

PROJECT-2

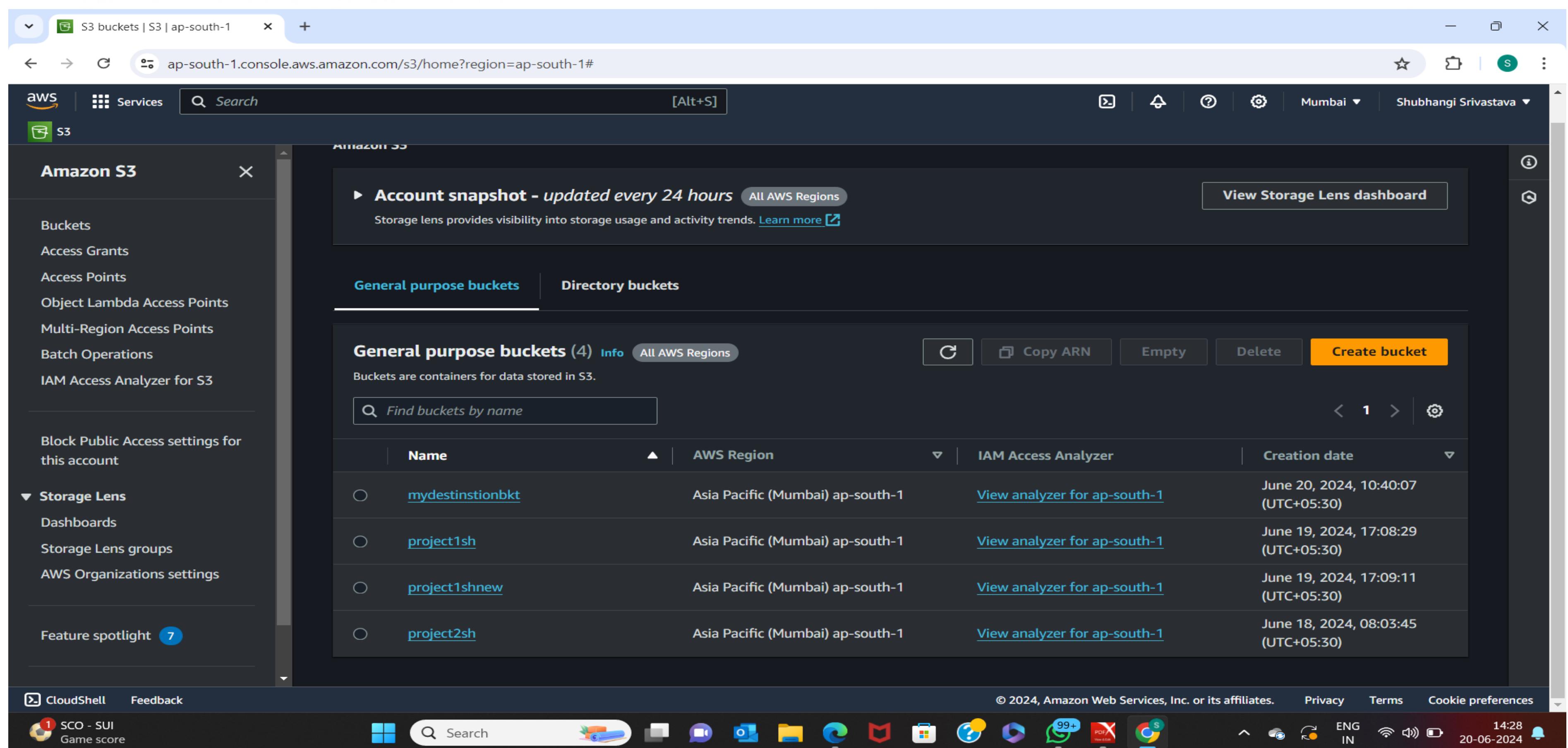
Deploy a static website on AWS

Step 1: Creating a Bucket

First, we have to launch our S3 instance. Follow these steps for creating a Bucket

Open the Amazon S3 console by logging into the AWS Management Console at <https://console.aws.amazon.com/s3/>.

Click on Create Bucket.



The screenshot shows the AWS S3 console interface. On the left, there is a sidebar with options like Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and IAM Access Analyzer for S3. Below this is a section for Block Public Access settings for this account. Under Storage Lens, there are options for Dashboards, Storage Lens groups, and AWS Organizations settings. A Feature spotlight section is also present. The main content area displays an Account snapshot and a General purpose buckets table. The table lists four buckets: mydestinationbkt, project1sh, project1shnew, and project2sh. Each entry includes the bucket name, AWS Region (Asia Pacific (Mumbai) ap-south-1), IAM Access Analyzer link, and Creation date. At the top right of the main area, there are buttons for Create bucket, Copy ARN, Empty, and Delete. A search bar and a 'Find buckets by name' input field are also visible. The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray.

