

Assignment-6

Problem Statement: Upload a static website on S3

The steps to do the above mentioned process are:

1. We need to create a public bucket first. So we go to s3 create bucket.

2. There we put the bucket name and click on ACLs enabled.

The screenshot shows the 'Create bucket' page in the AWS Management Console. The page is titled 'Create bucket' and includes a sub-header 'Buckets are containers for data stored in S3.' The main configuration section is divided into two parts: 'General configuration' and 'Object Ownership'.

General configuration

- AWS Region:** Asia Pacific (Mumbai) ap-south-1
- Bucket type:** ☒ 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:** tamoghrabucket120 (The text below the input field states: 'Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming.') A 'Choose bucket' button is visible below the input field.
- Copy settings from existing bucket - optional:** (Once the bucket settings in the following configuration are copied.)

Object Ownership

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 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. The object writer remains the object owner.)
- ☐ 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

3. Then we uncheck the Block all public access.

Amazon S3 > Buckets > Create bucket

If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control 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 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.

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](#)

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

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 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

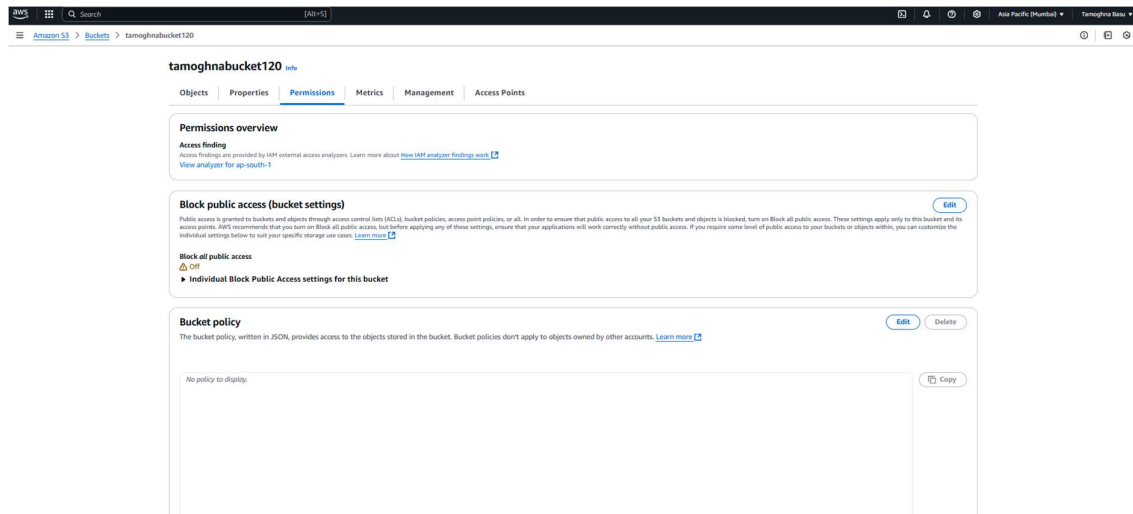
☒ Enable

Advanced settings

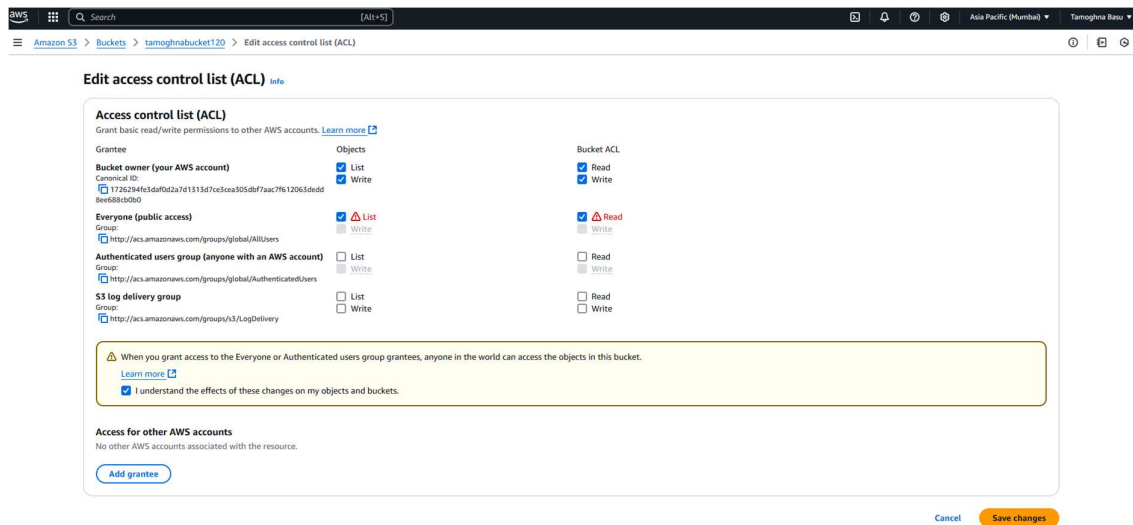
After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

