PROJECT DOCUMENTATION
For
CLOUD SECURITY AND MANAGEMENT PROJECT

UNDER THE GUIDANCE OF
DR. AVITA KATAL

BY-

NAME- ADITI NEGI

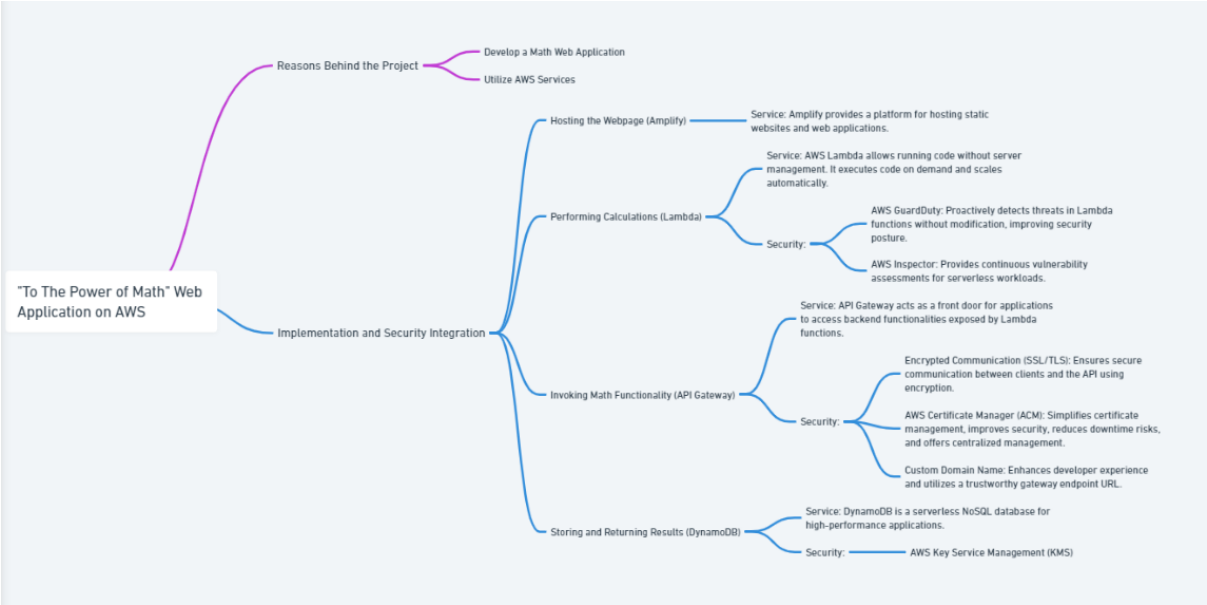
BATCH – 1 (HONORS)

SAP ID – 500091948

ROLL NUMBER- R2142210044

PROJECT DETAILS : The project builds a secure web application for calculating exponents on AWS. It utilizes various services like Amplify for hosting, Lambda for calculations, and DynamoDB for storing results and ensure the use of KMS for security purpose . Security is a major focus throughout. Services like GuardDuty and Inspector secure Lambda functions, while API Gateway enforces encrypted communication and IAM restricts access. CloudWatch and CloudTrail monitor and audit the application for improved security. Overall, the project demonstrates building a secure and scalable web application on AWS by integrating various services.

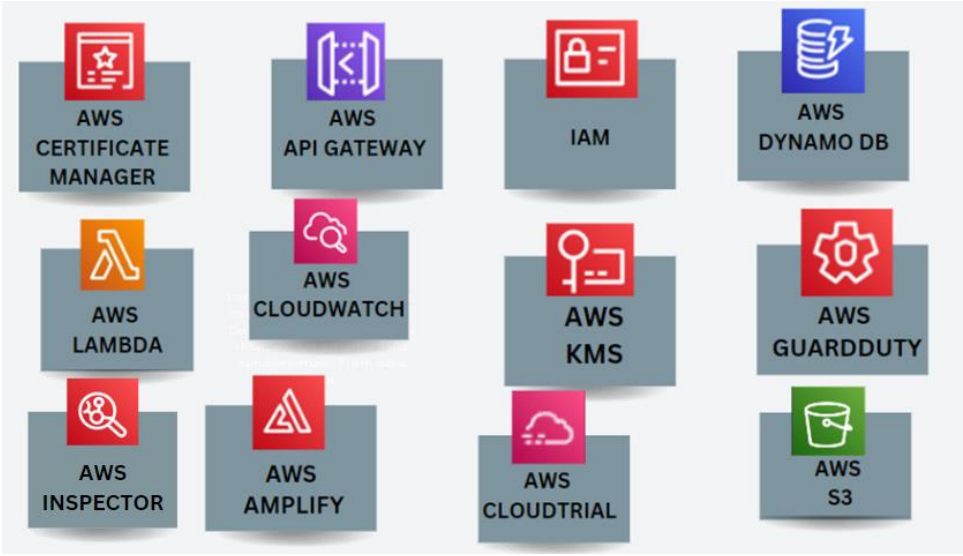
OUTLINE OF THE PROJECT-



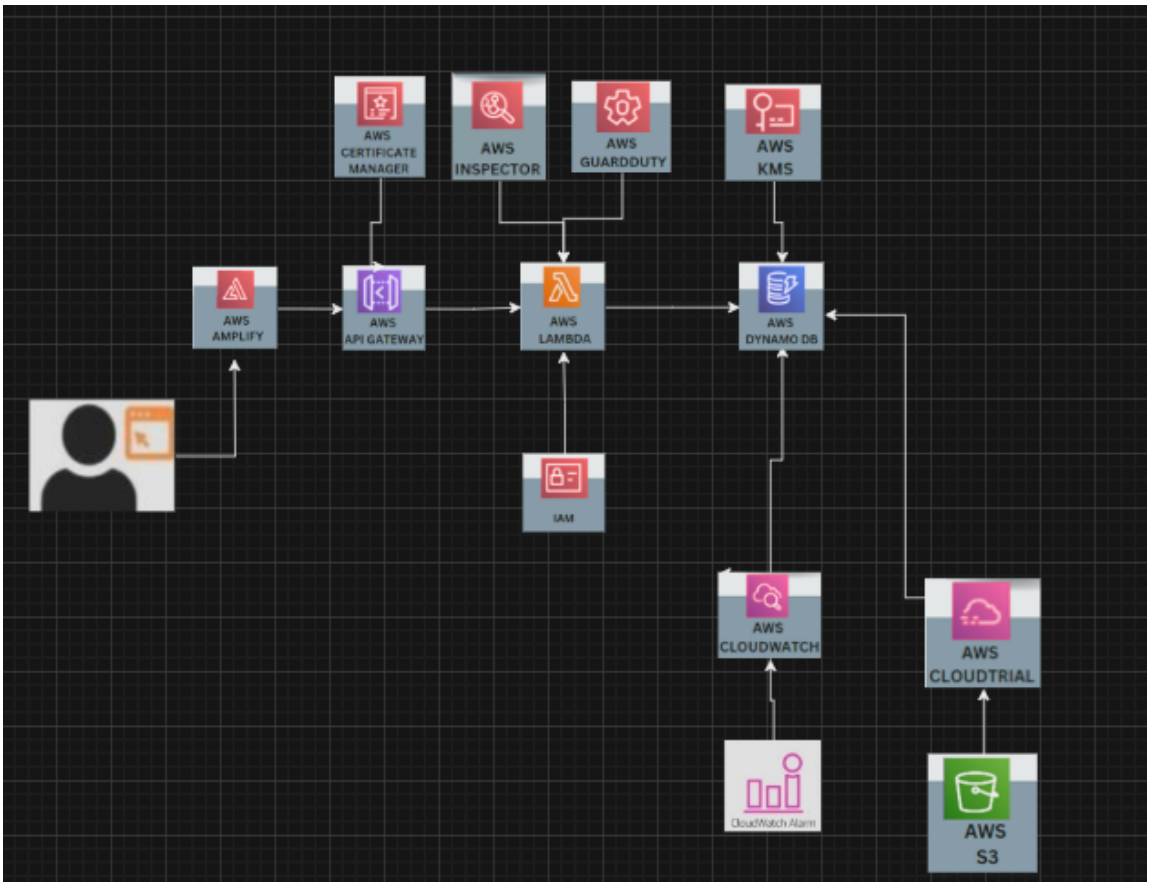
IMPLEMENTATION-

Here is how I implemented it –

The Services used are -



The Current architecture –



Workflow of the process is as follows-

As for the project, I have designed and build a simple web application from scratch. We had pick five different services—Amplify, Lambda, IAM, API Gateway and DynamoDB and why/where to use them, and how to get them to work with each other. As we go, we'll build out each of the services, resulting in a fully-functional math web application. After building math Web application, We have further use Different security services integrated with our App building services. Here is the overview of the services that i used to ensure the Confidentiality , Integrity and Accessibility (COI traids) .

