

ELEVATE LABS - TASK #1

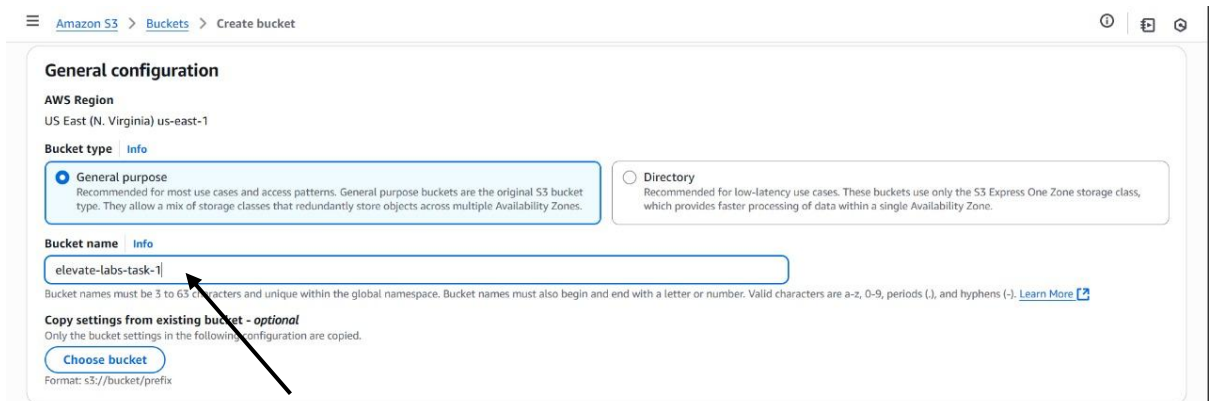
Name: Mohammed Aatef

Gmail: moatif1416@gmail.com

GitHub: <https://github.com/aatef14/Elevate-labs-task-1>

Q. Create s3 bucket in AWS and understand Object storage.

1. Login into Free tier AWS Account and go to s3 from the search bar.
2. Once in the s3 page click on create bucket, you will see something like this:-



Amazon S3 > Buckets > Create bucket

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.

☐ **Directory**
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.

Bucket name [Info](#)

elevate-labs-task-1

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](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

3. Once here, type unique name for the bucket eg- “elevate-labs-task-1”, name must be unique so aws will use it as subdomain.
4. Next, scroll down and untick block public access which will allow us to access the files in the bucket.

Amazon S3 > Buckets > Create bucket

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.

5. Make sure to accept the acknowledgement. And click submit to create the bucket.

Amazon S3 > Buckets

✓ **Successfully created bucket "elevate-labs-task-1"**
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

General purpose buckets All AWS Regions
Directory buckets

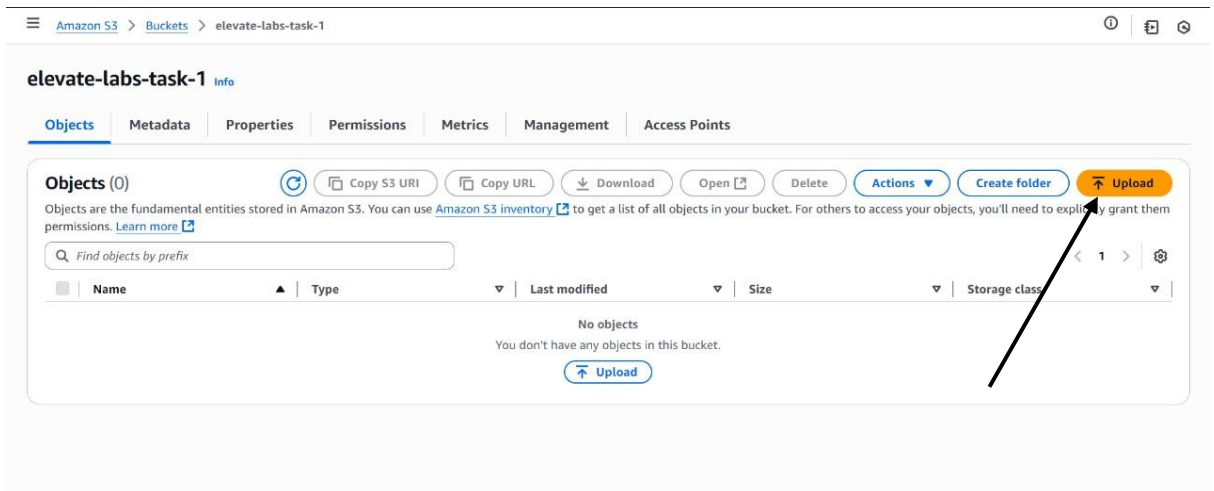
General purpose buckets (1) [Info](#)
🔄
📄 Copy ARN
Empty
Delete
Create bucket

Buckets are containers for data stored in S3.

