



TASK REPORT

Create a static website hosted on Amazon S3.

Name : Addala Venkata Lakshmi Sravani

Table of Contents

Description	2
Introduction	3
Create an S3 bucket on AWS	3
Upload Website files to S3 Bucket.....	5
Setting up Static Web Hosting in S3 Bucket.....	6
Setting up Permissions in S3 Bucket	7
Accessing the Website Through URL.....	8

Description

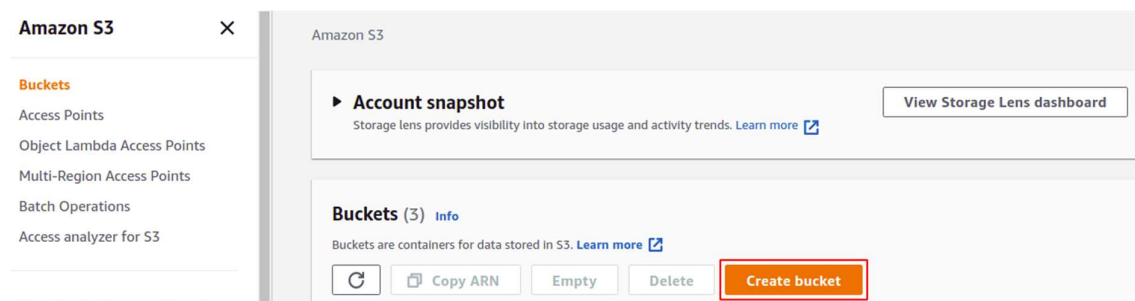
- Create a static website hosted on Amazon S3.
- Create a simple portfolio website using HTML and CSS, and host it on Amazon S3.
- Configure the necessary buckets, enable website hosting, and upload a basic HTML/CSS website.

Introduction

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. Customers of all sizes and industries can use Amazon S3 to store and protect any amount of data for a range of use cases, such as data lakes, websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides management features so that you can optimize, organize, and configure access to your data to meet your specific business, organizational, and compliance requirements.

Create an S3 bucket on AWS

- First login to your AWS management console and navigate to Amazon S3.
- Click on Create Bucket at the right corner of the S3 console:



- Now provide a globally unique bucket name and choose appropriate region.
- Enable the access control lists(ACLs).

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.

- Uncheck the Block all public access checkbox in the “Block Public Access setting for this bucket” section since we need the website to be accessible by everyone.

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with the AWS logo, 'Services' link, a search bar, and a keyboard shortcut '[Alt+S]'. Below the navigation bar is a blue banner with a message: 'We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose from...'. The main content area is titled 'Block Public Access settings for this bucket'. It contains a paragraph explaining public access and a 'Learn more' link. Below this, there's a section with a red box highlighting the 'Block all public access' checkbox, which is checked. A note states: 'Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.' Below this note are four sub-settings, each with a checked checkbox:

- ☒ **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.

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.

