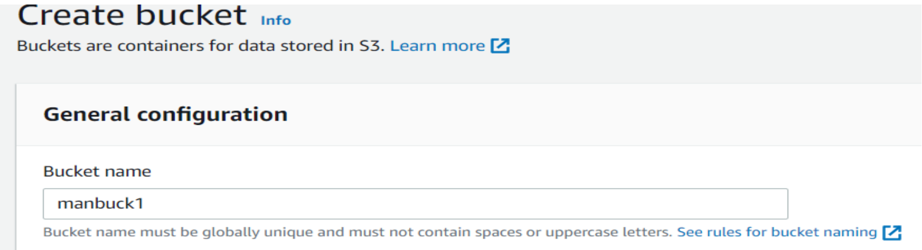
ASSIGNMENT NO-04

Problem Statement:-

Create a private bucket in AWS and upload a file and check by presigned URL that you can access the file or not.

Steps:-

1. Log in to AWS account and go to the S3 dashboard. Click on "Create bucket" to create a new S3 bucket. Choose a unique bucket name and select the region where user want to create the bucket.



Create bucket Info

Buckets are containers for data stored in S3. Learn more

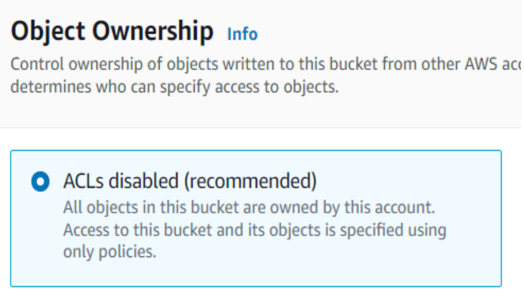
General configuration

Bucket name

manbuck1

Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming

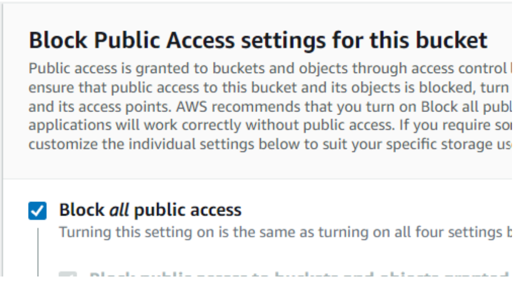
2. ACLs is disabled and left checked "Block all public access"and click create bucket.



Object Ownership Info

Control ownership of objects written to this bucket from other AWS acc determines who can specify access to objects.

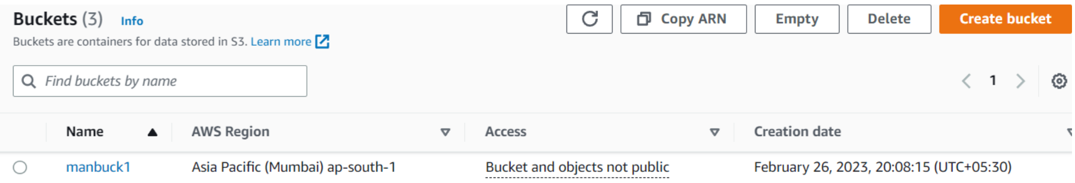
● ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.



Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control l ensure that public access to this bucket and its objects is blocked, turn and its access points. AWS recommends that you turn on Block all publ applications will work correctly without public access. If you require so customize the individual settings below to suit your specific storage us

☑ Block *all* public access
Turning this setting on is the same as turning on all four settings b

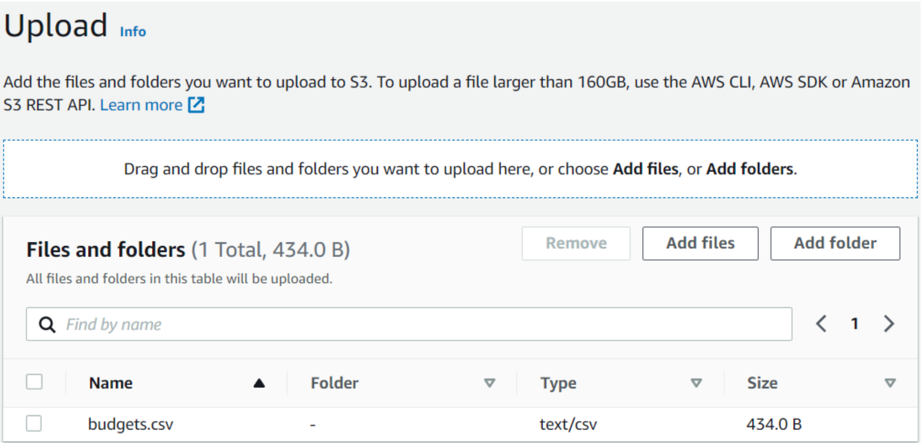


Buckets (3) Info

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	manbuck1	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 26, 2023, 20:08:15 (UTC+05:30)