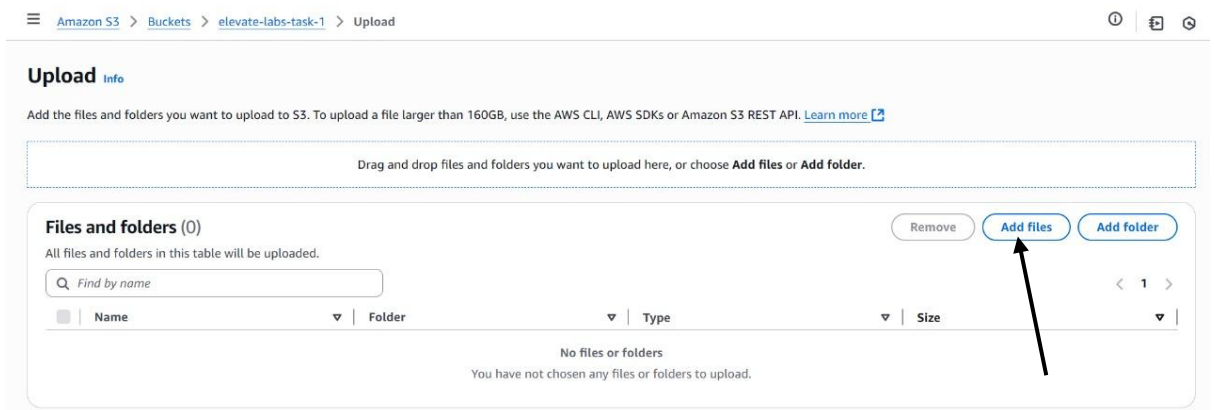
< 1 > ⚙️

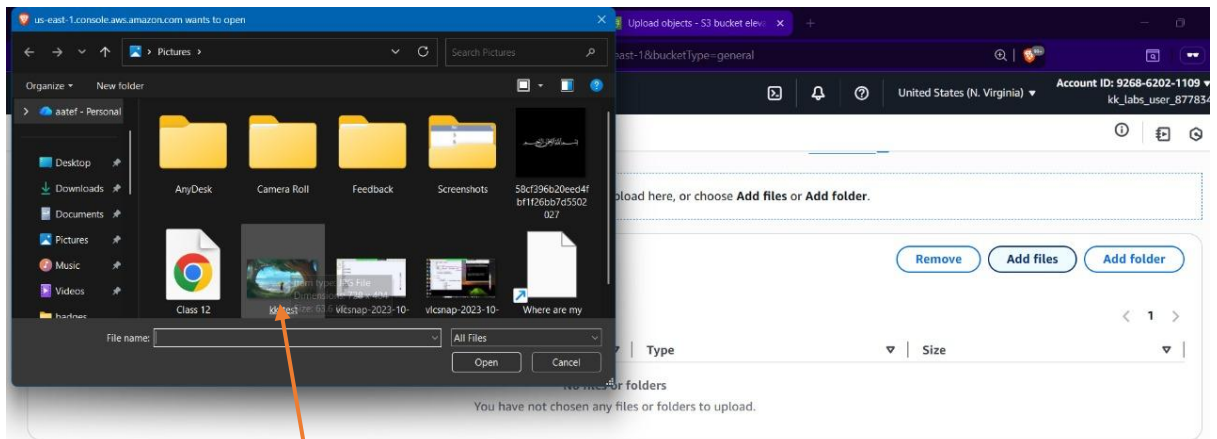
Name	AWS Region	Creation date
<input type="radio"/> elevate-labs-task-1	US East (N. Virginia) us-east-1	October 20, 2025, 12:53:34 (UTC+05:30)

