Project 2: Developing a Serverless application in AWS

Develop a serverless application in AWS using the following services:
- AWS S3,
- AWS Lambda and
- AWS DynamoDB

The application should perform the following operations:
- Operator/user uploads the JSON file having employee details to the S3 bucket.
- After every new file in S3 bucket, a Lambda function has to trigger which should process the JSON file and update the DynamoDB table with the employee details present in the JSON file

This Document Covers the follwoing sections:

1. Archtitctural Diagram

2. Creating IAM Policy and Role to Lambda

3. Creating Dynamo DB Table

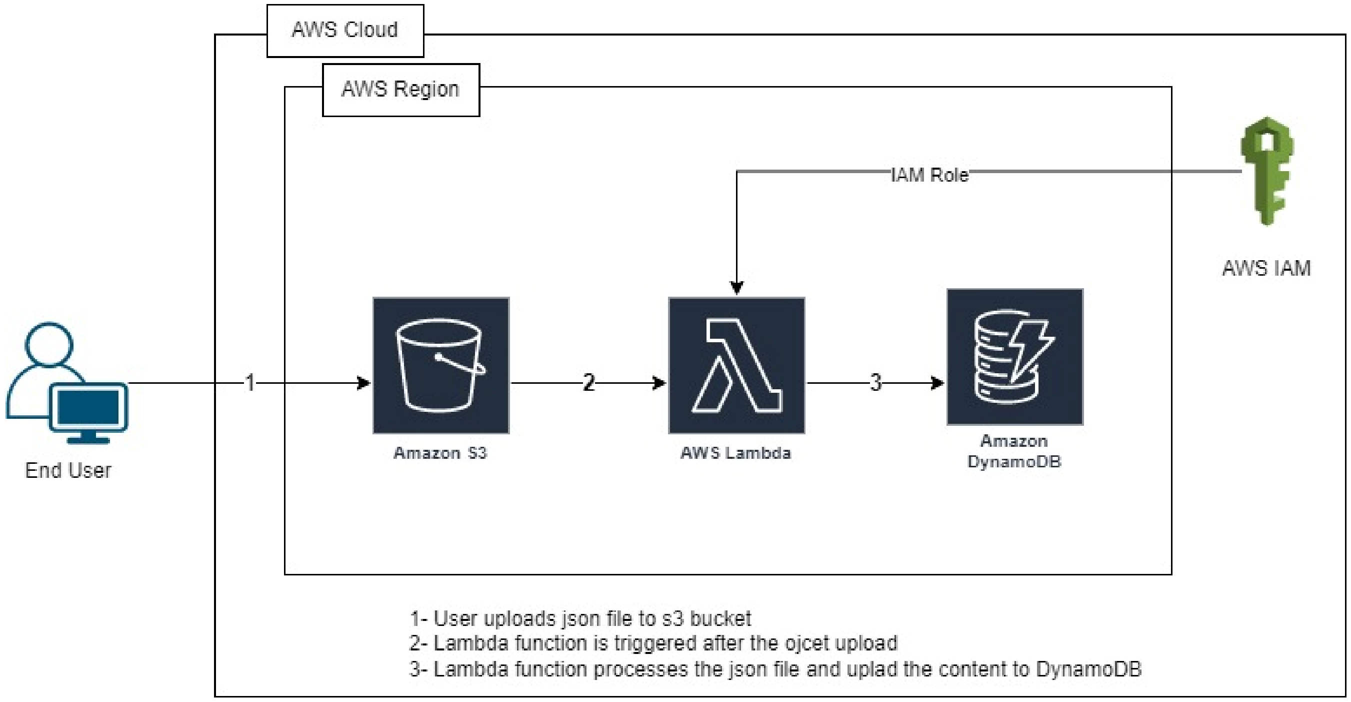
4. Creating S3 bucket

5. Creating Lambda function

6. Testing the serverless application

1. Architecture of Serverless Application in AWS

(AWS S3, AWS Lambda and AWS DynamoDB)

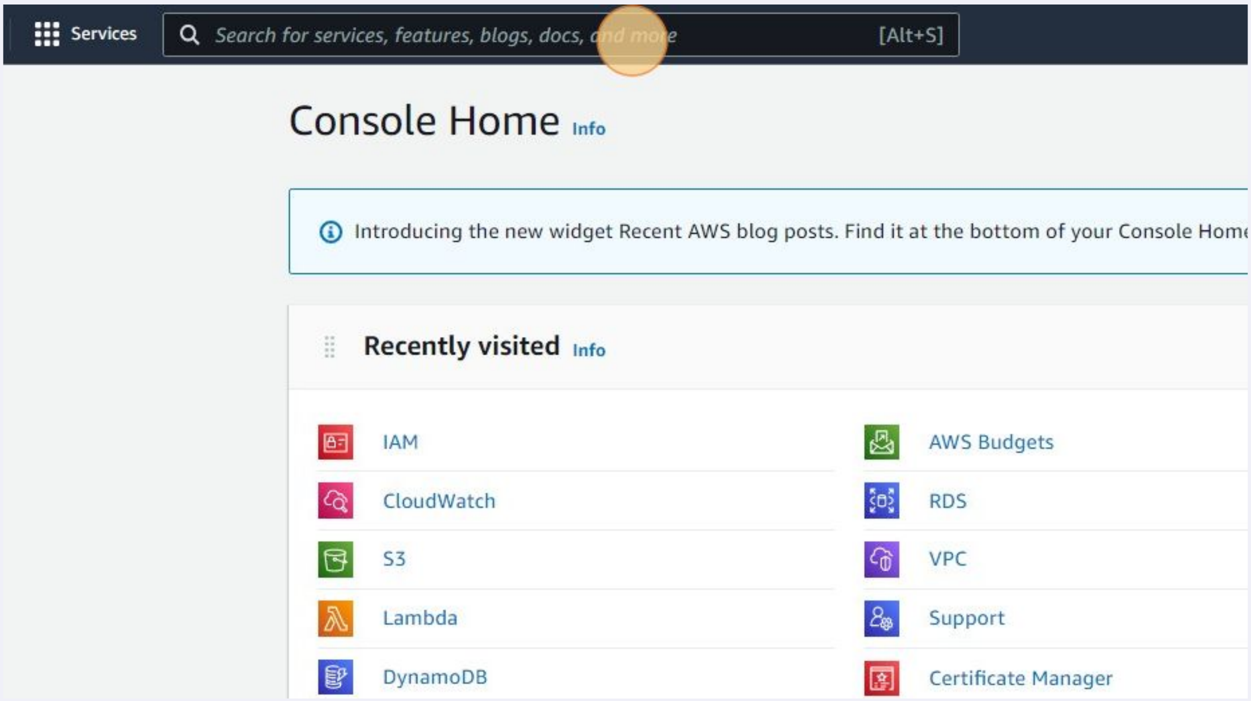


1- User uploads json file to s3 bucket
2- Lambda function is triggered after the ojcet upload
3- Lambda function processes the json file and uplad the content to DynamoDB

2. Creating IAM Policy and Role to Lambda

1 Navigate to https://ap-south-1.console.aws.amazon.com/console/home?region=ap-south-1

2 Click the "Search for services, features, blogs, docs, and more" field.



Console Home Info

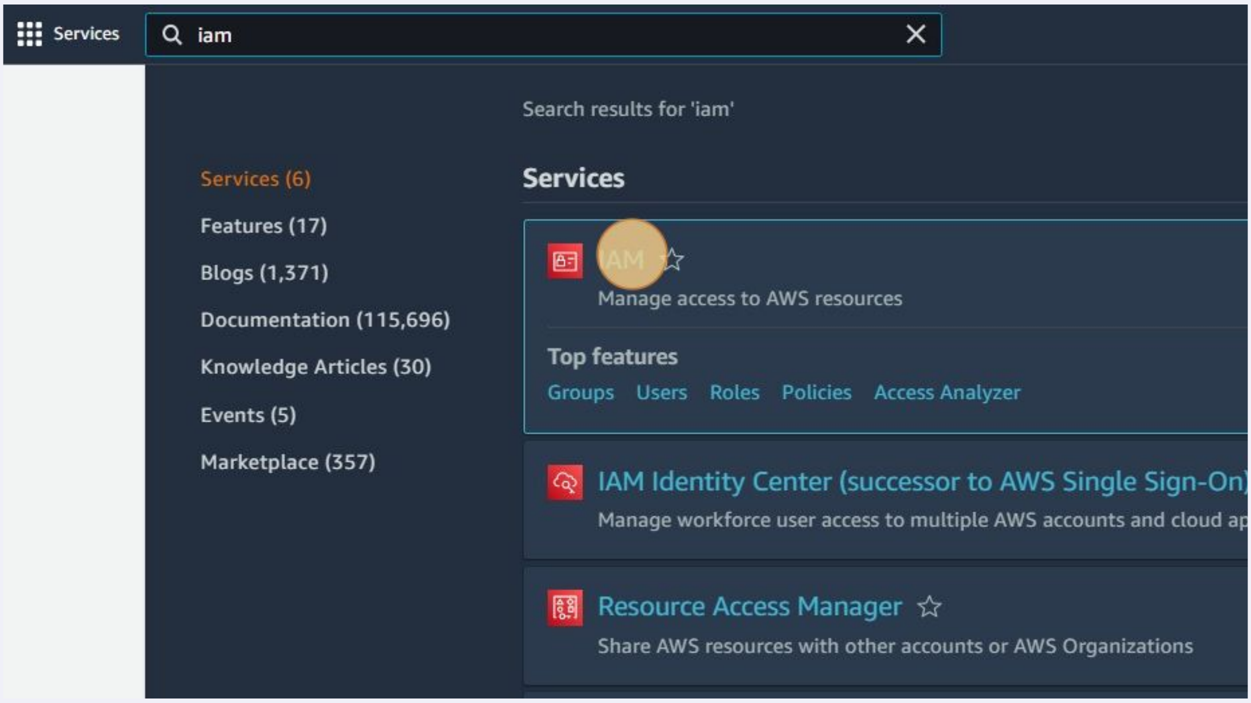
Introducing the new widget Recent AWS blog posts. Find it at the bottom of your Console Home

Recently visited Info

IAM	AWS Budgets
CloudWatch	RDS
S3	VPC
Lambda	Support
DynamoDB	Certificate Manager

3 Type "iam"

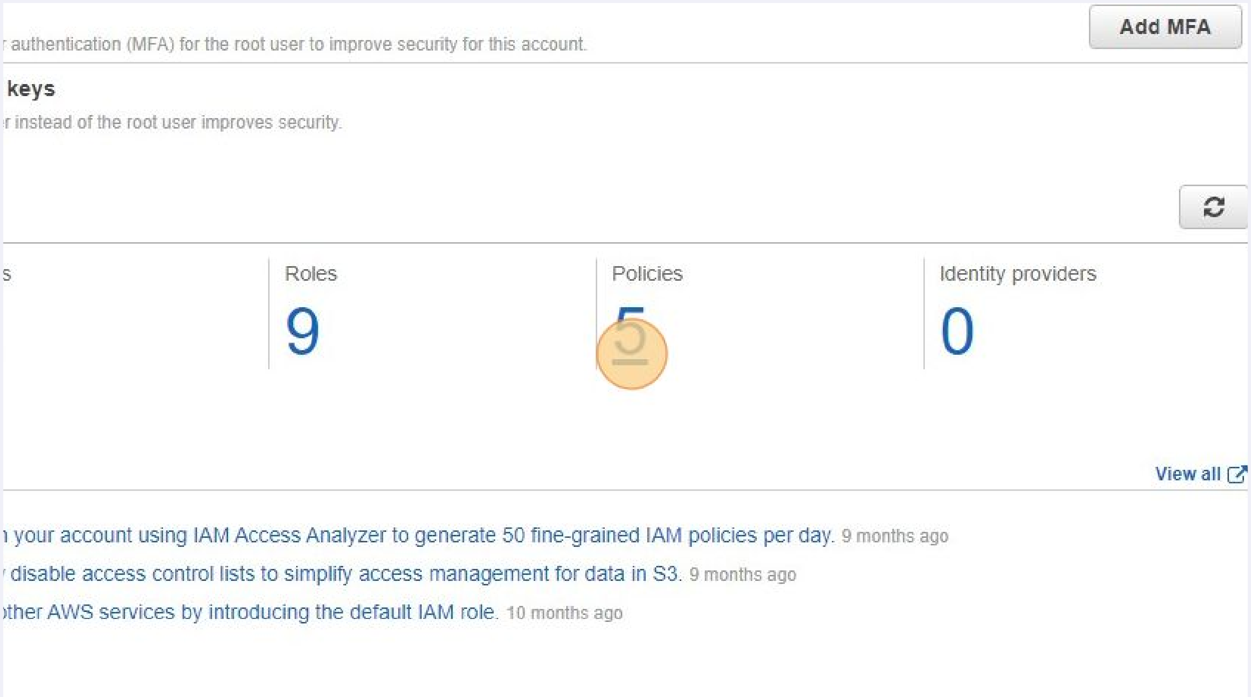
4 Click "IAM"



Search results for 'iam'

Services
iam
Services (6)
Features (17)
Blogs (1,371)
Documentation (115,696)
Knowledge Articles (30)
Events (5)
Marketplace (357)
Services
IAM
Manage access to AWS resources
Top features
Groups
Users
Roles
Policies
Access Analyzer
IAM Identity Center (successor to AWS Single Sign-On)
Manage workforce user access to multiple AWS accounts and cloud ap
Resource Access Manager
Share AWS resources with other accounts or AWS Organizations

5 Click "Policies"



authentication (MFA) for the root user to improve security for this account.

keys

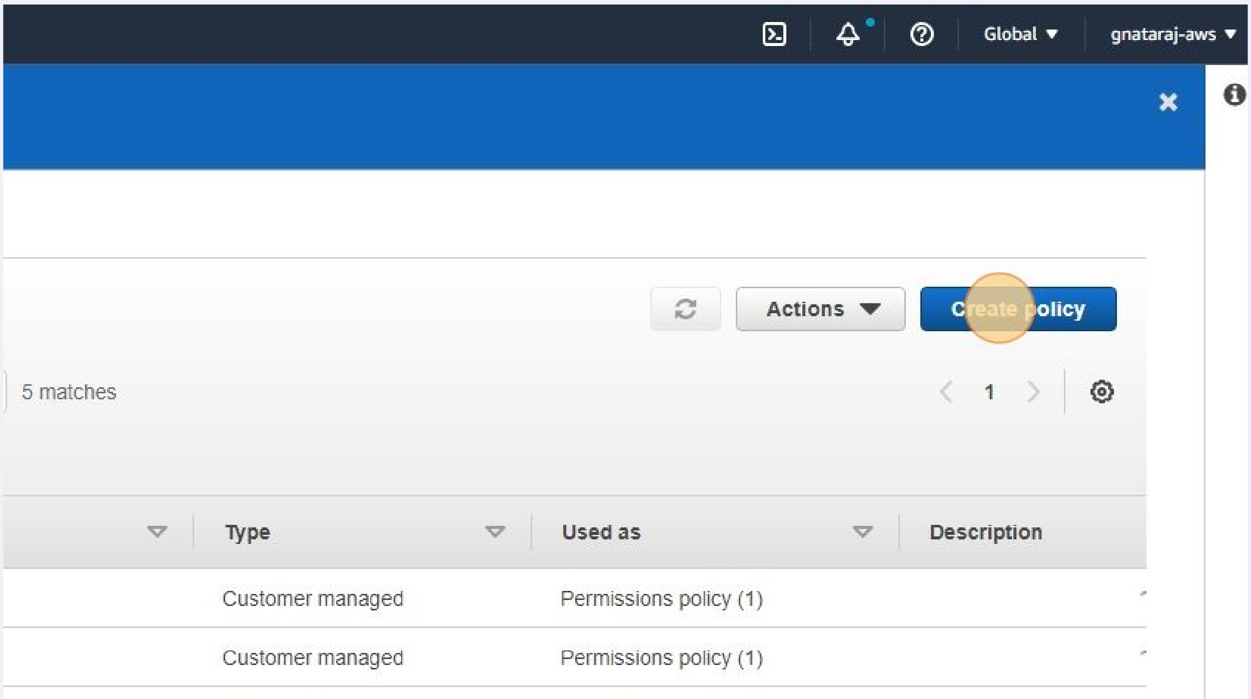
r instead of the root user improves security.

your account using IAM Access Analyzer to generate 50 fine-grained IAM policies per day. 9 months ago

disable access control lists to simplify access management for data in S3. 9 months ago

ther AWS services by introducing the default IAM role. 10 months ago

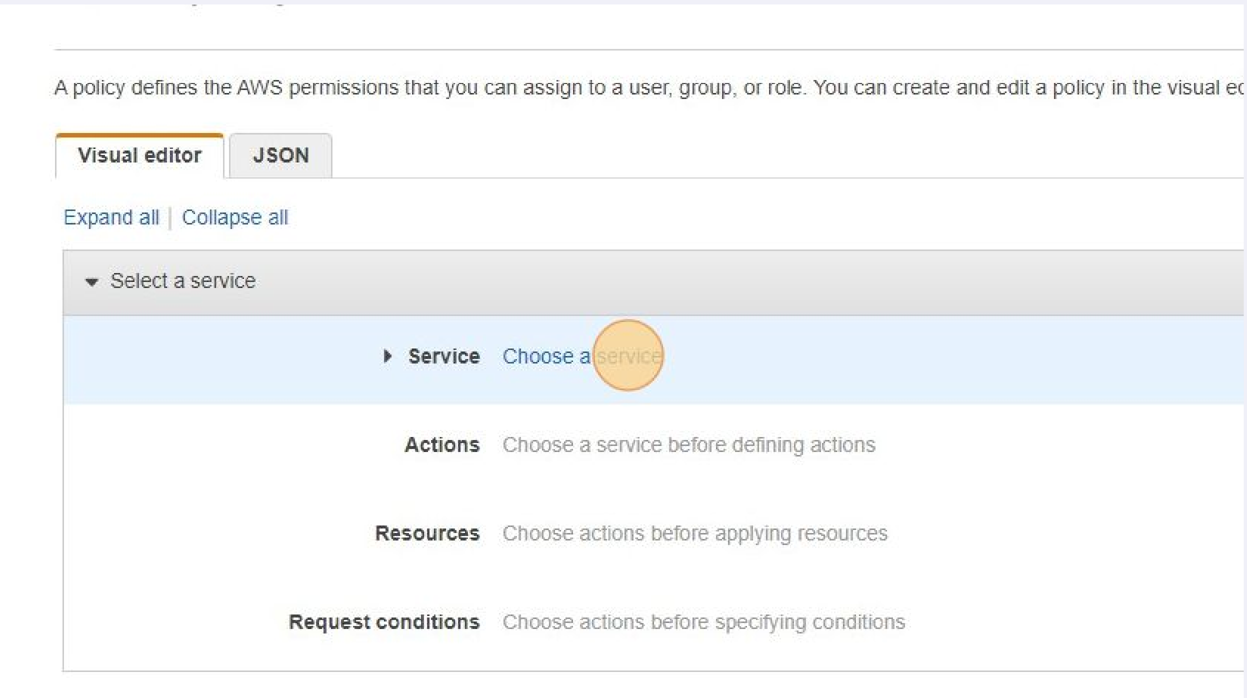
6 Click "Create policy"



5 matches

	Type	Used as	Description
	Customer managed	Permissions policy (1)	
	Customer managed	Permissions policy (1)	

7 Click here.



A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual ec

Service Choose a service

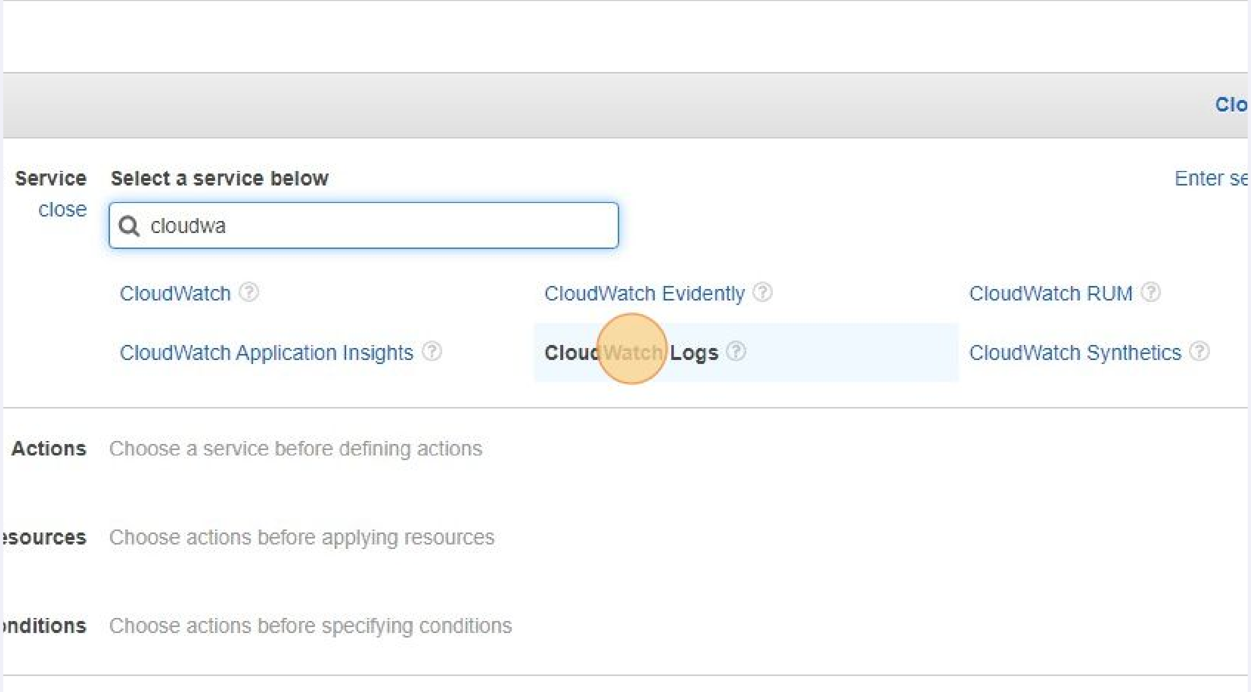
Actions Choose a service before defining actions

Resources Choose actions before applying resources

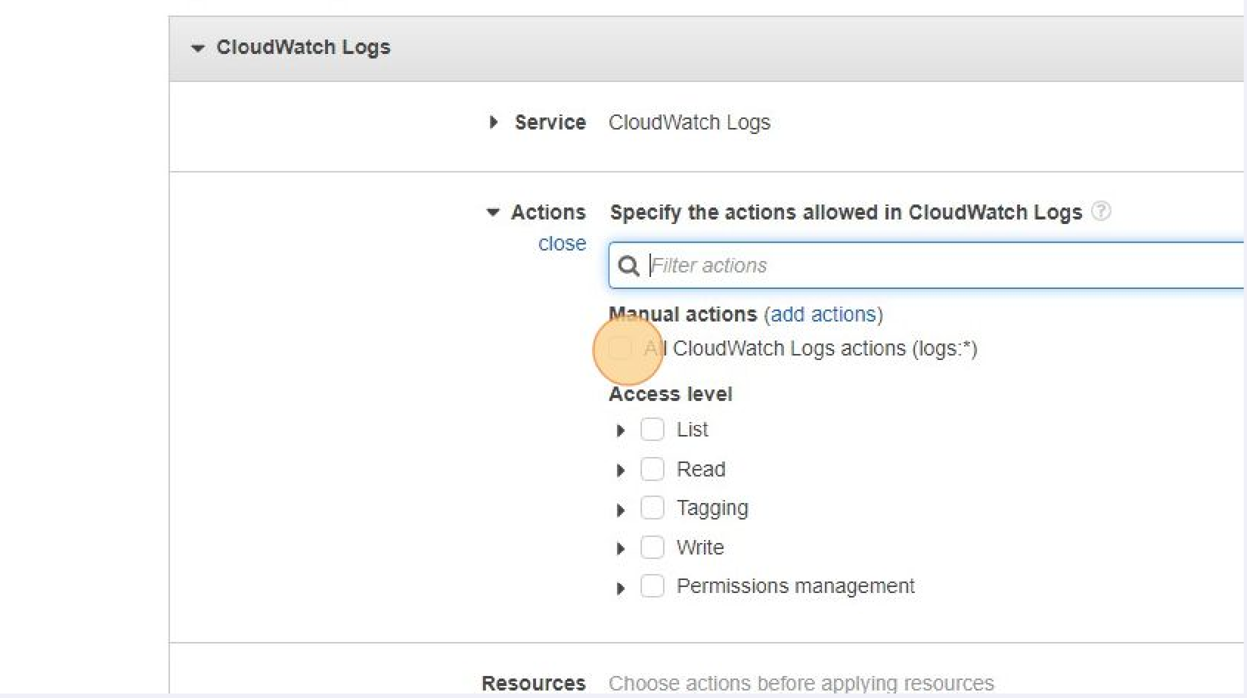
Request conditions Choose actions before specifying conditions

8 Type "CloudWatch Logs"

9 Click "CloudWatch Logs"



10 Select All CloudWatch Logs actions



CloudWatch Logs

Service CloudWatch Logs

Actions Specify the actions allowed in CloudWatch Logs
close

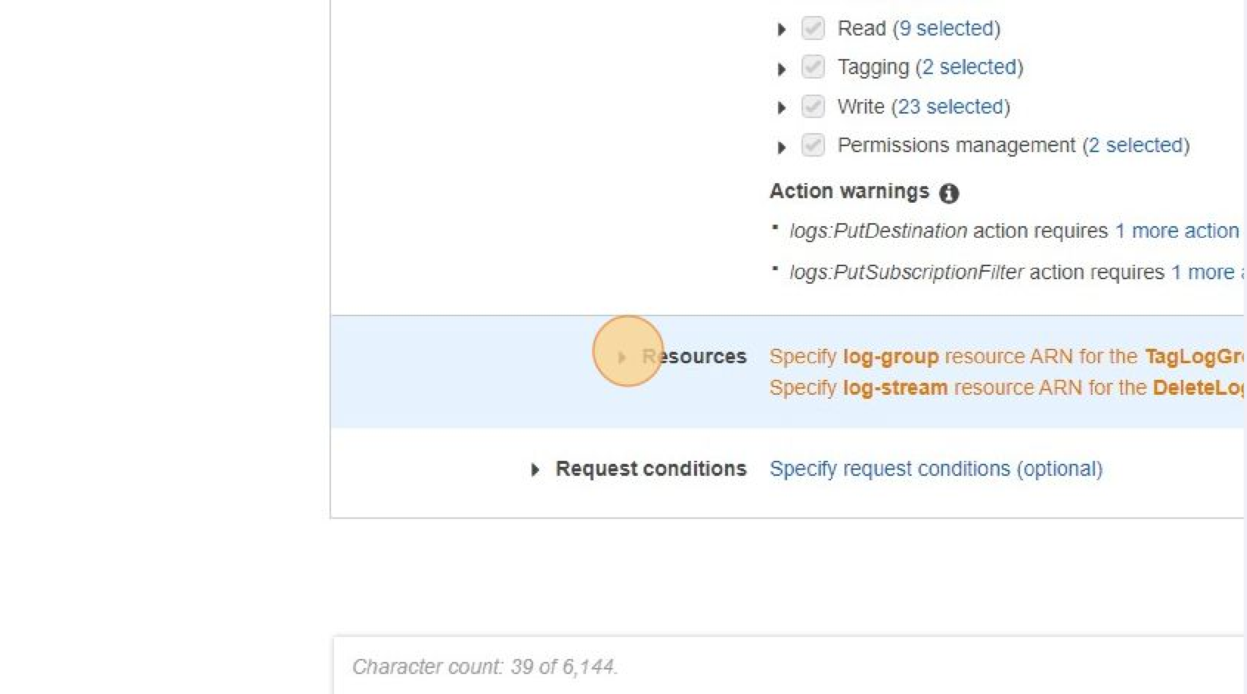
Filter actions

Manual actions (add actions)
□ All CloudWatch Logs actions (logs:*)

Access level
□ List
□ Read
□ Tagging
□ Write
□ Permissions management

Resources Choose actions before applying resources

11 Expand Resources



☑ Read (9 selected)
☑ Tagging (2 selected)
☑ Write (23 selected)
☑ Permissions management (2 selected)

Action warnings

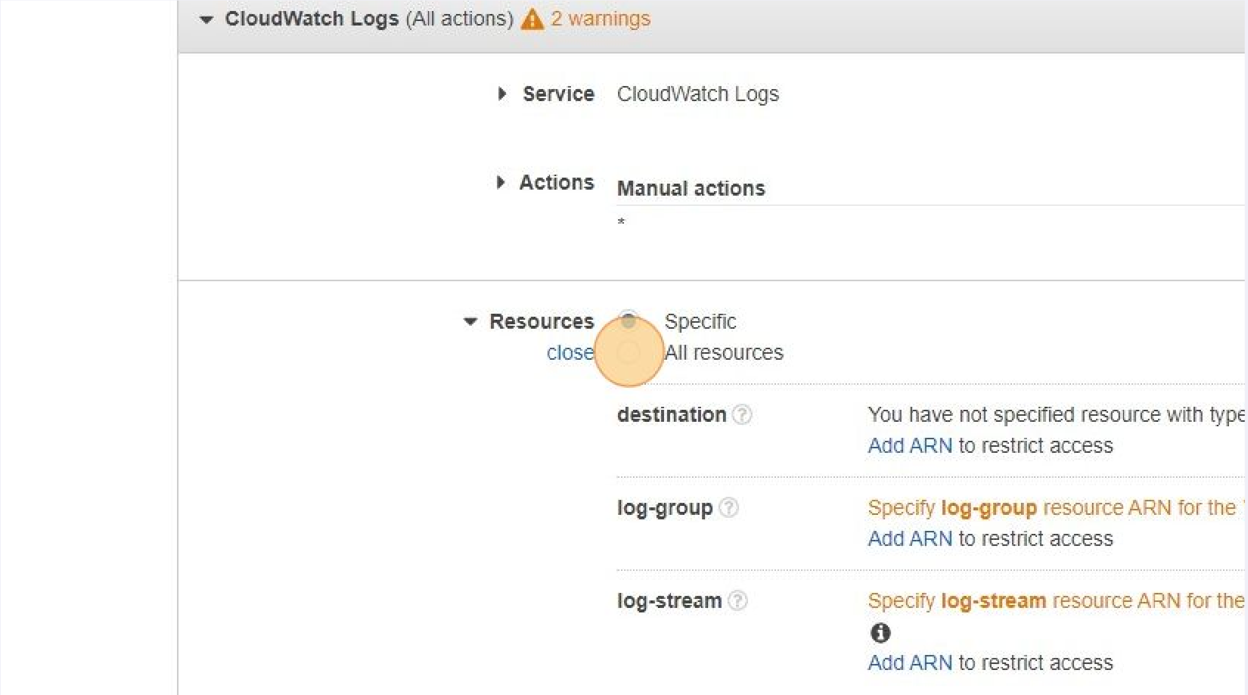
- logs:PutDestination action requires 1 more action
- logs:PutSubscriptionFilter action requires 1 more a

Resources Specify log-group resource ARN for the TagLogGr
Specify log-stream resource ARN for the DeleteLo

Request conditions Specify request conditions (optional)

Character count: 39 of 6,144.

