

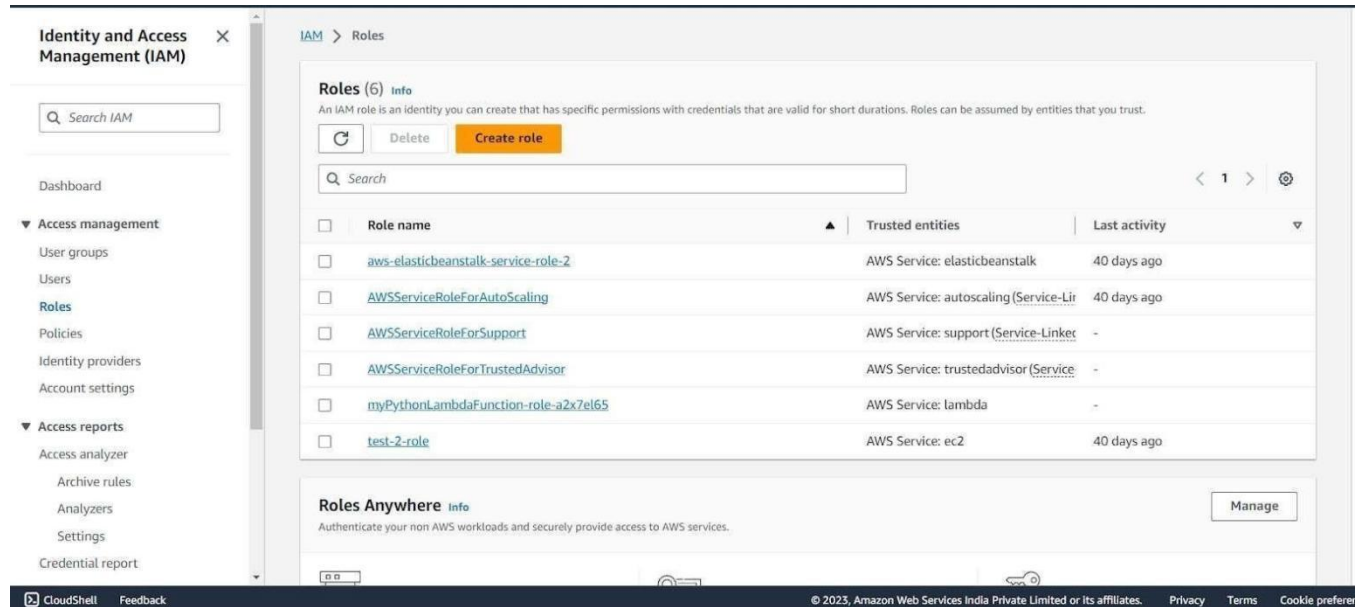
Adv. DevOps Exp. 12

Name: Ronit Santwani

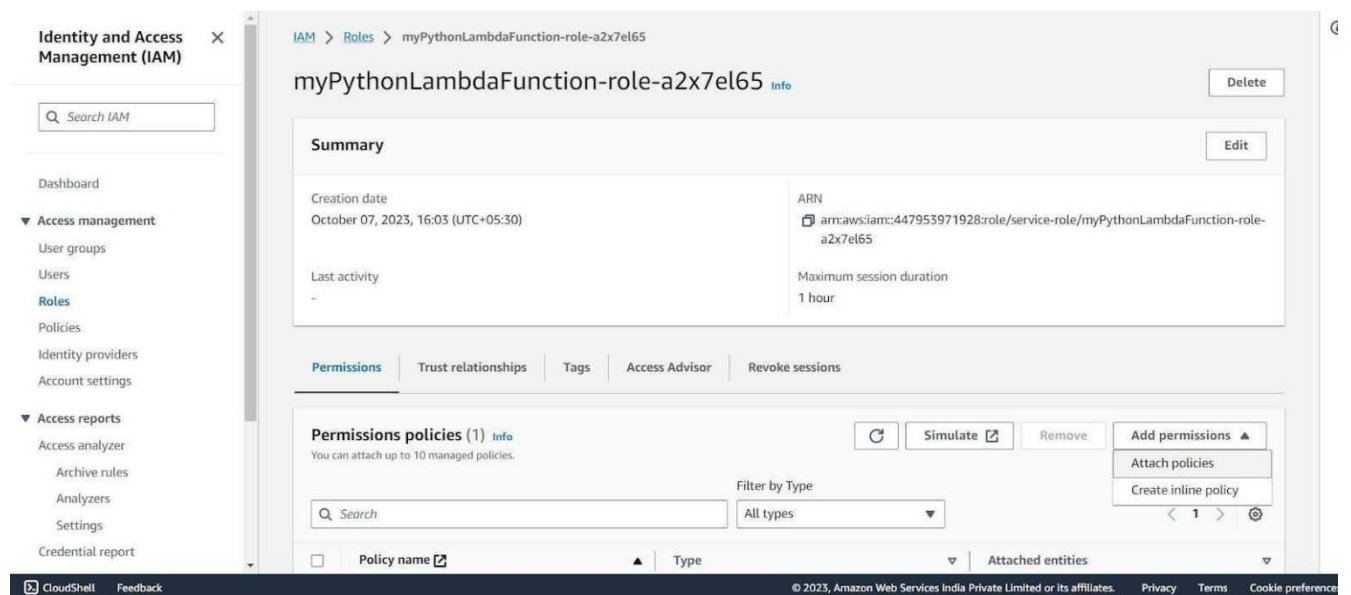
Class: D15A

Roll No: 49

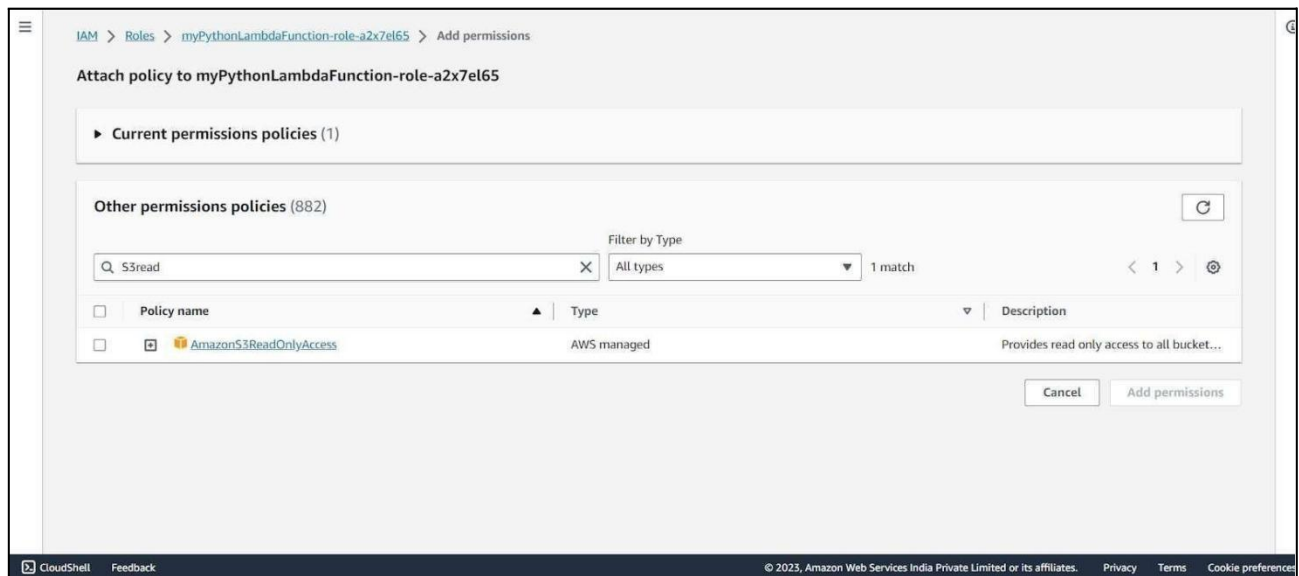
Step 1: Open up the IAM Console and under Roles, choose the Role