**STEP** **1**: Sign in to AWS Management Consol

1. Click on the Open Console button, and you will get redirected to AWS Console in a new browser tab.

2. On the AWS sign-in page, Leave the Account ID as default. Never edit/remove the 12 digit Account ID present in the AWS Console. Otherwise, you cannot proceed with the lab.

3. Now copy your Username and Password in the Lab Console to the IAM Username and Password in AWS Console and click on the Sign in button. 4. Once Signed in to the AWS Management Console, Make the default AWS Region as US East (N. Virginia) us-east-1.

STEP 2: Create an S3 Bucket

1. In this task, we are going to create an S3 bucket by providing the required configurations such as name, region, and ACLs.

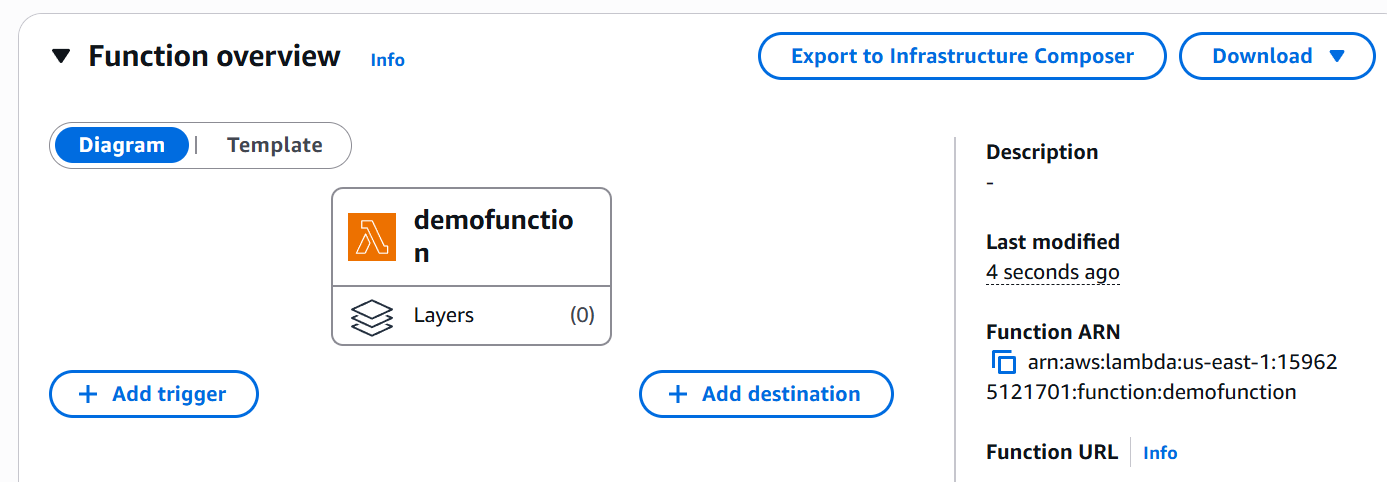
2. Navigate to the Services menu at the top. Click on S3 in the Storage section.

3. On the S3 dashboard, click on Create bucket button.

4. Bucket name: Enter any name Note: S3 bucket names are globally unique, choose a name that is available.

**STEP 4: Add S3 Trigger**

1. In the **Function overview** section, click "**Add trigger**".



1. **Select "S3" as the trigger source**.

A screenshot of a computer

AI-generated content may be incorrect.

1. Choose the **previously created S3 bucket**.

4. Set the event type to “All object create event”.

1. Click "Add".

**STEP 5: Add Code to Lambda Function**

Example (Python):

import json

def lambda\_handler(event, context):