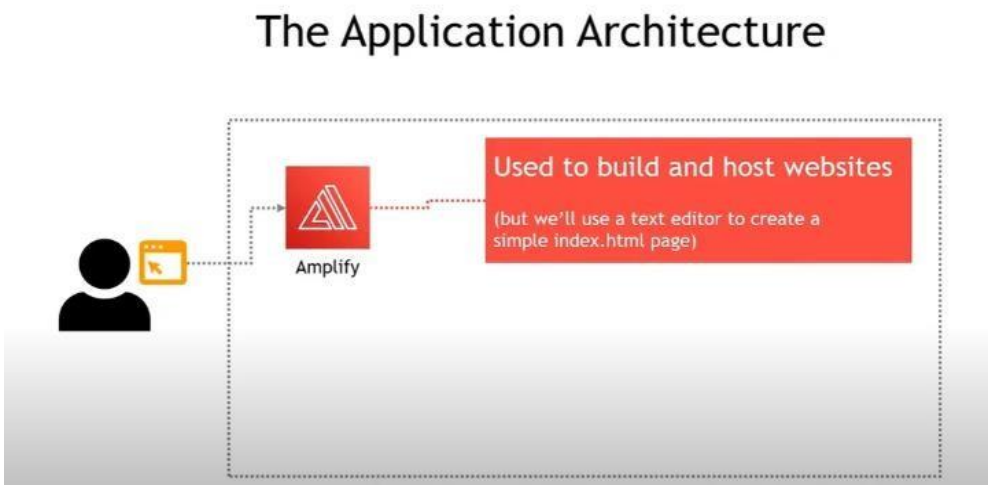
Here are the necessary steps we did –

To build a Math web application we need –

- A way to create/host a webpage

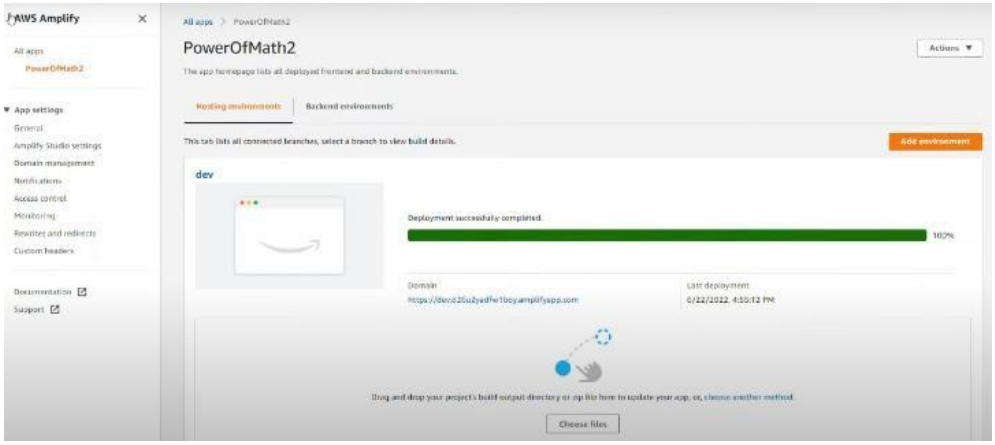
- A way to invoke the math functionality
- A way to do some Math
- Somewhere to store/return the math result
- A way to handle permissions

Step 1- Create/host a webpage

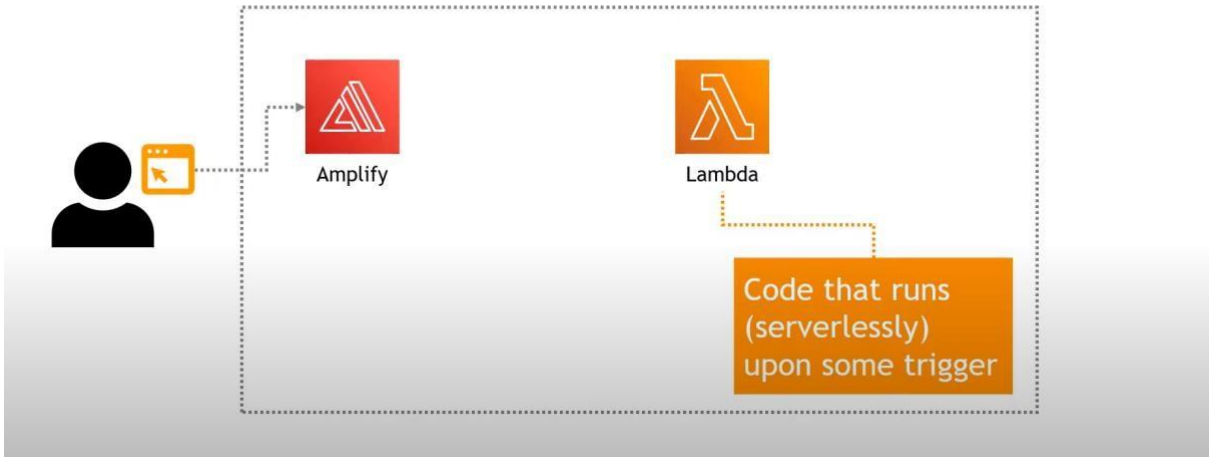


Host a static website using Amplify in the AWS console. AWS Amplify provides fully managed hosting for static websites and web apps. Amplify's hosting solution leverages Amazon CloudFront and Amazon S3 to deliver your site assets via the AWS content delivery network (CDN).

Here is how I created it-

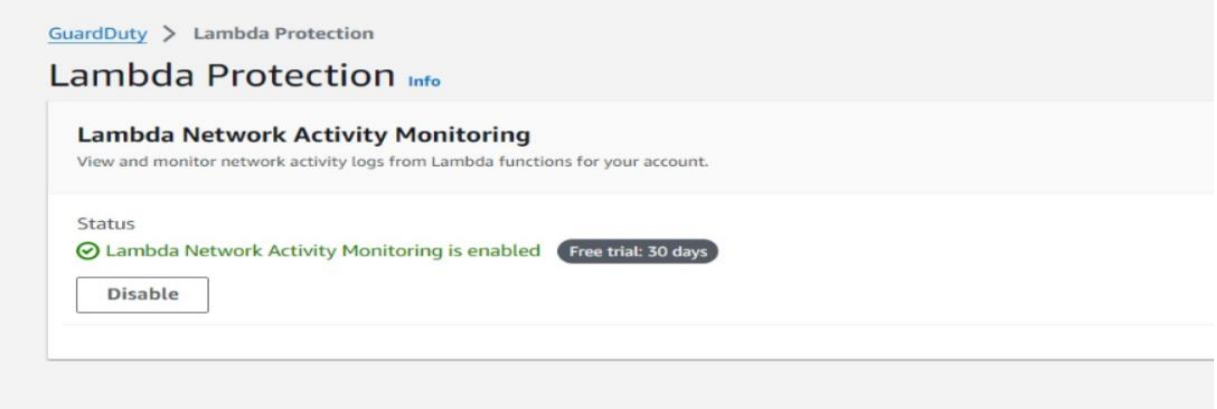


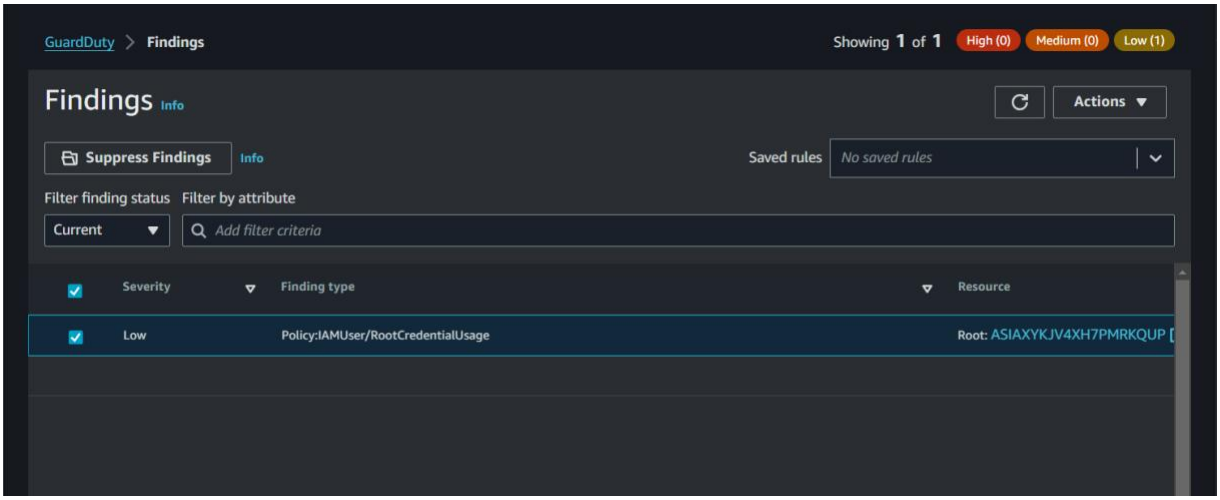
Step 2- To figure out a way to do some maths-

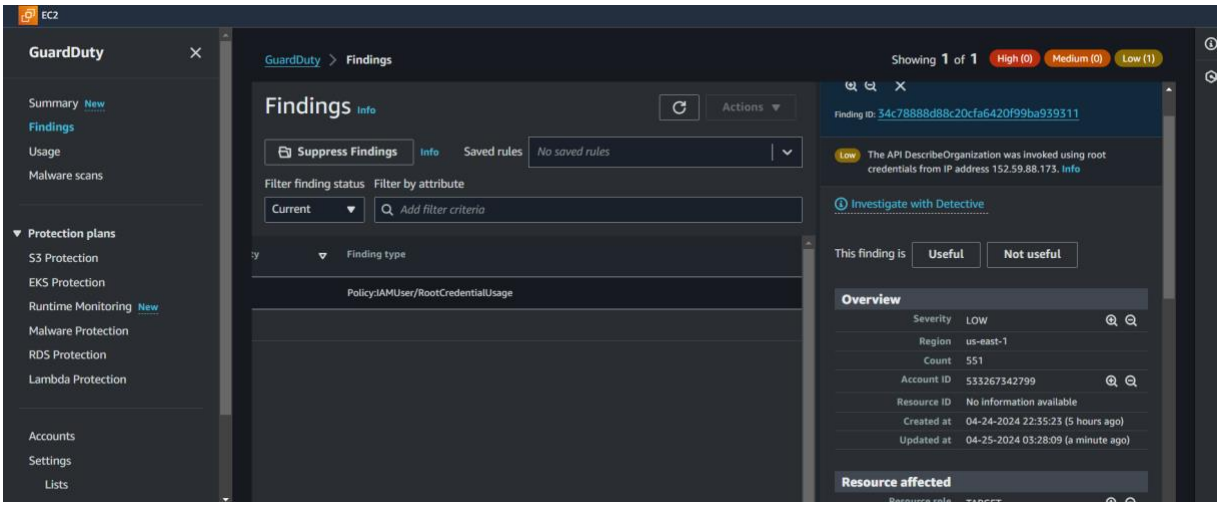


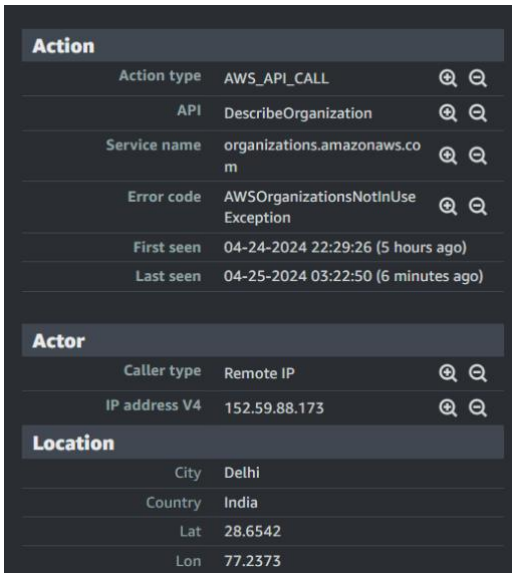
Amazon Web Services offers a service called AWS Lambda that lets customers run. code without having to worry about provisioning or managing servers. AWS Lambda has an event-driven architecture that executes code only when needed and scales automatically, one of its many benefits. Subscribers pay only for the compute time they consume and are not charged for time when their code is not running.

