

Assignment: 04

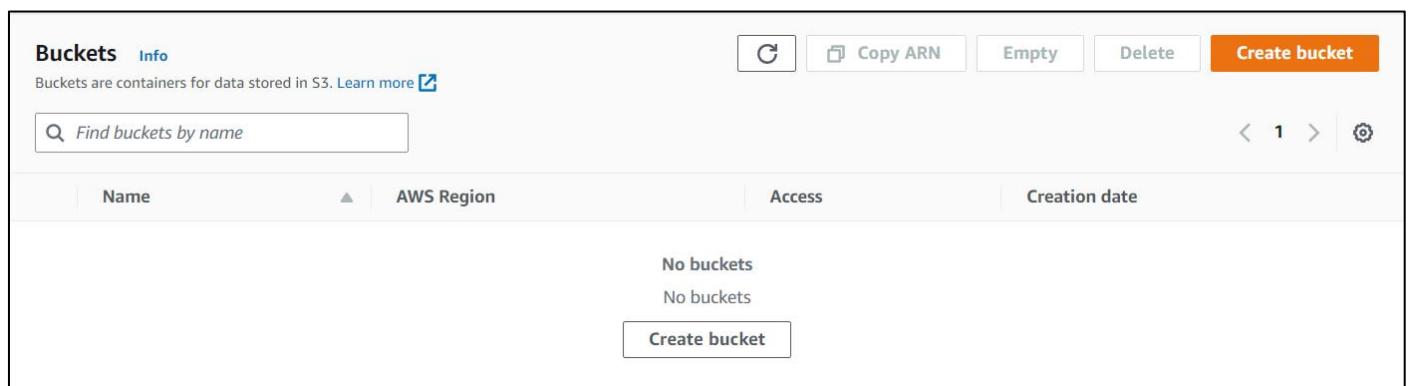
Title: Create a private bucket in AWS. Upload a file and check by presigned URL that you can access the file or not.

Simple Storage Service(S3) :

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. Customers of all sizes and industries can use Amazon S3 to store and protect any amount of data for a range of use cases, such as data lakes, websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides management features so that you can optimize, organize, and configure access to your data to meet your specific business, organizational, and compliance requirements.

Steps to create a private bucket.

1. Sign in to the AWS Management Console and open the Amazon S3 console .
2. In the left navigation pane, choose *Buckets*.
3. Choose *Create bucket*.



The *Create bucket* page opens.

4. For *Bucket name*, enter a name for your bucket. – ‘snehaprivatebucket’

The bucket name must:

- i. Be unique within a partition.
- ii. Be between 3 and 63 characters long.
- iii. Consist only of lowercase letters, numbers, dots (.), and hyphens (-). For best compatibility, we recommend that you avoid using dots (.) in bucket names, except for buckets that are used only for static website hosting.
- iv. Begin and end with a letter or number.

5. For *Region*, choose the AWS Region where you want the bucket to reside.

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

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

General configuration

Bucket name

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

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

6. Under *Object Ownership*, to disable ACLs to control ownership of objects uploaded in your bucket.

Bucket owner enforced – *ACLs are disabled*, and the bucket owner automatically owns and has full control over every object in the bucket. ACLs no longer affect access permissions to data in the S3 bucket. The bucket uses policies to define access control.

7. Check *Block Public Access settings for this bucket* checkbox to create private 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.

Object Ownership
Bucket owner enforced

Upcoming permission changes to disable ACLs
Starting in April 2023, to disable ACLs when creating buckets by using the S3 console, you will no longer need the `s3:PutBucketOwnershipControls` permission. [Learn more](#)

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.

8. Choose *Create bucket*.

The private bucket is created .

Steps to upload files and create presigned url:

1. Once the bucket is created , it is visible in the list of buckets.
2. Click on the *bucket* .

Buckets (1) [Info](#)

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

Find buckets by name

< 1 > ⚙

	Name	AWS Region	Access	Creation date
<input type="radio"/>	snehaprivatebucket	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 27, 2023, 23:06:09 (UTC+05:30)

3. Click on **upload**. The upload page opens – select **add files** and add the required files and documents required and then click on **upload**.

The files are uploaded in the private bucket.

snehaprivatebucket [Info](#)

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](#)

Find objects by prefix

Name	Type	Last modified	Size	Storage class
No objects				

You don't have any objects in this bucket.

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, 290.9 KB)

All files and folders in this table will be uploaded.