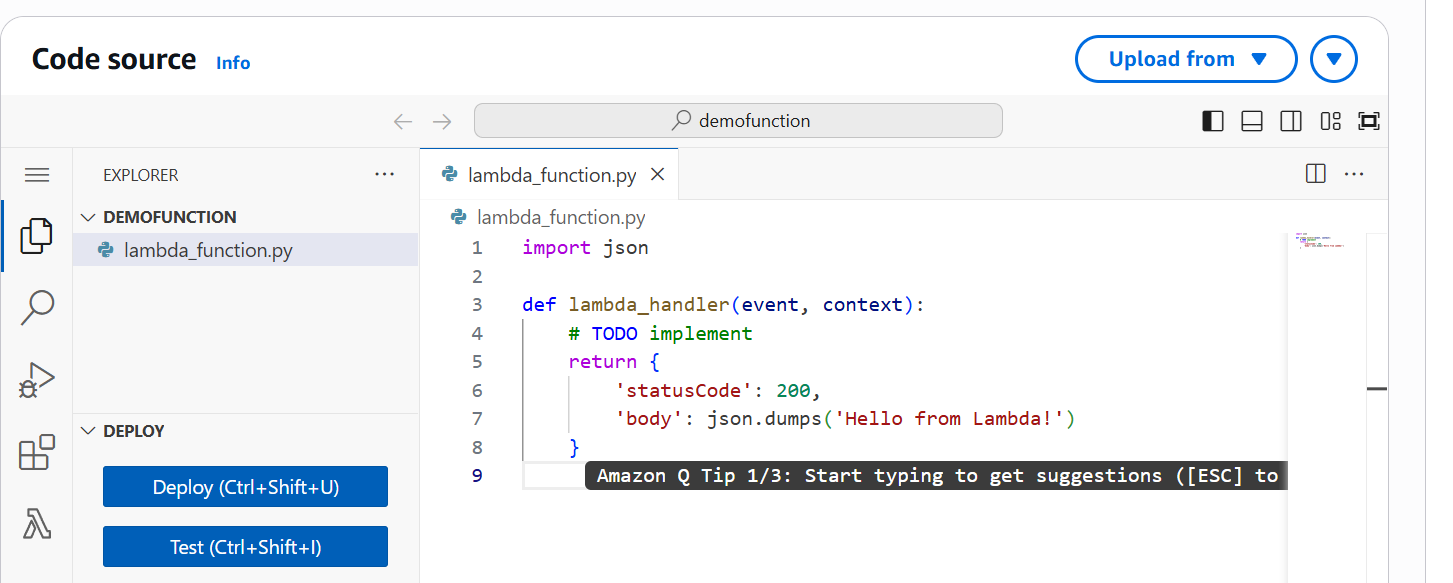
    # TODO implement

    return {

        'statusCode': 200,

        'body': json.dumps('Hello from Lambda!')

