LAMBA CROSS ACCOUNT WITH BUCKET POLICIES

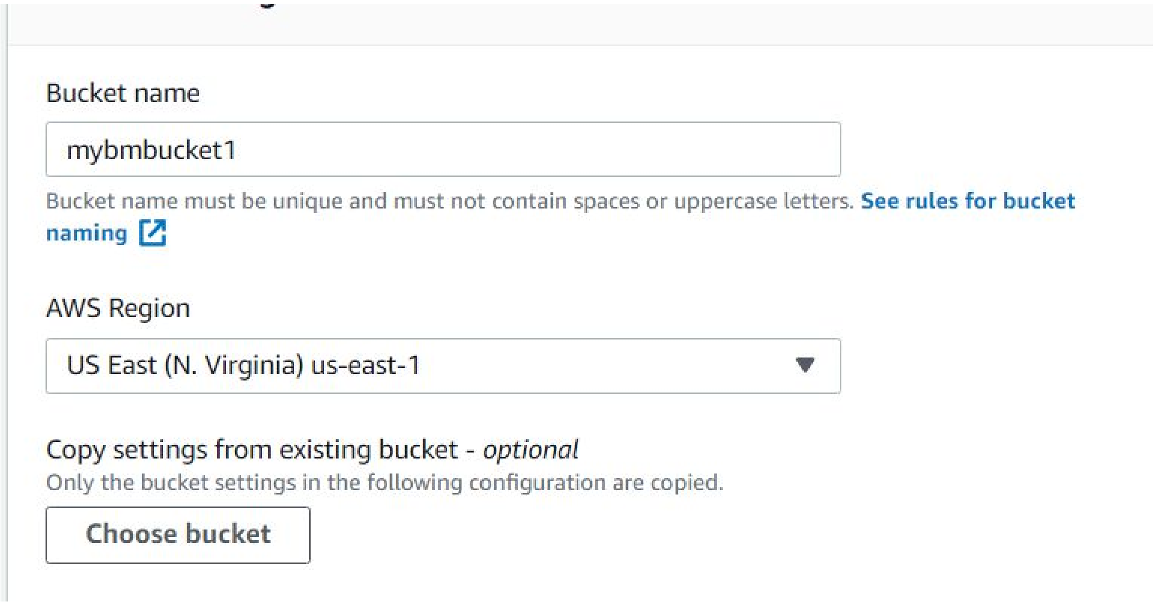
`This lab can be performed using two AWS accounts or one AWS account. Repeat the instruction in case the lab is performed using one AWS account only.

Steps - create the following:

- S3 bucket in account 2
- Lambda role in account 1
- Bucket policy for the S3 bucket in account 2
- Lambda in account 1
- Delete resources

Create new S3 bucket

- Go to the S3 console at https://console.aws.amazon.com/s3
- Type the bucket name and clcik on create bucket



Bucket name

mybmbucket1

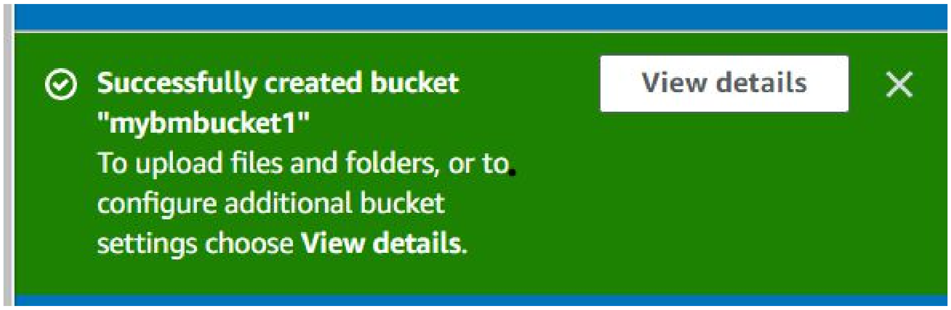
Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming

AWS Region

US East (N. Virginia) us-east-1

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

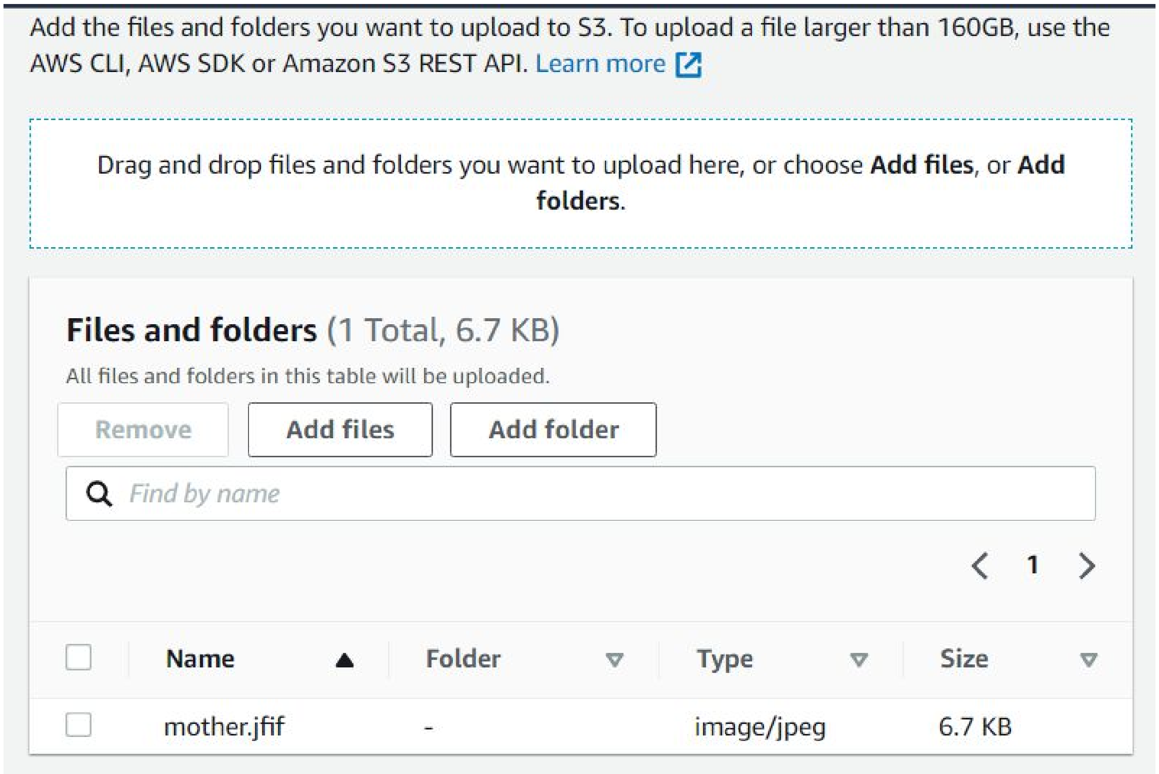


Successfully created bucket "mybmbucket1"

To upload files and folders, or to configure additional bucket settings choose **View details**.

