Assignment -8

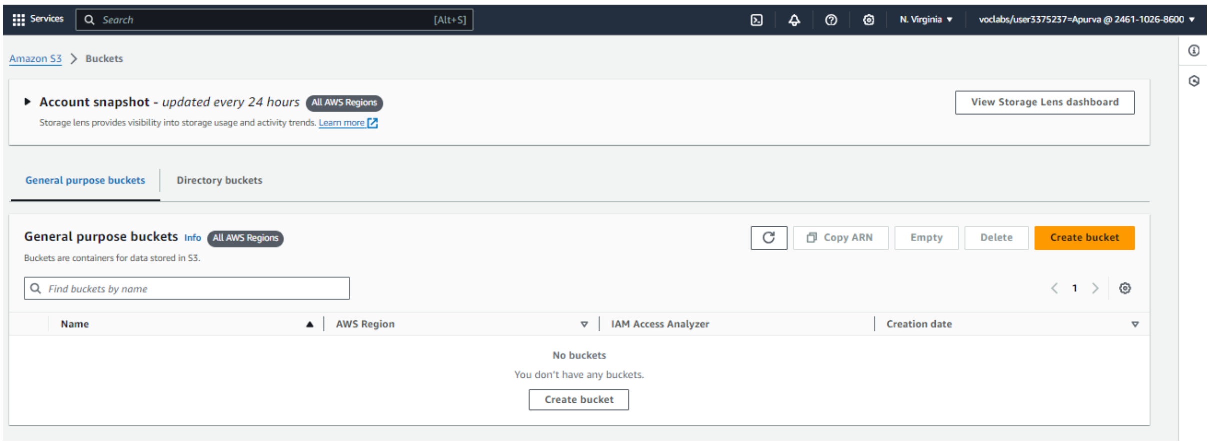
Practical Implementation of Storage as a Service Hosting a static website in AWS using S3. Prepare Screen shots file and also write down the steps. Make single word or PDF file

Step 1: Create an S3 Bucket

1. Log in to AWS Console.

2. Navigate to the S3 service from the AWS Management Console.

3. Click on Create bucket.



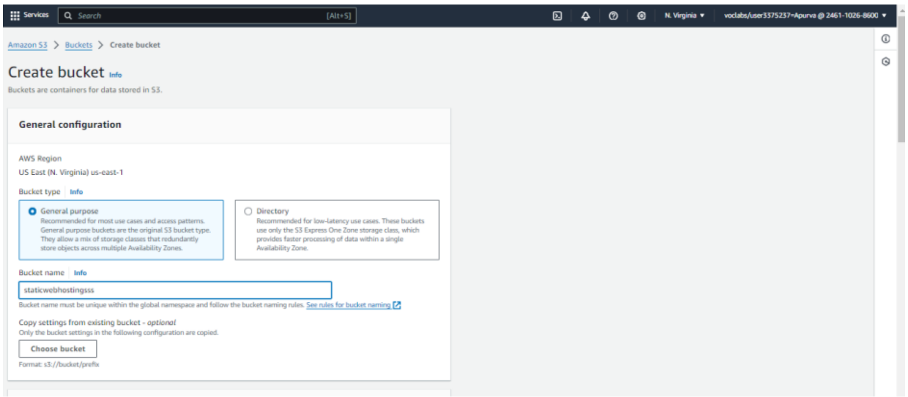
Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets are containers for data stored in S3.

No buckets

You don't have any buckets.

4. Bucket Name: Enter a unique bucket name (e.g., ` staticwebhostingsss `).



Services
Search [Alt+S]
N. Virginia ▾
voclabs/user3375237=Apurva @ 2461-1026-8600 ▾
Amazon S3 > Buckets > Create 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

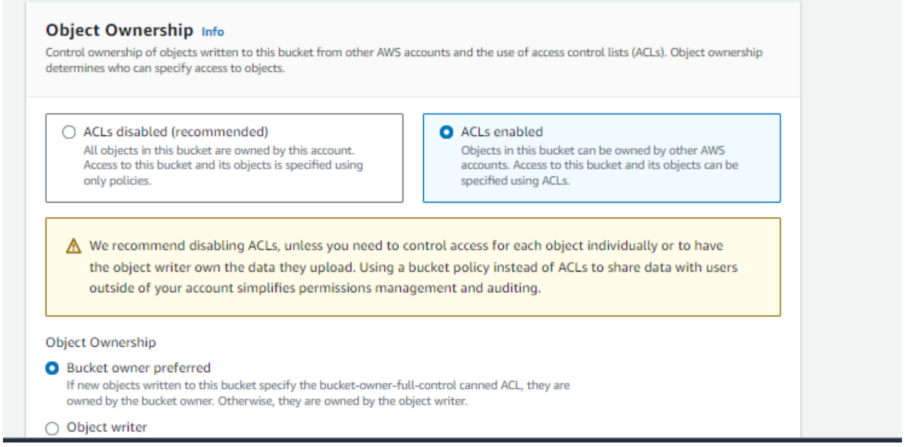
staticwebhostingsss

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

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

Format: s3://bucket/prefix

5.In Object Ownership,Enabled ACLs and keep all things as it is and click on Create Bucket.



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.

○ ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

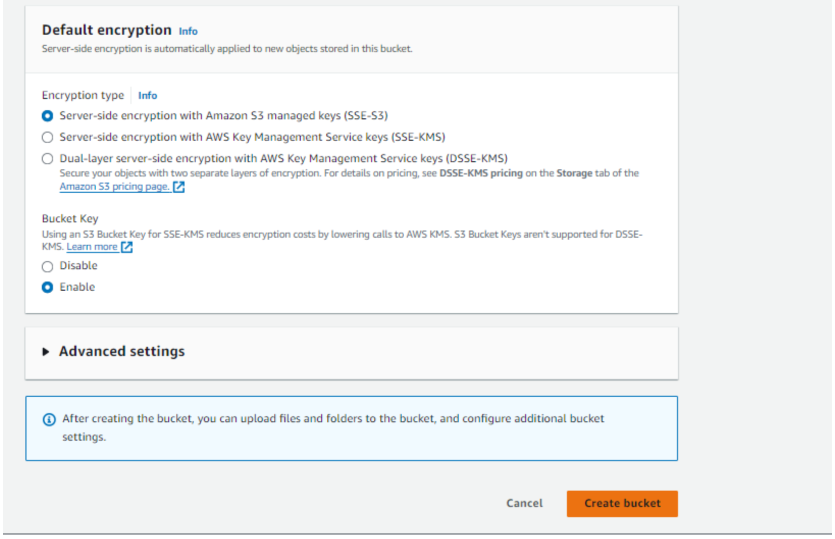
● ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

⚠ 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.

Object Ownership

● Bucket owner preferred
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.

○ Object writer



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

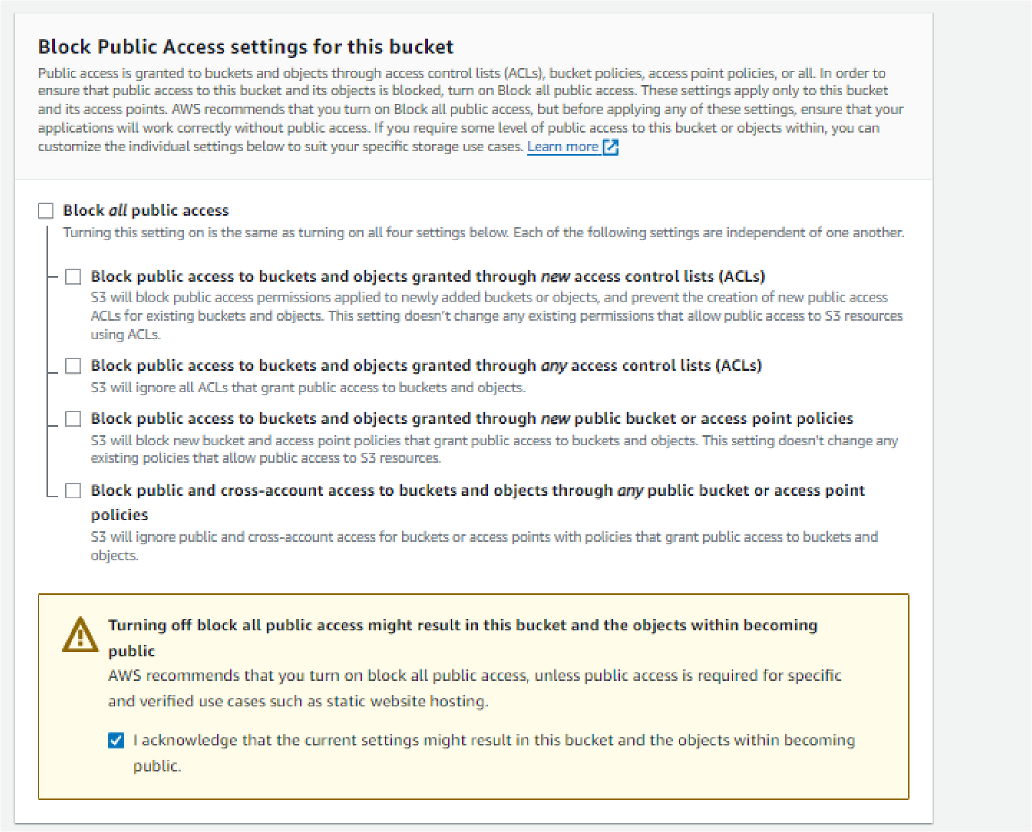
○ Disable

● Enable

▸ **Advanced settings**

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

6. Block Public Access: Uncheck the "Block all public access" option to allow public access to your website.



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.

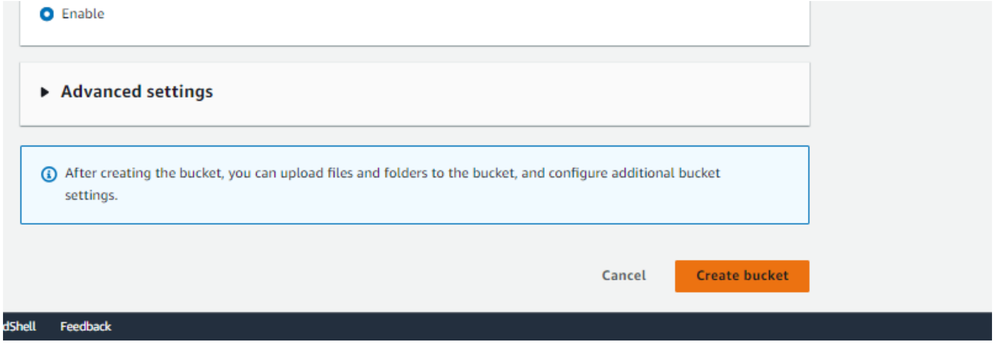
- □ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any 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.

