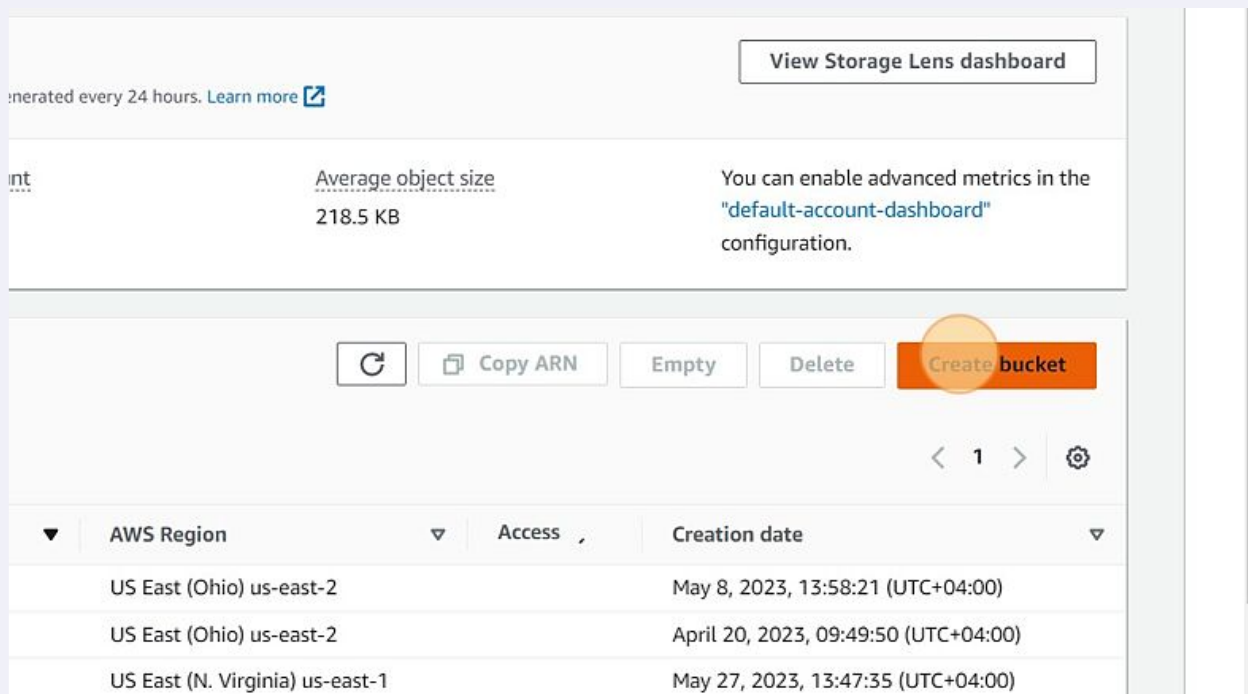


AWS Lambda@Edge Setup - Hands-on

Lambda@Edge Hands On - Created By Lasantha

1 Navigate to S3 console & Click "Create bucket"



The screenshot shows the AWS S3 console interface. At the top right, there is a button labeled "View Storage Lens dashboard". Below this, there is a section with the text "generated every 24 hours. [Learn more](#)". In the center, there is a table with two columns: "Average object size" and "You can enable advanced metrics in the 'default-account-dashboard' configuration." The "Average object size" column shows "218.5 KB". Below this, there is a row of buttons: "Refresh", "Copy ARN", "Empty", "Delete", and "Create bucket". The "Create bucket" button is highlighted with an orange circle. Below the buttons, there is a table with three columns: "AWS Region", "Access", and "Creation date". The table contains three rows of data:

AWS Region	Access	Creation date
US East (Ohio) us-east-2		May 8, 2023, 13:58:21 (UTC+04:00)
US East (Ohio) us-east-2		April 20, 2023, 09:49:50 (UTC+04:00)
US East (N. Virginia) us-east-1		May 27, 2023, 13:47:35 (UTC+04:00)

- 2 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

Bucket name must be globally 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.

[Choose bucket](#)

- 3 Type "lambda-edge-function-9671"

4 Click "Block all public access"

Object Ownership

Bucket owner enforced

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that you applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)


☒ **Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☒ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resource using ACLs.
- ☒ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- ☒ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

5 Click this checkbox.

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

 **Turning off block all public access might result in this bucket and the objects within becoming public**
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

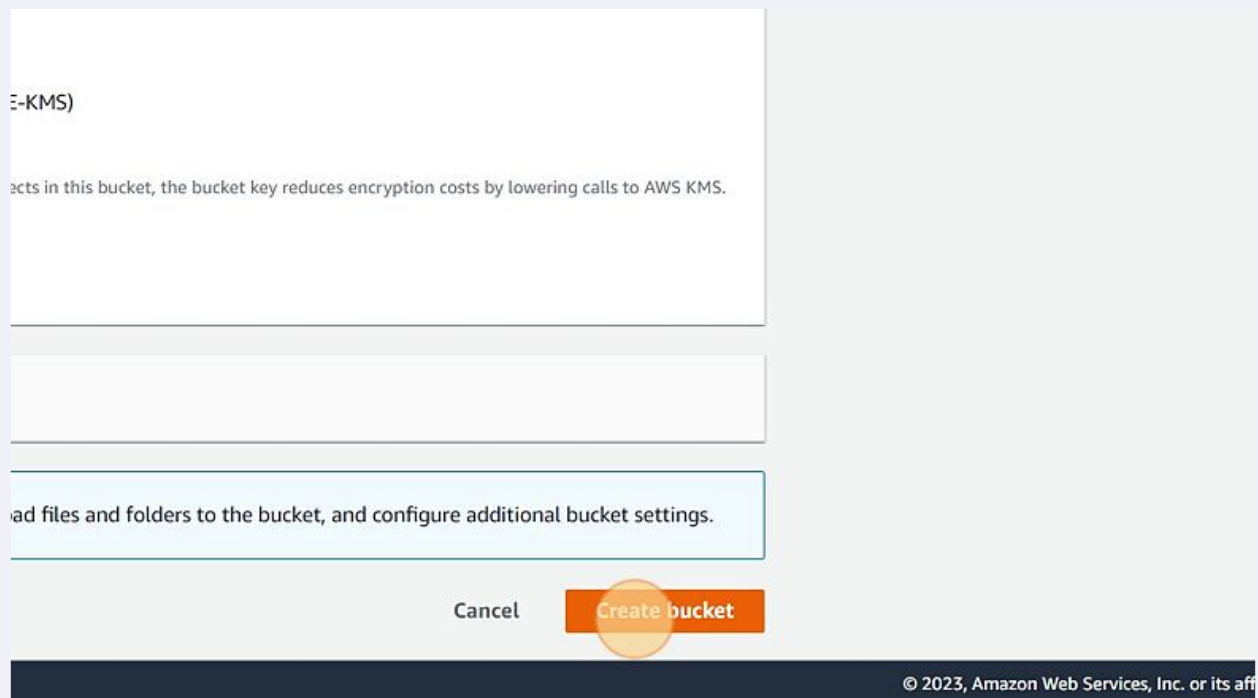
☐ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Bucket Versioning

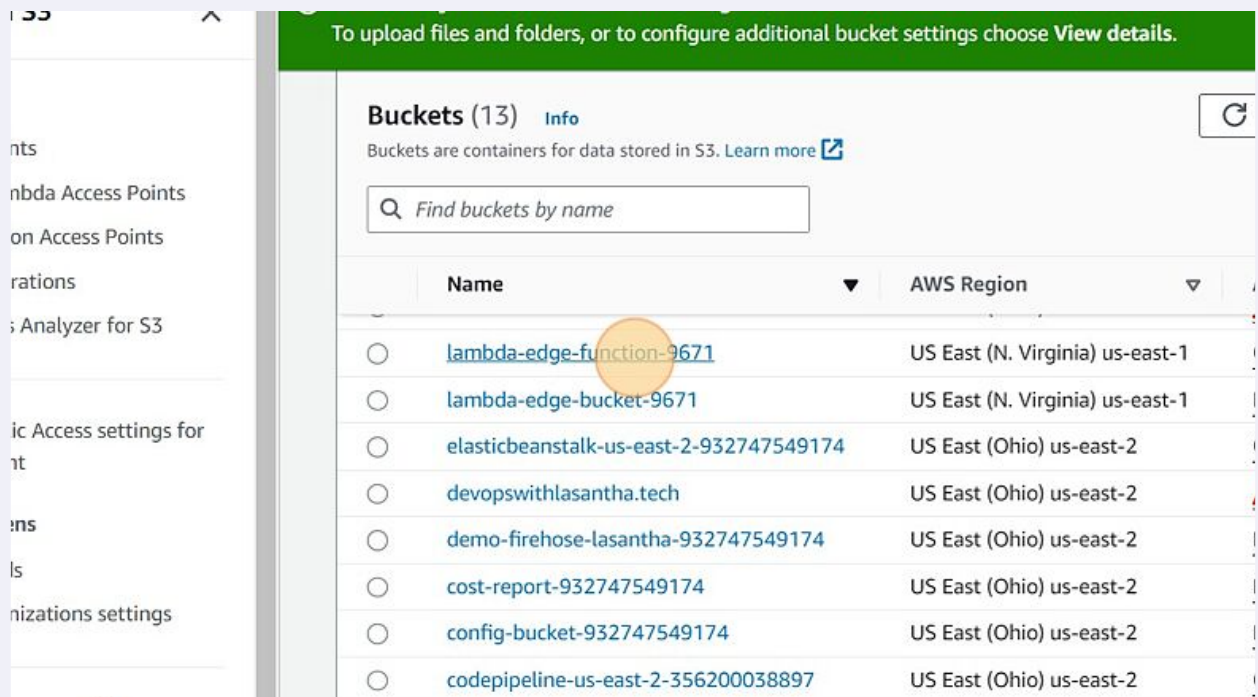
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures.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

CloudShell Feedback Language

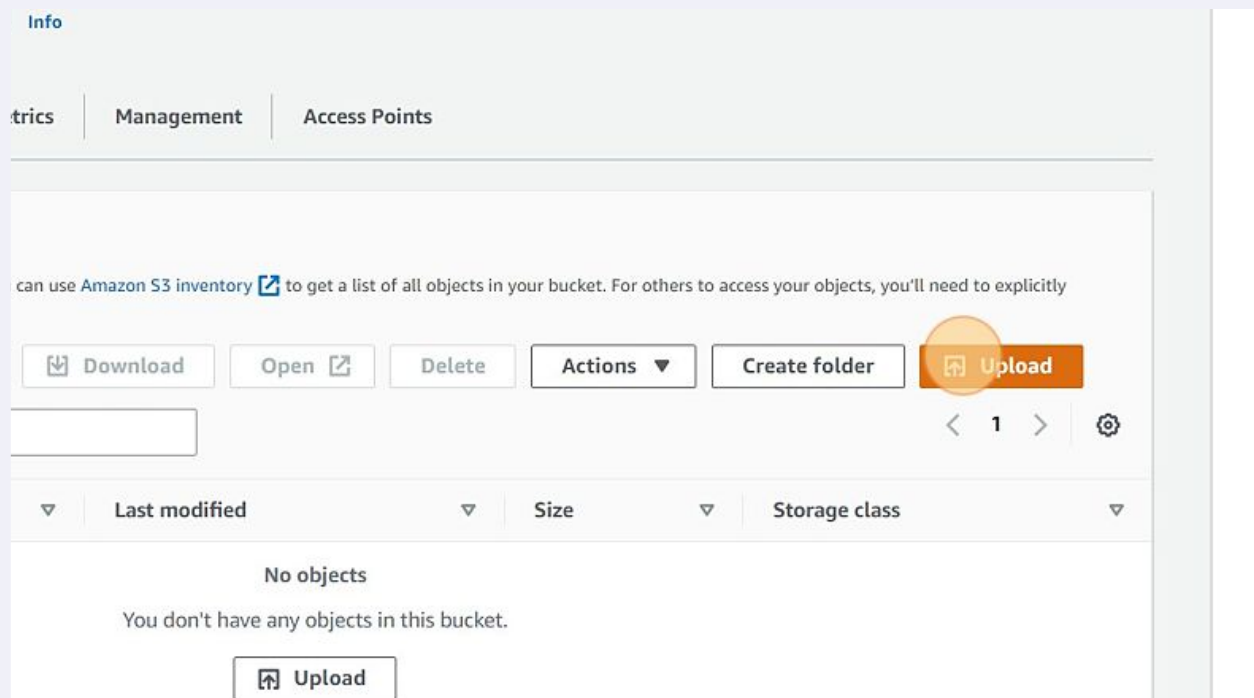
6 Click "Create bucket"