Find by name

Name	Folder	Type	Size
mcq.pdf	-	application/pdf	290.9 KB

4. Now click on the uploaded file and copy the **object URL** from its **properties** and open the url in a new window.

You will get a message as **Access denied** as the object in the bucket is private and therefore cannot be accessed publicly.

Amazon Resource Name (ARN)

arn:aws:s3:::snehaprivatebucket/mcq.pdf

Entity tag (Etag)

ac2a3ae93a70e083fe58ce8f7e619175

Object URL

<https://snehaprivatebucket.s3.ap-south-1.amazonaws.com/mcq.pdf>

← → ↻ 🔒 snehaprivatebucket.s3.ap-south-1.amazonaws.com/mcq.pdf

This XML file does not appear to have any style information associated with it

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>MHQC49TFHK1WWNR9</RequestId>
  <HostId>v9tU/EMXS9RqJSHgPrk8dv9nrudkhm0tCfbcZNNdzikpMUearsP21GtZivk</HostId>
</Error>

```

5. We can provide access to our private files by using the **presigned URL**.

Select the object(file) then click on **actions**.

From the list select and click on **Share with a presigned URL**.

Objects (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](#)

Find objects by prefix

	Name	Type	Last modified
<input checked="" type="checkbox"/>	mcq.pdf	pdf	February 27, 2023, 23:30:24 (UTC+05:30)

Download as

Share with a presigned URL

Calculate total size

Copy

Move

Initiate restore

