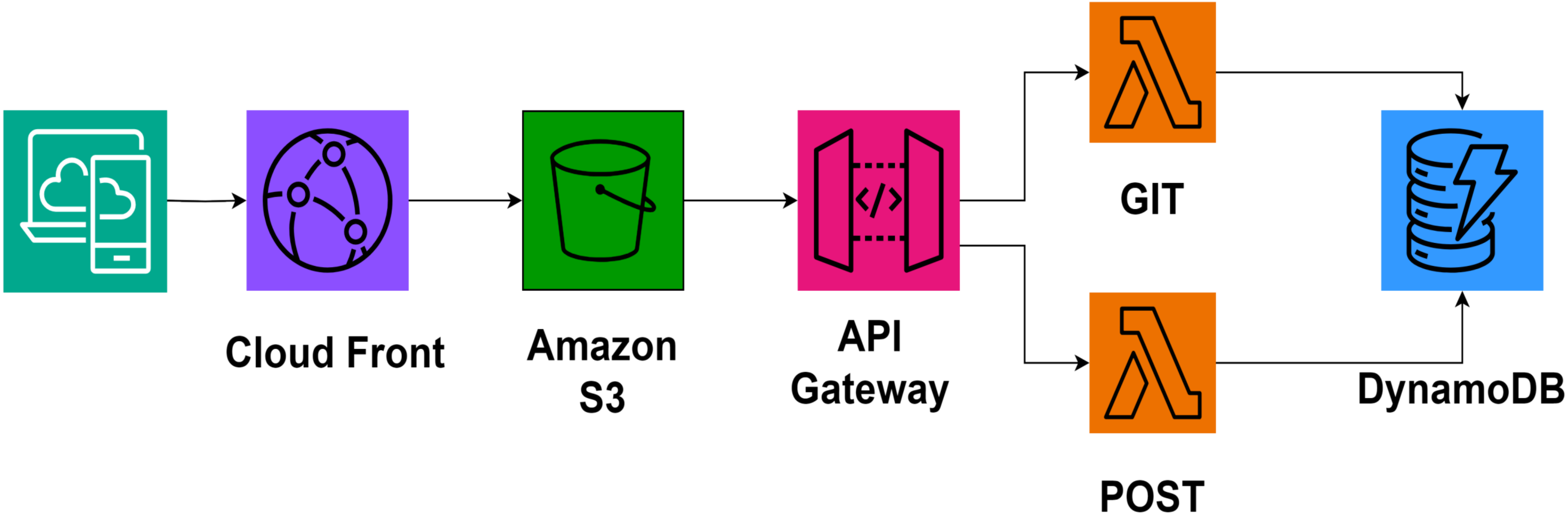
Deploying Serverless Web Application on AWS Using:

S3
API Gateway
Lambda
DynamoDB
CloudFront

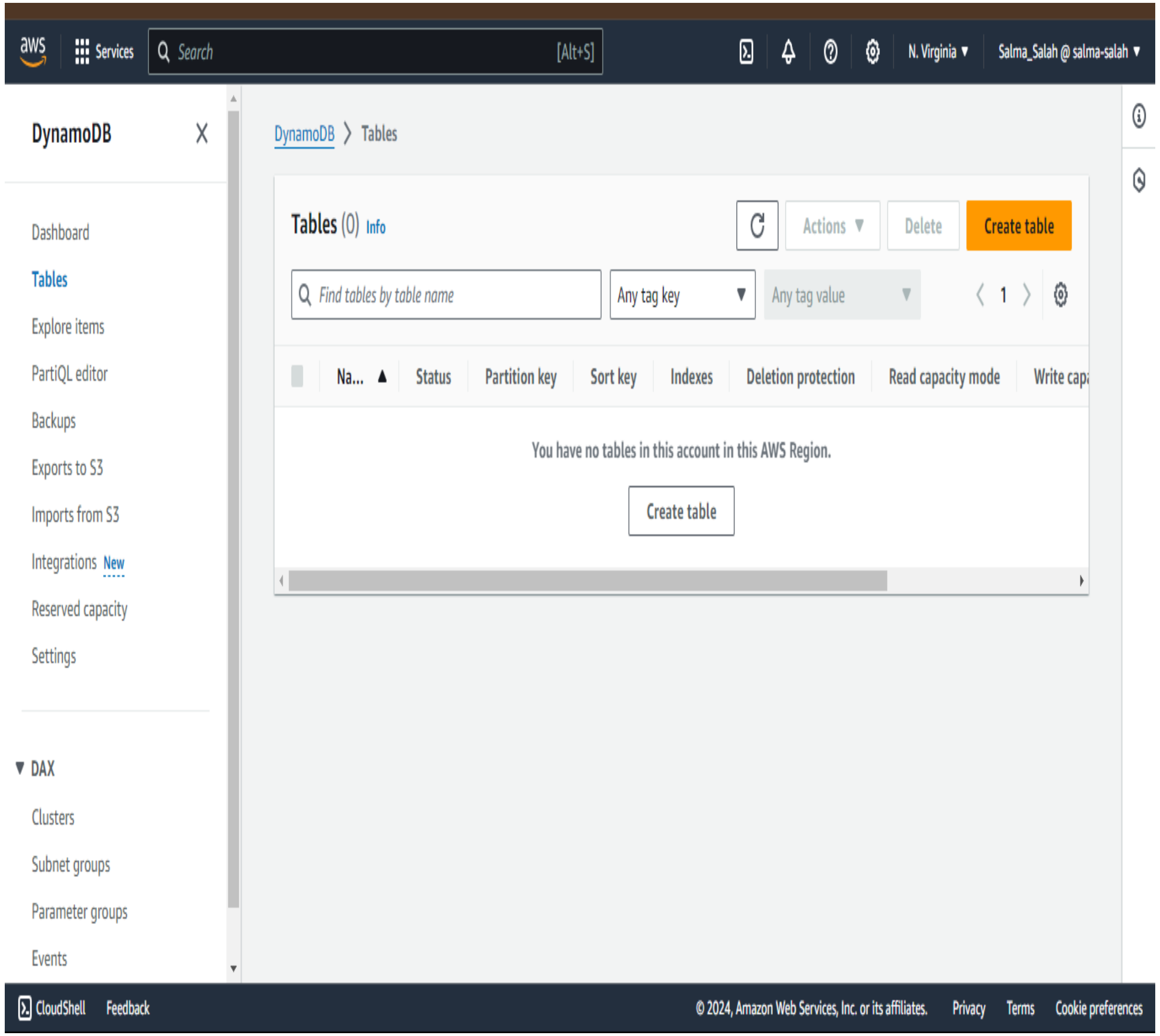
By: Salma Salah

Project’s Diagram

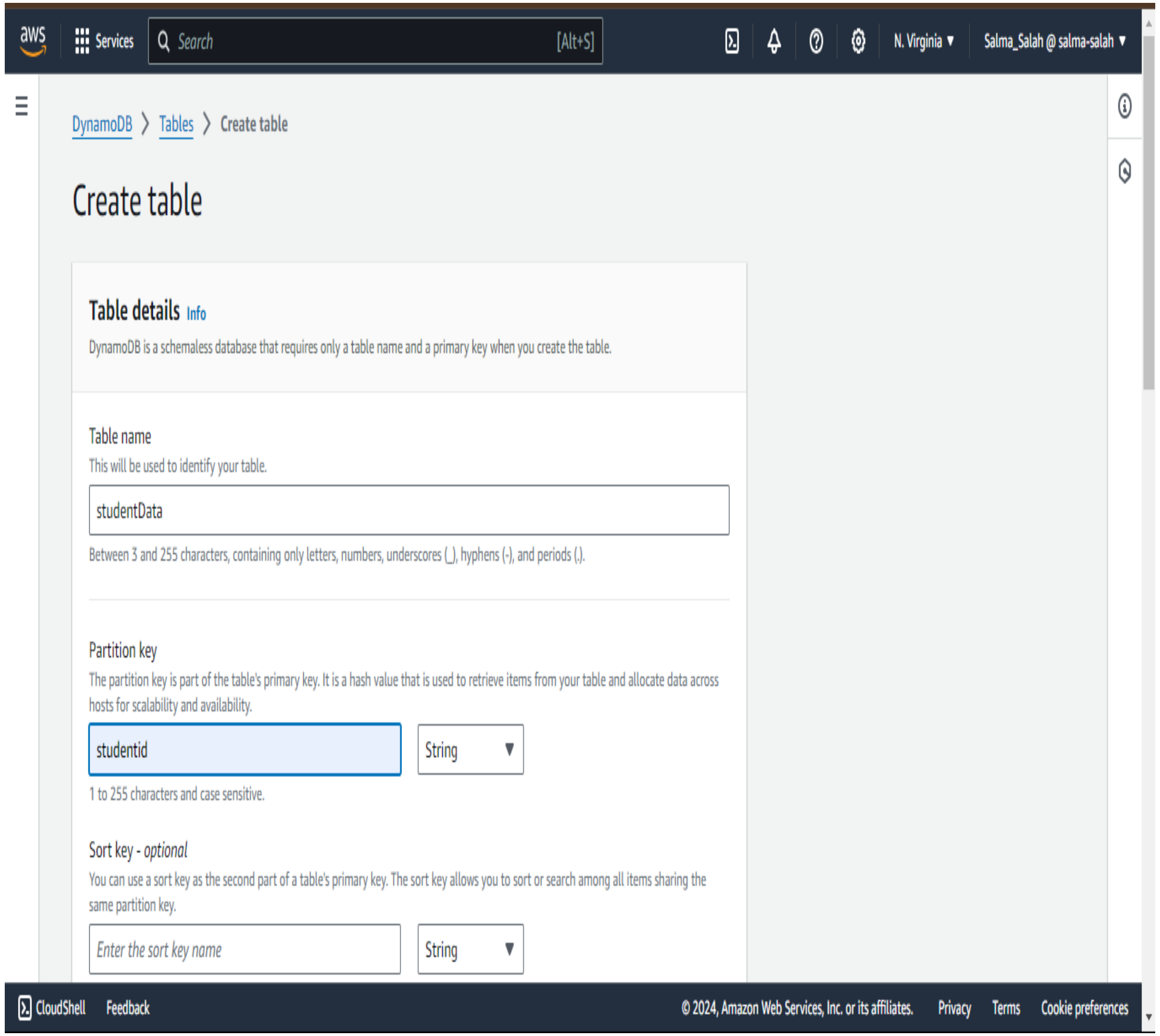


First

Create DynamoDB table



You have no tables in this account in this AWS Region.


aws
Services
Search
[Alt+S]
N. Virginia ▾
Salma_Salah @ salma-salah ▾
DynamoDB 〉 Tables 〉 Create table
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

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.

studentData

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.

studentid | String ▾

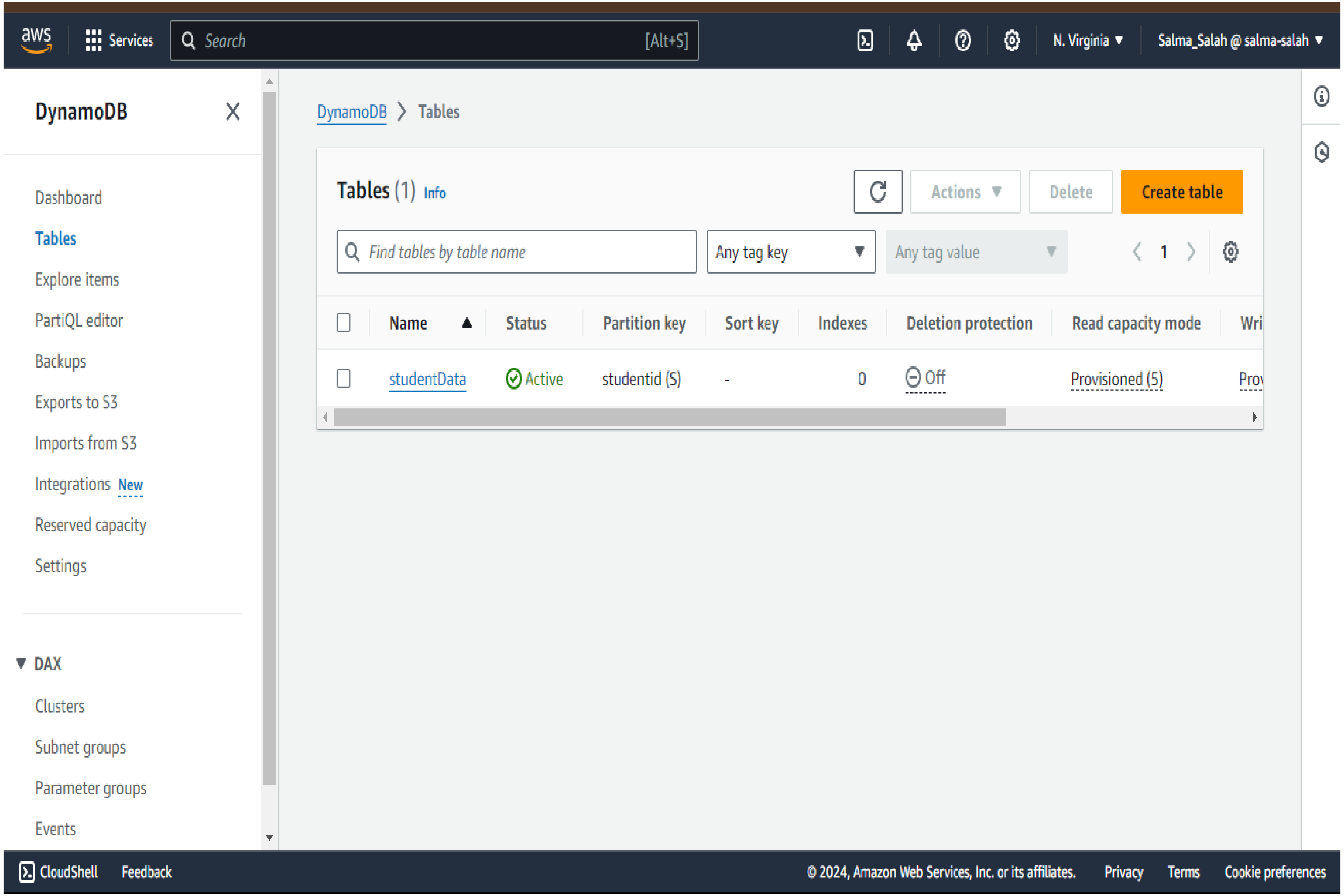
1 to 255 characters and case sensitive.

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 ▾

Table After Creation

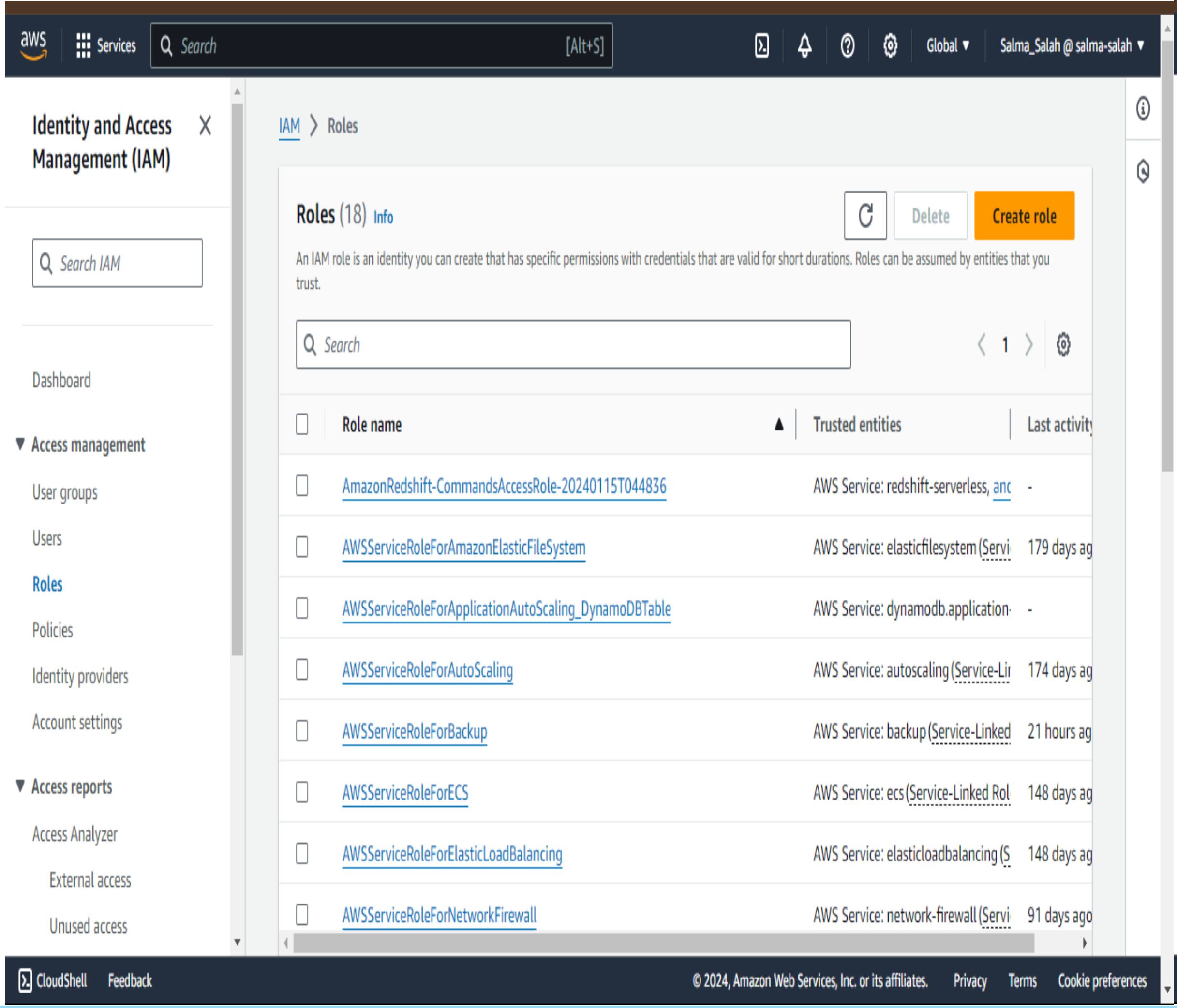


Tables (1) Info

□	Name ▲	Status	Partition key	Sort key	Indexes	Deletion protection	Read capacity mode	Wri
□	studentData	✓ Active	studentid (S)	-	0	⊖ Off	Provisioned (5)	Prov

Second

Create IAM Rule to Allow Lambda function to access DynamoDB



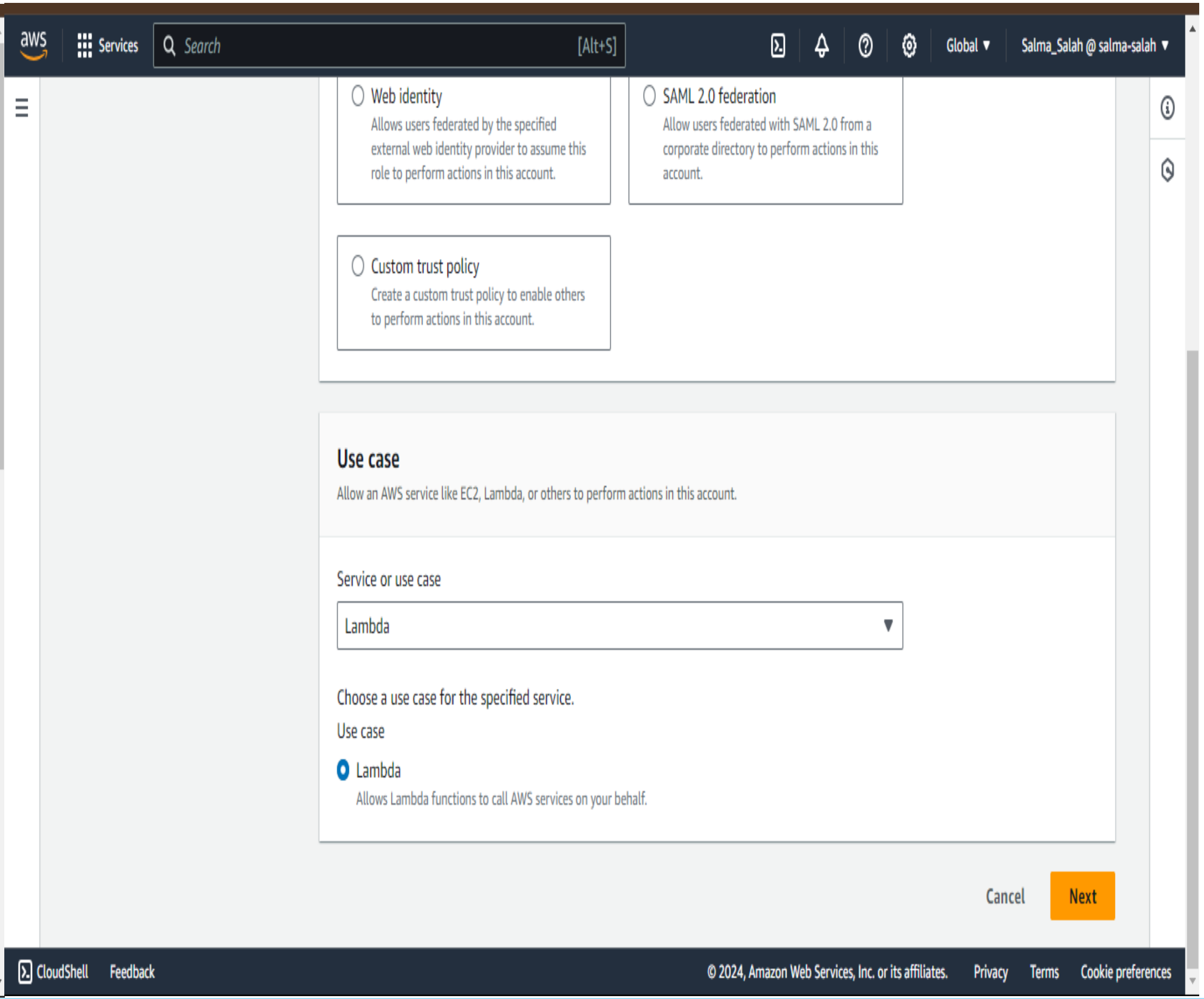
Identity and Access Management (IAM)

IAM > Roles

Roles (18) 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.

□	Role name ▲	Trusted entities	Last activity
□	AmazonRedshift-CommandsAccessRole-20240115T044836	AWS Service: redshift-serverless, anc	-
□	AWSServiceRoleForAmazonElasticFileSystem	AWS Service: elasticfilesystem (Servi	179 days ag
□	AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS Service: dynamodb.application-	-
□	AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Li	174 days ag
□	AWSServiceRoleForBackup	AWS Service: backup (Service-Linked	21 hours ag
□	AWSServiceRoleForECS	AWS Service: ecs (Service-Linked Rol	148 days ag
□	AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing (S	148 days ag
□	AWSServiceRoleForNetworkFirewall	AWS Service: network-firewall (Servi	91 days ago



○ 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.

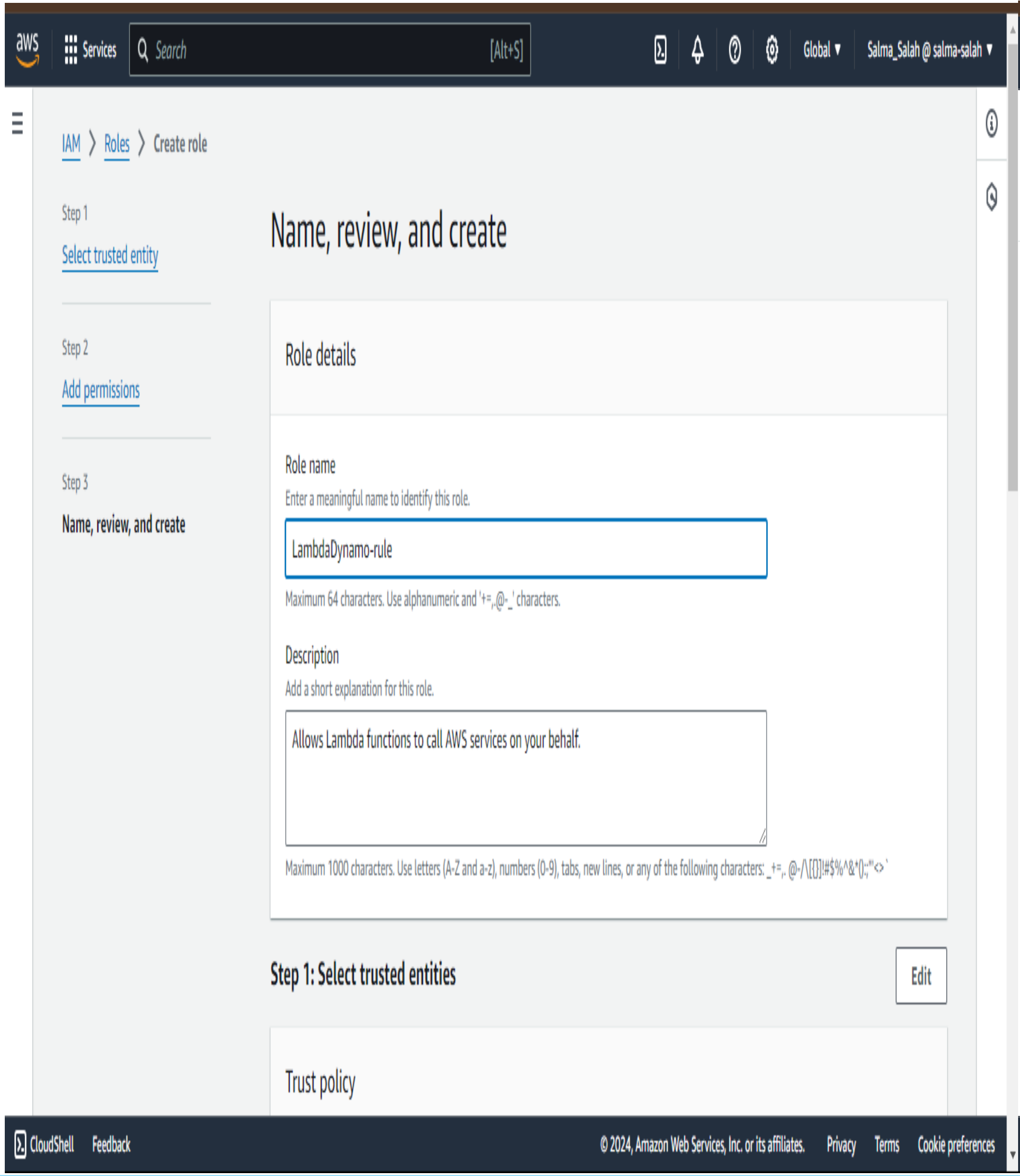
Service or use case: Lambda ▾

Choose a use case for the specified service.

