

S3 SERVICE In AWS

S3 is simple service storage. It is object-based storage you can storage images, word files, pdf files etc

The files which store in s3 in 0 byte to 5 kb. Files are stored in Bucket. A bucket is like a folder available in S3 that stores the files.

Built for 99.99 % availability for s3 platform

Amazon Guarantee 99.9999999999% availbale

Lifecycle management, Versioning, Encryption

Secure your data using Access control list and bucket policy

S3 allows the hosting static website

CREATING IN S3 BUCKET

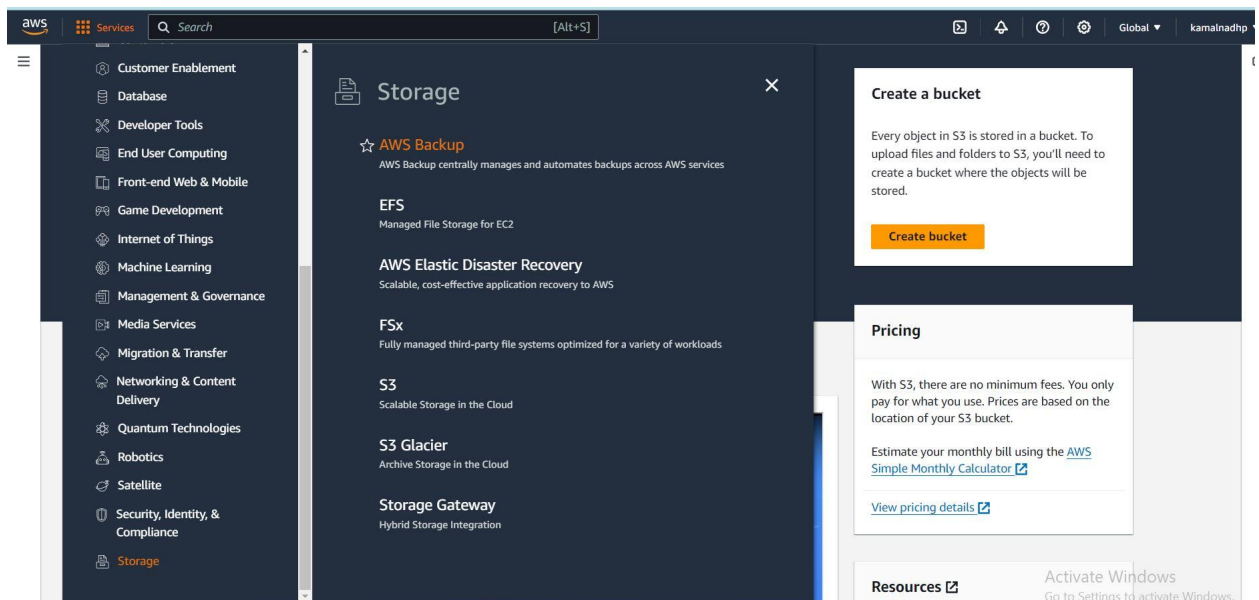
Bucket : bucket is the container used for storing the objects. Each bucket has own policies and configurations You can created 100 buckets in one aws account .but if requested more bucket you need the aws support

RULES OF CREATETING in s3 bucket

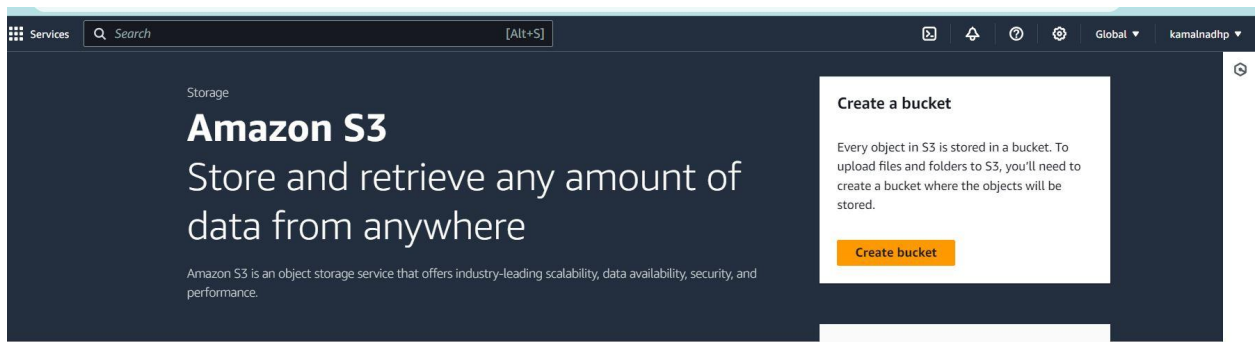
- * Bucket name should consist the lowercase , numbers, dots
- * Bucket name start and ends with numbers or letters
- * Bucket should not contains the adjacent sides
- * bucket name should not contains ip address
- * bucket name should be uniquely
- * bucket name should start with the ip address

STEPS OF CREATING IN S3 BUCKET

1. Go the storage select on s3 bucket



2. click the s3 storage if you want the storage can files you need to created s3 bucket



3.given bucketname should be unique

Create bucket [Info](#)

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

General configuration

AWS Region
Europe (Stockholm) eu-north-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 - New**
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](#)
kamalnadh123

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.

Choose bucket

Format: s3://bucket/prefix

4. ACL is the access control list it is used for control you bucket with respect the security

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

5.all the bucket by default is private as shown figure

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.