3. Click on the name(ex-manbuck1) and click on "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 folders**.

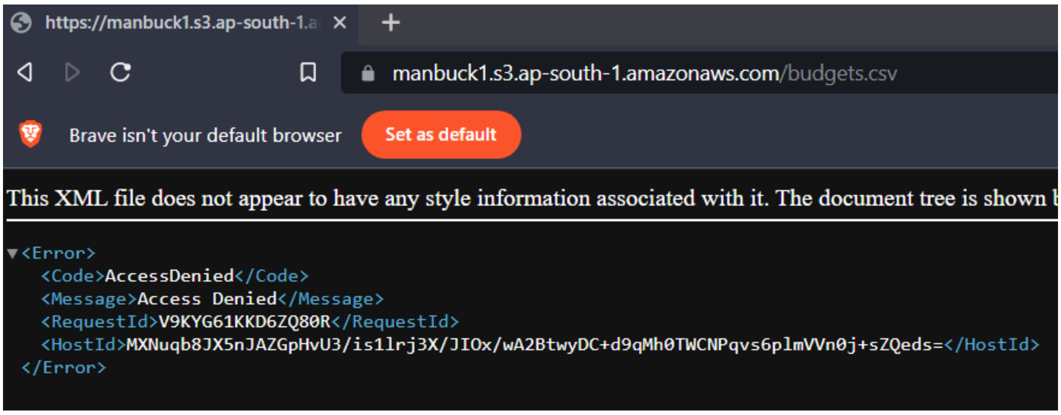
Files and folders (1 Total, 434.0 B)

All files and folders in this table will be uploaded.

□	Name	Folder	Type	Size
□	budgets.csv	-	text/csv	434.0 B

Now file is uploaded.

4. Now click on the file and click on object URLs and copy it and if it is pasted on a new tab then it can not be opened.

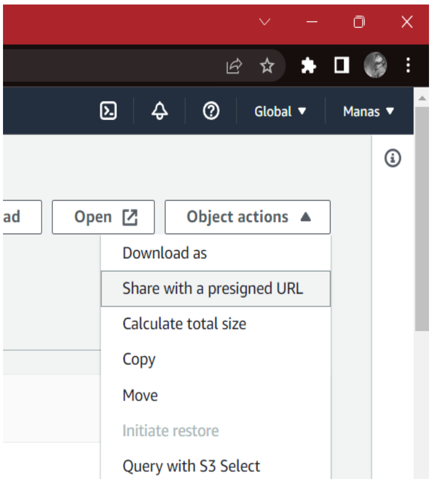


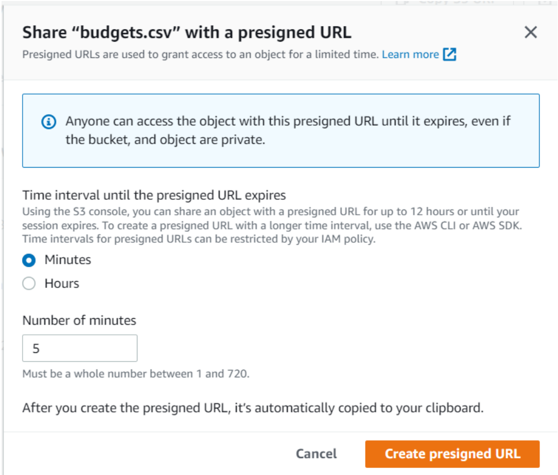
https://manbuck1.s3.ap-south-1.a
manbuck1.s3.ap-south-1.amazonaws.com/budgets.csv
Brave isn't your default browser
Set as default

This XML file does not appear to have any style information associated with it. The document tree is shown b

```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>V9KYG61KKD6ZQ80R</RequestId>
   <HostId>MXNuqb8JX5nJAZGpHvU3/is1lrj3X/JIOx/wA2BtwyDC+d9qMh0TWCNPqvs6plmVVn0j+sZQeds=</HostId>
 </Error>
```

5. Now click on the file which is uploaded on the bucket (ex-budgets.csv) And click on the “Object Actions” and click on the “Share with a presigned URL” and set timing as user’s choice and click on “create presigned URL”.





Share “budgets.csv” with a presigned URL

Presigned URLs are used to grant access to an object for a limited time. Learn more

Anyone can access the object with this presigned URL until it expires, even if the bucket, and object are private.

Time interval until the presigned URL expires

Using the S3 console, you can share an object with a presigned URL for up to 12 hours or until your session expires. To create a presigned URL with a longer time interval, use the AWS CLI or AWS SDK. Time intervals for presigned URLs can be restricted by your IAM policy.

