

Lambda in AWS

- **What is Lambda ?**

- AWS Lambda is a serverless, event-driven computing technology offered by Amazon as part of Amazon Web Services (AWS). This means Amazon Lambda handles all of your infrastructure requirements such as which AWS services to deploy and also how to maintain them.

- **How Does AWS Lambda Work?**

- First, you need to upload the AWS Lambda code or you can directly write it in the Lambda code editor in any language that Lambda supports. It supports a variety of AWS Lambda languages, including Java, **Python**, Go, and C#. AWS Lambda assists you in uploading code as well as the event information that should be used to trigger it. You need to mention the triggering conditions that activate the code.
- An AWS Lambda function is a piece of code that runs on the Lambda runtime environment. The AWS Lambda function is basically used when you just require a function for a short time.

PRACTICAL :

1. First we have to create s3 bucket for the lambda function's deployment package will be uploaded.

The screenshot shows the 'Create bucket' page in the AWS Management Console. The breadcrumb trail is 'Amazon S3 > Buckets > Create bucket'. The page title is 'Create bucket' with an 'Info' link. Below the title, it states 'Buckets are containers for data stored in S3.' The 'General configuration' section is active, showing the 'AWS Region' as 'US East (N. Virginia) us-east-1'. Under 'Bucket type', the 'General purpose' option is selected, with a description: 'Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.' The 'Directory - New' option is also visible. The 'Bucket name' field contains 'myawsbucket', with a note that the name must be unique and follow naming rules. There is a 'Copy settings from existing bucket - optional' section with a 'Choose bucket' button. The 'Object Ownership' section shows 'ACLs disabled (recommended)' selected. The footer includes 'CloudShell', 'Feedback', and copyright information for 2024.

The screenshot shows the 'demo-lambdabucket' page in the AWS Management Console. The breadcrumb trail is 'Amazon S3 > Buckets > demo-lambdabucket'. The page title is 'demo-lambdabucket' with an 'Info' link. Below the title, there are tabs for 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Objects (0)' tab is active, showing a search bar with the placeholder 'Find objects by prefix'. Above the table, there are buttons for 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'. The table has columns for 'Name', 'Type', 'Last modified', 'Size', and 'Storage class'. Below the table, it states 'No objects' and 'You don't have any objects in this bucket.' with an 'Upload' button. The footer includes 'CloudShell', 'Feedback', and copyright information for 2024.

2. Now create a buckets for lambda access and also create IAM user role for access.

The screenshot shows the Amazon S3 console interface. On the left, the 'Storage Lens' section is expanded, showing 'Dashboards', 'Storage Lens groups', and 'AWS Organizations settings'. The main content area displays 'General purpose buckets (8)' with a search bar and a table of buckets. The table has columns for Name, AWS Region, IAM Access Analyzer, and Creation date. The buckets listed are:

Name	AWS Region	IAM Access Analyzer	Creation date
demo-lambdabucket	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 6, 2024, 20:12:09 (UTC+05:30)
demo-mybucket-html	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 6, 2024, 20:27:50 (UTC+05:30)
demo-mybucket-jpeg	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 6, 2024, 20:27:20 (UTC+05:30)
demo-mybucket-pdf	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 6, 2024, 20:27:36 (UTC+05:30)
demo-mybucket-source	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 6, 2024, 20:27:00 (UTC+05:30)
infoperceptbucket	Asia Pacific (Sydney) ap-southeast-2	View analyzer for ap-southeast-2	July 27, 2024, 00:02:29 (UTC+05:30)
inforeplicabucket	Asia Pacific (Sydney) ap-southeast-2	View analyzer for ap-southeast-2	July 27, 2024, 01:11:59 (UTC+05:30)
ip-my-bucket-03	Asia Pacific (Sydney) ap-southeast-2	View analyzer for ap-southeast-2	August 2, 2024, 18:16:45 (UTC+05:30)

The screenshot shows the IAM console interface. On the left, the 'Access management' section is expanded, showing 'User groups', 'Users', 'Roles', 'Policies', 'Identity providers', and 'Account settings'. The main content area displays 'Roles (6)' with a search bar and a table of roles. The roles listed are:

