WELCOME

TO

THE PROJECT PRESENTATION

PROJECT 1;

TITLE

- Title: Serverless Image Processing Application
- Subtitle: Automatically Resizing and Optimizing Images on AWS

INTRODUCTION

- Project Overview
- Importance of Image Optimization
- Benefits of Serverless Architecture

OBJECTIVES

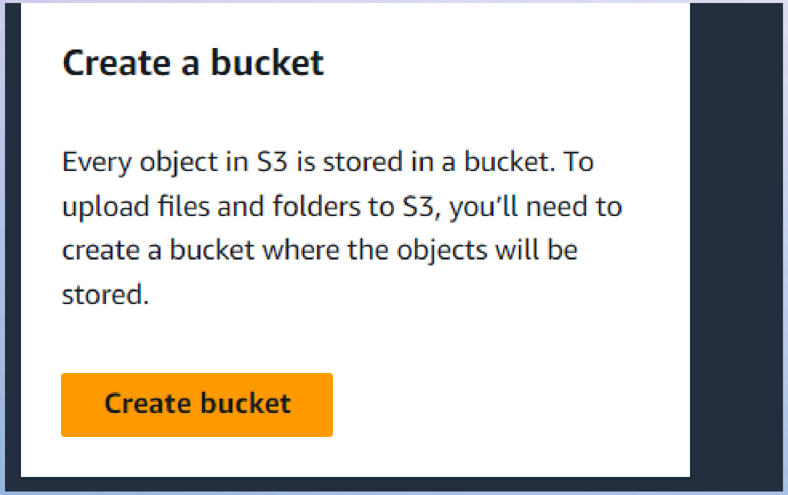
- Learn to Automate Image less Computing
- Demonstrate Image Optimization Workflow
- Processing on AWS
- Understand Benefits of Server

STEP1;

- Log in to the AWS Management Console.
- Navigate to the Amazon S3 service.
- Click on "Create bucket" and follow the prompts to create a new bucket

STEP 2 ;

CREATE AN S3 BUCKET;

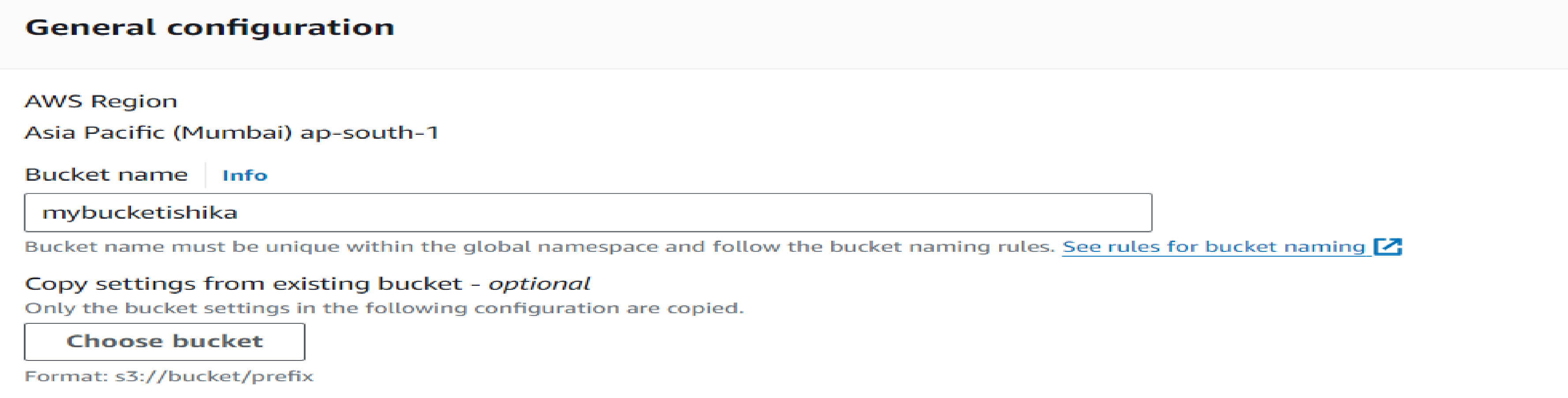


Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

STEP 3 ;

Explanation of amazon s3 bucket creation;



General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket name | Info

mybucketishika

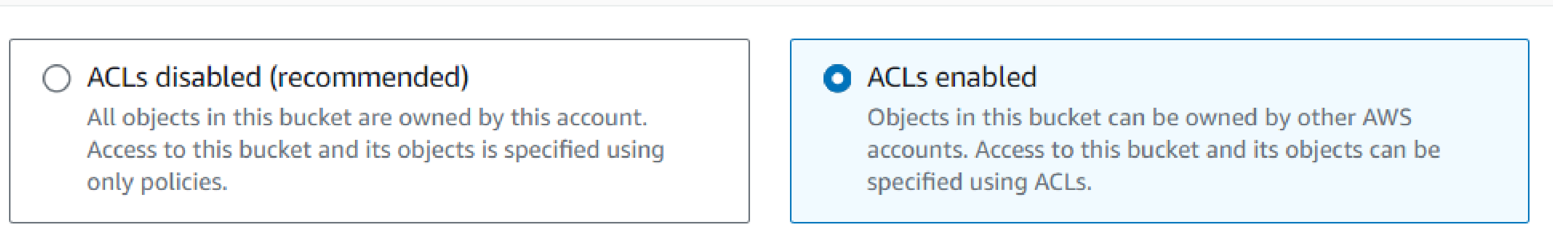
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

Click on acls ;



○ ACLs disabled (recommended)

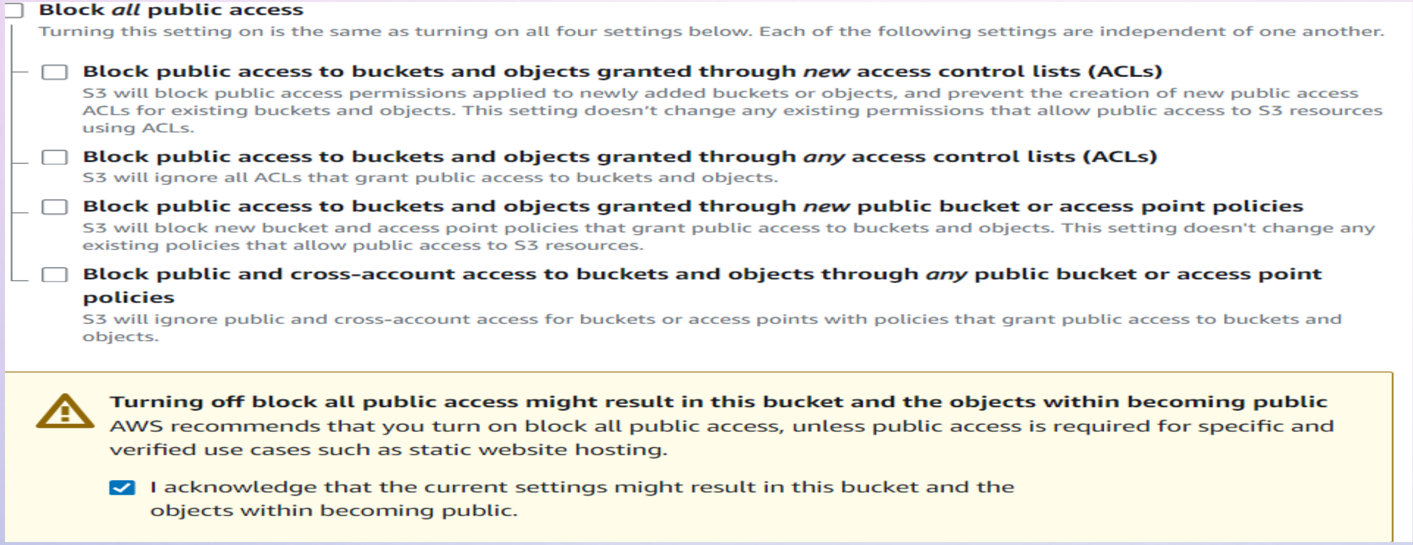
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

