

# **Module 6: S3 Bucket Creation**

## **Assignment**

**Assignment Submitted By:-Hitesh Chauhan**

**Course Offered: -Advanced Cloud Computing and Devops**

**Assignment By: -Intellipaat**

**Trainer: -Puneet Gavri**

**Date Of Submission: -24/10/2024**

**Problem Statement:**

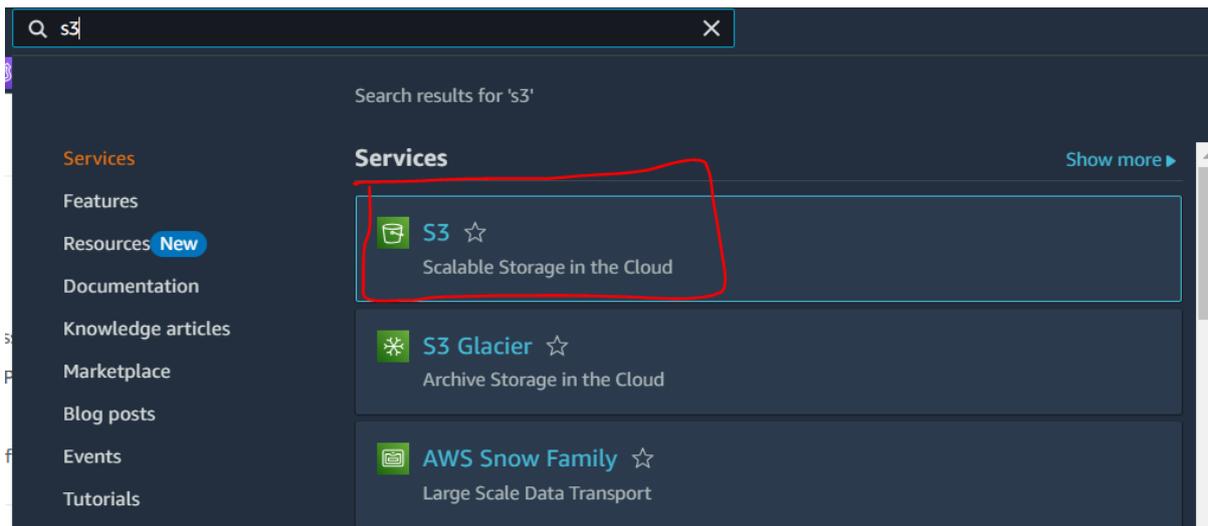
You work for XYZ Corporation. Their application requires a storage service that can store files and publicly share them if required. Implement S3 for the same.

Tasks To Be Performed:

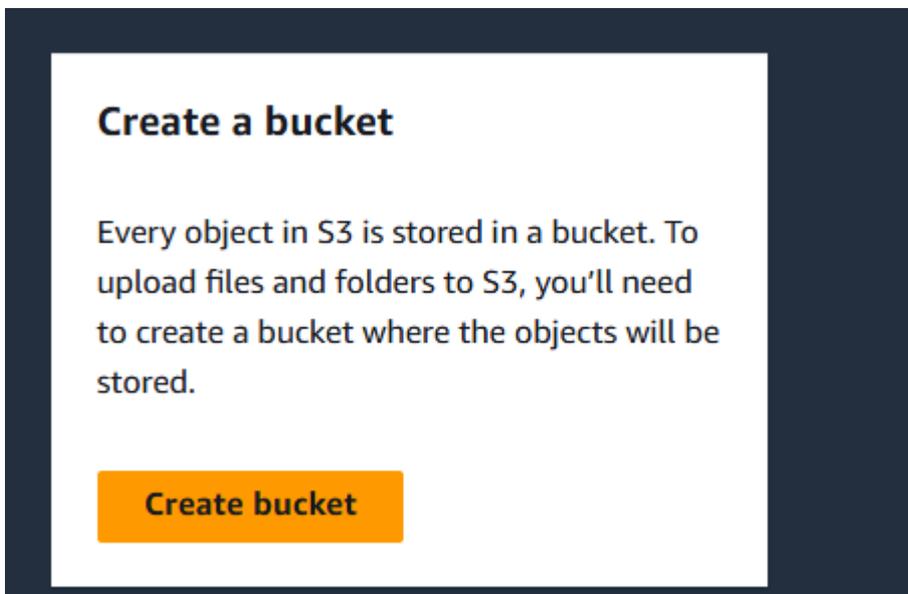
1. Create an S3 Bucket for file storage.
2. Upload 5 objects with different file extensions.