12 Select All resources



CloudWatch Logs (All actions) ⚠ 2 warnings

Service: CloudWatch Logs

Actions: Manual actions
*

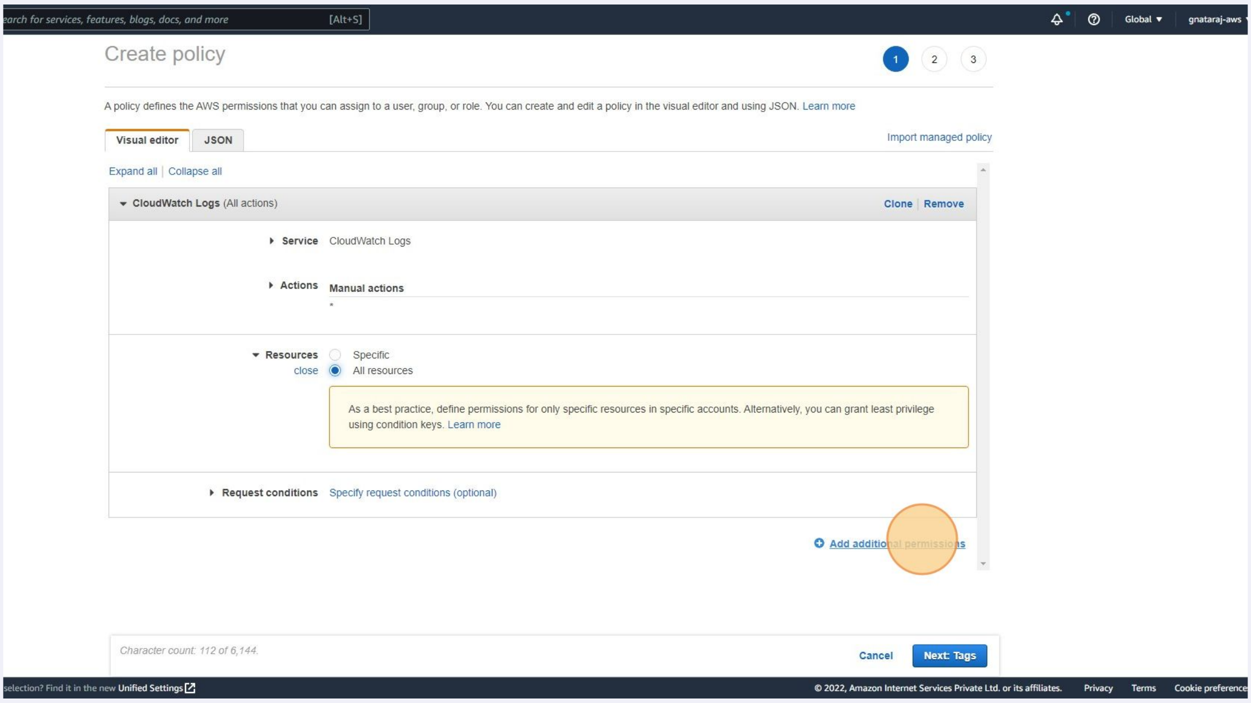
Resources (close): ○ Specific ○ All resources

destination: You have not specified resource with type
Add ARN to restrict access

log-group: Specify **log-group** resource ARN for the
Add ARN to restrict access

log-stream: Specify **log-stream** resource ARN for the
Add ARN to restrict access

13 Click "Add additional permissions"



earch for services, features, blogs, docs, and more [Alt+S]
Global ▾
gnataraj-aws
1
2
3

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

Visual editor
JSON
Import managed policy
Expand all | Collapse all
Clone | Remove

CloudWatch Logs (All actions)

Service: CloudWatch Logs

Actions: Manual actions
*

Resources (close): ○ Specific ● All resources

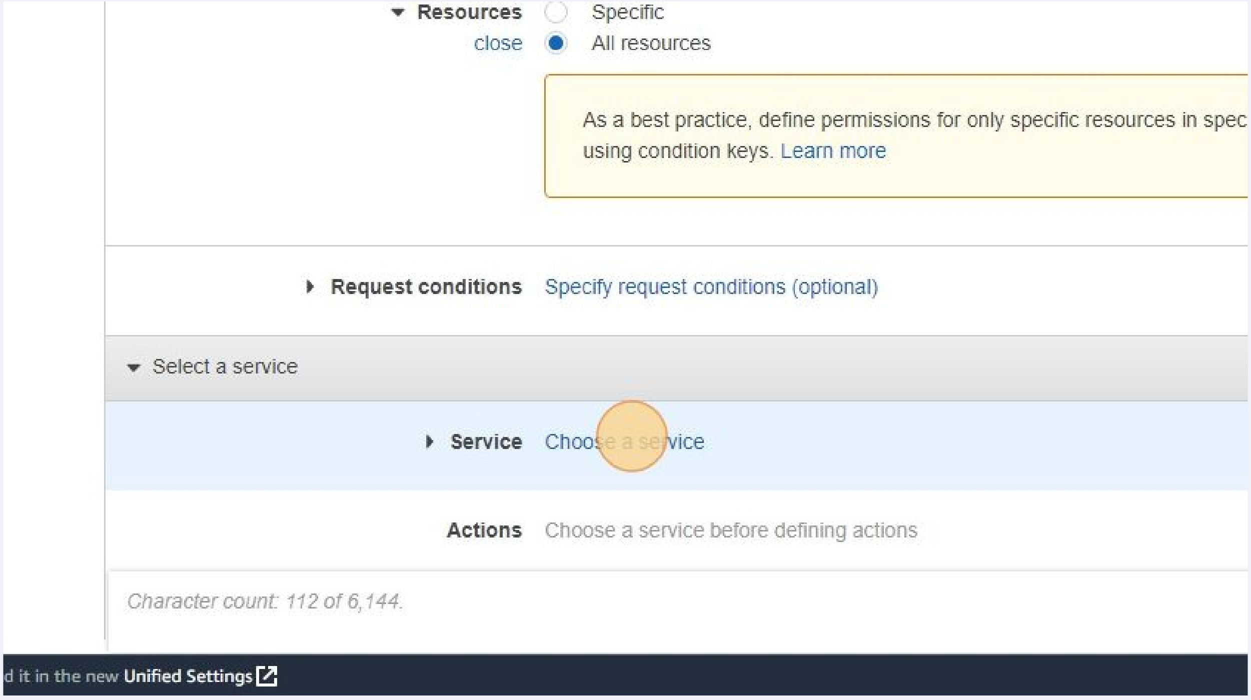
As a best practice, define permissions for only specific resources in specific accounts. Alternatively, you can grant least privilege using condition keys. Learn more

Request conditions: Specify request conditions (optional)

Character count: 112 of 6,144.

Cancel
Next: Tags
selection? Find it in the new Unified Settings
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preference

14 Click "Choose a service.



Resources ○ Specific
close ● All resources

As a best practice, define permissions for only specific resources in spec
using condition keys. Learn more

Request conditions Specify request conditions (optional)

Select a service

Service Choose a service

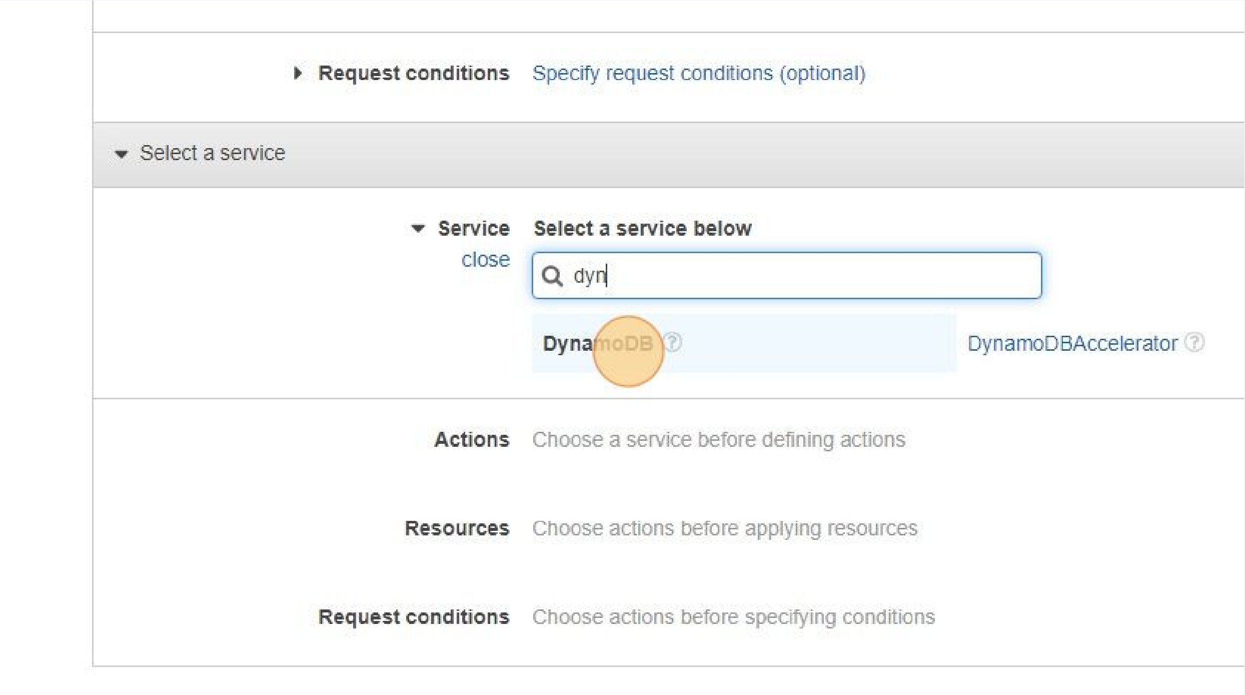
Actions Choose a service before defining actions

Character count: 112 of 6,144.

d it in the new **Unified Settings**

15 Type "DynamoDB"

16 Click "DynamoDB"



▸ Request conditions Specify request conditions (optional)

▾ Select a service

▾ Service Select a service below

close

dyn

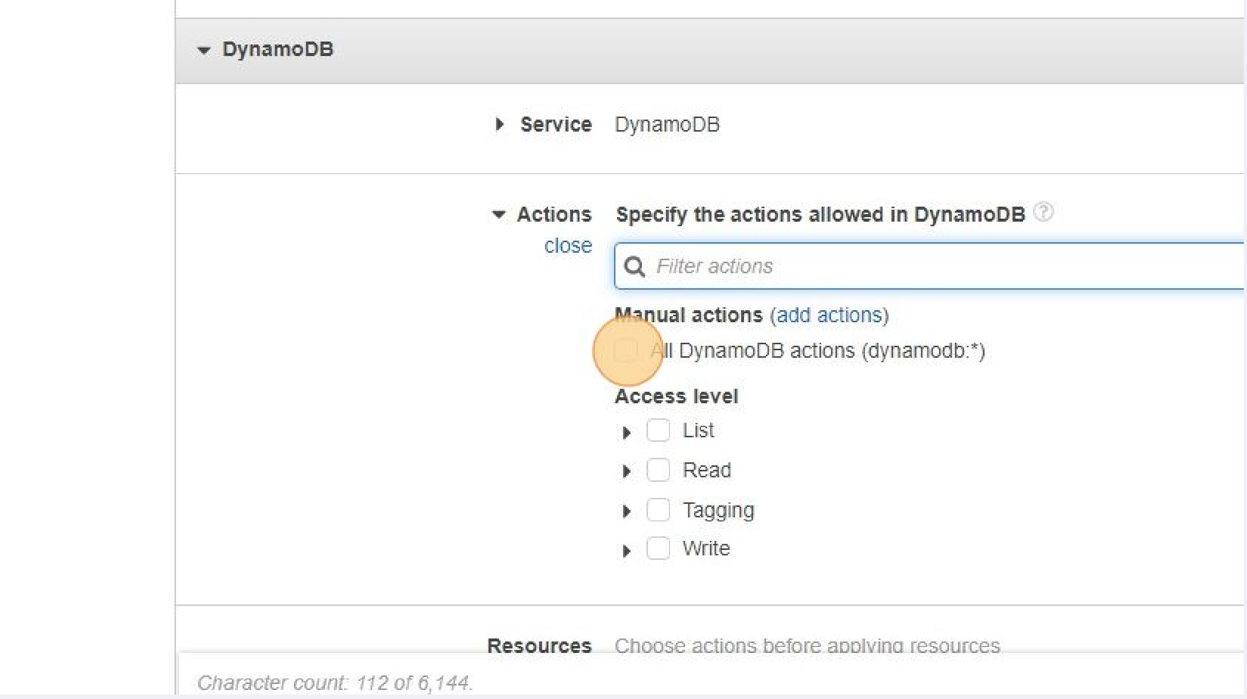
DynamoDB ⓘ DynamoDBAccelerator ⓘ

Actions Choose a service before defining actions

Resources Choose actions before applying resources

Request conditions Choose actions before specifying conditions

17 Select All DynamoDB actions



▾ DynamoDB

▸ Service DynamoDB

▾ Actions Specify the actions allowed in DynamoDB ⓘ

close

Filter actions

Manual actions (add actions)

□ All DynamoDB actions (dynamodb:*)

Access level

▸ □ List

▸ □ Read

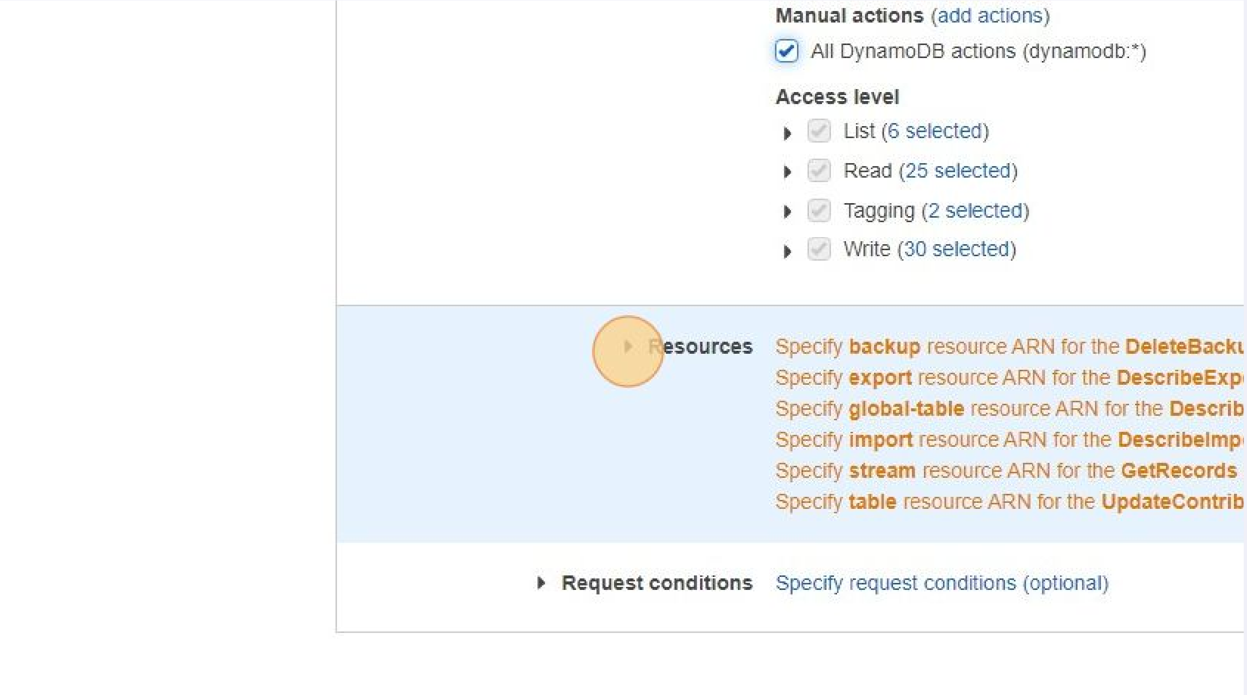
▸ □ Tagging

▸ □ Write

Resources Choose actions before applying resources

Character count: 112 of 6,144.

18 Expand Resources



Manual actions (add actions)

☑ All DynamoDB actions (dynamodb:*)

Access level

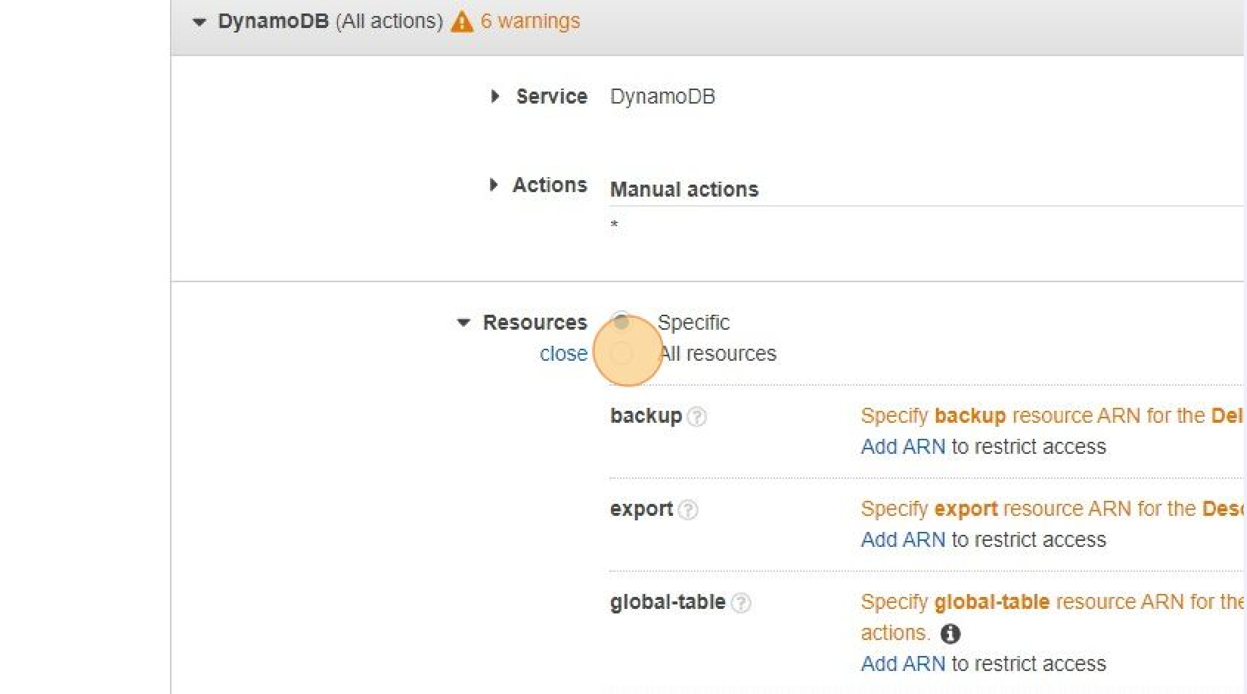
- ☑ List (6 selected)
- ☑ Read (25 selected)
- ☑ Tagging (2 selected)
- ☑ Write (30 selected)

Resources

Specify **backup** resource ARN for the **DeleteBacku**
Specify **export** resource ARN for the **DescribeExp**
Specify **global-table** resource ARN for the **Describ**
Specify **import** resource ARN for the **DescribeImp**
Specify **stream** resource ARN for the **GetRecords**
Specify **table** resource ARN for the **UpdateContrib**

Request conditions — Specify request conditions (optional)

19 Select All Resources



DynamoDB (All actions) ⚠ 6 warnings

Service: DynamoDB

Actions: Manual actions
*

Resources
close

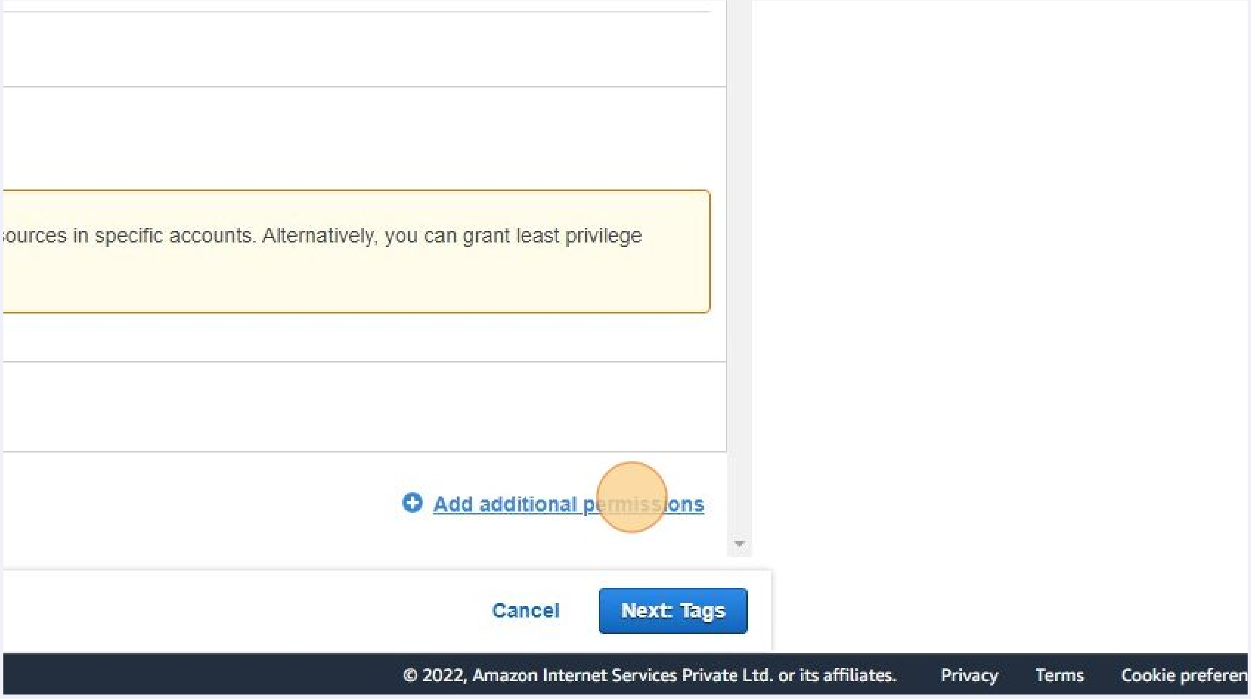
○ Specific
○ All resources

backup — Specify **backup** resource ARN for the **Del**
Add ARN to restrict access

export — Specify **export** resource ARN for the **Desc**
Add ARN to restrict access

global-table — Specify **global-table** resource ARN for the
actions.
Add ARN to restrict access

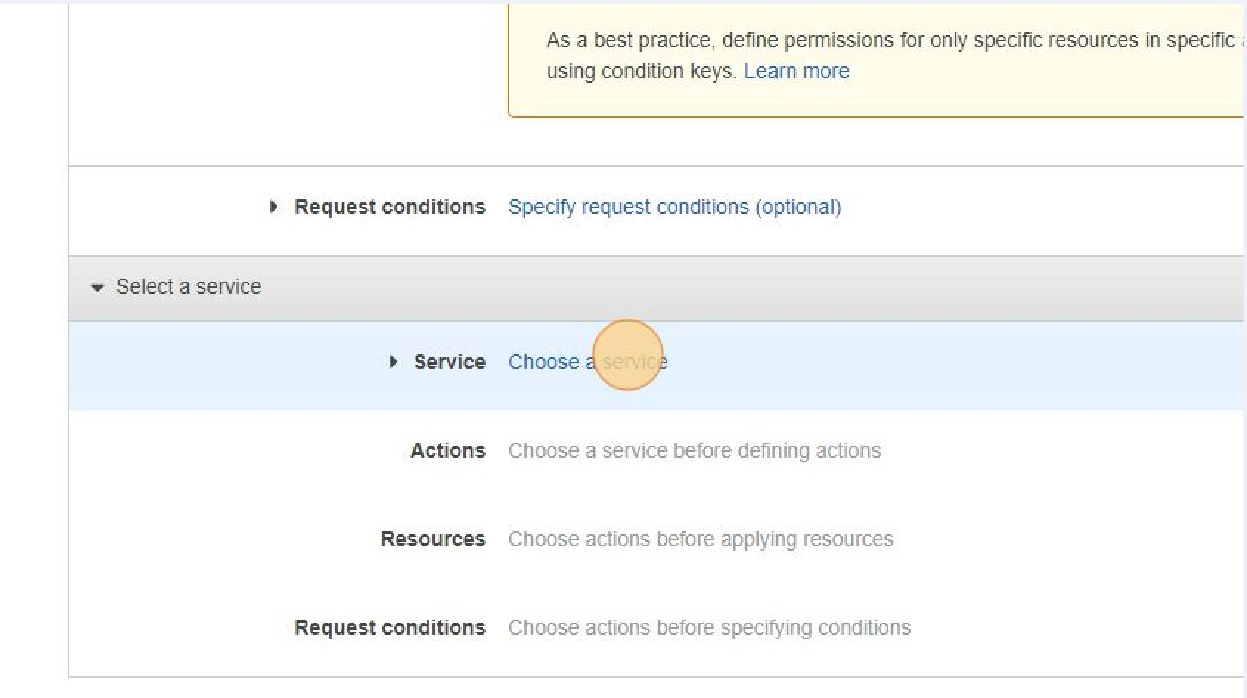
20 Click "Add additional permissions"



ources in specific accounts. Alternatively, you can grant least privilege

Add additional permissions
Cancel
Next: Tags
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferen

21 Click Choose a Service



As a best practice, define permissions for only specific resources in specific
using condition keys. Learn more

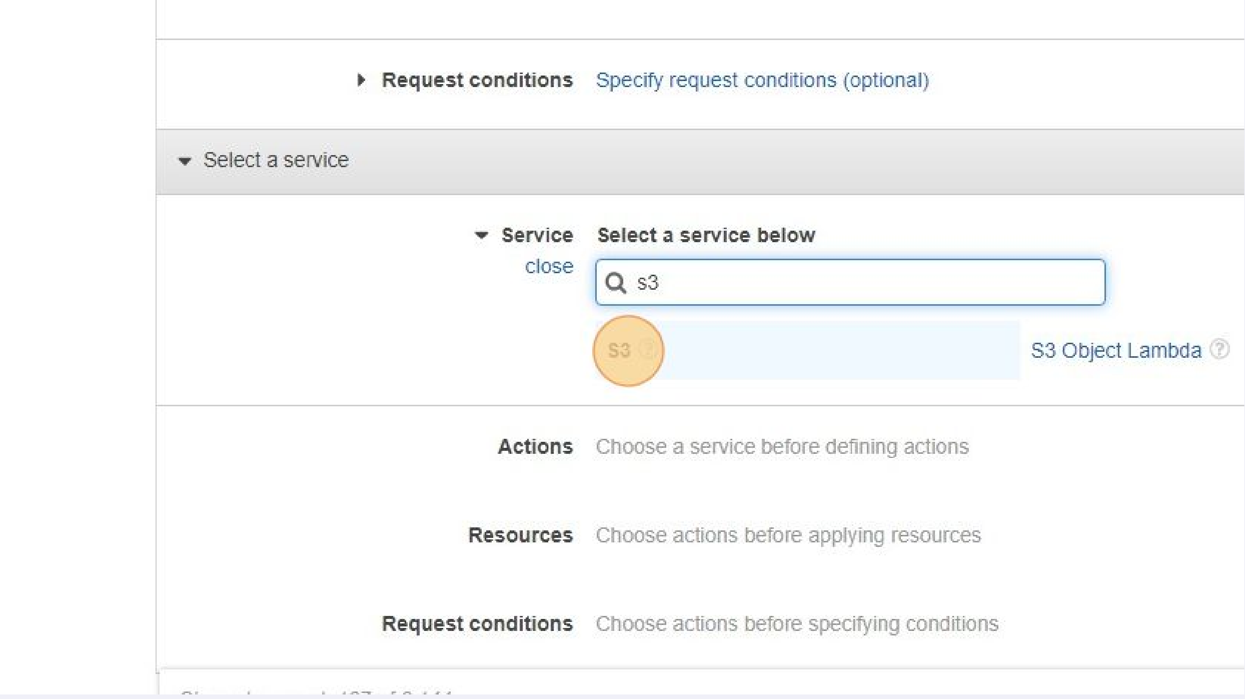
Request conditions	Specify request conditions (optional)

Select a service

Service	Choose a service
Actions	Choose a service before defining actions
Resources	Choose actions before applying resources
Request conditions	Choose actions before specifying conditions