● Minutes

○ Hours

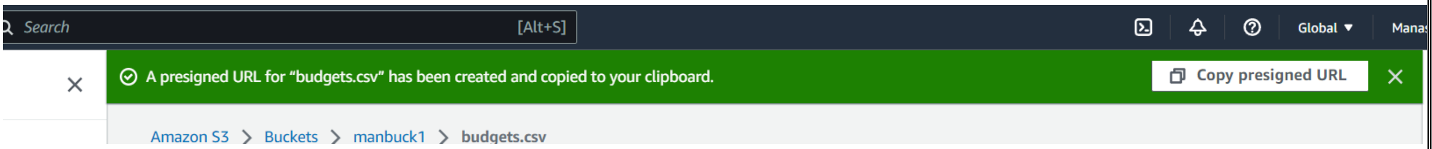
Number of minutes

5

Must be a whole number between 1 and 720.

After you create the presigned URL, it’s automatically copied to your clipboard.

6. Now copy presigned URL and paste it into a tab and download the file and it will be active for 5mins.and the owner can share it.



A presigned URL for “budgets.csv” has been created and copied to your clipboard.

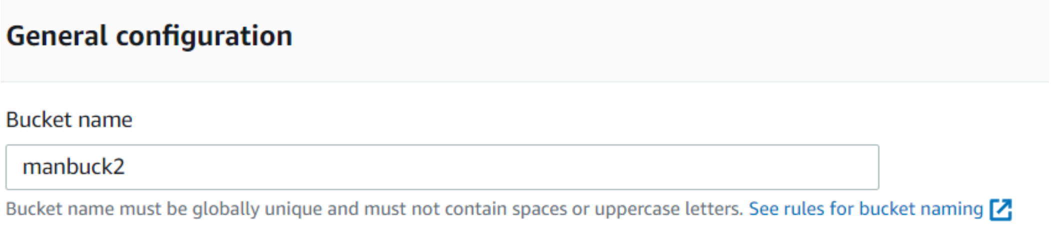
ASSIGNMENT NO-05

Problem Statement:-

Create a public bucket in AWS and upload a file and give the necessary permissions if the file URL working or not.

Steps:-

1. Log in to AWS account and go to the S3 dashboard. Click on "Create bucket" to create a new S3 bucket. Choose a unique bucket name and select the region where user want to create the bucket.



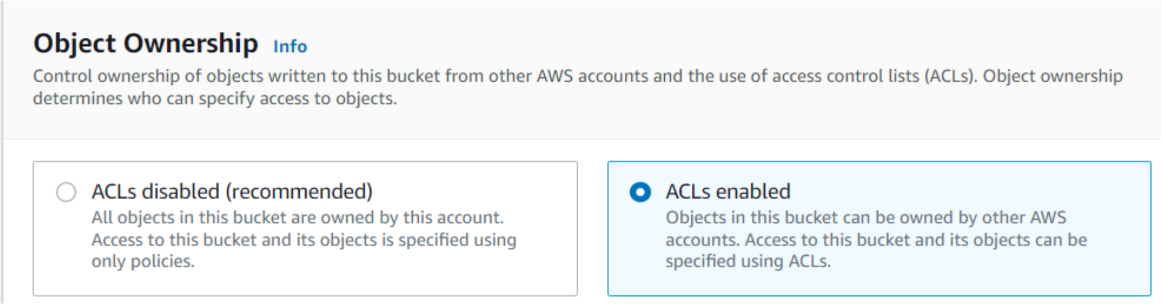
General configuration

Bucket name

manbuck2

Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming

2. ACLs is enabled and unchecked "Block all public access"and click create bucket and click on the box "I acknowledge…" and create bucket.

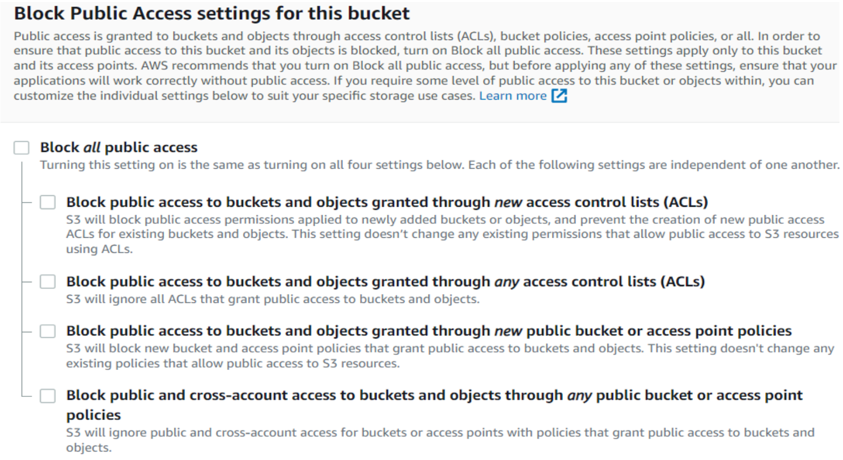


Object Ownership Info

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.