7. Confirm by acknowledging the warning about public access.

8. Click Create bucket.

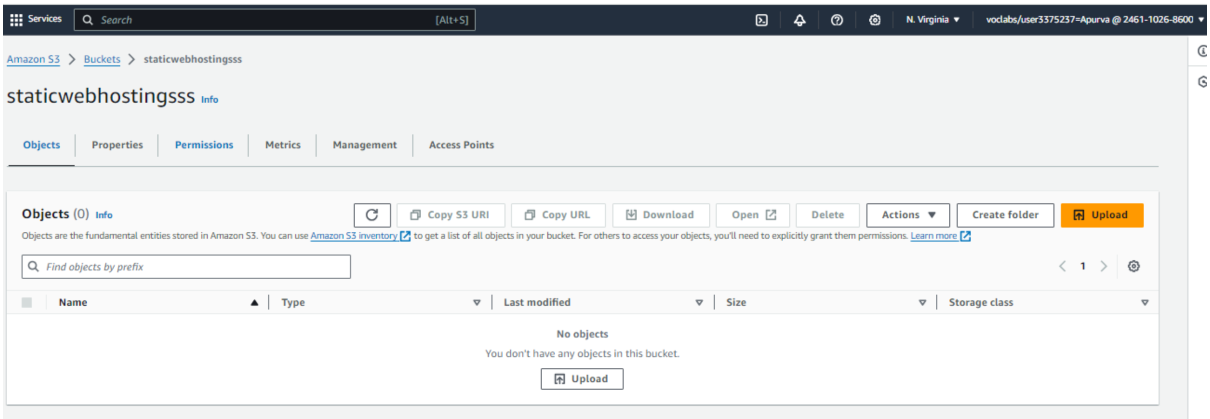


● Enable

▸ **Advanced settings**

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

9.In Bucket->permission edit the ACL and give list and read permission for public access of bucket.



Amazon S3 > Buckets > staticwebhostingsss

staticwebhostingsss

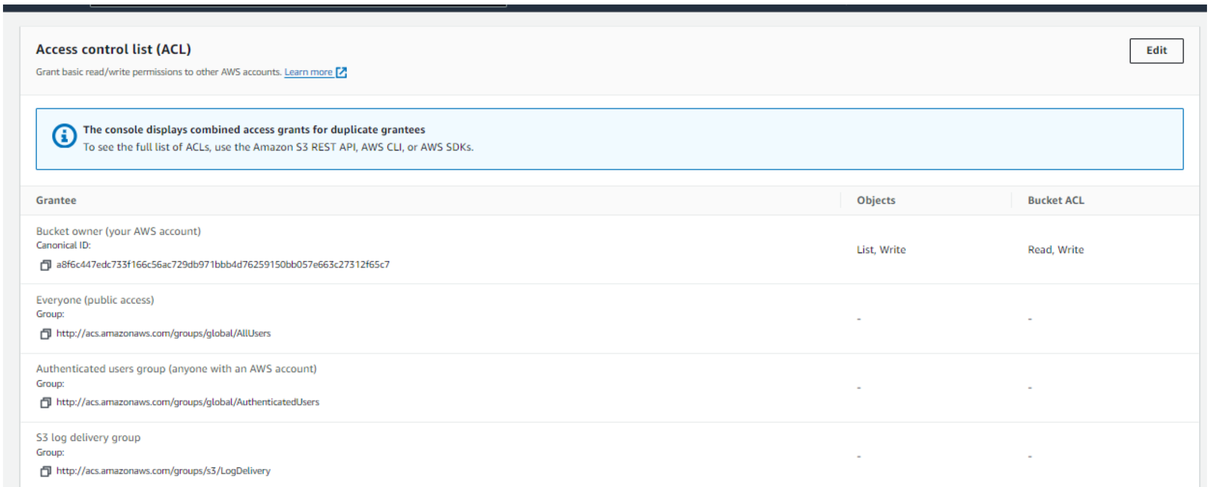
Objects (0)

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

Name	Type	Last modified	Size	Storage class

No objects

You don't have any objects in this bucket.