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support(Service-Linker)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor(Service)	-
lambda_prac_role	AWS Service: lambda	-
mylambda-fun-role-xSzos09	AWS Service: lambda	-
s3crr_role_for_infoperceptbucket	AWS Service: s3	10 days ago
SnowFamilyS3Import-DemoJob1-1	AWS Service: importexport	-

Below the table, there is a 'Roles Anywhere' section with a 'Manage' button. The section contains three cards:

- Access AWS from your non AWS workloads**: Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.
- X.509 Standard**: Use your own existing PKI infrastructure or use [AWS Certificate Manager Private Certificate Authority](#) to authenticate identities.
- Temporary credentials**: Use temporary credentials with ease and benefit from the enhanced security they provide.

3. Now create a function in lambda.

Create function [Info](#)

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.

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.
 [Refresh](#)

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](#).

Change the default execution role and select that role for which you create lambda function .

demo-lambda
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.
 [Refresh](#)

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.
 [Refresh](#)
[View the lambda_prac_role role](#) on the IAM console.

► Advanced settings

[Cancel](#) [Create function](#)

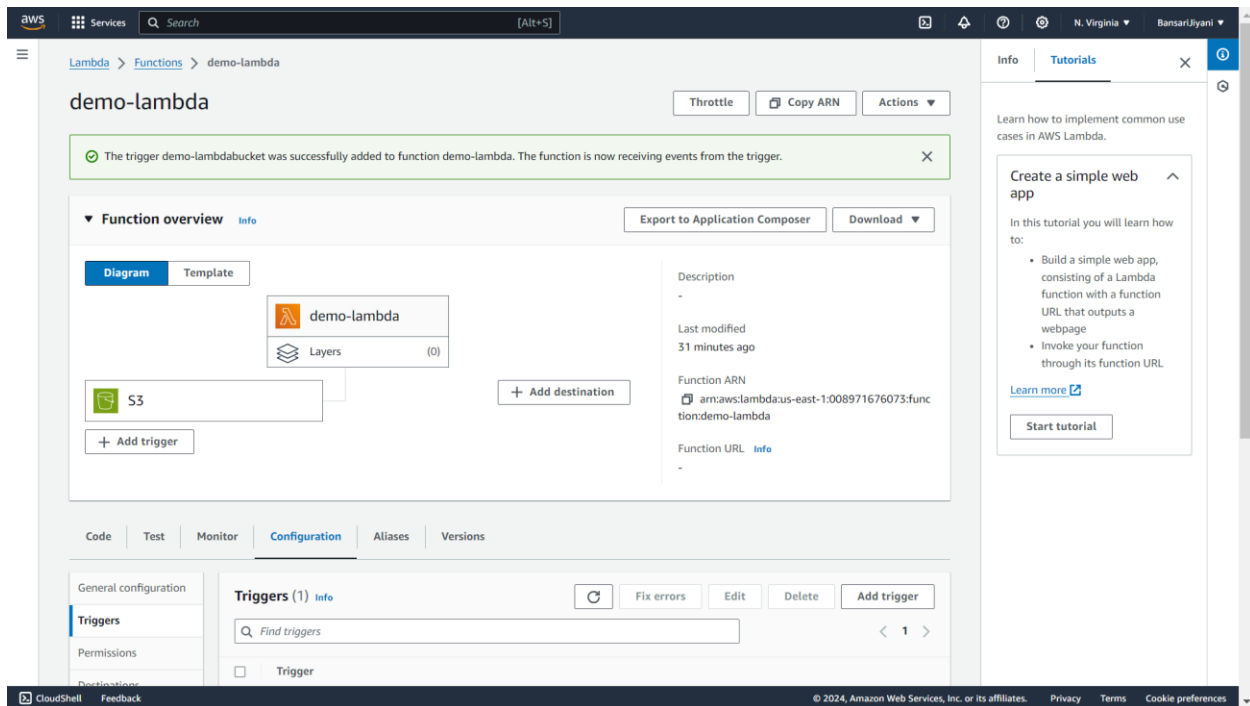
Add a trigger

The screenshot shows the AWS Lambda console for a function named 'demo-lambda'. The 'Function overview' tab is active, displaying a diagram of the function with a 'demo-lambda' box and a 'Layers' box. Below the diagram is a '+ Add trigger' button. To the right, the 'Description' section shows the function's details: 'Last modified 28 minutes ago', 'Function ARN: arn:aws:lambda:us-east-1:008971676073:function:demo-lambda', and 'Function URL: info'. Below the overview, the 'Monitor' tab is active, showing 'View CloudWatch logs', 'View X-Ray traces', 'View Lambda Insights', and 'View CodeGuru profiles' buttons. The 'CloudWatch metrics' section is also visible, showing a graph of metrics over time.

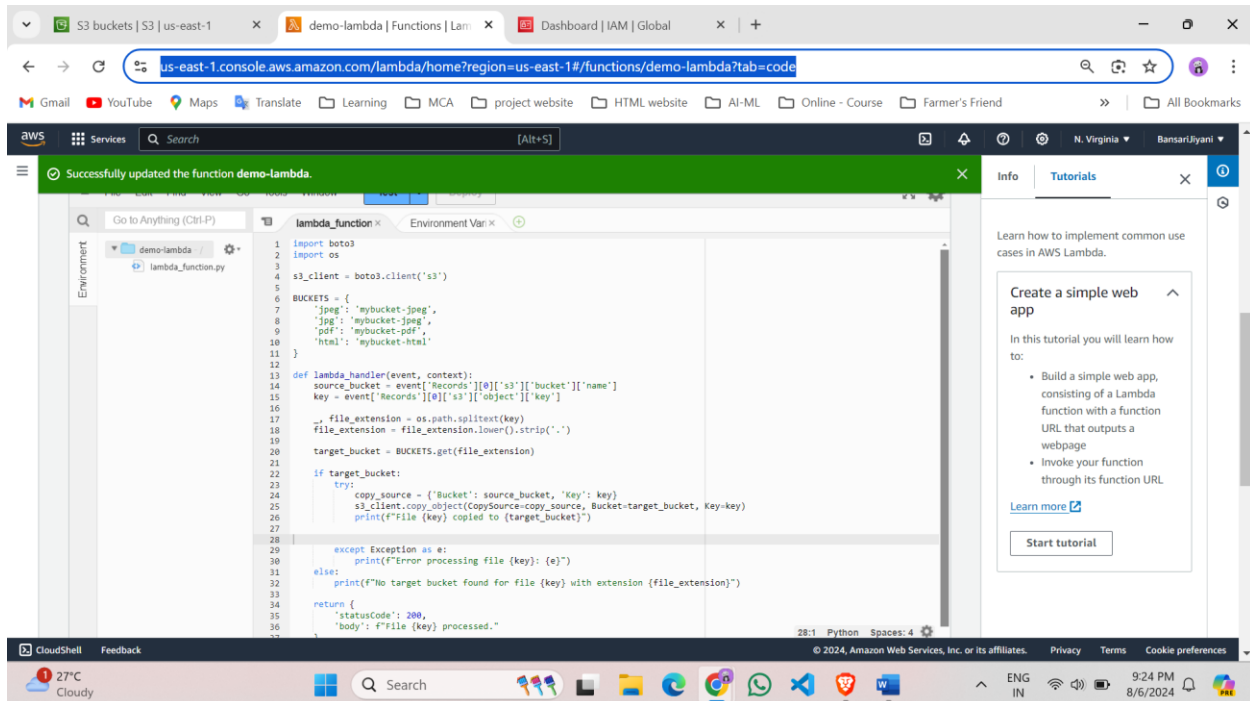
Select the bucket and event type and then add the trigger.

The screenshot shows the 'Add trigger' configuration page in the AWS Lambda console. The 'Trigger configuration' section is active, showing the 'S3' event source. The 'Bucket' field is set to 's3/demo-lambdabucket'. The 'Event types' section shows 'All object create events' selected. The 'Prefix - optional' field is set to 'images/' and the 'Suffix - optional' field is set to '.jpg'. The 'Recursive invocation' section is also visible, with a checkbox for 'I acknowledge that using the same S3 bucket for both input and output is not recommended'.