● 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.

STEP 4;

then block all access;



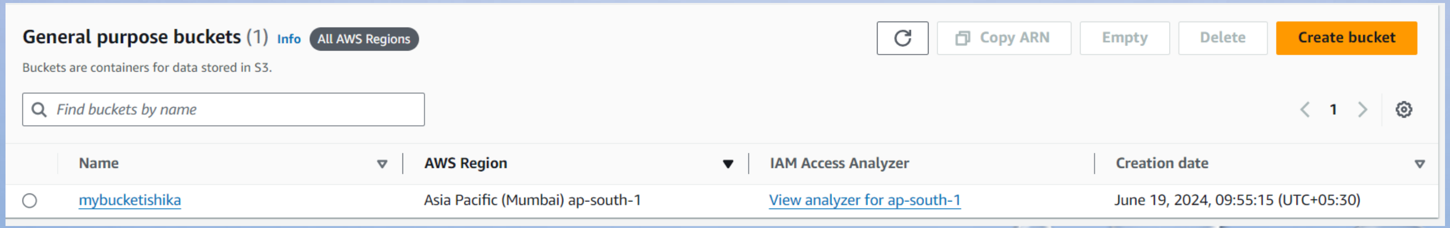
□ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- □ **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.

STEP 5 ;
BUCKET CREATE;

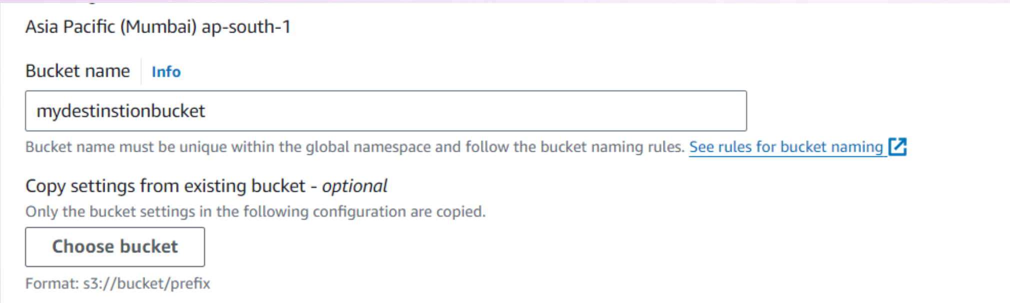


General purpose buckets (1) Info All AWS Regions
Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	mybucketishika	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	June 19, 2024, 09:55:15 (UTC+05:30)

STEP 6;

create an s3 destination bucket ;


Asia Pacific (Mumbai) ap-south-1

Bucket name Info

mydestinstionbucket

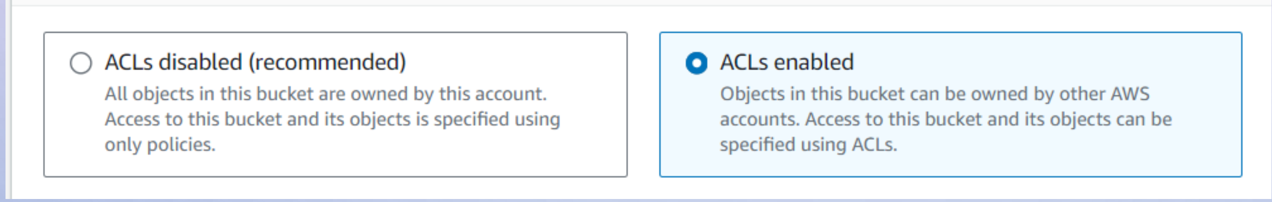
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

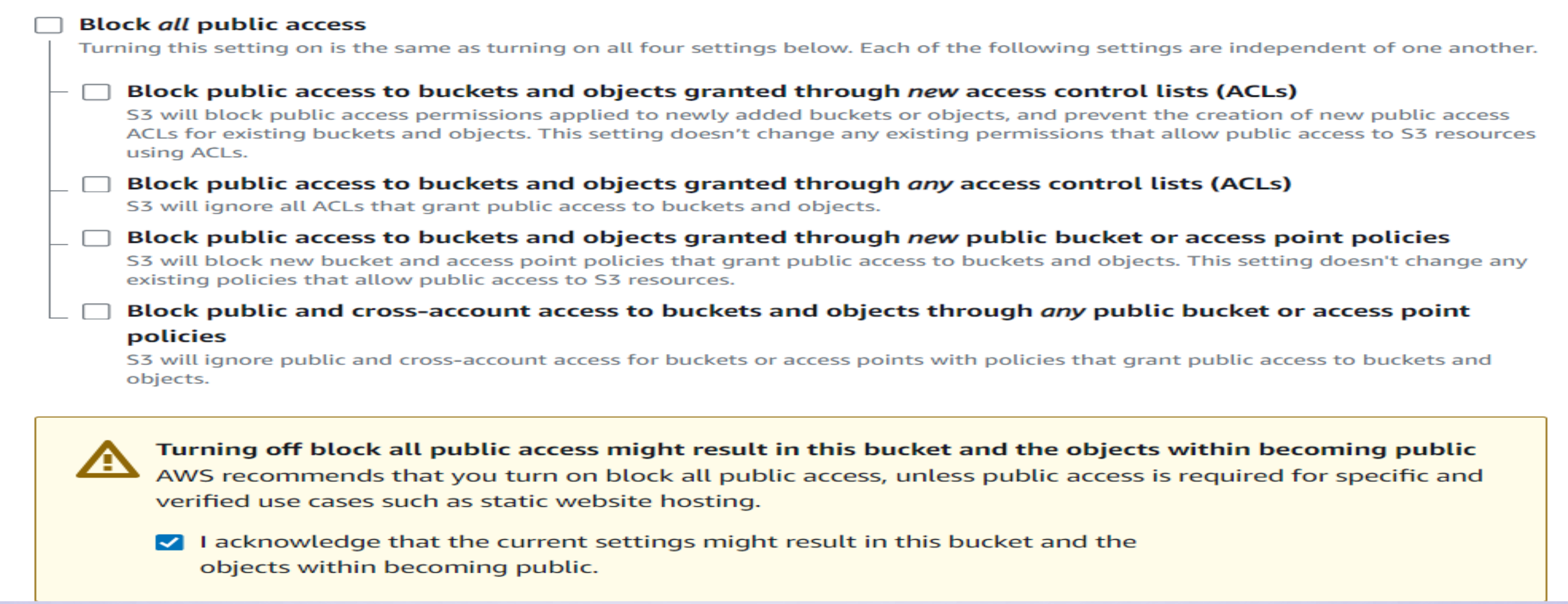
Click on acls


○ 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.

