

## Choosing an AWS storage service:

- AWS offers a broad portfolio of reliable, scalable, and secure storage services for storing, accessing, protecting, and analyzing your data.
- This makes it easier to match your storage methods with your needs, and provides storage options that are not easily achievable with on-premises infrastructure.
- When selecting a storage service, ensuring that it aligns with your access patterns will be critical to achieving the performance you want.
- You can select from block, file, and object storage services as well as cloud data migration options for your workload.
- Choosing the right storage service for your workload requires you to make a series of decisions based on your business needs.

<b>Purpose</b>	Help determine which AWS storage service is the best fit for your organization.
<b>Last updated</b>	June 26, 2024
<b>Covered services</b>	<ul style="list-style-type: none"> <li>• <a href="#">Amazon S3</a></li> <li>• <a href="#">Amazon EBS</a></li> <li>• <a href="#">Amazon EFS</a></li> <li>• <a href="#">Amazon FSx</a></li> <li>• <a href="#">Amazon File Cache</a></li> <li>• <a href="#">AWS Backup</a></li> <li>• <a href="#">AWS DataSync</a></li> <li>• <a href="#">AWS Snow Family</a></li> <li>• <a href="#">AWS Storage Gateway</a></li> <li>• <a href="#">AWS Transfer Family</a></li> </ul>

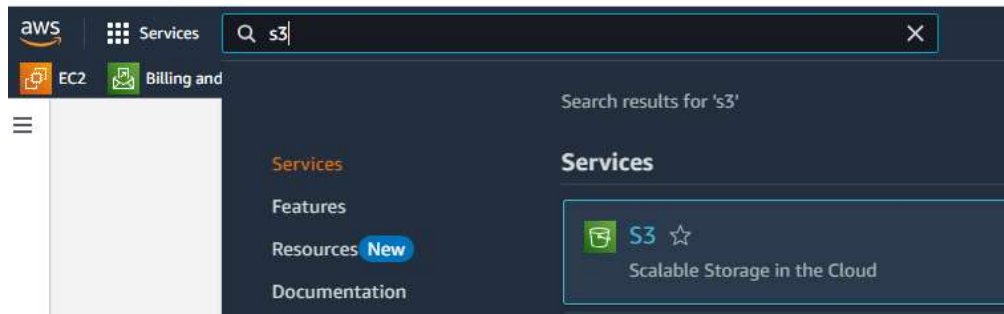
Storage type	What is it optimized for?	Storage services or tools
Object	Read-heavy workloads such as content distribution, web hosting, big data analytics, and ML workflows. Well-suited for scenarios where data needs to be stored, accessed, and distributed globally over the internet.	<a href="#">Amazon S3</a>

## Amazon S3

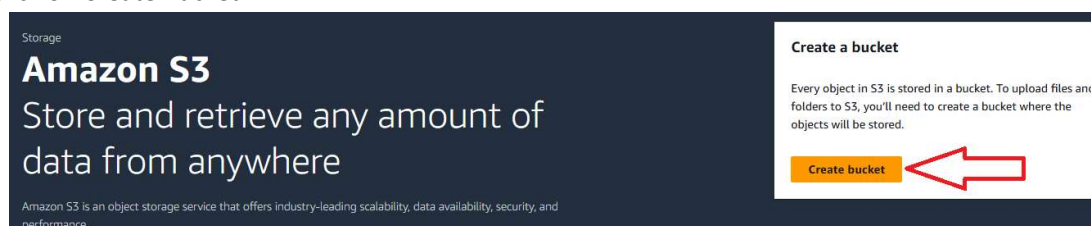
- You can get started with Amazon S3 by working with buckets and objects.
- A bucket is a container for objects. An object is a file and any metadata that describes that file.
- To store an object in Amazon S3, you create a bucket and then upload the object to the bucket.
- When the object is in the bucket, you can open it, download it, and move it.
- When you no longer need an object or a bucket, you can clean up your resources.
- With Amazon S3, you pay only for what you use.
- When you sign up for AWS, your AWS account is automatically signed up for all services in AWS, including Amazon S3. You are charged only for the services that you use.

## Creating S3 bucket:

- Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.
1. Search for S3 under Services, and click on S3.



2. Click on Create Bucket.



3. Give a name to the Bucket. Bucket name must be unique within the global namespace and follow the bucket naming rules.

## General purpose buckets naming rules:

The following naming rules apply for general purpose buckets.