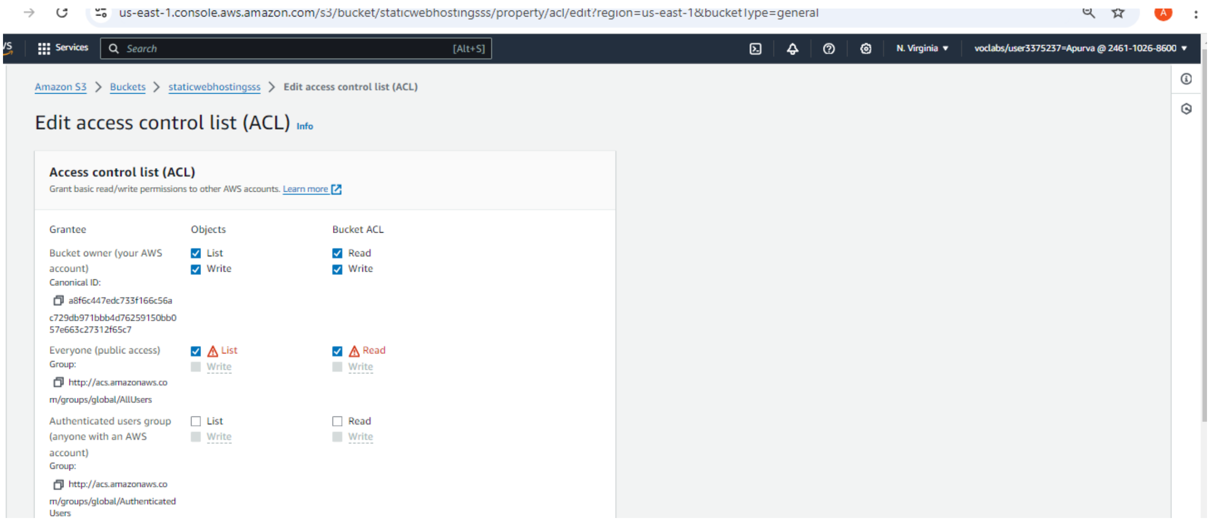


Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. Learn more

The console displays combined access grants for duplicate grantees
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: a8f6c447edc733f166c56ac729db971bbb4d76259150bb057e663c27312f65c7	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	-	-



us-east-1.console.aws.amazon.com/s3/bucket/staticwebhostingsss/property/acl/edit?region=us-east-1&bucketType=general

Amazon S3 > Buckets > staticwebhostingsss > Edit access control list (ACL)

Edit access control list (ACL)

Access control list (ACL)

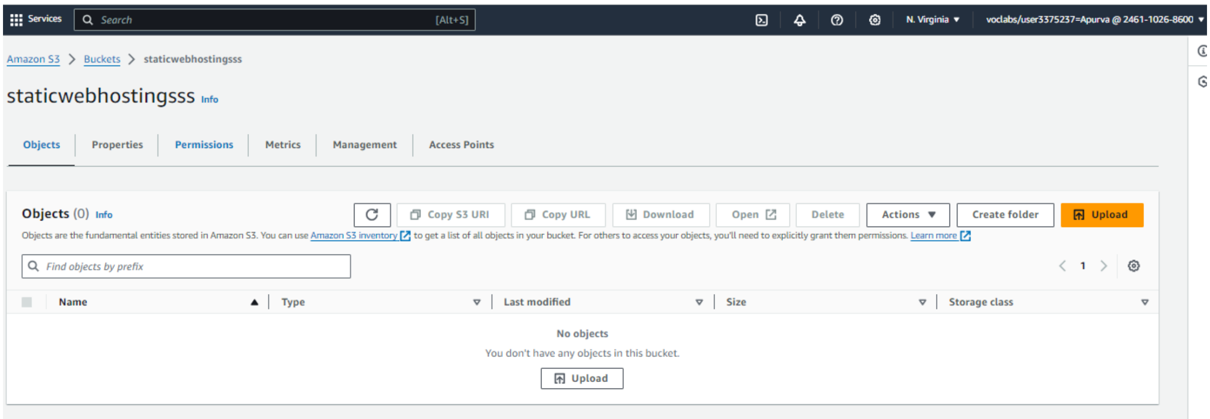
Grant basic read/write permissions to other AWS accounts. Learn more

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: a8f6c447edc733f166c56ac729db971bbb4d76259150bb057e663c27312f65c7	☑ List ☑ Write	☑ Read ☑ Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	☑ ⚠ List □ Write	☑ ⚠ Read □ Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	□ List □ Write	□ Read □ Write

Step 2: Upload Website Files

1. Click on your newly created bucket to open it.

2. Click on the Upload button.

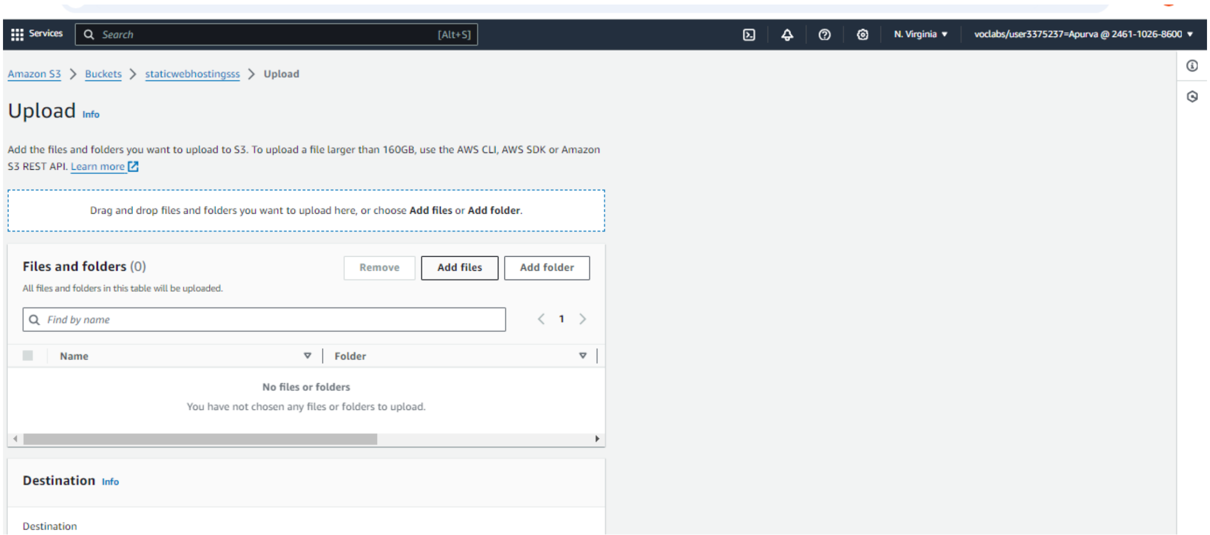


Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

No objects

You don't have any objects in this bucket.

