

Project : Host a Website on AWS

This beginner-friendly project which will guide us through setting up a personal website using Amazon S3 and connecting it with a custom domain through Amazon Route 53.

Step #1: Design Your Website

- Design your own personal website or download an existing template.
- You can find free templates at [free-css.com](https://www.free-css.com/).

Step #2: Set Up Amazon S3 Bucket

- Go to the AWS Management Console and open the Amazon S3 console.
- Click "Create bucket" and enter a unique name for your bucket.(caysusdilan.com)
- In the "Properties" section, enable "Static website hosting."
- Upload your website files to the bucket.
- Set the bucket permissions to allow public access.

Step #3: Purchase a Custom Domain through Amazon Route 53

- Open the Amazon Route 53 console.
- Choose "Domain registration" and then "Register domain."
- Follow the prompts to purchase your custom domain.
- In the "Route 53 hosted zones," create a new record set.
- Enter your S3 bucket's endpoint as the alias target.

- Additional time may be required for customizing the website design.

PROJECT OVERVIEW

- Bucket creation
Name of the Bucket is caysusdilan.com

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket name [Info](#)

caysusdilan.com

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

General purpose buckets (1) [Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

 Find buckets by name

Name ▲


AWS Region ▼



caysusdilan.com

Asia Pacific (Mumbai) ap-south-1

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.

- Uncheck every option so that your Bucket is publicly visible
- Keep the rest options as it is and create a 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](#)

- Click on the bucket created , go to permissions, scroll down to Bucket Policy , click on edit .
- Copy the Bucket ARN ,Click on policy generator.

Amazon S3 > Buckets > caysusdian > Edit static website hosting

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](#)

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](#)

1



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](#) [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

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

☐ All Services ("*")

Actions 1 Action(s) Selected

☐ All Actions ("*")

Amazon Resource Name (ARN)

arn:aws:s3:::my-bucket/*

ARNs should follow the following format: arn:aws:s3:::{BucketName}/{Key(Names)}. Use a comma to separate multiple values.

[Add Conditions \(Optional\)](#)