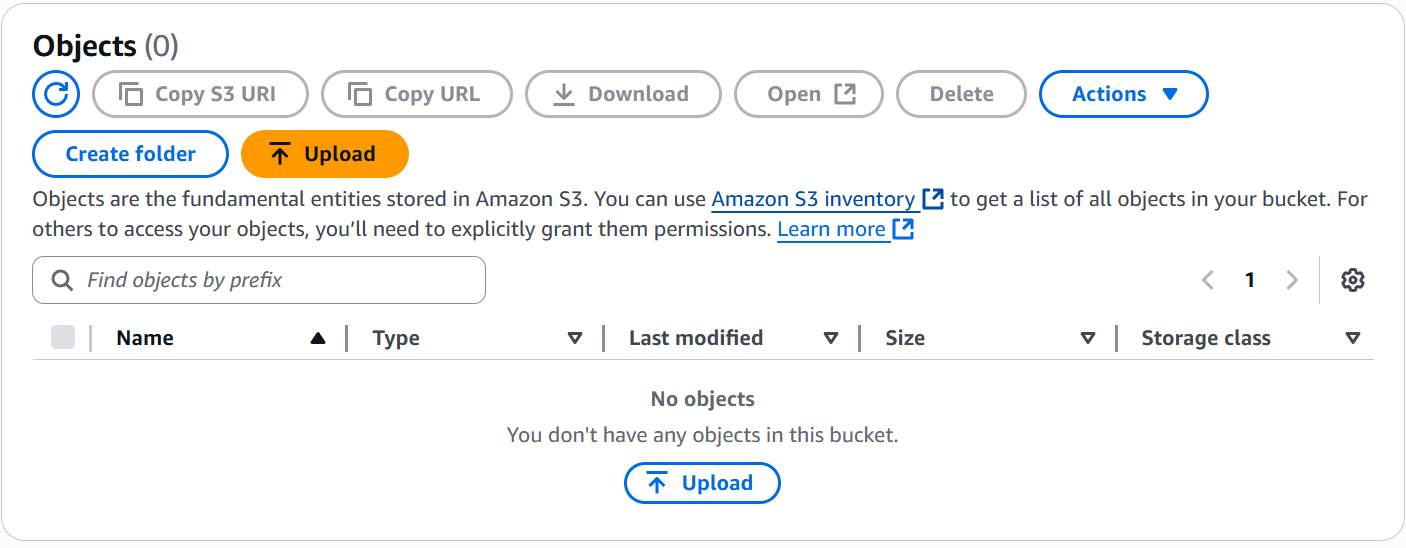
    }



**Click "Deploy"** after updating the function code

**STEP 6: Test the Setup**

Upload a file to the S3 bucket.

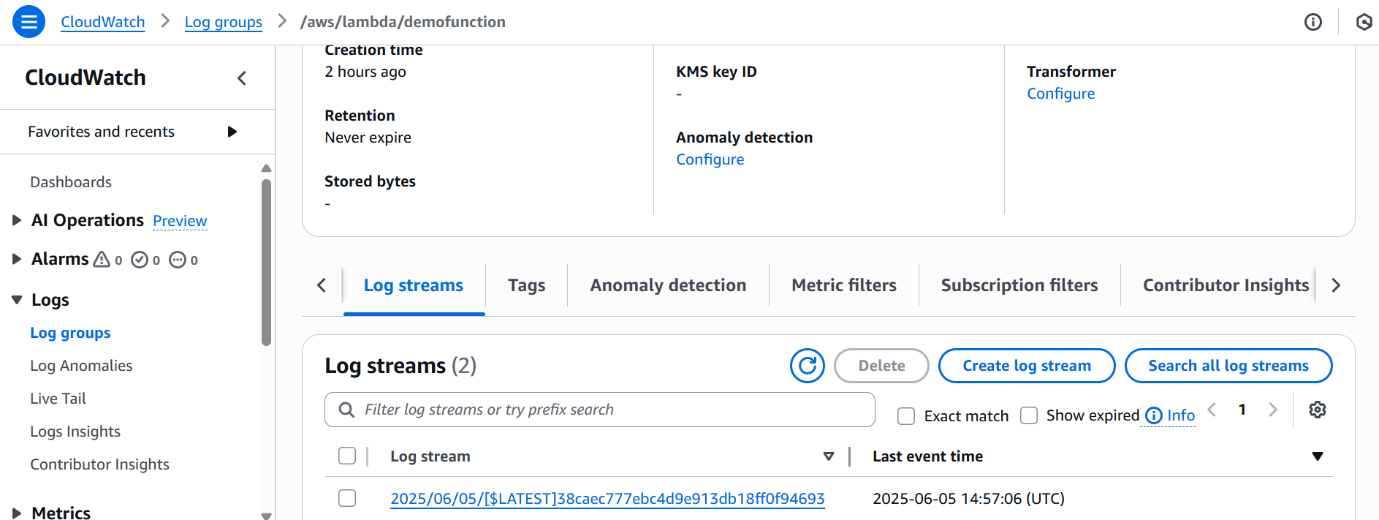


A screenshot of a computer

AI-generated content may be incorrect.