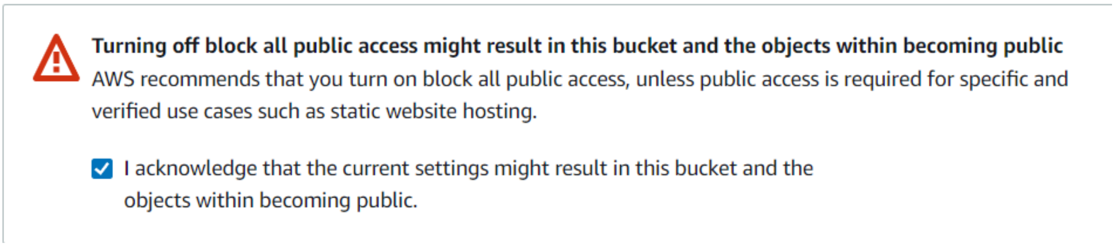


Block Public Access settings for this bucket

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.

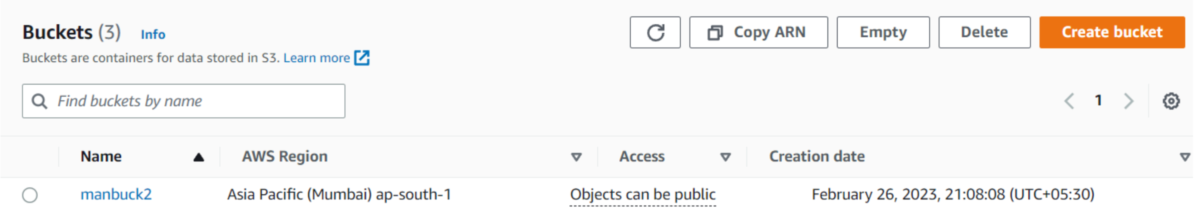
- □ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any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

Now ,bucket is created.

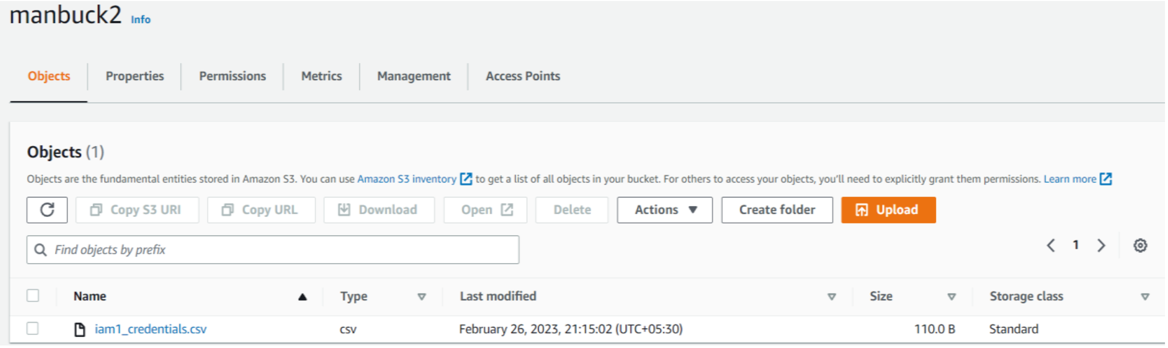


Buckets are containers for data stored in S3. Learn more

Find buckets by name

Name	AWS Region	Access	Creation date
○ manbuck2	Asia Pacific (Mumbai) ap-south-1	Objects can be public	February 26, 2023, 21:08:08 (UTC+05:30)

3. Now click on the bucket(ex-manbuck2) click on "Upload".



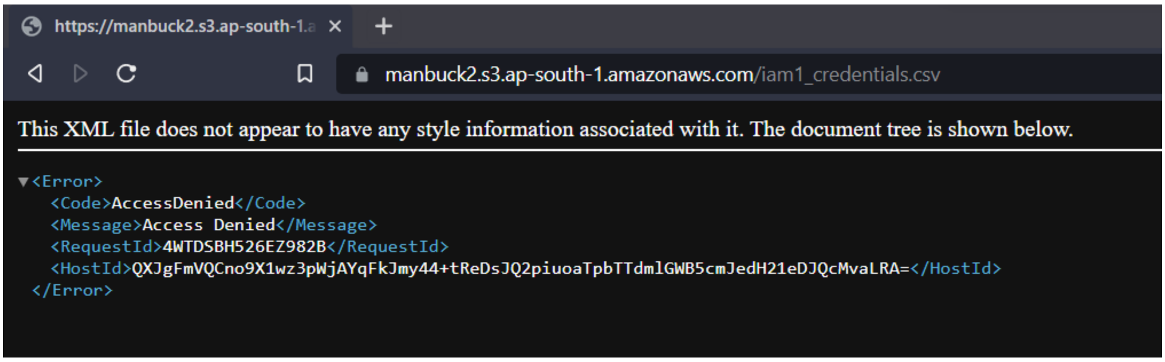
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix

□	Name	Type	Last modified	Size	Storage class
□	iam1_credentials.csv	csv	February 26, 2023, 21:15:02 (UTC+05:30)	110.0 B	Standard

Now, file is uploaded.

4. Click on the file name and click on "object URL" and copy it and paste it on the new tab and we can see that the link is not opened .

