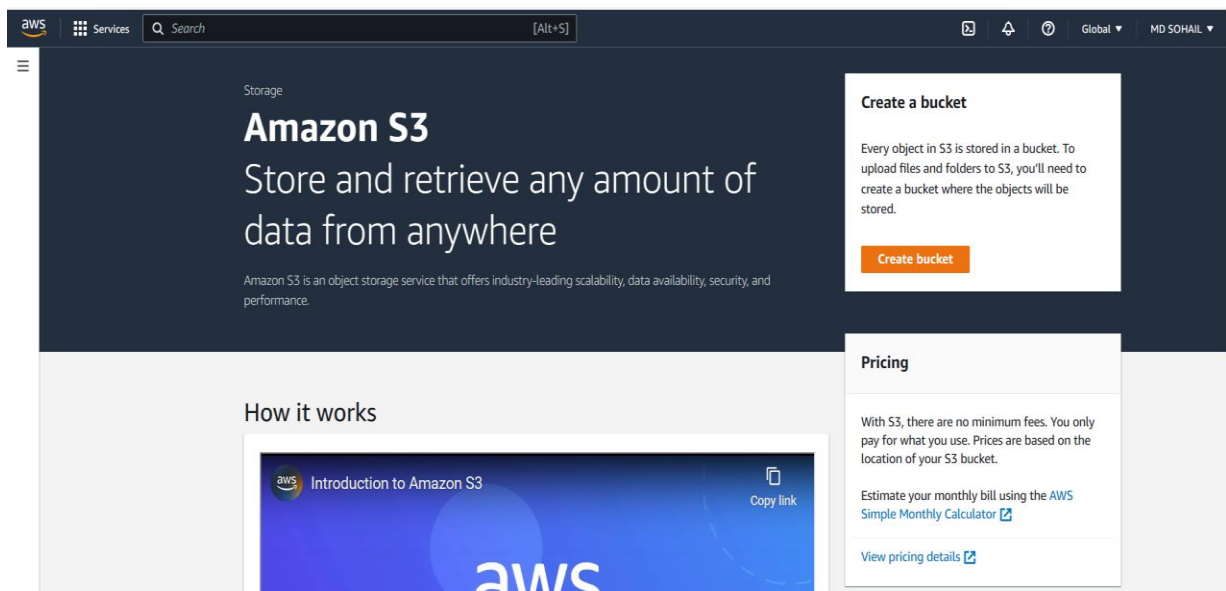


# Assignment 4

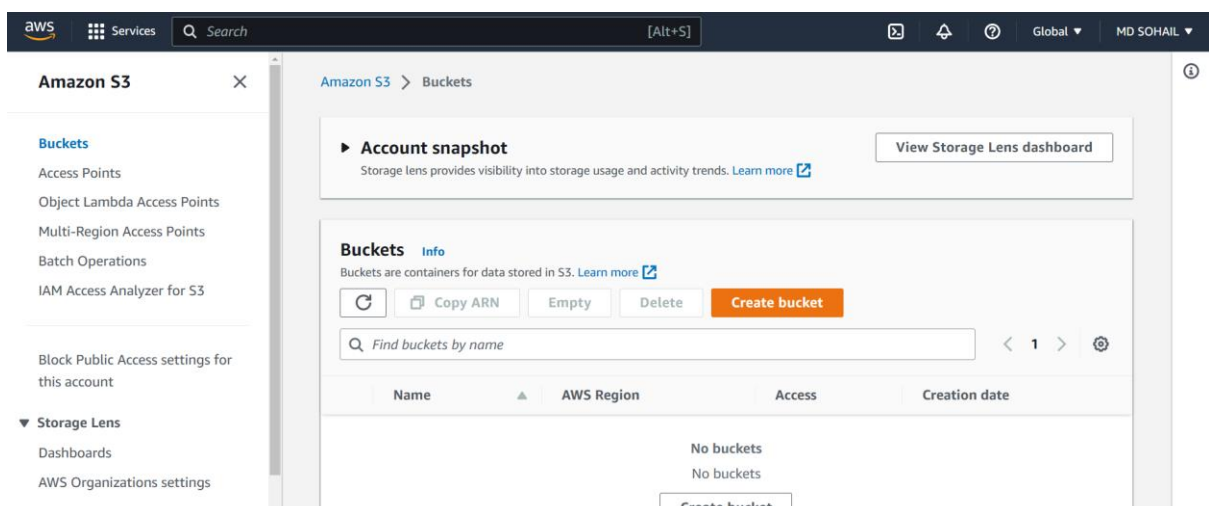
**Create a private bucket in AWS. Upload a file and check that through presigned URL you can access the file or not.**



