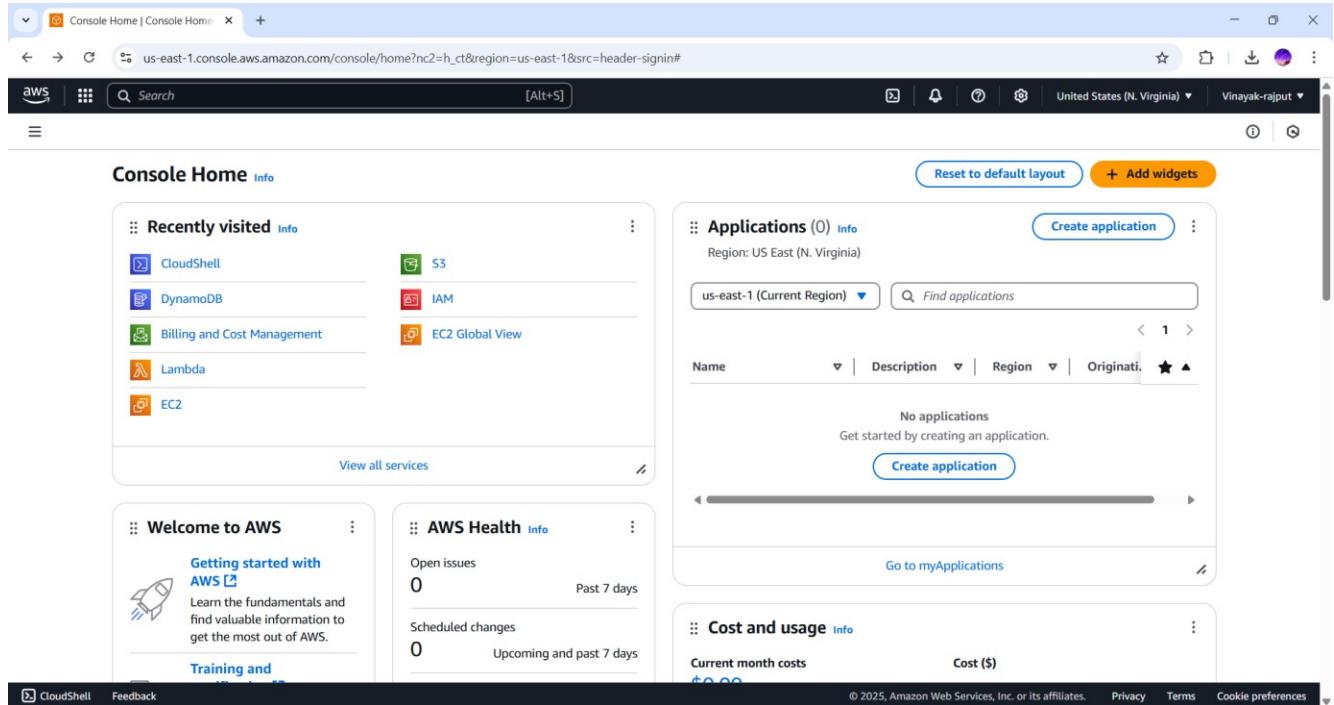


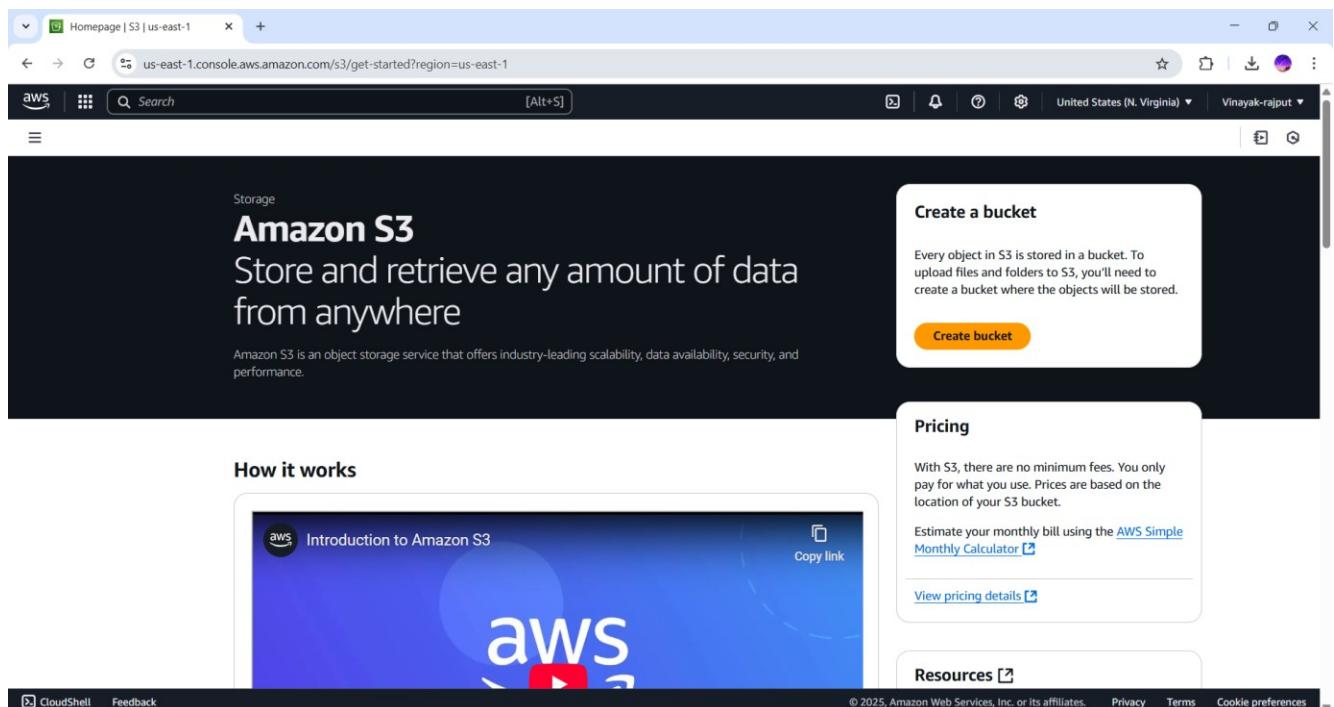
EXPERIMENT 2: Working with Amazon S3 Orchestrating Serverless Functions with AWS Step Functions

