

**Project in AWS  
Practice Lab**

# **Create a Static Website Using Amazon S3**

**Andra-Diana Popescu**

**2025**

## ABOUT THIS LAB

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. In this lab, we will create and configure a simple static website. We will go through configuring that static website with a custom error page. This will demonstrate how to create a cost-efficient website hosting for sites that consist of files like HTML, CSS, JavaScript, fonts, and images.

## LEARNING OBJECTIVES

- Create an S3 Bucket
- Enable Static Website Hosting
- Apply Bucket Policy

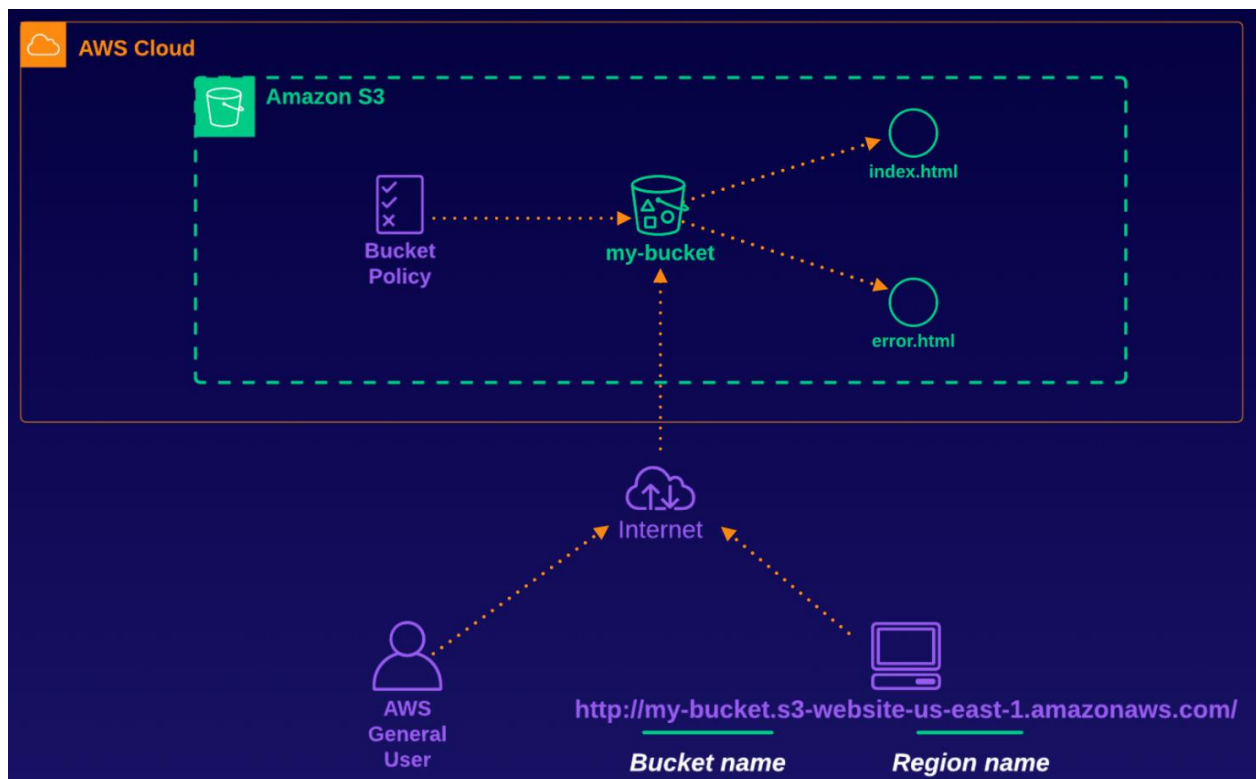
**AWS Documentation about S3:** [https://aws.amazon.com/s3/faqs/#Storage\\_Classes](https://aws.amazon.com/s3/faqs/#Storage_Classes)

