

# Project – Create and Host a Static Website on S3

## Scenario

In this project, how to create and host a static website on Amazon S3. You'll create an S3 bucket, configure it for static website hosting, upload website content, and access the website using the S3-generated URL.

## Steps:

1. Create an S3 bucket static-website-srinadhgdlr in region us-east-1.
2. Set up the S3 bucket for static website hosting with appropriate bucket properties and permission policies.
3. Upload content from the GitHub repository <https://github.com/srinadhgdlr/static-website> to the bucket root so that index.html shows up on the website root.
4. Access the website over a browser using the S3-generated link.
5. Clean up the resources created.

## Task 1 - Create an S3 Bucket

Open the AWS Management Console, Navigate to the S3 service.

Choose Create bucket

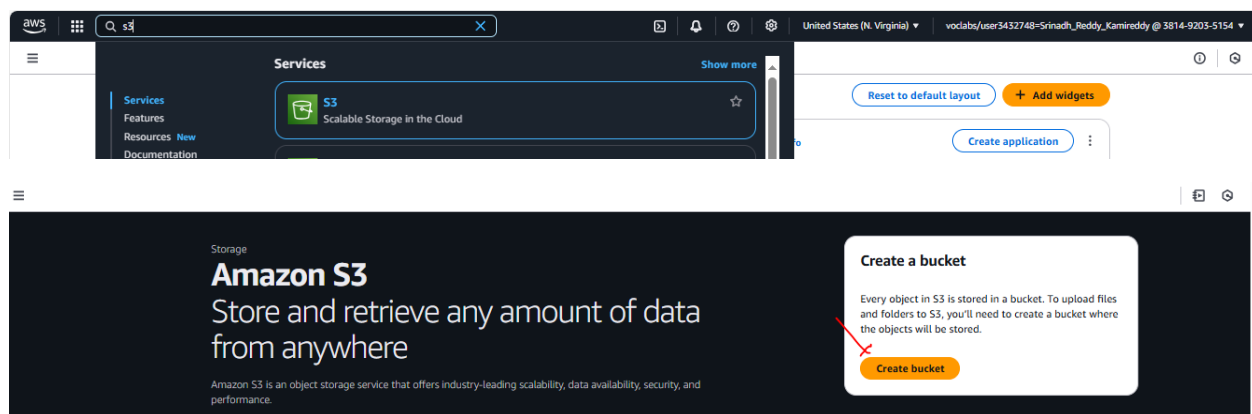
Select the region us-east-1

Enter a unique Bucket name: static-website-srinadhgdlr

Disable Block all public access.

Check "I acknowledge that the current settings might result in this bucket and the objects within becoming public."

Choose Create bucket



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

Bucket type | Info

- General purpose

- | Bucket type   | Use case                               |
|---|--|
| <ul style="list-style-type: none"> <li><b>General purpose</b><br/>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.</li> <li><b>Directory</b><br/>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.</li> </ul> | <p>Use cases for Amazon S3 buckets</p> |

static-website-srinadhgdlr

static-website-srinadhgdlr

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 number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). [Learn More](#)

Only the bucket settings in the following configuration are copied.

Only the bucket settings in the following configuration are copied.

Choose bucket

Format: s3://bucket/prefix

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.

Bucket owner enforced

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 to 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.

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](#)

☒ Disable

☐ Enable

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

No tags associated with this bucket.

Add tag

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

- Server-side encrypt

- ☒ 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](#).

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](#)

- ☒
- Enable

① After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Amazon S3 > Buckets

Successfully created bucket "static-website-srinadhgdlr"  
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 (1) 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"/>	static-website-srinadhgdlr	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	March 23, 2025, 18:28:02 (UTC+00:00)

## Task 2 - Set Up Static Website Hosting

Navigate to the S3 Bucket name static-website-srinadhgdlr and click on Bucket name

Go to the Properties tab.

Scroll down to the Static website hosting section.

Choose Edit.

Select Enable.

In the Index document box, enter index.html.

Choose Save changes.

Amazon S3 > Buckets > static-website-srinadhgdlr

static-website-srinadhgdlr 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::static-website-srinadhgdlr</a>	<b>Creation date</b> March 23, 2025, 18:28:02 (UTC+00:00)
--	---	--

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

[Edit](#)

**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 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.

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](#)

#### Redirection rules - optional

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

1	

JSON Ln 1, Col 1 | Errors: 0 | Warnings: 0

[Cancel](#) [Save changes](#)

🟢 Successfully edited static website hosting.