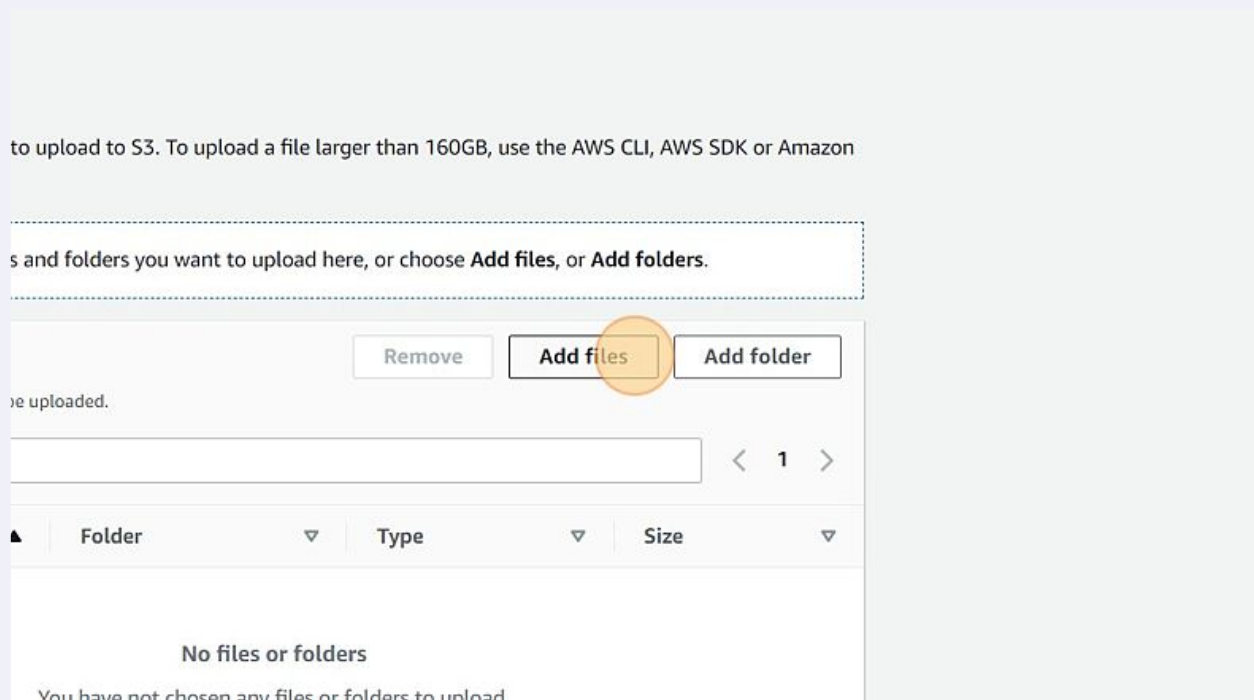
7 Click "lambda-edge-function-9671"



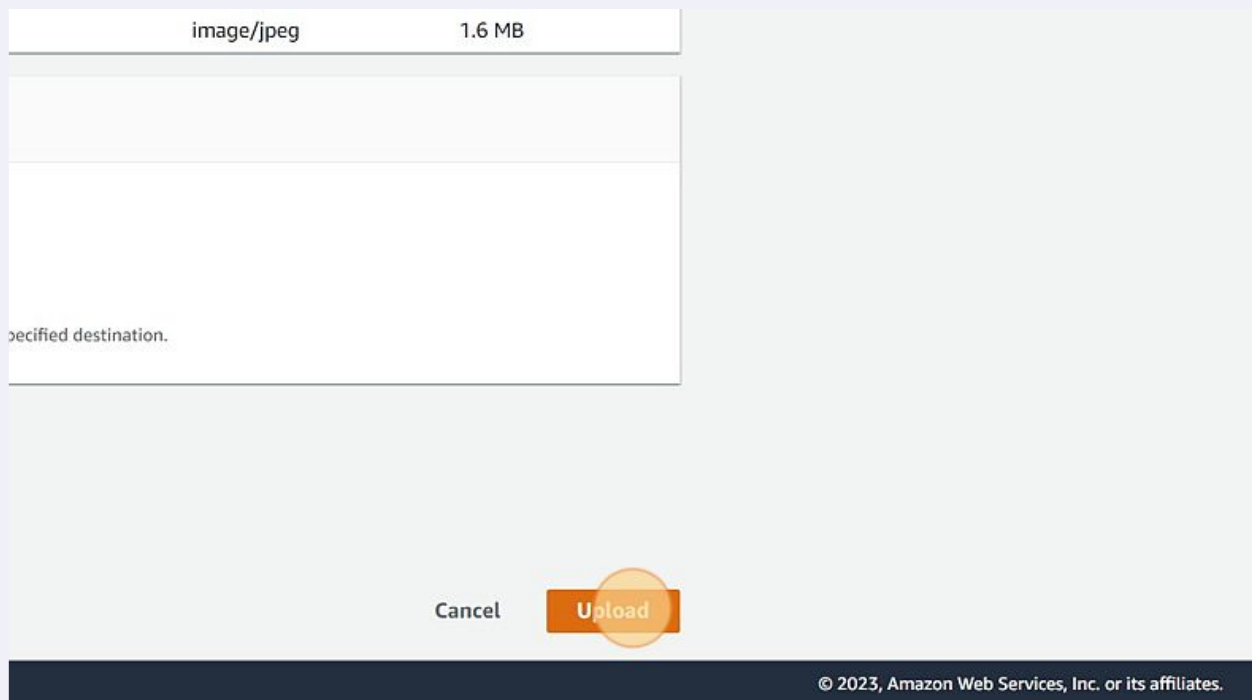
8 Click here.



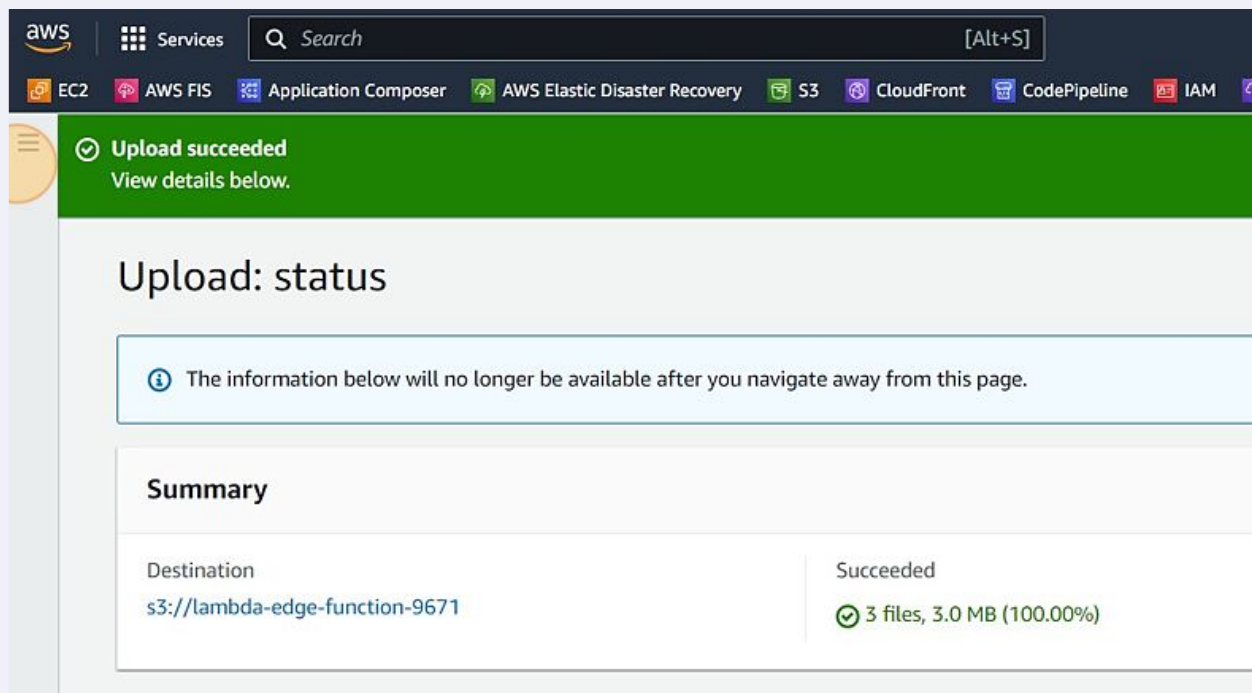
9 Click "Add files"



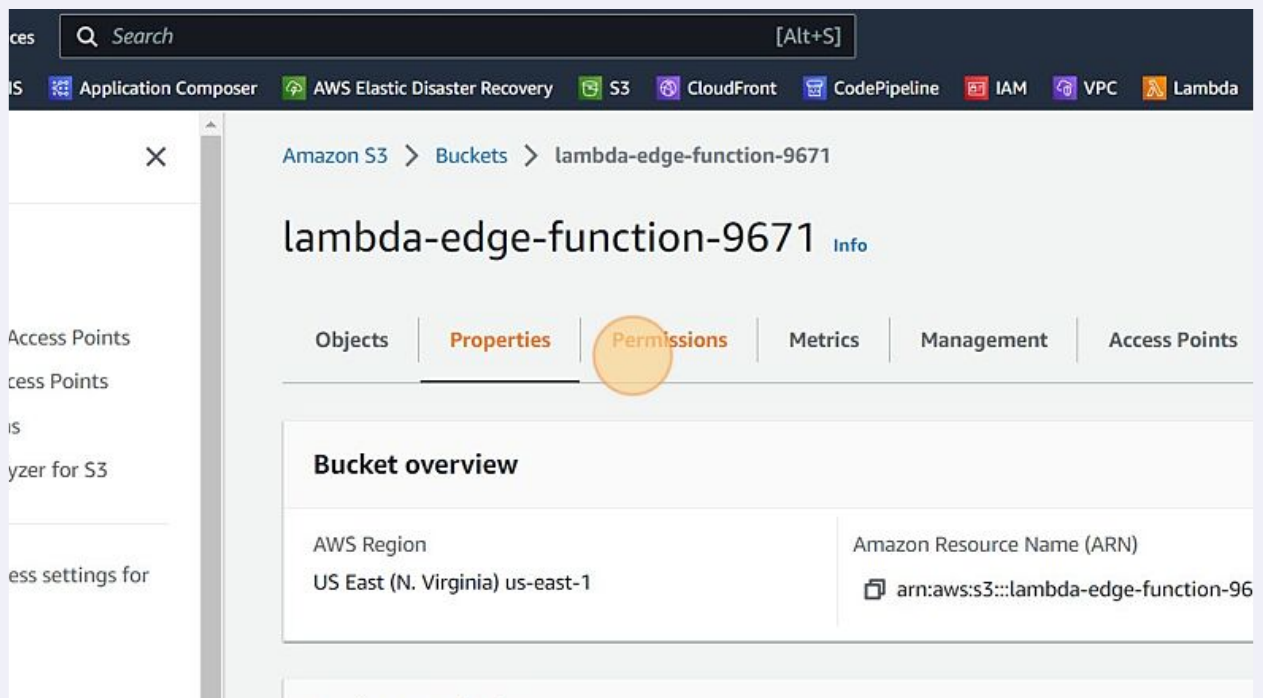
10 Click "Upload"