3.then, add files and folders in it and upload it.



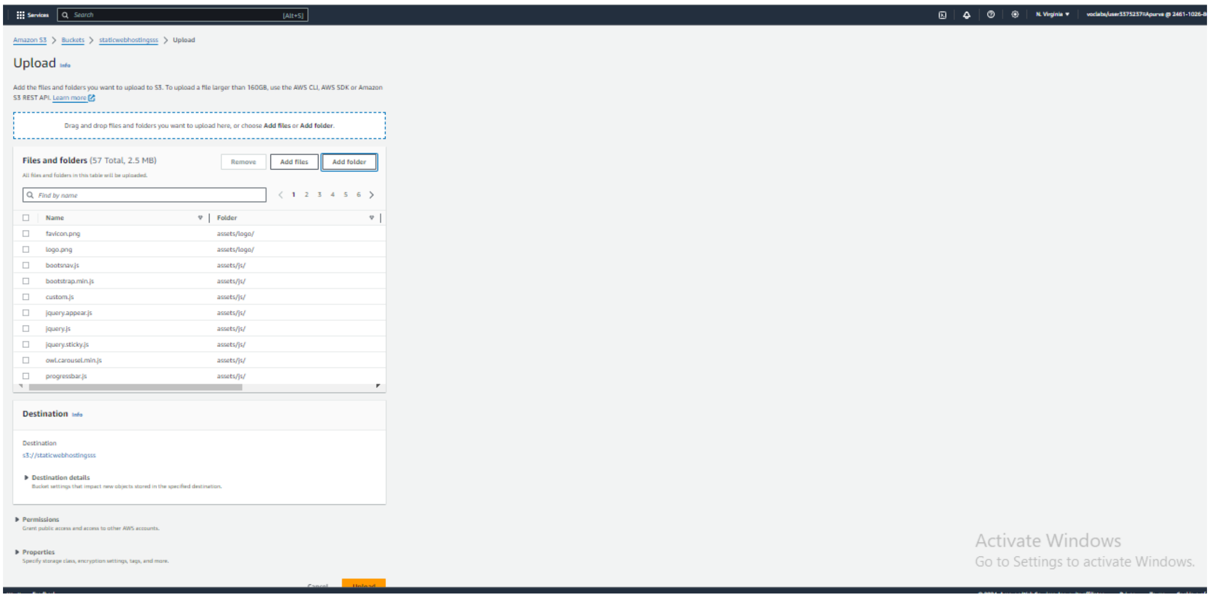
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

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

All files and folders in this table will be uploaded.

No files or folders

You have not chosen any files or folders to upload.


Services
Search
[Alt+S]
N. Virginia
voclabs/user3375237=Apurva @ 2461-1026-8
Amazon S3 > Buckets > staticwebhostingsss > Upload
Remove
Add files
Add folder
Find by name
1 2 3 4 5 6
Cancel
Upload
Activate Windows
Go to Settings to activate Windows.

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 (57 Total, 2.5 MB)

All files and folders in this table will be uploaded.

	Name	Folder
□	favicon.png	assets/logo/
□	logo.png	assets/logo/
□	bootsnav.js	assets/js/
□	bootstrap.min.js	assets/js/
□	custom.js	assets/js/
□	jquery.appear.js	assets/js/
□	jquery.js	assets/js/
□	jquery.sticky.js	assets/js/
□	owl.carousel.min.js	assets/js/
□	progressbar.js	assets/js/

Destination Info

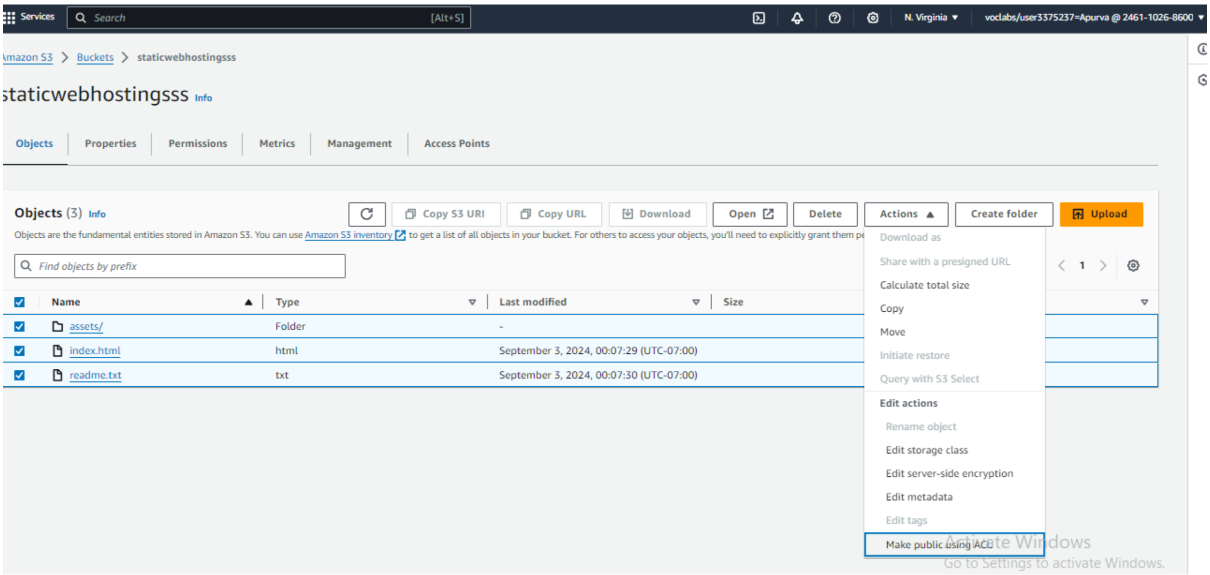
Destination
s3://staticwebhostingsss

▶ **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.