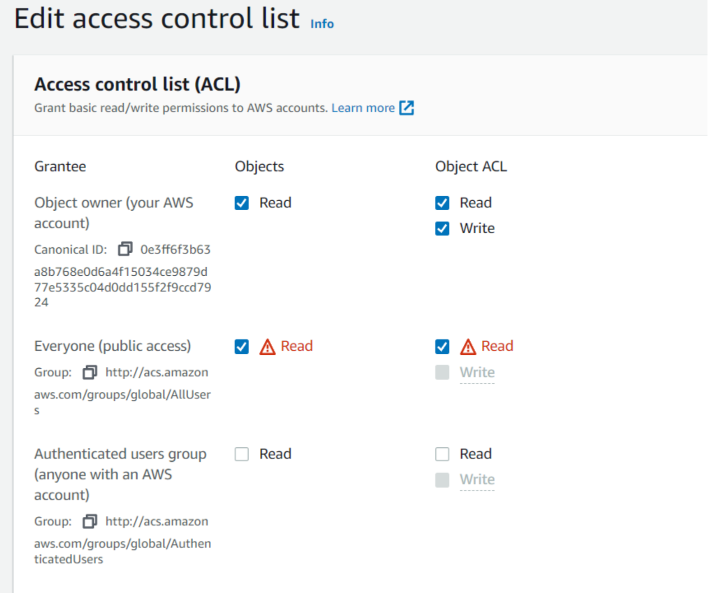


https://manbuck2.s3.ap-south-1.a
manbuck2.s3.ap-south-1.amazonaws.com/iam1_credentials.csv