- Now just click on the **Create Bucket** button at the bottom right corner

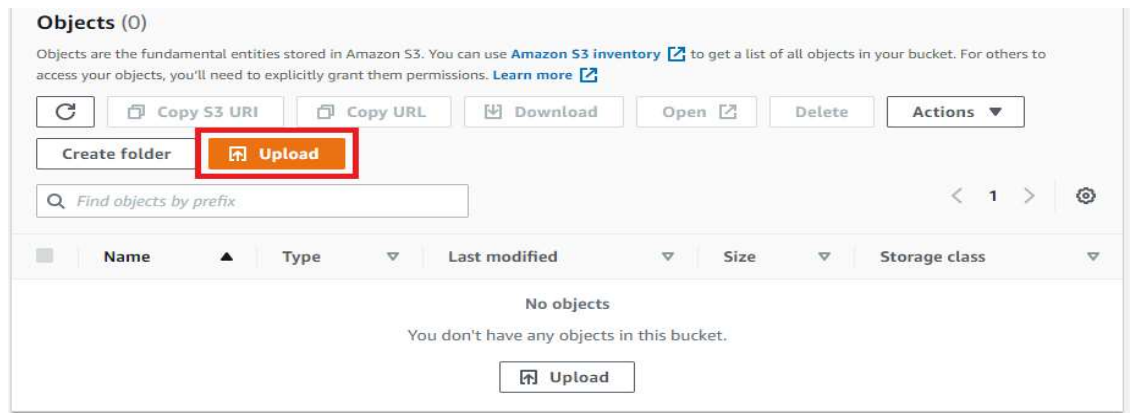
► **Advanced settings**

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

Cancel **Create bucket**

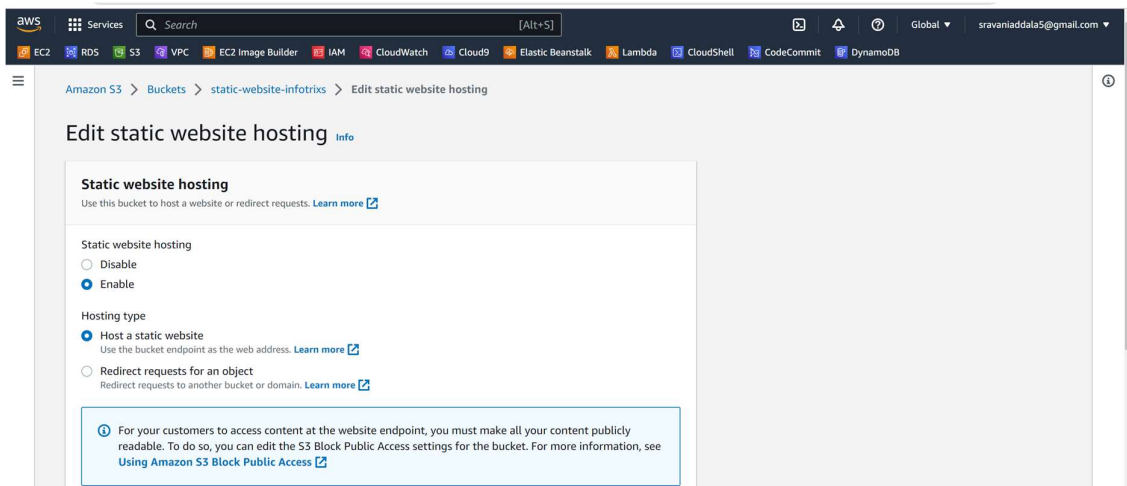
Upload Website files to S3 Bucket

- Go to the **Objects** section, and then Click on the upload button to browse and upload required website files

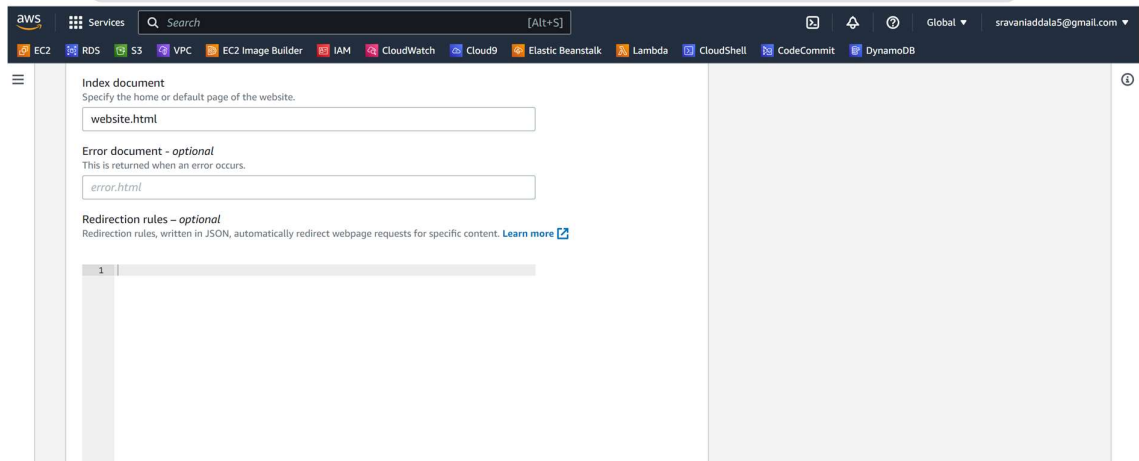


Setting up Static Web Hosting in S3 Bucket

- go to properties tab from the top menu in the S3 bucket to allow static web hosting.