Use case

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

Policies that are Attached to the Rule



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Name, review, and create

Role details

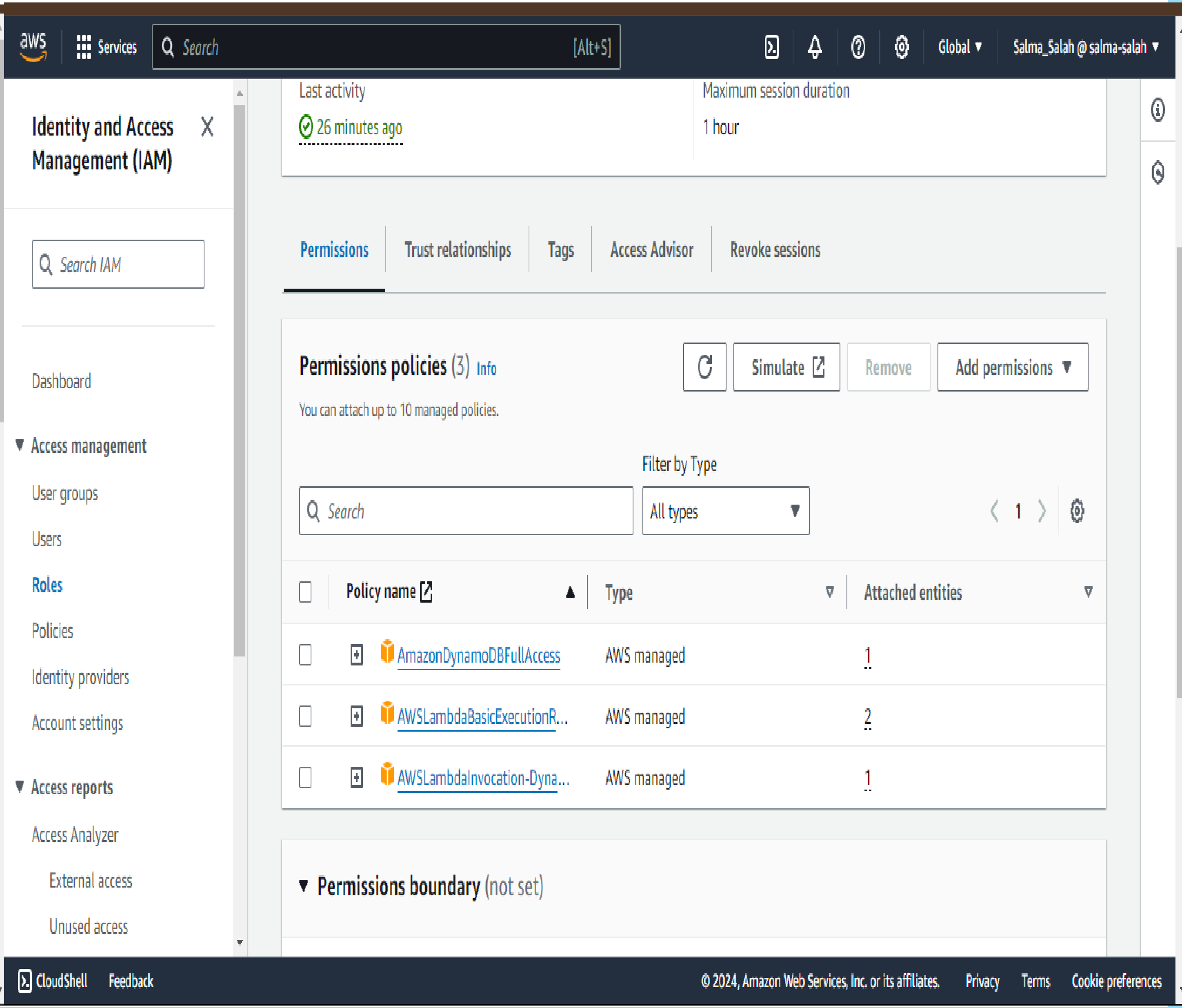
Role name
Enter a meaningful name to identify this role.
LambdaDynamo-rule
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this role.
Allows Lambda functions to call AWS services on your behalf.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,.@-/\[{()}]!#$%^&*();"'<>`

Step 1: Select trusted entities

Edit

Trust policy



Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

▼ Access reports

- Access Analyzer
- External access
- Unused access

Last activity: 26 minutes ago

Maximum session duration: 1 hour

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

Permissions policies (3) Info

You can attach up to 10 managed policies.

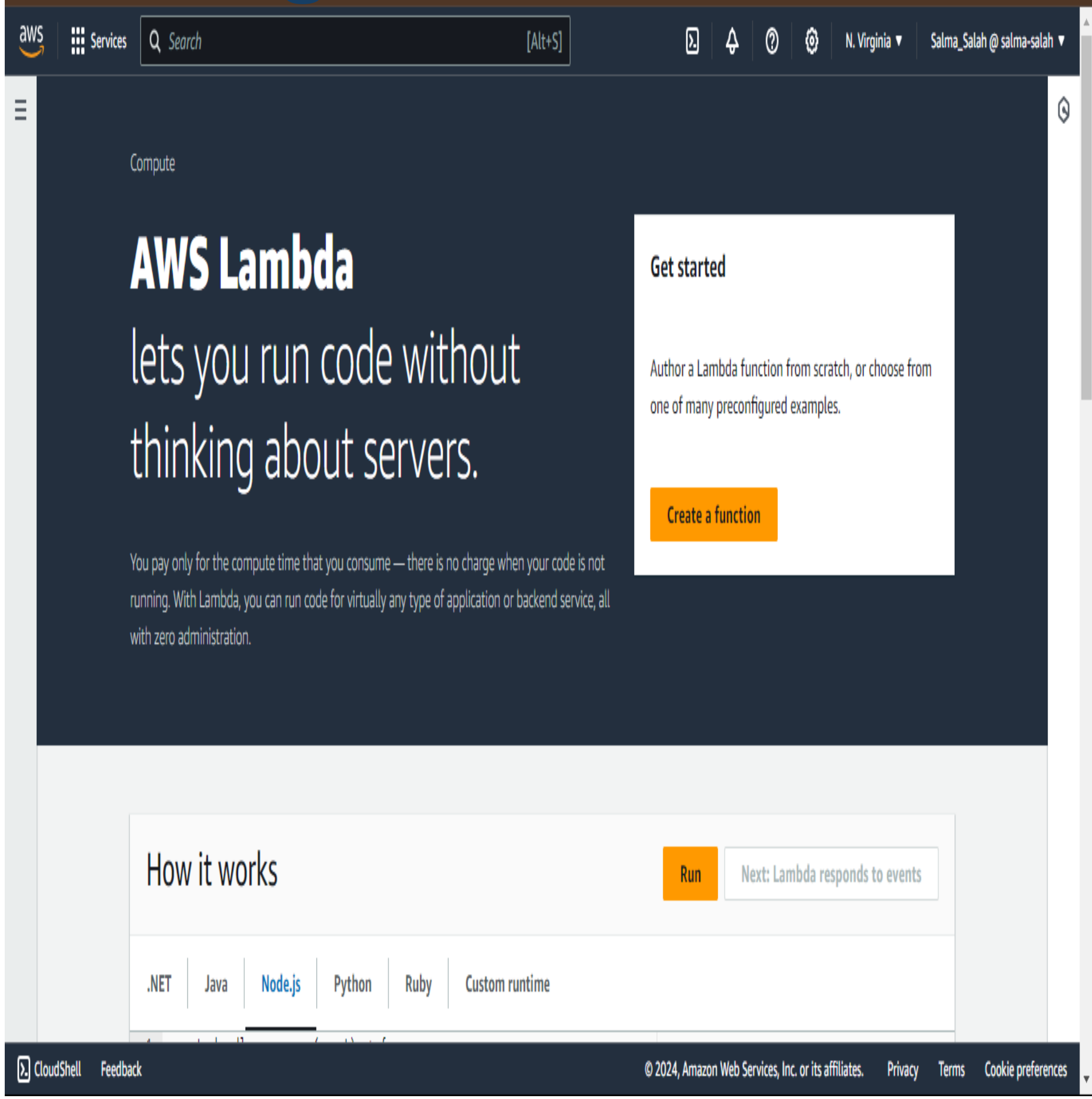
Filter by Type: All types

□	Policy name	Type	Attached entities
□	AmazonDynamoDBFullAccess	AWS managed	1
□	AWSLambdaBasicExecutionR...	AWS managed	2
□	AWSLambdaInvocation-Dyna...	AWS managed	1

▼ Permissions boundary (not set)

Third

Creating Two Lambda Functions



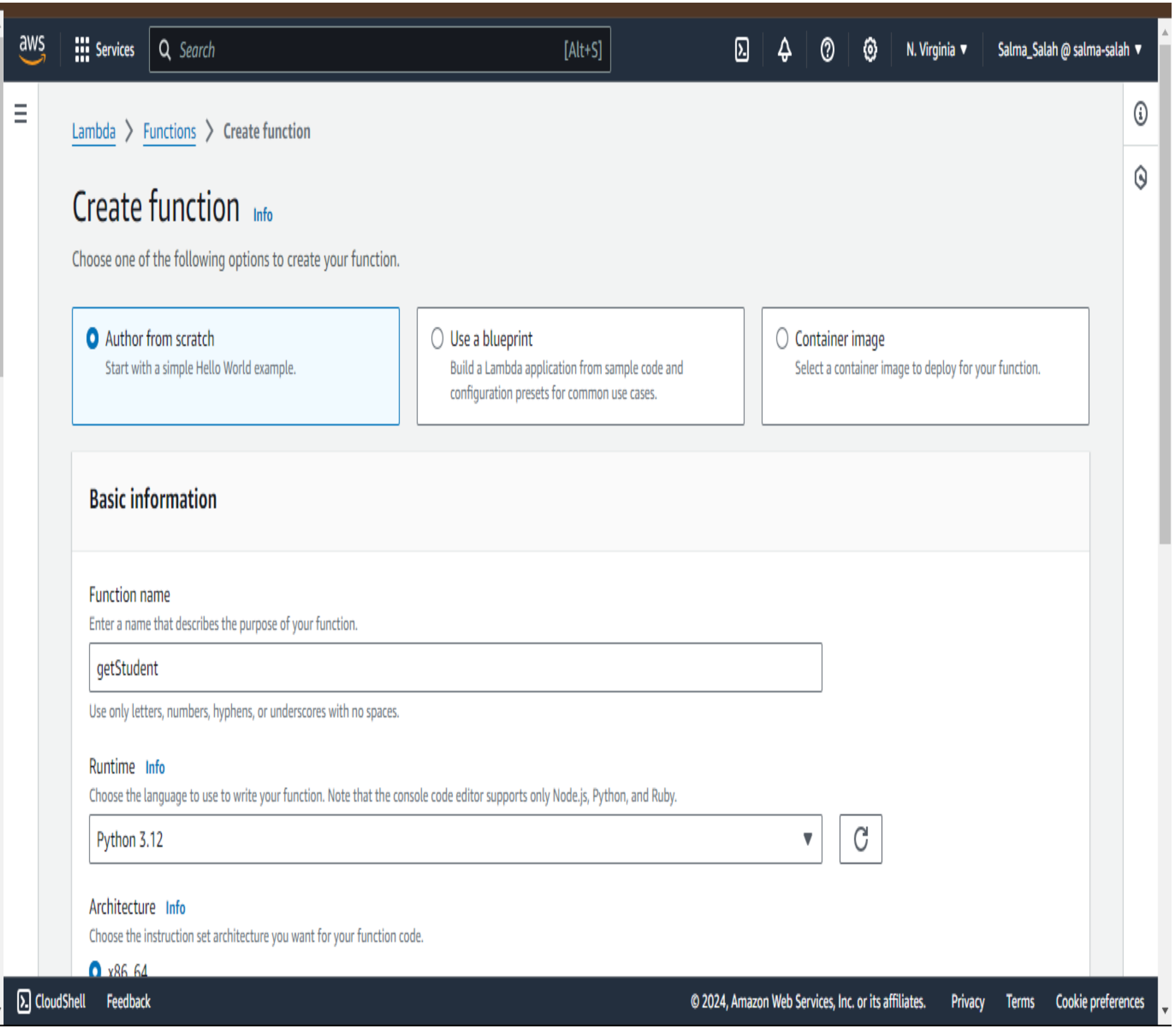
Compute

AWS Lambda lets you run code without thinking about servers.

You pay only for the compute time that you consume — there is no charge when your code is not running. With Lambda, you can run code for virtually any type of application or backend service, all with zero administration.

Get started

Author a Lambda function from scratch, or choose from one of many preconfigured examples.



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.

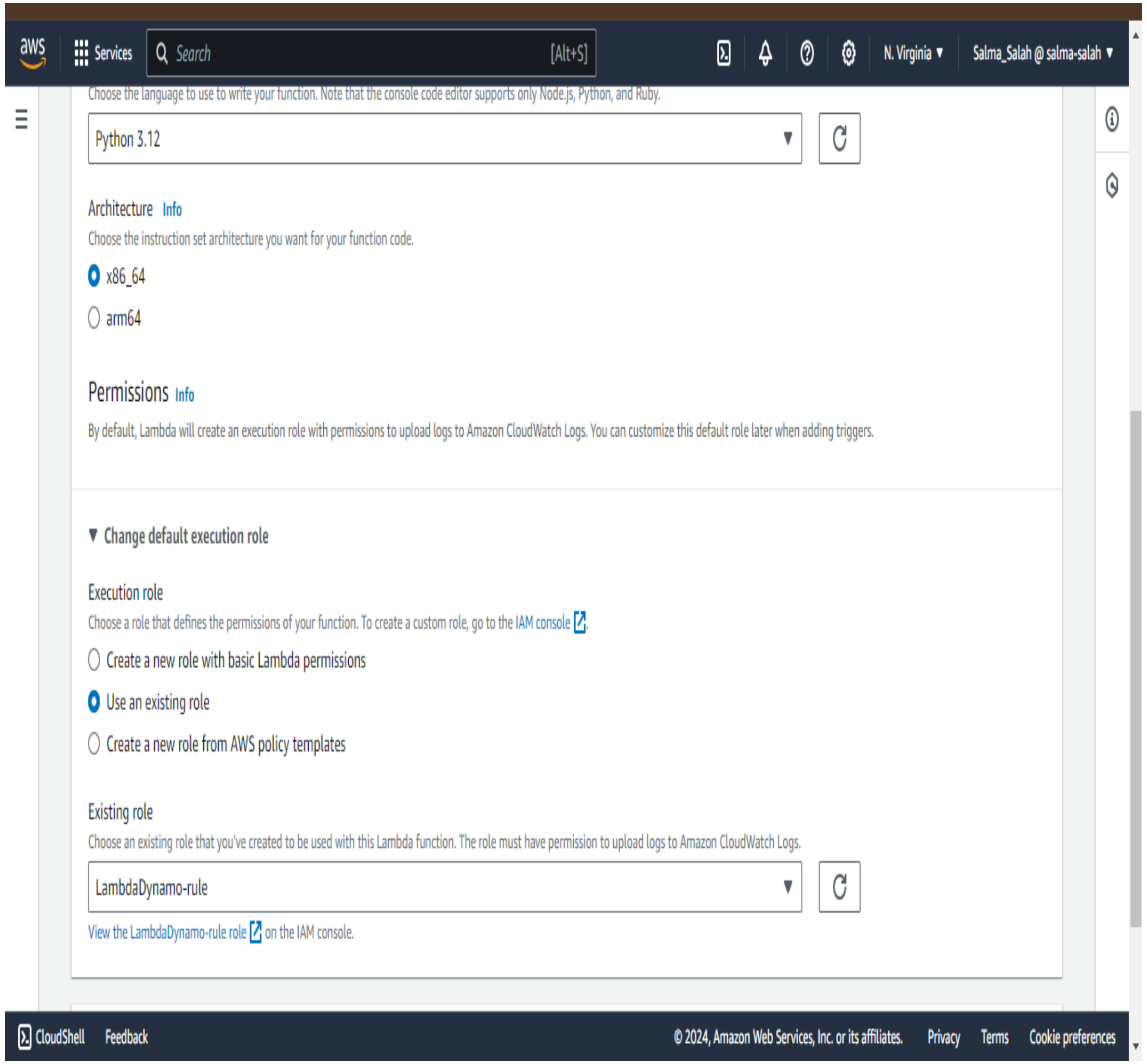
Basic information

Function name
Enter a name that describes the purpose of your function.
getStudent
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.
Python 3.12 ▾

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

First Lambda Function (getStudent) that will get data from DynamoDB table and adding python code source



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

Python 3.12 ▾

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

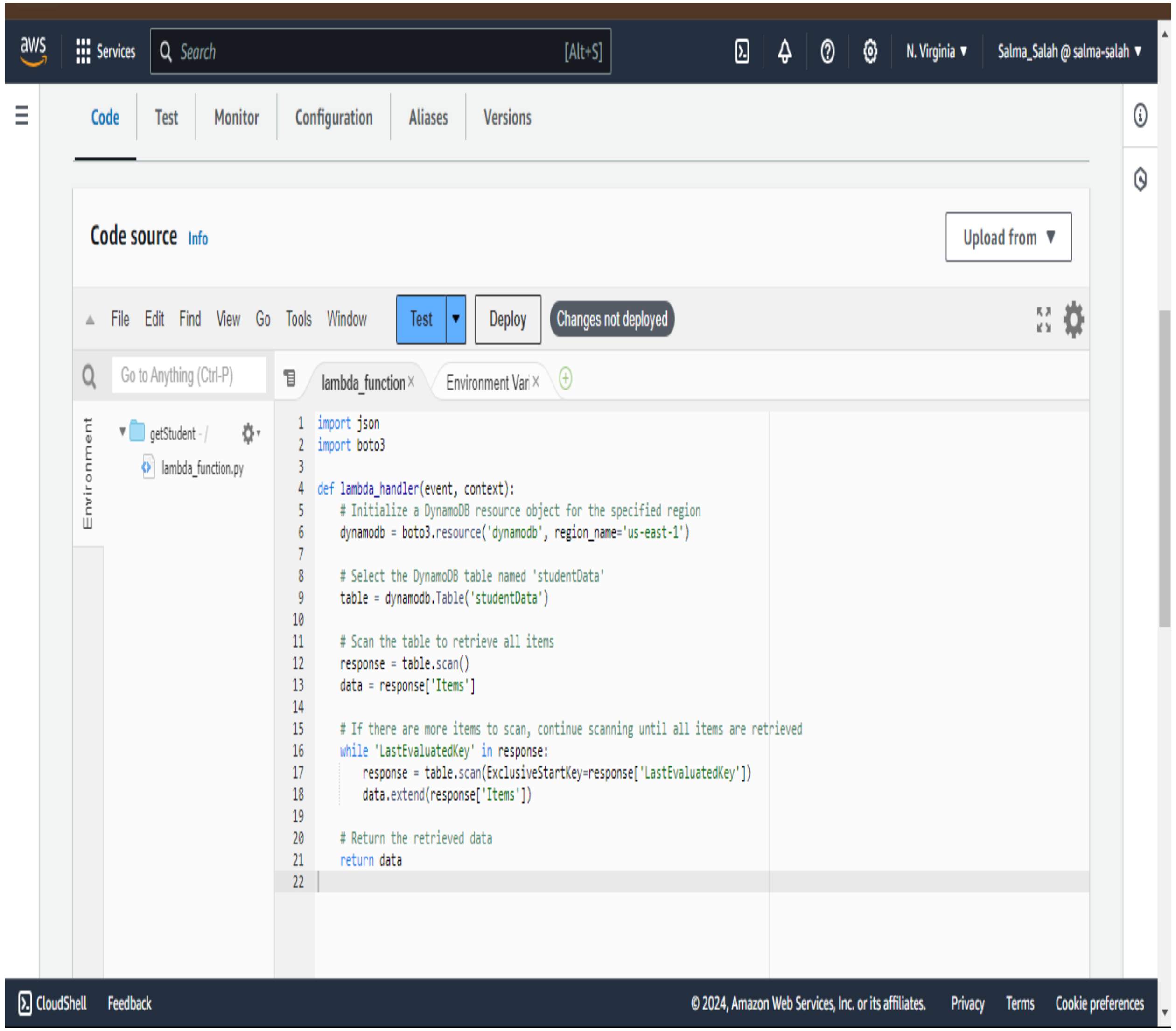
○ Create a new role from AWS policy templates

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.

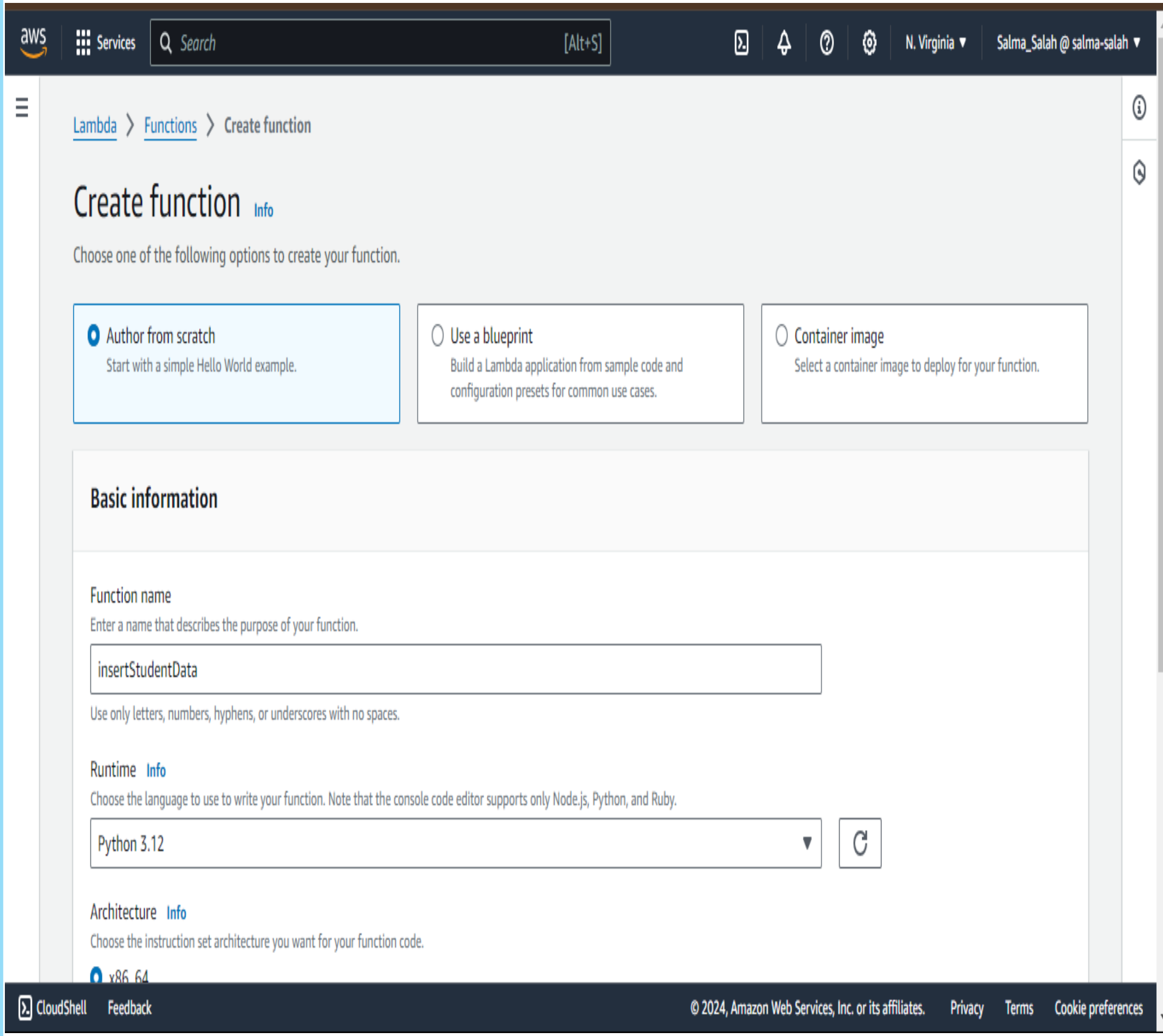
LambdaDynamo-rule ▾

View the LambdaDynamo-rule role on the IAM console.



```python
import json
import boto3

def lambda_handler(event, context):
    # Initialize a DynamoDB resource object for the specified region
    dynamodb = boto3.resource('dynamodb', region_name='us-east-1')

    # Select the DynamoDB table named 'studentData'
    table = dynamodb.Table('studentData')

    # Scan the table to retrieve all items
    response = table.scan()
    data = response['Items']

    # If there are more items to scan, continue scanning until all items are retrieved
    while 'LastEvaluatedKey' in response:
        response = table.scan(ExclusiveStartKey=response['LastEvaluatedKey'])
        data.extend(response['Items'])

    # Return the retrieved data
    return data
```

Creating Second Lambda Function (insertStudentdata) that will PUT in DynamoDB table


aws
Services
Search
[Alt+S]
N. Virginia ▾
Salma_Salah @ salma-salah ▾
Lambda › Functions › Create function
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

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.

