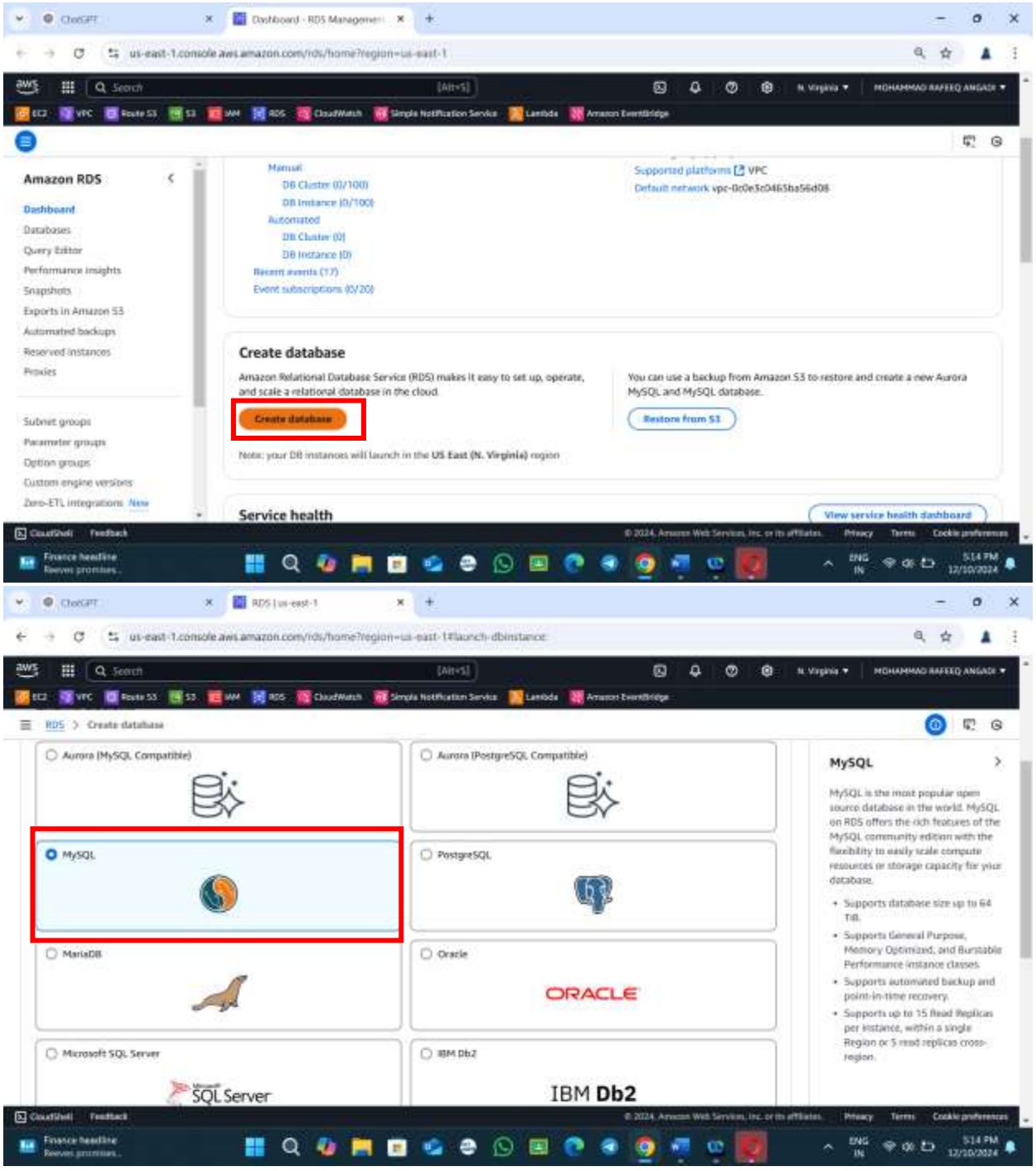
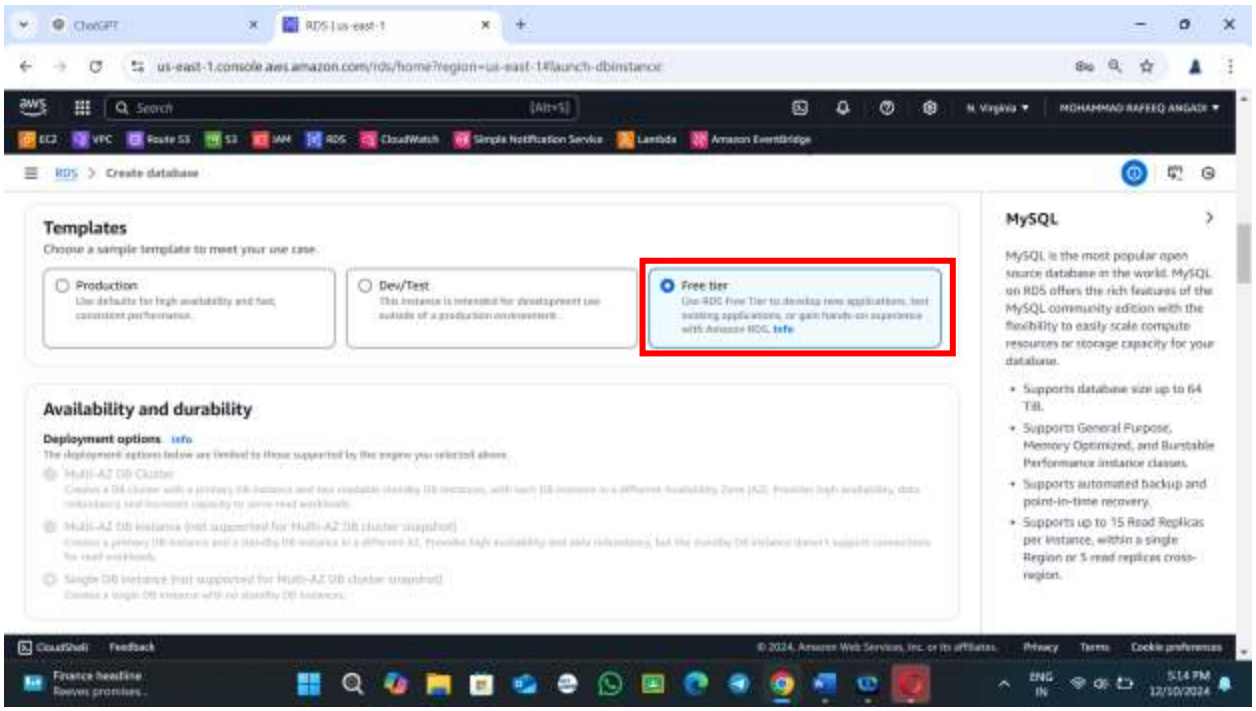
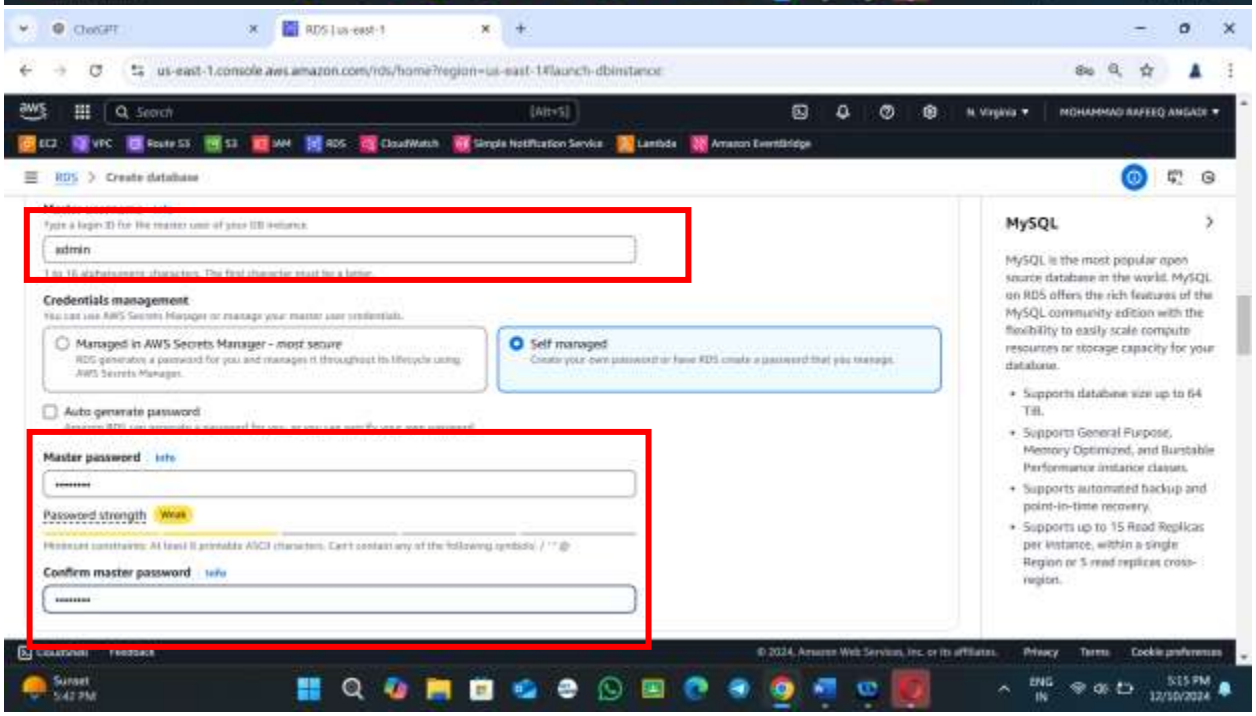
AWS Lambda to connect to an Amazon RDS

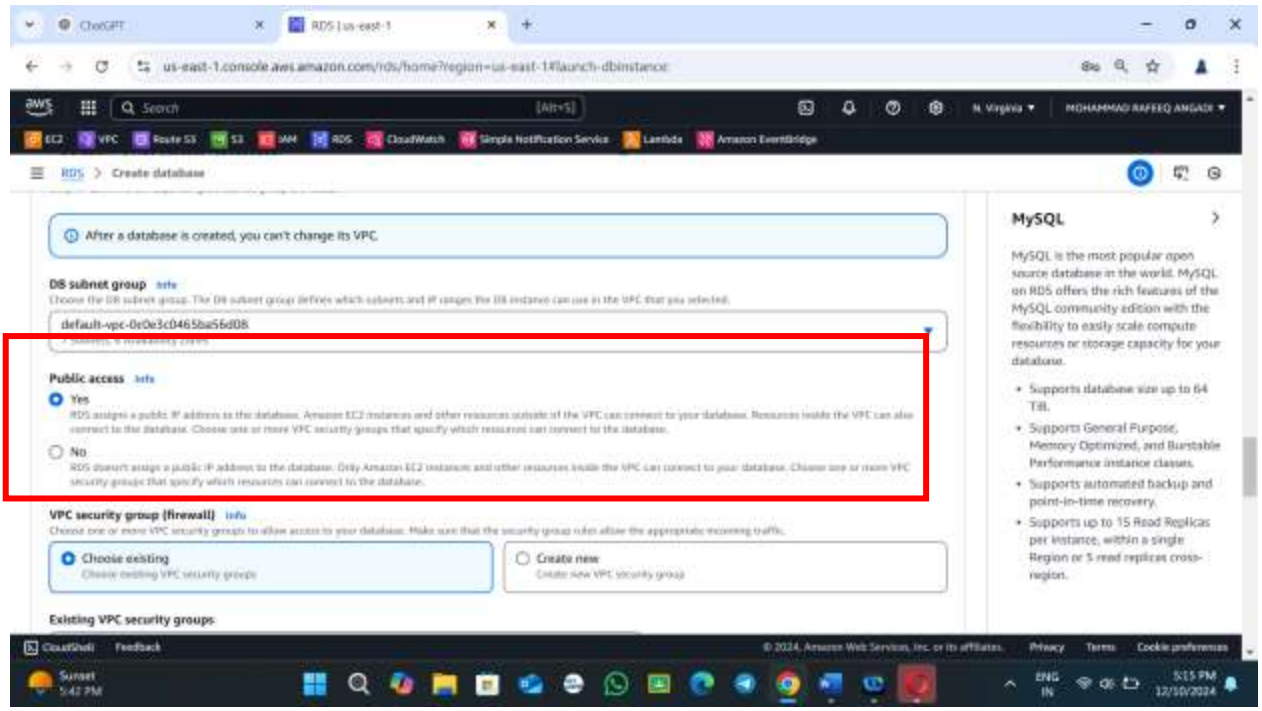
Using AWS Lambda to connect to an Amazon RDS (Relational Database Service) instance is a common approach to building serverless applications. Here's a step-by-step guide to achieve this:

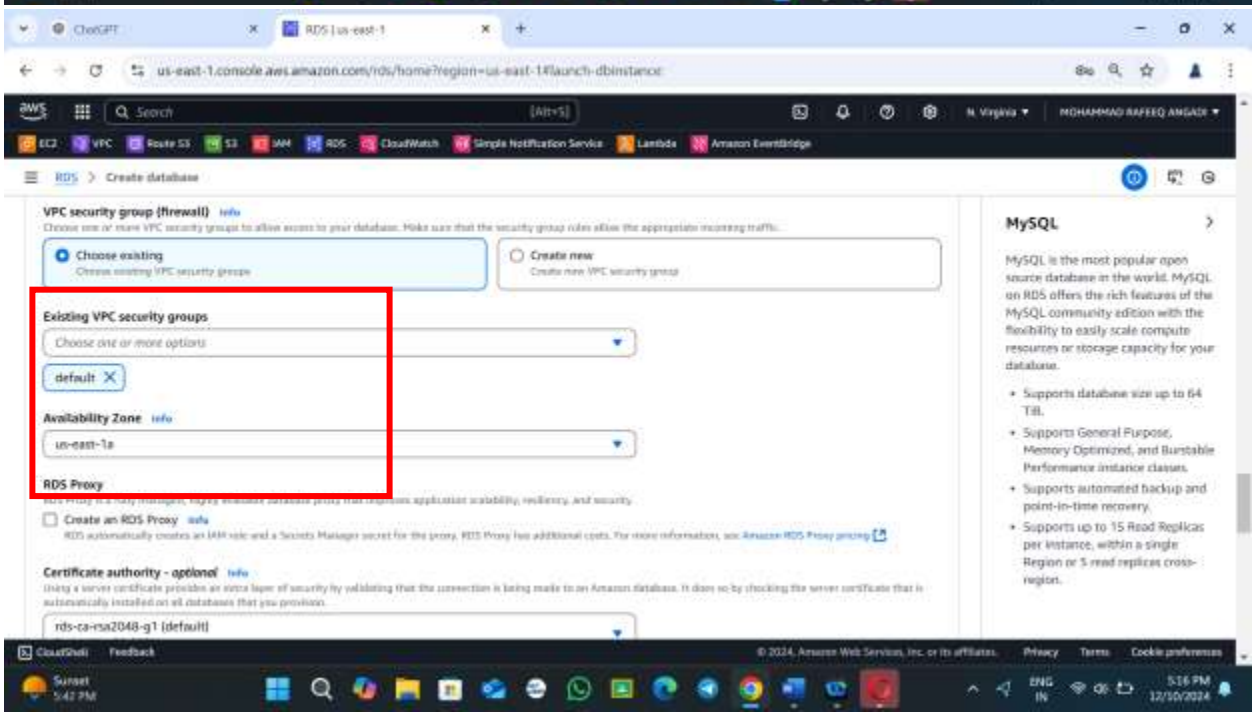
1. Set Up Your RDS Database

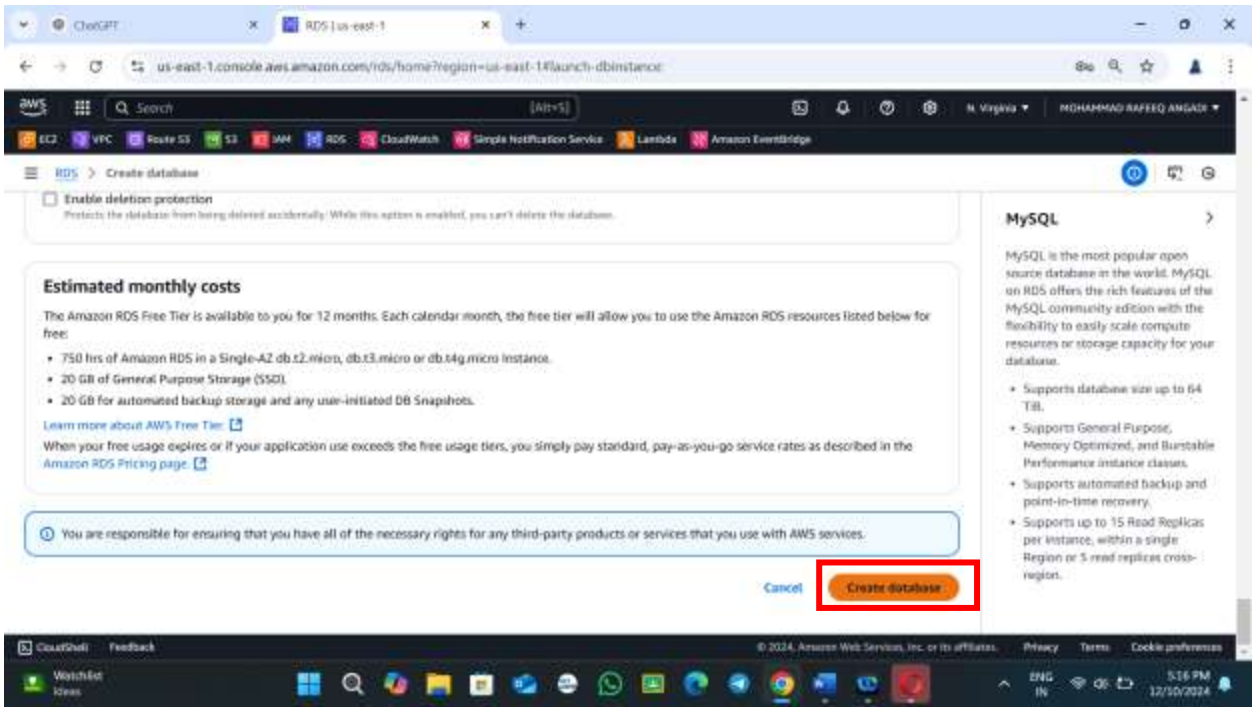



us-east-1.console.aws.amazon.com/rds/home?region=us-east-1#launch-dbinstance:
RDS > Create database
Templates
Choose a sample template to meet your use case.
Production
Dev/Test
Free tier
Availability and durability
Deployment options info
MySQL
MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.
Supports database size up to 64 TiB.
Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
Supports automated backup and point-in-time recovery.
Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.

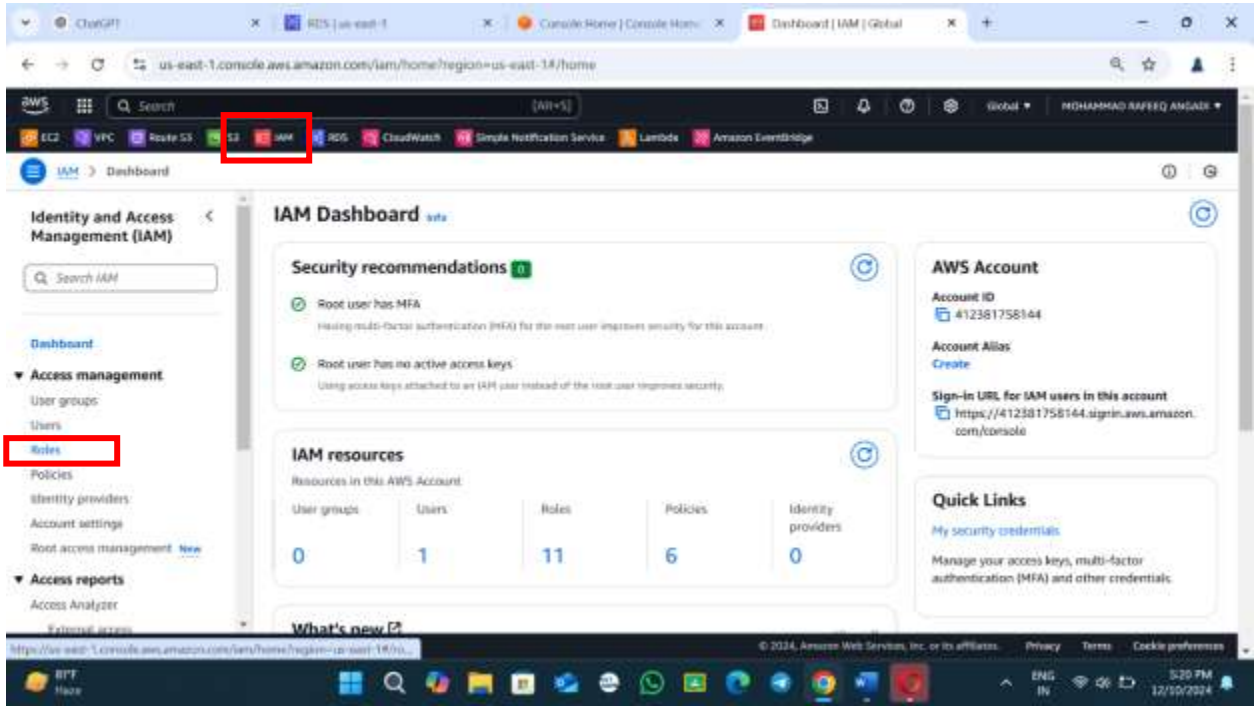

us-east-1.console.aws.amazon.com/rds/home?region=us-east-1#launch-dbinstance:
RDS > Create database
admin
Credentials management
Managed in AWS Secrets Manager - most secure
Self managed
Auto generate password
Master password info
Password strength Weak
Confirm master password info
MySQL
MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.
Supports database size up to 64 TiB.
Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
Supports automated backup and point-in-time recovery.
Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.

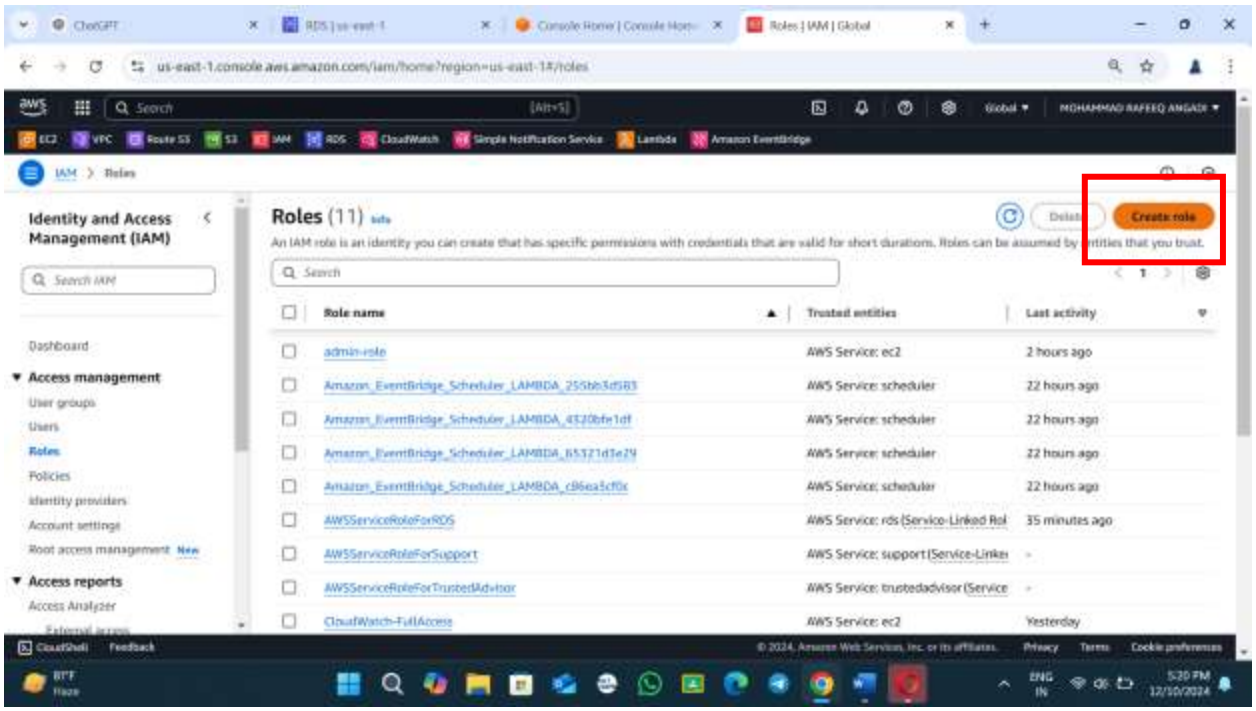

us-east-1.console.aws.amazon.com/rds/home?region=us-east-1#launch-dbinstance:
RDS > Create database
After a database is created, you can't change its VPC.
DB subnet group
default-vpc-0c0e3c0465ba56d08
Public access
Yes
No
VPC security group (firewall)
Choose existing
Create new
Existing VPC security groups
MySQL
MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.
Supports database size up to 64 TiB.
Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
Supports automated backup and point-in-time recovery.
Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.