Add object to an S3 bucket

- Click on the name of the bucket
- Drag the fileto upload to the bucket into the object upload area



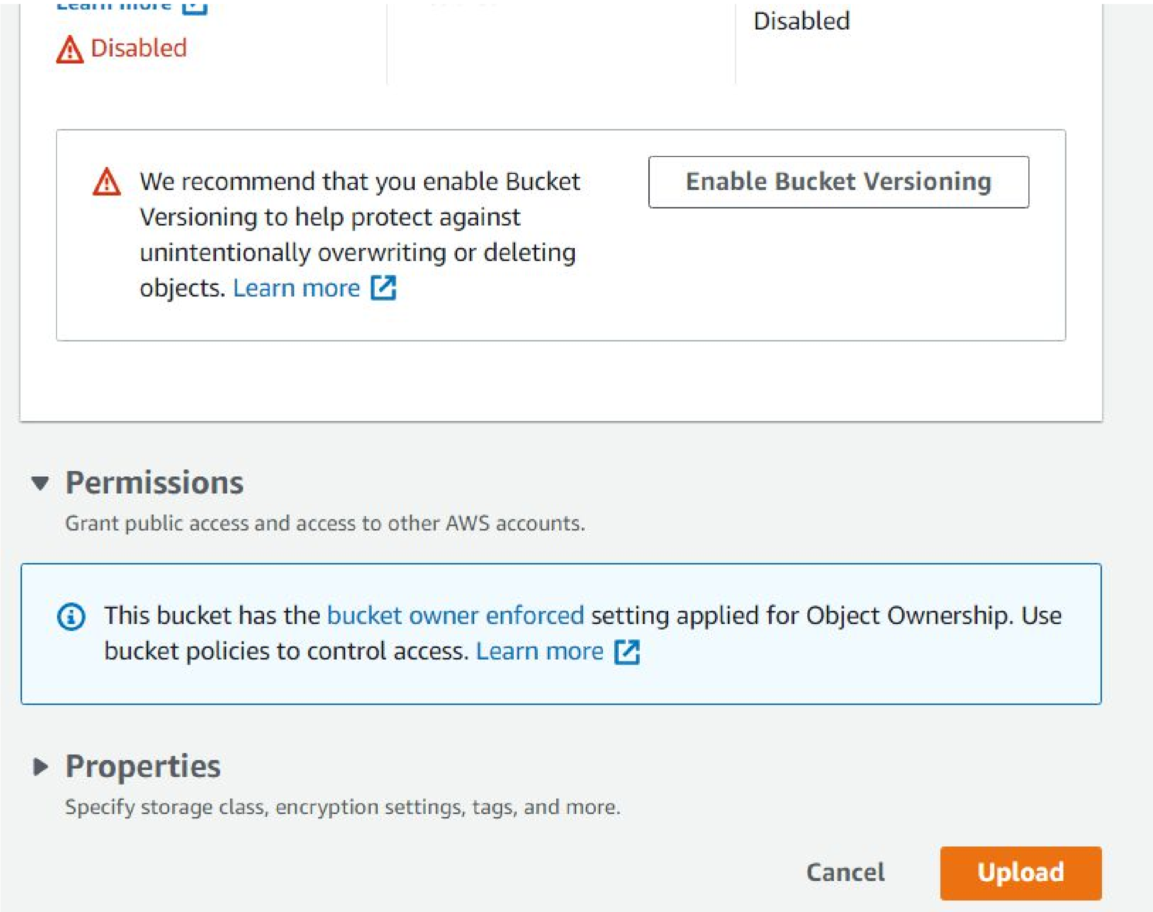
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

Files and folders (1 Total, 6.7 KB)

All files and folders in this table will be uploaded.

□	Name	Folder	Type	Size
□	mother.jfif	-	image/jpeg	6.7 KB



Learn more

⚠ Disabled

Disabled

⚠ We recommend that you enable Bucket Versioning to help protect against unintentionally overwriting or deleting objects. Learn more

▼ Permissions

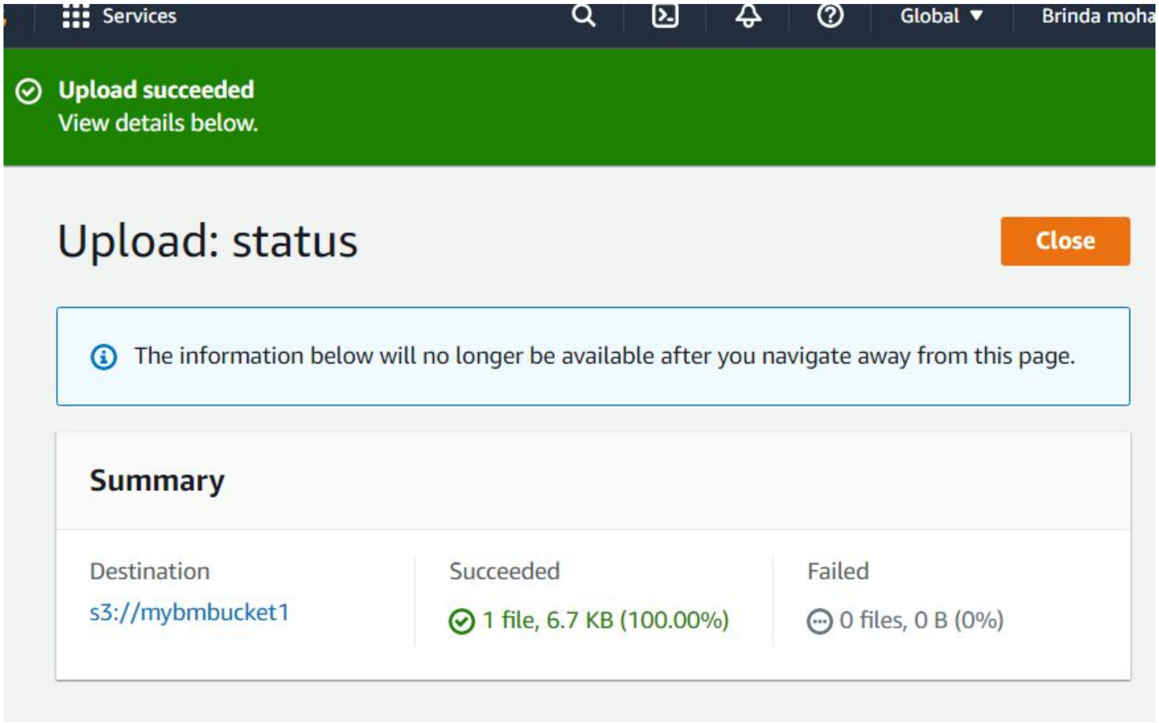
Grant public access and access to other AWS accounts.

ⓘ This bucket has the bucket owner enforced setting applied for Object Ownership. Use bucket policies to control access. Learn more

▶ Properties

Specify storage class, encryption settings, tags, and more.

Click Upload



Upload succeeded

View details below.

