

**Project in AWS  
Practice Lab**

# **Creating Amazon S3 Buckets, Managing Objects, and Enabling Versioning**

**Andra-Diana Popescu**

**2025**

## **ABOUT THIS LAB**

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. In this lab, we will create two S3 buckets and verify public versus non-public access to the buckets. We will also enable and validate versioning based on uploaded objects.

## **LEARNING OBJECTIVES**

- Create a Public and Private Amazon S3 Bucket
- Enable Versioning on the Public Bucket and Validate Access to Different Versions of Files with the Same Name

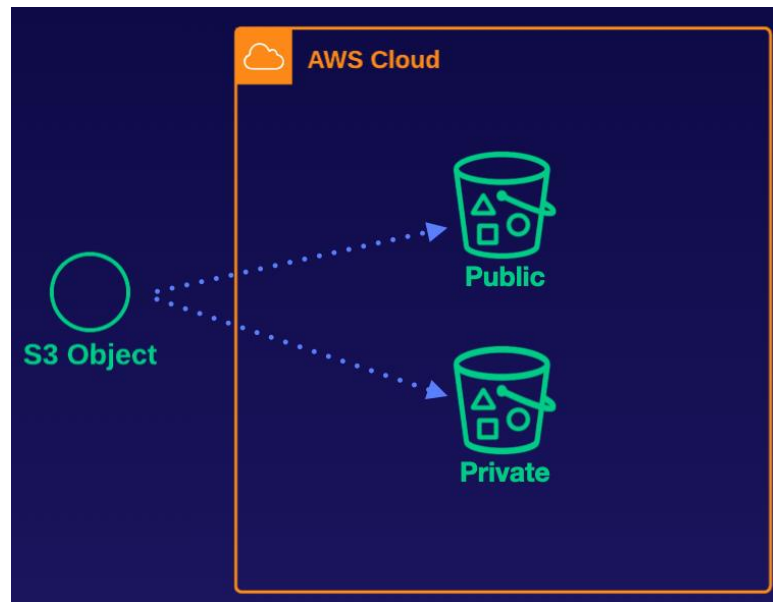
**AWS Documentation about S3:** [https://aws.amazon.com/s3/faqs/#Storage\\_Classes](https://aws.amazon.com/s3/faqs/#Storage_Classes)

**Source:** <https://learn.acloud.guru/course/certified-solutions-architect-associate/>

## Table of Contents

Lab Diagram .....	4
Log in to your AWS account .....	5
1. Create a Public S3 Bucket .....	5
1.1. Download the 2 files from GitHub .....	5
1.2. Create a Public S3 Bucket.....	6
1.3. Create a Private S3 Bucket.....	7
1.4. Upload a File in the Private Bucket .....	9
1.5. Upload a File in the Public Bucket .....	11
2. Enable Versioning on the Public Bucket and Validate Access to Different Versions of Files with the Same Name .....	13
2.1. Enable Versioning.....	13
2.2. Upload Another Image to Test Versioning .....	14
2.3. View the Image Versions .....	15

## Lab Diagram



We will begin by configuring an S3 bucket, managing objects, and enabling versioning. Our objective is to create a public and a private S3 bucket and evaluate results when the objects are accessed. We will also enable versioning and observe the effects of versioning on an S3 bucket. Use **us-east-1** for the all the lab activities.

Download the files needed for the lab here: <https://github.com/ACloudGuru-Resources/S3BucketsLabFiles> .