1. Open the **Amazon Web Services** home page (aws.amazon.com).
2. Choose **Sign into Console**.
3. Sign in as **Root user** using your email address and password.
4. Go to search and search S3 (S3: Simple Storage Service).



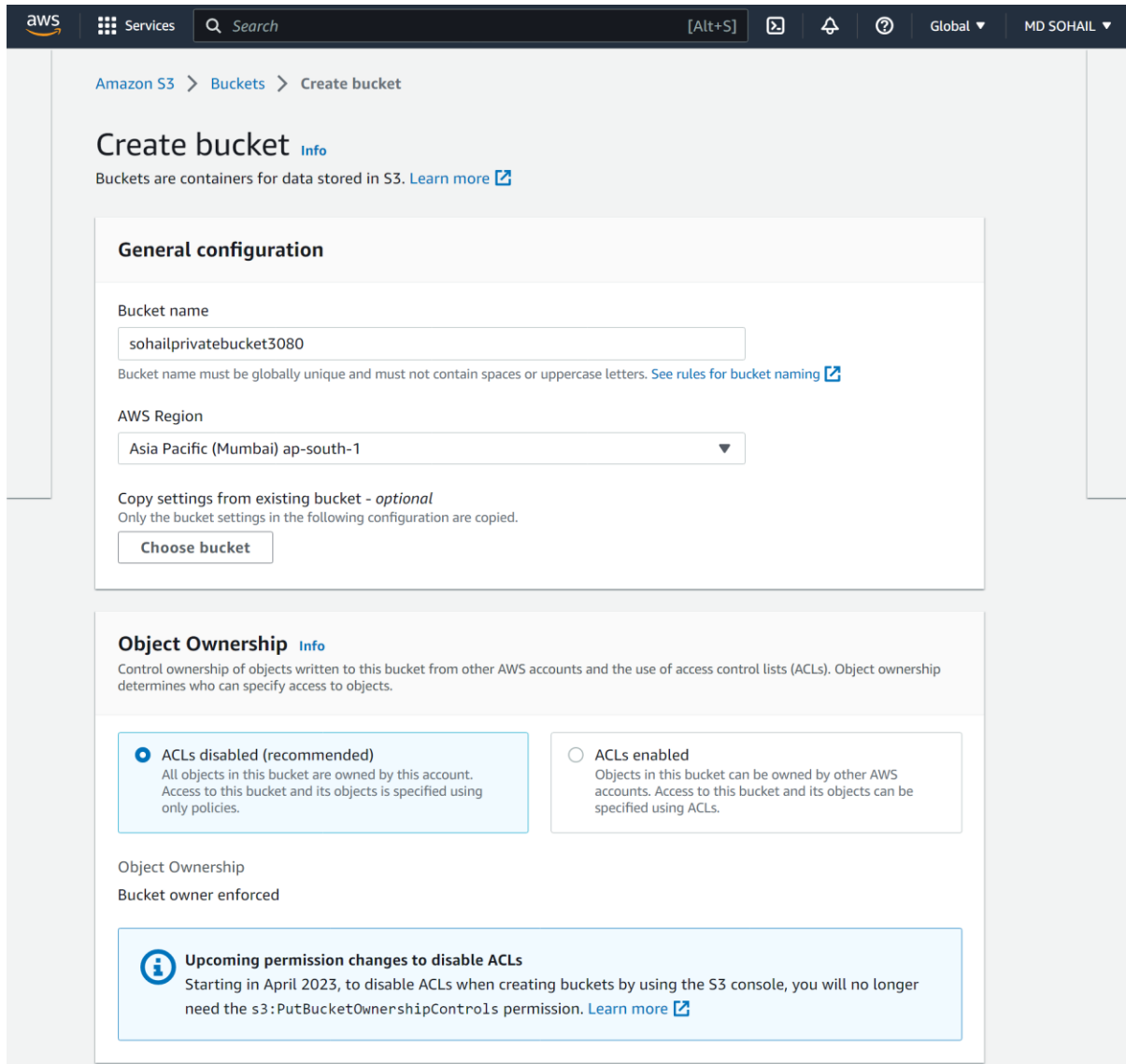
**or, go to buckets on the side panel and click on side panel. And click on **Create bucket**.**