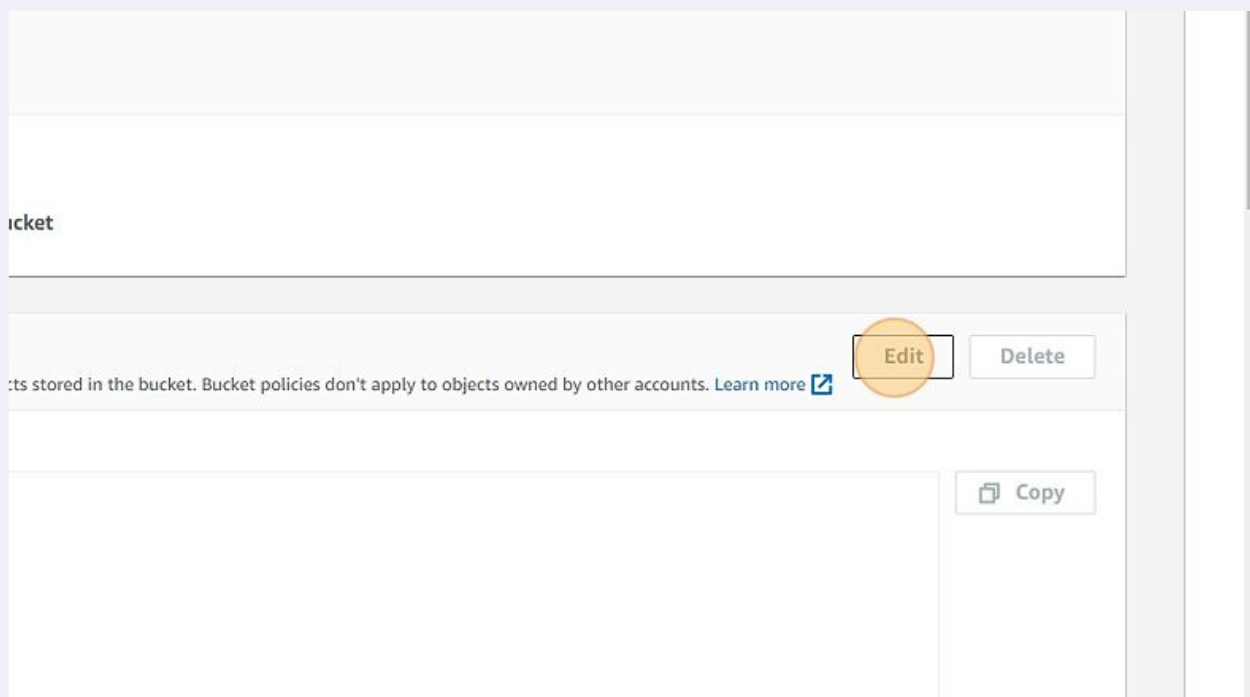
11 Click here.



12 Click "Permissions"



13 Click "Edit"



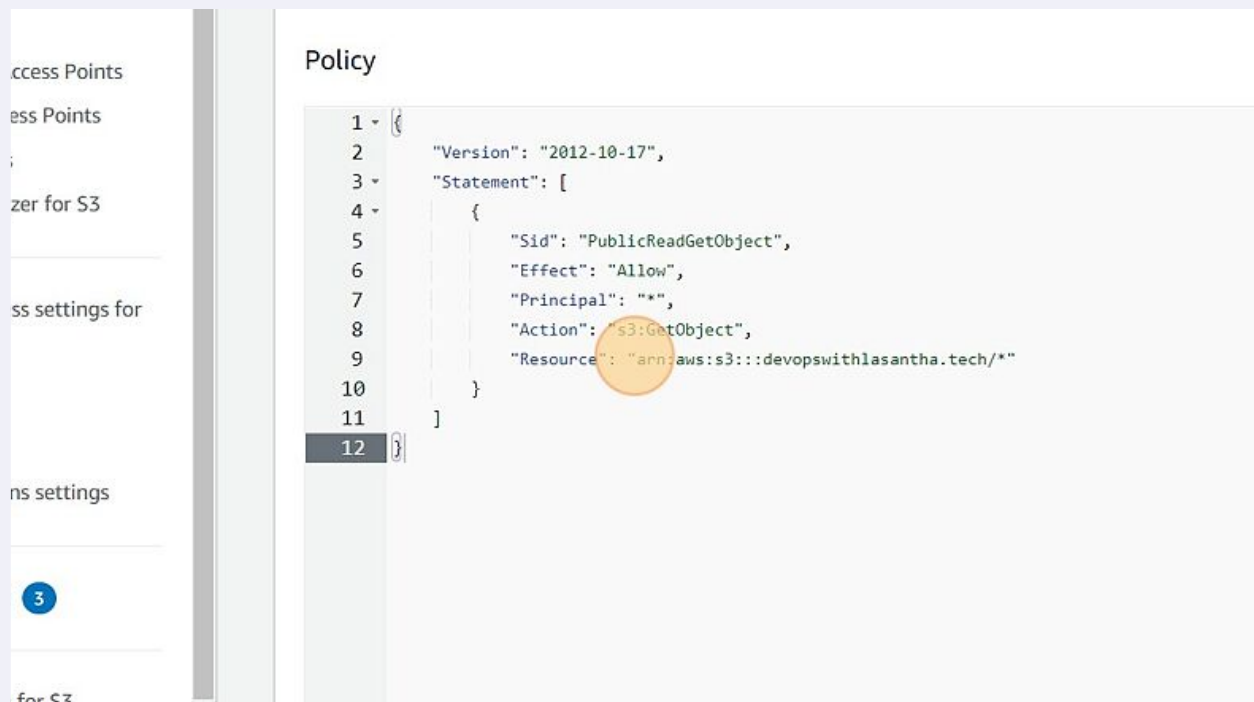
14 Right-click here.

The screenshot shows the AWS IAM console interface. On the left, there is a navigation menu with options like 'Multi-Region Access Points', 'Batch Operations', 'IAM Access Analyzer for S3', 'Storage Lens', and 'Feature spotlight'. The main content area is titled 'Bucket policy' and includes a description: 'The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket'. Below this, there are two buttons: 'Policy examples' and 'Policy generator'. A red circle is drawn around the 'Policy generator' button. The 'Bucket ARN' field shows 'arn:aws:s3:::lambda-edge-function-9671'. The 'Policy' section is currently empty, with a red circle highlighting the '1' in the list index.

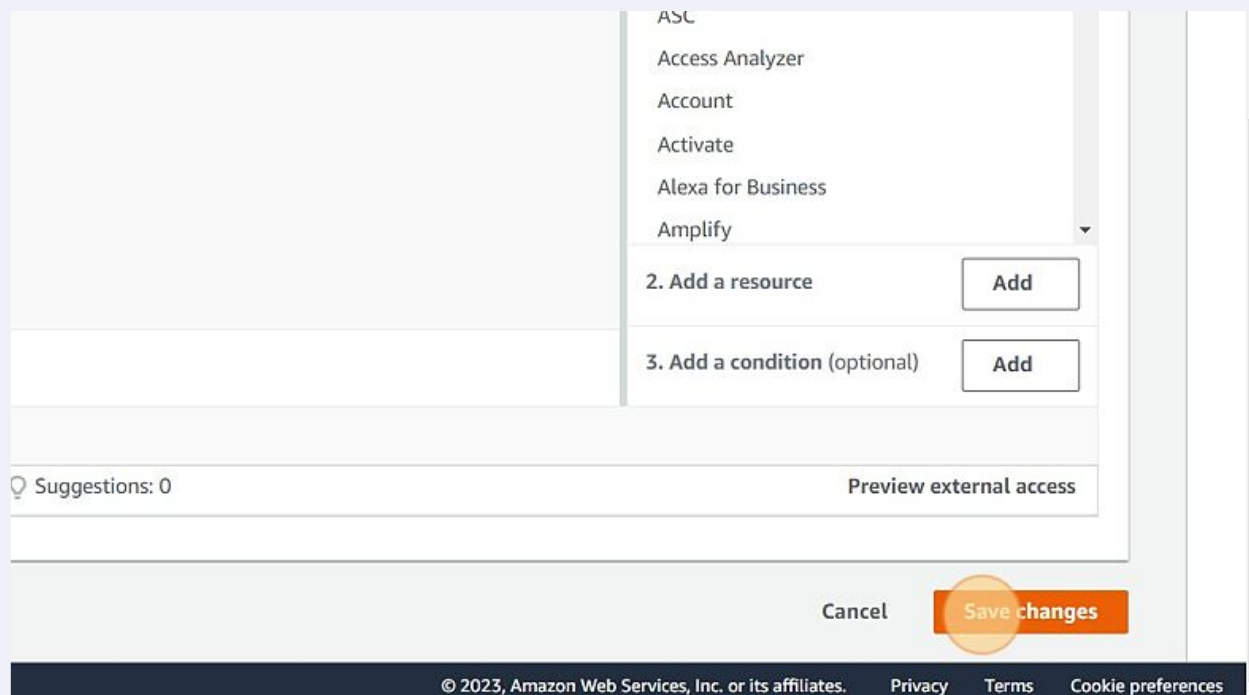
15 Click here.

The screenshot shows the AWS IAM console interface. On the left, there is a navigation menu with options like 'Buckets', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', 'IAM Access Analyzer for S3', 'Storage Lens', and 'Feature spotlight'. The main content area is titled 'Edit bucket policy' and includes a description: 'The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket'. Below this, there are two buttons: 'Policy examples' and 'Policy generator'. A red circle is drawn around the 'Policy generator' button. The 'Bucket ARN' field shows 'arn:aws:s3:::lambda-edge-function-9671'. The 'Policy' section is currently empty, with a red circle highlighting the '1' in the list index.

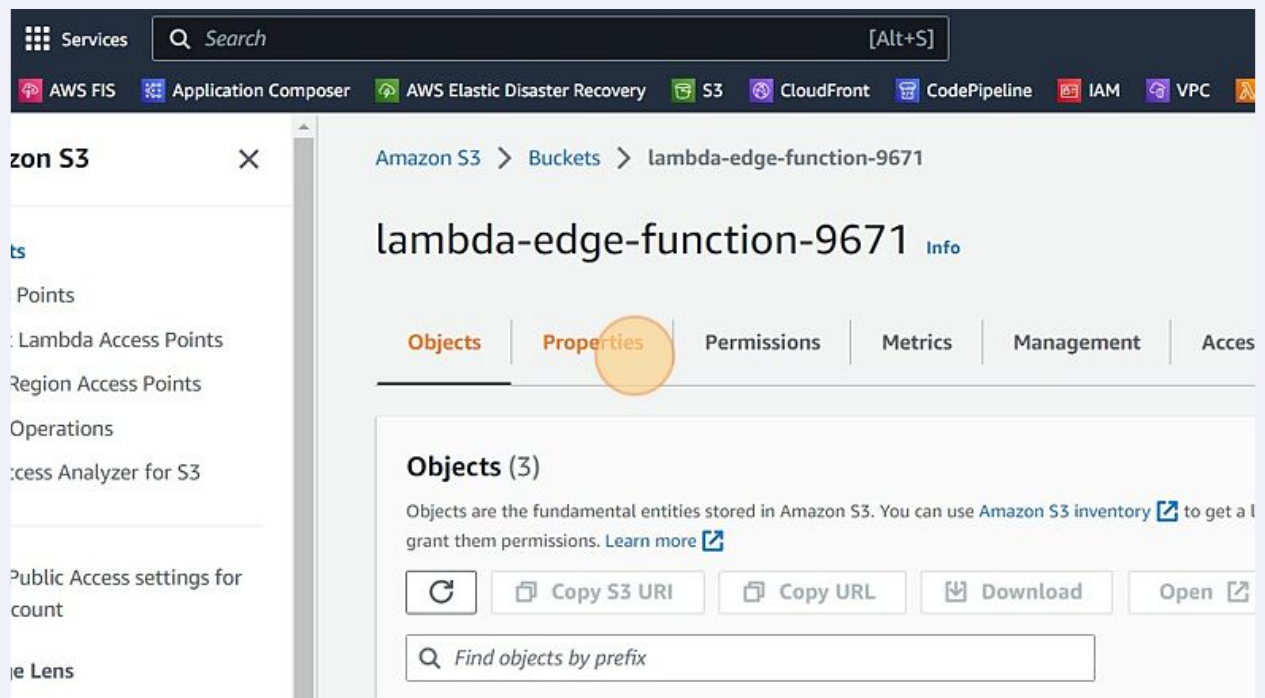
16 Click here.



