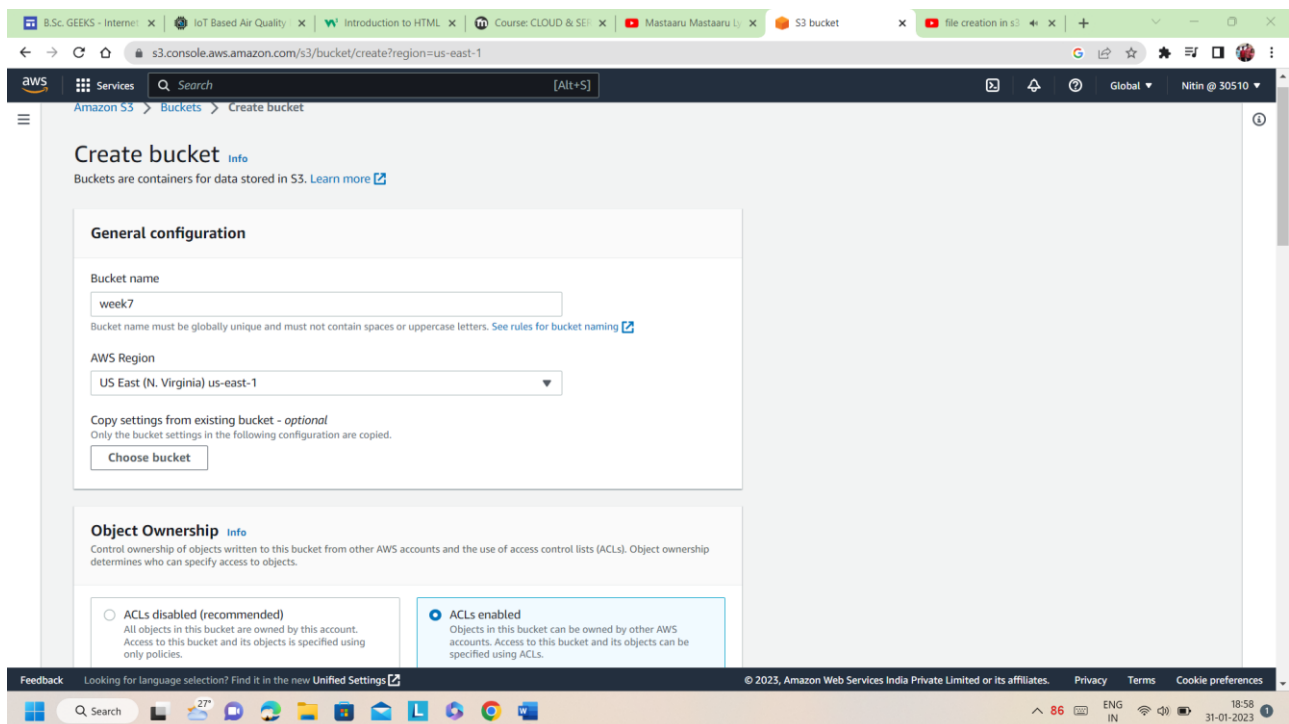# LAB-7

NAME: K.Nitin reddy

ID:2000030510

SECNO: 13

Create an Amazon S3 bucket and upload a test file to your new bucket. Your Lambda function retrieves information about this file when you test the function from the console.

s3.console.aws.amazon.com/s3/bucket/create?region=us-east-1

aws Services Q Search [Alt+S] Global ▼ Nitin @ 30510 ▼

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.

ⓘ **Upcoming permission changes to disable any Block Public Access setting**
Starting in April 2023, to disable any Block Public Access setting when creating buckets by using the S3 console, you must have the s3:PutBucketPublicAccessBlock permission. Learn more

---

us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/create/function

aws Services Q Search [Alt+S] N. Virginia ▼ Nitin @ 30510 ▼

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.

Basic information

Function name
Enter a name that describes the purpose of your function.

week7

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.