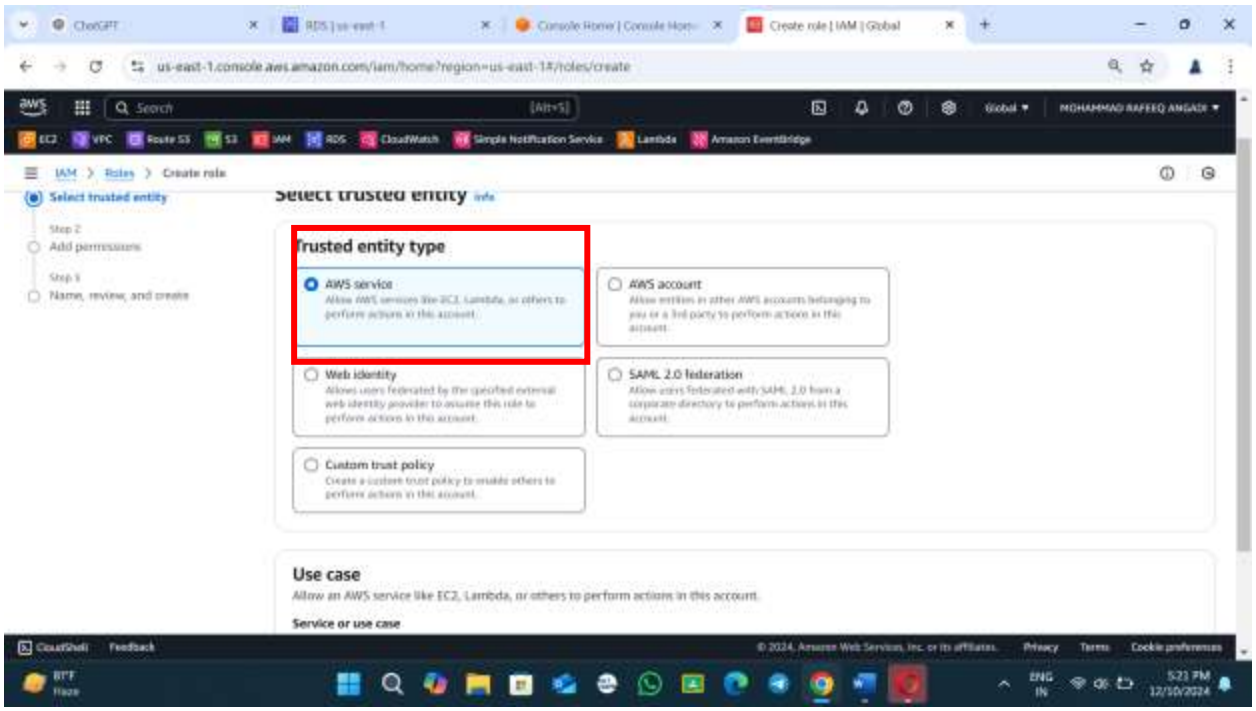

us-east-1.console.aws.amazon.com/rds/home?region=us-east-1#launch-dbinstance:
RDS > Create database
VPC security group (firewall)
Choose existing
Create new
Existing VPC security groups
Choose one or more options
default
Availability Zone
us-east-1a
RDS Proxy
Create an RDS Proxy
Certificate authority - optional
rds-ca-rsa2048-g1 (default)
MySQL
MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.
Supports database size up to 64 TiB.
Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
Supports automated backup and point-in-time recovery.
Supports up to 15 Read Replicas per instance, within a single Region or 5 read replicas cross-region.

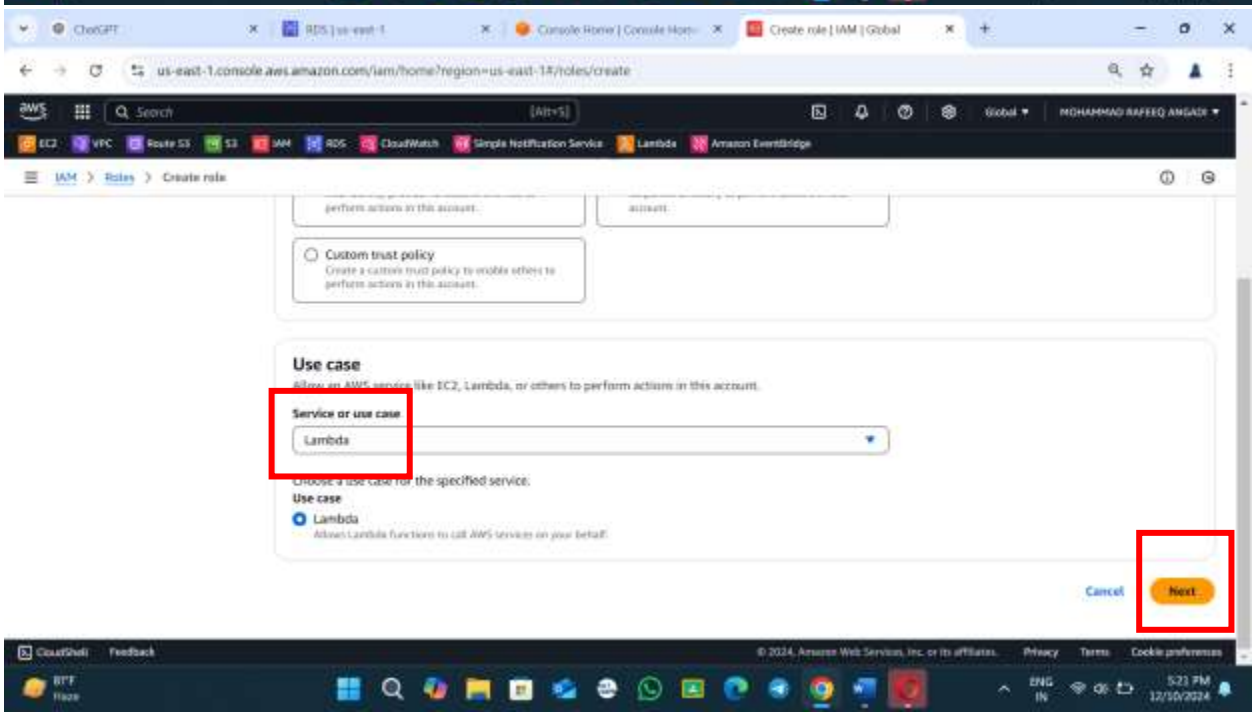


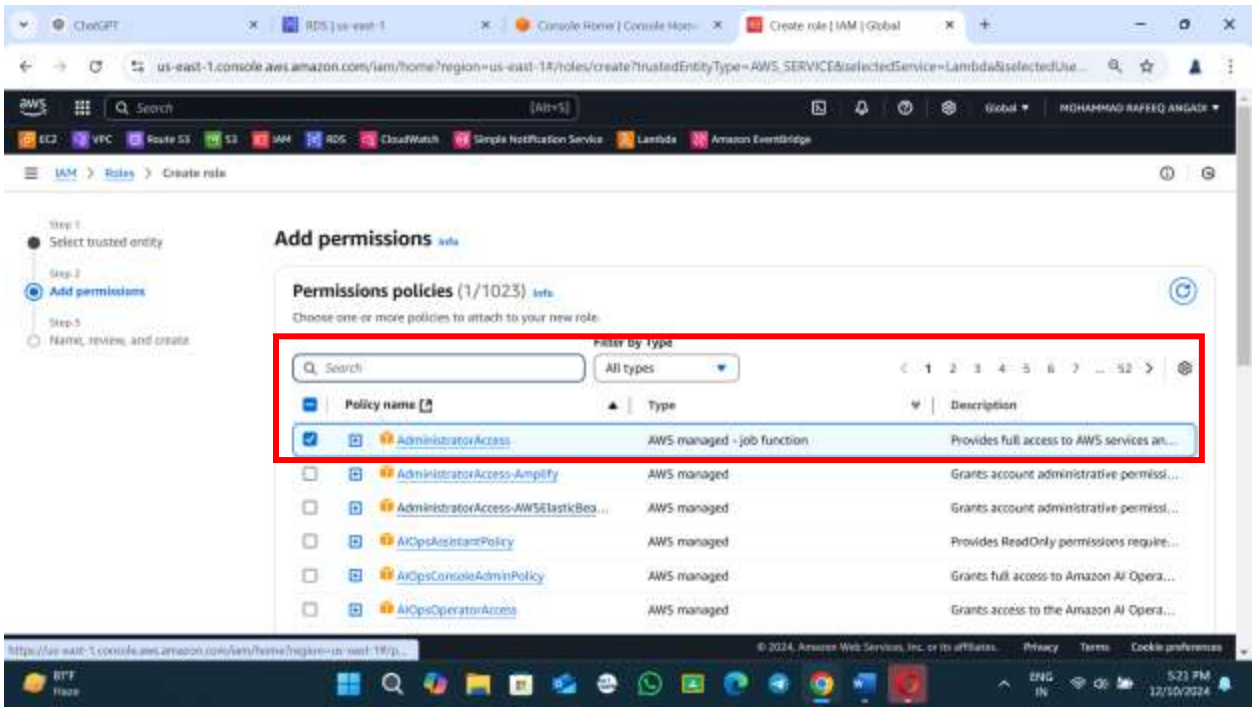
Create IAM Role For Lambda Function

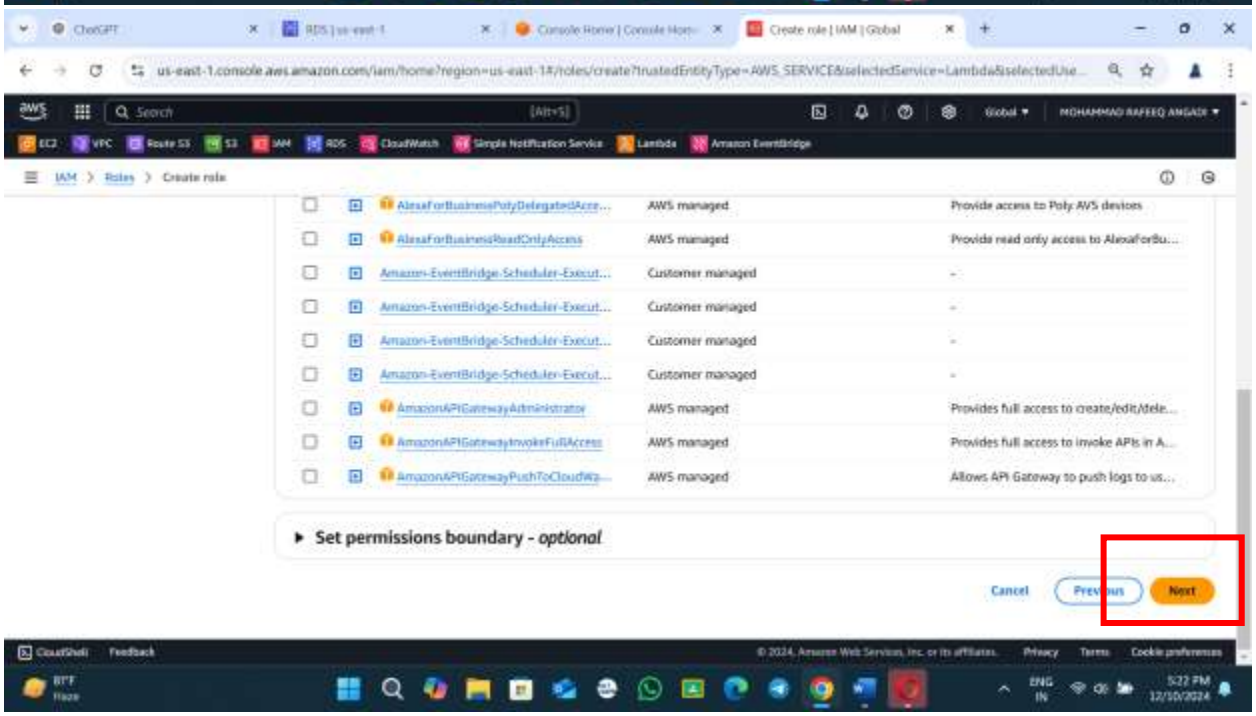


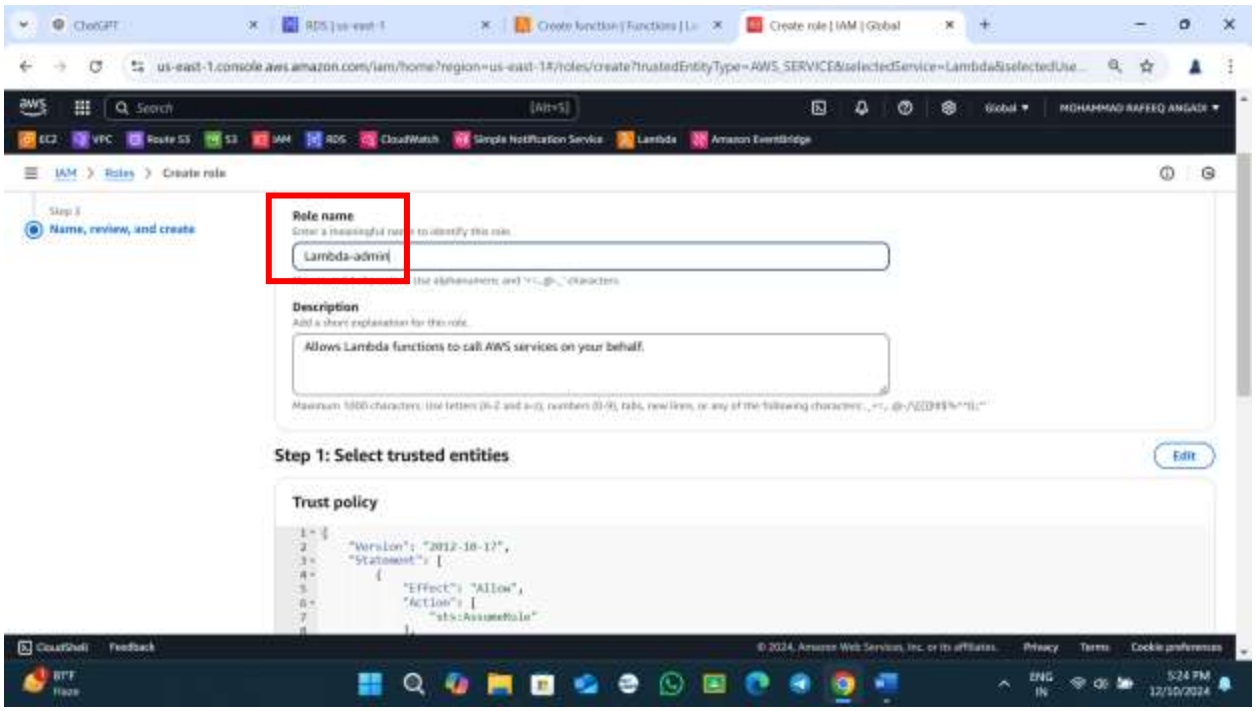

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles
Search
[Alt+S]
Global
MOHAMMAD RAFEEQ ANGADI
IAM > Roles
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
Roles (11) Info
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.
Delete
Create role
Search
Role name
Trusted entities
Last activity
admin-role
AWS Service: ec2
2 hours ago
Amazon_EventBridge_Scheduler_LAMBDA_25Sbb3d583
AWS Service: scheduler
22 hours ago
Amazon_EventBridge_Scheduler_LAMBDA_4320bfe1df
AWS Service: scheduler
22 hours ago
Amazon_EventBridge_Scheduler_LAMBDA_b5321d3e29
AWS Service: scheduler
22 hours ago
Amazon_EventBridge_Scheduler_LAMBDA_c86ea5cf0c
AWS Service: scheduler
22 hours ago
AWSServiceRoleForRDS
AWS Service: rds (Service-Linked Rol
35 minutes ago
AWSServiceRoleForSupport
AWS Service: support (Service-Linke
-
AWSServiceRoleForTrustedAdvisor
AWS Service: trustedadvisor (Service
-
CloudWatch-FullAccess
AWS Service: ec2
Yesterday
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
5:20 PM
12/10/2024

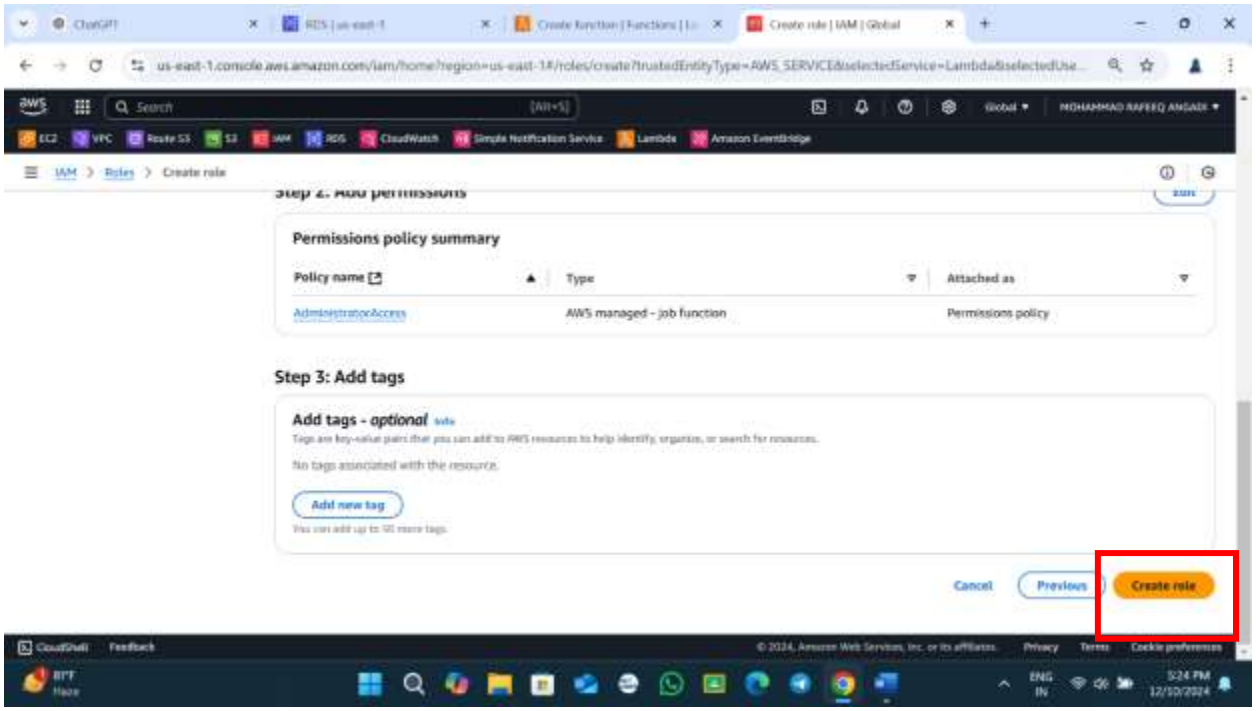

Create role | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create
IAM > Roles > Create role
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Trusted entity type
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.
Service or use case


Create role | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create
IAM > Roles > Create role
Custom trust policy
Use case
Service or use case
Lambda
Use case
Lambda
Cancel
Next


Add permissions
Permissions policies (1/1023)
Choose one or more policies to attach to your new role.
Filter by Type
All types
Policy name
Type
Description
AdministratorAccess
AWS managed - job function
Provides full access to AWS services an...
AdministratorAccess-Amplify
AWS managed
Grants account administrative permissi...
AdministratorAccess-AWSElasticBea...
AWS managed
Grants account administrative permissi...
AIOpsAssistantPolicy
AWS managed
Provides ReadOnly permissions require...
AIOpsConsoleAdminPolicy
AWS managed
Grants full access to Amazon AI Opera...
AIOpsOperatorAccess
AWS managed
Grants access to the Amazon AI Opera...