we previously created for the Python Lambda Function (You can find your role name configuration of your Lambda function).



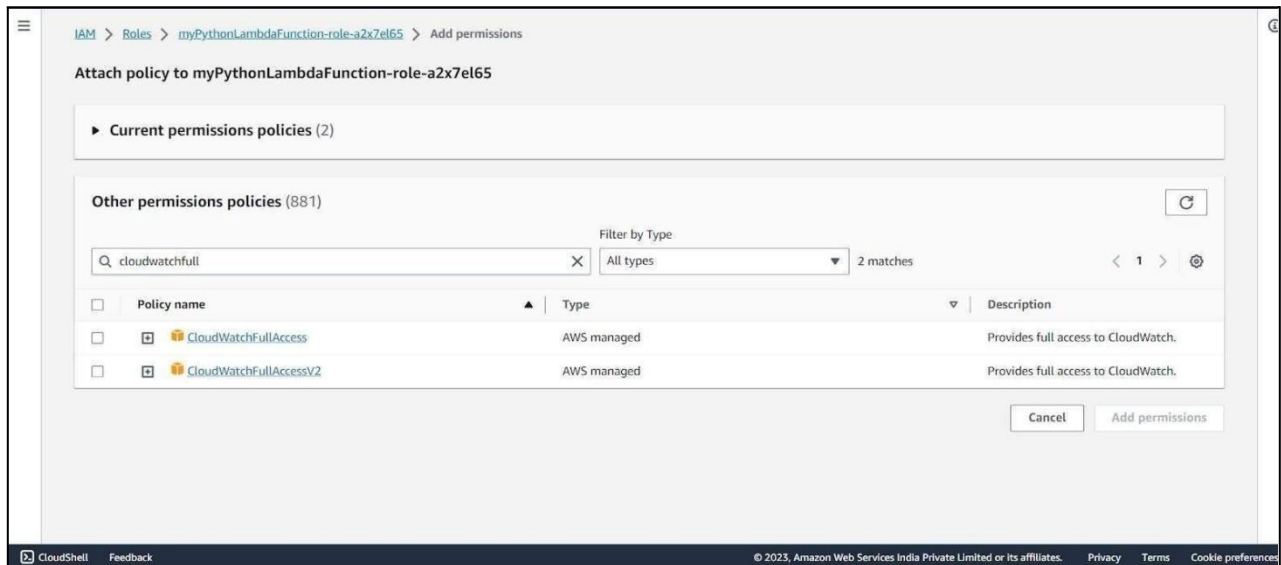
Step 2: Under Attach Policies, add S3-ReadOnly and CloudWatchFull permissions to this role.



