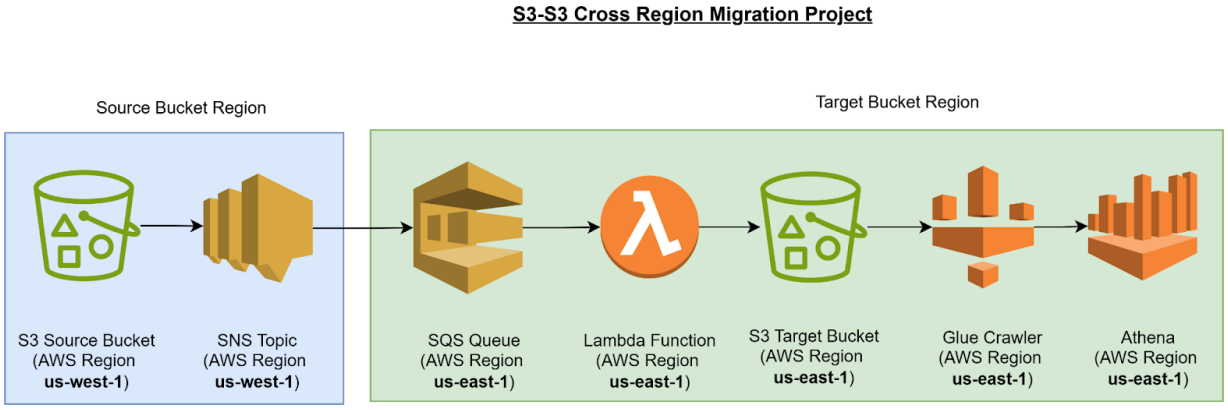
Architecture Diagram



Project Overview

1. In this project, we are using AWS S3, SNS, SQS, and Lambda to transfer a data file from an S3 bucket in the source region to an S3 bucket in the target region (your default region).
2. Once the data is loaded into the target region's S3 bucket, we will use SQS to send a notification to trigger Glue crawler to generate a table in the Glue catalog.
3. After the table is created in the Glue catalog, we will leverage AWS Athena to query the data and analyze its contents.

After completing this project in AWS, someone will learn how to:

1. Migrate data between S3 buckets in different regions using services like SNS, SQS, and Lambda.
2. Automate workflows with AWS Lambda, responding to events and triggering actions like data transfer.
3. Catalog data in AWS Glue by using Glue crawlers to create tables in the Glue Data Catalog.
4. Query data stored in S3 using AWS Athena with the Glue catalog for schema management.
5. Understand and work with cross-region data management and serverless architectures in AWS.

Overall, they will gain experience in building serverless, automated, and scalable data processing workflows in the cloud.

Project Steps

1. Create S3 Buckets

Set up two S3 buckets: one in the source region to hold the data file and one in the target region (your default region) for storing the transferred data.

2. Set Up SNS (Simple Notification Service)

Create an SNS topic that will be used to notify when a new file is uploaded to the source S3 bucket, which will trigger downstream actions.

3. Create SQS Queue

Set up an SQS queue that will receive notifications from SNS and trigger the Lambda function for processing the data file.

4. Develop Lambda Function

Create a Lambda function that listens to the SQS queue, moves the data file from the source S3 bucket to the target S3 bucket, and sends a notification to trigger the Glue crawler after the transfer.

5. Set Up Glue Crawler

Configure and run the Glue crawler to scan the target S3 bucket, detect the schema, and create a table in the Glue Data Catalog.

6. Configure S3 Event Notification

Configure an S3 event in the source bucket to publish notifications to the SQS topic whenever a new file is uploaded..

7. Set Up Athena for Querying

Configure Athena to use the Glue Data Catalog and run SQL queries to analyze the data stored in the target S3 bucket.

8. Test the Workflow

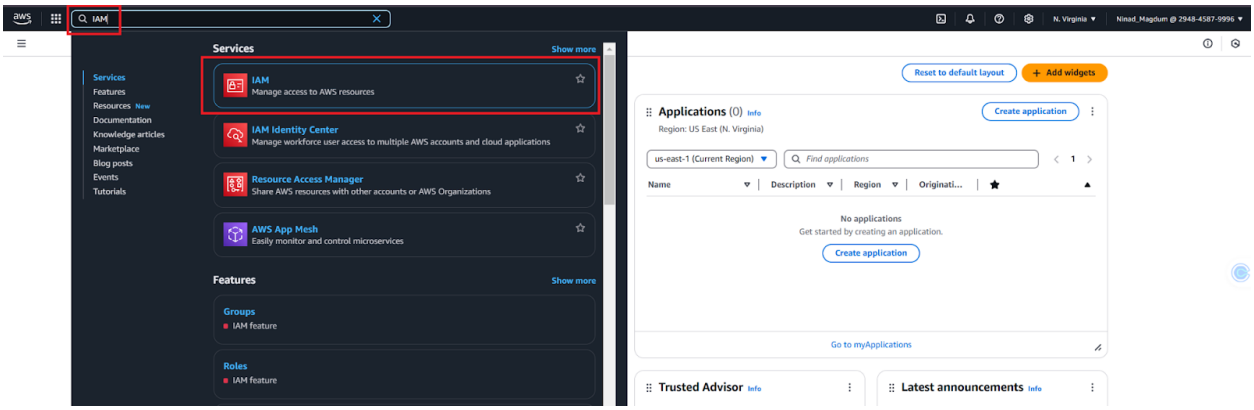
Upload a test file to the source S3 bucket, check if the data is transferred correctly, and ensure that the Glue crawler runs and Athena can query the data.

AWS IAM Role Creation guide

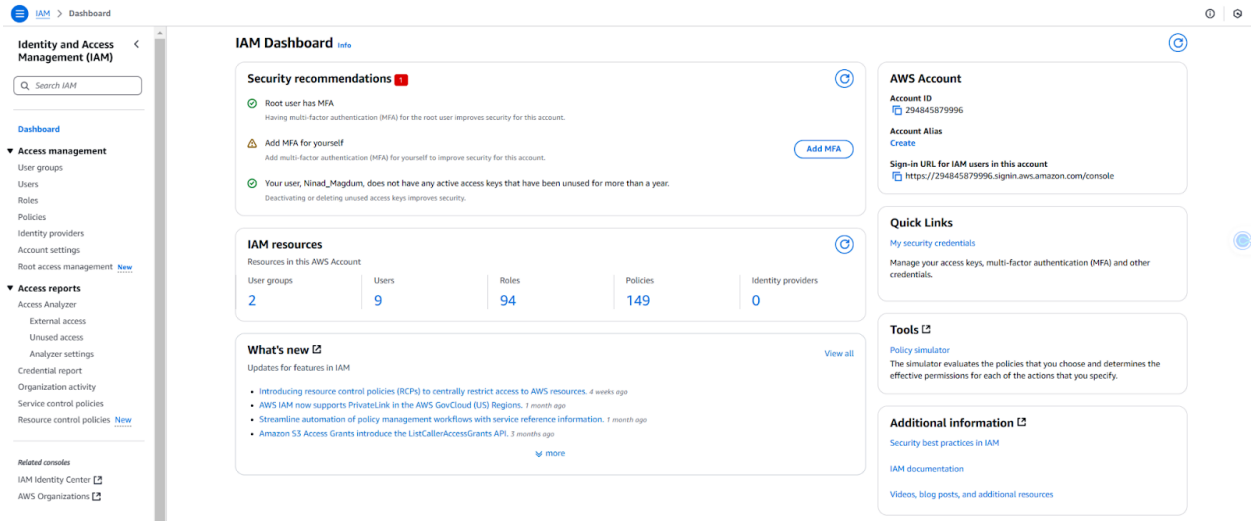
- Let us understand and walk through the process of creation of AWS IAM Role and attach specific Policies

Role Creation

- Open your AWS Management Console and navigate to AWS IAM (you can search for "IAM" in the search bar).

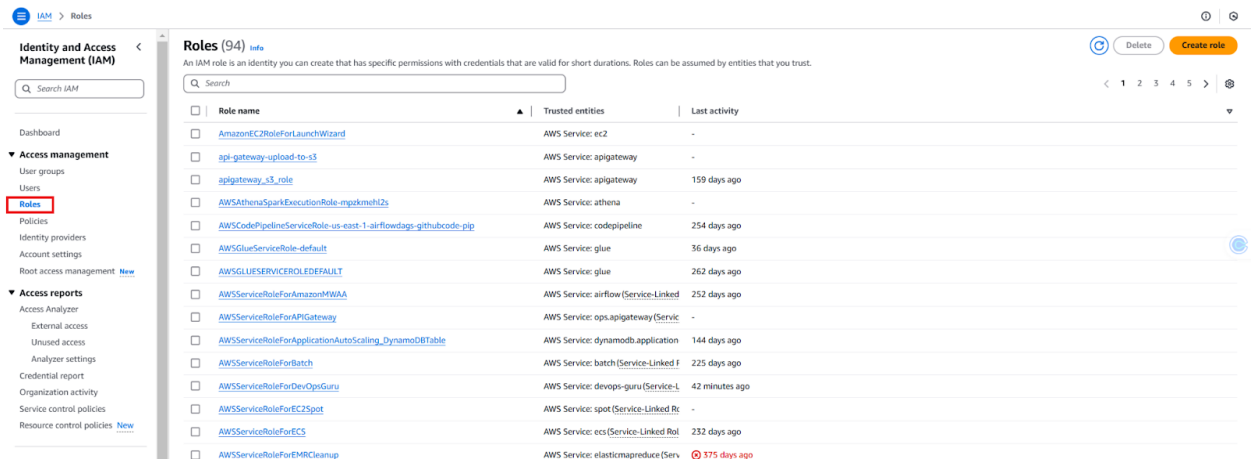


- Navigate to IAM, where you'll land on the page below. Here, you'll create the necessary role and policy that will be utilized in AWS Glue to write data to S3 buckets.

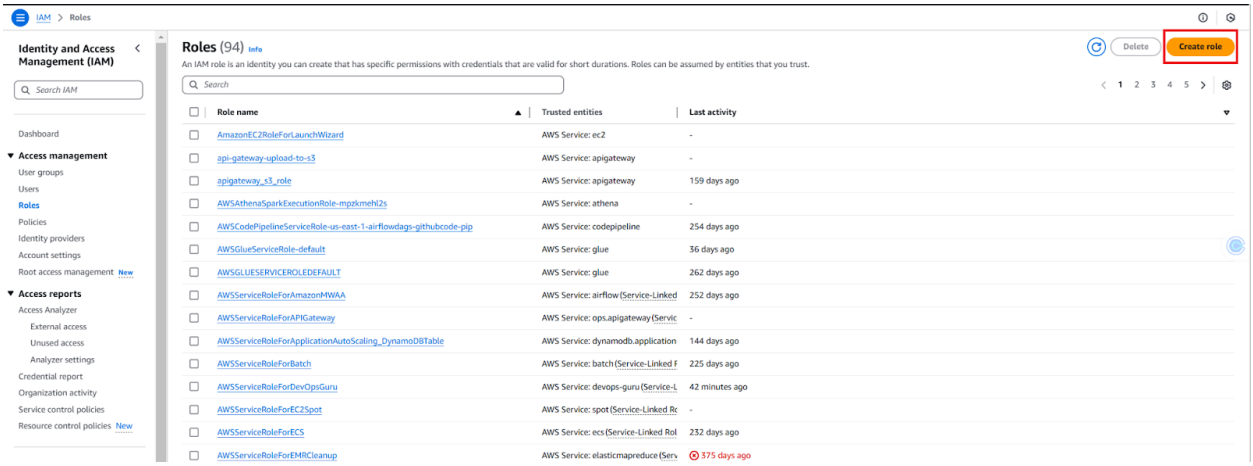


Role Creation

- Navigate to the “Roles” button located on the left-hand side of the page, which will direct us to the following page shown below.



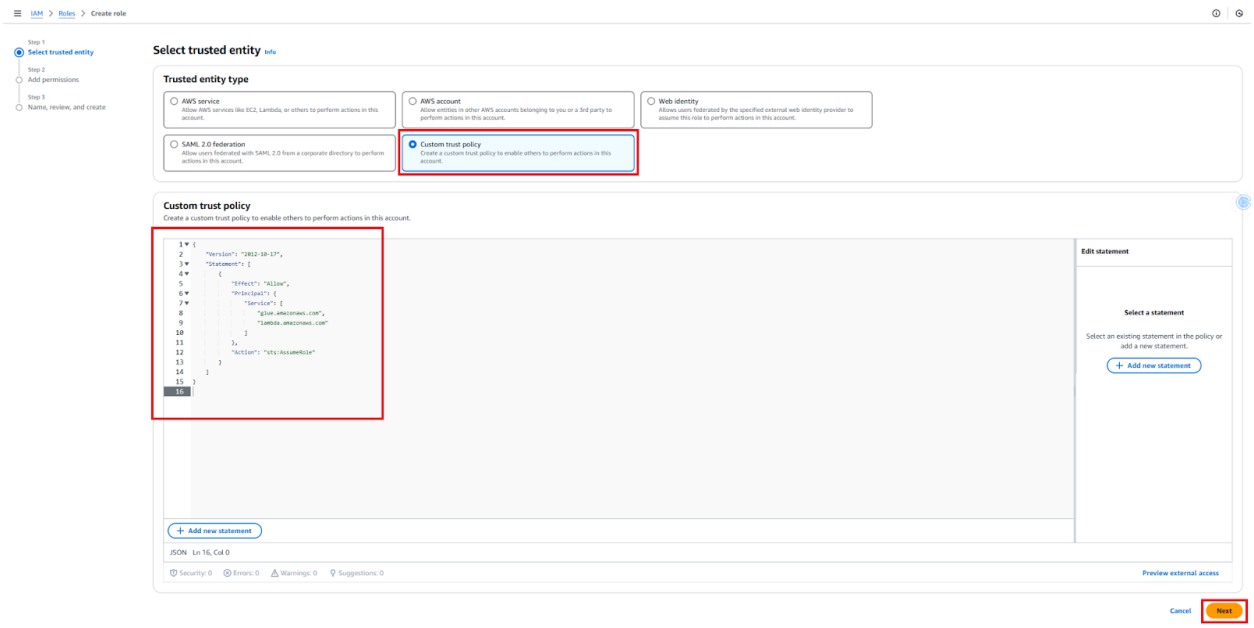
- Next, click on the "Create role" button.



- On the next page, choose Custom trust policy option as indicated below. Then, paste the following JSON into the Custom trust policy box and click Next.

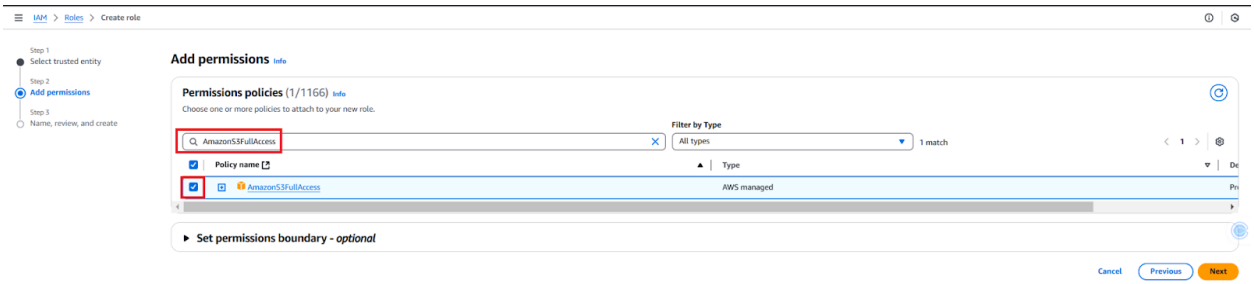
```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
```

```
        "Principal": {
            "Service": [
                "glue.amazonaws.com",
                "lambda.amazonaws.com"
            ]
        },
        "Action": "sts:AssumeRole"
    }
  ]
}
```

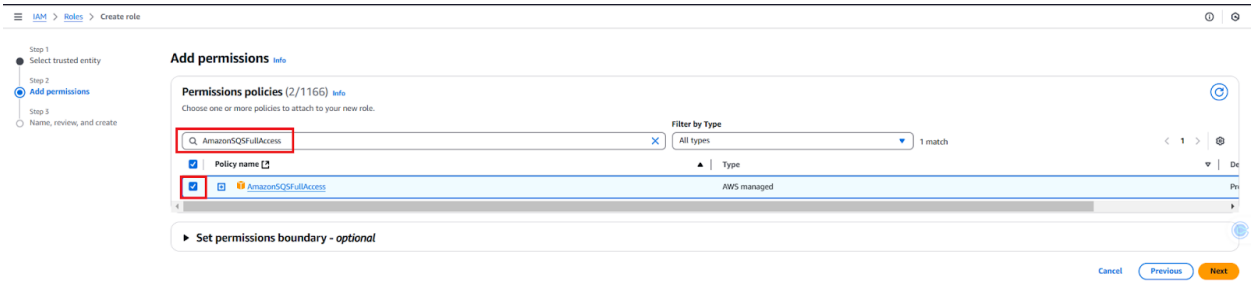


- On the following page for ADD permissions, please locate the below listed policies individually and select each one to include them in your role.

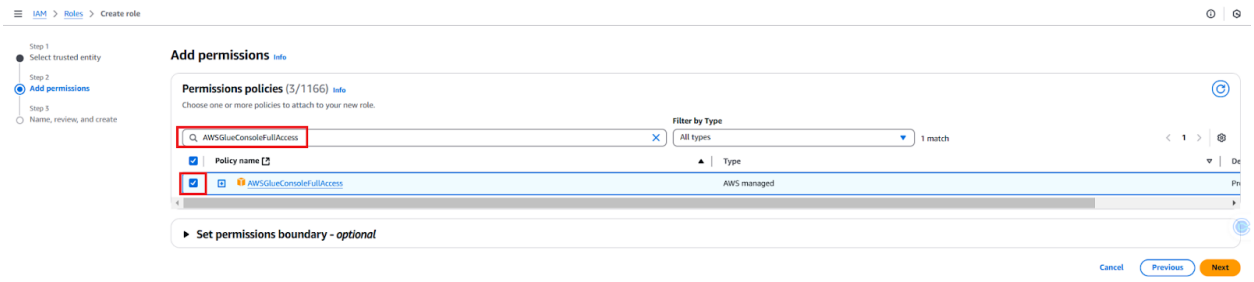
- AmazonS3FullAccess



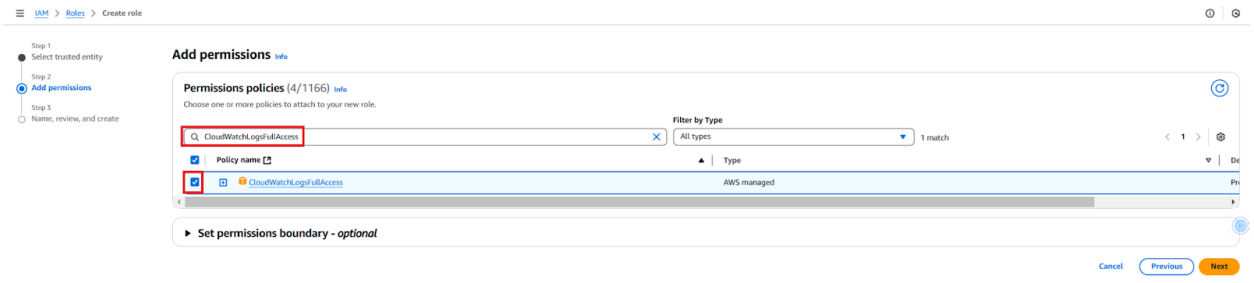
- AmazonSQSFullAccess



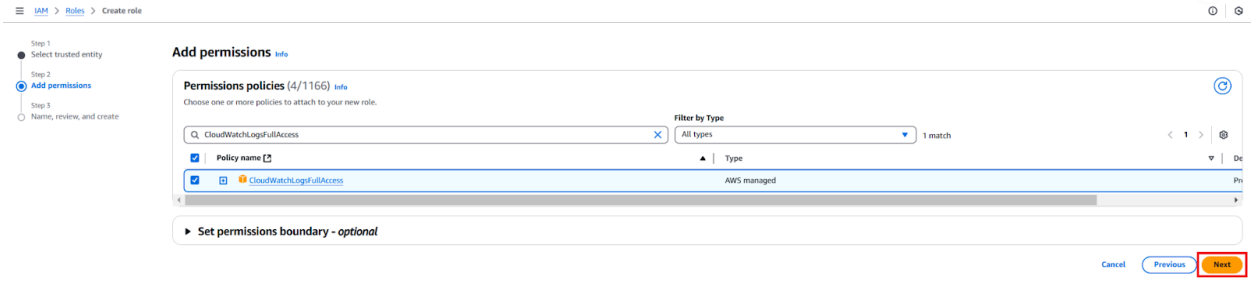
- AWSGlueConsoleFullAccess



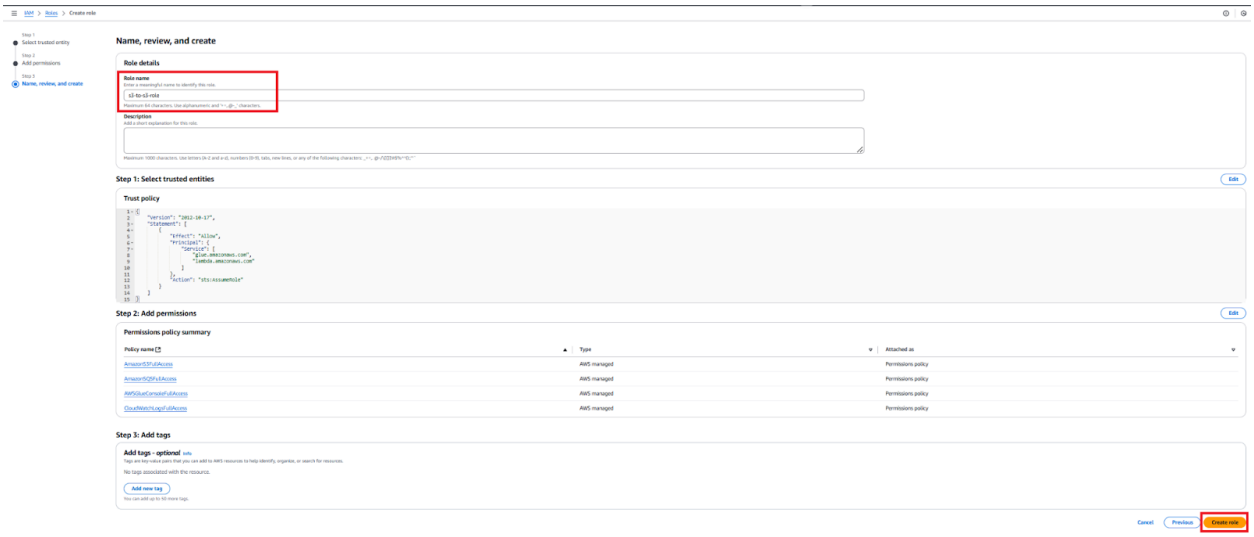
- CloudWatchLogsFullAccess



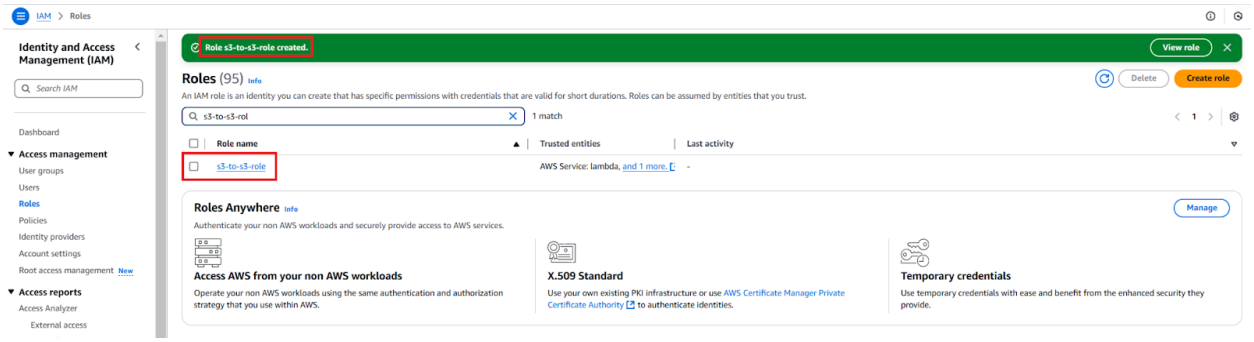
- After selecting all the policies, click on the "Next" button.



- On the following page, provide an appropriate name for the role <s3-to-s3-role>, then click the "Create role" button.



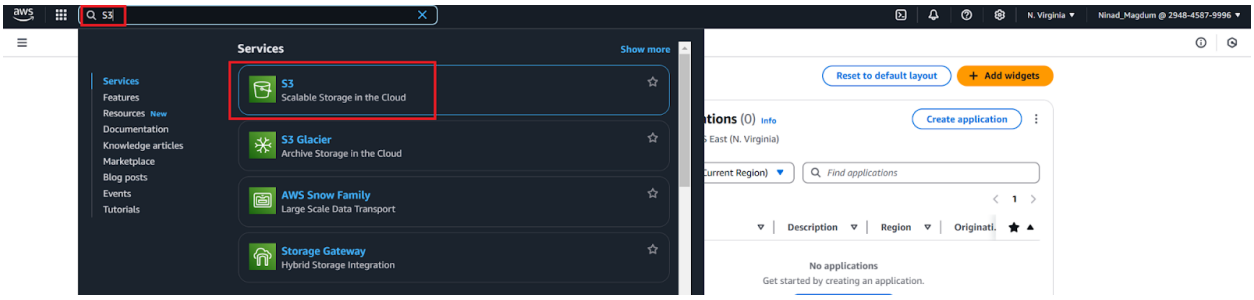
- The required role is created successfully



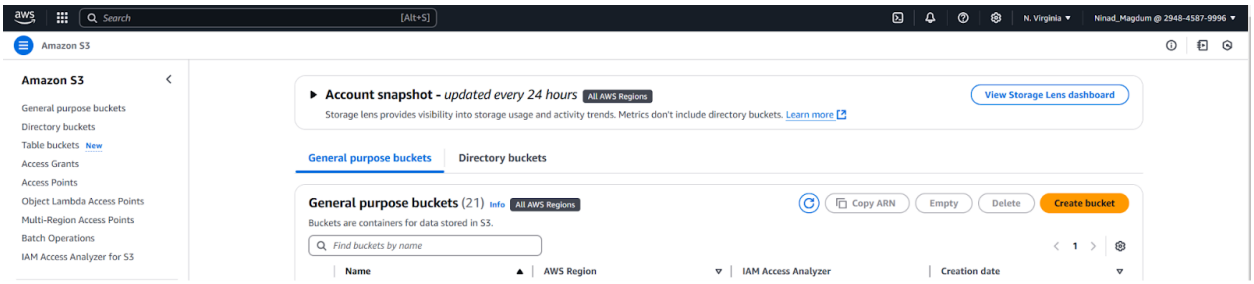
VOILA! YOUR SUCCESSFULLY CREATED YOUR S3 TO S3 IAM ROLE AND ATTACHED SPECIFIC POLICIES

AWS S3 Buckets Creation guide

- Access your AWS Management Console and find AWS S3 by entering "S3" in the search bar.