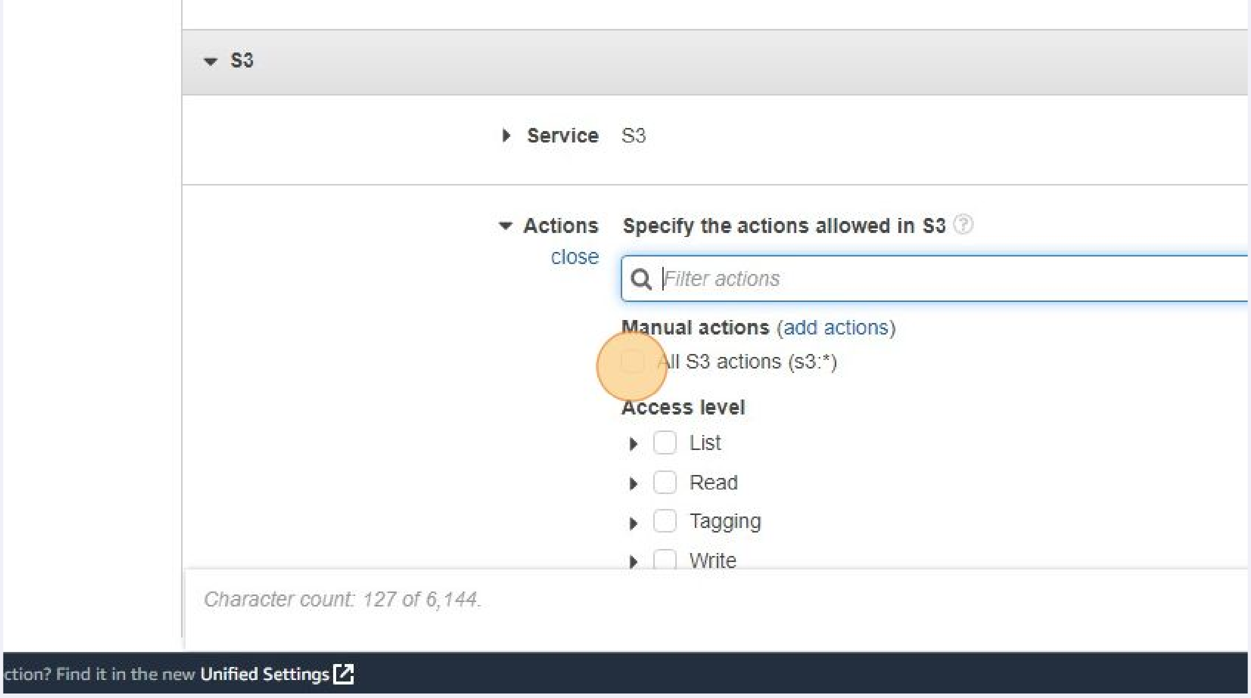
22 Type "s3"

23 Click "S3"



Request conditions
Specify request conditions (optional)
Select a service
Service
close
Select a service below
s3
S3
S3 Object Lambda
Actions
Choose a service before defining actions
Resources
Choose actions before applying resources
Request conditions
Choose actions before specifying conditions

24 Select All S3 Actions



▾ S3

▸ Service S3

▾ Actions close Specify the actions allowed in S3

Filter actions

Manual actions (add actions)

□ All S3 actions (s3:*)

Access level

▸ □ List

▸ □ Read

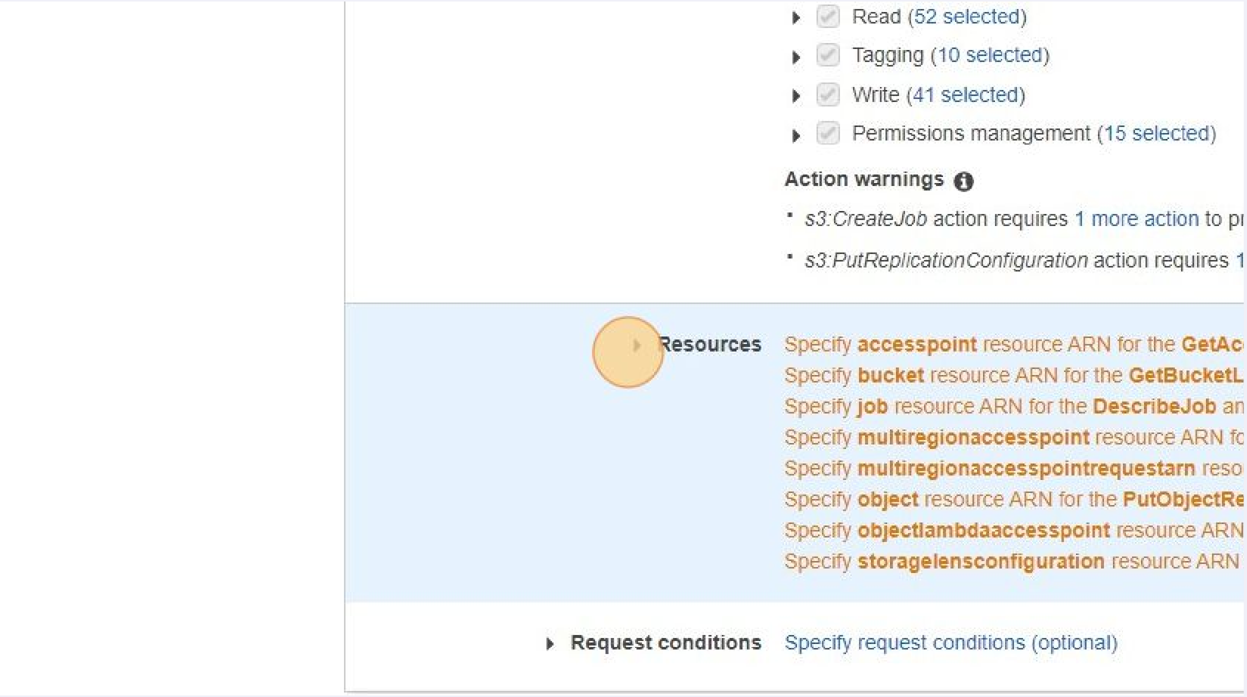
▸ □ Tagging

▸ □ Write

Character count: 127 of 6,144.

ction? Find it in the new Unified Settings

25 Expand Resources



▸ ☑ Read (52 selected)

▸ ☑ Tagging (10 selected)

▸ ☑ Write (41 selected)

▸ ☑ Permissions management (15 selected)

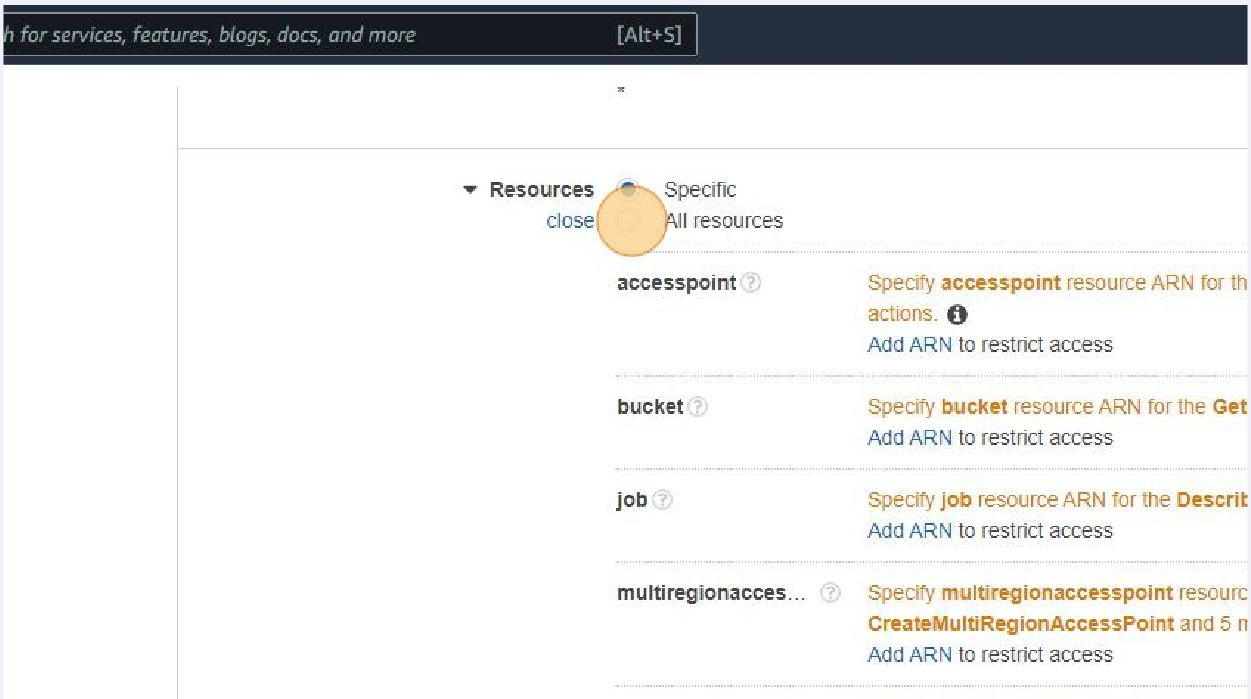
Action warnings

- s3:CreateJob action requires 1 more action to pr
- s3:PutReplicationConfiguration action requires 1

▸ Resources
Specify **accesspoint** resource ARN for the **GetAc**
Specify **bucket** resource ARN for the **GetBucketL**
Specify **job** resource ARN for the **DescribeJob** an
Specify **multiregionaccesspoint** resource ARN fo
Specify **multiregionaccesspointrequestarn** reso
Specify **object** resource ARN for the **PutObjectRe**
Specify **objectlambdaaccesspoint** resource ARN
Specify **storagelensconfiguration** resource ARN

▸ Request conditions Specify request conditions (optional)

26 Select All resources



h for services, features, blogs, docs, and more [Alt+S]

Resources ○ Specific
close ○ All resources

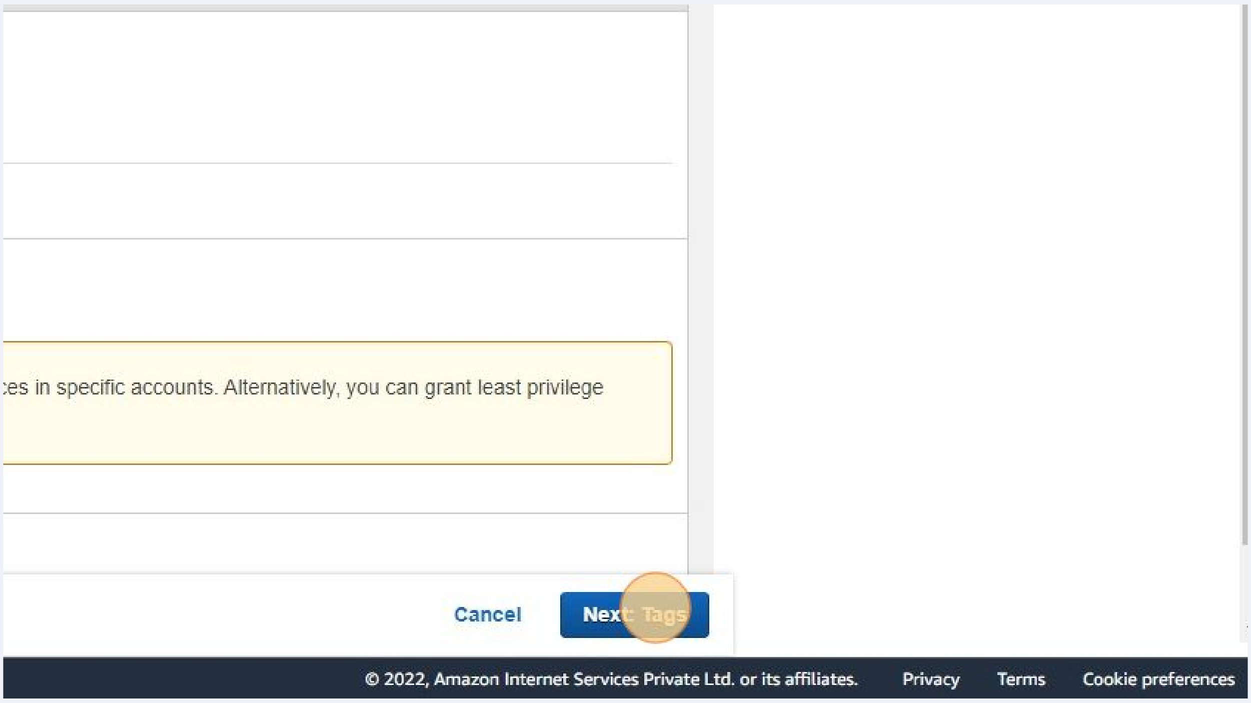
accesspoint ⓘ Specify **accesspoint** resource ARN for th actions. Add ARN to restrict access

bucket ⓘ Specify **bucket** resource ARN for the **Get** Add ARN to restrict access

job ⓘ Specify **job** resource ARN for the **Describ** Add ARN to restrict access

multiregionacces... ⓘ Specify **multiregionaccesspoint** resourc **CreateMultiRegionAccessPoint** and 5 m Add ARN to restrict access

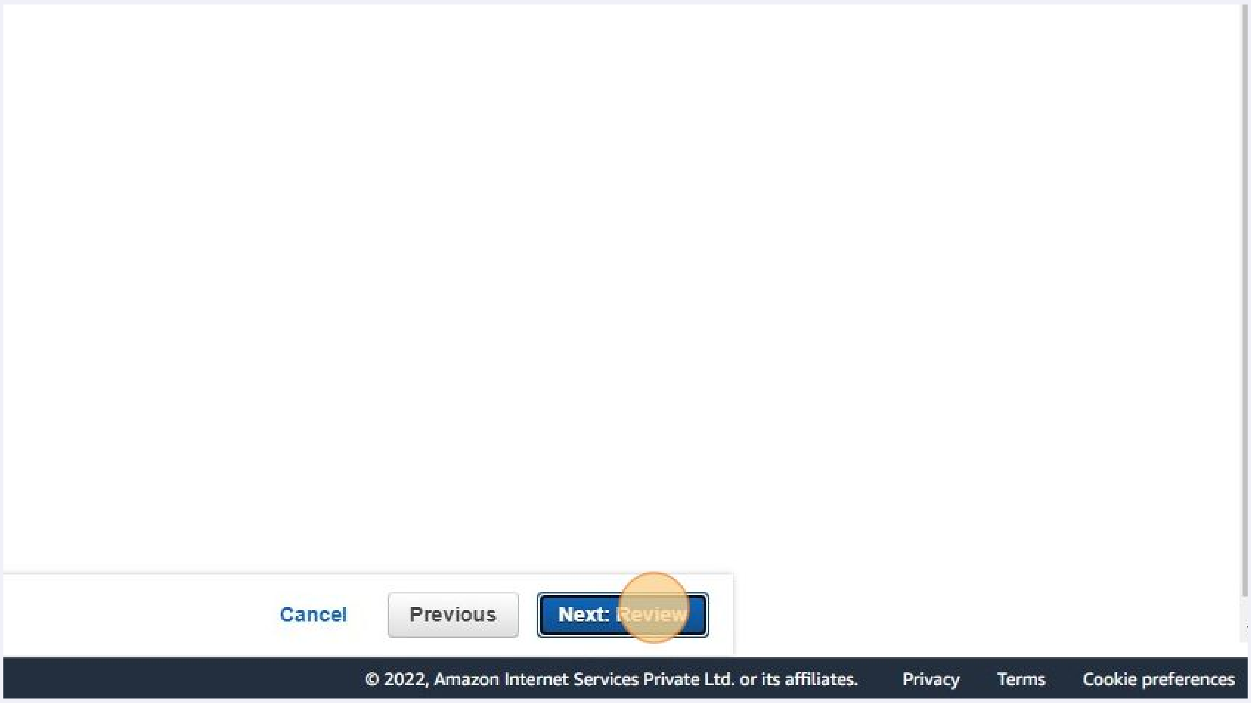
27 Click "Next: Tags"



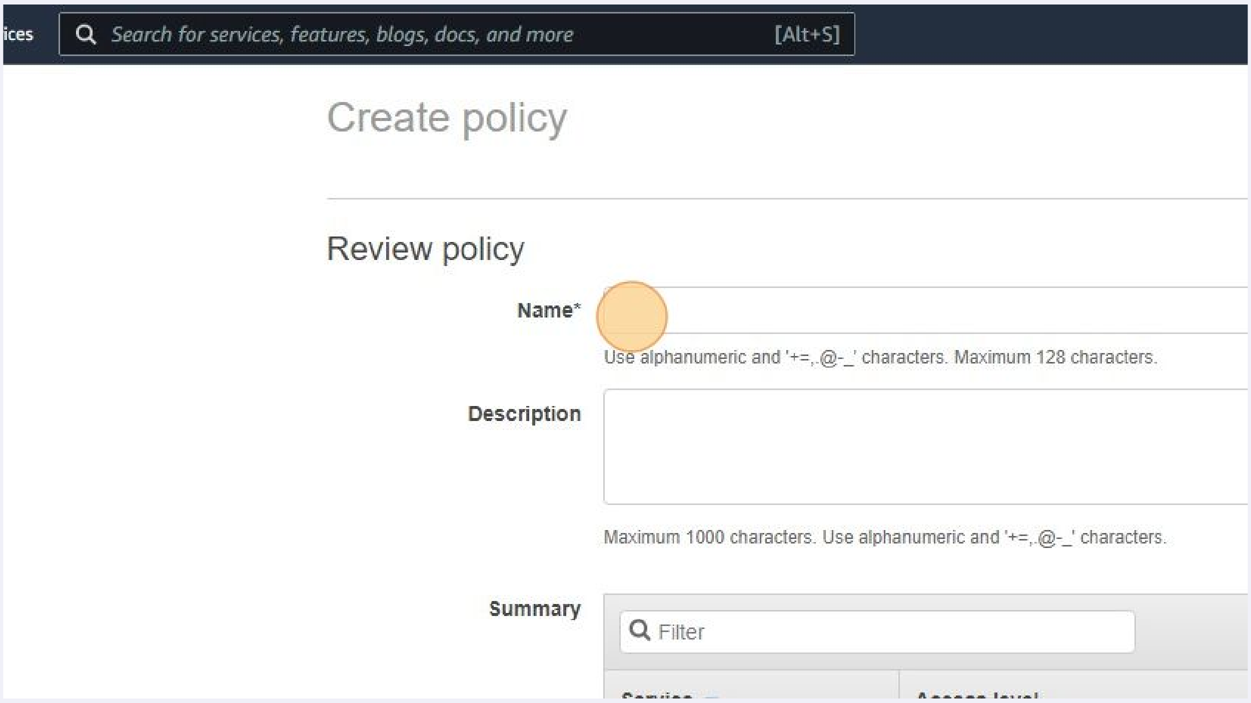
:es in specific accounts. Alternatively, you can grant least privilege

Cancel
Next: Tags
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

28 Click "Next: Review"

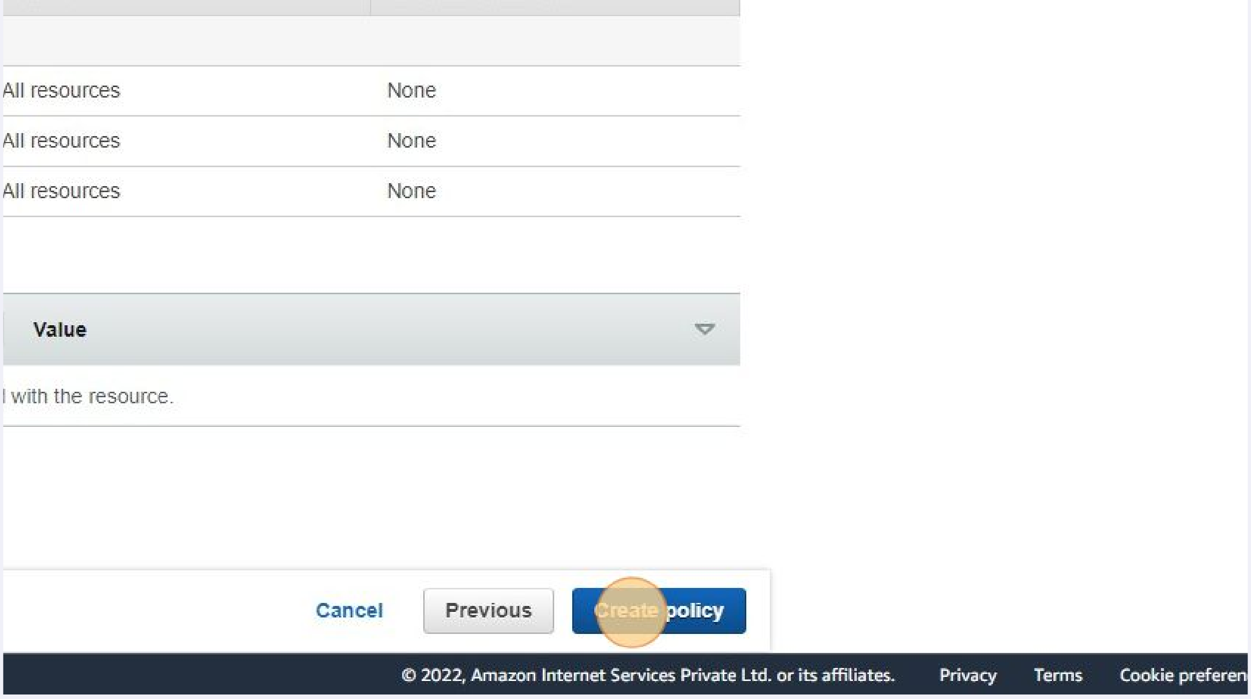

Cancel
Previous
Next: Review
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

29 Click the "Name" field.


ices
Search for services, features, blogs, docs, and more
[Alt+S]
Create policy
Review policy
Name*
Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.
Description
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Summary
Filter

30 Type "my_lambda_policy"

31 Click "Create policy"



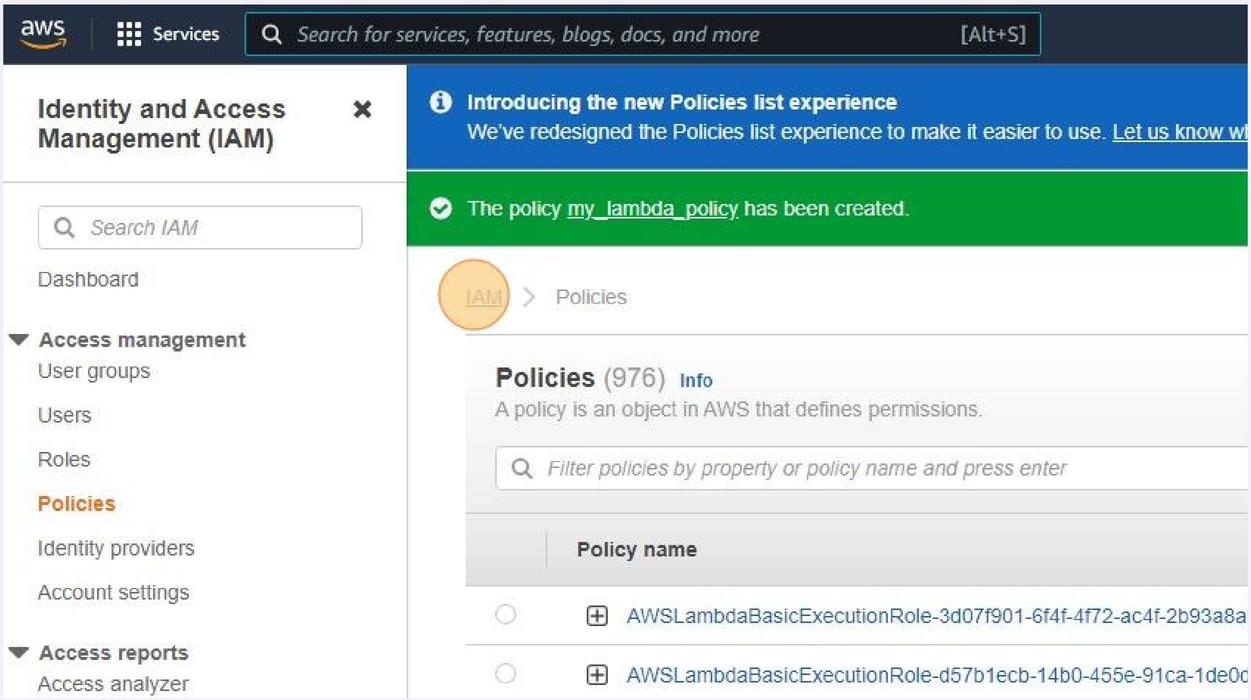
All resources	None
All resources	None
All resources	None

Value

l with the resource.

Cancel
Previous
Create policy
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferen

32 Click "IAM"



aws | Services | Search for services, features, blogs, docs, and more [Alt+S]

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Introducing the new Policies list experience
We've redesigned the Policies list experience to make it easier to use. Let us know wl

The policy my_lambda_policy has been created.

IAM > Policies

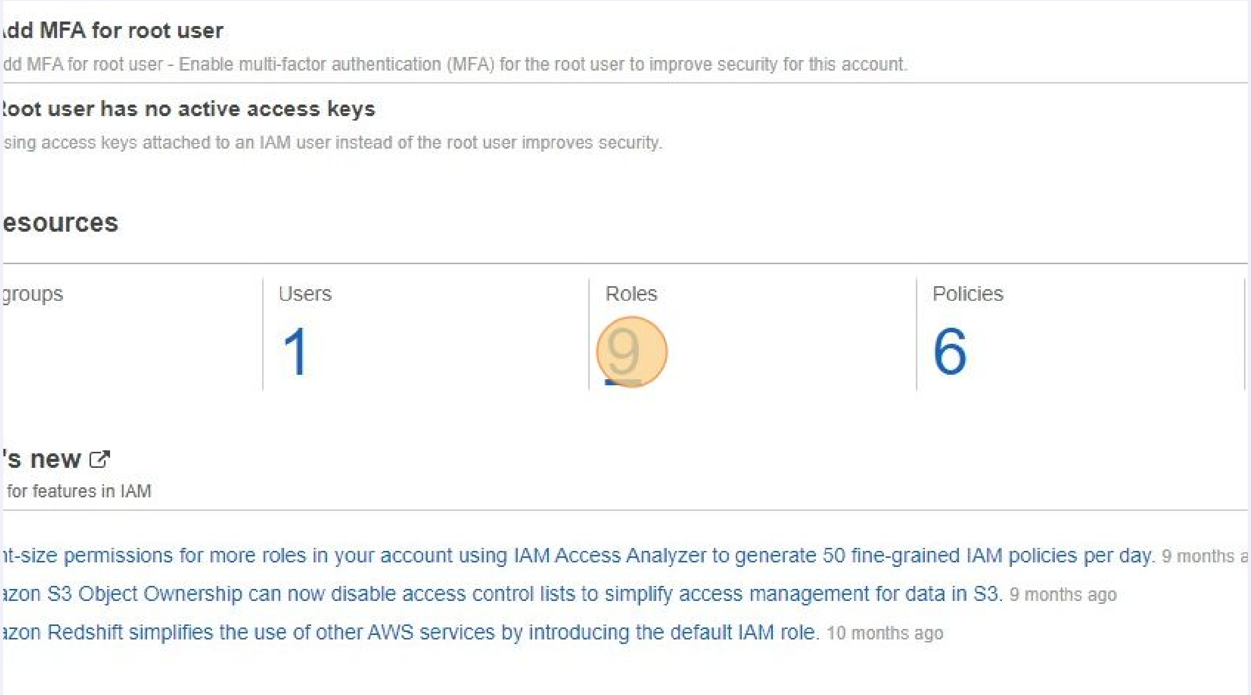
Policies (976) Info

A policy is an object in AWS that defines permissions.