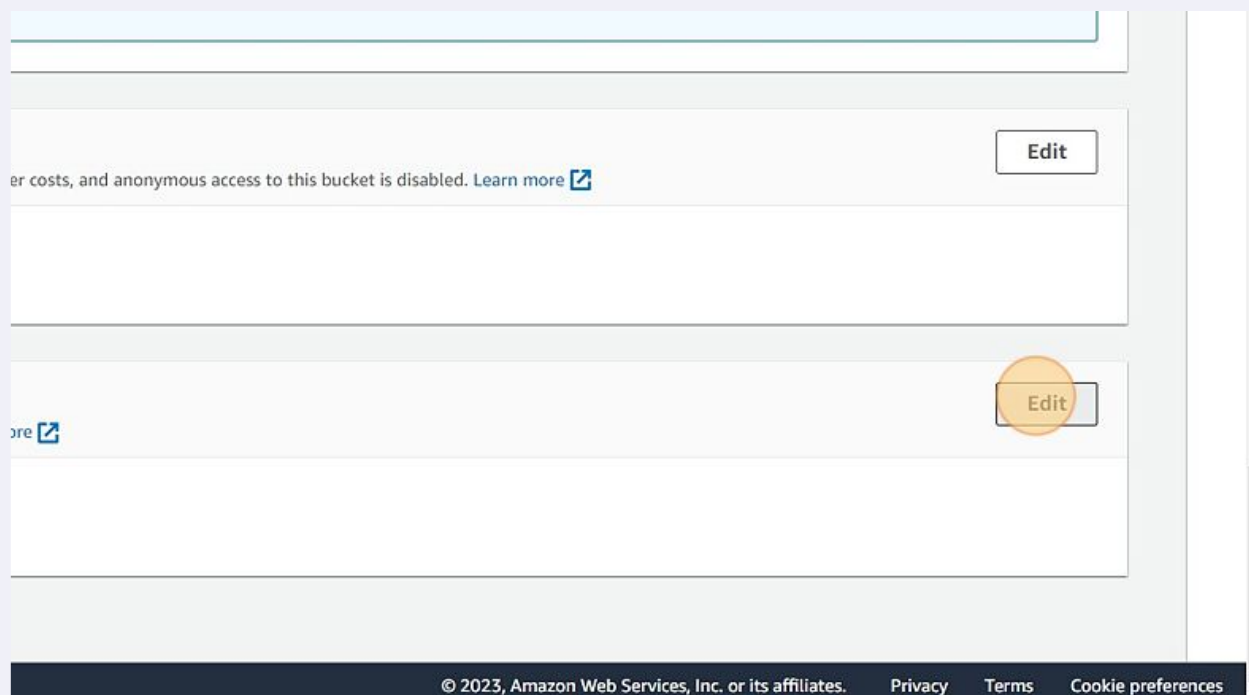
17 Click "Save changes"



18 Click "Properties"



19 Click "Edit"



20 Click "Enable"

Buckets

- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

▼ **Storage Lens**

- Dashboards
- AWS Organizations settings

Feature spotlight 3

Edit static website hosting [Info](#)

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

☒ Disable

☐ Enable

21 Click the "Index document" field.

Use the bucket endpoint as the web address. [Learn more](#)

☐ Redirect requests for an object

Redirect requests to another bucket or domain. [Learn more](#)

For your customers to access content at the website endpoint, you must make the content publicly readable. To do so, you can edit the S3 Block Public Access settings for this bucket. [Using Amazon S3 Block Public Access](#)

Index document

Specify the home or default page of the website.

Error document - optional

This is returned when an error occurs.

Redirection rules - optional

Redirection rules, written in JSON, automatically redirect webpage requests for specific content.

1

CloudShell Feedback Language

22 Type "index.html"

23 Click "Save changes"



Cancel

Save changes

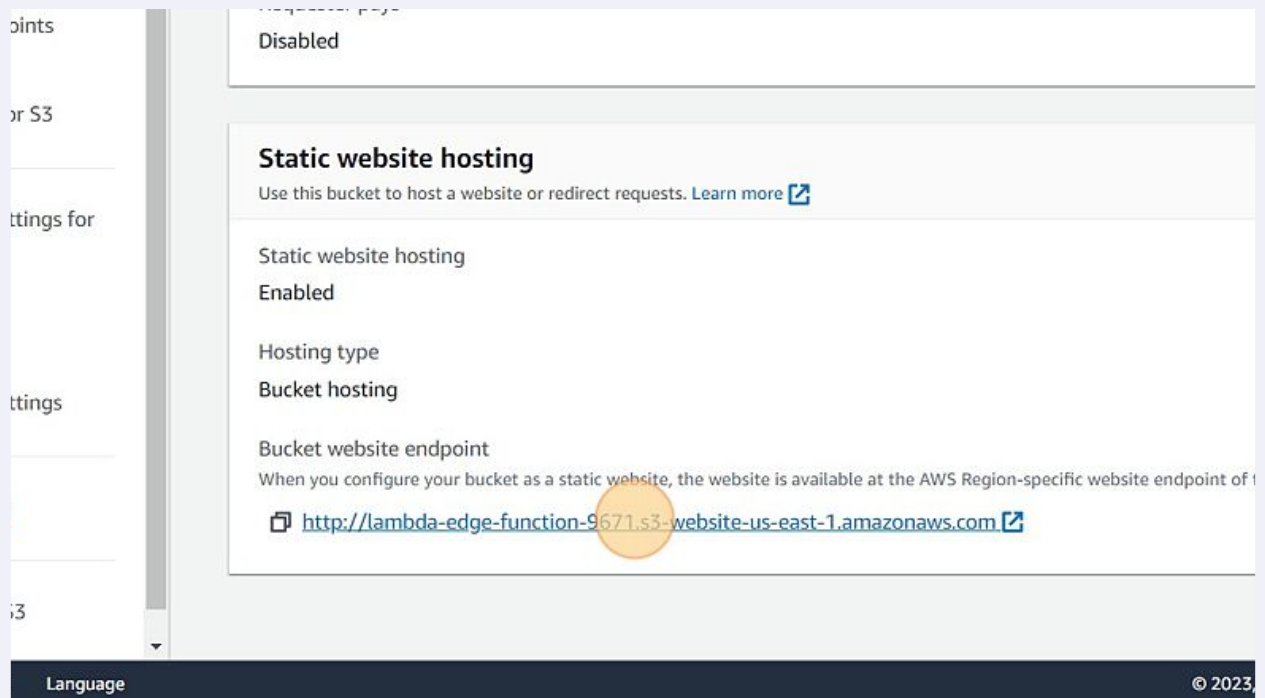
© 2023, Amazon Web Services, Inc. or its affiliates.

[Privacy](#)

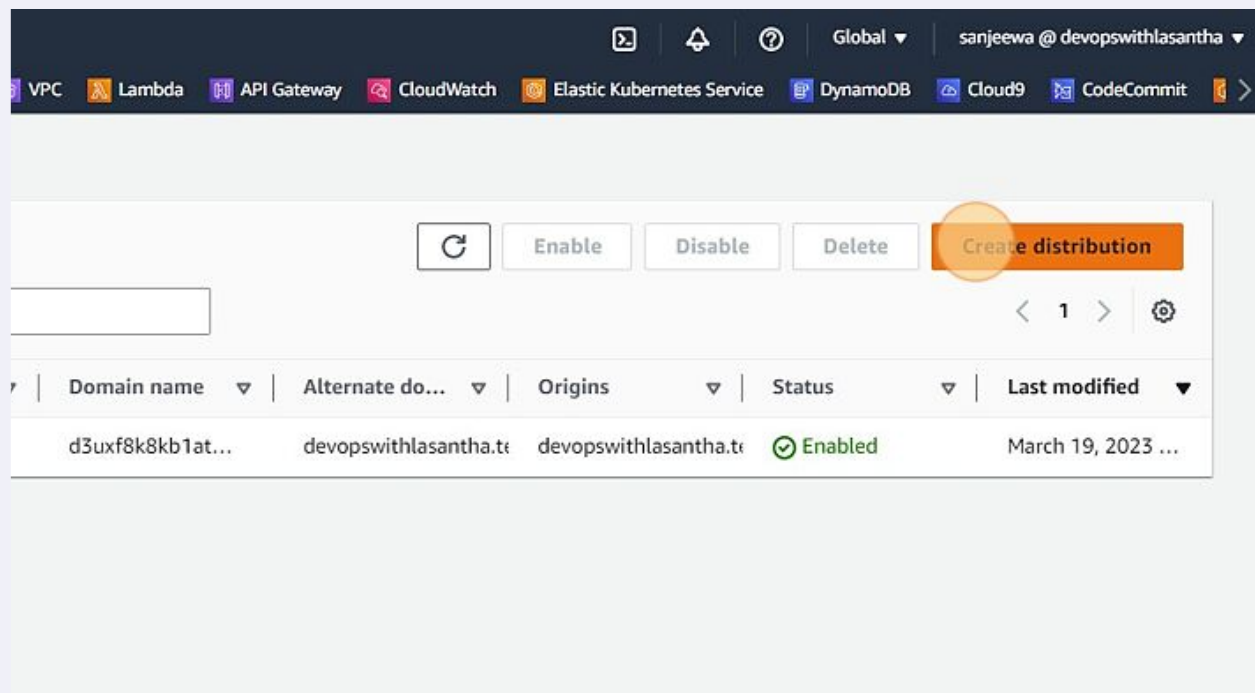
[Terms](#)

[Cookie](#)

24 Click "http://lambda-edge-function-9671.s3-website-us-east-1.amazonaws.com"



25 Navigate to CloudFront Console & Click "Create distribution"



- 26 Click the "Origin domain" field.

CloudFront > Distributions > Create

Create distribution

Origin

Origin domain
Choose an AWS origin, or enter your origin's domain name.

Origin path - optional [Info](#)
Enter a URL path to append to the origin domain name for origin requests.

Name
Enter a name for this origin.

- 27 Click "lambda-edge-function-9671.s3.amazonaws.com"

- codepipeline-us-east-1-410534556051.s3.amazonaws.com
- codepipeline-us-east-2-356200038897.s3.amazonaws.com
- config-bucket-932747549174.s3.amazonaws.com
- cost-report-932747549174.s3.amazonaws.com
- demo-firehose-lasantha-932747549174.s3.amazonaws.com
- devopswithlasantha.tech.s3.amazonaws.com
- elasticbeanstalk-us-east-2-932747549174.s3.amazonaws.com
- lambda-edge-function-9671.s3.amazonaws.com
- lasantha-fileshare-s3-932747549174-v1.s3.amazonaws.com
- s3-storage-lens-analysis-data.s3.amazonaws.com

Elastic Load Balancer

No origins available.

API Gateway

No

CloudShell Feedback Language

28 Click "Use website endpoint"

Origin domain
Choose an AWS origin, or enter your origin's domain name.

Q lambda-edge-function-9671.s3.us-east-1.amazonaws.com X

⚠ This S3 bucket has static web hosting enabled. If you plan to use this distribution as a website, we recommend using the S3 website endpoint rather than the bucket endpoint.

Use website endpoint

Origin path - optional [Info](#)
Enter a URL path to append to the origin domain name for origin requests.