For the Security Purpose ,we have ensure the AWS GuardDuty to ensure the Proactive threat detection for Lambda functions without modifying them and to Improved security posture by identifying potential vulnerabilities in your Lambda workloads.

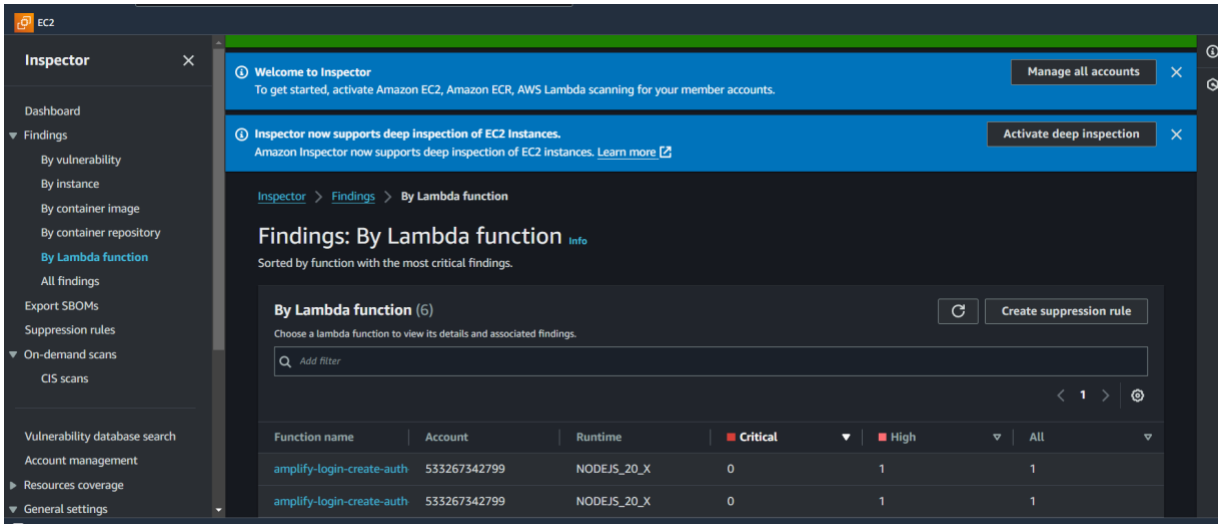

GuardDuty > Lambda Protection
Lambda Protection Info
Lambda Network Activity Monitoring
View and monitor network activity logs from Lambda functions for your account.
Status
Lambda Network Activity Monitoring is enabled
Free trial: 30 days
Disable

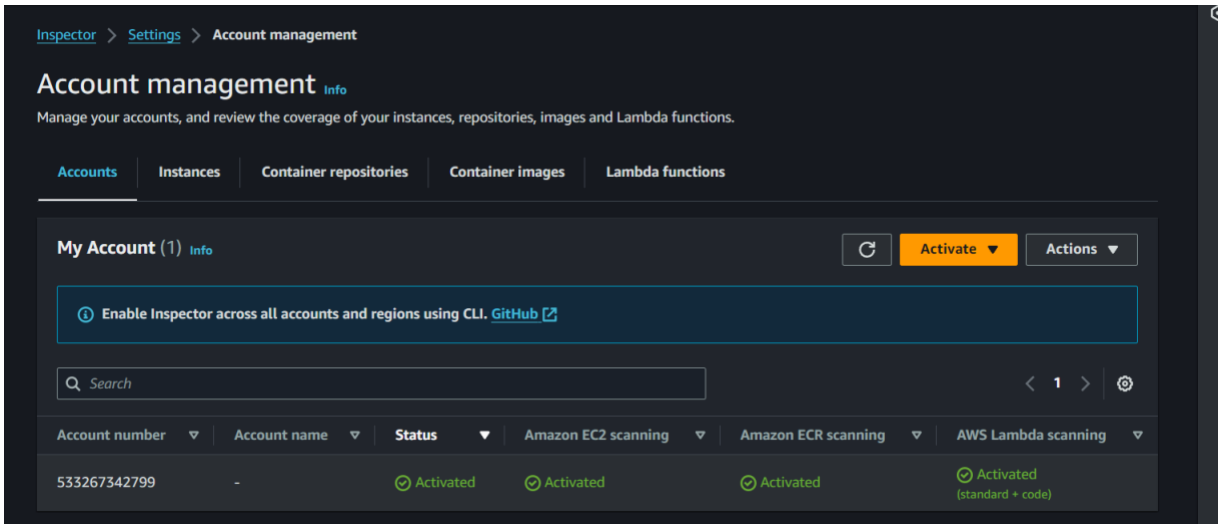

GuardDuty > Findings
Showing 1 of 1
High (0)
Medium (0)
Low (1)
Findings Info
Actions
Suppress Findings
Info
Saved rules
No saved rules
Filter finding status
Filter by attribute
Current
Add filter criteria
Severity
Finding type
Resource
Low
Policy:IAMUser/RootCredentialUsage
Root: ASIAXYKJV4XH7PMRKQUP


EC2
GuardDuty
Summary New
Findings
Usage
Malware scans
Protection plans
S3 Protection
EKS Protection
Runtime Monitoring New
Malware Protection
RDS Protection
Lambda Protection
Accounts
Settings
Lists
GuardDuty > Findings
Showing 1 of 1
High (0)
Medium (0)
Low (1)
Findings Info
Actions
Suppress Findings
Info
Saved rules
No saved rules
Filter finding status
Filter by attribute
Current
Add filter criteria
Finding type
Policy:IAMUser/RootCredentialUsage
Finding ID: 34c78888d88c20cfa6420f99ba939311
Low
The API DescribeOrganization was invoked using root credentials from IP address 152.59.88.173. Info
Investigate with Detective
This finding is
Useful
Not useful
Overview
Severity LOW
Region us-east-1
Count 551
Account ID 533267342799
Resource ID No information available
Created at 04-24-2024 22:35:23 (5 hours ago)
Updated at 04-25-2024 03:28:09 (a minute ago)
Resource affected

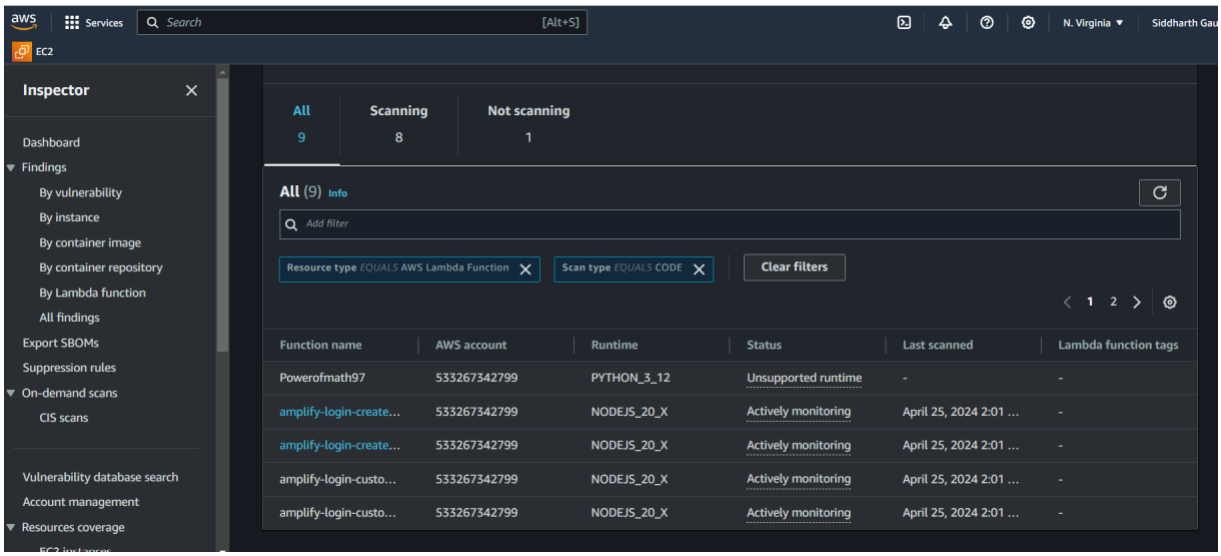


Also, we have used AWS Inspector for Lambda Function to gain continuous, automated vulnerability assessments for your serverless workloads.