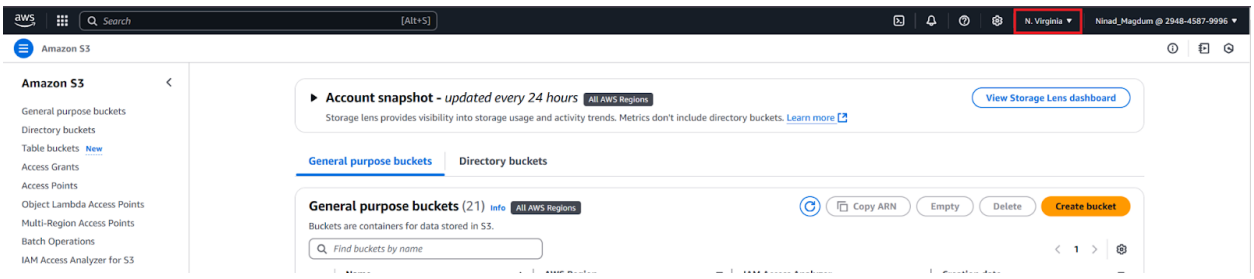


- Select S3 from the menu, which will direct you to the page where you can create an S3 Bucket.

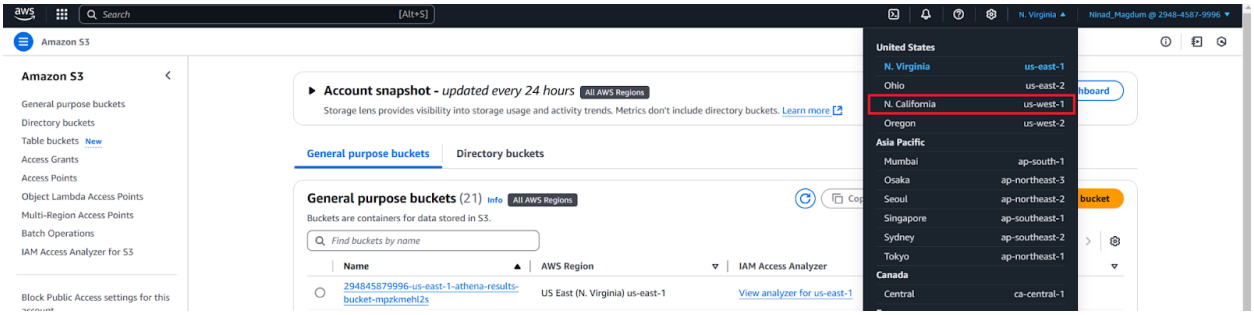


Source Bucket Creation

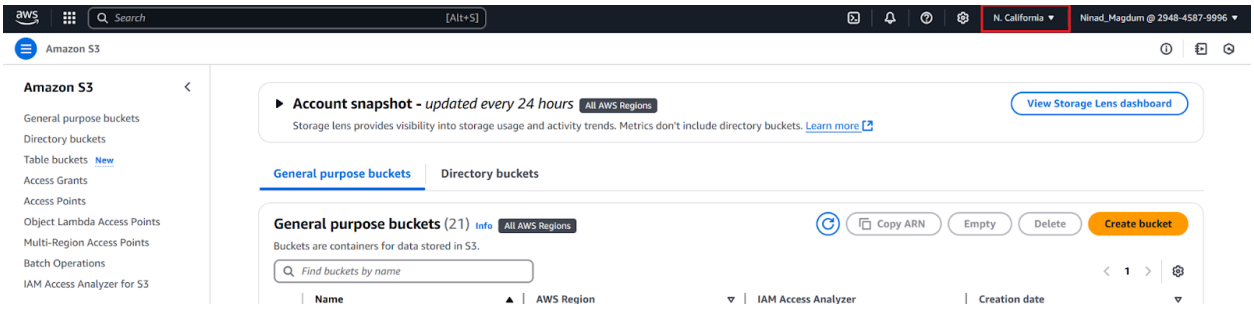
- Now let's create the source S3 bucket in the region other than your AWS default region. Click on the Region button on the top right hand corner of your AWS Management Console. Whatever is the existing region is your default region



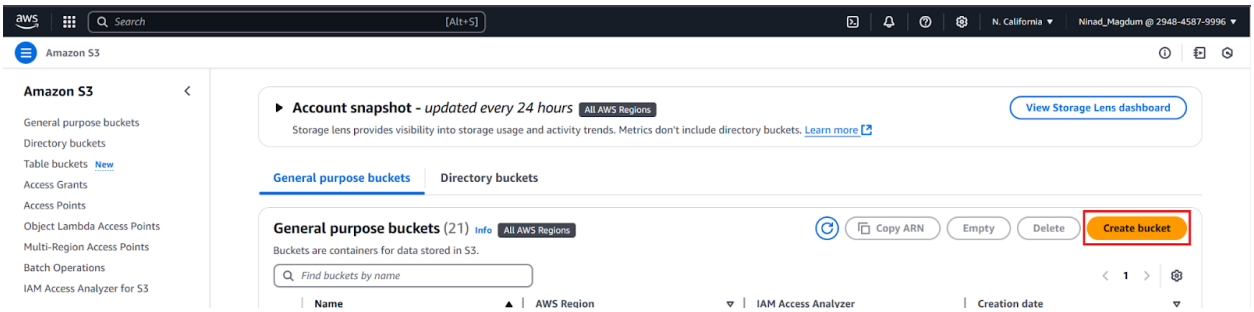
- Select any region other than your already existing AWS default region to create your Source bucket. I am selecting us-west-1 (my default AWS region is us-east-1 in your case it might be different)



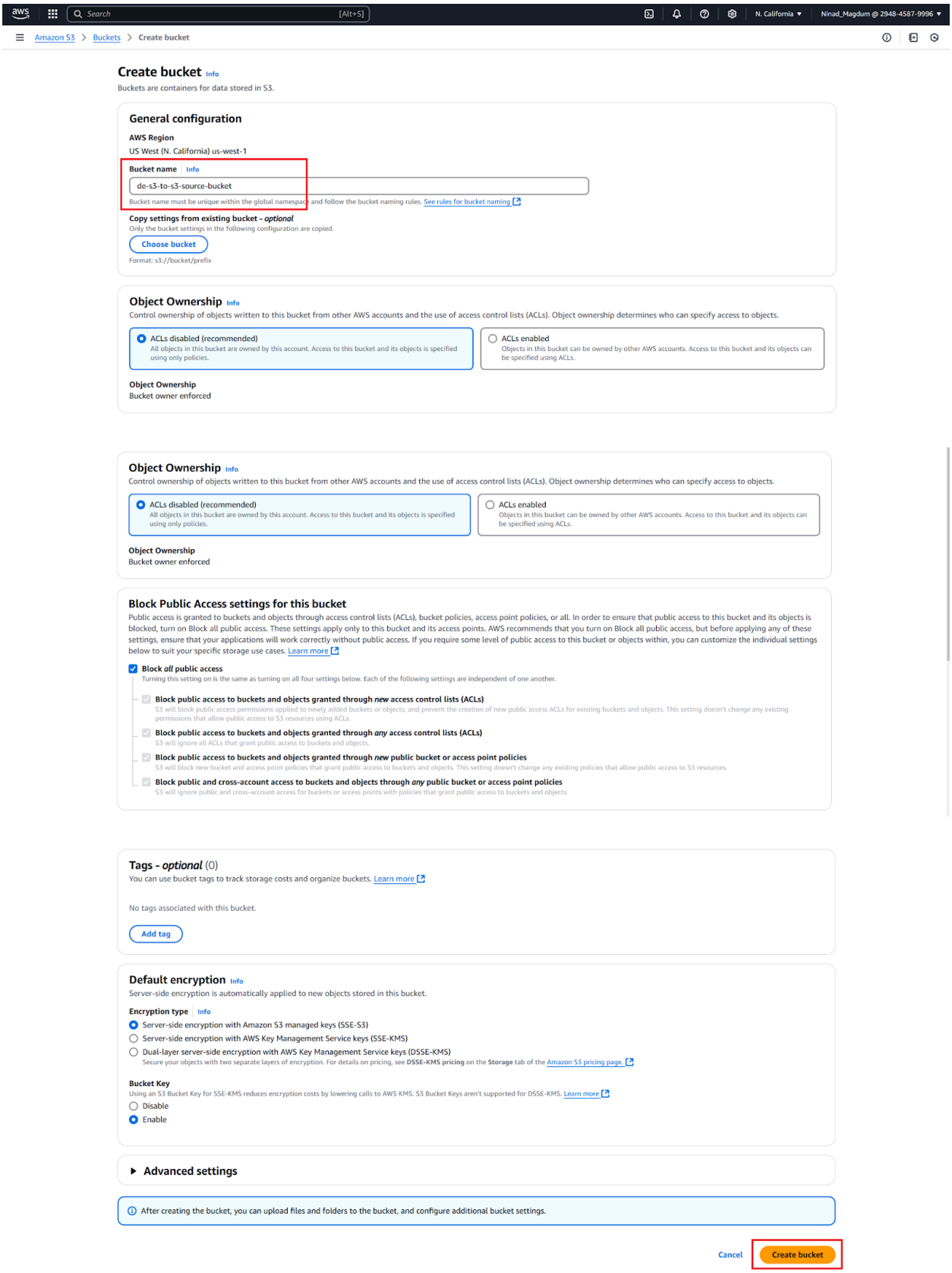
- Once selected validate your AWS region changes to the new region



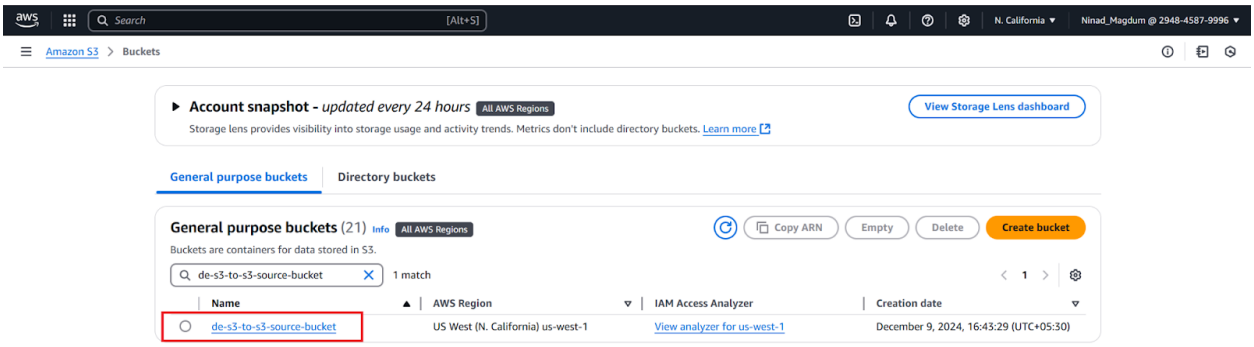
- Click on the Create bucket button to create the source bucket



- Once you click Create bucket, we will be landing onto the below page where first validate the region and then we need to fill the source bucket name <de-s3-to-s3-source-bucket> and click Create bucket

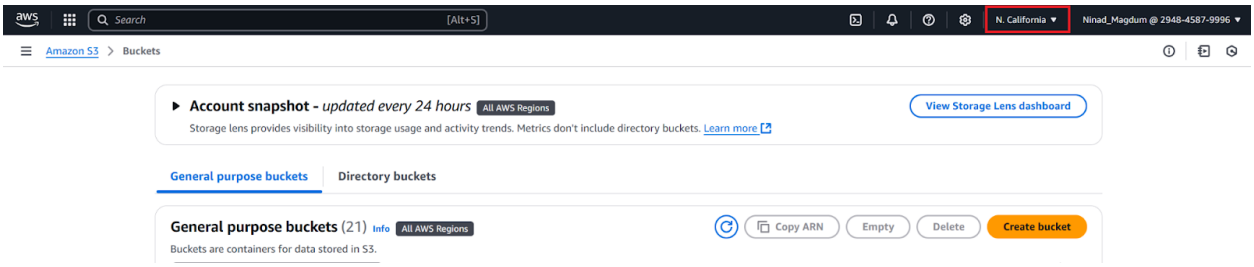

Search [Alt+S]
N. California
Ninad_Magdum @ 2948-4587-9996
Amazon S3 > Buckets > Create bucket
Create bucket Info
Buckets are containers for data stored in S3.
General configuration
AWS Region
US West (N. California) us-west-1
Bucket name Info
de-s3-to-s3-source-bucket
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Format: s3://bucket/prefix
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
Object Ownership
Bucket owner enforced
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
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 your 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 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 objects.
Tags - optional (0)
You can use bucket tags to track storage costs and organize buckets. Learn more
No tags associated with this bucket.
Add tag
Default encryption Info
Server-side encryption is automatically applied to new objects stored in this bucket.
Encryption type Info
Server-side encryption with Amazon S3 managed keys (SSE-S3)
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the Amazon S3 pricing page
Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more
Disable
Enable
Advanced settings
After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.
Cancel
Create bucket

- After clicking Create bucket, you will be directed to the following page confirming the successful creation of your s3 source bucket.

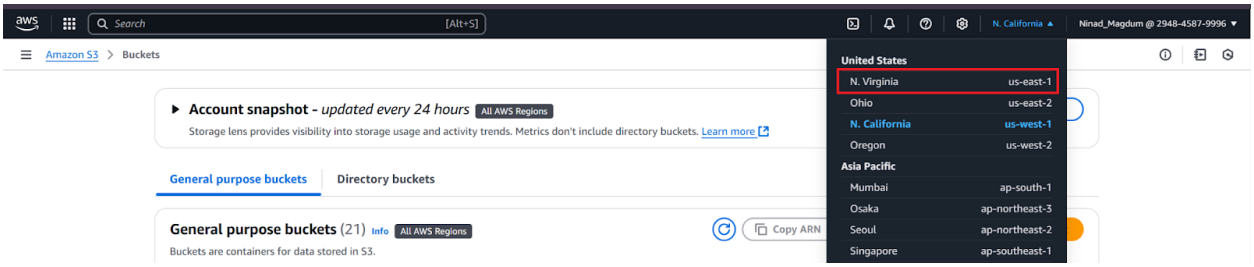


Target Bucket Creation

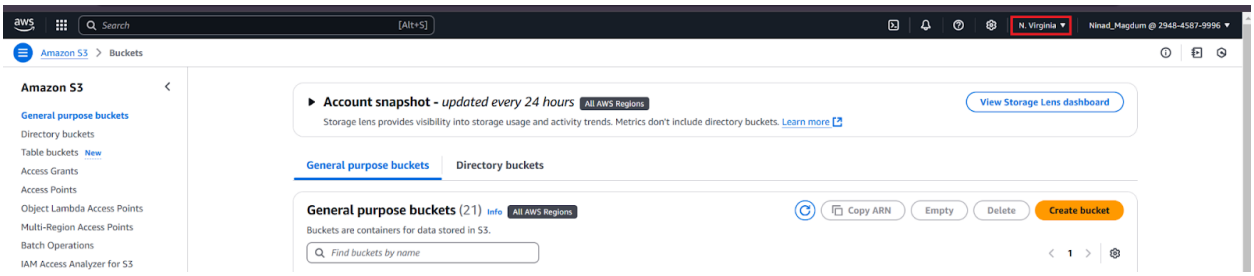
- Now let's create the target S3 bucket in your AWS default region. Click on the Region button on the top right hand corner of your AWS Management Console.



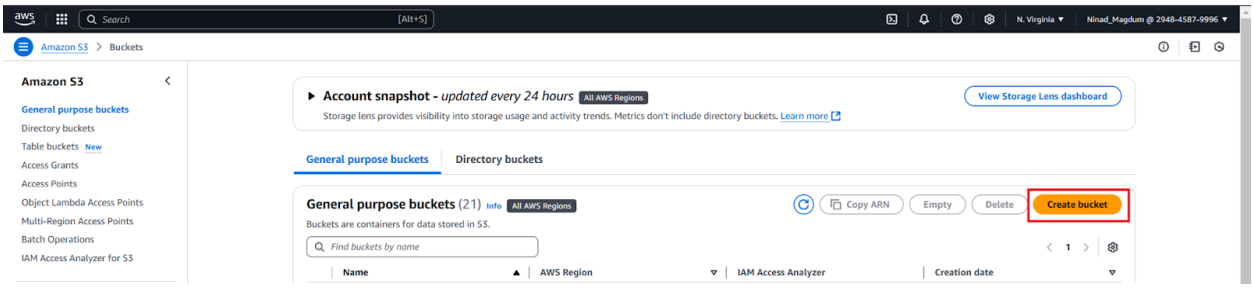
- Select your default AWS region. Mine is us-east-1, it will be different for you.



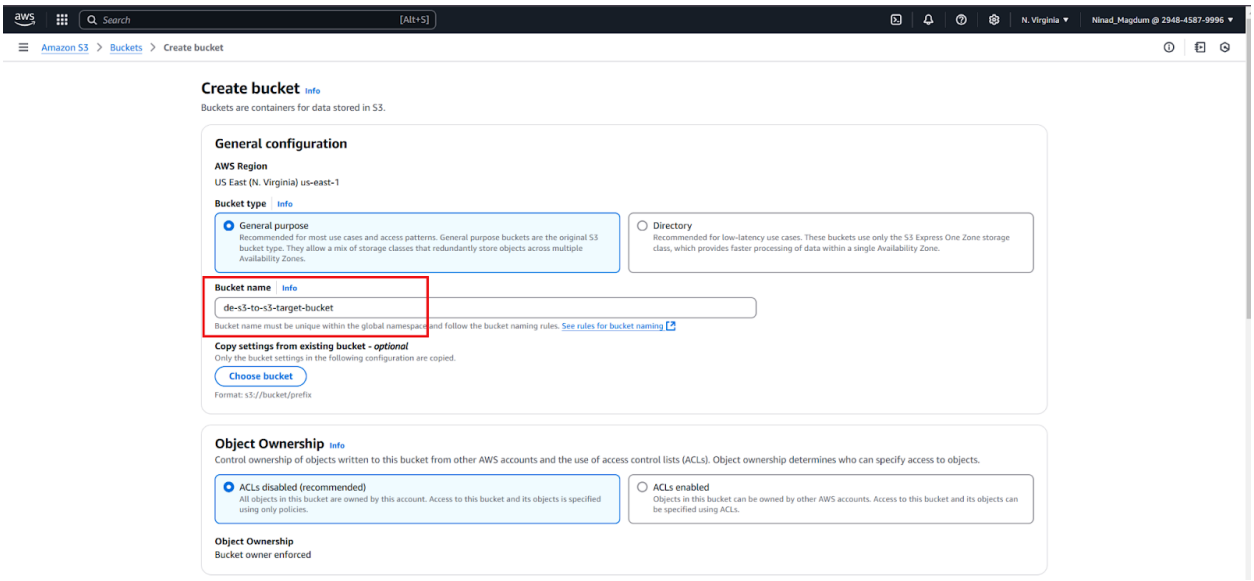
- Once selected validate your AWS region changes to the default AWS region

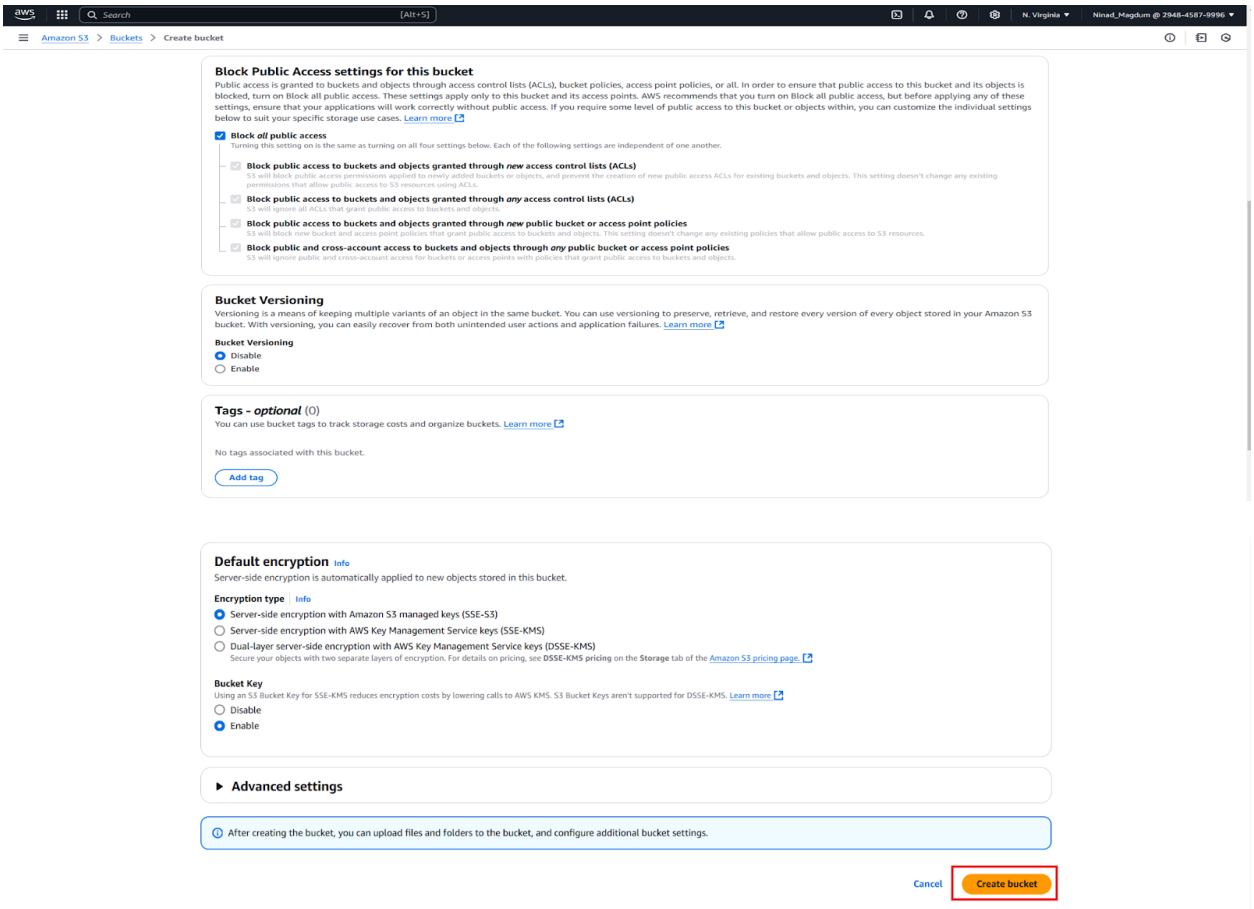


- Click on the Create bucket button to create the target bucket

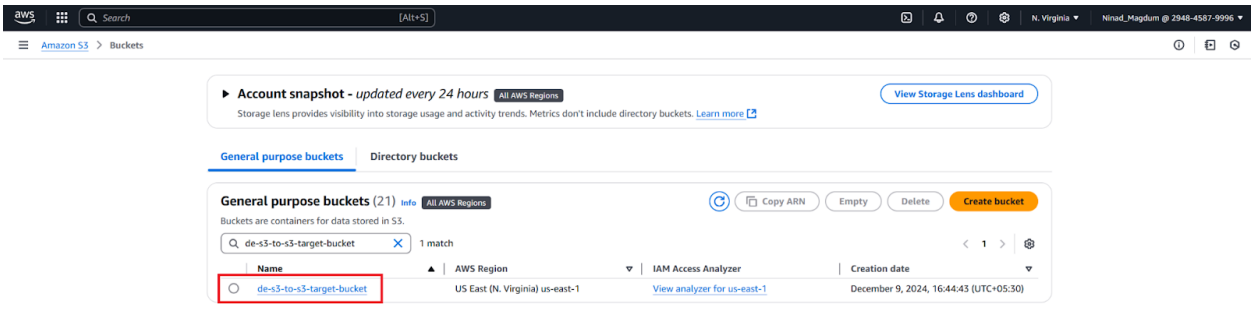


- Once you click Create bucket, we will be landing onto the below page where first validate the region and then we need to fill the target bucket name <de-s3-to-s3-target-bucket> and click Create bucket





- After clicking Create bucket, you will be directed to the following page confirming the successful creation of your s3 target bucket.



VOILA! YOU HAVE SUCCESSFULLY CREATED YOUR BOTH SOURCE AND TARGET S3 BUCKETS

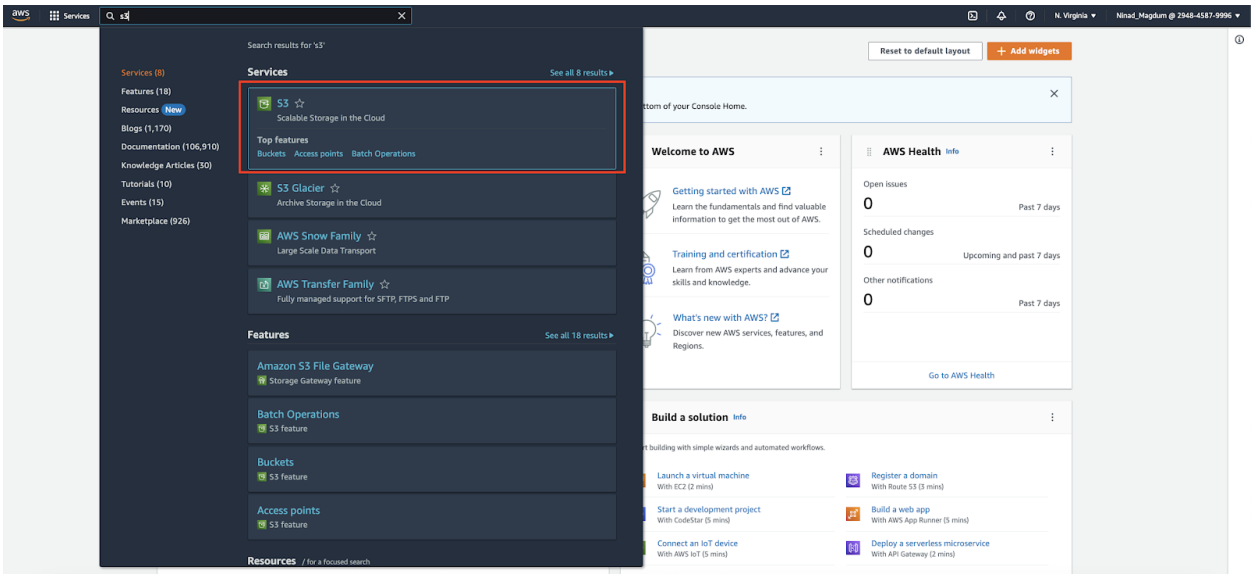
AWS SNS Topic Creation guide

- Let us understand and walk through the process of creation of AWS SNS (Simple Notification Service) Topic

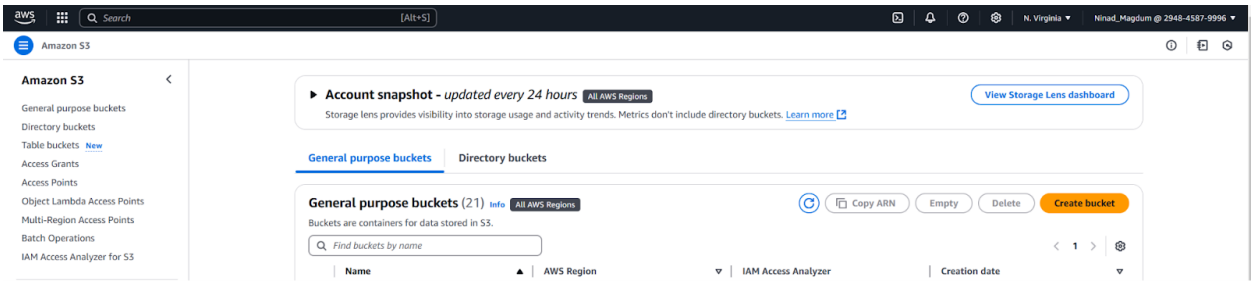
Identify the SNS Topic AWS Region

First we need to identify the AWS region in which we need to create the required SNS (Simple Notification Service) Topic

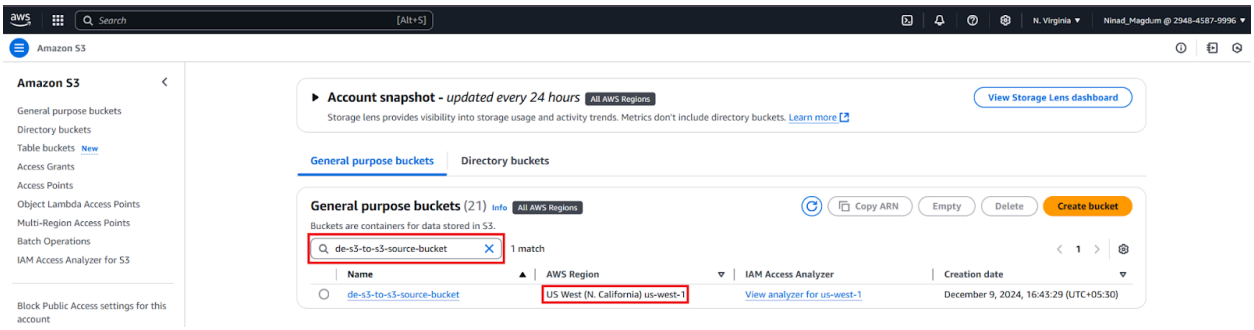
- Access your AWS Management Console and find AWS S3 by entering "S3" in the search bar.