Python 3.9 ▼

Architecture Info
Choose the instruction set architecture you want for your function code.
⦿ x86_64
○ arm64
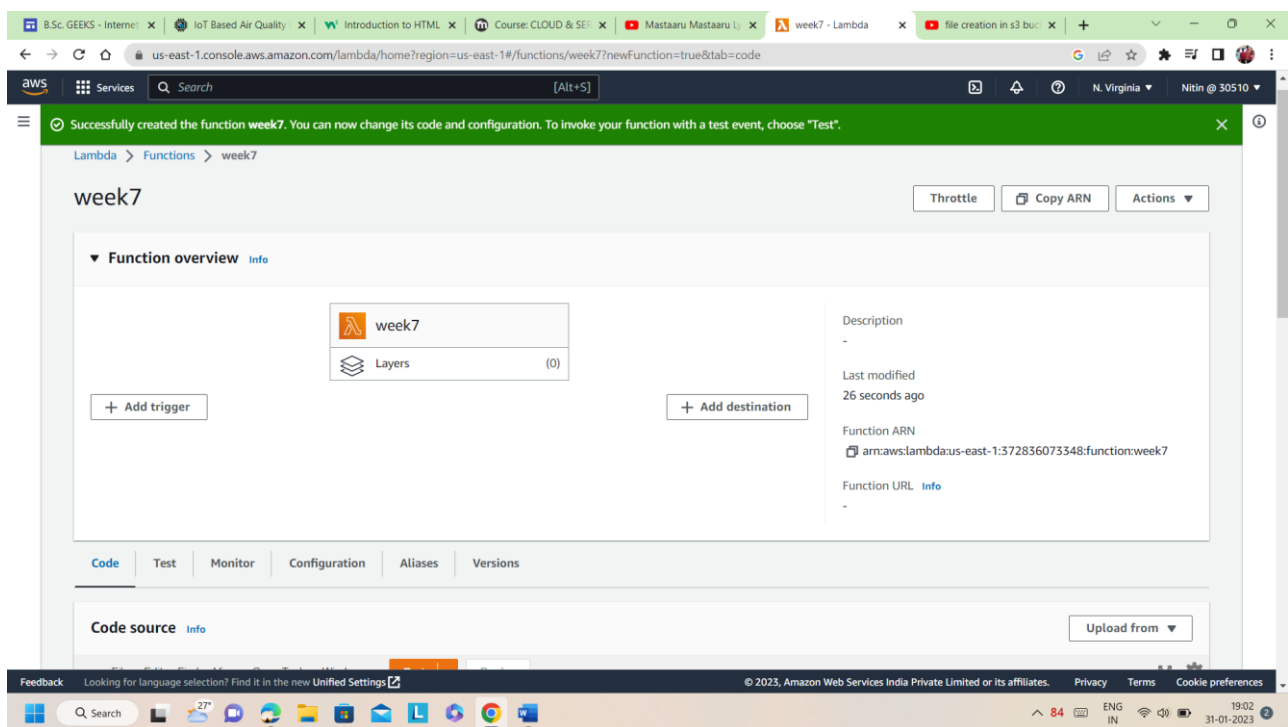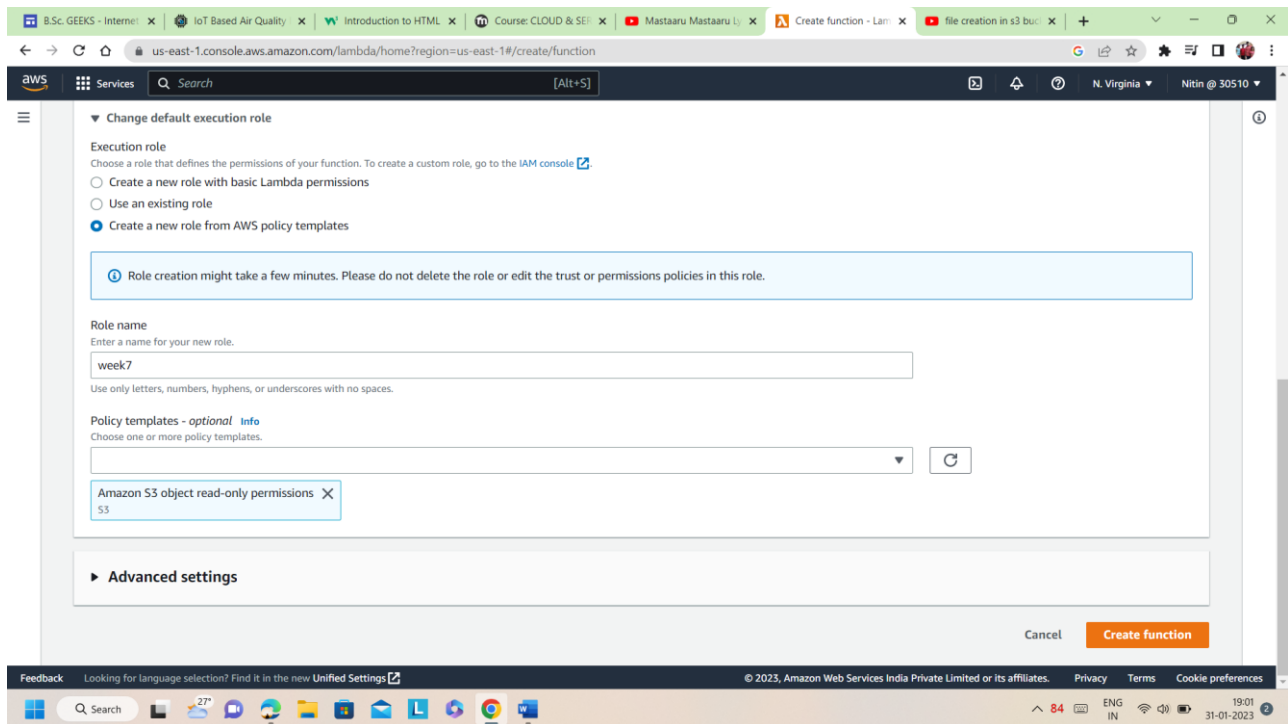
Permissions Info
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