- Bucket names must be between 3 (min) and 63 (max) characters long.
- Bucket names can consist only of lowercase letters, numbers, dots (.), and hyphens (-).
- Bucket names must begin and end with a letter or number.
- Bucket names must not contain two adjacent periods.
- Bucket names must not be formatted as an IP address (for example, 192.168.5.4).
- Bucket names must not start with the prefix xn--.
- Bucket names must not start with the prefix sthree-.
- Bucket names must not start with the prefix sthree-configurator.
- Bucket names must not start with the prefix amzn-s3-demo-.
- Bucket names must not end with the suffix -s3alias. This suffix is reserved for access point alias names.
- Bucket names must not end with the suffix --ol-s3. This suffix is reserved for Object Lambda Access Point alias names.
- Bucket names must not end with the suffix .mrp. This suffix is reserved for Multi-Region Access Point names.
- Bucket names must not end with the suffix --x-s3. This suffix is reserved for directory buckets.
- Bucket names must be unique across all AWS accounts in all the AWS Regions within a partition. A partition is a grouping of Regions. AWS currently has three partitions: aws (Standard Regions), aws-cn (China Regions), and aws-us-gov (AWS GovCloud (US)).
- A bucket name cannot be used by another AWS account in the same partition until the bucket is deleted.
- Buckets used with Amazon S3 Transfer Acceleration can't have dots (.) in their names.

Go with the default configuration and create the bucket.

[Amazon S3](#) > [Buckets](#) > Create bucket

## Create bucket [Info](#)

Buckets are containers for data stored in S3.

### General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket name [Info](#)

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

### 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

EC2 Billing and Cost Management IAM

Successfully created bucket "bucket-idream-100"  
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

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

Account snapshot - updated every 24 hours [All AWS Regions](#)  
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

[View Storage Lens dashboard](#)

[General purpose buckets](#) | [Directory buckets](#)

**General purpose buckets (1)** [Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

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

Name	AWS Region	IAM Access Analyzer	Creation date
<input type="radio"/> <a href="#">bucket-idream-100</a>	Asia Pacific (Mumbai) ap-south-1	<a href="#">View analyzer for ap-south-1</a>	November 10, 2024, 21:55:39 (UTC+05:30)

[Amazon S3](#) > [Buckets](#) > bucket-idream-100

**bucket-idream-100** [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](#)

[Copy](#) [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](#)

[Amazon S3](#) > [Buckets](#) > [bucket-idream-100](#) > 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 (1 Total, 4.0 B)

[Remove](#)

[Add files](#)

[Add folder](#)

All files and folders in this table will be uploaded.

< 1 >

<input type="checkbox"/>	Name	Folder
<input type="checkbox"/>	test.txt	-

[Services](#)

[Alt+S]

EC2
 Billing and Cost Management
 IAM

**Upload succeeded**  
View details below.

## Upload: status

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

### Summary

Destination <a href="#">s3://bucket-idream-100</a>	Succeeded 1 file, 4.0 B (100.00%)
---	--------------------------------------

[Files and folders](#)

[Configuration](#)

### Files and folders (1 Total, 4.0 B)


Name	Folder	Type	Size	Status	Error
<a href="#">test.txt</a>	-	text/plain	4.0 B	Succeeded	-

## Deleting the Bucket:

We cannot delete the bucket directly, we should clear the contents and then proceed for deletion.

Amazon S3 > Buckets > bucket-idream-100 > Delete bucket

### Delete bucket Info

 **This bucket is not empty**  
Buckets must be empty before they can be deleted.

Empty bucket


**Delete bucket "bucket-idream-100"?**

To confirm deletion, enter the name of the bucket in the text input field.

Cancel Delete bucket


Amazon S3 > Buckets > bucket-idream-100 > Empty bucket

### Empty bucket Info



- Emptying the bucket deletes all objects in the bucket and cannot be undone.
- Objects added to the bucket while the empty bucket action is in progress might be deleted.
- To prevent new objects from being added to this bucket while the empty bucket action is in progress, you might need to update your bucket policy to stop objects from being added to the bucket.

[Learn more](#)

 If your bucket contains a large number of objects, creating a lifecycle rule to delete all objects in the bucket might be a more efficient way of emptying your bucket. [Learn more](#)

Go to lifecycle rule configuration

**Permanently delete all objects in bucket "bucket-idream-100"?**

To confirm deletion, type *permanently delete* in the text input field.

Cancel Empty

## Deploy static website on AWS using S3:

1. Create a Bucket, and untick the "Block all public access" check box while creating the AWS S3 Bucket.
2. Upload one html file to it. If we will try to access the html file, it will through the error as Access Denied.

### 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.

Refer:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteAccessPermissionsReqd.html>

Add a bucket policy:

Go to:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteAccessPermissionsReqd.html#bucket-policy-static-site>

Copy the bucket policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::Bucket-Name/*"
      ]
    }
  ]
}
```

Replace the Bucket-name with your bucket name.

Select your bucket and select Permissions tab.



Edit the Bucket Policy and paste the content.  
Save the changes and now open your website.

[Amazon S3](#) > [Buckets](#) > test-bucket-idream-10

## test-bucket-idream-10 Info

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

### Permissions overview

Access finding

Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#)

[View analyzer for ap-south-1](#)

### Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::test-bucket-idream-10/*"
    }
  ]
}
```