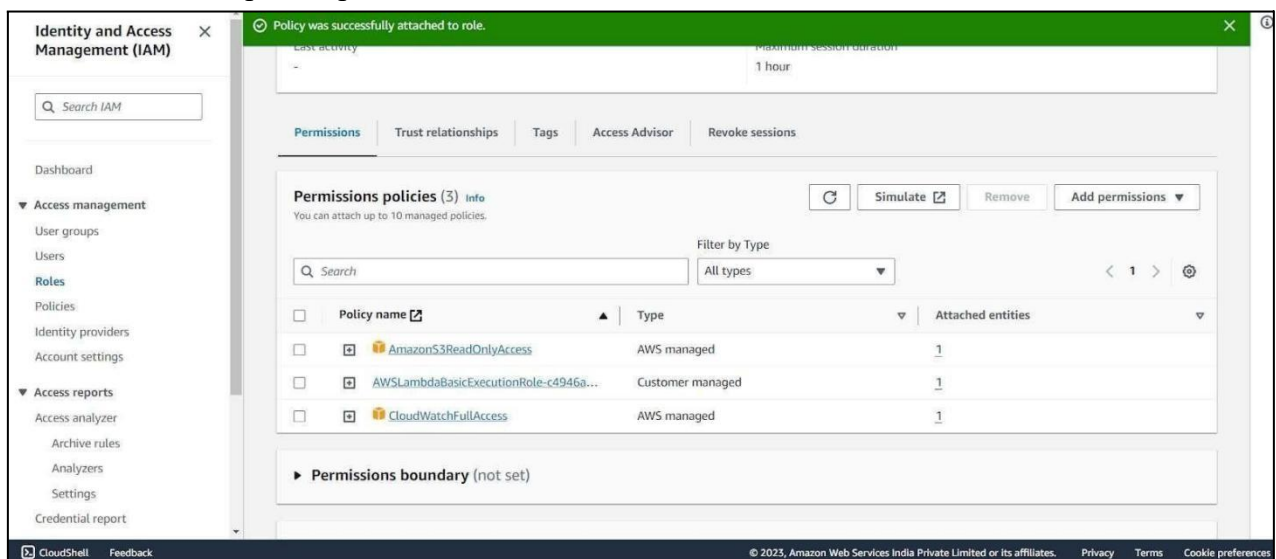
S3-ReadOnly



CloudWatchFull



After successful attachment of policy you will see something like this you will be able to see the updated policies.



[Lambda](#) > [Functions](#) > Create function

Create function Info

AWS Serverless Application Repository applications have moved to [Create application](#).

☒ **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.

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.

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.

CloudShell [Feedback](#) © 2023, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Step 3: Open up AWS Lambda and create a new Python function.

Under Execution Role, choose the existing role, then select the one which was previously created and to which we just added permissions.

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
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

Existing role
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.

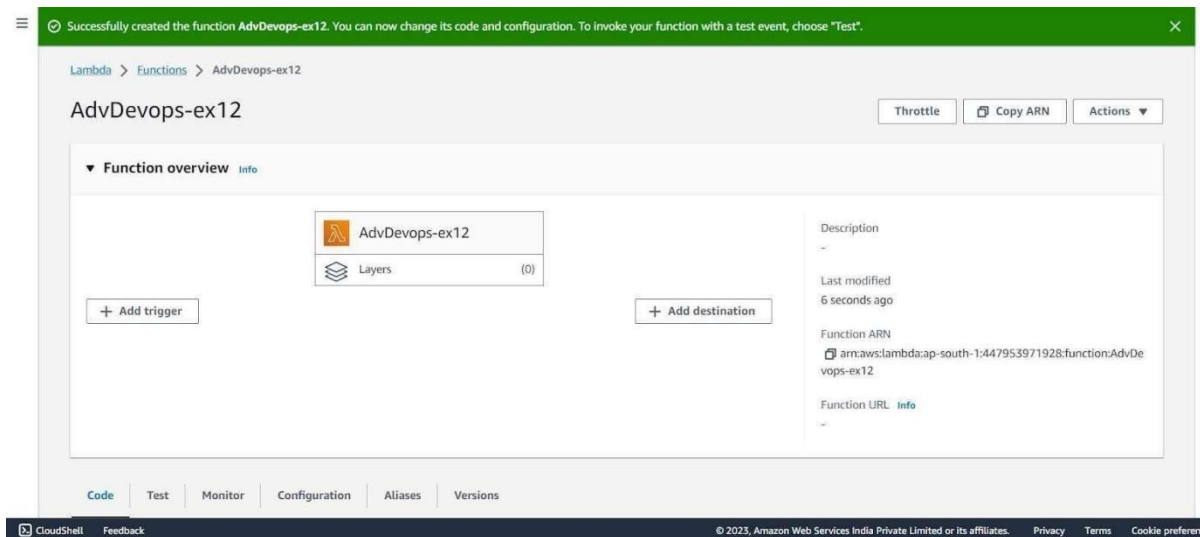
[View the myPythonLambdaFunction-role-a2x7el65 role](#) on the IAM console.

► **Advanced settings**

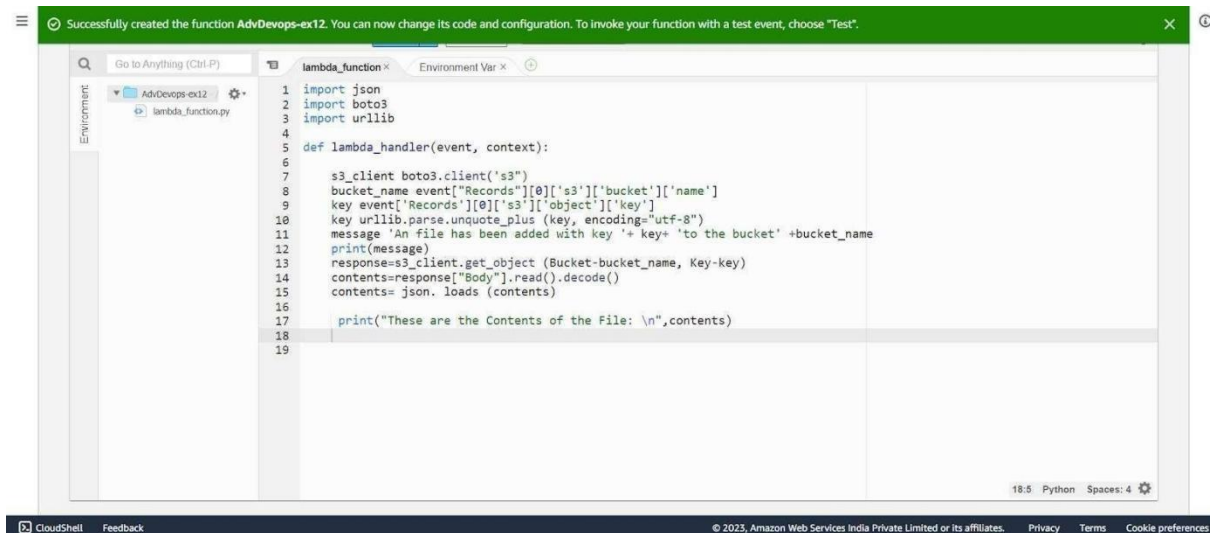
Cancel Create function

CloudShell [Feedback](#) © 2023, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