- Select S3 from the menu, which will direct you to the page where you can see all of your buckets.

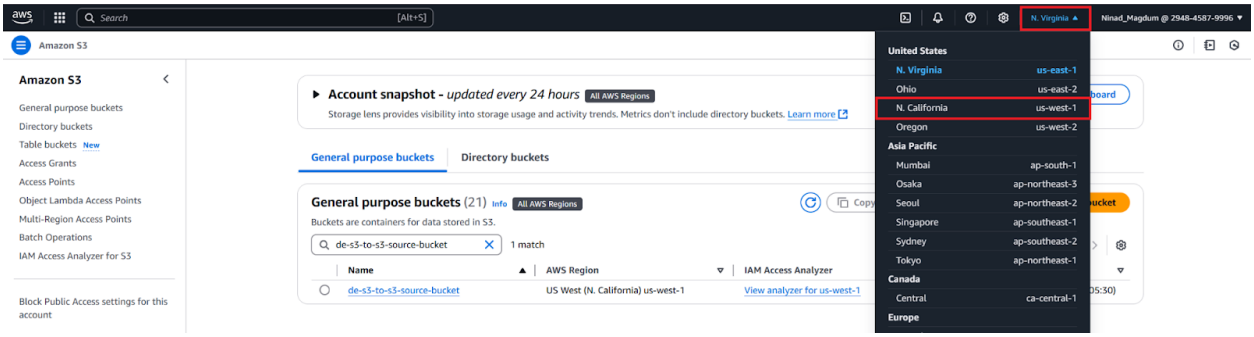


- Search your source bucket created for this project in the search bar and note down the AWS region of the same.

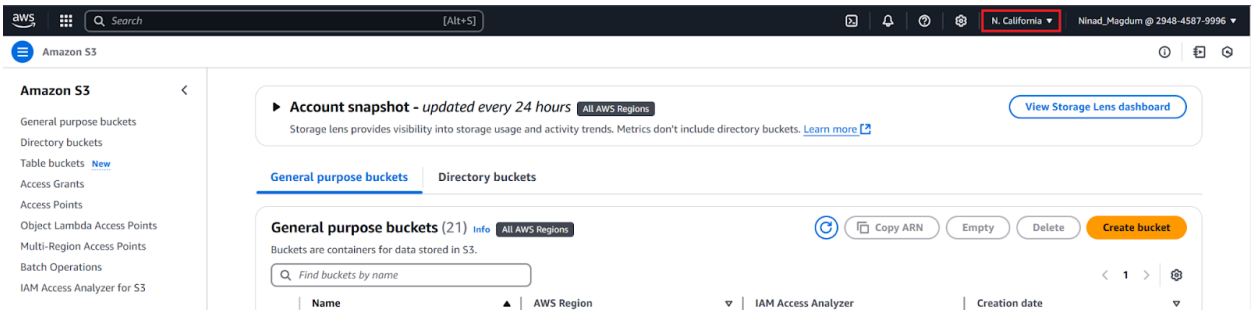


In my case the region is us-west-1, in your case it might be different

- Click on the Region button on the top right hand corner of your AWS Management Console. Change the AWS region to the source bucket region.



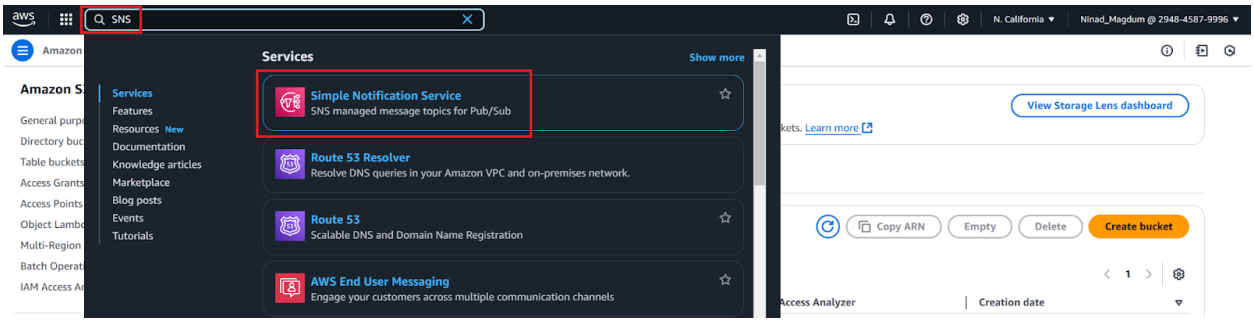
- Once selected validate your AWS region changed to the source bucket region.



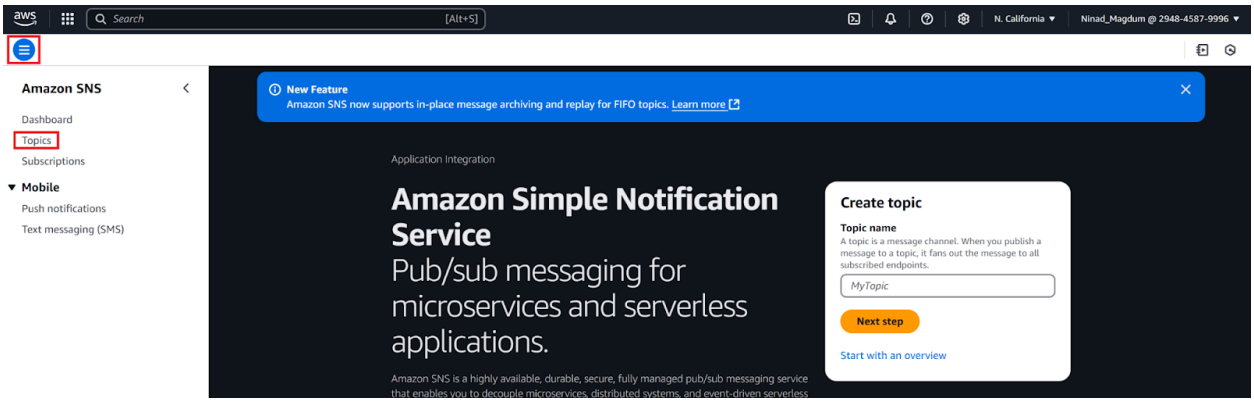
This is the region where we are going to create the SNS topic required for this project

Creation of SNS Topic

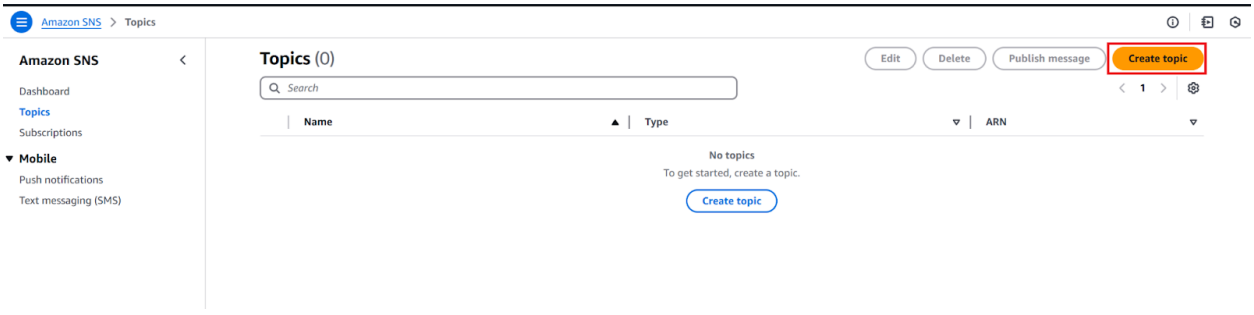
- In your AWS Management Console, search for SNS by entering "SNS" in the search bar and select Simple Notification Service



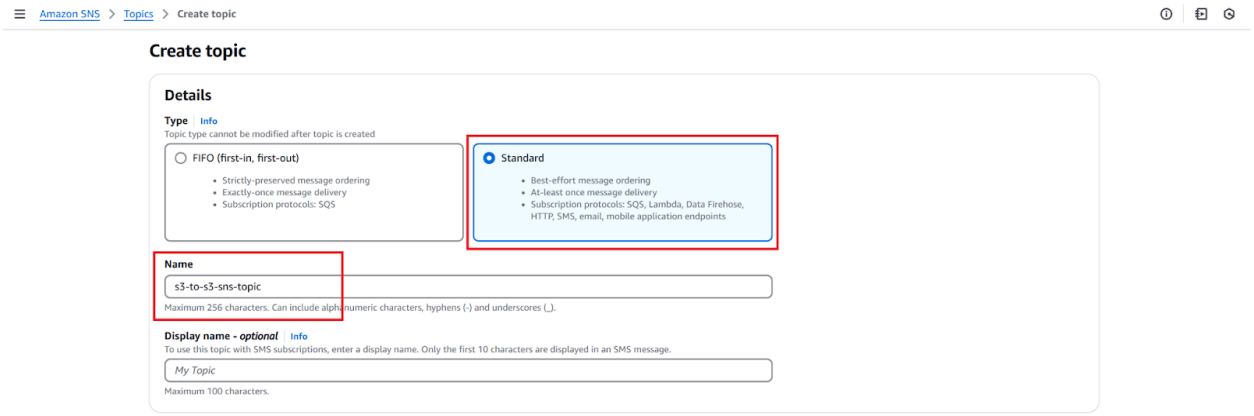
- On the SNS page , click the three line menu button on the left top corner and then click on the Topics button



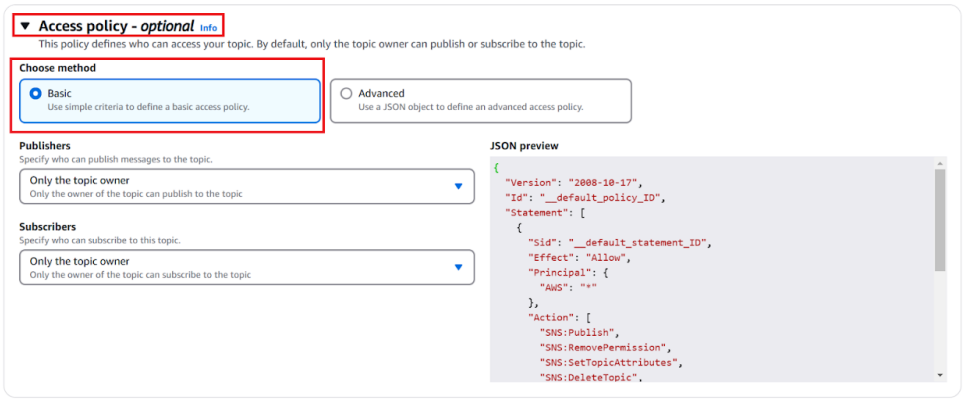
- Once in the Topics page, click on the Create topic button to create a new SNS topic



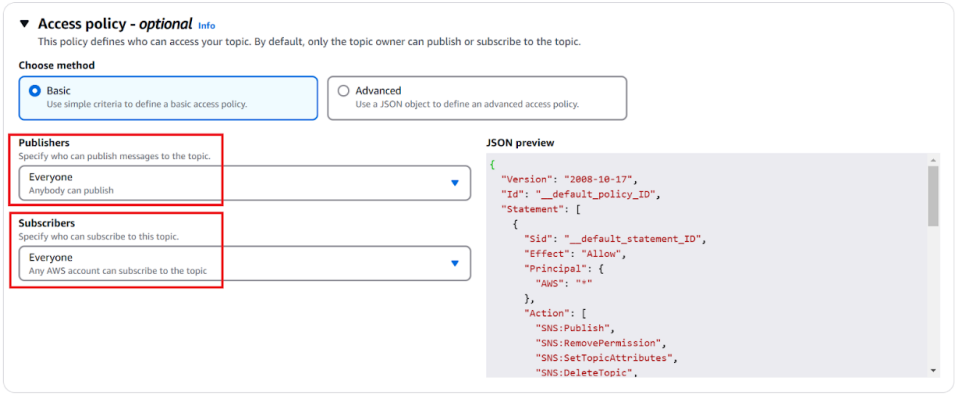
- Under the Create topic page, select the Type as Standard and provide the name of the topic <s3-to-s3-sns-topic>



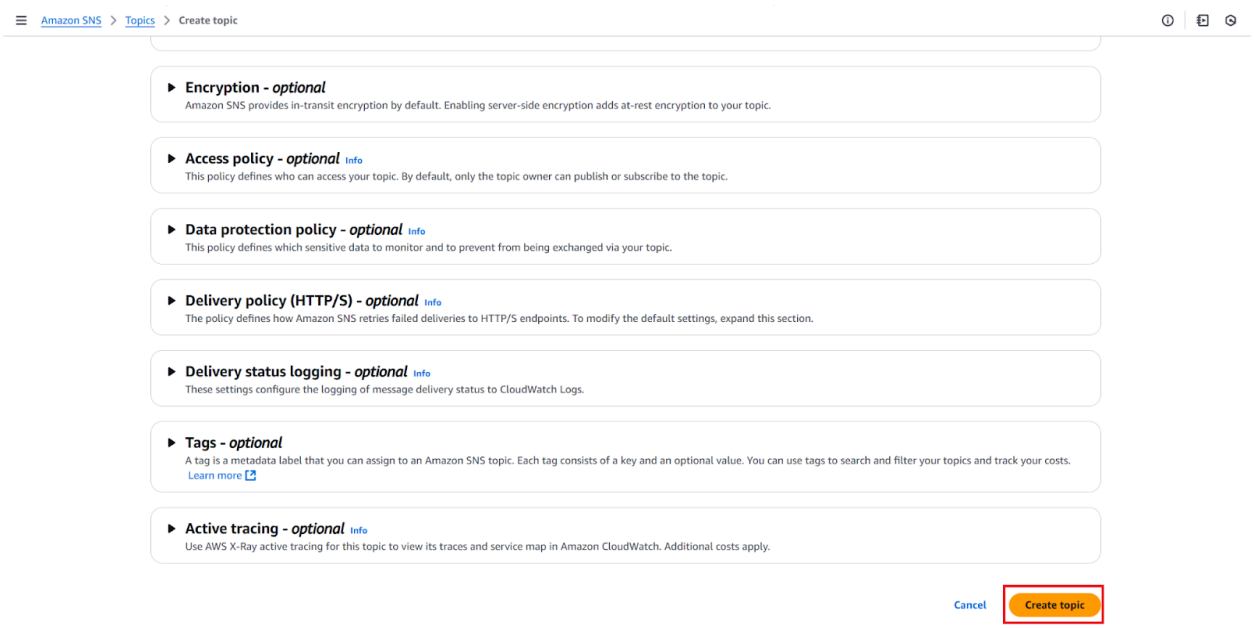
- On the same page click on the Access policy section and choose the method as Basic.



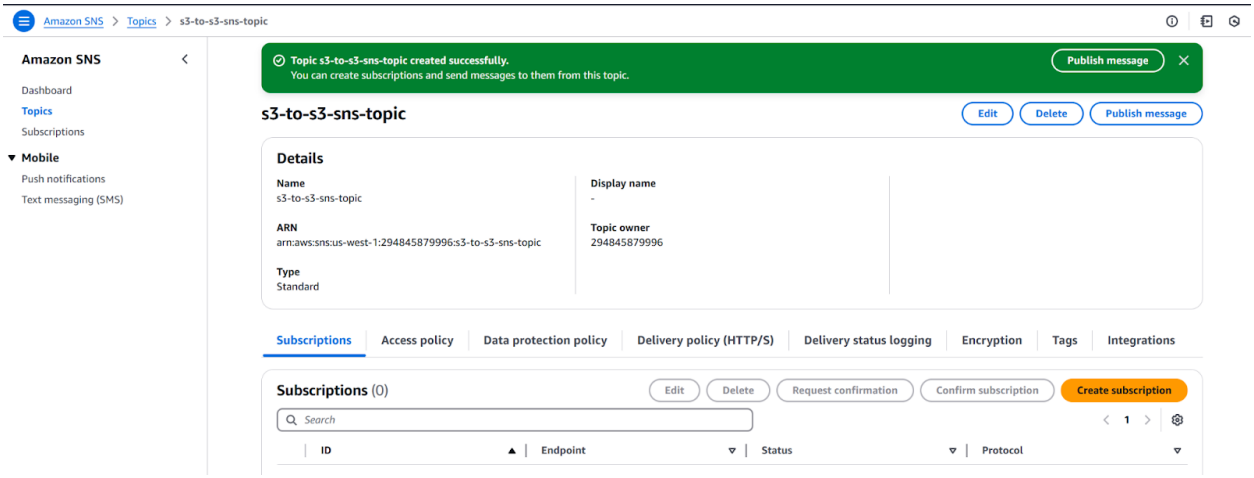
- Select Everyone in the both Publishers and Subscribers section



- Scroll down and click on the Create topic button to create your SNS topic.



- Once clicked your SNS topic will be created successfully.



VOILA! YOU HAVE SUCCESSFULLY CREATED YOUR SNS TOPIC IN YOUR SOURCE S3 BUCKET REGION

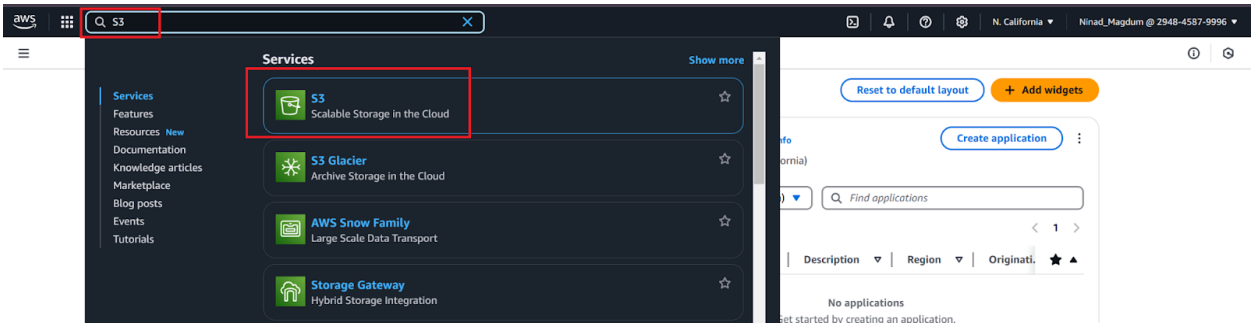
AWS SQS Queue Creation guide

- Let us understand and walk through the process of creation of AWS SQS (Simple Queue Service) Queue required for the lambda function

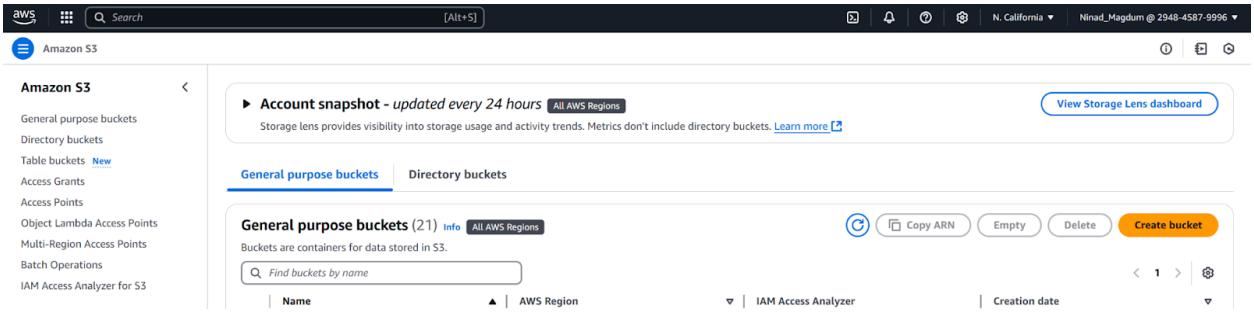
Identify the SQS Queue AWS Region

First we need to identify the AWS region in which we need to create the required AWS SQS (Simple Queue Service) Queue required for the lambda function

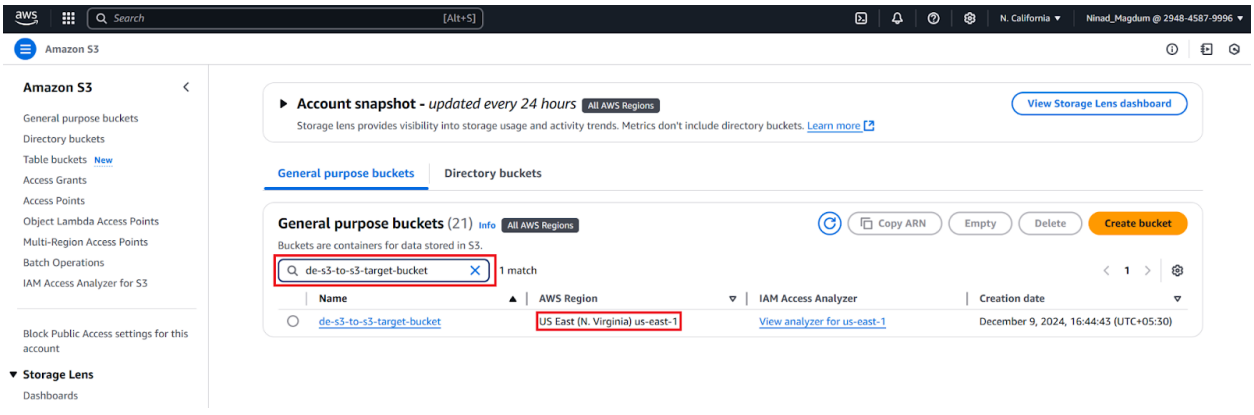
- Access your AWS Management Console and find AWS S3 by entering "S3" in the search bar.



- Select S3 from the menu, which will direct you to the page where you can see all of your buckets.

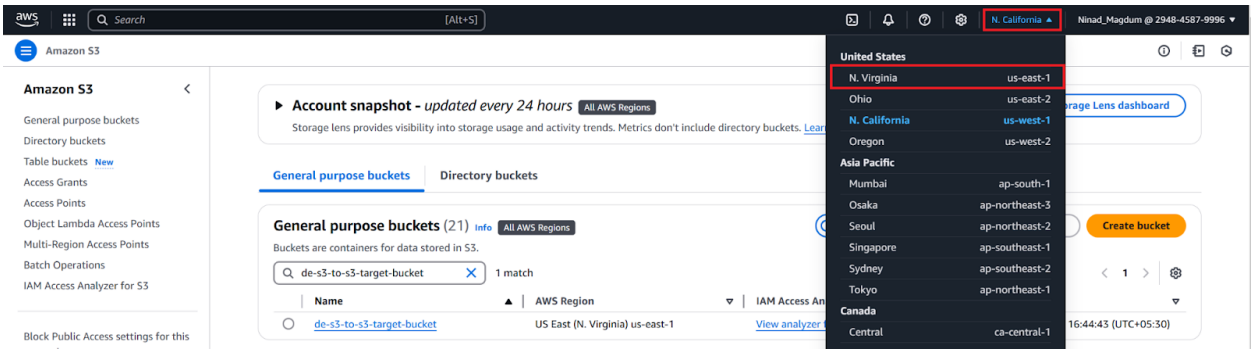


- Search your target bucket created for this project in the search bar and note down the AWS region of the same.

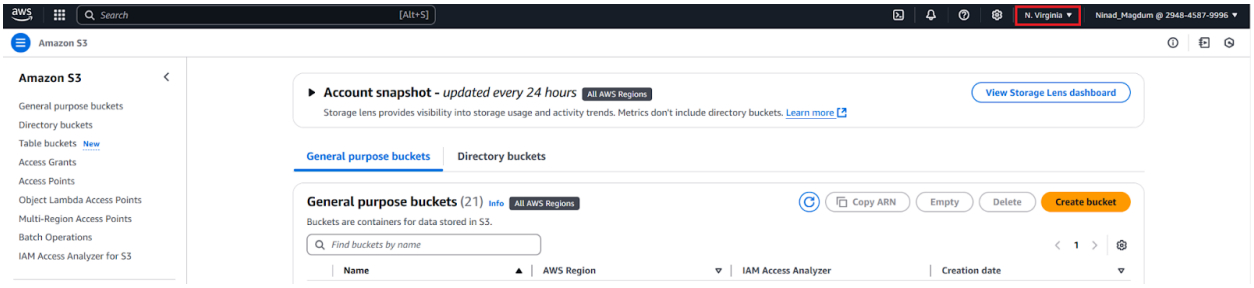


In my case the region is us-east-1, in your case it might be different.

- Click on the Region button on the top right hand corner of your AWS Management Console. Change the AWS region to the target bucket region.



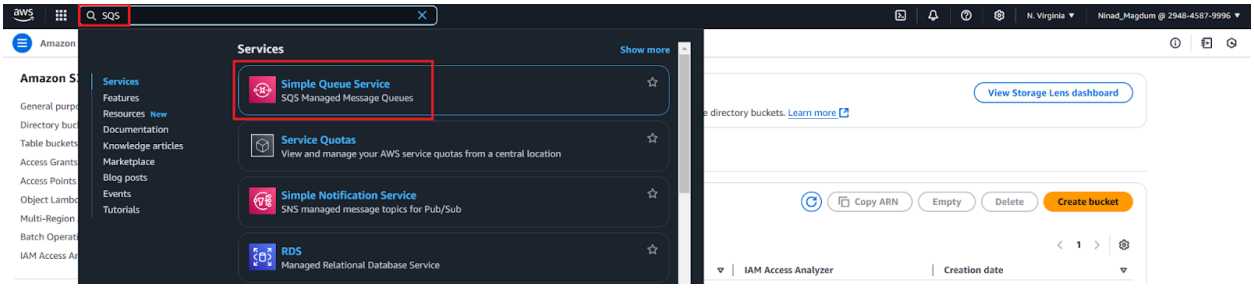
- Once selected validate your AWS region changed to the target bucket region.