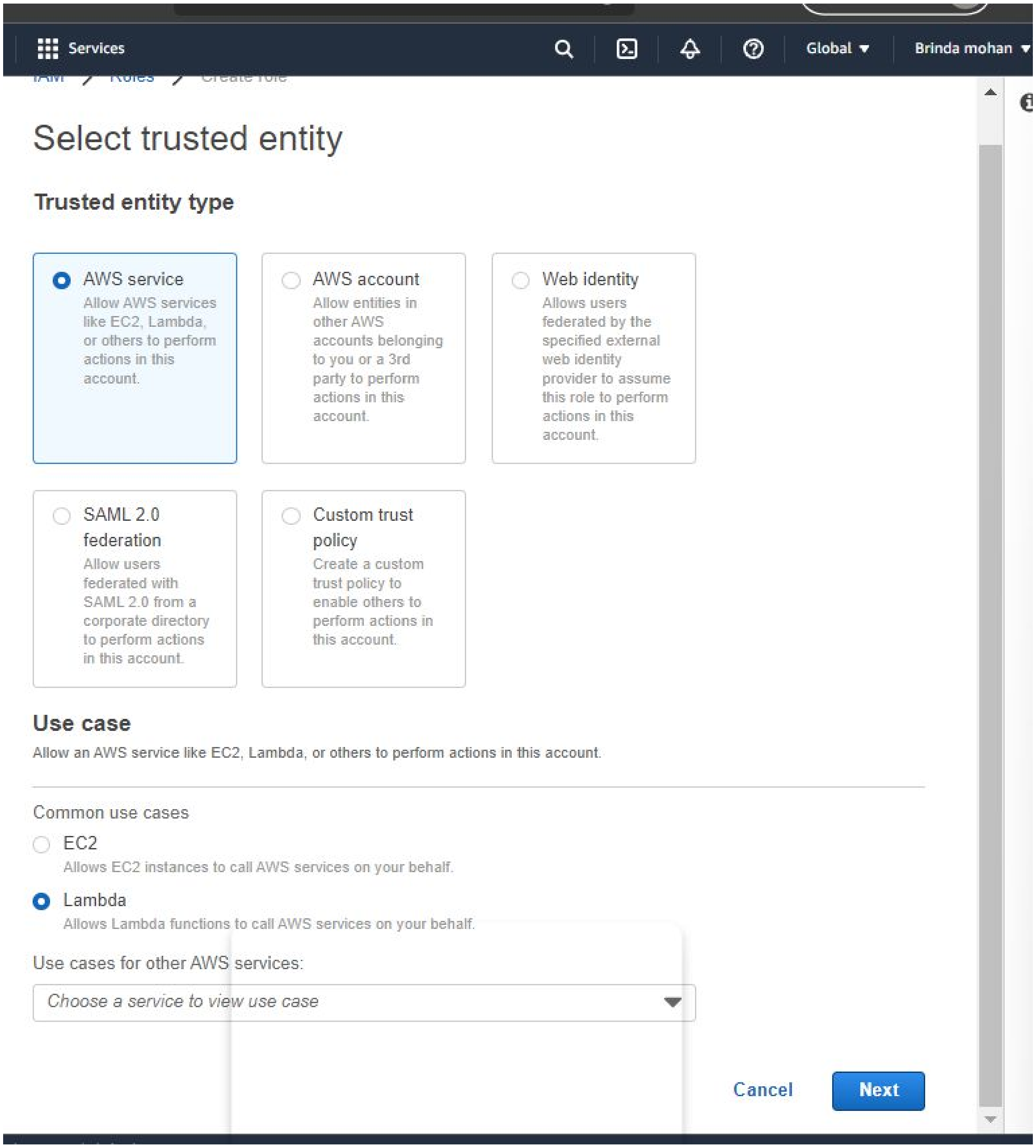
Upload: status

ⓘ The information below will no longer be available after you navigate away from this page.

Summary

Destination	Succeeded	Failed
s3://mybmbucket1	✓ 1 file, 6.7 KB (100.00%)	0 files, 0 B (0%)

Create Lambda role in account 1



Select trusted entity

Trusted entity type

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

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

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

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case

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

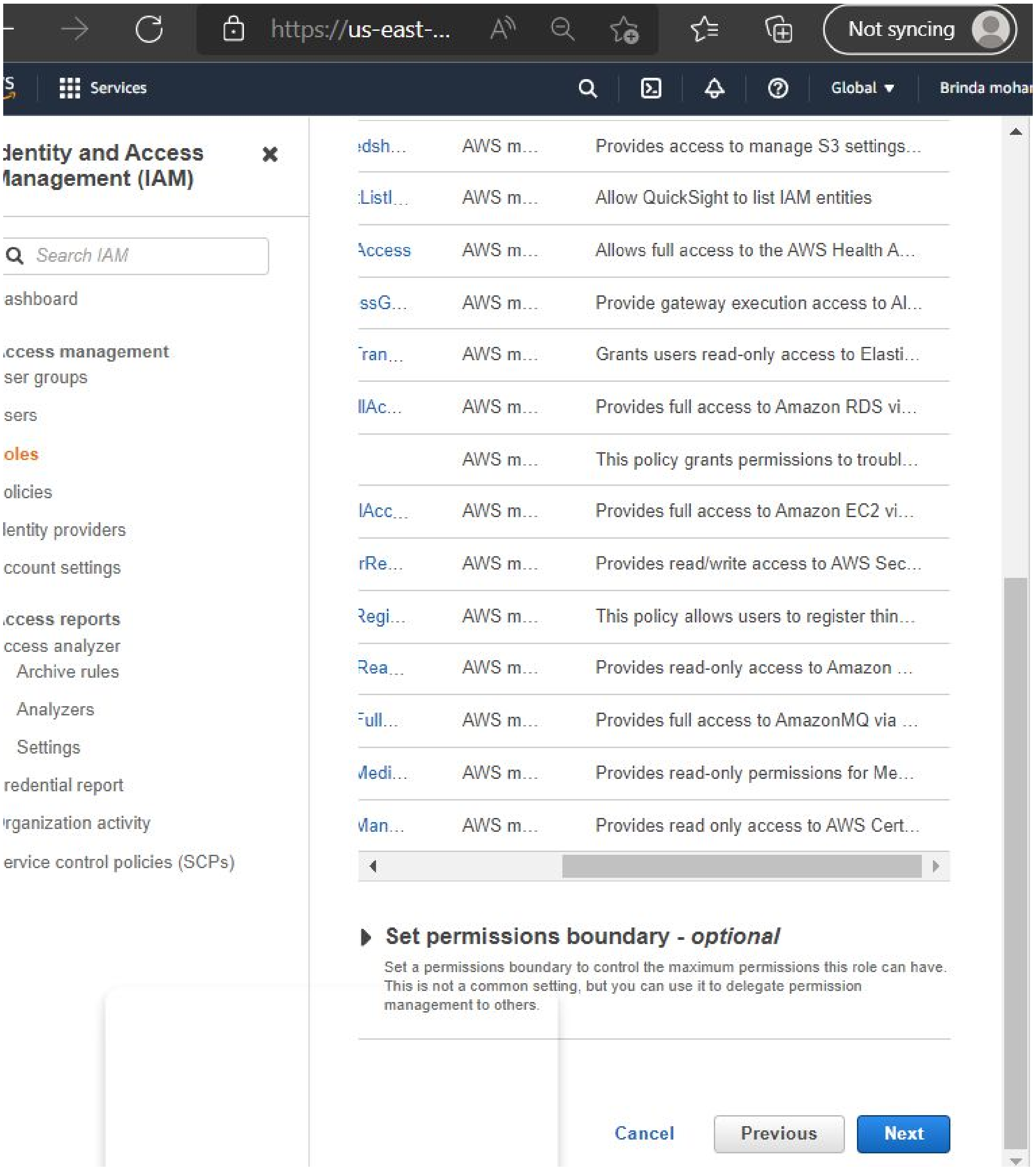
Common use cases

○ 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:

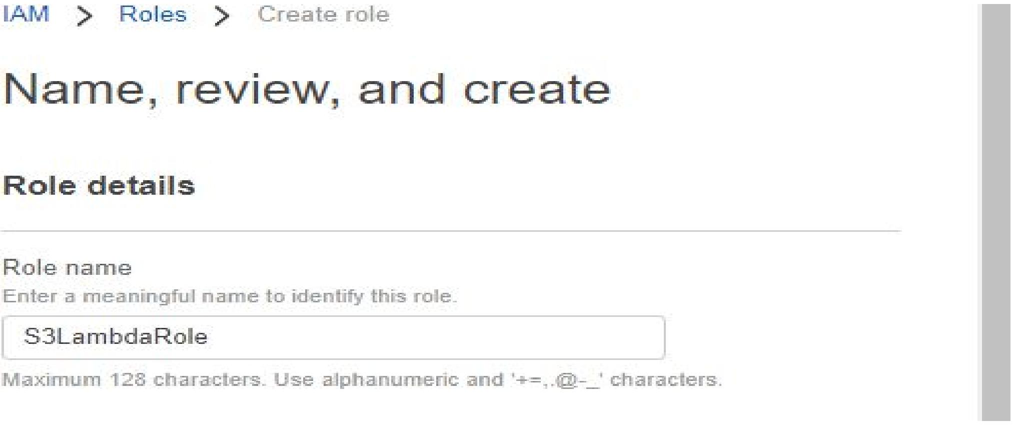
Choose a service to view use case



:dsh…	AWS m…	Provides access to manage S3 settings…
:Listl…	AWS m…	Allow QuickSight to list IAM entities
Access	AWS m…	Allows full access to the AWS Health A…
ssG…	AWS m…	Provide gateway execution access to Al…
Tran…	AWS m…	Grants users read-only access to Elasti…
llAc…	AWS m…	Provides full access to Amazon RDS vi…
	AWS m…	This policy grants permissions to troubl…
lAcc…	AWS m…	Provides full access to Amazon EC2 vi…
rRe…	AWS m…	Provides read/write access to AWS Sec…
Regi…	AWS m…	This policy allows users to register thin…
Rea…	AWS m…	Provides read-only access to Amazon …
Full…	AWS m…	Provides full access to AmazonMQ via …
Medi…	AWS m…	Provides read-only permissions for Me…
Man…	AWS m…	Provides read only access to AWS Cert…

Set permissions boundary - *optional*

Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.



