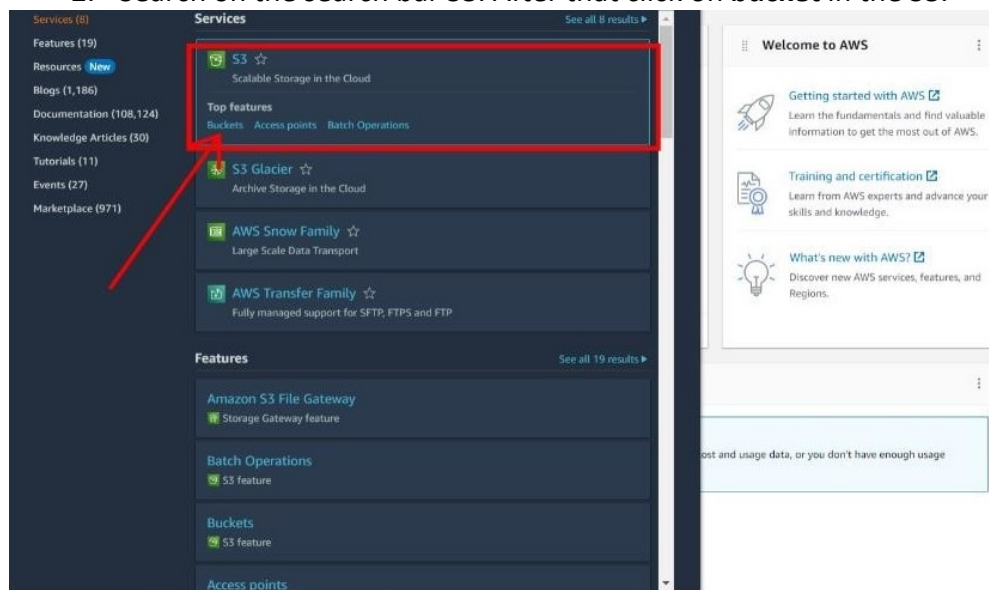


## Assignment 5

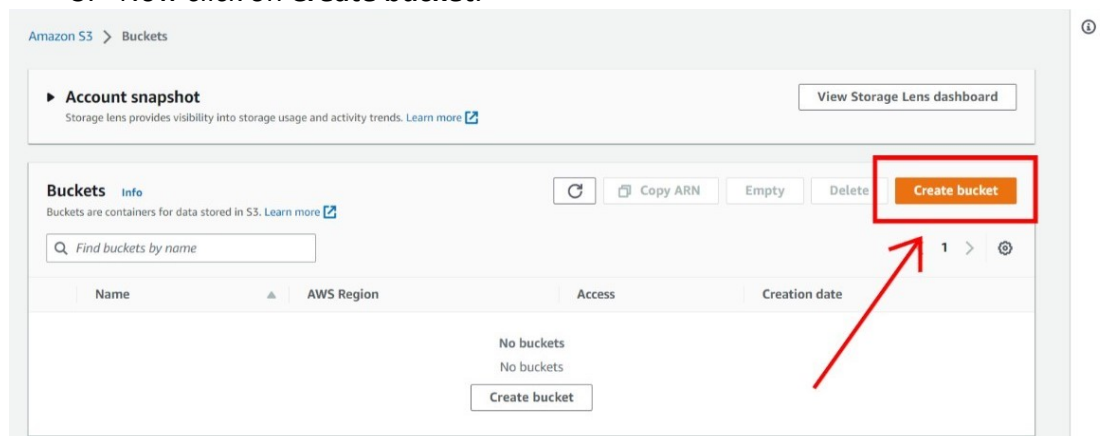
Create a public bucket in AWS. Upload a file and give the necessary permission to check the file url is working or not.

### Steps for creating an AWS account:

1. **Sign in.** Sign in as a root user. Provide username and password when prompted.
2. Search on the search bar **S3**. After that click on **bucket** in the **S3**.



3. Now click on **Create bucket**.



#### 4. Give a **Unique** bucket name.

aws Services Search [Alt+S]

Amazon S3 > Buckets > Create bucket

### Create bucket [Info](#)

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

#### General configuration

Bucket name

Dip12

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](#)

#### 5. Now click on **ACLs enable**. After that click on **Bucket owner preferred**.

### 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 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  
The object writer remains the object owner.

**i** 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](#)

**i** **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](#)


6. Uncheck the **Block all public access** and check **I acknowledge**.

**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. Now give the **Bucket versioning** as **disable**.

**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

8. In the **Default encryption** section don't change anything. Click on **create bucket**.

The screenshot shows the 'Default encryption' section of the Amazon S3 'Create bucket' wizard. A red box highlights the 'Default encryption' section, which includes the 'Encryption key type' (Amazon S3-managed keys (SSE-S3) is selected) and the 'Bucket Key' (Enable is selected). A red arrow points to the 'Create bucket' button at the bottom right.