▼ Change default execution role

Execution role

B.Sc. GEEKS - Inte × | IoT Based Air Qua × | Introduction to H × | Course: CLOUD & × | Mastaaru Mastai × | week7 - Lambda × | IAM Managemen × | file creation in s3 × | +

us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/week7?newFunction=true&tab=configure

aws Services Q Search [Alt+S] N. Virginia ▼ Nitin @ 30510 ▼

✓ Successfully created the function **week7**. You can now change its code and configuration. To invoke your function with a test event, choose "Test". ✕

| Code | Test | Monitor | Configuration | Aliases | Versions |

General configuration

Triggers

Permissions

Destinations

Function URL

Environment variables

Tags

VPC

Monitoring and operations tools

Concurrency

Asynchronous invocation

Code signing

~~Database proxies~~

Execution role

Edit

Role name

week7 ↗

Resource summary

View role document

Amazon CloudWatch Logs
3 actions, 2 resources ▼

To view the resources and actions that your function has permission to access, choose a service.

| By action | **By resource** |

Resource	Actions
arn:aws:logs:us-east-1:372836073348:*	Allow: logs:CreateLogGroup

---

B.Sc. GEEKS - Inte × | IoT Based Air Qua × | Introduction to H × | Course: CLOUD & × | Mastaaru Mastai × | week7 - Lambda × | IAM Managemen × | file creation in s3 × | +

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles/details/week7?section=permissions

aws Services Q Search [Alt+S] Global ▼ Nitin @ 30510 ▼

Identity and Access Management (IAM) ✕

January 31, 2023, 19:01 (UTC+05:30) arn:aws:iam::372836073348:role/service-role/week7

Q Search IAM

Dashboard

Last activity None

Maximum session duration 1 hour

▼ **Access management**

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ **Access reports**

Access analyzer

   Archive rules

   Analyzers

   Settings

Credential report

Organization activity

Service control policies (SCPs)

| **Permissions** | Trust relationships | Tags | Access Advisor | Revoke sessions |

Permissions policies (2) Info
You can attach up to 10 managed policies.

⟳ Simulate Remove Add permissions ▲

Attach policies

Create inline policy

Q Filter policies by property or policy name and press enter.

☐	Policy name ↗	▽	Type ▽	Description
☐	⊞ AWSLambdaBasicExecutionRole-72f8da2b-c1c0-4de0-977f-90e50feb17b3		Customer managed	
☐	⊞ AWSLambdaS3ExecutionRole-82da6fcc-f798-401e-83f3-986c27c0ce52		Customer managed	

Permissions boundary - (not set) Info

Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting but can be used to delegate permission management to others.