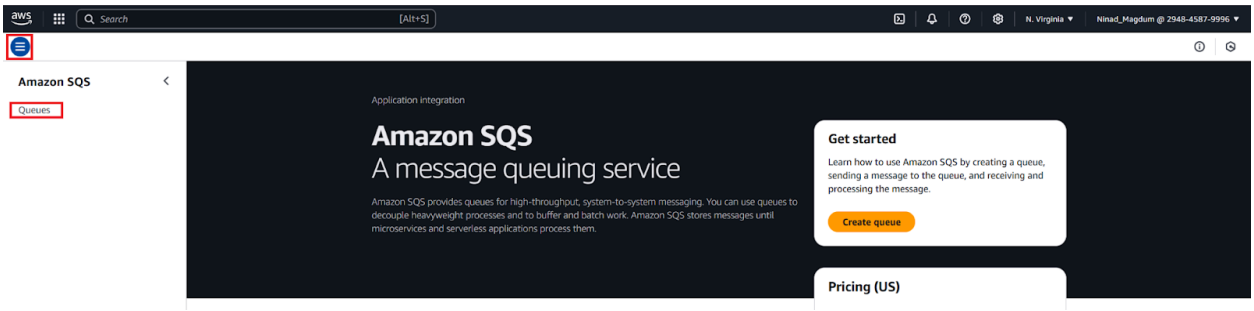
This is the region where we are going to create the SQS Queue required for this project lambda function

Creation of SQS Queue for the lambda

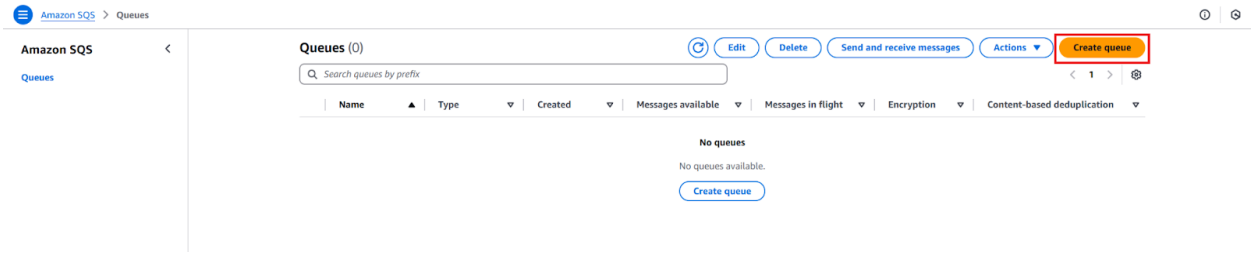
- In your AWS Management Console, search for SQS by entering "SQS" in the search bar and select Simple Queue Service



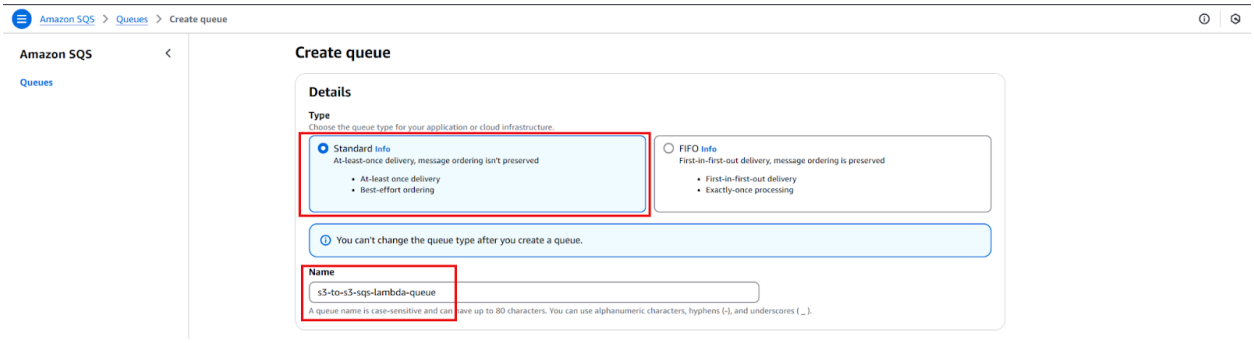
- On the SQS page , click the three line menu button on the left top corner and then click on the Queues button



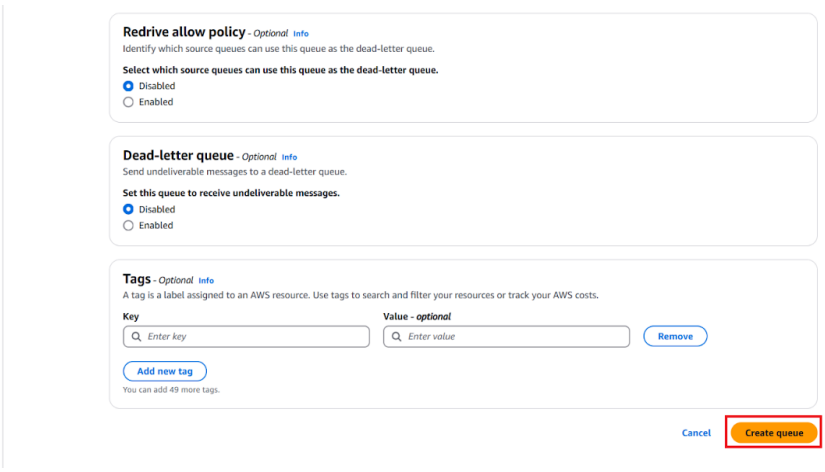
- Once in the Queues page, click on the Create queue button to create a new SQS queue



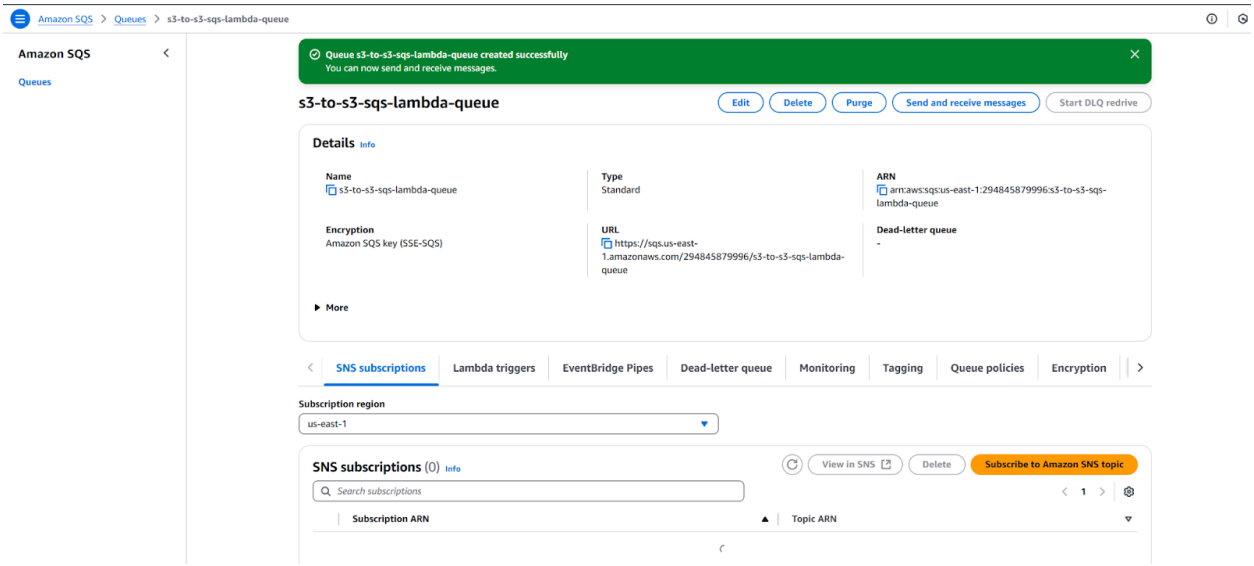
- Under the Create queue page, select the Type as Standard and provide the name of the queue <s3-to-s3-sqs-lambda-queue>



- Scroll down and click on the Create queue button to create your SQS queue for the lambda function.



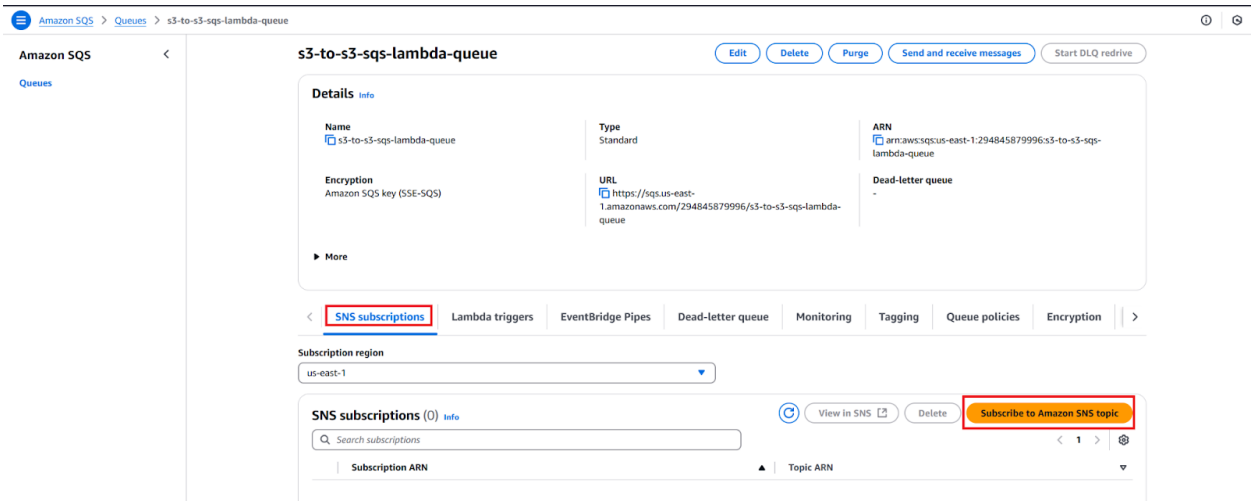
- Your SQS queue for the lambda function will be created successfully.



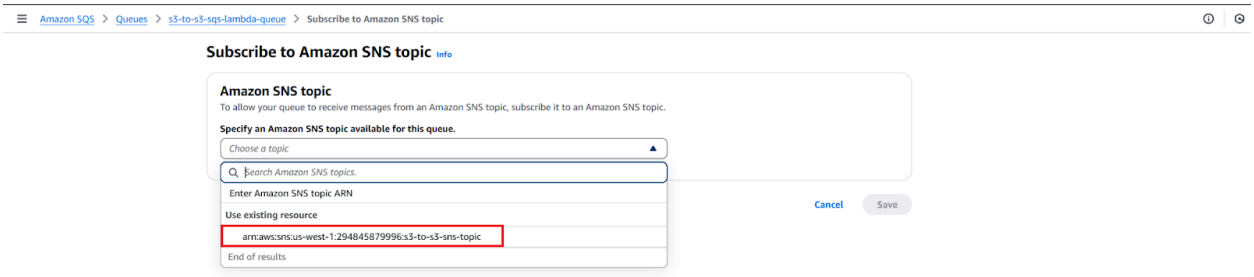
Creation of SNS subscription for the lambda queue

Once the lambda SQS queue is created successfully, we need to create the SNS subscription to receive notification from SNS topic created in the previous step

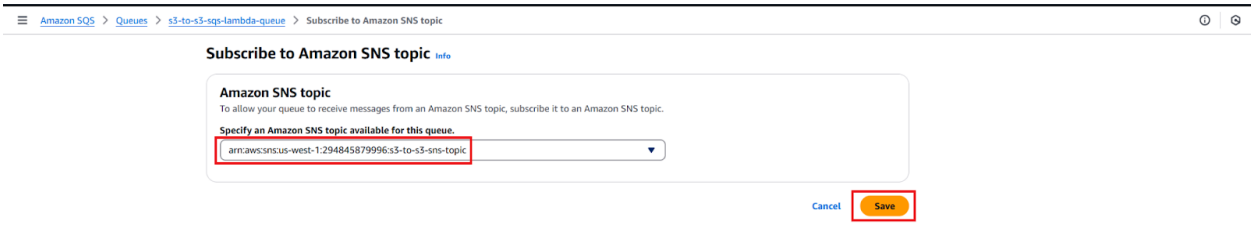
- On the lambda SQS queue page, click the SNS subscriptions tab, and then click the Subscribe to Amazon SNS topic button



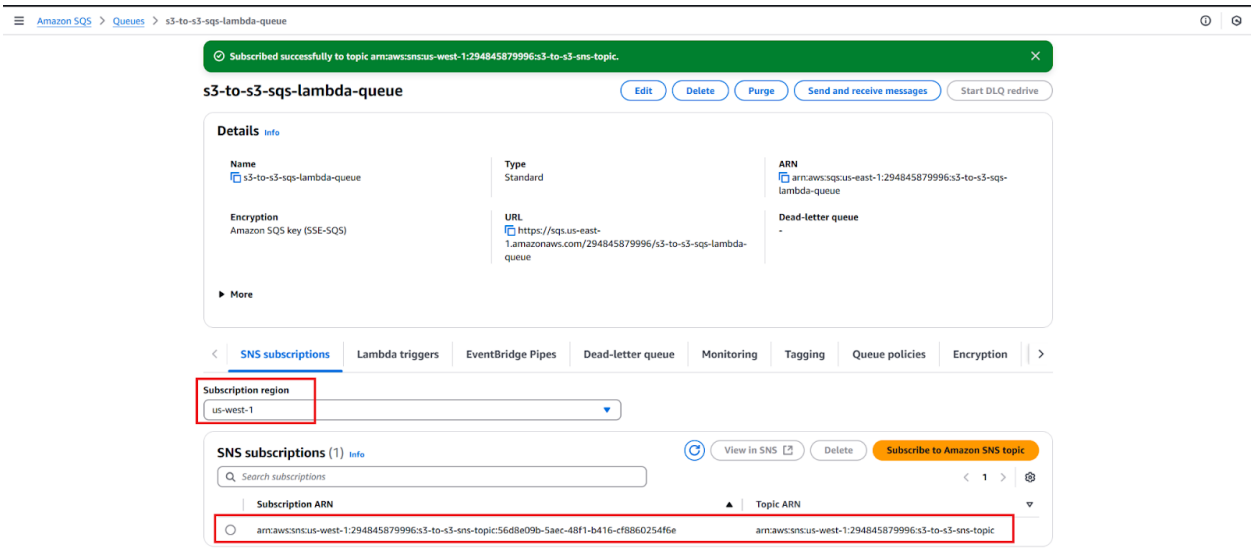
- Select the SNS topic created for the project on the next page



- Click the Save button after selecting the SNS topic



- Once the subscription is created successfully, select the region where your SNS topic is created to confirm the subscription is created



VOILA! YOU HAVE SUCCESSFULLY CREATED YOUR SQS QUEUE FOR YOUR LAMBDA FUNCTION

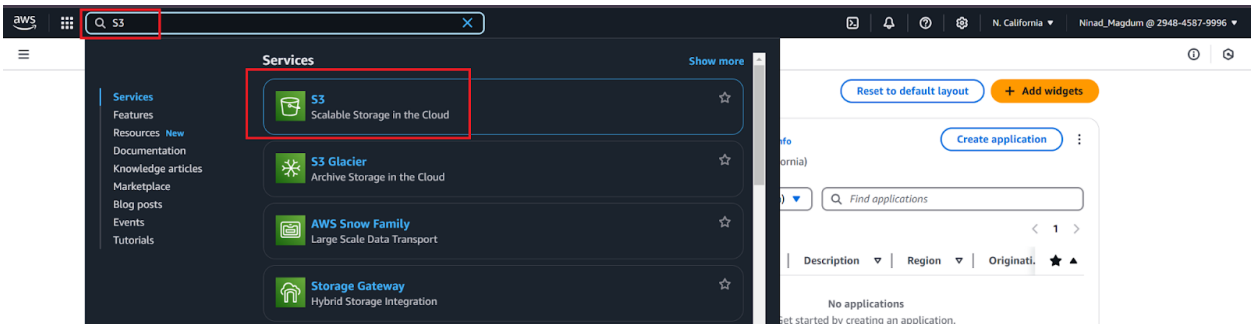
AWS Lambda Function Creation guide

- Let us understand and walk through the process of creation of AWS lambda function

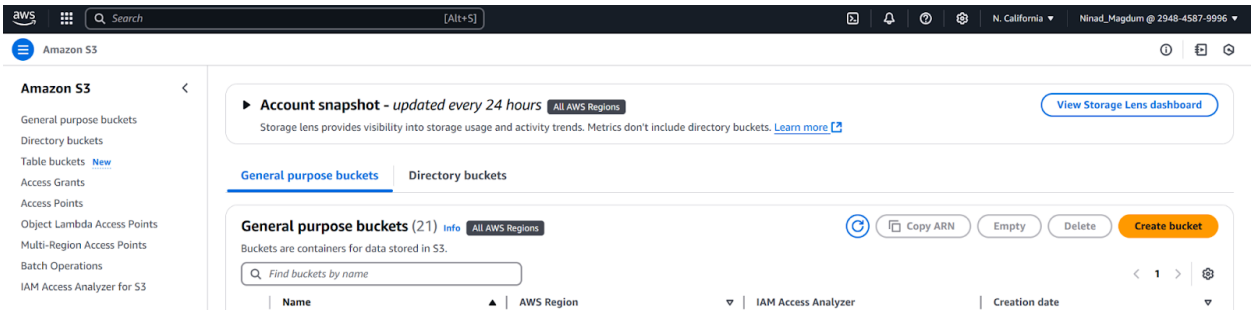
Identify the Lambda function AWS Region

First we need to identify the AWS region in which we need to create the required lambda function for this project

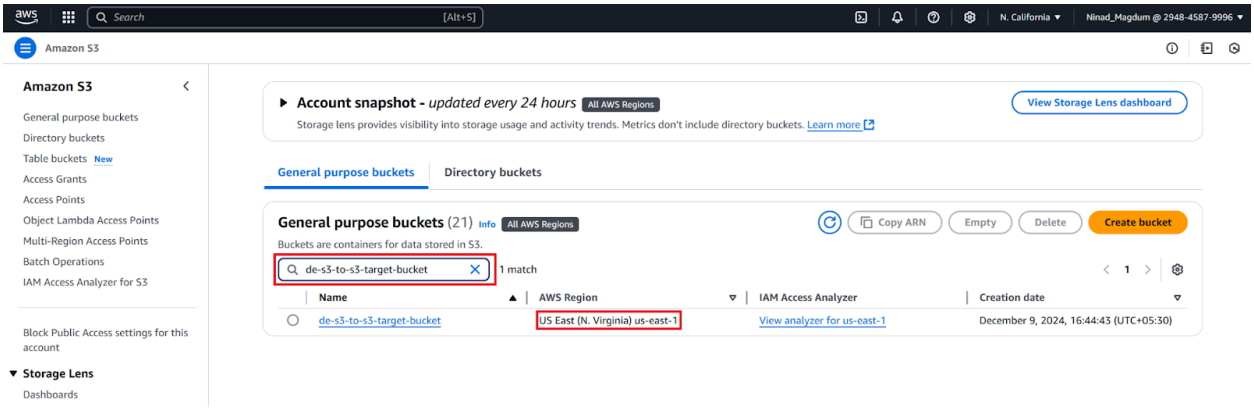
- Access your AWS Management Console and find AWS S3 by entering "S3" in the search bar.



- Select S3 from the menu, which will direct you to the page where you can see all of your buckets.

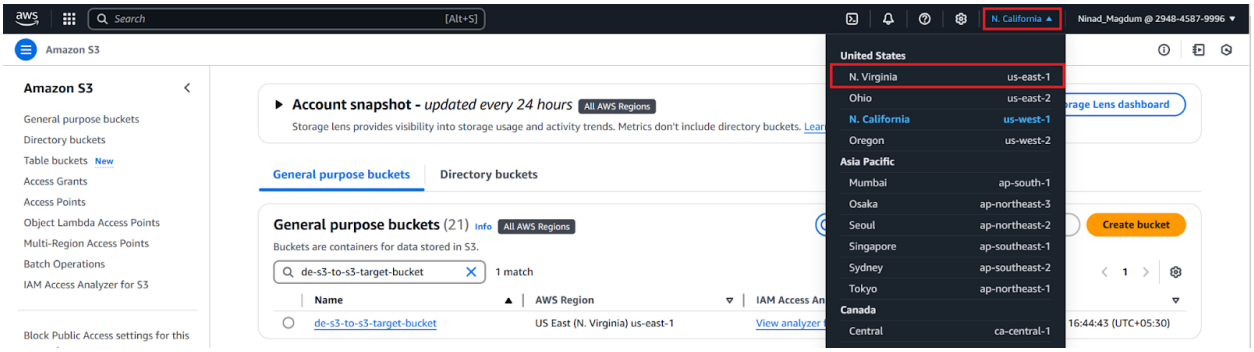


- Search your target bucket created for this project in the search bar and note down the AWS region of the same.

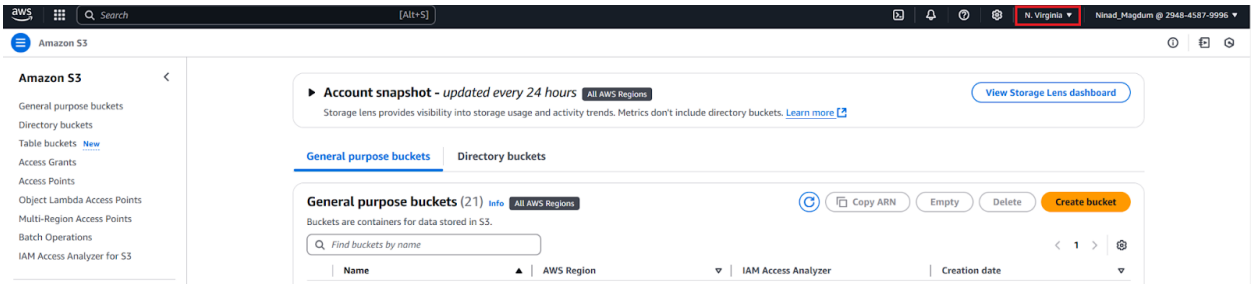


In my case the region is us-east-1, in your case it might be different.

- Click on the Region button on the top right hand corner of your AWS Management Console. Change the AWS region to the target bucket region.



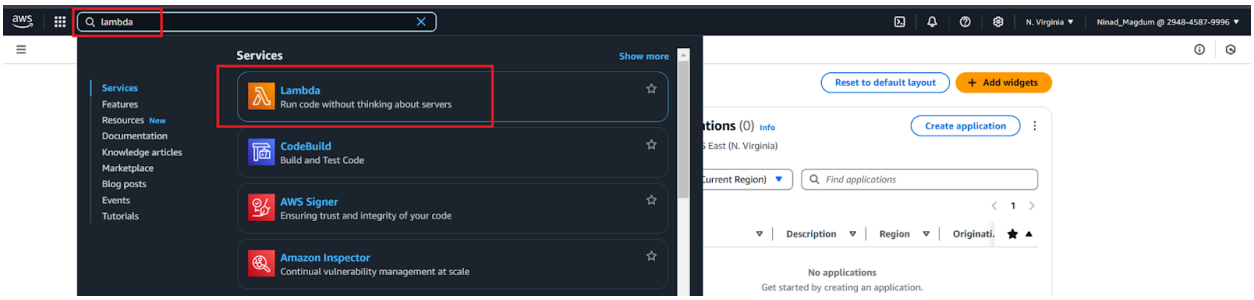
- Once selected validate your AWS region changed to the target bucket region.



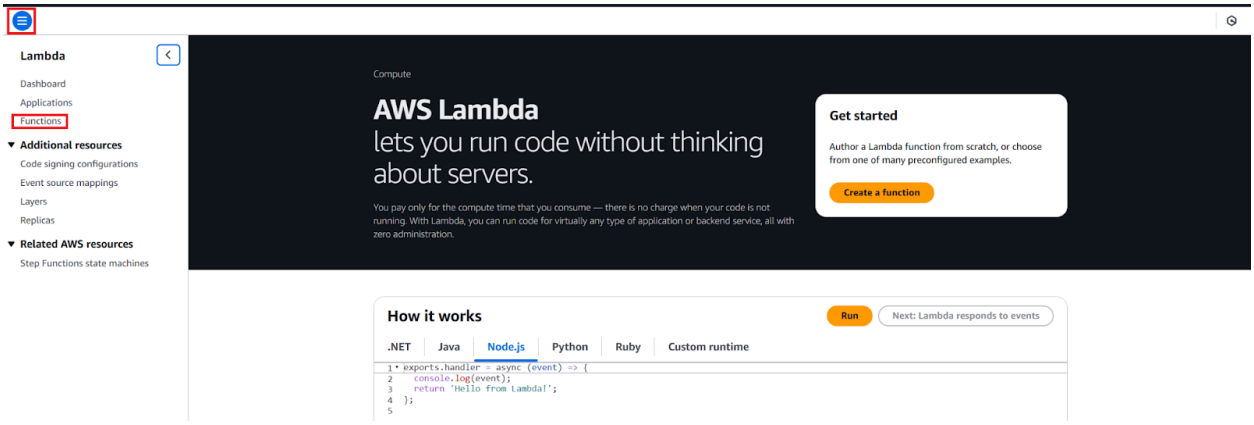
This is the region where we are going to create the lambda function required for this project

Creation of AWS Lambda Function

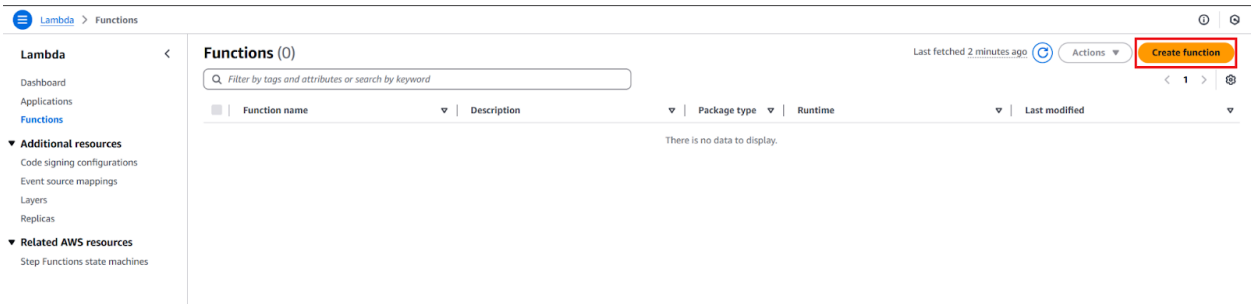
- Open your AWS Management Console and navigate to AWS Lambda by searching for "lambda" in the Search Bar.