Query with S3 Select

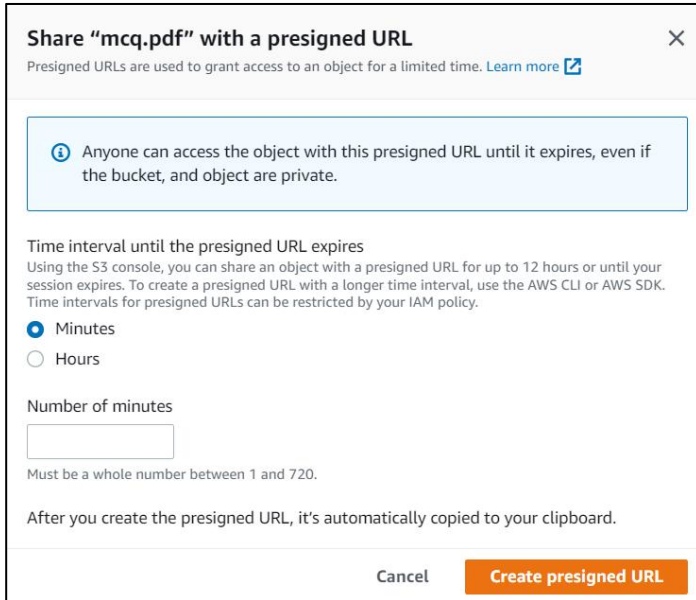
Edit actions

Rename object

Size	Storage class
290.9 KB	Standard

6. The Share with a presigned url dialogue appears.

Enter the *time interval* until the URL expires.



Share "mcq.pdf" 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

Must be a whole number between 1 and 720.

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

Cancel Create presigned URL

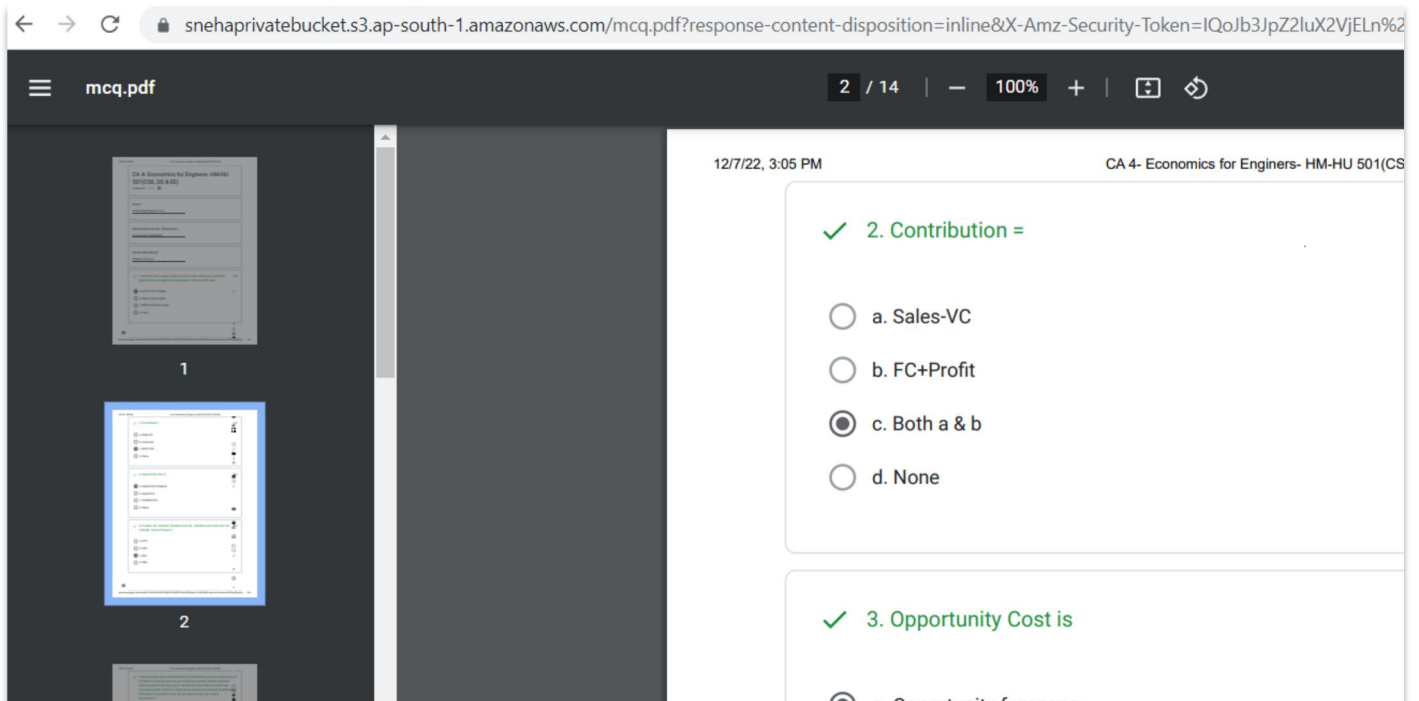
Click *Create presigned URL*.

The presigned URL for the object is created.

Copy the presigned URL and use it in a new tab to access the file publicly for the time limit assigned.



7. When you open the object URL in a new tab . The document uploaded in the private bucket or the object of the bucket is accessed publicly but only until the time limit by the created presigned URL.

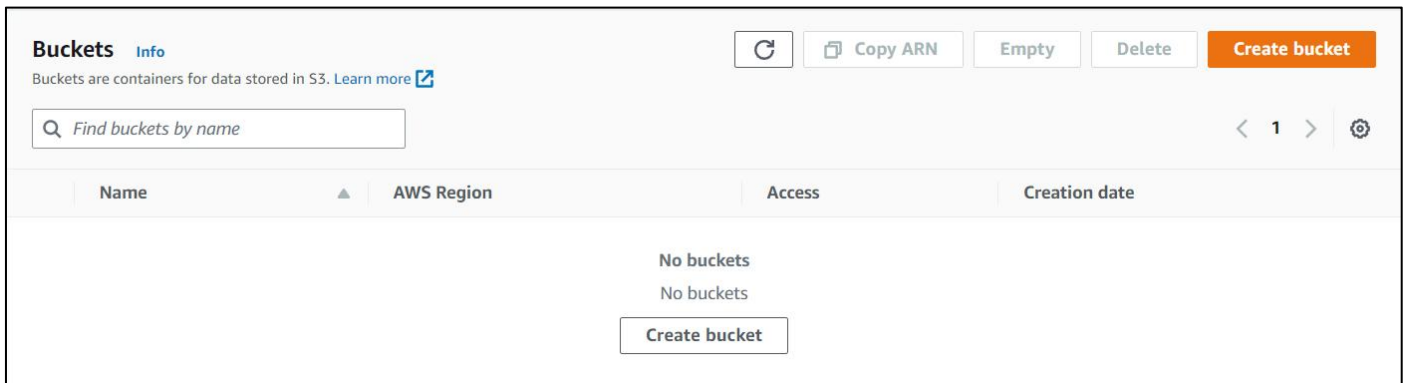


Assignment: 05

Title: Create a public bucket in AWS. Upload a file and give the necessary permission to check the file URL is working or not.

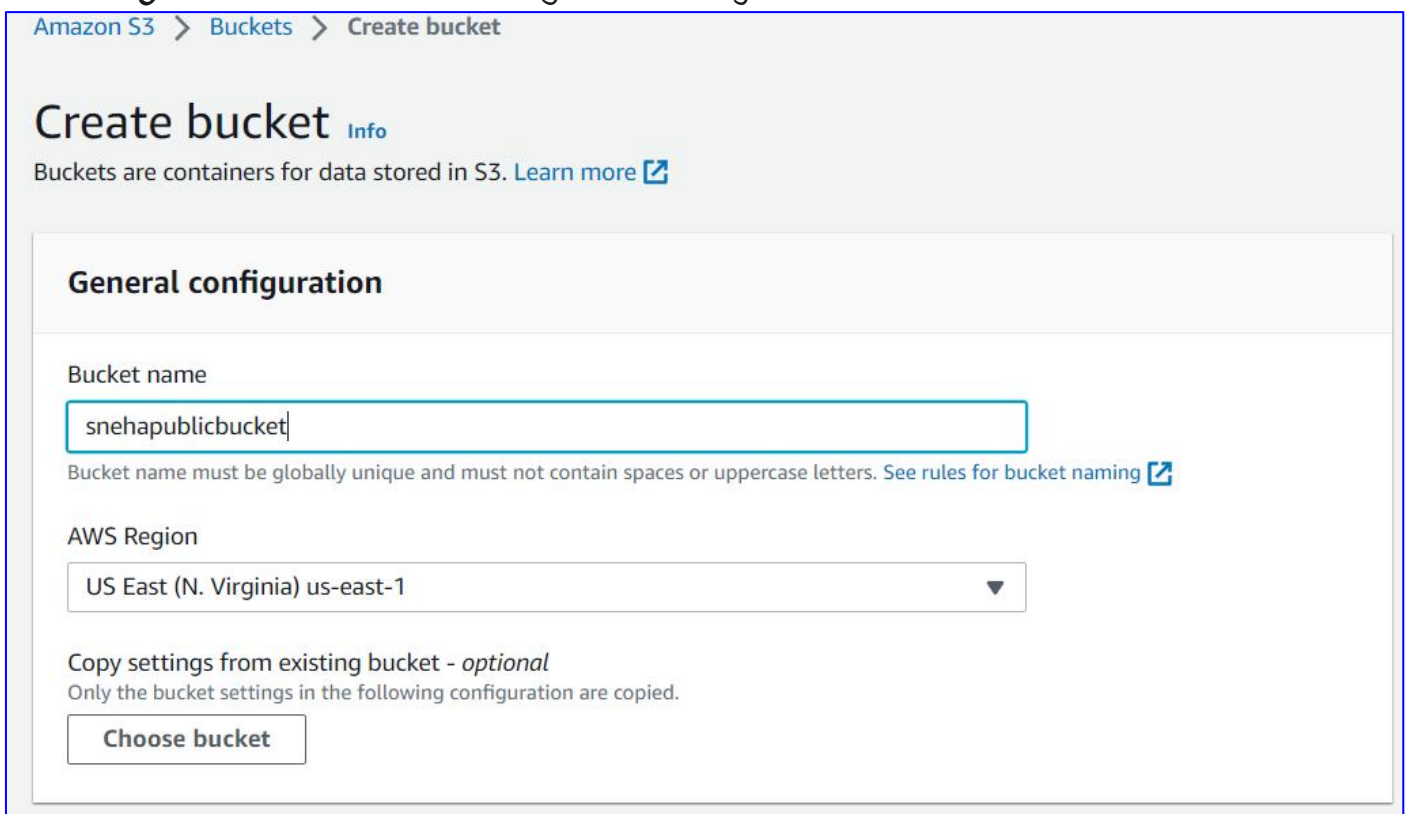
Steps to create a public bucket:

1. Sign in to the AWS Management Console and open the Amazon S3 console .
2. In the left navigation pane, choose **Buckets**.
3. Choose **Create bucket**.



The **Create bucket** page opens.

