

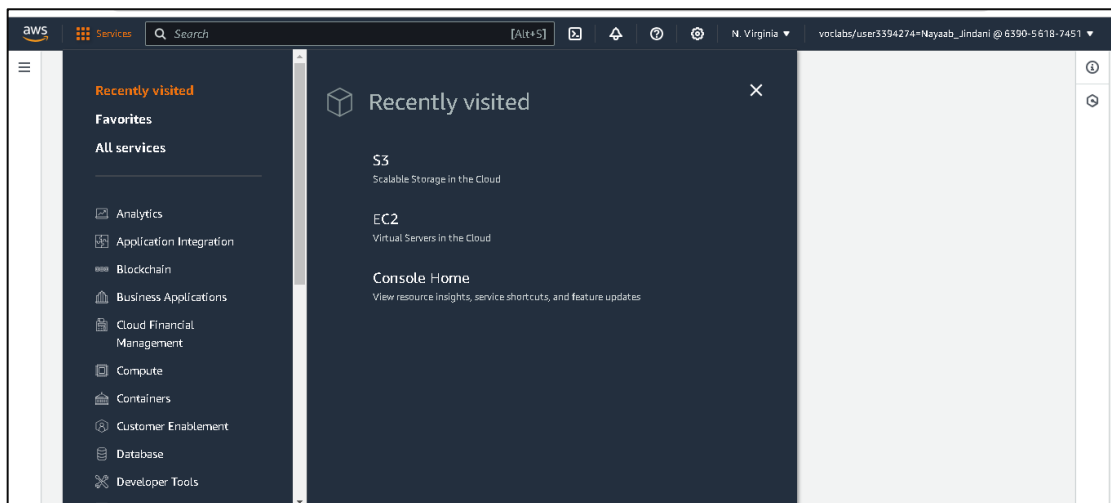
Advance DevOps

Experiment 1a

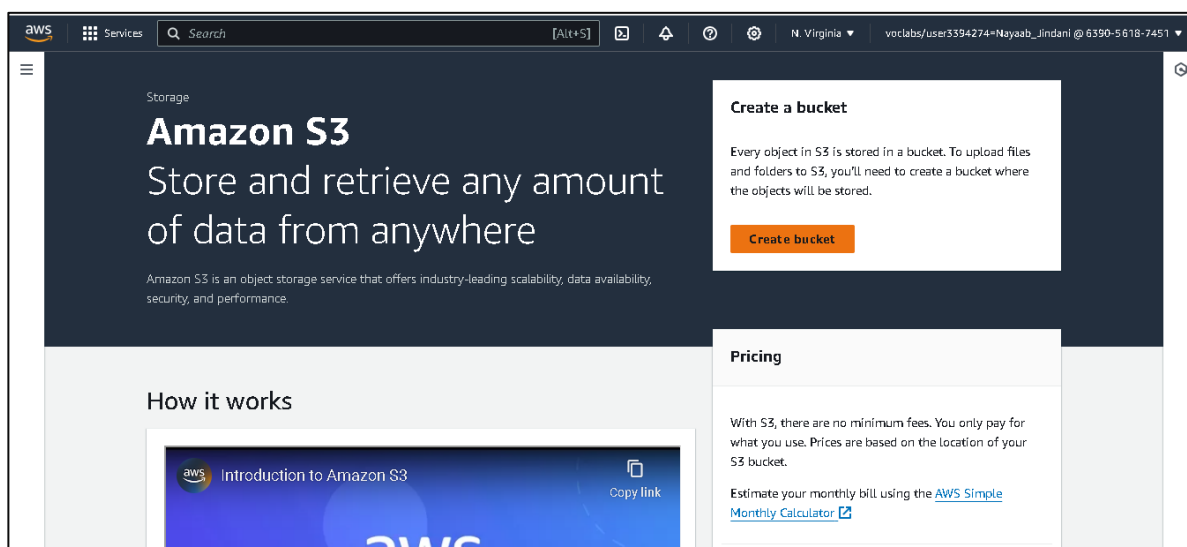
Part 2: Hosting a static website on Amazon S3

Steps:

1. Go to AWS console home -> services and select S3.



2. Select create a bucket



3. Enter bucket name and select create bucket.

4. Now upload the folder or files of the website to be hosted.

	Name	Folder	Type
<input type="checkbox"/>	test_doc.html	test_bucket/	text/html

5. After uploading the folder or files when you select the object URL of your file it will show access denied:

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>7R75XT2NFV2HMY48</RequestId>
  <HostId>PnyRp52k1NIJqU5T/ITdnTgvivnUnyOf3JzgesbK6QFmGKLL48p9luPmr78+eYFHa1LoFTVm9zbs9qiEFwxIRfHTXtmhHjs4v1/aKuKJg2Q=</HostId>
</Error>
```

- To provide access we need to enable static website hosting and to do so go to buckets -> your bucket -> properties -> static website hosting and enable static website hosting. Also Specify the home or default page of the website. Then click on save changes.

Amazon S3 > Buckets > nayaab > 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.

test_doc.html

- Now select the permission tab which is besides properties and uncheck block all public access.

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

Block public access (bucket settings)

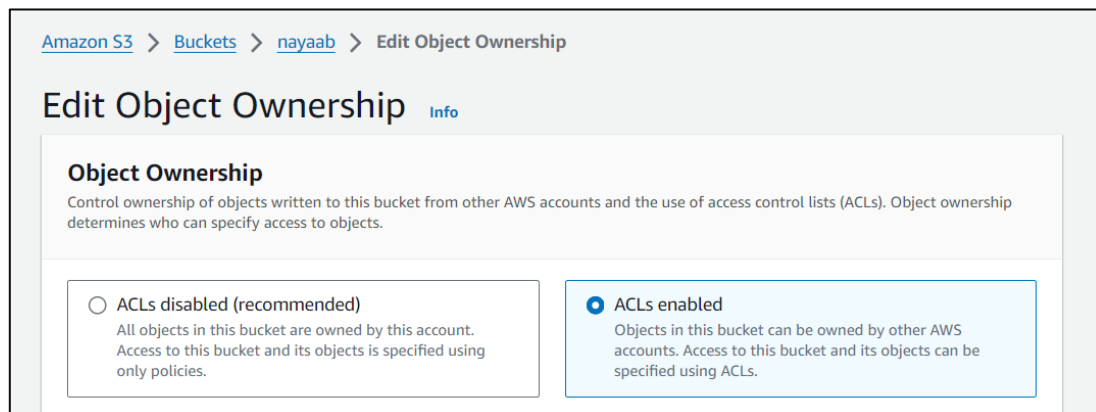
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access 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.

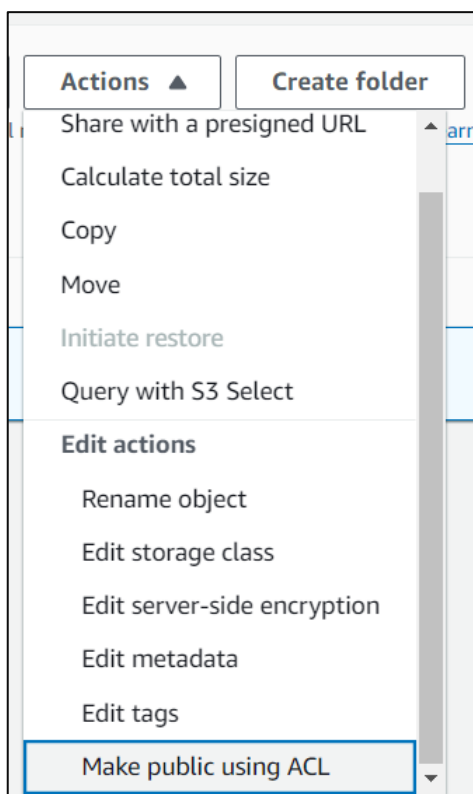
- ☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing 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.

- Now we have to make all objects related to our website publicly accessible and that can be done in 2 ways: either we can select each object and provide permission or use the bucket policy and provide permission for all files at once.

To select a file and give permission first go to permissions and enable ACL.



Now select the objects related to your website click on actions and then click on make public using ACL. Select make public.



6. Now when you open the URL you will be able to see the website.