STEP 7;

then block all access ;



□ **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.

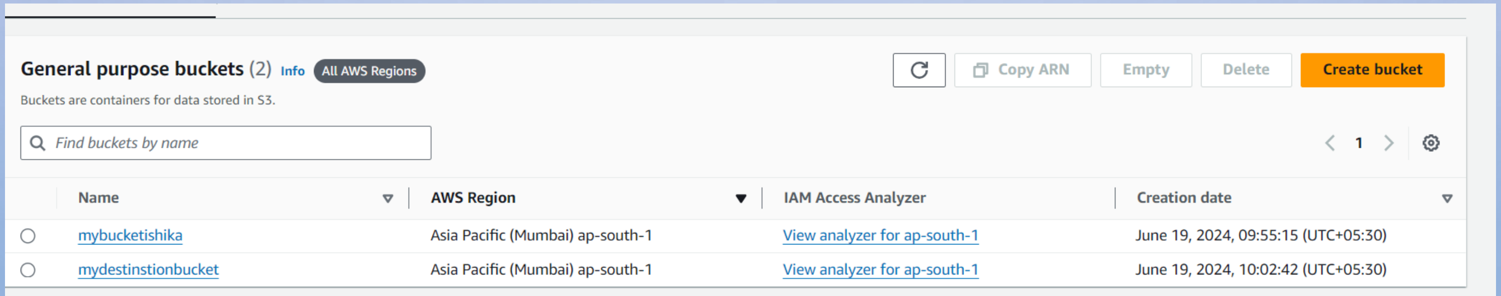
- □ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any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

STEP 8 ;

After 2bucket create;



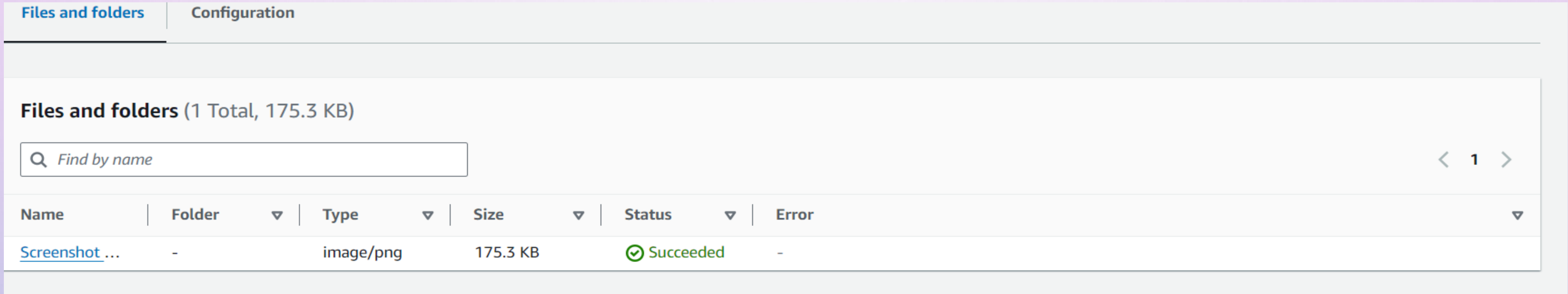
General purpose buckets (2)

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	mybucketishika	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	June 19, 2024, 09:55:15 (UTC+05:30)
○	mydestinstionbucket	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	June 19, 2024, 10:02:42 (UTC+05:30)

STEP 9;

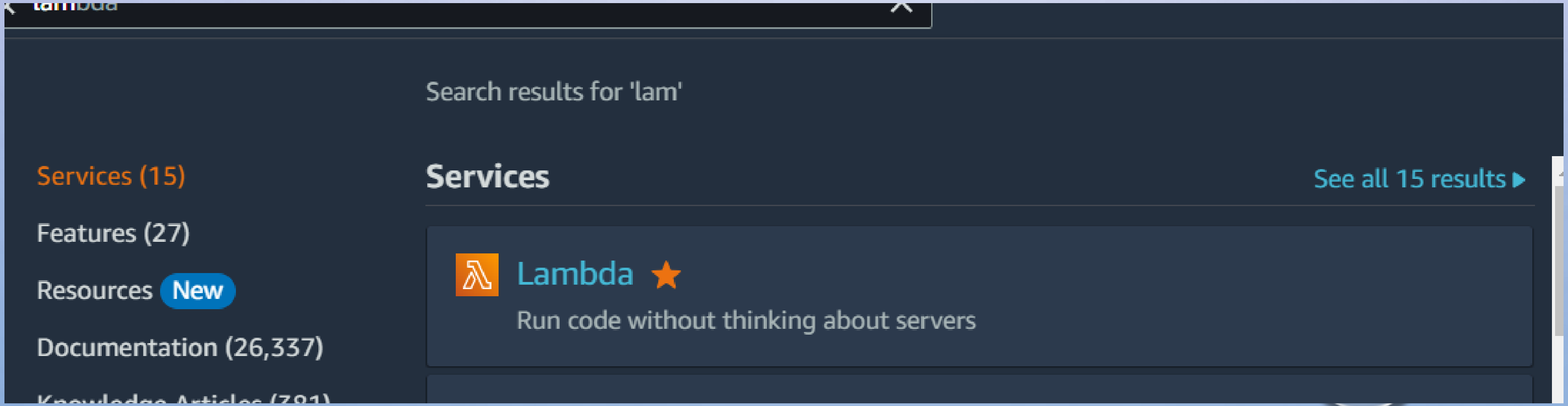
CONFIGURATION FOR STORING UPLOADED IMAGES



Files and folders (1 Total, 175.3 KB)

Name	Folder	Type	Size	Status	Error
Screenshot ...	-	image/png	175.3 KB	✓ Succeeded	-

SEARCH A LAMBDA FUNCTION ;



Search results for 'lam'

