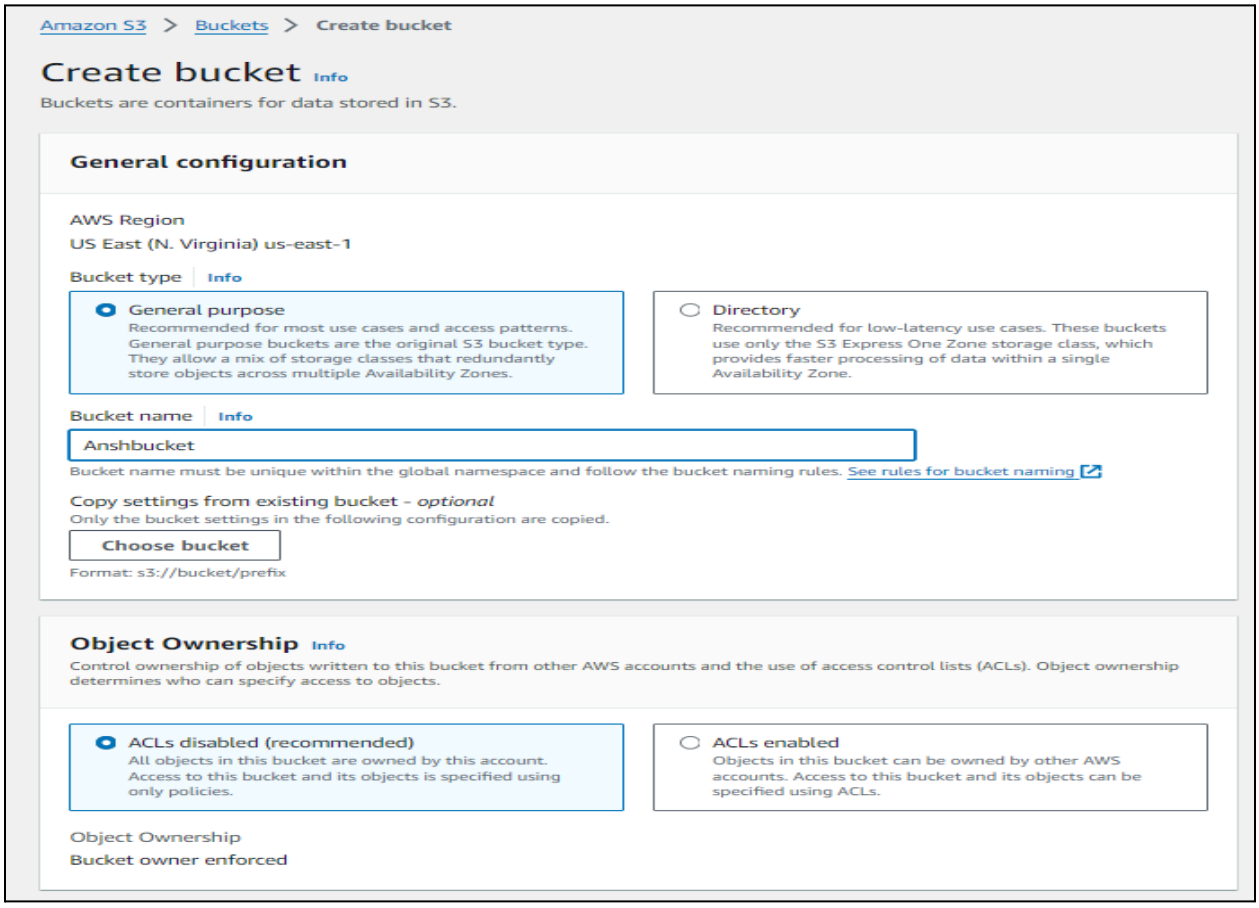
ADVANCE DEVOPS EXP-12

ANSH SARFARE **D15A/50**

Aim: To create a Lambda function which will log “An image has been added” once you add an object to a specific bucket in S3.

Step 1: Login to your AWS Personal account. Now open S3 from services and click on create S3 bucket and create a bucket.

Step 2: Now Give a name to the Bucket, select general purpose project and deselect the Block public access and keep other this to default.



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.

✓ **Successfully created bucket "anshbucketaws"**
To upload files and folders, or to configure additional bucket settings, choose **View details**.

View details

Amazon S3 > Buckets

▸ **Account snapshot** - *updated every 24 hours*
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. 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.