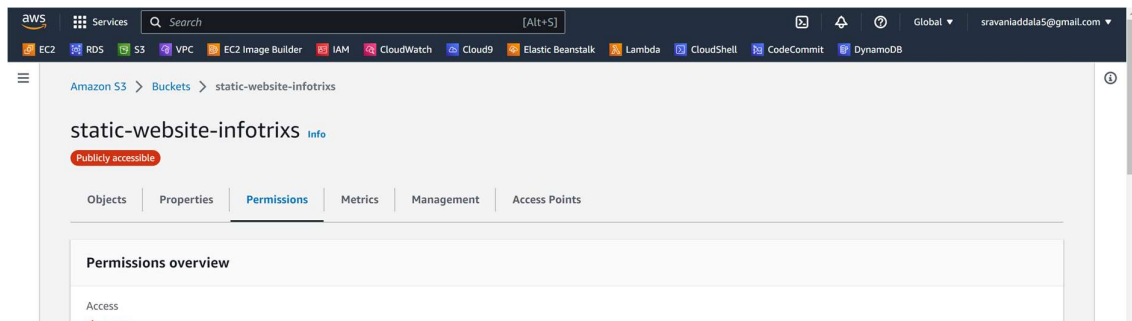
- Click on the Edit button in the Static website hosting section
- Enable the static web hosting reachable.
- Now give the name of Index Document (Eg:-Website.html)
- click on the **Save changes** button to apply the changes to your S3 bucket

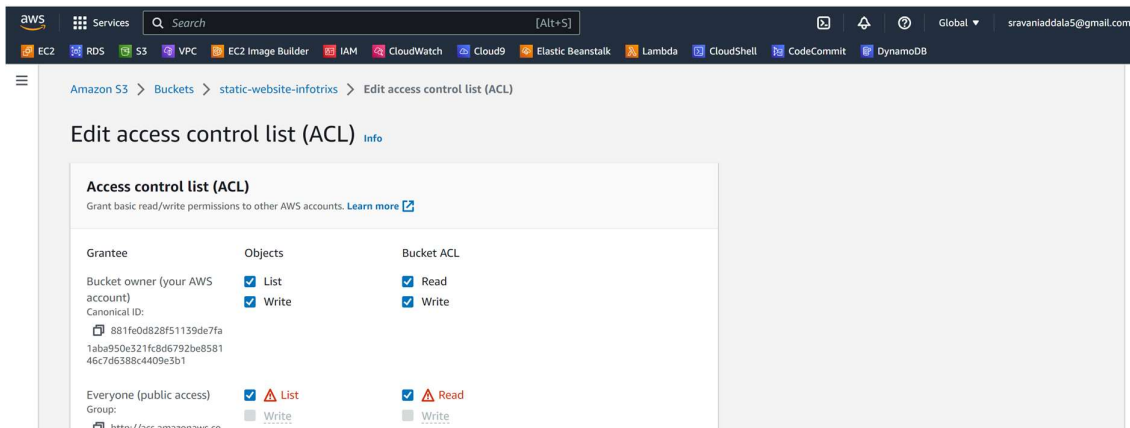
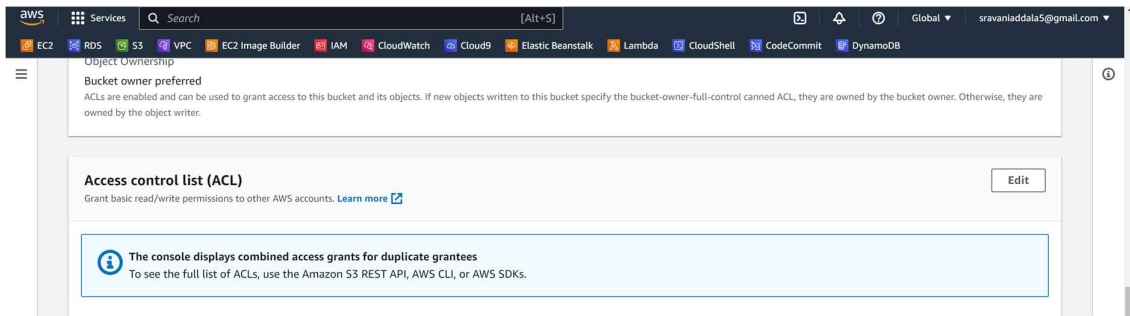


Setting up Permissions in S3 Bucket

Configure the bucket and object permissions to allow public access.

Use a bucket policy or access control lists (ACLs) to grant read permissions to "Everyone" or "All Users."





Accessing the Website Through URL

- Now access the webpage through the URL.

