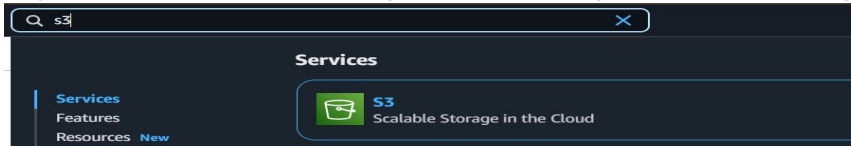
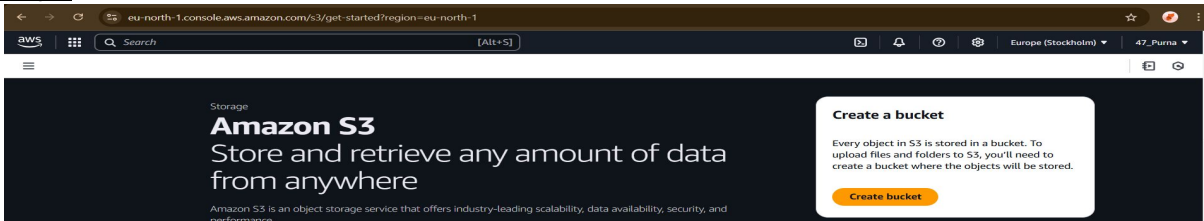


ASSIGNMENT 6 :- Upload a static website in s3.

Step 1 :- To create a s3 bucket , Log in to **AWS Management Console**. Navigate to **S3** (Simple Storage Service).



Step 2 :- Click **Create bucket**.



Step 3 :- Enter a **Bucket name** (must be unique across AWS).

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region
Europe (Stockholm) eu-north-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 faster processing of data within a single Availability Zone.

Bucket name [Info](#)
mckviepkbucket

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 :- Click **Object Ownership** as “ACLs enabled”. Uncheck **Block all public access** (so your website can be accessed). And Confirm the **acknowledgement** .

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](#)

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.

Step 5 :- Click **Create bucket**.

► **Advanced settings**

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

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

Step 6 :- To upload Website Files, Open newly created s3 bucket and go to the **Objects** tab.

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

[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
<input type="radio"/> mckviepkbucket	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	February 24, 2025, 19:36:32 (UTC+05:30)

Step 7 :- Click Upload.

mckviepkbucket

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (0)

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

Name	Type	Last modified	Size	Storage class
------	------	---------------	------	---------------

Step 8 :- Click Add files and select website files (Google.html, Next.html, etc.). Click Upload.

Files and folders (2 total, 510.0 B)

All files and folders in this table will be uploaded.

Find by name

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	Next.html	-	text/html	155.0 B
<input type="checkbox"/>	Google.html	-	text/html	355.0 B

Destination

Destination

s3://mckviepkbucket

► 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 9 :-Folder uploaded successfully so close .

✔ 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://mckviepkbucket

Succeeded
2 files, 510.0 B (100.00%)

Failed
0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (2 total, 510.0 B)

Find by name

Name	Folder	Type	Size	Status	Error
Next.html	-	text/html	155.0 B	✔ Succeeded	-
Google.html	-	text/html	355.0 B	✔ Succeeded	-

Step 10 :- Go to buckets -> Properties and edit the static website hosting.

Static website hosting

[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

Disabled

Step 11 :- Now enable static website hosting and in index document write Google.html and click on save changes.

PURNA KUNDU/CSE-DS/22/047

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.

Google.html

Step 12 :- Now go to bucket and click on **Google.html->permissions->everyone public access**

Google.html [info](#)

[Copy S3 URI](#)

[Download](#)

[Open](#)

[Object actions](#)

Properties

Permissions

Versions

Access control list (ACL)

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

[Edit](#)

Grantee	Object	Object ACL
Object owner (your AWS account) Canonical ID: effca1f37373c7a9b6733867e7aee2759b9de0a9f2a1adac6c4a7b34de57db50	Read	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	-	-

Step 13 :- . Enable both the read option and click on checkbox means the website can seen by anyone. And confirm the **acknowledgement**.

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: effca1f37373c7a9b6733867e7aee2759b9de0a9f2a1adac6c4a7b34de57db50	<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 checked="" type="checkbox"/> <input checked="" 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.

Step 14 :- Same steps followed for Next.html

Next.html [info](#)

[Copy S3 URI](#)

[Download](#)

[Open](#)

[Object actions](#)

Properties

Permissions

Versions

Access control list (ACL)

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

[Edit](#)

Grantee	Object	Object ACL
Object owner (your AWS account) Canonical ID: effca1f37373c7a9b6733867e7aee2759b9de0a9f2a1adac6c4a7b34de57db50	Read	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	-	-

Step 15 :- Click the URL, and open a new tab in browser and pest the link and entered, website is live!

[mckviepkbucket.s3.eu-north-1.amazonaws.com/Next.html](#)

[mckviepkbucket.s3.eu-north-1.amazonaws.com/Google.html](#)

This is next

This is a next

This is heading

this is paragraph

[Google Nexts](#)