Name	AWS Region	IAM Access Analyzer	Creation date
mydestinationbkt	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	June 20, 2024, 10:40:07 (UTC+05:30)
project1sh	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	June 19, 2024, 17:08:29 (UTC+05:30)
project1shnew	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	June 19, 2024, 17:09:11 (UTC+05:30)
project2sh	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	June 18, 2024, 08:03:45 (UTC+05:30)

- Choose **Bucket Name** – Bucket Name Should be Unique
- **AWS Region** – Choose a region close to you or the region where you want to create the bucket (Example – Mumbai)
- **Object Ownership** – Enable for making Public, Otherwise disable

The screenshot shows the AWS S3 'Create bucket' interface. In the 'General configuration' section, the 'Bucket name' field contains 'project2'. Under 'Object Ownership', 'ACLs disabled (recommended)' is selected. A note at the bottom of the ownership section states: '⚠️ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.'

Step 2: Block Public Access settings for the bucket

Uncheck (Block all public access) for the public, otherwise set default. If you uncheck (Block all public keys).

The screenshot shows the 'Create S3 bucket' wizard on the AWS Management Console. The current step is 'Block Public Access settings for this bucket'. It includes a warning about turning off block all public access and a checkbox for acknowledging the risk.

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.

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- **Bucket Versioning:- You have to do Nothing (Disable)**
 - **Tags(0) : Optional**
 - **Default encryption: Disable**
- Now, click on Create Bucket

The screenshot shows the 'Create S3 bucket' wizard on the AWS Management Console. The current step is 'Default encryption'. It allows selecting the encryption type (Server-side encryption with Amazon S3 managed keys (SSE-S3)) and enabling a Bucket Key.

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.

Create bucket

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Step 3: Now upload code files**
- **Select Bucket and Click your Bucket Name.**

The screenshot shows the AWS S3 console with the 'General purpose buckets' tab selected. There are four buckets listed:

Name	AWS Region	IAM Access Analyzer	Creation date
mydestinationbkt	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	June 20, 2024, 10:40:07 (UTC+05:30)
project1sh	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	June 19, 2024, 17:08:29 (UTC+05:30)
project1shnew	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	June 19, 2024, 17:09:11 (UTC+05:30)
project2sh	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	June 18, 2024, 08:03:45 (UTC+05:30)

Now, click on upload (then click add File/folder) and select your **HTML code** file from your PC/Laptop.

The screenshot shows the 'Upload' page for the 'project2sh' bucket. The 'Files and folders' section is currently empty, displaying the message 'No files or folders' and 'You have not chosen any files or folders to upload.'

Step 4: Once the Files are uploaded successfully, click on **Permissions** and now follow this Process –

. **Block public access:**

- . Click on **Edit**, under **Bucket Policy**.
- . Uncheck **Block all public access**.

. Save changes then type “confirm”.

The screenshot shows the AWS S3 console interface for creating a new bucket. The URL in the browser is `ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general`. The main content area is titled "Block Public Access settings for this bucket". It contains several checkboxes under the heading "Block all public access", each with a detailed description. A warning message in a yellow box states: "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." Below the message is a checkbox labeled "I acknowledge that the current settings might result in this bucket and the objects within becoming public." At the bottom of the page, there are standard AWS navigation links like CloudShell, Feedback, and a footer with copyright information and date (20-06-2024).

- **Object Ownership:**
 - Click on Edit.
 - Click on ACLs Enabled.
 - Check I acknowledge restored.
 - Choose Save Changes.

The screenshot shows the 'Create S3 bucket' wizard on the AWS console. The current step is 'Object Ownership'. It provides two options: 'ACLs disabled (recommended)' and 'ACLs enabled'. The 'ACLs enabled' option is selected, indicated by a blue border around its radio button. A warning message below it states: 'We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.' Under 'Object Ownership', the 'Bucket owner preferred' option is selected, marked with a blue dot. A note below it says: '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.' The bottom of the screen shows the AWS navigation bar with links for CloudShell, Feedback, and various services like CloudWatch, Lambda, and S3. The status bar at the bottom right shows the date (20-06-2024), time (14:29), and location (ENG IN).

Step 5:- Make public Object

- Now, Click on Objects.
- Select your All Objects.
- Now, Click on Actions.
- Select Make Public Using ACL.
- Now, Click on Make Public and Close.

Objects (1) [Info](#)

Name	Type	Last modified	Size	Storage class
shub.html	html	June 18, 2024, 08:10:59 (UTC+05:30)	89.0 B	Standard

Step 6: Copy your Object URL

- Now, click on your **HTML File Object Name**.
- Copy the **Object URL**.

Properties [Permissions](#) [Versions](#)

Object overview

Owner	S3 URI
9c86406e5cb9143b8126d1008b99cf2d35291d74d4203cbafc0abfc894469a77	s3://project2sh/shub.html
AWS Region	Amazon Resource Name (ARN)
Asia Pacific (Mumbai) ap-south-1	arn:aws:s3:::project2sh/shub.html
Last modified	Entity tag (Etag)
June 18, 2024, 08:10:59 (UTC+05:30)	8805e920283e959c1554b6c702db6788
Size	Object URL
89.0 B	https://project2sh.s3.ap-south-1.amazonaws.com/shub.html
Type	
html	
Key	
shub.html	

Step 7: Check out your Website!

- Directly Paste this URL into the Other Tab or your other System.
- Congratulation, Now Your Website is available in the Public.**

- You Successfully Host Your Website by AWS S3.to