**Method 1.** (A) Go to the Lambda function’s "Monitor" tab and open CloudWatch Logs.

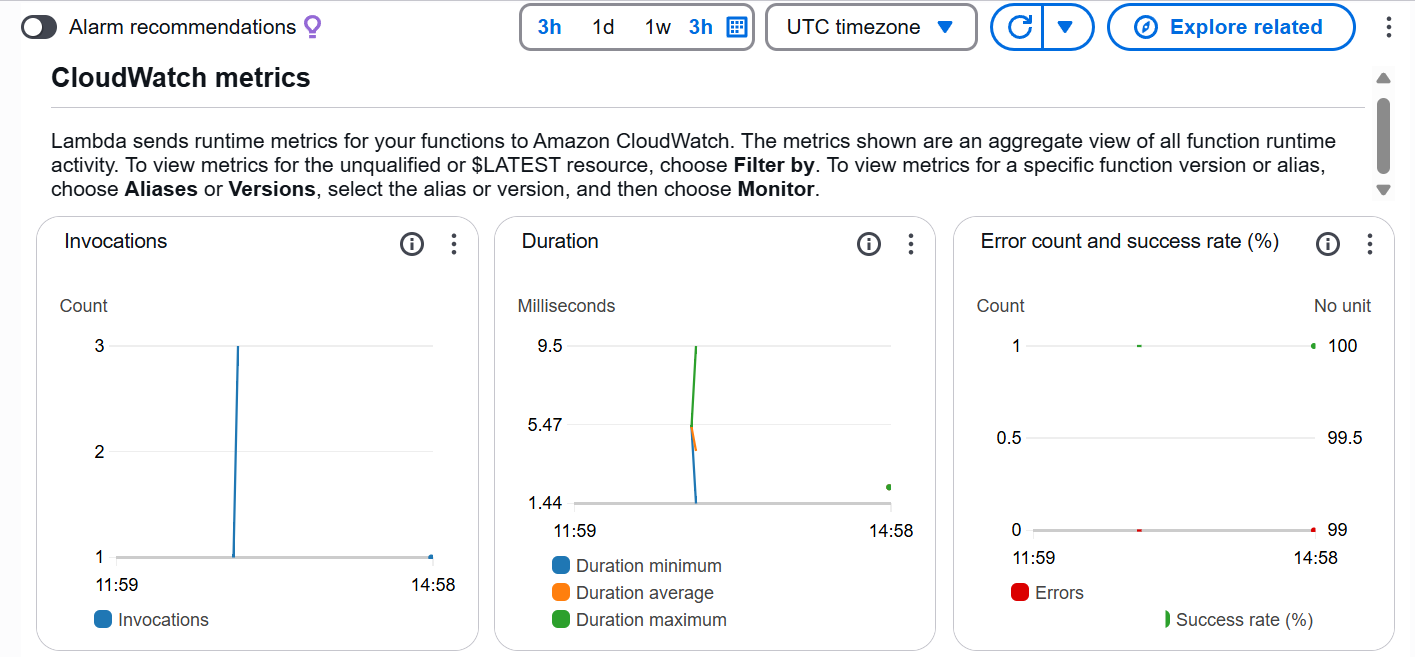
(B) Check the logs to verify if the function was triggered.



**Method 2:** Use Amazon CloudWatch Metrics

In CloudWatch > Metrics, navigate to: Lambda > By Function Name

Select your function to see the number of invocations and errors.



[Note on Permissions]

1. If access issues occur, go to the IAM console.

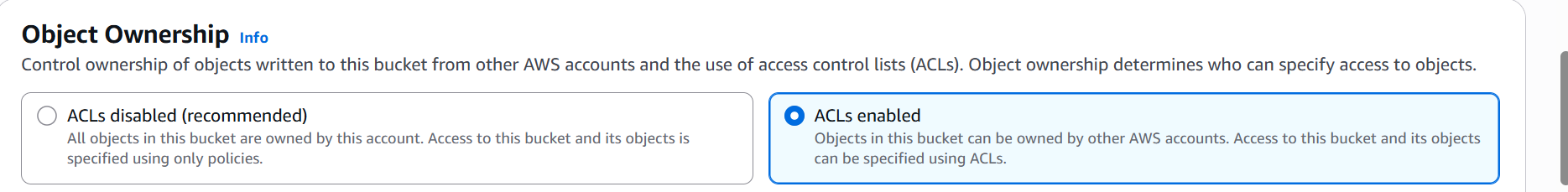
2. Locate the Lambda execution role and attach the "AmazonS3ReadOnlyAccess" policy or a custom policy with appropriate S3 permissions.