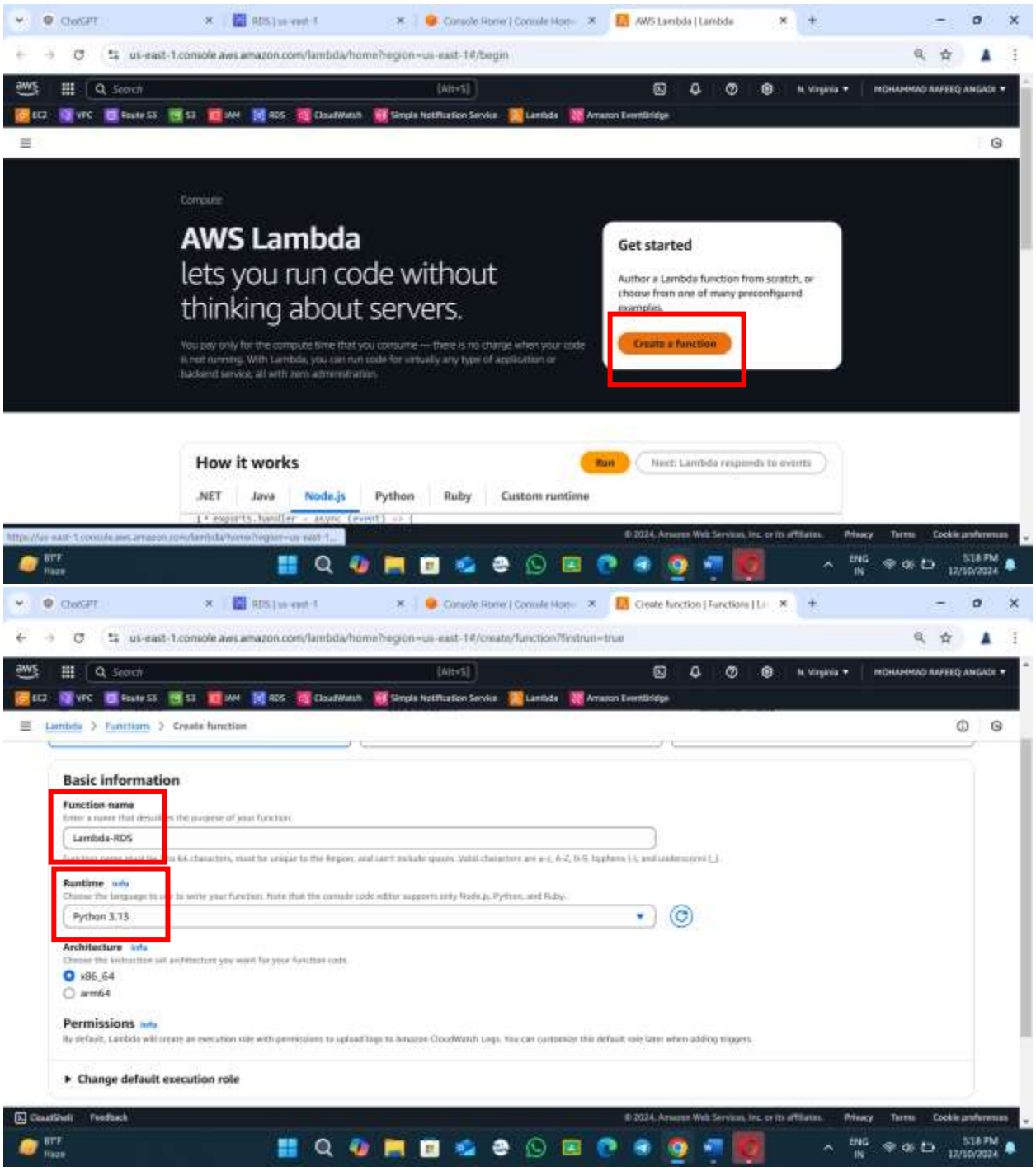

Set permissions boundary - optional
Cancel
Next

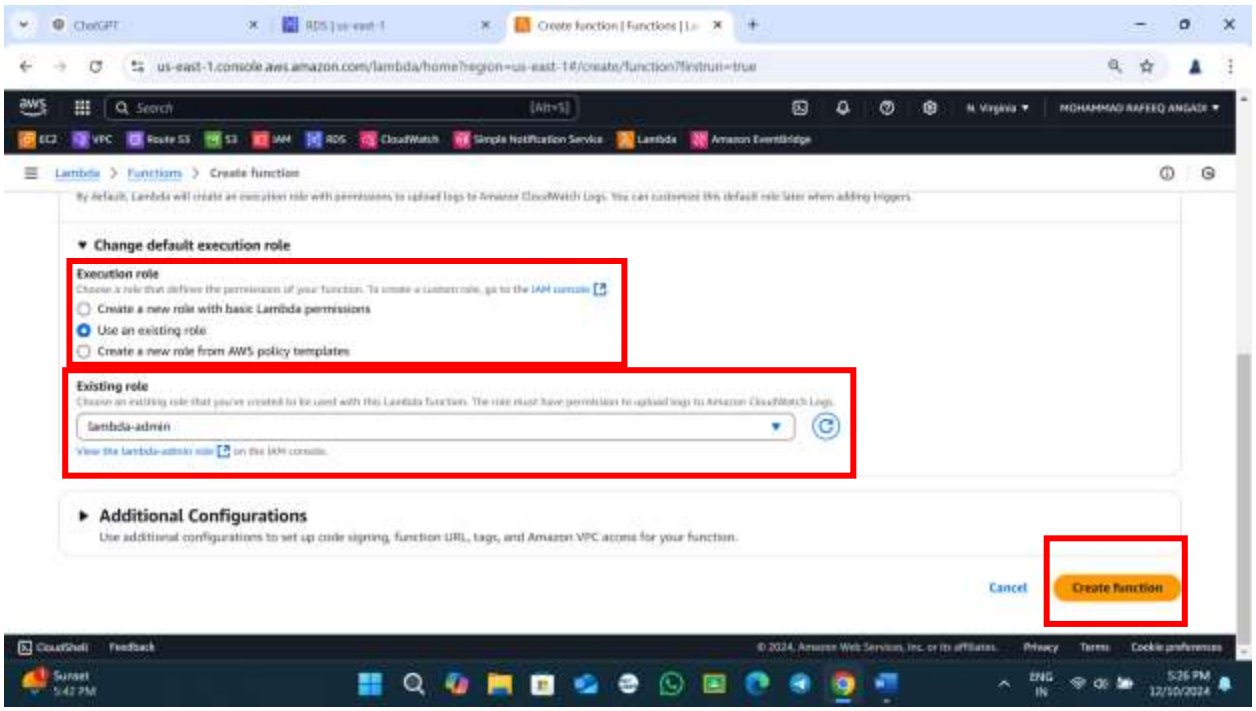

Role name
Lambda-admin
Description
Allows Lambda functions to call AWS services on your behalf.
Step 1: Select trusted entities
Edit
Trust policy
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"sts:AssumeRole"


Permissions policy summary
Policy name
Type
Attached as
AdministratorAccess
AWS managed - job function
Permissions policy
Step 3: Add tags
Add tags - optional
No tags associated with the resource.
Add new tag
Cancel
Previous
Create role

2. Create a Lambda Function

- Go to the **AWS Lambda Console** and create a new function.
- Choose a runtime supported by the database client library you'll use (e.g., Python, Node.js, Java).

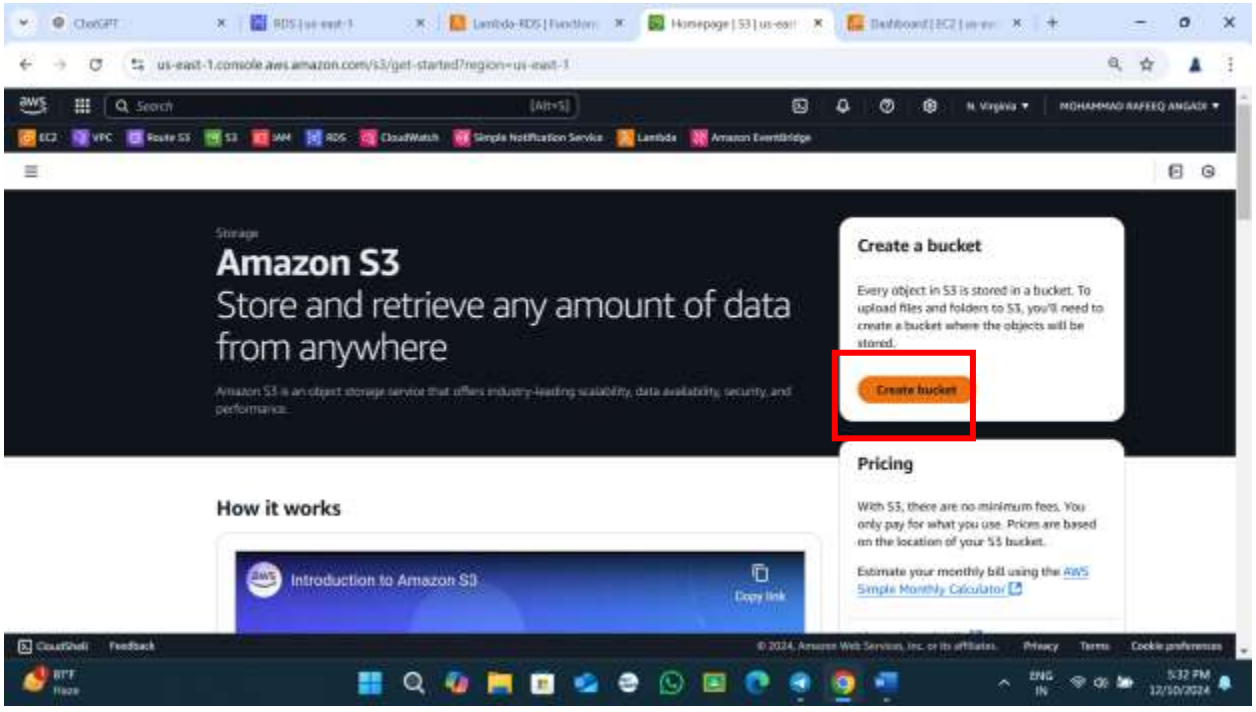


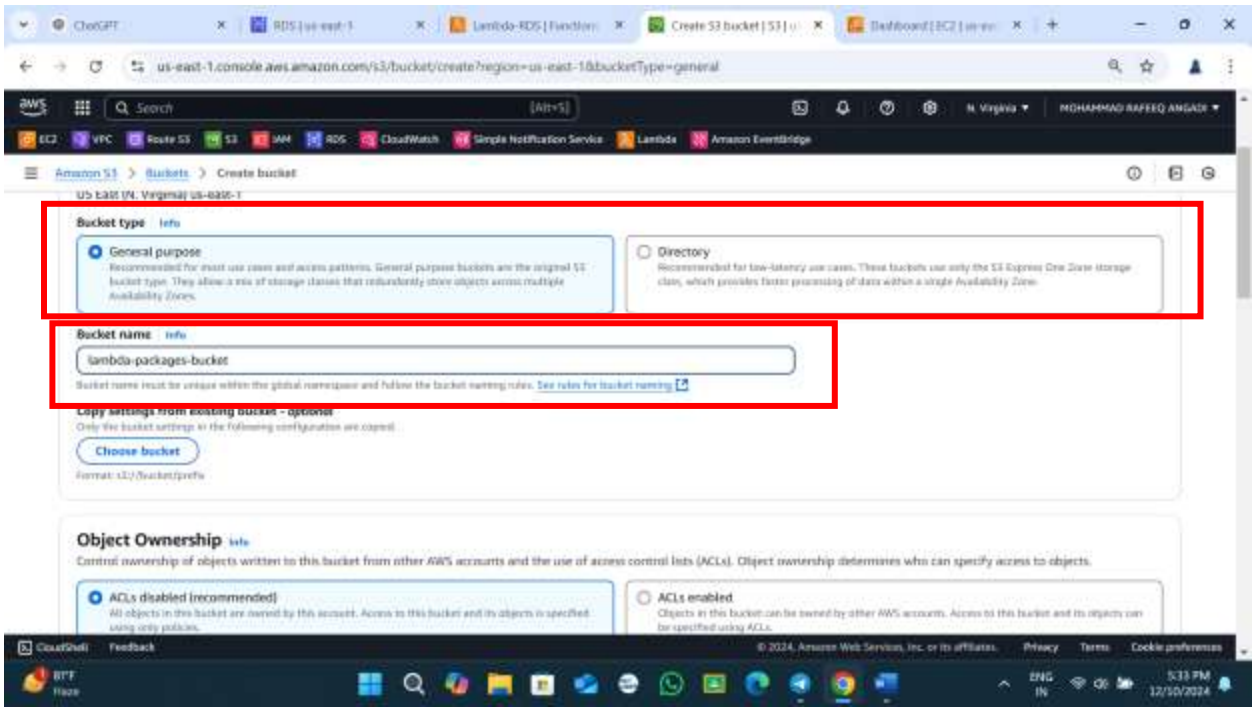


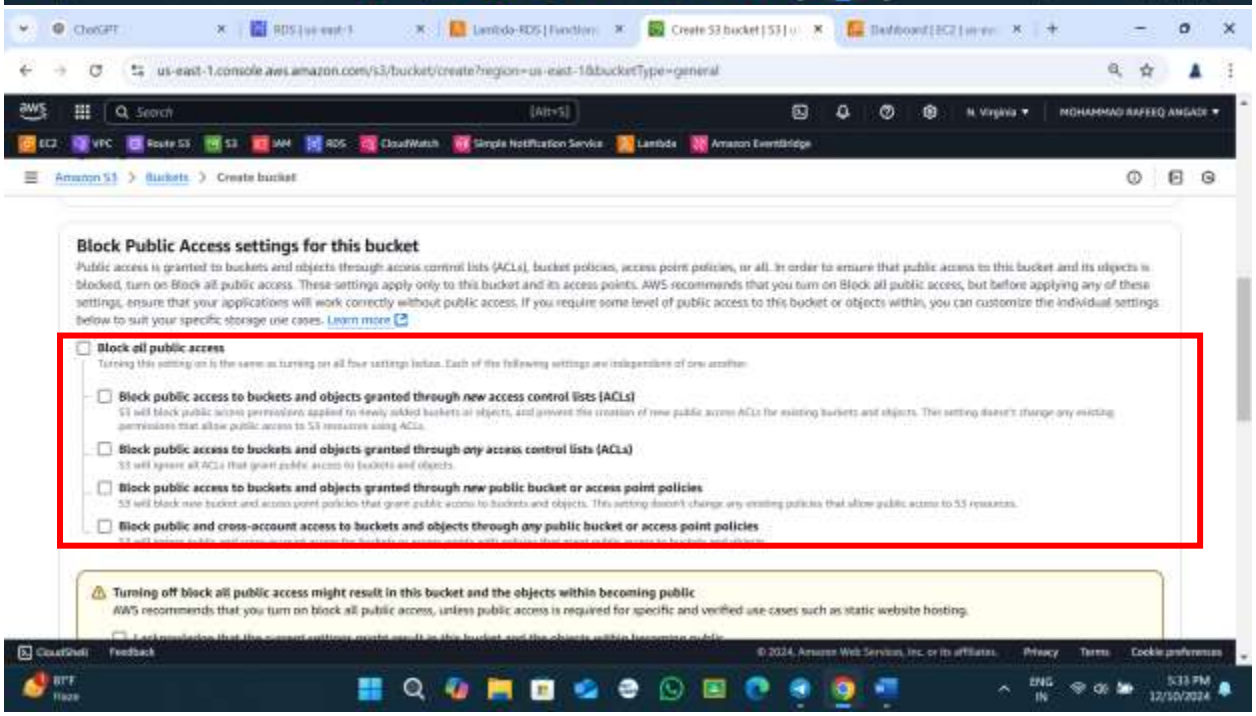
3. Install Database Client Library

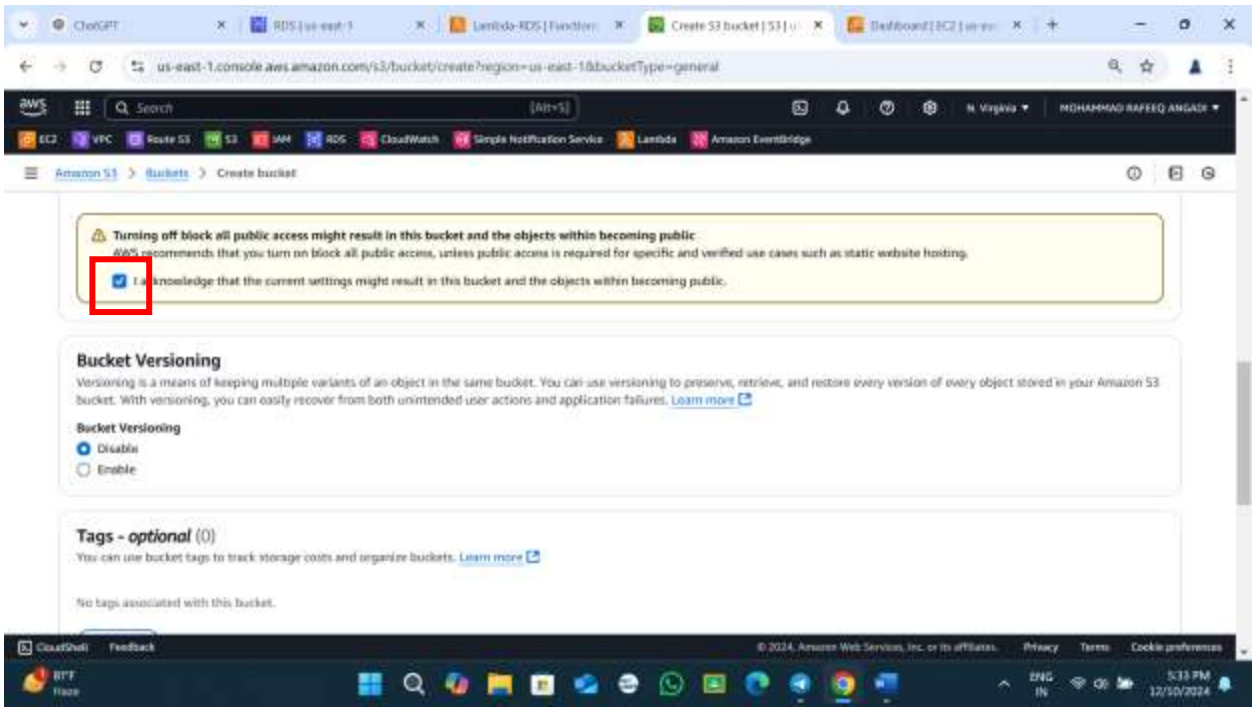
Connect the instance and install pymysql package and cp the package into s3

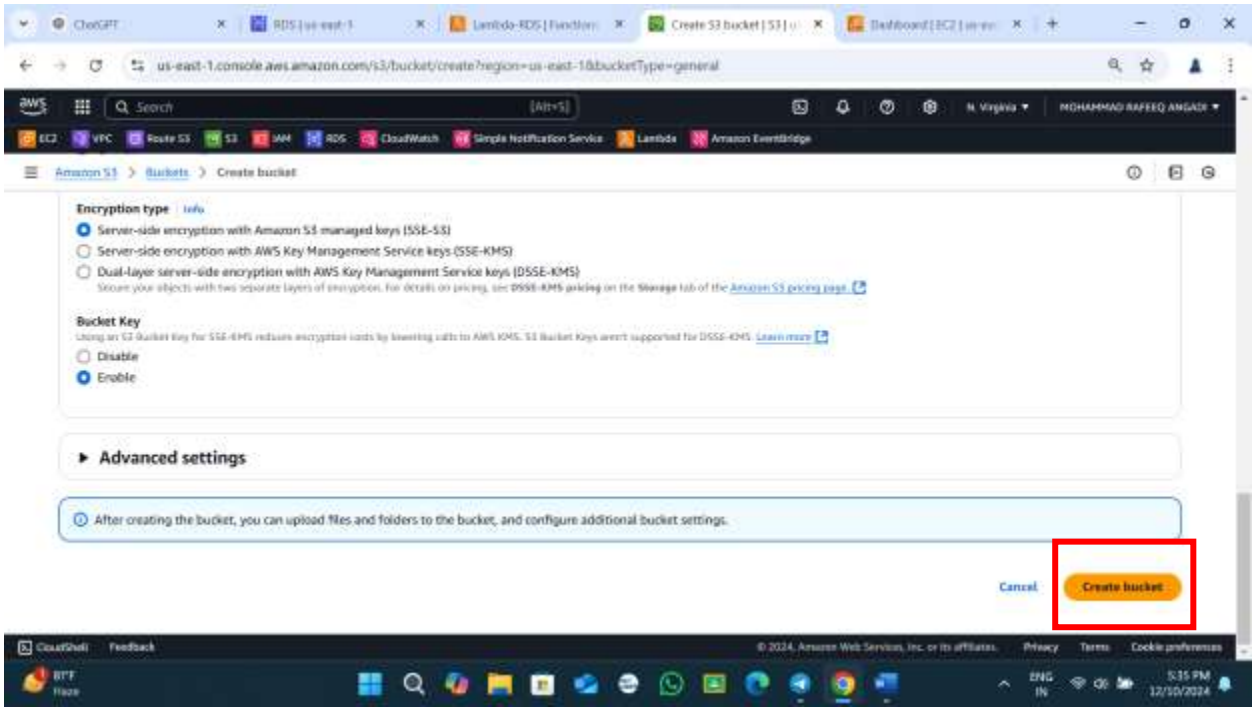
First we can create s3 bucket

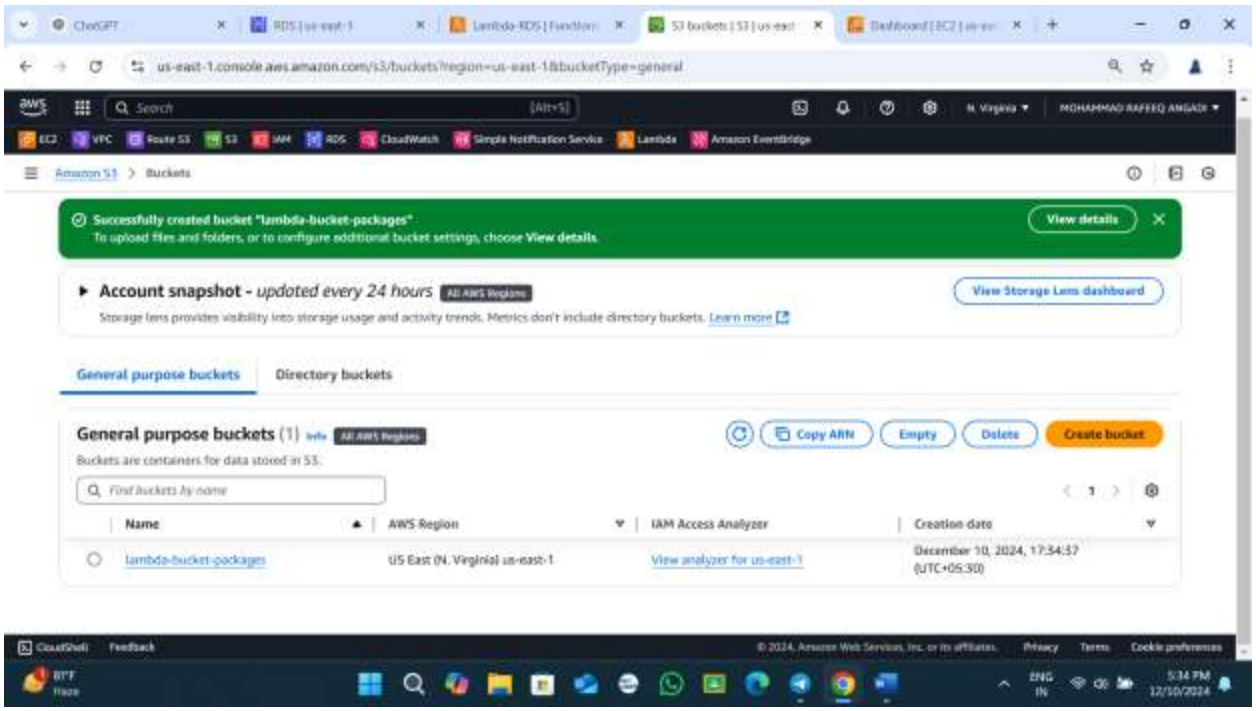



us-east-1.console.aws.amazon.com/s3/bucket/create?region=us-east-1&bucketType=general
Amazon S3 > Buckets > Create bucket
Bucket type Info
General purpose
Directory
Bucket name Info
lambda-packages-bucket
Choose bucket
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
ACLs enabled
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