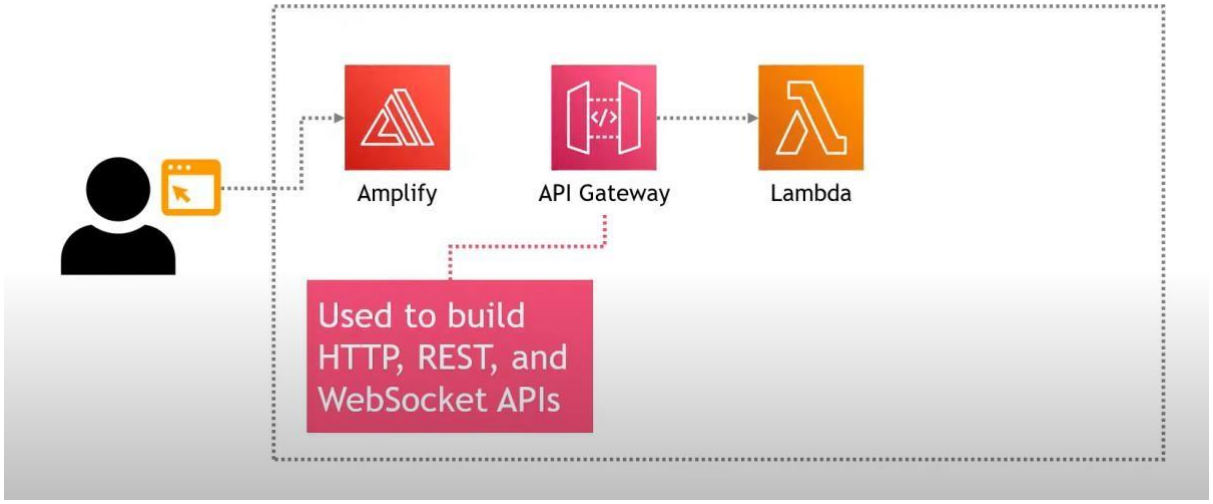


paPA



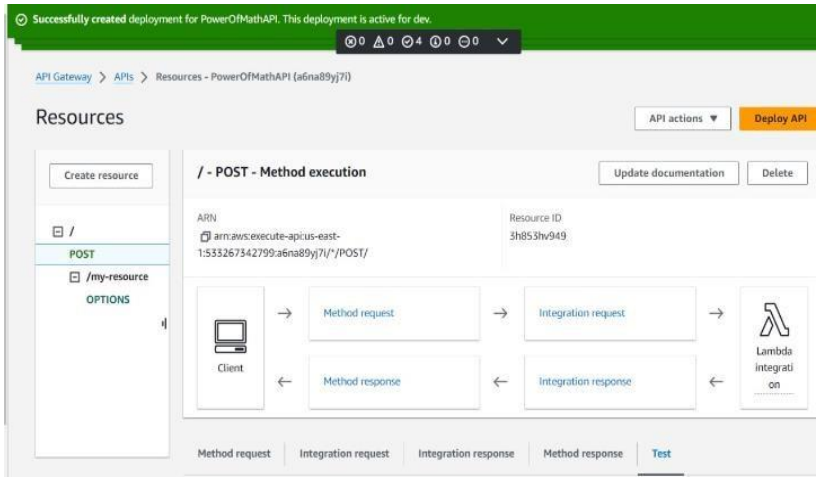
By using both Inspector and GuardDuty, you gain a comprehensive security posture for your Lambda functions. Inspector helps identify vulnerabilities in the code itself, while GuardDuty monitors runtime behavior for suspicious activity.

Step 3- To invoke the maths Functionality-



Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services.

Here is how I did it –



Test

/ - POST method test results

Request	Latency	Status
/	1081	200

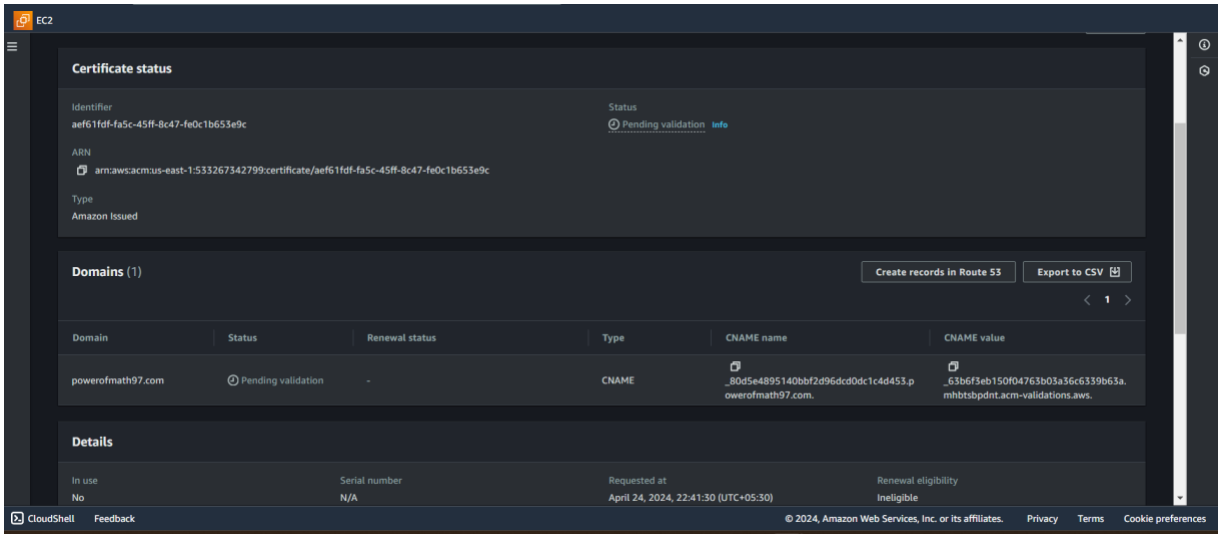
Response body


```
{"statusCode": 200, "body": "\"Your result is 16.0\""}
```


Response headers


```
{
  "Content-Type": "application/json",
  "X-Amzn-Trace-Id": "Root=1-65f8bc4a-
ba6943df59388b5f3629c912;Parent=6f8144f1a0ab964a;Sampled=0;lineage=ad58f198:0"
}
```

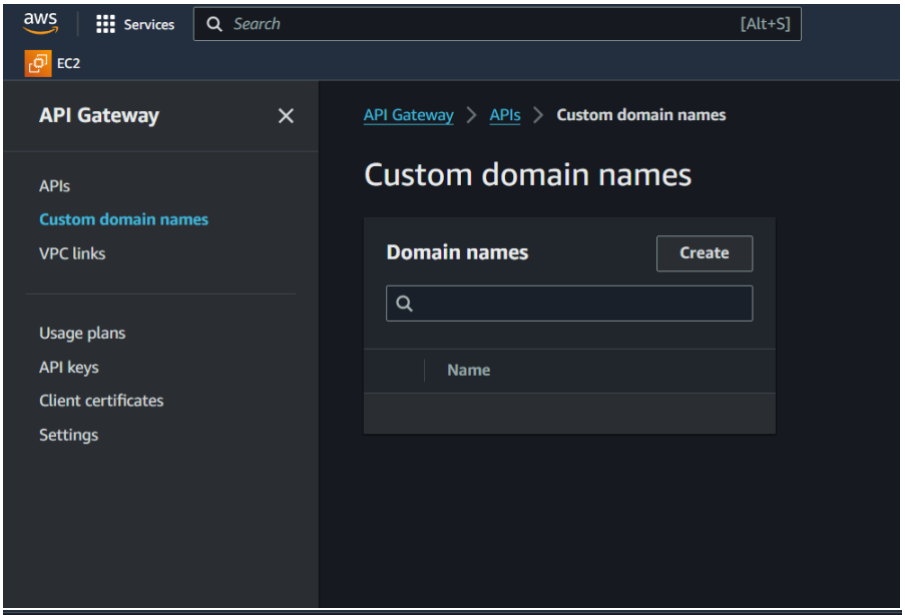

To Ensure the Confidentiality, Data Integrity and Data Authentication , we ensure that the communication between clients and Our API is Encrypted using SSL/TLS –

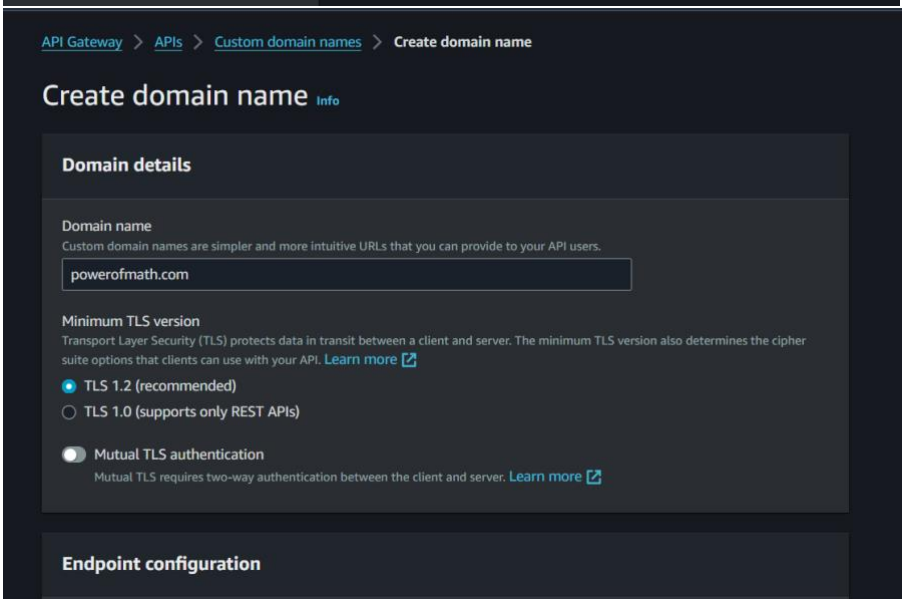


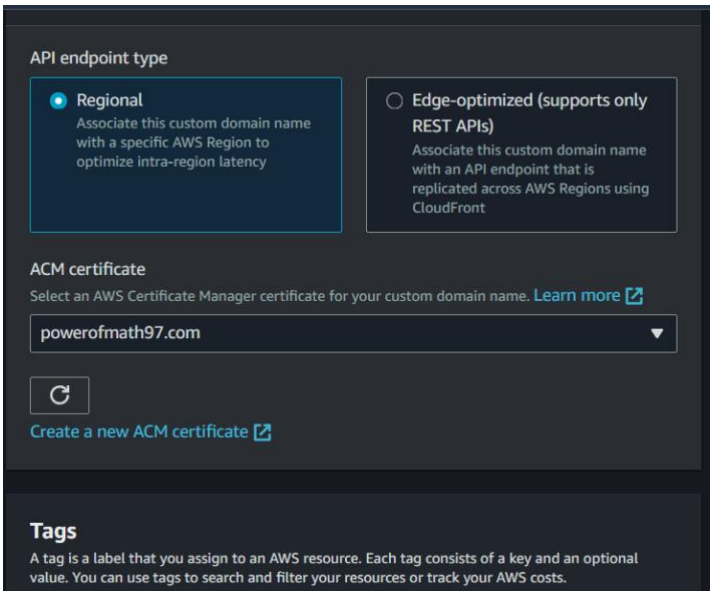
Using the ACM we get benefited by –

- Simplified Certificate Management
- Improved Security
- Reduce Downtime Risk
- Centralized Management