## Log in to your AWS account



Sign in as IAM user

Account ID (12 digits) or account alias

Type Account ID

IAM user name

Type IAM user name

Password

\*\*\*\*\*

☐ Remember this account

Sign in

Sign in using root user email

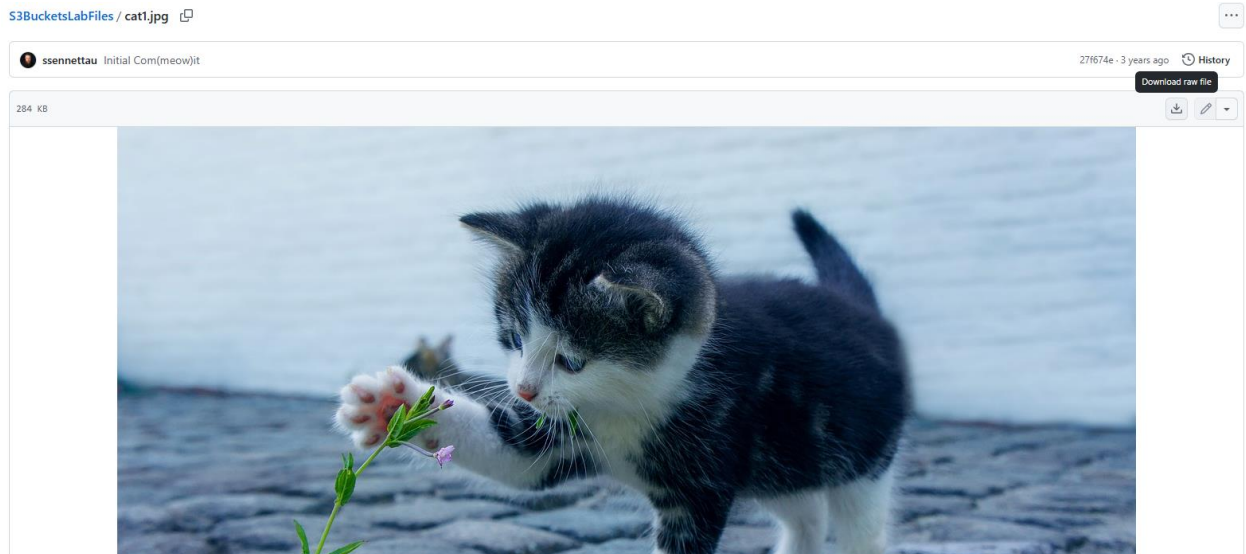
[Forgot password?](#)



## 1. Create a Public S3 Bucket

### 1.1. Download the 2 files from GitHub

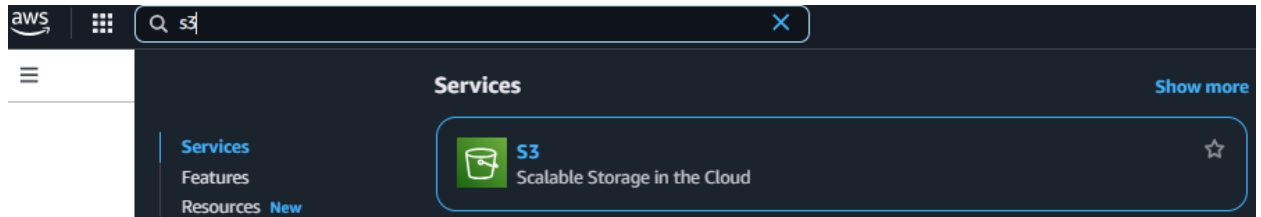
1. In a new browser tab, navigate to the GitHub repository for the files.
2. Download these 2 files (*cat1.jpg* and *cat2.jpg*) to the local machine so that we can upload them to S3.
3. Go to each file and click **Download raw file**.



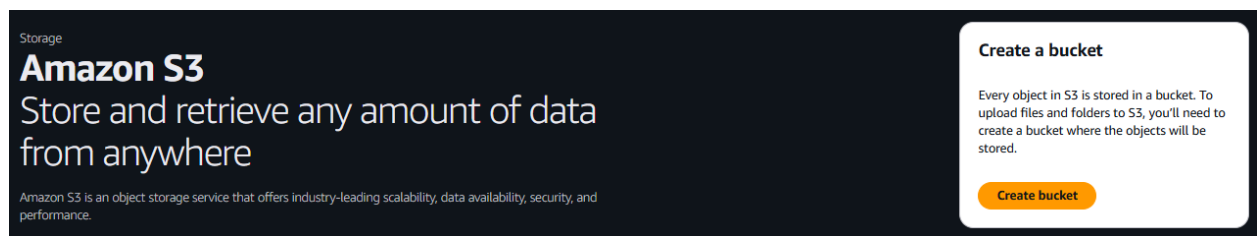
4. Repeat this for the *cat2.jpg* file.

## 1.2. Create a Public S3 Bucket

1. In the AWS Management Console, navigate to S3.



2. Click **Create bucket**.



3. Set Bucket name: **my-testlab-public-*<random numbers>*** with the AWS account ID or another series of numbers at the end to make it globally unique. Also, set the Region: US East (N. Virginia) us-east-1.