6. Bucket will be created click on it and will open a page which allows to upload files (object).

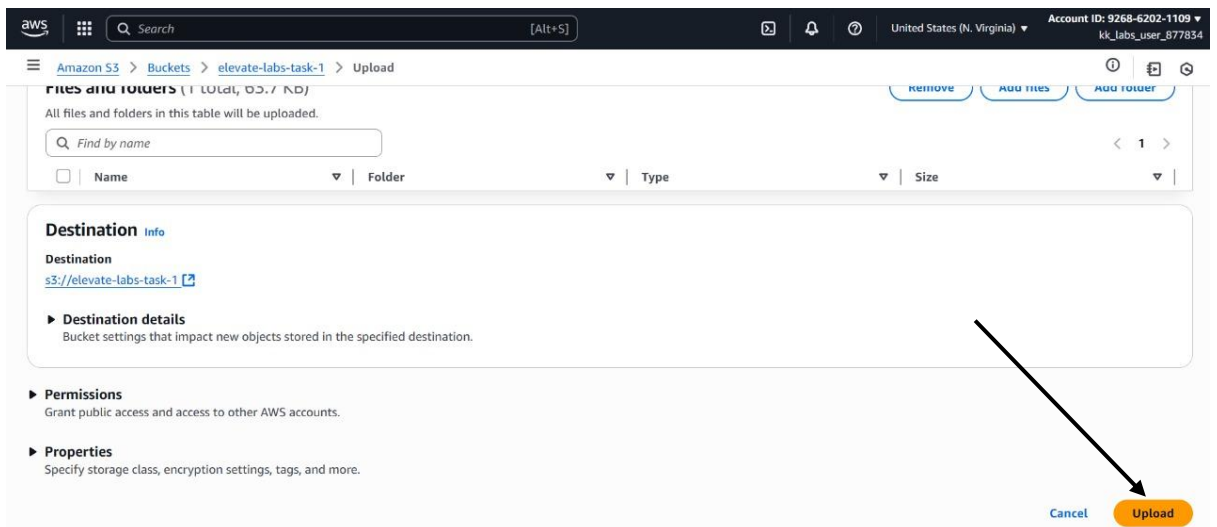


7. Click on upload and select files from your local machine.

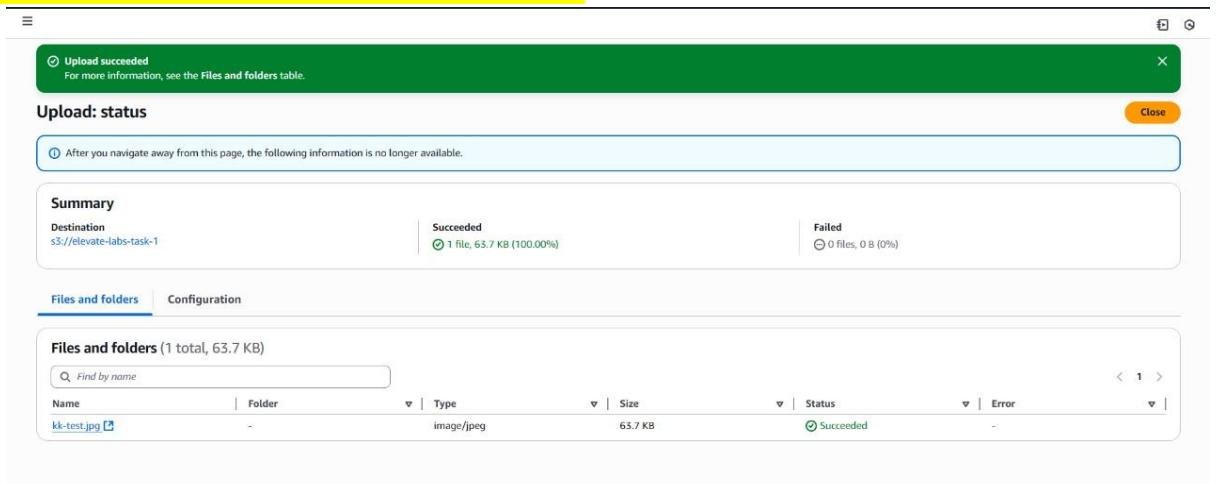




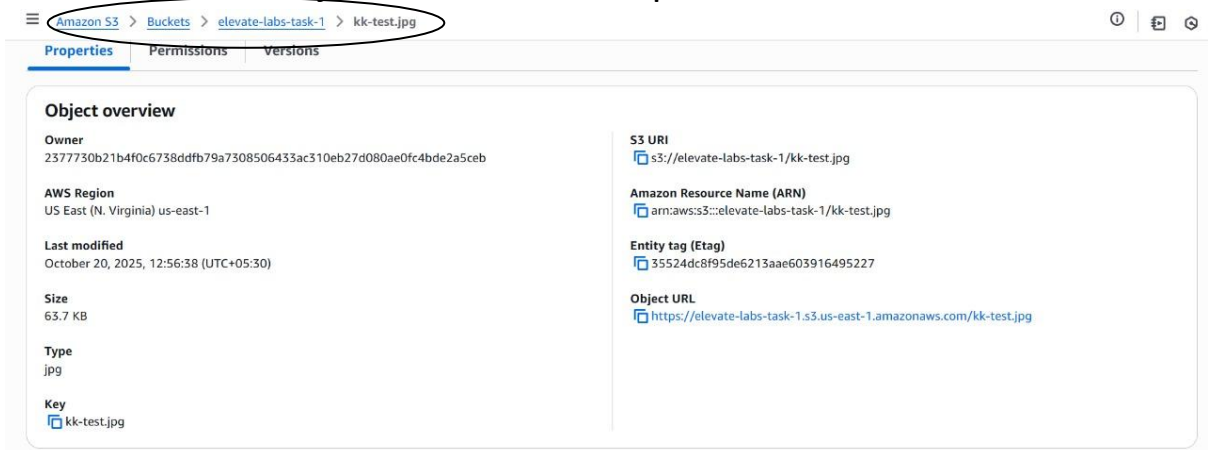
8. Once file selected click on “UPLOAD”



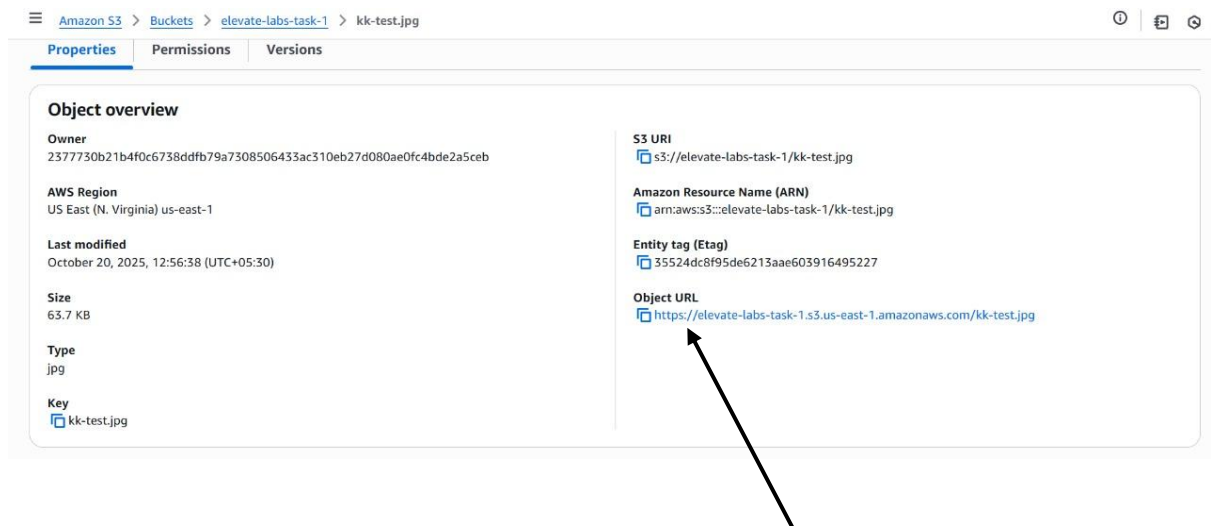
9. File will be uploaded successfully.



10. Go to the object file which we uploaded inside the bucket.



11. You will get Object URL.



12. In our example we got

<https://elevate-labs-task-1.s3.us-east-1.amazonaws.com/kk-test.jpg>

This defines bucket-name-which has to be unique to act as a subdomain.

<https://elevate-labs-task-1.s3.us-east-1.amazonaws.com/kk-test.jpg>

This define which aws service, in this case its AWS S3.

<https://elevate-labs-task-1.s3.us-east-1.amazonaws.com/kk-test.jpg>

This define location eg- us-east-1

<https://elevate-labs-task-1.s3.us-east-1.amazonaws.com/kk-test.jpg>

The main amazon AWS domain.

<https://elevate-labs-task-1.s3.us-east-1.amazonaws.com/kk-test.jpg>

The path or uri of our actual object.