Enter the origin path

Name
Enter a name for this origin.

lambda-edge-function-9671.s3.us-east-1.amazonaws.com

29 Click this radio button.

Services Search [Alt+S]

AWS FIS Application Composer AWS Elastic Disaster Recovery S3 CloudFront CodePipeline IAM VPC

Web Application Firewall (WAF)

☐ Enable security protections
Keep your application secure from the most common web threats and security vulnerabilities using AWS WAF. Blocked requests are stopped before they reach your web servers.

☐ Do not enable security protections
Select this option if your application does not need security protections from AWS WAF.

▼ Included security protections

- Protect against the most common vulnerabilities found in web applications.
- Protect against malicious actors discovering application vulnerabilities.
- Block IP addresses from potential threats based on Amazon internal threat intelligence

AWS recommends these protections for all applications as the first line of defense. You can make adjustments after your distribution is created.

30 Click "Create distribution"

root URL (/) instead of a specific object.

et.

Cancel Create distribution

© 2023, Amazon Web S

31 Click here.

Distributions

- Policies
- Functions
- What's new **NEW**

▼ **Telemetry**

- Monitoring
- Alarms
- Logs



▼ **Reports & analytics**

- Cache statistics
- Popular objects
- Top referrers
- Usage
- Viewers

E2UDTICE3OQHF3

General | Origins | Behaviors | Error pages | Geographic rest

Details

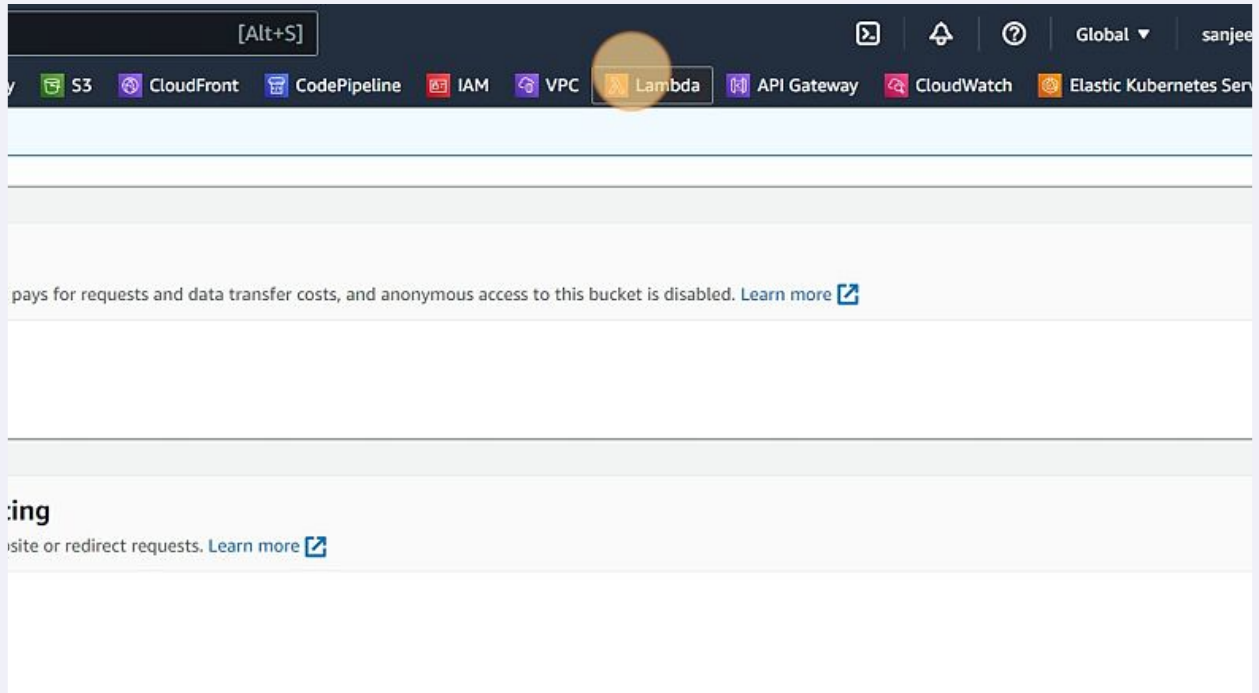
Distribution domain name	ARN
 d1hca5kyvuxcwq.cloudfront.net	 arn:aws:cloudfront:us-east-1:123456789012:distribution/E2UDTICE3OQHF3

Settings

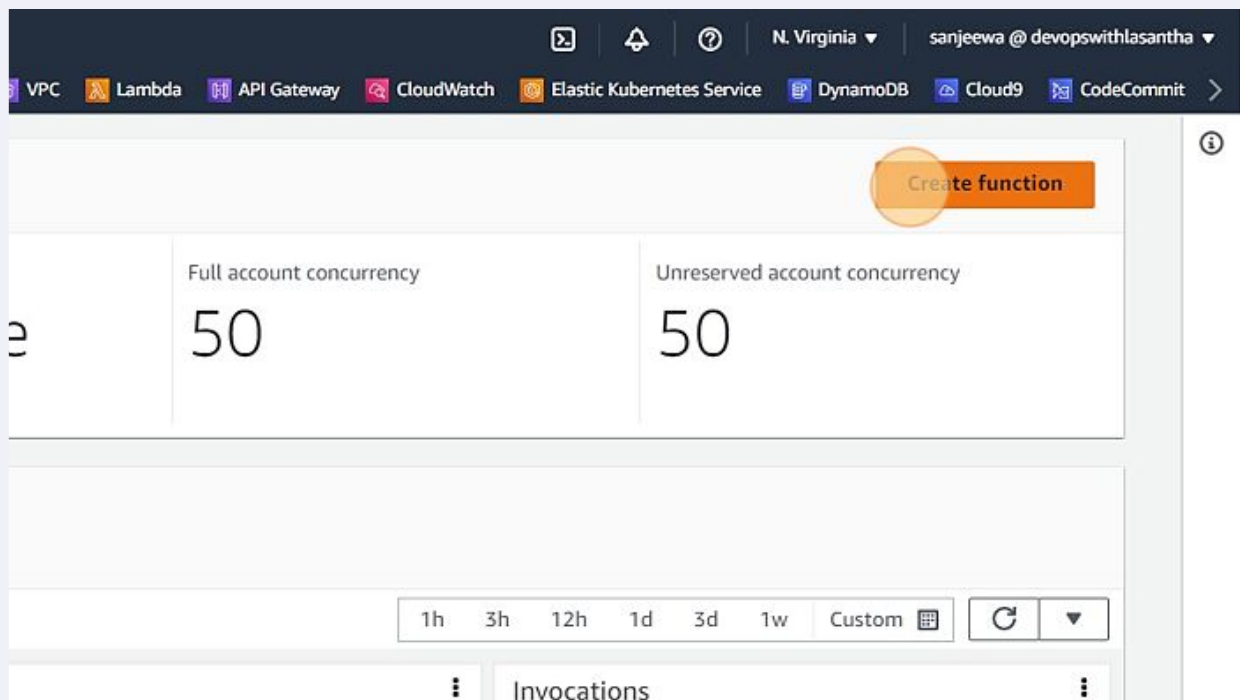
Description	Alternate c
-	-
Price class	

32 Open a new tab in the browser & check the web page

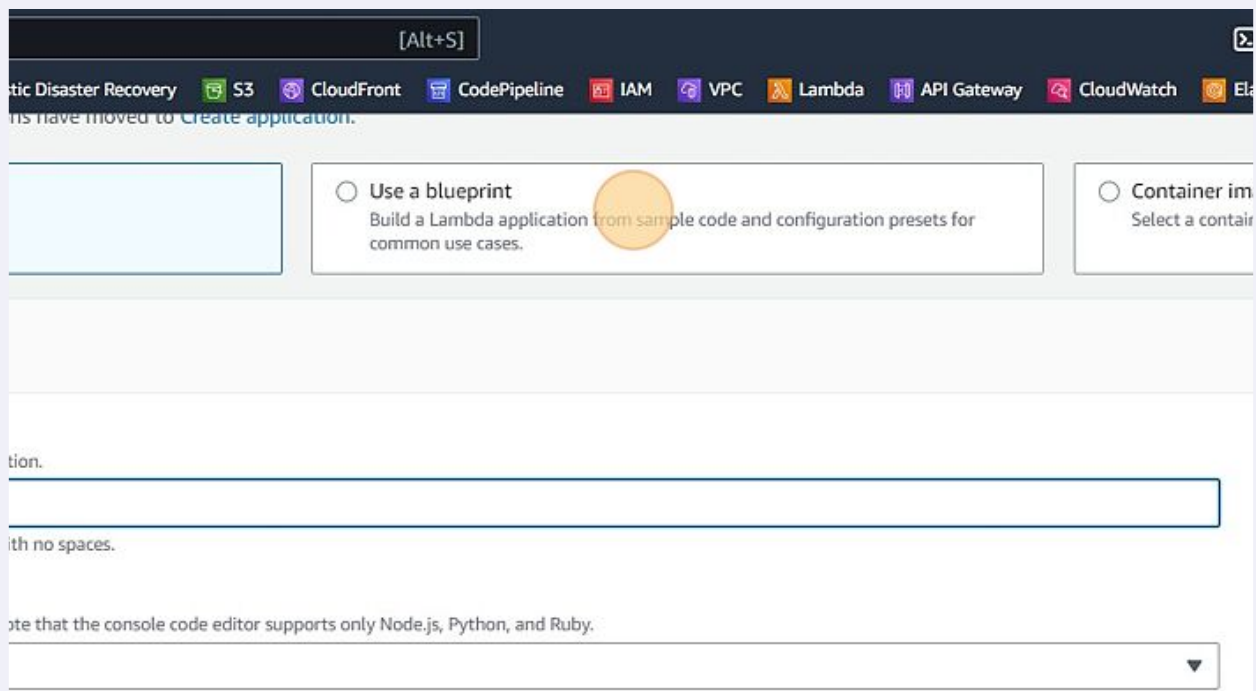
33 Click here.



34 Click "Create function"



35 Click "Build a Lambda application from sample code and configuration presets for common use cases."



36 Click "nodejs14.x"

☐ Container image
Select a container image to deploy for your function.

Basic information [Info](#)

Blueprint name
Hello world function nodejs14.x ▼
A starter AWS Lambda function.

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

Runtime
nodejs14.x

Architecture

37 Click "ont response header implemented in NodeJS."

☐ 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.