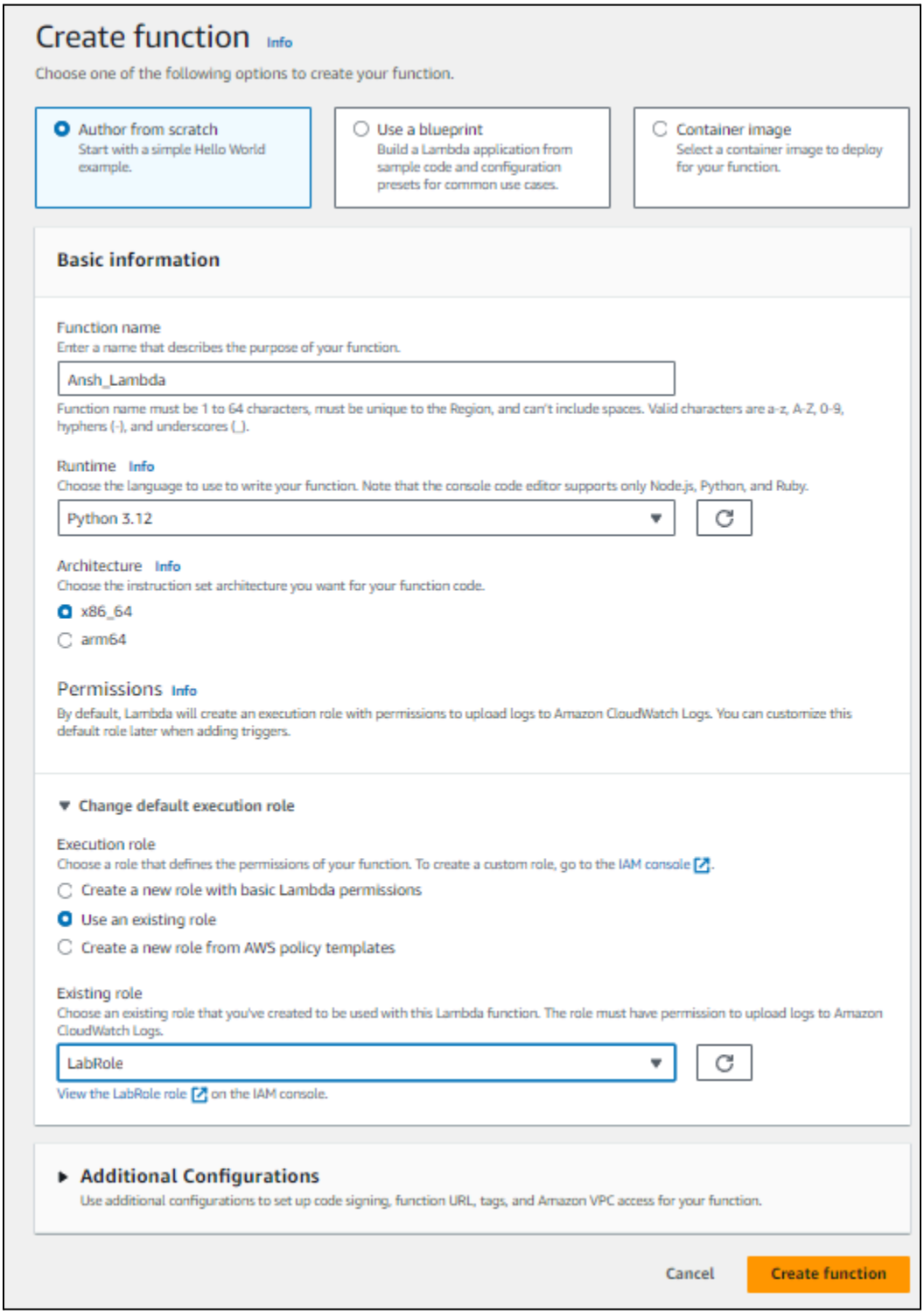
Copy ARN | Empty | Delete | Create bucket