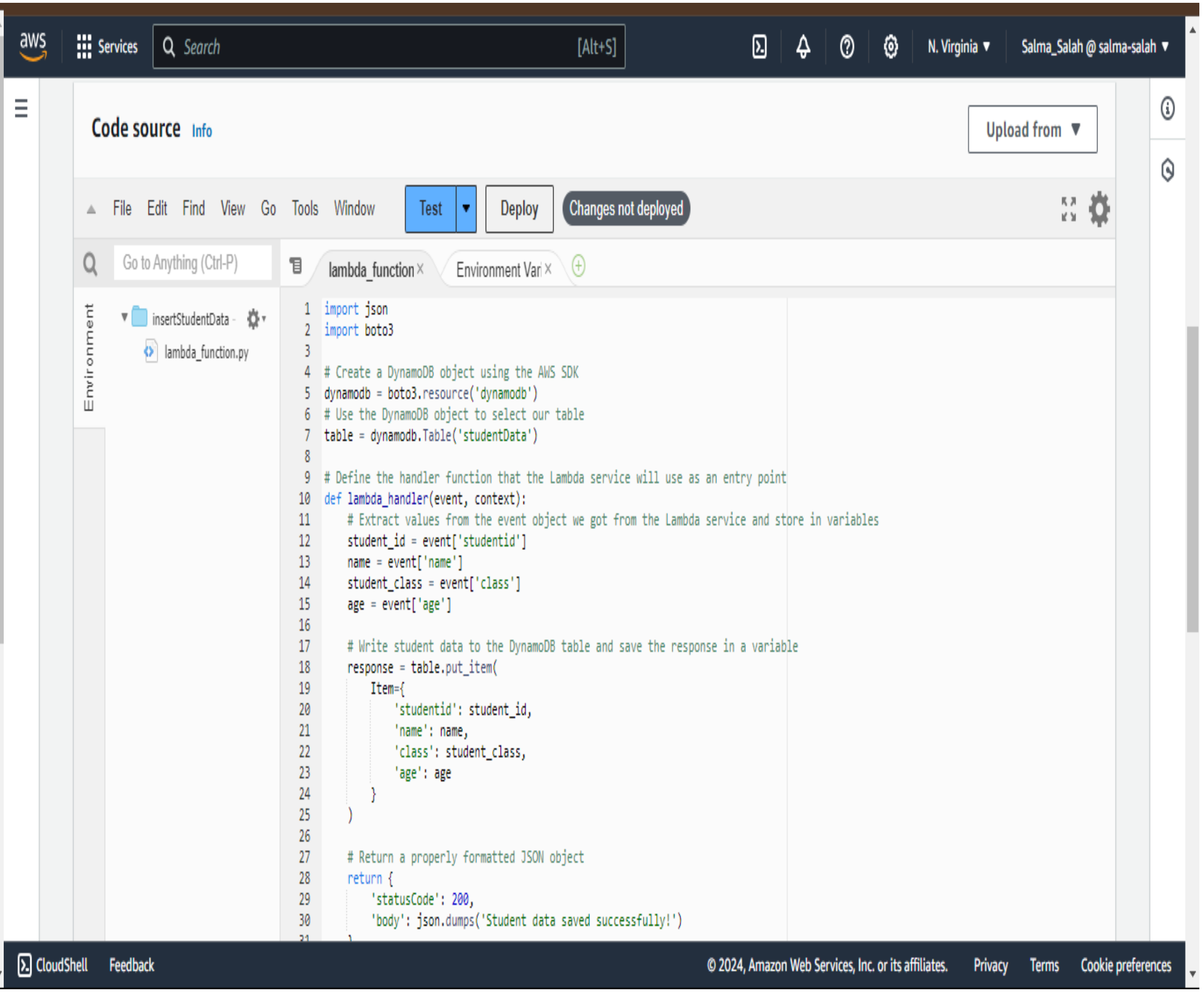
○ Container image
Select a container image to deploy for your function.

Basic information

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

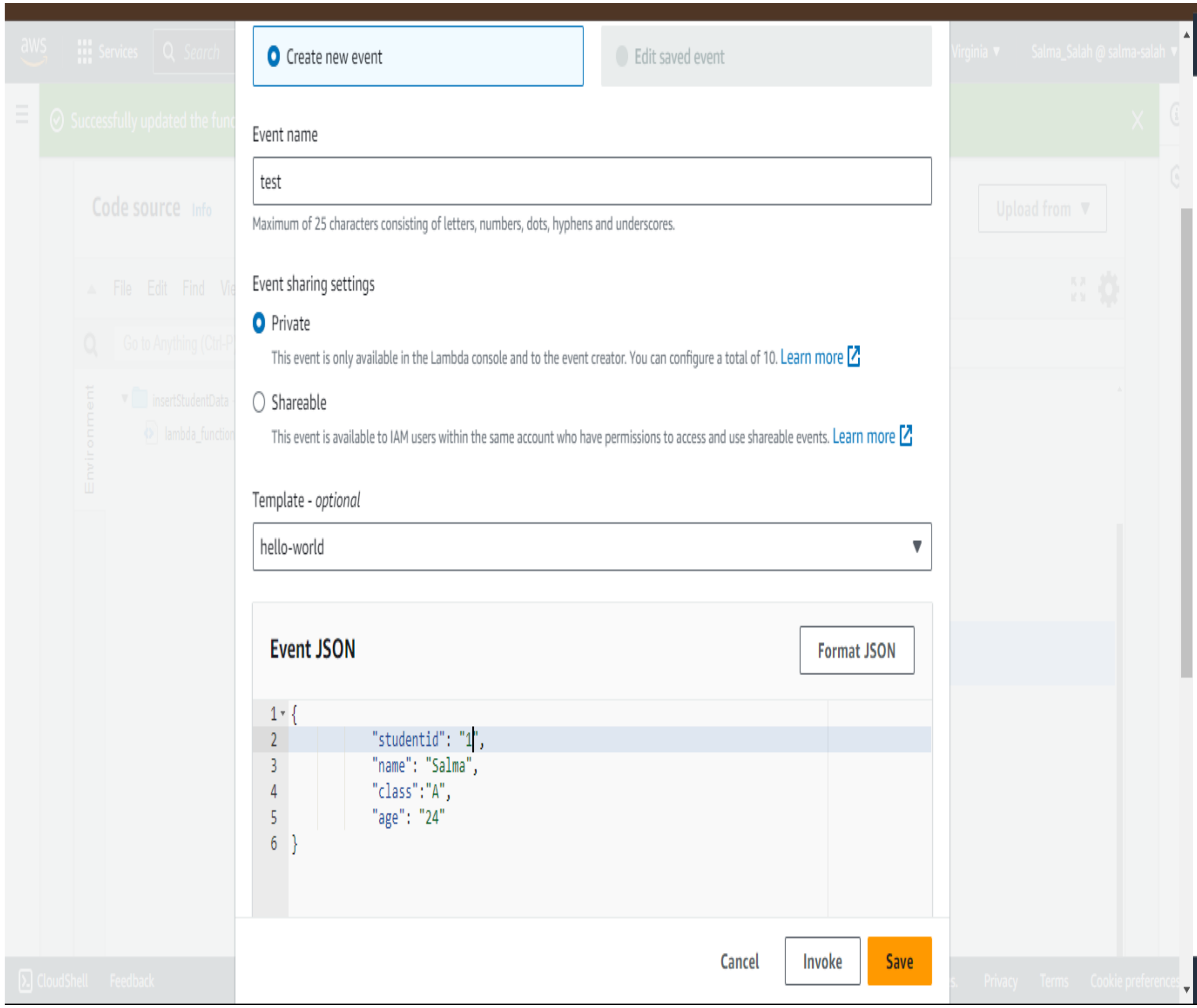
Runtime Info
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.
Python 3.12

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



```python
import json
import boto3

# Create a DynamoDB object using the AWS SDK
dynamodb = boto3.resource('dynamodb')
# Use the DynamoDB object to select our table
table = dynamodb.Table('studentData')

# Define the handler function that the Lambda service will use as an entry point
def lambda_handler(event, context):
    # Extract values from the event object we got from the Lambda service and store in variables
    student_id = event['studentid']
    name = event['name']
    student_class = event['class']
    age = event['age']

    # Write student data to the DynamoDB table and save the response in a variable
    response = table.put_item(
        Item={
            'studentid': student_id,
            'name': name,
            'class': student_class,
            'age': age
        }
    )

    # Return a properly formatted JSON object
    return {
        'statusCode': 200,
        'body': json.dumps('Student data saved successfully!')
```

Test the Execution of Second (PUT) lambda function by adding data to DynamoDB



Event name

test

Maximum of 25 characters consisting of letters, numbers, dots, hyphens and underscores.

Event sharing settings

● Private

This event is only available in the Lambda console and to the event creator. You can configure a total of 10. Learn more

○ Shareable

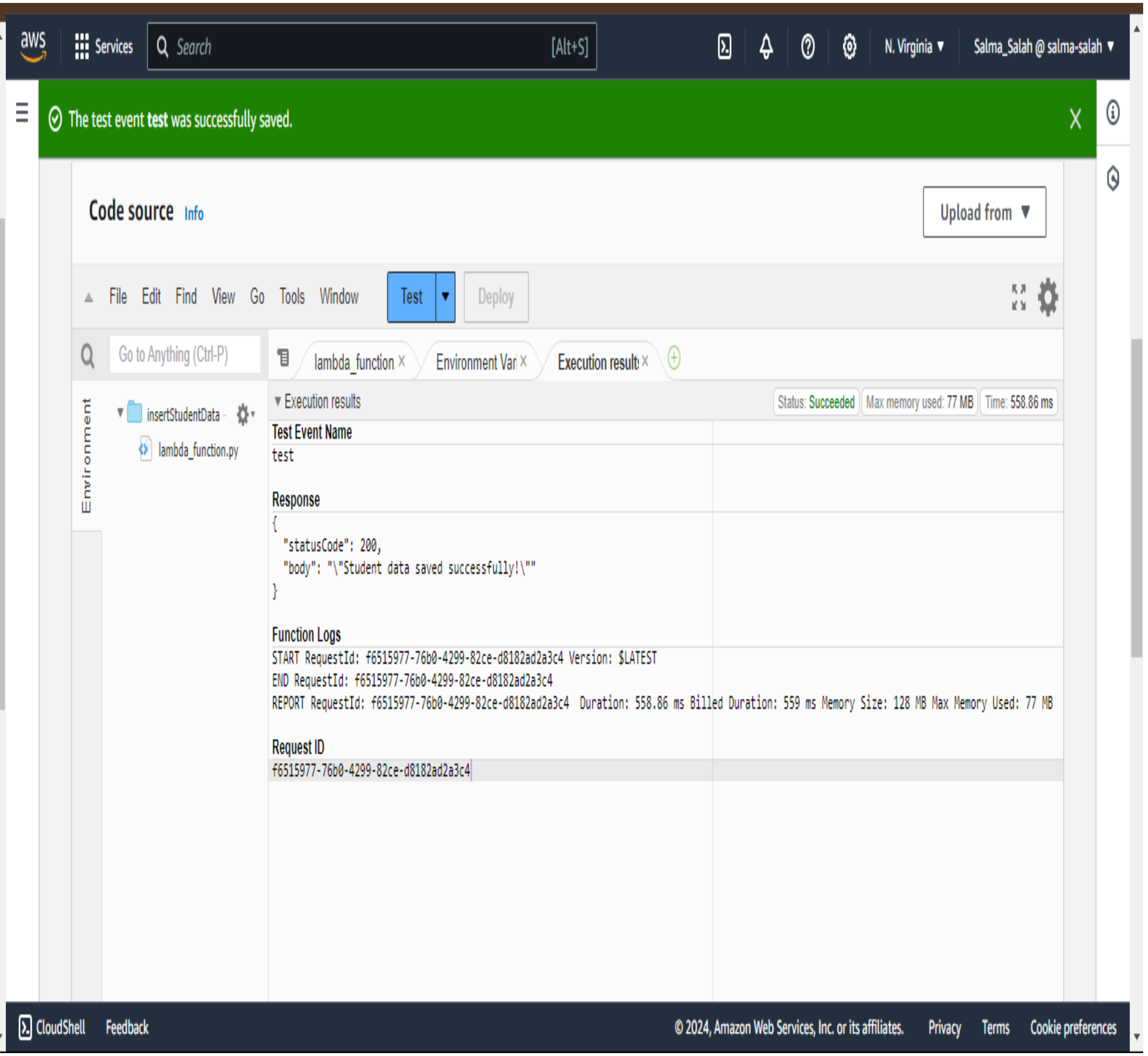
This event is available to IAM users within the same account who have permissions to access and use shareable events. Learn more

Template - *optional*

hello-world

Event JSON

```
{
        "studentid": "1",
        "name": "Salma",
        "class":"A",
        "age": "24"
}
```



The test event **test** was successfully saved.

Code source Info

▾ Execution results

Status: Succeeded | Max memory used: 77 MB | Time: 558.86 ms

Test Event Name

test

Response

```
{
  "statusCode": 200,
  "body": "\"Student data saved successfully!\""
}
```

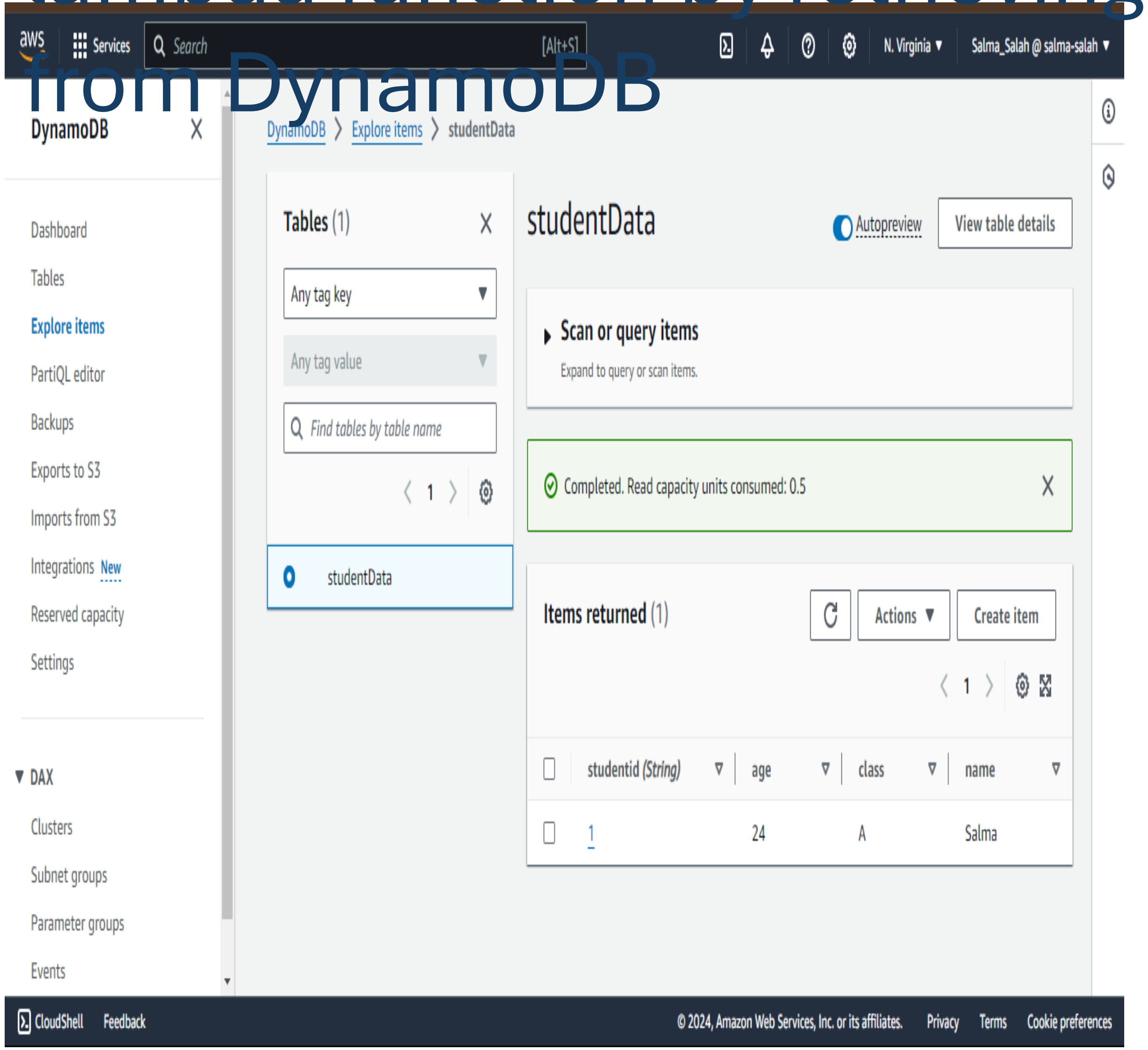
Function Logs

```
START RequestId: f6515977-76b0-4299-82ce-d8182ad2a3c4 Version: $LATEST
END RequestId: f6515977-76b0-4299-82ce-d8182ad2a3c4
REPORT RequestId: f6515977-76b0-4299-82ce-d8182ad2a3c4  Duration: 558.86 ms Billed Duration: 559 ms Memory Size: 128 MB Max Memory Used: 77 MB
```

Request ID

f6515977-76b0-4299-82ce-d8182ad2a3c4

Test the Execution of First (GET) lambda function by retrieving data from DynamoDB

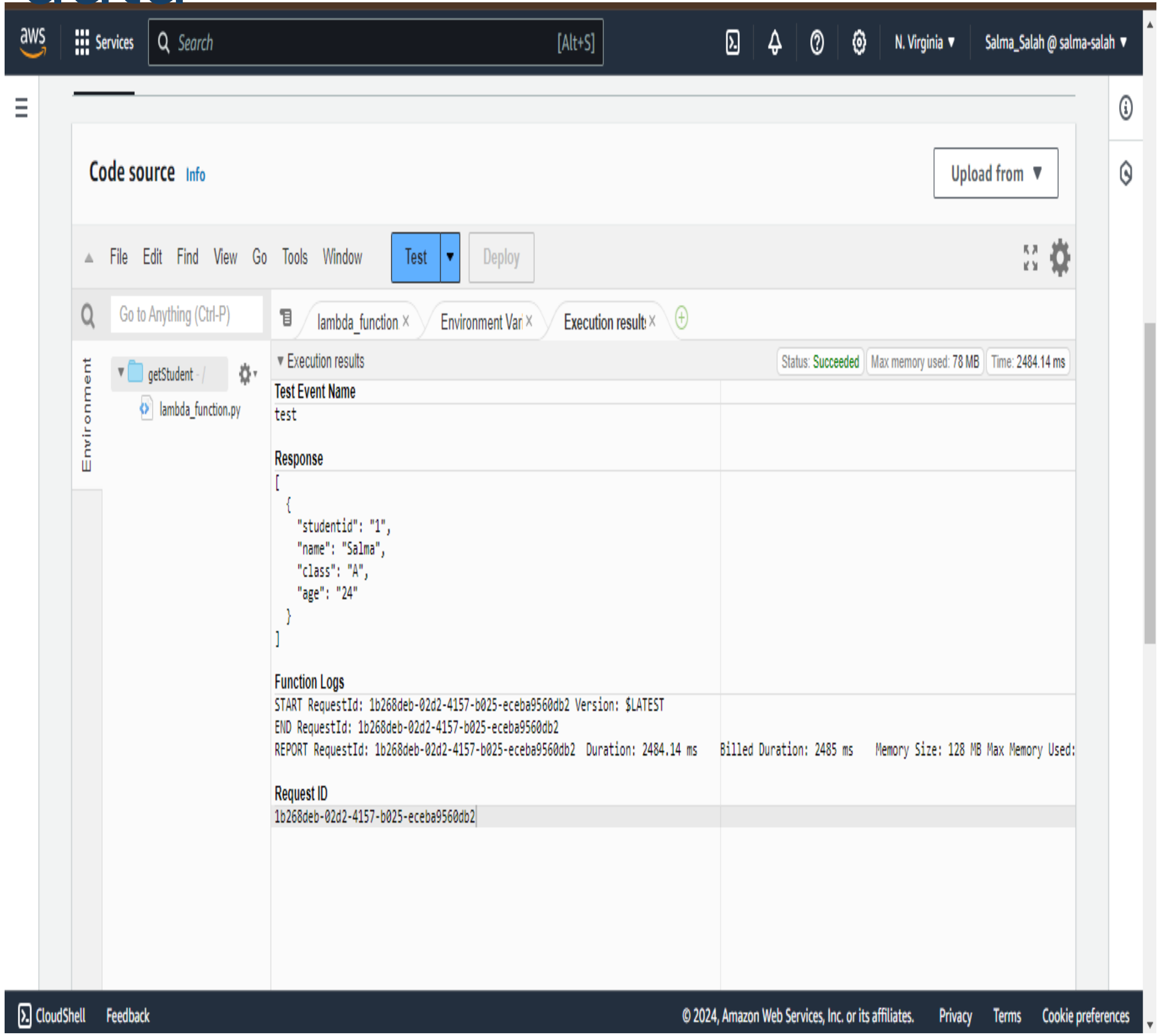


studentData

Completed. Read capacity units consumed: 0.5

Items returned (1)

□	studentid (String)	age	class	name
□	1	24	A	Salma



▾ Execution results

Status: Succeeded | Max memory used: 78 MB | Time: 2484.14 ms

Test Event Name

test

Response

```
[
  {
    "studentid": "1",
    "name": "Salma",
    "class": "A",
    "age": "24"
  }
]
```

Function Logs

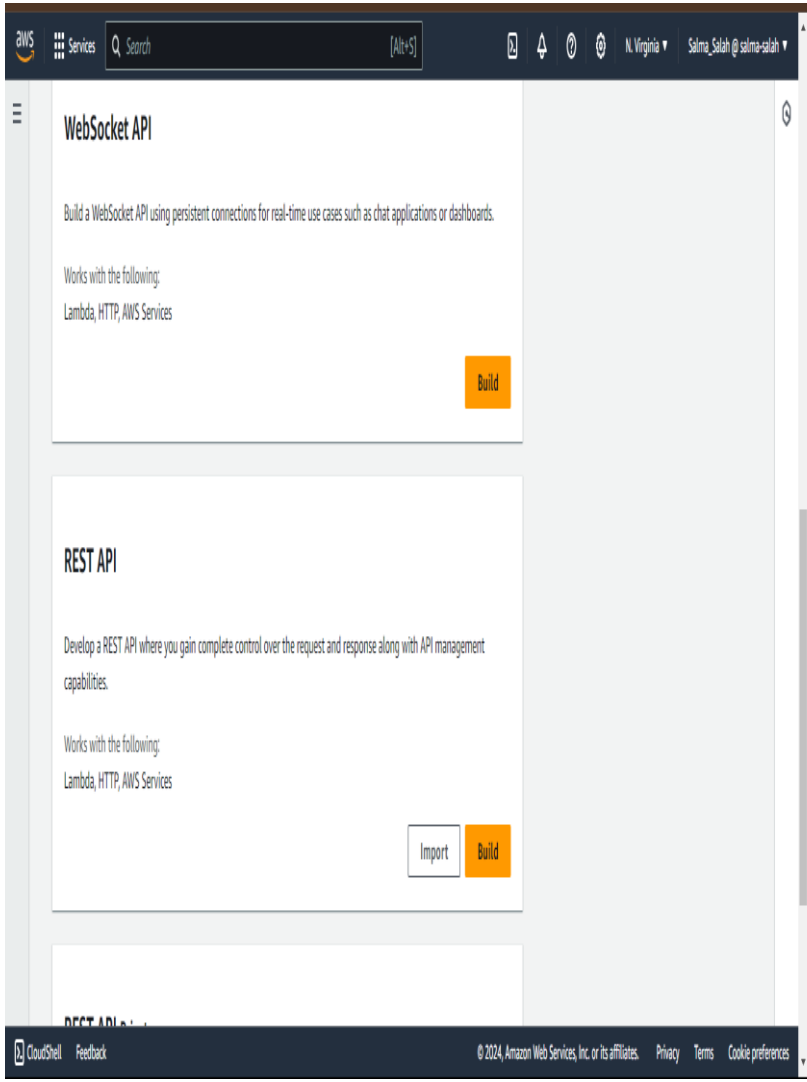
```
START RequestId: 1b268deb-02d2-4157-b025-eceba9560db2 Version: $LATEST
END RequestId: 1b268deb-02d2-4157-b025-eceba9560db2
REPORT RequestId: 1b268deb-02d2-4157-b025-eceba9560db2  Duration: 2484.14 ms   Billed Duration: 2485 ms   Memory Size: 128 MB Max Memory Used:
```