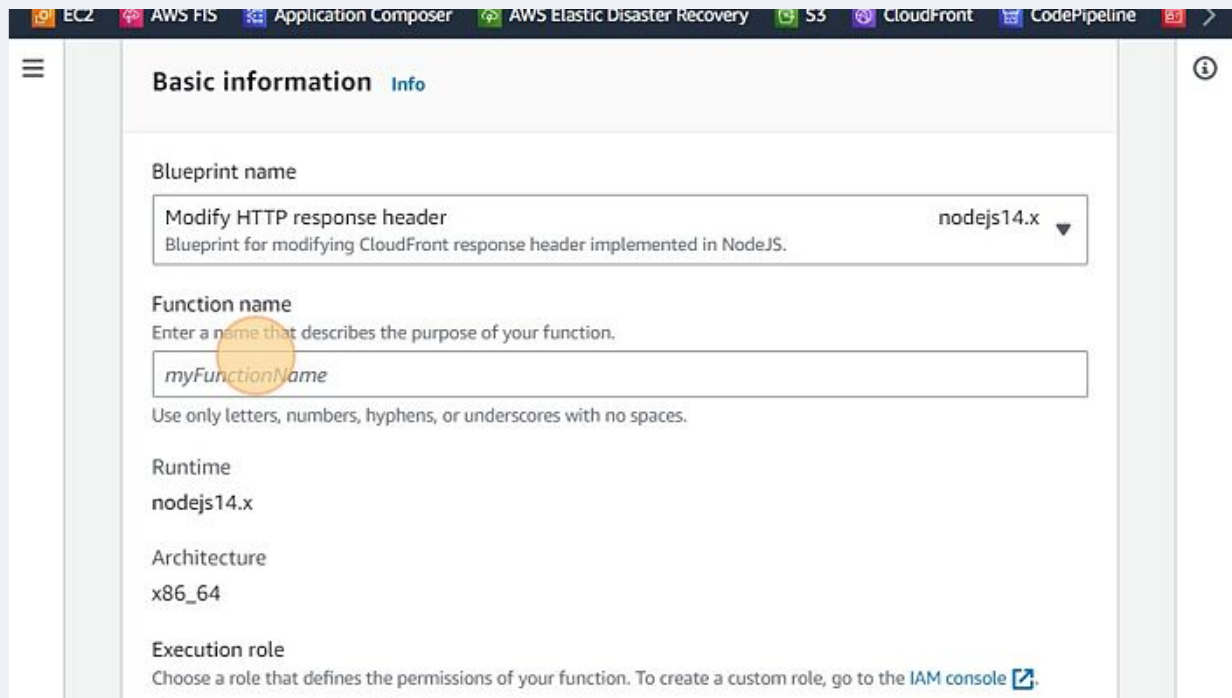
cloudfr

Get started

Modify HTTP response header Blueprint for modifying CloudFront response header implemented in NodeJS.	nodejs14.x
Return HTTP redirect response Blueprint for returning HTTP redirect implemented in NodeJS.	nodejs14.x
Return HTTP response 200 status code Blueprint for generating a response from viewer-request trigger implemented in NodeJS.	nodejs14.x
Hello world function A starter AWS Lambda function.	nodejs14.x ▲

Function name
Enter a name that describes the purpose of your function.
myFunctionName

38 Right-click the "Function name" field.



The screenshot shows the AWS Lambda console's 'Basic information' tab. The 'Blueprint name' is 'Modify HTTP response header' with a runtime of 'nodejs14.x'. The 'Function name' field contains 'myFunctionName' and is highlighted with a yellow circle. A right-click context menu is open over this field. Below it, the 'Runtime' is 'nodejs14.x' and the 'Architecture' is 'x86_64'. The 'Execution role' section has a link to the IAM console.

Basic information [Info](#)

Blueprint name

Modify HTTP response header nodejs14.x ▼
Blueprint for modifying CloudFront response header implemented in NodeJS.

Function name

Enter a name that describes the purpose of your function.

myFunctionName

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

Runtime

nodejs14.x

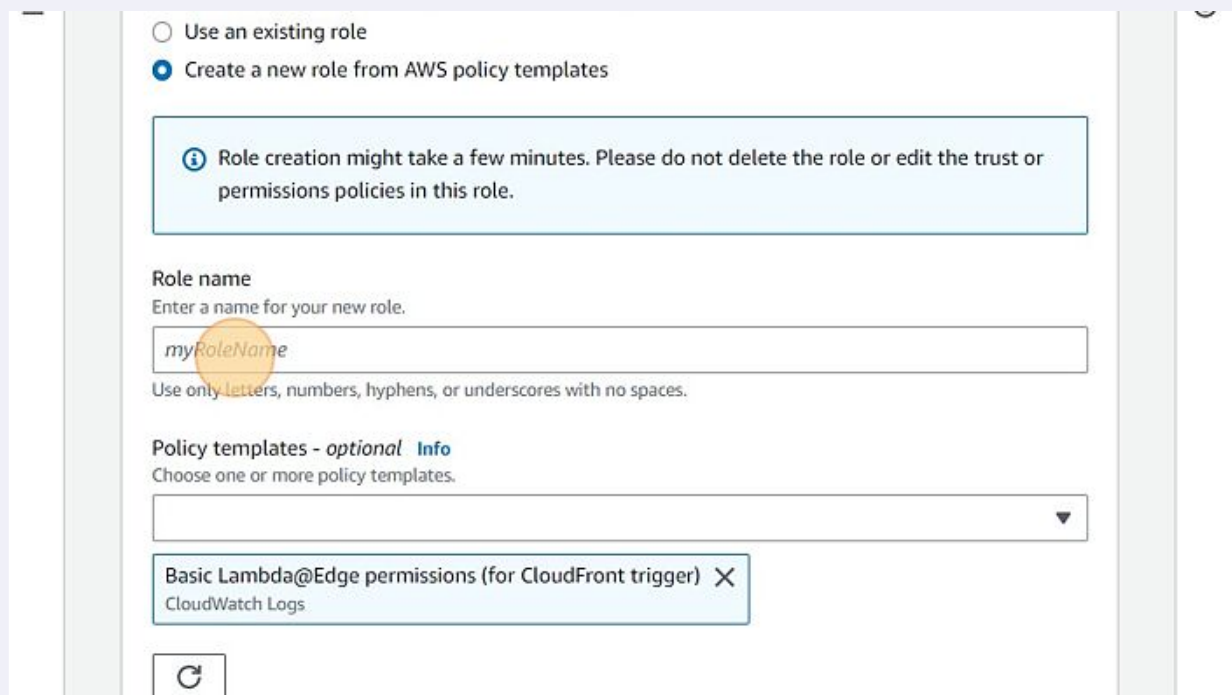
Architecture

x86_64

Execution role

Choose a role that defines the permissions of your function. To create a custom role, go to the [IAM console](#).

39 Click the "Role name" field.



The screenshot shows the AWS Lambda console's 'Role name' field. The 'Role name' field contains 'myRoleName' and is highlighted with a yellow circle. A right-click context menu is open over this field. Above the field, there are radio buttons for 'Use an existing role' and 'Create a new role from AWS policy templates'. Below the field, there is a section for 'Policy templates - optional' with a dropdown menu and a list of selected templates: 'Basic Lambda@Edge permissions (for CloudFront trigger)' and 'CloudWatch Logs'.

☐ Use an existing role

☒ Create a new role from AWS policy templates

[i](#) Role creation might take a few minutes. Please do not delete the role or edit the trust or permissions policies in this role.

Role name

Enter a name for your new role.

myRoleName

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

Policy templates - optional [Info](#)

Choose one or more policy templates.

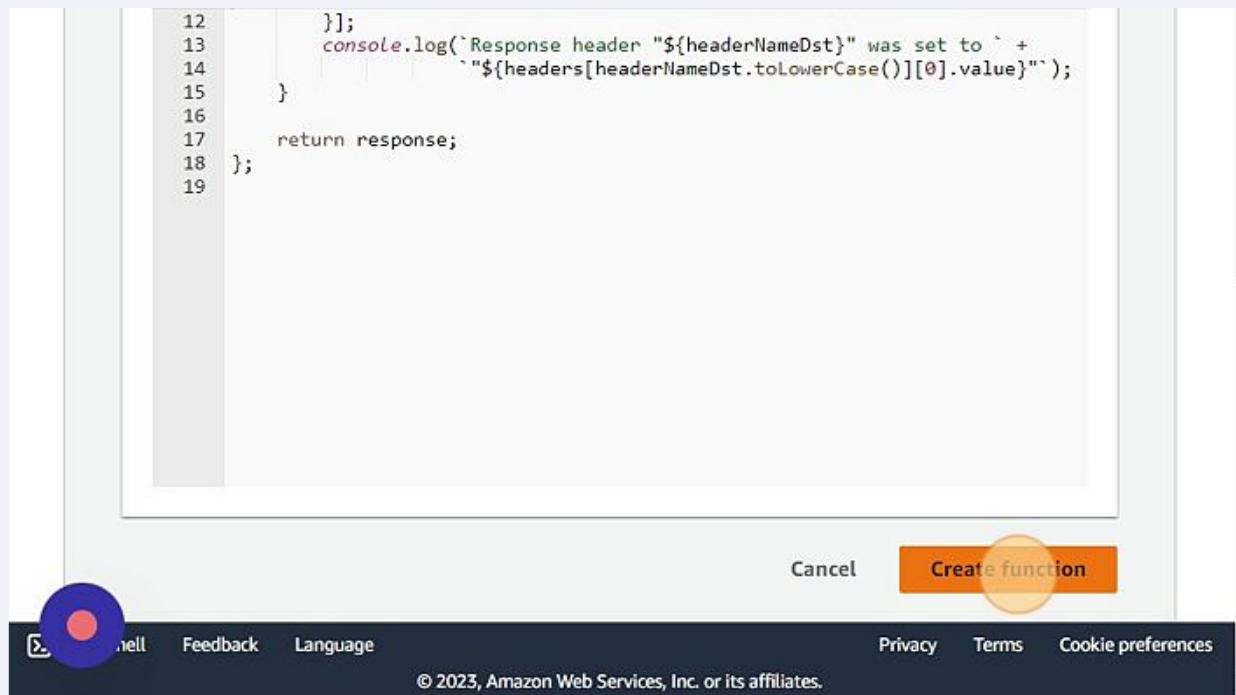
Basic Lambda@Edge permissions (for CloudFront trigger) X

CloudWatch Logs

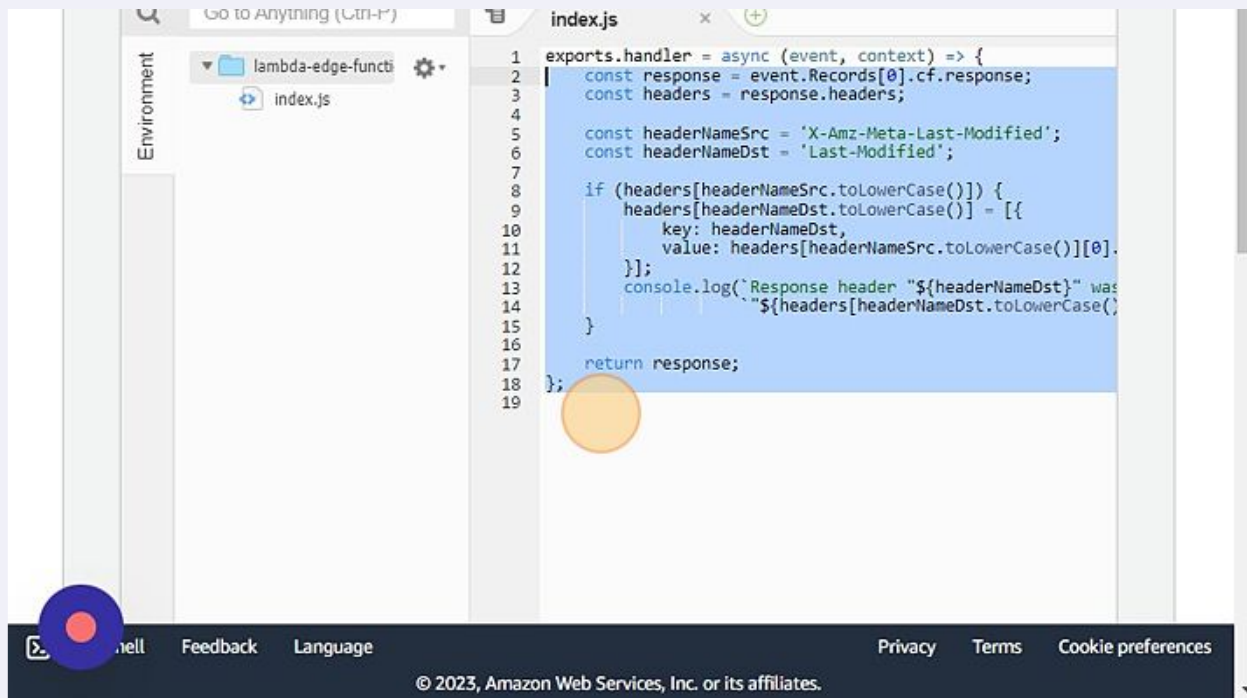
[↻](#)