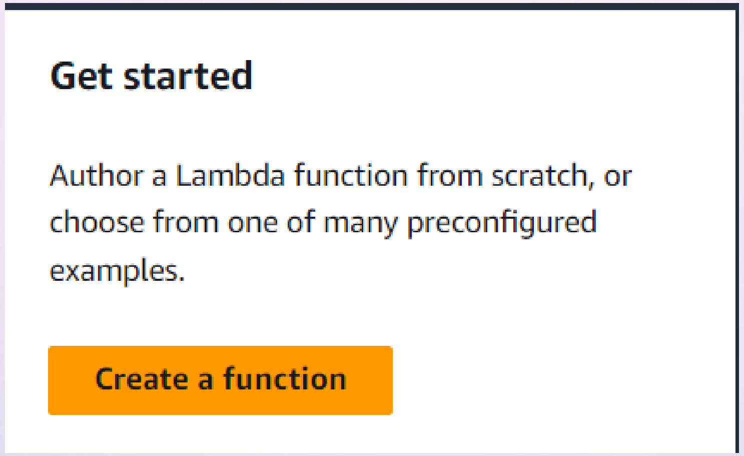
Run code without thinking about servers

STEP 10 : AWS LAMBDA FUNCTION

- Purpose of AWS Lambda in the architecture
- Programming language (e.g., Node.js, Python)
- Functionality:
- Image resizing using libraries like sharp (Node.js) or PIL (Python)
- Image optimization using tools like imagemin or AWS services like Amazon S3 Image

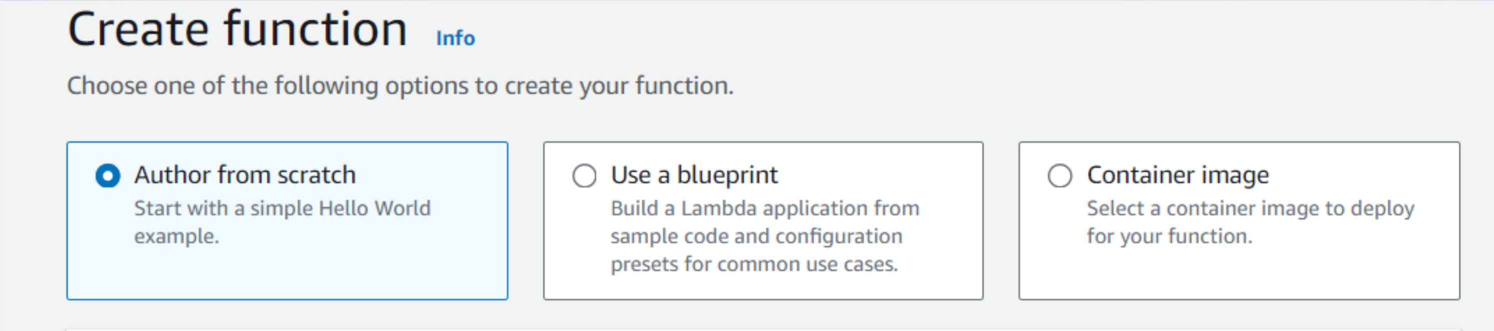
STEP 11;

CREATE A FUNCTION ;



Get started

Author a Lambda function from scratch, or choose from one of many preconfigured examples.



Create function

Choose one of the following options to create your function.

● Author from scratch
Start with a simple Hello World example.

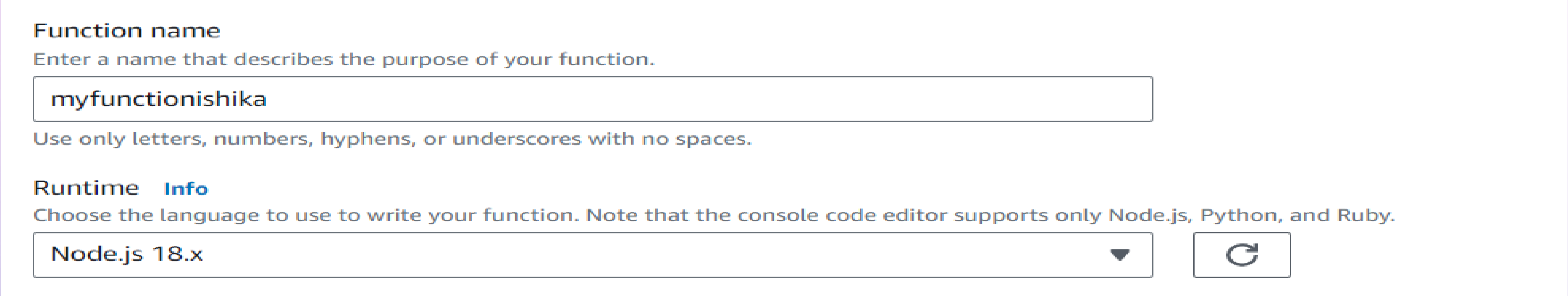
○ Use a blueprint
Build a Lambda application from sample code and configuration presets for common use cases.

○ Container image
Select a container image to deploy for your function.

STEP 12;

Create AWS Lambda Function;

Explanation of function creation ;



Function name

Enter a name that describes the purpose of your function.

myfunctionishika

Use only letters, numbers, hyphens, or underscores with no spaces.

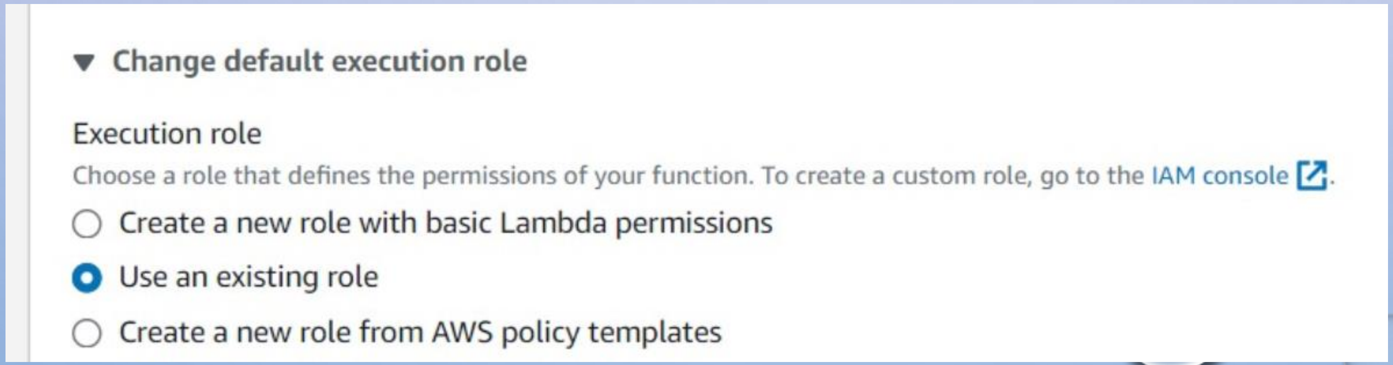
Runtime Info

Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.

