

AWS S3 Part II

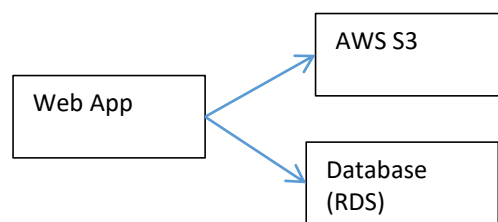
S3 ----> Simple Storage Service part 2 || Identity and Access Management (IAM)

S3 is a scalable storage service in AWS cloud, which supports unlimited storage and works on Object based storage (files like audio, video, image, txt file etc)

We create buckets to store data and every bucket should have unique name

By default, all the buckets and objects are private however, we can make them public as well

Advantages ----> unlimited storage, scalability, availability, security, backup ----> all taken care by AWS only



Web App stores data in the form of rows and columns in RDS. However, we have the option of storing data in S3 also but works based on objects not limited to data type or file extensions

----> Based on needs, we can create multiple buckets in S3

----> S3 is a global service where in buckets are regional, we could specify multiple regions also, but mostly regional specific only

Static Website Hosting using S3:

So far, we have used only VMs to host static website using httpd

Can we host website without VMs? About Static and Dynamic website we discussed earlier

For example, before we login into Udemy or any website it is a static website because everyone has the same data. After we login it changes

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

⚠ 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 ACL 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](#)

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 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 for 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.

☐ **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 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 is granted 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 to block 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.

☐ 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 already grant public access.

☐ 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.

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 objects deleted by users or applications, and to protect against unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☒ Disable

☐ Enable

Create bucket ---> Properties ---> S3 static website hosting

Disabled

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](#)

Object Lock

Disabled

Edit

Requester pays

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)


Requester pays

Disabled

Edit

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

 We recommend using AWS Amplify Hosting for static website hosting

Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. [Learn more about Amplify Hosting](#) or [View your existing Amplify apps](#)

Create Amplify app

S3 static website hosting

Disabled

Edit

Click Edit
Make it 'Enable'

Edit static website hosting [info](#)

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

- ☐ Disable
- ☒ Enable

Hosting type

- ☒ Host a static website
Use the bucket endpoint as the web address. [Learn more](#)
- ☐ Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings. [Public Access](#)

Index document

Specify the home or default page of the website.

index.html

Error document - optional

This is returned when an error occurs.

error.html

Redirection rules - optional

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

I create two html files and I upload into S3

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 file**

Files and folders (2 total, 87.0 B)

All files and folders in this table will be uploaded.

Find by name

<input type="checkbox"/>	Name	Folder	Type
<input type="checkbox"/>	error.html	-	text/html
<input type="checkbox"/>	index.html	-	text/html

Destination [info](#)

Destination

s3://devopsbucket432

After uploading files, edit Static Website Hosting

Edit static website hosting [Info](#)

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

- ☐ Disable
- ☒ Enable

Hosting type

- ☒ Host a static website
Use the bucket endpoint as the web address. [Learn more](#)
- ☐ Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

i For your customers to access content at the website endpoint, you must make all your content publicly accessible. [Public Access](#)

Index document

Specify the home or default page of the website.

index.html

Error document - optional

This is returned when an error occurs.

error.html

Redirection rules - optional

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

Go to Permissions ---> Access Control List (ACL) --> this doesn't work

Access control list (ACL) [Edit](#)

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

i The console displays combined access grants for duplicate grantees. To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: ec4a35908cf2521684b9fdb987aa35d6ac1c5c5bd07db486a7cc7d49a2a1bdc7	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	-	-

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: ec4a35908cf2521684b9fdb987aa35d6ac1c5c5bd07db486a7cc7d49a2a1bdc7	<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"/> <input checked="" type="checkbox"/> List <input type="checkbox"/> Write	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> Read <input type="checkbox"/> Write

IMPORTANT

Before you click Upload, add files then go to Permissions

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

Files and folders (2 total, 87.0 B)
All files and folders in this table will be uploaded.

☒

Name

▼

☒

error.html

-

text/html

46.0 B

☒

index.html

-

text/html

41.0 B

Destination Info

Destination
[s3://devopsbucket543](#)

► 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

Select Grant public-read access

▼ Permissions

Grant public access and access to other AWS accounts.