Now trigger is created.



Upload python lambda function here



Go to the s3 bucket list and select source bucket

us-east-1.console.aws.amazon.com/s3/buckets/demo-mybucket-source?region=us-east-1&bucketType=general&tab=properties

Amazon S3 > Buckets > demo-mybucket-source

demo-mybucket-source

Objects Properties Permissions Metrics Management Access Points

Bucket overview

AWS Region US East (N. Virginia) us-east-1	Amazon Resource Name (ARN) arn:aws:s3::demo-mybucket-source	Creation date August 6, 2024, 20:27:00 (UTC+05:30)
---	--	---

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning
Disabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

28°C Cloudy

Search

ENG IN 9:39 PM 8/6/2024

Scroll down and Go to event notification and create event notification

Access

No data events
No data events to display.
[Configure in CloudTrail](#)

Event notifications (0)

Send a notification when specific events occur in your bucket. [Learn more](#)

Edit Delete Create event notification

Name	Event types	Filters	Destination type	Destination
No event notifications Choose Create event notification to be notified when a specific event occurs. Create event notification				

Amazon EventBridge

For additional capabilities, use Amazon EventBridge to build event-driven applications at scale using S3 event notifications. [Learn more](#) or [see EventBridge pricing](#)

Send notifications to Amazon EventBridge for all events in this bucket
Off

Edit

Transfer acceleration

Use an accelerated endpoint for faster data transfers. [Learn more](#)

Transfer acceleration
Disabled

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Services

Search

[Alt+S]

N. Virginia

BansariJiyani

Amazon S3

Buckets

demo-mybucket-source

Create event notification

Create event notification

To enable notifications, you must first add a notification configuration that identifies the events you want Amazon S3 to publish and the destinations where you want Amazon S3 to send the notifications.

General configuration

Event name

file-upload-event

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

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Services

Search

[Alt+S]

N. Virginia

BansariJiyani

Intelligent-Tiering

☐ Intelligent-Tiering archive events
s3:IntelligentTiering

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

demo-lambda

Cancel

Save changes

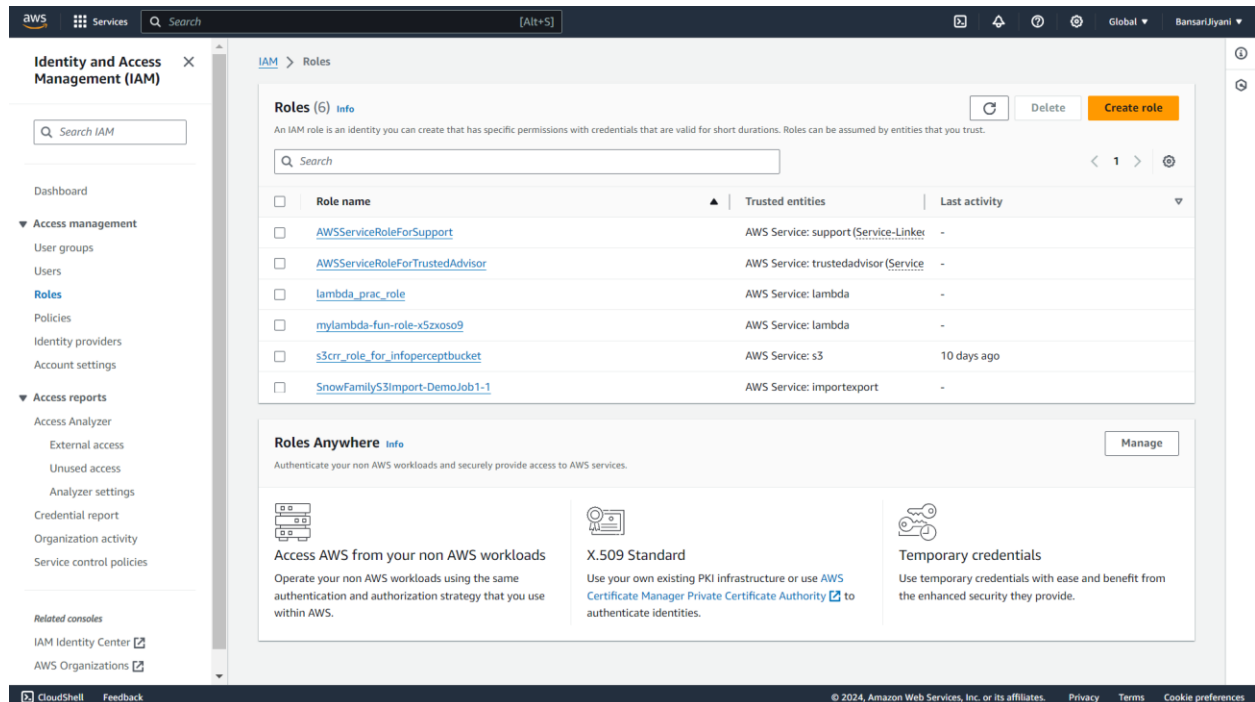
CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Update IAM role policies