## 5. In **Create bucket** page:

Give globally unique name as it is created globally.

- Give the Bucket name in the General configuration section.
- Select **ACL Disabled** in the Object Ownership section.
- Check **Block all public access** in the Block Public Access settings for this bucket section.



aws Services Search [Alt+S] Global MD SOHAIL

Amazon S3 > Buckets > Create bucket

### Create bucket [Info](#)

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

#### General configuration

Bucket name

sohailprivatebucket3080

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

AWS Region

Asia Pacific (Mumbai) ap-south-1

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

[Choose 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.
- ☒ 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.



#### Upcoming permission changes to enable all Block Public Access settings

Starting in April 2023, to enable all Block Public Access settings when creating buckets by using the S3 console, you will no longer need the `s3:PutBucketPublicAccessBlock` permission. [Learn more](#)

### 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

- ☒ Disable  
☐ Enable

### Tags (0) - optional

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

Add tag

### Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

#### Encryption key type [Info](#)

- ☒ Amazon S3-managed keys (SSE-S3)  
☐ AWS Key Management Service key (SSE-KMS)

#### Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS 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.

Cancel

Create bucket

Feedback Language

© 2023 Amazon Web Services India Private Limited or its affiliates.

Privacy Terms Cookie preferences

Keep other things at default and **click on Create Bucket.**

6. Now check your bucket will be created. Next Click on the bucket that you have created.

Amazon S3

Successfully created bucket "sohailprivatebucket3080"  
To upload files and folders, or to configure additional bucket settings choose [View details](#).

Amazon S3 > Buckets

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

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

Find buckets by name

Name	AWS Region	Access	Creation date
sohailprivatebucket3080	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 26, 2023, 19:26:11 (UTC+05:30)

7. Then click on upload.

sohailprivatebucket3080 Info

Objects Properties Permissions Metrics Management Access Points

**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](#)

Create folder Upload

Find objects by prefix

Name	Type	Last modified	Size	Storage class
No objects You don't have any objects in this bucket.				

8. In Upload page:

Click on **Add files** to upload a file, select the file and click on **Upload**.

Amazon S3 > Buckets > sohailprivatebucket3080 > Upload

## Upload [Info](#)

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

**Files and folders (1 Total, 3.4 MB)** Remove Add files Add folder

All files and folders in this table will be uploaded.

<input checked="" type="checkbox"/>	Name	Folder	Type	Size
<input checked="" type="checkbox"/>	Power_hourly.txt	-	text/plain	3.4 MB

**Destination**

Destination  
[s3://sohailprivatebucket3080](#)

► **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.

Cancel Upload

9. Then click on the file uploaded file on the upload status page.

Upload succeeded  
[View details below.](#)

## Upload: status Close

The information below will no longer be available after you navigate away from this page.

**Summary**

Destination <a href="#">s3://sohailprivatebucket3080</a>	Succeeded ✔ 1 file, 3.4 MB (100.00%)	Failed ✘ 0 files, 0 B (0%)
---	---	-------------------------------

**Files and folders** | Configuration

**Files and folders (1 Total, 3.4 MB)**

Name	Folder	Type	Size	Status	Error
Power_hourly.txt	-	text/plain	3.4 MB	✔ Succeeded	-

Copy the URL and open in new tab.