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>4WTDSBH526EZ982B</RequestId>
   <HostId>QXJgFmVQCno9X1wz3pWjAYqFkJmy44+tReDsJQ2piuoaTpbTTdmlGWB5cmJedH21eDJQcMvaLRA=</HostId>
 </Error>
```

5. Now click on the file and go to permissions and click the edit button. And checked "Everyone (public access)" and check "I understand…"and click save changes.



Access control list (ACL)

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

Grantee	Objects	Object ACL
Object owner (your AWS account) Canonical ID: 0e3ff6f3b63a8b768e0d6a4f15034ce9879d77e5335c04d0dd155f2f9ccd7924	☑ Read	☑ Read ☑ Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	☑ ⚠ Read	☑ ⚠ Read □ Write
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	□ Read	□ Read □ Write

Now, if we click on the "object URL" the link can be opened and it is public now.

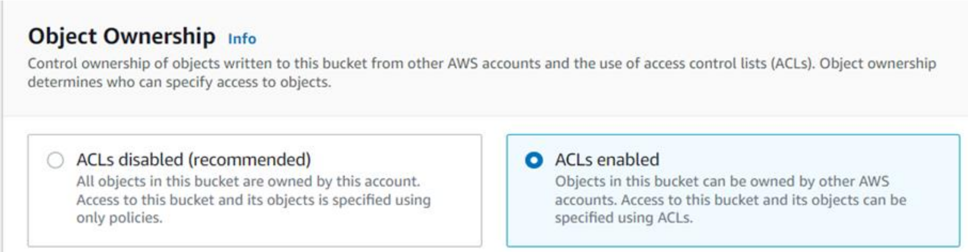
ASSIGNMENT NO-06

Problem Statement:-

Upload a static website on S3 and run it.

Steps:-

1. Log in to AWS account and go to the S3 dashboard. Click on "Create bucket" to create a new S3 bucket. Choose a unique bucket name and select the region where user want to create the bucket. ACLs is **enabled** and **unchecked** "Block all public access"and click create bucket and click on the box "I acknowledge…" and create bucket.

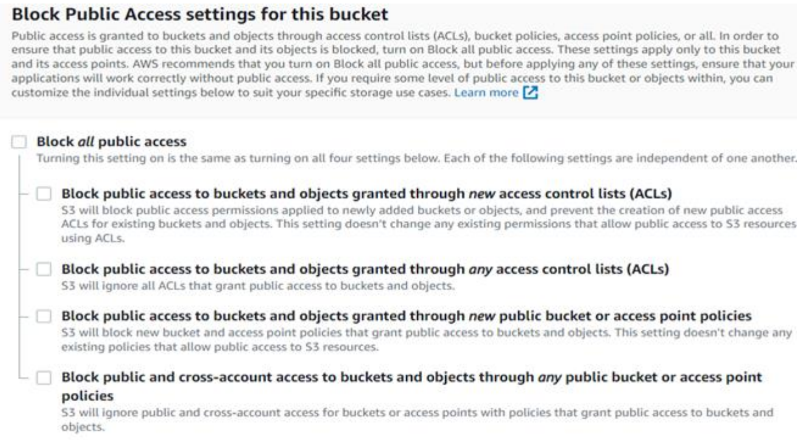


Object Ownership Info

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.