4.then,select the all files,and folders and go to Actions and click on Make public using ACL.



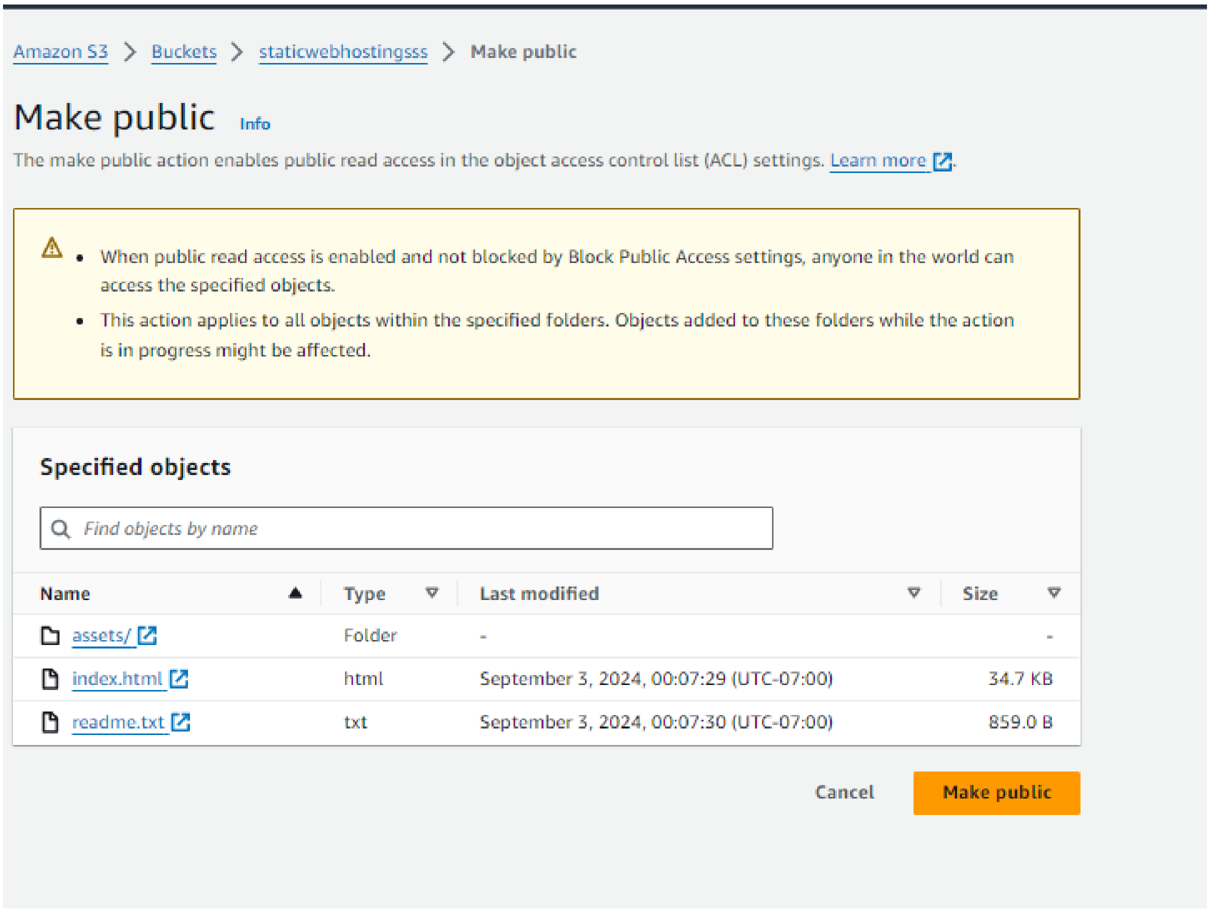
staticwebhostingsss Info

Objects (3) Info

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 pe

☑	Name	Type	Last modified	Size
☑	assets/	Folder	-	
☑	index.html	html	September 3, 2024, 00:07:29 (UTC-07:00)	
☑	readme.txt	txt	September 3, 2024, 00:07:30 (UTC-07:00)	

5.And then click on make public.



Amazon S3 > Buckets > staticwebhostingsss > Make public

Make public Info

The make public action enables public read access in the object access control list (ACL) settings. Learn more

- When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.
- This action applies to all objects within the specified folders. Objects added to these folders while the action is in progress might be affected.