**Source:** <https://learn.acloud.guru/course/certified-solutions-architect-associate/>

## Table of Contents

Lab Diagram .....	4
Log in to your AWS account .....	5
1. Create an S3 Bucket.....	5
1.1. Download the 2 HTML files from GitHub .....	5
1.2. Create an S3 Bucket.....	6
2. Enable Static Website Hosting.....	9
3. Apply Bucket Policy .....	10

## Lab Diagram



We will begin by configuring an S3 bucket for website hosting, then upload our content to that bucket (*index.html* and *error.html*) and the bucket must have a public read access enabled and its intentional to everyone in the world will have read access to the bucket (*bucket policy*).

The website will be available at the AWS S3 endpoint (which is going to look something like the URL from the diagram). Make sure you are in us-east-1 (N. Virginia) for the lab environment.

The 2 HTML files required from this lab can be downloaded by Saving As these 2 files: *index.html* and *error.html* . You will find these files in the following GitHub repository: <https://github.com/ACloudGuru-Resources/Course-Certified-Solutions-Architect-Associate/tree/master/labs/creating-a-static-website-using-amazon-s3> .

## Log in to your AWS account



Sign in as IAM user

Account ID (12 digits) or account alias

Type Account ID

IAM user name

Type IAM user name

Password

\*\*\*\*\*

☐ Remember this account

Sign in

Sign in using root user email

[Forgot password?](#)



## 1. Create an S3 Bucket

### 1.1. Download the 2 HTML files from GitHub

1. In a new browser tab, navigate to the GitHub repository for the code.
2. Download these 2 files (***error.html*** and ***index.html***) to the local machine so that we can upload them to S3.
3. Go to each file and click **Download raw file**.

Course-Certified-Solutions-Architect-Associate / labs / creating-a-static-website-using-amazon-s3 /

mrhichman Added static website assets 5766c1d · 5 years ago History

Name	Last commit message	Last commit date
..		
error.html	Added static website assets	5 years ago
index.html	Added static website assets	5 years ago

Course-Certified-Solutions-Architect-Associate / labs / creating-a-static-website-using-amazon-s3 / error.html

mrhichman Added static website assets 5766c1d · 5 years ago History Download raw file

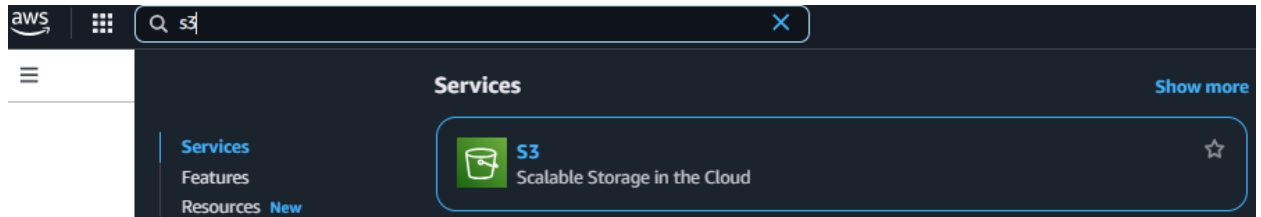
Code Blame 95 lines (80 loc) · 3.47 KB

```
1 <!doctype html>
2 <html lang="en">
3
4 <head>
5   <meta charset="utf-8">
6   <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
7   <title>Creating a Static Website Using Amazon S3</title>
```

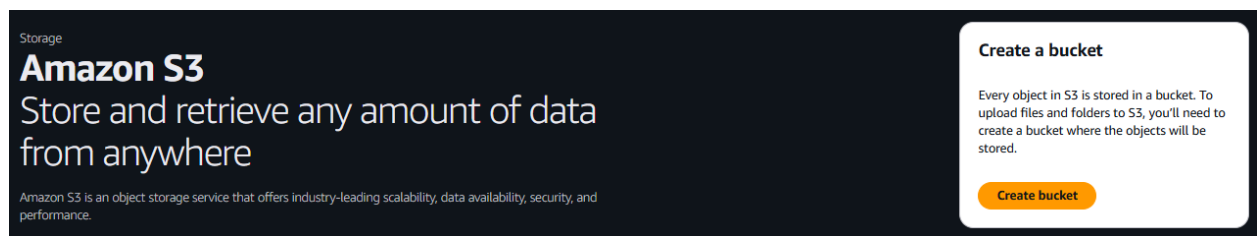
4. Repeat this for the ***index.html*** file.