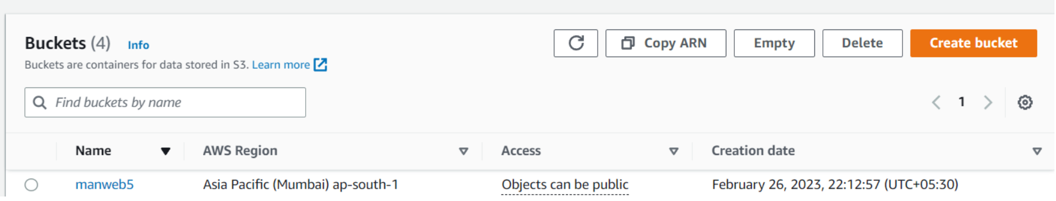


Block Public Access settings for this bucket

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.



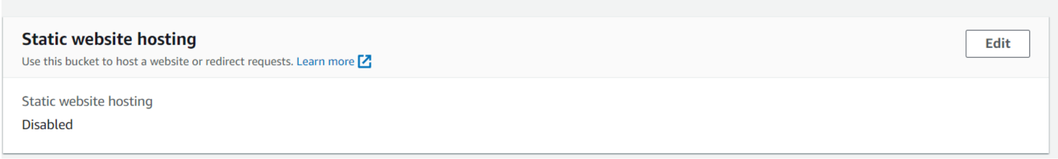
Buckets (4) Info

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	manweb5	Asia Pacific (Mumbai) ap-south-1	Objects can be public	February 26, 2023, 22:12:57 (UTC+05:30)

Now, bucket is created.

2. Click on the bucket and go to **properties .** at the bottom of the properties there is a option "Static website hosting" click on edit option.

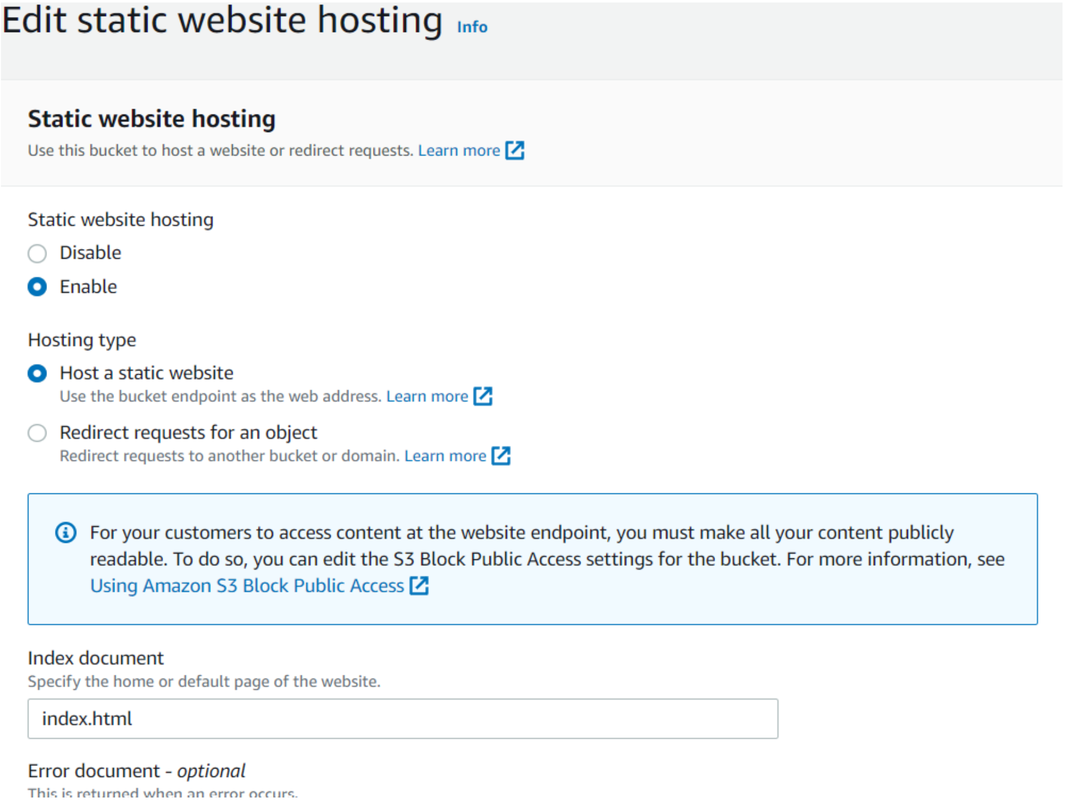


Static website hosting

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

Static website hosting
Disabled

3. Click on enable . Enter the name in "Index document" index.html as it is index/main page of the website and left others as it is and click "Save changes".



Edit static website hosting

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

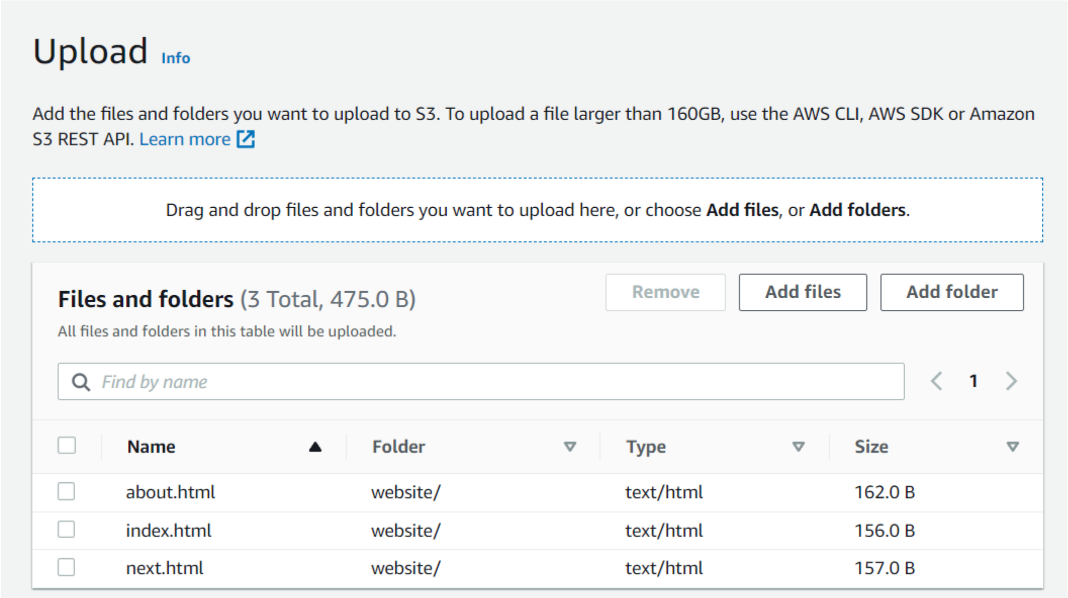
Specify the home or default page of the website.

index.html

Error document - *optional*

This is returned when an error occurs.

4. Now go to object again and click on "Upload" and upload more than one .html files or we can directly upload a folder which contains more than one .html files and click upload.



Upload

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 folders**.

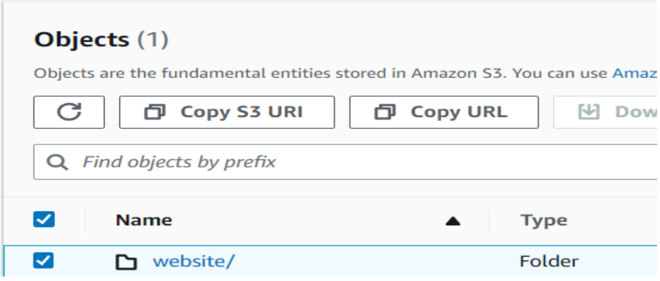
Files and folders (3 Total, 475.0 B)