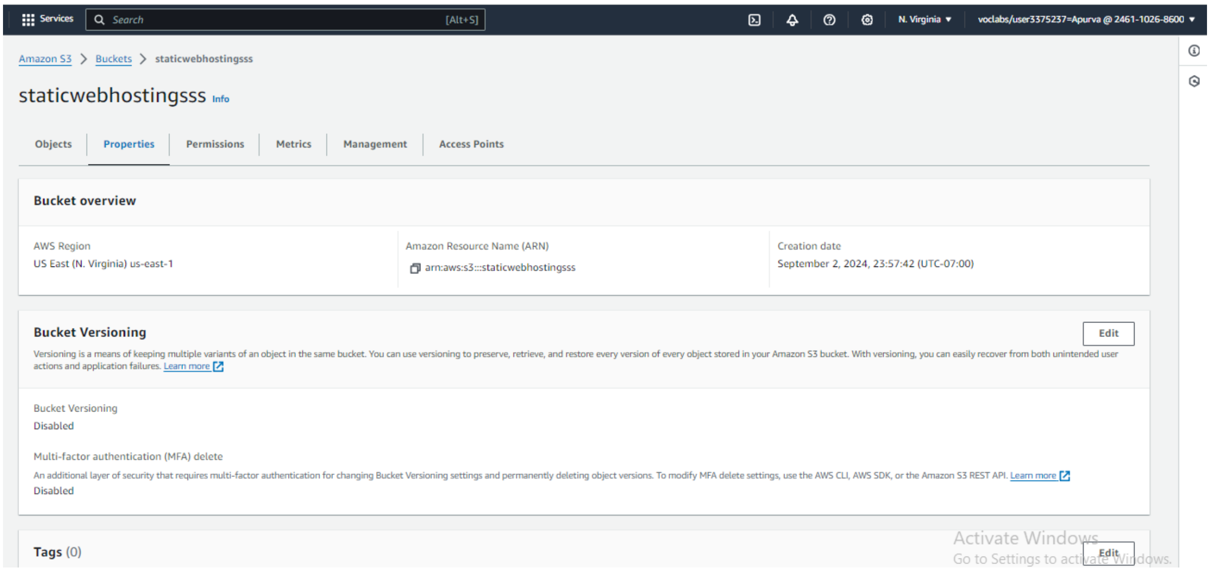
Specified objects

Find objects by name

Name	Type	Last modified	Size
assets/	Folder	-	-
index.html	html	September 3, 2024, 00:07:29 (UTC-07:00)	34.7 KB
readme.txt	txt	September 3, 2024, 00:07:30 (UTC-07:00)	859.0 B

Step 3: Configure Bucket for Static Website Hosting

1.In the S3 bucket, go to the Properties tab.



Amazon S3 > Buckets > staticwebhostingsss

staticwebhostingsss Info

Bucket overview

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

Amazon Resource Name (ARN)
arn:aws:s3:::staticwebhostingsss

Creation date
September 2, 2024, 23:57:42 (UTC-07:00)

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
Disabled

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)

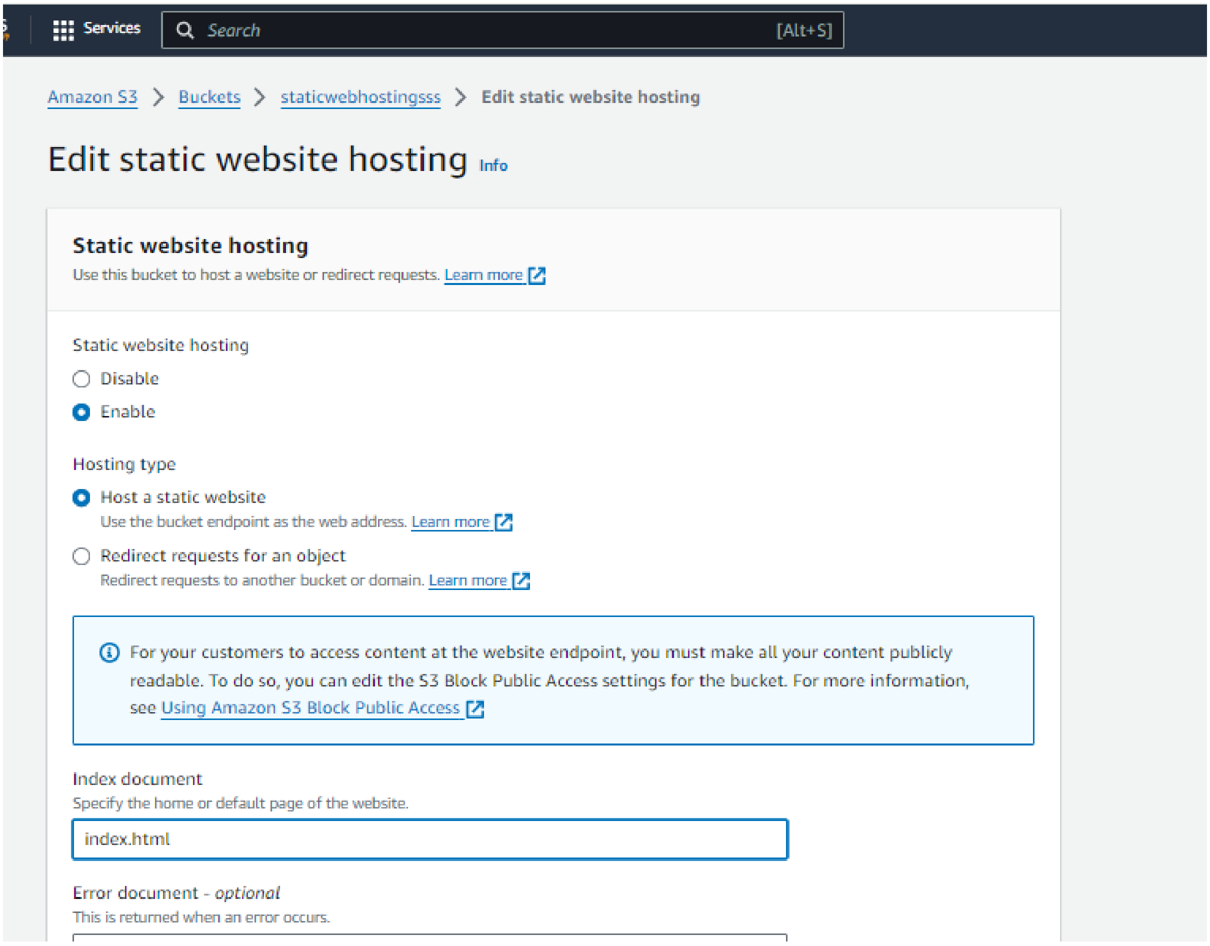
2. Scroll down to the Static website hosting section.