1. Select the role of lambda user

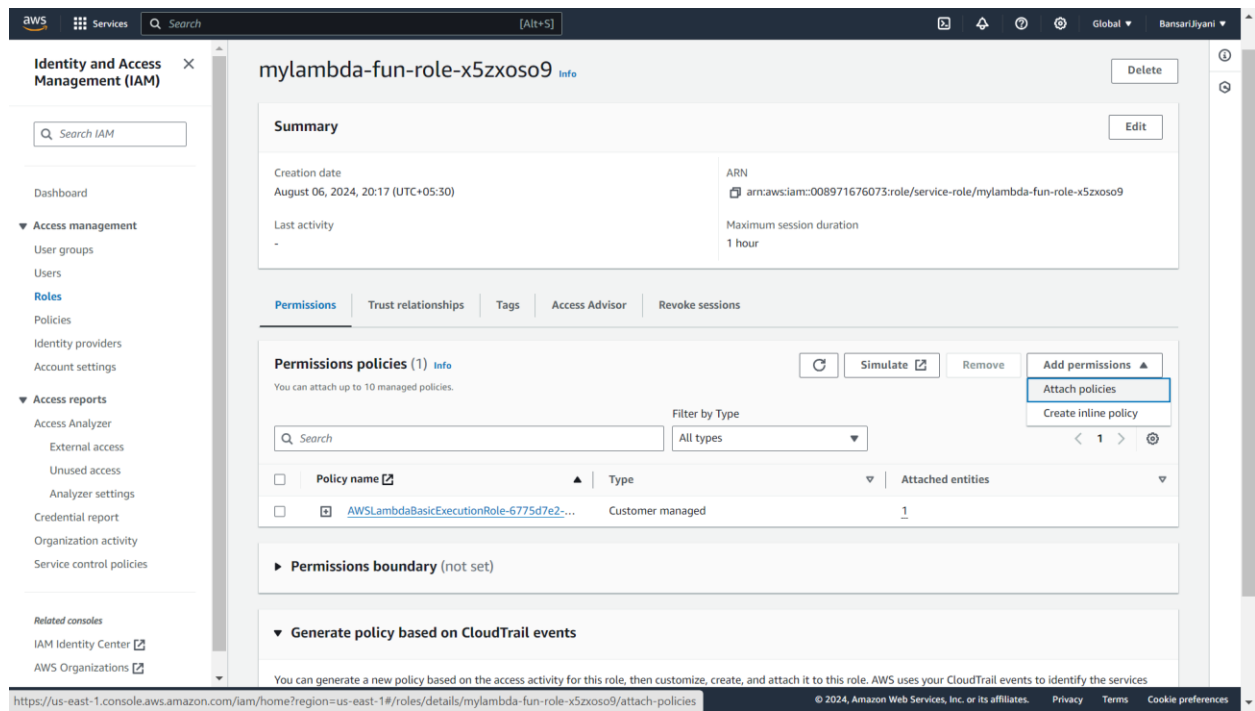


The screenshot shows the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible with options like Dashboard, Access management, Roles, Policies, and Access reports. The main content area displays the 'Roles (6)' section, which includes a table of roles. The roles listed are:

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linker)	-
lambda_prac_role	AWS Service: lambda	-
mylambda-fun-role-x5zxo9	AWS Service: lambda	-
s3crr_role_for_infoperceptbucket	AWS Service: s3	10 days ago
SnowFamilyS3Import-DemoJob1-1	AWS Service: importexport	-

Below the table, the 'Roles Anywhere' section is visible, which includes options for 'Access AWS from your non AWS workloads', 'X.509 Standard', and 'Temporary credentials'.