### 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.

##### Bucket name [Info](#)

my-testlab-public-12345

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or num

4. And at **Object Ownership**: Select **ACLs enabled**, and **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.



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](#)

5. In the **Block Public Access settings for this bucket** section, un-check Block all public access. Ensure all four permissions restrictions beneath it are also un-checked.
6. Check the box stating **I acknowledge that the current settings might result in this bucket and the objects within becoming public** to confirm that we understand the bucket is going to be public.

**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. Leave the rest of the settings as their defaults.
8. Click **Create bucket**.

**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

► **Advanced settings**

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#) [Create bucket](#)

## 1.3. Create a Private S3 Bucket

1. On the **Buckets** screen, click **Create bucket**.

☑ **Successfully created bucket "my-testlab-public-12345"**  
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

► **Account snapshot - updated every 24 hours** [All AWS Regions](#) [View Storage Lens dashboard](#)  
Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

**General purpose buckets** | Directory buckets

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

Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	IAM Access Analyzer	Creation date
<a href="#">my-testlab-public-12345</a>	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	April 5, 2025, 20:55:21 (UTC+03:00)

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

- Set Bucket name: *my-testlab-private-**<random numbers>*** with the AWS account ID or another series of numbers at the end to make it globally unique. Also, set the Region: US East (N. Virginia) us-east-1.

## 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.

#### Bucket name [Info](#)

my-testlab-private-12345

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or num

- Leave the rest of the settings as their defaults, including the public access, because this is going to be a private bucket. So, we really want to block all public access by default.

## 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.

##### ☒ 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.

- Click **Create bucket**.
- The buckets are created, so we need to upload some files to them.

✔ Successfully created bucket "my-testlab-private-12345"  
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

▶ Account snapshot - updated every 24 hours [All AWS Regions](#)  
Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

[View Storage Lens dashboard](#)

[General purpose buckets](#) | Directory buckets

### General purpose buckets (2) [Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

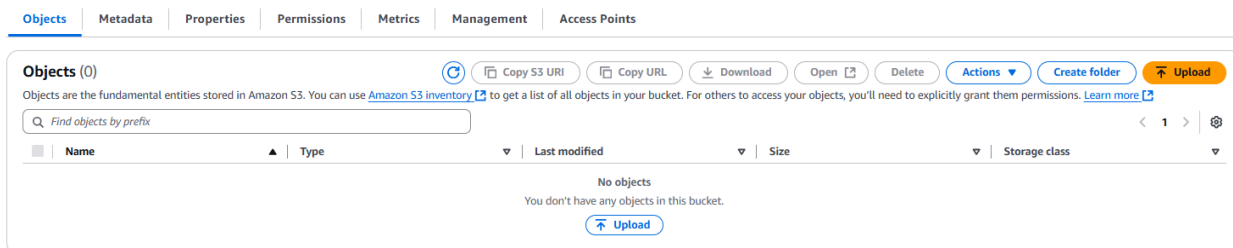
Find buckets by name

	Name	AWS Region	IAM Access Analyzer	Creation date
<input type="radio"/>	<a href="#">my-testlab-private-12345</a>	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	April 5, 2025, 21:04:17 (UTC+03:00)
<input type="radio"/>	<a href="#">my-testlab-public-12345</a>	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	April 5, 2025, 20:55:21 (UTC+03:00)