Filter policies by property or policy name and press enter

	Policy name
○	⊞ AWSLambdaBasicExecutionRole-3d07f901-6f4f-4f72-ac4f-2b93a8a
○	⊞ AWSLambdaBasicExecutionRole-d57b1ecb-14b0-455e-91ca-1de0c

33 Click "Roles"



ıdd MFA for root user

ıdd MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

ᒧoot user has no active access keys

ısing access keys attached to an IAM user instead of the root user improves security.

esources

groups	Users	Roles	Policies
	1	9	6

's new

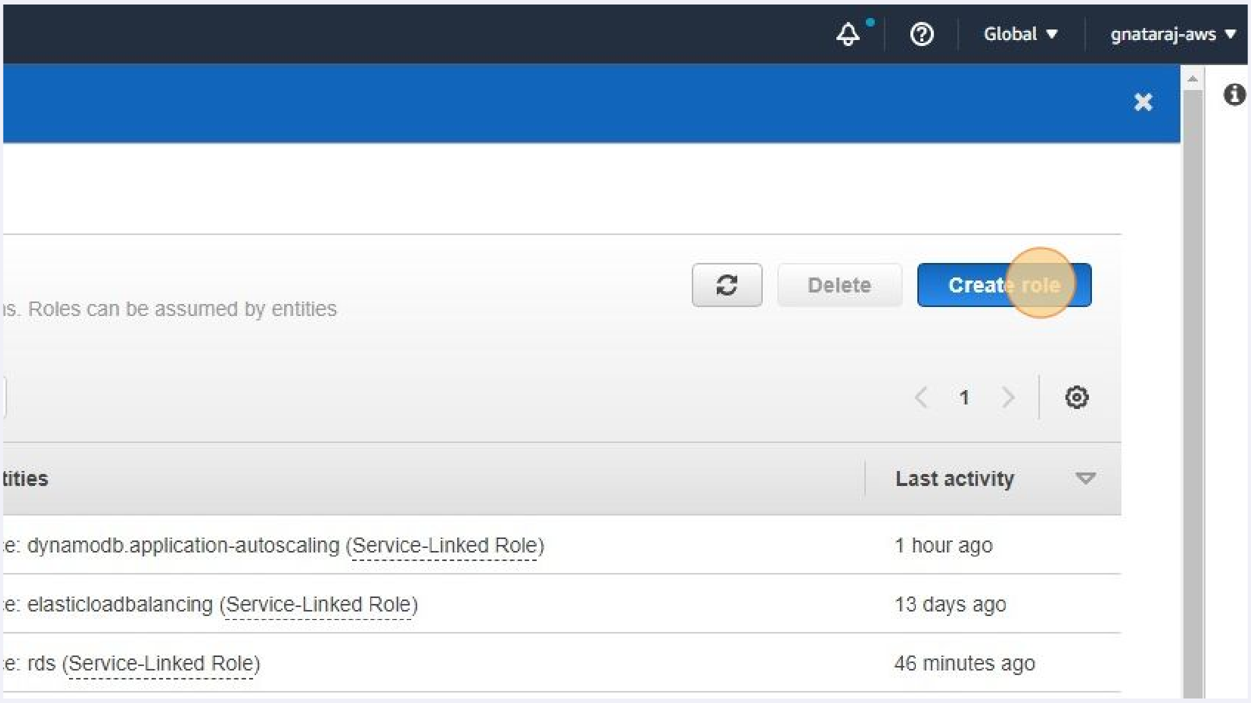
for features in IAM

ıt-size permissions for more roles in your account using IAM Access Analyzer to generate 50 fine-grained IAM policies per day. 9 months a

ızon S3 Object Ownership can now disable access control lists to simplify access management for data in S3. 9 months ago

ızon Redshift simplifies the use of other AWS services by introducing the default IAM role. 10 months ago

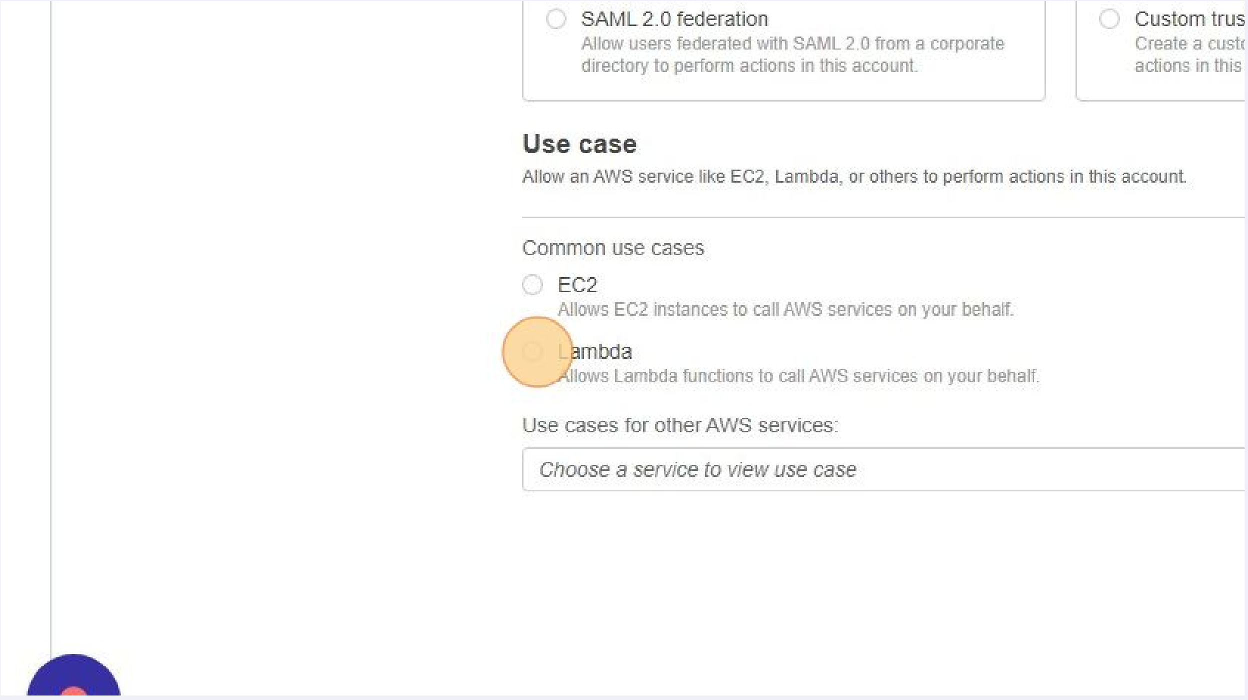
34 Click "Create role"



ɪs. Roles can be assumed by entities

tities	Last activity
e: dynamodb.application-autoscaling (Service-Linked Role)	1 hour ago
e: elasticloadbalancing (Service-Linked Role)	13 days ago
e: rds (Service-Linked Role)	46 minutes ago

35 Click the "LambdaAllows Lambda functions to call AWS services on your behalf." field.



○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trus
Create a custo
actions in this

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

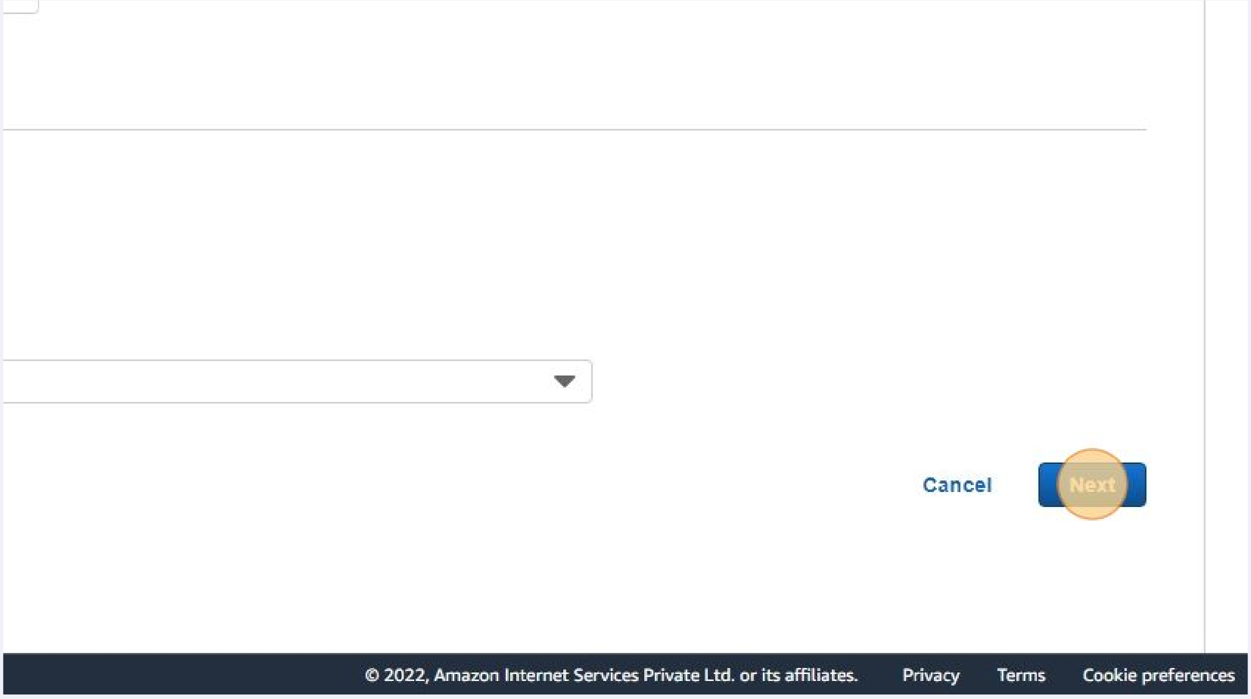
○ EC2
Allows EC2 instances to call AWS services on your behalf.

○ Lambda
Allows Lambda functions to call AWS services on your behalf.

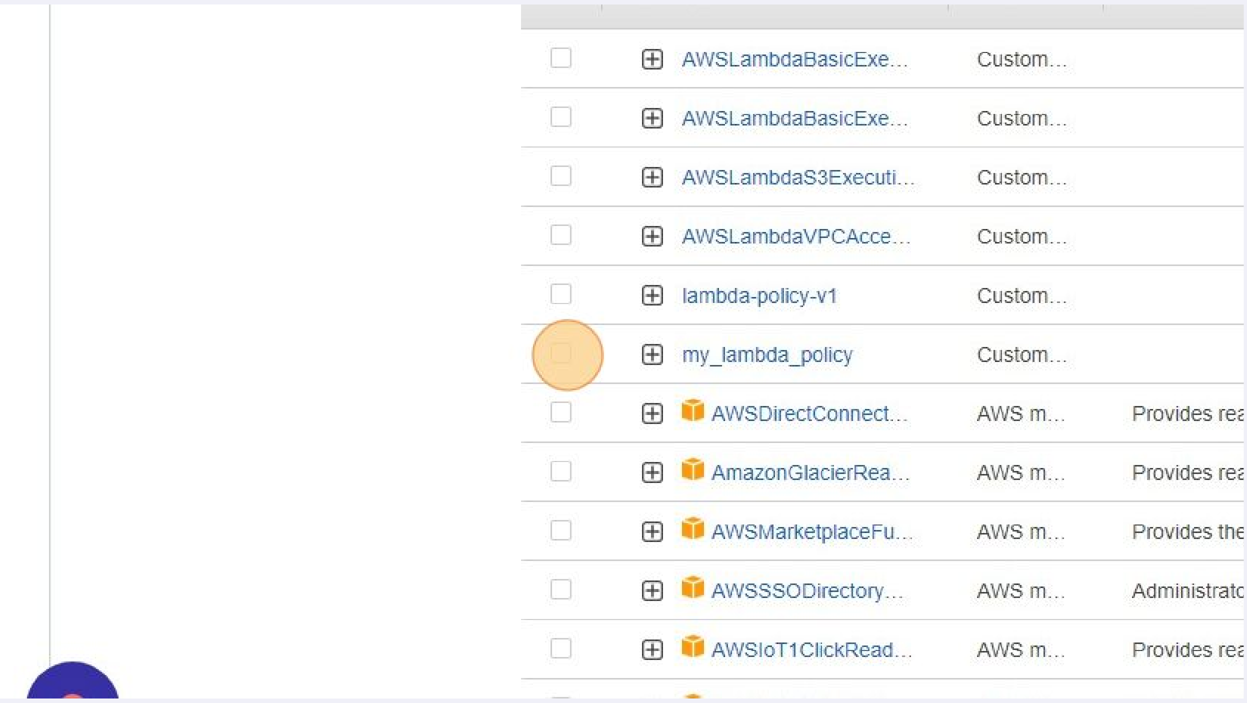
Use cases for other AWS services:

Choose a service to view use case

36 Click "Next"

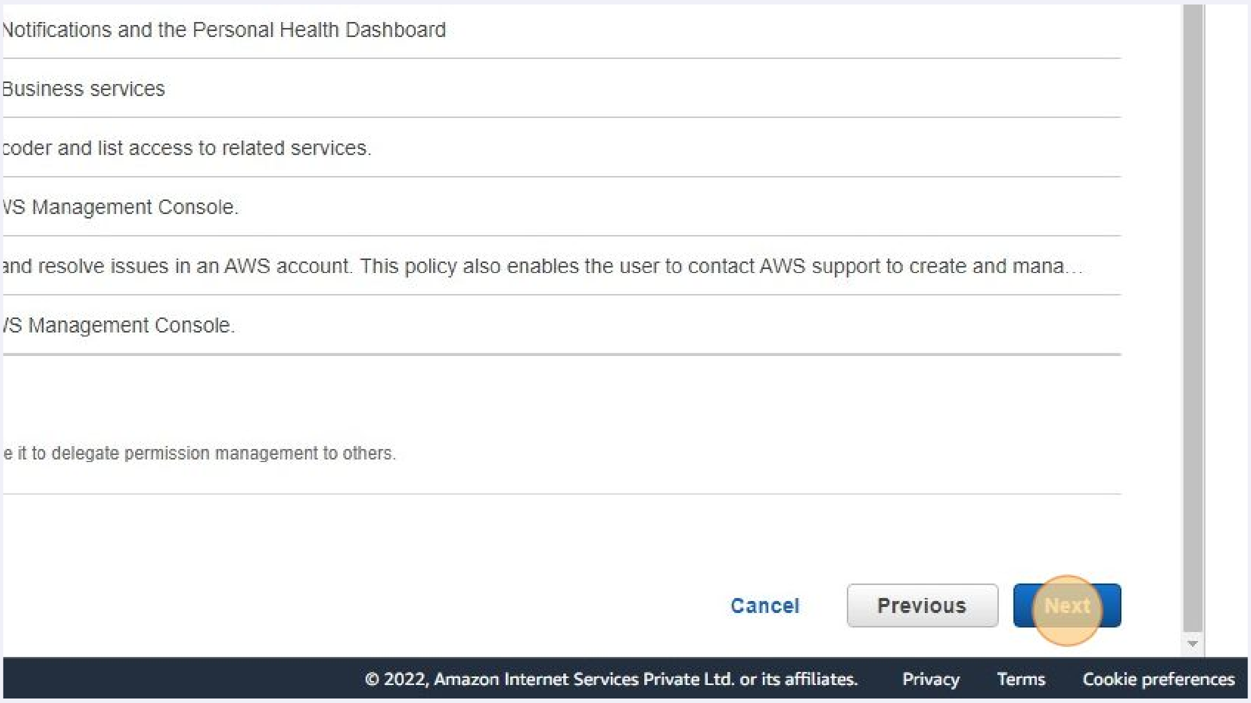

Cancel
Next
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

37 Select the my_lambda_policy, which was created in the previous step



☐	⊞ AWSLambdaBasicExe...	Custom...	
☐	⊞ AWSLambdaBasicExe...	Custom...	
☐	⊞ AWSLambdaS3Executi...	Custom...	
☐	⊞ AWSLambdaVPCAcce...	Custom...	
☐	⊞ lambda-policy-v1	Custom...	
☐	⊞ my_lambda_policy	Custom...	
☐	⊞ AWSDirectConnect...	AWS m...	Provides rea
☐	⊞ AmazonGlacierRea...	AWS m...	Provides rea
☐	⊞ AWSMarketplaceFu...	AWS m...	Provides the
☐	⊞ AWSSSODirectory...	AWS m...	Administrato
☐	⊞ AWSIoT1ClickRead...	AWS m...	Provides rea

38 Click "Next"



Notifications and the Personal Health Dashboard

Business services

coder and list access to related services.

VS Management Console.

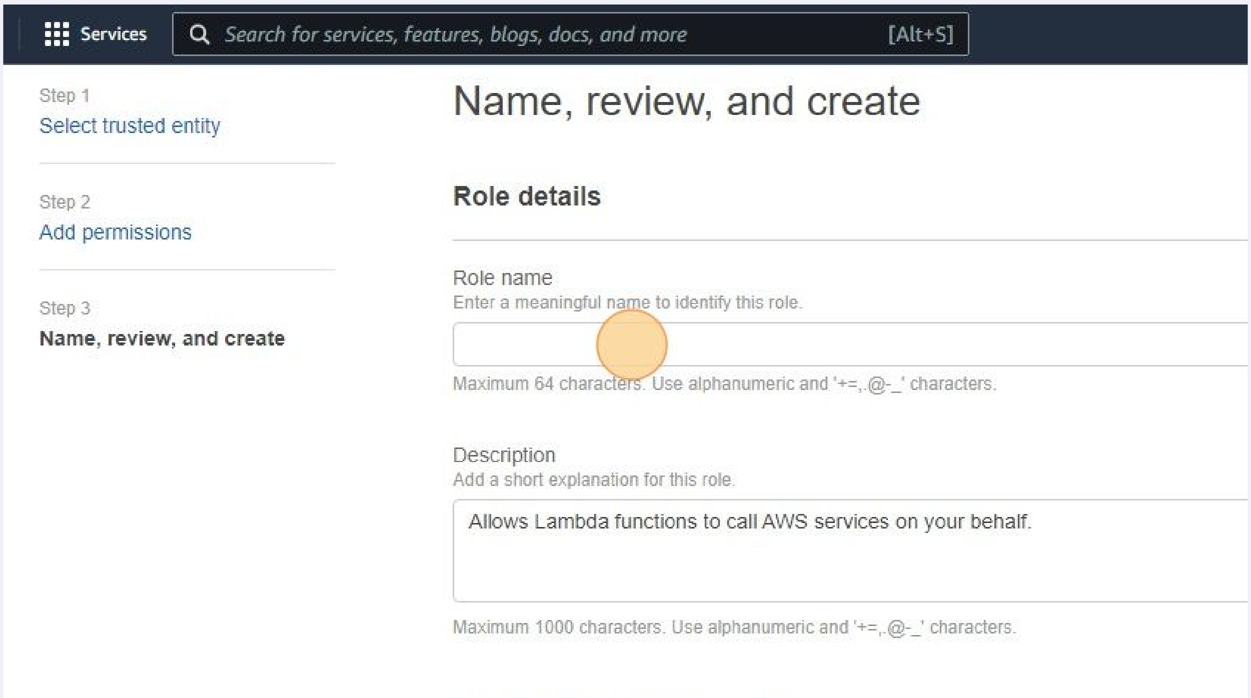
and resolve issues in an AWS account. This policy also enables the user to contact AWS support to create and mana...

/S Management Console.

e it to delegate permission management to others.

Cancel
Previous
Next
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

39 Click the "Role name" field.



Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description

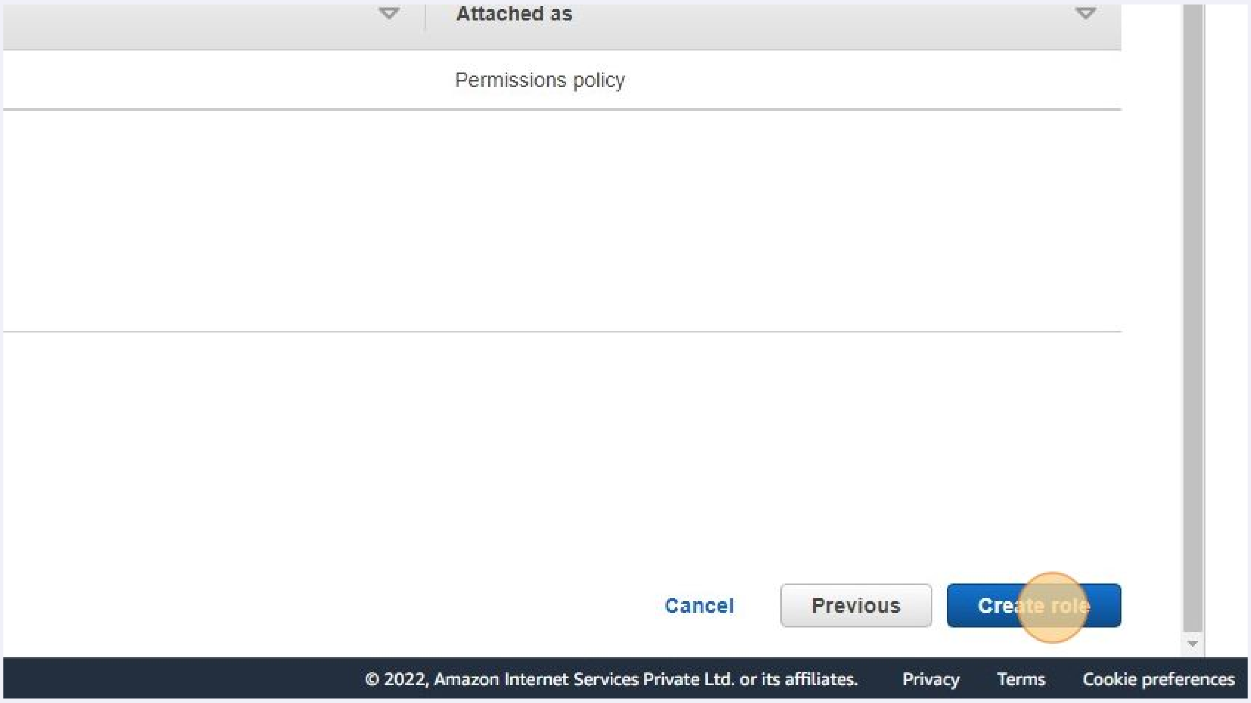
Add a short explanation for this role.

Allows Lambda functions to call AWS services on your behalf.

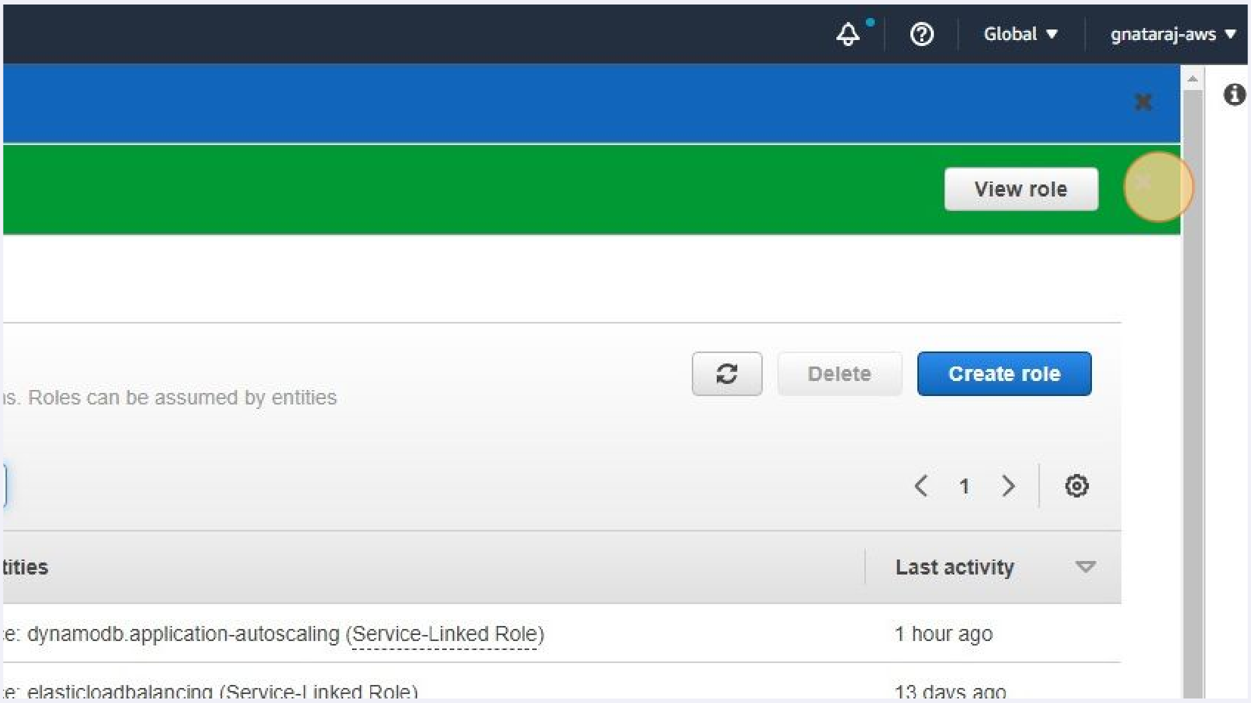
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

40 Type "my_lambda_role"

41 Click "Create role"



42 Click this button.



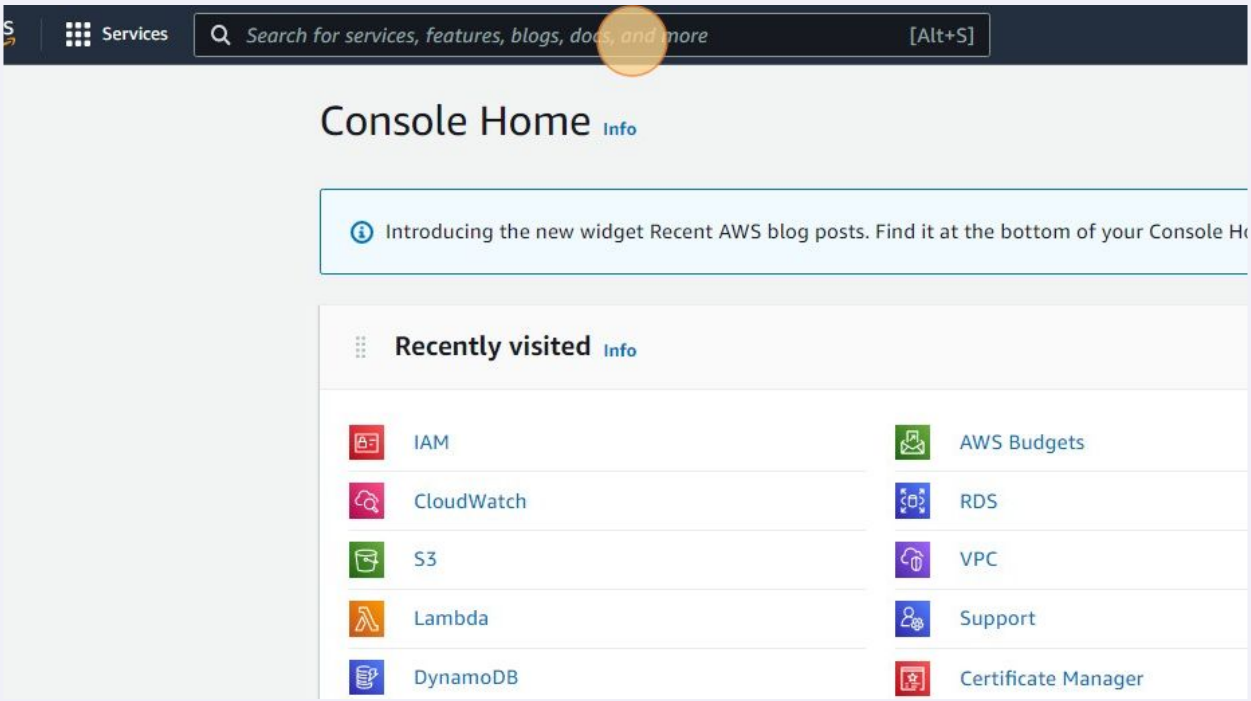
ıs. Roles can be assumed by entities

tities	Last activity
:e: dynamodb.application-autoscaling (Service-Linked Role)	1 hour ago
:e: elasticloadbalancing (Service-Linked Role)	13 days ago

3. Creating Dynamo DB Table

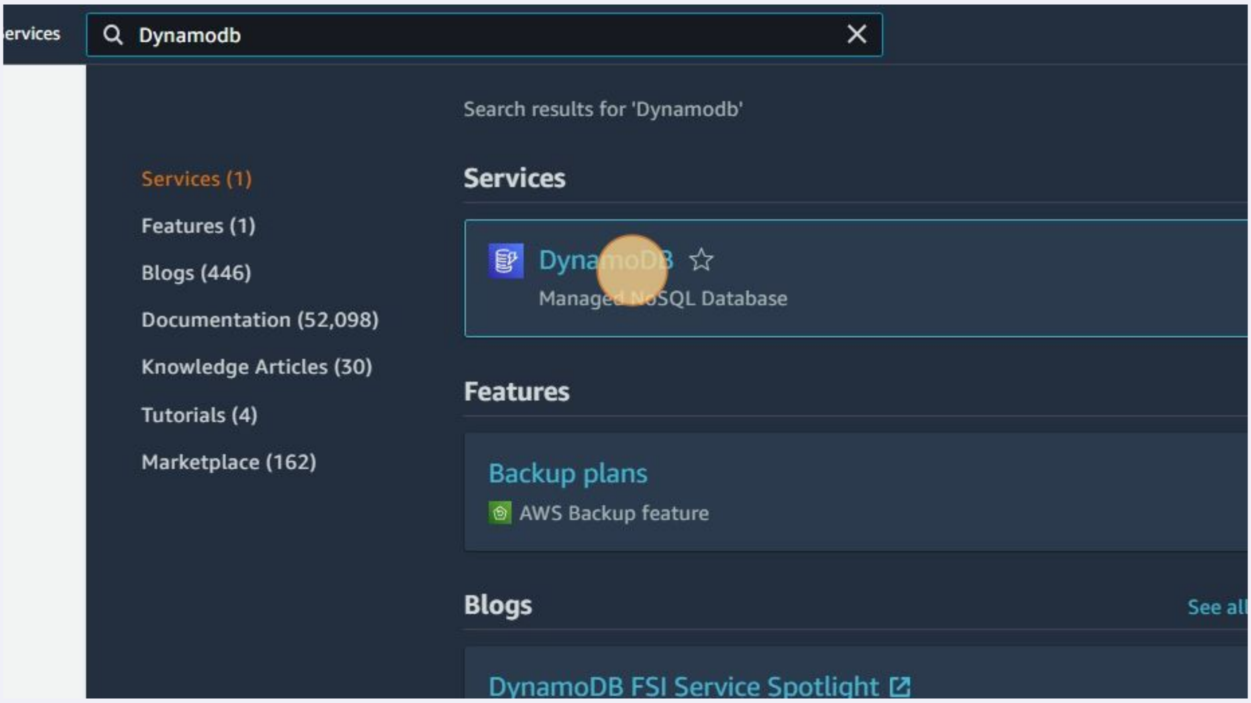
1 Navigate to https://ap-south-1.console.aws.amazon.com/console/home?region=ap-south-1

2 Click the "Search for services, features, blogs, docs, and more" field.


Services
Search for services, features, blogs, docs, and more
[Alt+S]
Console Home Info
Introducing the new widget Recent AWS blog posts. Find it at the bottom of your Console Ho
Recently visited Info
IAM
AWS Budgets
CloudWatch
RDS
S3
VPC
Lambda
Support
DynamoDB
Certificate Manager

3 Type "Dynamodb"

4 Click "DynamoDB"



ervices

Dynamodb

Search results for 'Dynamodb'

Services (1)

Features (1)

Blogs (446)

Documentation (52,098)

Knowledge Articles (30)

Tutorials (4)

Marketplace (162)

