

## ASSIGNMENT 6

AIM : To learn how to use Lamda in order to find the ContentType of Object uploaded in S3 Bucket.

### THEORY :

Create bucket:

The screenshot shows the AWS S3 console 'Create bucket' page. The 'General configuration' section includes a text input for 'Bucket name' containing 'mynewbucket' and a dropdown for 'AWS Region' set to 'Asia Pacific (Mumbai) ap-south-1'. Below these is a section for 'Object Ownership' with two radio buttons: 'ACLs disabled (recommended)' (selected) and 'ACLs enabled'. The 'Block Public Access settings for this bucket' section is at the bottom.

create a new policy from iam dashboard;

while creating policy select json tab and paste the following code:

```
{  
  "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:::*/*"

}

]

}

```

The screenshot shows the AWS IAM console interface. The left sidebar is titled "Identity and Access Management (IAM)" and includes a search bar and a navigation menu with sections like "Access management", "Access reports", and "Related consoles". The main content area is titled "Policies (1127)" and contains a table listing various IAM policies. The table has columns for Policy name, Type, Used as, and Description. It lists several AWS managed policies (like AdministratorAccess, PowerUserAccess) and customer managed policies (like AWSLambdaBasicExecutionRole, AWSLambdaS3ExecutionRole).

Policy name	Type	Used as	Description
AWSLambdaBasicExecutionRole-6939cbef-b679-49f4-9759-3e9eb1d3208c	Customer managed	Permissions policy (1)	
AWSLambdaBasicExecutionRole-bc3f17ef-7f7c5-4a0d-9852-4644e8dec70e	Customer managed	Permissions policy (1)	
AWSLambdaBasicExecutionRole-bf11a1ec-26a7-4e97-8e53-6e5c00213d96	Customer managed	Permissions policy (1)	
AWSLambdaS3ExecutionRole-77f8c449-cea9-4eaa-866a-ea6921b47727	Customer managed	Permissions policy (1)	
AWSLambdaS3ExecutionRole-c802badc-2a97-41c2-926f-e1115a9c0f6e	Customer managed	Permissions policy (1)	
AWSLambdaS3ExecutionRole-fed8c33a5-6f18-425d-9560-b5c31236c294	Customer managed	Permissions policy (1)	
AdministratorAccess	AWS managed - job function	None	
PowerUserAccess	AWS managed - job function	None	
ReadOnlyAccess	AWS managed - job function	None	
AWSCloudFormationReadOnlyAccess	AWS managed	None	
CloudFrontFullAccess	AWS managed	None	
AWSCloudHSMFullAccess	AWS managed	None	
AWSCloudHSMReadOnlyAccess	AWS managed	None	
ResourceGroupsandTagEditorFullAccess	AWS managed	None	
ResourceGroupsandTagEditorReadOnlyAccess	AWS managed	None	
CloudFrontReadOnlyAccess	AWS managed	None	
CloudSearchFullAccess	AWS managed	None	
CloudSearchReadOnlyAccess	AWS managed	None	

create policy and name it:

The screenshot shows the 'Review and create' page in the AWS IAM console. The 'Policy details' section has a 'Policy name' field containing 's3-trigger-tutorial'. Below it is a 'Description - optional' field. The 'Permissions defined in this policy' section shows a table with two permissions:

Service	Access level	Resource	Request condition
S3	Limited Read	BucketName   string like   All ObjectPath   string like   All	None
CloudWatch Logs	Limited Write	region   string like   All	None

Below the table, there is an 'Add tags - optional' section with a note: 'No tags associated with the resource.' and an 'Add tag' button.

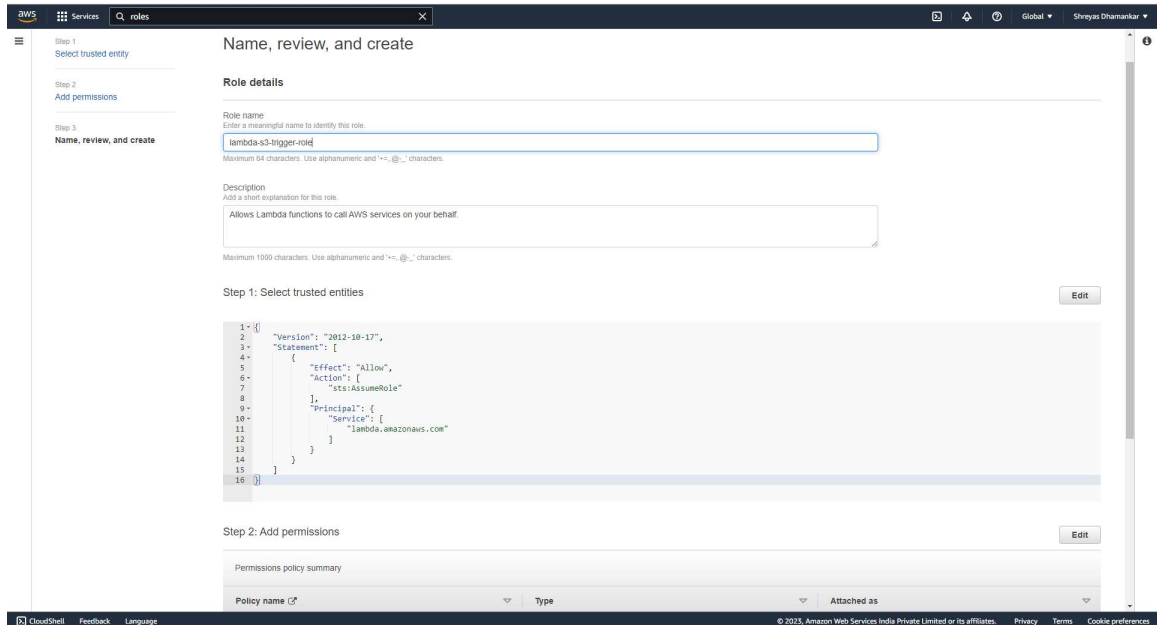
go to roles page and select create a new role