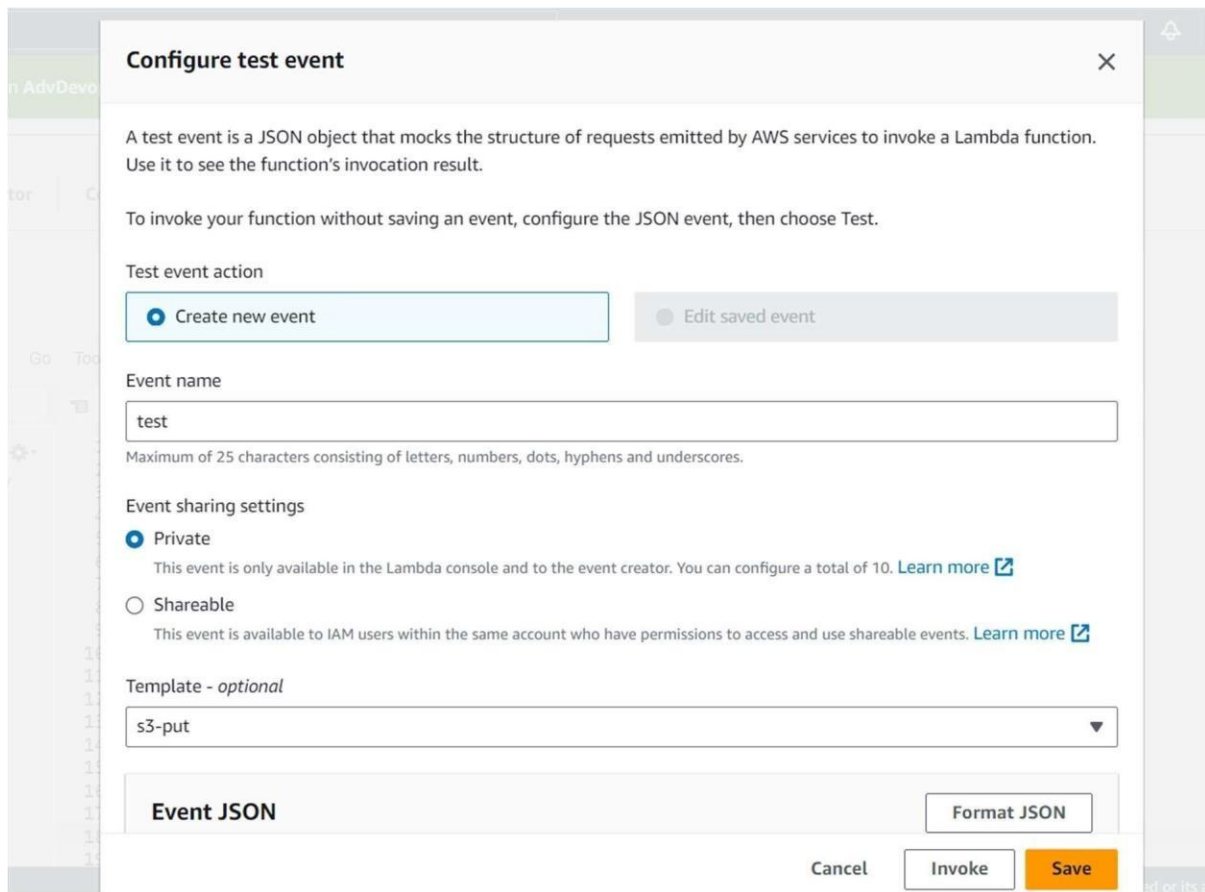
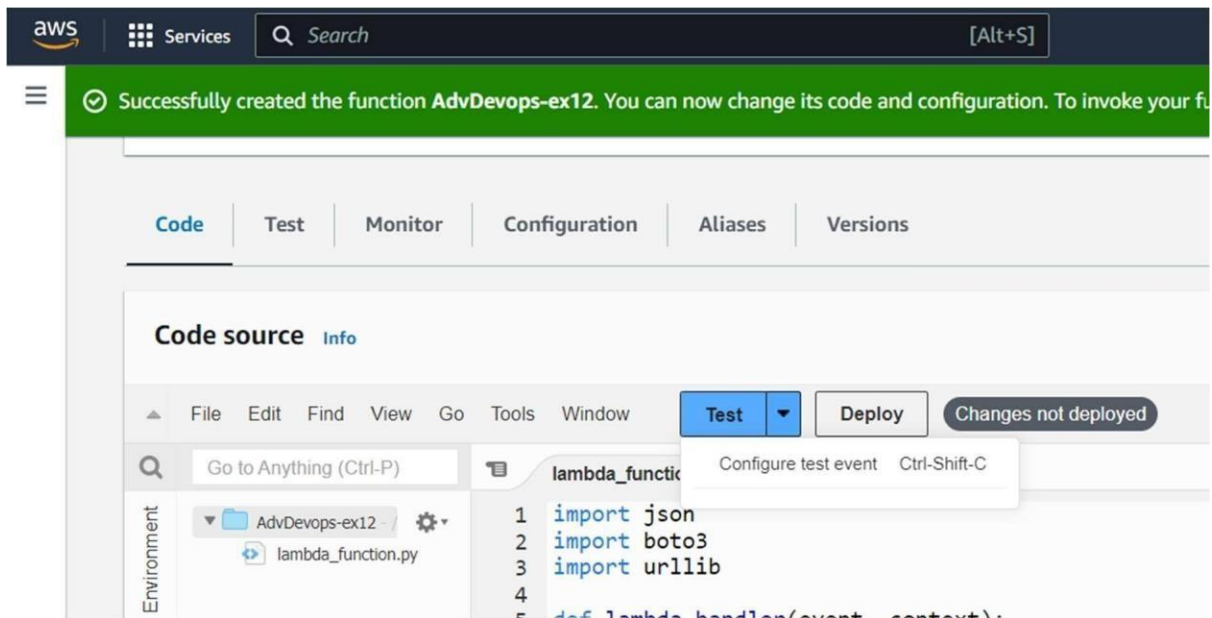
Step 4: The function is up and running.