Node.js 18.x

LAMBDA EXECUTION ROLE;

Create an IAM role for your lambda function with permissions to read from
The source s3 bucket and write to the destination bucket



▼ Change default execution role

Execution role

Choose a role that defines the permissions of your function. To create a custom role, go to the IAM console.

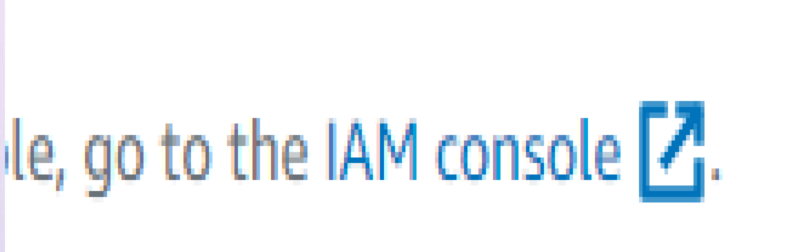
○ Create a new role with basic Lambda permissions

● Use an existing role

○ Create a new role from AWS policy templates

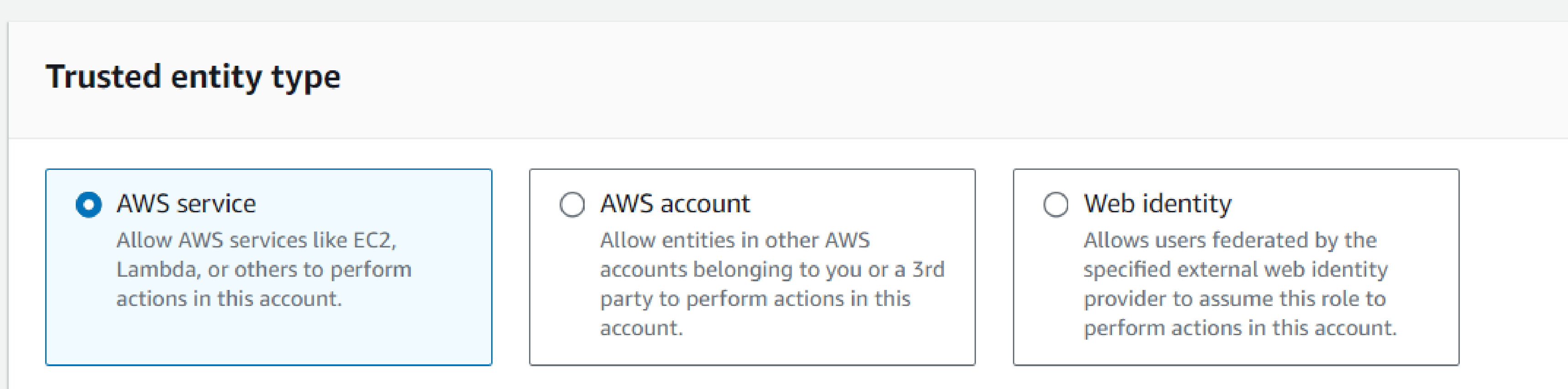
STEP 13 ;

Click on IAM console ;



le, go to the IAM console .

Select a AWS service



Trusted entity type

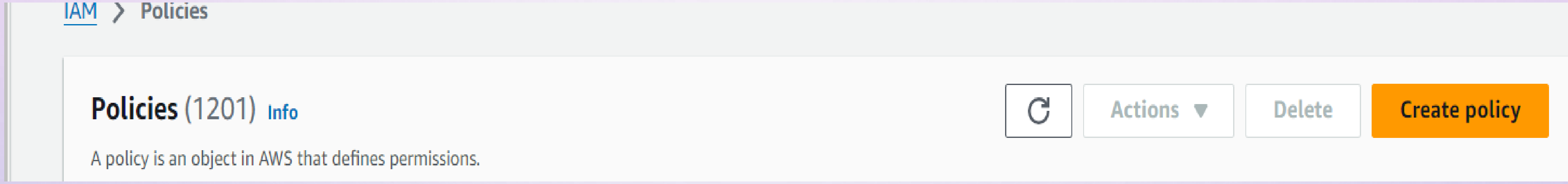
● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

STEP 14 ;

Then create policy;

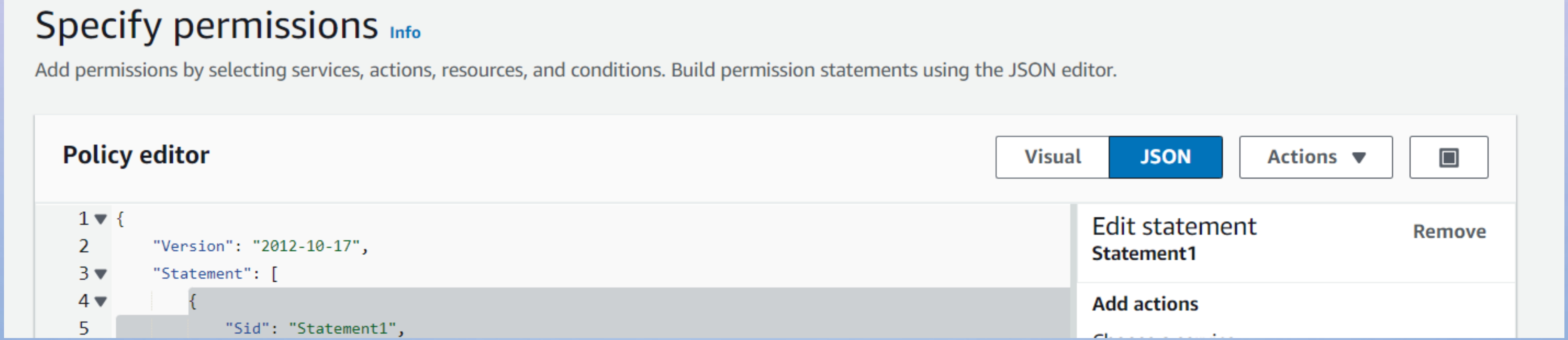


Policies (1201) Info

A policy is an object in AWS that defines permissions.