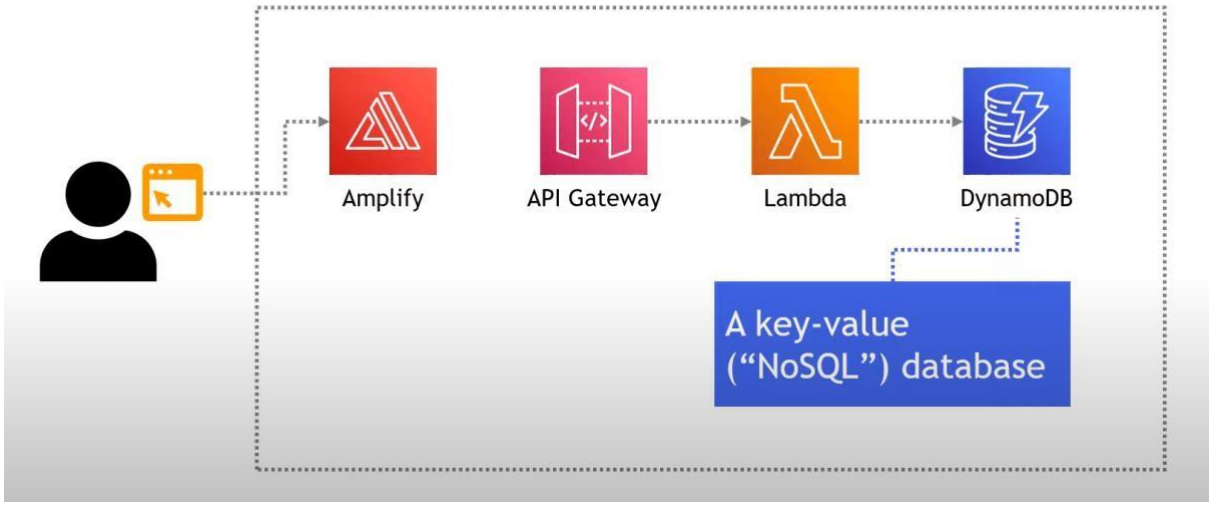
To Improve the Developer Experience and use of trustworthy gateway endpoint URL we use a custom Domain name to our API Gateway and here is how I did it –



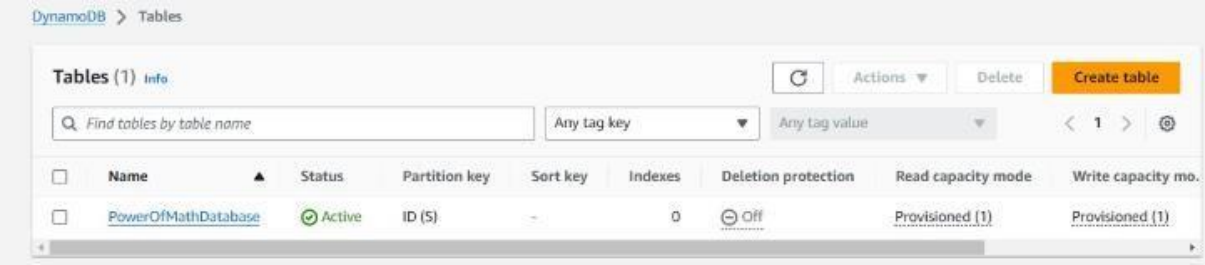


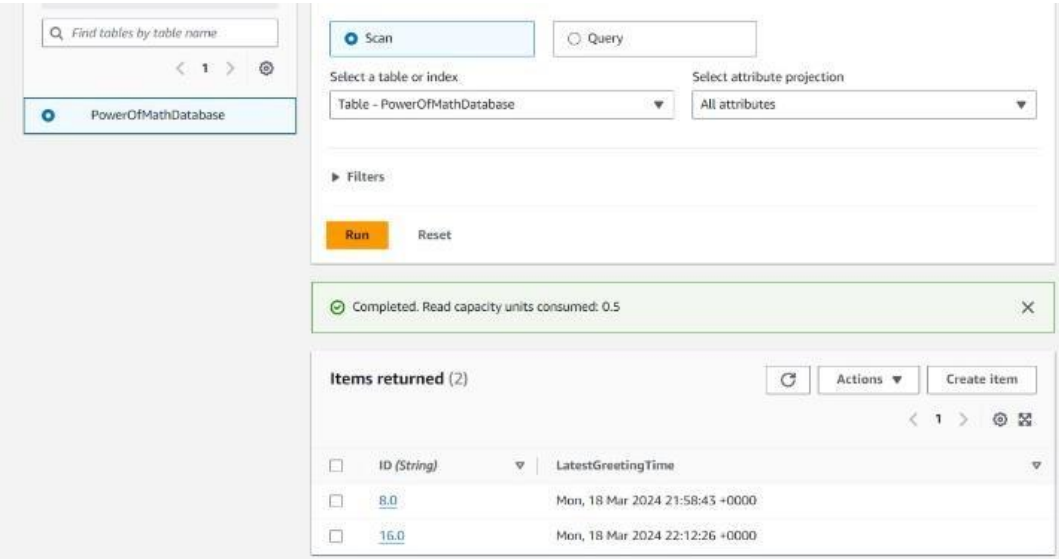


Step 4- To Store/return the math result



Amazon DynamoDB is a serverless, NoSQL, fully managed database service with single-digit millisecond response times at any scale, enabling you to develop and run modern applications while only paying for what you use. The diagram shows the core features of Amazon DynamoDB and integrations with other AWS services.





For Security Purpose we use Key Management Service (KMS) in DynamoDB to enhance the security of your data at rest by-

• **Secure Data in DynamoDB:** KMS encrypts data at rest with separate keys, protecting it even if someone breaches DynamoDB.

• **Comply with Regulations:** KMS helps meet data encryption mandates.

• **Control & Audit Keys:** KMS grants granular control and auditing of who can access/use encryption keys.

• **Stronger Security:** KMS centralizes key management, improving security posture in DynamoDB.

Manage encryption Info

All data stored in Amazon DynamoDB is fully encrypted at rest. By default, DynamoDB manages the encryption key, and you are not charged any fee for using it.

Encryption at rest

Encryption key management

- ○ Owned by Amazon DynamoDB
  The AWS KMS key is owned and managed by DynamoDB. You are not charged an additional fee for using this key.
- ◉ AWS managed key
  Key alias: aws/dynamodb. The key is stored in your account and is managed by AWS Key Management Service (AWS KMS). AWS KMS charges apply.
- ○ Stored in your account, and owned and managed by you
  The key is stored in your account and is owned and managed by you. AWS KMS charges apply.

Cancel | Save changes

DynamoDB > Tables > Powerofmath97table

Tables (1)

Any tag key

Any tag value

Find tables by table name

1

Powerofmath97table

Powerofmath97table

Actions | Explore table items

Global tables | Backups | Exports and streams | Permissions - *new* | Additional settings

Read/write capacity Info

Edit

The read/write capacity mode controls how you are charged for read and write throughput and how you manage capacity.

Capacity mode
Provisioned

Table capacity

Read capacity auto scaling On	Write capacity auto scaling On
Provisioned read capacity units 1	Provisioned write capacity units 1
Provisioned range for reads 1 - 10	Provisioned range for writes 1 - 10