Access control list (ACL)

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

i AWS recommends using S3 bucket policies or IAM policies for access control. [Learn more](#)

Access control list (ACL)

- ☒ Choose from predefined ACLs
☐ Specify individual ACL permissions

Predefined ACLs

- ☐ Private (recommended)
Only the object owner will have read and write access.
- ☒ Grant public-read access
Anyone in the world will be able to access the specified objects. The object owner will have read and write access. [Learn more](#)

⚠ Granting public-read access is not recommended
Anyone in the world will be able to access the specified objects. [Learn more](#)

☐ I understand the risk of granting public-read access to the specified objects.

Then Click Upload

Now go to Static Website Hosting

Edit static website hosting [Info](#)

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

- ☐ Disable
- ☒ Enable

Hosting type

- ☒ Host a static website
Use the bucket endpoint as the web address. [Learn more](#)
- ☐ Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

i For your customers to access content at the website endpoint, you must make all your content publicly [Public Access](#)

Index document

Specify the home or default page of the website.

index.html

Error document - optional

This is returned when an error occurs.

error.html

Redirection rules – optional

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

Click Save changes

Scroll down after making changes to see Bucket website endpoint

Requester pays

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

Requester pays
Disabled

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

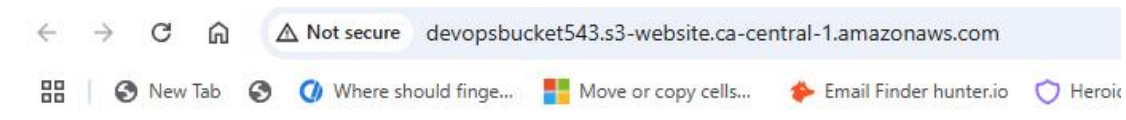
i We recommend using **AWS Amplify Hosting** for static website hosting
Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. [Learn more about Amplify Hosting](#) or [View your existing website](#)

S3 static website hosting
Enabled

Hosting type
Bucket hosting

Bucket website endpoint
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)
<http://devopsbucket543.s3-website-ca-central-1.amazonaws.com>

Click that link:



Welcome to HTML

Can we host a Static website on Amazon without creating any VMs? Answer is Yes

Delete all buckets and empty contents

There is something called as 1. Versioning, 2. Locking, 3. Transfer Acceleration, 4. Storage classes in S3

Create new S3 bucket ---> upload alien.txt
While uploading Grant public-read access

▼ Permissions
Grant public access and access to other AWS accounts.

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

○ AWS recommends using S3 bucket policies or IAM policies for access control. [Learn more](#)

Access control list (ACL)
☒ Choose from predefined ACLs
☐ Specify individual ACL permissions

Predefined ACLs
☐ Private (recommended)
Only the object owner will have read and write access.
☒ Grant public-read access
Anyone in the world will be able to access the specified objects. The object owner will have read and write access. [Learn more](#)

⚠ **Granting public-read access is not recommended**
Anyone in the world will be able to access the specified objects. [Learn more](#)
☒ I understand the risk of granting public-read access to the specified objects.

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

Cancel Upload

File is uploaded

Find objects by prefix			
<input type="checkbox"/>	Name	Type	Last modified
<input type="checkbox"/>	alien.txt	txt	March 16, 2025, 16:45:16 (UTC-04:00)

Mar 16 2025, 16:45:16

Again Upload --> Add file ---> go to the same folder and select alien.txt

I open alien.txt then I make changes in that file

<input type="checkbox"/>	Name	Type	Last modified
<input type="checkbox"/>	alien.txt	txt	March 16, 2025, 16:48:00 (UTC-04:00)

I again upload ---> Mar 16, 2025 16:48:00

Currently it is only replacing the existing file

The solution is Versioning, if you don't want anyone to modify or replace then we go with Locking

If you want to upload huge file very fast, then go for 'Transfer Acceleration'

If you want to frequently access or download files from S3 unlimited storage, then go for 'Storage classes'. Based on the access frequency, we can decide which storage class to use

Again I try to upload the same file --> go to Properties ---> Storage class

▼ Properties

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

Storage class

Info

Amazon S3 offers a range of storage classes designed for different use cases. [Learn more](#) or see [Amazon S3 pricing](#)