STEP 15;

Then go to JSON;



Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

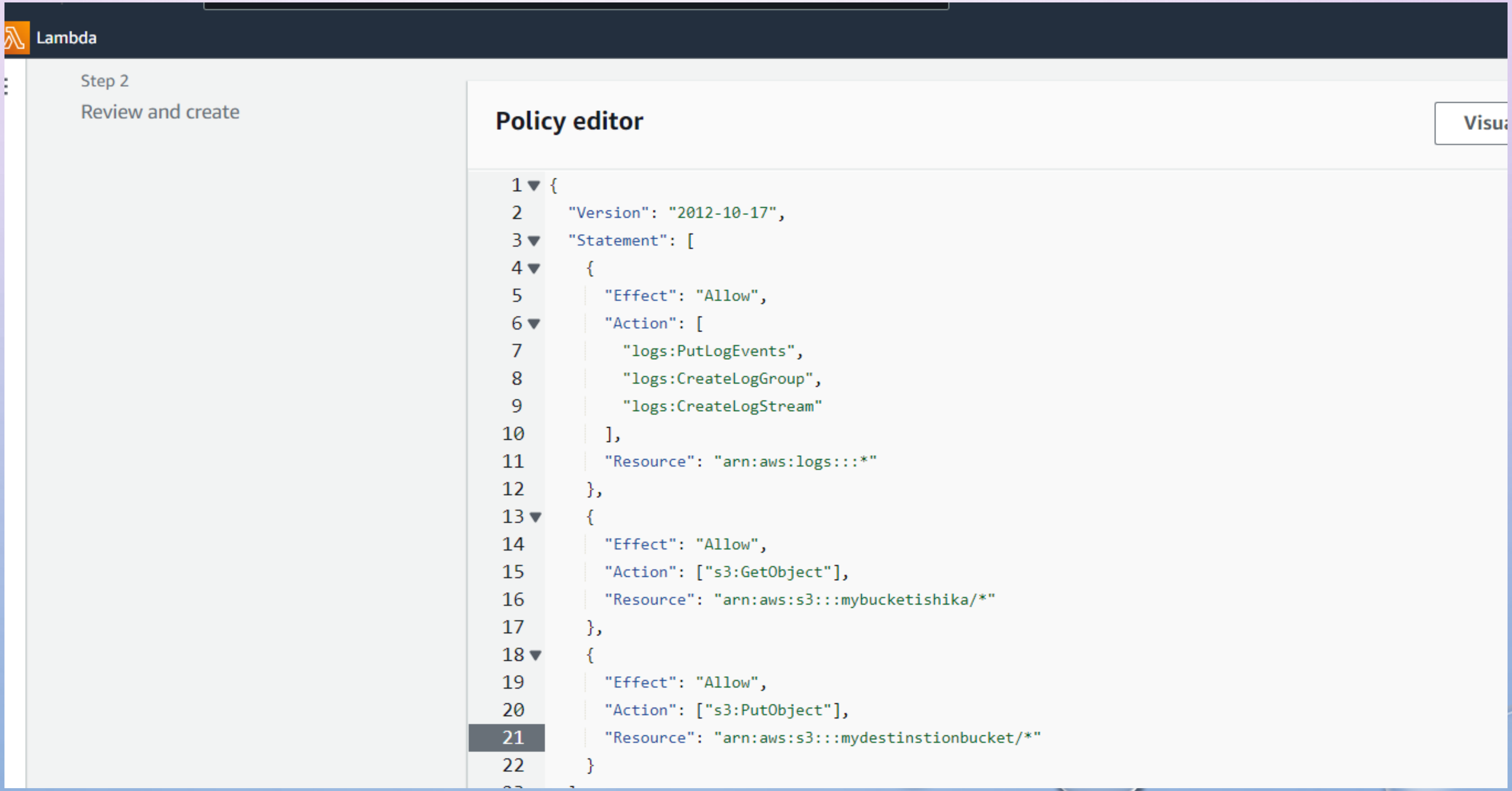
Policy editor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
```

Edit statement
Statement1

STEP 16;

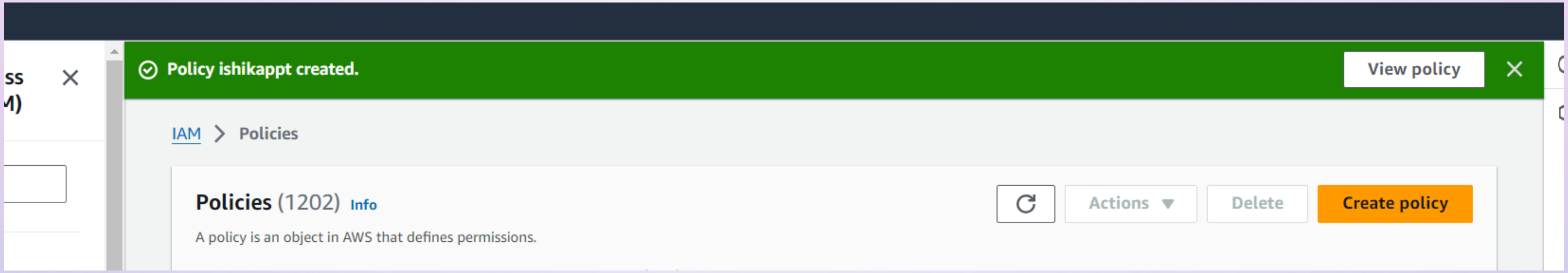
Write the above code in the policy editor



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents",
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource": "arn:aws:logs:::*"
    },
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": "arn:aws:s3:::mybucketishika/*"
    },
    {
      "Effect": "Allow",
      "Action": ["s3:PutObject"],
      "Resource": "arn:aws:s3:::mydestinstionbucket/*"
    }
```

STEP17;

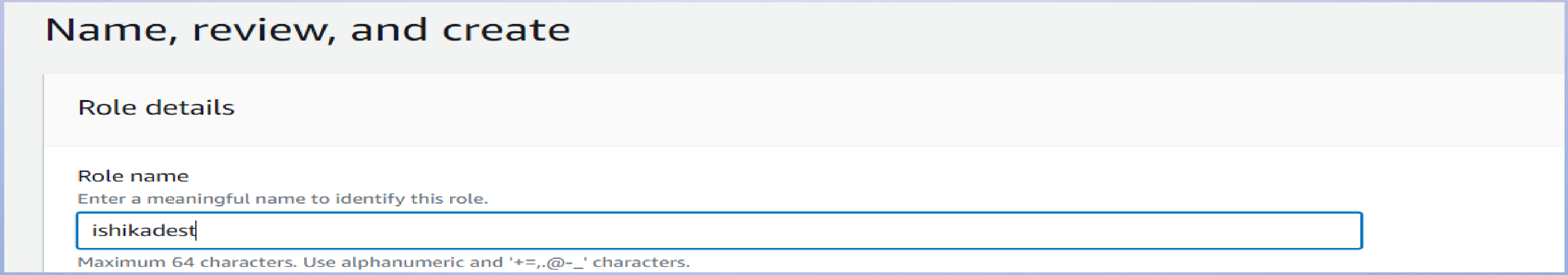
Explanation of create a policy ;



Policy ishikappt created.

Policies (1202) Info

A policy is an object in AWS that defines permissions.