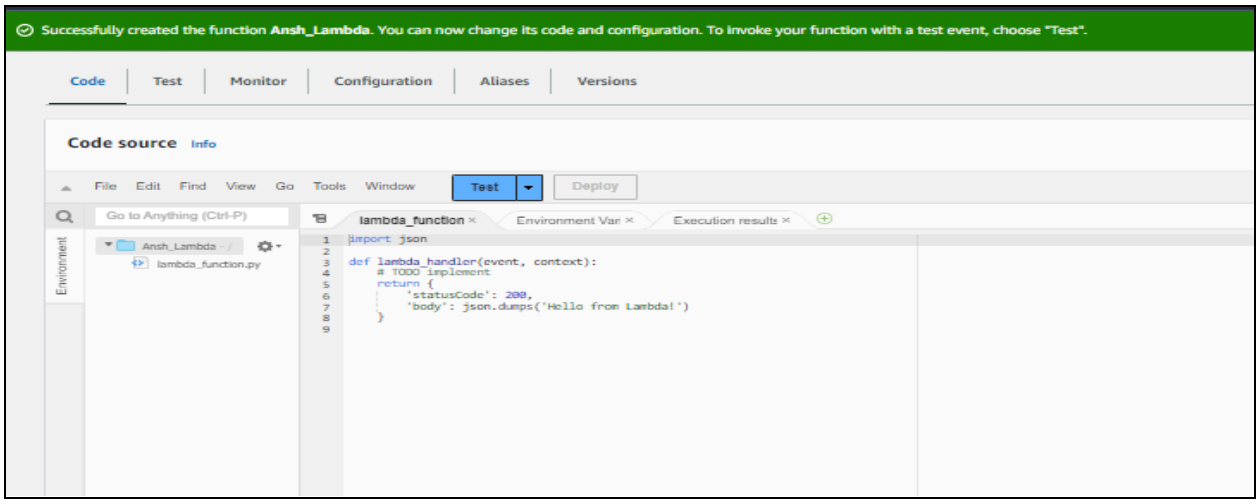
Find buckets by name

1

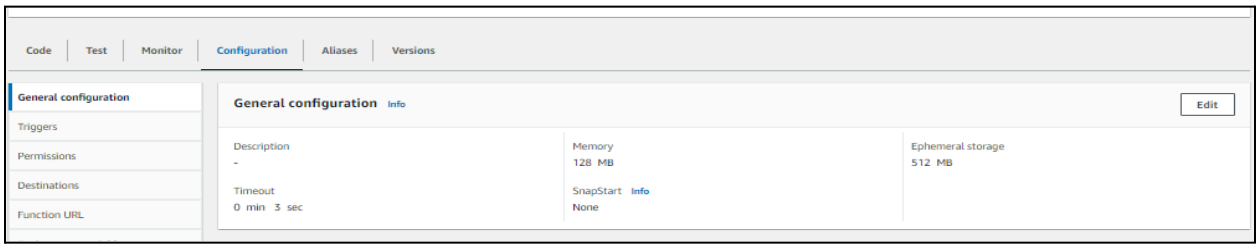
Name	AWS Region	IAM Access Analyzer	Creation date
anshbucketaws	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 4, 2024, 12:35:42 (UTC+05:30)