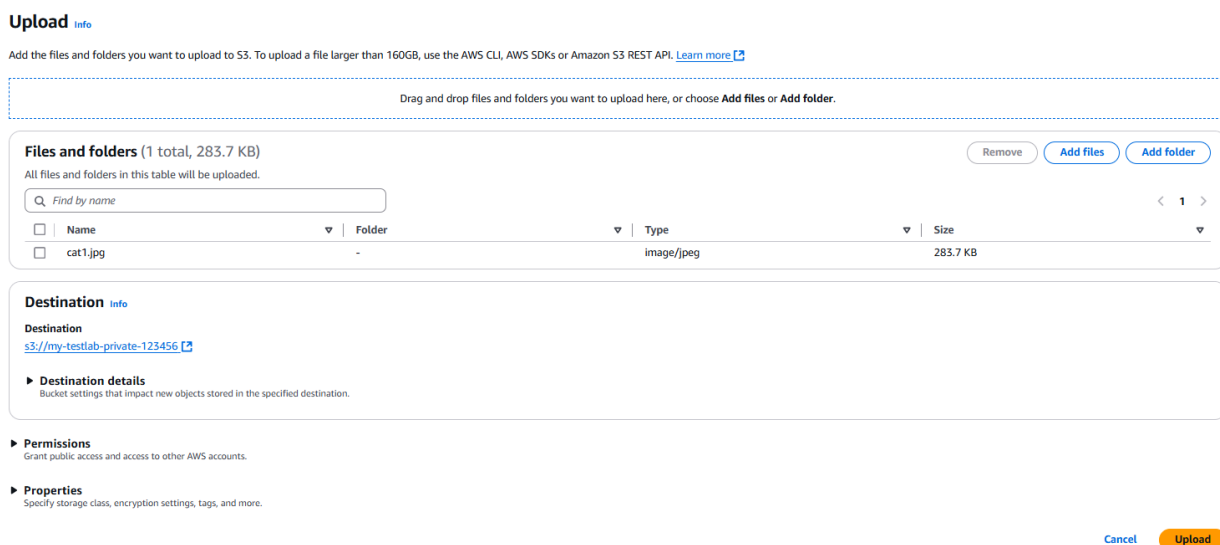


## 1.4. Upload a File in the Private Bucket

1. Select the private bucket name to open it.
2. In the **Objects** section, click **Upload**.



3. Click **Add files**.
4. Navigate to the files you downloaded for the lab and upload the *cat1.jpg* image.
5. Leave the rest of the settings on the page as their defaults.
6. Click **Upload**.



7. After the file uploads successfully, click its name to view its properties.

Upload succeeded  
For more information, see the [Files and folders](#) table.

### Upload: status

Close

After you navigate away from this page, the following information is no longer available.

#### Summary

Destination  
[s3://my-testlab-private-123456](#)

Succeeded  
1 file, 283.7 KB (100.00%)

Failed  
0 files, 0 B (0%)

[Files and folders](#) | [Configuration](#)

#### Files and folders (1 total, 283.7 KB)

Find by name							
Name	Folder	Type	Size	Status	Error		
<a href="#">cat1.jpg</a>	-	image/jpeg	283.7 KB	Succeeded	-		

8. Open the **Object URL** in a new browser tab. Since it's a private bucket, you'll see an error message. That's because this bucket doesn't allow public access.

[cat1.jpg](#) [Info](#) [Copy S3 URI](#) [Download](#) [Open](#) [Object actions](#)

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

#### Object overview

<b>Owner</b> lab+ Prod-6C	<b>S3 URI</b> <a href="#">s3://my-testlab-private-123456/cat1.jpg</a>
<b>AWS Region</b> US East (N. Virginia) us-east-1	<b>Amazon Resource Name (ARN)</b> <a href="#">arn:aws:s3::my-testlab-private-123456/cat1.jpg</a>
<b>Last modified</b> April 5, 2025, 23:19:52 (UTC+03:00)	<b>Entity tag (Etag)</b> 691 b6a22
<b>Size</b> 283.7 KB	<b>Object URL</b> <a href="#">https://my-testlab-private-123456.s3.us-east-1.amazonaws.com/cat1.jpg</a>
<b>Type</b> jpg	
<b>Key</b> <a href="#">cat1.jpg</a>	

[←](#) [→](#) [↺](#) [🔍](#) my-testlab-private-123456.s3.us-east-1.amazonaws.com/cat1.jpg