Services

DynamoDB ☆

Managed NoSQL Database

Features

Backup plans

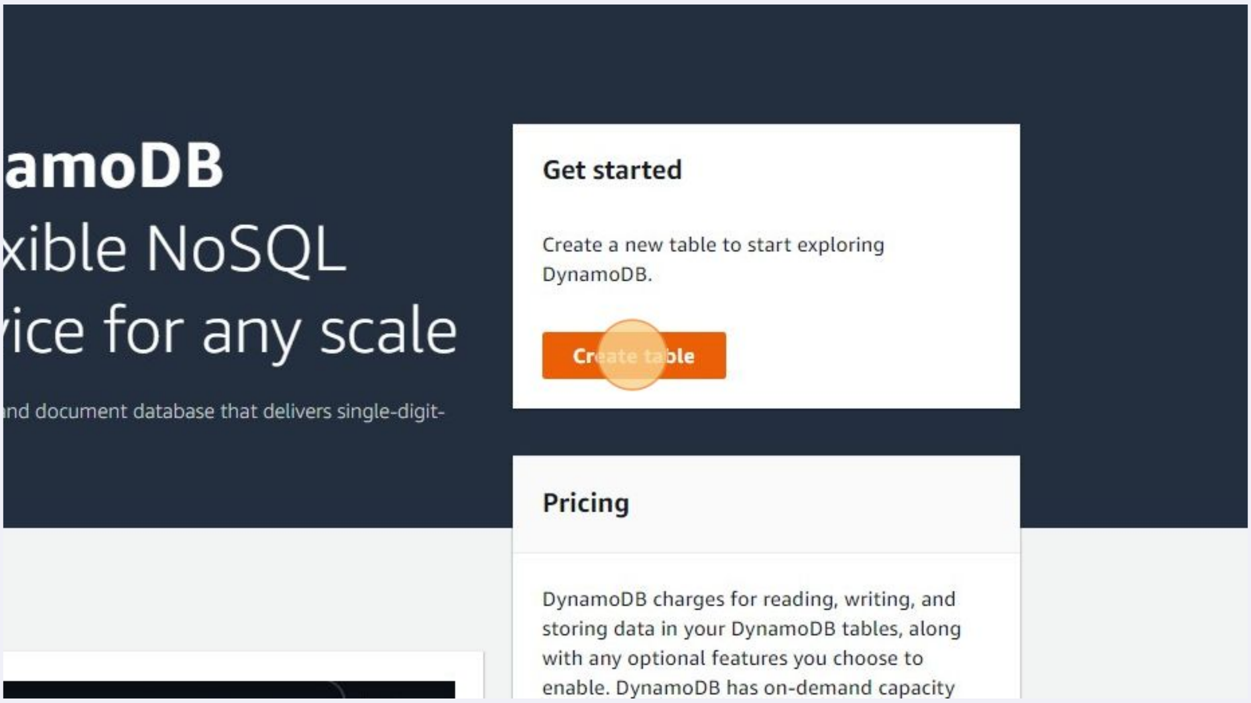
AWS Backup feature

Blogs

See all

DynamoDB FSI Service Spotlight

5 Click "Create table"



amoDB

xible NoSQL

ice for any scale

nd document database that delivers single-digit-

Get started

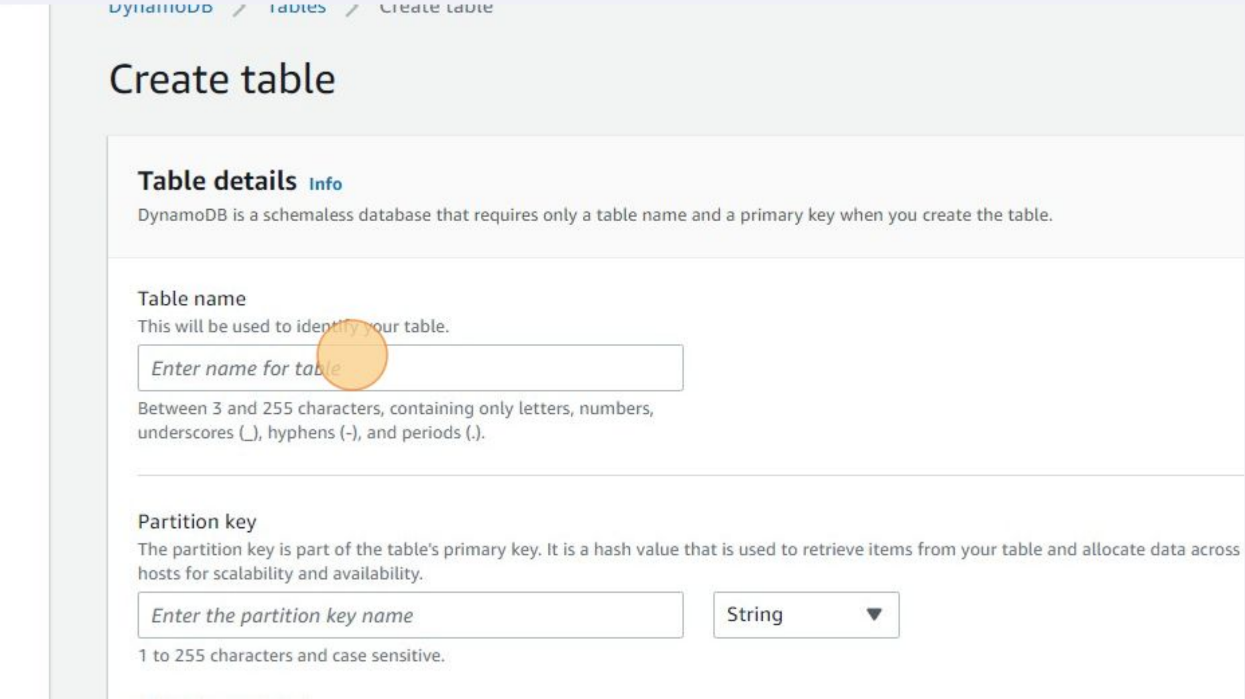
Create a new table to start exploring DynamoDB.

Create table

Pricing

DynamoDB charges for reading, writing, and storing data in your DynamoDB tables, along with any optional features you choose to enable. DynamoDB has on-demand capacity

6 Click the "Table name" field.



DynamoDB / Tables / Create table

Create table

Table details Info

DynamoDB is a schemaless database that requires only a table name and a primary key when you create the table.

Table name

This will be used to identify your table.

Enter name for table

Between 3 and 255 characters, containing only letters, numbers, underscores (_), hyphens (-), and periods (.).

Partition key

The partition key is part of the table's primary key. It is a hash value that is used to retrieve items from your table and allocate data across hosts for scalability and availability.

Enter the partition key name

String ▼

1 to 255 characters and case sensitive.

7 Type "employees"

8 Click the "Partition key" field.

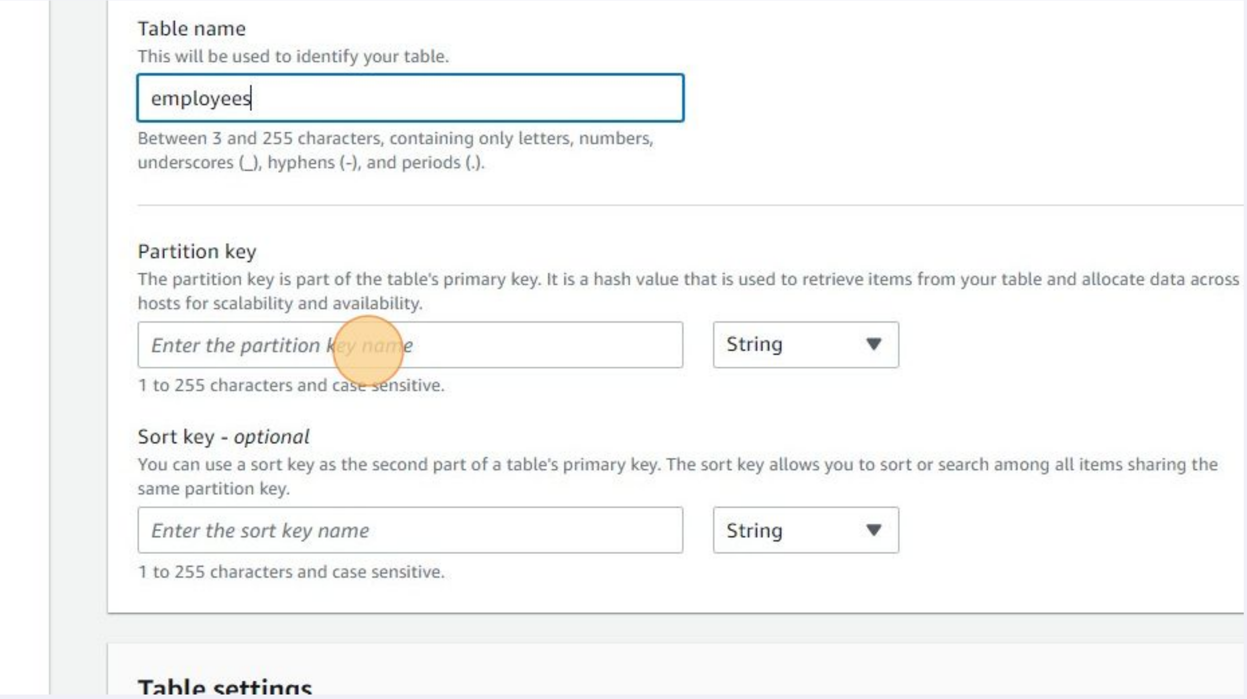


Table name

This will be used to identify your table.

employees

Between 3 and 255 characters, containing only letters, numbers, underscores (_), hyphens (-), and periods (.).

Partition key

The partition key is part of the table's primary key. It is a hash value that is used to retrieve items from your table and allocate data across hosts for scalability and availability.

Enter the partition key name | String ▼

1 to 255 characters and case sensitive.

Sort key - *optional*

You can use a sort key as the second part of a table's primary key. The sort key allows you to sort or search among all items sharing the same partition key.

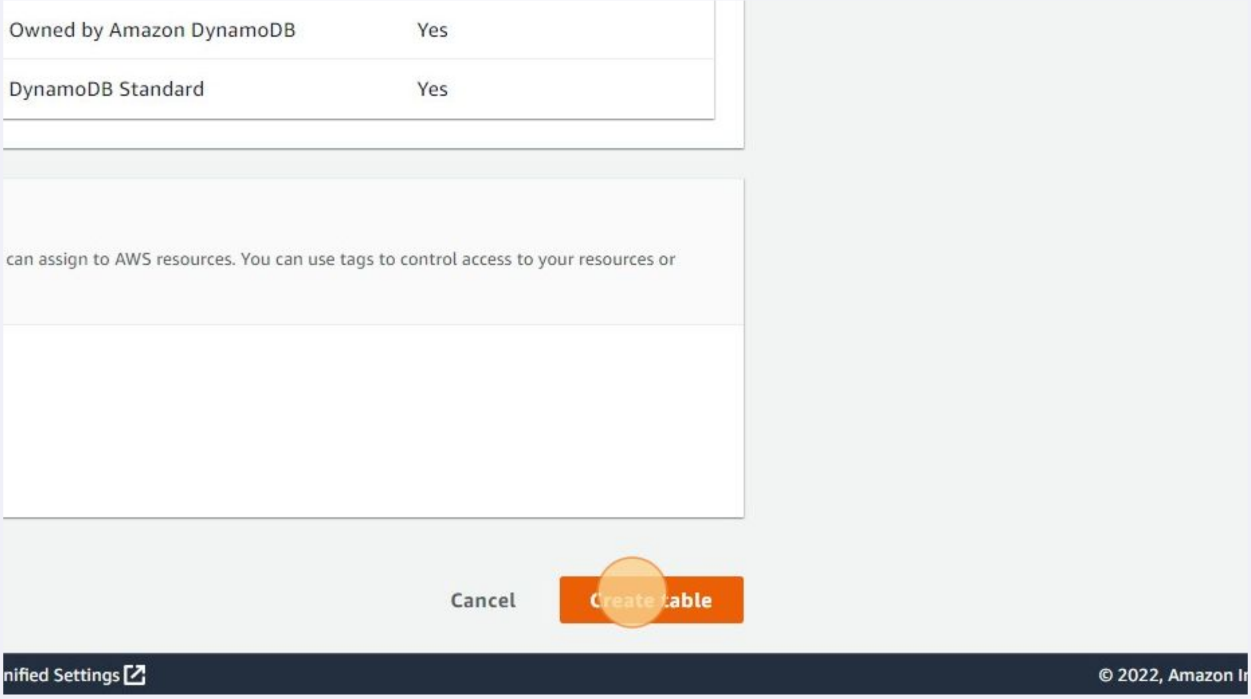
Enter the sort key name | String ▼

1 to 255 characters and case sensitive.

Table settings

9 Type "emp_id"

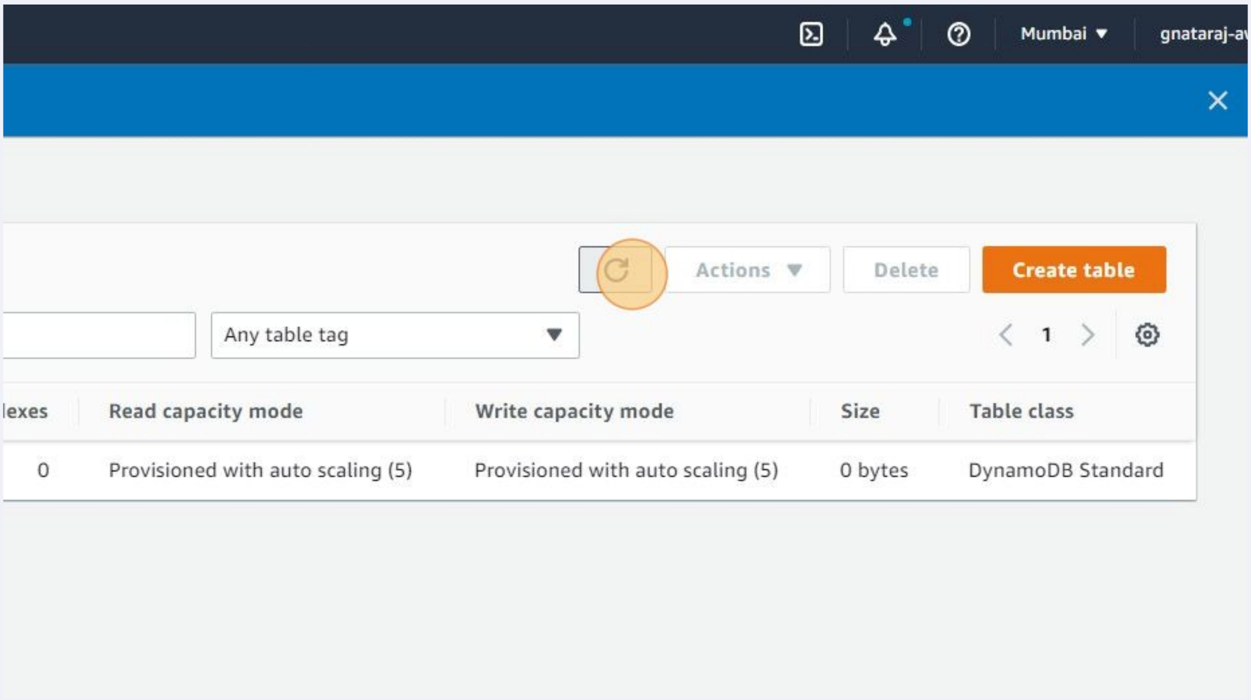
10 Click "Create table"



Owned by Amazon DynamoDB	Yes
DynamoDB Standard	Yes

can assign to AWS resources. You can use tags to control access to your resources or

11 Click this button.



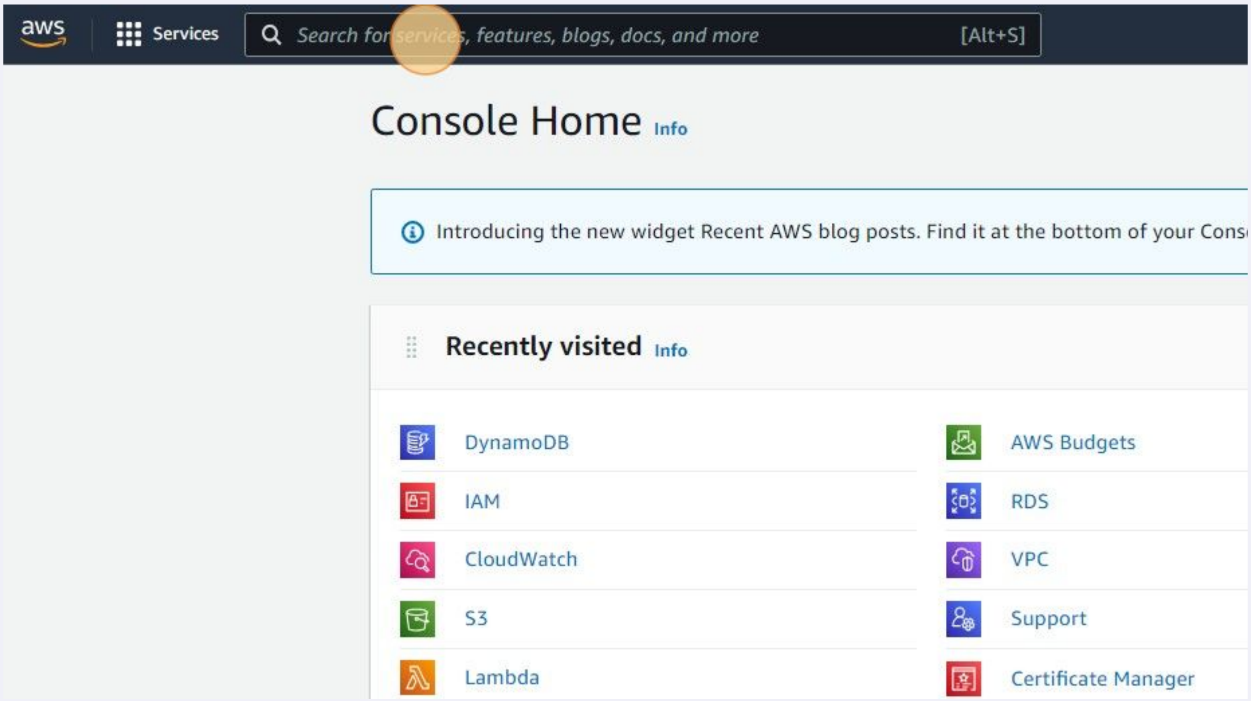
lexes	Read capacity mode	Write capacity mode	Size	Table class
0	Provisioned with auto scaling (5)	Provisioned with auto scaling (5)	0 bytes	DynamoDB Standard

4. Creating S3 bucket

Scribe

1 Navigate to https://ap-south-1.console.aws.amazon.com/console/home?region=ap-south-1

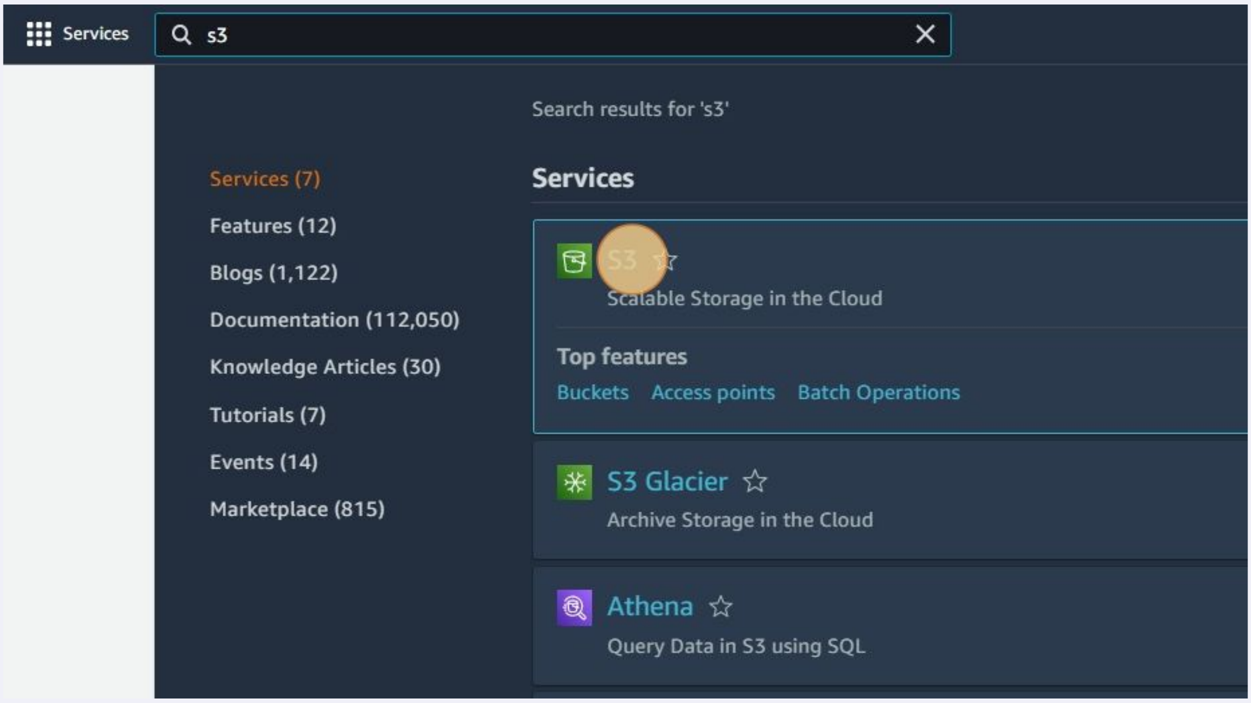
2 Click the "Search for services, features, blogs, docs, and more" field.



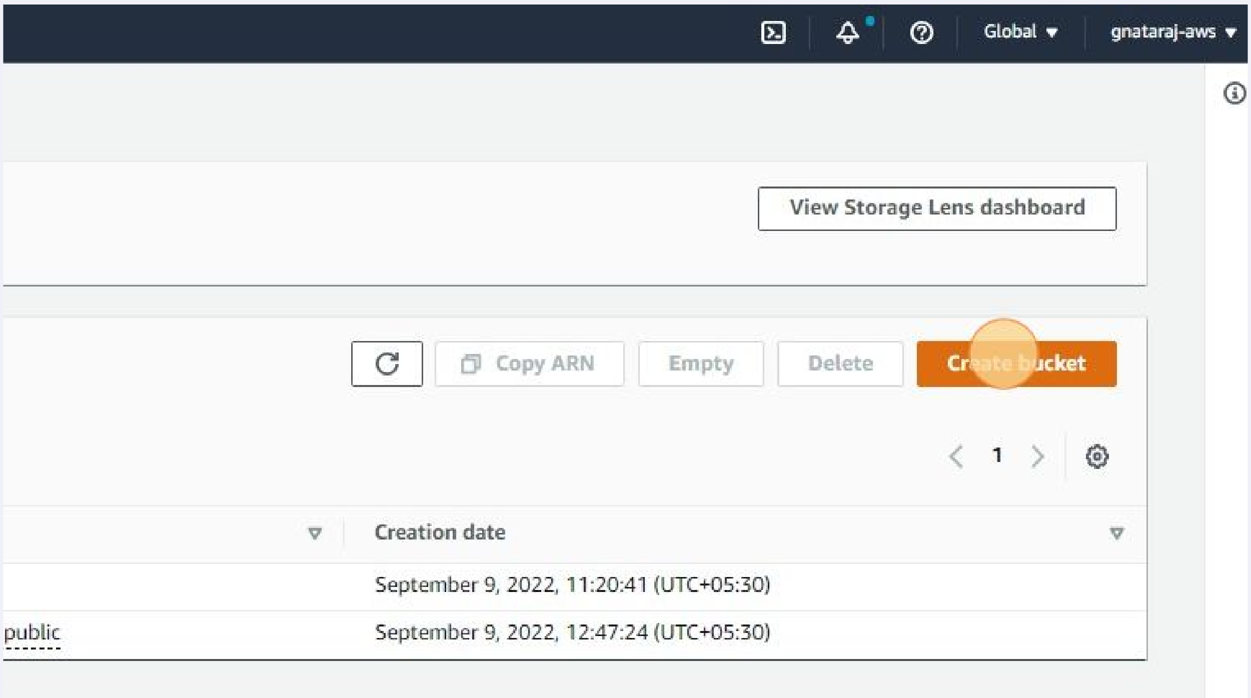
Introducing the new widget Recent AWS blog posts. Find it at the bottom of your Cons

3 Type "s3"

4 Click "S3"

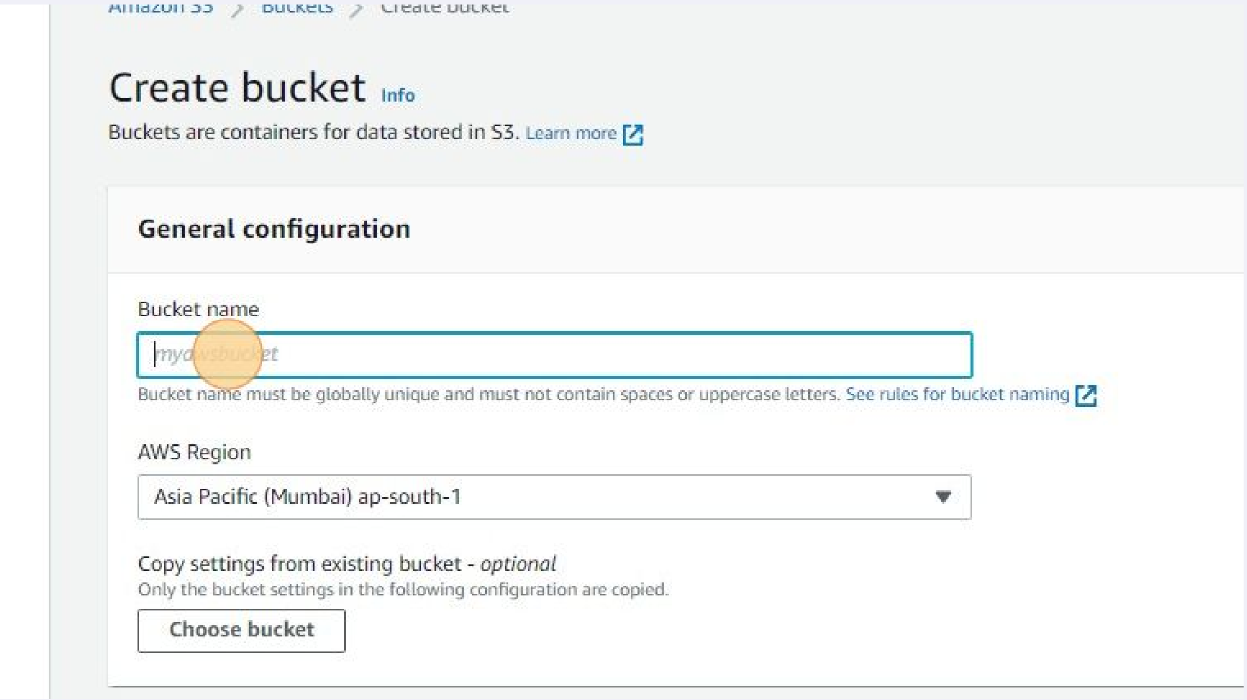


5 Click "Create bucket"



September 9, 2022, 11:20:41 (UTC+05:30)
September 9, 2022, 12:47:24 (UTC+05:30)

6 Click the "Bucket name" field.



Amazon S3 > Buckets > Create bucket

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

myawsbucket

Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming

AWS Region

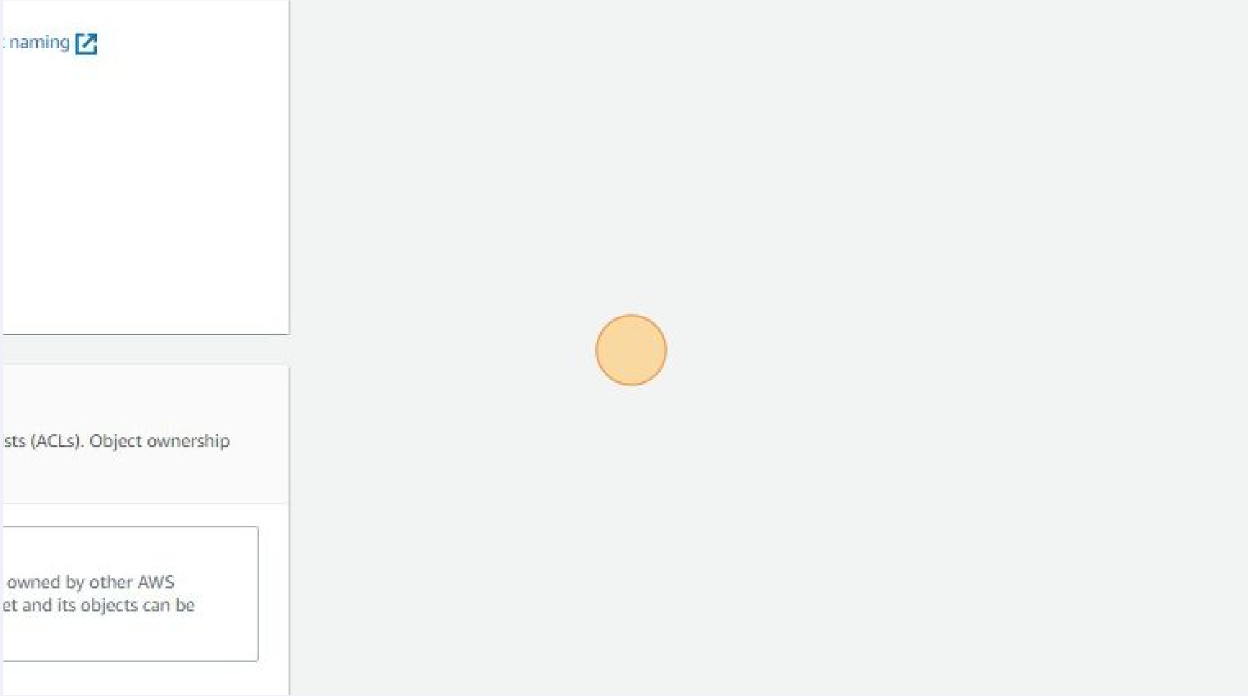
Asia Pacific (Mumbai) ap-south-1

Copy settings from existing bucket - *optional*

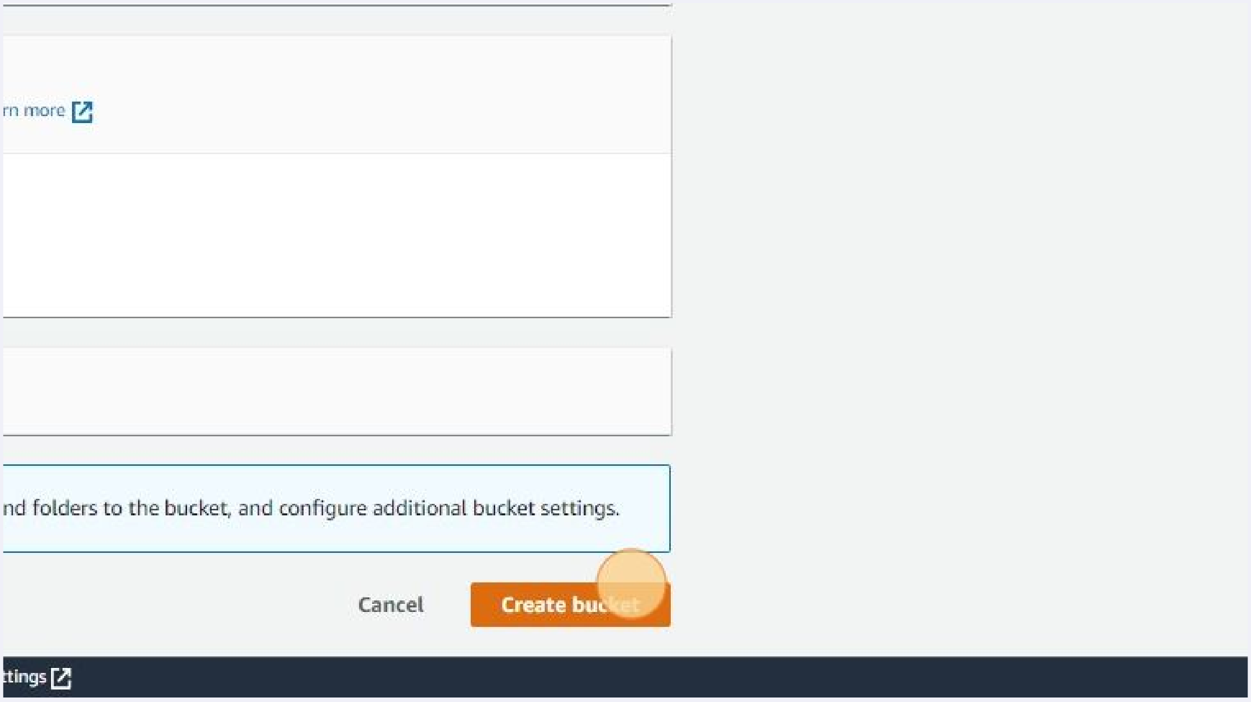
Only the bucket settings in the following configuration are copied.