Request ID

1b268deb-02d2-4157-b025-eceba9560db2

Fourth

Creating REST API using API Gateway



WebSocket API

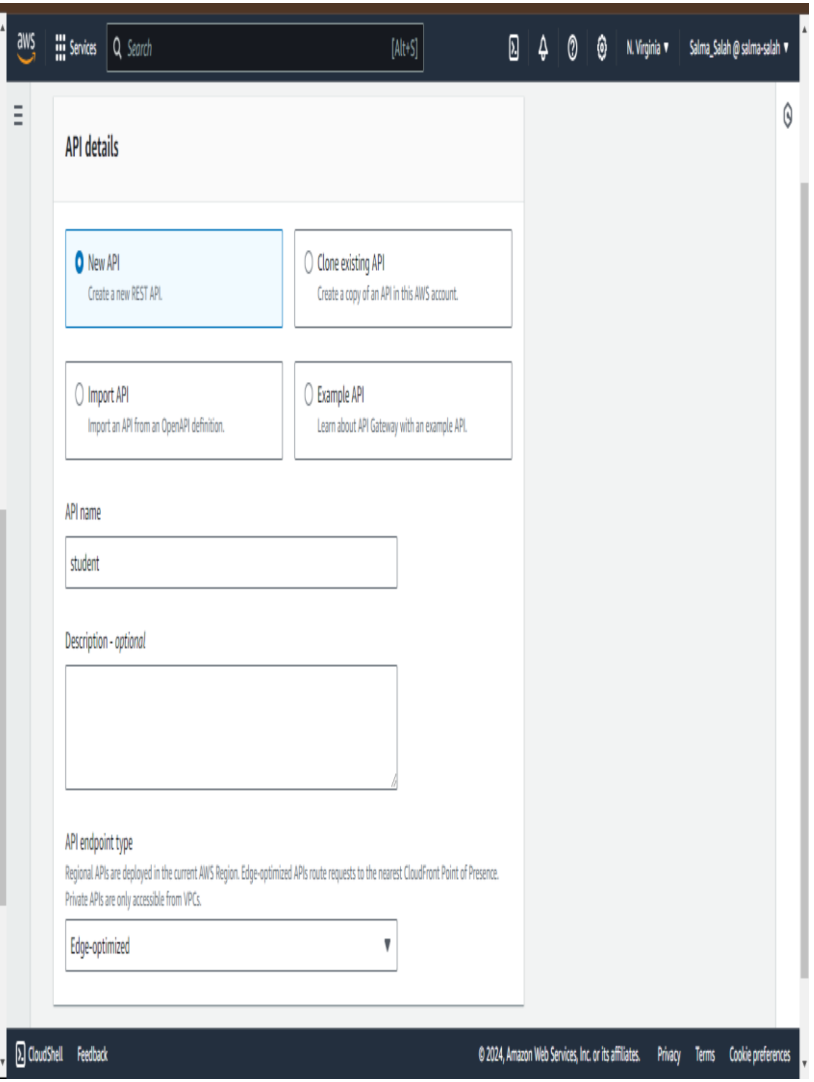
Build a WebSocket API using persistent connections for real-time use cases such as chat applications or dashboards.

Works with the following:
Lambda, HTTP, AWS Services

REST API

Develop a REST API where you gain complete control over the request and response along with API management capabilities.

Works with the following:
Lambda, HTTP, AWS Services



API details

● New API
Create a new REST API.

○ Clone existing API
Create a copy of an API in this AWS account.

○ Import API
Import an API from an OpenAPI definition.

○ Example API
Learn about API Gateway with an example API.

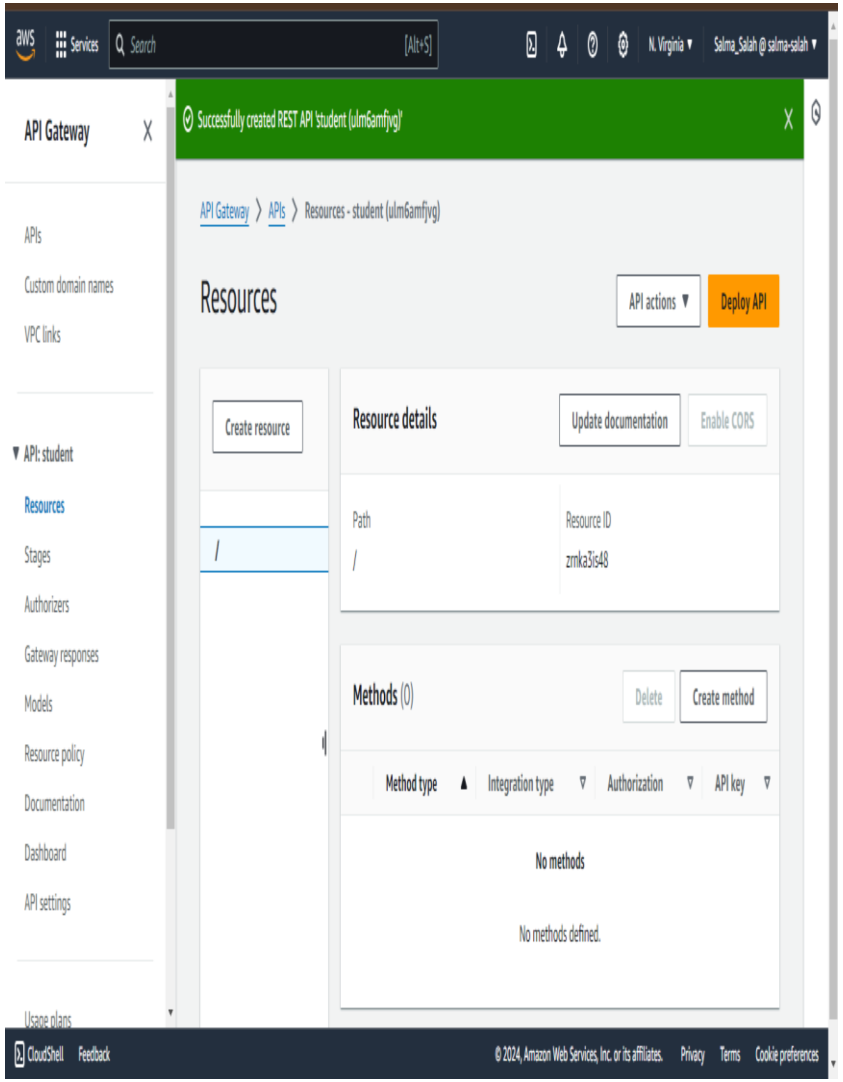
API name: student

Description - optional

API endpoint type

Regional APIs are deployed in the current AWS Region. Edge-optimized APIs route requests to the nearest CloudFront Point of Presence. Private APIs are only accessible from VPCs.

Edge-optimized ▾



Successfully created REST API 'student (ulm6amfjvg)'

API Gateway 〉 APIs 〉 Resources - student (ulm6amfjvg)

Resources

Resource details

Path: /

Resource ID: zmka3is48

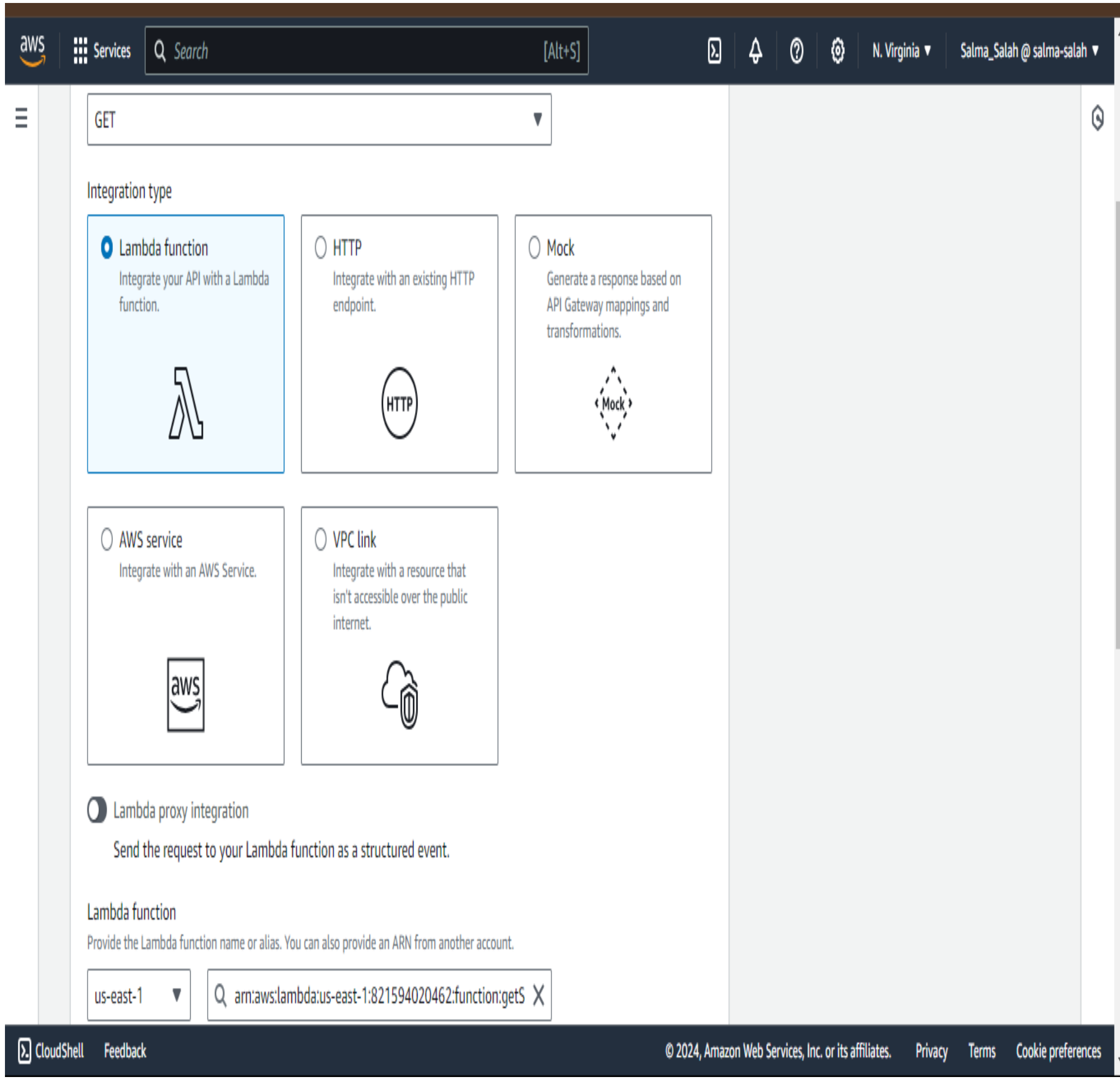
Methods (0)

Method type ▲	Integration type ▽	Authorization ▽	API key ▽

No methods

No methods defined.

Creating GET Method and checking that it’s working



GET ▾

Integration type

● Lambda function
Integrate your API with a Lambda function.

○ HTTP
Integrate with an existing HTTP endpoint.

○ Mock
Generate a response based on API Gateway mappings and transformations.

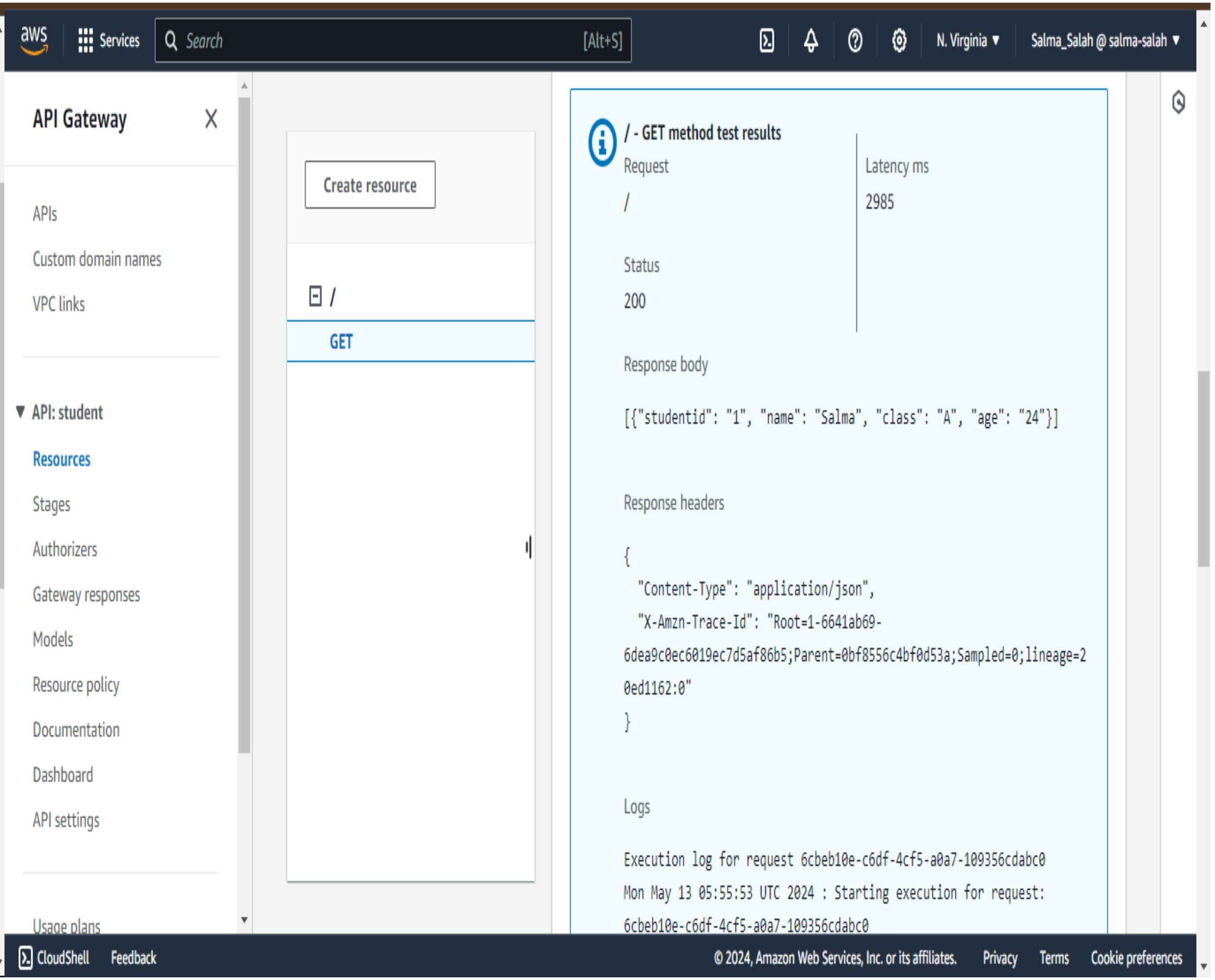
○ AWS service
Integrate with an AWS Service.

○ VPC link
Integrate with a resource that isn't accessible over the public internet.

Lambda proxy integration
Send the request to your Lambda function as a structured event.

Lambda function
Provide the Lambda function name or alias. You can also provide an ARN from another account.

us-east-1 ▾ | arn:aws:lambda:us-east-1:821594020462:function:getS X



/ - GET method test results

Request
/

Latency ms
2985

Status
200

Response body

```
[{"studentid": "1", "name": "Salma", "class": "A", "age": "24"}]
```

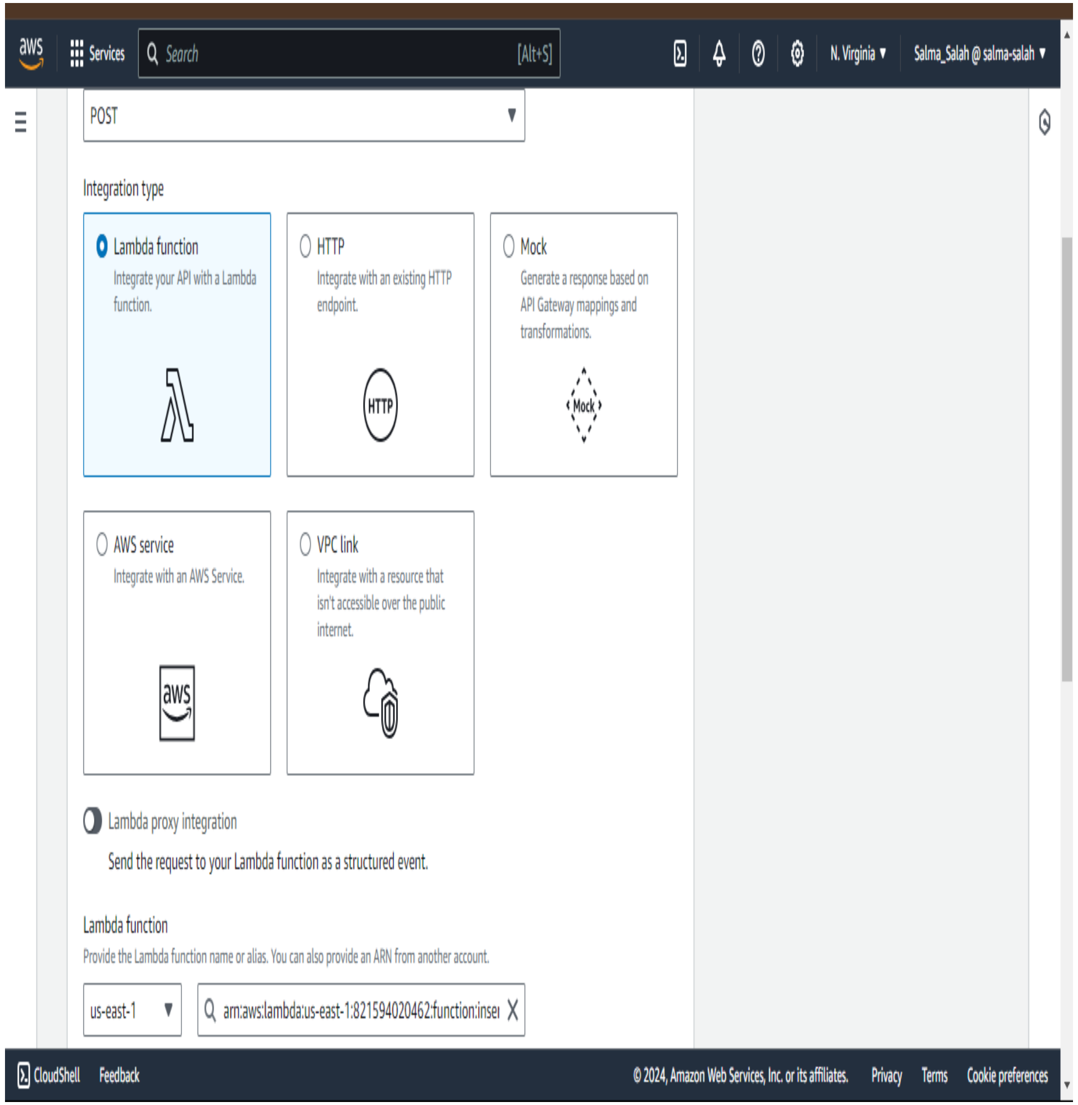
Response headers

```
{
  "Content-Type": "application/json",
  "X-Amzn-Trace-Id": "Root=1-6641ab69-
6dea9c0ec6019ec7d5af86b5;Parent=0bf8556c4bf0d53a;Sampled=0;lineage=2
0ed1162:0"
}
```

Logs

```
Execution log for request 6cbeb10e-c6df-4cf5-a0a7-109356cdabc0
Mon May 13 05:55:53 UTC 2024 : Starting execution for request:
6cbeb10e-c6df-4cf5-a0a7-109356cdabc0
```

Creating PUT Method and Post Method



POST ▼

Integration type

● Lambda function
Integrate your API with a Lambda function.

○ HTTP
Integrate with an existing HTTP endpoint.

○ Mock
Generate a response based on API Gateway mappings and transformations.

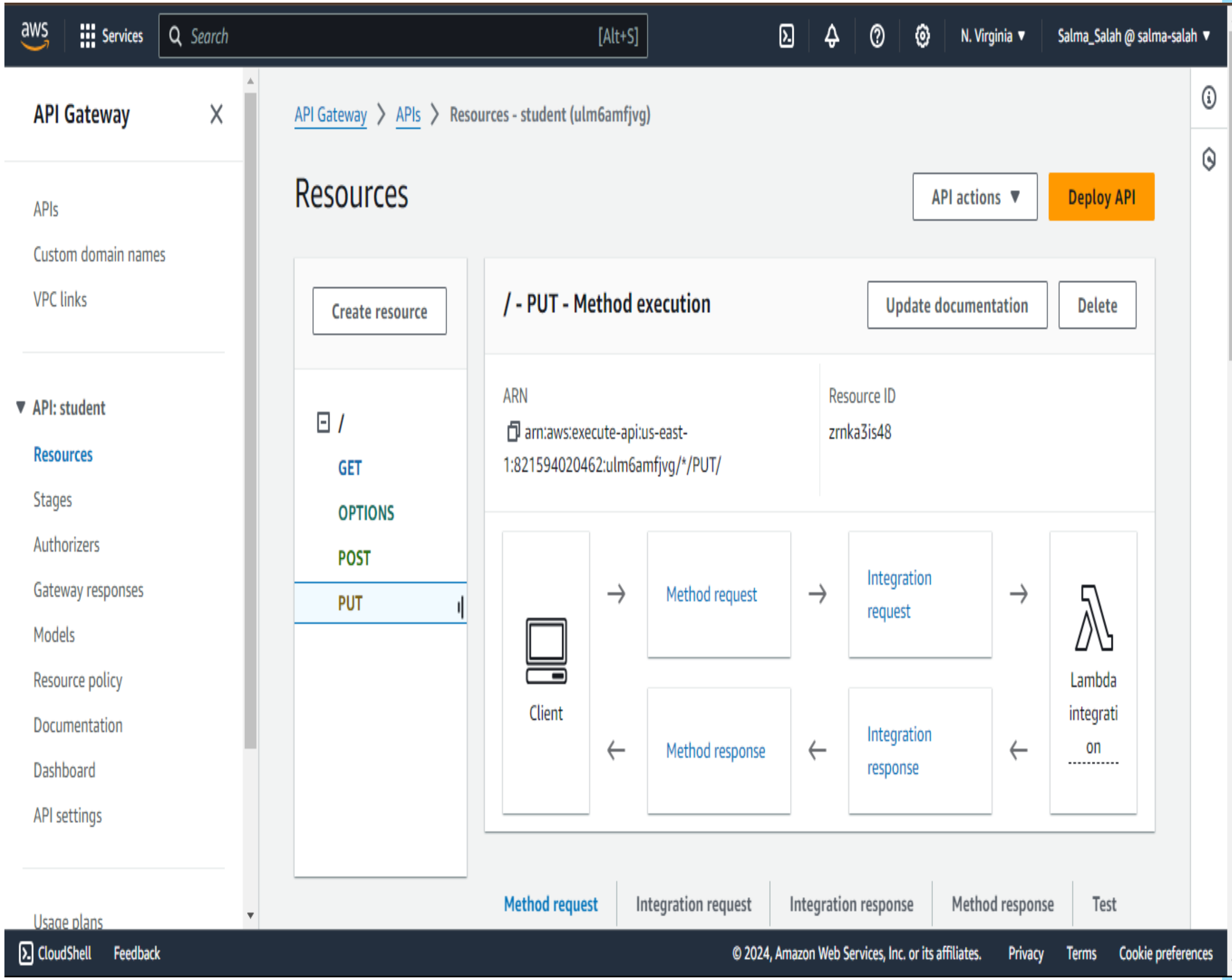
○ AWS service
Integrate with an AWS Service.