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>Q85...HK</RequestId>
  <HostId>puUZW6H1h...uUyEnDA2HmfNw=</HostId>
</Error>
```

9. Back on the *cat1.jpg* page, select the **Object actions** dropdown.

10. Note that the **Make public using ACL** option is grayed out, because the bucket is private, and we set the ownership to not use ACLs.

[cat1.jpg](#) [Info](#) [Copy S3 URI](#) [Download](#) [Open](#) [Object actions](#)

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

#### Object overview

<b>Owner</b> lab+ -Prod-6	<b>S3 URI</b> <a href="#">s3://my-testlab-private-123456/cat1.jpg</a>
<b>AWS Region</b> US East (N. Virginia) us-east-1	<b>Amazon Resource Name (ARN)</b> <a href="#">arn:aws:s3::my-testlab-private-123456/cat1.jpg</a>
<b>Last modified</b> April 5, 2025, 23:19:52 (UTC+03:00)	<b>Entity tag (Etag)</b> 691 22
<b>Size</b> 283.7 KB	<b>Object URL</b> <a href="#">https://my-testlab-private-123456.s3.us-east-1.amazonaws.com/cat1.jpg</a>
<b>Type</b> jpg	
<b>Key</b> <a href="#">cat1.jpg</a>	

Download as

Share with a presigned URL

Calculate total size

Copy

Move

Initiate restore

Query with S3 Select

Edit actions

Rename object

Edit storage class

Edit server-side encryption

Edit metadata

Edit tags

Make public using ACL

## 1.5. Upload a File in the Public Bucket

1. Click **Buckets** in the link trail at the top.
2. Select the **public** bucket name to open it.

General purpose buckets | Directory buckets

General purpose buckets (2) [info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

Find buckets by name

	Name	AWS Region	IAM Access Analyzer	Creation date
<input type="radio"/>	<a href="#">my-testlab-private-123456</a>	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	April 5, 2025, 23:15:44 (UTC+03:00)
<input type="radio"/>	<a href="#">my-testlab-public-123456</a>	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	April 5, 2025, 23:15:05 (UTC+03:00)

3. In the **Objects** section, click **Upload**.
4. Click **Add files**.
5. Navigate to the files you downloaded for the lab and upload the *cat1.jpg* image.
6. Leave the rest of the settings on the page as their defaults.
7. Click **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, 283.7 KB) [Remove](#) [Add files](#) [Add folder](#)

All files and folders in this table will be uploaded.

Find by name

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	cat1.jpg	-	image/jpeg	283.7 KB

**Destination** [info](#)

**Destination**  
[s3://my-testlab-public-123456](#)

**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](#)

8. After the file uploads successfully, click its name to view its properties.

**Upload succeeded**  
For more information, see the [Files and folders](#) table.

**Upload: status** [Close](#)

After you navigate away from this page, the following information is no longer available.

**Summary**

<b>Destination</b> <a href="#">s3://my-testlab-public-123456</a>	<b>Succeeded</b> 1 file, 283.7 KB (100.00%)	<b>Failed</b> 0 files, 0 B (0%)
---	--	------------------------------------

[Files and folders](#) | Configuration

**Files and folders** (1 total, 283.7 KB)

Find by name

Name	Folder	Type	Size	Status	Error
<a href="#">cat1.jpg</a>	-	image/jpeg	283.7 KB	Succeeded	-

- Open the **Object URL** in a new browser tab. You should receive an error message because although the bucket is public, the object is not.

cat1.jpg Info

Copy S3 URI Download Open Object actions

Properties Permissions Versions

**Object overview**

Owner: lab+ -Prod-6

AWS Region: US East (N. Virginia) us-east-1

Last modified: April 5, 2025, 23:31:22 (UTC+03:00)

Size: 283.7 KB

Type: jpg

Key: cat1.jpg

S3 URI: s3://my-testlab-public-123456/cat1.jpg

Amazon Resource Name (ARN): arn:aws:s3::my-testlab-public-123456/cat1.jpg

Entity tag (Etag): 691 a22

**Object URL**: https://my-testlab-public-123456.s3.us-east-1.amazonaws.com/cat1.jpg

← → ↺ my-testlab-public-123456.s3.us-east-1.amazonaws.com/cat1.jpg

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>ZDf...iH</RequestId>
  <HostId>qquh0/LMrv...6RvXtmBk=</HostId>
</Error>
```

- Back on the *cat1.jpg* page, select **Object actions** → **Make public using ACL**.

cat1.jpg Info

Copy S3 URI Download Open Object actions

Properties Permissions Versions

**Object overview**

Owner: lab+ -Prod-60

AWS Region: US East (N. Virginia) us-east-1

Last modified: April 5, 2025, 23:31:22 (UTC+03:00)

Size: 283.7 KB

Type: jpg

Key: cat1.jpg

S3 URI: s3://my-testlab-public-123456/cat1.jpg

Amazon Resource Name (ARN): arn:aws:s3::my-testlab-public-123456/cat1.jpg

Entity tag (Etag): 691 b6a22

Object URL: https://my-testlab-public-123456.s3.us-east-1.amazonaws.com/cat1.jpg

Object actions menu:

- Download as
- Share with a presigned URL
- Calculate total size
- Copy
- Move
- Initiate restore
- Query with S3 Select
- Edit actions
  - Rename object
  - Edit storage class
  - Edit server-side encryption
- Edit metadata
- Edit tags
- Make public using ACL**

- Click **Make public**.