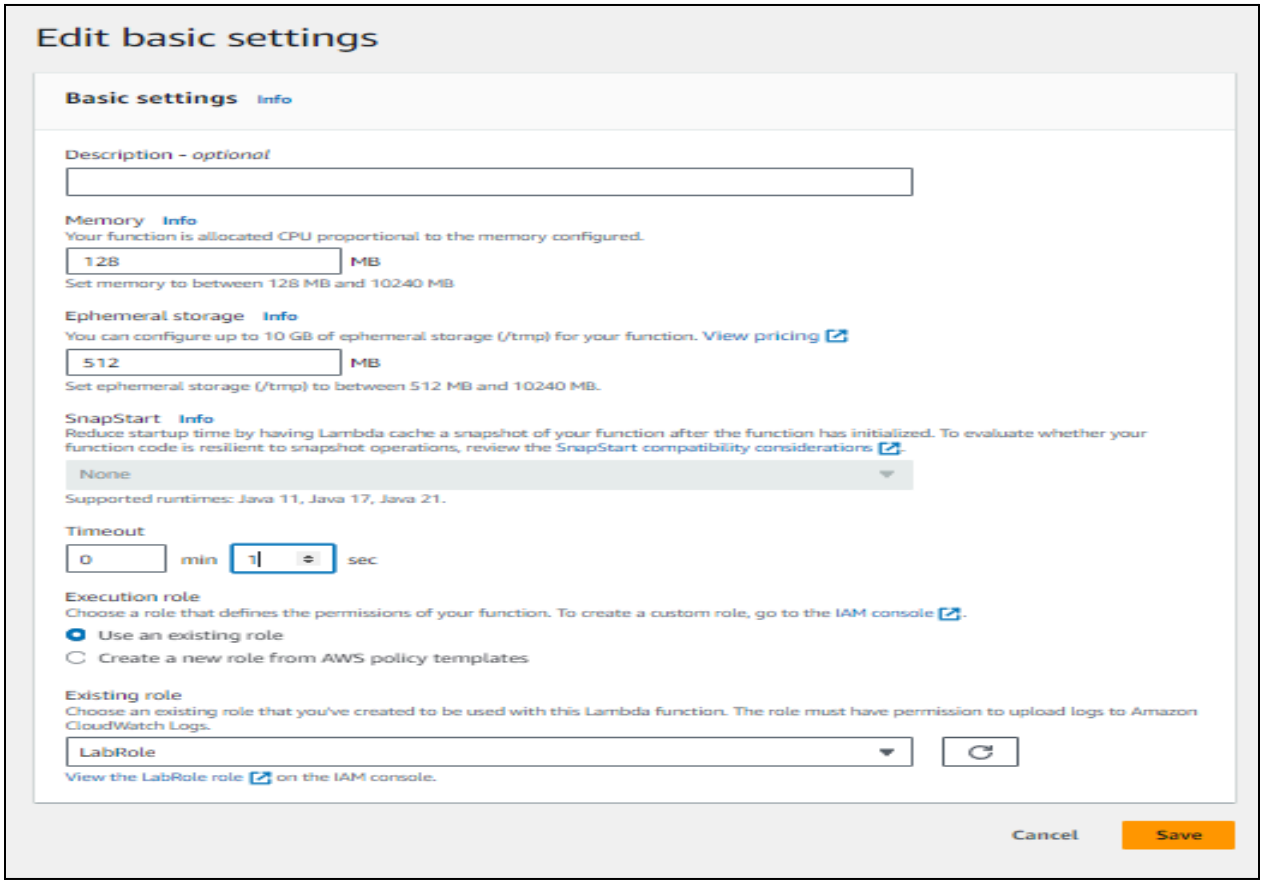
Step 3: Open lambda console and click on create function button.Give a name to your Lambda function, Select the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby. So will select Python 3.12 , Architecture as x86, and existing Execution role