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**

9. After your bucket has created click on the **bucket name**.

The screenshot shows the 'Buckets' page in the Amazon S3 console. A red arrow points to the bucket name 'dip12' in the table.

Amazon S3 > Buckets

► Account snapshot Info  
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](#)

Find buckets by name

Name	AWS Region	Access	Creation date
dip12	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	February 20, 2023, 19:25:24 (UTC+05:30)

10. After that click on **upload** to upload files or folders.

The screenshot shows the 'Objects' page for the bucket 'dip12'. A red arrow points to the 'Upload' button at the bottom.

Amazon S3 > Buckets > dip12

**dip12** 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](#)

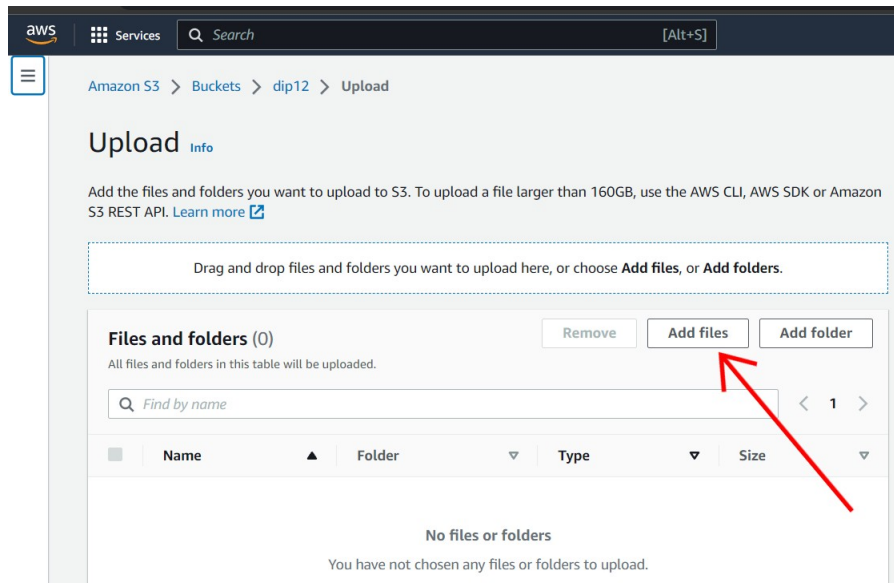
Copy S3 URI Copy URL Download Open Delete Actions Create folder **Upload**

Find objects by prefix

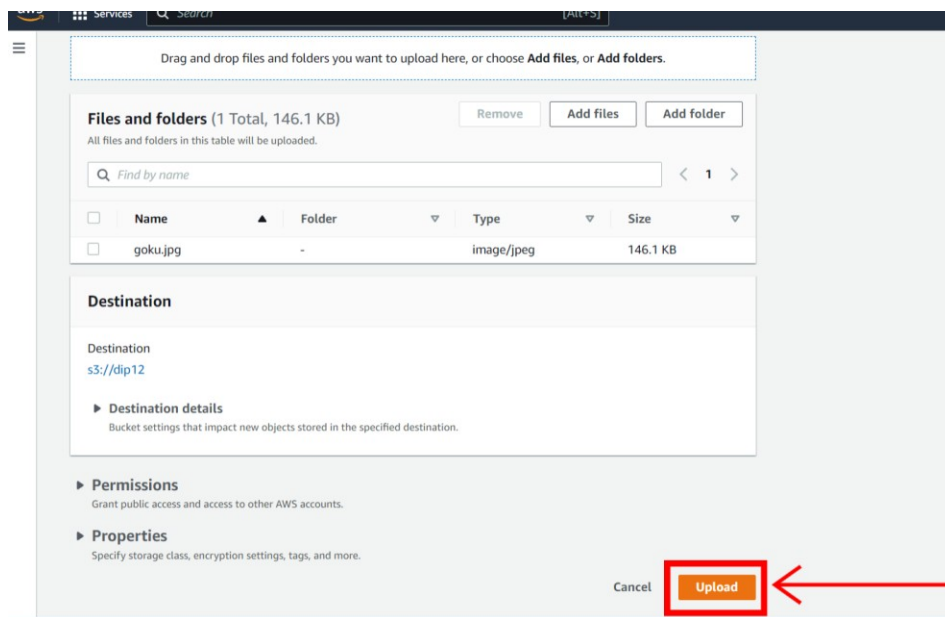
Name	Type	Last modified	Size	Storage class
No objects You don't have any objects in this bucket.				