Name, review, and create

Role details

Role name

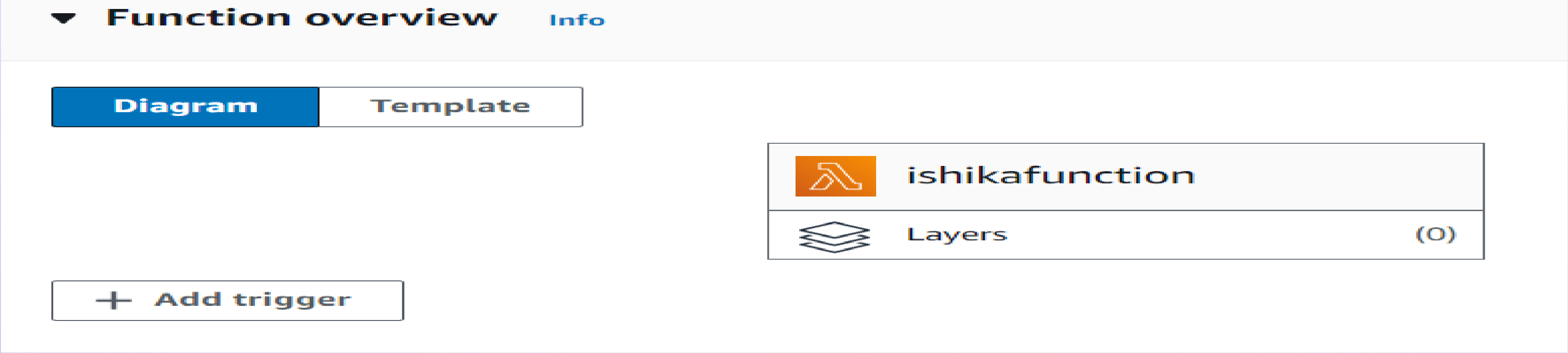
Enter a meaningful name to identify this role.

ishikadest

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

STEP 18;

First click on function overview;



Function overview Info

Diagram Template

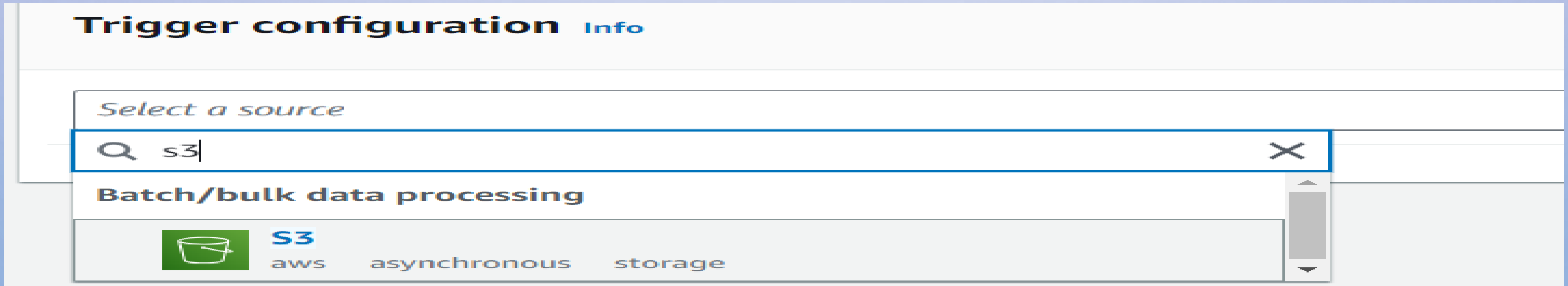
ishikafunction

Layers (0)

+ Add trigger

STEP 19;

After that go to trigger configuration and search s3 bucket ;



Trigger configuration Info

Select a source

s3

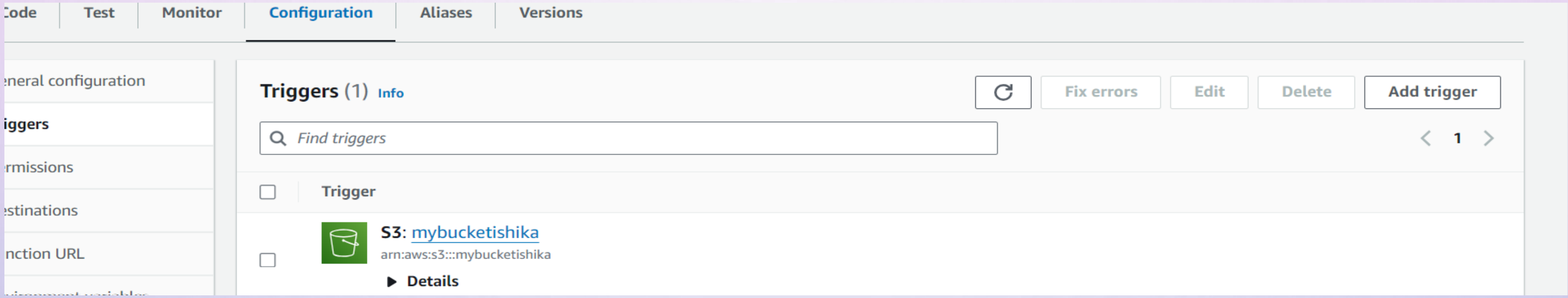
Batch/bulk data processing

S3

aws asynchronous storage

Step 20;

The bucket is now ready ;

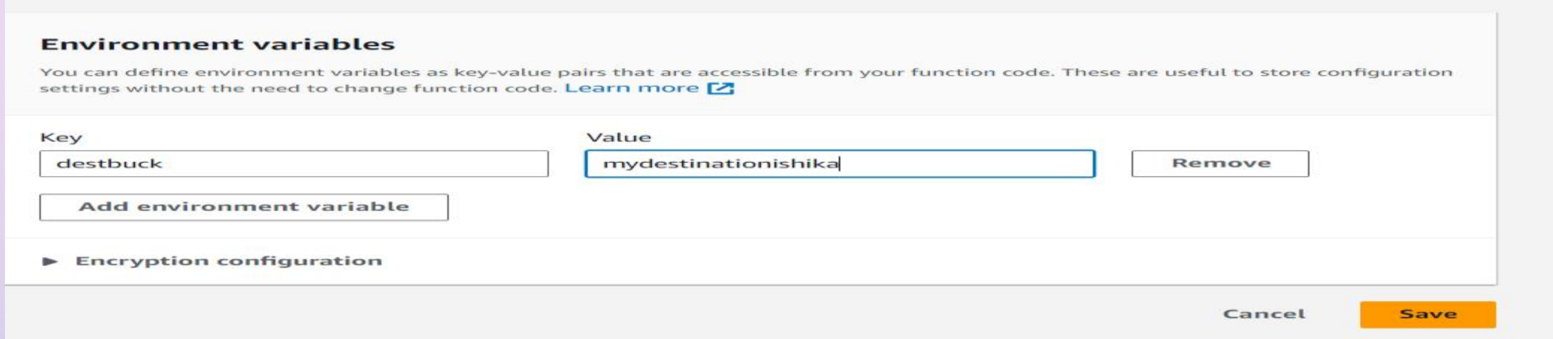


Triggers (1) Info

□	Trigger
□	S3: mybucketishika arn:aws:s3:::mybucketishika

STEP 21;