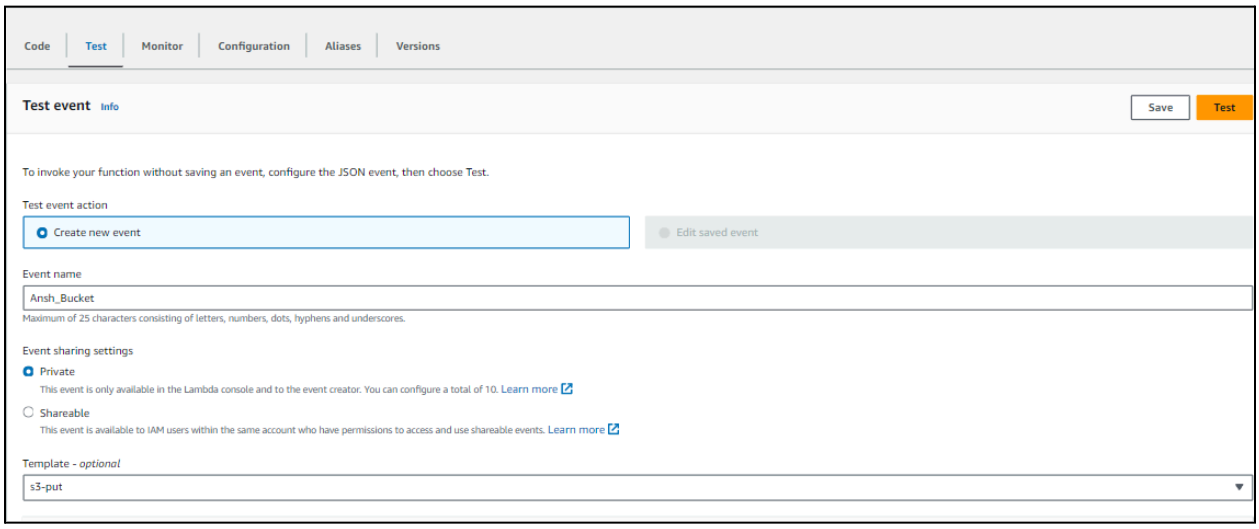


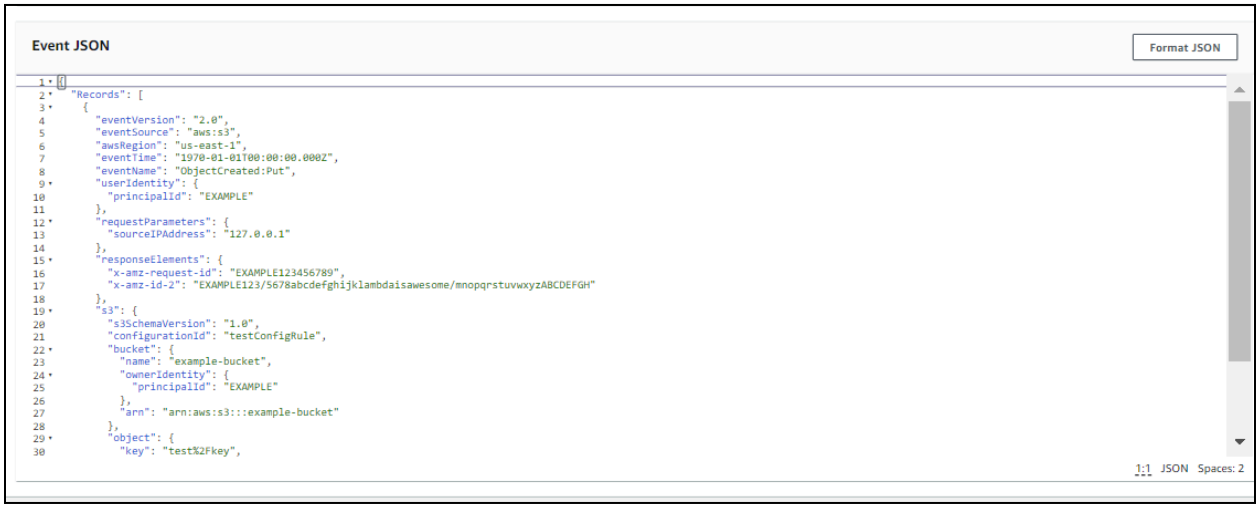
So See or Edit the basic settings go to configuration then click on edit general setting.



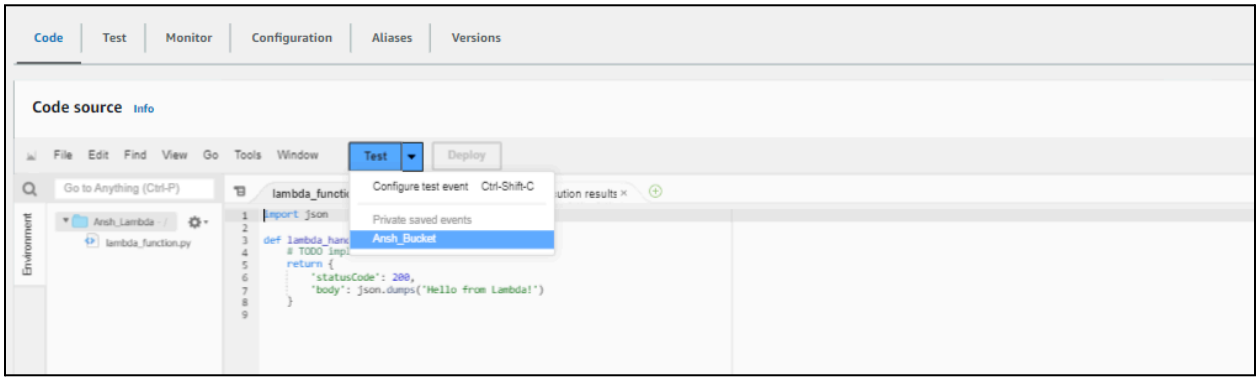


Step 4: Now Click on the Test tab then select Create a new event, give a name to the event and select Event Sharing to private, and select s3 put template.