40 Type "lambda-edge-function-role"

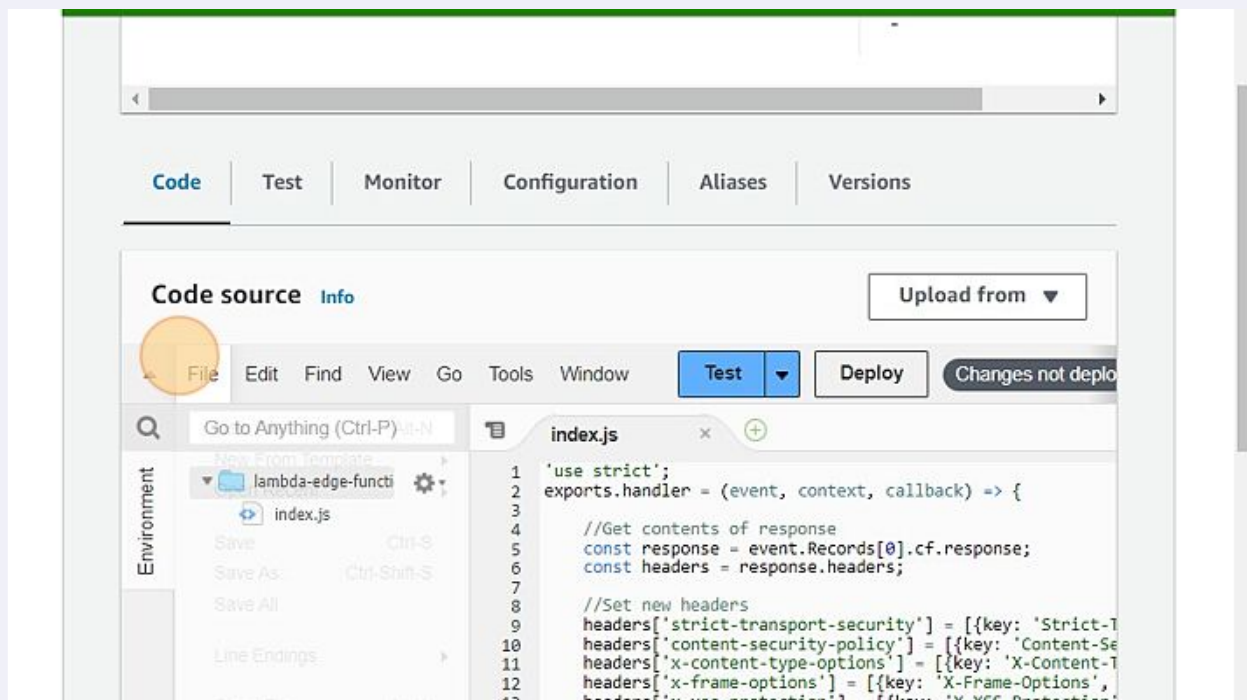
41 Click "Create function"



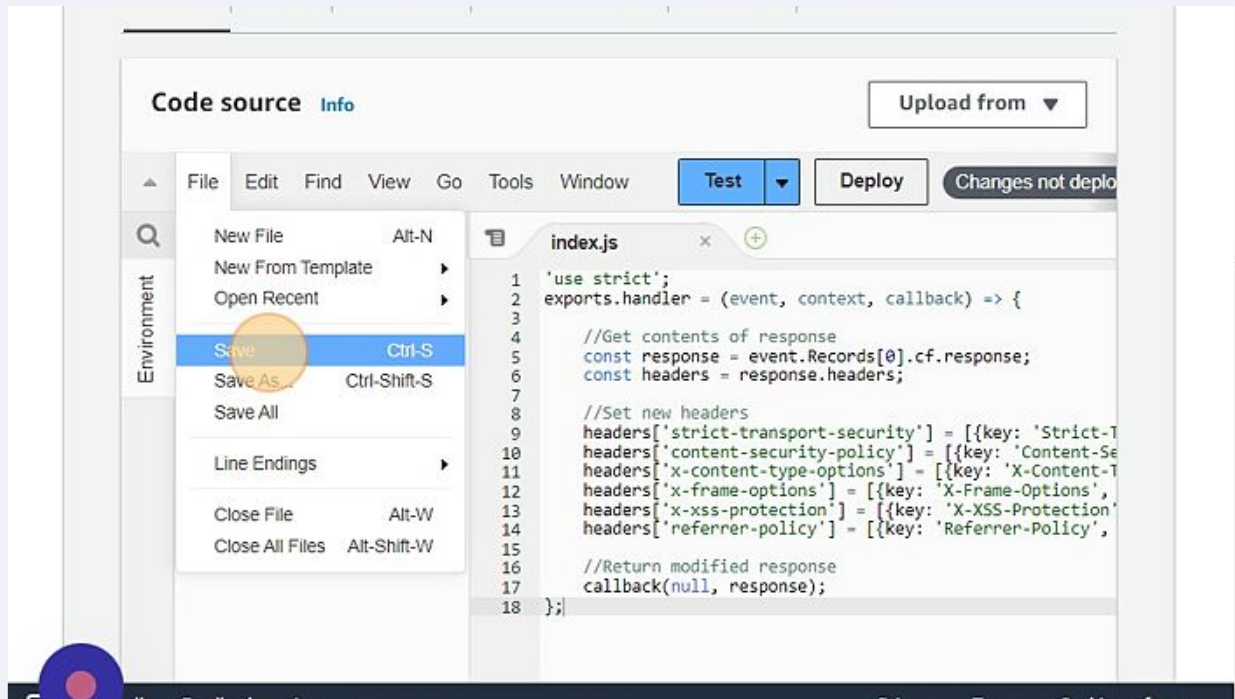
42 Click here.



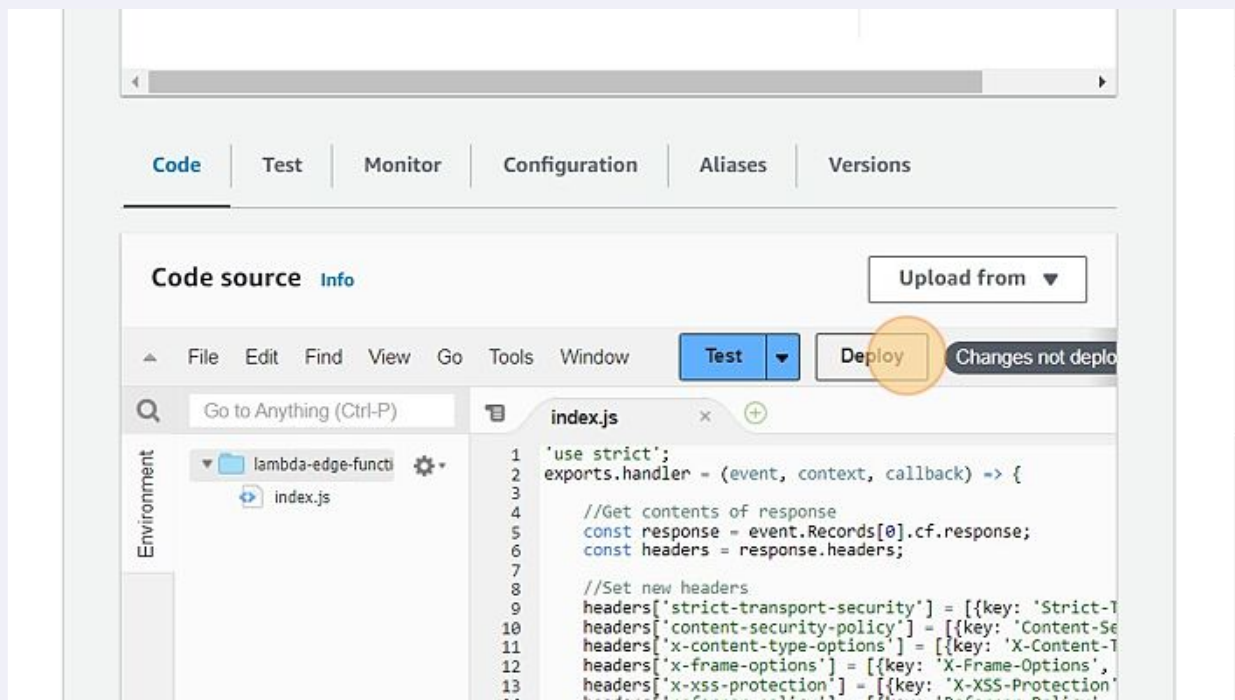
43 Click here.



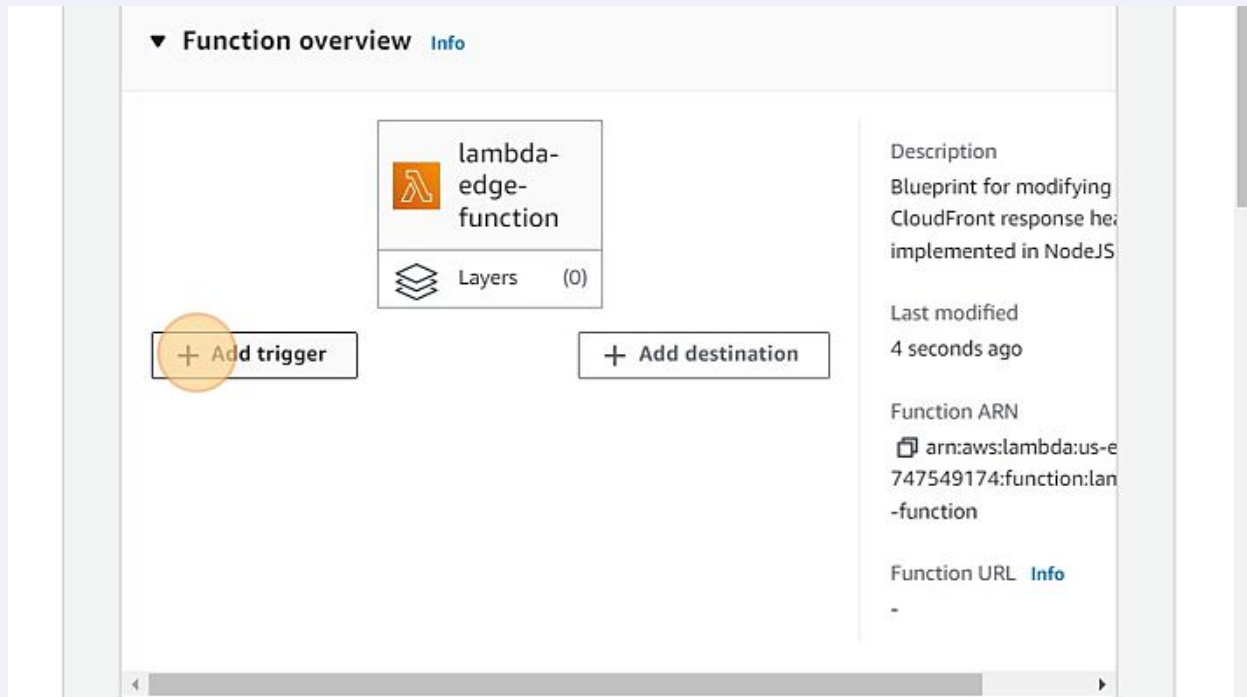
44 Click here.