7 Type any globally unique name for S3 bucket ("employees-detatils-json" in this example)

8 Click here.



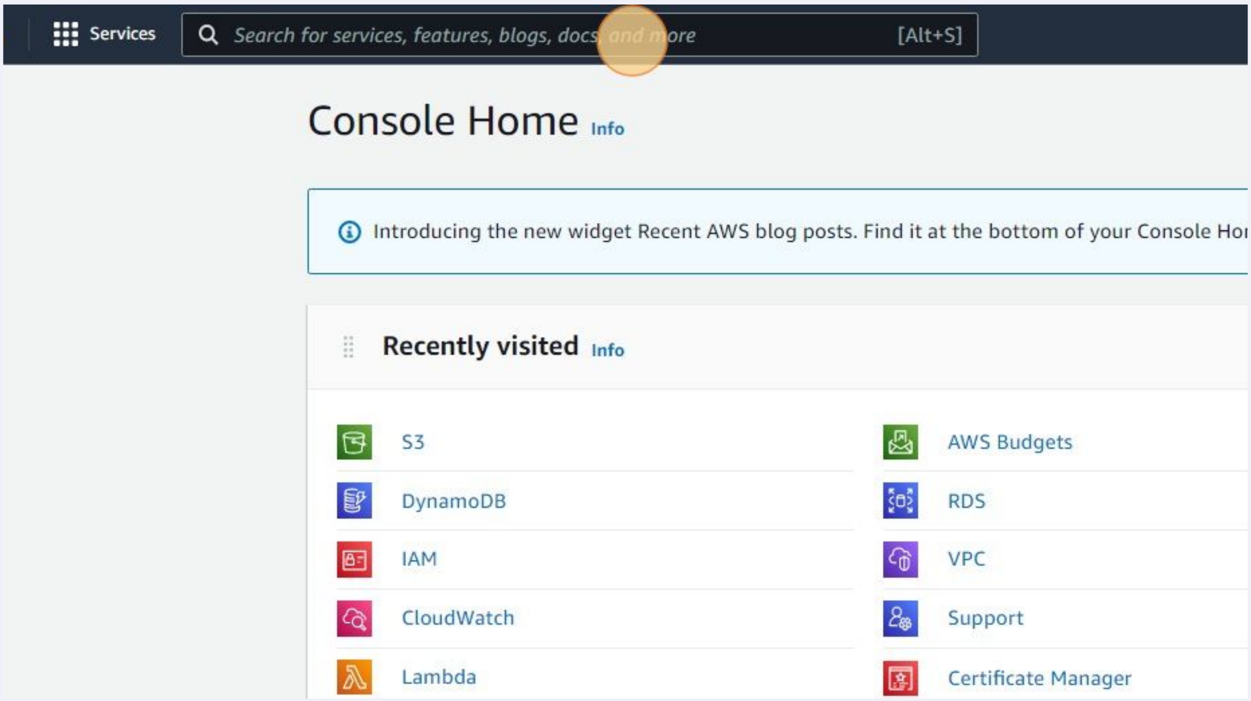
9 Click "Create bucket"


rn more
nd folders to the bucket, and configure additional bucket settings.
Cancel
Create bucket
tings

5. Creating Lambda function

1 Navigate to https://ap-south-1.console.aws.amazon.com/console/home?region=ap-south-1

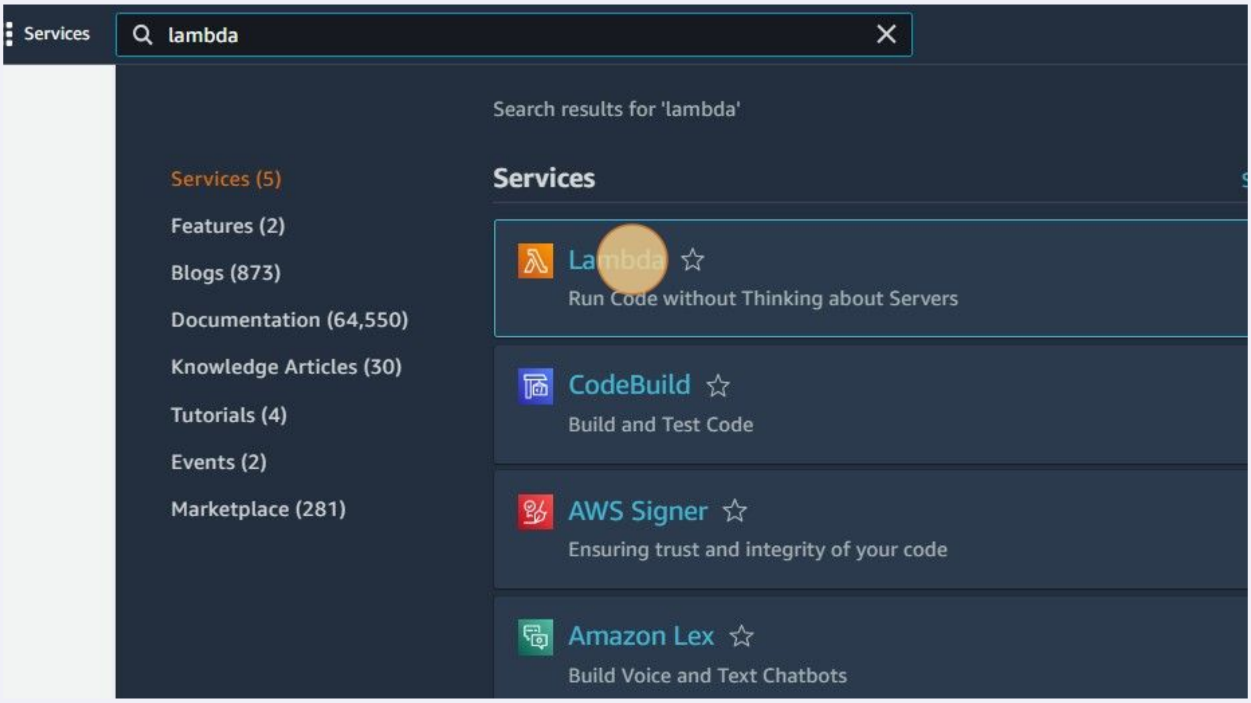
2 Click the "Search for services, features, blogs, docs, and more" field.



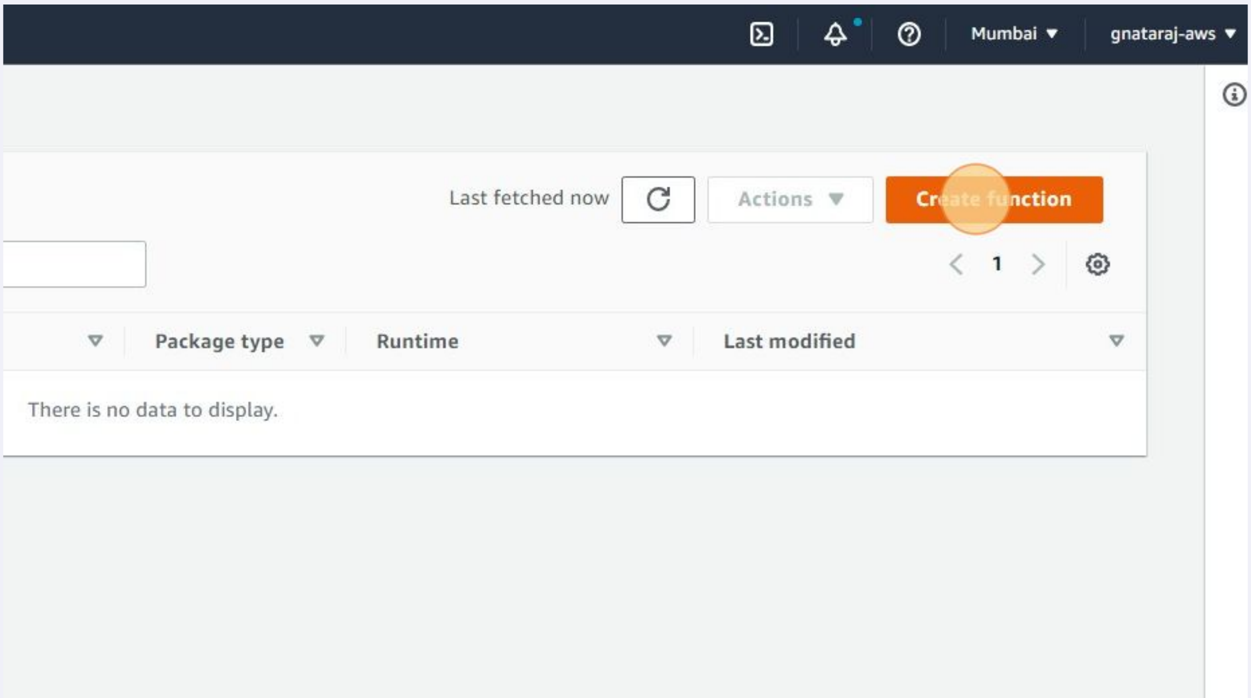
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Console Home
Info
Introducing the new widget Recent AWS blog posts. Find it at the bottom of your Console Hor
Recently visited
Info
S3
DynamoDB
IAM
CloudWatch
Lambda
AWS Budgets
RDS
VPC
Support
Certificate Manager

3 Type "lambda"

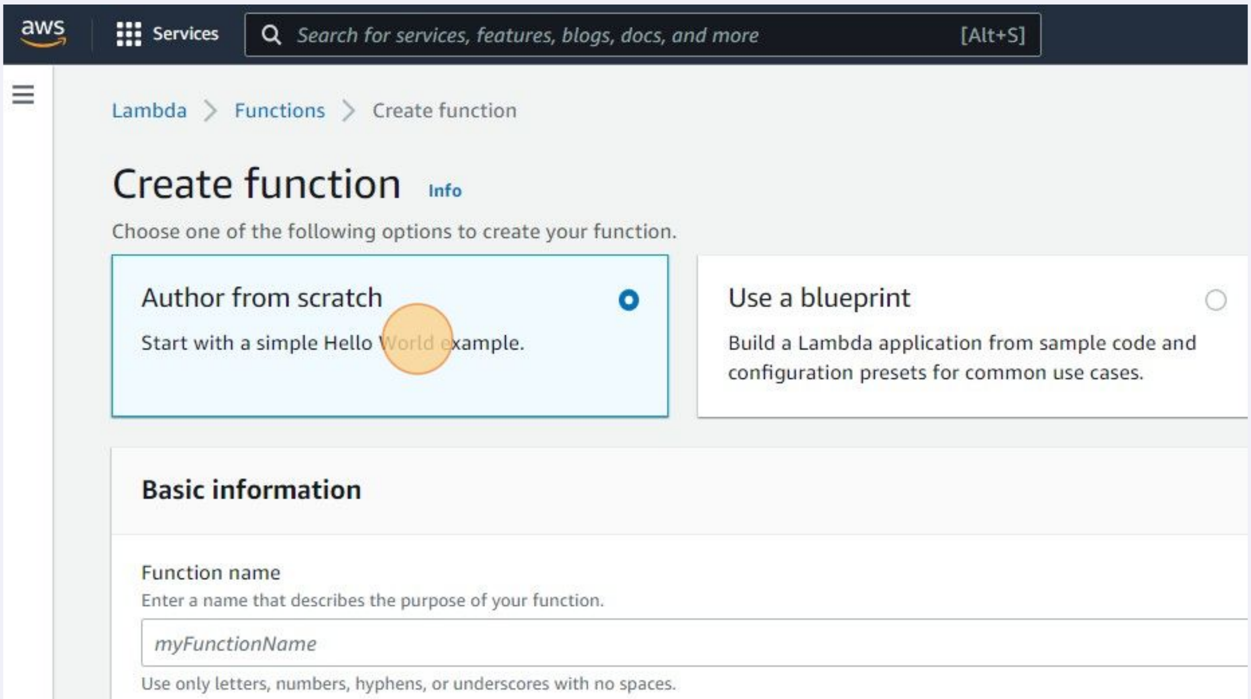
4 Click "Lambda"



5 Click "Create function"



6 Select Author from scratch



aws Services Search for services, features, blogs, docs, and more [Alt+S]

Lambda > Functions > Create function

Create function Info

Choose one of the following options to create your function.

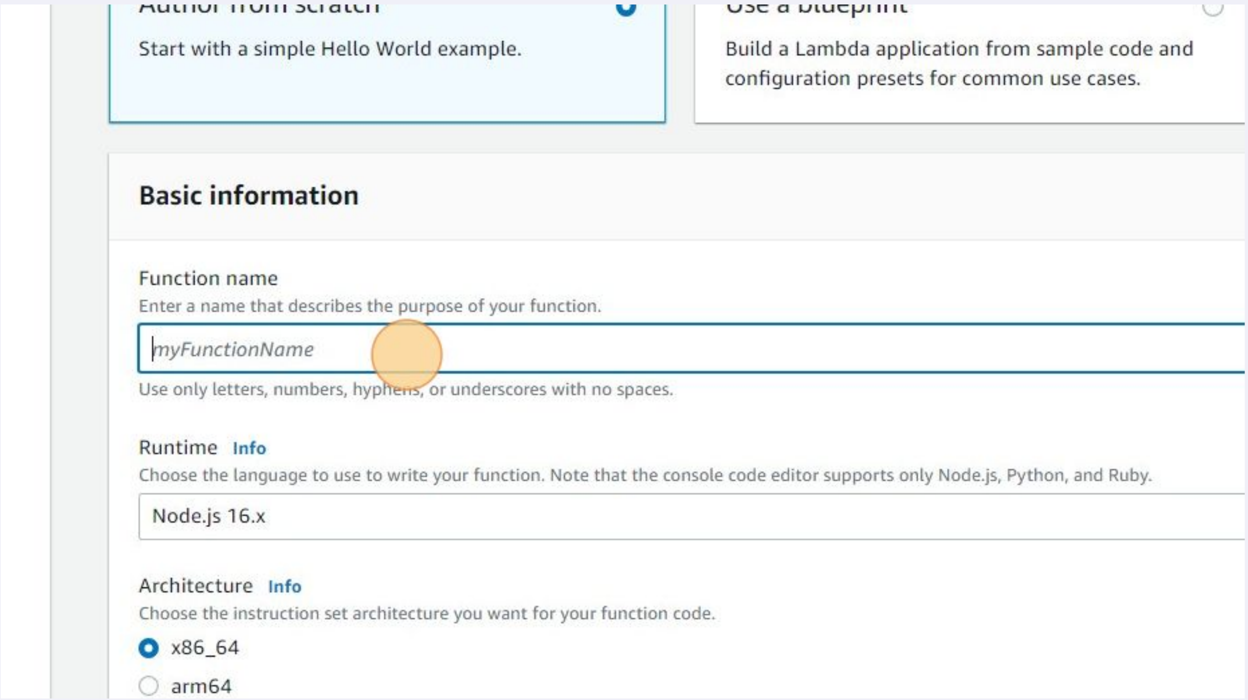
Author from scratch ●
Start with a simple Hello World example.

Use a blueprint ○
Build a Lambda application from sample code and configuration presets for common use cases.

Basic information

Function name
Enter a name that describes the purpose of your function.
myFunctionName
Use only letters, numbers, hyphens, or underscores with no spaces.

7 Click the "Function name" field.



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.

Basic information

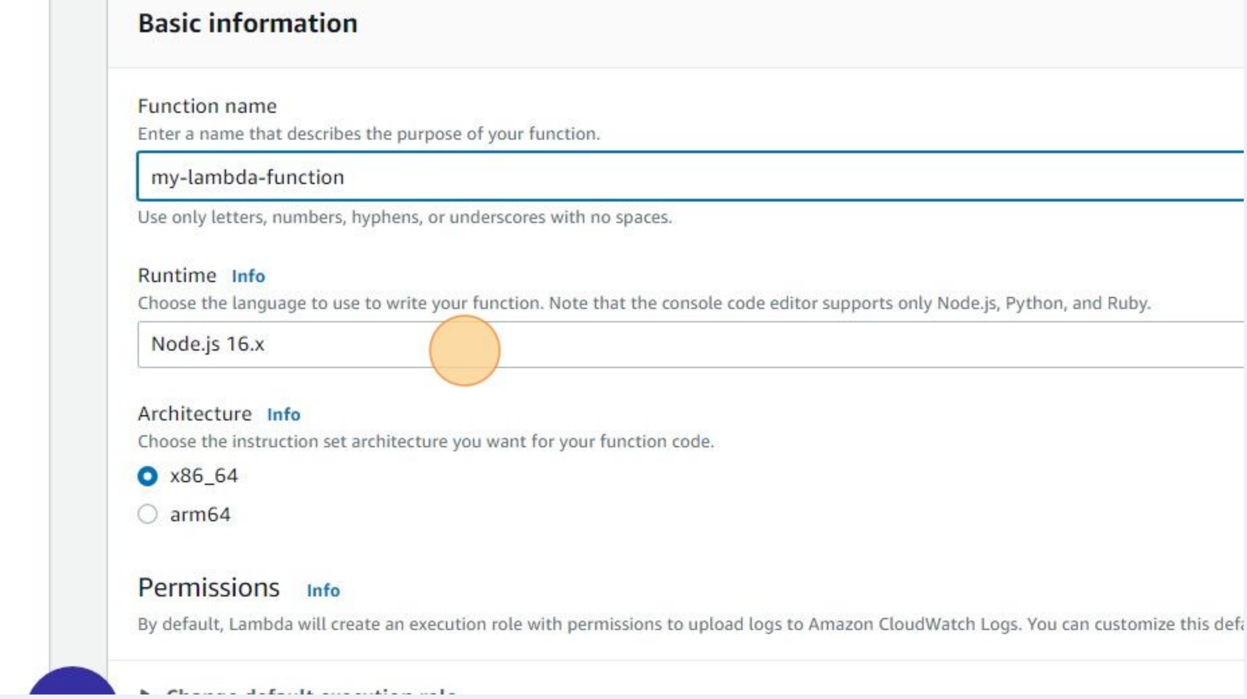
Function name
Enter a name that describes the purpose of your function.
myFunctionName
Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.
Node.js 16.x

Architecture Info
Choose the instruction set architecture you want for your function code.
● x86_64
○ arm64

8 Type "my-lambda-function"

9 In the Runtime dropdown,



Basic information

Function name

Enter a name that describes the purpose of your function.

my-lambda-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.

Node.js 16.x

Architecture Info

Choose the instruction set architecture you want for your function code.

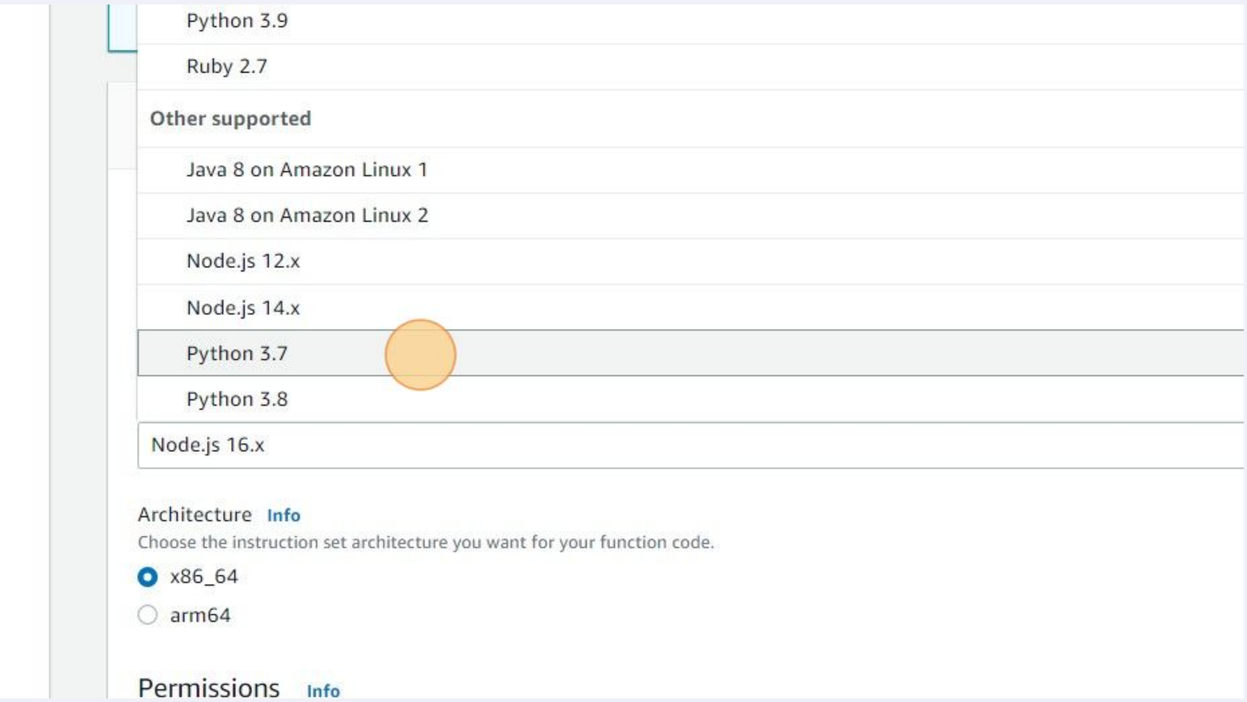
● x86_64

○ arm64

Permissions Info

By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this defa

10 Select Python3.7



Python 3.9

Ruby 2.7

Other supported

Java 8 on Amazon Linux 1

Java 8 on Amazon Linux 2

Node.js 12.x

Node.js 14.x

Python 3.7

Python 3.8

Node.js 16.x

Architecture Info

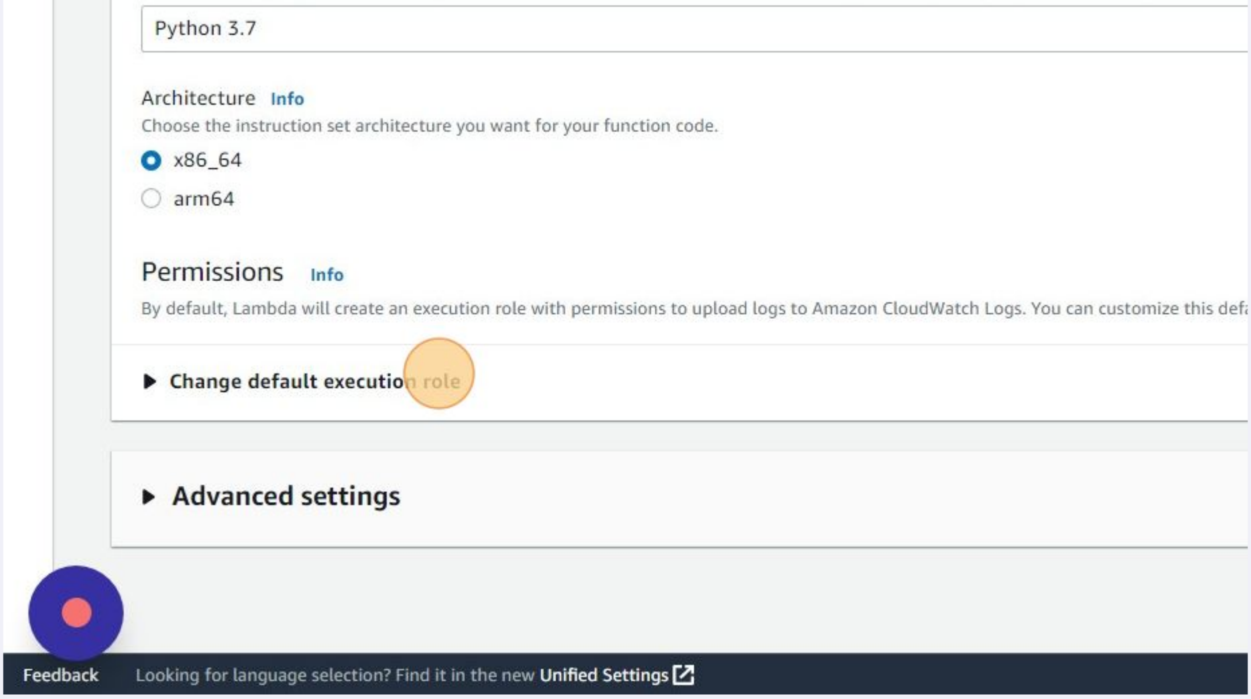
Choose the instruction set architecture you want for your function code.

● x86_64

○ arm64

Permissions Info

11 Click - Change default execution role



Python 3.7

Architecture Info

Choose the instruction set architecture you want for your function code.