Upload

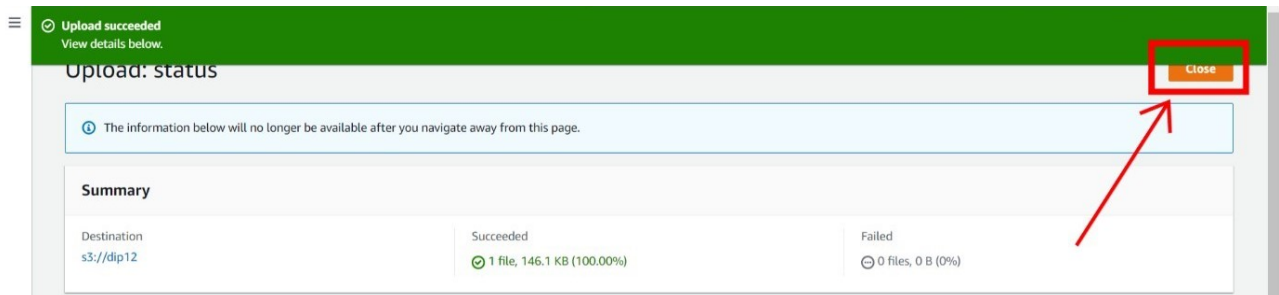
11. Click on **Add files** to add files or **Add folder** to add folders.



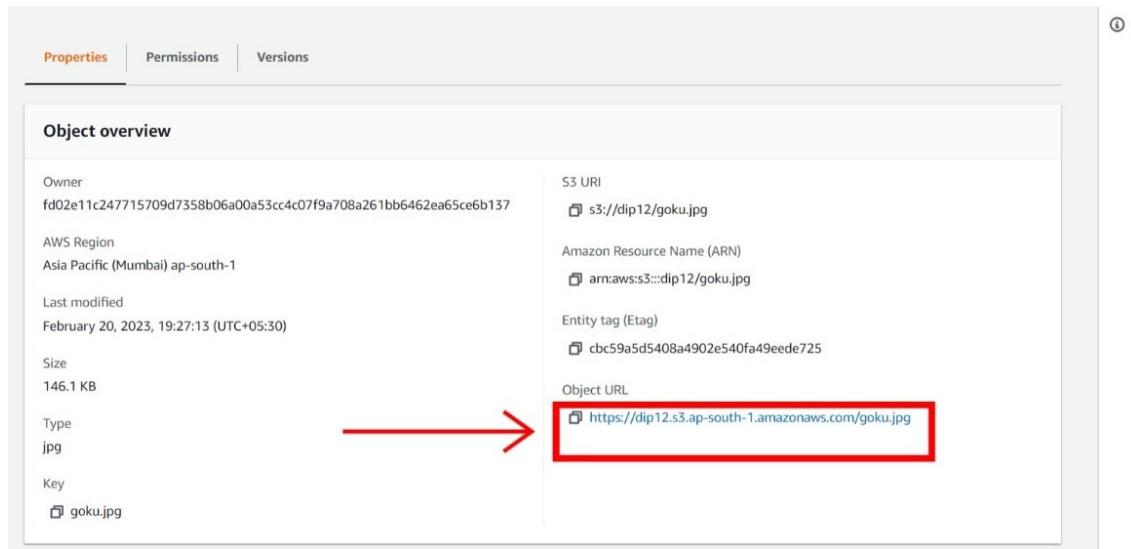
12. After that click on **upload**.



13. Now click **Close**.



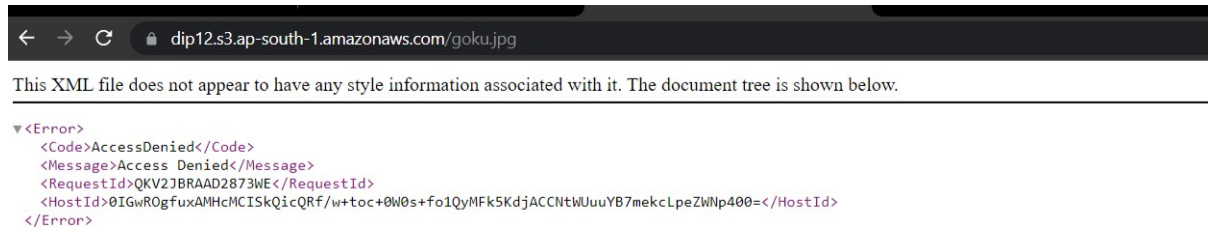
14. Click on the **object URL** to copy the URL so that we can see the file on web.