Step 5: Make the following changes to the function and click on the deploy button. This code basically logs a message and logs the contents of a JSON file which is uploaded to an S3 Bucket and then deploy the code.

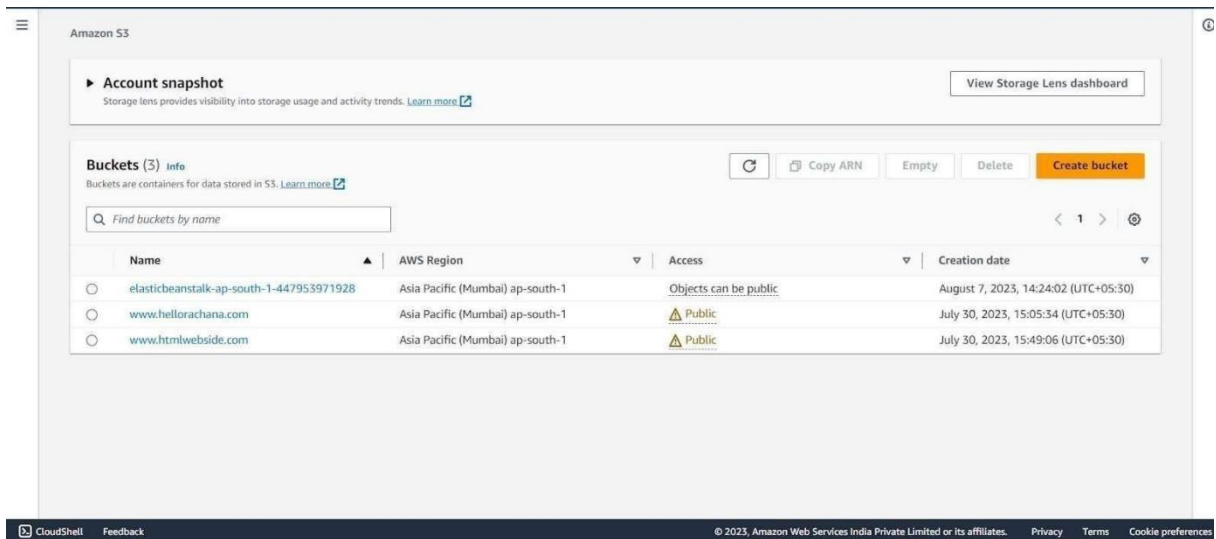


Step 6: Click on Test and choose the 'S3 Put' Template.

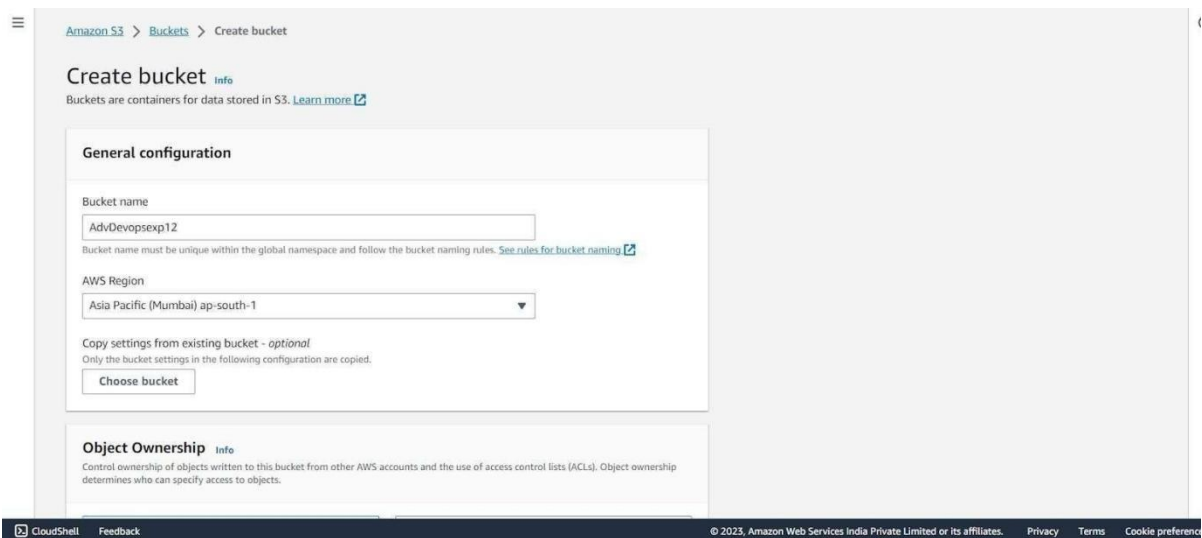


And Save it.