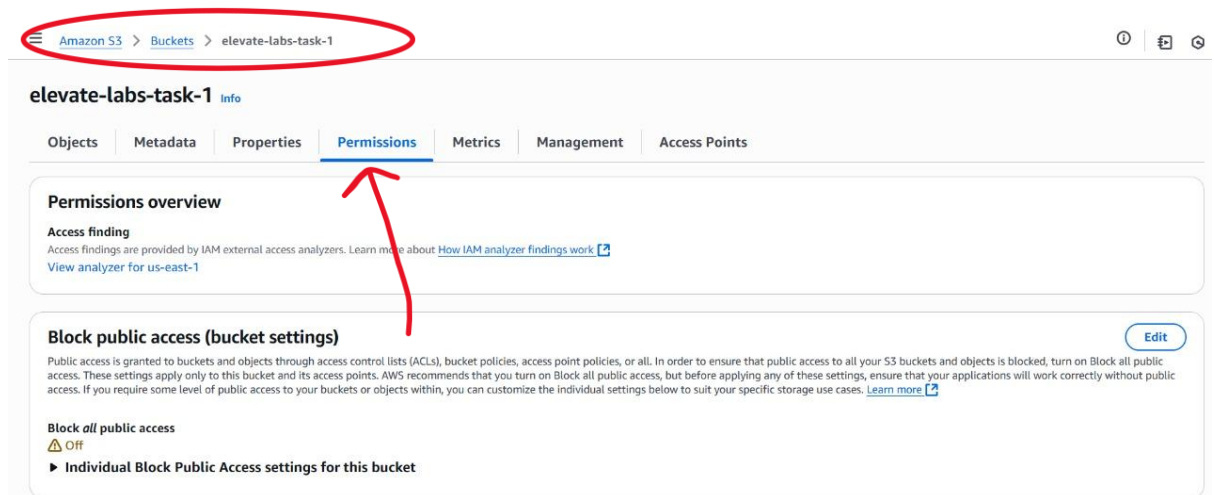
Now, lets try to access the URL from a browser.

13. When truing to access the url from browser we are getting Access denied error. Even though we have allowed public access for all in set "4".