4. For **Bucket name**, enter a name for your bucket. – 'snehapublicbucket'
5. For **Region**, choose the AWS Region where you want the bucket to reside.



6. Under **Object Ownership**, to enable ACLs to control ownership of objects uploaded in your bucket.

Bucket owner enforced – **ACLs are enabled**,

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.

7. Uncheck *Block Public Access settings for this bucket* checkbox to create private bucket. Tick the acknowledgement box.

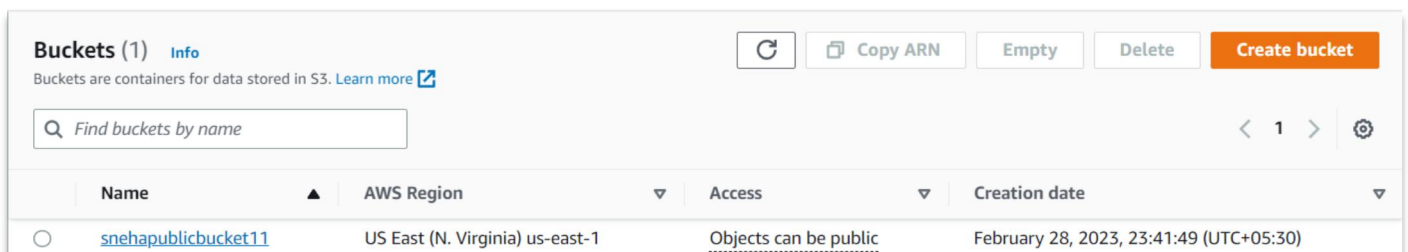
- ☐ **Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
- ☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions 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.

Click on *Create Bucket*.

-  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.

Steps to upload files and allow public access:

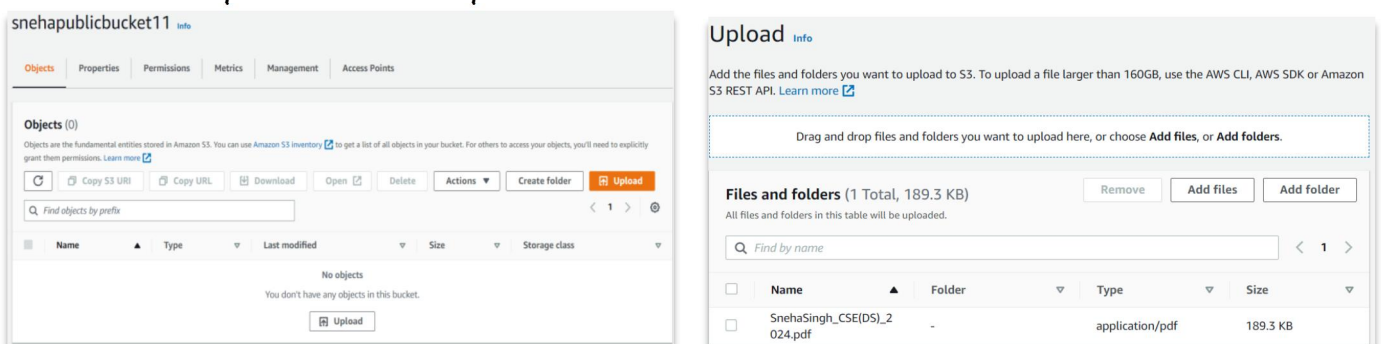
1. Once the bucket is created , it is visible in the list of buckets.
2. Click on the *bucket*.



Name	AWS Region	Access	Creation date
<input type="radio"/> snehapublicbucket11	US East (N. Virginia) us-east-1	Objects can be public	February 28, 2023, 23:41:49 (UTC+05:30)

3. Click on *upload*. The upload page opens – select *add files* and add the required files and documents required and then click on *upload*.

The files are uploaded in the public bucket.