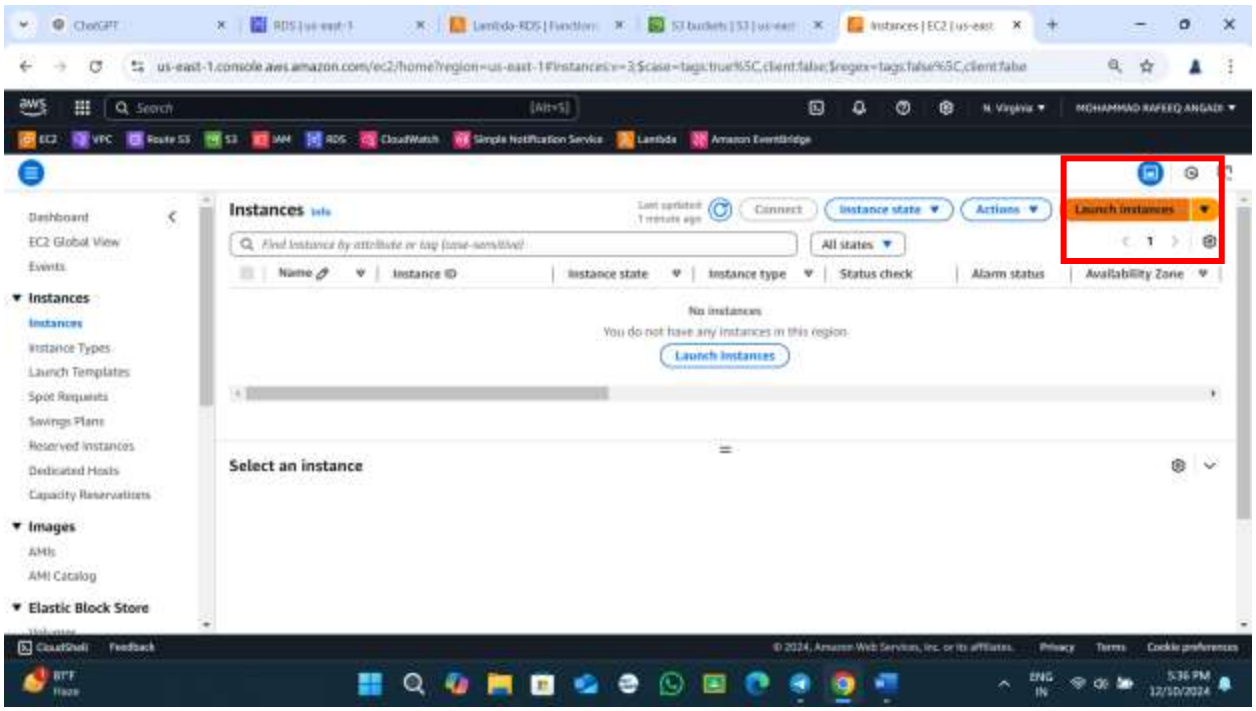

us-east-1.console.aws.amazon.com/s3/bucket/create?region=us-east-1&bucketType=general
Amazon S3 > Buckets > Create bucket
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In 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
Block public access to buckets and objects granted through new access control lists (ACLs)
Block public access to buckets and objects granted through any access control lists (ACLs)
Block public access to buckets and objects granted through new public bucket or access point policies
Block public and cross-account access to buckets and objects through any public bucket or access point policies
Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

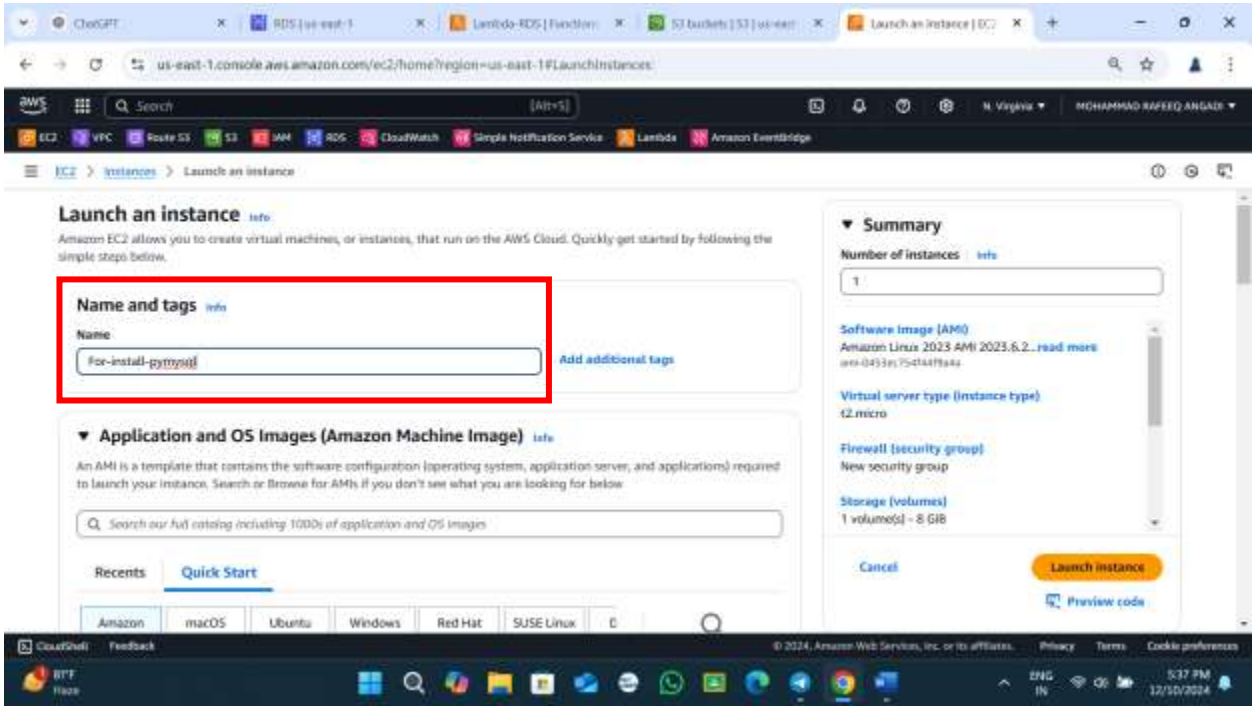

Turning off block all public access might result in this bucket and the objects within becoming public
I acknowledge that the current settings might result in this bucket and the objects within becoming public.
Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Bucket Versioning
Disable
Enable
Tags - optional (0)
You can use bucket tags to track storage costs and organize buckets. Learn more
No tags associated with this bucket.

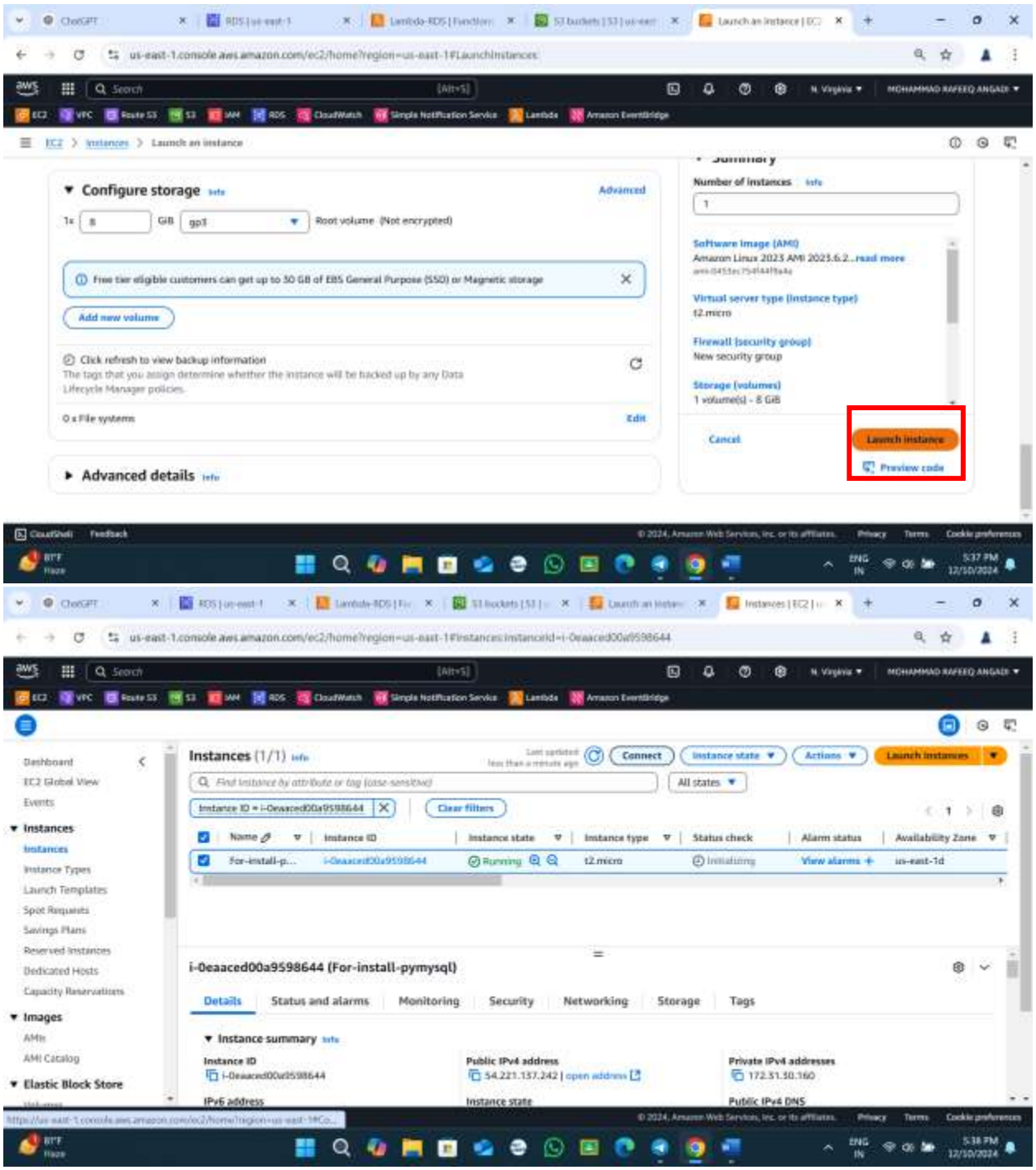

Encryption type
Server-side encryption with Amazon S3 managed keys (SSE-S3)
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Bucket Key
Disable
Enable
Advanced settings
After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.
Cancel
Create bucket



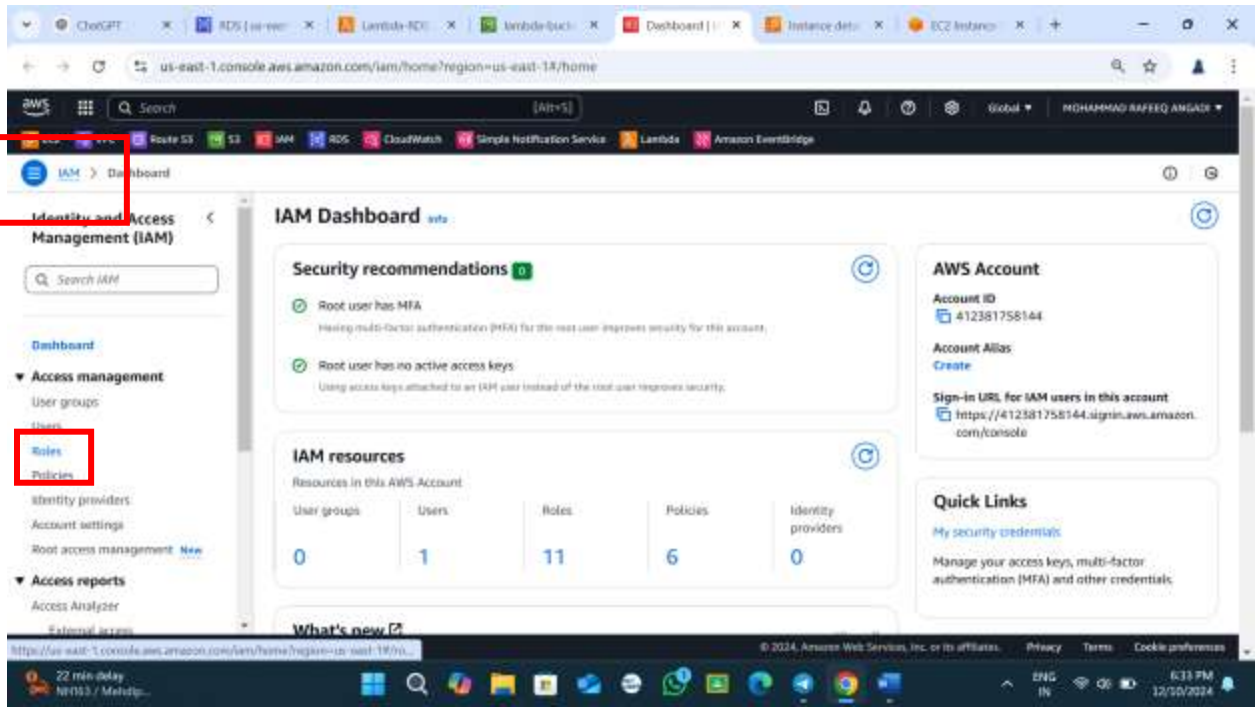
And next create instance for pymysql Install package and cp to s3 bucket

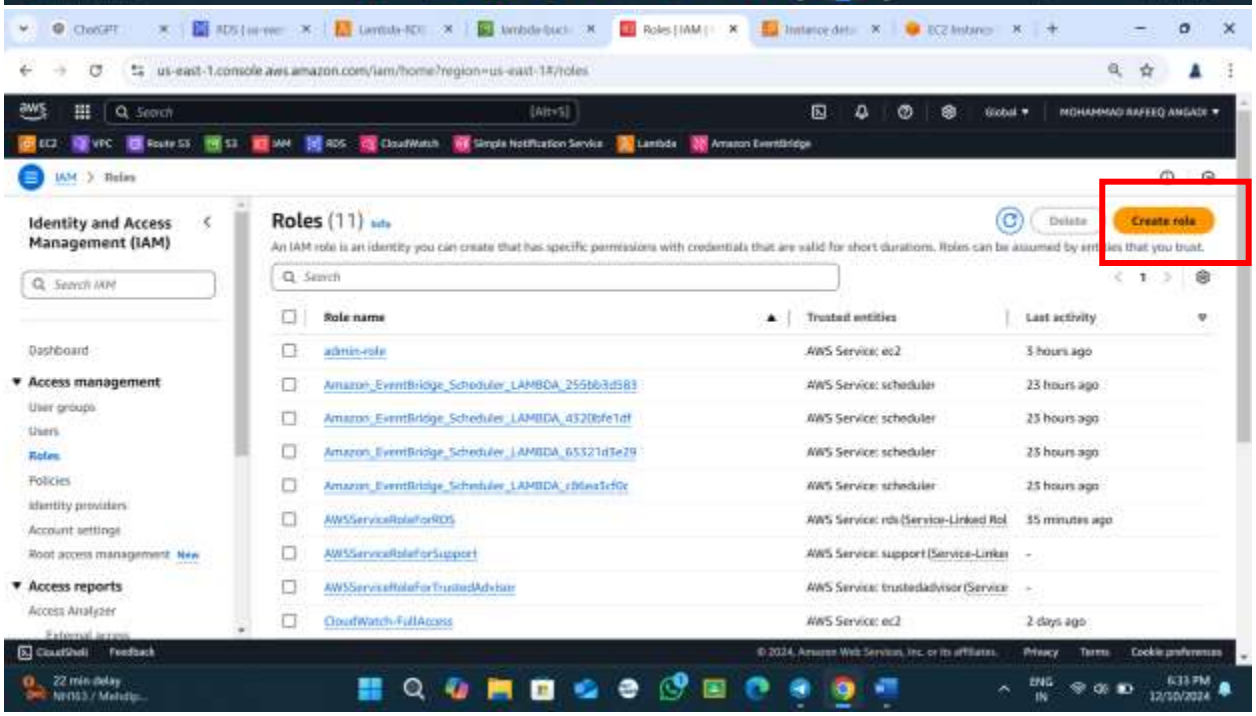

Instances
Launch instances
Select an instance

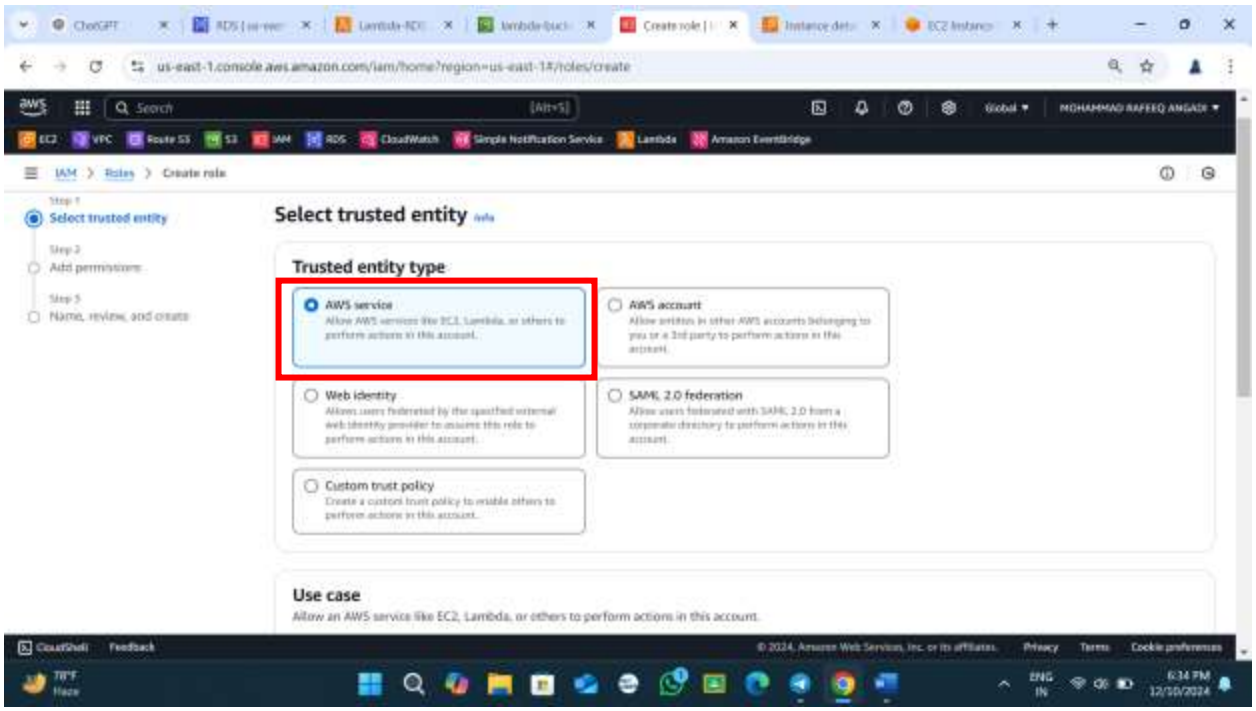

Launch an instance
Name and tags
For-install-pymysql
Add additional tags
Application and OS Images (Amazon Machine Image)
Summary
Launch instance

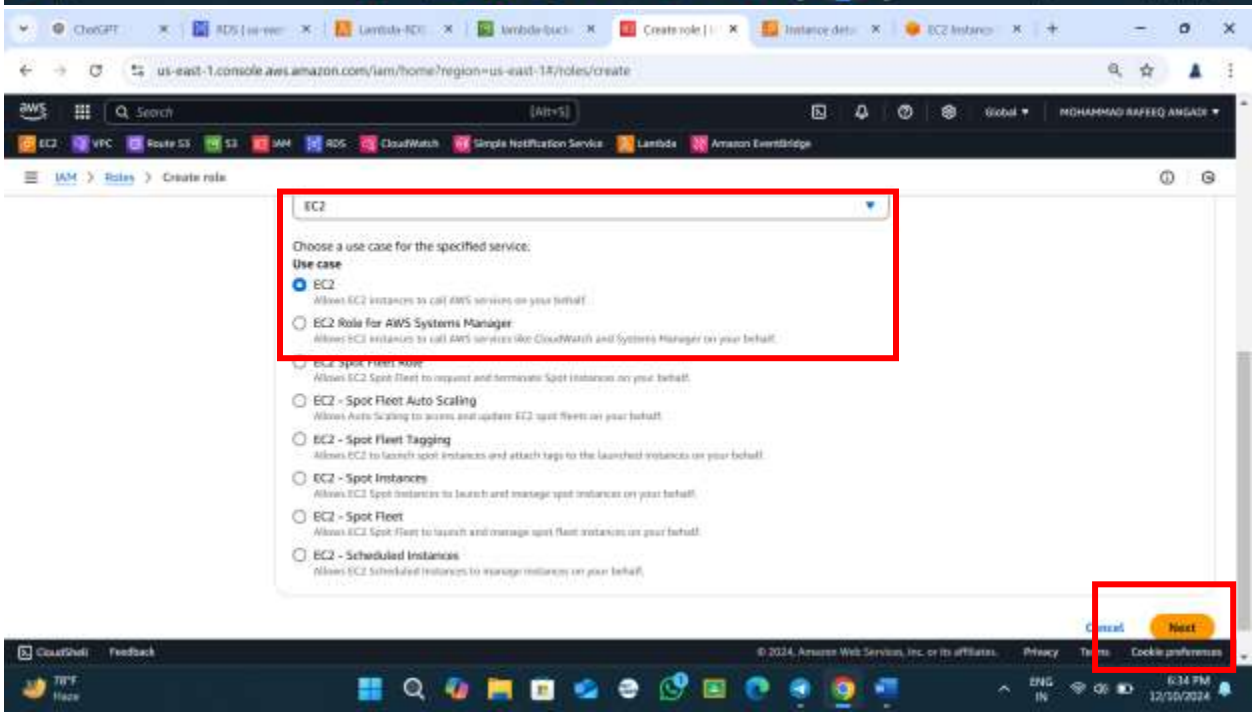


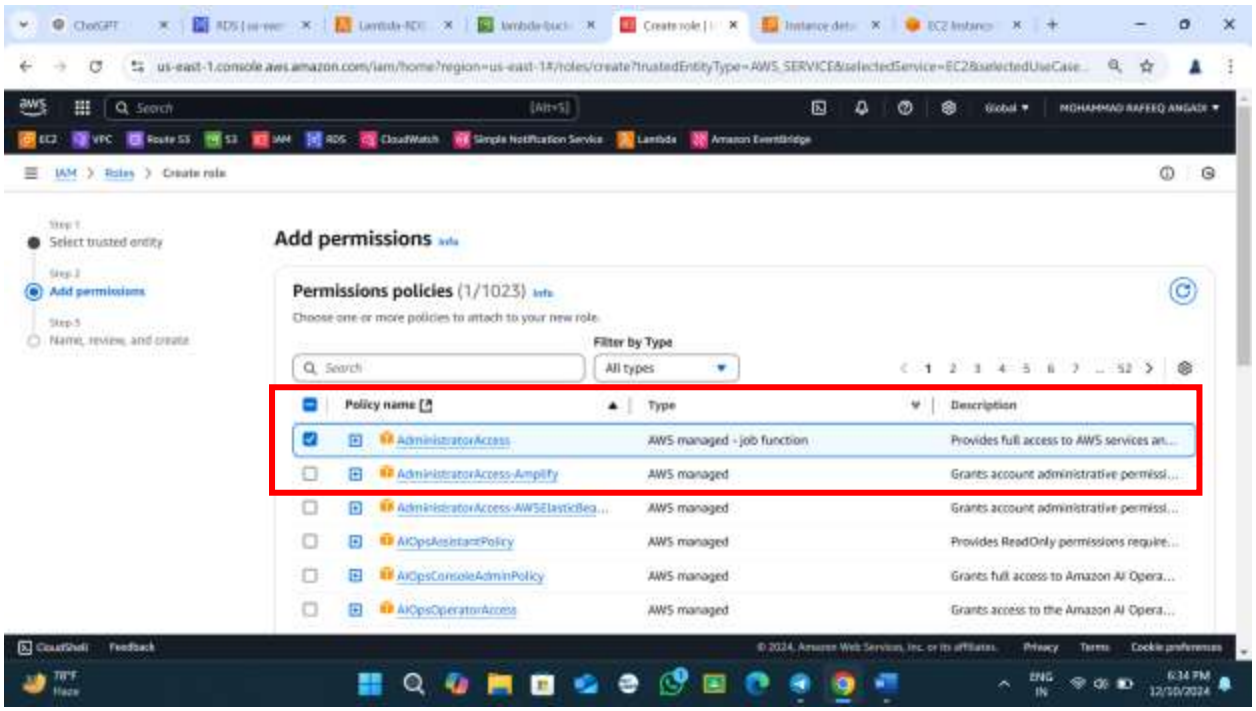
Create the IAM Role for instance

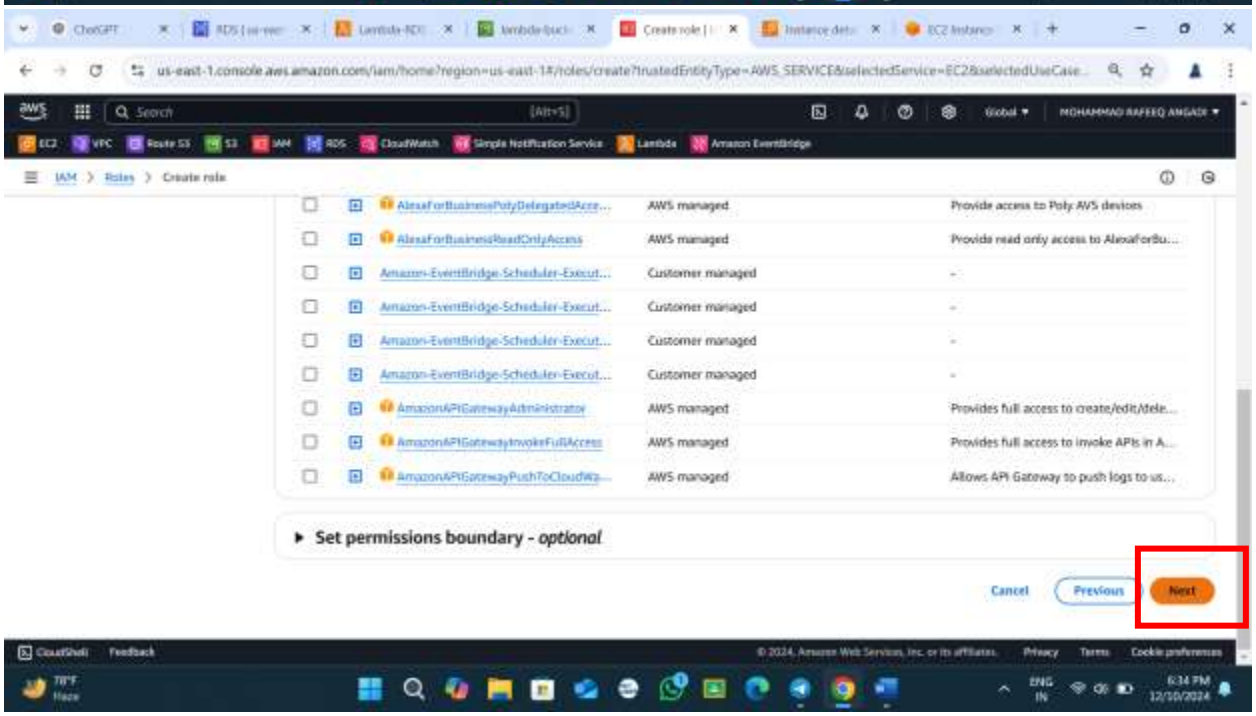

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/home
IAM > Dashboard
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
IAM Dashboard
Security recommendations 0
Root user has MFA
Root user has no active access keys
IAM resources
Resources in this AWS Account
User groups 0
Users 1
Roles 11
Policies 6
Identity providers 0
What's new
AWS Account
Account ID
412381758144
Account Alias
Create
Sign-in URL for IAM users in this account
https://412381758144.signin.aws.amazon.com/console
Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