Steps for creating a S3 Bucket

Step 1: Login to AWS Account



Step 2: Open Amazon S3 Dashboard and click on Create Bucket button



Step 3: In General Configuration, Select Bucket type as General and type a Bucket name (e.g. Vinayak-aws-bucket)

Create bucket Info

Buckets are containers for data stored in S3.

General configuration

AWS Region
US East (N. Virginia) us-east-1

Bucket type Info

- General purpose

Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
- Directory

Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name Info

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

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

Format: s3://bucket/prefix

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.

Step 4: Uncheck Block all public access option under Block Public Access settings for this bucket and also check the acknowledgement displayed inside Yellow Caution box

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](#)

Step 5: Turn on Bucket Versioning by checking Enable option

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

Tags - optional (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

[Add tag](#)

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Step 6: Leave rest of options as default and click on Create Bucket button

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

Advanced settings

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

[Cancel](#) [Create bucket](#)

Step 7: Notification regarding successful creation of bucket would be displayed

The screenshot shows the AWS S3 buckets page in the US East (N. Virginia) region. A green success message at the top states: "Successfully created bucket 'vinayak-aws-bucket'". Below it, a note says: "To upload files and folders, or to configure additional bucket settings, choose View details." A "View details" button is shown. Under the "Account snapshot" section, there is a note about Storage lens and a "View Storage Lens dashboard" button. The "General purpose buckets" tab is selected, showing one bucket named "vinayak-aws-bucket". The table includes columns for Name, AWS Region, IAM Access Analyzer, and Creation date. The bucket details show it was created on March 23, 2025, at 01:26:34 (UTC+05:30). Action buttons for Copy ARN, Empty, Delete, and Create bucket are available.

Steps for Uploading a File

Step 1: Go to General purpose buckets and Click on bucket created.

The screenshot shows the AWS S3 buckets page in the US East (N. Virginia) region. The left sidebar has sections for General purpose buckets, Directory buckets, Table buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and IAM Access Analyzer for S3. It also includes a Block Public Access settings for this account section and a Storage Lens section with Dashboards, Storage Lens groups, and AWS Organizations settings. A Feature spotlight section is at the bottom. The main content area shows the "General purpose buckets" section with one item: "General purpose buckets (1/1)". The table lists the bucket "vinayak-aws-bucket" with details: Name (vinayak-aws-bucket), AWS Region (US East (N. Virginia) us-east-1), IAM Access Analyzer (View analyzer for us-east-1), and Creation date (March 23, 2025, 01:26:34 (UTC+05:30)). Action buttons for Copy ARN, Empty, Delete, and Create bucket are present.