2. Attach/add policies

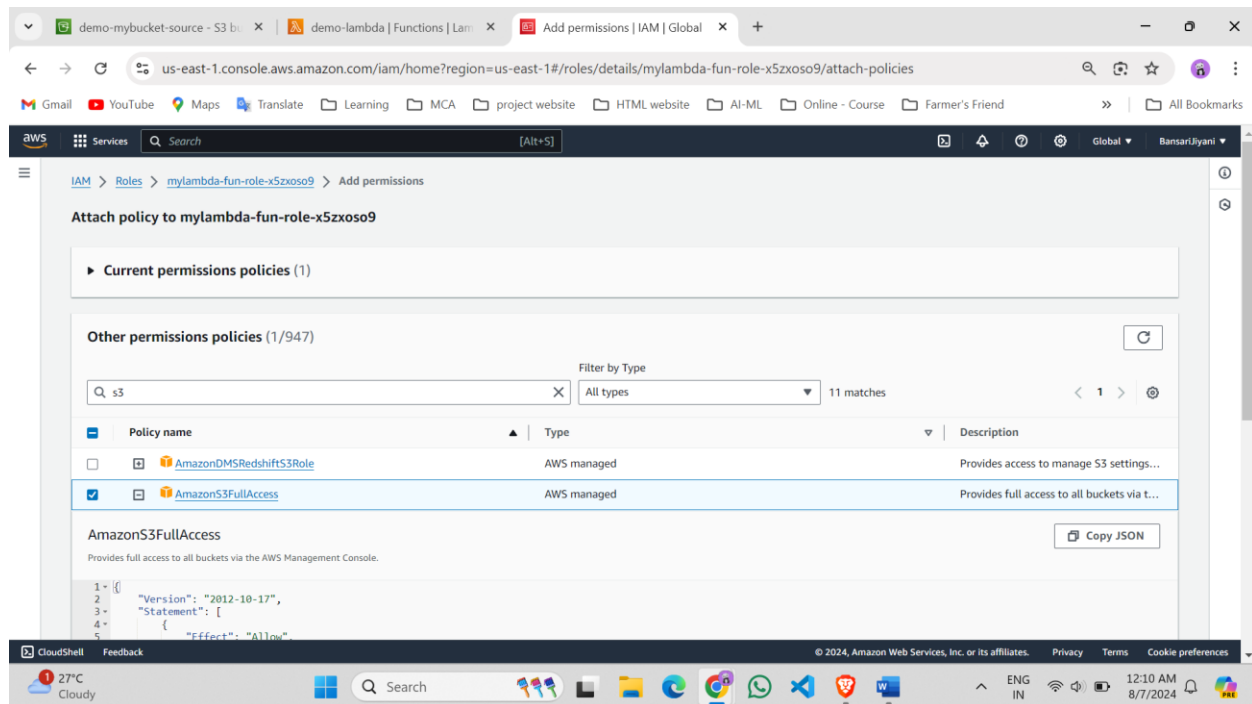


The screenshot shows the AWS IAM console interface for the 'mylambda-fun-role-x5zxo9' role. The 'Permissions' tab is selected, displaying a list of attached policies. The policies listed are:

Policy name	Type	Attached entities
AWSLambdaBasicExecutionRole-6775d7e2-...	Customer managed	1

Below the table, the 'Permissions boundary' section is visible, which is currently 'not set'. The 'Generate policy based on CloudTrail events' section is also visible, which allows users to generate a new policy based on the access activity for this role.

3. Add permission AmazonS3FullAccess



4. Add the files using this command

`aws s3 cp sample.jpg s3://mybucket-source/sample.jpg`

`aws s3 cp document.pdf s3://mybucket-source/document.pdf`

`aws s3 cp index.html s3://mybucket-source/index.html`