Dismiss

### 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

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://static-website-srinadhgdlr.s3-website-us-east-1.amazonaws.com>

[Edit](#)

## Task 3 - Set Bucket Permissions

Navigate to the Permissions tab.

Under Block public access section, click Edit.

Deselect Block all public access, then select the first two options (ACLs).

Save changes

To confirm the settings, enter *confirm* in the field.

static-website-srinadhgdlr [Info](#)

Objects | Metadata | 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 us-east-1](#)

### Block public access (bucket settings)

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

- ☒ **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.

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

**Block public access (bucket settings)**  
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**  
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.

[Cancel](#) [Save changes](#)

Scroll down to Bucket policy and choose Edit.

Add the following bucket policy to allow public access to the bucket contents.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::static-website-srinadhgdlr/*"
    }
  ]
}
```

Amazon S3 > Buckets > static-website-srinadhdgr

**Bucket policy**

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](#)

**Public access is blocked because Block Public Access settings are turned on for this bucket**

To determine which settings are turned on, check your Block Public Access settings for this bucket. [Learn more about using Amazon S3 Block Public Access](#)

No policy to display. [Copy](#)

**Edit bucket policy** [info](#)

**Bucket policy**

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](#)

**Bucket ARN**

arn:aws:s3::static-website-srinadhdgr

**Policy**

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": "*",
7       "Action": "s3:GetObject",
8       "Resource": "arn:aws:s3::static-website-srinadhdgr/*"
9     }
10  ]
11 }
12
```

[+ Add new statement](#)

**Edit statement**

Select a statement

Select an existing statement in the policy or add a new statement.

[+ Add new statement](#)

JSON Ln 12, Col 0

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0 [Preview external access](#)

[Cancel](#) [Save changes](#)

Choose Save changes.

## Task 4 - Upload Website Content

### Clone the GitHub Repository Locally:

Open terminal or command prompt. Navigate to directory where you want to save the website project.

Clone the repository using the following command:

```
git clone https://github.com/srinadhdgr/static-website.git
```

Navigate to the cloned repository directory:

```
cd static-website
```

```
C:\Users\DELL\Desktop>
C:\Users\DELL\Desktop>git clone https://github.com/srinadhdgr/static-website.git
Cloning into 'static-website'...
remote: Enumerating objects: 5, done.
remote: Counting objects: 100% (5/5), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 5 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (5/5), 5.77 KiB | 1.92 MiB/s, done.

C:\Users\DELL\Desktop>
C:\Users\DELL\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 5699-DF80

Directory of C:\Users\DELL\Desktop
```

```
C:\Users\DELL\Desktop>
C:\Users\DELL\Desktop>cd static-website

C:\Users\DELL\Desktop\static-website>dir
Volume in drive C has no label.
Volume Serial Number is 5699-DF80

Directory of C:\Users\DELL\Desktop\static-website

23/03/2025  19:09    <DIR>          .
23/03/2025  19:09    <DIR>          ..
23/03/2025  19:09             3,427  index.html
23/03/2025  19:09             11,558  LICENSE.txt
23/03/2025  19:09              41  README.md
                3 File(s)              15,026 bytes
                2 Dir(s)  150,102,220,800 bytes free

C:\Users\DELL\Desktop\static-website>
```

### Upload Content to S3 Using AWS CLI:

Ensure that the AWS CLI is installed and configured with the necessary permissions.

Configure the profile settings for your profile or use default one.

Run the following command in to sync the content from the cloned repository to your S3 bucket:

```
aws s3 sync . s3://static-website-srinadghdlr
```