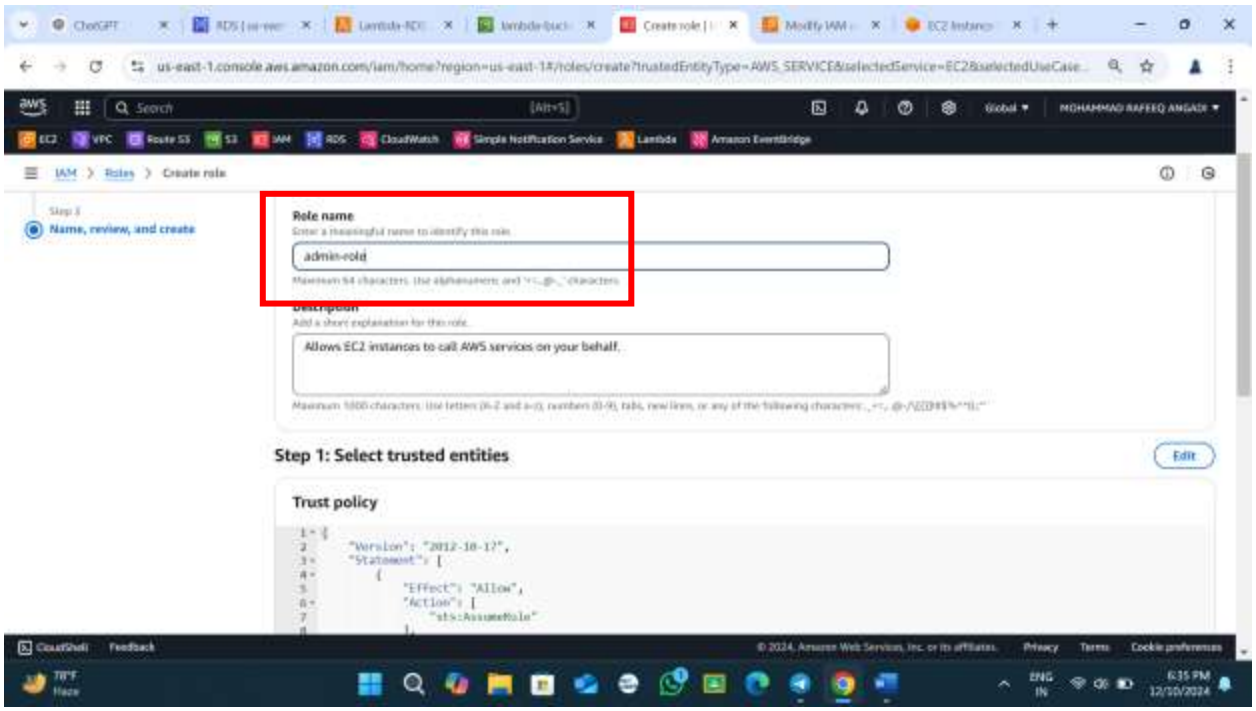

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles
IAM > Roles
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
Roles (11)
Delete
Create role
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.
Search
Role name
Trusted entities
Last activity
admin-role
AWS Service: ec2
5 hours ago
Amazon_EventBridge_Scheduler_LAMBDA_255bb3d583
AWS Service: scheduler
23 hours ago
Amazon_EventBridge_Scheduler_LAMBDA_4320bfe1df
AWS Service: scheduler
23 hours ago
Amazon_EventBridge_Scheduler_LAMBDA_65321d3e29
AWS Service: scheduler
23 hours ago
Amazon_EventBridge_Scheduler_LAMBDA_c06ea1cf0c
AWS Service: scheduler
23 hours ago
AWSServiceRoleForRDS
AWS Service: rds (Service-Linked Rol
35 minutes ago
AWSServiceRoleForSupport
AWS Service: support (Service-Linke
-
AWSServiceRoleForTrustedAdvisor
AWS Service: trustedadvisor (Service
-
CloudWatch-FullAccess
AWS Service: ec2
2 days ago

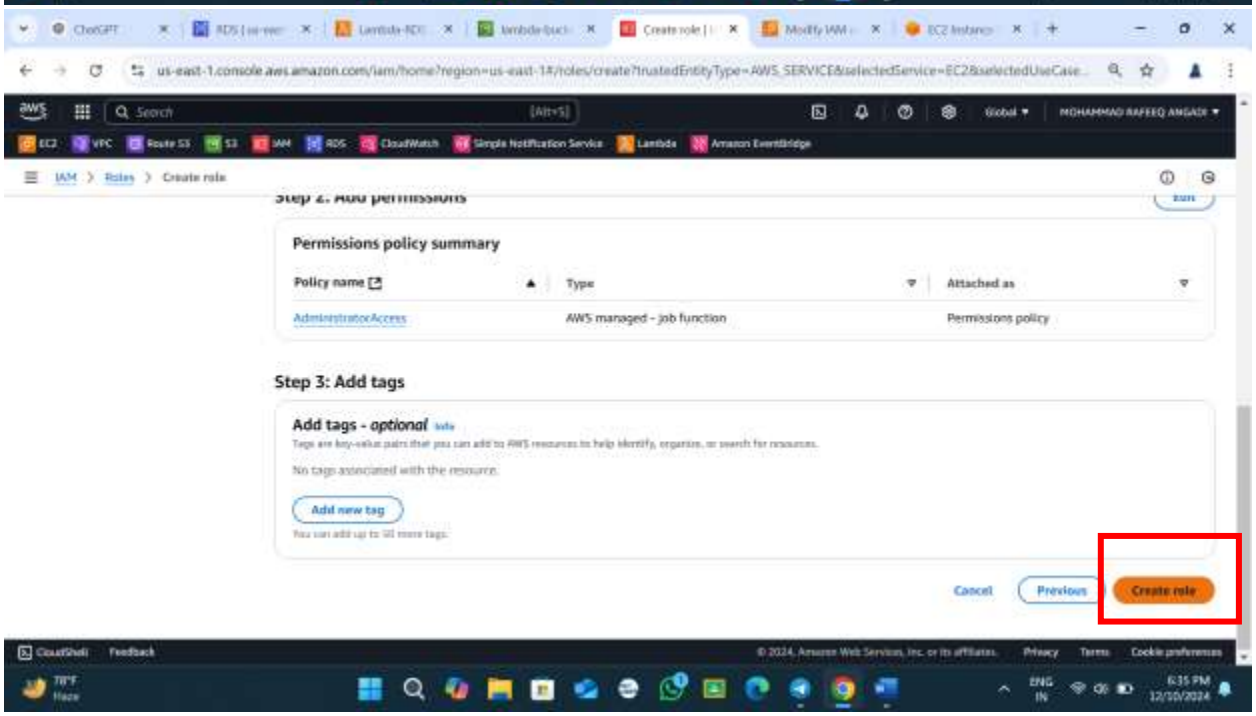

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create
Search
IAM > Roles > Create role
Select trusted entity
Add permissions
Name, review, and create
Select trusted entity info
Trusted entity type
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create
Search
IAM > Roles > Create role
EC2
Choose a use case for the specified service:
Use case
EC2
Allows EC2 instances to call AWS services on your behalf.
EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
EC2 - Spot Fleet
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.
EC2 - Scheduled Instances
Allows EC2 Scheduled Instances to manage instances on your behalf.
Cancel
Next
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Cookie preferences

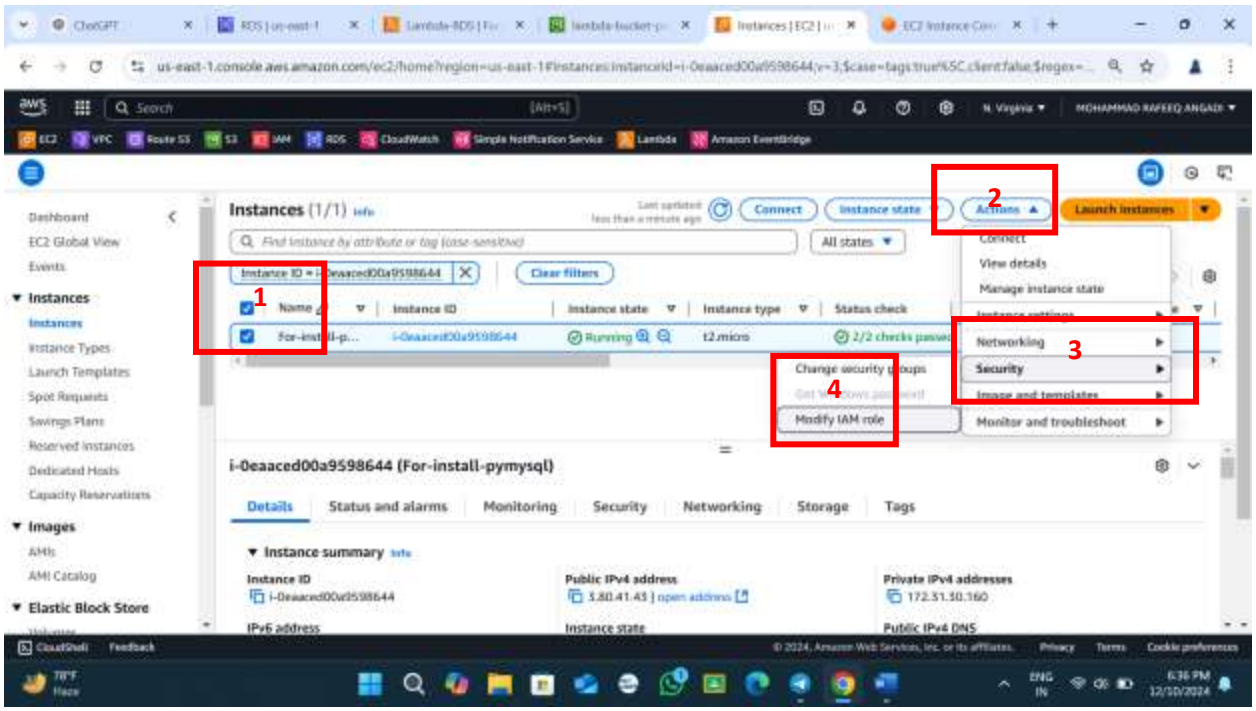

Add permissions
Permissions policies (1/1023)
Choose one or more policies to attach to your new role.
Filter by Type
Search
All types
Policy name
Type
Description
AdministratorAccess
AWS managed - job function
Provides full access to AWS services an...
AdministratorAccess-Amplify
AWS managed
Grants account administrative permissi...
AIOpsAssistantPolicy
AWS managed
Provides ReadOnly permissions require...
AIOpsConsoleAdminPolicy
AWS managed
Grants full access to Amazon AI Opera...
AIOpsOperatorAccess
AWS managed
Grants access to the Amazon AI Opera...

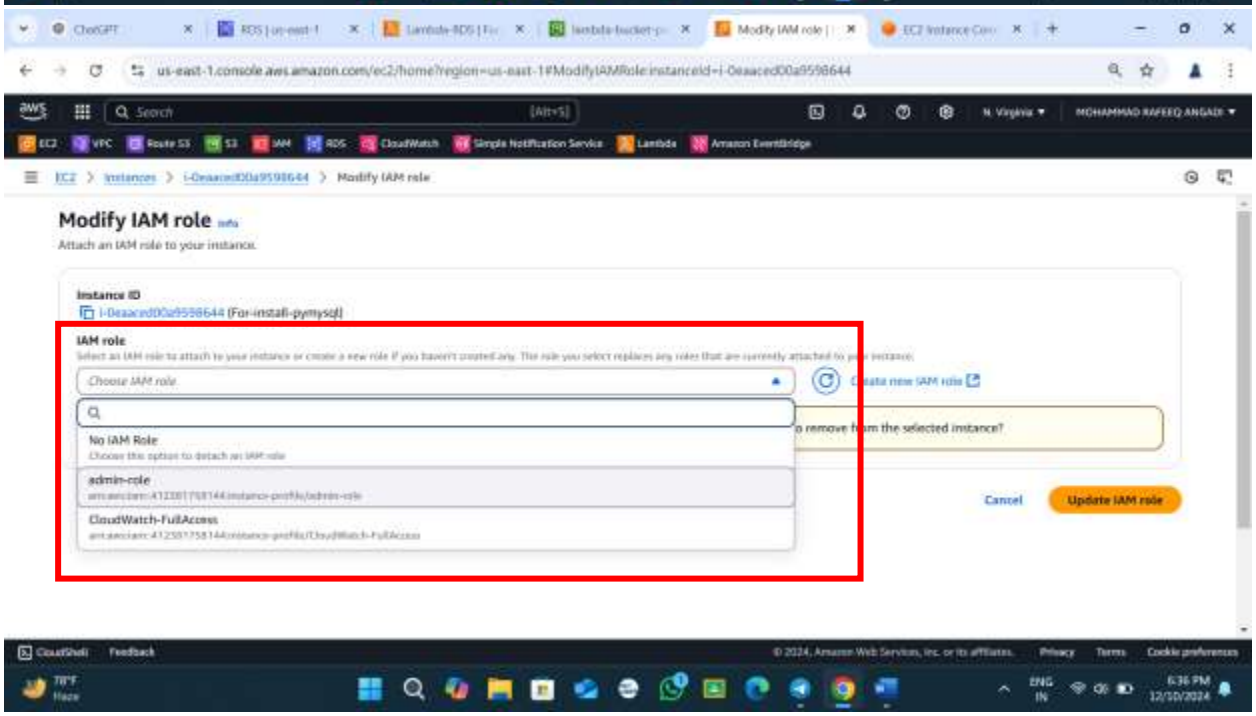

AlexaForBusinessPolyDelegatedAcce...
AWS managed
Provide access to Poly AVS devices
AlexaForBusinessReadOnlyAccess
AWS managed
Provide read only access to AlexaForBu...
Amazon-EventBridge-Scheduler-Execut...
Customer managed
AmazonAPIGatewayAdministrator
AWS managed
Provides full access to create/edit/dele...
AmazonAPIGatewayInvokeFullAccess
AWS managed
Provides full access to invoke APIs in A...
AmazonAPIGatewayPushToCloudWa...
AWS managed
Allows API Gateway to push logs to us...
Set permissions boundary - optional
Cancel
Previous
Next

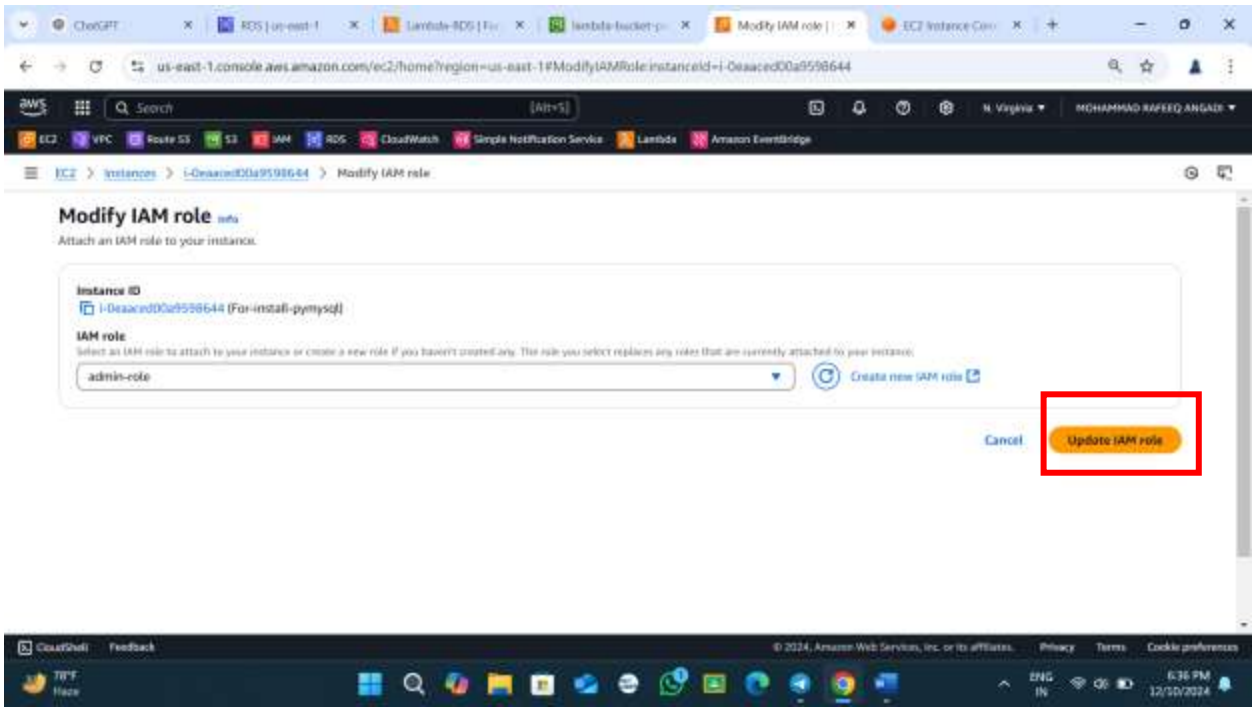




And attach to ec2 instance


Instances (1/1)
Connect
Instance state
Actions
Launch instances
Clear filters
All states
Name
Instance ID
Instance state
Instance type
Status check
t2.micro
2/2 checks passed
Connect
View details
Manage instance state
Networking
Security
Image and templates
Monitor and troubleshoot
Change security groups
Modify IAM role
1
2
3
4
i-0eaaced00a9598644 (For-install-pymysql)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary
Instance ID
Public IPv4 address
Private IPv4 addresses
IPv6 address
Instance state
Public IPv4 DNS

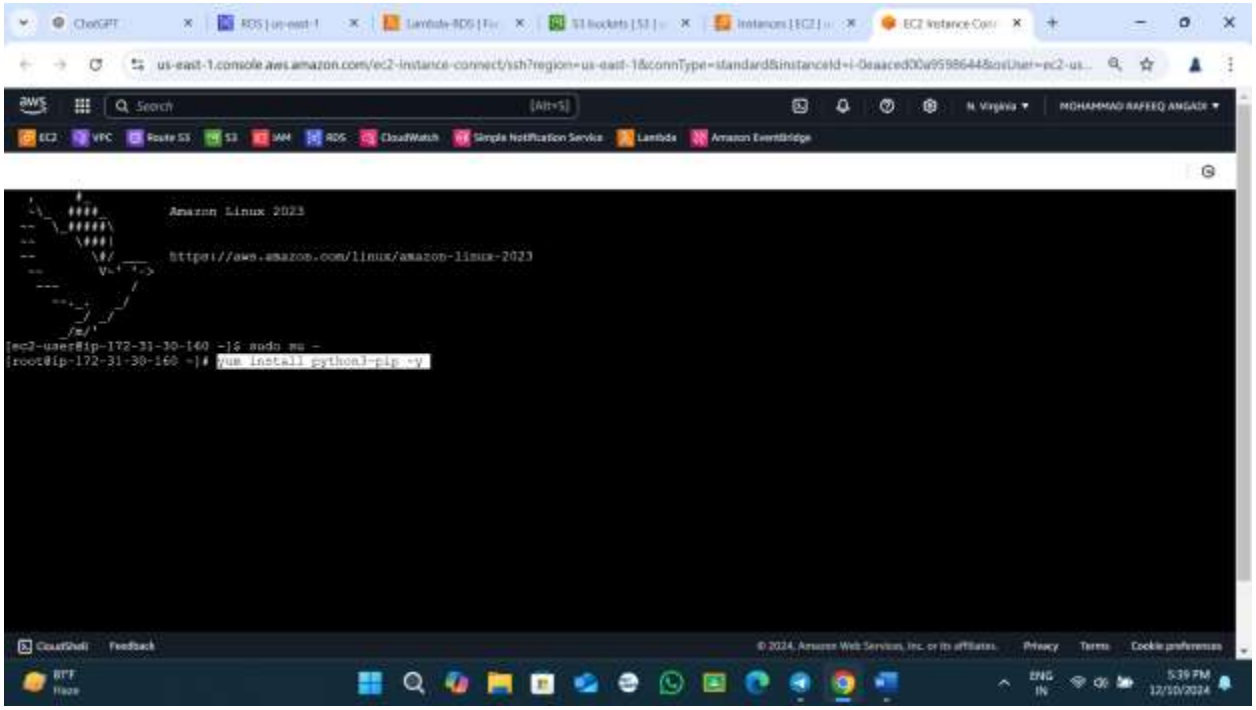

Modify IAM role
Attach an IAM role to your instance.
Instance ID
IAM role
Choose IAM role
No IAM Role
admin-role
CloudWatch-FullAccess
Cancel
Update IAM role