snehapublicbucket11 [Info](#)

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](#)

No objects
You don't have any objects in this bucket.

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, 189.3 KB)

All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	SnehaSingh_CSE(DS)_2024.pdf	-	application/pdf	189.3 KB

7. Now click on the uploaded file and go to *Permissions* and then in the *Access Control List* , click *edit* and a dialogue box appears.

Properties	Permissions	Versions
Access control list (ACL) Edit Grant basic read/write permissions to AWS accounts. Learn more		
Grantee	Object	Object ACL
Object owner (your AWS account) Canonical ID: 05a78f2ad4e1a5f6f0c8146cb330a6f352c466226abf1d50f4711408ea7dbad7	Read	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	-	-

8. Check the read permission for **object** and **object's ACL** under **Everyone(public access)**.

Tick **I Understand the effects...**

9. Click on **save changes**.

Edit access control list [Info](#)
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: 05a78f2ad4e1a5f6f0c8146cb330a6f352c466226abf1d50f4711408ea7dbad7	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	<input checked="" type="checkbox"/> ⚠ Read	<input checked="" type="checkbox"/> ⚠ Read <input type="checkbox"/> Write

⚠ When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.
[Learn more](#)

☒ I understand the effects of these changes on this object.

Access for other AWS accounts
 No other AWS accounts associated with the resource.

[Add grantee](#)

Specified objects

Name	Type	Last modified	Size
SnehaSingh_CSE(DS)_2024.pdf	pdf	February 28, 2023, 23:47:47 (UTC+05:30)	189.3 KB

[Cancel](#) [Save changes](#)

10. Now click on the uploaded file and copy the **object URL** from its **properties** and open the url in a new window.

11. When you open the object URL in a new tab . The document uploaded in the public bucket or the object of the bucket is accessed publicly

S3 URI

s3://snehapublicbucket11/SnehaSingh_CSE(DS)_2024.pdf

Amazon Resource Name (ARN)

arn:aws:s3:::snehapublicbucket11/SnehaSingh_CSE(DS)_2024.pdf

Entity tag (Etag)

b6e7d80fdc4a46fed4e5e0cbcf6eba2d

Object URL

[https://snehapublicbucket11.s3.amazonaws.com/SnehaSingh_CSE\(DS\)_2024.pdf](https://snehapublicbucket11.s3.amazonaws.com/SnehaSingh_CSE(DS)_2024.pdf)

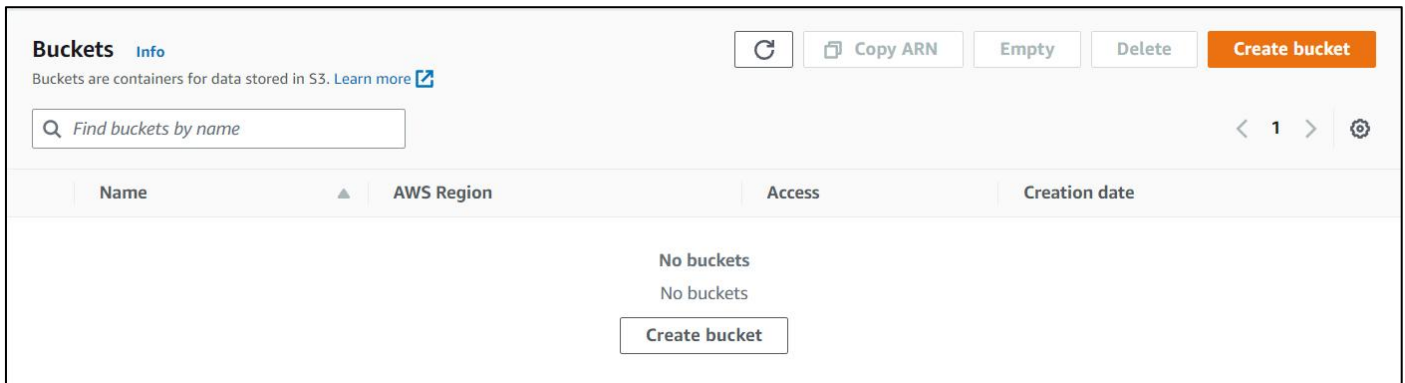
NOTE : If you do not edit the permissions of the ACL list , the access of the object will still be denied even if it is an object of a public bucket.

Assignment: 06

Title: Upload a static website in S3

Steps to create a public bucket, change permissions and host a static website on S3:

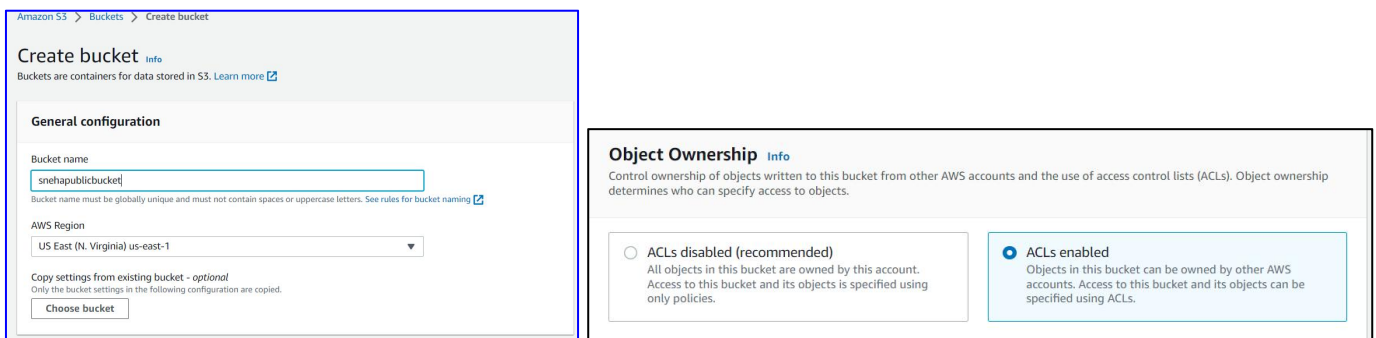