**Make public** Info

The make public action enables public read access in the object access control list (ACL) settings. [Learn more](#)

⚠ When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.

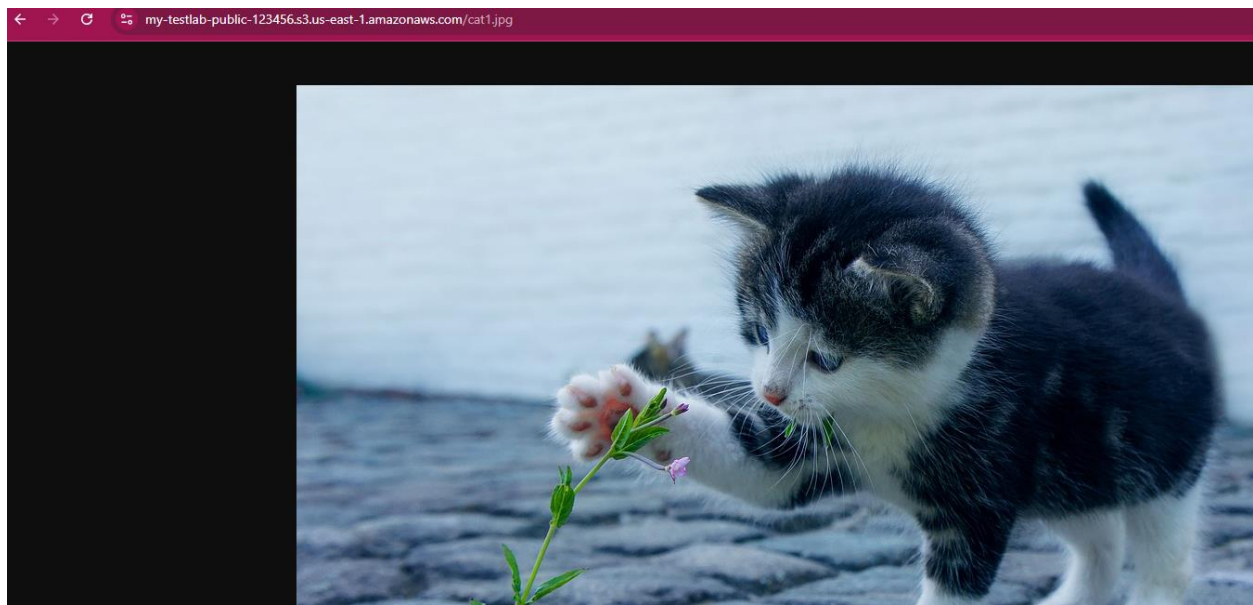
**Specified objects**

Find objects by name

Name	Type	Last modified	Size
cat1.jpg	jpg	April 5, 2025, 23:31:22 (UTC+03:00)	283.7 KB

Cancel Make public

- Open the **Object URL** in a new browser tab again. This time, the image should load.



## 2. Enable Versioning on the Public Bucket and Validate Access to Different Versions of Files with the Same Name

### 2.1. Enable Versioning

1. Back on the public bucket page, click the **Properties** tab.
2. In the **Bucket Versioning** section, click **Edit**.

my-testlab-public-123456 [Info](#)

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

---

**Bucket overview**

<b>AWS Region</b> US East (N. Virginia) us-east-1	<b>Amazon Resource Name (ARN)</b> <a href="#">arn:aws:s3:::my-testlab-public-123456</a>	<b>Creation date</b> April 5, 2025, 23:15:05 (UTC+03:00)
--	--	---

---

**Bucket Versioning** [Edit](#)

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**  
Disabled

3. Click **Enable** to enable bucket versioning.
4. Click **Save changes**.

## Edit Bucket Versioning [Info](#)

### 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

☐ Suspend

This suspends the creation of object versions for all operations but preserves any existing object versions.

☒ Enable

After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.

#### Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

[Cancel](#)

[Save changes](#)

## 2.2. Upload Another Image to Test Versioning

1. Click the **Objects** tab.
2. Click **Upload**, and then click **Add files**.

my-testlab-public-123456 [Info](#)

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

### Objects (1)

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](#)

Find objects by prefix

☐ Show versions

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	cat1.jpg	jpg	April 5, 2025, 23:31:22 (UTC+03:00)	283.7 KB	Standard

3. Rename *cat2.jpg* to *cat1.jpg* (this way, you'll upload a different image than the original *cat1.jpg* image).
4. Upload the newly renamed *cat1.jpg* image.
5. Click **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, 99.0 KB)

All files and folders in this table will be uploaded.