## S3 Bucket Creation Assignment

Login to the AWS Console providing your credentials



In Search bar search for S3 then select S3 in results



In S3 Console Click on "Create Bucket"

# Create bucket [Info](#)

Buckets are containers for data stored in S3.

## General configuration

AWS Region

US East (N. Virginia) us-east-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**

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](#)

hiteshfilestorage

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

## 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.

Provide Bucket Name should be unique

Select the region in which region you wanted to create that bucket

## Object Ownership

ACLs Disabled

Select “Block All Public Access” to avoid publishing your bucket to public

### 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 - optional (0)

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 type [Info](#)

Server-side encryption with Amazon S3 managed keys (SSE-S3)

Server-side encryption with AWS Key Management Service keys (SSE-KMS)

Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the [Storage](#) tab of the [Amazon S3 pricing page](#).

### Advanced settings

#### Object Lock

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](#)

Disable

Enable

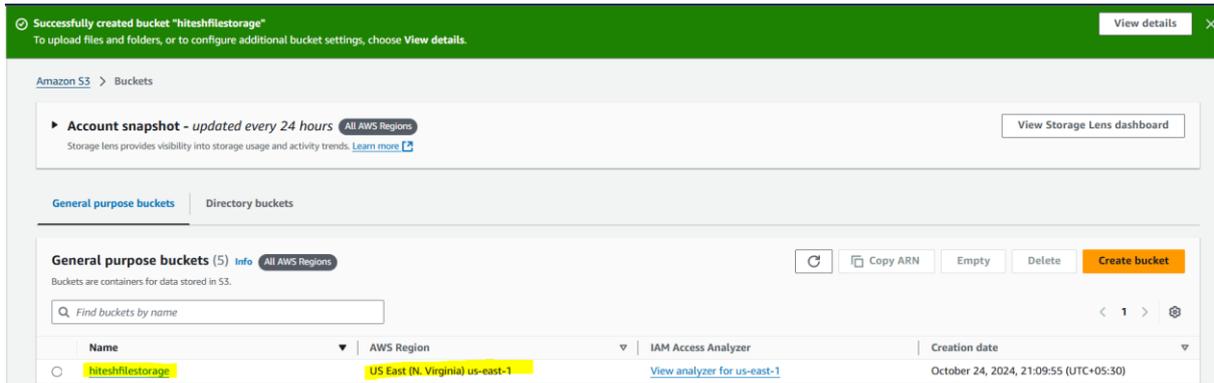
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

[i](#) Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Versioning.

[i](#) After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel [Create bucket](#)