[Alt+S]

GlobalMD SOHAIL

PropertiesPermissionsVersions

Object overview

Owner

be7f5e639210abc9e141fb0824f69eccbe04bff1bc9c37c536030f356938a0c3

AWS Region

Asia Pacific (Mumbai) ap-south-1

Last modified

February 26, 2023, 19:35:50 (UTC+05:30)

Size

3.4 MB

Type

txt

Key

Power\_hourly.txt

S3 URI

s3://sohailprivatebucket3080/Power\_hourly.txt

Amazon Resource Name (ARN)

arn:aws:s3::sohailprivatebucket3080/Power\_hourly.txt

Entity tag (Etag)

15d0917e9952d5954a1fea9532525b63

https://sohailprivatebucket3080.s3.ap-south-1.amazonaws.com/Power\_hourly.txt

Object management overview

The following bucket properties and object management configurations impact the behavior of this object.

Object URL Copied

You can see Object URL cannot be accessed.

https://sohailprivatebucket3080.s3.ap-south-1.amazonaws.com/Power\_hourly.txt

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

<Error>

<Code>AccessDenied</Code>

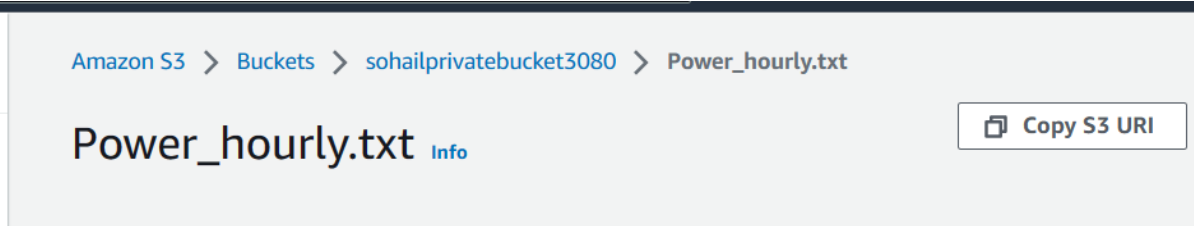
<Message>Access Denied</Message>

<RequestId>XCP6NA7PXFHF06CRM</RequestId>

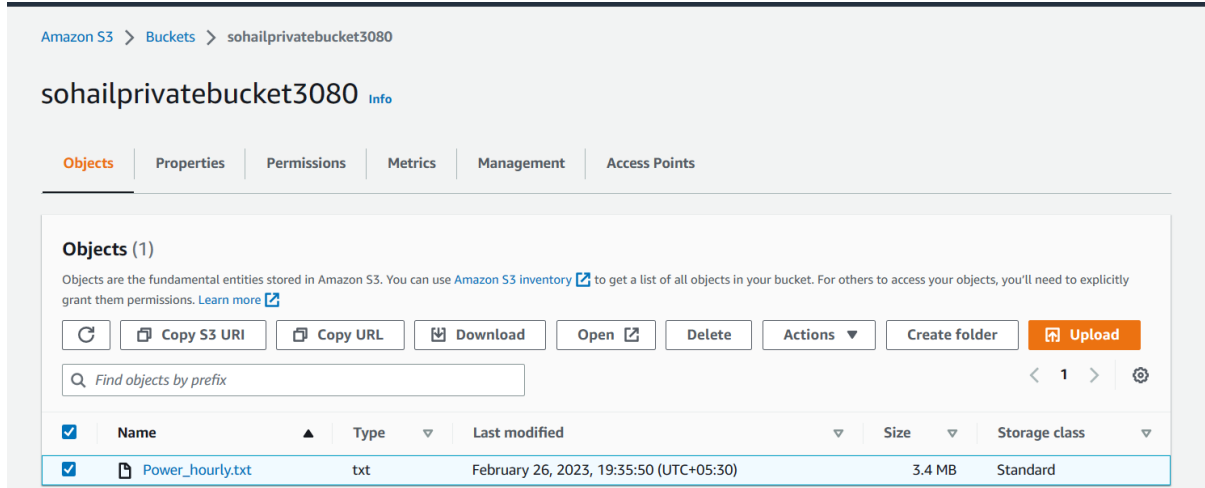
<HostId>rH3nJ6xJp2ge0EDAb6z5szx+hWStP4BNb8FYY5Iv6cx3uoqZxw81etoPLboDRALBXCEICPMh2Fo5s1eocJevJA==</HostId>