Name, review, and create

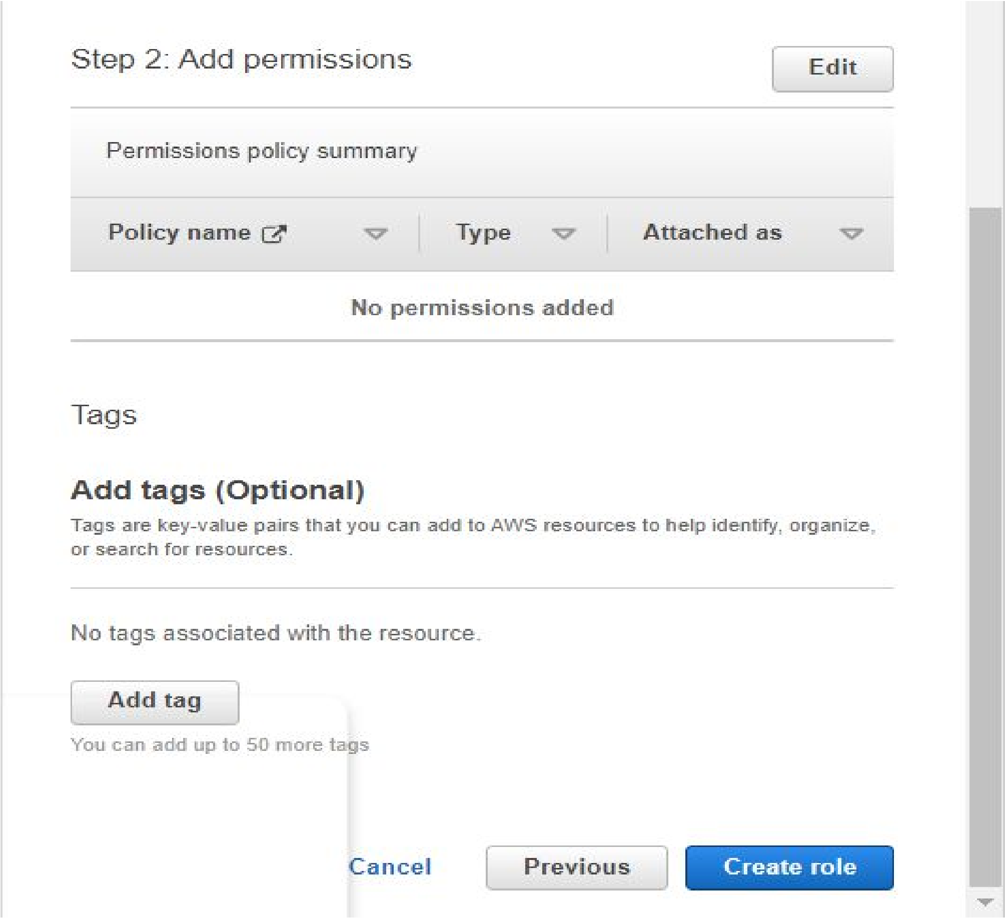
Role details

Role name

Enter a meaningful name to identify this role.