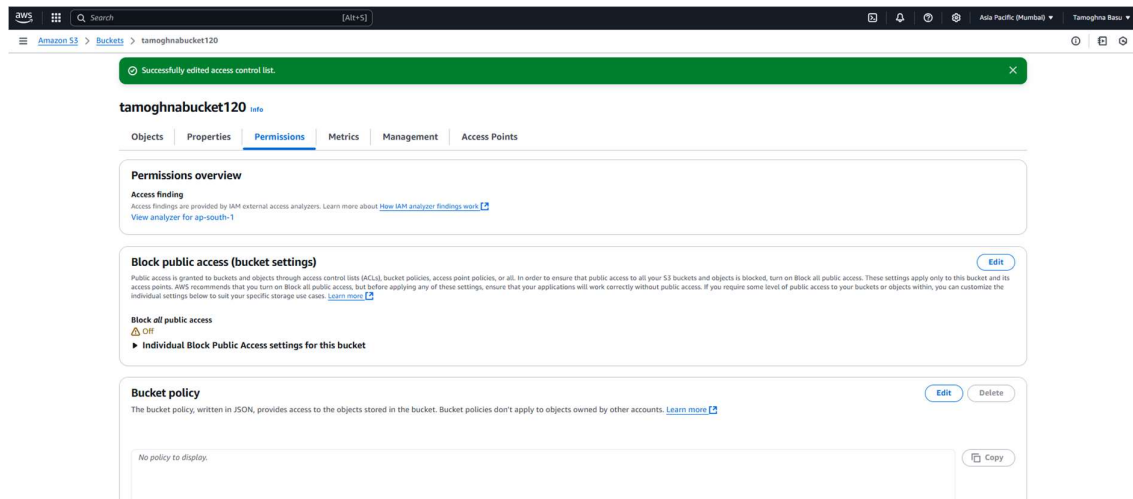
[Cancel](#) [Create bucket](#)

4. After that we click on create. By this new public bucket is created.



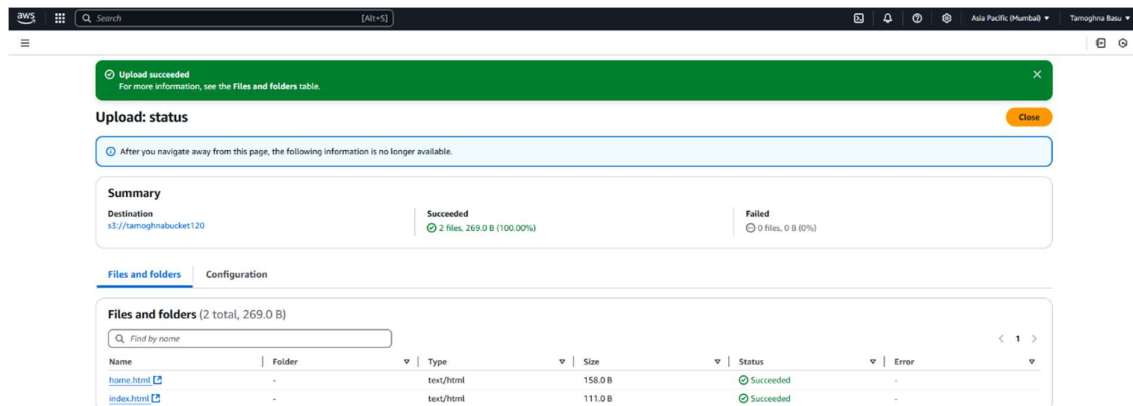
5.Next we change the permission of the bucket for public access to everyone.





6.After this we add the files(.html files) into the bucket for the website.

7.After click on the upload all files are uploaded.



tamoghnabucket120 [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](#)

Block public access (bucket settings) [Edit](#)

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
Off
► Individual Block Public Access settings for this bucket

Bucket policy [Edit](#) [Delete](#)

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

No policy to display. [Copy](#)

tamoghnabucket120 [info](#)

Objects **Properties** Permissions Metrics Management Access Points

Bucket overview

AWS Region: Asia Pacific (Mumbai) ap-south-1
Amazon Resource Name (ARN): [arn:aws:s3::tamoghnabucket120](#)
Creation date: February 16, 2025, 14:10:45 (UTC+05:30)

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

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

Tags (0) [Edit](#)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

Key	Value
No tags associated with this resource.	

Default encryption [info](#) [Edit](#)

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)

Bucket Key
When S3-KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)
Enabled

8. Then we enable the static website hosting. And put the name of the index file on the index document block.

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 for the bucket. For more information, see [Using Amazon S3 Block Public Access](#)

Index document
Specify the home or default page of the website.

Error document - optional
This is returned when an error occurs.

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

1

9. By this a static website is hosted on aws server and the link of static website is also created.

Successfully edited static website hosting.

tamoghnabucket120 [info](#)

Objects **Properties** Permissions Metrics Management Access Points

Bucket overview

AWS Region Asia Pacific (Mumbai) ap-south-1	Amazon Resource Name (ARN) arn:aws:s3::tamoghnabucket120	Creation date February 16, 2025, 14:10:45 (UTC+05:30)
---	--	---

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

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](#)

Multi-factor authentication (MFA) delete
Disabled

Tags (0) [Edit](#)
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

Key	Value
No tags associated with this resource.	

Default encryption [info](#) [Edit](#)
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)

Object Lock [Edit](#)
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

Requester pays [Edit](#)
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 [info](#) [Edit](#)
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
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://tamoghnabucket120.s3-website-ap-south-1.amazonaws.com/>