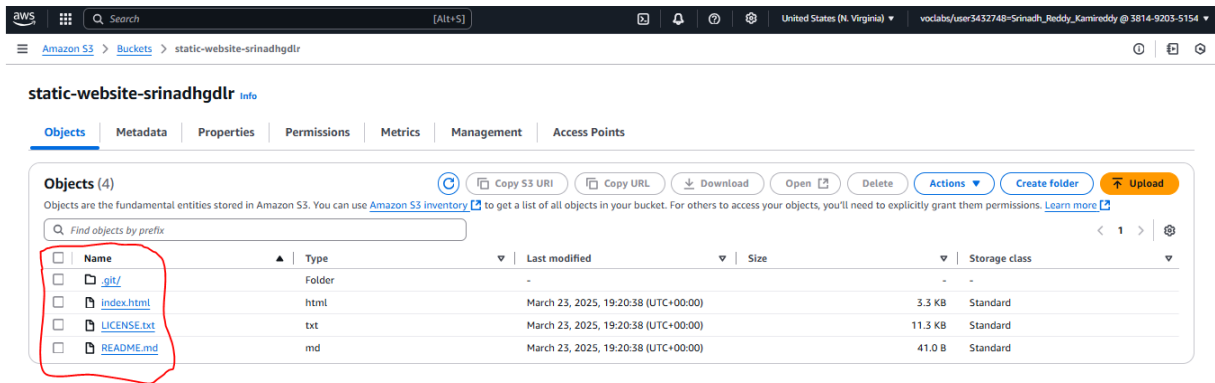
```
PS C:\Users\DELL\Desktop\static-website>
PS C:\Users\DELL\Desktop\static-website> $env:AWS_ACCESS_KEY_ID="AS1AVRUVSP121X63UP1P"
PS C:\Users\DELL\Desktop\static-website> $env:AWS_SECRET_ACCESS_KEY="bwh5o071r0x011D0v1T4x07HLzxF7p68CaPeb"
PS C:\Users\DELL\Desktop\static-website> $env:AWS_SESSION_TOKEN="1001b33p221u02VJEL1////////wEaC2vSLXG1c3qM13HREUCIQcadvJgudsAaU1CL/8BwaZ3FFD4cQ8a1+2nD2du0Yg1gthMD0RwYX181jD1g4z5db2Thc+h
TRgELKXEE01aWhkang5121////////ARAAgns0DE80T1WZUKNTQ1DhyUqpXASH9EwF1kF5Q0ANw0+56EQ7F205du216A70kmc9tybuuMBK2MLVh1pa/BsD1pYPBVLcUBN7aAnPudfXqY1VqH0T291ne1v0pxPK3FuqzmkPdvG3q+AQpDhh1SG0
nYc4KYgaKUTst+mkahX1H5K26AMH0M5s0zDnwpO/19B71KcD18Cmk522Rk2XAM5PaddfsgnJqlyxCLgevm/CHjYemec3J5pYK0m/hcZxkopl1Au04bp9LkR6kFY633JH1Tp0PyTpUw57PdbBTQVv0TLTK2Cm7b1/HfancD09Ek3F40R68PMAoH2bg8+Qv
0LJq2KHfV/vRUCc3+77ia1pgp0BAC7x0aTro/2ndUR/LV04kgBT0uYg/BjddAco3HP4v12P8LksEP8T2N765a1k3JN03Ukca1AS11X0dKv12Qmd+w31363u0tAHL3u/Fg5113P6JPFa3ES/3h00BKED0T1cDMCrcUgzE9f/XD2A6hq1cy478Pp
55q9Pbcs+6541n7+71o1fF33Q2c3106a0H010ULF51+18a/RH1SH3Wq1NVIYKn0FHK26w0Cj2F01c9E+"
PS C:\Users\DELL\Desktop\static-website>
PS C:\Users\DELL\Desktop\static-website>
PS C:\Users\DELL\Desktop\static-website> aws s3 sync . s3://static-website-srinadghdlr
upload: .git\description to s3://static-website-srinadghdlr/.git\description
upload: .git\hooks\pre-push.sample to s3://static-website-srinadghdlr/.git\hooks\pre-push.sample
upload: .git\hooks\pre-rebase.sample to s3://static-website-srinadghdlr/.git\hooks\pre-rebase.sample
upload: .git\hooks\pre-receive.sample to s3://static-website-srinadghdlr/.git\hooks\pre-receive.sample
upload: .git\hooks\prepare-commit-msg.sample to s3://static-website-srinadghdlr/.git\hooks\prepare-commit-msg.sample
upload: .git\hooks\push-to-checkout.sample to s3://static-website-srinadghdlr/.git\hooks\push-to-checkout.sample
upload: .git\hooks\sendemail-validate.sample to s3://static-website-srinadghdlr/.git\hooks\sendemail-validate.sample
upload: .git\hooks\update.sample to s3://static-website-srinadghdlr/.git\hooks\update.sample
upload: .git\index to s3://static-website-srinadghdlr/.git\index
upload: .git\info\exclude to s3://static-website-srinadghdlr/.git\info\exclude
upload: .git\logs\HEAD to s3://static-website-srinadghdlr/.git\logs\HEAD
upload: .git\logs\refs\heads\main to s3://static-website-srinadghdlr/.git\logs\refs\heads\main
upload: .git\logs\refs/remotes\origin\HEAD to s3://static-website-srinadghdlr/.git\logs\refs/remotes\origin\HEAD
upload: .git\objects\pack\pack-5f688df0660d4186af9e197b7bb873e4a3c851a6.idx to s3://static-website-srinadghdlr/.git\objects\pack\pack-5f688df0660d4186af9e197b7bb873e4a3c851a6.idx
upload: .git\objects\pack\pack-5f688df0660d4186af9e197b7bb873e4a3c851a6.pack to s3://static-website-srinadghdlr/.git\objects\pack\pack-5f688df0660d4186af9e197b7bb873e4a3c851a6.pack
upload: .git\objects\pack\pack-5f688df0660d4186af9e197b7bb873e4a3c851a6.rev to s3://static-website-srinadghdlr/.git\objects\pack\pack-5f688df0660d4186af9e197b7bb873e4a3c851a6.rev
upload: .git\packed-refs to s3://static-website-srinadghdlr/.git\packed-refs
upload: .git\hooks\fsmonitor-watchman.sample to s3://static-website-srinadghdlr/.git\hooks\fsmonitor-watchman.sample
upload: .git\config to s3://static-website-srinadghdlr/.git\config
upload: .git\hooks\pre-commit.sample to s3://static-website-srinadghdlr/.git\hooks\pre-commit.sample
upload: .git\HEAD to s3://static-website-srinadghdlr/.git\HEAD
upload: .git\refs\heads\main to s3://static-website-srinadghdlr/.git\refs\heads\main
upload: .git\hooks\pre-merge-commit.sample to s3://static-website-srinadghdlr/.git\hooks\pre-merge-commit.sample
upload: .git\refs\remotes\origin\HEAD to s3://static-website-srinadghdlr/.git\refs/remotes\origin\HEAD
upload: .git\hooks\commit-msg.sample to s3://static-website-srinadghdlr/.git\hooks\commit-msg.sample
upload: .git\hooks\post-update.sample to s3://static-website-srinadghdlr/.git\hooks\post-update.sample
upload: .git\hooks\applypatch-msg.sample to s3://static-website-srinadghdlr/.git\hooks\applypatch-msg.sample
upload: .git\hooks\pre-applypatch.sample to s3://static-website-srinadghdlr/.git\hooks\pre-applypatch.sample
upload: .LICENSE.txt to s3://static-website-srinadghdlr/LICENSE.txt
upload: .index.html to s3://static-website-srinadghdlr/index.html
upload: .README.md to s3://static-website-srinadghdlr/README.md
PS C:\Users\DELL\Desktop\static-website>
```