THEN GO TO ENVIRONMENT VARIABLES ;



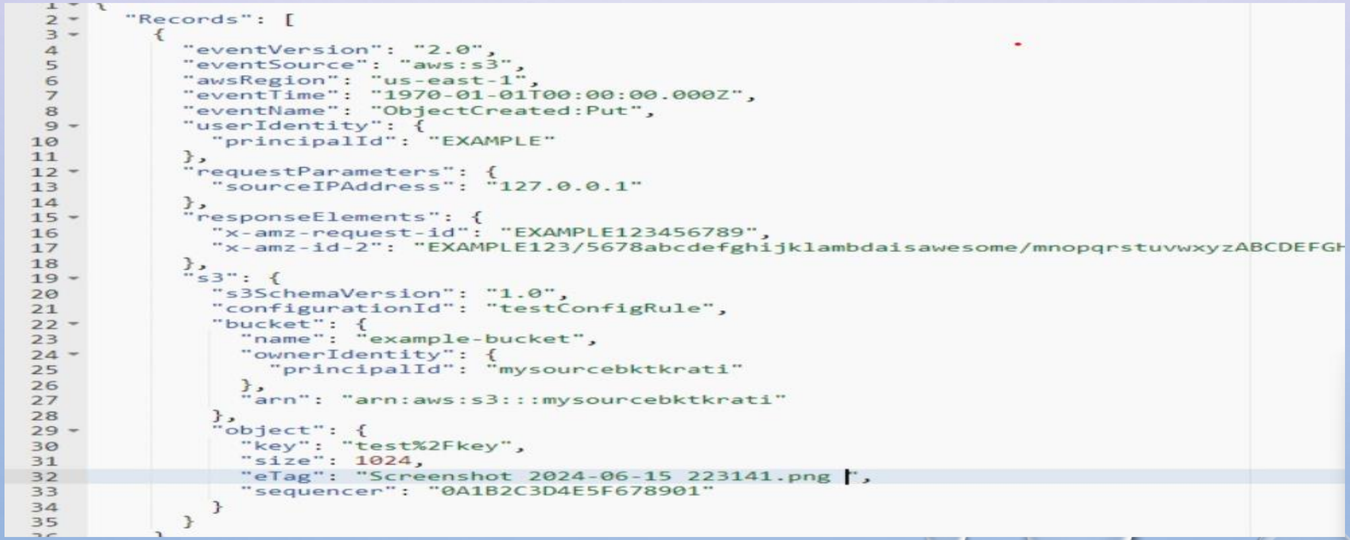
Environment variables

You can define environment variables as key-value pairs that are accessible from your function code. These are useful to store configuration settings without the need to change function code. Learn more

Key: destbuck

Value: mydestinationishika

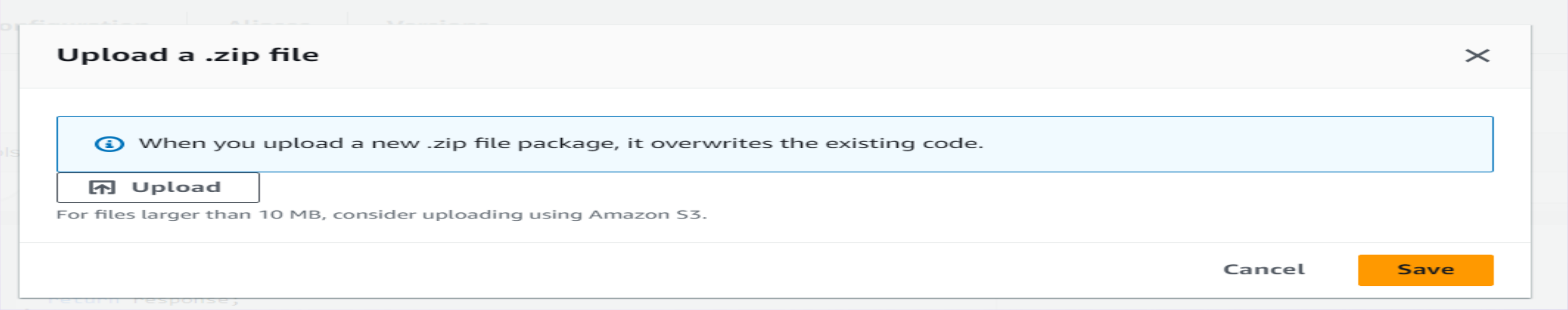
THEN WRITE THE CODE;



```
{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "aws:s3",
      "awsRegion": "us-east-1",
      "eventTime": "1970-01-01T00:00:00.000Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "EXAMPLE"
      },
      "requestParameters": {
        "sourceIPAddress": "127.0.0.1"
      },
      "responseElements": {
        "x-amz-request-id": "EXAMPLE123456789",
        "x-amz-id-2": "EXAMPLE123/5678abcdefghijklambdaisawesome/mnopqrstuvwxyzABCDEFGH
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "testConfigRule",
        "bucket": {
          "name": "example-bucket",
          "ownerIdentity": {
            "principalId": "mysourcebktkrati"
          },
          "arn": "arn:aws:s3:::mysourcebktkrati"
        },
        "object": {
          "key": "test%2Fkey",
          "size": 1024,
          "eTag": "Screenshot 2024-06-15 223141.png ",
          "sequencer": "0A1B2C3D4E5F678901"
        }
      }
    }
```

STEP 22;

THEN UPLOAD AN IMAGE TO THE UPLOAD ZIP FILE;

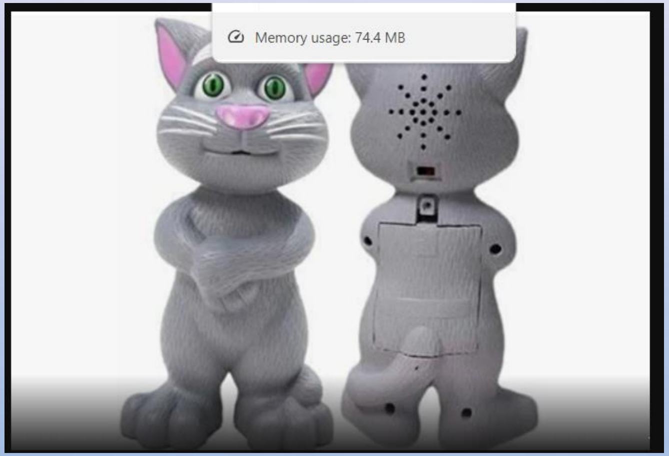


Upload a .zip file

When you upload a new .zip file package, it overwrites the existing code.

For files larger than 10 MB, consider uploading using Amazon S3.

THEN THE IMAGE IS SHOW ;



SUBMITTED

BY ;

ISHIKA SHUKLA

Thankyou

SUBMITTED BY ;
ISHIKA SHUKLA