And run this command

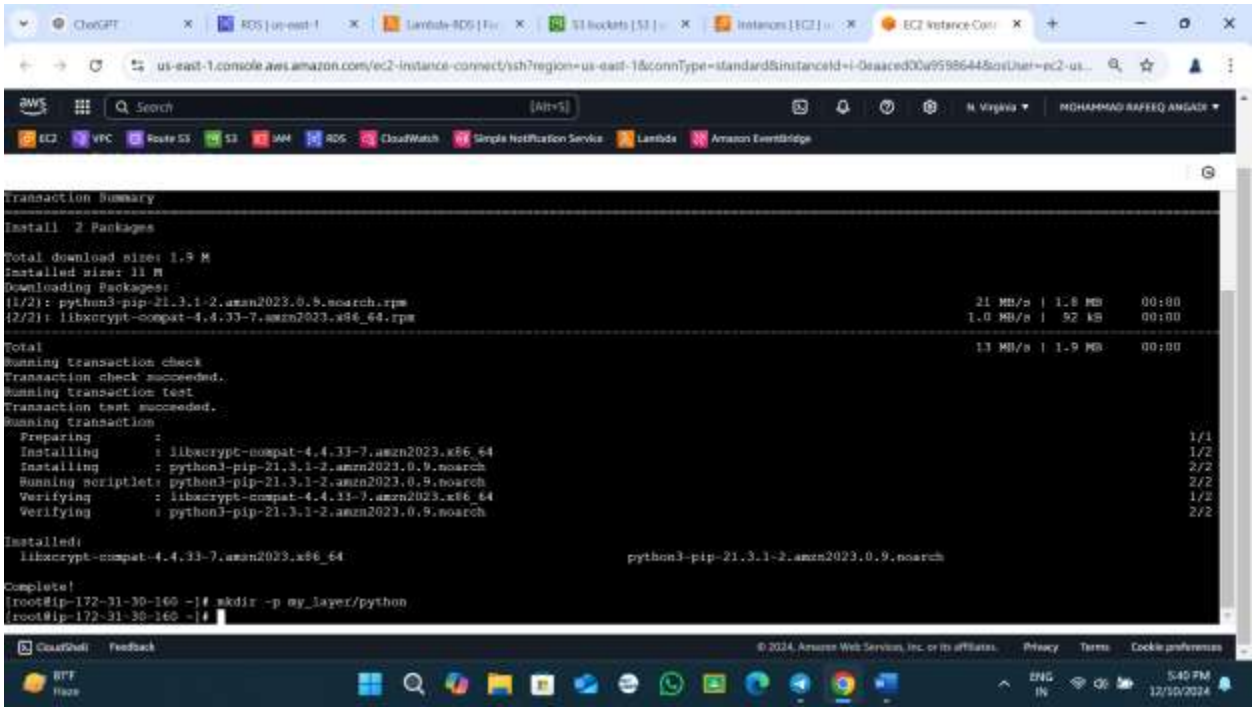
sudo su –

yum install python3-pip -y



And next run this command

mkdir -p my_layer/python



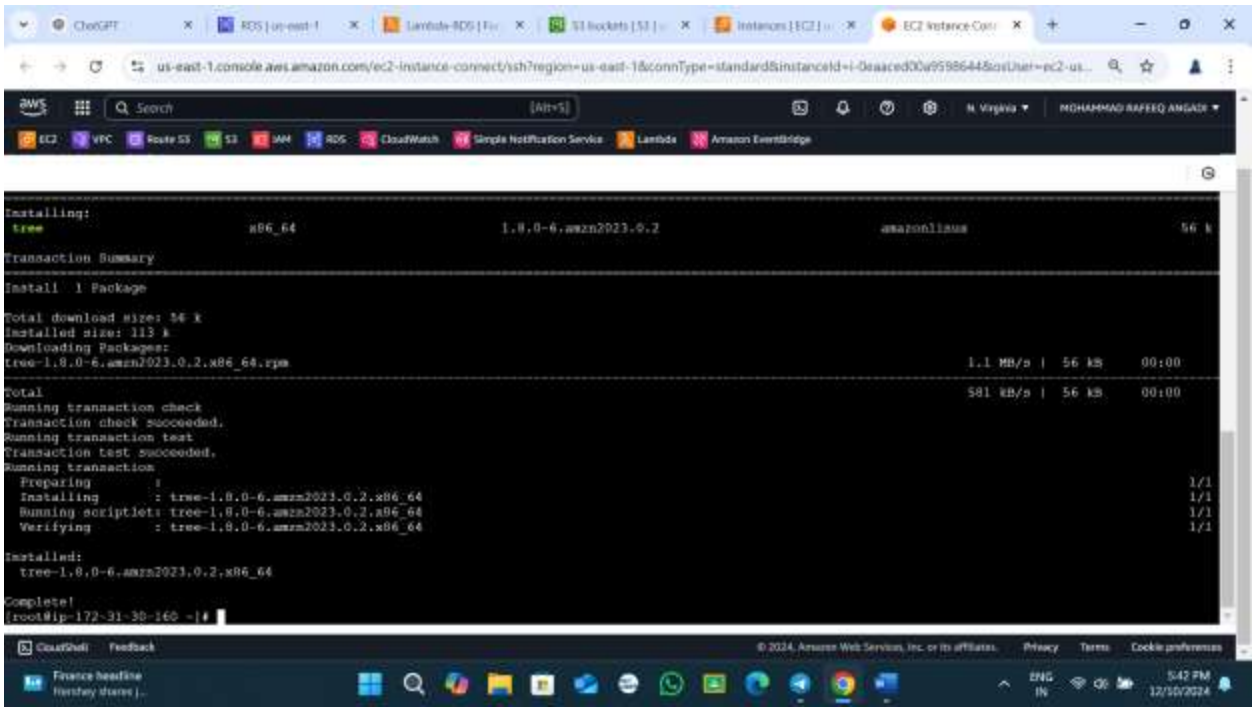
And run this command

pip install pymysql -t my_layer/python

```
[root@ip-172-31-10-41 ~]# mkdir -p my_layer/python
[root@ip-172-31-10-41 ~]# pip install pymysql -t my_layer/python
Collecting pymysql
  Downloading PyMySQL-1.1.1-py3-none-any.whl (44 kB)
     |████████████████████████████████| 44 kB 3.6 MB/s
Installing collected packages: pymysql
Successfully installed pymysql-1.1.1
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behavio
commended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
[root@ip-172-31-10-41 ~]#
```

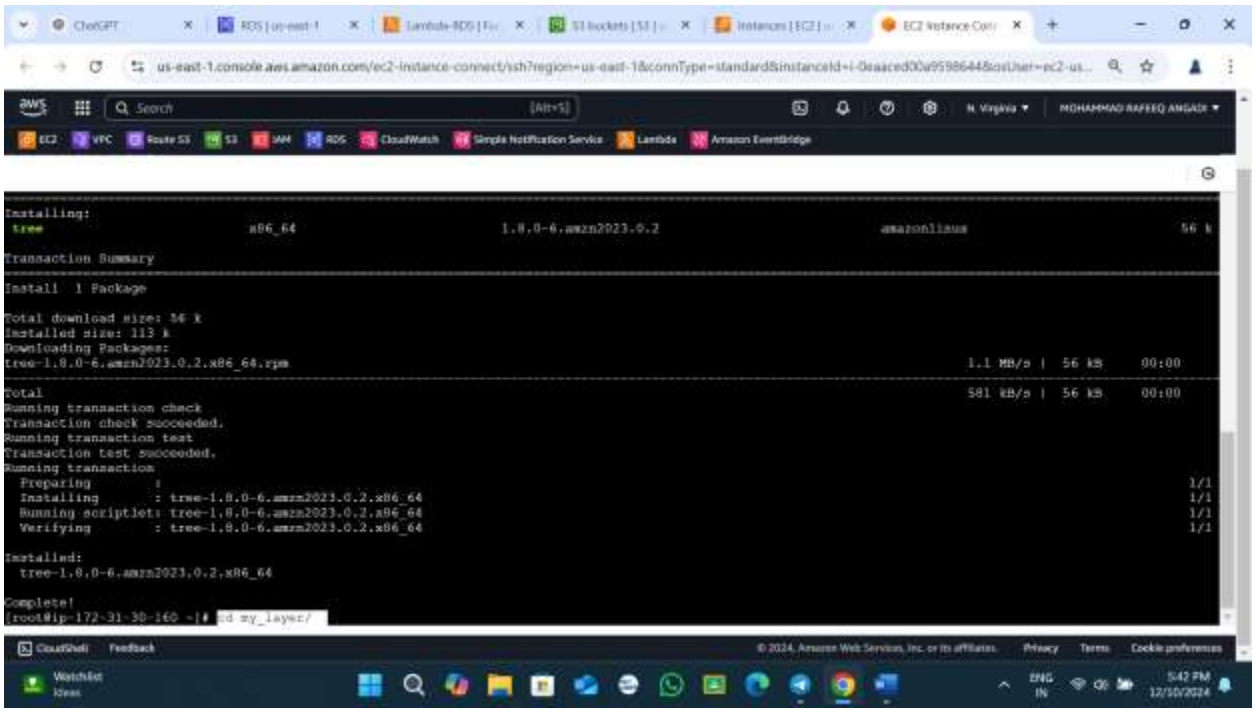
Run this command

yum install tree -y



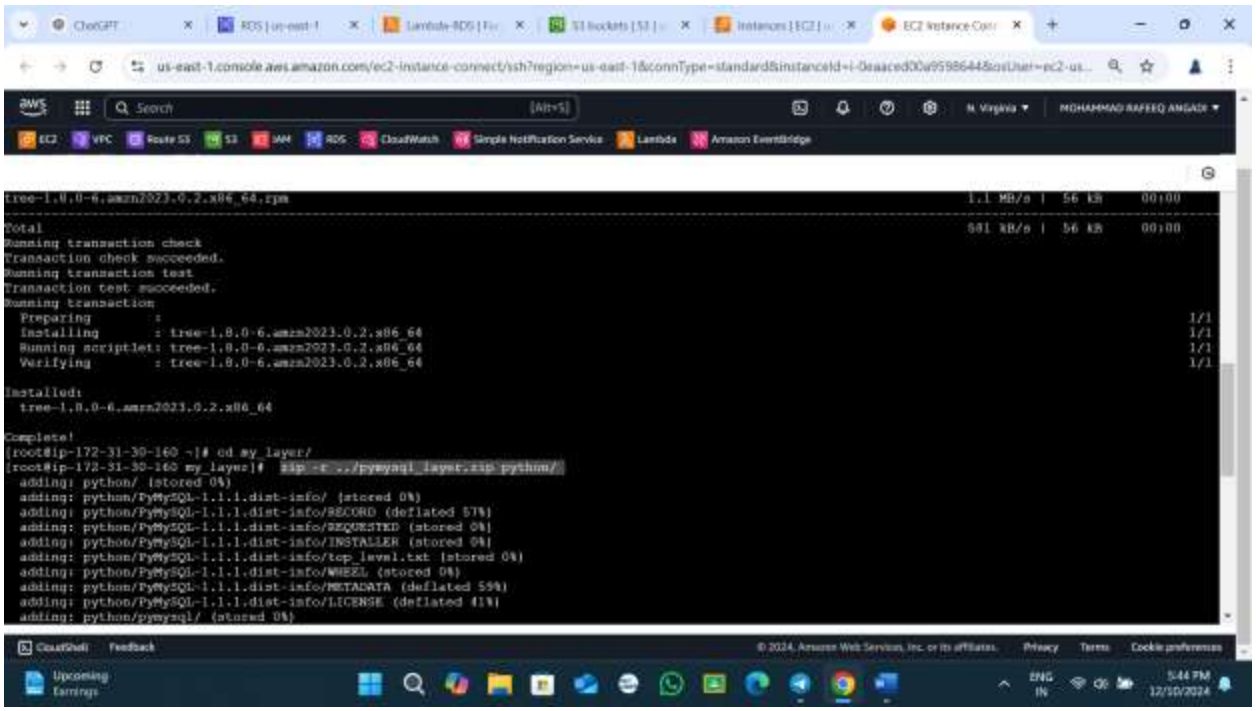
and run this command

cd my_layer/



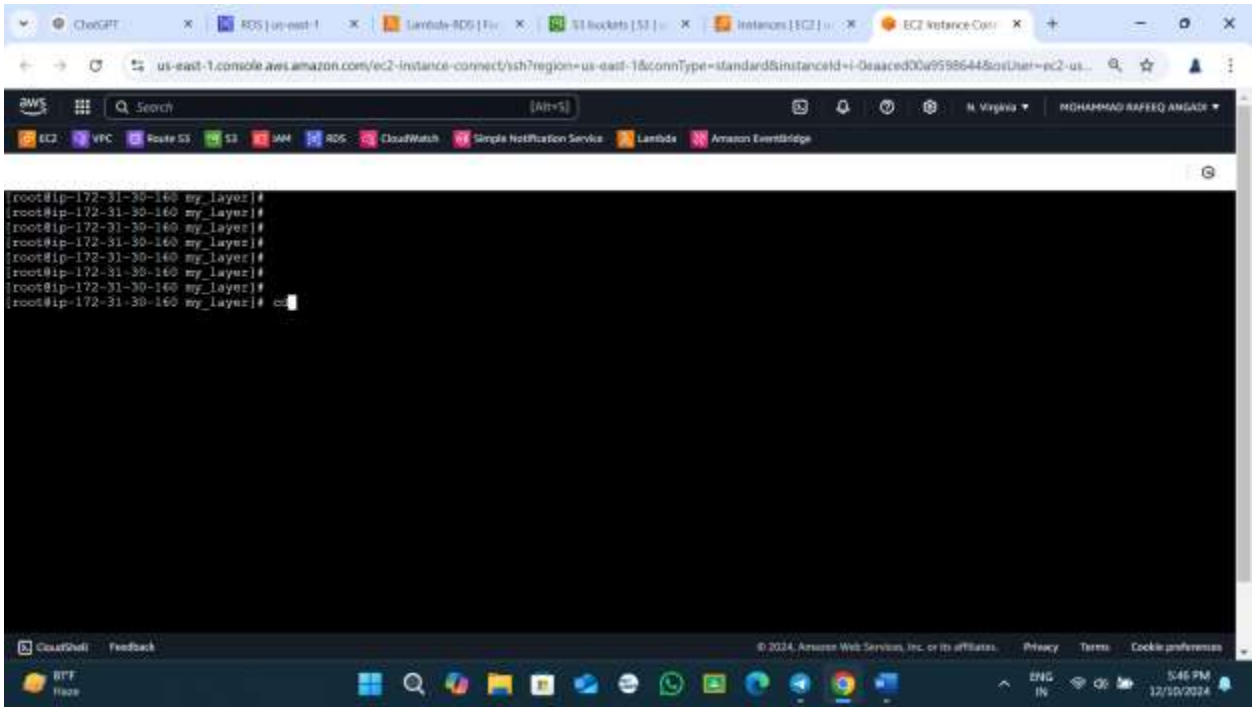
run this commad

zip -r ../pymysql_layer.zip python/



And next Come back run this command one by one

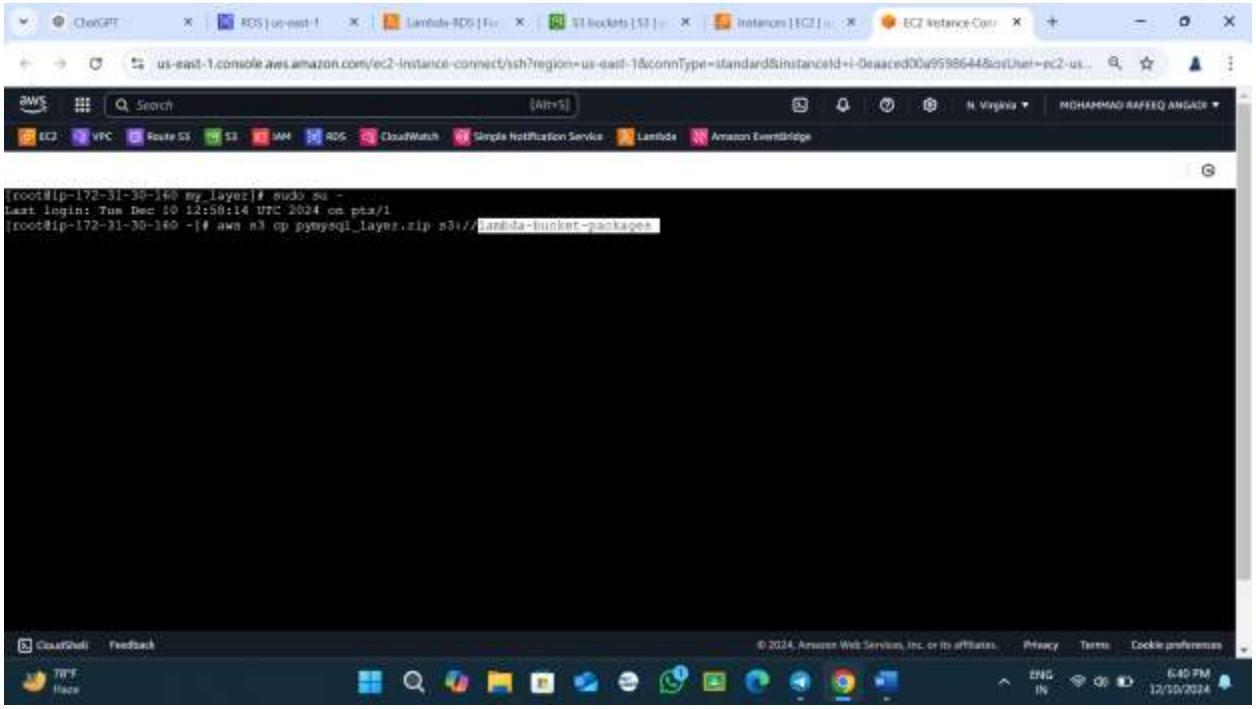
cd



Run this below command for cp the pymysql package into s3 bucket

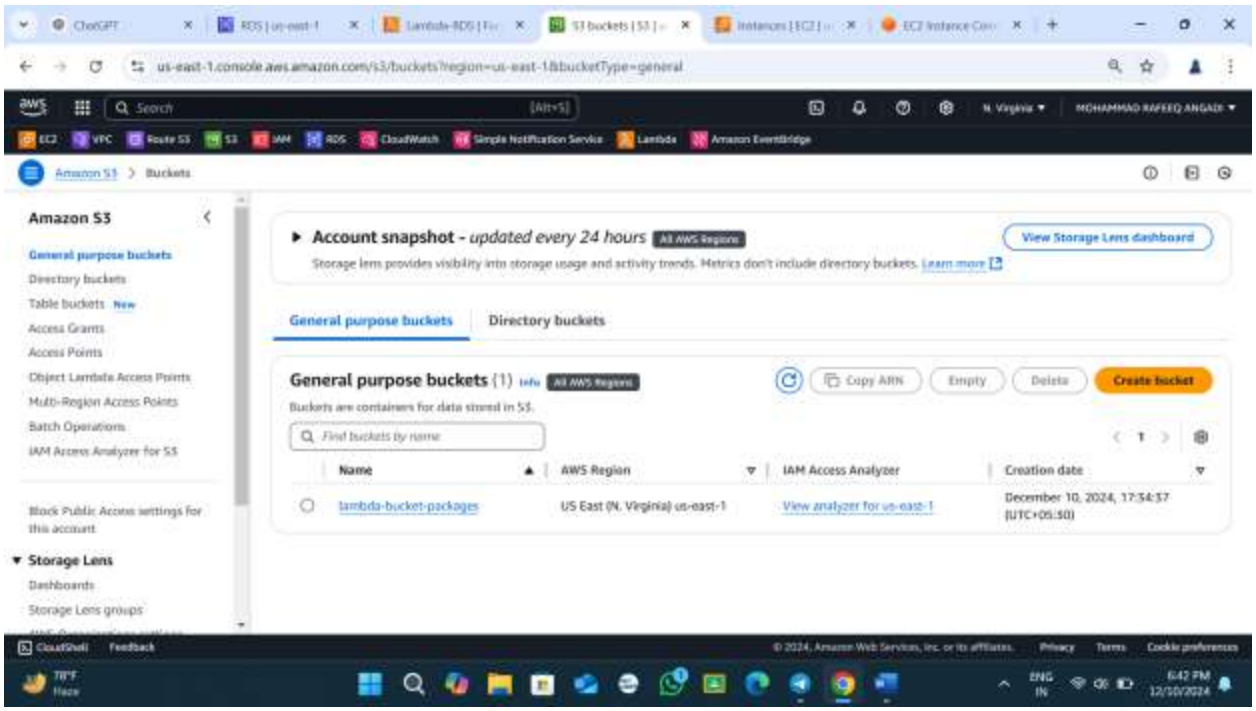
Copy the s3 bucket name and past in below command

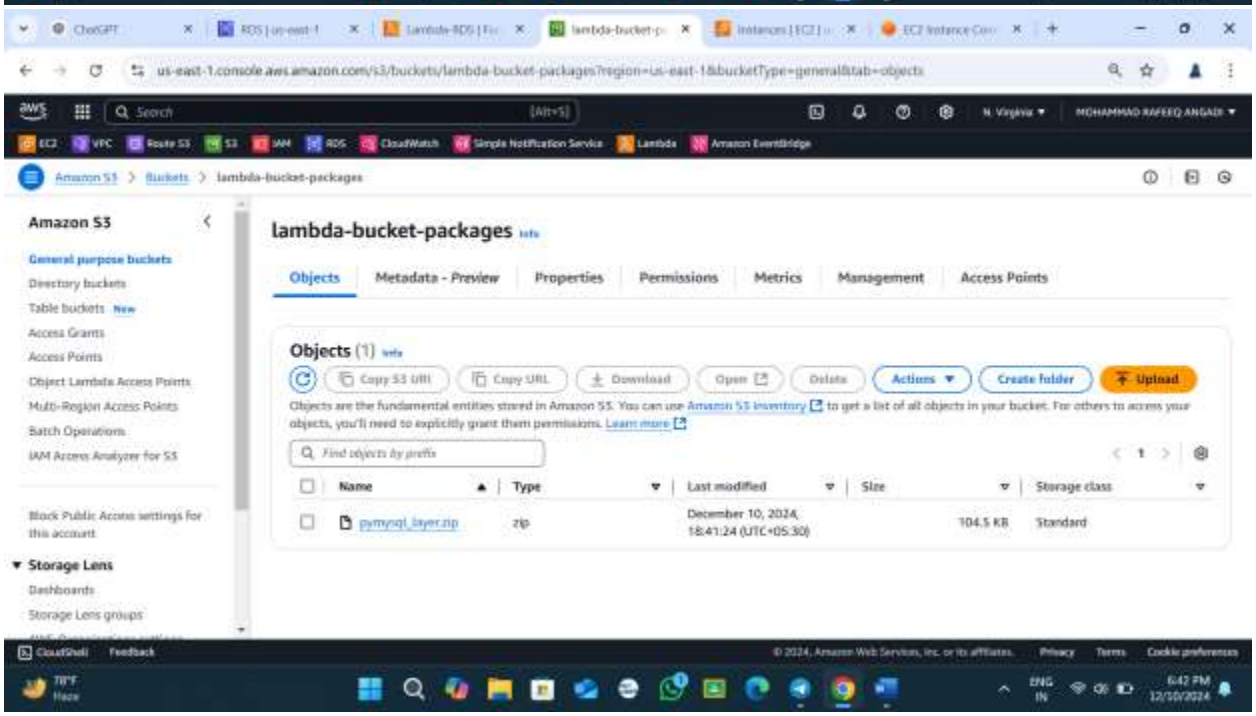
aws s3 cp pymysql_layer.zip s3://your-bucket-name