A screenshot of a computer

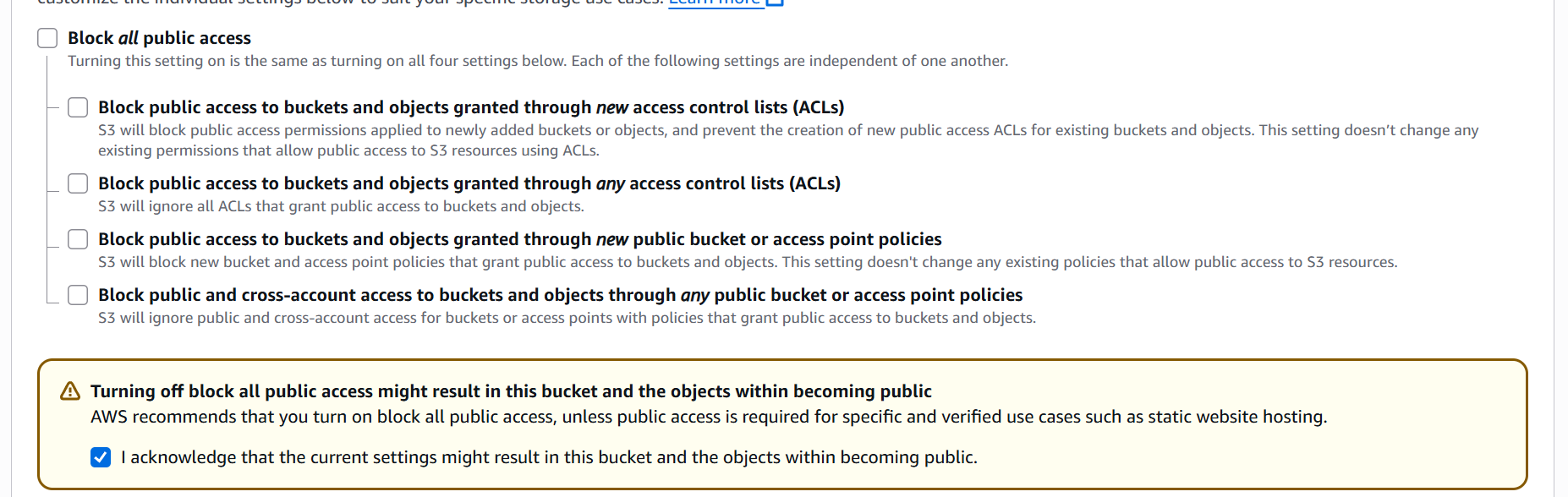
AI-generated content may be incorrect.

5. Region: Select US East (N. Virginia) us-east-1

6. Object ownership: Select ACLs disabled (recommended) option



7. Uncheck block all public access box and check the acknowledge box.



8. Click on the **Create bucket** button

**STEP 3: Create a Lambda Function**

1. Go to the AWS Lambda console.   
2. Click "**Create function**".   
3. Choose "**Author from scratch**".  
4. Enter a function name (e.g., demo function)

A screenshot of a computer

AI-generated content may be incorrect.

5. Select a **runtime** (e.g., Python 3.x or Node.js).

A screenshot of a computer

AI-generated content may be incorrect.

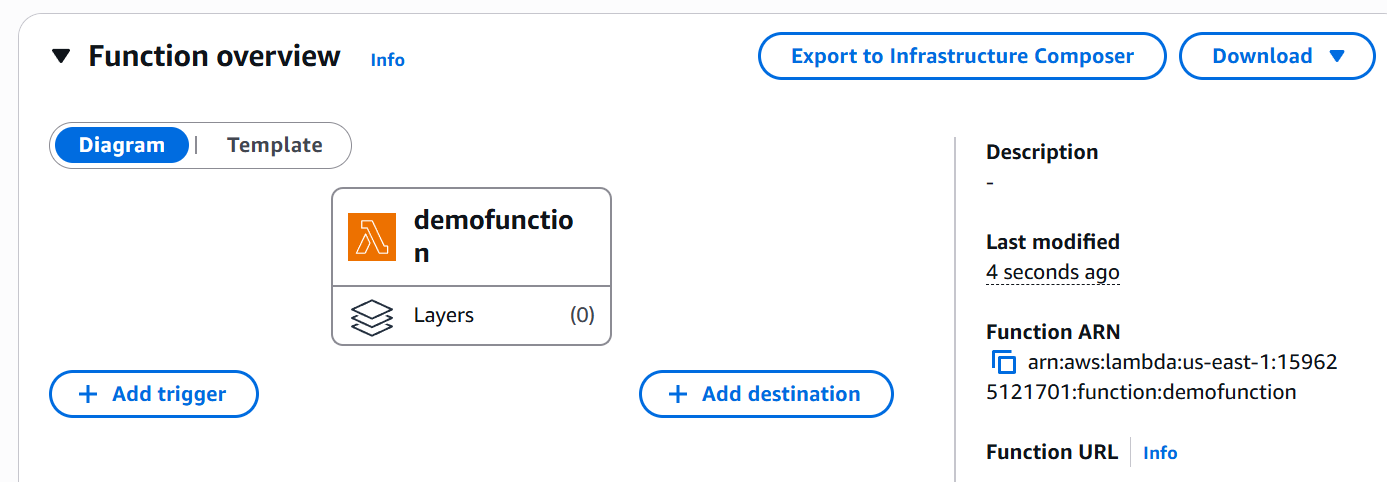
6. For permissions, choose "Create a new role with basic Lambda permissions".  
7. Click "Create function".