</Error>

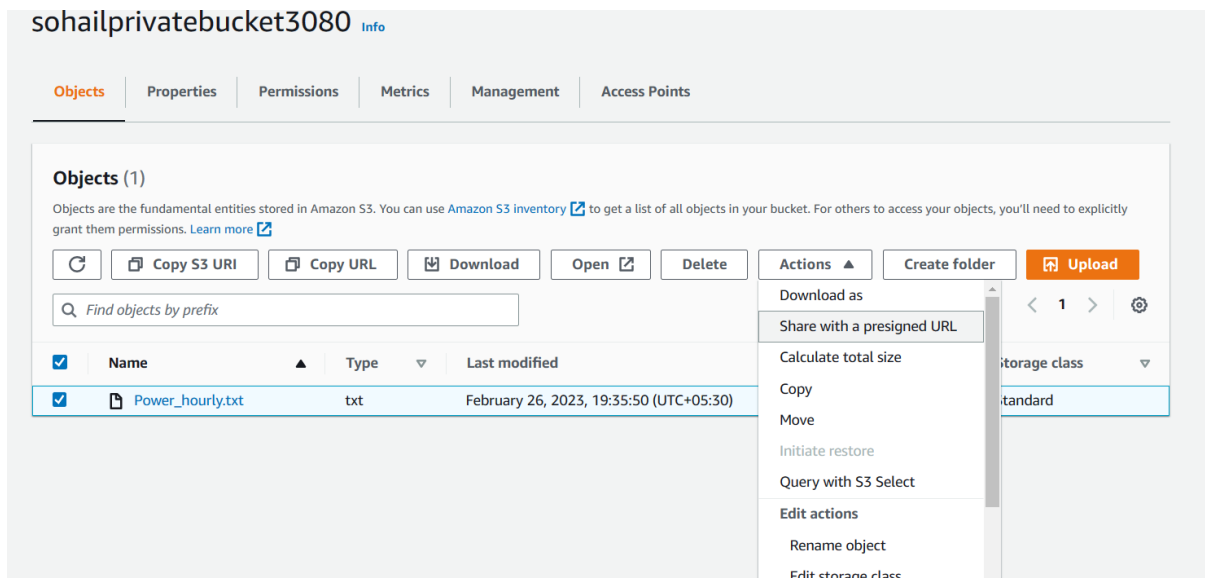
10. Go back to bucket.



11. Select the file uploaded.



12. Then Click on action and select **Share with a presigned URL**.



13. Give a time duration and click **Create presigned URL**.

### Share "Power\_hourly.txt" 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**

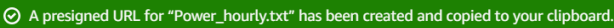
Must be a whole number between 1 and 720.

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

CancelCreate presigned URL



14. Copy the **presigned URL**. Go to another browser and paste the URL [We create a presigned URL because we want give a permission for a time to a private bucket].



Copy presigned URL

Amazon S3 > Buckets > sohailprivatebucket3080

sohailprivatebucket3080 [Info](#)

Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (1)

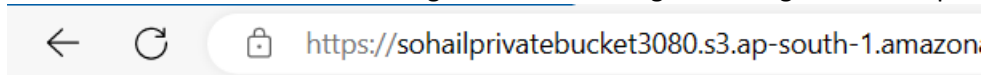
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

< 1 >

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	Power_hourly.txt	txt	February 26, 2023, 19:35:50 (UTC+05:30)	3.4 MB	Standard

You can access the file now for the given duration assigned during creation of presigned URL.