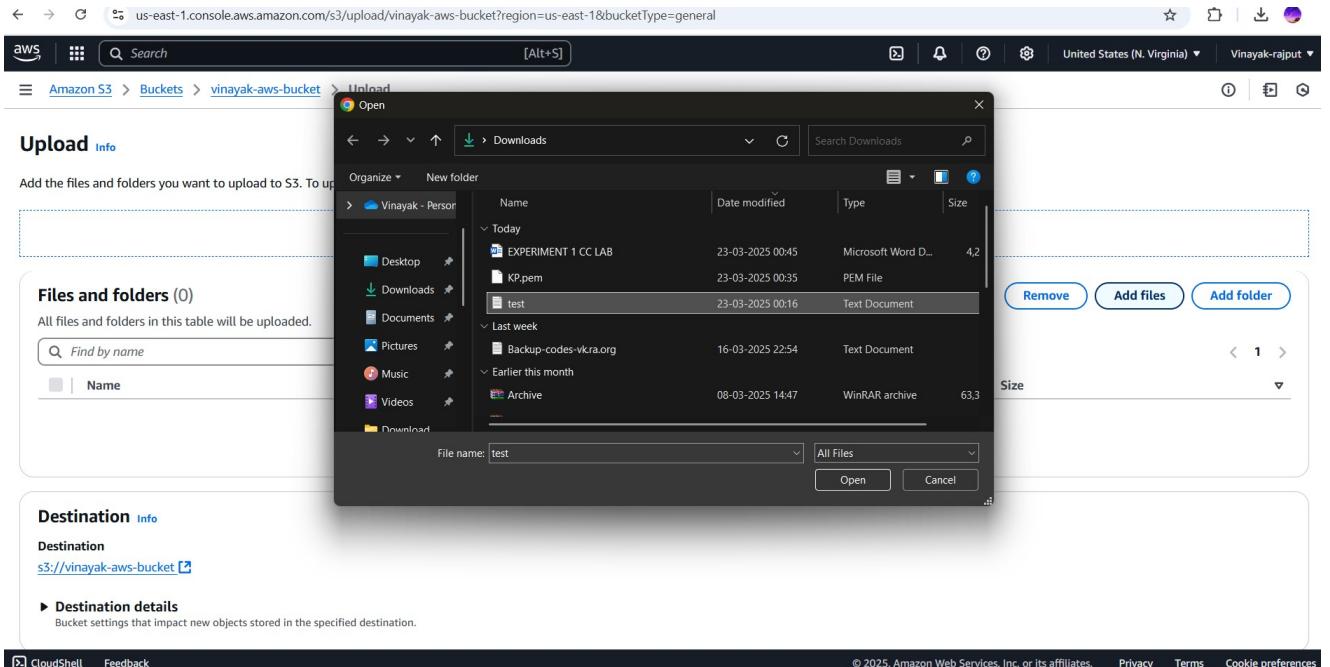
Step 2: Click on Upload button

The screenshot shows the AWS S3 console interface. The top navigation bar includes the AWS logo, a search bar, and account information for 'United States (N. Virginia)' and 'Vinayak-rajput'. Below the navigation is a breadcrumb trail: 'Amazon S3 > Buckets > vinayak-aws-bucket'. The main content area is titled 'vinayak-aws-bucket' with a 'Info' link. A horizontal menu bar below the title includes 'Objects', 'Metadata', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects' tab is selected. Under the heading 'Objects (0)', there is a note: '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](#)'. Below this is a search bar labeled 'Find objects by prefix' and a set of sorting and filtering options: 'Name' (sorted ascending), 'Type', 'Last modified' (sorted descending), 'Size' (sorted descending), and 'Storage class'. A message 'No objects' indicates that the bucket currently contains no files. At the bottom of the list is a prominent blue 'Upload' button.