Set permissions boundary

us-east-1.console.aws.amazon.com/iam/home#/roles/week7$createPolicy?step=edit

aws | Services | Q Search [Alt+S] | Global ▼ | Nitin @ 30510 ▼

Visual editor | JSON | Import managed policy

Expand all | Collapse all

▼ S3 (64 actions) | Clone | Remove

▸ Service S3

▸ Actions **List**

ListAccessPoints	ListBucketMultipartUploads	ListMultiRegionAccessPoints
ListAccessPointsForObjectLambda	ListBucketVersions	ListStorageLensConfigurations
ListAllMyBuckets	ListJobs	
ListBucket	ListMultipartUploadParts	

Read

DescribeJob	GetBucketOwnershipControls	GetObject
DescribeMultiRegionAccessPointOperation	GetBucketPolicy	GetObjectAcl
GetAccelerateConfiguration	GetBucketPolicyStatus	GetObjectAttributes
GetAccessPoint	GetBucketPublicAccessBlock	GetObjectLegalHold
GetAccessPointConfigurationForObjectLambda	GetBucketRequestPayment	GetObjectRetention
GetAccessPointForObjectLambda	GetBucketTagging	GetObjectTagging
GetAccessPointPolicy	GetBucketVersioning	GetObjectTorrent
GetAccessPointPolicyForObjectLambda	GetBucketWebsite	GetObjectVersion
GetAccessPointPolicyStatus	GetEncryptionConfiguration	GetObjectVersionAcl
GetAccessPointPolicyStatusForObjectLambda	GetIntelligentTieringConfiguration	GetObjectVersionAttributes
GetAccountPublicAccessBlock	GetInventoryConfiguration	GetObjectVersionForReplication
GetAnalyticsConfiguration	GetJobTagging	GetObjectVersionTagging
GetBucketAcl	GetLifecycleConfiguration	GetObjectVersionTorrent
GetBucketCORS	GetMetricsConfiguration	GetStorageLensConfiguration
GetBucketLocation	GetMultiRegionAccessPoint	GetStorageLensConfiguration

Q Search   27°   82   ENG IN   19:06 31-01-2023

---

us-east-1.console.aws.amazon.com/iam/home#/roles/week7$createPolicy?step=edit

aws | Services | Q Search [Alt+S] | Global ▼ | Nitin @ 30510 ▼

GetBucketAcl	GetLifecycleConfiguration	GetObjectVersionTorrent
GetBucketCORS	GetMetricsConfiguration	GetReplicationConfiguration
GetBucketLocation	GetMultiRegionAccessPoint	GetStorageLensConfiguration
GetBucketLogging	GetMultiRegionAccessPointPolicy	GetStorageLensConfigurationTagging
GetBucketNotification	GetMultiRegionAccessPointPolicyStatus	GetStorageLensDashboard
GetBucketObjectLockConfiguration	GetMultiRegionAccessPointRoutes	

Write

PutObject

▼ Resources ○ Specific
   close   ● All resources

> As a best practice, define permissions for only specific resources in specific accounts. Alternatively, you can grant least privilege using condition keys. Learn more

▸ Request conditions Specify request conditions (optional)

⊕ Add additional permissions

Character count: 1,937 of 10,240.
The current character count includes character for all inline policies in the role: week7.

Cancel **Review policy**

Q Search   27°   82   ENG IN   19:06 31-01-2023

aws | Services | Q Search [Alt+S] | Global ▼ | Nitin @ 30510 ▼

Create policy

① ②

Review policy

Before you create this policy, provide the required information and review this policy.

Name* `week7lambda`

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Q Filter

Service ▾	Access level	Resource	Request condition
Allow (1 of 364 services) Show remaining 363			
S3	**Full**: List, Read **Limited**: Write	All resources	None

* Required

Cancel | Previous | **Create policy**

---

aws | Services | Q Search [Alt+S] | N. Virginia ▼ | Nitin @ 30510 ▼

Bucket

Please select the S3 bucket that serves as the event source. The bucket must be in the same region as the function.

Q s3/week7

Bucket region: us-east-1

Event type

Select the events that you want to have trigger the Lambda function. You can optionally set up a prefix or suffix for an event. However, for each bucket, individual events cannot have multiple configurations with overlapping prefixes or suffixes that could match the same object key.