The screenshot shows the 'Object overview' page in the AWS S3 console. The 'Object URL' field is highlighted with a red box, and a red arrow points to it. The URL is <https://dip12.s3.ap-south-1.amazonaws.com/goku.jpg>.

Property	Value
Owner	fd02e11c247715709d7358b06a00a53cc4c07f9a708a261bb6462ea65ce6b137
AWS Region	Asia Pacific (Mumbai) ap-south-1
Last modified	February 20, 2023, 19:27:13 (UTC+05:30)
Size	146.1 KB
Type	jpg
Key	goku.jpg
S3 URI	s3://dip12/goku.jpg
Amazon Resource Name (ARN)	arn:aws:s3:::dip12/goku.jpg
Entity tag (Etag)	cbc59a5d5408a4902e540fa49eede725
Object URL	<a href="https://dip12.s3.ap-south-1.amazonaws.com/goku.jpg">https://dip12.s3.ap-south-1.amazonaws.com/goku.jpg</a>

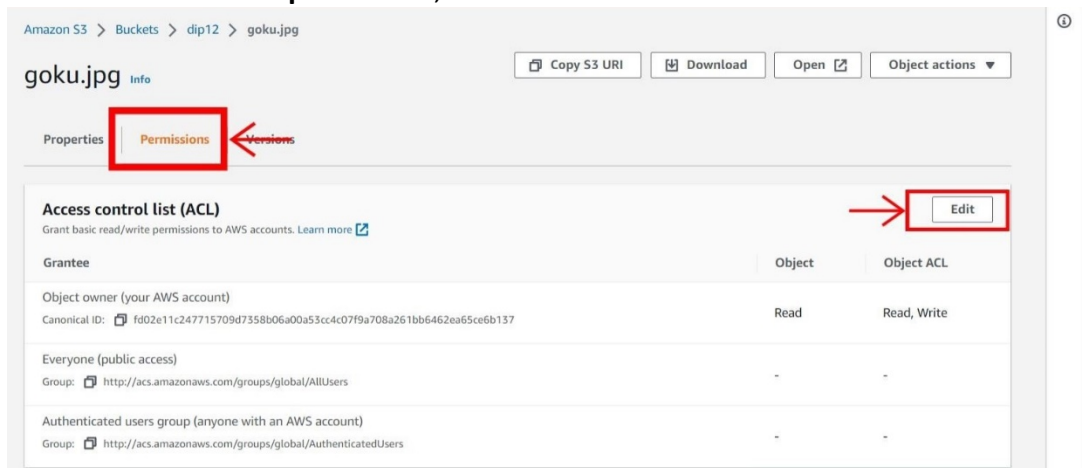
15. As we have not given the permission as public we can't able to see the file.



The screenshot shows a web browser displaying an 'Access Denied' error. The address bar shows the URL [dip12.s3.ap-south-1.amazonaws.com/goku.jpg](https://dip12.s3.ap-south-1.amazonaws.com/goku.jpg). The error message states: "This XML file does not appear to have any style information associated with it. The document tree is shown below." followed by an XML error snippet.

```
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>QKV2JBRAAD2873WE</RequestId>
  <HostId>0IGwROgfuxAMHcMCISkQicQRf/w+toC+0W0s+fo1QyMFk5KdjACCNTWUuYB7mekcLpeZWnp400=</HostId>
</Error>
```

16. Now click on **permission**, after that click on **edit**.



The screenshot shows the 'Permissions' page in the AWS S3 console for the object 'goku.jpg'. The 'Permissions' tab is selected and highlighted with a red box. An 'Edit' button is also highlighted with a red box. The page displays the 'Access control list (ACL)' for the object.

Grantee	Object	Object ACL
Object owner (your AWS account) Canonical ID: fd02e11c247715709d7358b06a00a53cc4c07f9a708a261bb6462ea65ce6b137	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	-	-



17. Check on **Read and Read** in the **Everyone (public access)**.

Amazon S3 > Buckets > dip12 > goku.jpg > Edit access control list

### 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: fd02e11c247715709d7358b06a00a53cc4c07f9a708a261bb6462ea65ce6b137	<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"/> <b>Read</b> ←	<input checked="" type="checkbox"/> <b>Read</b> ← <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

18. Check on **I understand**.

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

**Warning:** 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](#)

19. Check 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
 goku.jpg	jpg	February 20, 2023, 19:30:53 (UTC+05:30)	146.1 KB

Cancel **Save changes** ←

20. Now if you copy the object URL and open in new tab you can see the file which I have uploaded.