Storage class	Designed for	Bucket type	Availability Zones	Min storage duration	Min billable object size	Monitoring and auto-tiering fees	Retrieval fees
<input checked="" type="radio"/> Standard	Frequently accessed data (more than once a month) with milliseconds access	General purpose	≥ 3	-	-	-	-
<input type="radio"/> Intelligent-Tiering	Data with changing or unknown access patterns	General purpose	≥ 3	-	-	Per-object fees apply for objects >= 128 KB	-
<input type="radio"/> Standard-IA	Infrequently accessed data (once a month) with milliseconds access	General purpose	≥ 3	30 days	128 KB	-	Per-GB fees apply
<input type="radio"/> One Zone-IA	Recreateable, infrequently accessed data (once a month) with milliseconds access	General purpose or directory	1	30 days	128 KB	-	Per-GB fees apply

99.999 security, availability, backup guarantee is there

Click bucket name ---> Properties ---> Bucket versioning

devops-test-654

Info

Objects

Properties

Permissions

Metrics

Management


Access Points

Bucket overview

AWS Region

Canada (Central) ca-central-1

Amazon Resource Name (ARN)

 arn:aws:s3:::devops-test-654

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

Disabled

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting objects

Disabled

Edit then Enable

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 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 object

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting objects. Disabled

I click the file then Versions

alien.txt [Info](#)

Properties Permissions Versions

Versions (3)

<input type="checkbox"/>	Version ID	Type	Last modified	Size
<input type="checkbox"/>	NP6tGk2W6PSgZw8fDkasZkV8D4Xx... (Current version)	txt	March 16, 2025, 18:21:48 (UTC-04:00)	
<input type="checkbox"/>	mAEg38INXIGcmsLuGApUolZwJbj...	txt	March 16, 2025, 18:19:50 (UTC-04:00)	
<input type="checkbox"/>	null	txt	March 16, 2025, 16:48:00 (UTC-04:00)	

Click on 'Show versions'

Objects (5)

☐ Copy S3 URI ☐ Copy URL Download Upload

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 can use [Access control](#).

☒ Show versions

<input type="checkbox"/>	Name	Type	Version ID	Last modified
<input type="checkbox"/>	alien.txt	txt	NP6tGk2W6PSgZw8fDkasZkV8D4Xxv28T	March 16, 2025, 18:21:48 (UTC-04:00)
<input type="checkbox"/>	alien.txt	txt	mAEg38INXIGcmsLuGApUolZwJbjmmdlf	March 16, 2025, 18:19:50 (UTC-04:00)
<input type="checkbox"/>	alien.txt	txt	null	March 16, 2025, 16:48:00 (UTC-04:00)

Versioning: It is used to maintain multiple variants of the same file. By default, Versioning is disabled for S3 bucket. However, we can enable in properties ---> Bucket versioning--enable
Since by default Versioning is disabled whenever we add new same file again in bucket, it will replace or overwrite the old one and if you don't want to replace old objects with new objects from bucket, then go with Versioning

Note: Once Versioning is enabled then we cannot disable but we can suspend it

S3 Storage classes:

Used to specify how frequently you can/want to access the objects from S3

We have multiple Storage classes in S3

Write Once Read Many times ----> Object locking

Same in the Bucket Properties we see

The screenshot shows the 'Properties' tab for an Amazon S3 bucket named 'devops-test-654'. It features three main sections: 'Send notifications to Amazon EventBridge for all events in this bucket' (Off), 'Transfer acceleration' (Disabled), and 'Object Lock' (Disabled). Each section includes a brief description of the feature.

[S3](#) > [Buckets](#) > devops-test-654

Send notifications to Amazon EventBridge for all events in this bucket
Off

Transfer acceleration
Use an accelerated endpoint for faster data transfers. [Learn more](#)

Transfer acceleration
Disabled

Object Lock
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten

Object Lock
Disabled

Transfer Acceleration:

Speed up data transfer process in S3 bucket

Amazon S3 Transfer Acceleration is a bucket-level feature that enables fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. Transfer Acceleration is designed to optimize transfer speeds from across the world into S3 bucket

Look into Multi-region access point