3. Select Enable.

4. For Index document, enter `index.html`.

5. Optionally, add an Error document (e.g., `error.html`).

6. Click Save changes.



Services
Search
[Alt+S]
Amazon S3 > Buckets > staticwebhostingsss > Edit static website hosting

Edit static website hosting Info

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.

index.html

Error document - *optional*

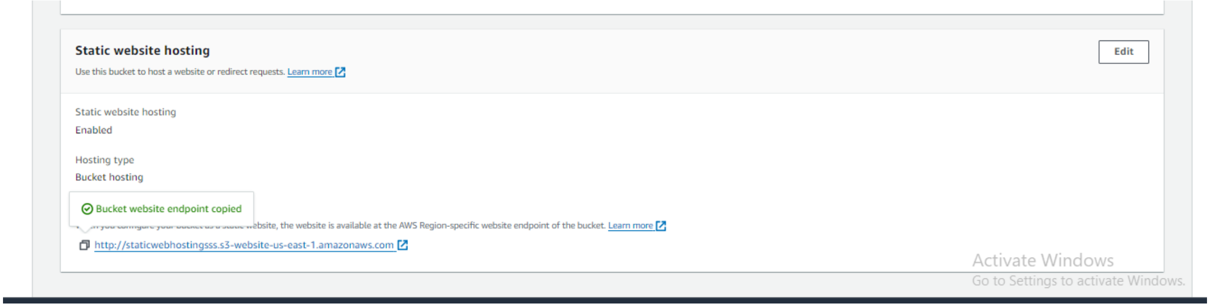
This is returned when an error occurs.

Step 4: Access Your Static Website

1. Go back to the Properties tab.

2. Scroll to the Static website hosting section.

3. Note the Bucket website endpoint URL (e.g., ` http://my-static-website-bucket.s3-website-us-west-1.amazonaws.com `).



Static website hosting

Use this bucket to host a website or redirect requests. Learn more

Static website hosting
Enabled

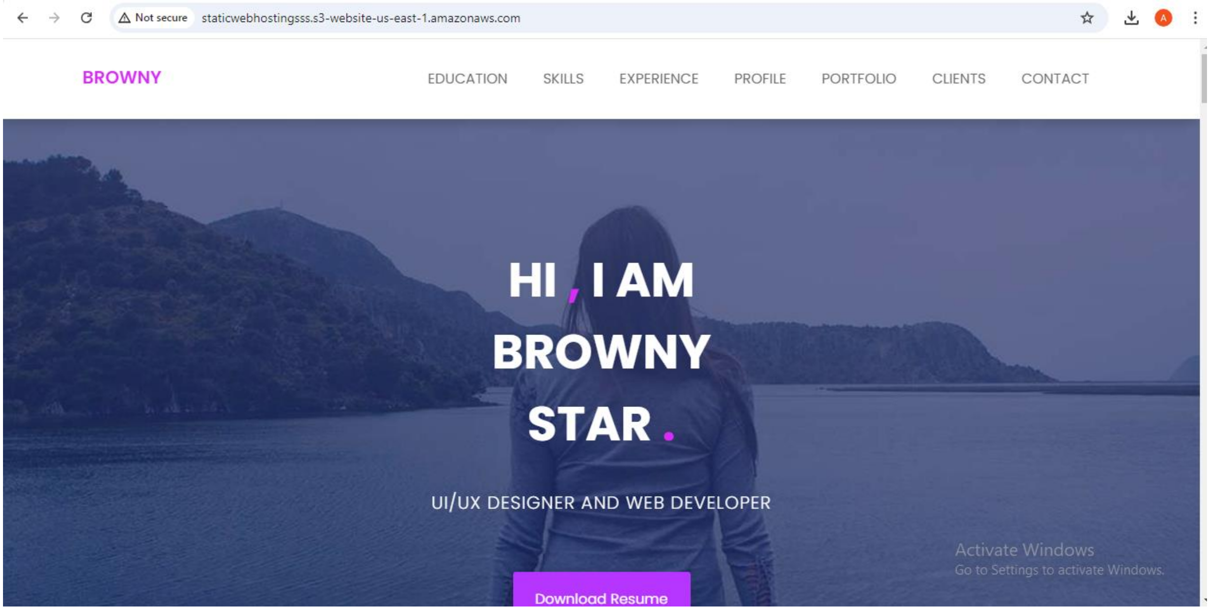
Hosting type
Bucket hosting

Bucket website endpoint copied

website, the website is available at the AWS Region-specific website endpoint of the bucket. Learn more

http://staticwebhostingsss.s3-website-us-east-1.amazonaws.com

4. Open this URL in a web browser to view your hosted static website.



Not secure staticwebhostingsss.s3-website-us-east-1.amazonaws.com

`.