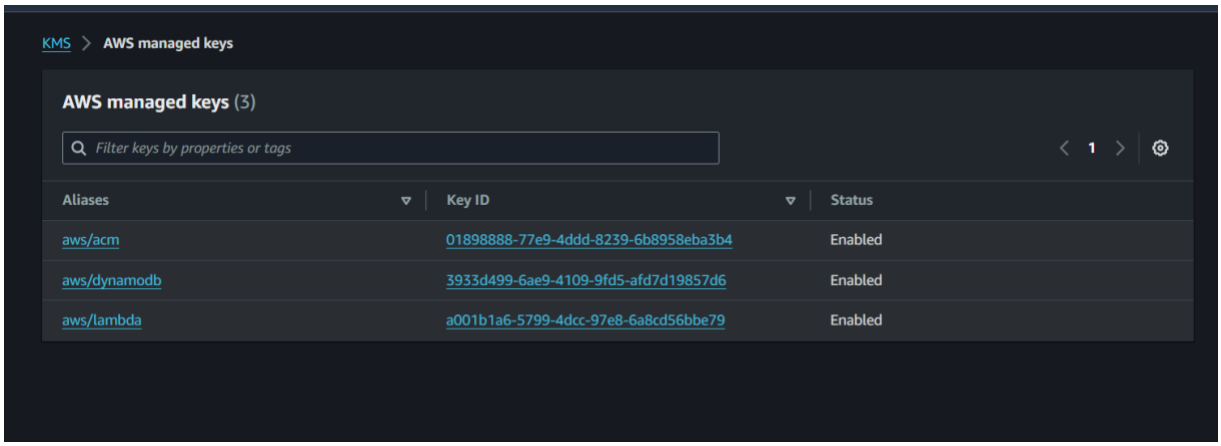
Encryption Info

Manage encryption

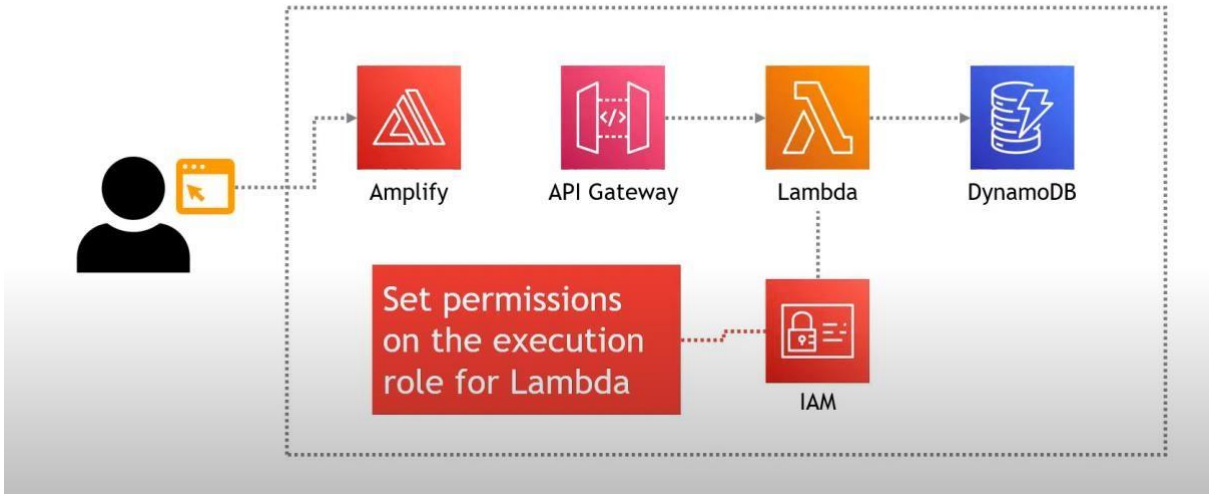
Provides enhanced security by encrypting all your data at rest using encryption keys stored in AWS Key Management Service.

Key management
Managed by AWS KMS

Key ID
arn:aws:kms:us-east-1:533267342799:key/3933d499-6ae9-4109-9fd5-afd7d19857d6



Step 5- A way to handle all the permissions –



All AWS resources, including the roots, OUs, accounts, and policies in an organization, are owned by an AWS account, and permissions to create or access a resource are governed by permissions policies. For an organization, its management account owns all resources. An account administrator can control access to AWS resources by attaching permissions policies to IAM identities (users, groups, and roles).

We ensure IAM Authorization to Configure IAM roles or policies for your API Gateway endpoint to restrict access based on specific user identities or groups. This ensures that only authorized users can access your API resources.

Create policy

1 2

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

```
1  {
2  "Version": "2012-10-17",
3  "Statement": [
4      {
5          "Sid": "VisualEditor0",
6          "Effect": "Allow",
7          "Action": [
8              "dynamodb:PutItem",
9              "dynamodb:DeleteItem",
10             "dynamodb:GetItem",
11             "dynamodb:Scan",
12             "dynamodb:Query",
13             "dynamodb:UpdateItem"
14         ],
15         "Resource": "arn:aws:dynamodb:us-west-2:324712927967:table/PowerOfMathDatabase2"
16     }
17     ]
18 }
```

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
  - Analyzer settings
- Credential report

Policy PowerOfMathDynamoPolicy created.

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

Permissions policies (2) Info

You can attach up to 10 managed policies.

Simulate | Remove | Add permissions

Filter by Type

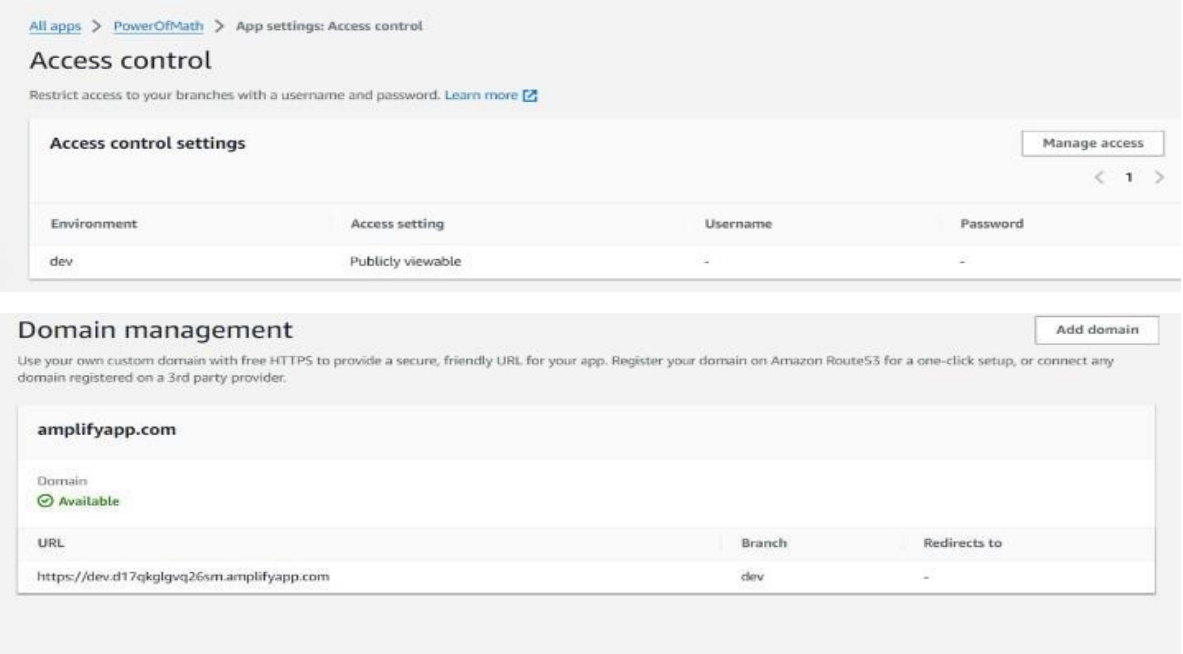
Search | All types

Policy name	Type	Attached entities
AWSLambdaBasicExec...	Customer managed	1
PowerOfMathDynam...	Customer inline	0

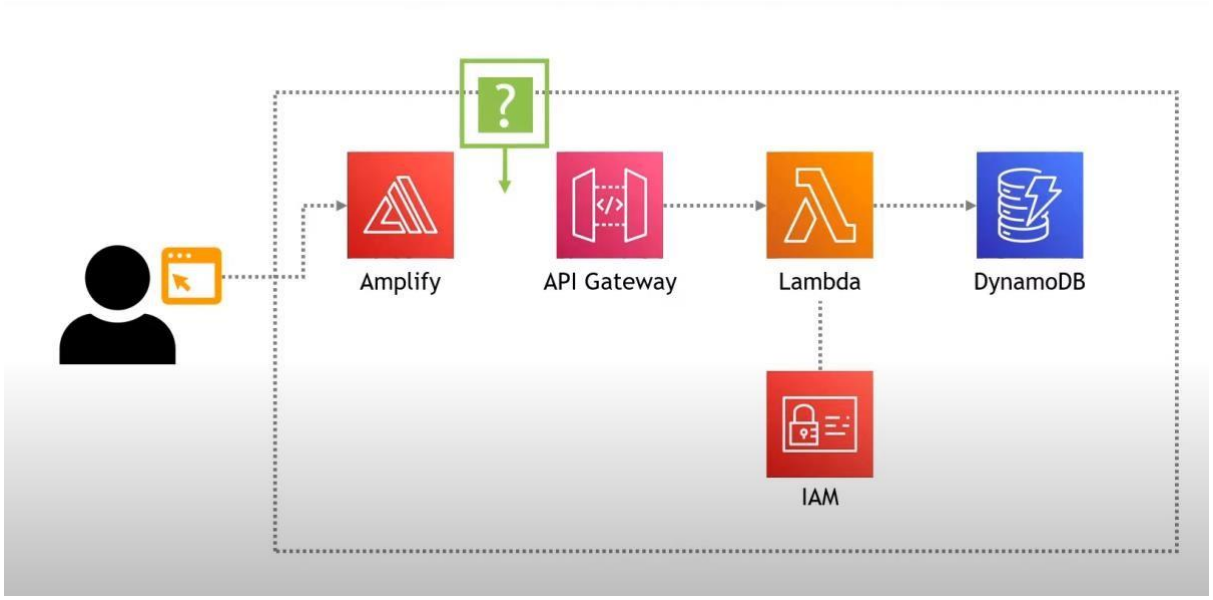
Permissions boundary (not set)

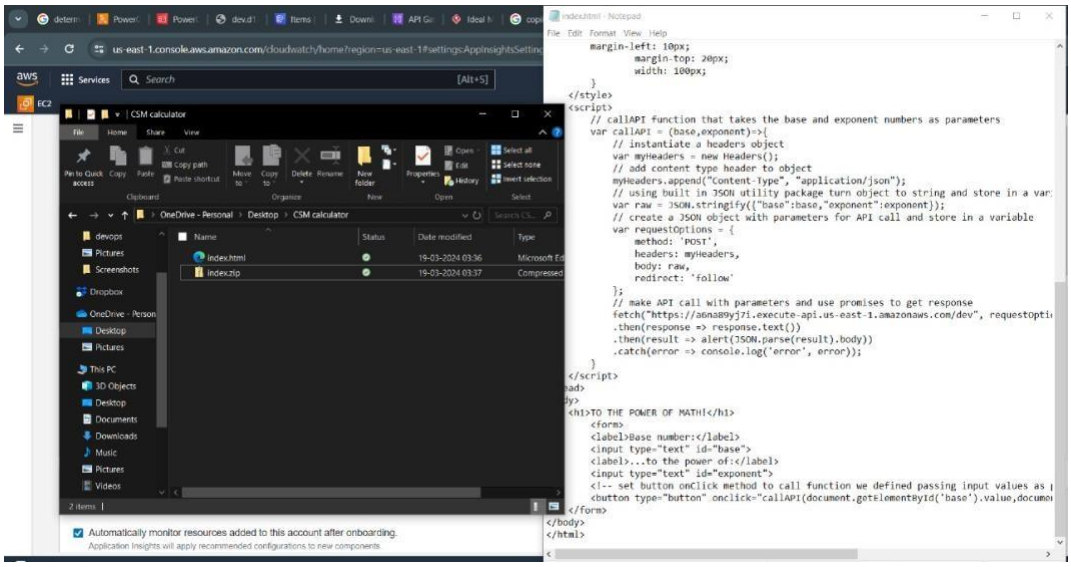
Generate policy based on CloudTrail events