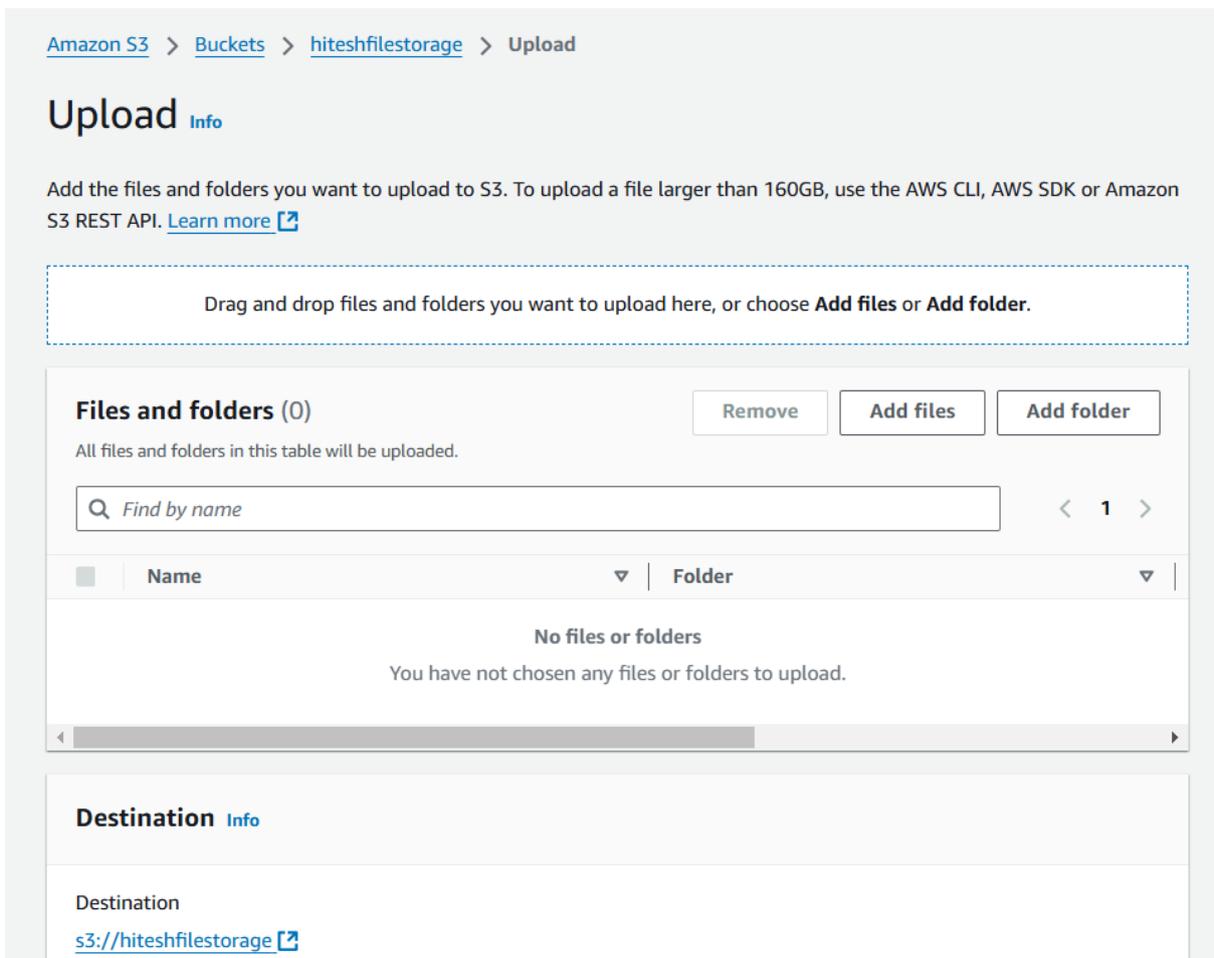
Keep all the Default options Click on “Create Bucket”



Bucket is creation is successful

Now Upload the Objects

Click on the Bucket Name Click Upload Then Click Add files



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 (5 Total, 5.5 MB)

Remove

Add files

Add folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

<input type="checkbox"/>	Name	Folder
<input type="checkbox"/>	Book1.xlsx	-
<input type="checkbox"/>	Capture.JPG	-
<input type="checkbox"/>	Case-Study--VPC-And-Peering.pdf	-
<input type="checkbox"/>	docker-compose.yml	-
<input type="checkbox"/>	epson-3150-3160-adjustment-prog.rar	-

### Destination [Info](#)

Destination

[s3://hiteshfilestorage](#)

#### 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

Then Click Upload

Upload succeeded

View details below.

Destination  
[s3://hiteshfilestorage](#)

Succeeded  
✔ 5 files, 5.5 MB (100.00%)

Failed  
☹ 0 files, 0 B (0%)

Files and folders

Configuration

### Files and folders (5 Total, 5.5 MB)

Find by name

Name	Folder	Type	Size	Status	Error
<a href="#">Book1.xlsx</a>	-	application/v...	9.2 KB	✔ Succeeded	-
<a href="#">Capture.JPG</a>	-	image/jpeg	35.6 KB	✔ Succeeded	-
<a href="#">Case-Study-...</a>	-	application/pdf	151.1 KB	✔ Succeeded	-
<a href="#">docker-comp...</a>	-	-	589.0 B	✔ Succeeded	-
<a href="#">epson-3150-...</a>	-	-	5.3 MB	✔ Succeeded	-

Objects are uploaded successfully