● x86_64

○ arm64

Permissions Info

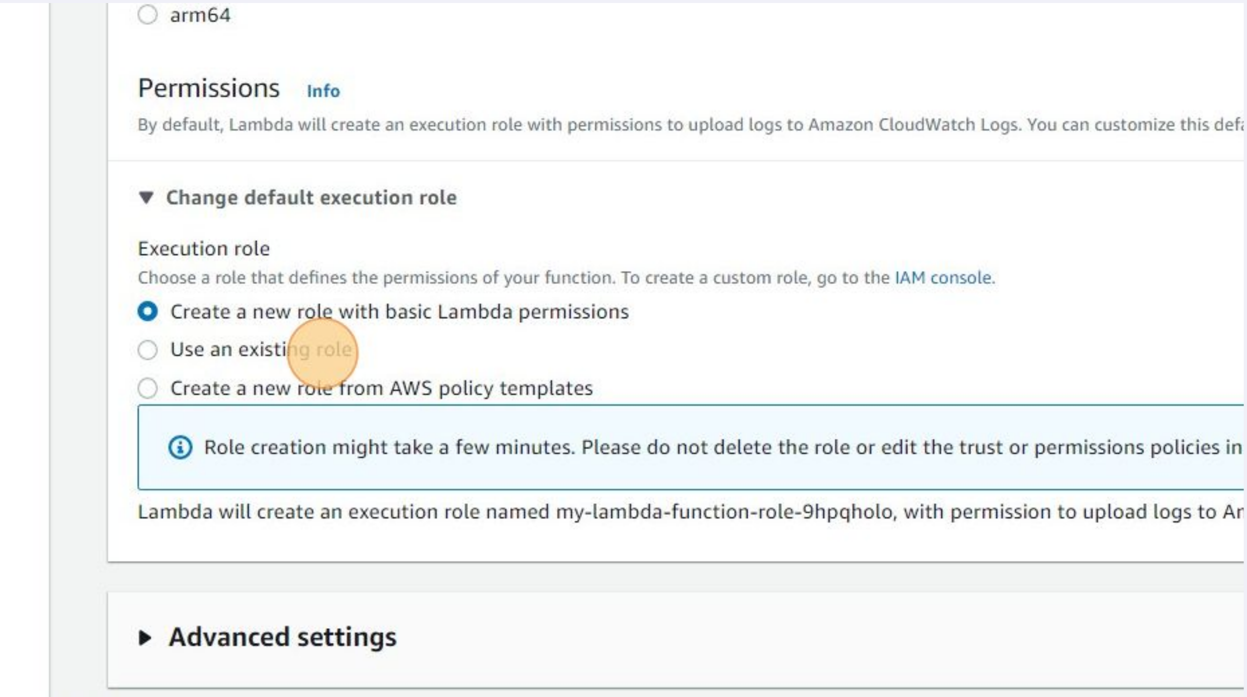
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this defa

▶ Change default execution role

▶ Advanced settings

Feedback Looking for language selection? Find it in the new Unified Settings

12 Click "Use an existing role"



○ arm64

Permissions Info

By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this defa

▼ 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

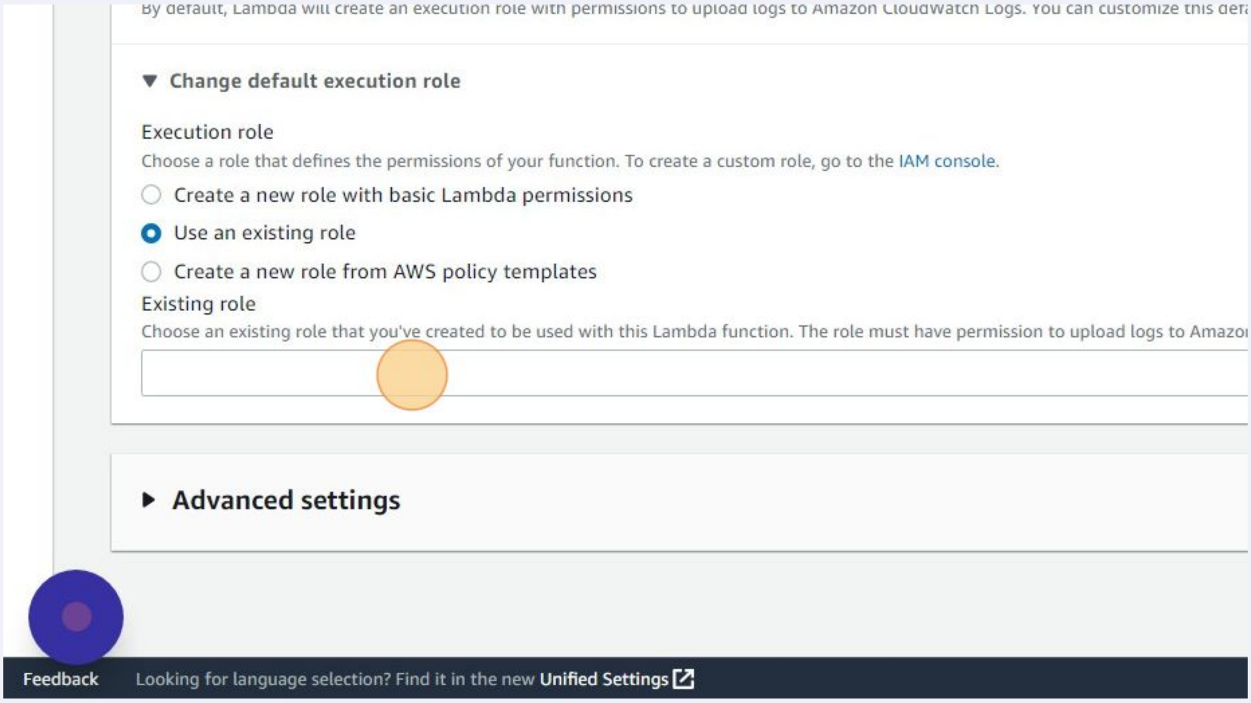
○ Create a new role from AWS policy templates

ⓘ Role creation might take a few minutes. Please do not delete the role or edit the trust or permissions policies in

Lambda will create an execution role named my-lambda-function-role-9hpqholo, with permission to upload logs to Ar

▶ Advanced settings

13 Click Use an existing role



By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this defa

▼ 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

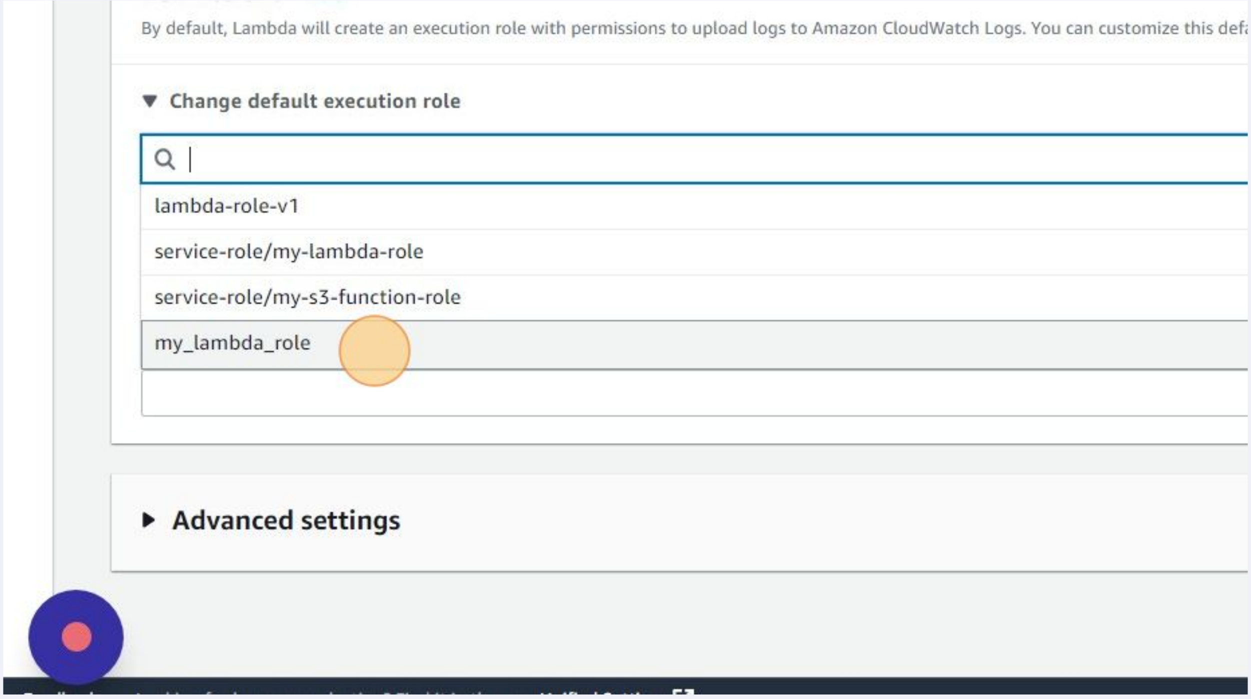
Existing role

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

▶ Advanced settings

Feedback
Looking for language selection? Find it in the new Unified Settings

14 Select the my_lambda_role (which was created earlier)



By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this defa

▼ Change default execution role

lambda-role-v1

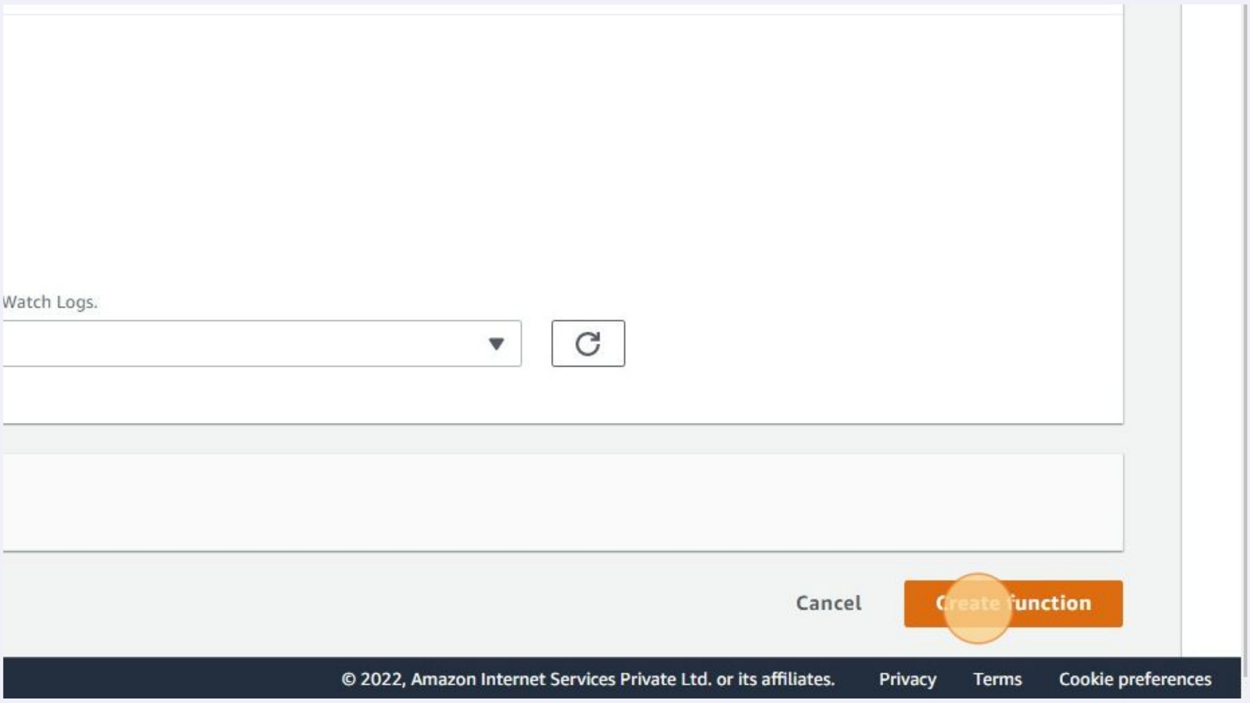
service-role/my-lambda-role

service-role/my-s3-function-role

my_lambda_role

▶ Advanced settings

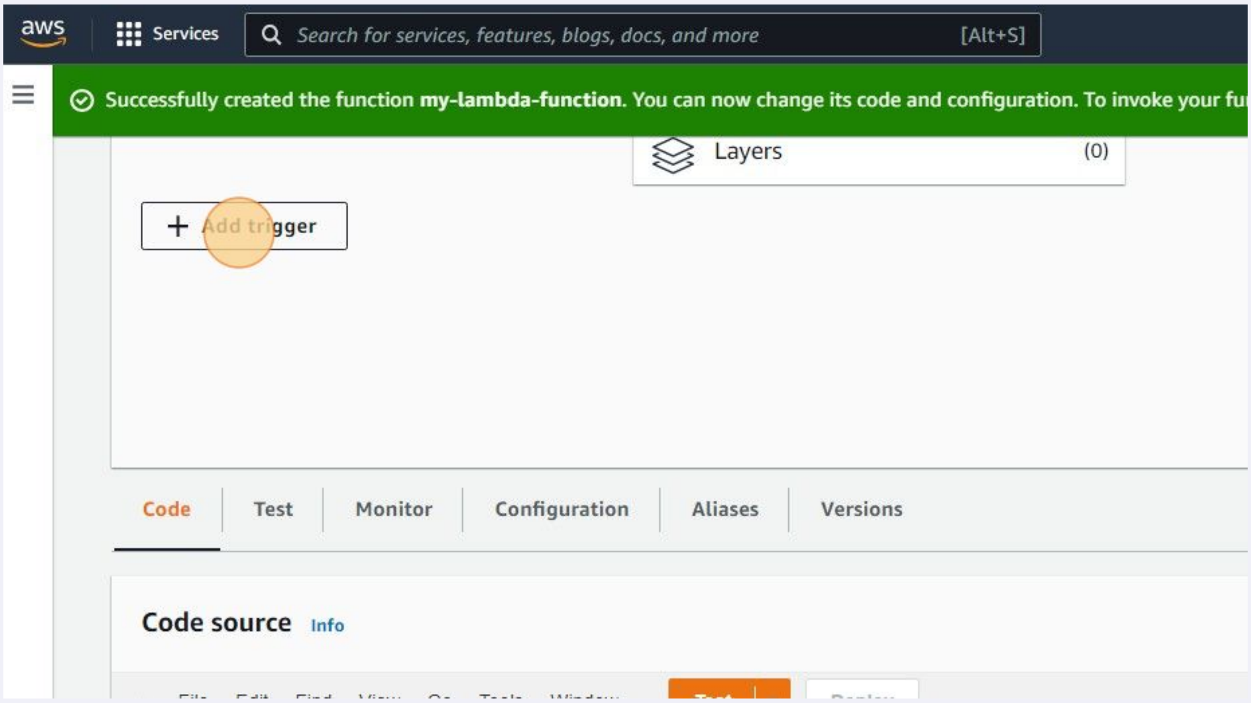
15 Click "Create function"



Watch Logs.

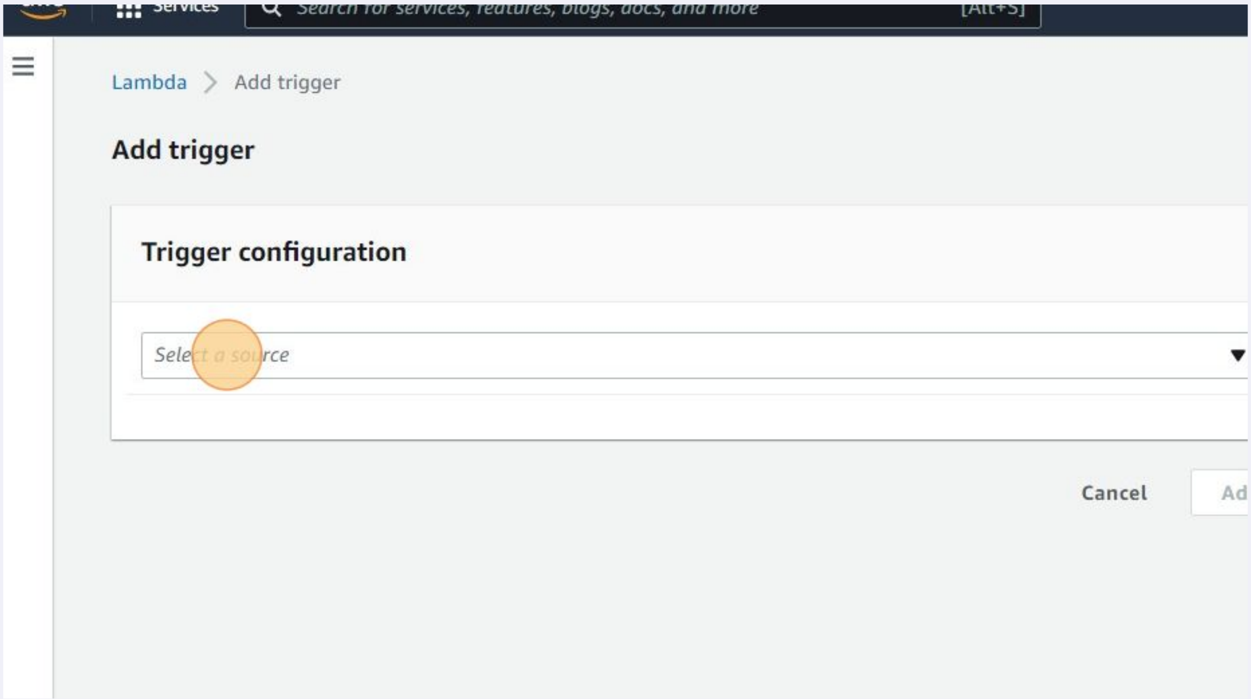
Cancel
Create function
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

16 Click "Add trigger"



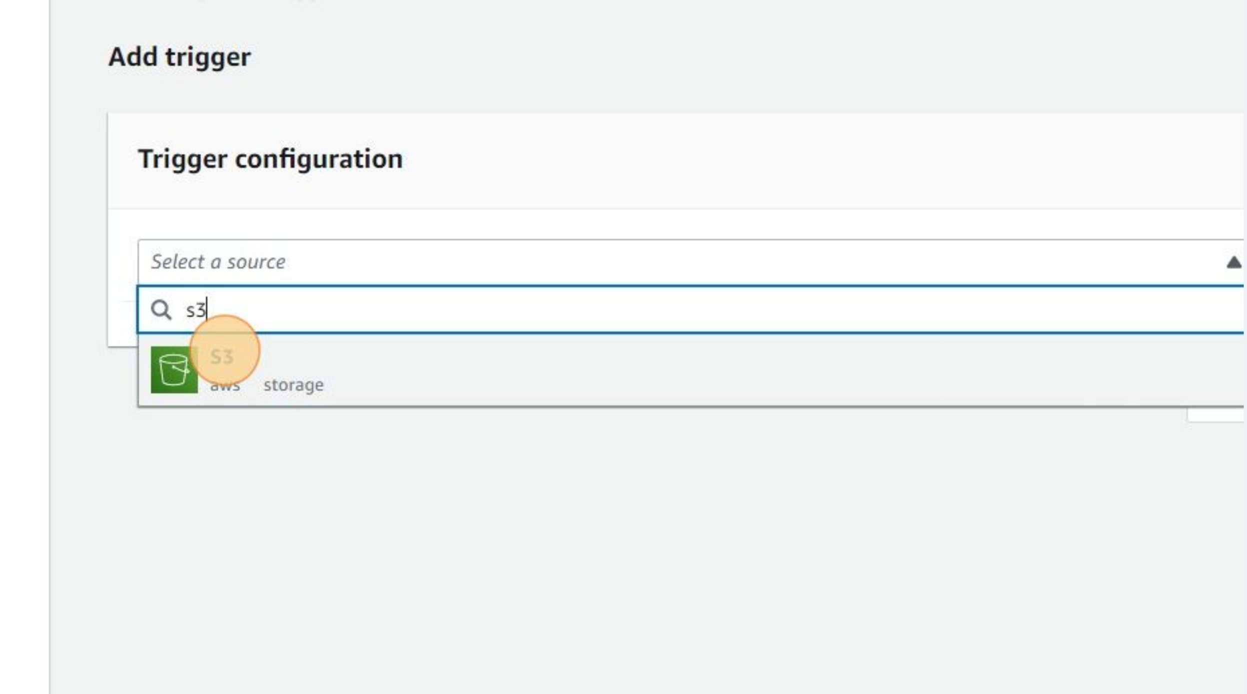
Successfully created the function **my-lambda-function**. You can now change its code and configuration. To invoke your fu

17 Click "Select a source"



18 Type "s3"

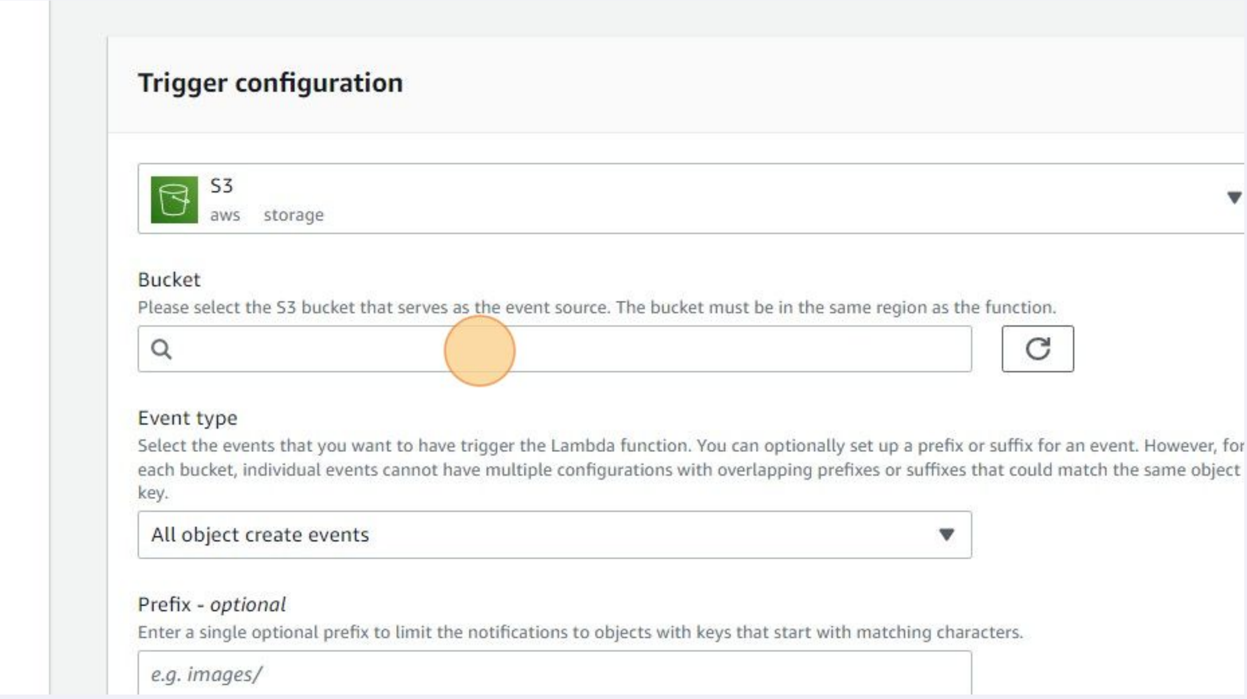
19 Click "S3"



Add trigger

Trigger configuration

20 Click the "Bucket" field.



Trigger configuration

S3
aws storage

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

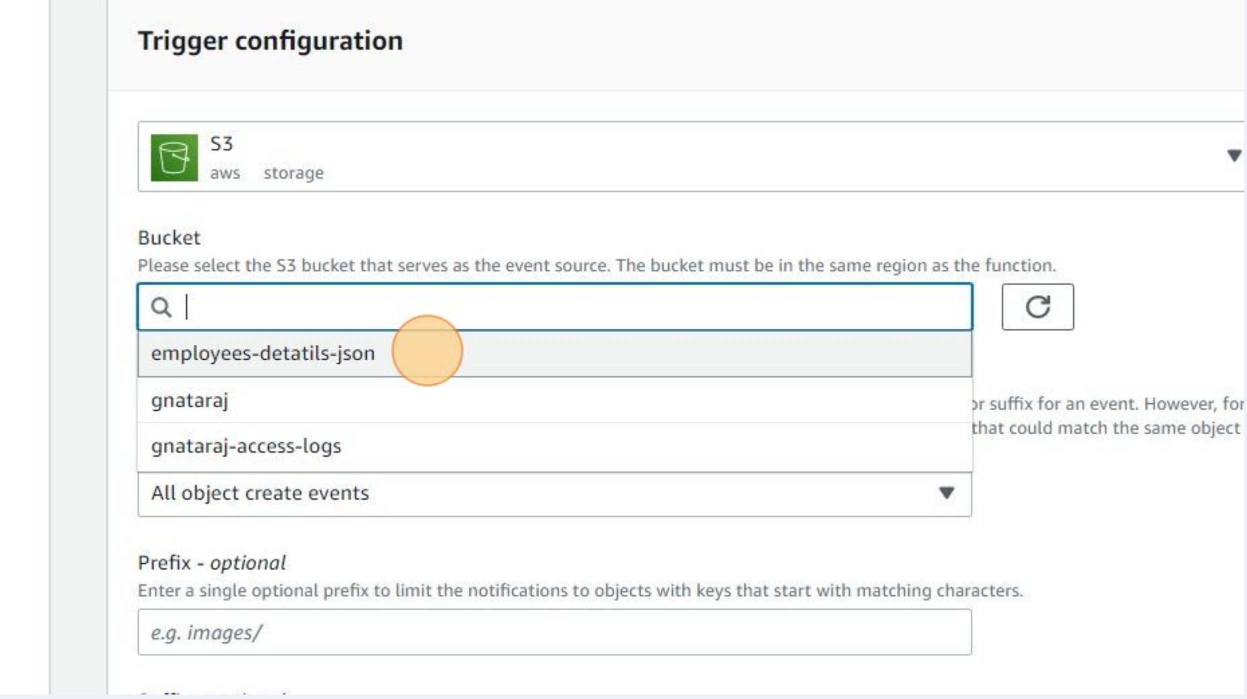
Event type
Select the events that you want to have trigger the Lambda function. You can optionally set up a prefix or suffix for an event. However, for each bucket, individual events cannot have multiple configurations with overlapping prefixes or suffixes that could match the same object key.

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/

21 Select the bucket created for this purpose



Trigger configuration

S3
aws storage

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

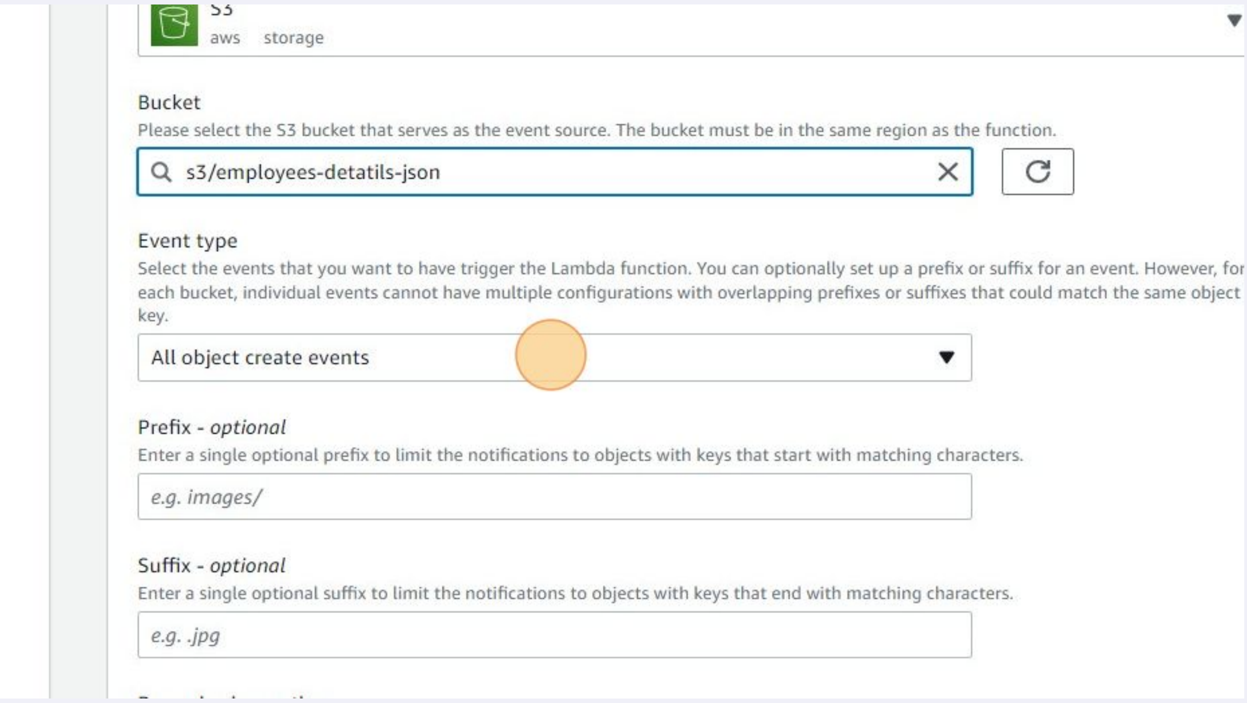
employees-detatils-json
gnataraj
gnataraj-access-logs

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/

22 Click "All object create events"



S3
aws storage

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

s3/employees-detatils-json

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

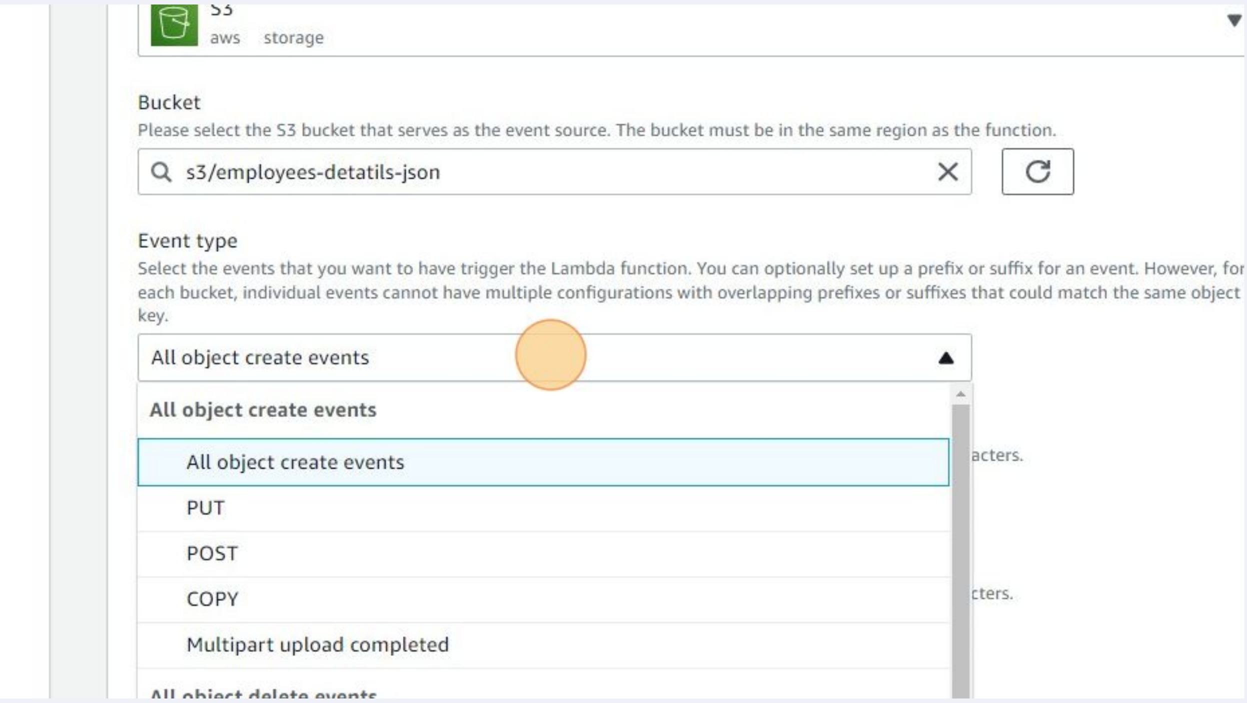
Prefix - *optional*
Enter a single optional prefix to limit the notifications to objects with keys that start with matching characters.