### Verify the Upload:

Navigate to the S3 bucket static-website-srinadghdlr in the AWS Management Console.

Ensure that the content from the GitHub repository has been uploaded successfully to the bucket root.

With this, you will have uploaded the website content to your S3 bucket using AWS CLI commands.



## Task 5 - Access the Website

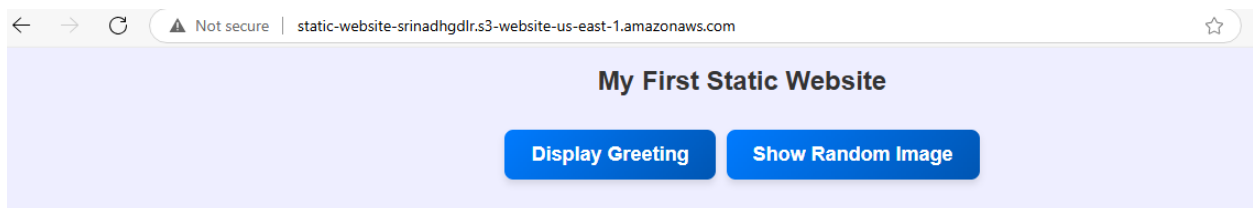
Navigate to the Properties tab of the S3 bucket static-website-srinadhgdlr

Scroll down to the Static website hosting section.

Copy the Bucket website endpoint URL `http://static-website-srinadhgdlr.s3-website-us-east-1.amazonaws.com`

Open a web browser and paste the copied URL to access the website.

Verify that the website content is displayed correctly.



## Task 6 - Clean Up

Navigate to the S3 bucket static-website-srinadhgdlr

Select all the objects in the bucket and choose Delete.

Confirm the deletion.

Delete the S3 bucket static-website-srinadhgdlr