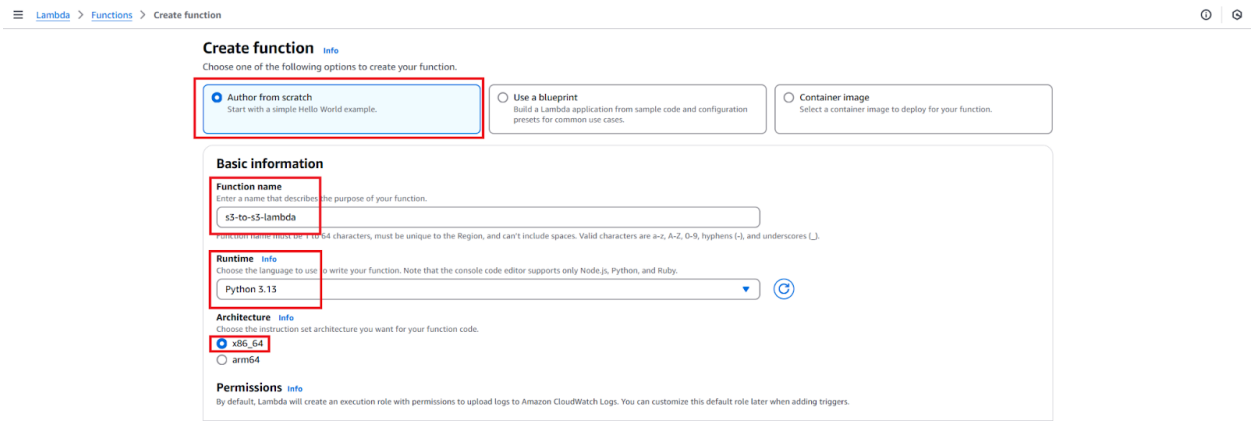
- Click on "Lambda," and you'll land on the page where click the three line menu button on the left top corner and then click on the Functions button



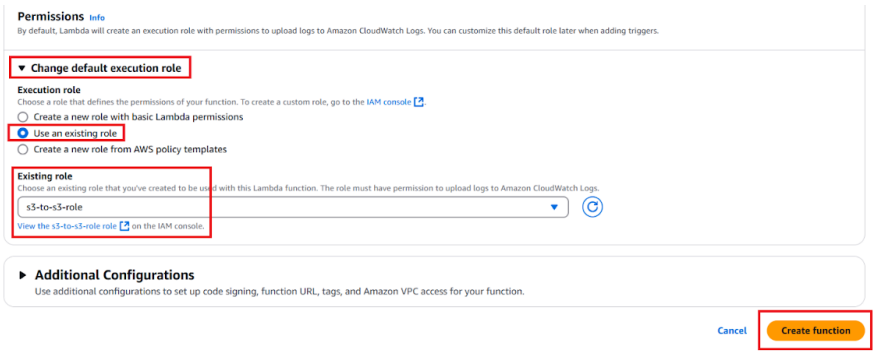
- On the functions page,click on the "Create function" button to create a new lambda function.



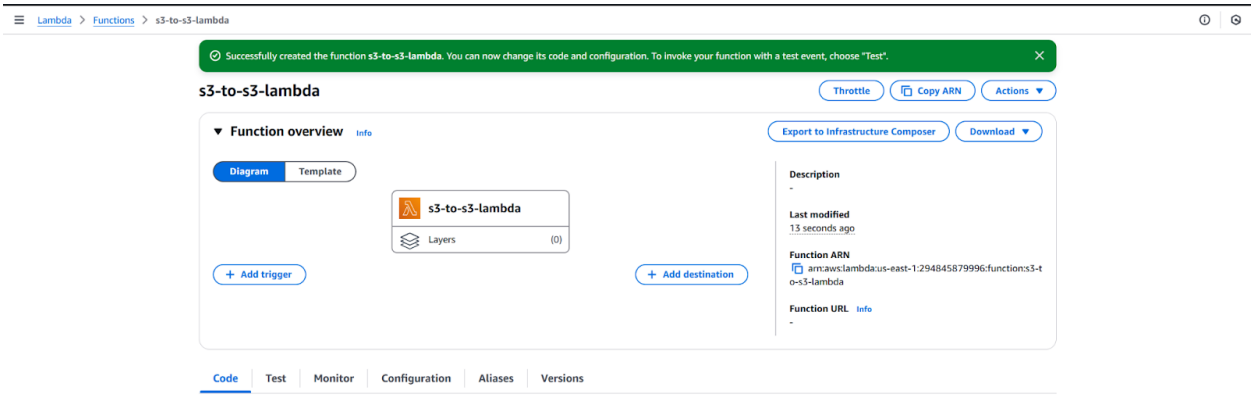
- Once you click "Create function," you'll be directed to the following page where you need to fill in the following information accordingly.
    - Select Author from scratch option
    - Provide name to your function under Function name section <s3-to-s3-lambda>
    - Select runtime as the latest python version
    - Keep the architecture as default x86_64



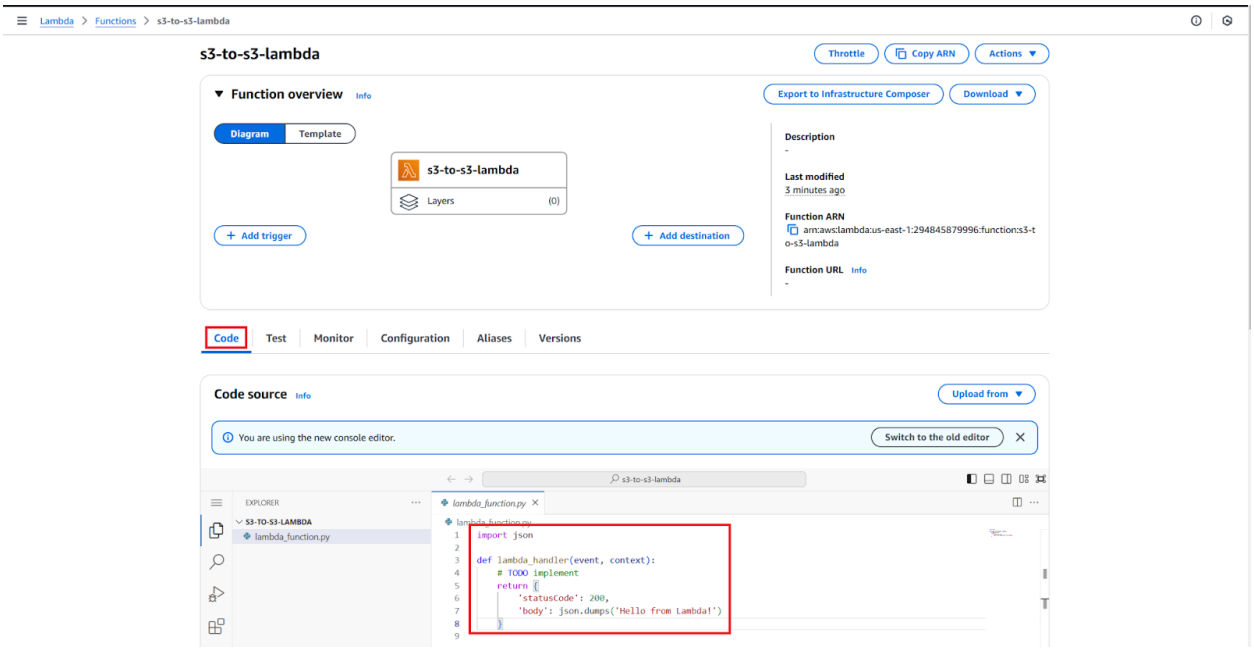
- Expand the "Change default execution role" section and select the option "Use an existing role." and select the already created role created previously for this project and click on “Create Function” button



- Once you click "Create function," you will land on the following page confirming that your Lambda function has been created successfully.



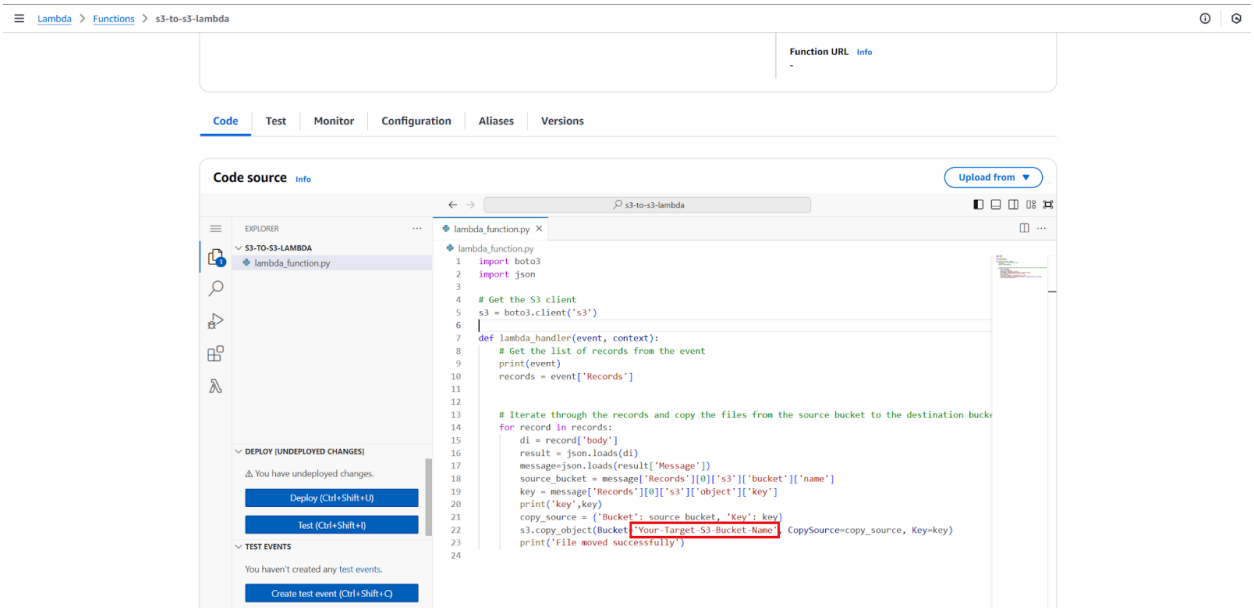
- Navigate to the "Code" section of the function and delete the existing code that is currently available.



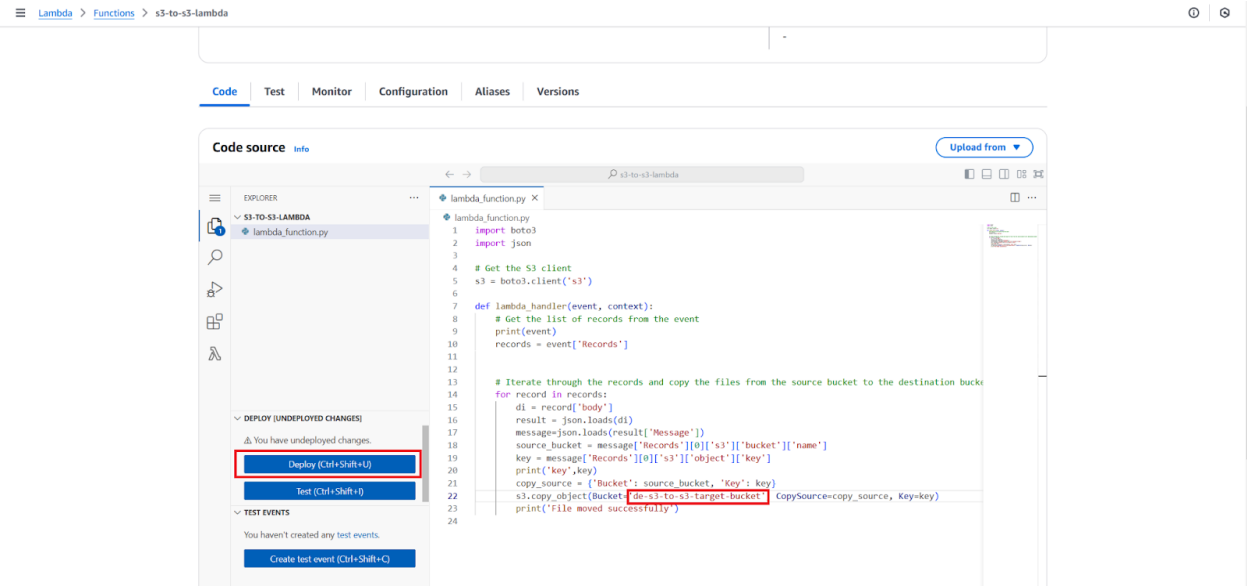
- Paste the following code into the code editor and update the “Your-Target-S3-Bucket-Name” value with your actual target s3 bucket name.

```
import boto3

import json


# Get the S3 client

s3 = boto3.client('s3')


def lambda_handler(event, context):

    # Get the list of records from the event

    print(event)

    records = event['Records']
```

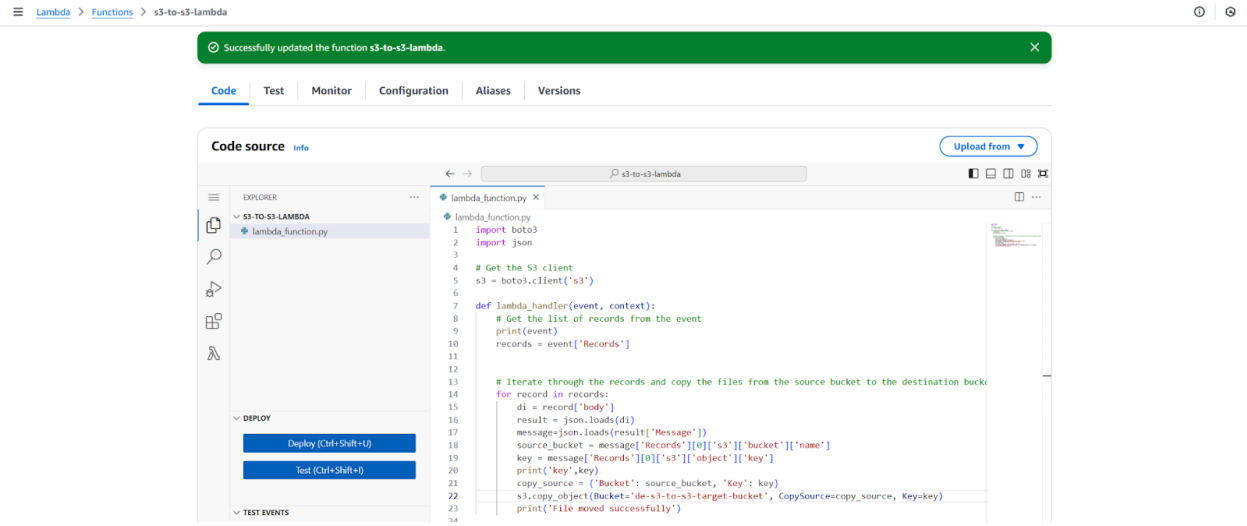
```
    # Iterate through the records and copy the files from the source bucket to the destination bucket

    for record in records:

        di = record['body']

        result = json.loads(di)

        message=json.loads(result['Message'])

        source_bucket = message['Records'][0]['s3']['bucket']['name']

        key = message['Records'][0]['s3']['object']['key']

        print('key',key)

        copy_source = {'Bucket': source_bucket, 'Key': key}

        s3.copy_object(Bucket='Your-Target-S3-Bucket-Name', CopySource=copy_source, Key=key)

        print('File moved successfully')
```



- Once you update the Your-Target-S3-Bucket-Name value with your actual target s3 bucket name, click on the "Deploy" button to update your Lambda function

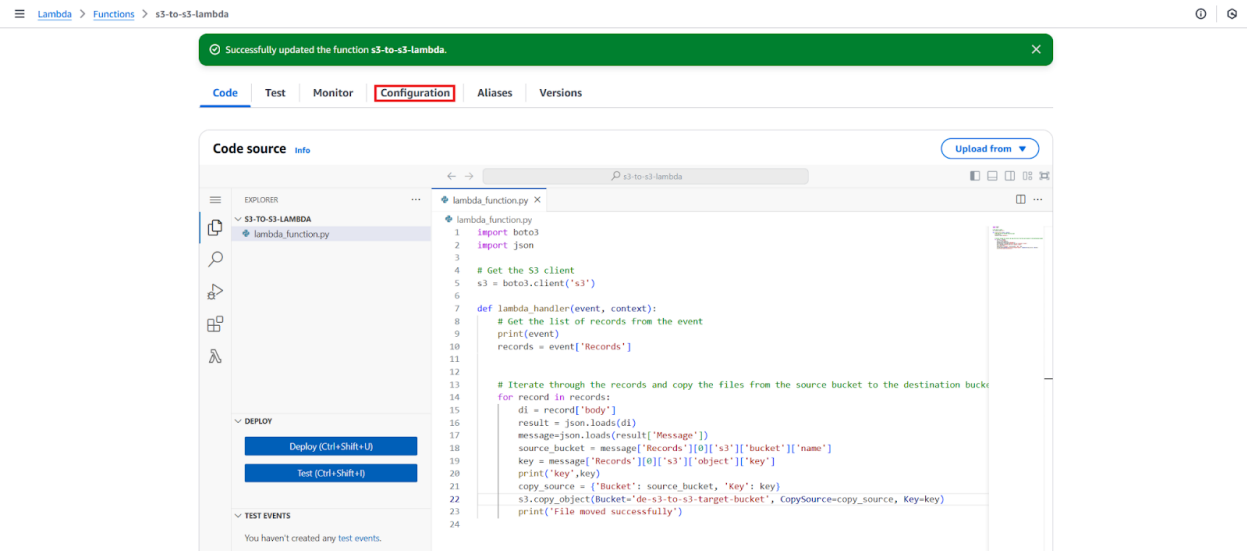


- One clicked Deploy button, your lambda function will be created with the updated code

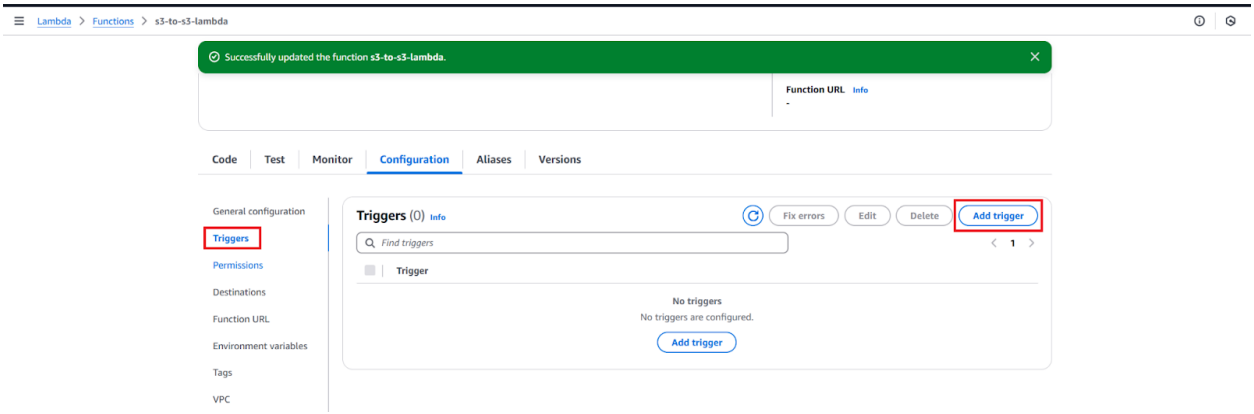


Setup the SQS Trigger to AWS Lambda Function

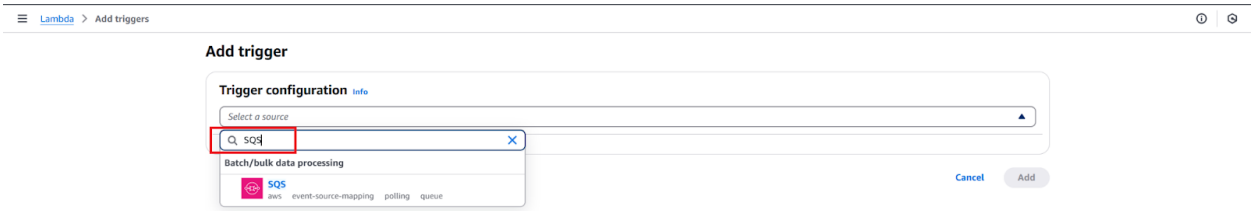
- Once the lambda function is deployed with the updated code,click on the Configuration tab



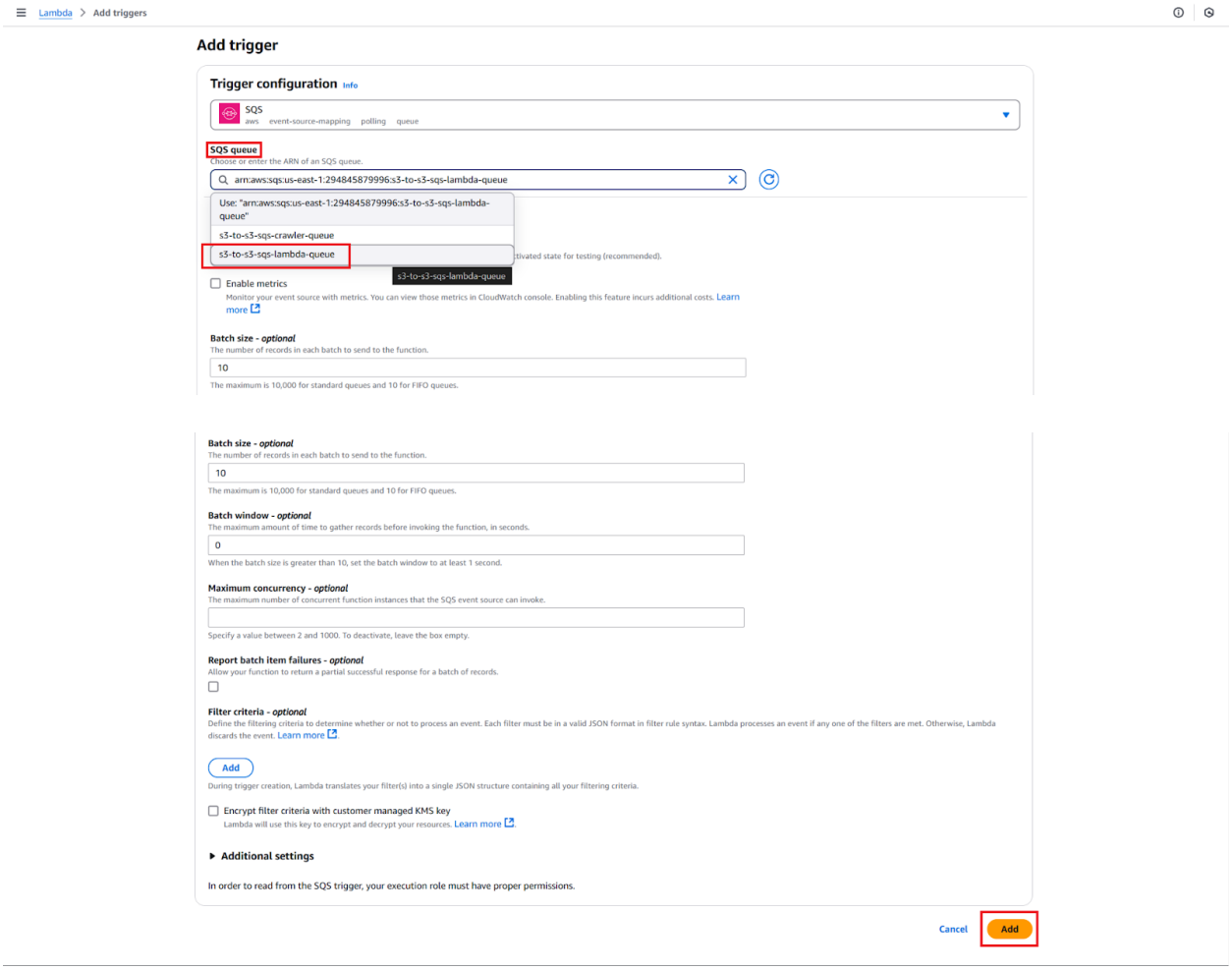
- Under the Configuration tab, click on the Trigger button and then click Add trigger button to create a new trigger



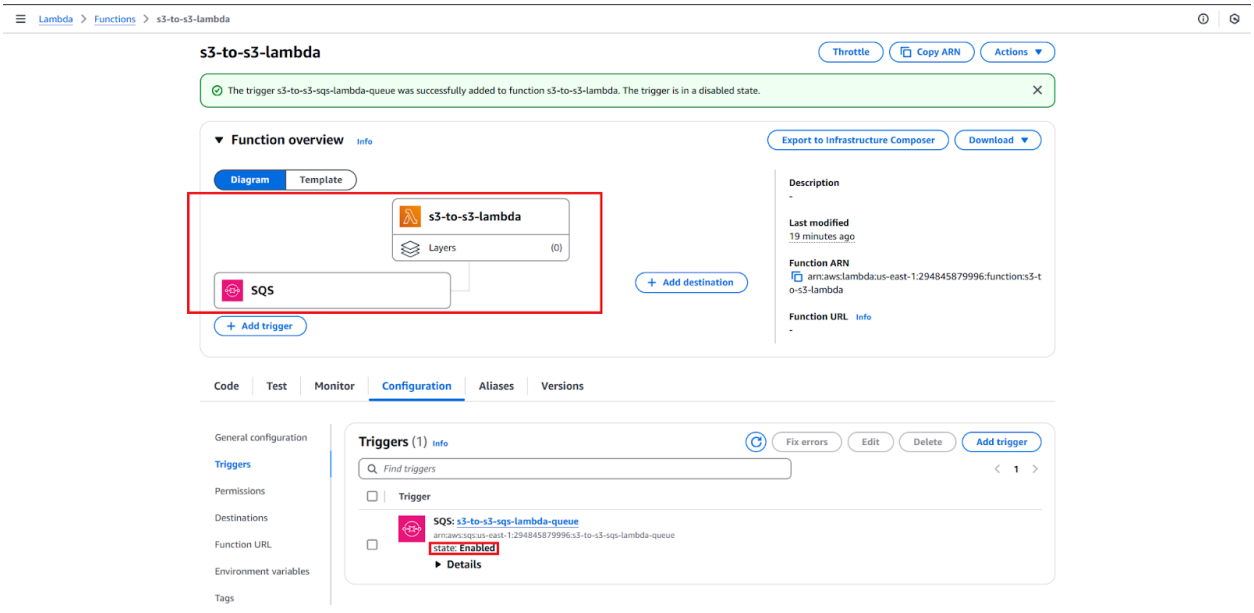
- On the Trigger configuration page, select the source as SQS and select the SQS from the below list



- Once you select SQS from the list, select the previously created lambda SQS queue in the SQS queue section and then click the Add button.