S3LambdaRole

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



Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
No permissions added		

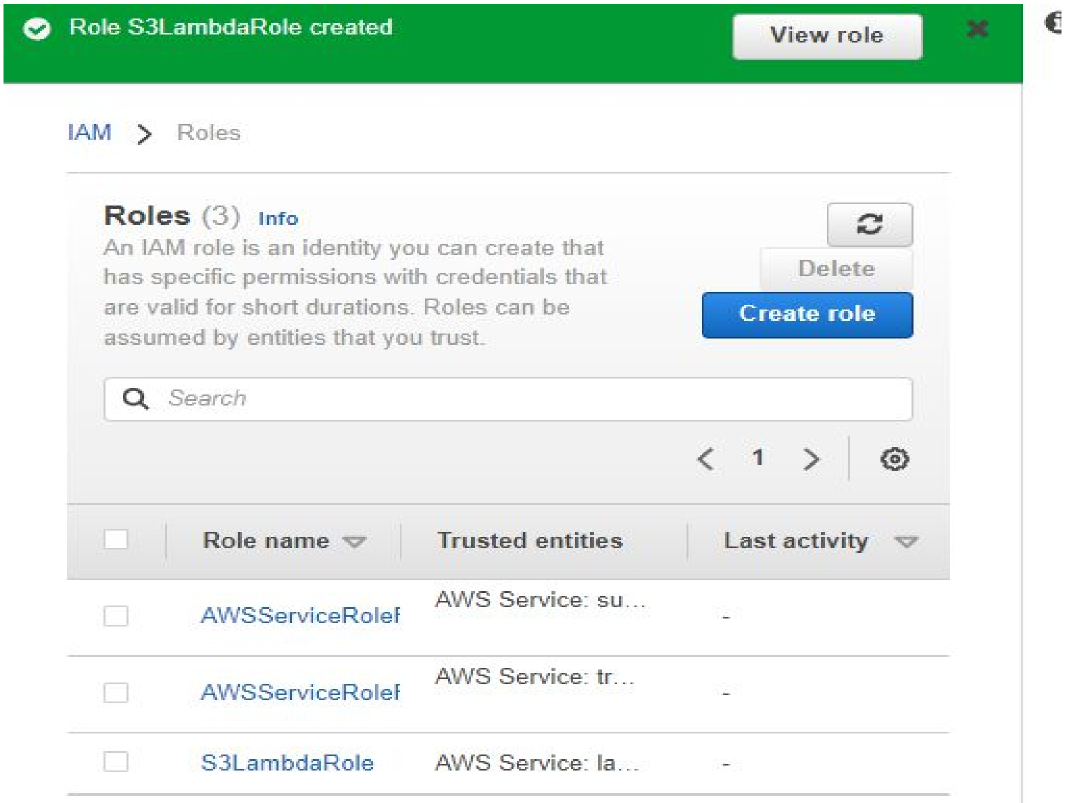
Tags

Add tags (Optional)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

You can add up to 50 more tags

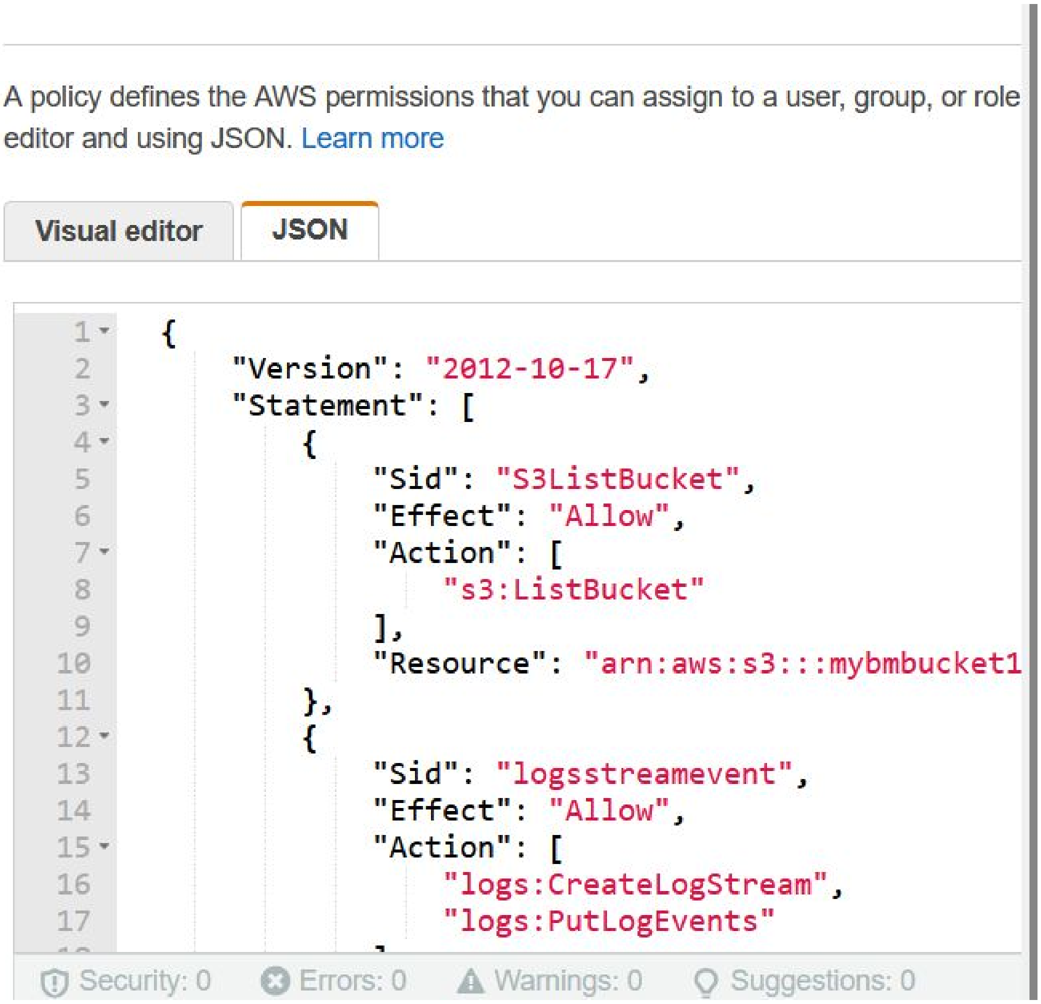


Role S3LambdaRole created

Roles (3)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

□	Role name	Trusted entities	Last activity
□	AWSServiceRoleF	AWS Service: su…	-
□	AWSServiceRoleF	AWS Service: tr…	-
□	S3LambdaRole	AWS Service: la…	-



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

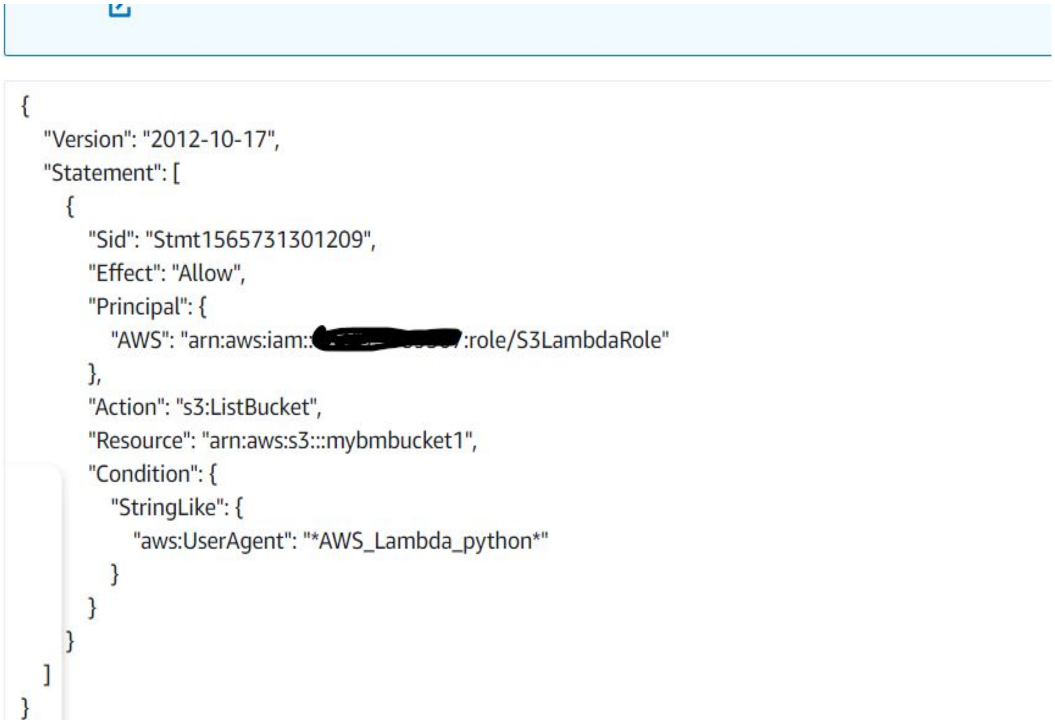
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3ListBucket",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::mybmbucket1
        },
        {
            "Sid": "logsstreamevent",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
```

Create S3 bucket policy in account 2

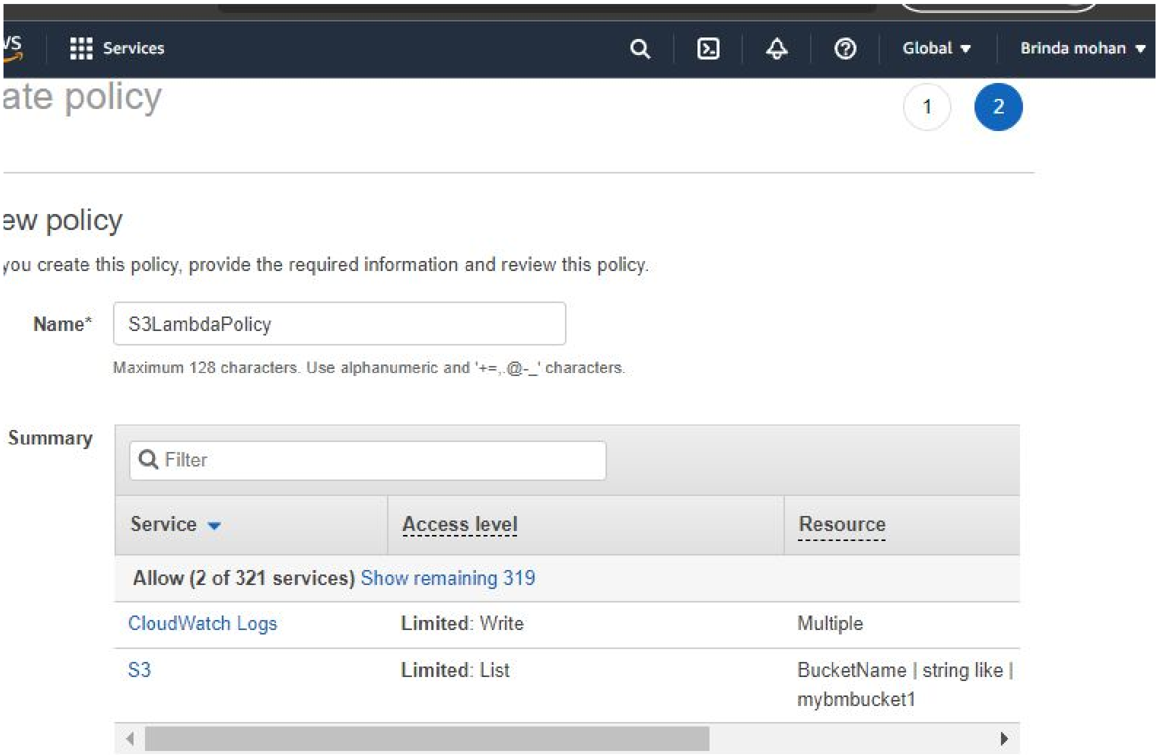
Sign in to the S3 Management Console as an IAM user or role in your AWS account, and open the S3 console at https://console.aws.amazon.com/s3 for account 2

Enter the following JSON policy, in the permissions tab of the Bucket policy.

- Replace account1 with the AWS Account number account 1
- Replace bucketname with the S3 bucket name from account 2



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1565731301209",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::[redacted]:role/S3LambdaRole"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::mybmbucket1",
      "Condition": {
        "StringLike": {
          "aws:UserAgent": "*AWS_Lambda_python*"
        }
      }
    }
  ]
}
```