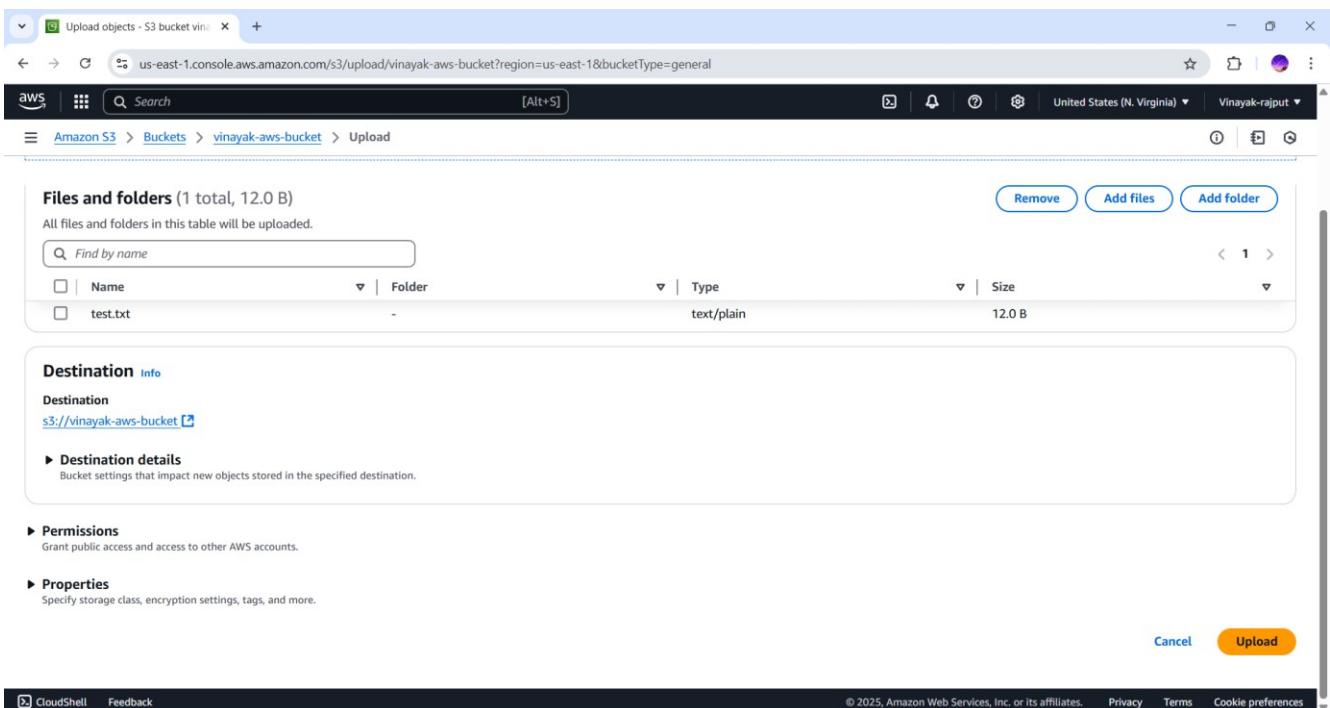
Step 3: Click on Add files

The screenshot shows the AWS S3 console interface, similar to the previous one but with a different tab selected. The top navigation bar and account information are the same. The breadcrumb trail shows the user has navigated to the 'Upload' section of the 'vinayak-aws-bucket'. The main content area is titled 'Upload' with a 'Info' link. Below it is a note: 'Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)'. A large blue 'Upload' button is prominently displayed. Below this is a section titled 'Files and folders (0)' with a note: 'All files and folders in this table will be uploaded.' A search bar 'Find by name' and sorting/filtering options for 'Name', 'Type', and 'Size' are present. A message 'No files or folders' indicates nothing has been uploaded yet. At the bottom, there is a 'Destination' section with a 'Info' link, showing the destination as 's3://vinayak-aws-bucket'. A 'Destination details' section provides information about bucket settings. The footer includes standard AWS links: CloudShell, Feedback, © 2025, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

Step 4: Select the file to upload and click on open



Step 5: Scroll down and click on Upload



Step 6: Upload successful notification is displayed we can see the properties of the file (test.txt) by clicking on the file name

The screenshot shows the AWS S3 console with the following details:

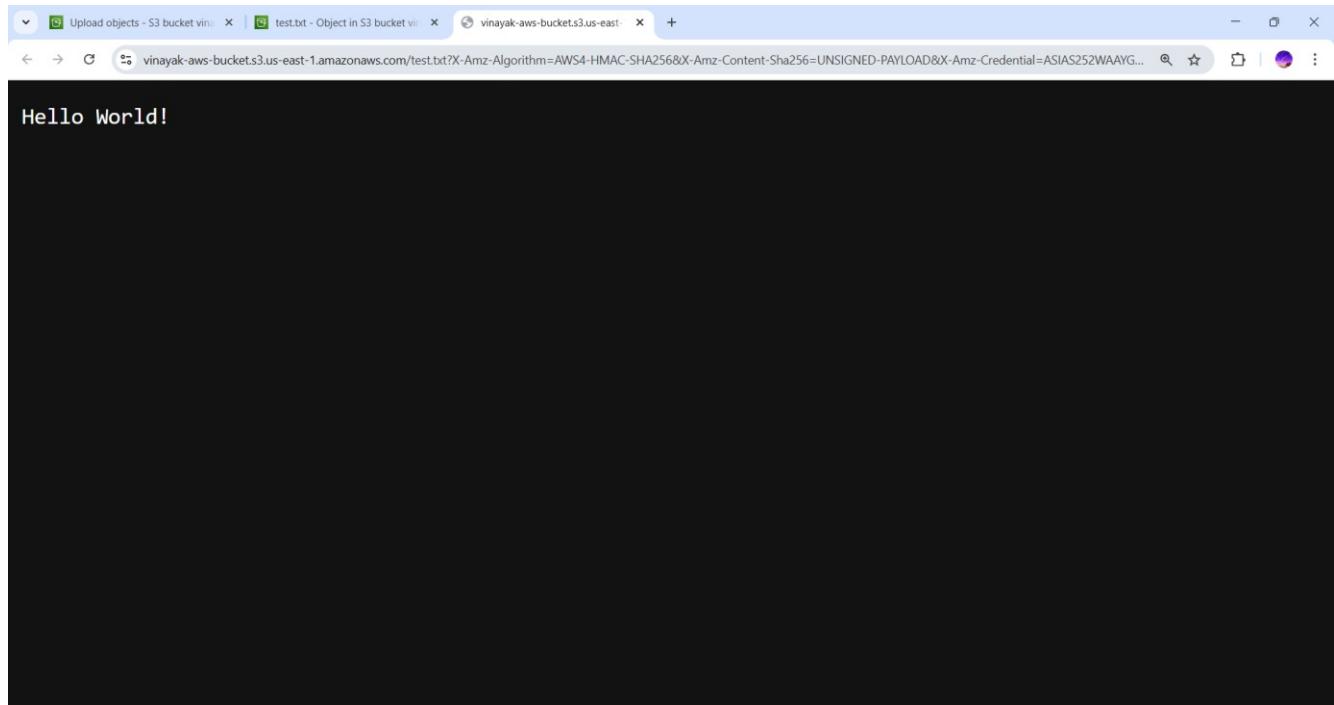
- Upload status:** A green banner at the top indicates "Upload succeeded".
- Summary:**
 - Destination:** s3://vinayak-aws-bucket
 - Succeeded:** 1 file, 12.0 B (100.00%)
 - Failed:** 0 files, 0 B (0%)
- Files and folders:** A table showing 1 total file (test.txt). The file is text/plain, 12.0 B, and has a status of "Succeeded".