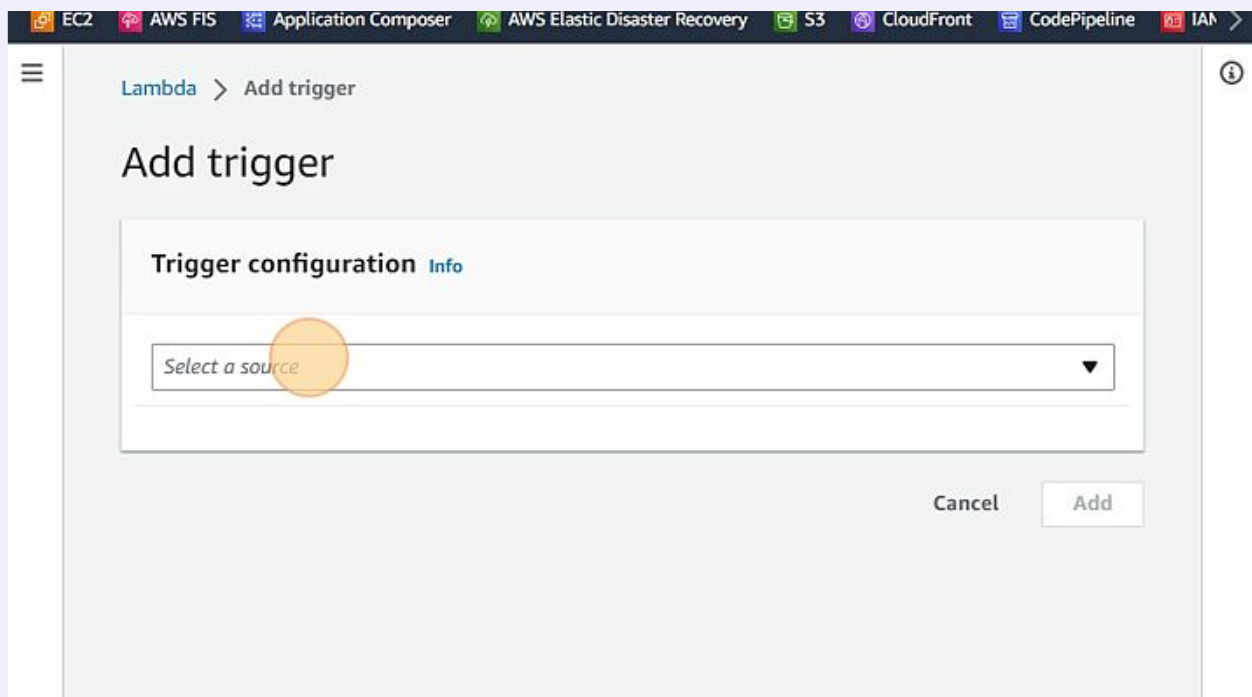
45 Click here.



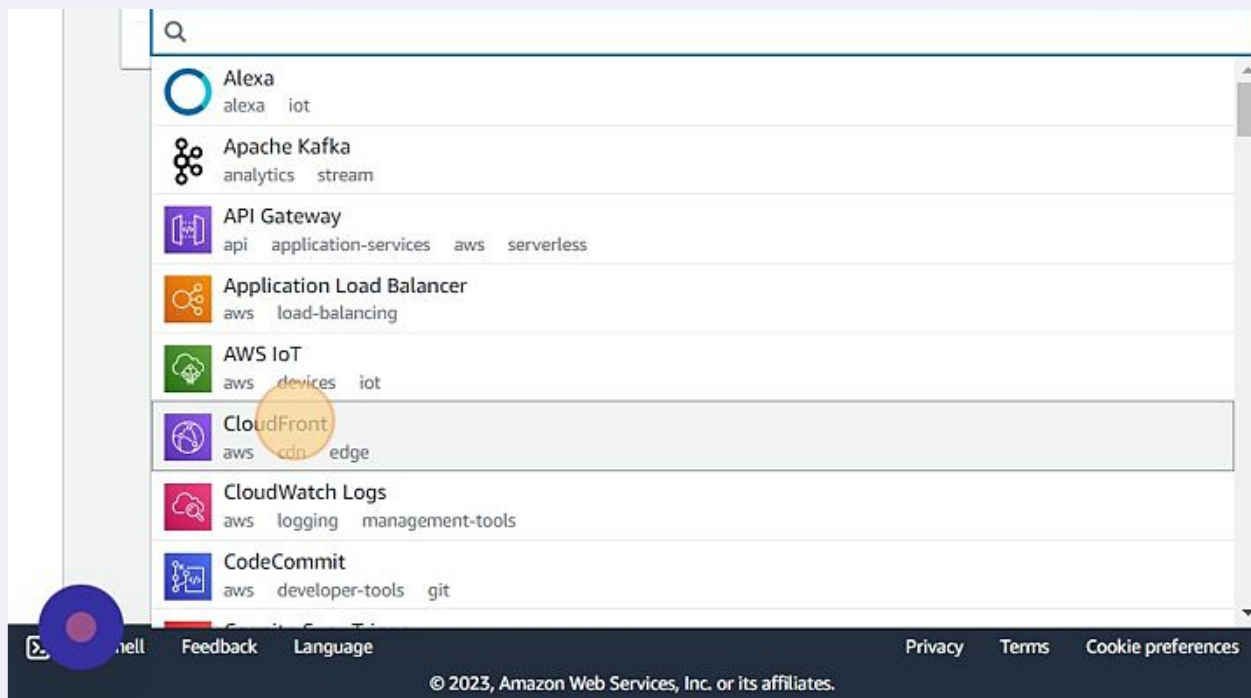
46 Click "Add trigger"



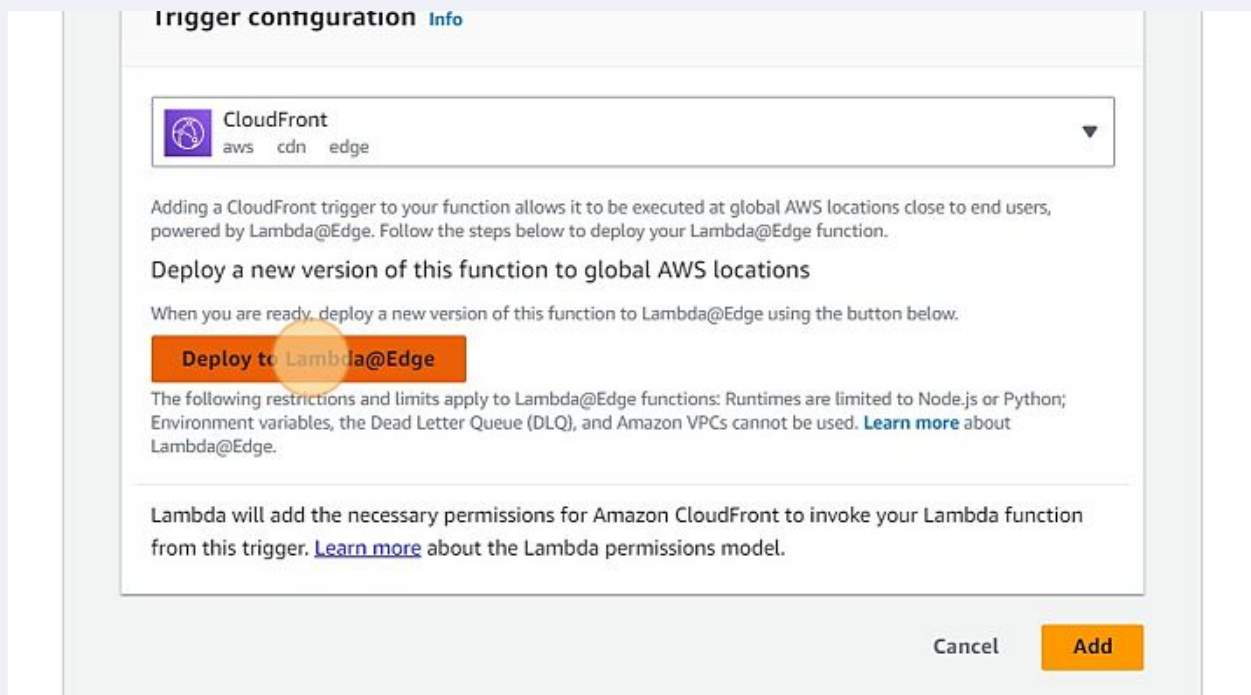
47 Click "Select a source"



48 Click "CloudFront"



49 Click "Deploy to Lambda@Edge"



50 Click the "Distribution" field.

Select an option

☒ Configure new CloudFront trigger

☐ Use existing CloudFront trigger on this function

Configure CloudFront trigger

Distribution
The CloudFront distribution that will send events to your Lambda function.

d3uxf8k8kb1at0.cloudfront.net	E111AVW3FW9GZF
Cache behavior	
Choose the cache behavior you would like this Lambda function to be associated with.	
d1hca5kyvuxcwq.cloudfront.net	E2UDTICE3OQHF3
<input type="text" value="Q *"/>	<input type="button" value="X"/>

CloudFront event
Choose one CloudFront event to listen for.

▼

51 Click "d1hca5kyvuxcwq.cloudfront.net"

☐ Use existing CloudFront trigger on this function

Configure CloudFront trigger

Distribution
The CloudFront distribution that will send events to your Lambda function.

d3uxf8k8kb1at0.cloudfront.net	E111AVW3FW9GZF
Personal Blog Website	
d1hca5kyvuxcwq.cloudfront.net	E2UDTICE3OQHF3

CloudFront event
Choose one CloudFront event to listen for.

▼

☐ Include body
Select "Include body" if you want to read the request body for viewer request or origin request events.
[Learn more.](#)

52 Click "Origin request"

Distribution
The CloudFront distribution that will send events to your Lambda function.

Cache behavior
Choose the cache behavior you would like this Lambda function to be associated with.

CloudFront event
Choose one CloudFront event to listen for.

▼

☐ **Include body**
Select "Include body" if you want to read the request body for viewer request or origin request events.
[Learn more.](#)

☐ **Confirm deploy to Lambda@Edge**
Deploy to Lambda@Edge will create replica of lambda version in all regions

Lambda will add the necessary permissions for Amazon CloudFront to invoke your Lambda function from this trigger.
[Learn more](#) about the Lambda permissions model.

53 Click "Origin response"


Cache behavior
Choose the cache behavior you would like this Lambda function to be associated with.

CloudFront event
Choose one CloudFront event to listen for.

Origin request	▲
Origin request	✓
Origin response	
Viewer request	
Viewer response	

Deploy to Lambda@Edge will create replica of lambda version in all regions

Lambda will add the necessary permissions for Amazon CloudFront to invoke your Lambda function from this trigger.
[Learn more](#) about the Lambda permissions model.



54 Click this checkbox.

THE CLOUDFRONT DISTRIBUTION THAT WILL SEND EVENTS TO YOUR LAMBDA FUNCTION.

Cache behavior
Choose the cache behavior you would like this Lambda function to be associated with.

CloudFront event
Choose one CloudFront event to listen for.

☐ **Confirm deploy to Lambda@Edge**
Deploy to Lambda@Edge will create replica of lambda version in all regions

Lambda will add the necessary permissions for Amazon CloudFront to invoke your Lambda function from this trigger.
[Learn more](#) about the Lambda permissions model.

55 Click "Deploy"

THE CLOUDFRONT DISTRIBUTION THAT WILL SEND EVENTS TO YOUR LAMBDA FUNCTION.

Cache behavior
Choose the cache behavior you would like this Lambda function to be associated with.

CloudFront event
Choose one CloudFront event to listen for.

☒ **Confirm deploy to Lambda@Edge**
Deploy to Lambda@Edge will create replica of lambda version in all regions

Lambda will add the necessary permissions for Amazon CloudFront to invoke your Lambda function from this trigger.
[Learn more](#) about the Lambda permissions model.

56 Click "Distributions"

The screenshot shows the AWS CloudFront console. The left sidebar has a 'Distributions' link highlighted with an orange circle. The main content area shows the details for a distribution named 'E2UDTICE3OQHF3'. A green notification bubble says 'Distribution domain name copied'. The 'General' tab is selected, showing the domain name 'd1hca5kyvuxcwq.cloudfront.net' and the ARN 'arn:aws:cloudfront::932747549174:distribution/E2UDTICE3OQHF3'.

57 Click this button.

The screenshot shows the AWS CloudFront console. The left sidebar has a 'Distributions' link highlighted with an orange circle. The main content area shows the 'Distributions (2)' page. The 'Create distribution' button is highlighted with an orange circle. The page shows a list of two distributions:

ID	Description	Type
E2UDTICE3OQHF3	-	Production
E111AVW3FW9GZF	Personal ...	Production

58 In a new tab, navigate to d1hca5kyvuxcwq.cloudfront.net

59 Right-click "Lambda@Edge Demo"

Lambda@Edge Demo



60 In Web Browser open Inspect section. Next, could you check the in-network section. You can see the newly added headers. Ex : strict-transport-security, x-content-type-options.