- Once created you should be able to see the SQS trigger setup for your lambda function and it's in Enable state



VOILA! YOUR SUCCESSFULLY CREATED YOUR LAMBDA FUNCTION AND SETUP THE SQS TRIGGER

1. aws_module
2. Cross region S3-S3 migration using Lambda
3. AWS Glue Crwaler
4. Documentation

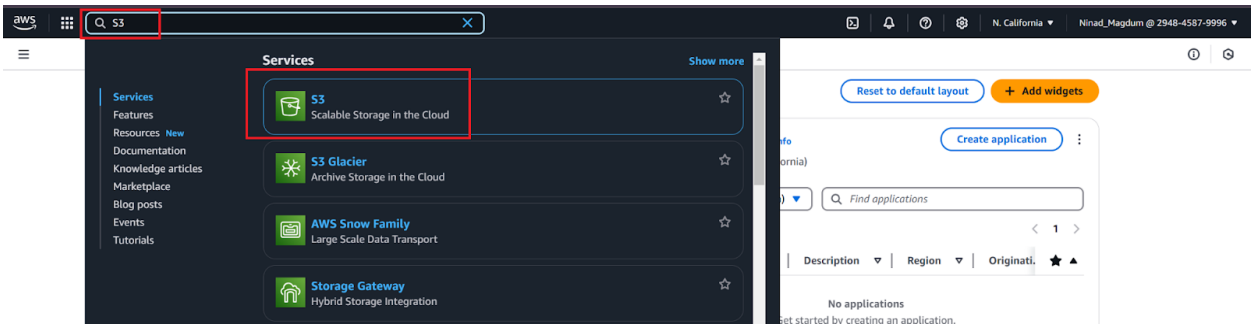
AWS Glue Crawler Creation guide

- Let us understand and walk through the process of creation of Crawler in the AWS Glue

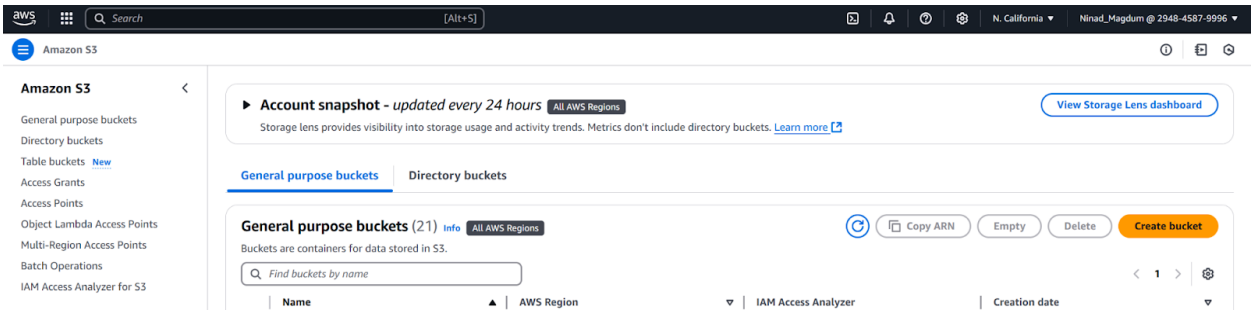
Identify the Glue Crawler AWS Region

First we need to identify the AWS region in which we need to setup the required Glue crawler for this project

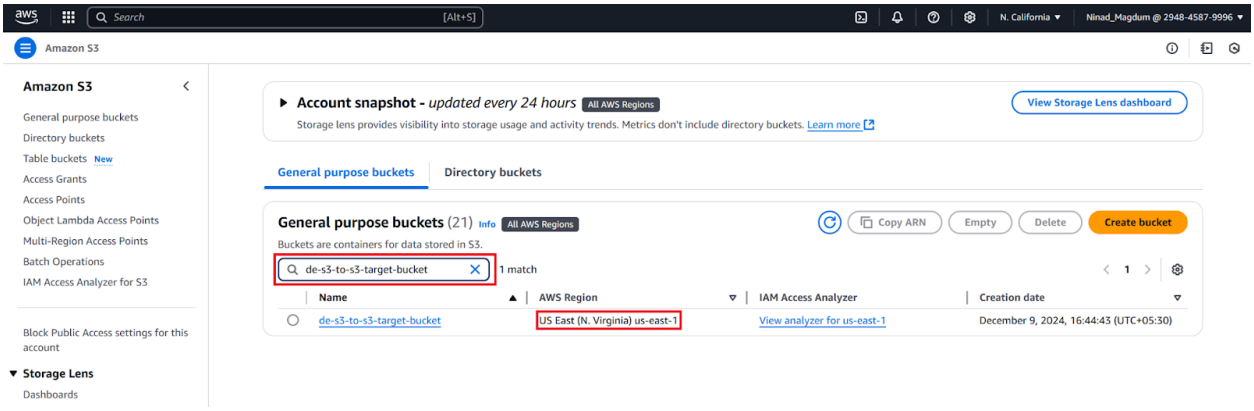
- Access your AWS Management Console and find AWS S3 by entering "S3" in the search bar.



- Select S3 from the menu, which will direct you to the page where you can see all of your buckets.

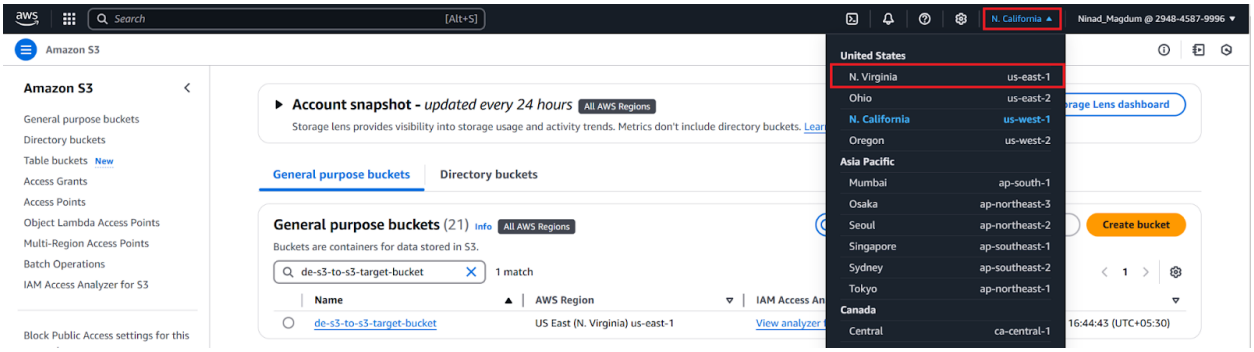


- Search your target bucket created for this project in the search bar and note down the AWS region of the same.

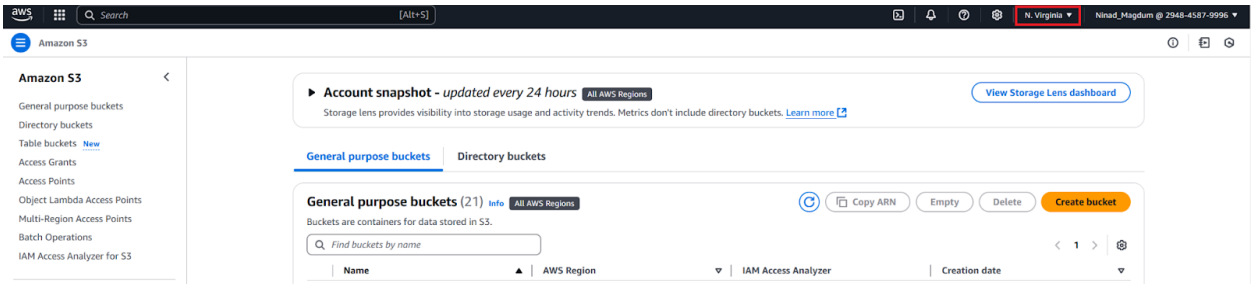


In my case the region is us-east-1, in your case it might be different.

- Click on the Region button on the top right hand corner of your AWS Management Console. Change the AWS region to the target bucket region.



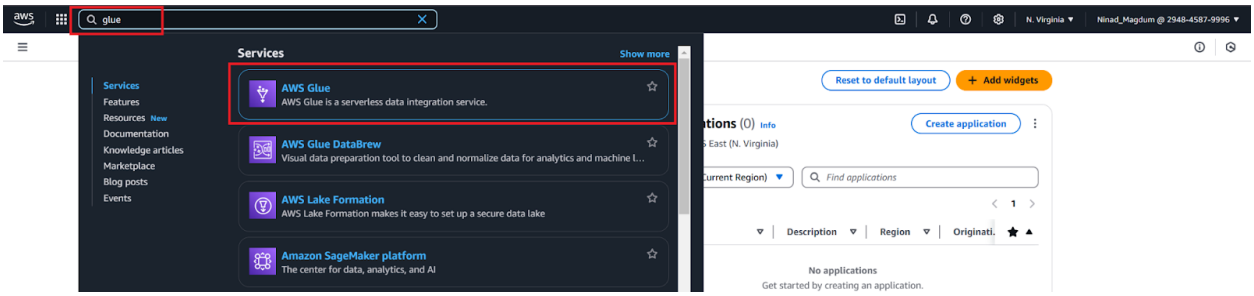
- Once selected validate your AWS region changed to the target bucket region.



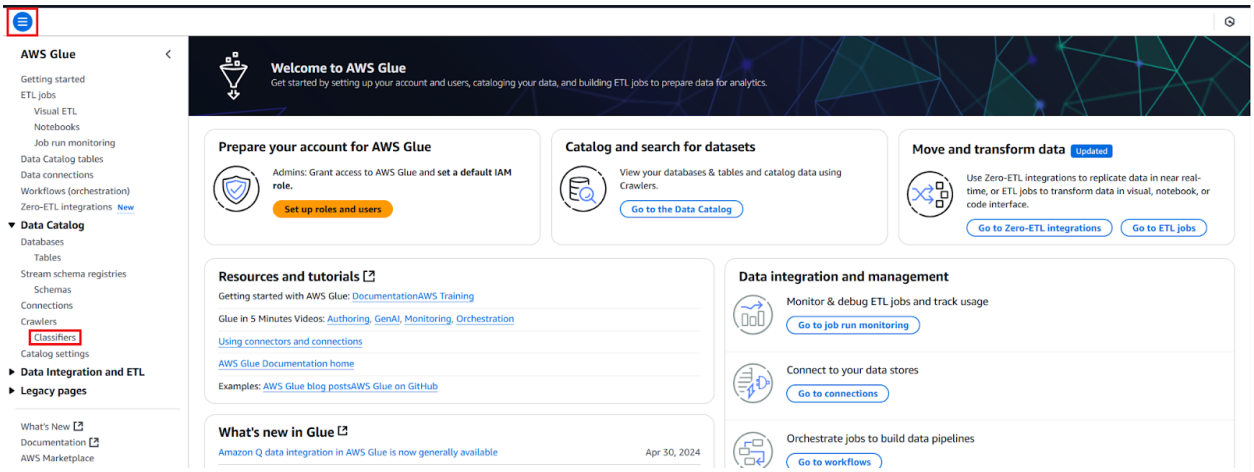
This is the region where we are going to create the lambda function required for this project (In your case it might be different)

Creation of AWS Glue Crawler Classifiers

- Open your AWS Management Console and navigate to AWS Glue by searching for "Glue" in the Search Bar.

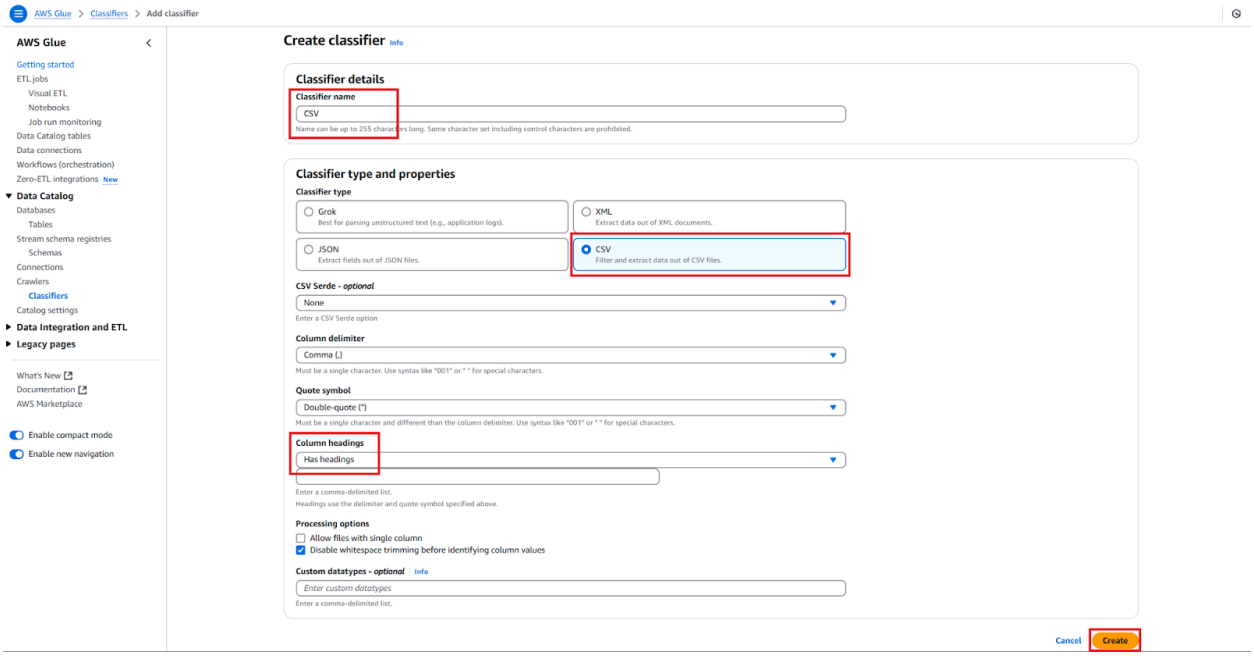


- Click on "AWS Glue," and you'll land on the page where click the three line menu button on the left top corner and then click on the Classifier button under crawlers

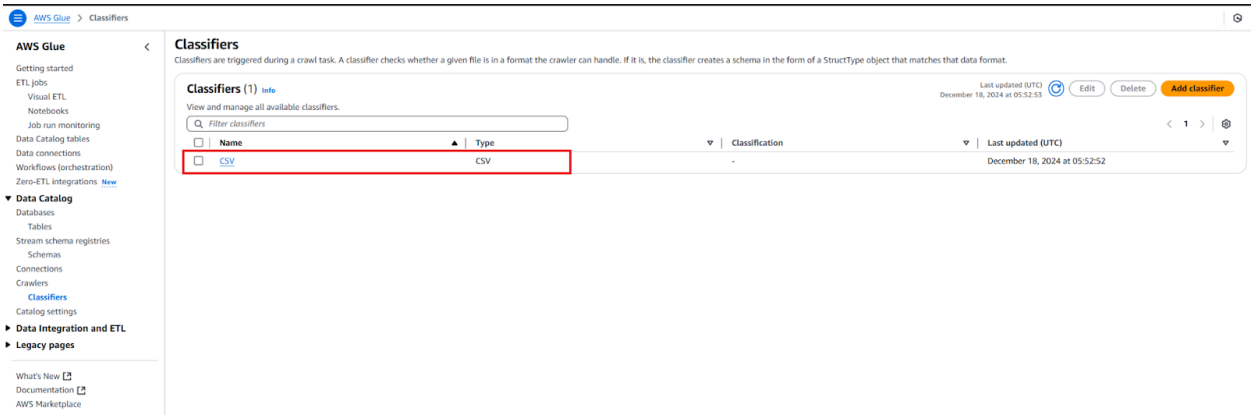


- On the classifiers page,click on the "Add classifier" button to create a new crawler classifier.

- Once you click "Add classifier", you'll be directed to the following page where you need to fill in the following information accordingly and then click on Create button to create your crawler classifier
    - Classifier name : CSV
    - Classifier Type : CSV
    - Column headings : Has headings

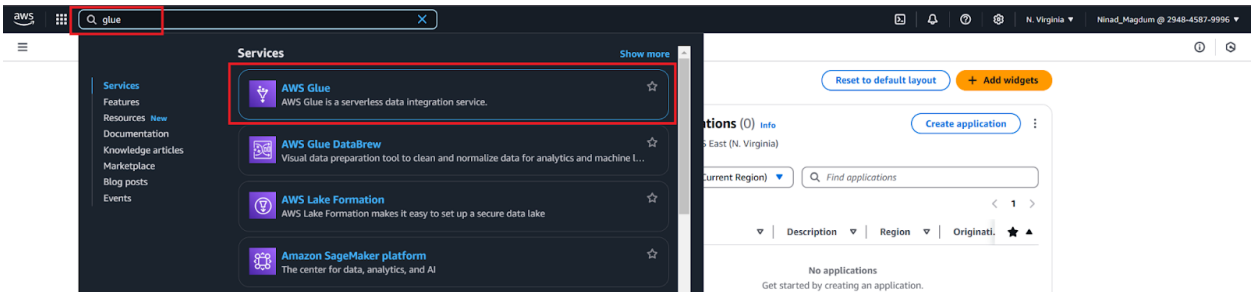


- Once you click "Create", your crawler classifier will be created successfully.

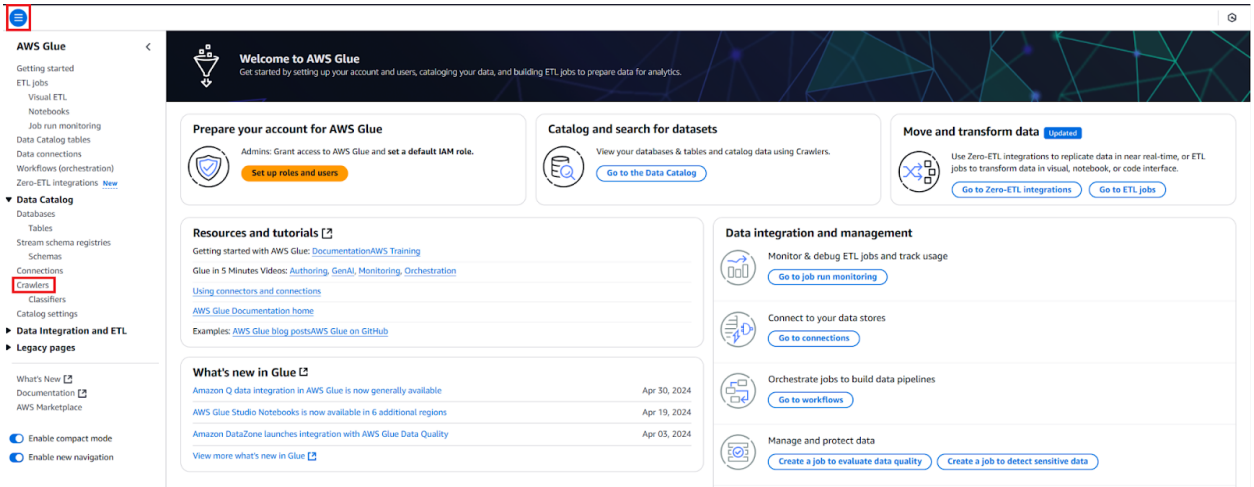


Creation of AWS Glue Crawler Job

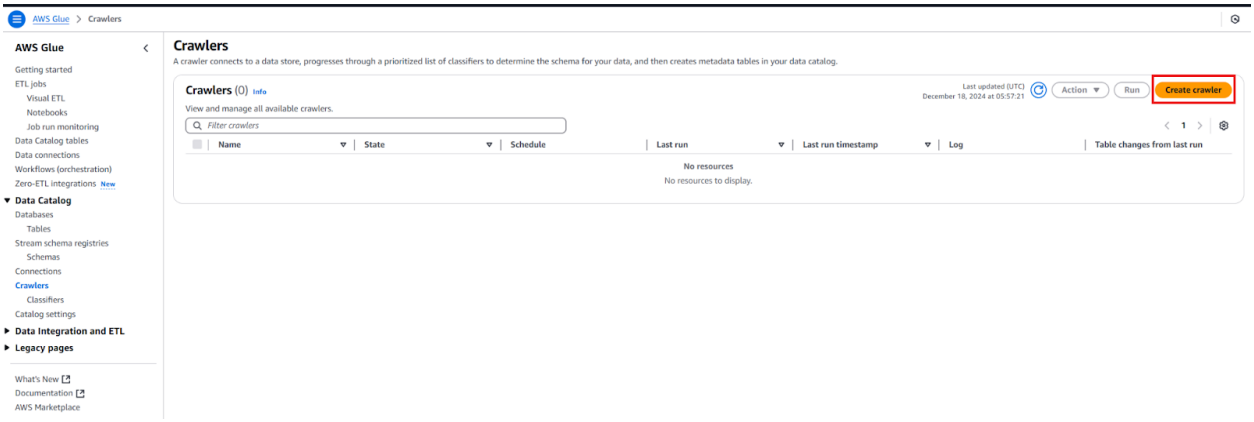
- Open your AWS Management Console and navigate to AWS Glue by searching for "Glue" in the Search Bar.



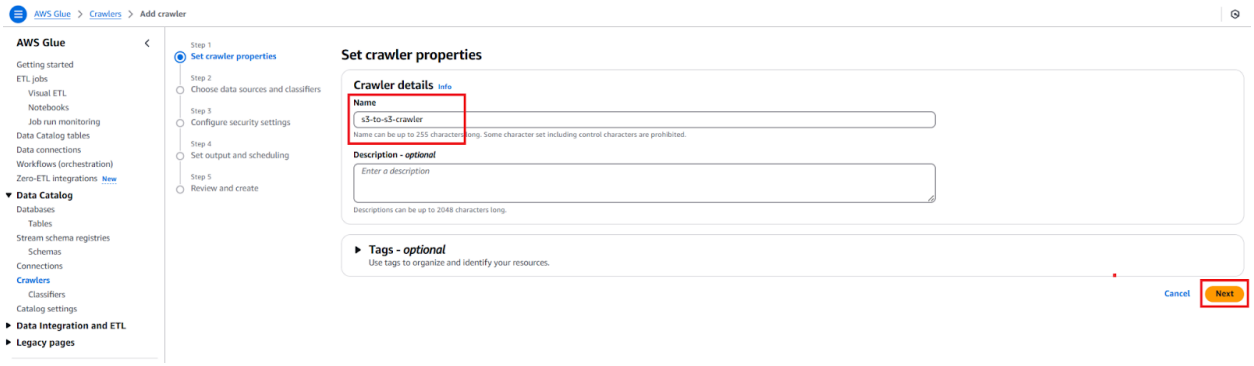
- Click on "AWS Glue," and you'll land on the page where click the three line menu button on the left top corner and then click on the Crawlers button



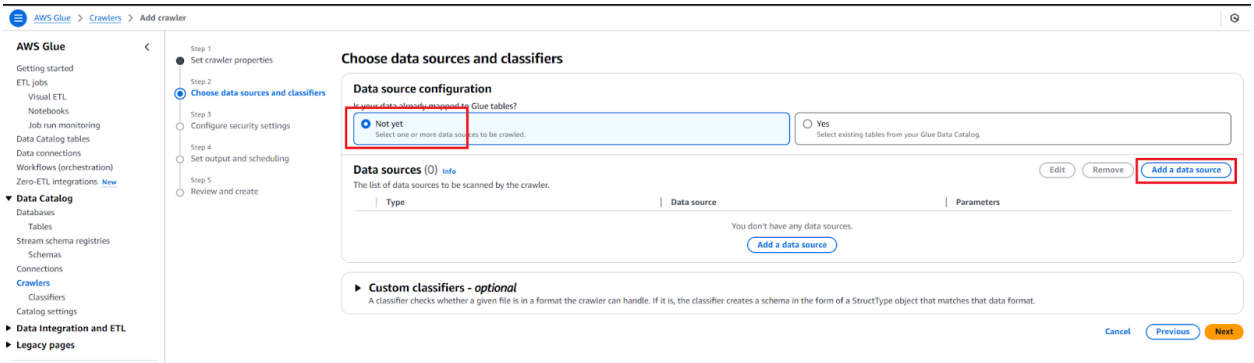
- On the crawlers page,click on the "Create crawler" button to create a new crawler



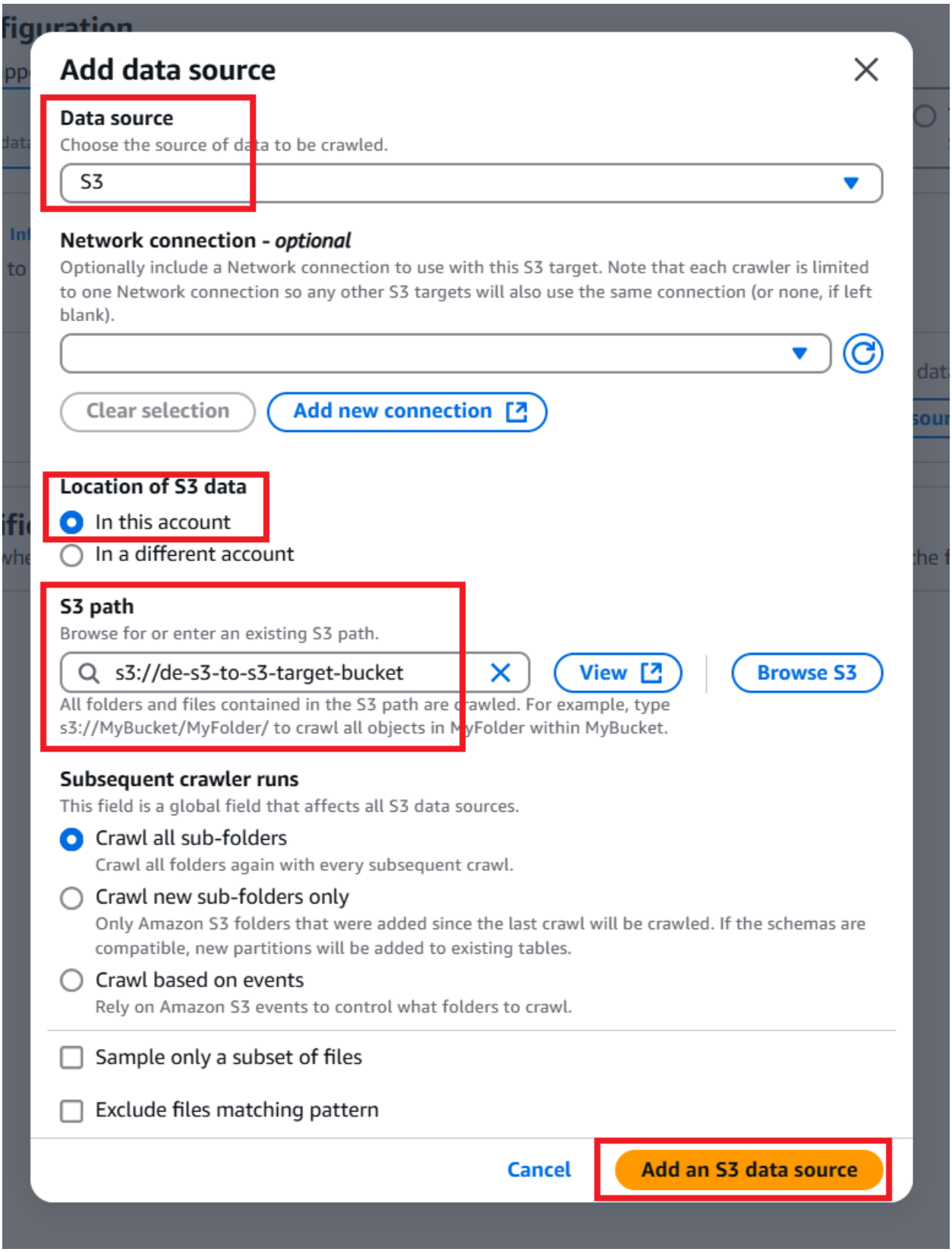
- .Once you click "Create crawler", you'll be directed to the following pages where you need to fill in the following
- Set crawler properties Page
    - On this page provide the name of your crawler <s3-to-s3-crawler> and click Next button



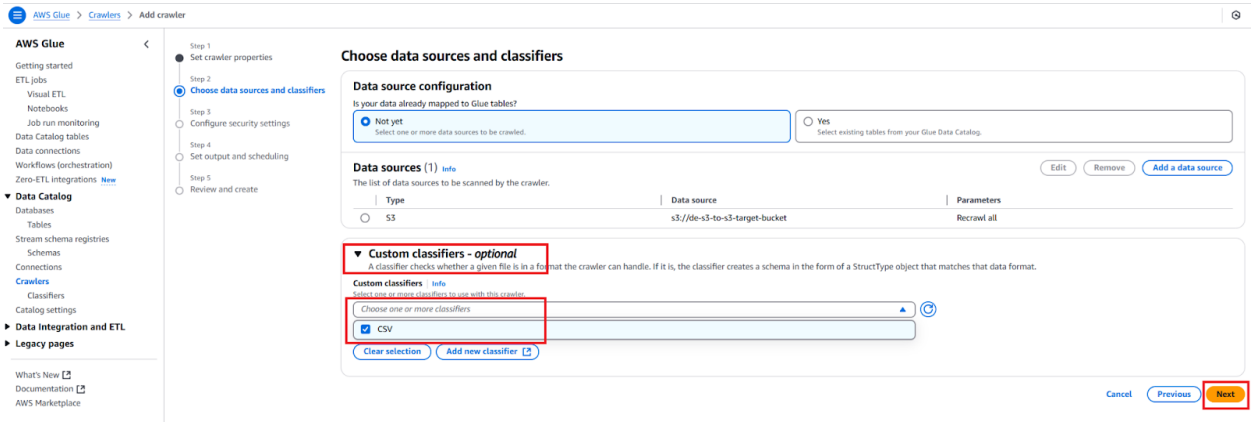
- Choose data sources and classifiers Page
    - On this page select the Not yet option under the Data source configuration and then click on Add a Data Source button