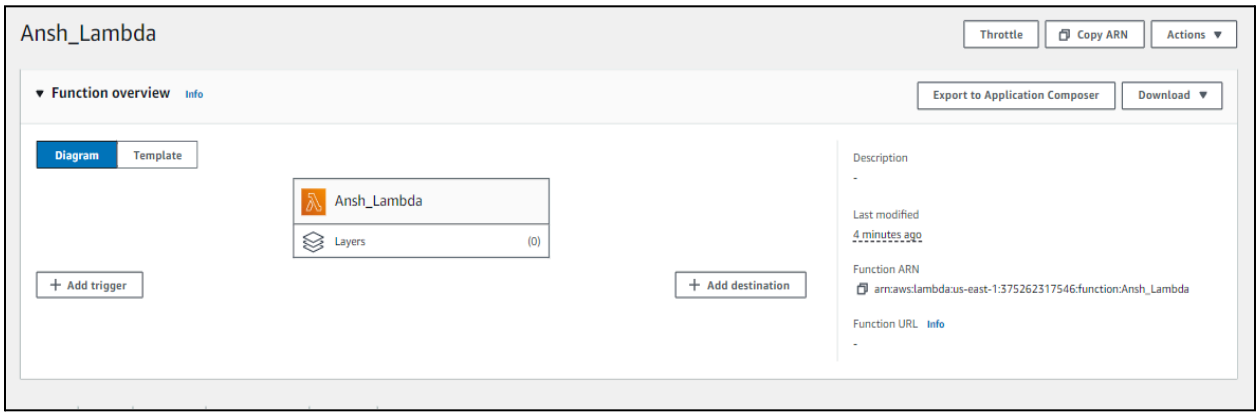




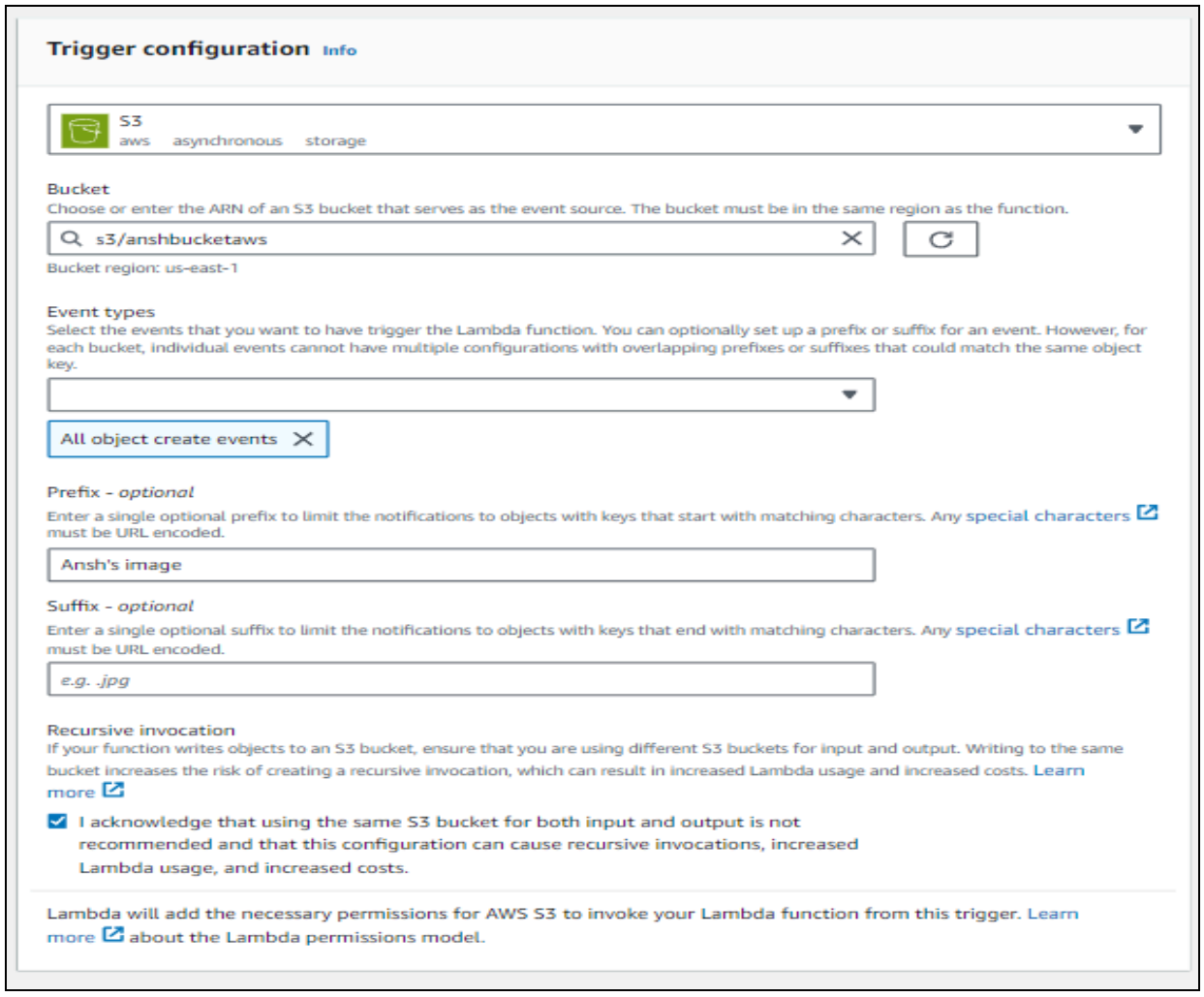
Step 5: Now In Code section select the created event from the dropdown .



