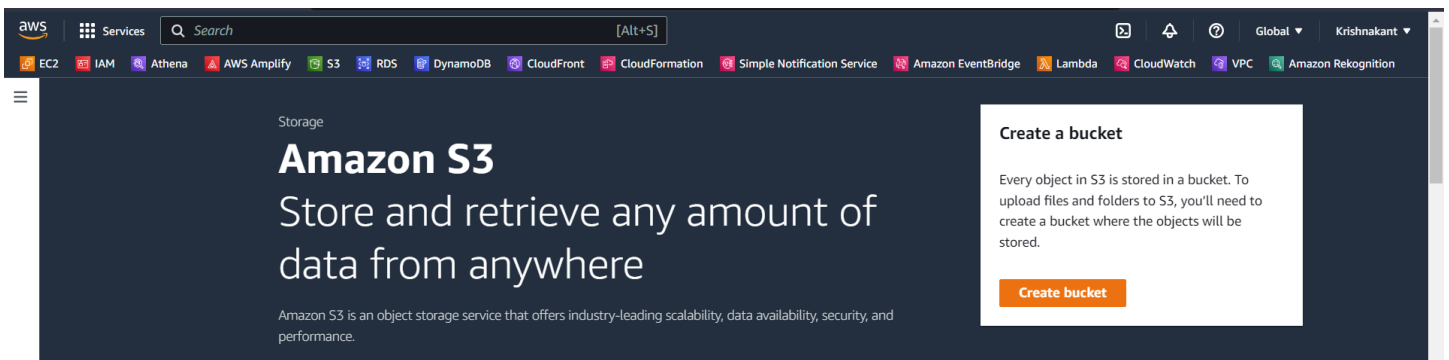


Task-1

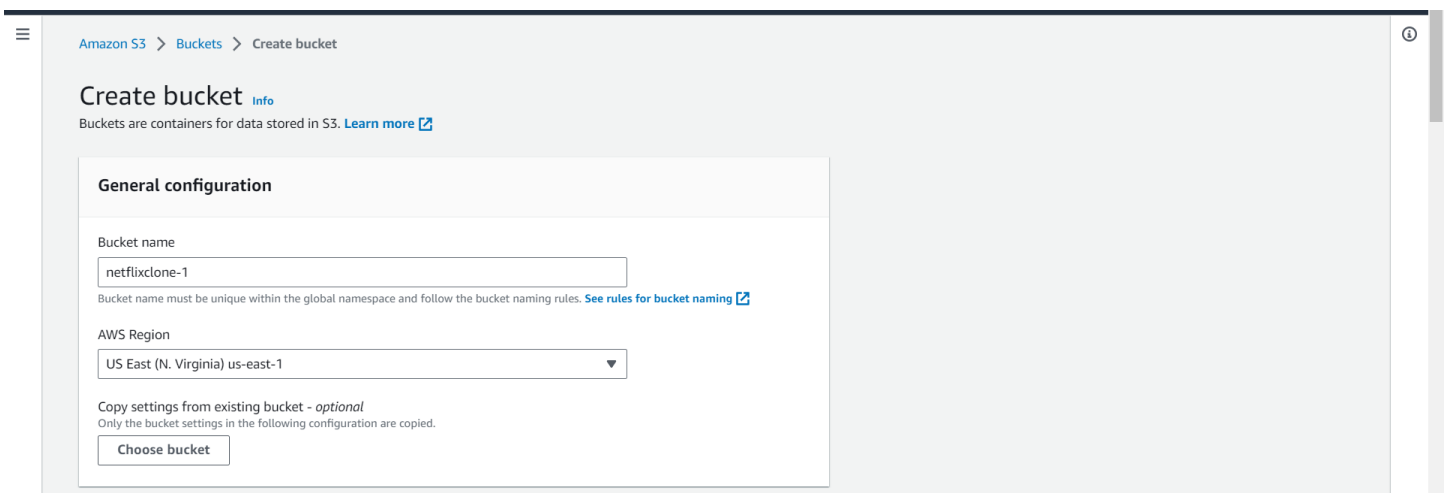
(Static Website Hosting on AWS S3)

Aim: Build a simple static website and host it on Amazon S3 (Simple Storage Service). Create an S3 bucket, upload your website files (HTML, CSS, and JavaScript), and configure the bucket for static website hosting. Access your website using the provided \$3 endpoint URL.

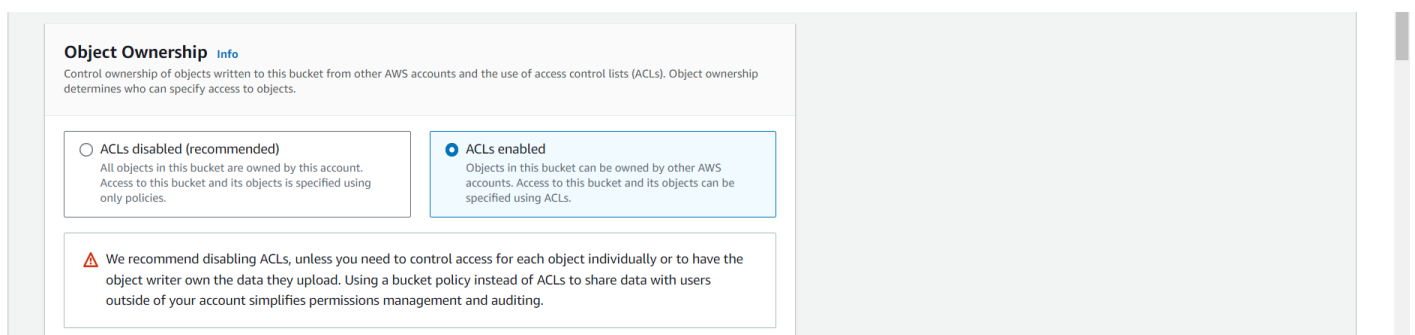
Step1: To Creating Bucket



1. Create a bucket with the name "netflixclone-1."



2. During the bucket creation process, look for the option to enable ACLs (Access Control Lists) and select it.



3. Uncheck or disable the "Block all public access" option to allow public access.

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.