ate policy

ew policy

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

Name* S3LambdaPolicy

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

Summary

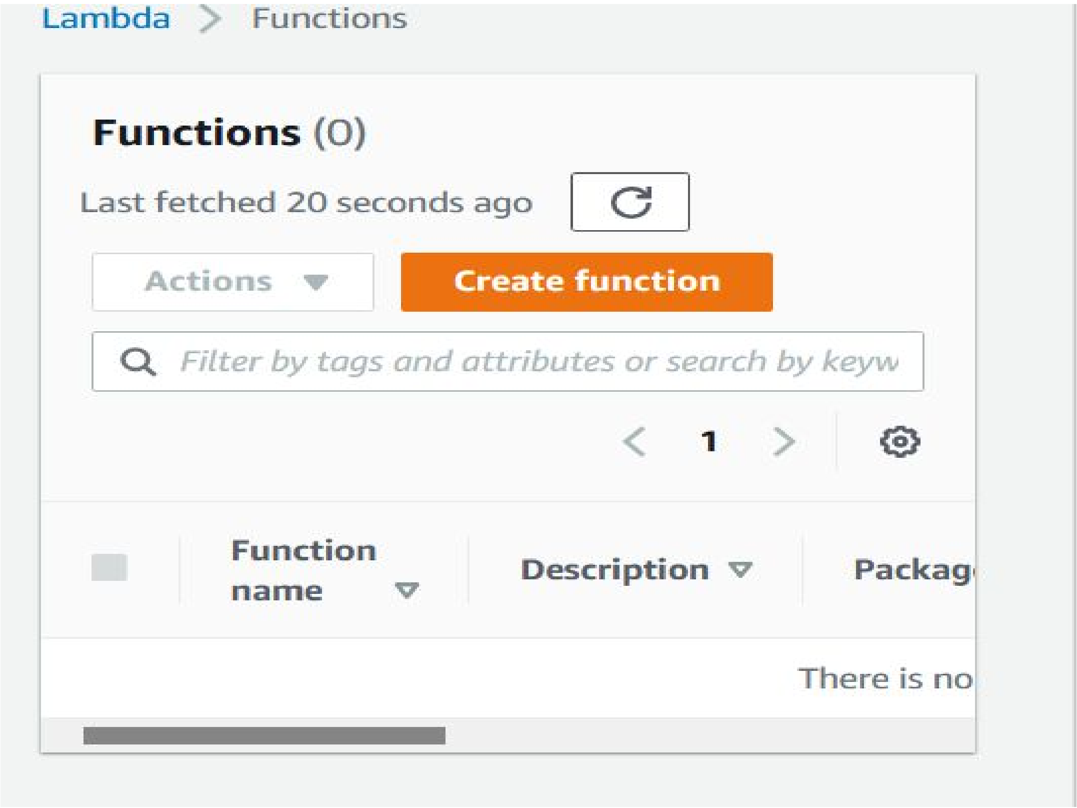
Service	Access level	Resource
Allow (2 of 321 services) Show remaining 319		
CloudWatch Logs	Limited: Write	Multiple
S3	Limited: List	BucketName | string like | mybmbucket1

Name this policy S3LambdaPolicy, then click Create policy

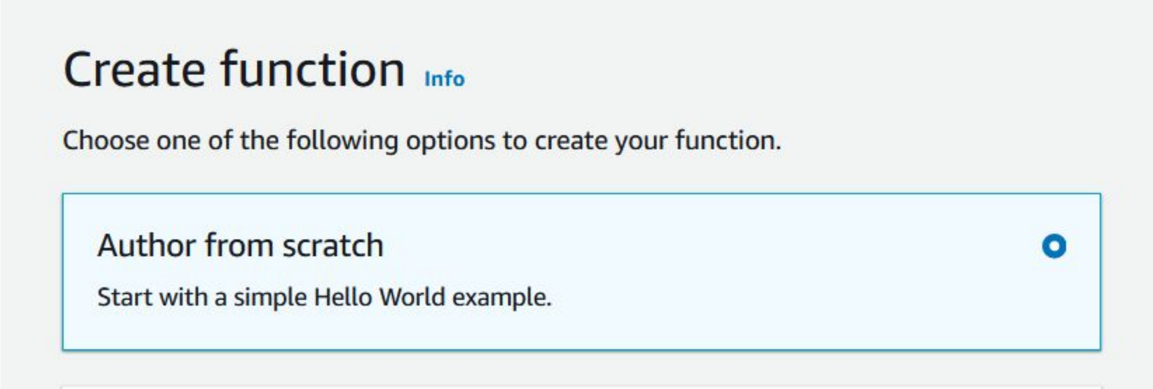
CREATE LAMBDA IN ACCOUNT 1

Open the Lambda console https://console.aws.amazon.com/lambda

Click Create a function



- Accept the default Author from scratch
- Enter function name as S3Lambda
- Select Python 3.7 runtime
- Expand Permissions, click Use an existing role, then select the S3LambdaRole
- Click Create function
- Replace the example function code with the following
- Replace bucketname with the S3 bucket name from account 2
- Click Save.
- Click Test, accept the default event template, enter an event name for the test, then click Create
- Click Test again, and in a few seconds the function output should highlight green and you can expand the detail to see the response from the S3 API

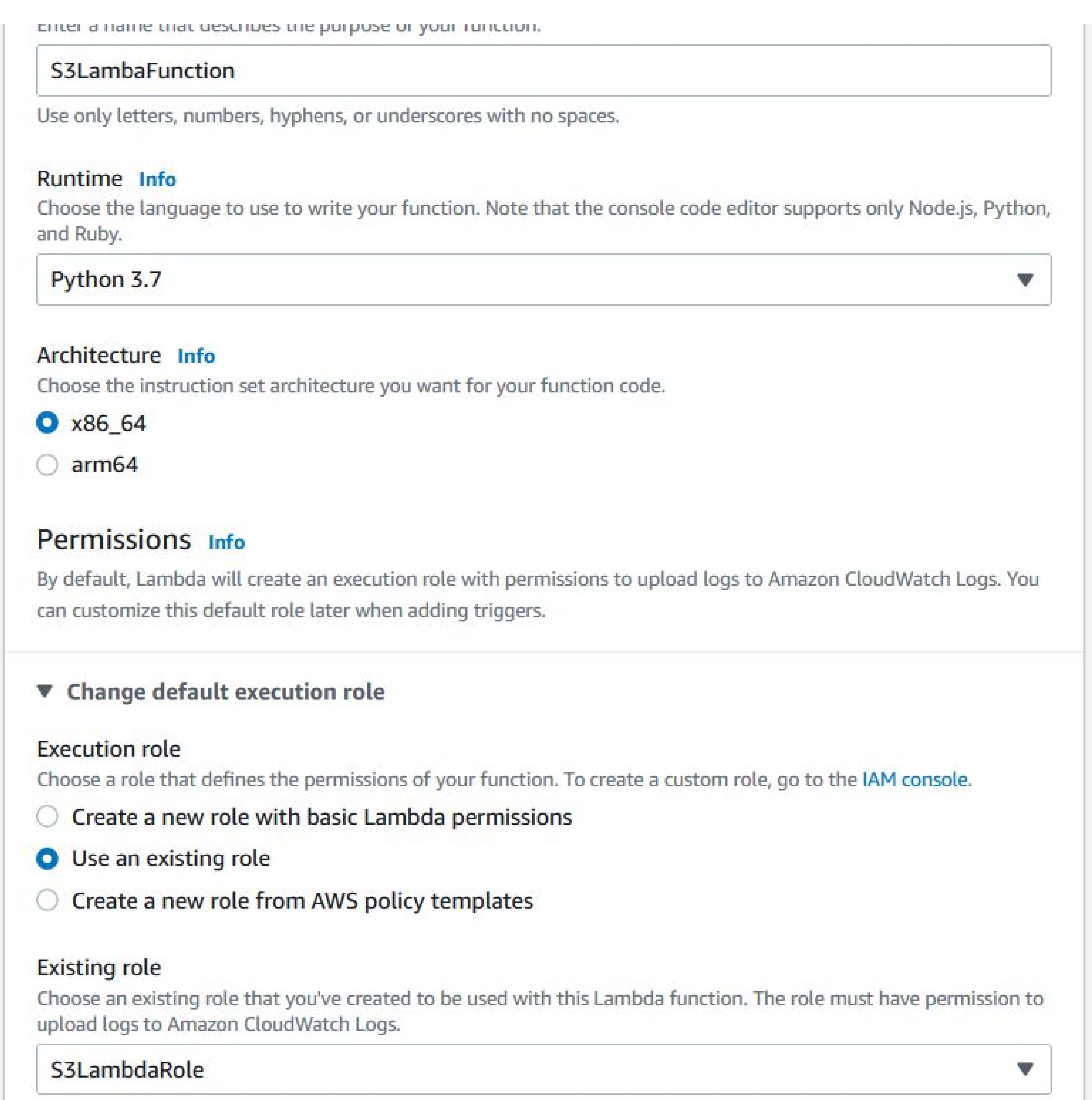


Create function

Choose one of the following options to create your function.