The screenshot shows the 'Roles' page in the AWS IAM console. It displays a list of roles with columns for 'Role name', 'Trusted entities', and 'Last activity'. The roles listed are:

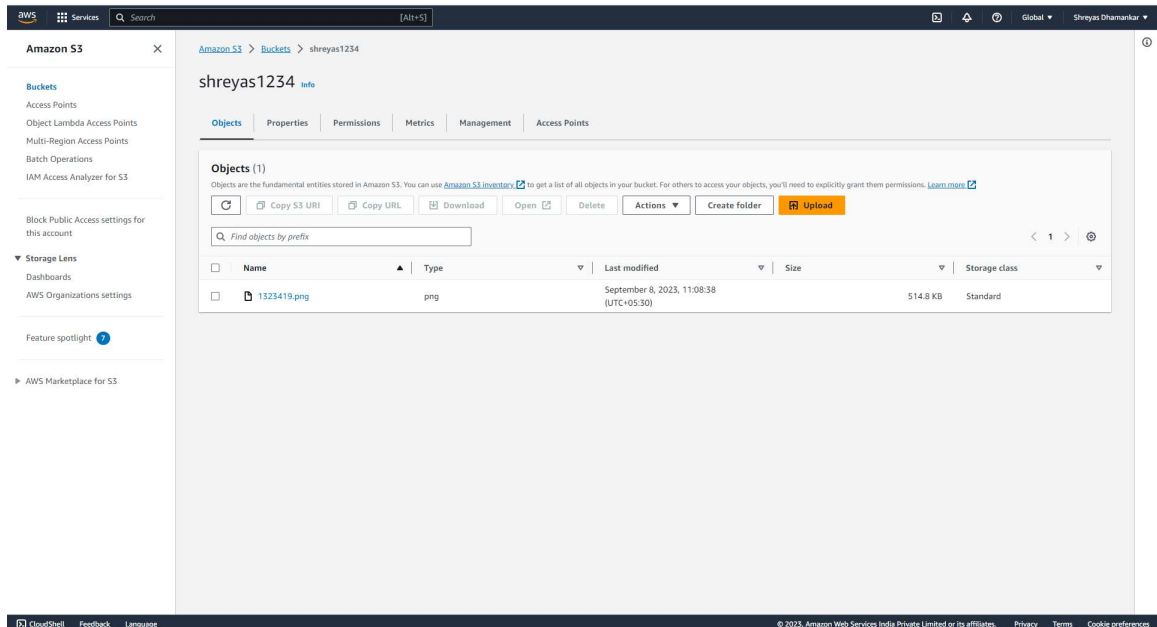
Role name	Trusted entities	Last activity
AWSCloudSSMAccessRole	AWS Service: cloud9 and 1 more	33 days ago
AWSServiceRoleForAWSCloud9	AWS Service: cloud9 (Service-Linked Role)	33 days ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
shreyas	AWS Service: lambda	36 minutes ago
shreyas1	AWS Service: lambda	32 minutes ago
shreyas2	AWS Service: lambda	27 minutes ago

Below the list, there is a 'Roles Anywhere' section with three options: 'Access AWS from your non AWS workloads', 'X.509 Standard', and 'Temporary credentials'. Each option has a brief description and a 'Manage' button.

under policies for role select the policy that you have created and click next. Then name the role as follows:

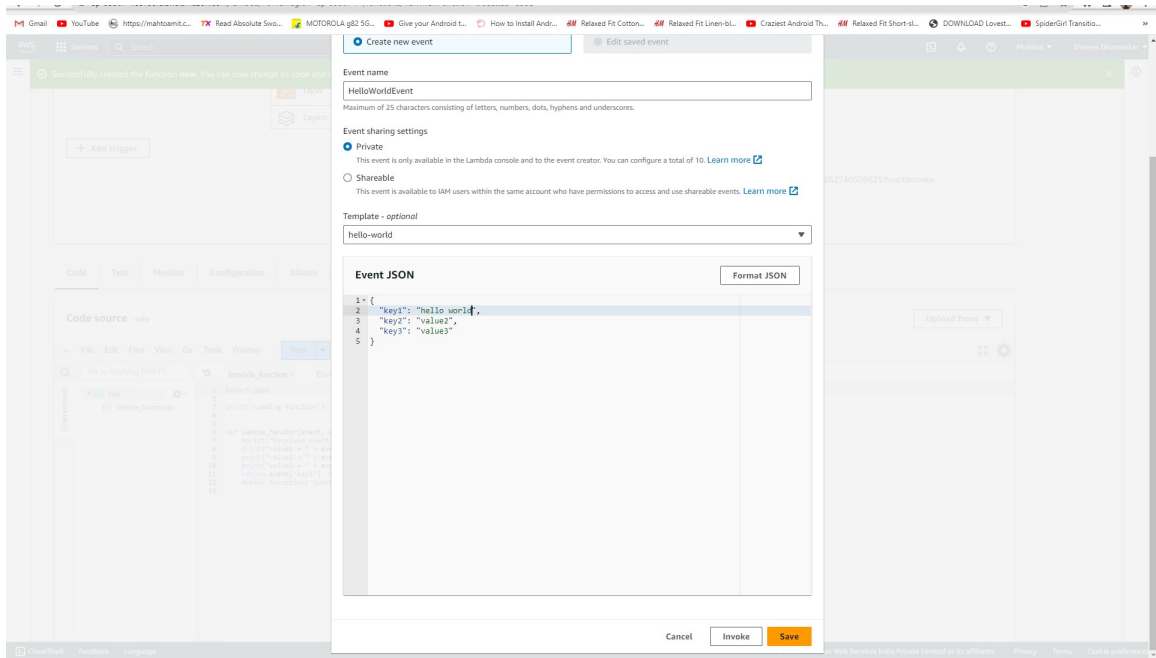


Upload an image file in the S3 bucket.



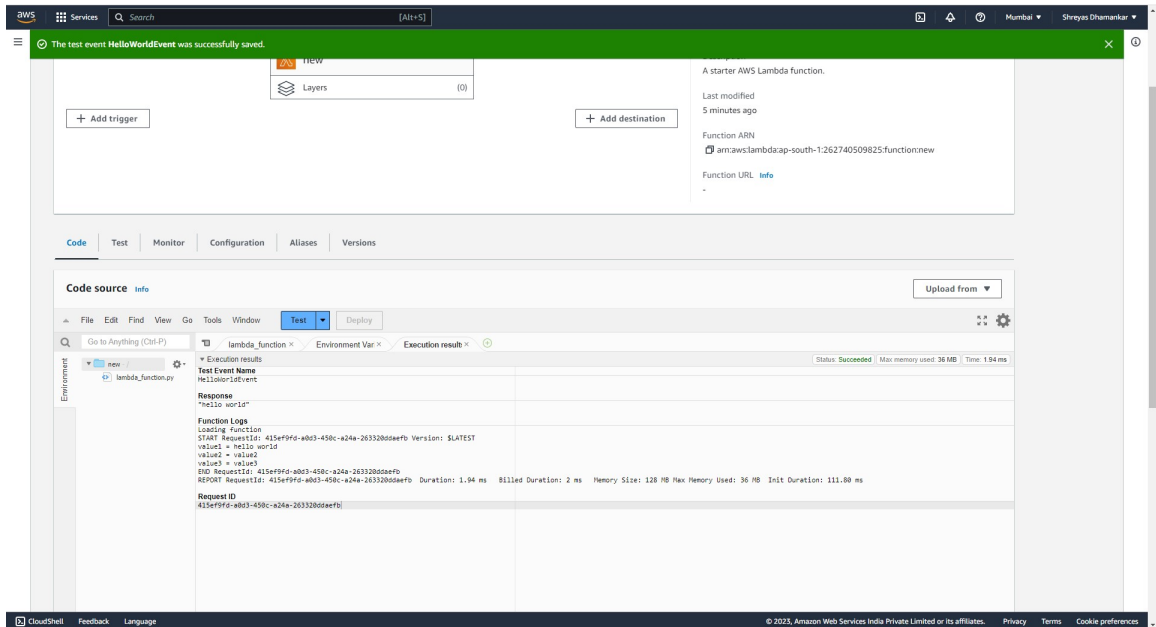
Go to lambda dashboard in aws and create a new function named s3-trigger tutorial. select use existing blueprint and choose 'hello world python 3.7 blueprint'.

Click on create function. Once function is created go to test and create new Test event.



Change Key 1 to Hello World.

Click on test and obtain the results in Execution tab.



**CONCLUSION :** In this assignment we learnt how to use Lambda function to run a basic Hello World program in Python.