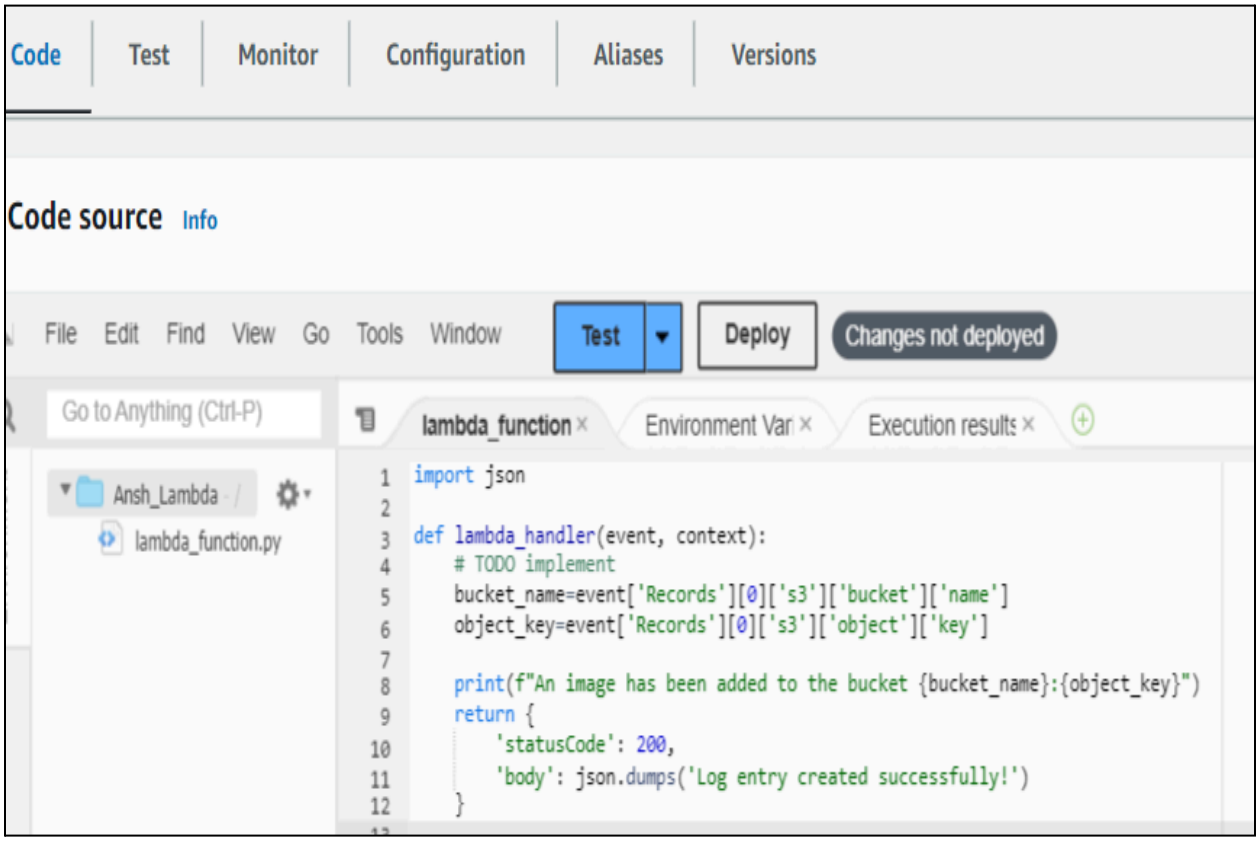
Step 6: Now In the Lambda function click on add tigger.