## 1.2. Create an S3 Bucket

1. In the AWS Management Console, navigate to S3.



2. Click **Create bucket**.



3. Set Bucket name: **my-bucket-** with the AWS account ID or another series of numbers at the end to make it globally unique. Also, set the Region: US East (N. Virginia) us-east-1.

### Create bucket [Info](#)

Buckets are containers for data stored in S3.

#### General configuration

##### AWS Region

US East (N. Virginia) us-east-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.

##### Bucket name [Info](#)

my-bucket-123456789111

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.

4. In the **Block Public Access settings for this bucket** section, un-check Block all public access. Ensure all four permissions restrictions beneath it are also un-checked.
5. Check the box to acknowledge that turning off all public access might result in the bucket and its objects becoming public.

### 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.

6. Leave the rest of the settings as their defaults.

7. Click **Create bucket**.

### Default encryption Info

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 Storage tab of 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

8. Click the bucket name.

☑ Successfully created bucket "my-bucket-123456789111"

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

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) Info All AWS Regions

Buckets are containers for data stored in S3.

🔄 📄 Copy ARN Empty Delete Create bucket

	Name	AWS Region	IAM Access Analyzer	Creation date
<input type="radio"/>	<a href="#">my-bucket-123456789111</a>	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	April 3, 2025, 22:14:35 (UTC+03:00)

9. Click **Upload**.

my-bucket-123456789111 Info

ObjectsMetadataPropertiesPermissionsMetricsManagementAccess Points

Objects (0)

Copy S3 URICopy URLDownloadOpenDeleteActionsCreate folderUpload

Find objects by prefix

NameTypeLast modifiedSizeStorage class

No objects  
You don't have any objects in this bucket.

Upload

10. Click **Add files**, and upload the *error.html* and *index.html* files you previously saved from GitHub. Leave the rest of the settings as their defaults. Click **Upload**.

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 files** or **Add folder**.

Files and folders (2 total, 7.2 KB)

RemoveAdd filesAdd folder

Find by name

	Name	Folder	Type	Size
<input type="checkbox"/>	error.html	-	text/html	3.5 KB
<input type="checkbox"/>	index.html	-	text/html	3.8 KB

Destination Info

Destination

s3://my-bucket-123456789111

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.

CancelUpload

11. Click **Close** in the upper right.

Upload succeeded

For more information, see the **Files and folders** table.

Close

Upload: status

After you navigate away from this page, the following information is no longer available.

Summary

Destination

s3://my-bucket-123456789111

Succeeded

2 files, 7.2 KB (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (2 total, 7.2 KB)

Find by name

Name	Folder	Type	Size	Status	Error
error.html	-	text/html	3.5 KB	Succeeded	-
index.html	-	text/html	3.8 KB	Succeeded	-



## 2. Enable Static Website Hosting

1. Click the **Properties** tab.

my-bucket-123456789111 [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> arn:aws:s3:::my-bucket-123456789111	<b>Creation date</b> April 3, 2025, 22:14:35 (UTC+03:00)
--	--	---

2. Scroll to the bottom of the screen to find the **Static website hosting** section.
3. On the right in the **Static website hosting** section, click **Edit**.

**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**  
Disabled

4. On the **Edit static website hosting** page, set the following values:
  - **Static website hosting**: Select **Enable**.
  - **Hosting type**: Select **Host a static website**.
  - **Index document**: Enter index.html.
  - **Error document**: Enter error.html.
5. At the bottom, click **Save changes**.