Add Statement

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/* | None |

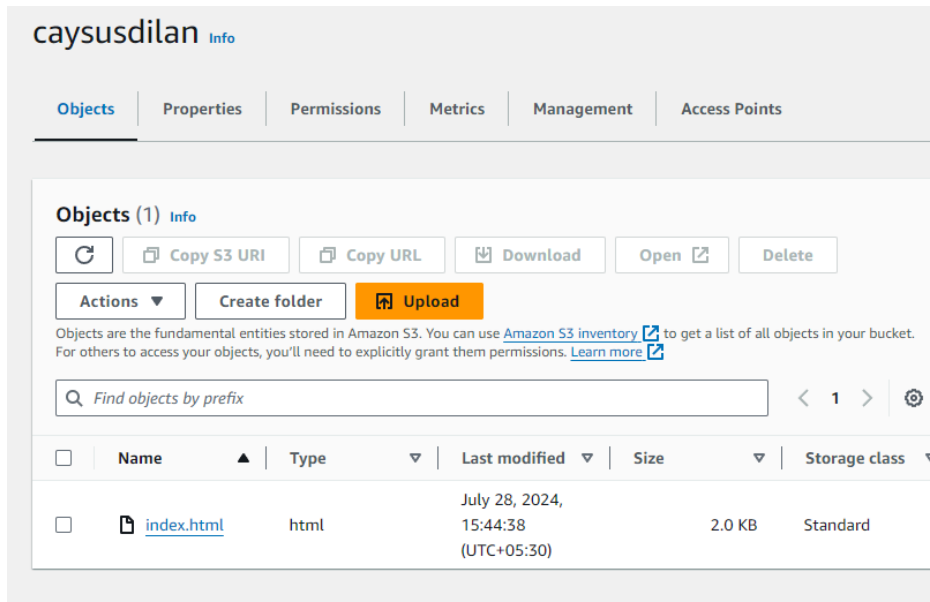
Step 3: Generate Policy

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

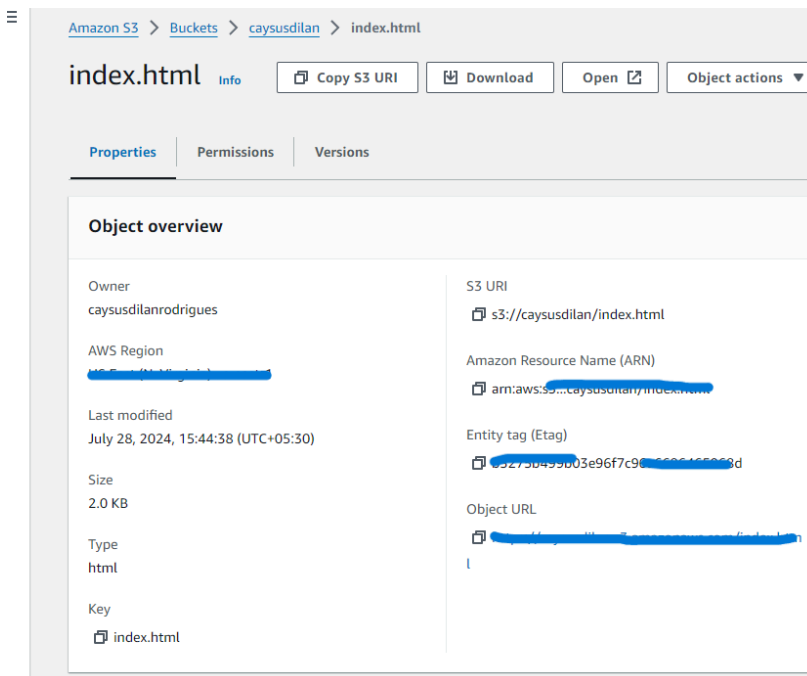
Generate Policy

[Start Over](#)

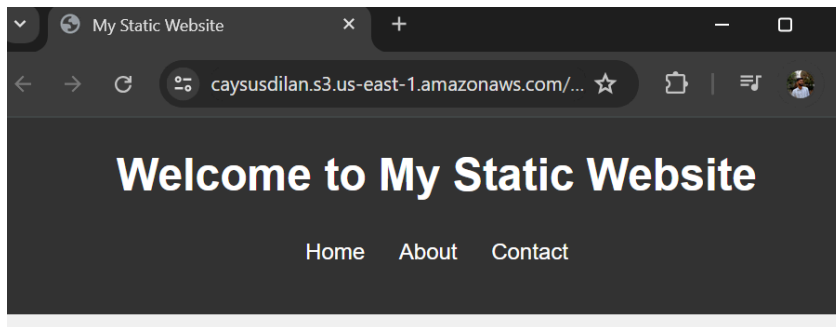
- Go to permissions and scroll down and **enable the Static website Hosting** option.(off by default) . Once enabled enter the name of the index file and save .
- Fill in all the required fields and click on generate policy
- To generate a policy: Choose **S3 bucket policy** in the choose type of policy >> type * in the principal section >> **Allow** Effect >> select **Get Object from the actions** - **copy the arn** from bucket edit policy and while pasting add /* to the end - **add statement** - **generate policy** - **copy the policy** and **paste it in edit policy section** - **save the policy** - then upload the files into the bucket .



- Click on the bucket , above you can see that I have uploaded a file name index.html
- Click on the file , then click open on the options or copy the object url provided .
- Paste the url in your browser's address bar , you can view the static website that I hoisted just now .



- Your website is visible publicly



Home

This is the home section of the website. Welcome!

About

This section is about us. We create cool things!

Contact

Feel free to reach out to us via email or social media.

- Now the Static website is hosted by the link provided by the Aws s3.
- Now to **connect your S3 bucket to the custom Amazon provided Url** , to redirect the purchased domain to this S3 bucket go to Route 53 , **purchase a domain with the available top level domain**(example: .com, .uk, .us)
- **Click on the hosted zone** in the Route 53 dashboard ,you will find your domain you purchased.
- Click on the domain name, here we need to **add an additional record to make sure that the bucket is connected to the route 53 domain name.**
- Click on **add record >> choose simple routing policy >> define a simple record >>** in the Value/Route traffic to option **select Alias to S3 bucket >>** next choose the **region where you hosted the bucket >> select the s3 endpoint** (provided automatically) >> evaluate target health=NO >> **click define simple record >>** double the fields entered and **click create record**(it may take some time to propagate) .
- Once it's propagated any user types your domain the browser they can view the website .You can see that url you enter will be pointing to route 53 domain and contents are from the S3 bucket you hosted.