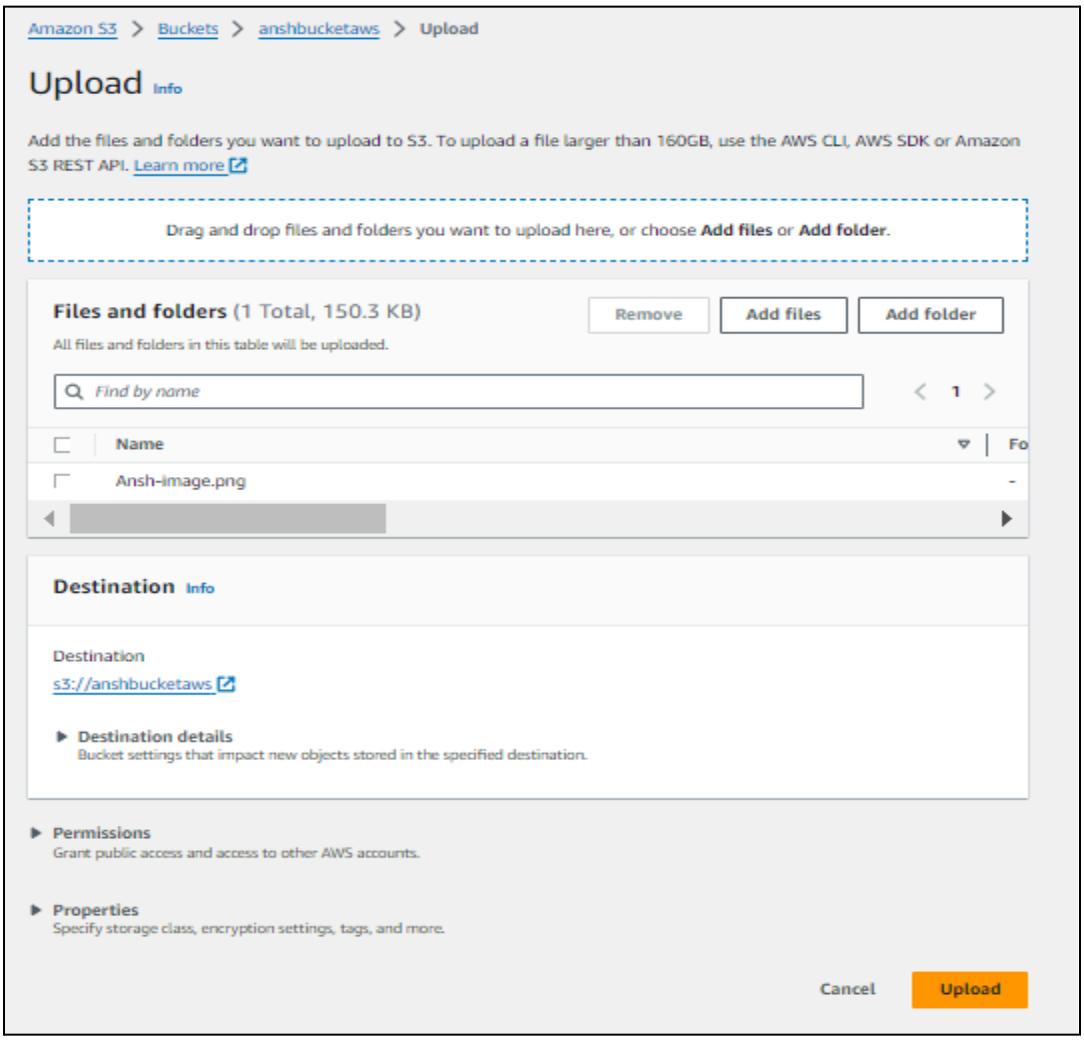
Now select the source as S3 then select the bucket name from the dropdown, keep other things to default and also you can add prefix to image.

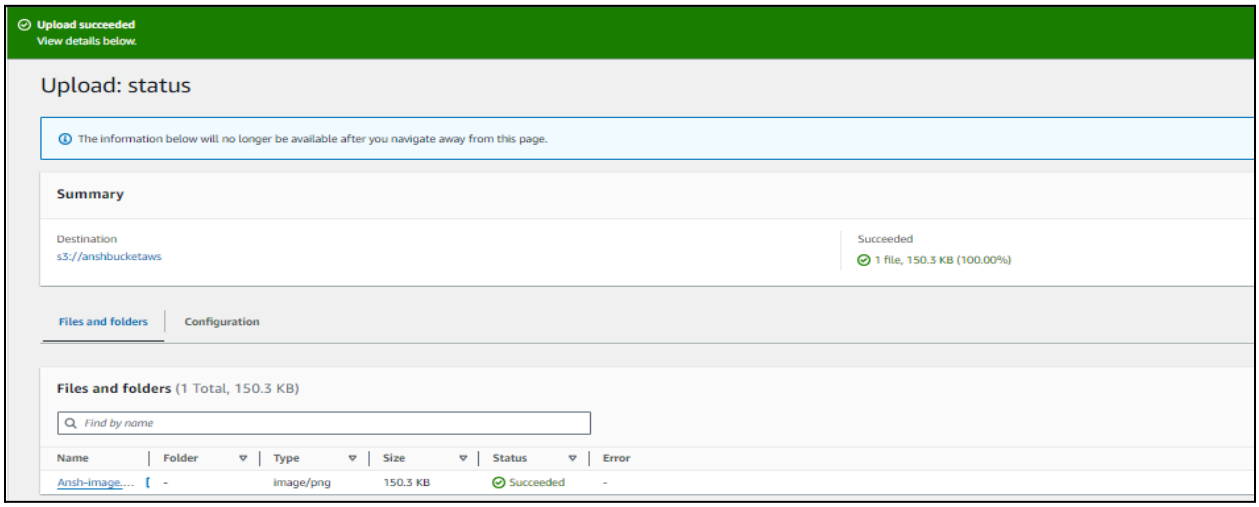


Step 7: Now Write code that logs a message like “An Image has been added” when triggered. Save the file and click on deploy



Step 8: Now upload any image to the bucket





Step 10: Now to click on test in lambda to check whether it is giving log when image is added to S3.

Step 11: Now Lets see the log on Cloud watch.To see it go to monitor section and then click on view cloudwatch logs.