Edit static website hosting [info](#)

**Static website hosting** [info](#)

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.

6. In the **Static website hosting** section, open the listed endpoint URL in a new browser tab. Once opened, you'll see a **403 Forbidden** error message.

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://my-bucket-123456789111.s3-website-us-east-1.amazonaws.com>

- This error means that although the website is running, we haven't explicitly allowed permission to read the files that are contained in the bucket. So we need to return to our bucket to update the permissions.

←

→

↺

⚠ Not secure

my-bucket-123456789111.s3-website-us-east-1.amazonaws.com

403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: AC7
- HostId: SEFYk

81G

QuIMTE=

An Error Occurred While Attempting to Retrieve a Custom Error Document

- Code: AccessDenied
- Message: Access Denied

### 3. Apply Bucket Policy

- Back in S3, click the **Permissions** tab.
- In the **Bucket policy** section, click **Edit**.

my-bucket-123456789111 [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

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](#)

3. Above the code entry box, **copy the bucket ARN**.
4. On the right, click **Policy generator** to create our policy.

**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::my-bucket-1234567891111

**Policy**

1

**Edit statement**

**Select a statement**


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

[+ Add new statement](#)

5. Select the following values:

- **Select Type of Policy:** Select **S3 Bucket Policy**.
- **Effect:** Select **Allow**.
- **Principal:** Enter **\***. This means anyone.
- **Actions:** Select **GetObject**. This is going to give read access to the objects in the bucket.
- **Amazon Resource Name (ARN):** Paste the name you added earlier followed by **/\*** so the policy applies to all objects within the bucket.

← → ↻ 🔍 awspolicygen.s3.amazonaws.com/policygen.html



### AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to [Amazon Web Services \(AWS\)](#) products and resources. For more information about creating policies, see [key concepts in Using AWS Identity and Access Management](#). Here are [sample policies](#).

#### Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of Policy S3 Bucket Policy

#### Step 2: Add Statement(s)

A statement is the formal description of a single permission. See [a description of elements](#) that you can use in statements.

**Effect** ☒ Allow ☐ Deny

**Principal**

Use a comma to separate multiple values.

**AWS Service** Amazon S3 ☐ All Services (\*\*)

Use multiple statements to add permissions for more than one service.

**Actions** 1 Action(s) Selected ☐ All Actions (\*\*)

**Amazon Resource Name (ARN)**

ARN should follow the following format: arn:aws:s3:::{BucketName}/{Key\*Name}.  
Use a comma to separate multiple values.

**Add Conditions (Optional)**

[Add Statement](#)

#### Step 3: Generate Policy

A policy is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

**Add one or more statements above to generate a policy.**

6. Click **Add Statement → Generate Policy**.

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• *	Allow	• s3:GetObject	arn:aws:s3::my-bucket-1234567891111/*	None

**Step 3: Generate Policy**

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

**Generate Policy**

[Start Over](#)