Step 7: Click on Open option to view contents of file uploaded

The screenshot shows the AWS S3 object details page for "test.txt". The object overview includes the following information:

- Owner:** vk21112002ra
- AWS Region:** US East (N. Virginia) us-east-1
- Last modified:** March 23, 2025, 01:36:18 (UTC+05:30)
- Size:** 12.0 B
- Type:** txt
- Key:** test.txt
- S3 URI:** s3://vinayak-aws-bucket/test.txt
- Amazon Resource Name (ARN):** arn:aws:s3:::vinayak-aws-bucket/test.txt
- Entity tag (Etag):** ed076287532e86365e841e92bfc50d8c
- Object URL:** https://vinayak-aws-bucket.s3.us-east-1.amazonaws.com/test.txt

Step 8: Contents of the file will be opened in a new tab



Step 9: Go back and click on Version tab of Uploaded Files and keep track of version of uploaded file

A screenshot of the AWS S3 console. The left sidebar shows navigation options like 'Amazon S3', 'General purpose buckets', and 'Storage Lens'. The main content area shows the 'test.txt' file in the 'vinayak-aws-bucket' bucket. The 'Versions' tab is selected. A table lists one version of the file:

	Version ID	Type	Last modified	Size	Storage class
<input type="checkbox"/>	AzF4X4NudwbH_L0sgT...	txt	March 23, 2025, 01:36:18 (...)	12.0 B	Standard

Step 10: Now change the contents of same file on local system and upload the file again and check the versions tab and observe the newer version created and once again open the file

Version ID	Type	Last modified	Size	Storage class
s_APXdekVdu5aWG4EhTfpkf4dA...	txt	March 23, 2025, 01:43:25 (UTC+05:30)	32.0 B	Standard
AzfFX4NudwbH_L0sg.TBk02U...	txt	March 23, 2025, 01:36:18 (UTC+05:30)	12.0 B	Standard

Step 11: Observe the changes made in the file contents

Steps for Static Website Hosting:

Step 1: Go to properties tab of your bucket

Bucket overview

AWS Region: US East (N. Virginia) us-east-1

Amazon Resource Name (ARN): arn:aws:s3:::vinayak-aws-bucket

Creation date: March 23, 2025, 09:05:16 (UTC+05:30)

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: Enabled

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

Tags (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

Step 2: In Static Website Hosting click on edit

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. Object Lock works only in versioned buckets. [Learn more](#)

Object Lock: Disabled

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](#)

We recommend using AWS Amplify Hosting for static website hosting. Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) or [View your existing Amplify apps](#).

Create Amplify app

S3 static website hosting: Disabled

Step 3: Select Enable and give document name which you want to be used as your Index page in your static website

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

Static website hosting

Disable
 Enable

Hosting type

Host a static website
Use the bucket endpoint as the web address. [Learn more](#)

Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

ⓘ 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.
host.txt

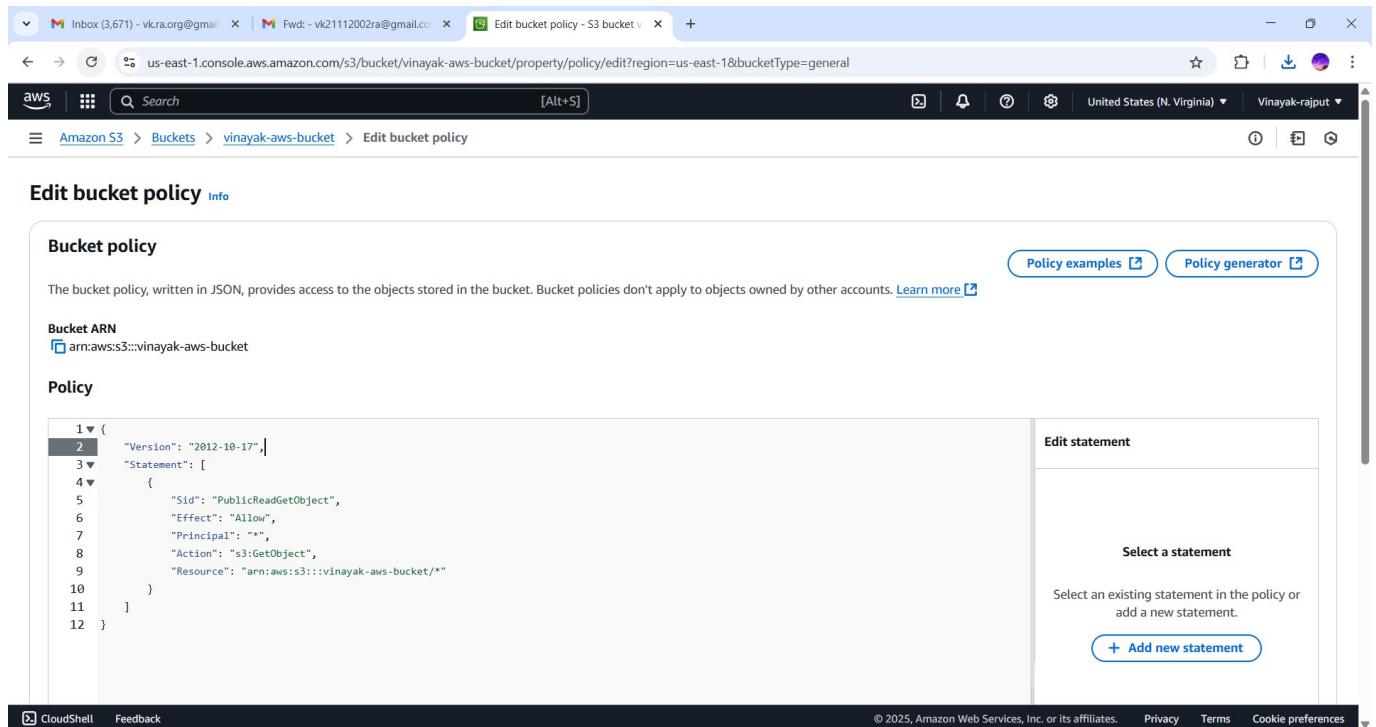
Error document - optional
This is returned when an error occurs.
error.html

Step 4: Scroll down and click on Save changes

JSON Ln 1, Col 1 Errors: 0 Warnings: 0

Cancel Save changes

Step 5: Go to Permissions tab > Edit Bucket Policy



The screenshot shows the AWS S3 Bucket Policy editor. The left pane displays the JSON policy code:

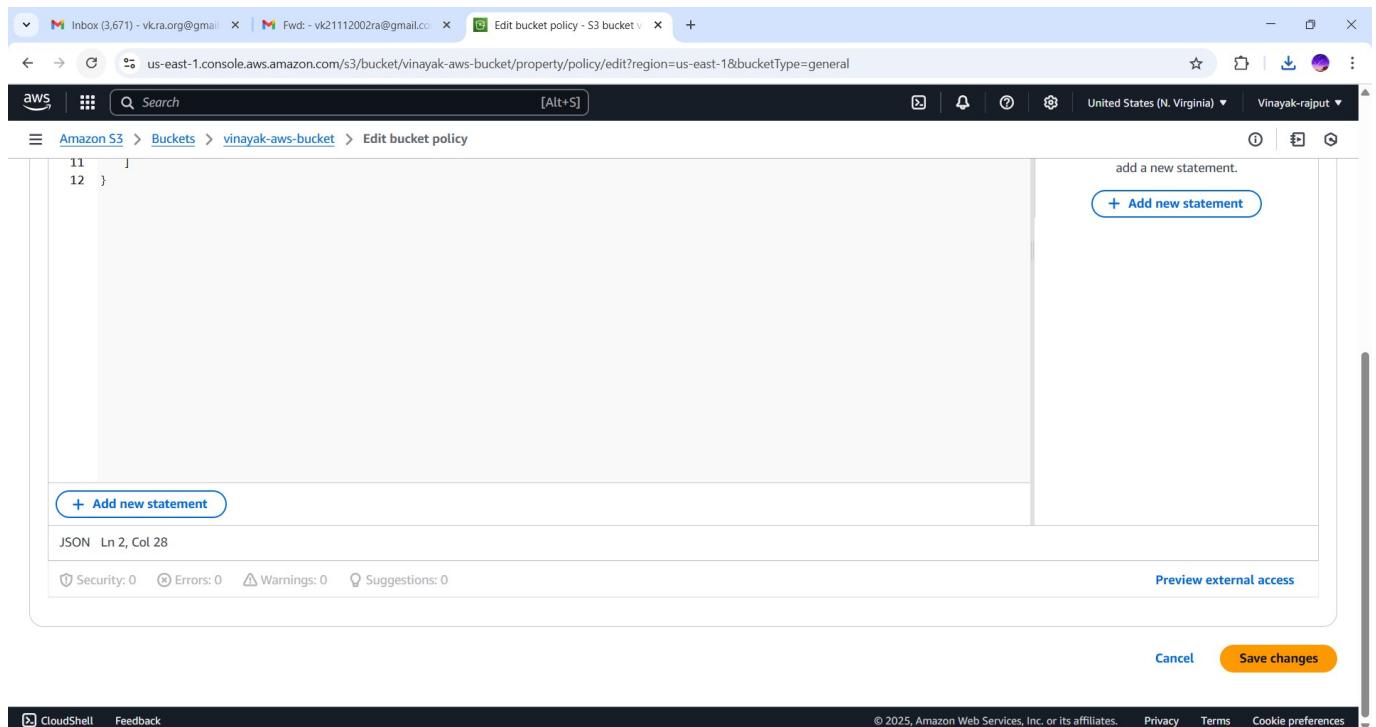
```

1  {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "PublicReadGetObject",
6       "Effect": "Allow",
7       "Principal": "*",
8       "Action": "s3:GetObject",
9       "Resource": "arn:aws:s3:::vinayak-aws-bucket/*"
10    }
11  ]
12 }