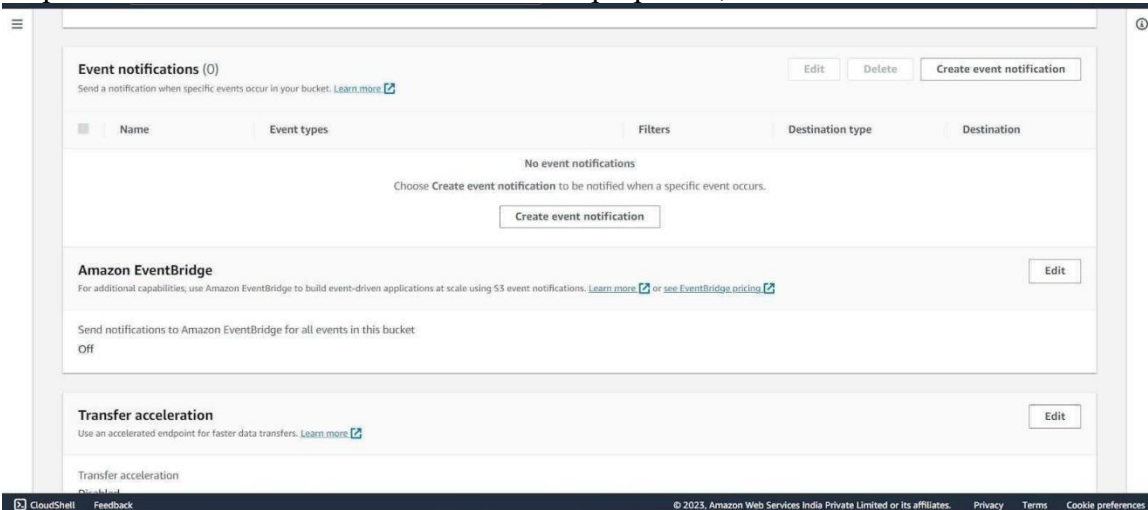
Step 7: Open up the S3 Console and create a new bucket.



Step 8: With all general settings, create the bucket in the same region as the function.



Step 9: Click on the created bucket and under properties, look for events.



Click on Create Event Notification.

Step 10: Mention an event name and check Put under event types.

The screenshot shows the 'General configuration' page in the AWS Event Notifications console. At the top, there's a header with the AWS logo, 'Services', a search bar, and a '[Alt+S]' shortcut. A sidebar on the left contains a menu icon. The main content area is divided into two sections. The first section, 'General configuration', contains three input fields: 'Event name' with the value 'S3putrequest', 'Prefix - optional' with the value 'images/', and 'Suffix - optional' with the value '.jpg'. Each field has a small text note below it: 'Event name can contain up to 255 characters.', 'Limit the notifications to objects with key starting with specified characters.', and 'Limit the notifications to objects with key ending with specified characters.' respectively. The second section, 'Event types', has a descriptive paragraph and a sub-section 'Object creation'. Under 'Object creation', there are two columns of options. The left column has an unchecked checkbox for 'All object create events' with the event name 's3:ObjectCreated:*'. The right column has a checked checkbox for 'Put' with the event name 's3:ObjectCreated:Put' and an unchecked checkbox for 'Post' with the event name 's3:ObjectCreated:Post'. At the bottom of the console, there's a footer bar with 'CloudShell', 'Feedback', and a copyright notice '© 2023, Amazon Web Services India Pr'.

aws Services [Alt+S]

General configuration

Event name
S3putrequest
Event name can contain up to 255 characters.

Prefix - optional
Limit the notifications to objects with key starting with specified characters.
images/

Suffix - optional
Limit the notifications to objects with key ending with specified characters.
.jpg

Event types
Specify at least one event for which you want to receive notifications. For each group, you can choose an event type for all events, or you can choose one or more individual events.

Object creation

☐ All object create events
s3:ObjectCreated:*

☒ Put
s3:ObjectCreated:Put

☐ Post
s3:ObjectCreated:Post

CloudShell Feedback © 2023, Amazon Web Services India Pr

Choose Lambda function as destination and choose your lambda function and save the changes.

The screenshot shows the 'Destination' page in the AWS Event Notifications console. The header and sidebar are identical to the previous screenshot. The main content area has a light blue informational box at the top stating: 'Before Amazon S3 can publish messages to a destination, you must grant the Amazon S3 principal the necessary permissions to call the relevant API to publish messages to an SNS topic, an SQS queue, or a Lambda function. Learn more'. Below this, the 'Destination' section has a heading and a 'Learn more' link. There are three radio button options: 'Lambda function' (selected), 'SNS topic', and 'SQS queue'. Each option has a brief description: 'Run a Lambda function script based on S3 events.', 'Fanout messages to systems for parallel processing or directly to people.', and 'Send notifications to an SQS queue to be read by a server.' respectively. The 'Specify Lambda function' section has two radio button options: 'Choose from your Lambda functions' (selected) and 'Enter Lambda function ARN'. Below this is a dropdown menu labeled 'Lambda function' with the value 'AdvDevops-ex12'. At the bottom right, there are 'Cancel' and 'Save changes' buttons. The footer bar is also identical to the previous screenshot.

aws Services [Alt+S]

Destination

Before Amazon S3 can publish messages to a destination, you must grant the Amazon S3 principal the necessary permissions to call the relevant API to publish messages to an SNS topic, an SQS queue, or a Lambda function. [Learn more](#)

Destination
Choose a destination to publish the event. [Learn more](#)

☒ Lambda function
Run a Lambda function script based on S3 events.

☐ SNS topic
Fanout messages to systems for parallel processing or directly to people.

☐ SQS queue
Send notifications to an SQS queue to be read by a server.