See uploaded into s3

Go to s3 bucket see package is copied or not

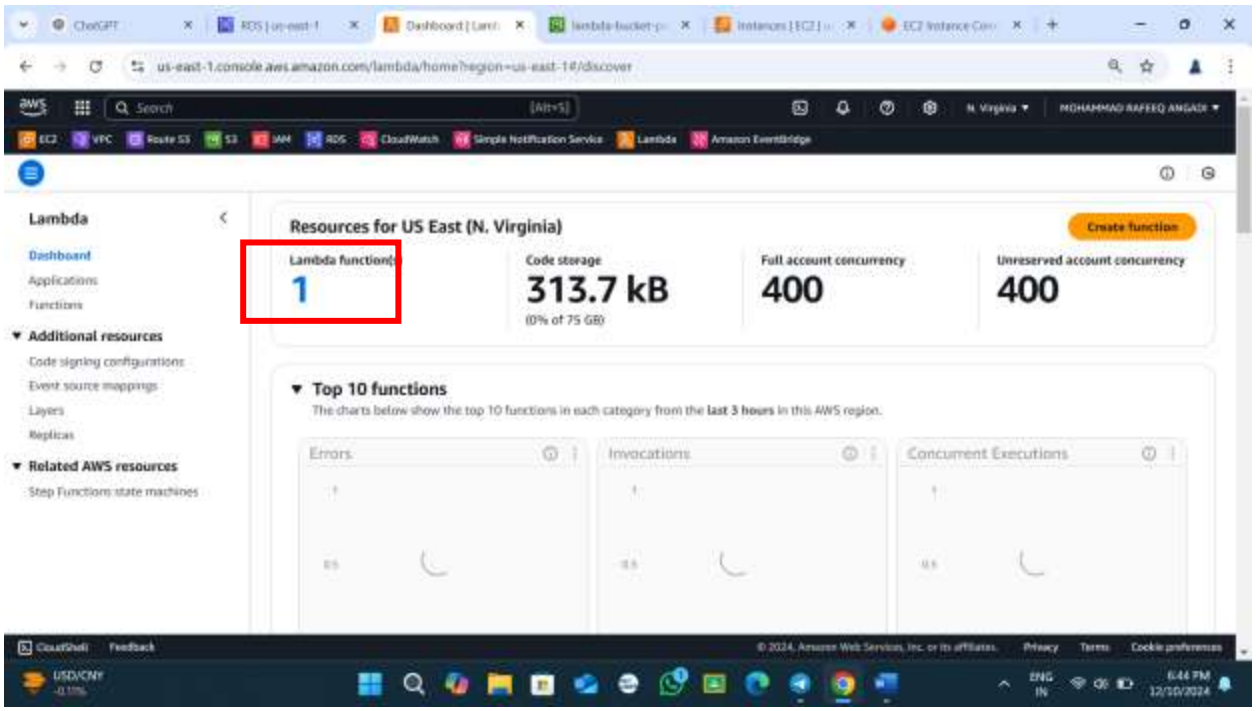


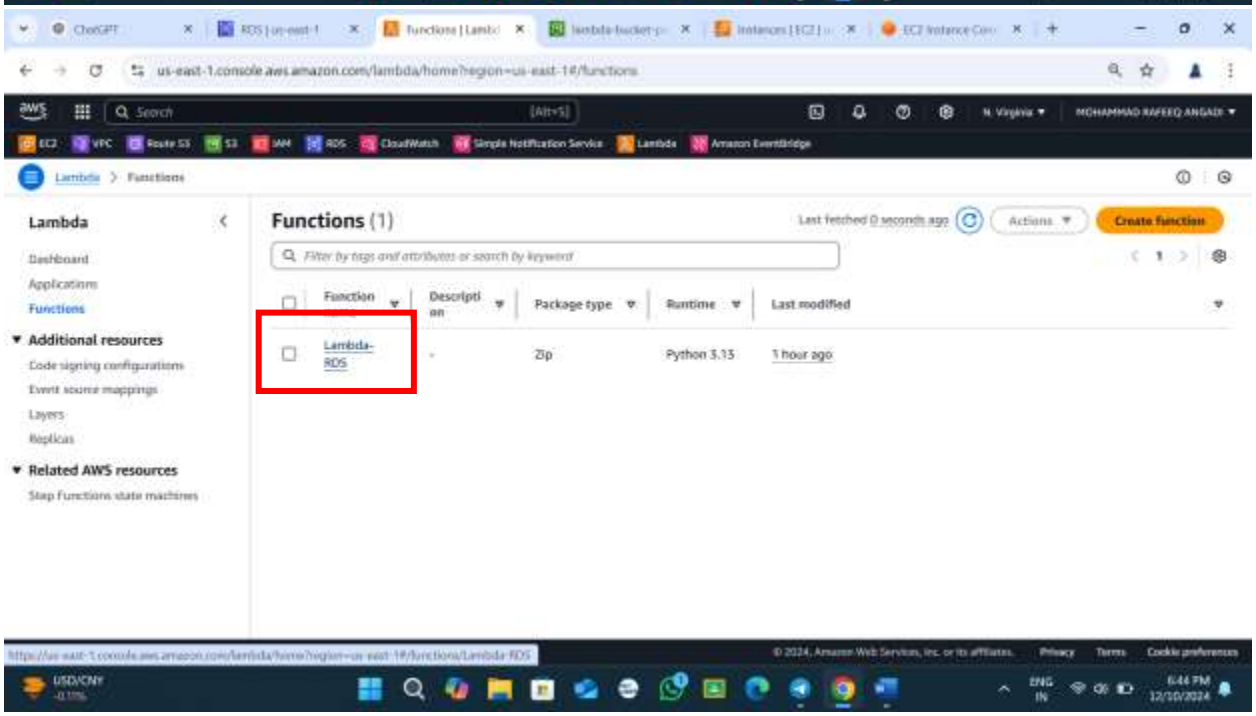


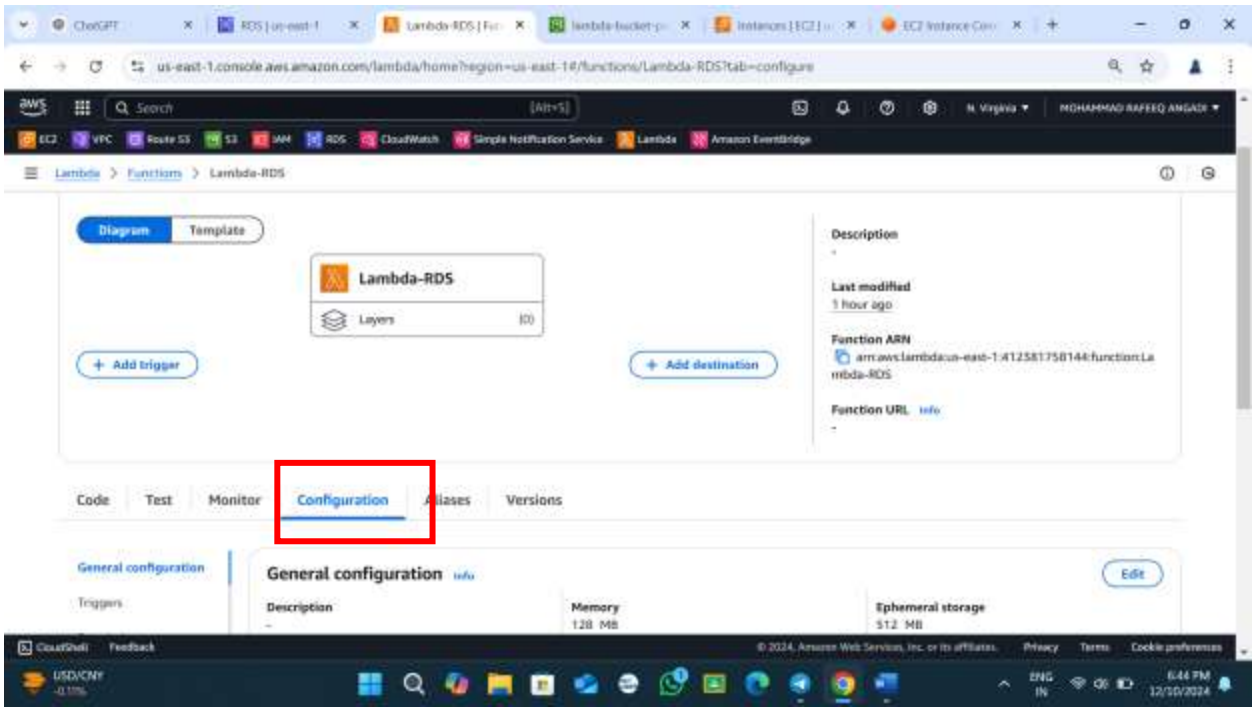
6. Enable VPC Access in Lambda

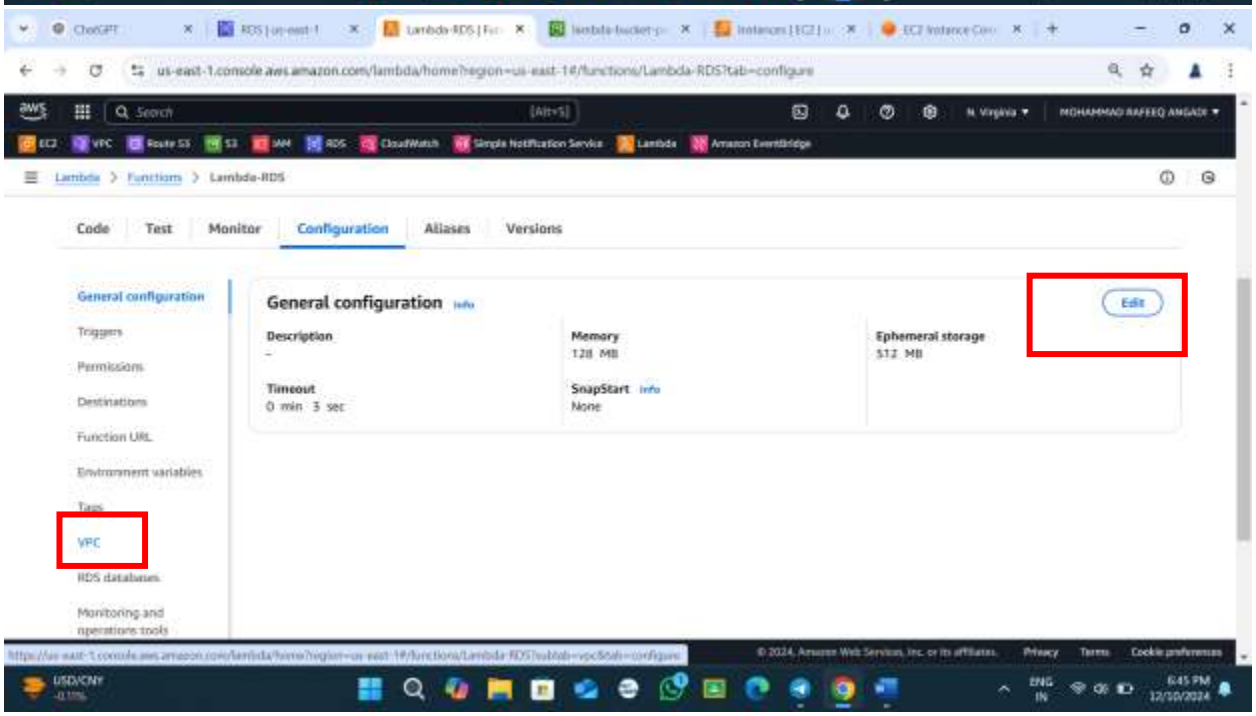
If your RDS is in a private subnet:

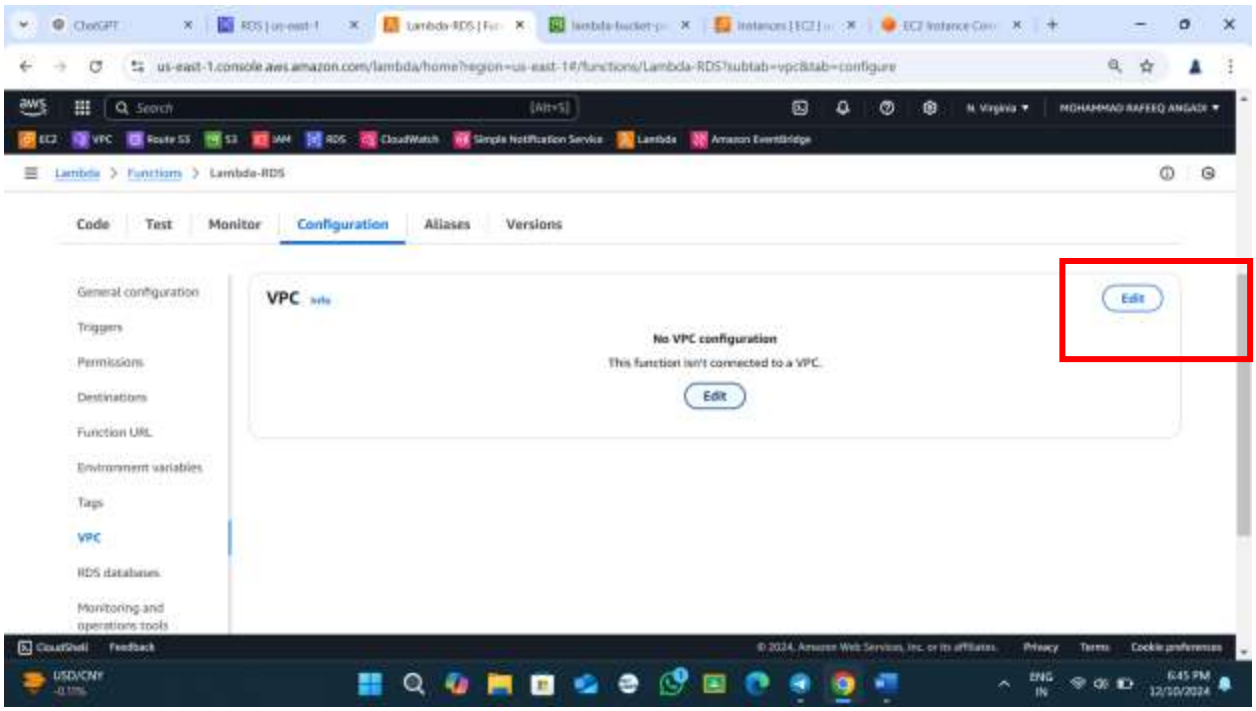
- Attach the Lambda function to the same VPC as the RDS instance.
- Configure the Lambda function's VPC settings to include subnets and security groups.

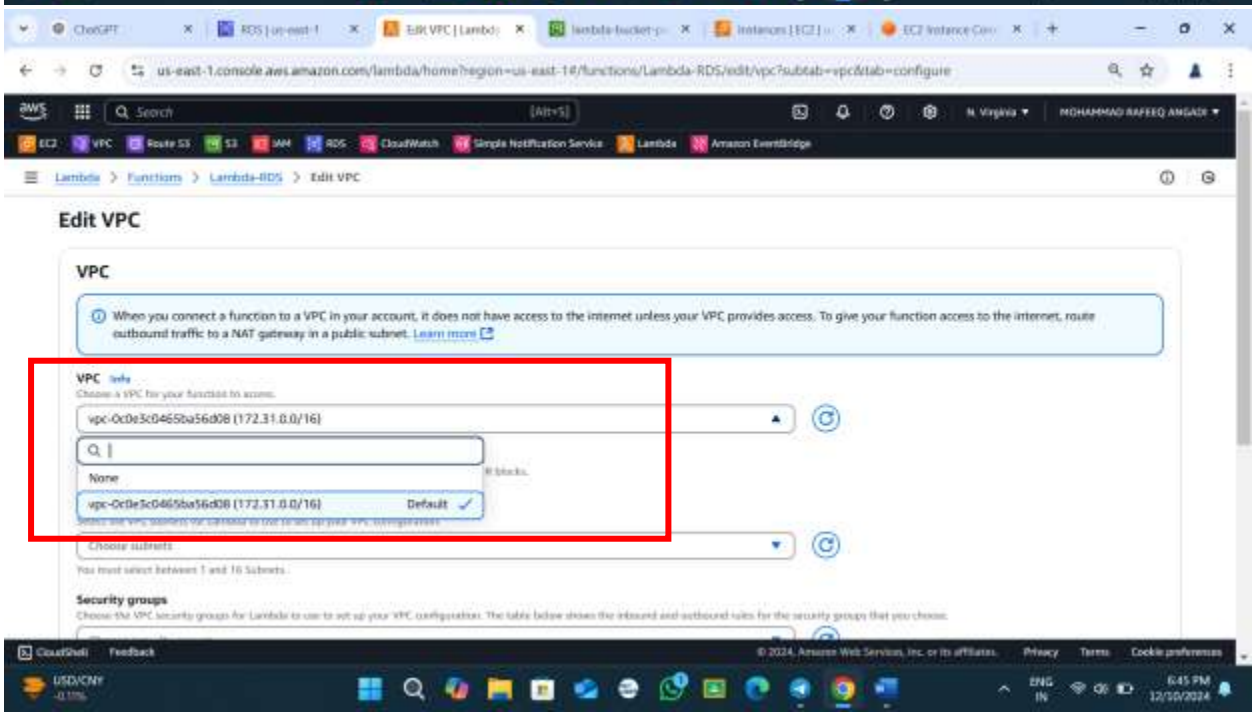

us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/discover
Lambda
Dashboard
Applications
Functions
Additional resources
Code signing configurations
Event source mappings
Layers
Replicas
Related AWS resources
Step Functions state machines
Resources for US East (N. Virginia)
Create function
Lambda function(s)
1
Code storage
313.7 kB
(0% of 75 GB)
Full account concurrency
400
Unreserved account concurrency
400
Top 10 functions
The charts below show the top 10 functions in each category from the last 3 hours in this AWS region.
Errors
Invocations
Concurrent Executions

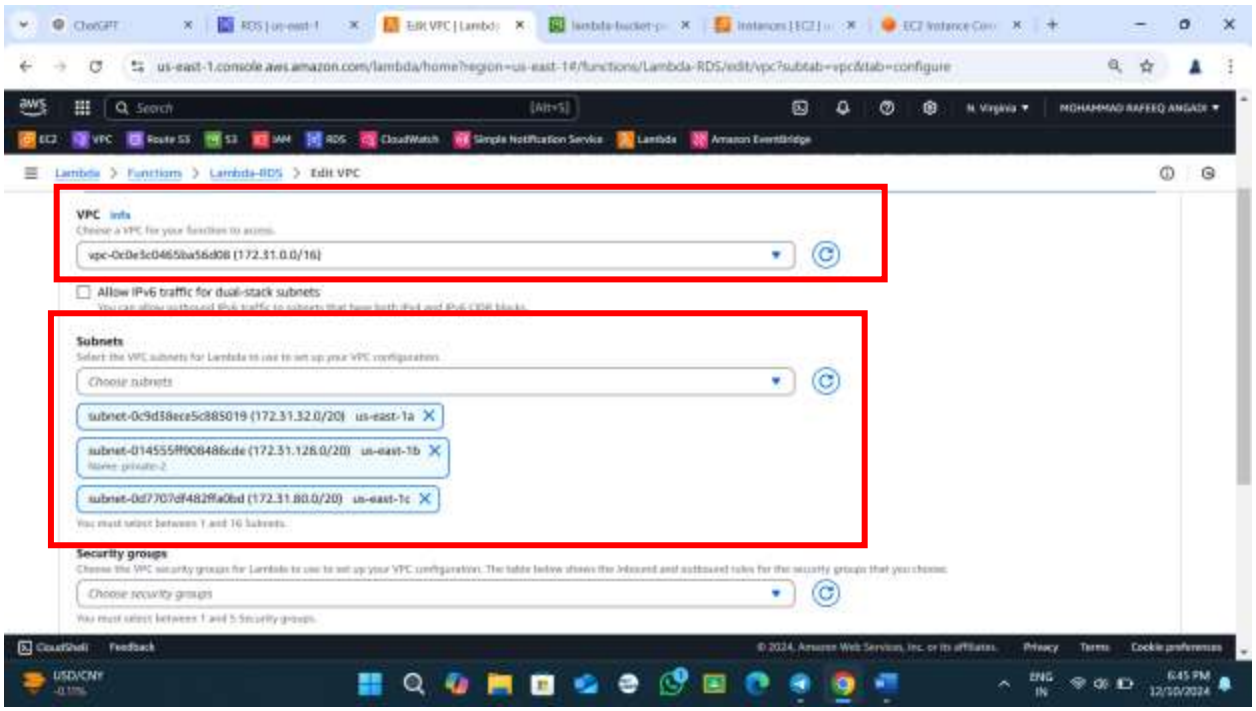

us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions
Lambda > Functions
Lambda
Dashboard
Applications
Functions
Additional resources
Code signing configurations
Event source mappings
Layers
Replicas
Related AWS resources
Step Functions state machines
Functions (1)
Last fetched 0 seconds ago
Actions
Create function
Filter by tags and attributes or search by keyword
Function
Description
Package type
Runtime
Last modified
Lambda-RDS
Zip
Python 3.13
1 hour ago

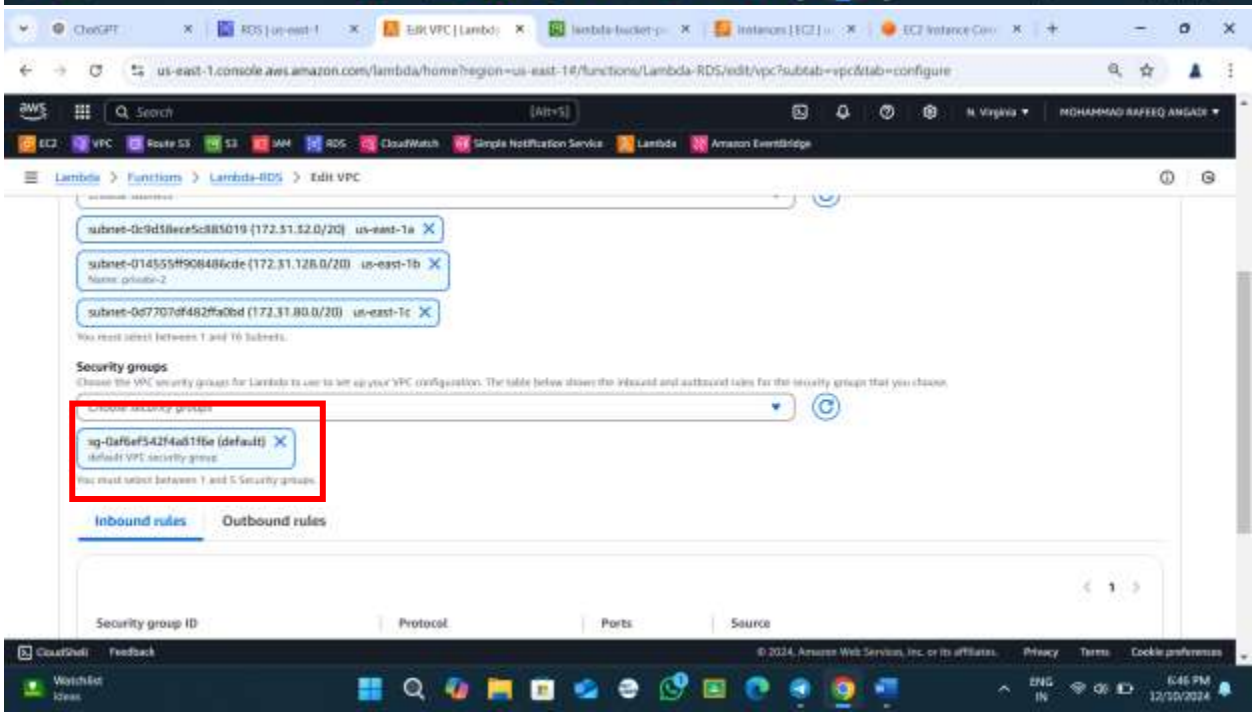

us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/Lambda-RDS?tab=configure
Lambda > Functions > Lambda-RDS
Diagram
Template
Lambda-RDS
Layers
+ Add trigger
+ Add destination
Description
Last modified
1 hour ago
Function ARN
Function URL
Code
Test
Monitor
Configuration
Aliases
Versions
General configuration
Triggers
General configuration
Edit
Description
Memory
128 MB
Ephemeral storage
512 MB