4. You may see a warning or acknowledgment statement about the risks of making data public. Read and understand the implications.

**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.

5. Leave all other settings as they are, unless you have specific requirements that need customization.
6. Once all the settings are configured, you will be able to access and view your bucket effortlessly.

☰

✔ Successfully created bucket "netflixclone-1"
To upload files and folders, or to configure additional bucket settings choose [View details](#).


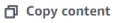


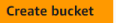
View details × ⓘ

Amazon S3 > Buckets


▶ Account snapshot
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

View Storage Lens dashboard

Buckets (1) [Info](#)
Buckets are containers for data stored in S3. [Learn more](#)

  Copy content  Empty  Delete  Create bucket

< 1 > ⓘ

	Name ▲	AWS Region ▼	Access ▼	Creation date ▼
	netflixclone-1	US East (N. Virginia) us-east-1	Objects can be public	August 4, 2023, 13:34:58 (UTC+05:30)

Step2: To upload your HTML, CSS, and JS files to the bucket, open the bucket and proceed with the following steps:

1. Click on the "Upload" button to begin the file upload process.
2. Select your HTML, CSS, and JS files from your local computer.
3. Confirm the upload by clicking the "Upload" button.
4. Once the files are successfully uploaded, you can access them within the bucket.

Amazon S3 > Buckets > netflixclone-1 > Upload

Upload

Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (19 Total, 1.2 MB)

RemoveAdd filesAdd folder

All files and folders in this table will be uploaded.

Find by name

< 1 2 >

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	fav.png	-	image/png	21.7 KB
<input type="checkbox"/>	favicon.ico.jpg	-	image/jpeg	17.2 KB
<input type="checkbox"/>	index.css	-	text/css	8.9 KB
<input type="checkbox"/>	index.html	-	text/html	15.9 KB
<input type="checkbox"/>	index.js	-	text/javascript	724.0 B

Destination

Destination

s3://netflixclone-1

Destination details

Bucket settings that impact new objects stored in the specified destination.

Permissions

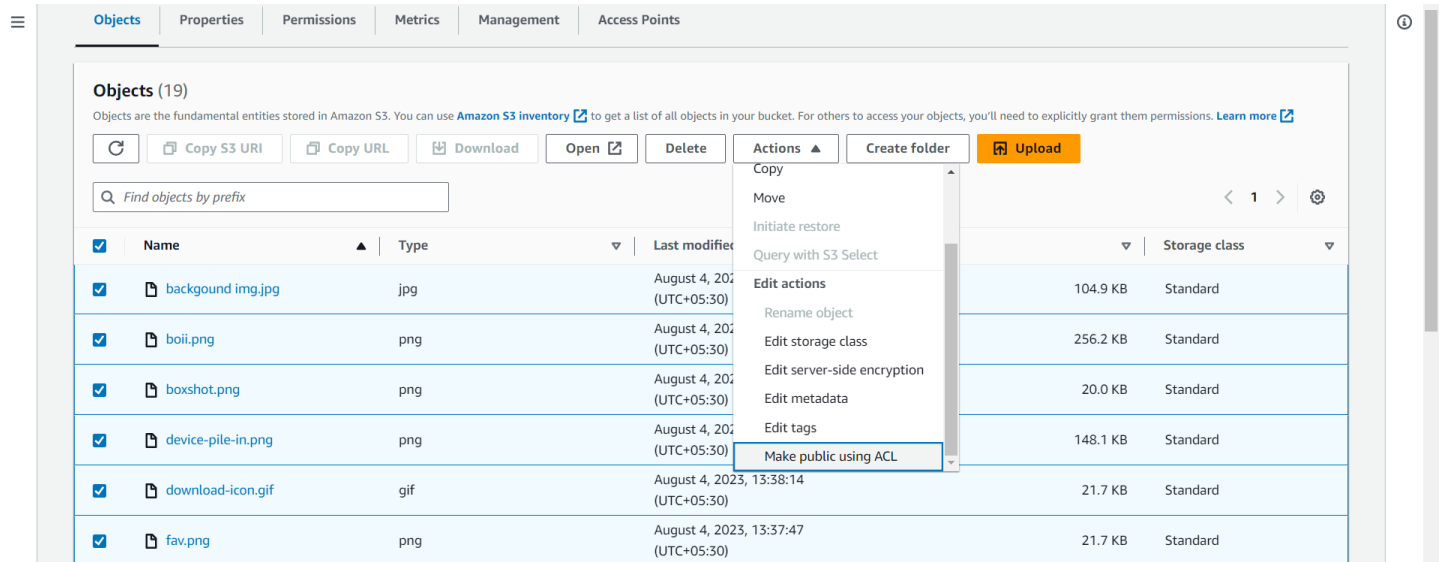
Grant public access and access to other AWS accounts.

Properties

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

CancelUpload

Step3: Select all the files and click on the Action drop-down menu. Then, click on "Make Public" using ACL (Access Control List).



Step4: To view the static website, you can simply copy the HTML object URL and paste it into your web browser's address bar. This will allow you to access and explore the content of the static website.