Specify Lambda function

☒ Choose from your Lambda functions

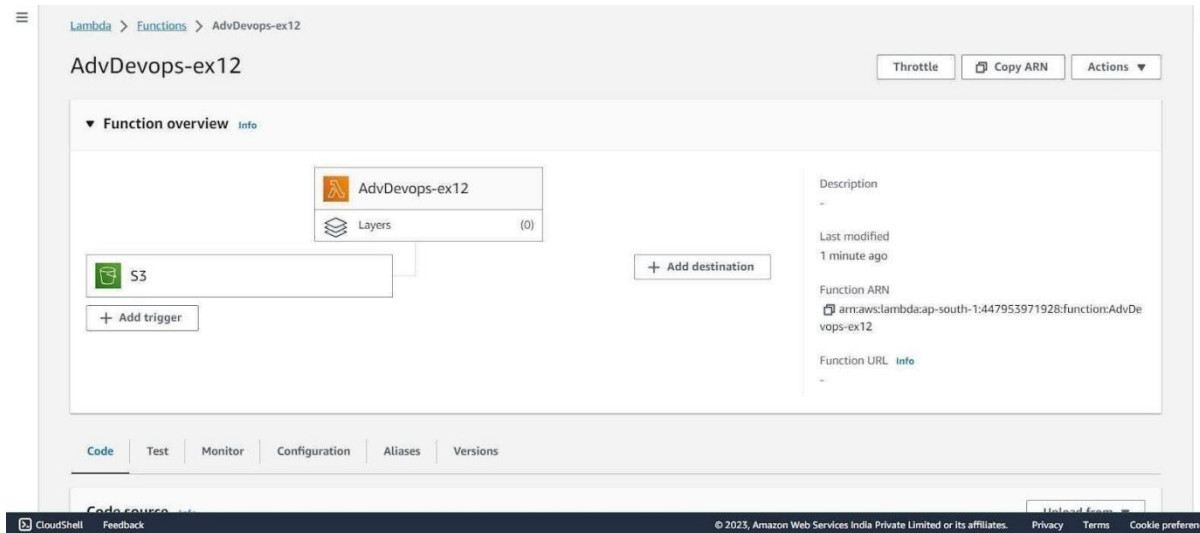
☐ Enter Lambda function ARN

Lambda function
AdvDevops-ex12

Cancel Save changes

CloudShell Feedback © 2023, Amazon Web Serv

Step 11: Refresh the Lambda function console and you should be able to see an S3 Trigger in the overview.

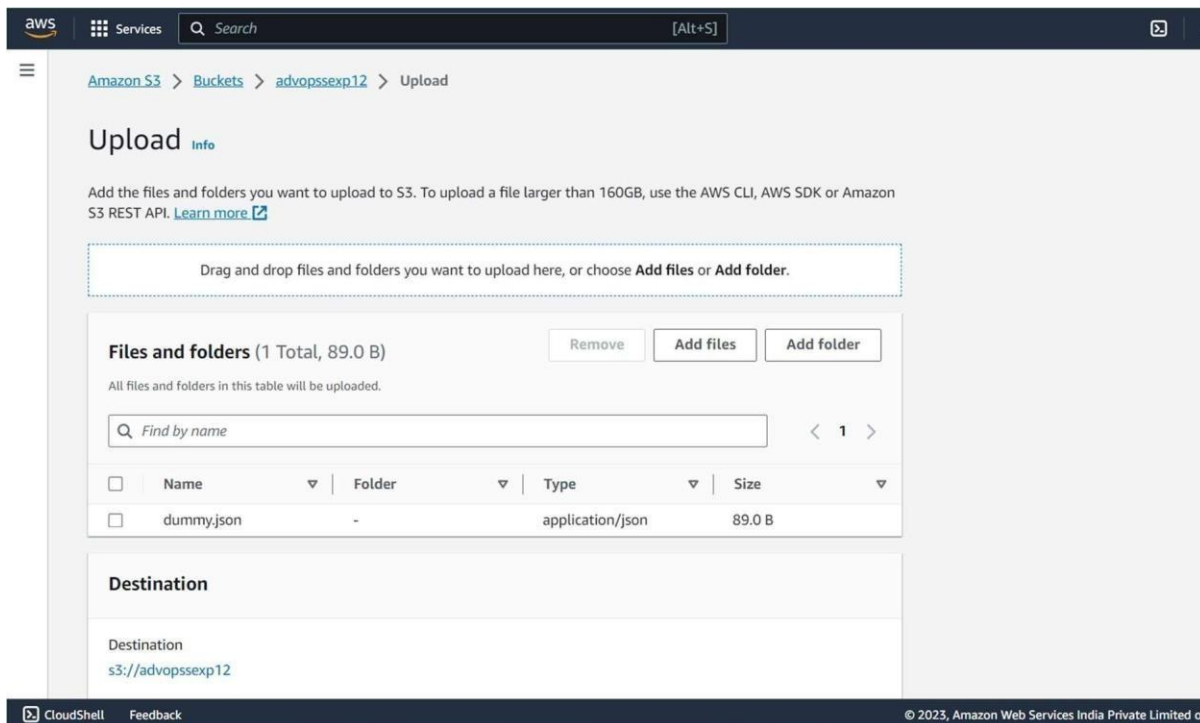


Step 12: Now, create a dummy JSON file locally.