A screenshot of a computer

AI-generated content may be incorrect.

**STEP 4: Add S3 Trigger**

1. In the **Function overview** section, click "**Add trigger**".



1. **Select "S3" as the trigger source**.

A screenshot of a computer

AI-generated content may be incorrect.

1. Choose the **previously created S3 bucket**.

4. Set the event type to “All object create event”.

A screenshot of a computer

AI-generated content may be incorrect.

1. Click "Add".

**STEP 5: Add Code to Lambda Function**

Example (Python):

import json

def lambda\_handler(event, context):

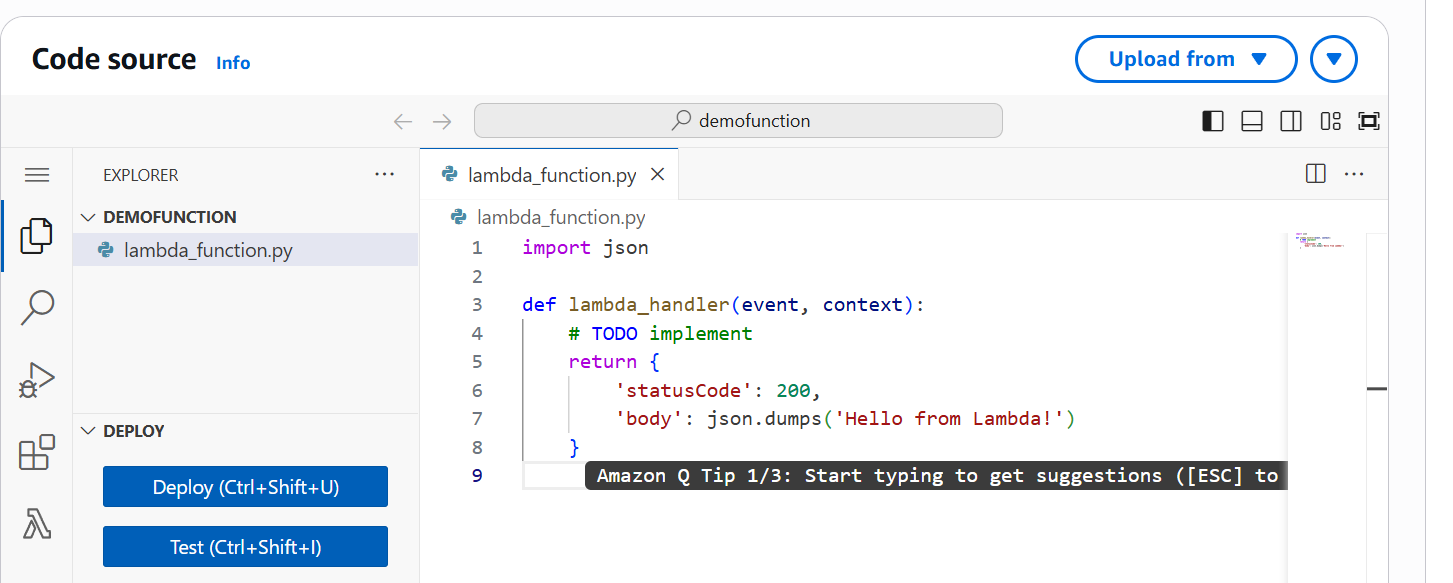
    # TODO implement

    return {

        'statusCode': 200,

        'body': json.dumps('Hello from Lambda!')