Here we update the lambda function code to write to the DynamoDB table-

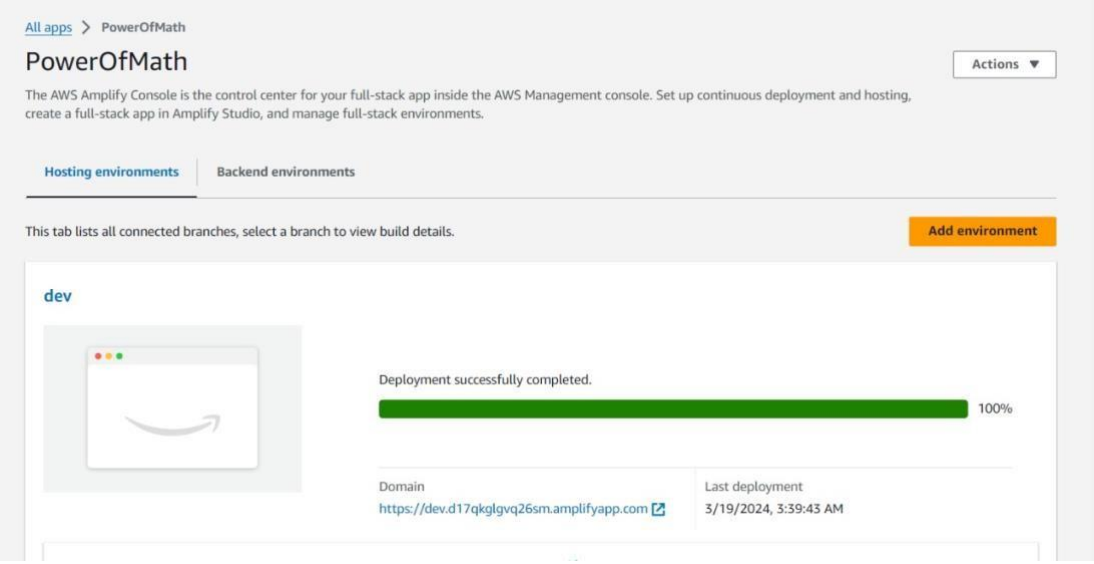


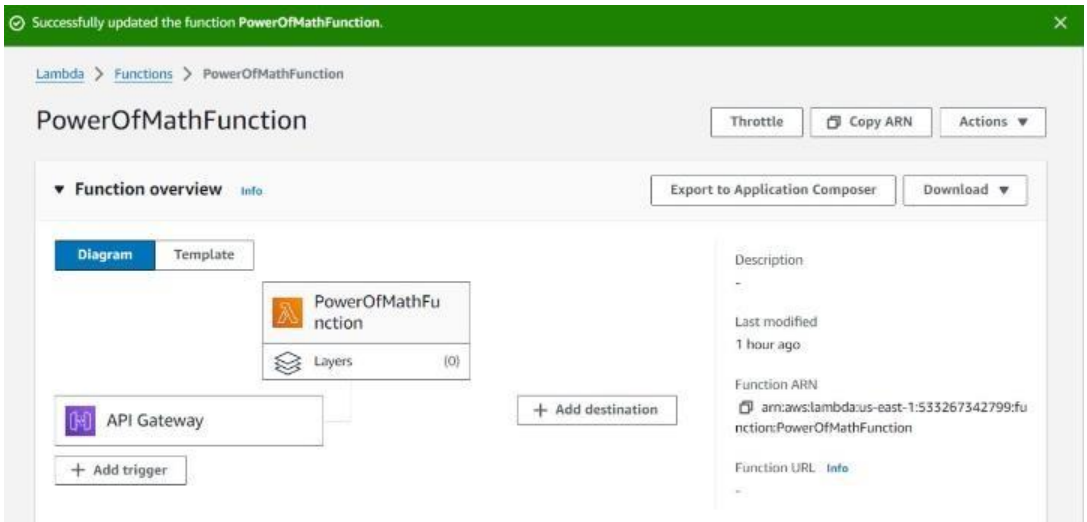
Step 6- Now, We invoke the API gateway endpoint from the index,html page in amplify





Now , we will Re-deploy our index.html page using Amplify



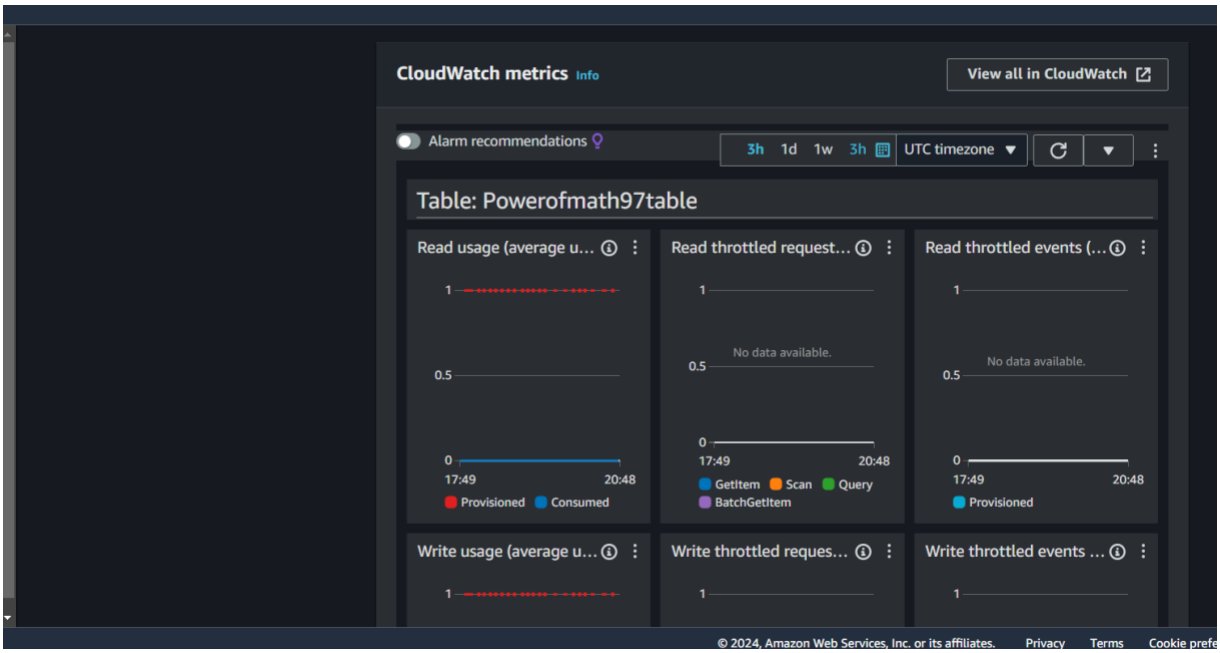


Step 7 – Integration of our application with cloud watch Amazon CloudWatch and CloudWatch alarms .

Amazon CloudWatch is an open-source lightweight tool that is used to collect the data of the resources in which they are deployed. Some of the data is as follows

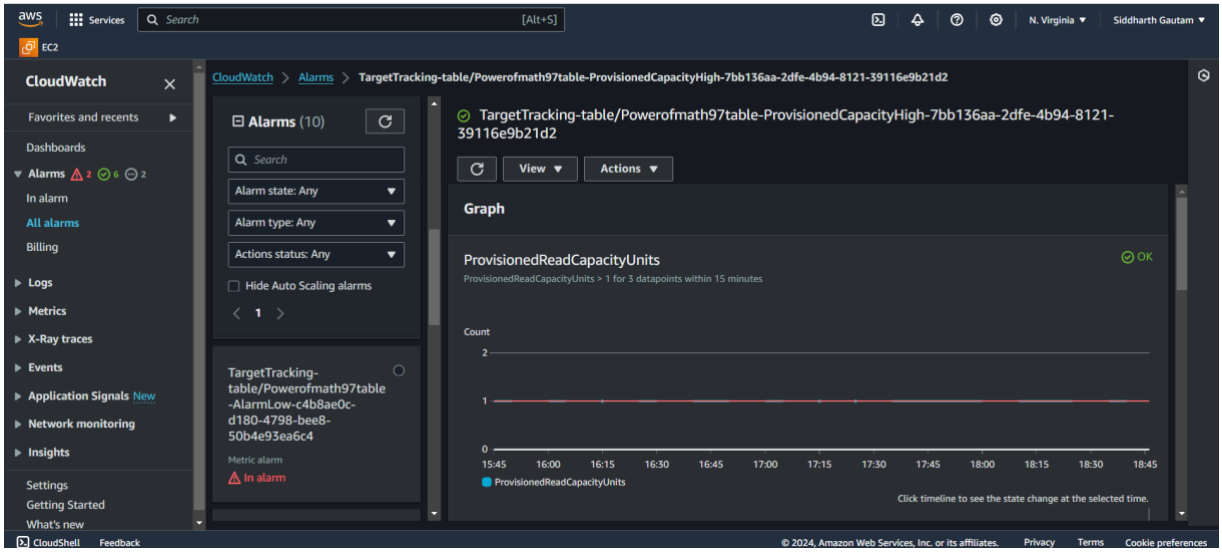
- Metrics: Amazon CloudWatch agent will record the data of CPU utilization, memory usage, disk I/O other system-level stats.
- Logs: It will collect all the logs which are used for the further analysis
- Events: Launching of significant instances, modifications to security groups, and other events.