Find by name

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	cat1.jpg	-	image/jpeg	99.0 KB

### Destination [Info](#)

#### Destination

[s3://my-testlab-public-123456](#)

#### 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](#)

6. After the file uploads successfully, click its name to view its properties.

**Upload succeeded**  
For more information, see the Files and folders table.

**Upload: status** Close

After you navigate away from this page, the following information is no longer available.

**Summary**

<b>Destination</b> s3://my-testlab-public-123456	<b>Succeeded</b> 1 file, 99.0 KB (100.00%)	<b>Failed</b> 0 files, 0 B (0%)
---	---	------------------------------------

**Files and folders** | Configuration

**Files and folders** (1 total, 99.0 KB)

Find by name

Name	Folder	Type	Size	Status	Error
<a href="#">cat1.jpg</a>	-	image/jpeg	99.0 KB	Succeeded	-

7. Click the **Versions** tab. You should see there are two versions of the *cat1.jpg* file.

**cat1.jpg** Info Copy S3 URI Download Open Object actions

**Properties** | **Permissions** | **Versions**

**Versions** (2) Download Open Delete Actions

<input type="checkbox"/>	Version ID	Type	Last modified	Size	Storage class
<input type="checkbox"/>	5OIKBy3g1bxEf8aJr.DD6DcE4znHE3.a (Current version)	jpg	April 6, 2025, 00:00:18 (UTC+03:00)	99.0 KB	Standard
<input type="checkbox"/>	<a href="#">null</a>	jpg	April 5, 2025, 23:58:34 (UTC+03:00)	283.7 KB	Standard

8. Before, we were able to access this file publicly. Now, we have to make it public again.

9. The reason: even though it has the same name, this is effectively a new object.

## 2.3. View the Image Versions

1. Select **Object actions** → **Make public using ACL**.

**cat1.jpg** Info Copy S3 URI Download Open Object actions

**Properties** | **Permissions** | **Versions**

**Versions** (2) Download Open Delete

<input type="checkbox"/>	Version ID	Type	Last modified	Size	Storage class
<input type="checkbox"/>	5OIKBy3g1bxEf8aJr.DD6DcE4znHE3.a (Current version)	jpg	April 6, 2025, 00:00:18 (UTC+03:00)	99.0 KB	Standard
<input type="checkbox"/>	<a href="#">null</a>	jpg	April 5, 2025, 23:58:34 (UTC+03:00)	283.7 KB	Standard

- Download as
- Share with a presigned URL
- Calculate total size
- Copy
- Move
- Initiate restore
- Query with S3 Select
- Edit actions
- Rename object
- Edit storage class
- Edit server-side encryption
- Edit metadata
- Edit tags
- Make public using ACL**

2. Click **Make public**.

### Make public [Info](#)

The make public action enables public read access in the object access control list (ACL) settings. [Learn more](#)

When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.

#### Specified objects

Find objects by name

Name	Type	Last modified	Size
 <a href="#">cat1.jpg</a>	jpg	April 6, 2025, 00:00:18 (UTC+03:00)	99.0 KB

[Cancel](#) [Make public](#)

3. Click the **Properties** tab.

4. Open the **Object URL** in a new browser tab. This time, you should see the new image.

### cat1.jpg [Info](#)

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

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

#### Object overview

Owner  
lab+ :-Prod-

AWS Region  
US East (N. Virginia) us-east-1


Last modified  
April 6, 2025, 00:00:18 (UTC+03:00)

