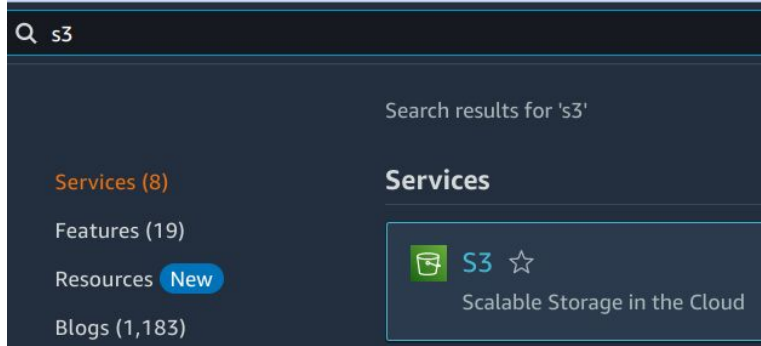


Hosting Static Website in S3

Storage based lab

After completing this lab we will be able to

1. Create a bucket in Amazon S3
2. Upload content to your bucket
3. Enable access to the bucket objects
4. Update the website



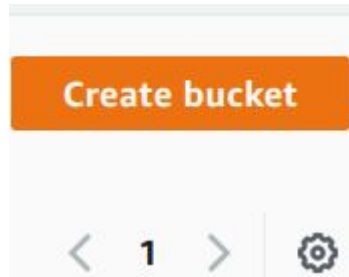
Task 1:

Amazon S3

Buckets

1: Choose for the S3 service in console

2: Choose **Buckets** option



3: Click on **Create Bucket**

Task 2: Fill every data needed to create bucket in **create bucket** section

1. Enter bucket name (name must be unique globally).
2. Select region.
3. Object ownership: ACL enabled and bucket owner preferred.
4. Public Access setting for bucket.
5. Bucket versioning.
6. Tags (optional).
7. Default encryption.
8. Finally, click on **create bucket**.

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#) 

General configuration

Bucket name

Static-Website-Bucket-Mukesh

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#) 

AWS Region

Asia Pacific (Mumbai) ap-south-1



Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

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

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.



Enabling ACLs turns off the bucket owner enforced setting for Object Ownership

Once the bucket owner enforced setting is turned off, access control lists (ACLs) and their associated permissions are restored. Access to objects that you do not own will be based on ACLs and not the bucket policy.



I acknowledge that ACLs will be restored.

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 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 (2) - optional

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

Key

Value - optional

Owner

Mukesh

Remove

Environment

Intern-Test

Remove

Add tag

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption key type [Info](#)

Environment

Intern-Test

Remove

Add tag

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption key type [Info](#)

- ☒ Amazon S3 managed keys (SSE-S3)
- ☐ AWS Key Management Service key (SSE-KMS)

Bucket Key

When 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](#) 

- ☐ 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

Amazon S3 > Buckets > static-website-bucket-mukesh

static-website-bucket-mukesh [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:::static-website-bucket-mukesh

Creation date

March 22, 2023, 13:49:20 (UTC+05:45)

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 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.

`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](#)

Task 3: Working in bucket

1. Select properties tab.
2. Scroll down to static website hosting.
3. Then perform following task:

Configure the following settings:

- Static web hosting: Enable
- Hosting type: Host a static website
- Index document: `index.html`
 - **Note:** You must enter this value, even though it is already displayed.
- Error document: `error.html`

Choose **Save changes**

Task 4: Uploading content to bucket

1. Select objects tab.
2. Click in the upload option.
3. Browse the website files from local device and upload them.

Note:

We can also update the data that is uploaded in the bucket in the local device and re-upload the data in cloud after updating it.
For eg: we can update “index.html” file and the re-upload it.

Task 5: Enabling access to the objects

Objects stored in S3 are private by default which ensures the security of the data. In this lab we will make the objects publicly accessible.

There are two ways to make S3 objects public:

1. Make whole bucket public or some directory in bucket public using a bucket policy.
2. Make individual objects public using ACL.

Steps:

1. Select the uploaded objects.
2. Choose make public via ACL from actions tab.
3. Choose make public.

Task 6: We can now access the website using link from static website hosting option from properties tab



Demo of the static website