All object create events ▼

Prefix - *optional*

Enter a single optional prefix to limit the notifications to objects with keys that start with matching characters.

e.g. images/

Suffix - *optional*

Enter a single optional suffix to limit the notifications to objects with keys that end with matching characters.

e.g. .jpg

Recursive invocation

If your function writes objects to an S3 bucket, ensure that you are using different S3 buckets for input and output. Writing to the same bucket increases the risk of creating a recursive invocation, which can result in increased Lambda usage and increased costs. Learn more
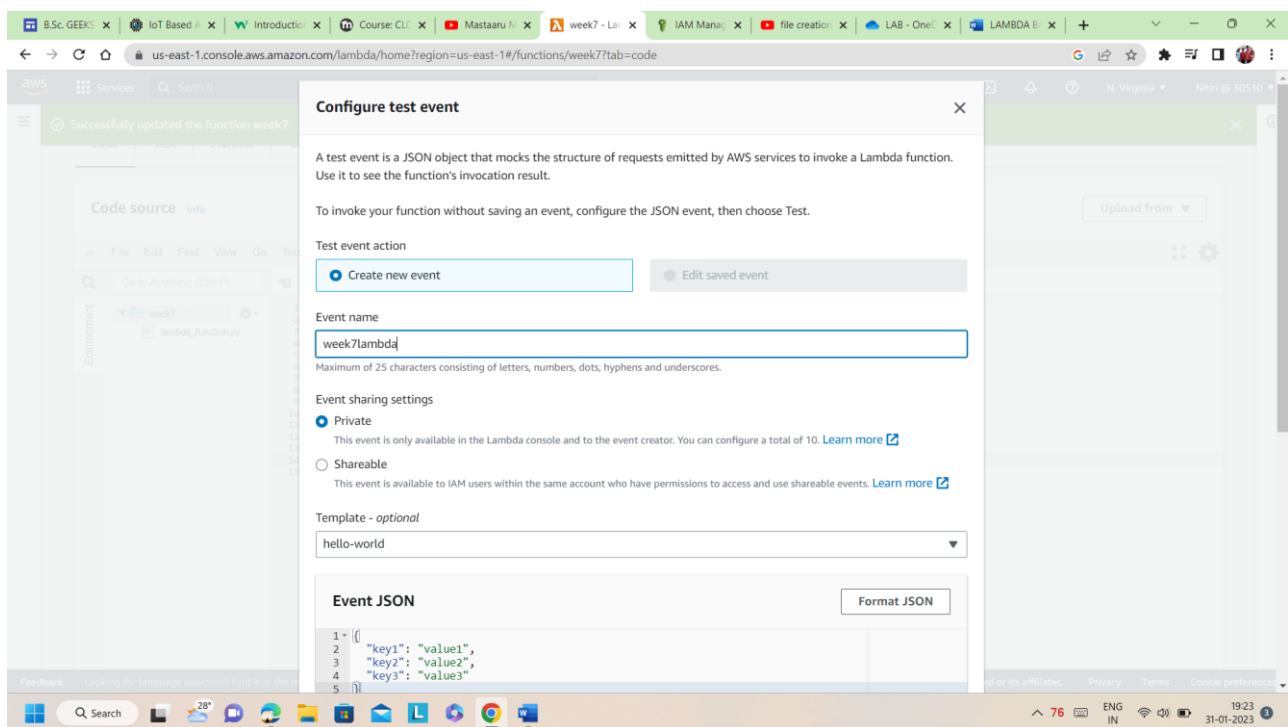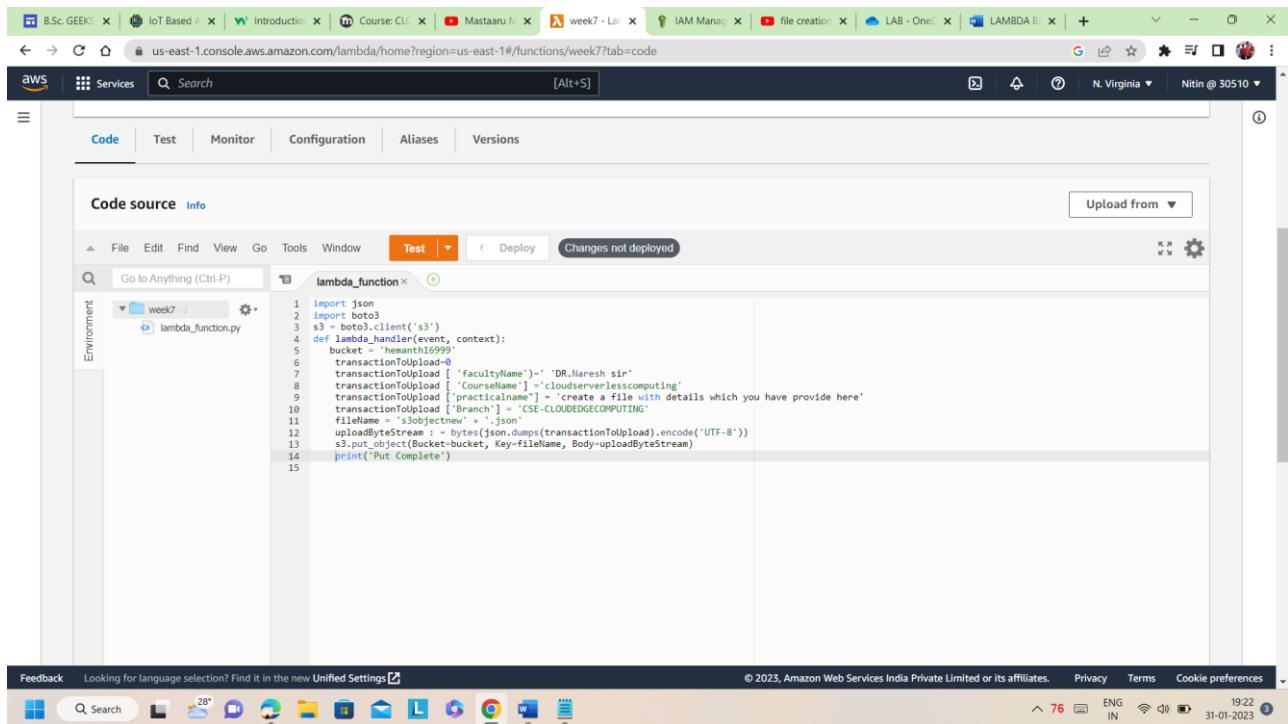
☑ I acknowledge that using the same S3 bucket for both input and output is not recommended and that this configuration can cause recursive invocations, increased Lambda usage, and increased costs.