```

The right pane contains buttons for "Edit statement", "Select a statement", and "+ Add new statement". Below these buttons is a note: "Select an existing statement in the policy or add a new statement." At the bottom of the right pane is a large blue button labeled "+ Add new statement".

Step 6: Scroll down and click on Save Changes



The screenshot shows the AWS S3 Bucket Policy editor with the cursor at the end of the JSON code. The right pane includes a note: "add a new statement." and a blue button "+ Add new statement". At the bottom of the right pane is a large blue button labeled "+ Add new statement".

At the bottom of the editor, there is a status bar with "JSON Ln 2, Col 28" and a security summary: "Security: 0 Errors: 0 Warnings: 0 Suggestions: 0". To the right of the status bar are buttons for "Preview external access", "Cancel", and a large orange "Save changes" button.

Step 7: Upload the Index document (if yet to be uploaded) and got to Static Website hosting again and click on URL provided

The screenshot shows the AWS S3 console interface for a bucket named 'vinayak-aws-bucket'. The 'Static website hosting' section is open, indicating that the bucket is configured to host a website. A note recommends using AWS Amplify Hosting for static website hosting. The 'Bucket website endpoint' field displays the URL <http://vinayak-aws-bucket.s3-website-us-east-1.amazonaws.com>.

Step 8: Observe the Contents of your file hosted as a static webpage

The screenshot shows a web browser window displaying the static website hosted by the S3 bucket. The page content reads 'Hello AWS! Contents are changed!'.

Steps for Deletion of Files and S3 bucket:

Step 1: Go back to bucket name tab, select the file and click on Delete option

vinayak-aws-bucket [Info](#)

Objects (1/1)

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](#)

<input checked="" type="checkbox"/> Name	Type	Last modified	Size	Storage class
test.txt	txt	March 23, 2025, 01:43:25 (UTC+05:30)	32.0 B	Standard

Step 2: Type delete and click on Delete objects option

Delete objects - S3 bucket vinayak-aws-bucket

If a folder is selected for deletion, all objects in the folder will be deleted, and any new objects added while the delete action is in progress might also be deleted. If an object is selected for deletion, any new objects with the same name that are uploaded before the delete action is completed will also be deleted.

Deleting the specified objects adds delete markers to them. If you need to undo the delete action, you can delete the delete markers. [Learn more](#)

Specified objects

<input checked="" type="checkbox"/> Find objects by name
<input checked="" type="checkbox"/> test.txt

Delete objects?

To confirm deletion, type **delete** in the text input field.