5.click on the created bucket

General purpose buckets (1) [Info](#)

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

[Refresh](#) [Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

Name	AWS Region	Access	Creation date
kamalnadh123	Europe (Stockholm) eu-north-1	Bucket and objects not public	December 13, 2023, 16:12:40 (UTC+09:00)

6.upload the file the kamalnadh123 bucket click upload the files as shown in figure

[Amazon S3](#) > [Buckets](#) > kamalnadh123

kamalnadh123 [Info](#)

[Objects](#) | [Properties](#) | [Permissions](#) | [Metrics](#) | [Management](#) | [Access Points](#)

Objects (0) [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 permissions. [Learn more](#)

[Refresh](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

Name	Type	Last modified	Size	Storage class
No objects				

You don't have any objects in this bucket.

[Upload](#)

Click upload add file or add folder as you requirements

The image shows two screenshots of the AWS S3 Upload interface. The top screenshot shows the initial state where no files are selected. The bottom screenshot shows the state after uploading a file named 'LAUGHINING APPLIC...'.

Top Screenshot: Initial State

Amazon S3 > Buckets > kamalnadh123 > 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 folder**.

Files and folders (0) Remove Add files Add folder

All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder	Type	Size
No files or folders				
You have not chosen any files or folders to upload.				

Bottom Screenshot: After Upload

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

Files and folders (1 Total, 1.2 MB) Remove Add files Add folder

All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	LAUGHINING APPLIC...	-	application/pdf	1.2 MB

Destination Info

Destination
[s3://kamalnadh123](#)

► **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

After upload the files in click on it go the properties copy url as shown below

Amazon S3 > Buckets > [kamalnadh123](#) > LAUGHINING Application load balance IN TWO MACHINE.pdf

LAUGHINING Application load balance IN TWO MACHINE.pdf [Info](#)

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

[Properties](#)
[Permissions](#)
[Versions](#)

Object overview

Owner	15a3997f88708f18561d014c637d140b3250efb7febf8b578f28c6df4e56e78	S3 URI	s3://kamalnadh123/LAUGHINING Application load balance IN TWO MACHINE.pdf
AWS Region	Europe (Stockholm) eu-north-1	Amazon Resource Name (ARN)	arn:aws:s3:::kamalnadh123/LAUGHINING Application load balance IN TWO MACHINE.pdf
Last modified	December 13, 2023, 16:35:17 (UTC+09:00)	Entity tag (Etag)	911d7ebdf4c331080a13e14162d44388
Size	1.2 MB	Object URL	https://kamalnadh123.s3.eu-north-1.amazonaws.com/LAUGHINING++APPLICATION+load+balance+IN+TWO+MACHINE.pdf
Type	pdf		
Key	LAUGHINING Application load balance IN TWO MACHINE.pdf		

Activate Windows
Go to Settings to activate Windows

The url copy and paste it will be error because bucket and object are private you need the change to public

← → ↻ 🔒 kamalnadh123.s3.eu-north-1.amazonaws.com/LAUGHINING++APPLICATION+load+balance+IN+TWO+MACHINE.pdf

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

```
<?xml version="1.0" encoding="UTF-8"?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>0RC3FBY2M01PE19R</RequestId>
  <HostId>tndGrv1OK11h0HfdT5OLKh8GV591Nj1NR5b69Sunt1MfCapo067W31Ry3nKVrfzU55Pc83/10M=</HostId>
</Error>
```

Go the bucket change permissssions block public access edit

kamalnadh123 [Info](#)

[Objects](#) | [Properties](#) | [Permissions](#) | [Metrics](#) | [Management](#) | [Access Points](#)

Permissions overview

Access

Bucket and objects not public

Block public access (bucket settings)

[Edit](#)

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 all your S3 buckets and 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block *all* public access

☒ On

► Individual Block Public Access settings for this bucket

Edit Block public access (bucket settings) [Info](#)

Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets 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.

Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Edit Block public access (bucket settings)

⚠ Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

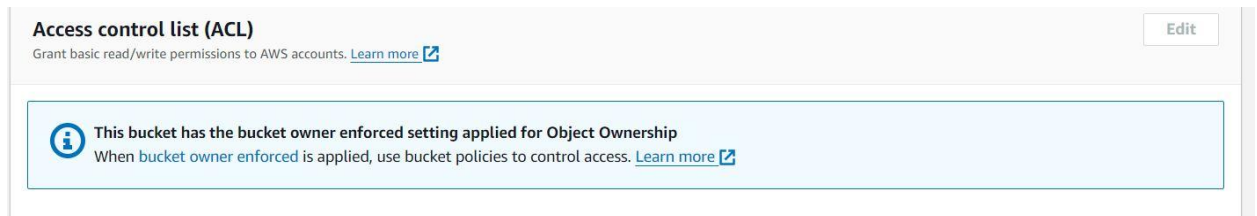
To confirm the settings, enter *confirm* in the field.

confirm

[Cancel](#)

[Confirm](#)

You upload the file in bucket change the object in public go object permissions change acl disable as shown in figure



Click on the bucket owner enforced change ACLS enabled as shown figure

☐ **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.

⚠ **Enabling ACLs turns off the bucket owner enforced setting for Object Ownership**
 Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.

☒ I acknowledge that ACLs will be restored.

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.

🔗 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](#)

Click on read object and read the object ACL as shown in figure

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: 15a3997f88708f18561d0 14c637d140b3250efb7febf8b 578f28c6df4e56e78	<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

Copy the url the paste chrome it open as shown in figure