○ VPC link
Integrate with a resource that isn't accessible over the public internet.

Lambda proxy integration
Send the request to your Lambda function as a structured event.

Lambda function
Provide the Lambda function name or alias. You can also provide an ARN from another account.

us-east-1 ▼ arn:aws:lambda:us-east-1:821594020462:function:insei X



API Gateway > APIs > Resources - student (ulm6amfjvg)

Resources

/ - PUT - Method execution

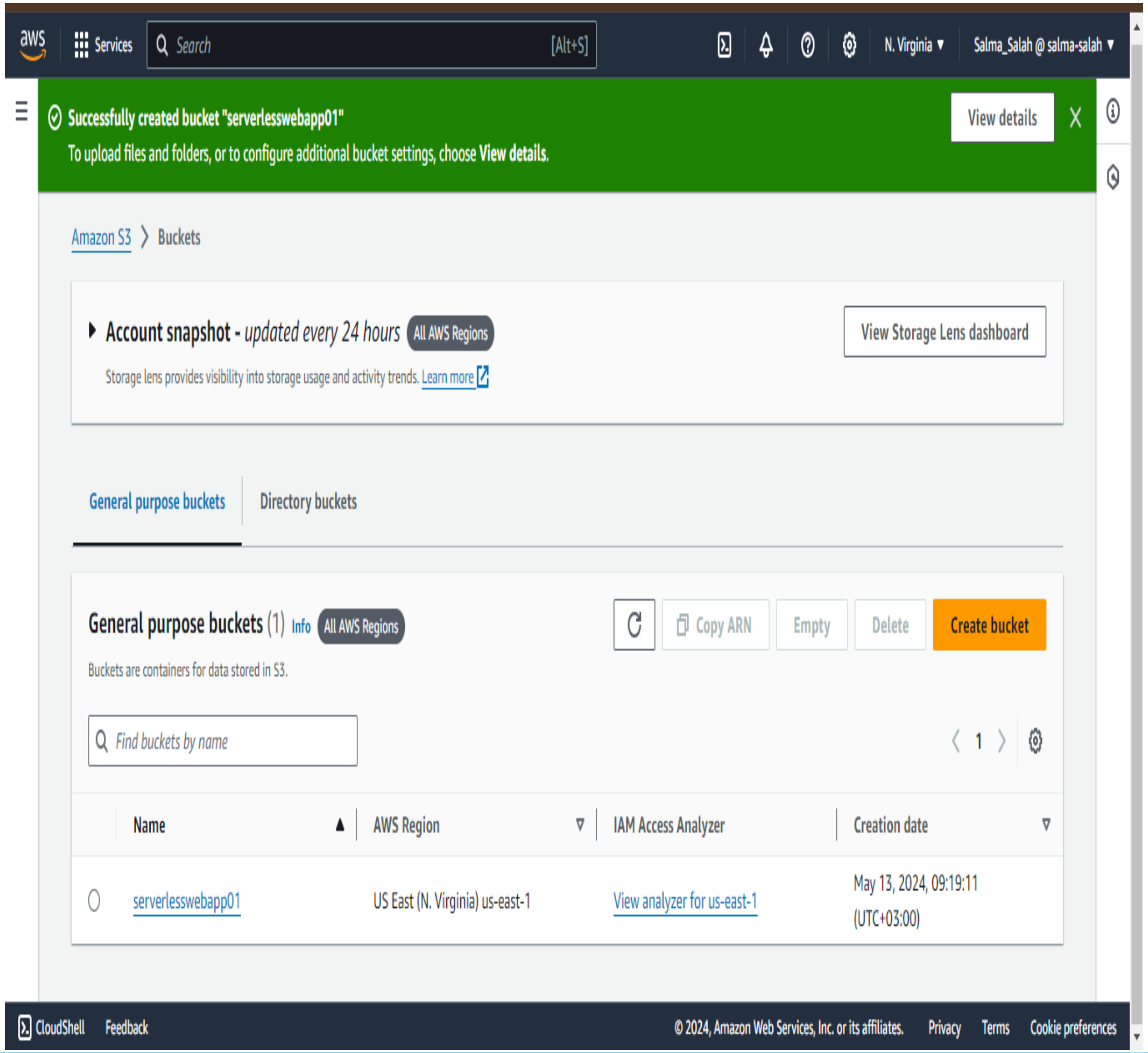
ARN
arn:aws:execute-api:us-east-1:821594020462:ulm6amfjvg/*/PUT/

Resource ID
zrnka3is48

Client → Method request → Integration request → Lambda integration
Client ← Method response ← Integration response ← Lambda integration

Fifth

Creating S3 Bucket and Uploading code files



Successfully created bucket "serverlesswebapp01"

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

Account snapshot - *updated every 24 hours* All AWS Regions

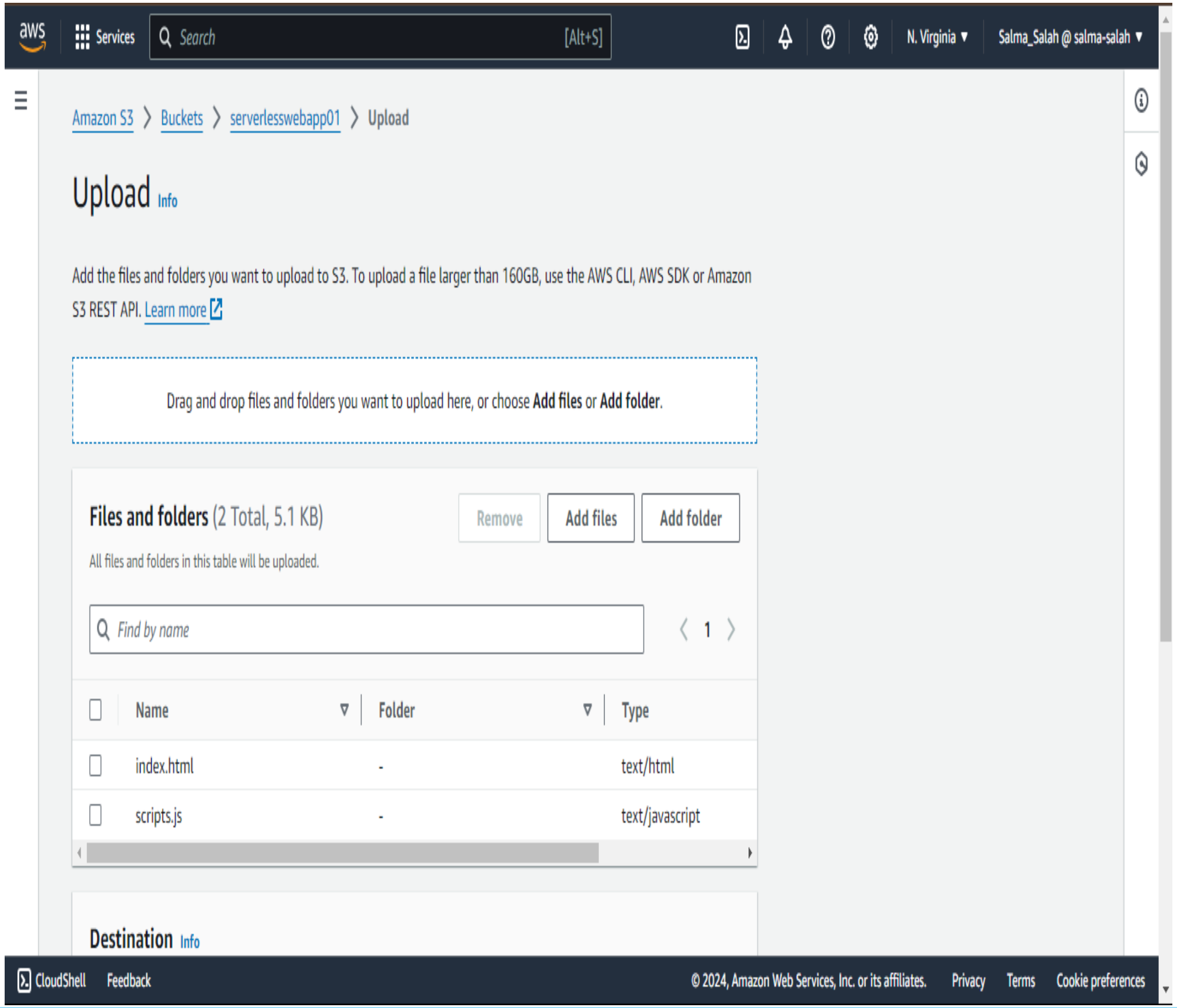
Storage lens provides visibility into storage usage and activity trends. Learn more

General purpose buckets (1) Info All AWS Regions

Buckets are containers for data stored in S3.

	Name	AWS Region	IAM Access Analyzer	Creation date
○	serverlesswebapp01	US East (N. Virginia) us-east-1	View analyzer for us-east-1	May 13, 2024, 09:19:11 (UTC+03:00)

© 2024, Amazon Web Services, Inc. or its affiliates.



Upload Info

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 folder**.

Files and folders (2 Total, 5.1 KB)

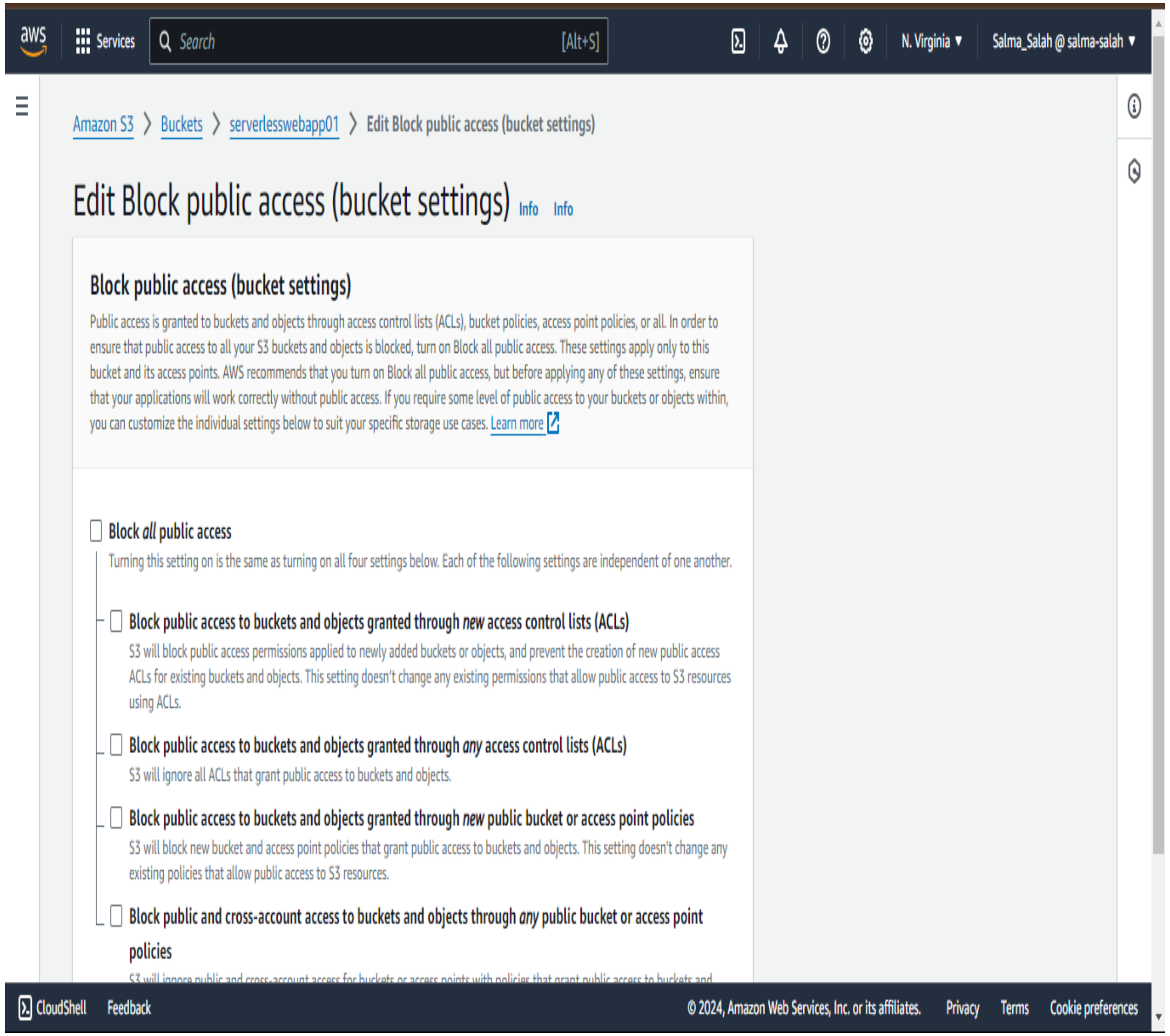
All files and folders in this table will be uploaded.

□	Name	Folder	Type
□	index.html	-	text/html
□	scripts.js	-	text/javascript

Destination Info

© 2024, Amazon Web Services, Inc. or its affiliates.

Enable Public Access and Static website hosting



Amazon S3 > Buckets > serverlesswebapp01 > Edit Block public access (bucket settings)

Edit Block public access (bucket settings) Info Info

Block public access (bucket settings)

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 all your S3 buckets and 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 your applications will work correctly without public access. If you require some level of public access to your buckets 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 resources using ACLs.

- □ Block public access to buckets and objects granted through *any* access control lists (ACLs)

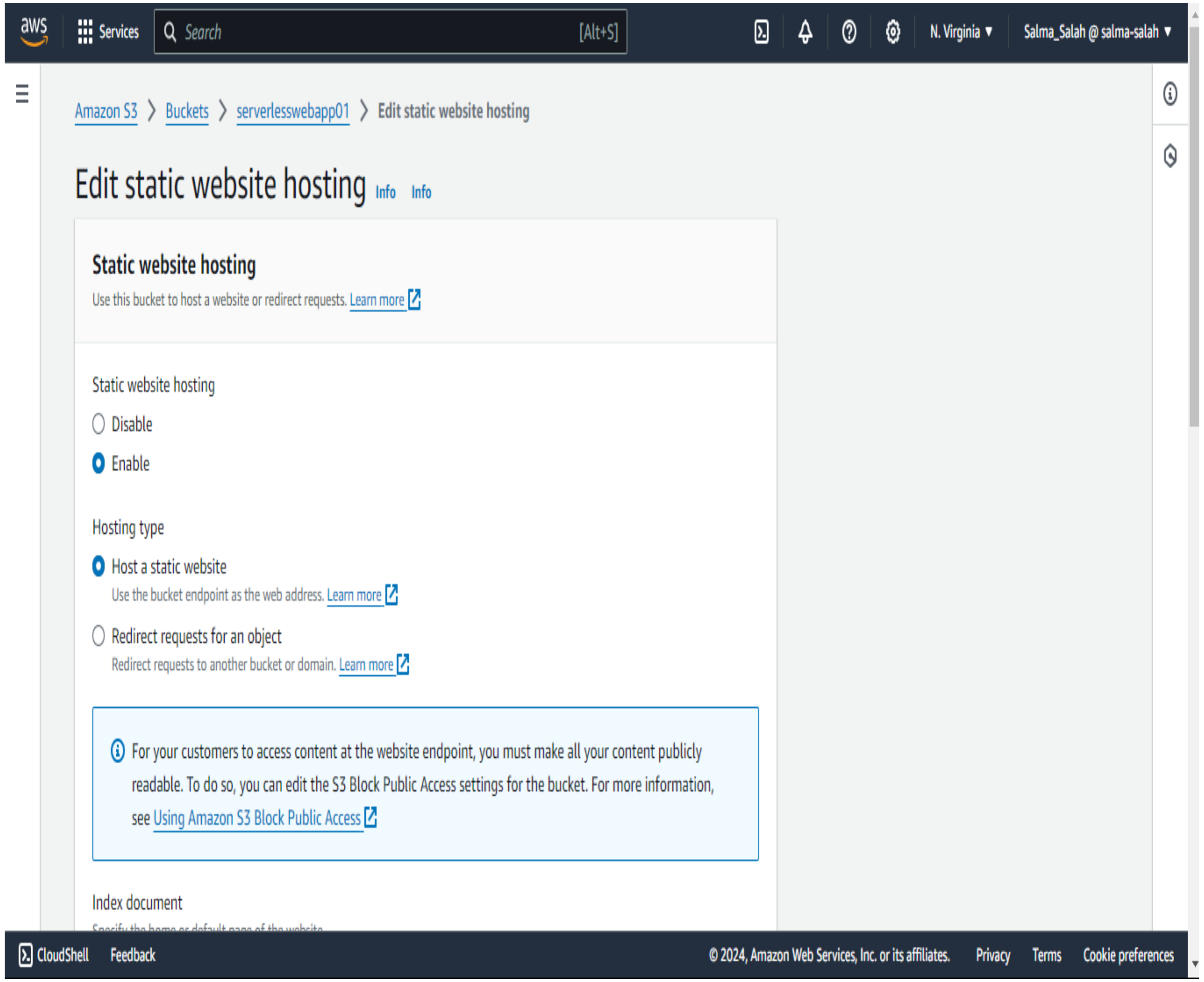
  S3 will ignore all ACLs that grant public access to buckets and objects.

- □ 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.

- □ 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



Amazon S3 > Buckets > serverlesswebapp01 > Edit static website hosting

Edit static website hosting Info Info

Static website hosting

Use this bucket to host a website or redirect requests. Learn more

Static website hosting

○ Disable

● Enable

Hosting type

● Host a static website

Use the bucket endpoint as the web address. Learn more

○ Redirect requests for an object

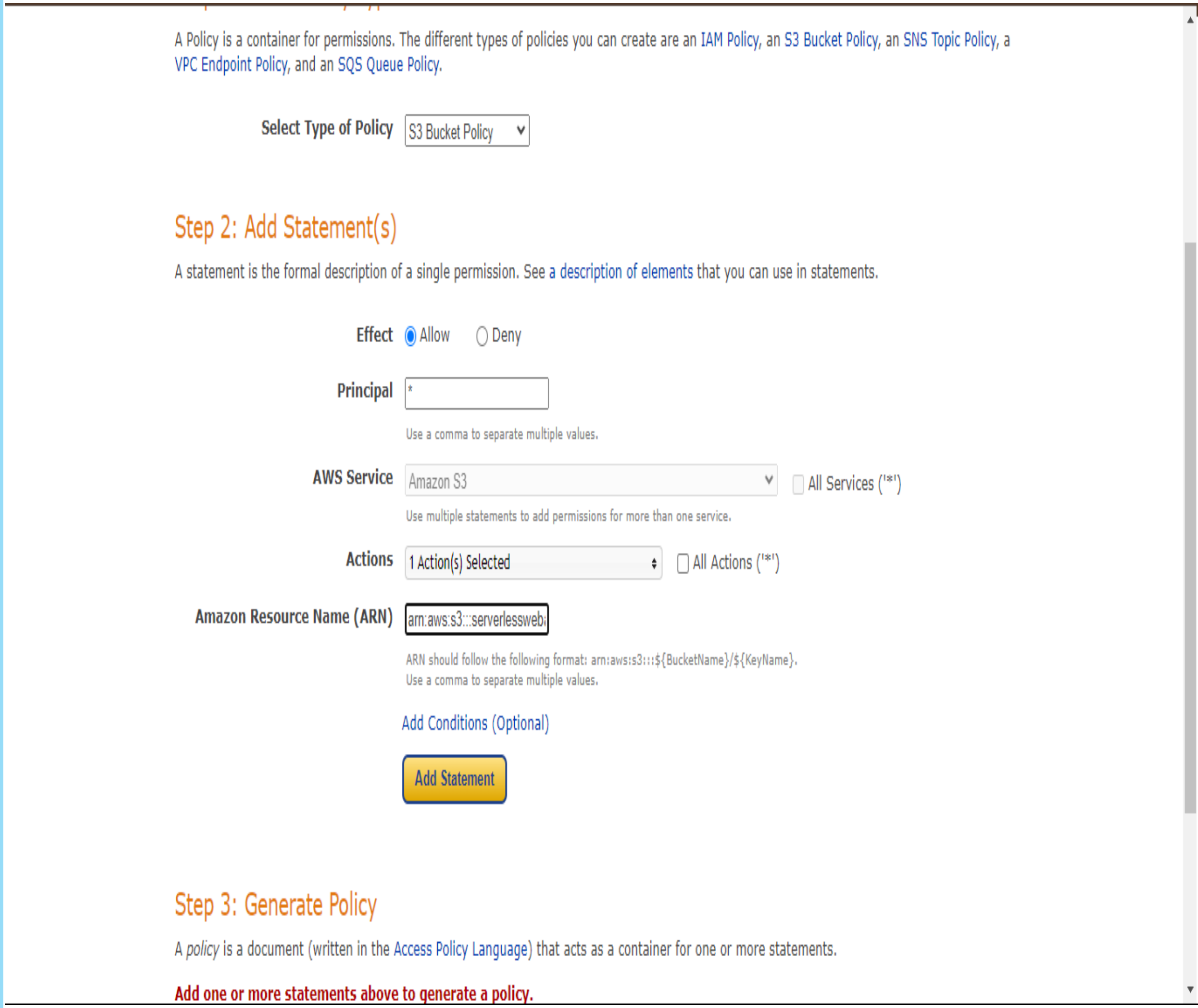
Redirect requests to another bucket or domain. Learn more

ⓘ For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access

Index document

Specify the home or default page of the website.

Generating Bucket Policy



A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy: S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect	● Allow ○ Deny
Principal	* Use a comma to separate multiple values.
AWS Service	Amazon S3 □ All Services ('*') Use multiple statements to add permissions for more than one service.
Actions	1 Action(s) Selected □ All Actions ('*')
Amazon Resource Name (ARN)	arn:aws:s3:::serverlessweb ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}. Use a comma to separate multiple values.

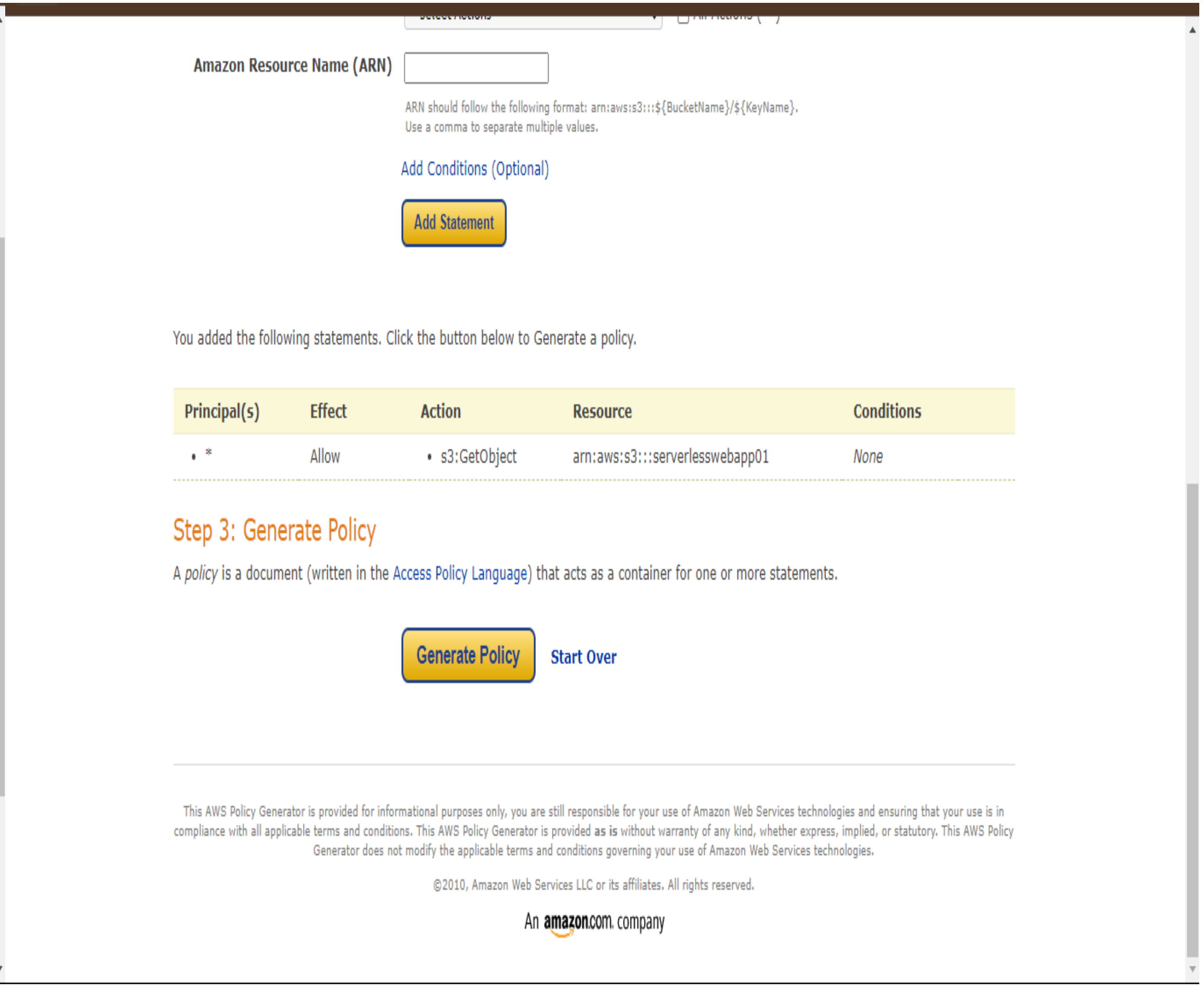
Add Conditions (Optional)

Add Statement

Step 3: Generate Policy

A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more statements.