delete

Cancel **Delete objects**

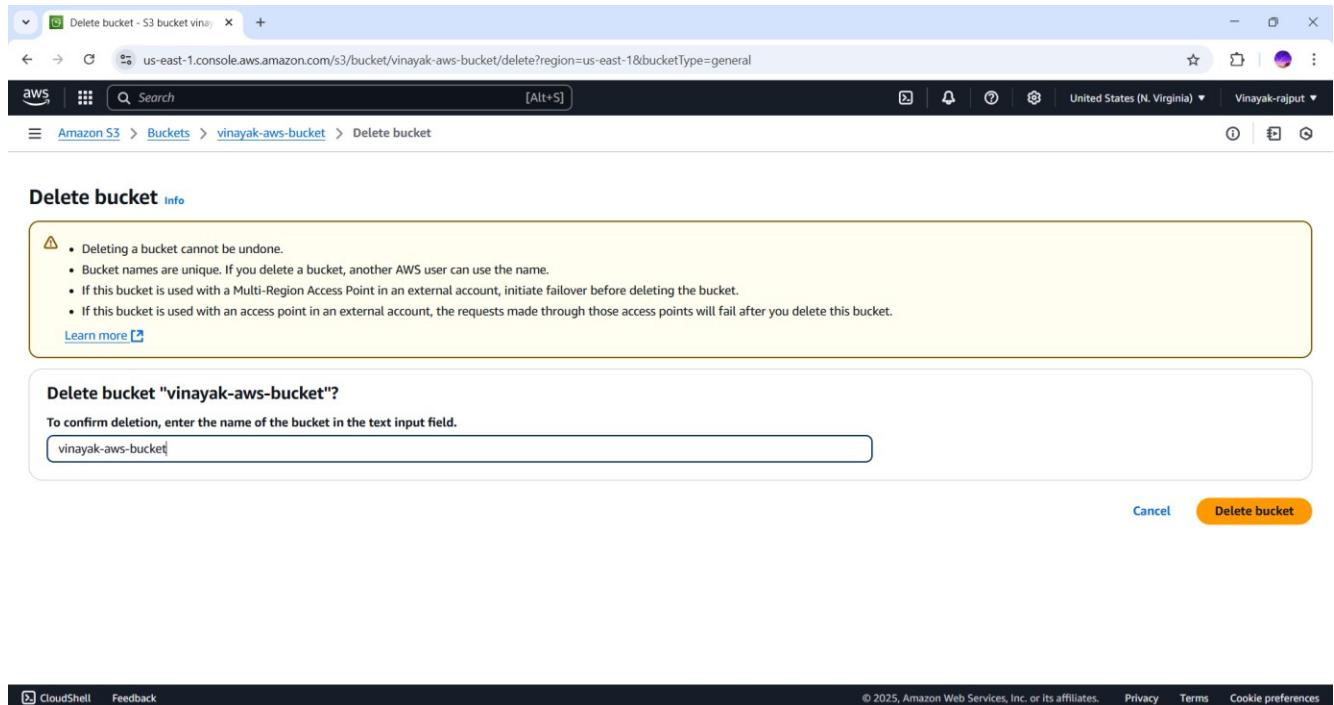
Step 3: Similarly go to General purpose buckets and select the bucket to be deleted and click on Delete option

The screenshot shows the AWS S3 console with the URL us-east-1.console.aws.amazon.com/s3/buckets?region=us-east-1&bucketType=general. The page title is "S3 buckets | S3 | us-east-1". The navigation bar includes "Search" and "Amazon S3 > Buckets". The main content area has tabs for "General purpose buckets" (selected) and "Directory buckets". A banner at the top says "Account snapshot - updated every 24 hours" and "Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)". Below this, a table lists the bucket "vinayak-aws-bucket" with details: Name (vinayak-aws-bucket), AWS Region (US East (N. Virginia) us-east-1), IAM Access Analyzer (View analyzer for us-east-1), and Creation date (March 23, 2025, 01:26:34 (UTC+05:30)). Action buttons include "Copy ARN", "Empty", "Delete", and "Create bucket". The bottom of the page includes links for CloudShell, Feedback, and various AWS terms like Privacy, Terms, and Cookie preferences.

Step 4: Confirm the permanent deletion of all objects inside the bucket

The screenshot shows the AWS S3 console with the URL us-east-1.console.aws.amazon.com/s3/bucket/vinayak-aws-bucket/empty?region=us-east-1&bucketType=general. The page title is "Empty bucket - S3 bucket vinayak-aws-bucket". The navigation bar includes "Search" and "Amazon S3 > Buckets > vinayak-aws-bucket > Empty bucket". The main content area has a heading "Empty bucket" with a "Info" link. A warning box contains the following text: "Emptying the bucket deletes all objects in the bucket and cannot be undone. Objects added to the bucket while the empty bucket action is in progress might be deleted. To prevent new objects from being added to this bucket while the empty bucket action is in progress, you might need to update your bucket policy to stop objects from being added to the bucket." It also includes a "Learn more" link. Below this, a note says "If your bucket contains a large number of objects, creating a lifecycle rule to delete all objects in the bucket might be a more efficient way of emptying your bucket." with a "Learn more" link and a "Go to lifecycle rule configuration" link. A large input field contains the text "permanently delete". At the bottom right are "Cancel" and "Empty" buttons. The bottom of the page includes links for CloudShell, Feedback, and various AWS terms like Privacy, Terms, and Cookie preferences.

Step 5: Delete the bucket by typing its name



Step 6: Successful deletion notification is displayed indicating successful deletion of our bucket After this we can sign out from our AWS account