Datetime	AEP_MW
2004-12-31 01:00:00	13478.0
2004-12-31 02:00:00	12865.0
2004-12-31 03:00:00	12577.0
2004-12-31 04:00:00	12517.0
2004-12-31 05:00:00	12670.0
2004-12-31 06:00:00	13038.0
2004-12-31 07:00:00	13692.0
2004-12-31 08:00:00	14297.0
2004-12-31 09:00:00	14719.0
2004-12-31 10:00:00	14941.0
2004-12-31 11:00:00	15184.0
2004-12-31 12:00:00	15009.0

# Assignment 5

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



1. Open the **Amazon Web Services** home page (aws.amazon.com).
2. Choose **Sign into Console**.
3. Sign in as **Root user** using your email address and password.
4. Go to search and search s3 (S3: simple storage service).

**or**, go to buckets on the side panel and click on side panel. And click on **Create bucket**.

5. In **Create bucket** page:

Give globally unique name as it is created globally.

- Give the Bucket name in the General configuration section.
- Select **ACL enabled** in the Object Ownership section.
- Uncheck **Block all public access** in the Block Public Access settings for this bucket section.
- Check **I acknowledge in Turning off block all public access**.

The screenshot shows the AWS Management Console 'Create bucket' page. The breadcrumb navigation at the top reads 'Amazon S3 > Buckets > Create bucket'. The main heading is 'Create bucket' with an 'Info' link. Below this, a sub-header states 'Buckets are containers for data stored in S3. [Learn more](#)'. The page is divided into two main sections: 'General configuration' and 'Object Ownership'.

**General configuration**

Bucket name: . A note below states: '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. A 'Choose bucket' button is present.

**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.

Two radio buttons are shown for Object Ownership: 'ACLs disabled (recommended)' (unselected) and 'ACLs enabled' (selected). The 'ACLs enabled' option has a description: 'Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.'

Below this, 'Object Ownership' is further detailed with two radio buttons: 'Bucket owner preferred' (selected) and 'Object writer' (unselected). The 'Bucket owner preferred' option has a description: '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.'

Two informational boxes are present at the bottom:

- Info:** If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)
- Upcoming permission changes to enable ACLs:** Starting in April 2023, to enable ACLs when creating buckets by using the S3 console, you must have 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.

#### ☐ 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.



### Upcoming permission changes to disable any Block Public Access setting

Starting in April 2023, to disable any Block Public Access setting when creating buckets by using the S3 console, you must have the `s3:PutBucketPublicAccessBlock` permission. [Learn more](#)

## 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

- ☒ Disable  
☐ Enable

## Tags (0) - optional

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

Add tag

## Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

### Encryption key type [Info](#)

- ☒ Amazon S3-managed keys (SSE-S3)  
☐ AWS Key Management Service key (SSE-KMS)

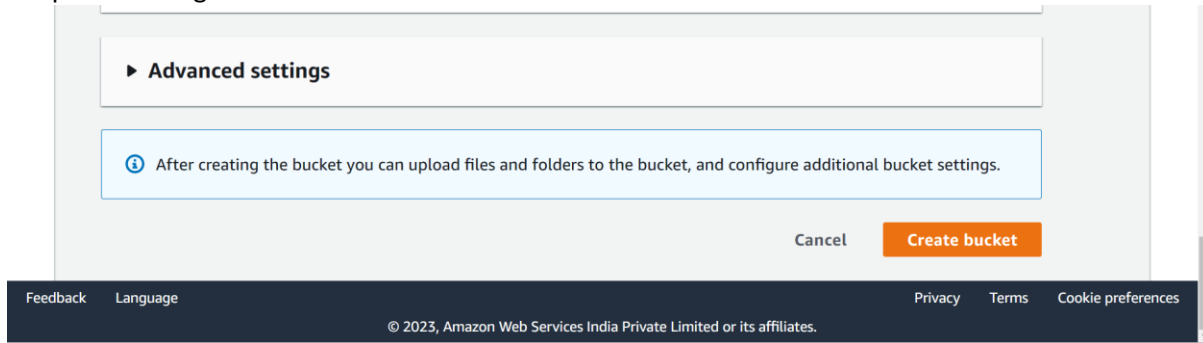
### Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS.