All files and folders in this table will be uploaded.

□	Name	Folder	Type	Size
□	about.html	website/	text/html	162.0 B
□	index.html	website/	text/html	156.0 B
□	next.html	website/	text/html	157.0 B

Now, files are uploaded.

5. Now come to bucket->object and click the check box in the left of folder(ex-website).
If we upload files separately then click every box.

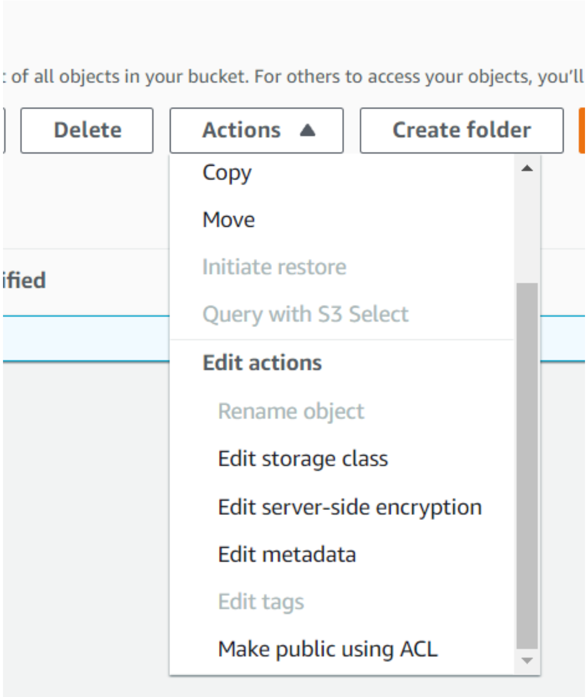


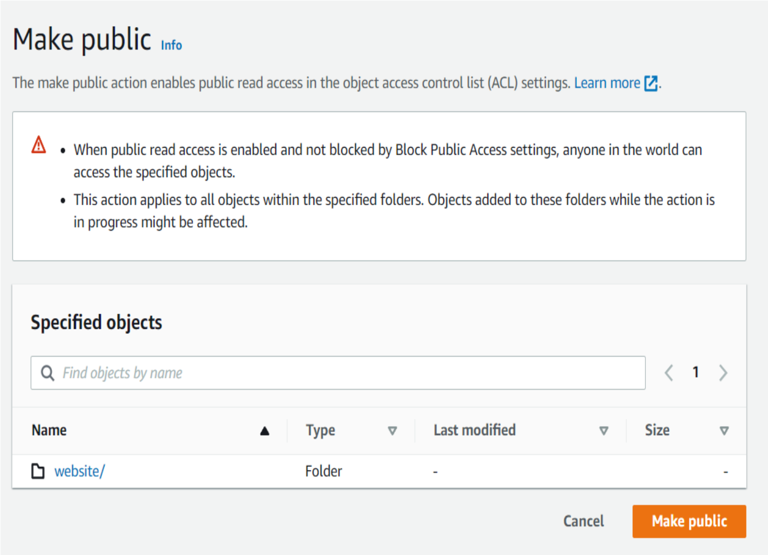
Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amaz

☑	Name	Type
☑	website/	Folder

6. Click on “Actions” and click “Make public using ACL” then click make public.





Make public Info

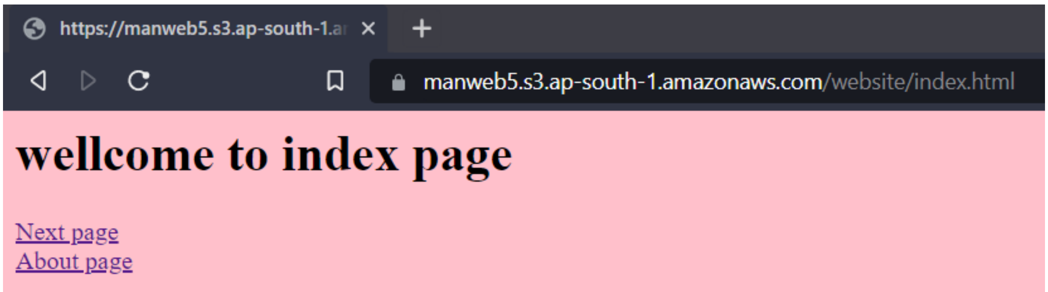
The make public action enables public read access in the object access control list (ACL) settings. Learn more.

- 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

Name	Type	Last modified	Size
website/	Folder	-	-

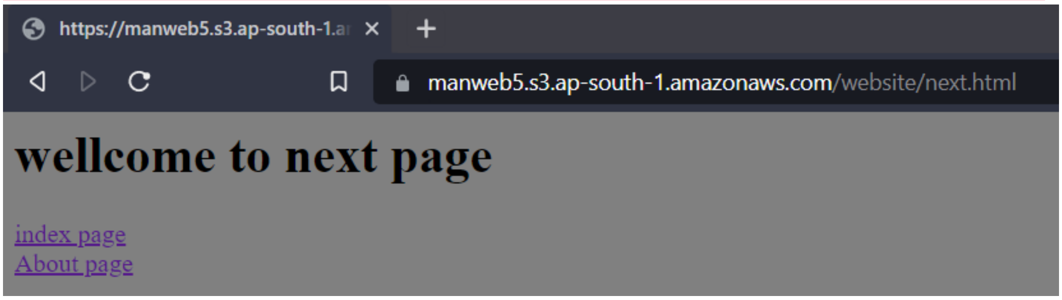
7. Now if we click on index.html and copy “Object URL”and paste it to another tab,these links are now public and can be opened .



manweb5.s3.ap-south-1.amazonaws.com/website/index.html

wellcome to index page

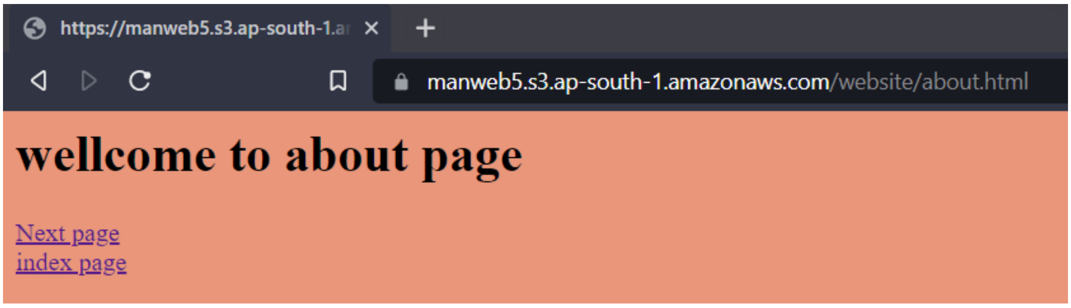
Next page
About page



manweb5.s3.ap-south-1.amazonaws.com/website/next.html

wellcome to next page

index page
About page



manweb5.s3.ap-south-1.amazonaws.com/website/about.html

wellcome to about page

Next page
index page