Add one or more statements above to generate a policy.



Amazon Resource Name (ARN):

ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

Add Statement

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• *	Allow	• s3:GetObject	arn:aws:s3:::serverlesswebapp01	*None*

Step 3: Generate Policy

A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more statements.

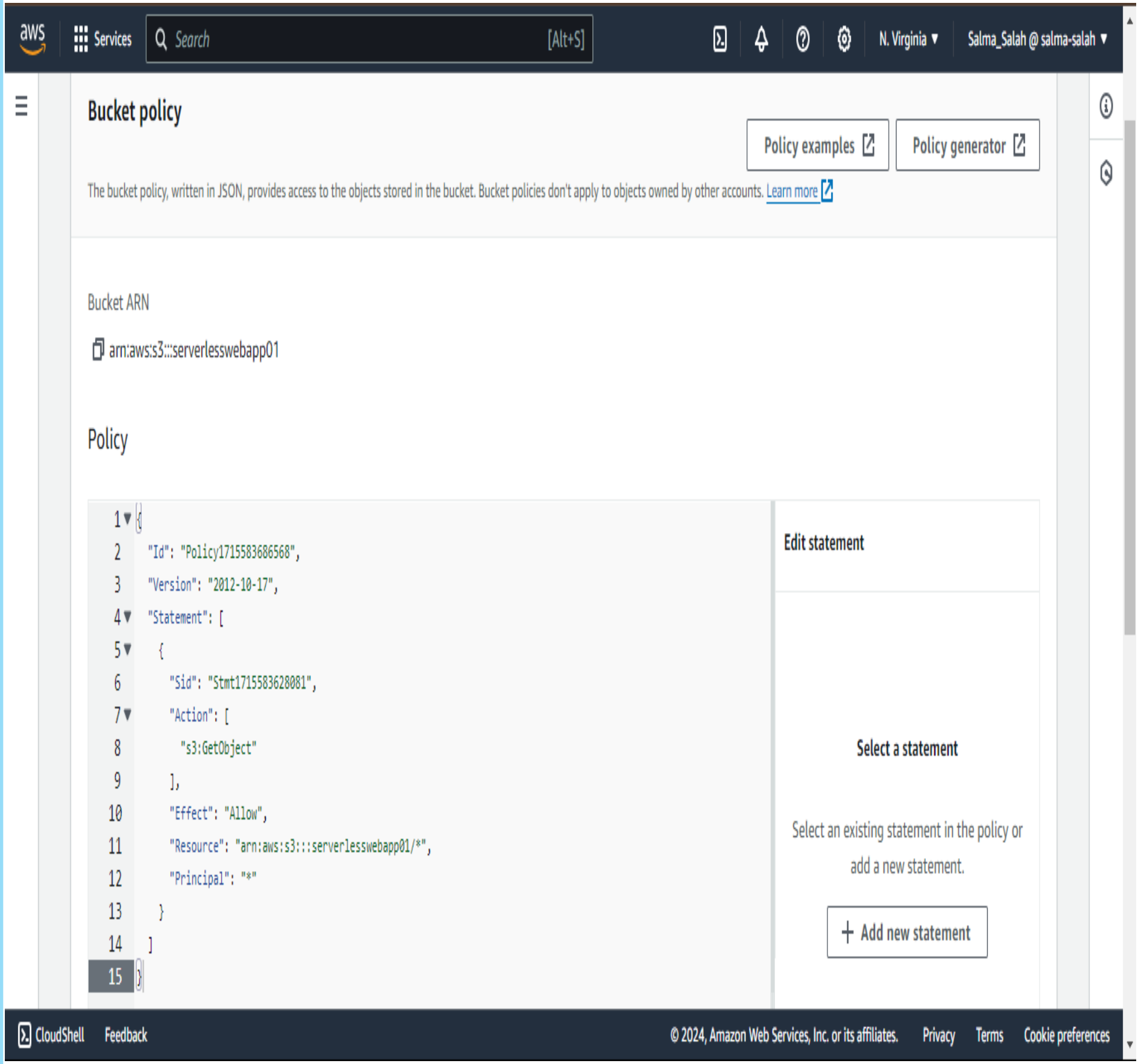
Generate Policy   Start Over

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided **as is** without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

©2010, Amazon Web Services LLC or its affiliates. All rights reserved.

An amazon.com. company

Adding Pucket Policy and Editing CORS in S3



Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

Bucket ARN

arn:aws:s3:::serverlesswebapp01

Policy

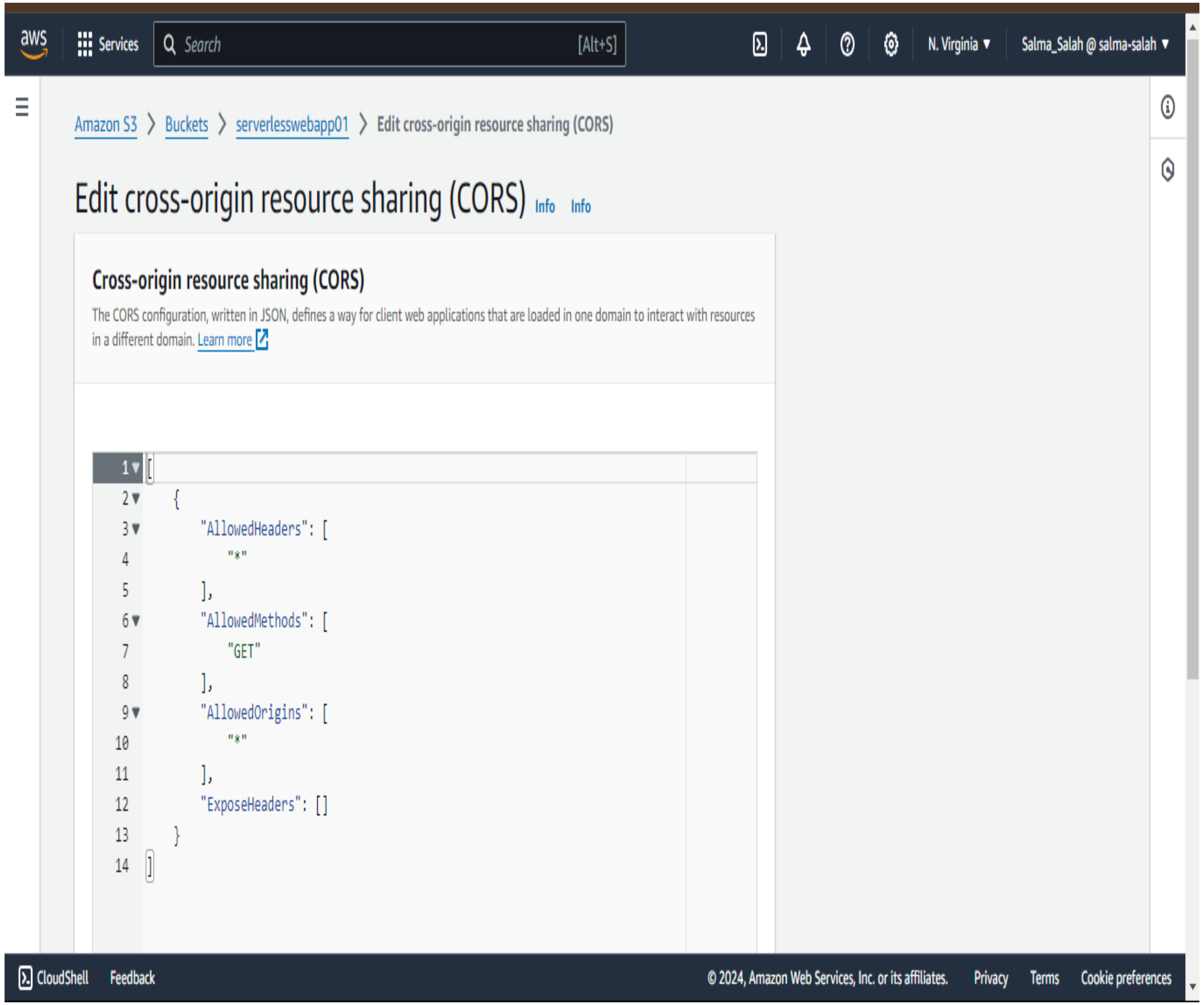
```
{
  "Id": "Policy1715583686568",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1715583628081",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::serverlesswebapp01/*",
      "Principal": "*"
    }
  ]
}
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



aws
Services
Search
[Alt+S]
N. Virginia ▾
Salma_Salah @ salma-salah ▾
Amazon S3 › Buckets › serverlesswebapp01 › Edit cross-origin resource sharing (CORS)

Edit cross-origin resource sharing (CORS) Info Info

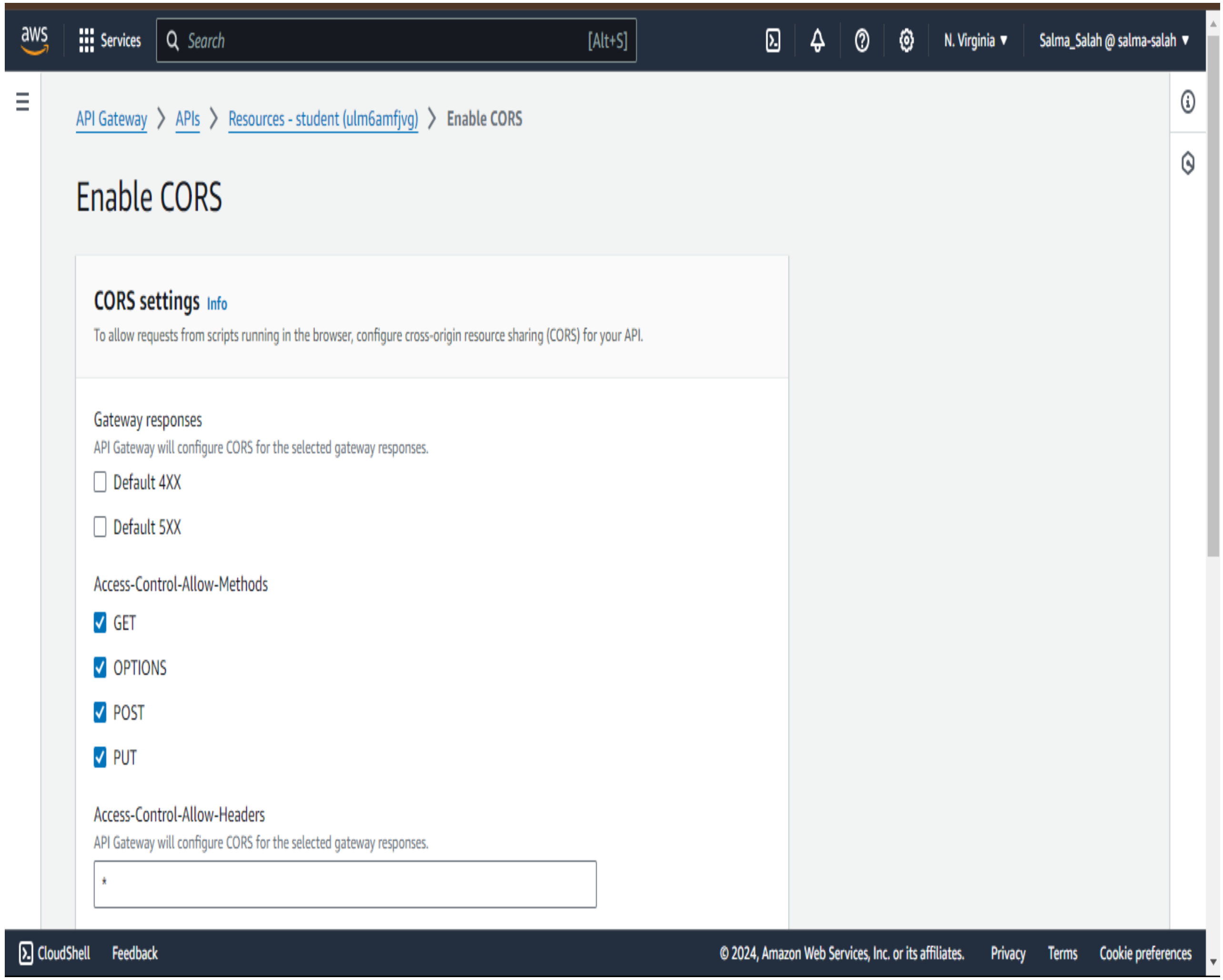
Cross-origin resource sharing (CORS)

The CORS configuration, written in JSON, defines a way for client web applications that are loaded in one domain to interact with resources in a different domain. Learn more

```
[
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "GET"
        ],
        "AllowedOrigins": [
            "*"
        ],
        "ExposeHeaders": []
    }
]
```

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

Enable CORS on API Gateway and adding S3 buckets's Endpoint as Origin



API Gateway > APIs > Resources - student (ulm6amfjvg) > Enable CORS

Enable CORS

CORS settings Info

To allow requests from scripts running in the browser, configure cross-origin resource sharing (CORS) for your API.

Gateway responses

API Gateway will configure CORS for the selected gateway responses.

□ Default 4XX

□ Default 5XX

Access-Control-Allow-Methods

☑ GET

☑ OPTIONS

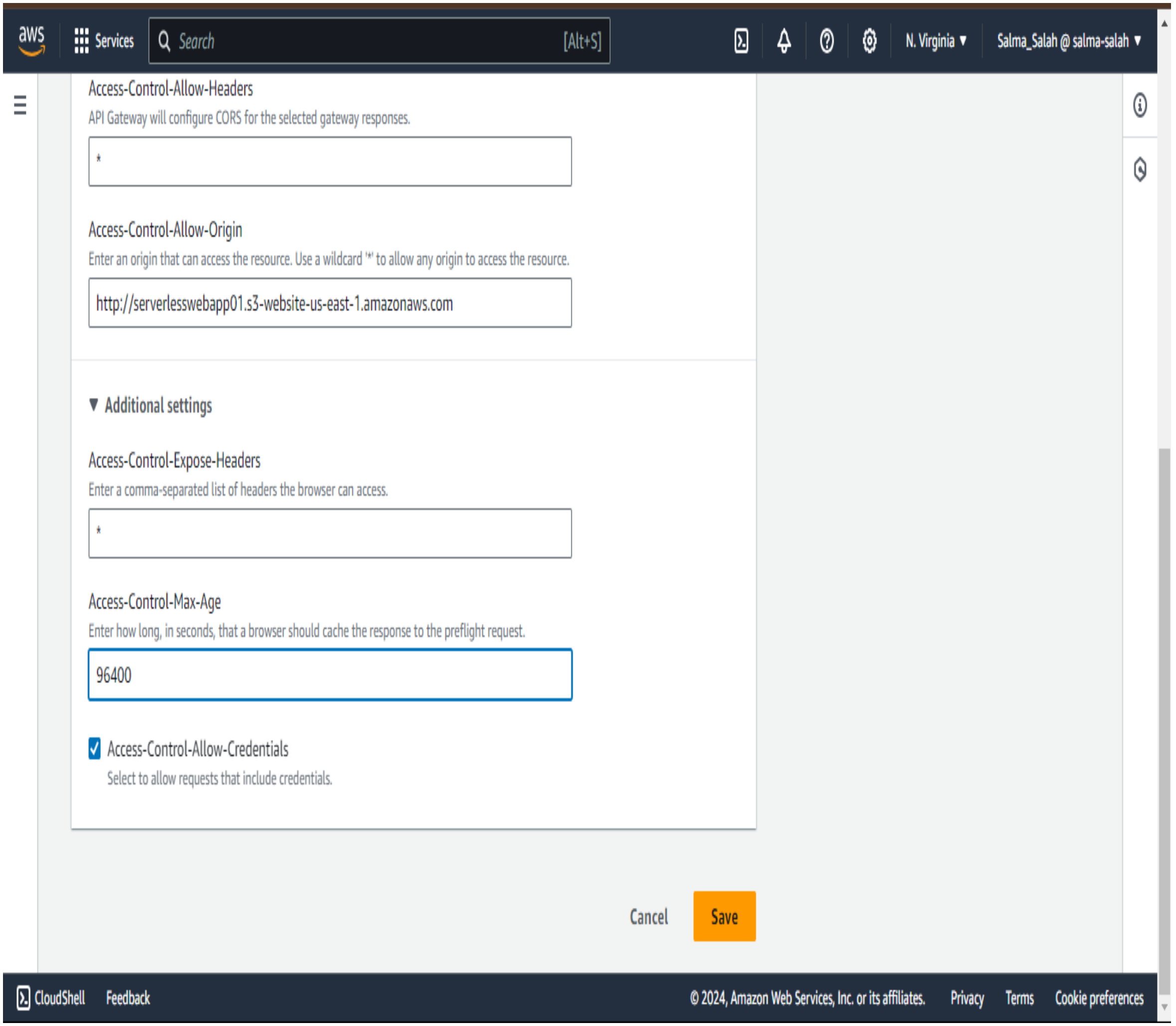
☑ POST

☑ PUT

Access-Control-Allow-Headers

API Gateway will configure CORS for the selected gateway responses.

*



Access-Control-Allow-Headers

API Gateway will configure CORS for the selected gateway responses.

*

Access-Control-Allow-Origin

Enter an origin that can access the resource. Use a wildcard '*' to allow any origin to access the resource.

http://serverlesswebapp01.s3-website-us-east-1.amazonaws.com

▼ Additional settings

Access-Control-Expose-Headers

Enter a comma-separated list of headers the browser can access.

*

Access-Control-Max-Age

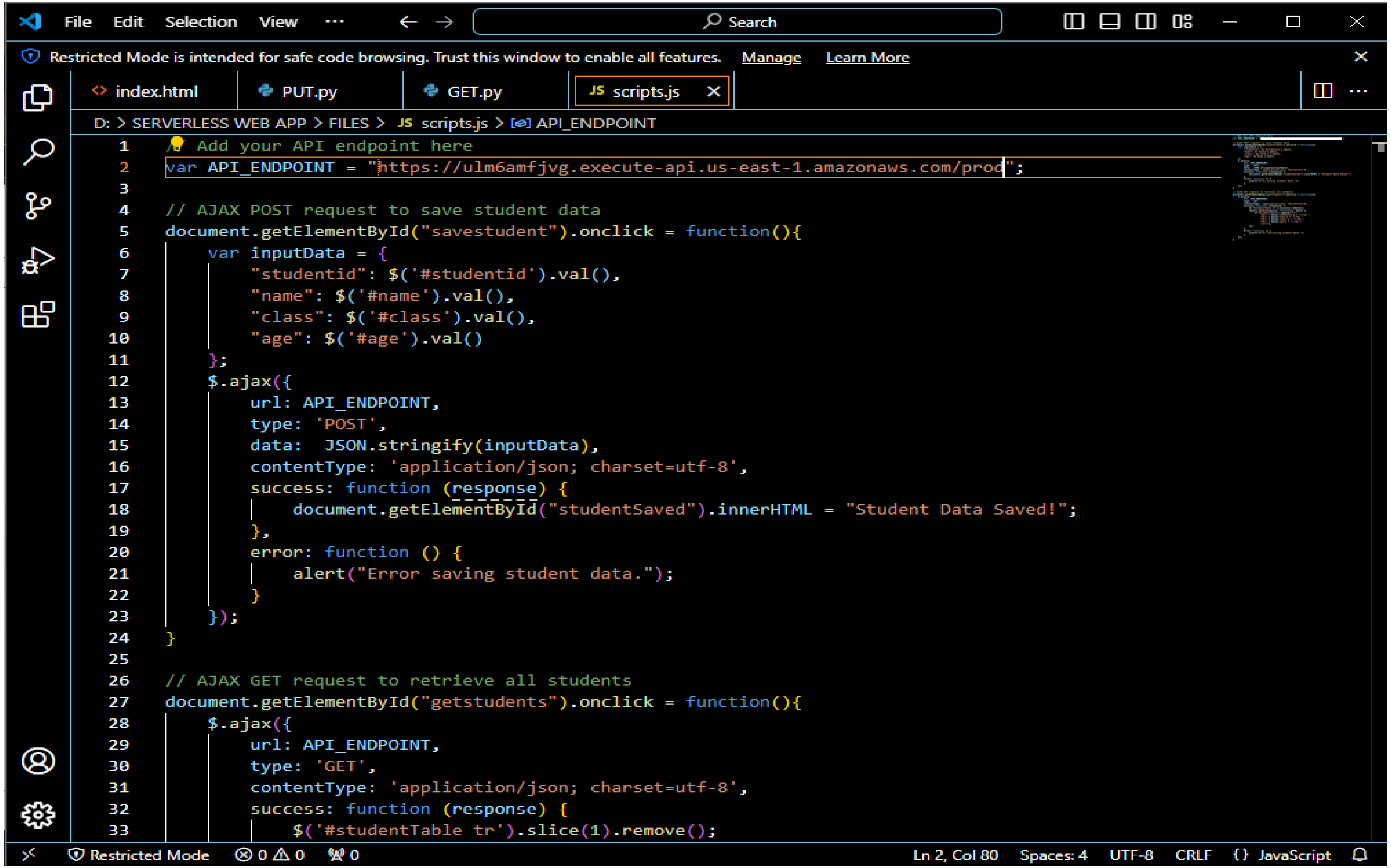
Enter how long, in seconds, that a browser should cache the response to the preflight request.

96400

☑ Access-Control-Allow-Credentials

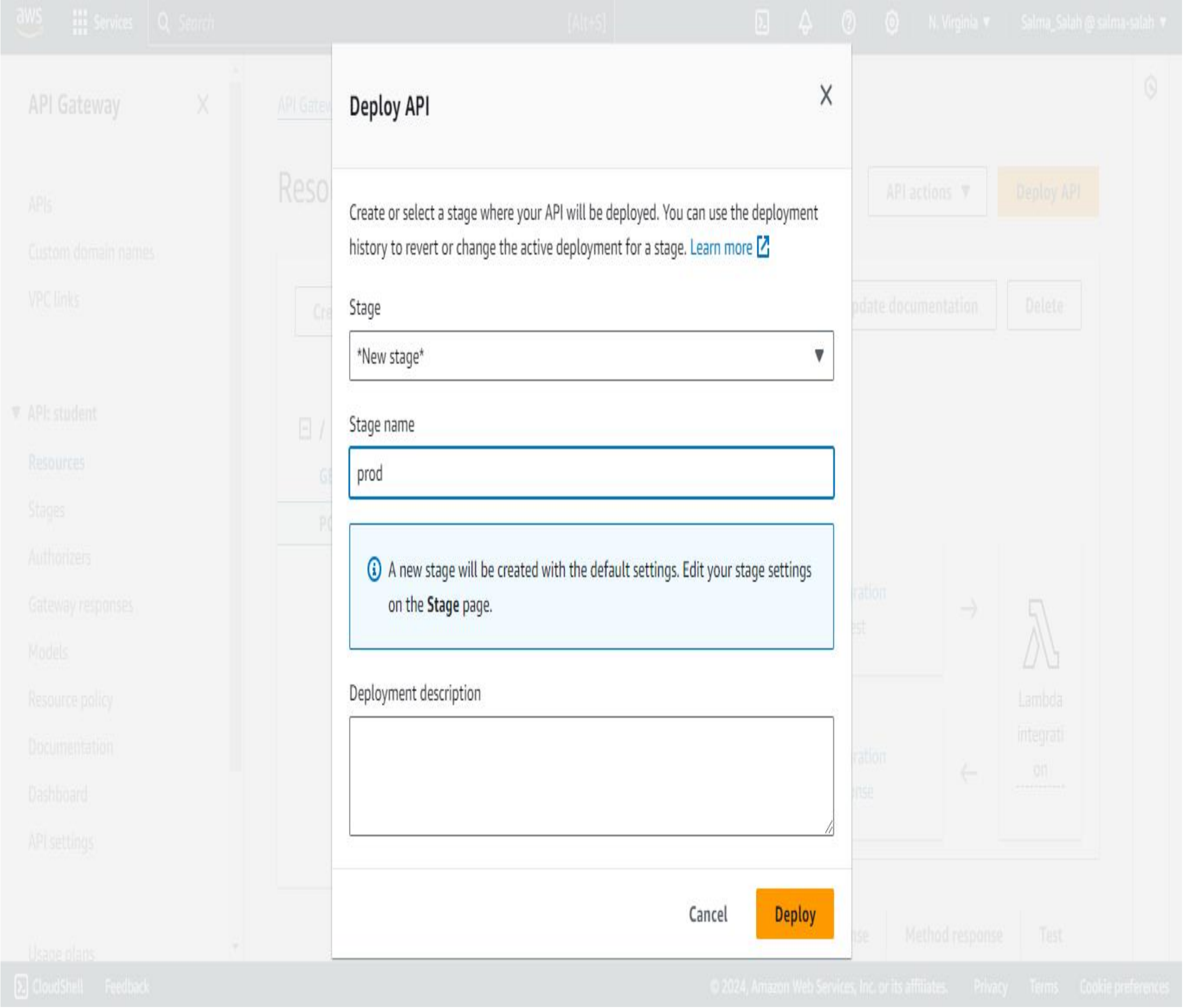
Select to allow requests that include credentials.

Adding API EndPoint in backend code


File
Edit
Selection
View
Search
Restricted Mode is intended for safe code browsing. Trust this window to enable all features.
Manage
Learn More
index.html
PUT.py
GET.py
scripts.js
D: > SERVERLESS WEB APP > FILES > scripts.js > API_ENDPOINT
Restricted Mode
0 0
0
Ln 2, Col 80
Spaces: 4
UTF-8
CRLF
JavaScript