7. Copy the displayed policy, and go back to the bucket policy screen and paste the JSON.  
You can ignore any errors.

Policy JSON Document

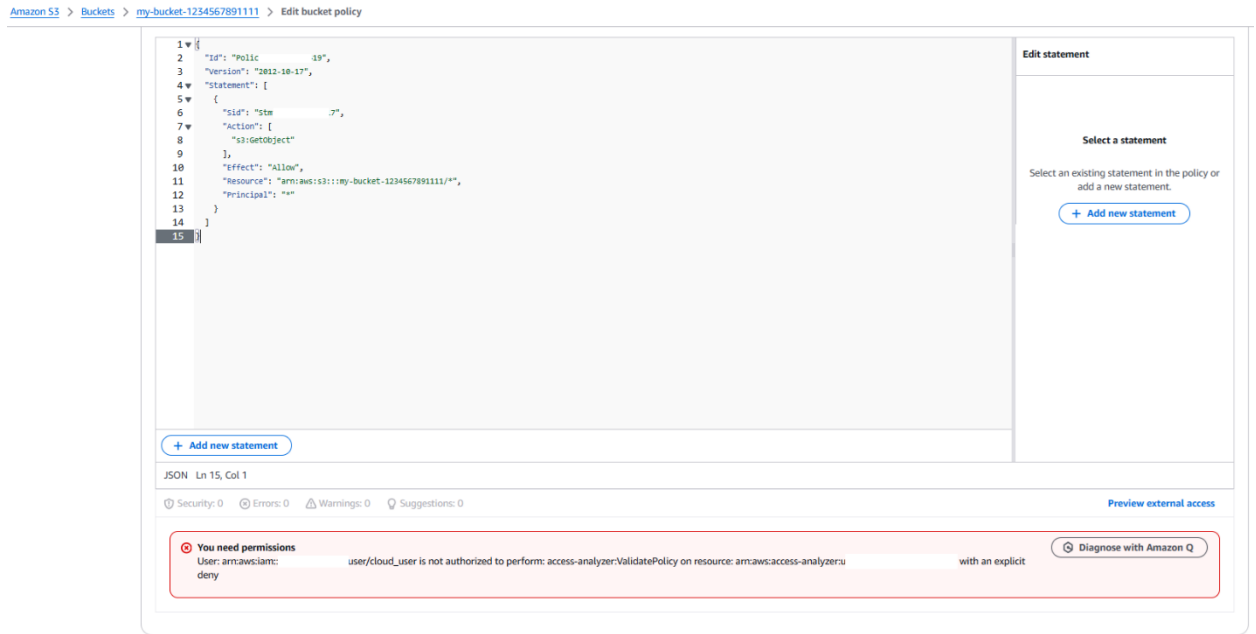
Click below to edit. To save the policy, copy the text below to a text editor.  
Changes made below will not be reflected in the policy generator tool.

```
{
  "Id": "Policy174[REDACTED]19",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt[REDACTED]7",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3::my-bucket-1234567891111/*",
      "Principal": "*"
    }
  ]
}
```

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable laws and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether expressed or implied.

**Close**

8. Click **Save changes**.



- Refresh the browser tab with the static website (the endpoint URL you opened earlier). This time, the site should load correctly.

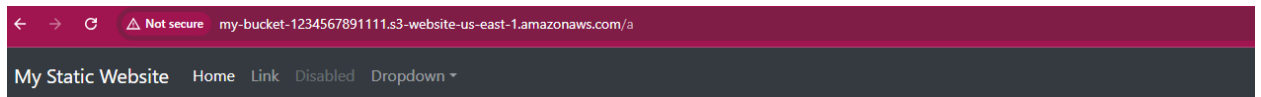


## Creating a Static Website Using Amazon S3

In this live AWS hands-on lab, we will create and configure a simple static website. We will go through configuring that static website with a custom error page. This will demonstrate how to create very cost-efficient website hosting for sites that consist of files like HTML, CSS, JavaScript, fonts, and images.

Navigation and search functions are intentionally not implemented.

- Add a / at the end of the URL and some random letters (anything that's knowingly an error). This will display your error.html page



## Error

Did you mean to go to [index.html?](#)

Navigation and search functions are intentionally not implemented.

**Note:** When creating the bucket, *uncheck* all four checkboxes on step — Set Permissions. If you skip this step, you will not be allowed to create the bucket policy later. If you made a mistake and created the bucket without unchecking the checkboxes, you may go to **Bucket > Permissions > Public access settings > Edit**, and uncheck all four restrictions. Then add a bucket policy, go to **Bucket > Permissions > Bucket Policy**, and add the following JSON statement (replacing `<BUCKET_ARN>` with your bucket ARN):

```
{
  "Version": "2012-10-17",
  "Id": "Policy1645724938586",
  "Statement": [
    {
      "Sid": "Stmt1645724933619",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "<BUCKET_ARN>/*"
    }
  ]
}
```

**Note:** You must make sure that the `/*` is at the end of the ARN. Click **Save changes**.