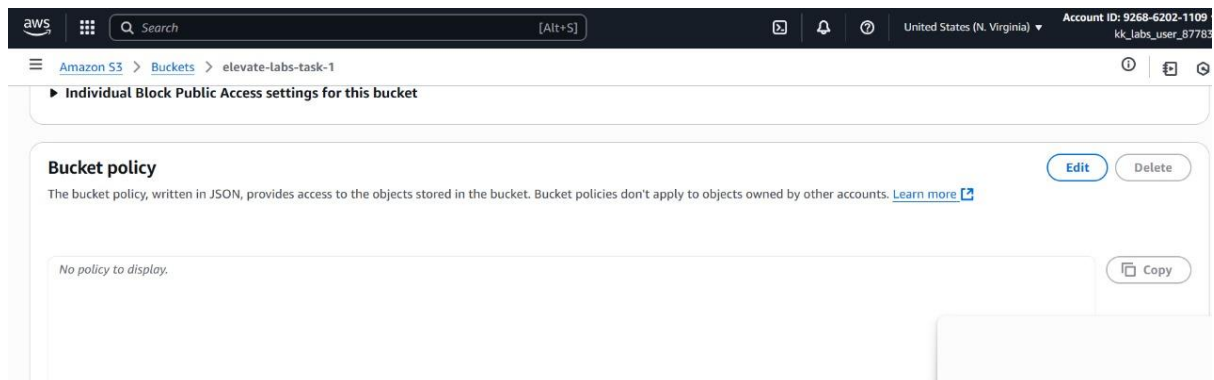


14. That's expected because public access is enabled but to actually access the object we need "GET" api permission.

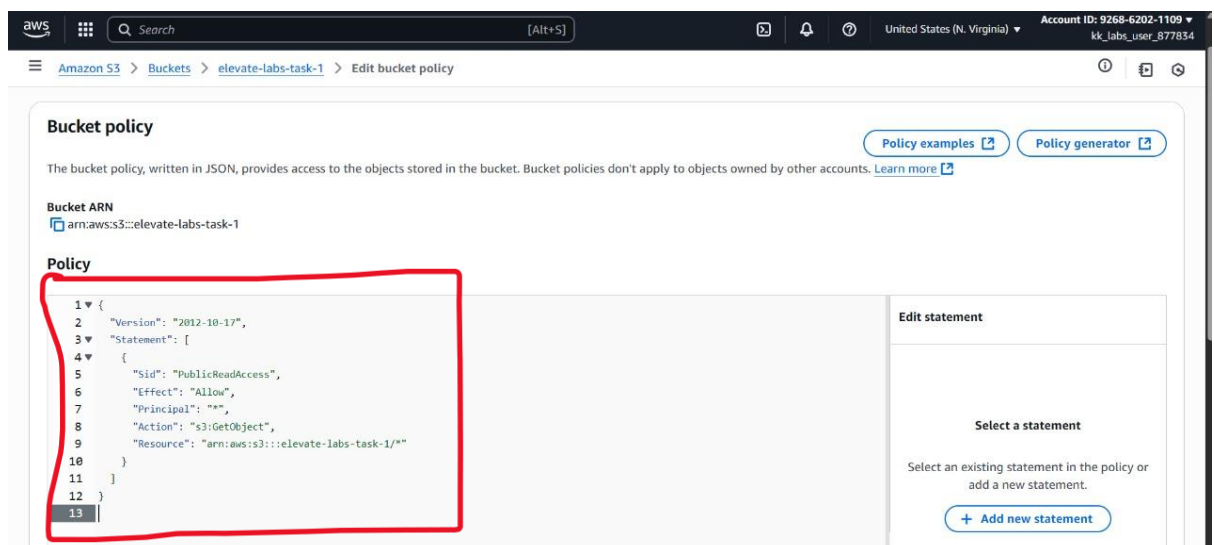
15. Go to your bucket and navigate to permission tab.



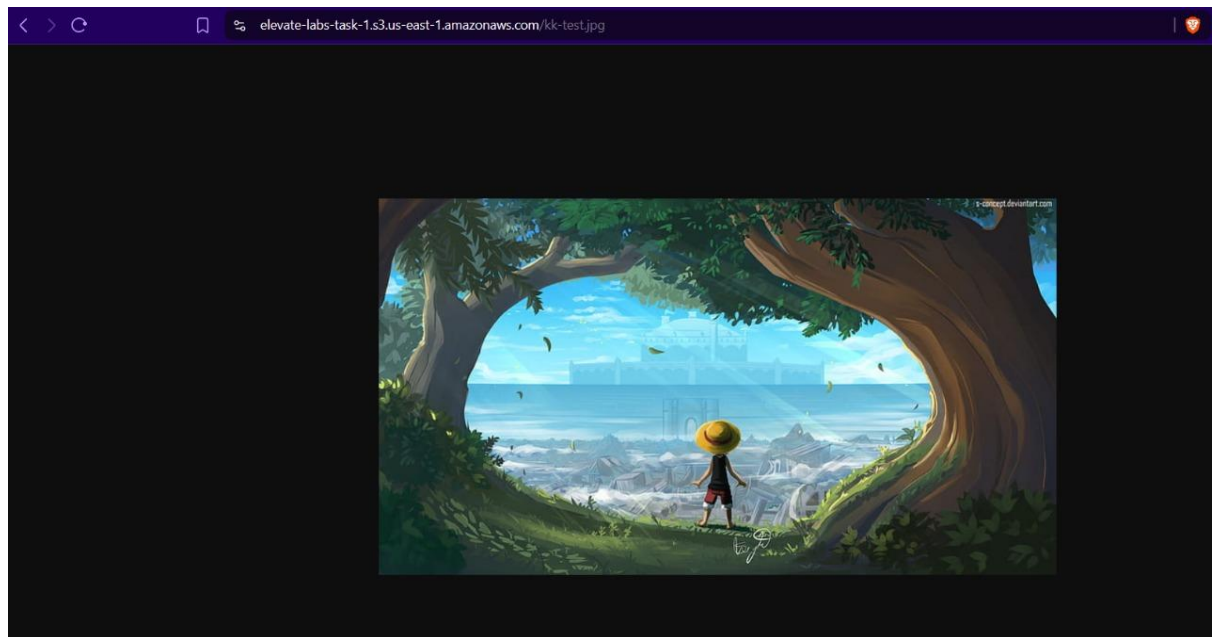
16. Scroll down till you find bucket policy and click on edit.



17. And paste the json policy.



18. Now if we try to access the URL we will be able to see the contents.



----- END -----