1. Sign in to the AWS Management Console and open the Amazon S3 console.
2. In the left navigation pane, choose **Buckets**.
3. Choose **Create bucket**.



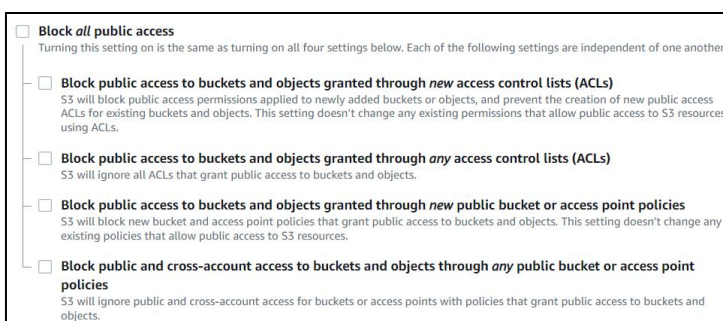
The **Create bucket** page opens.

4. For **Bucket name**, enter a name for your bucket. - 'snehapublicbucket'
5. For **Region**, choose the AWS Region where you want the bucket to reside.
6. Under **Object Ownership**, to enable ACLs to control ownership of objects uploaded in your bucket.

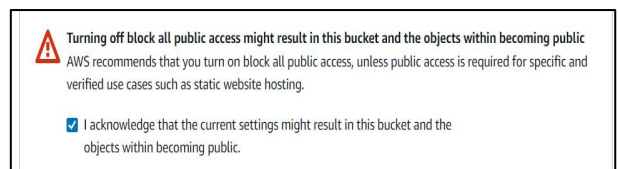
Bucket owner enforced – ACLs are enabled,



7. Uncheck **Block Public Access settings for this bucket** checkbox to create private bucket. Tick the acknowledgement box.

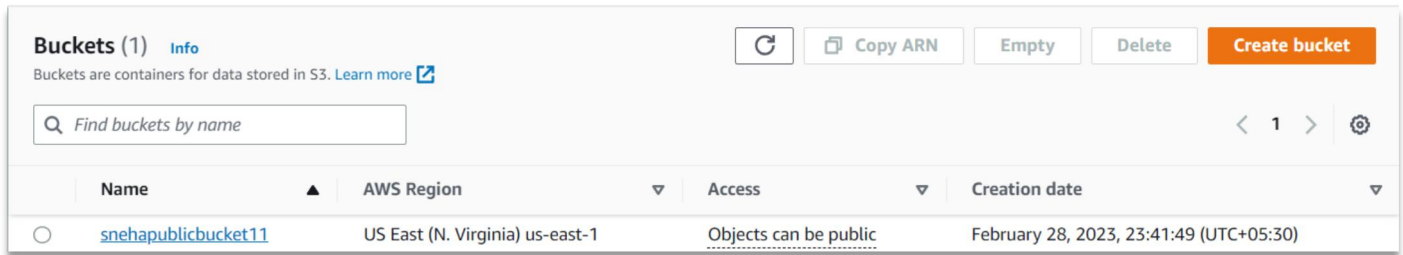


Click on **Create Bucket**.



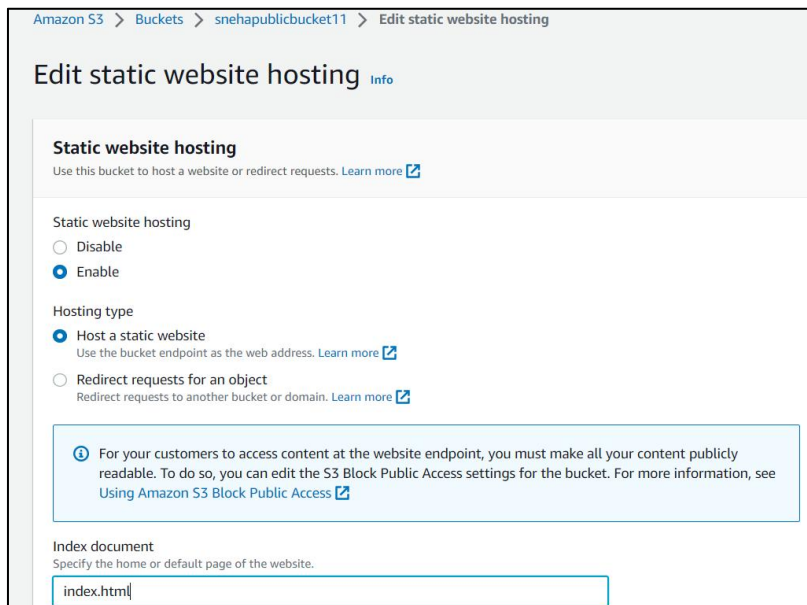
Public bucket is created.

8. Once the bucket is created , it is visible in the list of buckets. Click on the *bucket* .



9. Go to *properties* , and scroll down to *Static Website hosting* and click on *Edit*.

10. In the *Edit static Website hosting*, Enable the Static Website hosting and specify the index document as *Index.html*.



Now we will upload a folder containing 3 files in .html which will be our static websites namely - index.html, next.html, about.html .

The code snippet for example :