Author from scratch ●

Start with a simple Hello World example.



Enter a name that describes the purpose of your function.

S3LambaFunction

Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime

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

Python 3.7 ▼

Architecture

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

● x86_64

○ arm64

Permissions

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

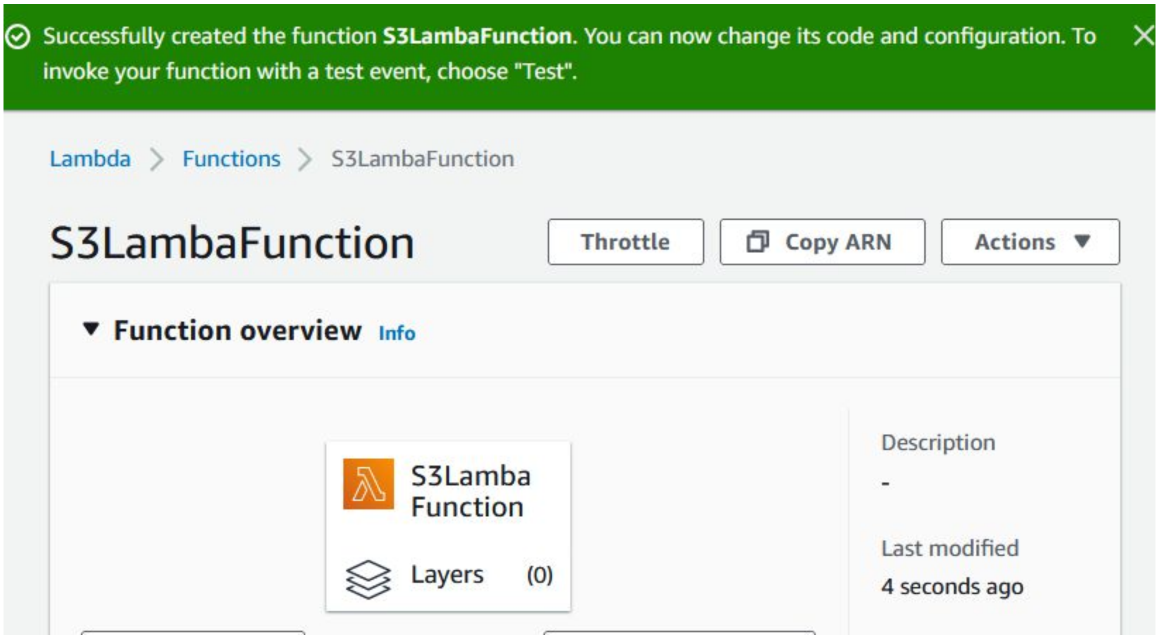
● Use an existing role

○ 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.

S3LambdaRole ▼



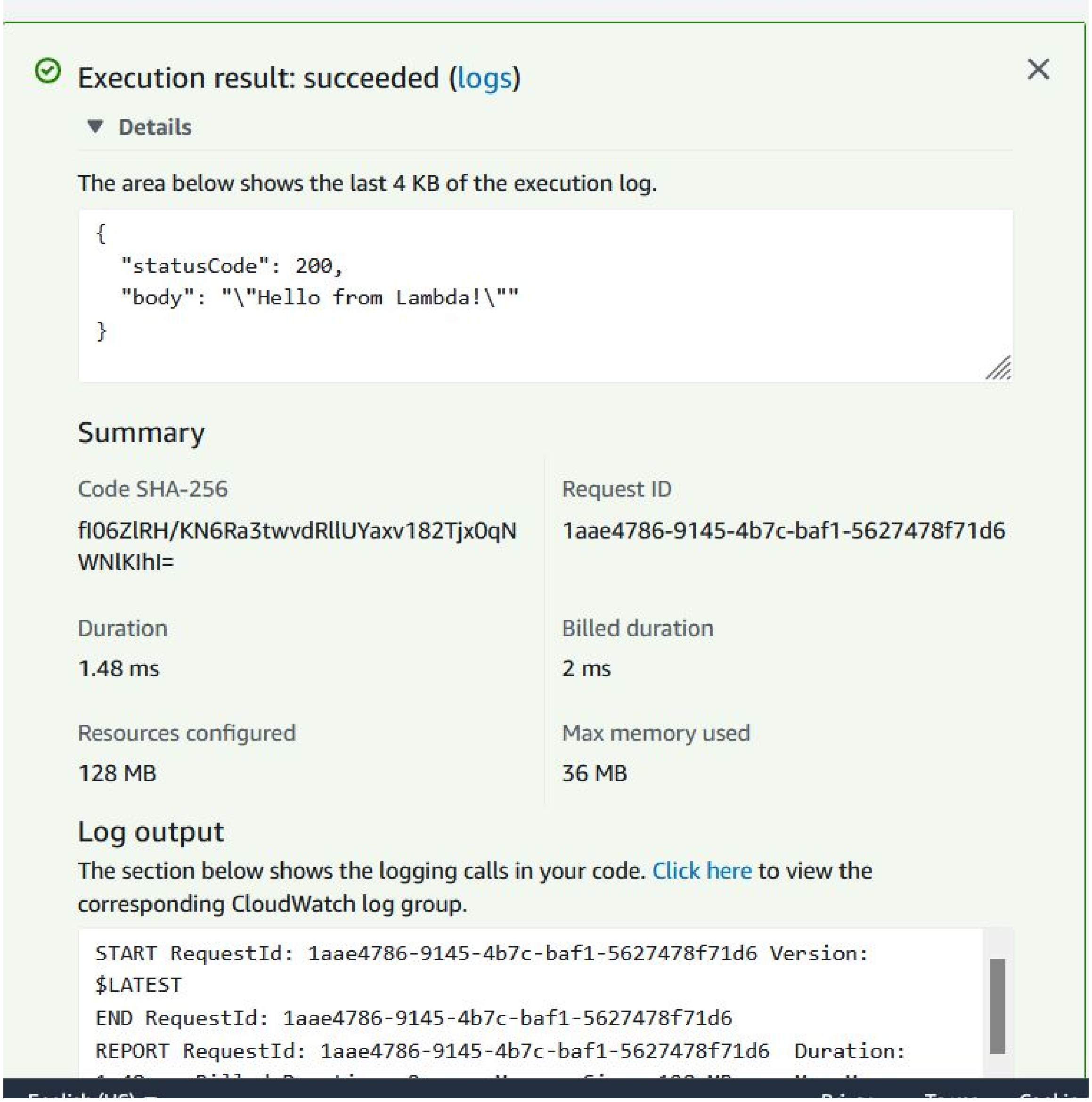
Successfully created the function **S3LambaFunction**. You can now change its code and configuration. To invoke your function with a test event, choose "Test".