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

23 Click "All object create events"



S3
aws storage

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

s3/employees-detatils-json

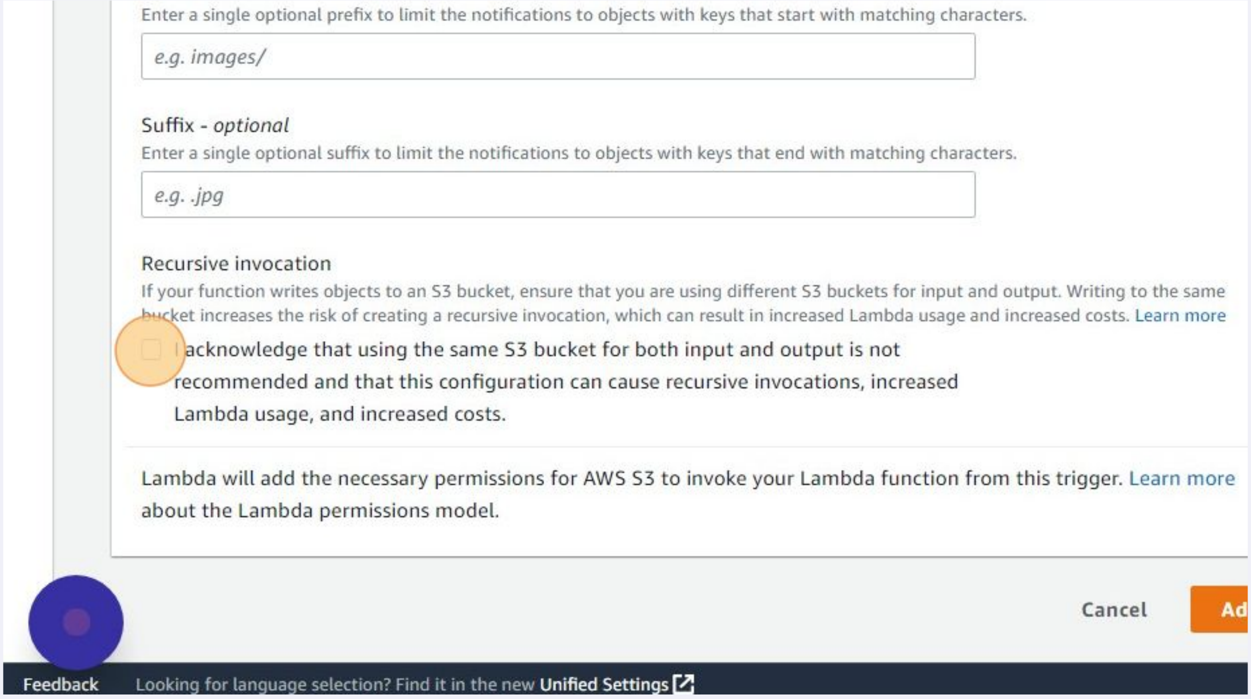
Event type
Select the events that you want to have trigger the Lambda function. You can optionally set up a prefix or suffix for an event. However, for each bucket, individual events cannot have multiple configurations with overlapping prefixes or suffixes that could match the same object key.

All object create events

All object create events
- All object create events
- PUT
- POST
- COPY
- Multipart upload completed

All object delete events

24 Click the "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." field.



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

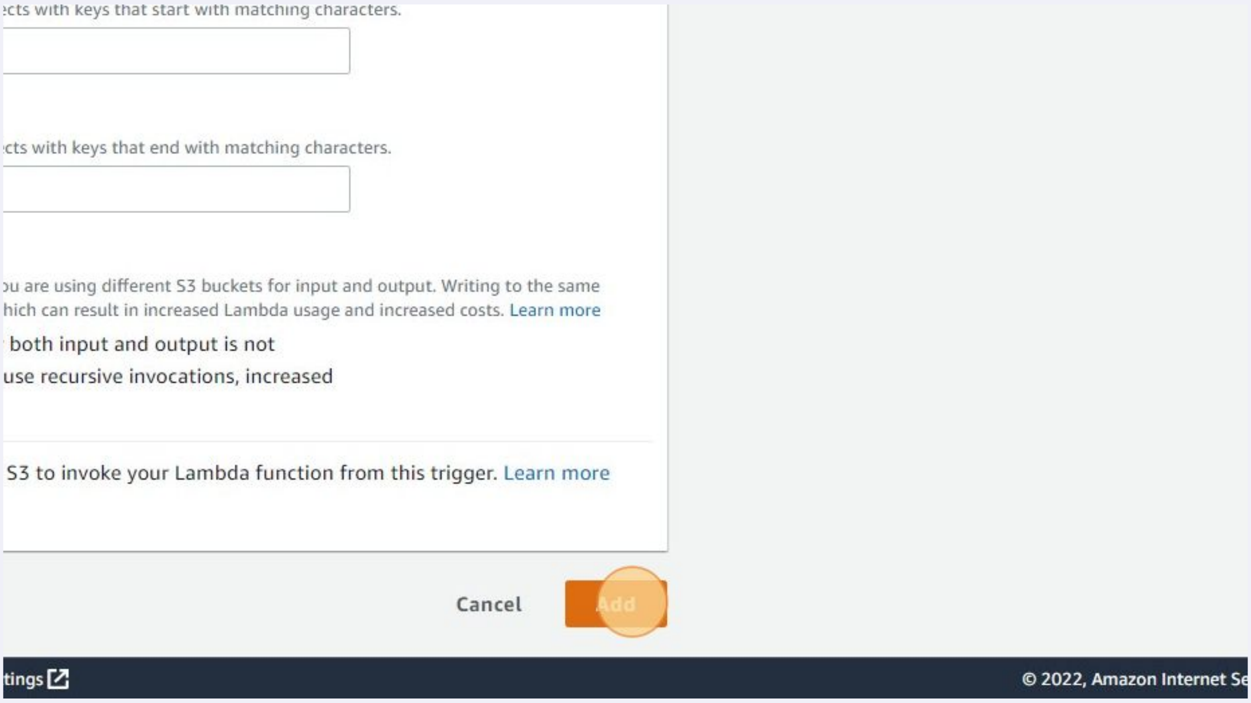
If your function writes objects to an S3 bucket, ensure that you are using different S3 buckets for input and output. Writing to the same bucket increases the risk of creating a recursive invocation, which can result in increased Lambda usage and increased costs. Learn more

□ 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.

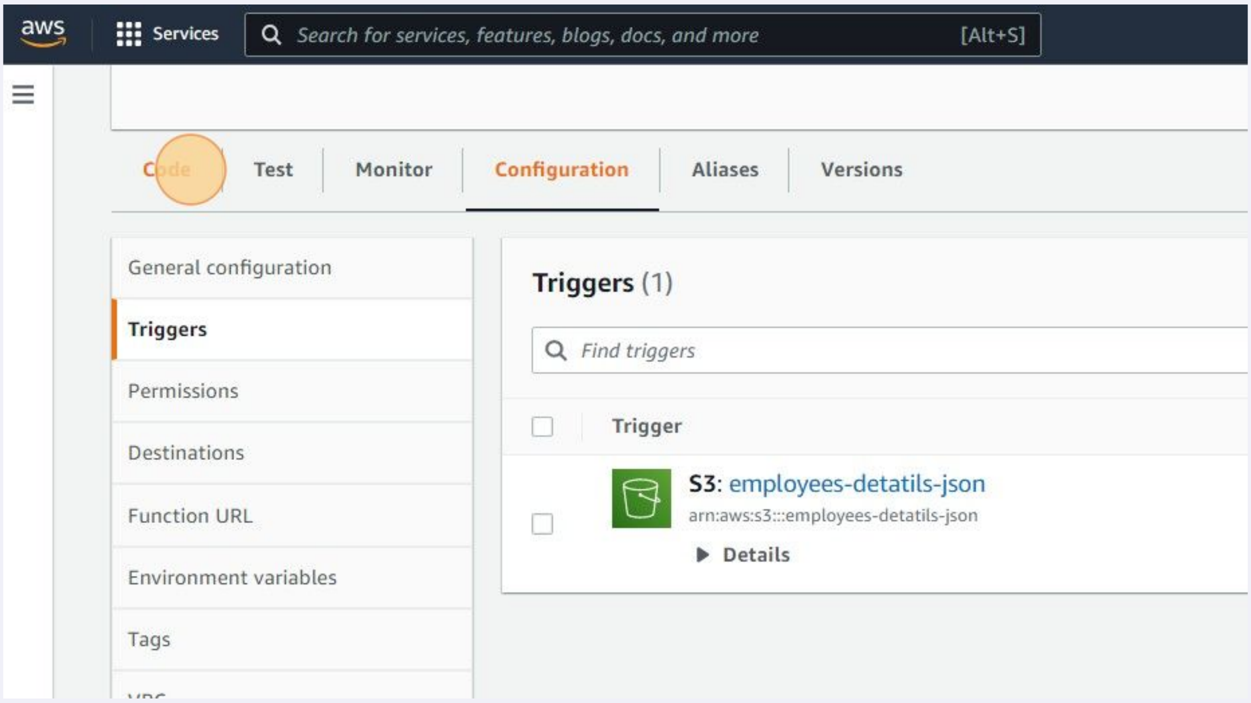
Cancel
Ad
Feedback
Looking for language selection? Find it in the new Unified Settings

25 Click "Add"



ects with keys that start with matching characters.
cts with keys that end with matching characters.
ou are using different S3 buckets for input and output. Writing to the same
hich can result in increased Lambda usage and increased costs. Learn more
both input and output is not
use recursive invocations, increased
S3 to invoke your Lambda function from this trigger. Learn more
Cancel
Add
tings
© 2022, Amazon Internet Se

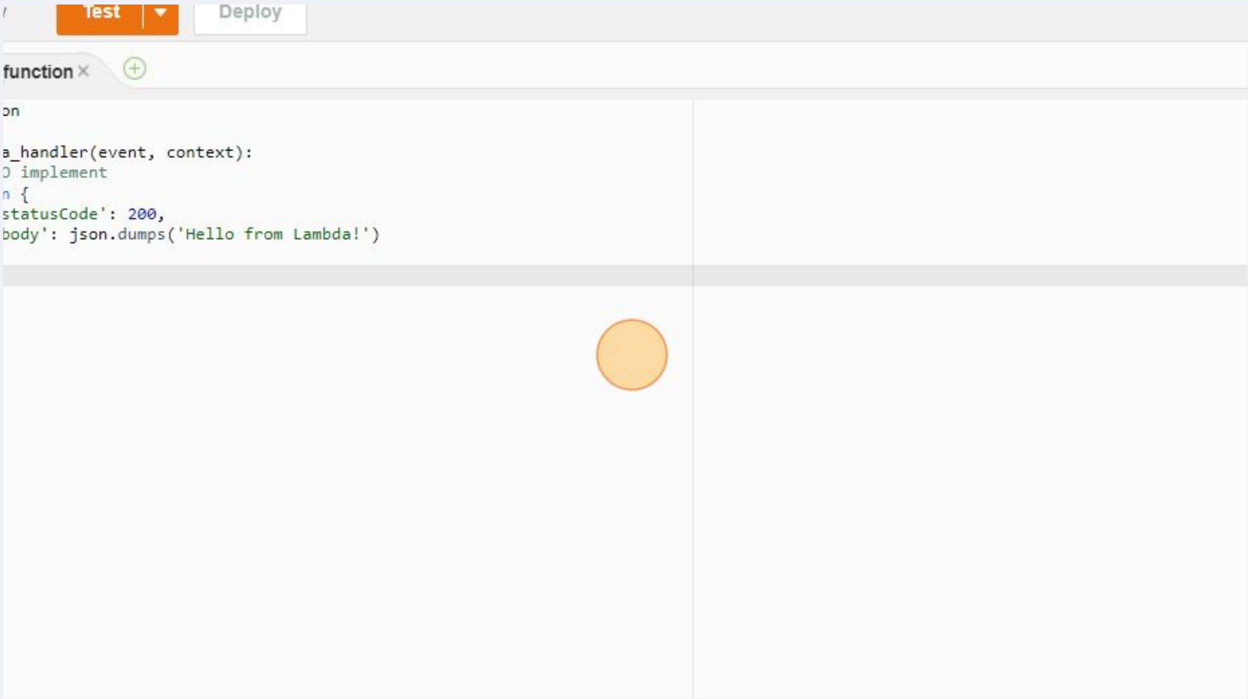
26 Click "Code"



□ Trigger

□ S3: employees-detatils-json
arn:aws:s3:::employees-detatils-json

27 Delete the template code created

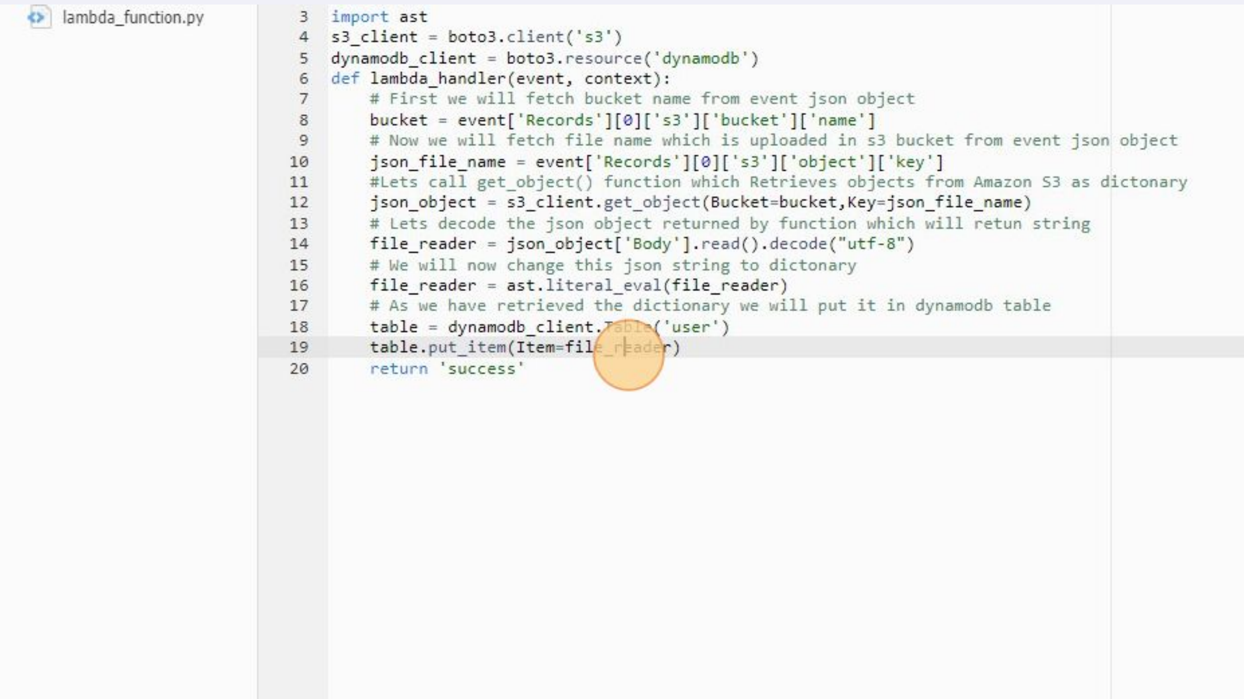


```
on

a_handler(event, context):
O implement
n {
statusCode': 200,
body': json.dumps('Hello from Lambda!')
```

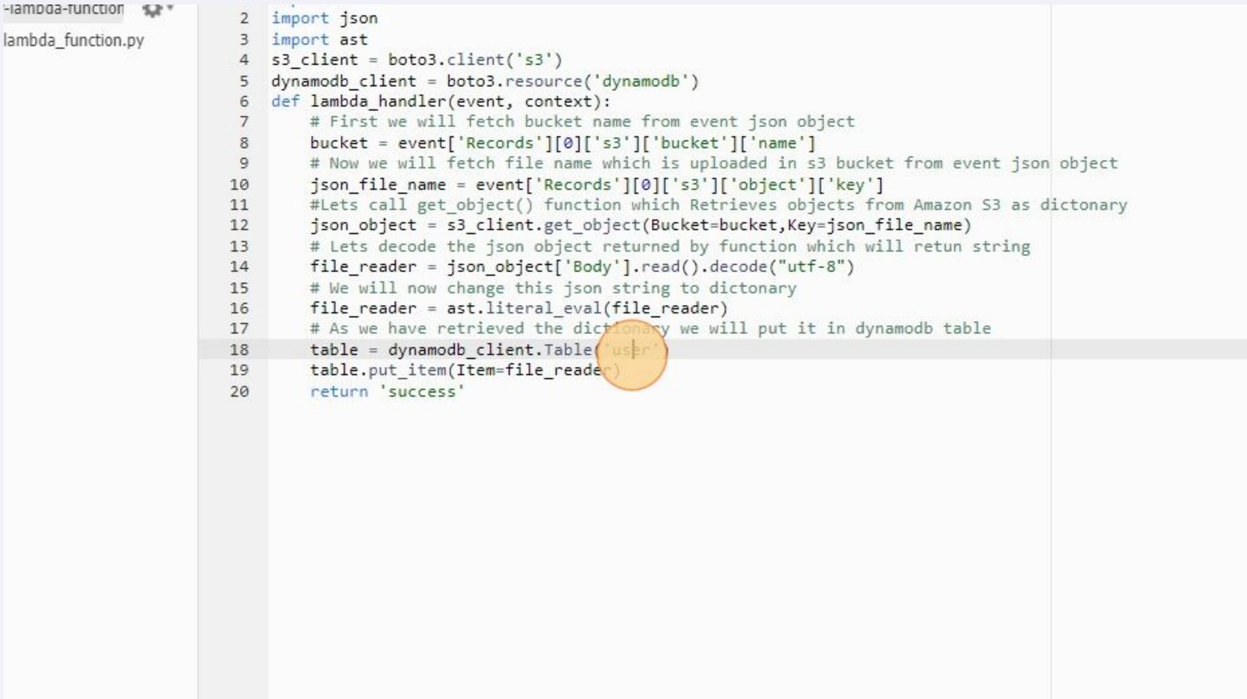
28 Switch to tab "https://raw.githubusercontent.com/gnataraj/aws-lambda/main/emp-json-s3-dynamodb.py"

29 Copy and Paste the code to the code editor



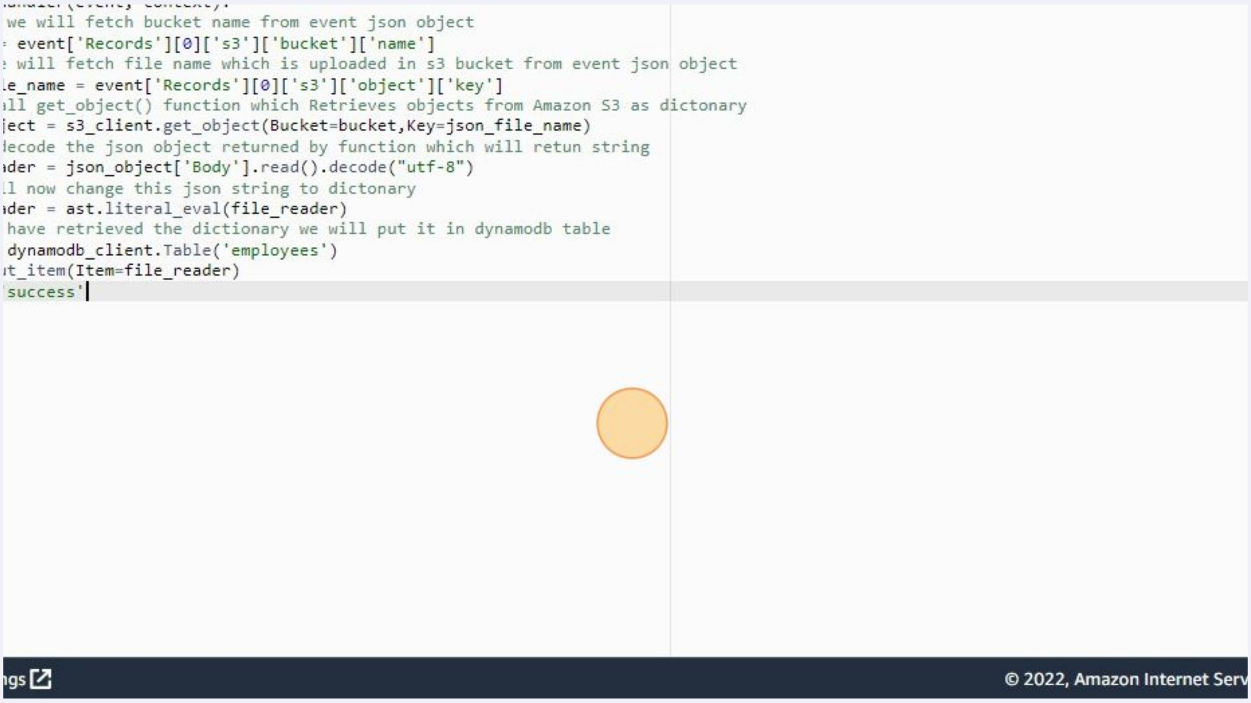
```python
import ast
s3_client = boto3.client('s3')
dynamodb_client = boto3.resource('dynamodb')
def lambda_handler(event, context):
    # First we will fetch bucket name from event json object
    bucket = event['Records'][0]['s3']['bucket']['name']
    # Now we will fetch file name which is uploaded in s3 bucket from event json object
    json_file_name = event['Records'][0]['s3']['object']['key']
    #Lets call get_object() function which Retrieves objects from Amazon S3 as dictonary
    json_object = s3_client.get_object(Bucket=bucket,Key=json_file_name)
    # Lets decode the json object returned by function which will retun string
    file_reader = json_object['Body'].read().decode("utf-8")
    # We will now change this json string to dictonary
    file_reader = ast.literal_eval(file_reader)
    # As we have retrieved the dictionary we will put it in dynamodb table
    table = dynamodb_client.Table('user')
    table.put_item(Item=file_reader)
    return 'success'
```

30 Update the table name to the table you created (employees)



```
import json
import ast
s3_client = boto3.client('s3')
dynamodb_client = boto3.resource('dynamodb')
def lambda_handler(event, context):
    # First we will fetch bucket name from event json object
    bucket = event['Records'][0]['s3']['bucket']['name']
    # Now we will fetch file name which is uploaded in s3 bucket from event json object
    json_file_name = event['Records'][0]['s3']['object']['key']
    #Lets call get_object() function which Retrieves objects from Amazon S3 as dictonary
    json_object = s3_client.get_object(Bucket=bucket,Key=json_file_name)
    # Lets decode the json object returned by function which will retun string
    file_reader = json_object['Body'].read().decode("utf-8")
    # We will now change this json string to dictonary
    file_reader = ast.literal_eval(file_reader)
    # As we have retrieved the dictionary we will put it in dynamodb table
    table = dynamodb_client.Table('user')
    table.put_item(Item=file_reader)
    return 'success'
```

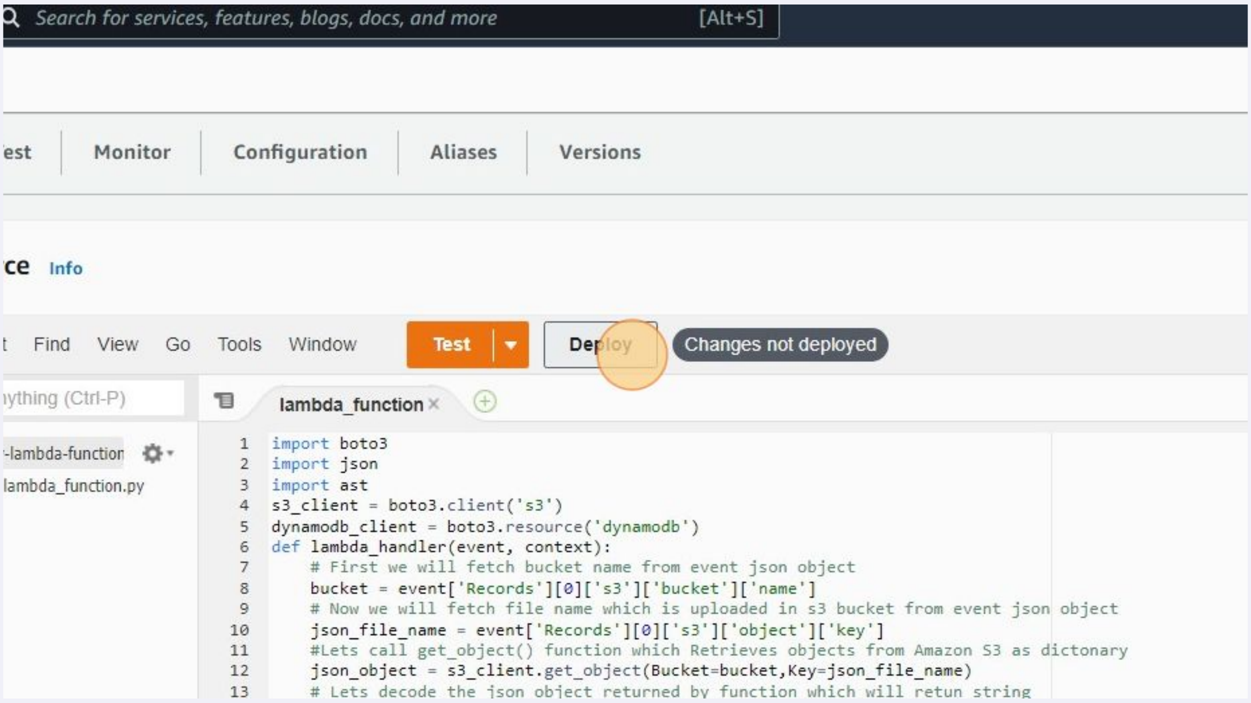
31 Click here.



```
 we will fetch bucket name from event json object
 event['Records'][0]['s3']['bucket']['name']
 will fetch file name which is uploaded in s3 bucket from event json object
le_name = event['Records'][0]['s3']['object']['key']
ll get_object() function which Retrieves objects from Amazon S3 as dictonary
ject = s3_client.get_object(Bucket=bucket,Key=json_file_name)
decode the json object returned by function which will retun string
ader = json_object['Body'].read().decode("utf-8")
ll now change this json string to dictonary
ader = ast.literal_eval(file_reader)
 have retrieved the dictionary we will put it in dynamodb table
 dynamodb_client.Table('employees')
ut_item(Item=file_reader)
'success'
```

32

Click "Deploy"

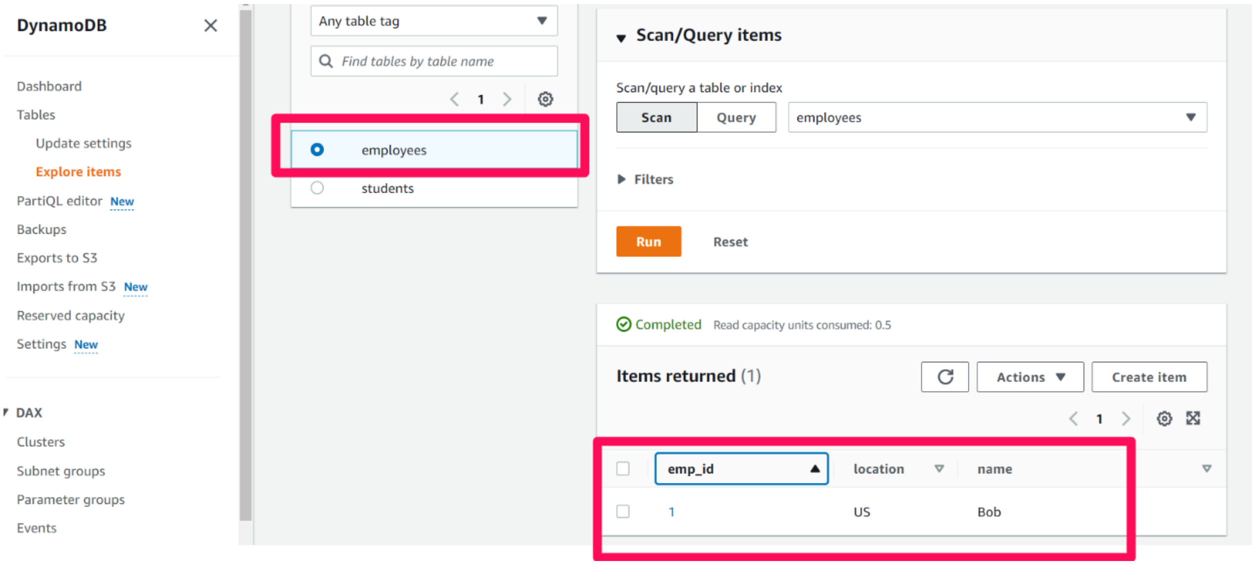


```
import boto3
import json
import ast
s3_client = boto3.client('s3')
dynamodb_client = boto3.resource('dynamodb')
def lambda_handler(event, context):
    # First we will fetch bucket name from event json object
    bucket = event['Records'][0]['s3']['bucket']['name']
    # Now we will fetch file name which is uploaded in s3 bucket from event json object
    json_file_name = event['Records'][0]['s3']['object']['key']
    #Lets call get_object() function which Retrieves objects from Amazon S3 as dictonary
    json_object = s3_client.get_object(Bucket=bucket,Key=json_file_name)
    # Lets decode the json object returned by function which will retun string
```

6. Testing the Serverless Application.

1. Create employee specific JSON files in your workstation in the following format:
   - emp_1.json

     ```
     {
        "emp_id": "1",
        "name": "Bob",
        "location": "US"
     }
     ```
2. Upload the emp_1.json to s3 bucket.
3. You should be able to see DynamoDB table automatically updated with this employee details as below.



Scan/query a table or index: Scan, employees

✓ Completed Read capacity units consumed: 0.5

Items returned (1)

	emp_id	location	name
□	1	US	Bob

4. Repeat the above steps with few more employee files uploaded in to S3 bucket.