Lambda will add the necessary permissions for AWS S3 to invoke your Lambda function from this trigger. Learn more about the Lambda permissions model.

```python
import json
import boto3
s3 = boto3.client('s3')
def lambda_handler(event, context):
    bucket = 'hemanth16999'
    transactionToUpload=0
    transactionToUpload [ 'facultyName')=' 'DR.Naresh sir'
    transactionToUpload [ 'CourseName' ] ='cloudserverlesscomputing'
    transactionToUpload ['practicalname"] = 'create a file with details which you have provide here'
    transactionToUpload ['Branch' ] = 'CSE-CLOUDEDGECOMPUTING'
    fileName = 's3objectnew' + '.json'
    uploadByteStream : = bytes(json.dumps(transactionToUpload).encode('UTF-8'))
    s3.put_object(Bucket=bucket, Key=fileName, Body=uploadByteStream)
    print('Put Complete')
```

Configure test event

A test event is a JSON object that mocks the structure of requests emitted by AWS services to invoke a Lambda function. Use it to see the function's invocation result.

To invoke your function without saving an event, configure the JSON event, then choose Test.

Test event action

- Create new event
- Edit saved event

Event name

week7lambda

Maximum of 25 characters consisting of letters, numbers, dots, hyphens and underscores.

Event sharing settings

- Private

  This event is only available in the Lambda console and to the event creator. You can configure a total of 10. Learn more ⧉

- Shareable

  This event is available to IAM users within the same account who have permissions to access and use shareable events. Learn more ⧉

Template - optional

hello-world

Event JSON   Format JSON

```json
{
    "key1": "value1",
    "key2": "value2",
    "key3": "value3"
}
```