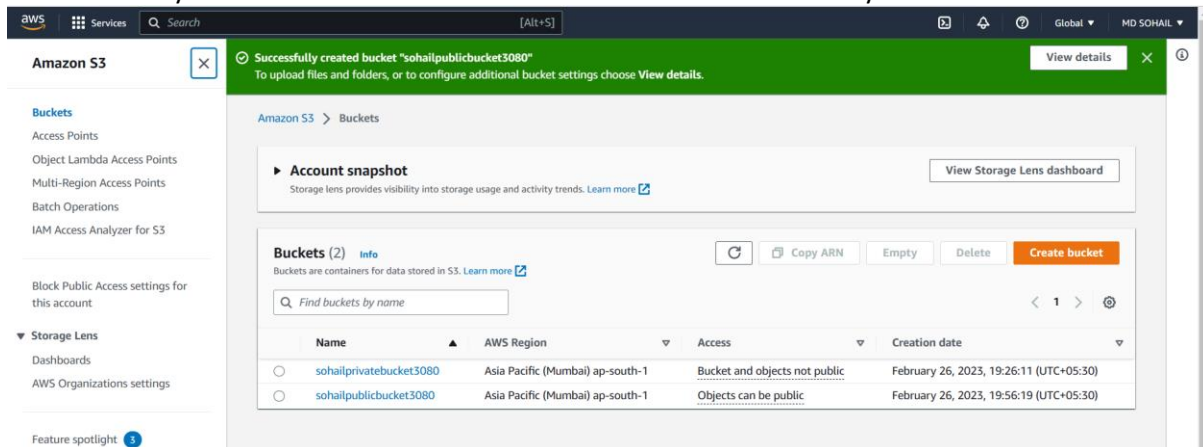
[Learn more](#)

- ☐ Disable  
☒ Enable

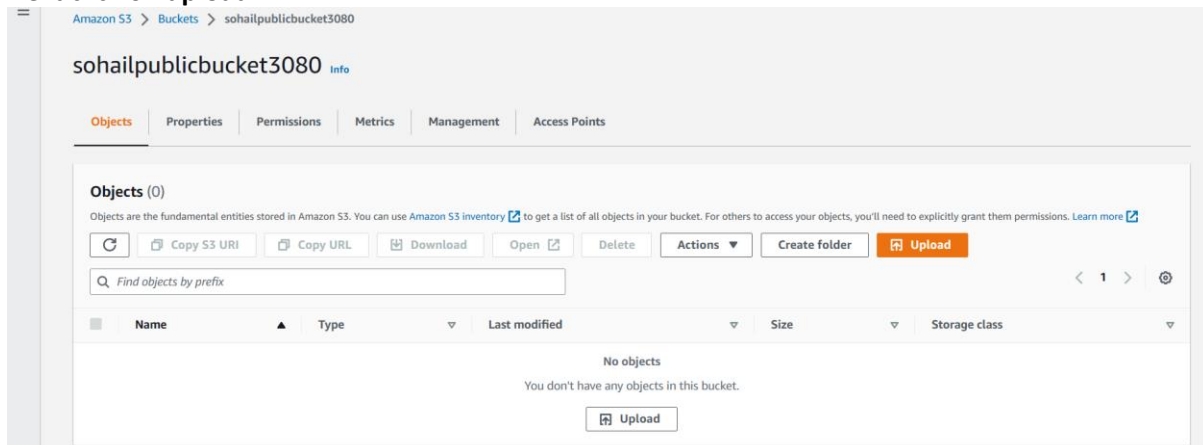
Keep other things at default and **click on Create Bucket.**



6. Now check your bucket will be created. Next Click on the bucket that you have created.



Next click on **upload.**



## 7. In Upload page:

Click on **Add files** to upload a file.

Amazon S3 > Buckets > sohailpublicbucket3080 > 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 (0)**

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

	Name	Folder	Type	Size
No files or folders				
You have not chosen any files or folders to upload.				

Destination

Select the file and click on **Upload**.

Amazon S3 > Buckets > sohailpublicbucket3080 > 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, 3.4 MB)**

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

<input checked="" type="checkbox"/>	Name	Folder	Type	Size
<input checked="" type="checkbox"/>	Power_hourly.txt	-	text/plain	3.4 MB

Destination

Destination  
s3://sohailpublicbucket3080

► 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.