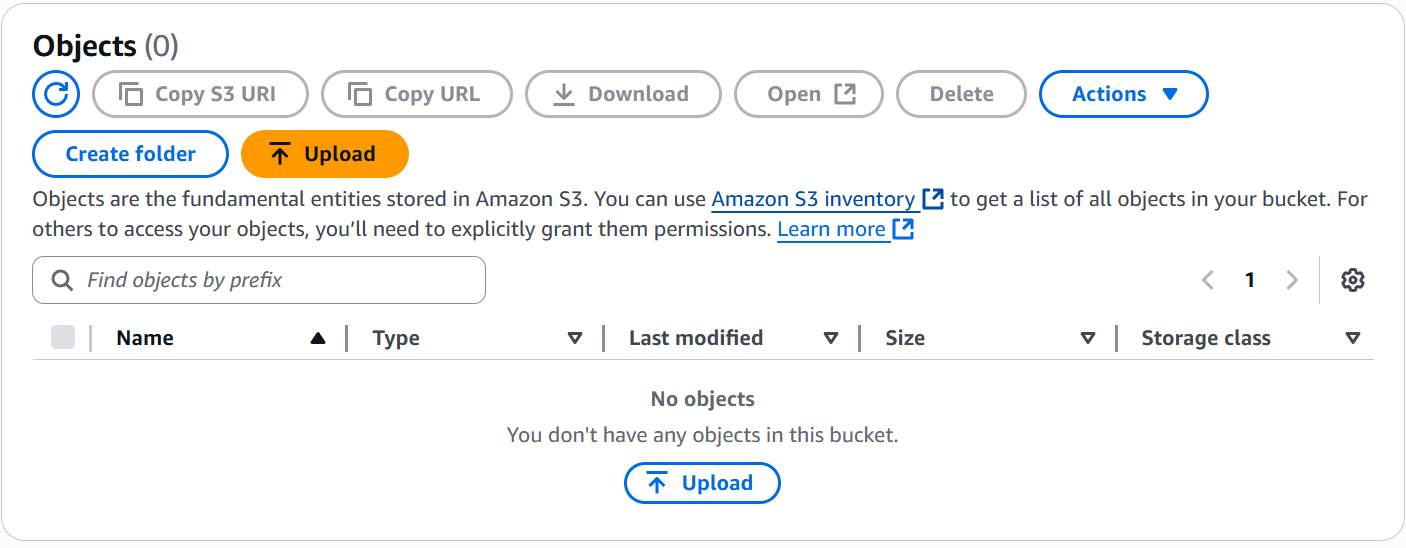
    }



**Click "Deploy"** after updating the function code

**STEP 6: Test the Setup**

Upload a file to the S3 bucket.

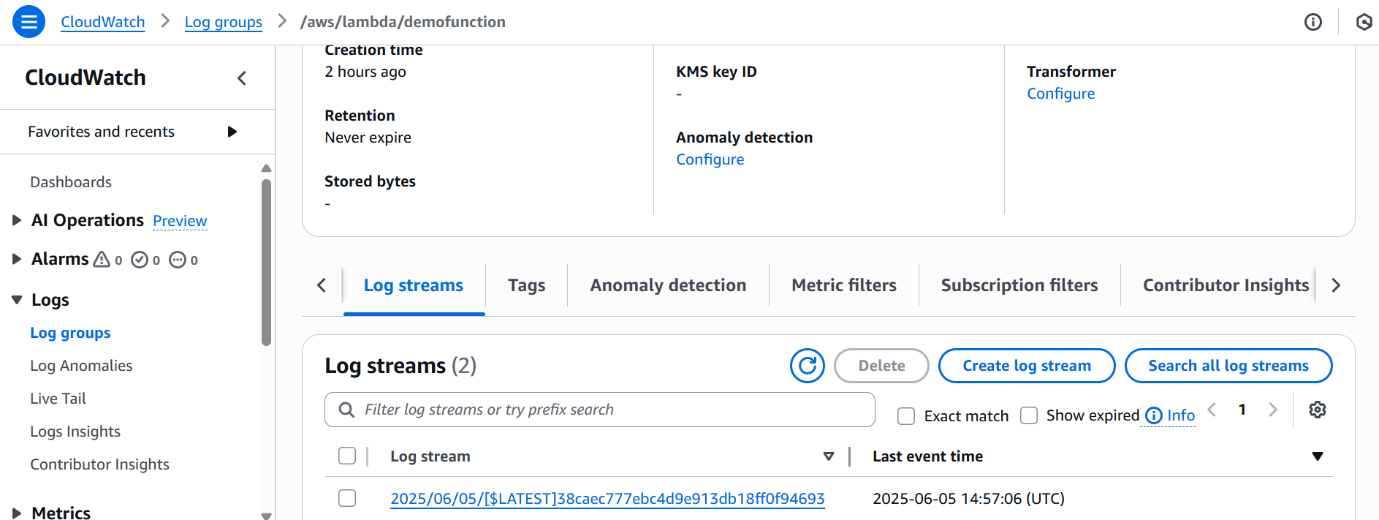


A screenshot of a computer

AI-generated content may be incorrect.