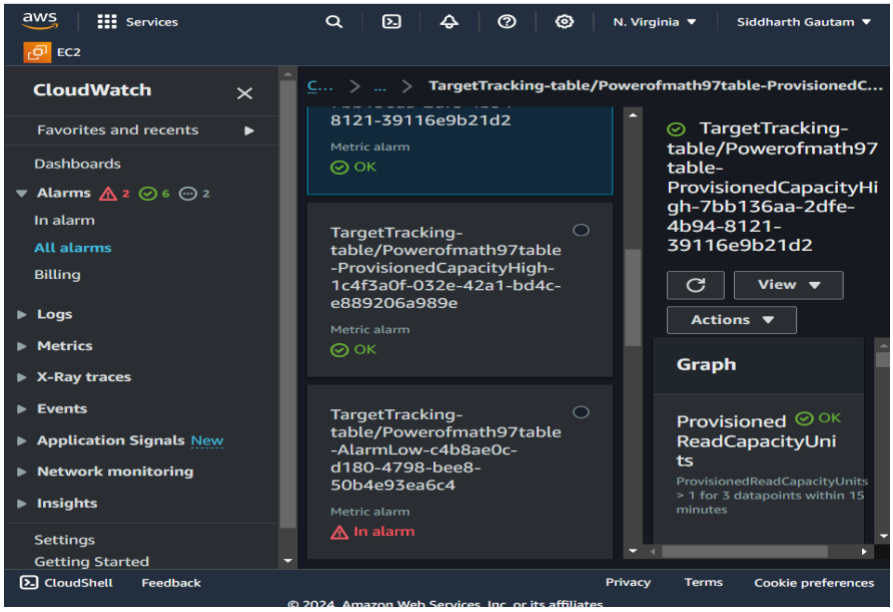
Here is the overview of it-



Here is Cloud watch alarms-

Amazon CloudWatch Alarms used to monitor a single cloud watch metric or the result of Match expression using cloud watch metrics.

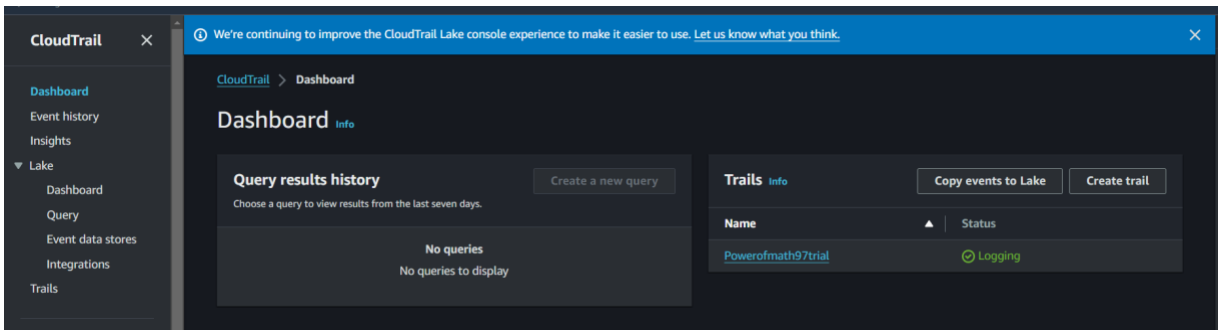


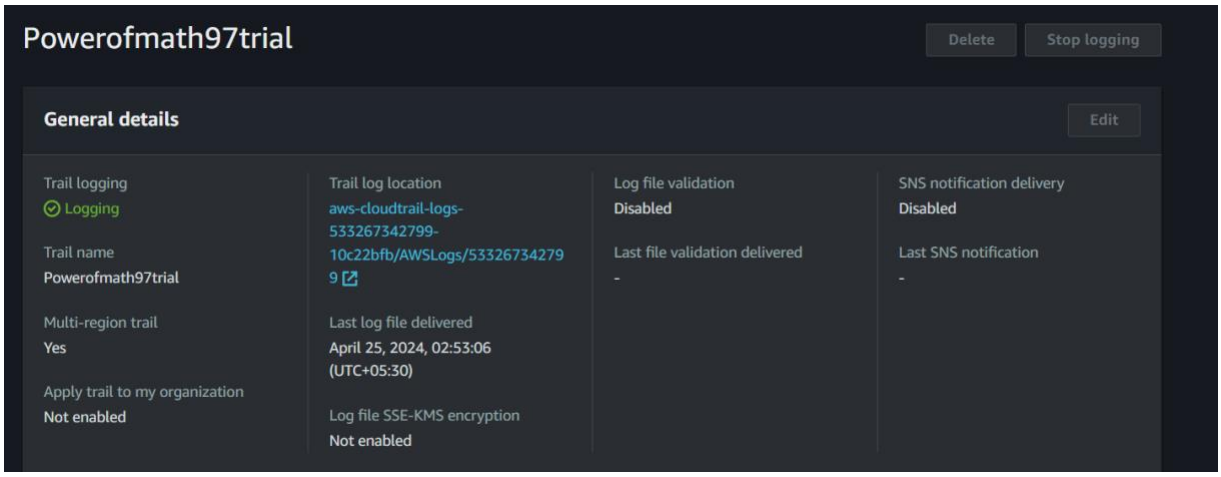


Cloud Trial for API Gateway Audit Logs :

Since, it ensures that –

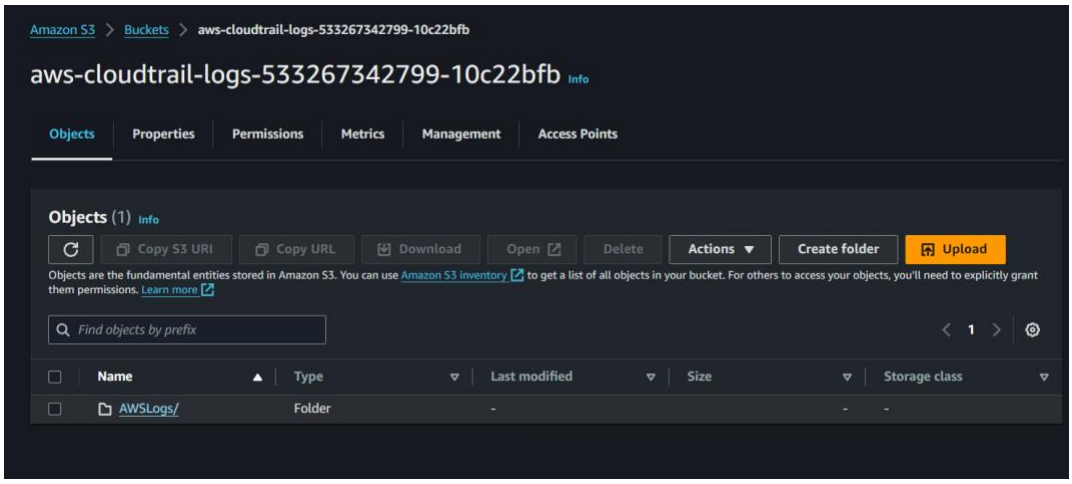
- CloudTrail captures API calls made to manage your API Gateway resources, not the actual API calls processed by your API itself.
- This includes actions like creating an API, deploying an API stage, or updating an API key.
- By logging these administrative actions, CloudTrail provides an audit trail for tracking changes and identifying potential security concerns.





CloudTrail Logs in S3 Bucket:

- CloudTrail delivers its logs to an S3 bucket you specify. These logs are in JSON format and contain details about the API calls made to manage your API Gateway.
- You can then use various AWS services or third-party tools to analyze these logs for security purposes or operational insights.



In essence, CloudTrail with an S3 bucket offers a way to monitor and audit administrative actions taken on your API Gateway itself, not the actual API requests processed by your endpoint. For logging API requests, you'll need separate logging.

Here is the integrated working of our project -

lambda_function × | Environment Var × | Execution results ×

```python
# import the JSON utility package
import json
# import the Python math library
import math

# import the AWS SDK (for Python the package name is boto3)
import boto3
# import two packages to help us with dates and date formatting
from time import gmtime, strftime

# create a DynamoDB object using the AWS SDK
dynamodb = boto3.resource('dynamodb')
# use the DynamoDB object to select our table
table = dynamodb.Table('PowerOfMathDatabase')
# store the current time in a human readable format in a variable
now = strftime("%a, %d %b %Y %H:%M:%S +0000", gmtime())

# define the handler function that the Lambda service will use an entry point
def lambda_handler(event, context):

# extract the two numbers from the Lambda service's event object
    mathResult = math.pow(int(event['base']), int(event['exponent']))

# write result and time to the DynamoDB table using the object we instantiated and save response in a variable
    response = table.put_item(
        Item={
            'ID': str(mathResult),
            'LatestGreetingTime':now
            })

# return a properly formatted JSON object
    return {
    'statusCode': 200,
    'body': json.dumps('Your result is ' + str(mathResult))
    }
```

12:38 Python Spaces: 4

lambda_function × | Environment Var × | Execution results ×

Execution results — Status: Succeeded | Max memory used: 77 MB | Time: 590.04

Test Event Name

PowerOfMathFunction

Response

```
{
  "statusCode": 200,
  "body": "\"Your result is 8.0\""
}
```

Function Logs

```
START RequestId: 3b193aab-3366-4789-b56c-d7000e368c1d Version: $LATEST
END RequestId: 3b193aab-3366-4789-b56c-d7000e368c1d
REPORT RequestId: 3b193aab-3366-4789-b56c-d7000e368c1d  Duration: 590.04 ms Billed Duration: 591 ms Memory Size: 128 MB Max Memory Used: 77 MB  Init D
```

Request ID

3b193aab-3366-4789-b56c-d7000e368c1d

dev.d17qkglgvq26sm.amplifyapp.com

TO THE POWER OF MATH!

Base number: 2 ...to the power of: 8 CALCULATE


TO THE POWER OF MATH!
Base number: 2
...to the power of: 8
CALCULATE
dev.d26u2yadfw1boy.amplifyapp.com says
"Your result is 256.0"
OK