```
<html>
<body bgcolor="lightgreen">
welcome
<a href="next.html">Next page</a>
<a href="about.html">Aboutpage</a>
</body>
</html>
```

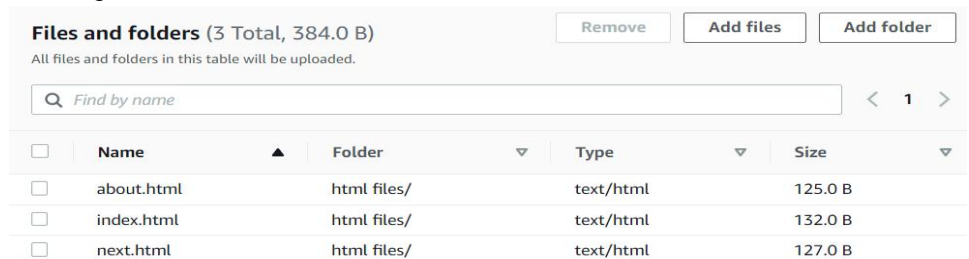
11. Upload the folder containing the files:

Upload ->

Add folders ->

select folder->

Upload



12. Now select all the folders to change their ACL permissions such that the files will now be accessed publicly.

Select the three files (objects) ,then go to actions and click on the downward arrows , scroll down to click on *Make public using ACL*. In the make public page all the files will be listed just click on *Make public* and the files will now be available publicly.

Objects (3)

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

[Copy S3 URI](#) [Copy URL](#)

Find objects by prefix

<input checked="" type="checkbox"/>	Name	Type
<input checked="" type="checkbox"/>	about.html	html
<input checked="" type="checkbox"/>	index.html	html
<input checked="" type="checkbox"/>	next.html	html

Make public using ACL

Actions ▲

Create folder

Move

Initiate restore

Query with S3 Select

Edit actions

Rename object

Edit storage class

Edit server-side encryption

Edit metadata

Edit tags

Make public using ACL

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.

Specified objects

Find objects by name

Name	Type	Last modified	Size
about.html	html	March 2, 2023, 10:57:48 (UTC+05:30)	125.0 B
index.html	html	March 2, 2023, 10:57:50 (UTC+05:30)	132.0 B
next.html	html	March 2, 2023, 10:57:51 (UTC+05:30)	127.0 B

Cancel

Make public

13. Click on

index.html

Go to properties

In Object overview ,

see the object URL.

Copy the object URL

Paste it in a new web

window to see

whether it can be

accessed publicly.

Object Properties :

index.html [Info](#)

[Copy S3 URI](#) [Download](#) [Open](#) [Object actions](#)

Properties **Permissions** **Versions**

Object overview

Owner: kija3928

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

Last modified: March 2, 2023, 10:57:50 (UTC+05:30)

Size: 132.0 B

Type: html

Key: html files/index.html

S3 URI: s3://snehapublicbucket11/html files/index.html

Amazon Resource Name (ARN): arn:aws:s3::snehapublicbucket11/html files/index.html

Entity tag (ETag): 1c2a3625cc3b265701262366010ea3b

Object URL: https://snehapublicbucket11.s3.amazonaws.com/html+files/index.html

1.Index.html

https://snehapublicbucket11.s3.amazonaws.com/html+files/index.html

welcome [Next page](#) [Next page](#)

2.About.html

https://snehapublicbucket11.s3.amazonaws.com/html+files/about.html

welcome [Next page](#) [Next page](#)

3.Next.html

https://snehapublicbucket11.s3.amazonaws.com/html+files/next.html

welcome [Next page](#) [Next page](#)