Size  
99.0 KB


Type  
jpg

Key  
 cat1.jpg

#### S3 URI

 s3://my-testlab-public-12345/cat1.jpg

#### Amazon Resource Name (ARN)

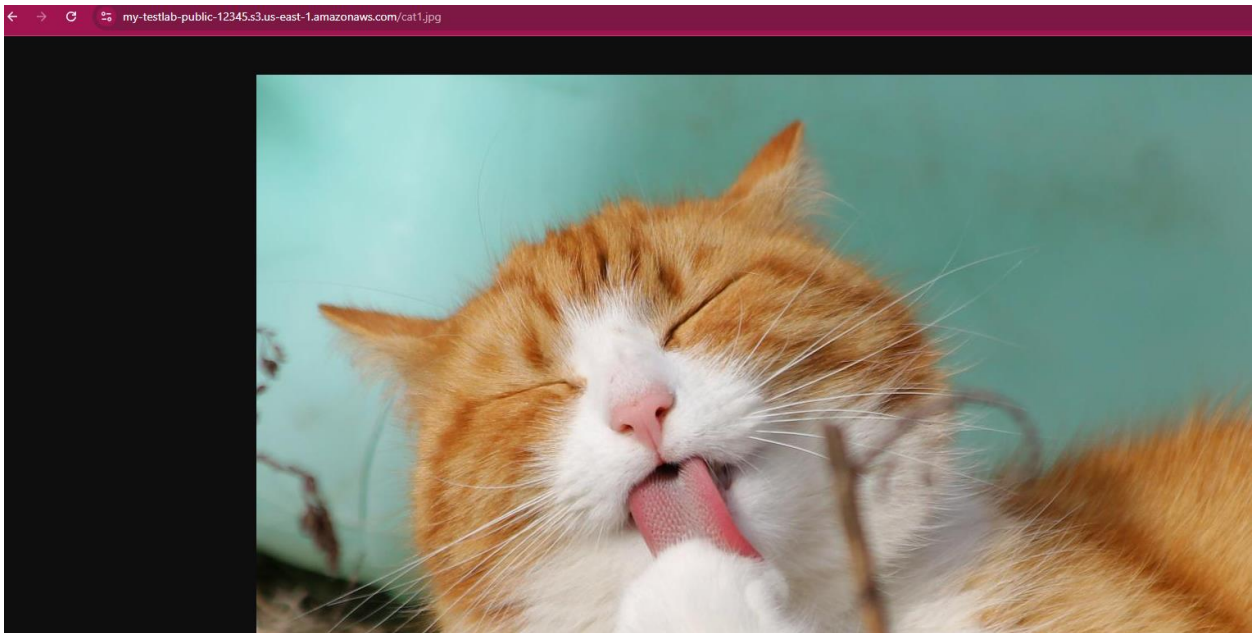
 arn:aws:s3::my-testlab-public-12345/cat1.jpg

#### Entity tag (Etag)

 448 i756

#### Object URL

 <https://my-testlab-public-12345.s3.us-east-1.amazonaws.com/cat1.jpg>



5. But the important part about versioning is that we can also see our previous file versions.

6. Back on the **cat1.jpg** page, click the **Versions** tab.

7. Click the **null** object.



cat1.jpg [Info](#)

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

Properties Permissions **Versions**

Versions (2) [Download](#) [Open](#) [Delete](#) [Actions](#)

<input type="checkbox"/>	Version ID	Type	Last modified	Size	Storage class
<input type="checkbox"/>	50IKBy3g1bxEF8aJr-DD6DcE4znHE3.a (Current version)	jpg	April 6, 2025, 00:00:18 (UTC+03:00)	99.0 KB	Standard
<input type="checkbox"/>	<b>Ⓛ null</b>	jpg	April 5, 2025, 23:58:34 (UTC+03:00)	283.7 KB	Standard

8. Open its **Object URL** in a new browser tab. Also, notice that it has a *version ID=null* at the end.

cat1.jpg [Info](#)

Version ID: [Ⓛ null](#) [Copy S3 URI](#) [Download](#) [Open](#) [Object actions](#)

Properties Permissions Versions

**Object overview**

**Owner**  
lab+ -Prod-

**AWS Region**  
US East (N. Virginia) us-east-1

**Last modified**  
April 5, 2025, 23:58:34 (UTC+03:00)

**Size**  
283.7 KB

**Type**  
jpg

**Key**  
[Ⓛ cat1.jpg](#)

**S3 URI**  
[Ⓛ s3://my-testlab-public-12345/cat1.jpg](#)

**Amazon Resource Name (ARN)**  
[Ⓛ arn:aws:s3::my-testlab-public-12345/cat1.jpg](#)

**Entity tag (Etag)**  
[Ⓛ 65](#) 22

**Object URL**  
[Ⓛ https://my-testlab-public-12345.s3.us-east-1.amazonaws.com/cat1.jpg?versionId=null](#)

9. You should see the original *cat1.jpg* image you uploaded. So, we're still able to keep the original version of the file.