Cancel

Upload

Feedback

Language

© 2023, Amazon Web S

Then click on the file uploaded file on the upload status page.

Upload succeeded  
View details below.

Upload: status

The information below will no longer be available after you navigate away from this page.

Summary

Destination  
s3://sohailpublicbucket3080

Succeeded  
1 file, 3.4 MB (100.00%)

Failed  
0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 Total, 3.4 MB)

Find by name

Name	Folder	Type	Size	Status	Error
Power_hourly.txt	-	text/plain	3.4 MB	Succeeded	-

Copy the URL and open in new tab.

Power\_hourly.txt

Copy S3 URI

Download

Open

Object actions

Properties

Permissions

Versions

Object overview

Owner  
be7f5e639210abc9e141fb0824f69eccbe04bff1bc9c37c536030f356938a0c3

AWS Region  
Asia Pacific (Mumbai) ap-south-1

Last modified  
February 26, 2023, 19:59:28 (UTC+05:30)

Size  
3.4 MB

Type  
txt

Key  
Power\_hourly.txt

S3 URI  
s3://sohailpublicbucket3080/Power\_hourly.txt

Amazon Resource Name (ARN)  
arn:aws:s3:::sohailpublicbucket3080/Power\_hourly.txt

Entity tag (Etag)  
15d0917e9952d5954a1fea9532525b63

Object URL Copied  
https://sohailpublicbucket3080.s3.ap-south-1.amazonaws.com/Power\_hourly.txt

You can see **Object URL** cannot be accessed.

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>FW316QCD2DYCGY62</RequestId>

<HostId>YWeyx00zlwkvjabodwxyIbFD5E+1ba6PqbYBsPGzRxEqeM0V3NQ/YjsjAwbGrDGDPi6Kl03j7cs=</HostId>

</Error>

8. Next Go to **Permission** tab beside the Properties tab (it shows access control list).

Properties Permissions Versions		
<b>Access control list (ACL)</b> <span>Edit</span>		
Grant basic read/write permissions to AWS accounts. <a href="#">Learn more</a>		
Grantee	Object	Object ACL
Object owner (your AWS account) Canonical ID:  be7f5e639210abc9e141fb0824f69eccbe04bff1bc9c37c536030f356938a0c3	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	-	-

Next Click on **Edit**.

9. Under **ACL** section, In Everyone (public access), check two read boxes.

Services

Search

[Alt+S]

≡


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:  be7f5e639210abc9e141fb0824f69eccbe04bff1bc9c37c536030f356938a0c3	<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
Authenticated users group (anyone with an AWS account) Group:  http://acs.amazonaws.com/groups/global/AuthenticatedUsers	<input type="checkbox"/> Read	<input type="checkbox"/> Read <input type="checkbox"/> Write

10. Then check **I understand the effects of these changes on this object.**  
Next Click on **Save changes.**

 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
 <a href="#">Power_hourly.txt</a>	txt	February 26, 2023, 19:59:28 (UTC+05:30)	3.4 MB

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

11. Now Refresh the object URL open in another browser you can access the file now.

   [https://sohailpublicbucket3080.s3.ap-south-1.amazonaws.com/Power\\_hourly.txt](https://sohailpublicbucket3080.s3.ap-south-1.amazonaws.com/Power_hourly.txt)

```
Datetime      AEP_MW
2004-12-31 01:00:00,13478.0
2004-12-31 02:00:00,12865.0
2004-12-31 03:00:00,12577.0
2004-12-31 04:00:00,12517.0
2004-12-31 05:00:00,12670.0
2004-12-31 06:00:00,13038.0
2004-12-31 07:00:00,13692.0
2004-12-31 08:00:00,14297.0
2004-12-31 09:00:00,14719.0
2004-12-31 10:00:00,14941.0
2004-12-31 11:00:00,15184.0
2004-12-31 12:00:00,15009.0
2004-12-31 13:00:00,14808.0
2004-12-31 14:00:00,14522.0
2004-12-31 15:00:00,14349.0
2004-12-31 16:00:00,14107.0
-----
```