Lambda > Functions > S3LambaFunction

S3LambaFunction

Description
-

Last modified
4 seconds ago



Execution result: succeeded (logs)

▼ Details

The area below shows the last 4 KB of the execution log.

```
{
  "statusCode": 200,
  "body": "\"Hello from Lambda!\""
}
```

Summary

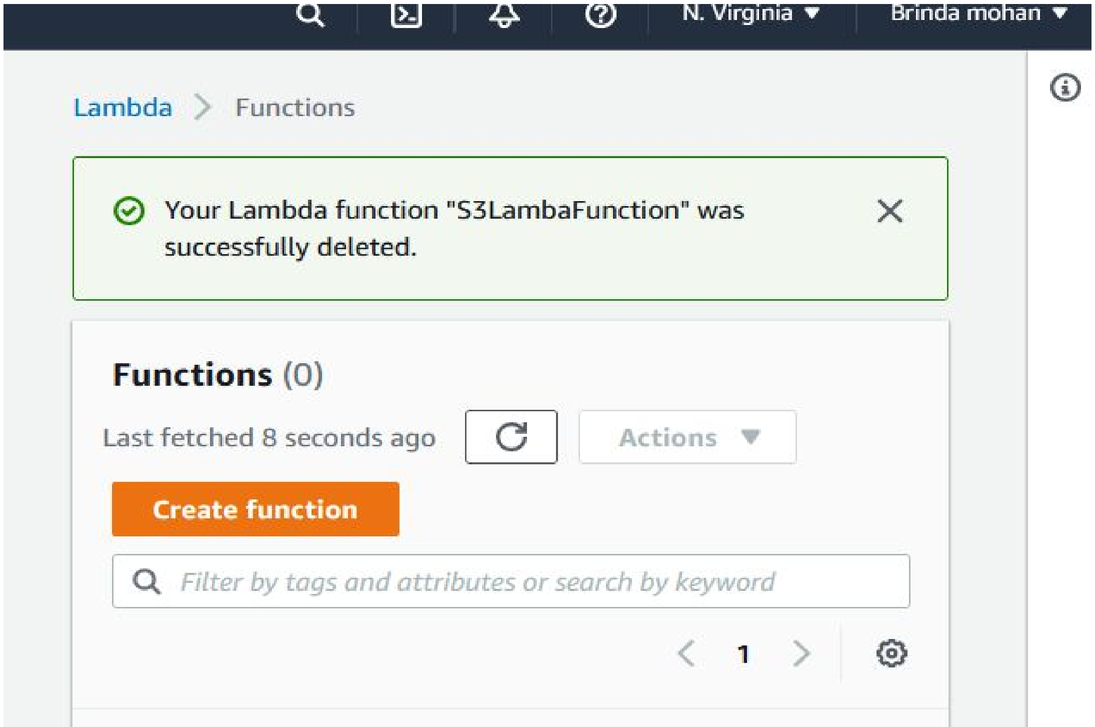
Code SHA-256	Request ID
fI06ZlRH/KN6Ra3twvdRllUYaxv182Tjx0qNWNlKIhI=	1aae4786-9145-4b7c-baf1-5627478f71d6
Duration	Billed duration
1.48 ms	2 ms
Resources configured	Max memory used
128 MB	36 MB

Log output

The section below shows the logging calls in your code. Click here to view the corresponding CloudWatch log group.

```
START RequestId: 1aae4786-9145-4b7c-baf1-5627478f71d6 Version:
$LATEST
END RequestId: 1aae4786-9145-4b7c-baf1-5627478f71d6
REPORT RequestId: 1aae4786-9145-4b7c-baf1-5627478f71d6  Duration:
```

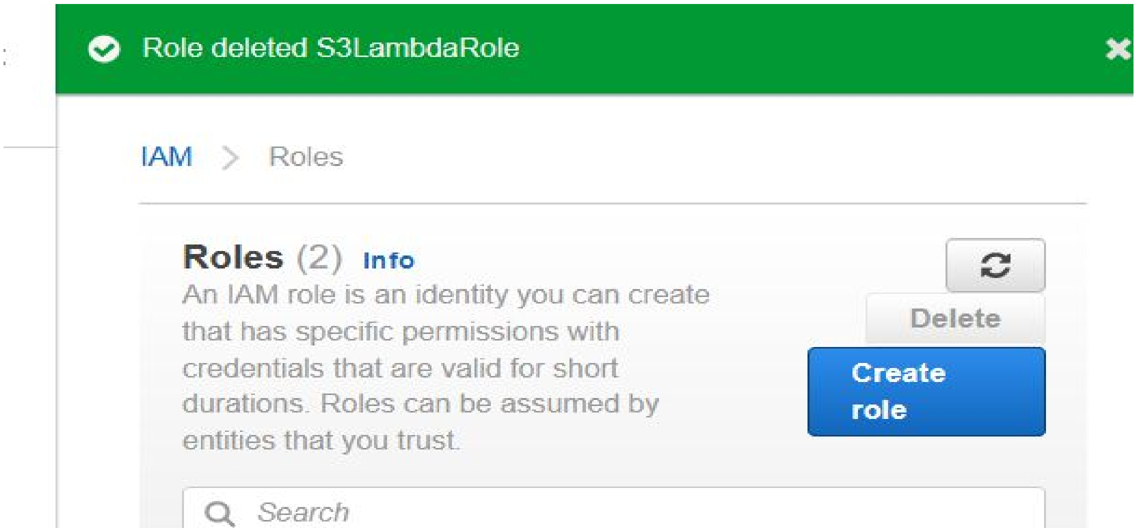
Delete Resources



Your Lambda function "S3LambaFunction" was successfully deleted.

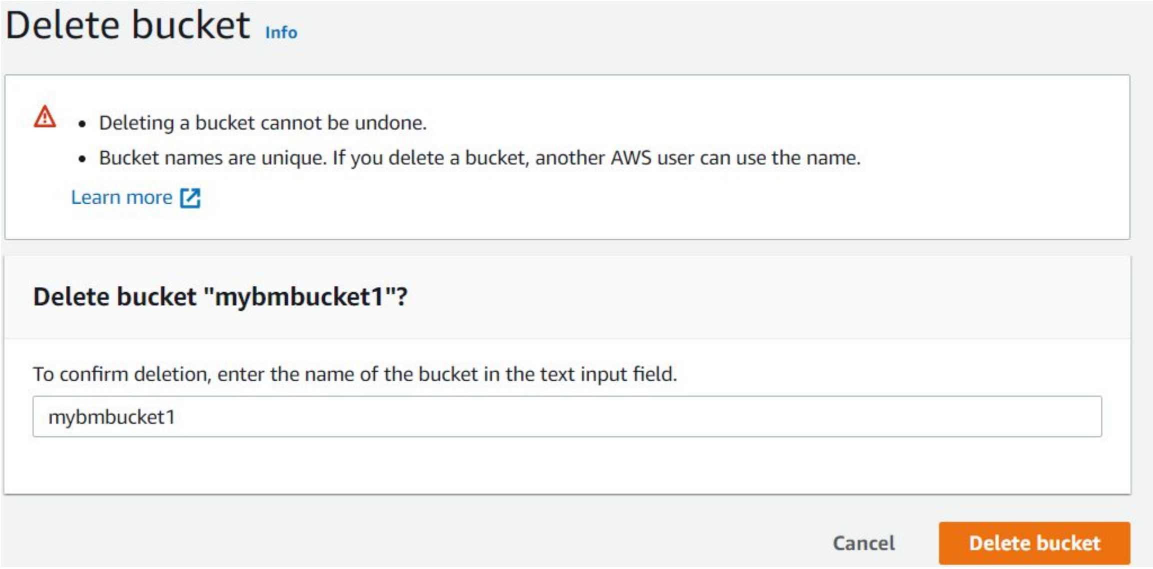
Functions (0)

Last fetched 8 seconds ago


Role deleted S3LambdaRole

Roles (2) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.



Delete bucket Info

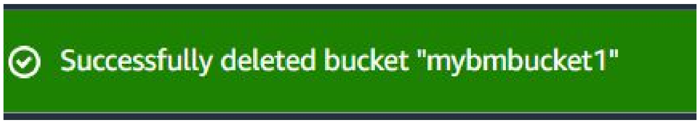
- Deleting a bucket cannot be undone.
- Bucket names are unique. If you delete a bucket, another AWS user can use the name.

Learn more

Delete bucket "mybmbucket1"?

To confirm deletion, enter the name of the bucket in the text input field.

mybmbucket1



Successfully deleted bucket "mybmbucket1"