```javascript
// Add your API endpoint here
var API_ENDPOINT = "https://ulm6amfjvg.execute-api.us-east-1.amazonaws.com/prod";

// AJAX POST request to save student data
document.getElementById("savestudent").onclick = function(){
    var inputData = {
        "studentid": $('#studentid').val(),
        "name": $('#name').val(),
        "class": $('#class').val(),
        "age": $('#age').val()
    };
    $.ajax({
        url: API_ENDPOINT,
        type: 'POST',
        data:  JSON.stringify(inputData),
        contentType: 'application/json; charset=utf-8',
        success: function (response) {
            document.getElementById("studentSaved").innerHTML = "Student Data Saved!";
        },
        error: function () {
            alert("Error saving student data.");
        }
    });
}

// AJAX GET request to retrieve all students
document.getElementById("getstudents").onclick = function(){
    $.ajax({
        url: API_ENDPOINT,
        type: 'GET',
        contentType: 'application/json; charset=utf-8',
        success: function (response) {
            $('#studentTable tr').slice(1).remove();
```

Deploying API



Deploy API X

Create or select a stage where your API will be deployed. You can use the deployment history to revert or change the active deployment for a stage. Learn more

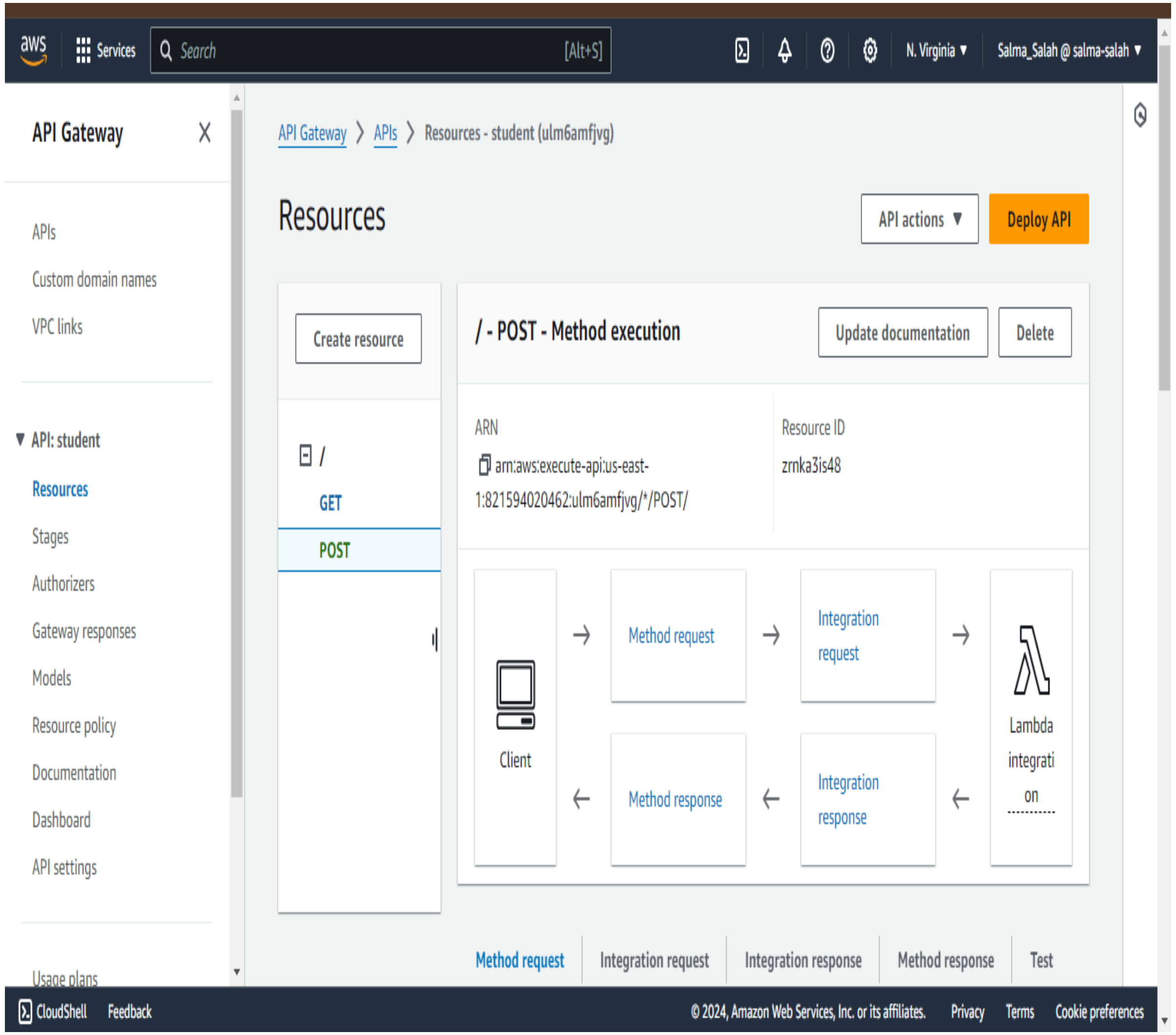
Stage: *New stage* ▼

Stage name: prod

ⓘ A new stage will be created with the default settings. Edit your stage settings on the **Stage** page.

Deployment description:

Cancel | Deploy



API Gateway X

- APIs
- Custom domain names
- VPC links
- ▼ API: student
  - Resources
  - Stages
  - Authorizers
  - Gateway responses
  - Models
  - Resource policy
  - Documentation
  - Dashboard
  - API settings
- Usage plans

API Gateway > APIs > Resources - student (ulm6amfjvg)

Resources

API actions ▼ | Deploy API

Create resource

- /
  - GET
  - POST

/ - POST - Method execution

Update documentation | Delete

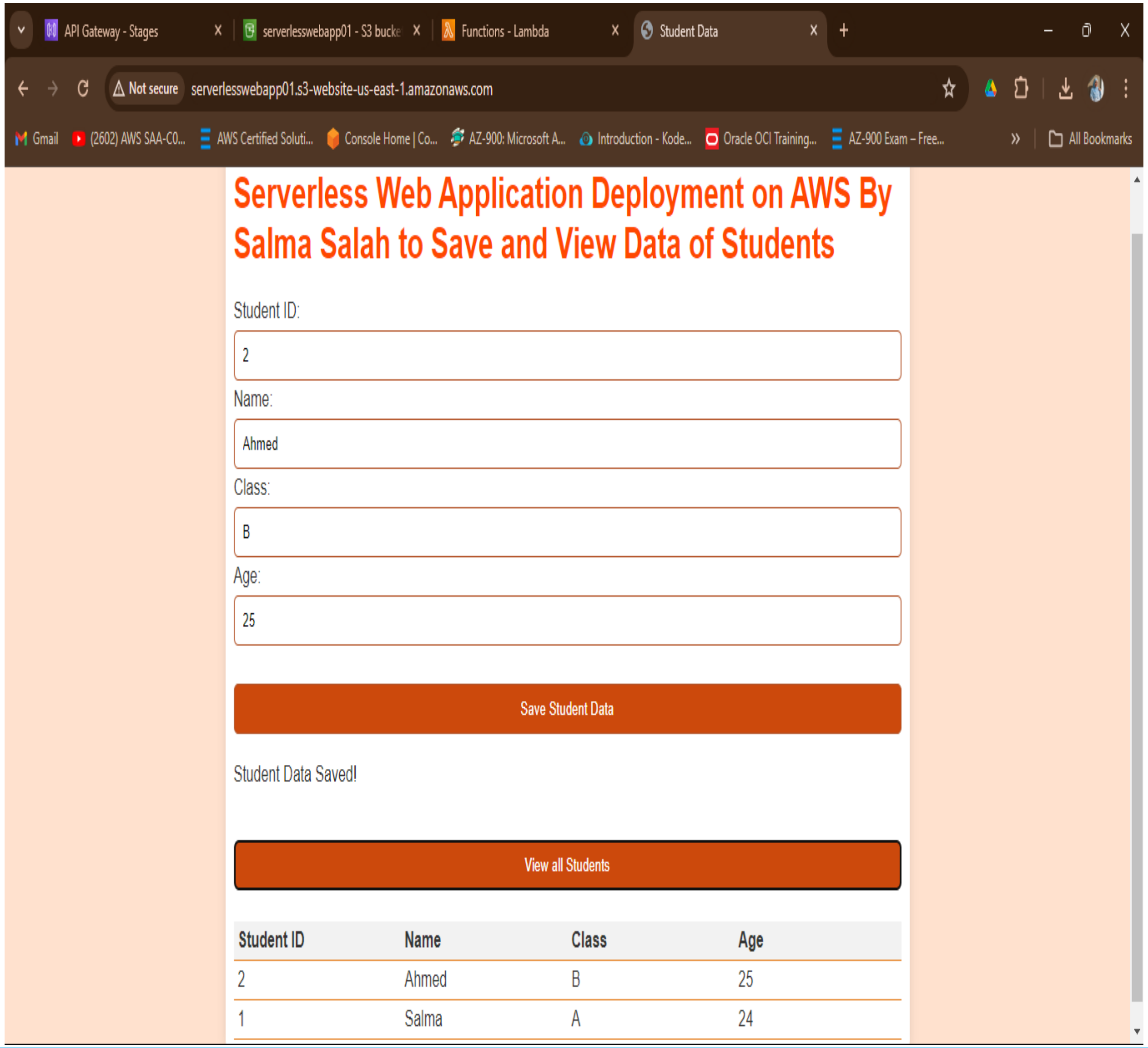
ARN: arn:aws:execute-api:us-east-1:821594020462:ulm6amfjvg/*/POST/

Resource ID: zmka3is48

Client
→ Method request → Integration request → Lambda integration
← Method response ← Integration response ←

Method request | Integration request | Integration response | Method response | Test

Testing the Application and it’s successfully working and adding new records and retrieving all records



Serverless Web Application Deployment on AWS By Salma Salah to Save and View Data of Students

Student ID: 2

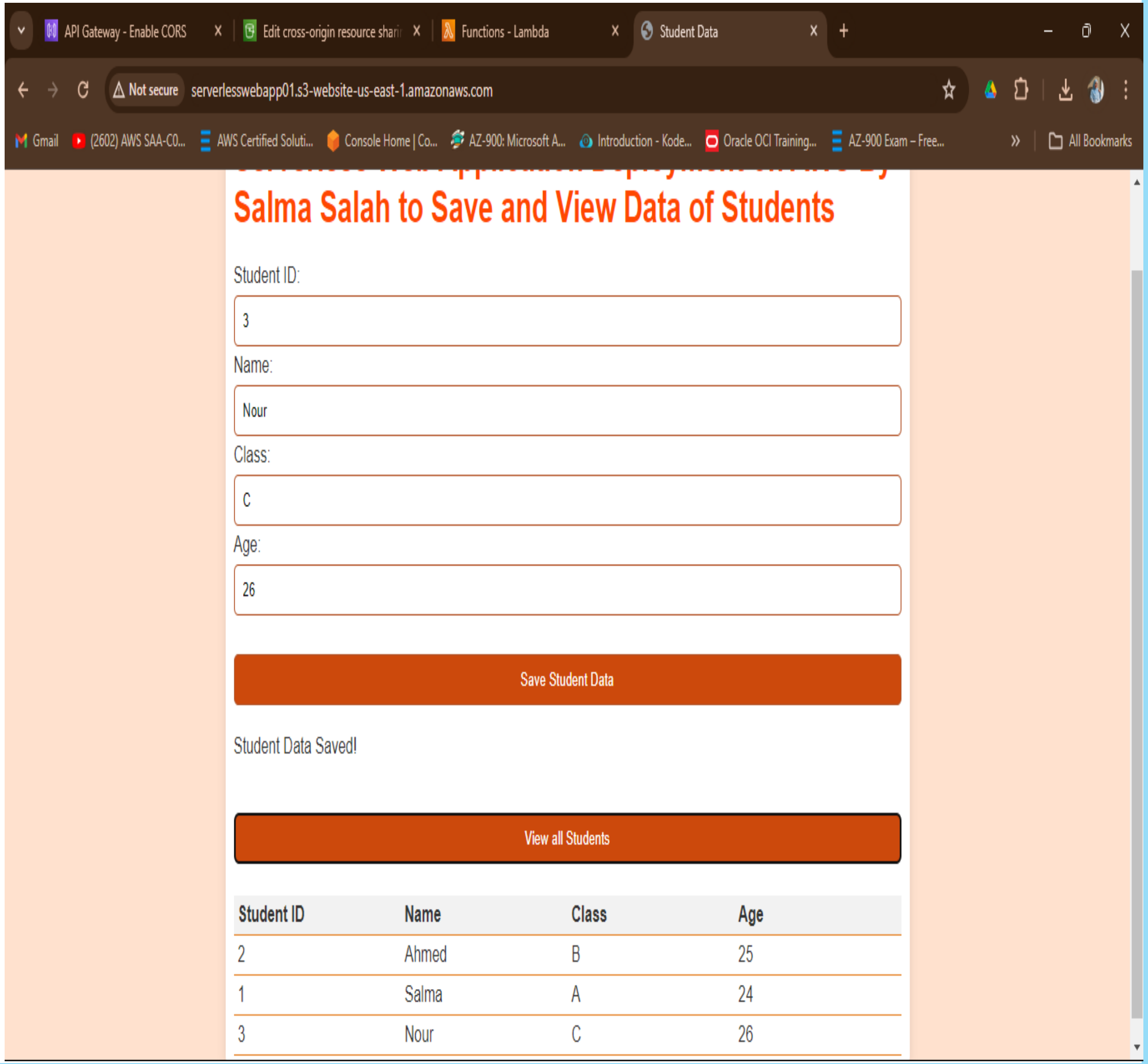
Name: Ahmed

Class: B

Age: 25

Student Data Saved!

Student ID	Name	Class	Age
2	Ahmed	B	25
1	Salma	A	24



Salma Salah to Save and View Data of Students

Student ID: 3

Name: Nour

Class: C

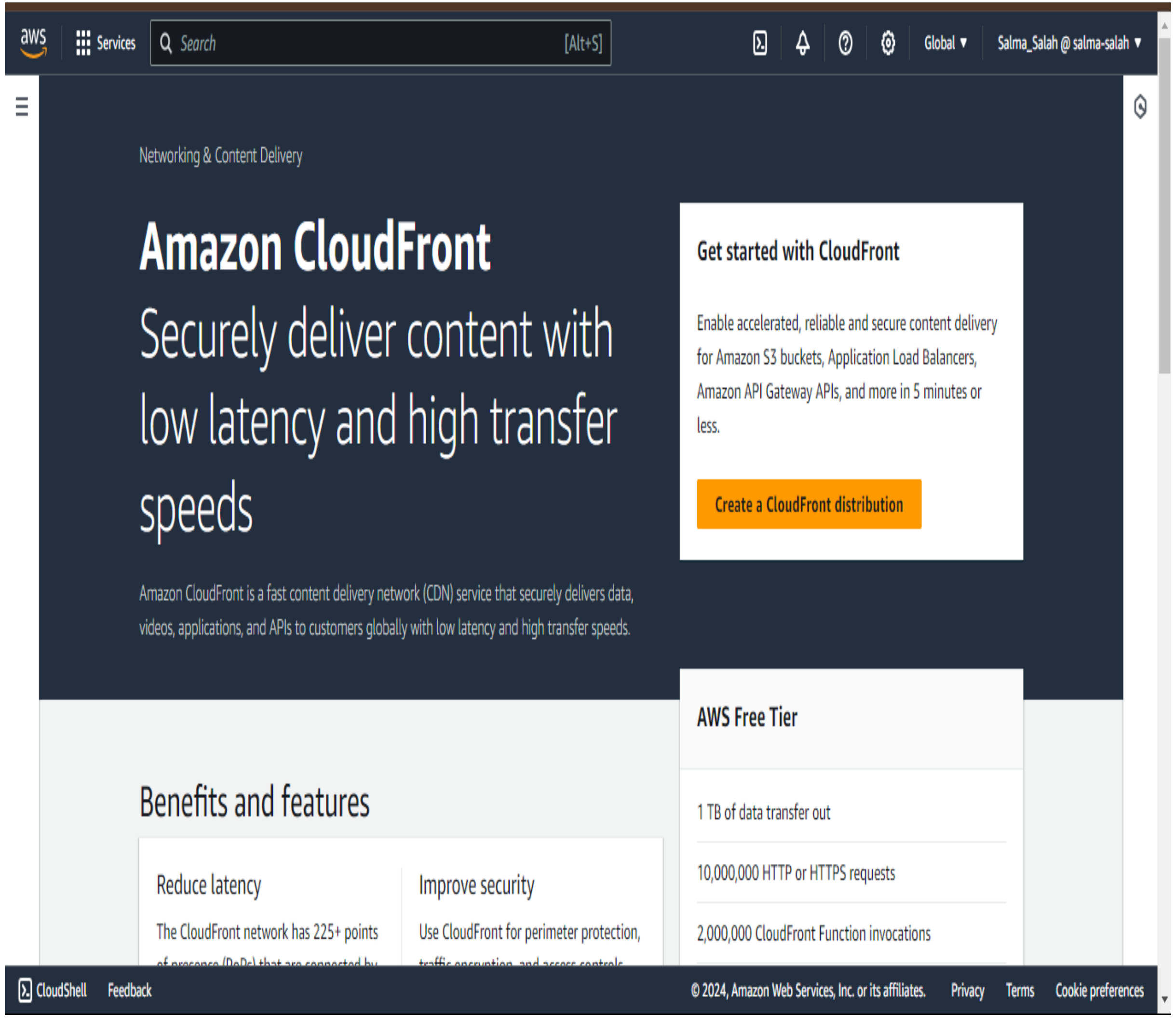
Age: 26

Student Data Saved!

Student ID	Name	Class	Age
2	Ahmed	B	25
1	Salma	A	24
3	Nour	C	26

Last Step

Creating Cloud Front Distribution to make the Connection Secured (HTTPS)



Networking & Content Delivery

Amazon CloudFront

Securely deliver content with low latency and high transfer speeds

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.

Get started with CloudFront

Enable accelerated, reliable and secure content delivery for Amazon S3 buckets, Application Load Balancers, Amazon API Gateway APIs, and more in 5 minutes or less.

AWS Free Tier

1 TB of data transfer out

10,000,000 HTTP or HTTPS requests

2,000,000 CloudFront Function invocations

Benefits and features

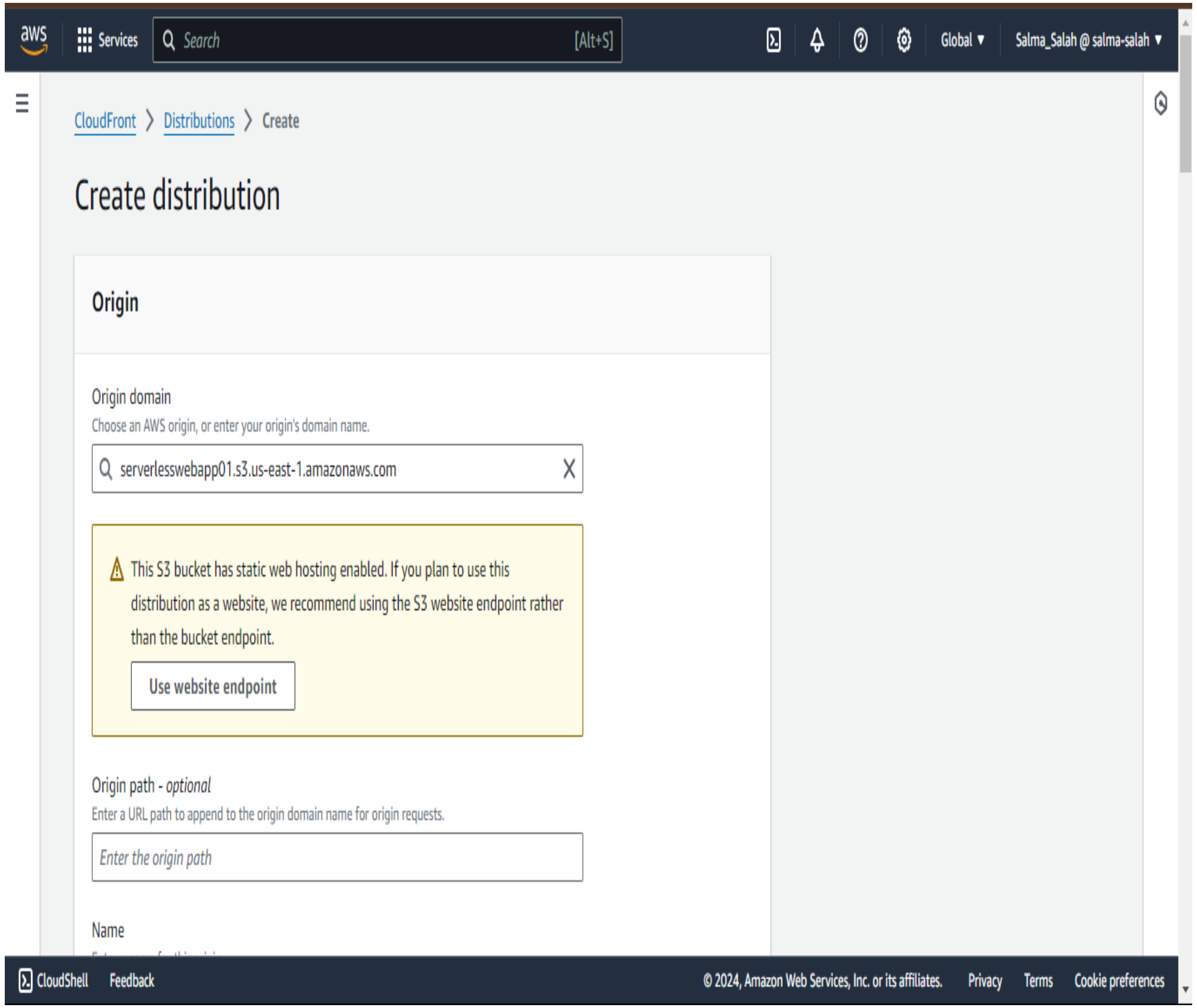
Reduce latency

The CloudFront network has 225+ points of presence (PoPs) that are connected by

Improve security

Use CloudFront for perimeter protection, traffic encryption, and access controls

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


aws
Services
Search
[Alt+S]
Global ▾
Salma_Salah @ salma-salah ▾
CloudFront > Distributions > Create

Create distribution

Origin

Origin domain

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

serverlesswebapp01.s3.us-east-1.amazonaws.com

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.

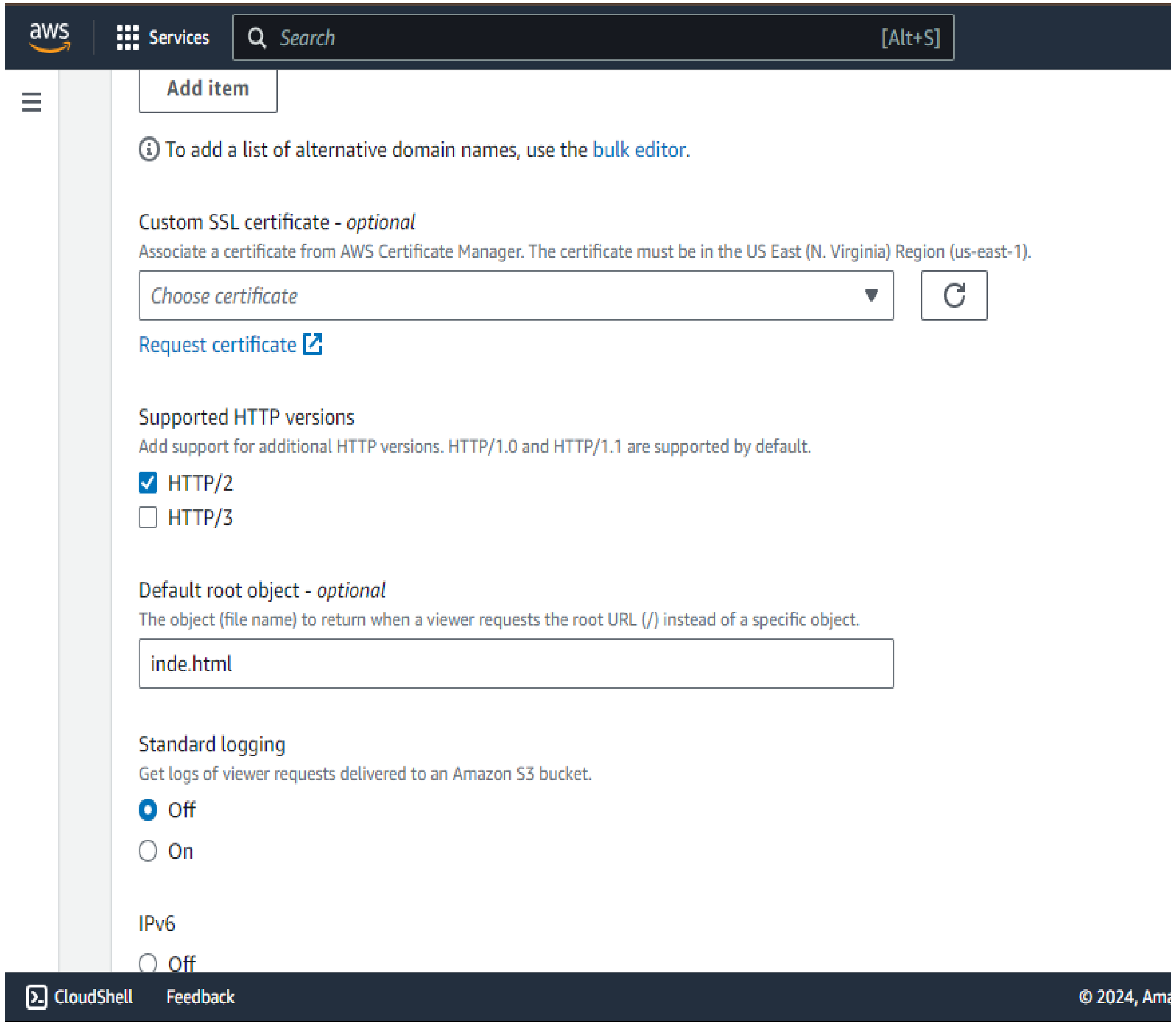
Origin path - *optional*

Enter a URL path to append to the origin domain name for origin requests.

Enter the origin path

Name

Cloud Front Configuration



ⓘ To add a list of alternative domain names, use the bulk editor.

Custom SSL certificate - *optional*

Associate a certificate from AWS Certificate Manager. The certificate must be in the US East (N. Virginia) Region (us-east-1).