**Method 1.** (A) Go to the Lambda function’s "Monitor" tab and open CloudWatch Logs.

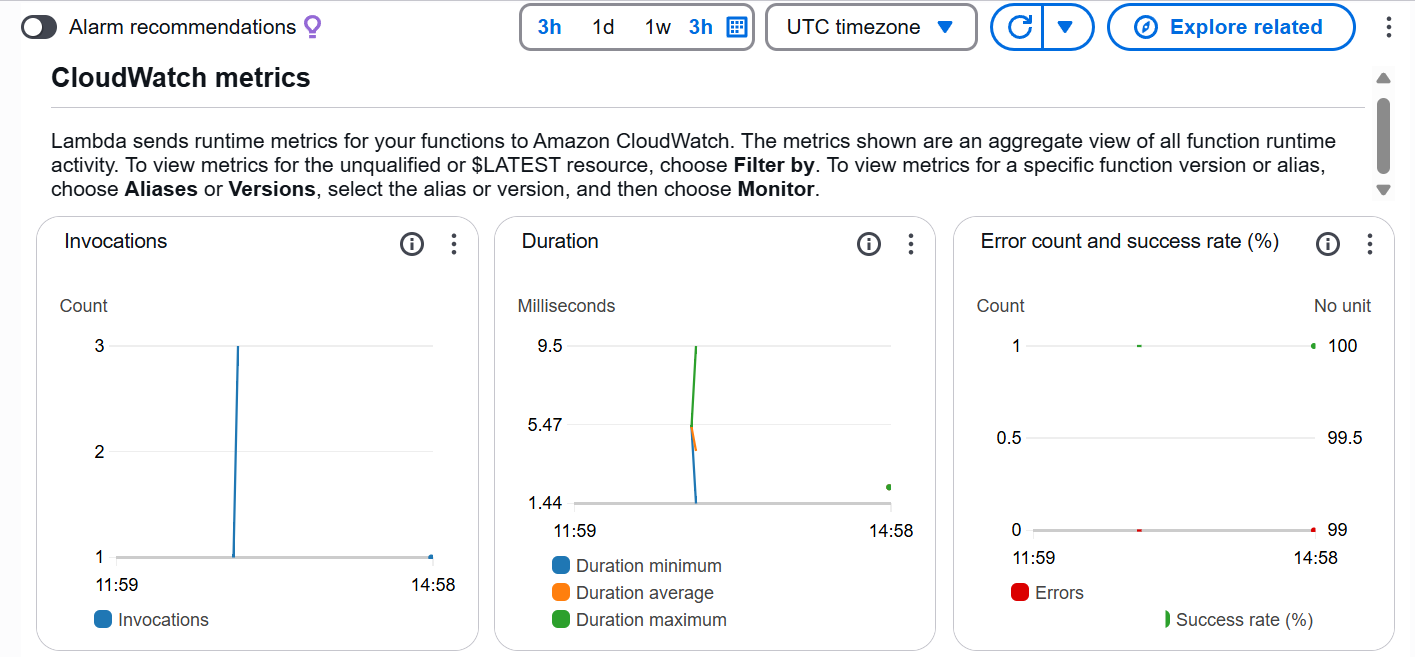
(B) Check the logs to verify if the function was triggered.



**Method 2:** Use Amazon CloudWatch Metrics

In CloudWatch > Metrics, navigate to: Lambda > By Function Name

Select your function to see the number of invocations and errors.



[Note on Permissions]

1. If access issues occur, go to the IAM console.

2. Locate the Lambda execution role and attach the "AmazonS3ReadOnlyAccess" policy or a custom policy with appropriate S3 permissions.