

Experiment 3 : Create and configure storage services and upload files and objects using Amazon EBS, Amazon EFS and Amazon S3

Step 1 : Login into the AWS learners lab

Step 2 : Navigate to the S3 Bucket Section and Click on Create new Bucket

Step 3 : In General Configuration select General purpose and give name to the 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
22bd1a05dr

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

Step 4 : In the Object Ownership section select ACLs enabled

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.

 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.


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](#)

Step 5 : In the Block Public Access settings for this Disable all check boxes

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.

Step 6 : Enable Bucket Versioning

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**

Step 7 : Keep the rest configuration default selected checks

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](#).

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

☐ **Disable**

☒ **Enable**

Edit access control list (ACL) [Info](#)

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: 33e58d42e11a310847419af92f7a1c0f304401cd3a7f01b9289b b0387260c5ed	<input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Write	<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"/> List <input type="checkbox"/> Write	<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"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write

⚠ When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access the objects in this bucket.

[Learn more](#)

☒ I understand the effects of these changes on my objects and buckets.

Access for other AWS accounts

No other AWS accounts associated with the resource.

[Add grantee](#)

[Cancel](#)

[Save changes](#)

Step 10 : Upload a single file and click on 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 SDKs 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, 151.7 KB)

All files and folders in this table will be uploaded.

Find by name

< 1 >

<div><div><div></div></div></div> <div>Name</div>	<div><div><div></div></div></div> <div>Folder</div>	<div><div><div></div></div></div> <div>Type</div>	<div><div><div></div></div></div> <div>Size</div>	<div><div><div></div></div></div>
<div><div><div></div></div><div>kmit.jpg</div></div>	<div>-</div>	<div>image/jpeg</div>	<div>151.7 KB</div>	

Destination [Info](#)

Destination

<s3://22bd1a05dr>

► Destination details

Bucket settings that impact new objects stored in the specified destination.

► Permissions

Grant public access and access to other AWS accounts.

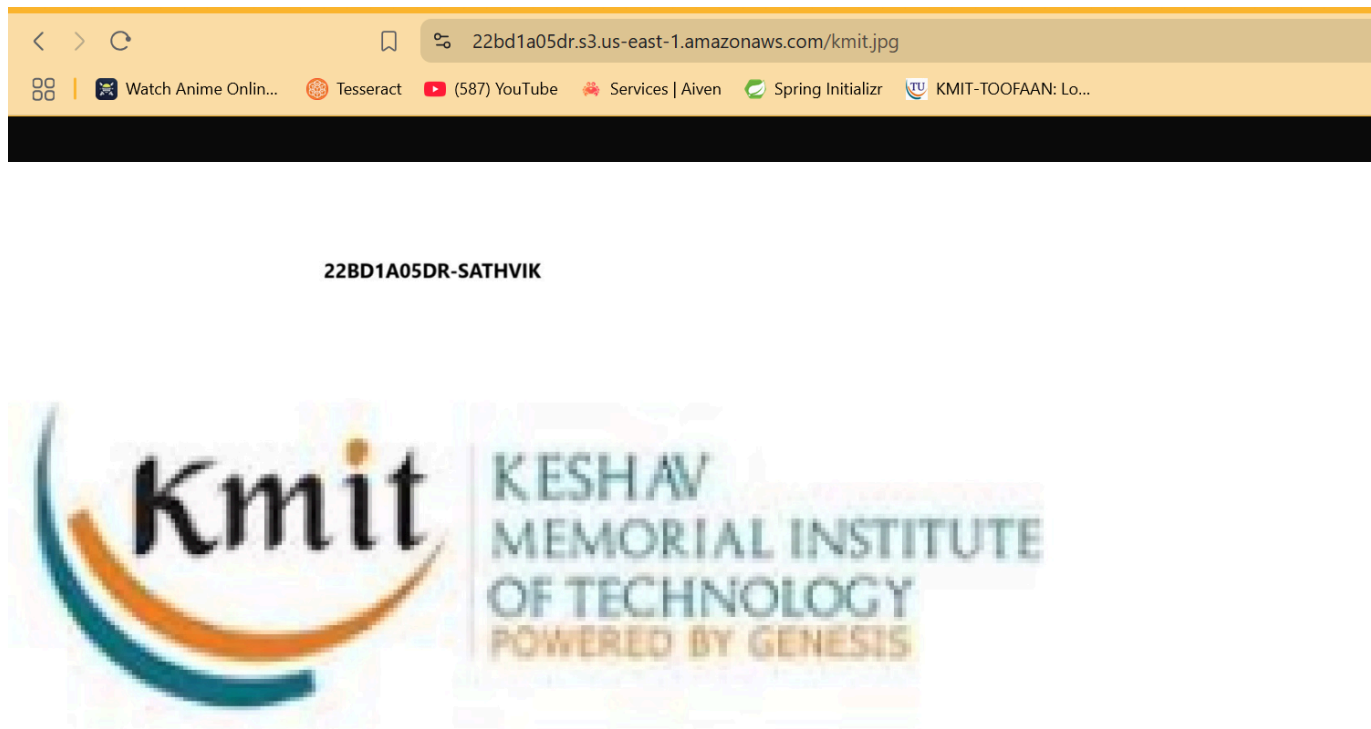
► Properties

Specify storage class, encryption settings, tags, and more.

[Cancel](#)

[Upload](#)

Step 11 : The image is ready to view as shown in the output



Step 12 : Upload 4 versions with the same name

22bd1a05dr Info

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

Objects (4)

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](#)

☒ Show versions < 1 > ⚙

<input type="checkbox"/>	Name	Type	Version ID	Last modified	Size	Storage class
<input type="checkbox"/>	kmit.jpg	jpg	nGZaOCqP_pXaSRuwFFeLE0z20xIZL_Gb	March 1, 2025, 11:16:17 (UTC+05:30)	318.6 KB	Standard
<input type="checkbox"/>	kmit.jpg	jpg	_WiiYw3kmNsmCogNXHlqW1ogVIDDAMkob	March 1, 2025, 11:10:31 (UTC+05:30)	151.5 KB	Standard
<input type="checkbox"/>	kmit.jpg	jpg	aCbzozo78y3JjNnRC7VKI3je1vfzUEv8	March 1, 2025, 11:01:27 (UTC+05:30)	148.1 KB	Standard
<input type="checkbox"/>	kmit.jpg	jpg	qp9TswKEpjbkoQyDoJqdWXcuAUwkgpbH	March 1, 2025, 10:56:08 (UTC+05:30)	151.7 KB	Standard

Step 13 : Give permission to the latest version image

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: 33e58d42e11a310847419af92f7a1c0f304401cd3a7f01b9289b b0387260c5ed	<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"/> <input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> <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

⚠ 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.☒ You must select the check box to continue.

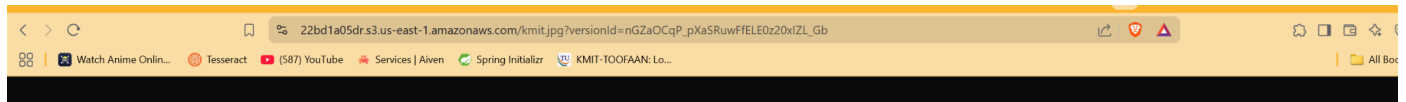
Access for other AWS accounts

No other AWS accounts associated with the resource.

[Add grantee](#)

Specified objects

Step 14 : Display the image in browser



22BD1A05DR-SATHVIK