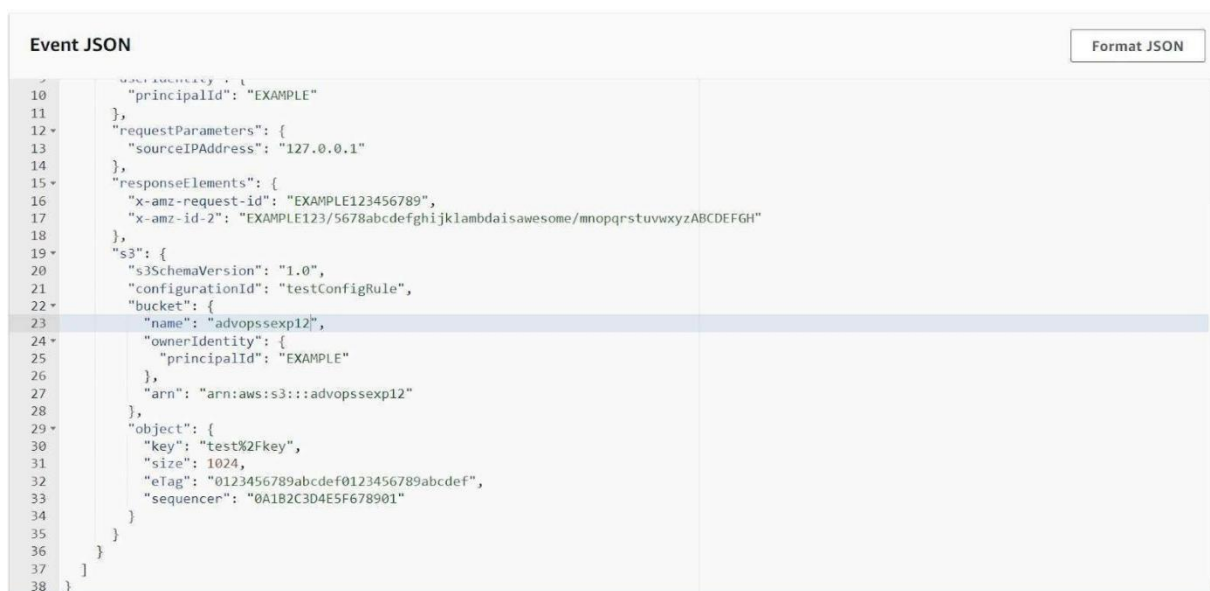


Step 13: Go back to your S3 Bucket and click on Add Files to upload a new file.

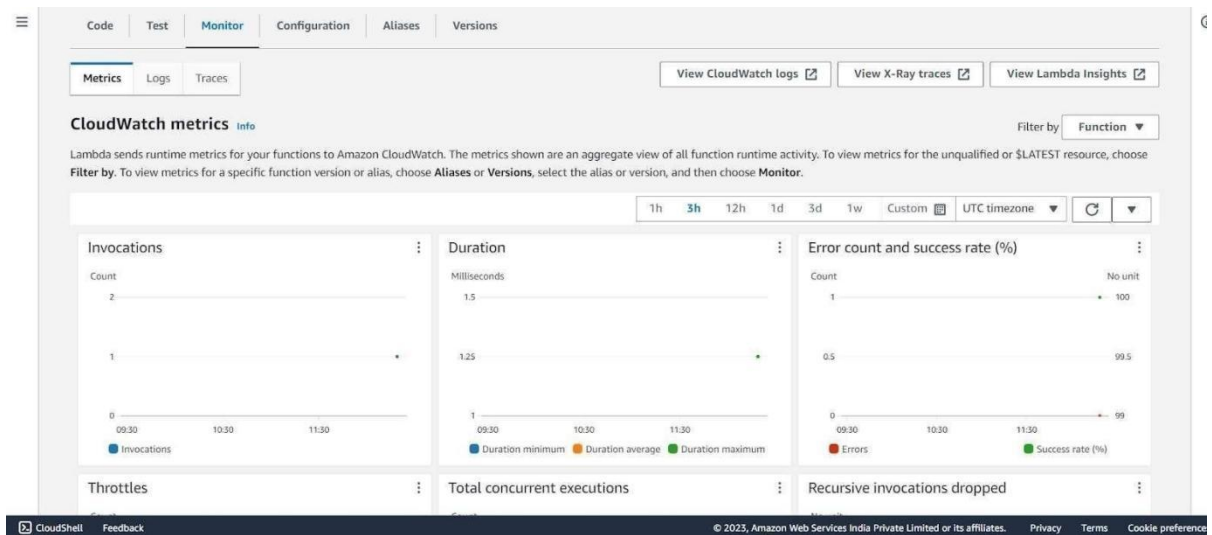
Step 14: Select the dummy data file from your computer and click Upload.



Step 15: After this make the necessary changes in the Test configuration file which we created it previously by replacing the Bucket Name and the ARN of Bucket.



Step 16: Go back to your Lambda function , Refresh it and check the Monitor tab.



Under Log streams, click on View logs in Cloudwatch to check the Function logs.

The screenshot shows the AWS Lambda Log group details page. The page is divided into two main sections: Log group details and Log streams. The Log group details section includes the following information:

- ARN: arn:aws:logs:ap-south-1:447953971928:log-group:/aws/lambda/AdvDevs-ex12:
- Stored bytes: -
- Contributor Insights rules: -
- Creation time: 10 minutes ago
- Retention: Never expire
- Metric filters: 0
- Subscription filters: 0
- KMS key ID: -
- Data protection: -
- Sensitive data count: -

The Log streams section shows a single log stream with the last event time. The log stream is named '2023/10/07/[\$LATEST]e8be4f77339d429081d3b08762b22cab' and the last event time is '2023-10-07 17:49:20 (UTC+05:30)'.

Step 17: Click on this log Stream that was created to view what was logged by your function.

The screenshot shows the AWS Lambda Log events page for a specific log stream. The page displays a list of log events with the following columns: Timestamp and Message. The events are as follows:

Timestamp	Message
2023-10-07T17:49:20.002+05:30	INIT_START Runtime Version: python:3.11.v14 Runtime Version ARN: arn:aws:lambda:ap-south-1::runtime:9c87c21a94b293e1a30aadc23c...
2023-10-07T17:49:20.110+05:30	START RequestId: a189471e-867f-4db4-824f-26b02f956879 Version: \$LATEST
2023-10-07T17:49:20.111+05:30	END RequestId: a189471e-867f-4db4-824f-26b02f956879
2023-10-07T17:49:20.111+05:30	REPORT RequestId: a189471e-867f-4db4-824f-26b02f956879 Duration: 1.25 ms Billed Duration: 2 ms Memory Size: 128 MB Max Memory Us...

Conclusion: Thus, we have created a Lambda function which logs “An Image has been added” once you add an object to a specific bucket in S3.