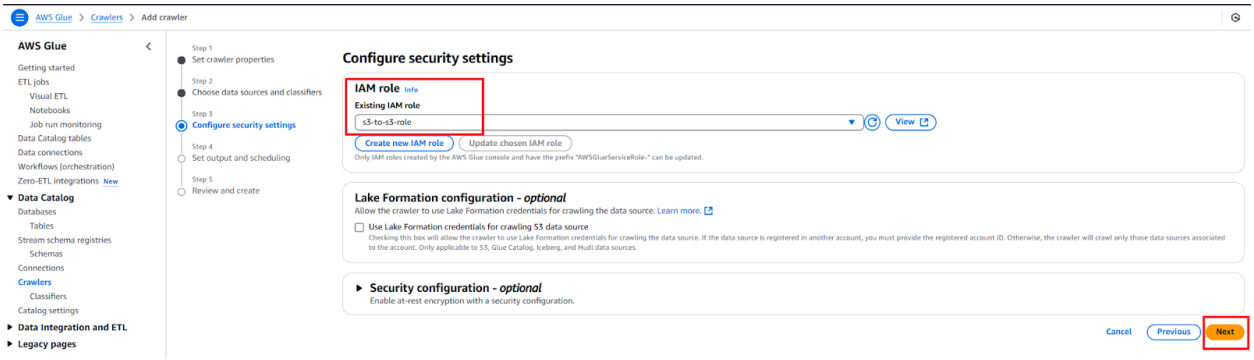
- On the Add data source page, fill the below details accordingly and click Add an S3 data source button
    - Data Source : S3
    - Location of S3 data : In this account
    - S3 Path : Your S3 Target bucket location


Add data source
Data source
Choose the source of data to be crawled.
S3
Network connection - optional
Optionally include a Network connection to use with this S3 target. Note that each crawler is limited to one Network connection so any other S3 targets will also use the same connection (or none, if left blank).
Clear selection
Add new connection
Location of S3 data
In this account
In a different account
S3 path
Browse for or enter an existing S3 path.
s3://de-s3-to-s3-target-bucket
View
Browse S3
All folders and files contained in the S3 path are crawled. For example, type s3://MyBucket/MyFolder/ to crawl all objects in MyFolder within MyBucket.
Subsequent crawler runs
This field is a global field that affects all S3 data sources.
Crawl all sub-folders
Crawl all folders again with every subsequent crawl.
Crawl new sub-folders only
Only Amazon S3 folders that were added since the last crawl will be crawled. If the schemas are compatible, new partitions will be added to existing tables.
Crawl based on events
Rely on Amazon S3 events to control what folders to crawl.
Sample only a subset of files
Exclude files matching pattern
Cancel
Add an S3 data source

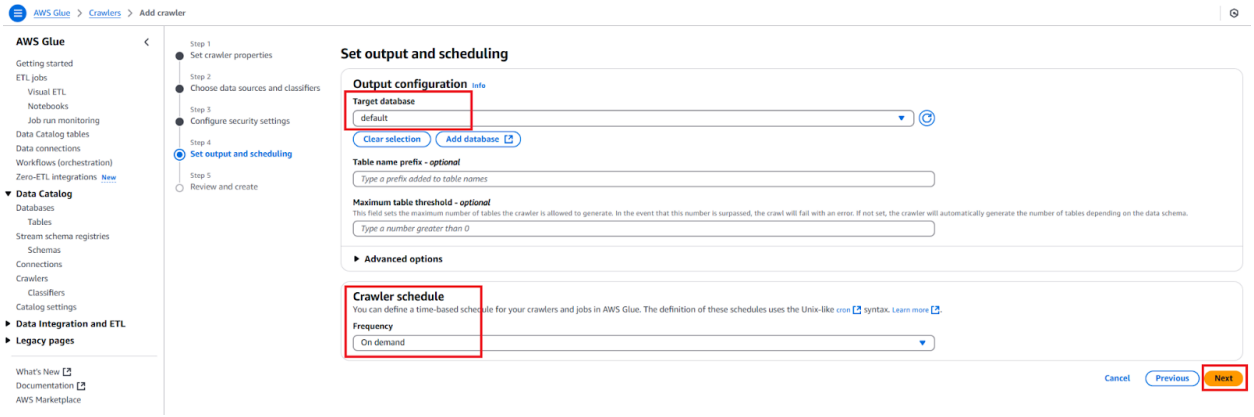
- Choose the already existing CSV classifier under the Custom classifiers section and click on the Next button.



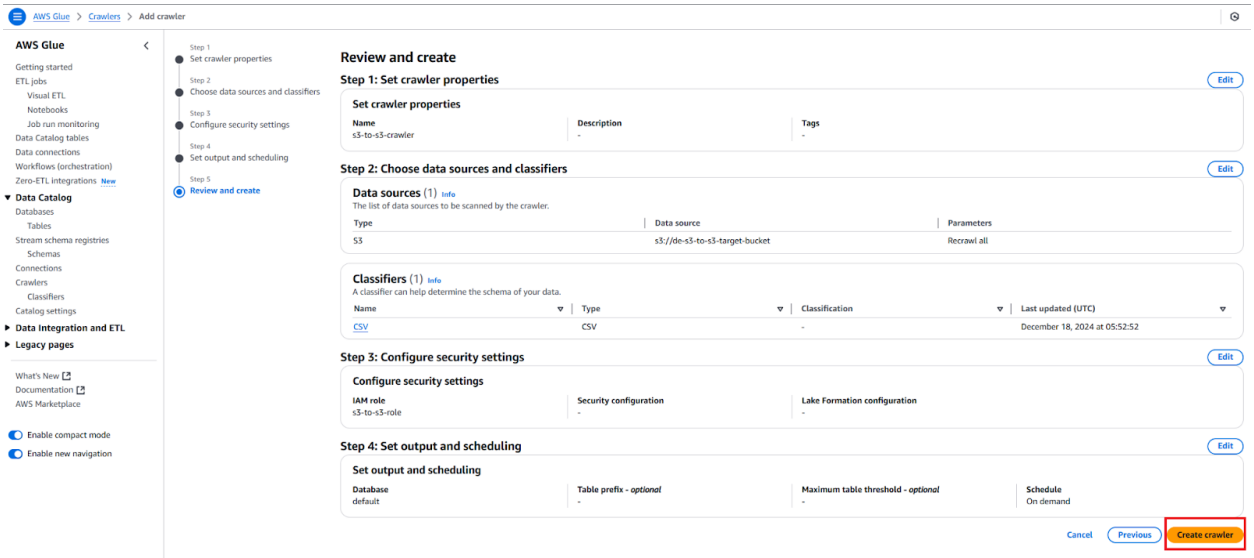
- Configure security settings page
  - On this page, choose the already existing IAM role created for this project and click on the Next button.



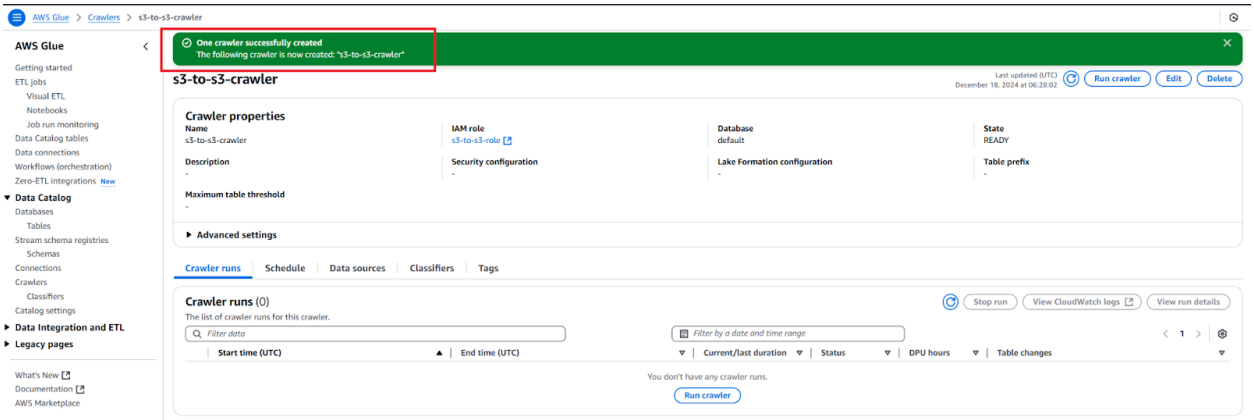
- Set output and scheduling page
  - On this page, choose the Target Database as default and the Frequency as On demand under Crawler Schedule and then click on the Next button.



- On the Review and create page, click Create crawler to create you job



- Once you click "Create crawler", your crawler job will be created successfully.

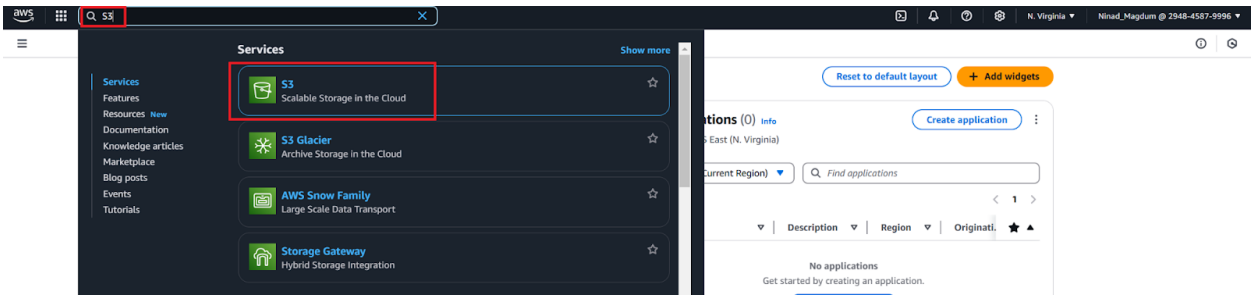


VOILA! YOUR SUCCESSFULLY CREATED YOUR AWS GLUE CRAWLER

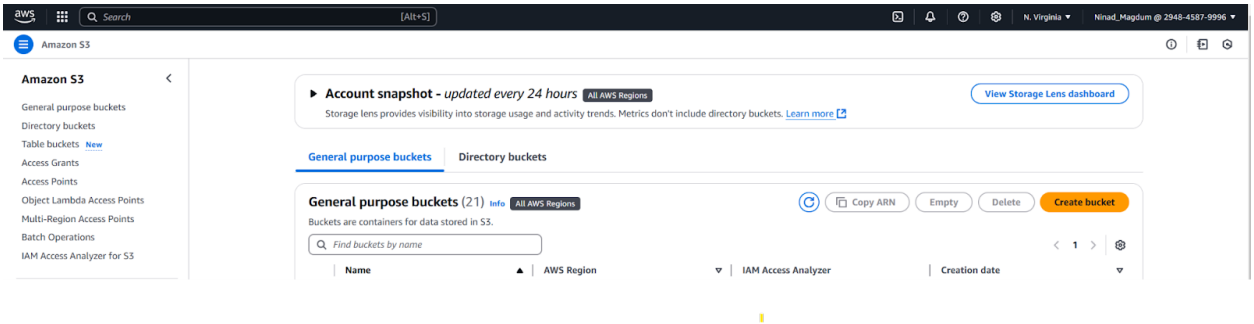
AWS S3 Source Bucket Event Notification Creation guide

Let us understand and walk through the process of Event notification creation on the S3 source bucket

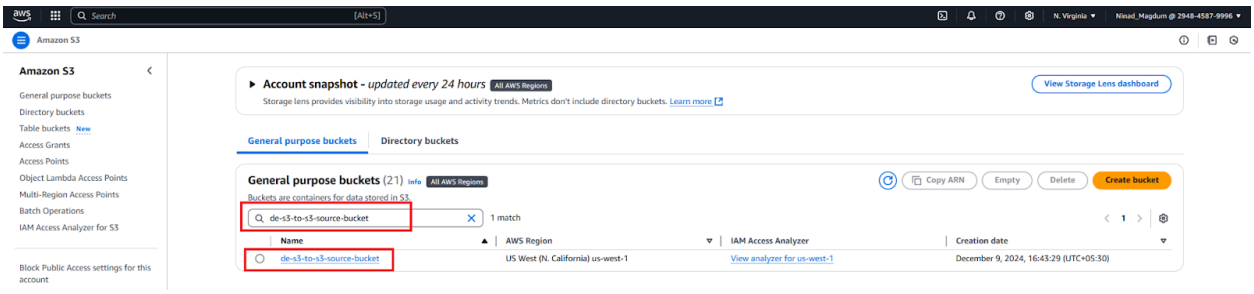
- Access your AWS Management Console and find AWS S3 by entering "S3" in the search bar.



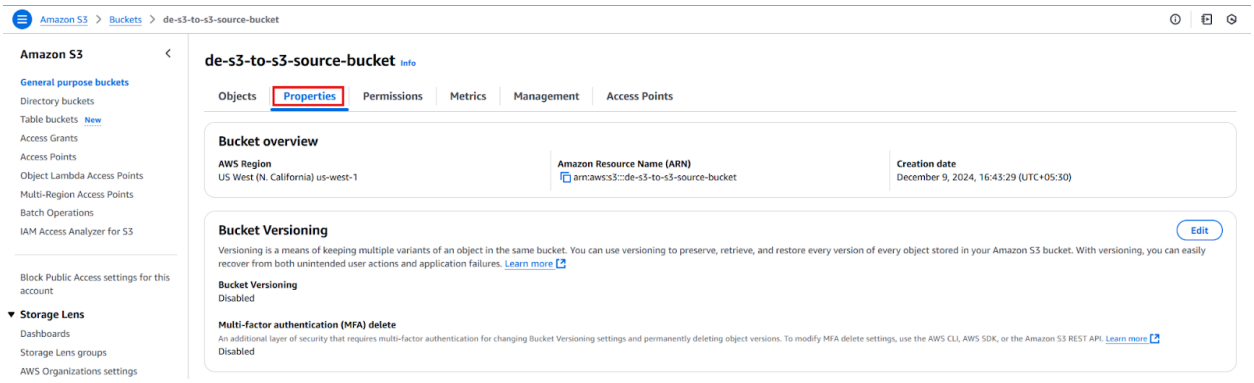
- Select S3 from the menu, which will direct you to the page where you can create an S3 Bucket.



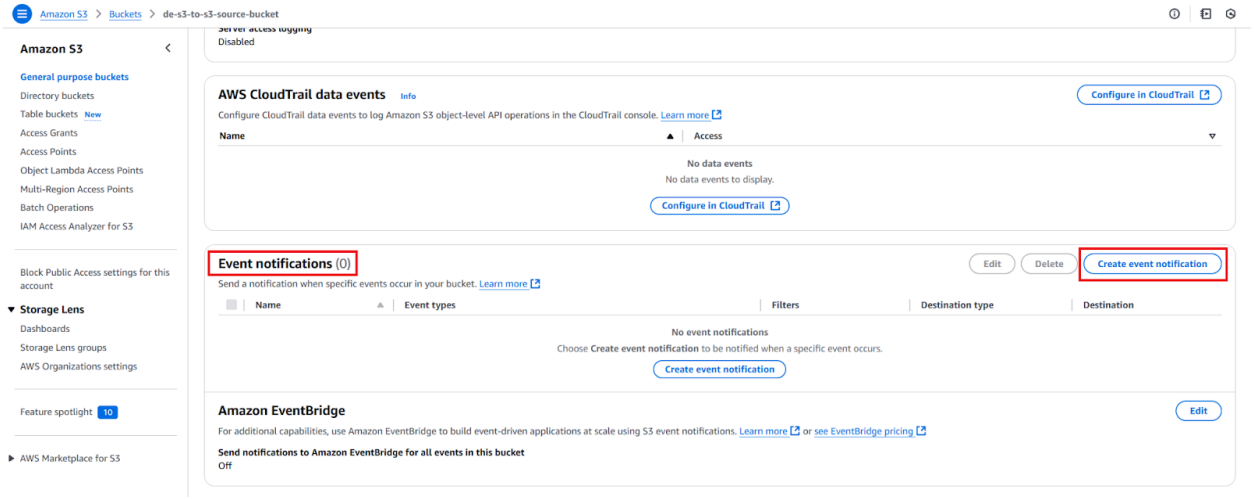
- Search your source bucket created for this project in the search bar and click on the bucket to open it.



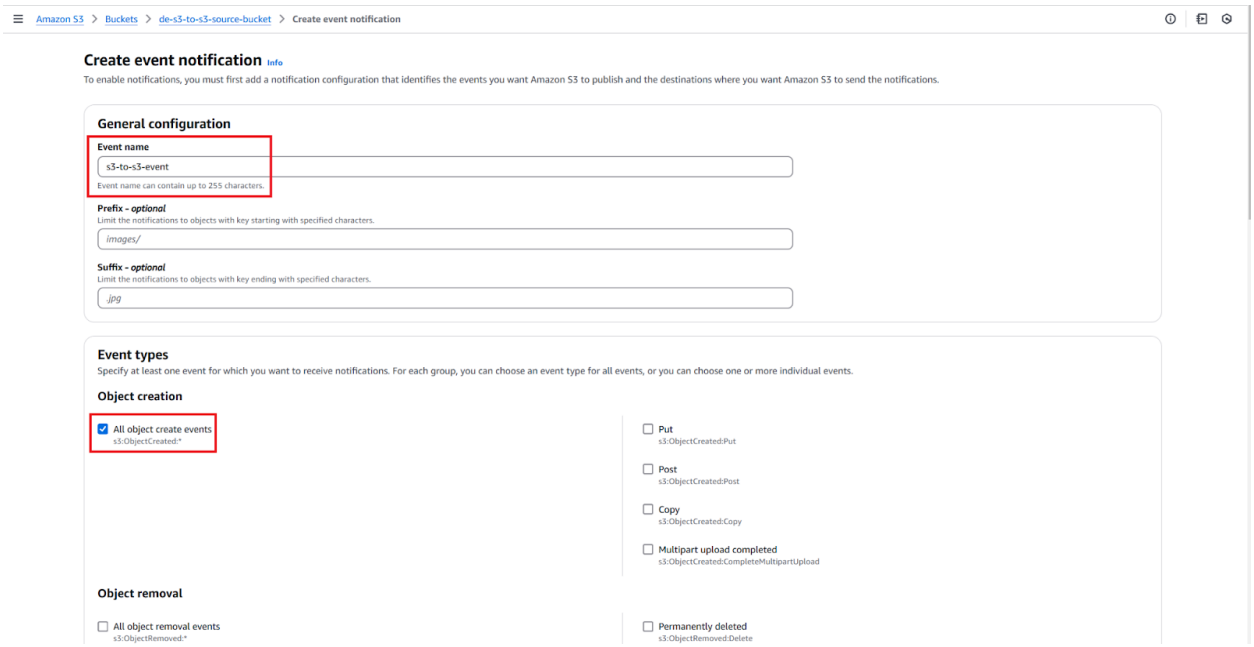
- On the source bucket page, click on the Properties tab



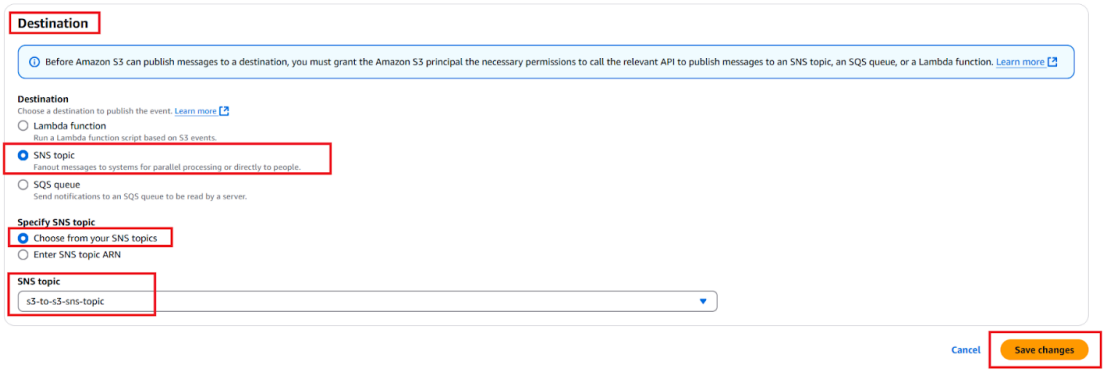
- On the Properties tab,Scroll down to the Event Notification section and click on Create event notification.



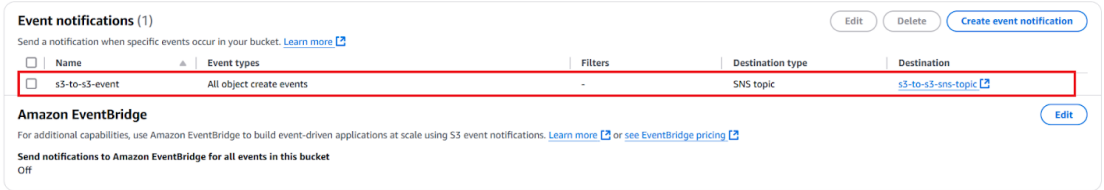
- Give a name to the Event notification and select All object create events under the Event types



- Now scroll down to the Destination section and select SNS topic as destination, select Choose from your SNS topics and select the already created SNS topic for this project . Then click on Save changes.



- Your event notification for your source s3 bucket is now set up successfully under the Event notification section of S3



VOILA! YOU HAVE SUCCESSFULLY CREATED THE EVENT NOTIFICATION ON THE SOURCE S3 BUCKETS

Test Data Flow

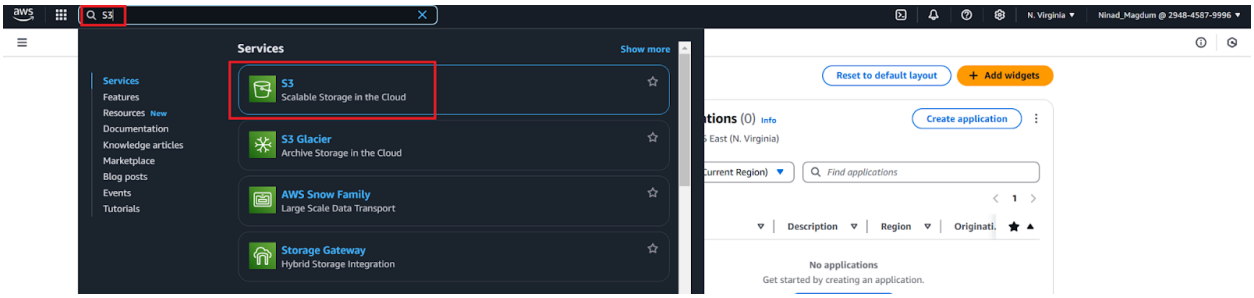
Step1: Download the customer Data File

- Download the customers.csv file shared along with the project to your local machine

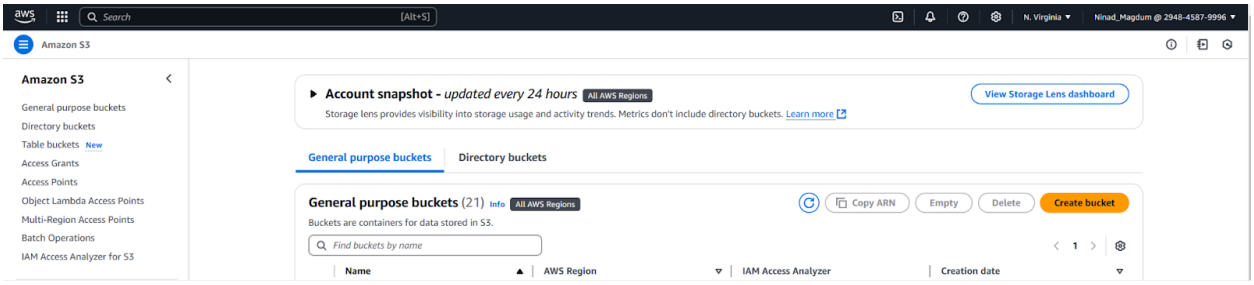
Step2: Upload file to S3 Source Bucket

In this step we will upload the downloaded customers.csv file to the source S3 bucket setup for this project

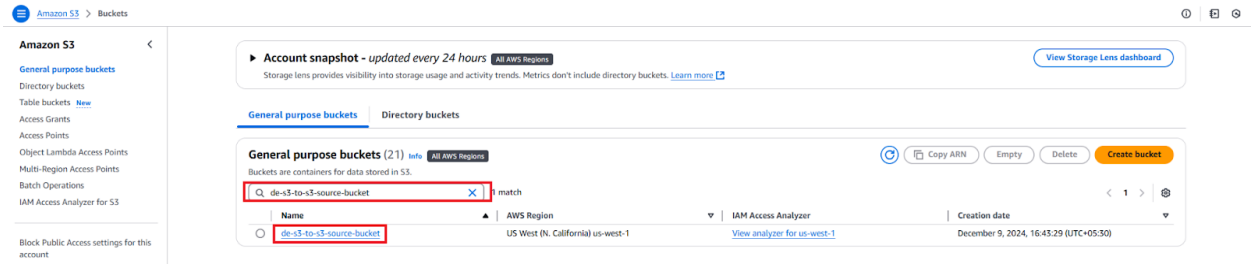
- Access your AWS Management Console and find AWS S3 by entering "S3" in the search bar.



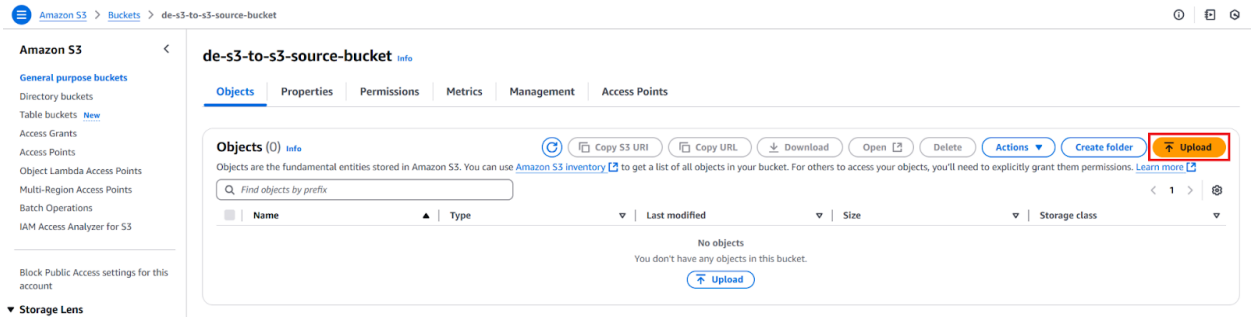
- Select S3 from the menu, which will direct you to the page where you can create an S3 Bucket.