Choose certificate ▼

Request certificate

Supported HTTP versions

Add support for additional HTTP versions. HTTP/1.0 and HTTP/1.1 are supported by default.

☑ HTTP/2

□ HTTP/3

Default root object - *optional*

The object (file name) to return when a viewer requests the root URL (/) instead of a specific object.

inde.html

Standard logging

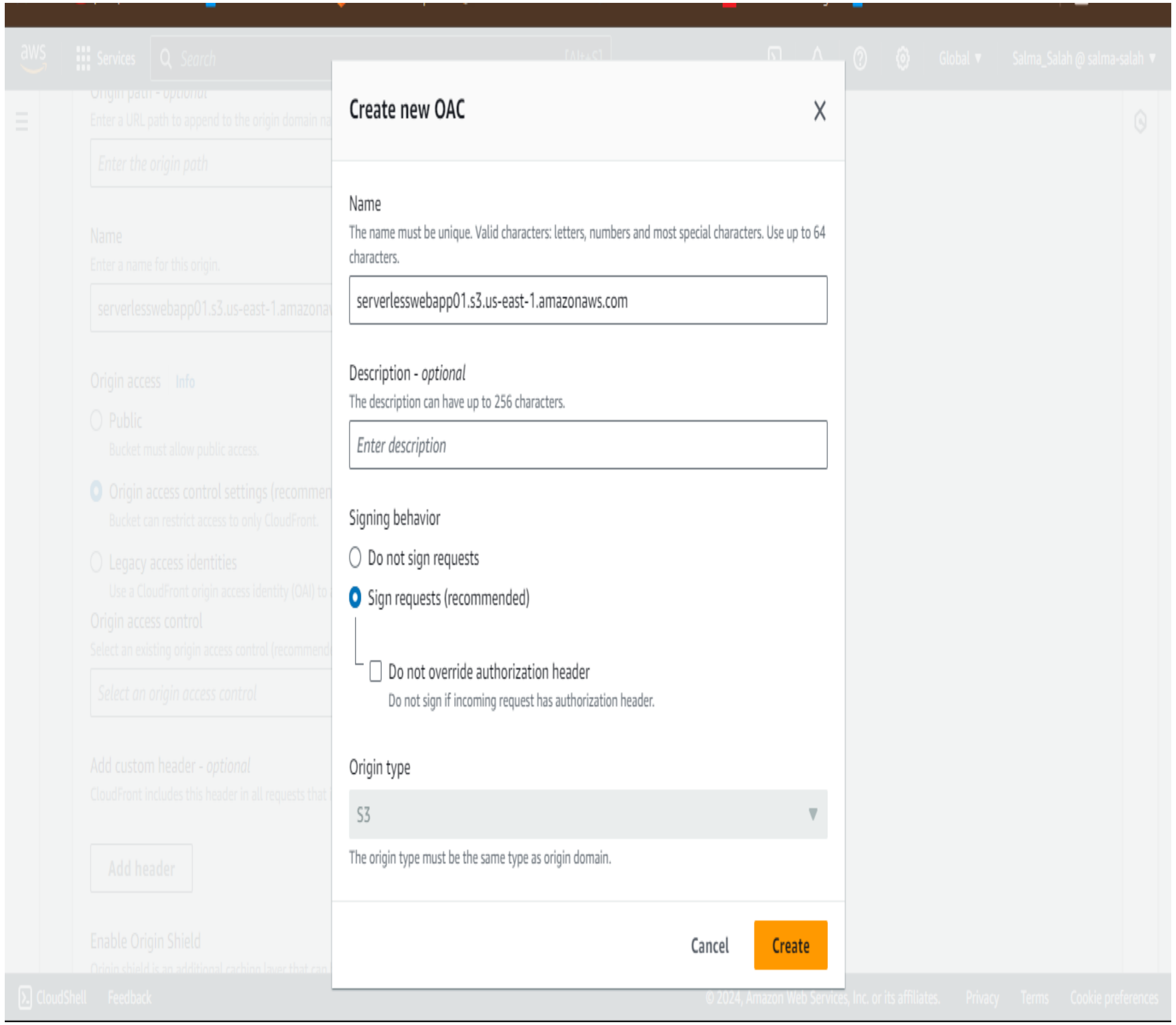
Get logs of viewer requests delivered to an Amazon S3 bucket.

● Off

○ On

IPv6

○ Off



Create new OAC X

Name

The name must be unique. Valid characters: letters, numbers and most special characters. Use up to 64 characters.

serverlesswebapp01.s3.us-east-1.amazonaws.com

Description - *optional*

The description can have up to 256 characters.

Enter description

Signing behavior

○ Do not sign requests

● Sign requests (recommended)

□ Do not override authorization header

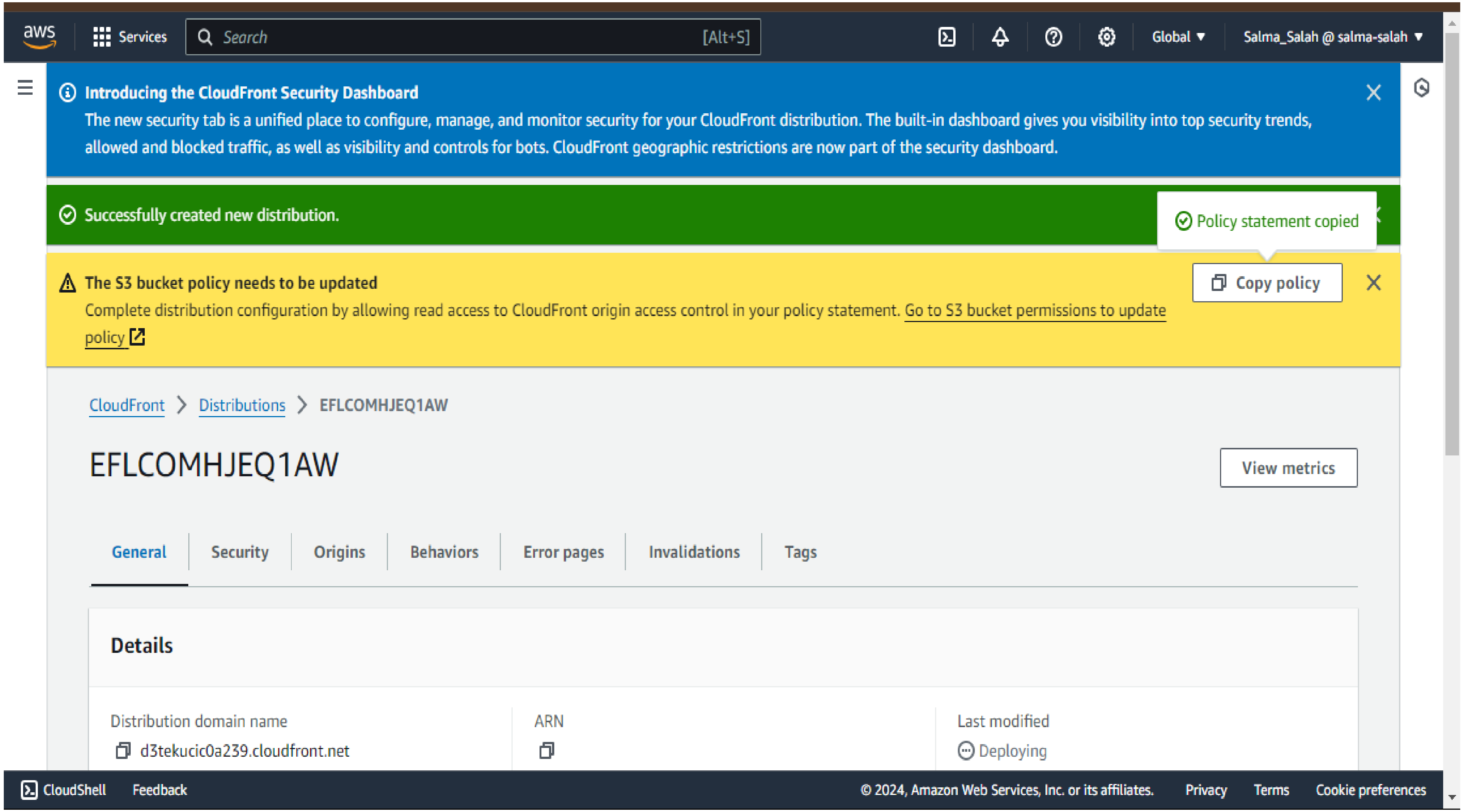
Do not sign if incoming request has authorization header.

Origin type

S3 ▼

The origin type must be the same type as origin domain.

Coping New policy after Creating Cloud Front Distribution



Introducing the CloudFront Security Dashboard

The new security tab is a unified place to configure, manage, and monitor security for your CloudFront distribution. The built-in dashboard gives you visibility into top security trends, allowed and blocked traffic, as well as visibility and controls for bots. CloudFront geographic restrictions are now part of the security dashboard.

Successfully created new distribution.

Policy statement copied

The S3 bucket policy needs to be updated

Complete distribution configuration by allowing read access to CloudFront origin access control in your policy statement. Go to S3 bucket permissions to update policy

EFLCOMHJEQ1AW

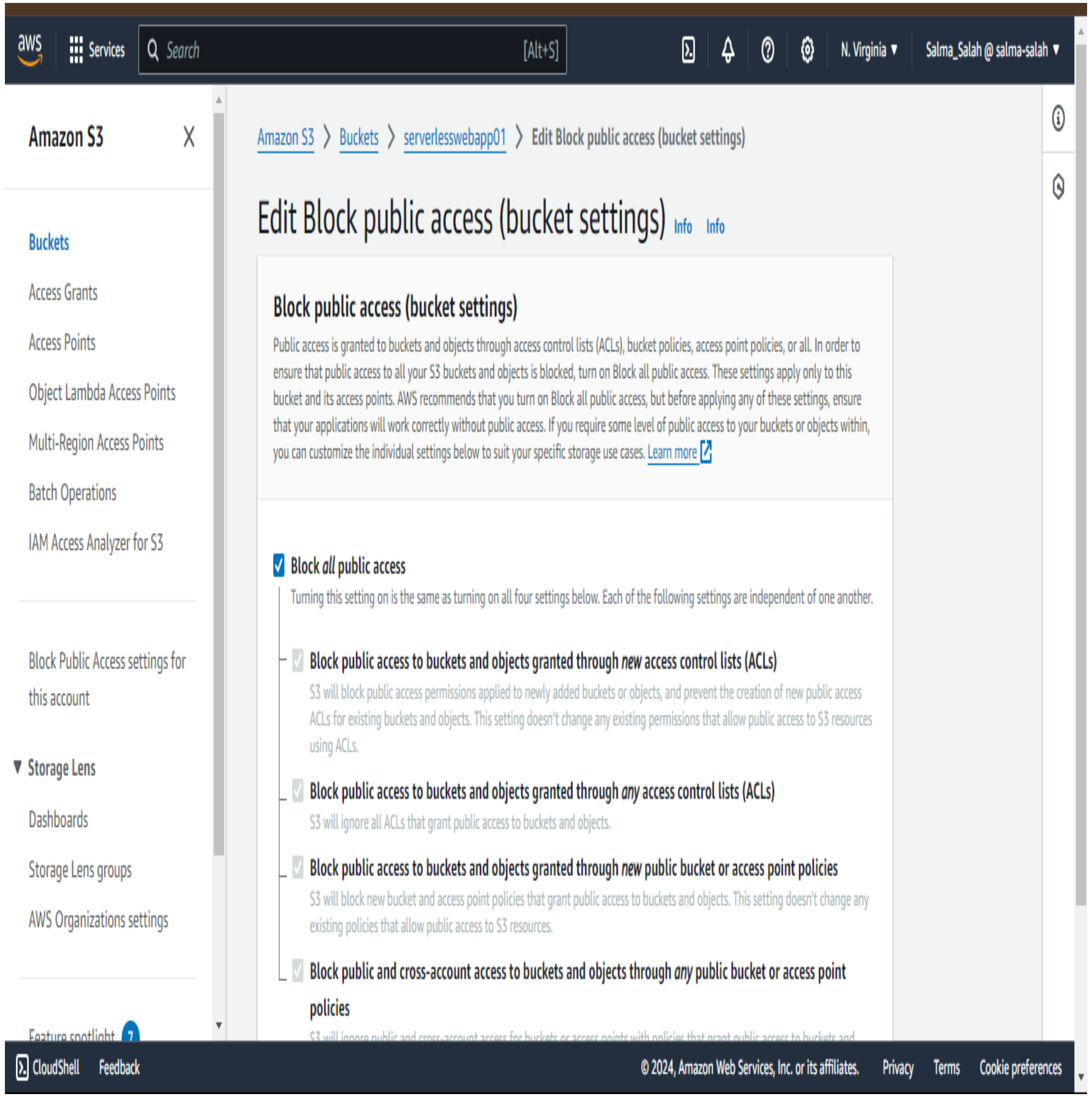
Details

Distribution domain name: d3tekucic0a239.cloudfront.net

ARN

Last modified: Deploying

Block Public Access in S3 and adding new policy to make access only through CloudFront


aws
Services
Search
[Alt+S]
N. Virginia ▾
Salma_Salah @ salma-salah ▾
Amazon S3
Buckets
Access Grants
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
Storage Lens groups
AWS Organizations settings
Feature spotlight 7
Amazon S3 › Buckets › serverlesswebapp01 › Edit Block public access (bucket settings)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Edit Block public access (bucket settings) Info Info

Block public access (bucket settings)

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 all your S3 buckets and 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 your applications will work correctly without public access. If you require some level of public access to your buckets 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 resources using ACLs.

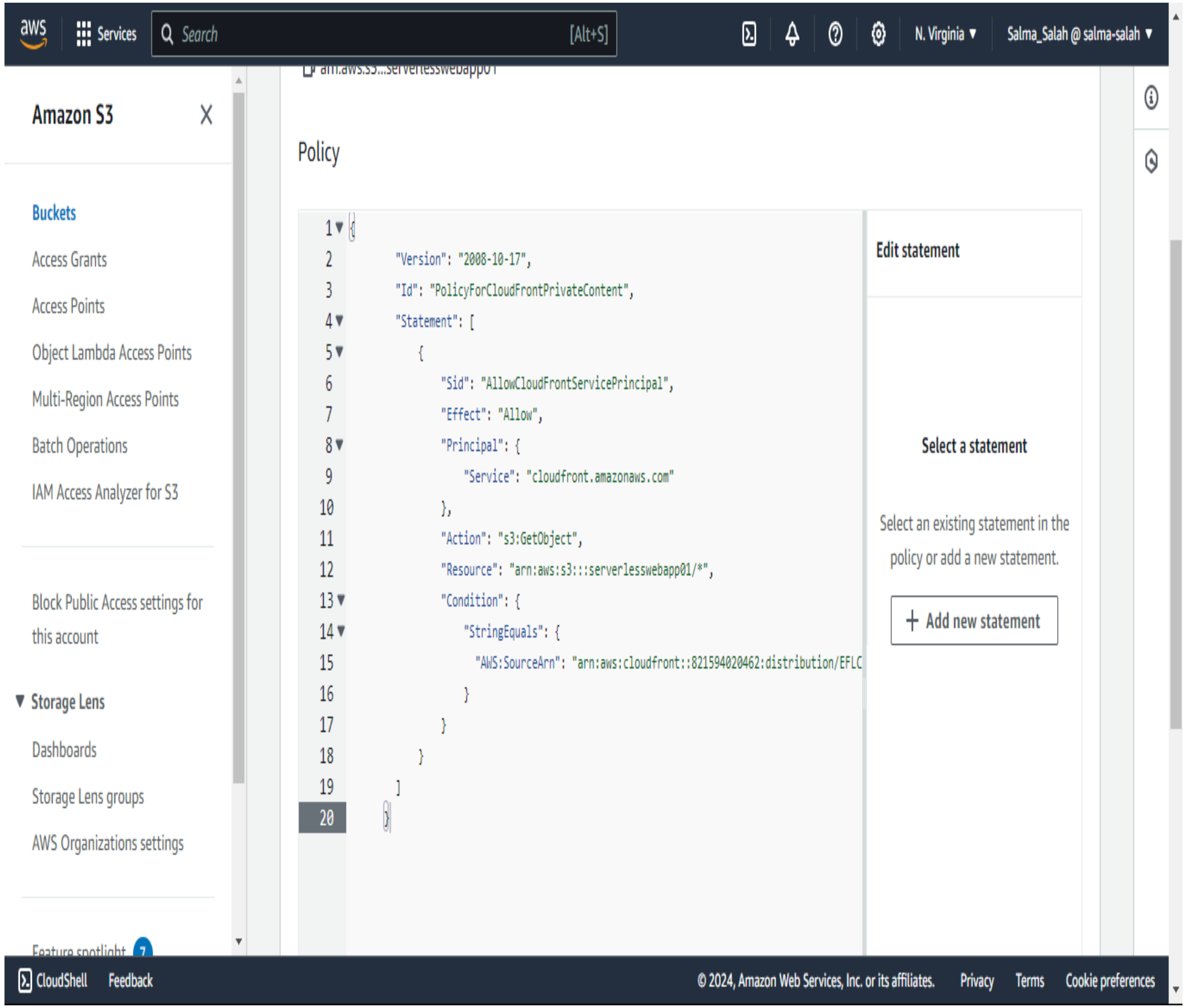
- ☑ Block public access to buckets and objects granted through *any* access control lists (ACLs)

  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.

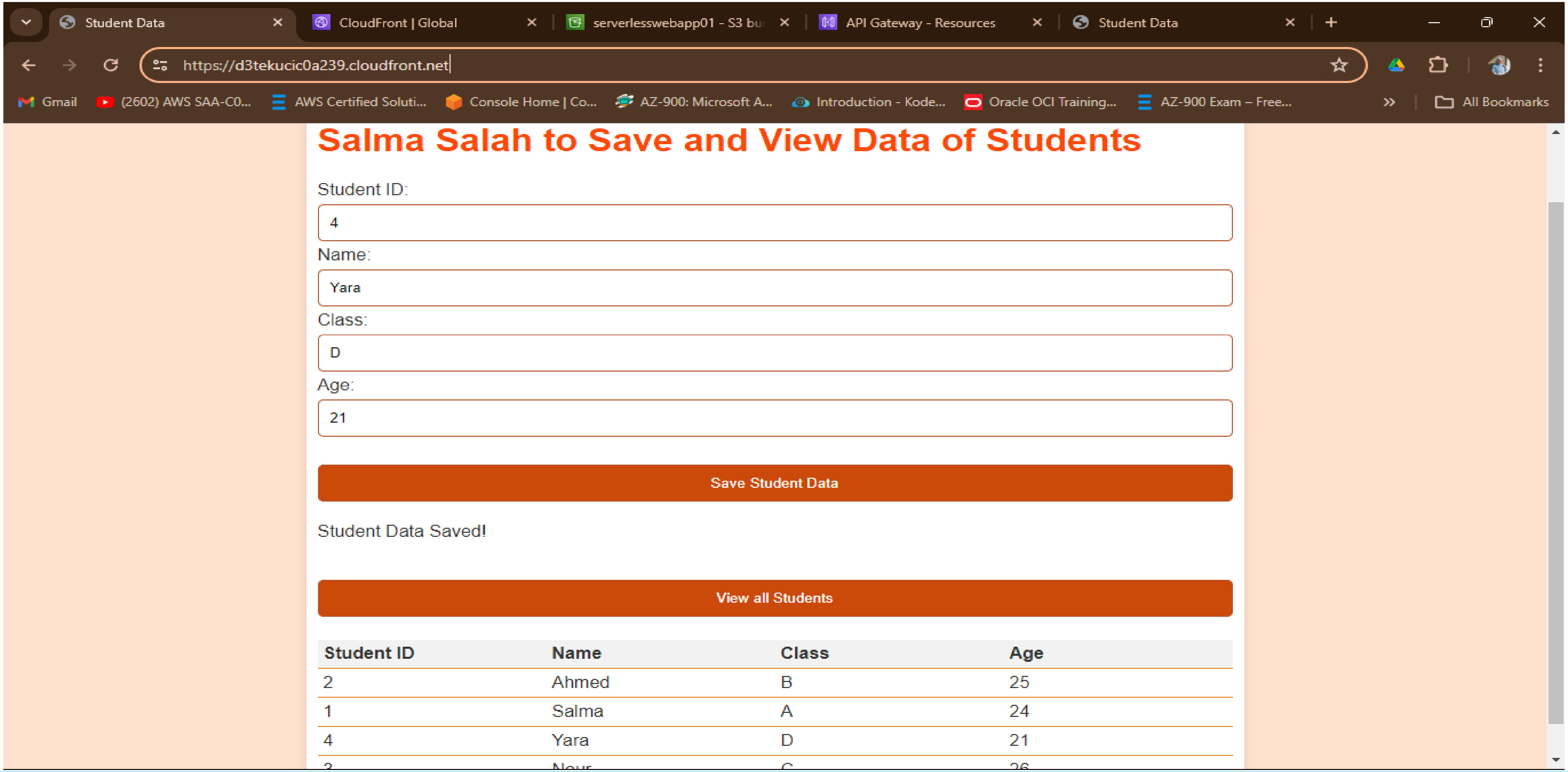
- ☑ Block public and cross-account access to buckets and objects through *any* public bucket or access point policies


aws
Services
Search
[Alt+S]
N. Virginia ▾
Salma_Salah @ salma-salah ▾
Amazon S3
Buckets
Access Grants
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
Storage Lens groups
AWS Organizations settings
Feature spotlight 7
arn:aws:s3:::serverlesswebapp01
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Policy

```
{
        "Version": "2008-10-17",
        "Id": "PolicyForCloudFrontPrivateContent",
        "Statement": [
            {
                "Sid": "AllowCloudFrontServicePrincipal",
                "Effect": "Allow",
                "Principal": {
                    "Service": "cloudfront.amazonaws.com"
                },
                "Action": "s3:GetObject",
                "Resource": "arn:aws:s3:::serverlesswebapp01/*",
                "Condition": {
                    "StringEquals": {
                      "AWS:SourceArn": "arn:aws:cloudfront::821594020462:distribution/EFLC
                    }
                }
            }
        ]
}
```

Testing with Cloud Front End Point and now the connection is Secured (HTTPS)



Salma Salah to Save and View Data of Students

Student ID:

4

Name:

Yara

Class:

D

Age:

21

Save Student Data

Student Data Saved!

View all Students

Student ID	Name	Class	Age
2	Ahmed	B	25
1	Salma	A	24
4	Yara	D	21
3	Nour	C	26