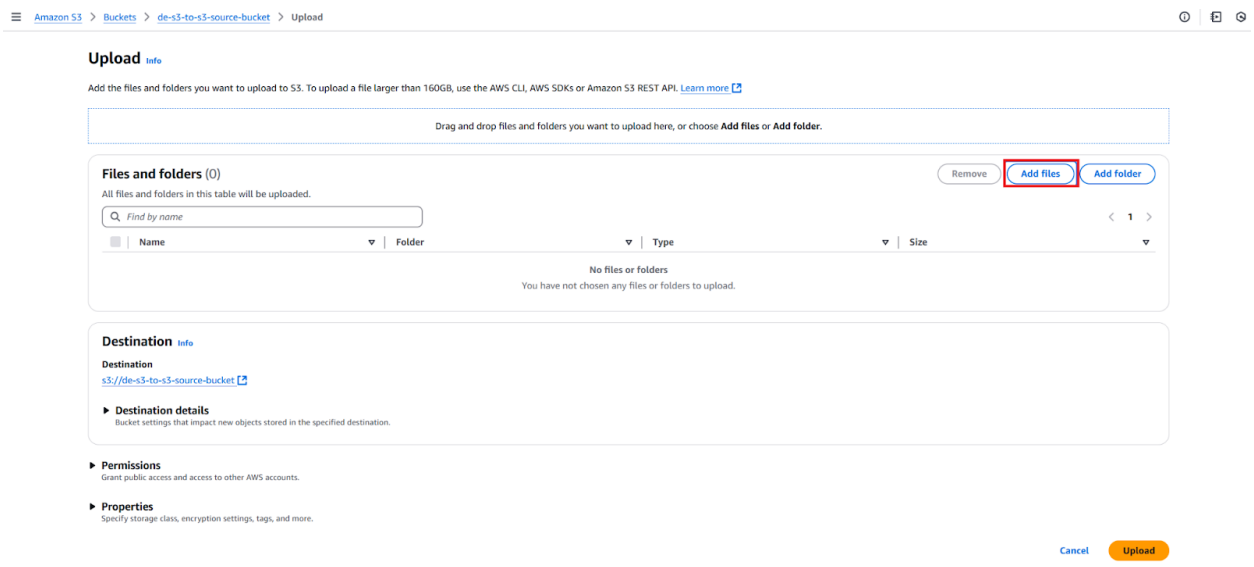
- Search your s3 source bucket and click it to open it



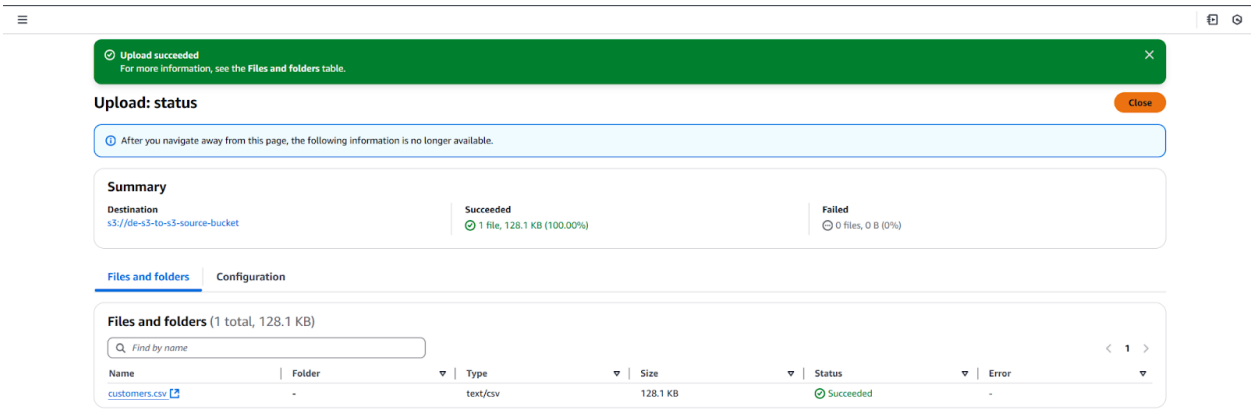
- On the s3 source bucket page, click on the Upload button to upload the customers.csv file



- On the Upload page, click the Add file button and select the customer.csv from your local machine



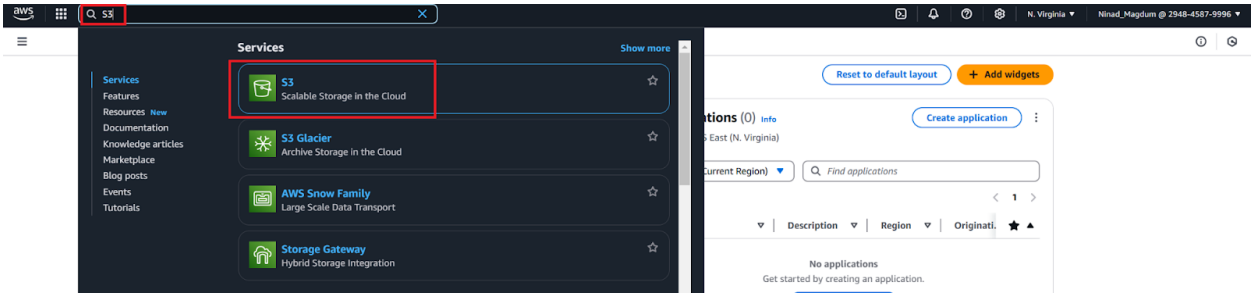
- Once the customer.csv is selected, click the Upload button to upload the file in the source S3 bucket



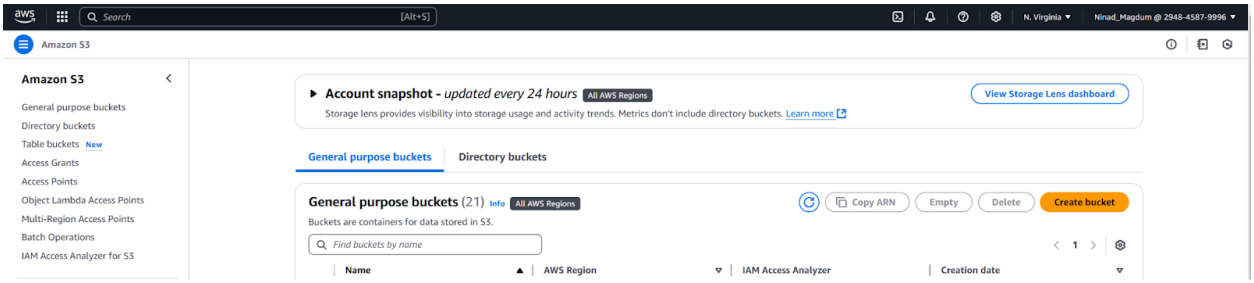
Step3: Validate if file is migrated to S3 Target Bucket

In this step we will validate if the customers.csv file is migrated to the target S3 bucket setup for this project

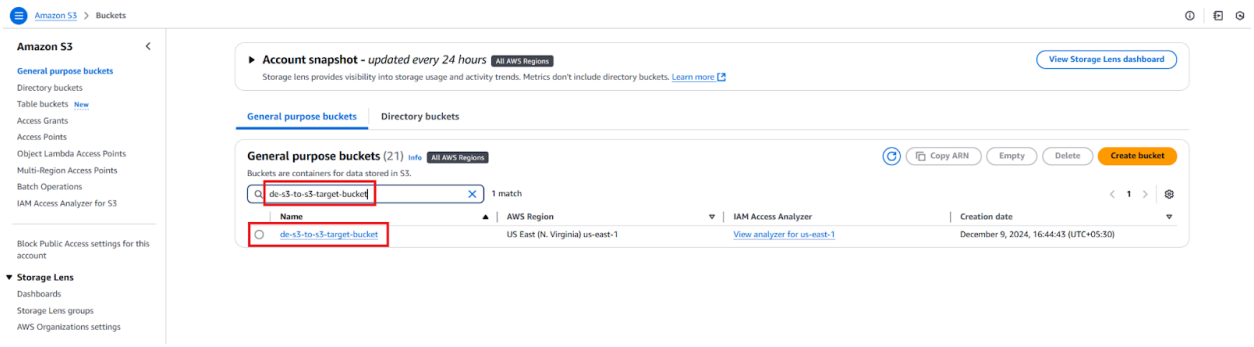
- Access your AWS Management Console and find AWS S3 by entering "S3" in the search bar.



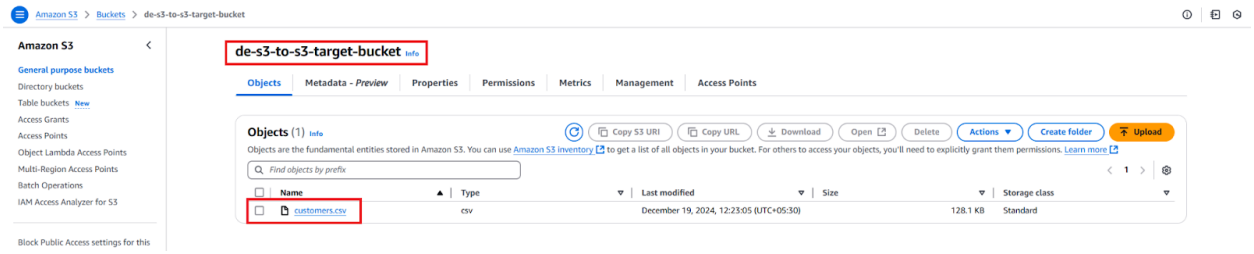
- Select S3 from the menu, which will direct you to the page where you can create an S3 Bucket.



- Search your s3 target bucket and click it to open it



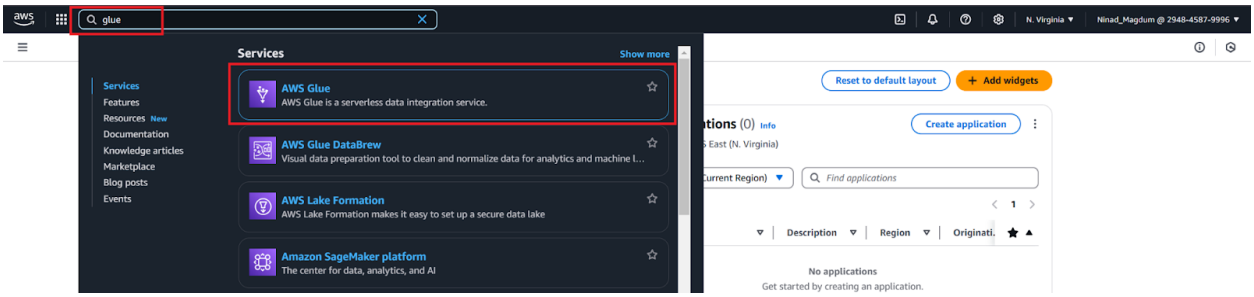
- On the s3 target bucket page, you should be able to see the customers.csv file migrated successfully if all of the previous steps are set up correctly.



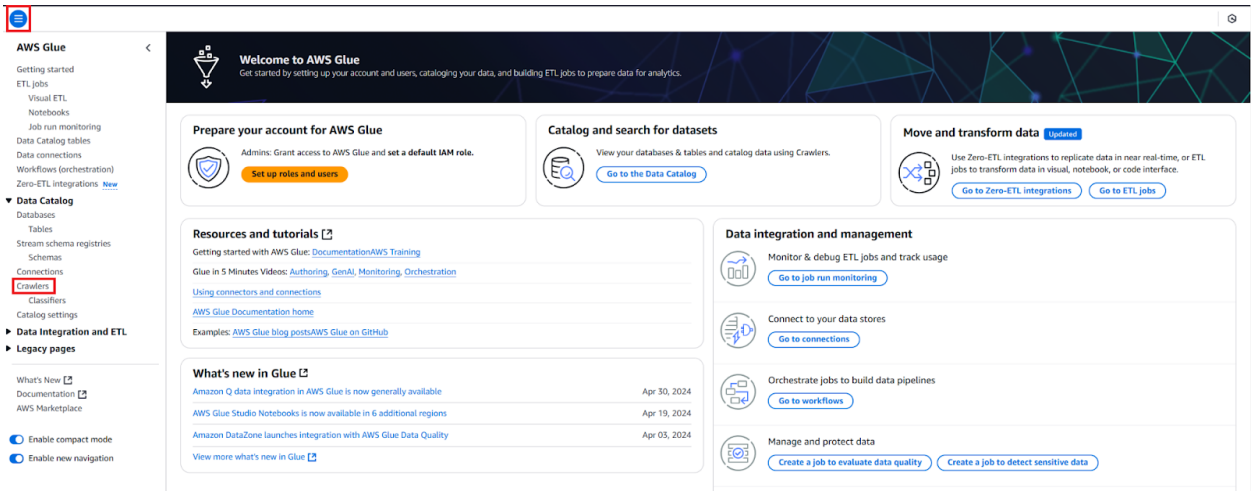
Step4: Trigger Crawler to create table in Glue Catalog

In this step we will execute the glue crawler to create a table in the Glue catalog for the data analysis

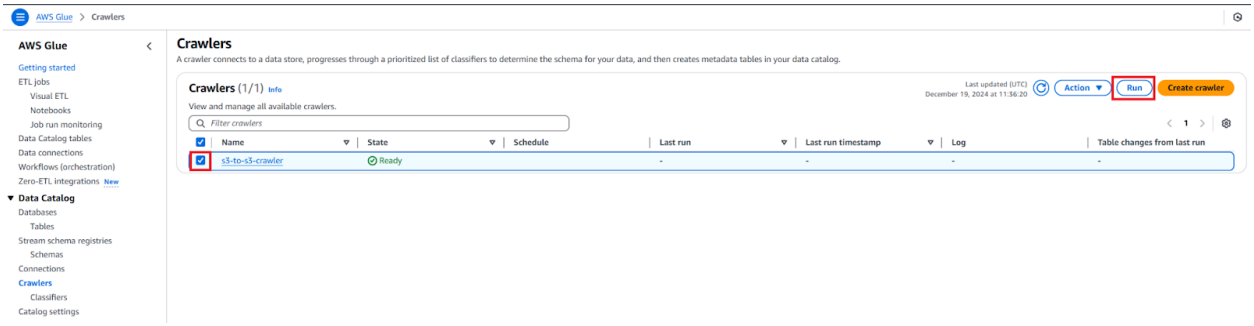
- Open your AWS Management Console and navigate to AWS Glue by searching for "Glue" in the Search Bar.



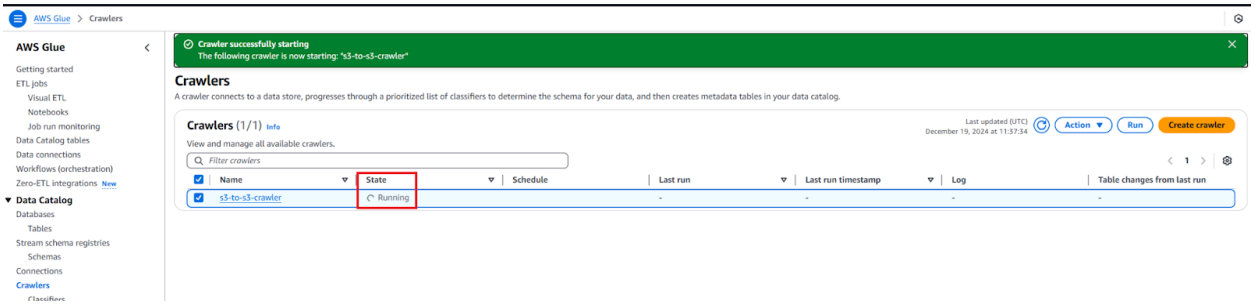
- Click on "AWS Glue," and you'll land on the page where click the three line menu button on the left top corner and then click on the Crawlers button



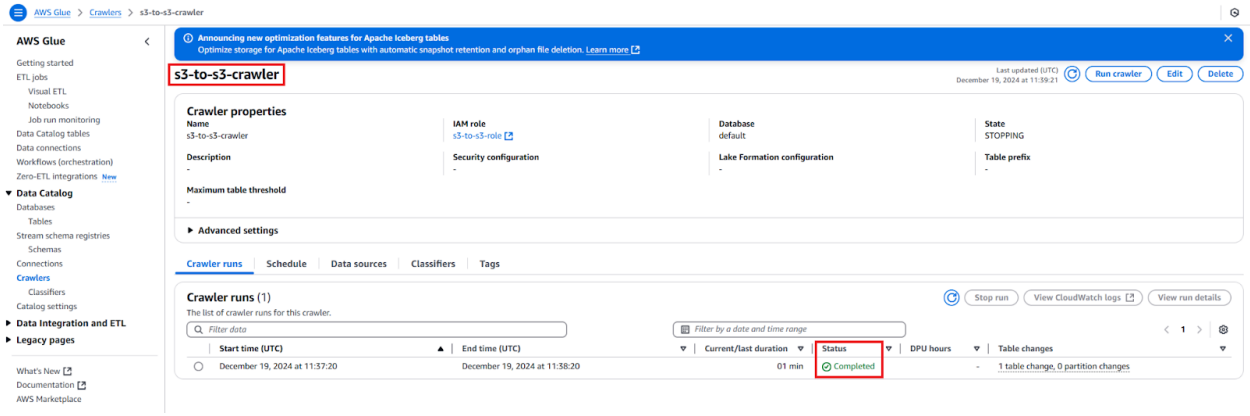
- On the crawlers page, select the already created crawler and click the Run button



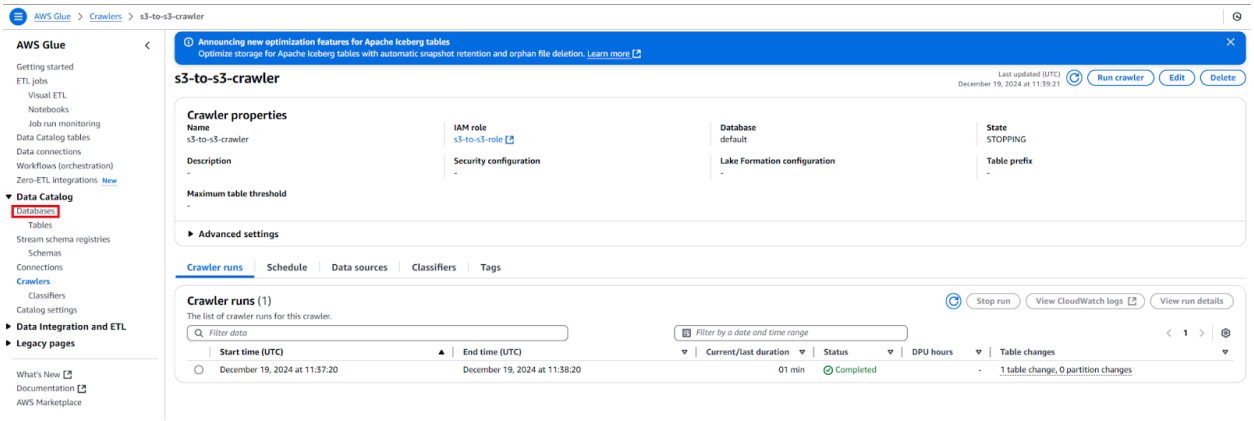
- Once you click the Run button, your crawler will be in the running phase. Wait for the crawler to finish



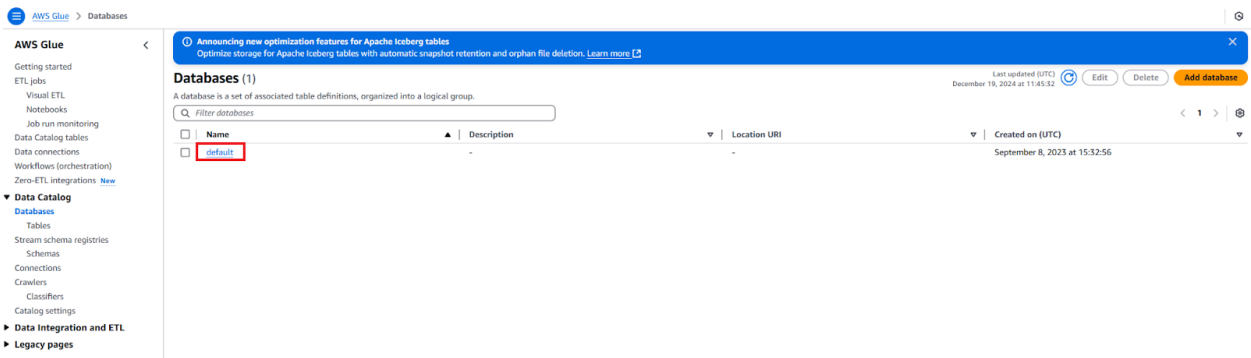
- Click the crawler to check the status of the execution. If everything is setup correctly it should be completed successfully



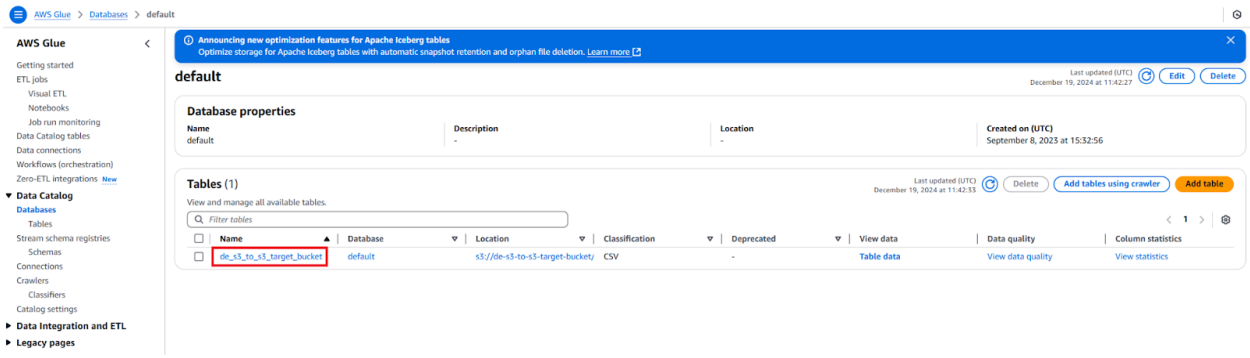
- Once the crawler completed successfully, Click on the Databases button on the left hand side menu



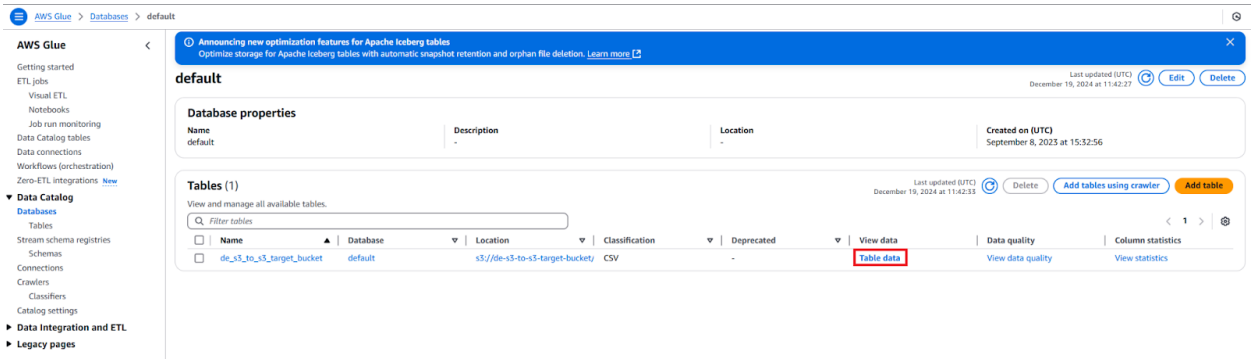
- Once you are on the databases page, click on the already existing default database to open it



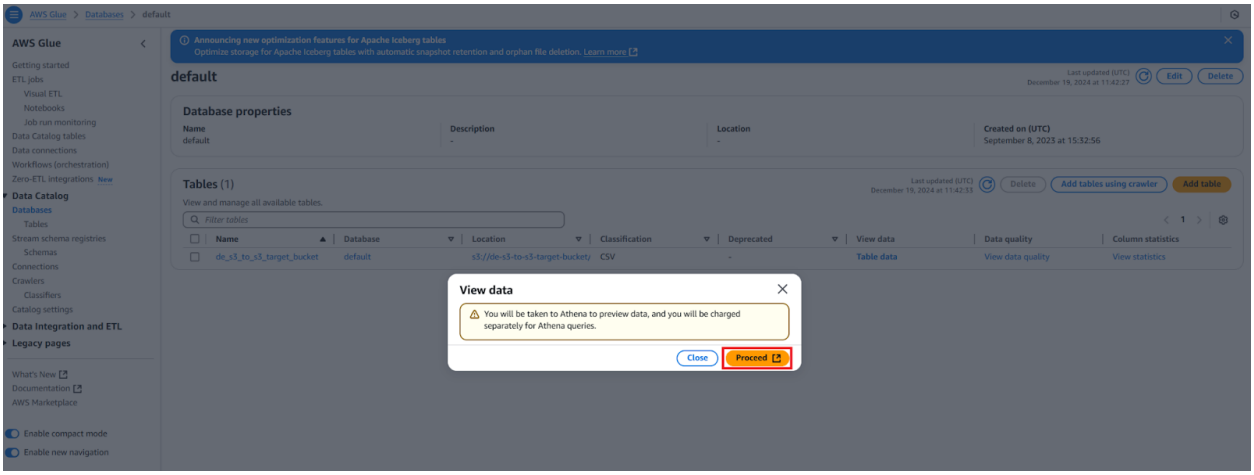
- On the tables page, you should be able to see a table with your S3 target bucket name.



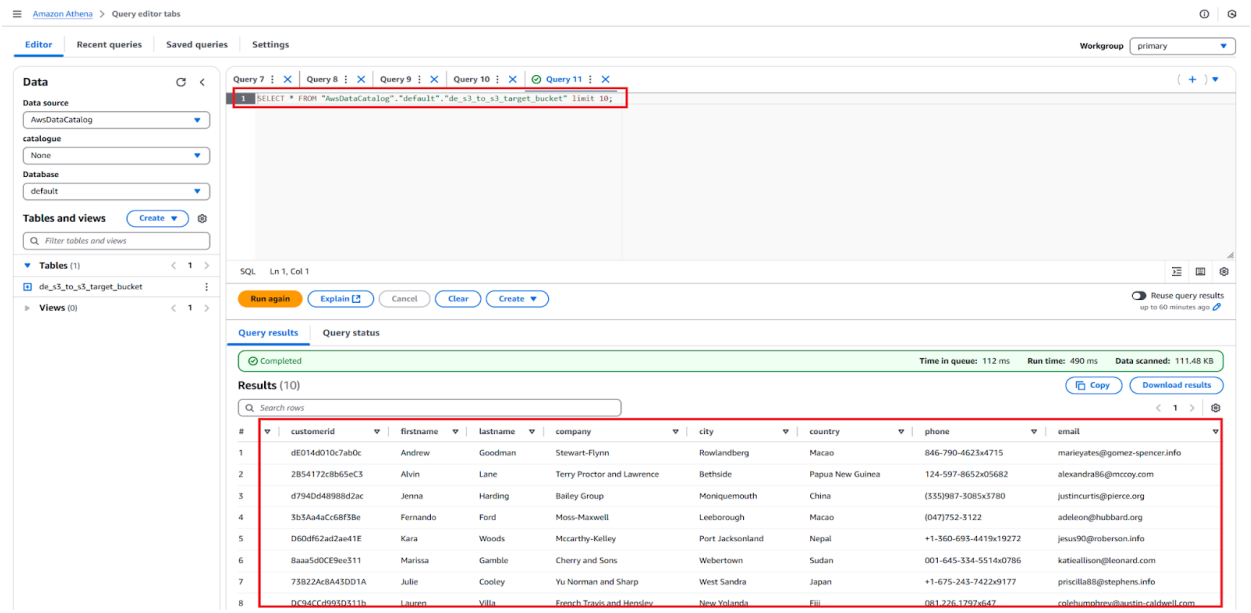
- Click on the Table data option to see this table data in the AWS Athena



- Click on the Proceed button to open this table in the AWS Athena



- Once you clicked on Procced, AWS will open the Athena Query editor with a simple select statement with your table data



VOILA! YOU HAVE SUCCESSFULLY TESTED YOUR S3-S3 CROSS REGION MIGRATION PROJECT AND ABLE TO QUERY THE DATA IN THE AWS ATHENA