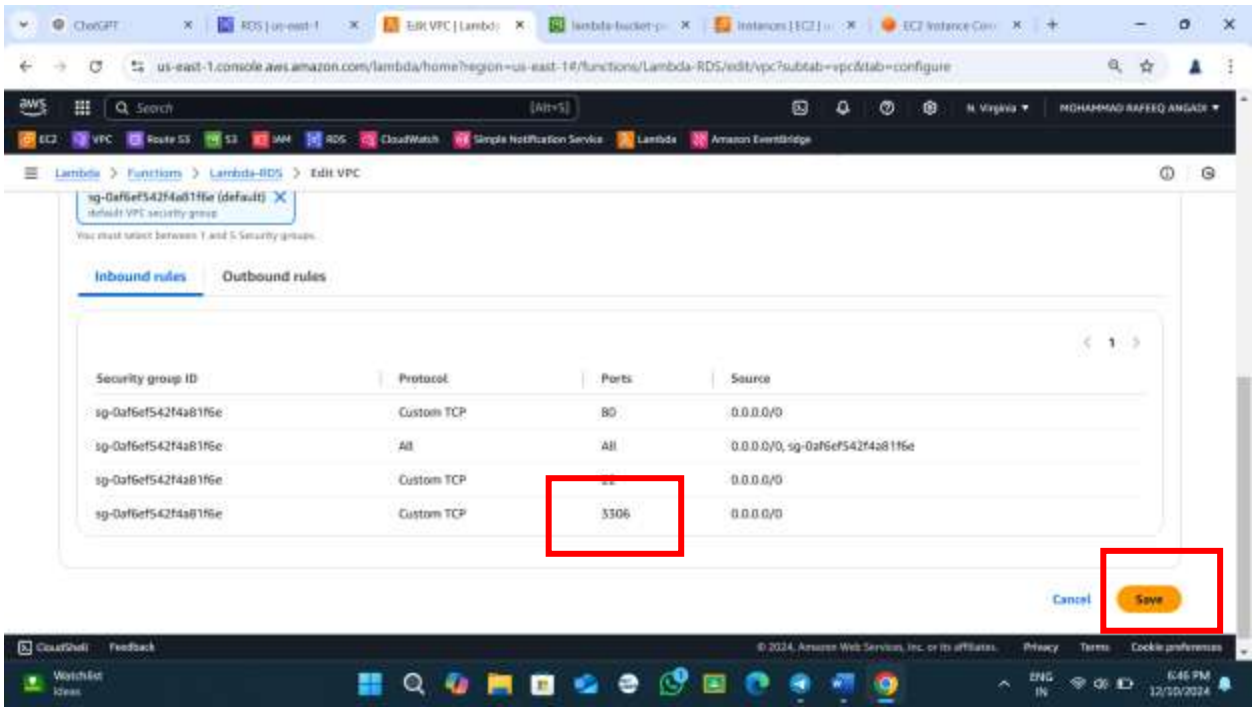

us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/Lambda-RDS?tab=configure
Lambda > Functions > Lambda-RDS
Code
Test
Monitor
Configuration
Aliases
Versions
General configuration
Triggers
Permissions
Destinations
Function URL
Environment variables
Tags
VPC
RDS databases
Monitoring and operations tools
General configuration
Edit
Description
Memory
128 MB
Ephemeral storage
512 MB
Timeout
0 min 3 sec
SnapStart
None


us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/Lambda-RDS?subtab=vpc&tab=configure
Lambda > Functions > Lambda-RDS
Code
Test
Monitor
Configuration
Aliases
Versions
General configuration
Triggers
Permissions
Destinations
Function URL
Environment variables
Tags
VPC
RDS databases
Monitoring and operations tools
VPC
Edit
No VPC configuration
This function isn't connected to a VPC.
Edit

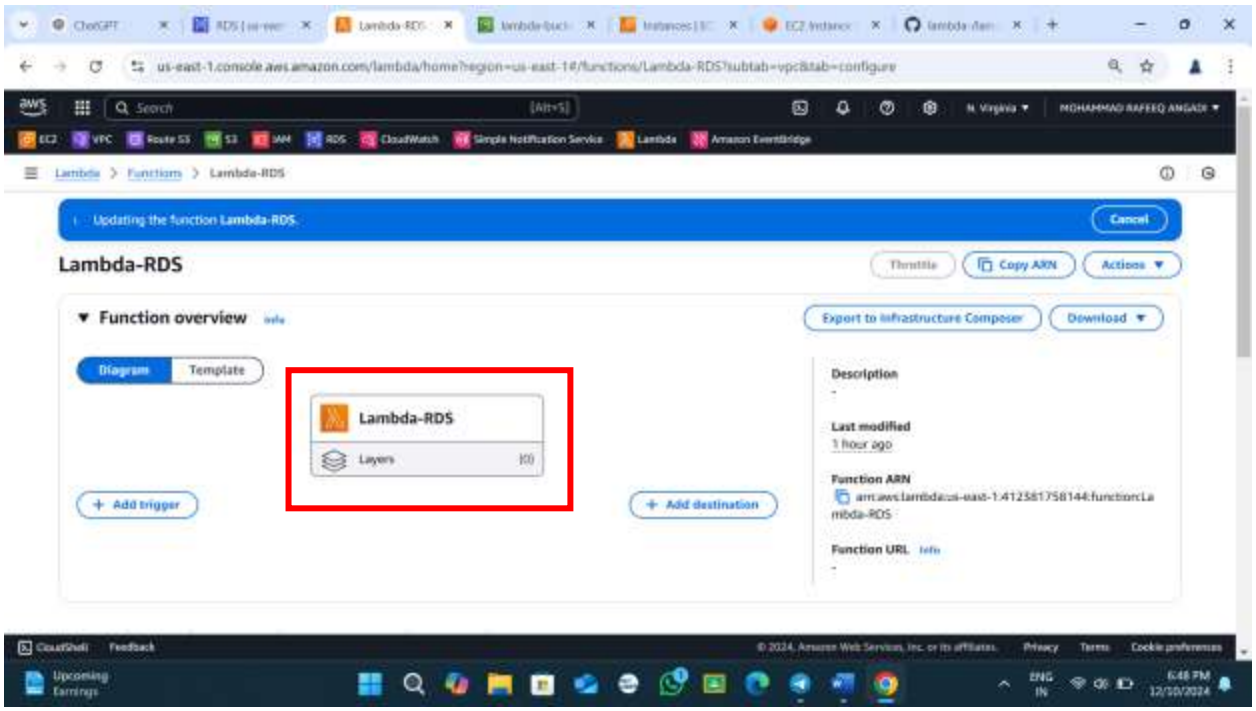

us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/Lambda-RDS/edit/vpc?subtab=vpc&tab=configure
Lambda > Functions > Lambda-RDS > Edit VPC
Edit VPC
VPC
When you connect a function to a VPC in your account, it does not have access to the internet unless your VPC provides access. To give your function access to the internet, route outbound traffic to a NAT gateway in a public subnet. Learn more
VPC
vpc-0c0e3c0465ba56d08 (172.31.0.0/16)
None
vpc-0c0e3c0465ba56d08 (172.31.0.0/16) Default
Choose subnets
Security groups

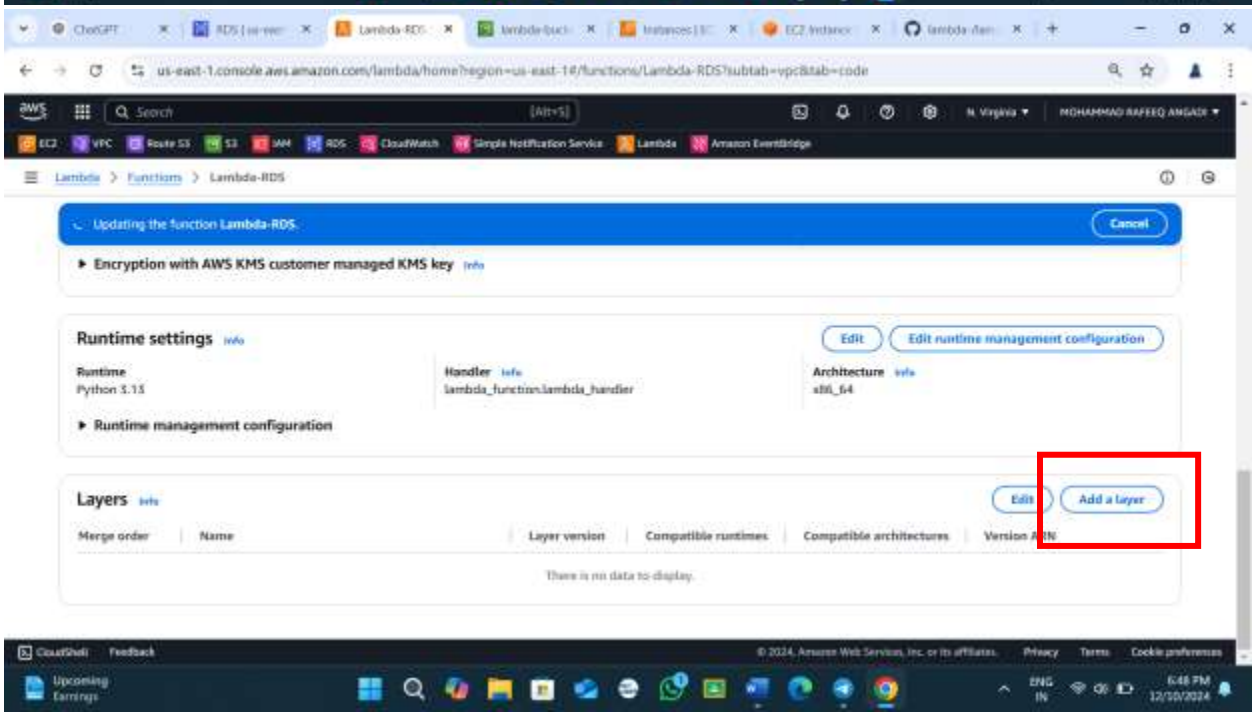

us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/Lambda-RDS/edit/vpc?subtab=vpc&tab=configure
Lambda > Functions > Lambda-RDS > Edit VPC
VPC info
vpc-0c0e3c0465ba56d08 (172.31.0.0/16)
Allow IPv6 traffic for dual-stack subnets
Subnets
Choose subnets
subnet-0c9d38ece5c885019 (172.31.32.0/20) us-east-1a
subnet-014555ff908486cde (172.31.128.0/20) us-east-1b
subnet-0d7707df482ffa0bd (172.31.80.0/20) us-east-1c
Security groups
Choose security groups

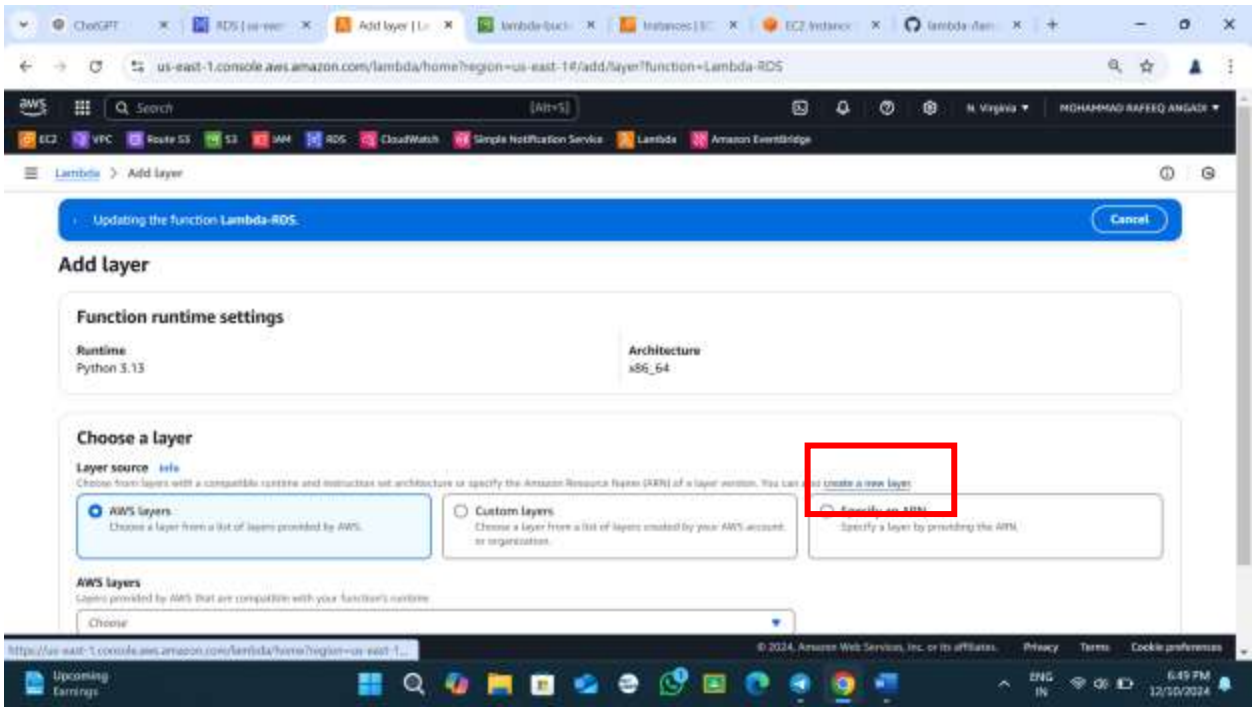

us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/Lambda-RDS/edit/vpc?subtab=vpc&tab=configure
Lambda > Functions > Lambda-RDS > Edit VPC
subnet-0c9d38ece5c885019 (172.31.32.0/20) us-east-1a
subnet-014555ff908486cde (172.31.128.0/20) us-east-1b
subnet-0d7707df482ffa0bd (172.31.80.0/20) us-east-1c
Security groups
sg-0af6ef542f4a61f8e (default)
Inbound rules
Outbound rules
Security group ID
Protocol
Ports
Source

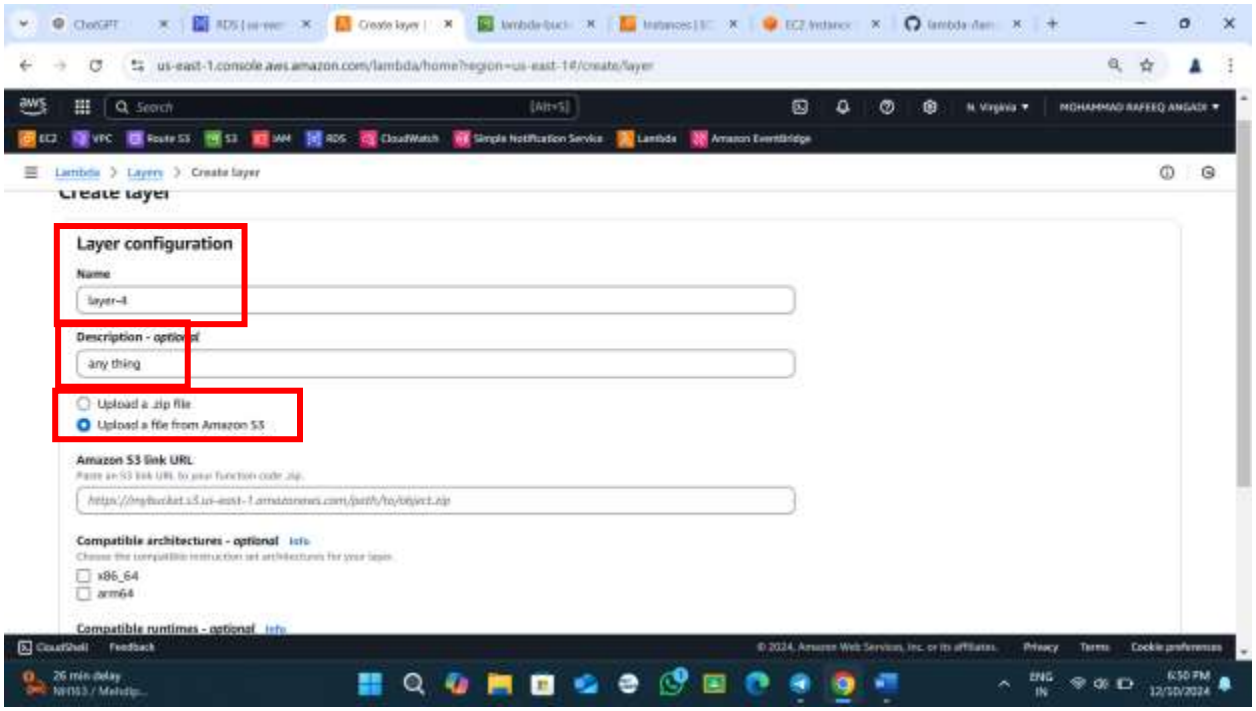


And add layer to the lambda like given below

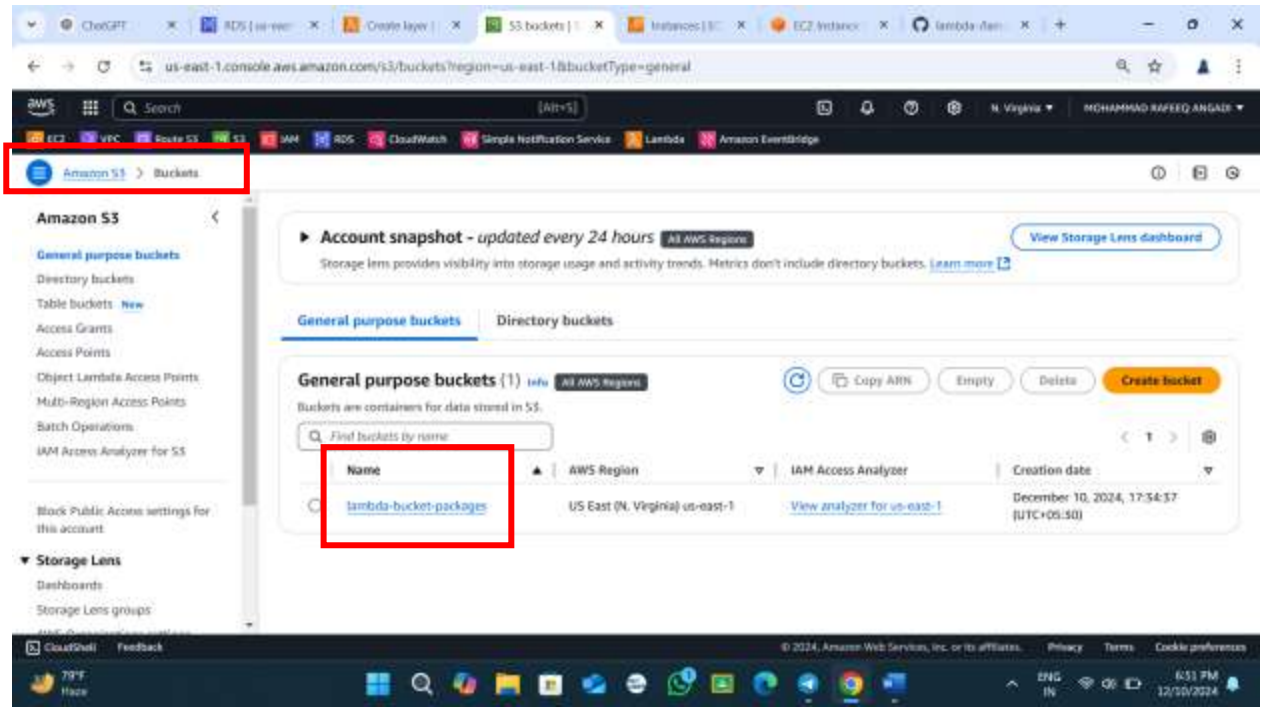

us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/Lambda-RDS?subtab=vpc&tab=configure
Lambda > Functions > Lambda-RDS
Updating the function Lambda-RDS.
Cancel
Lambda-RDS
Throttle
Copy ARN
Actions
Function overview
Export to Infrastructure Composer
Download
Diagram
Template
Lambda-RDS
Layers
(0)
+ Add trigger
+ Add destination
Description
-
Last modified
1 hour ago
Function ARN
arn:aws:lambda:us-east-1:412581758144:function:Lambda-RDS
Function URL
-
CloudShell
Feedback
Privacy
Terms
Cookie preferences

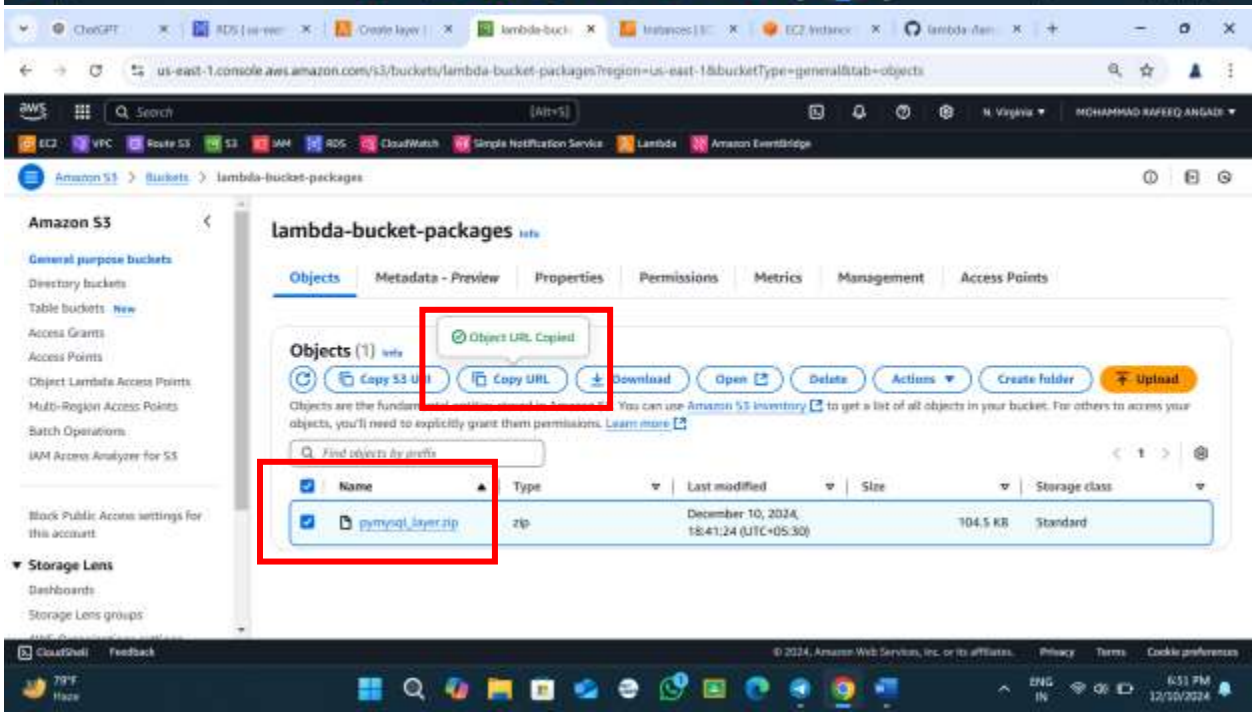

us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/Lambda-RDS?subtab=vpc&tab=code
Lambda > Functions > Lambda-RDS
Updating the function Lambda-RDS.
Cancel
Encryption with AWS KMS customer managed KMS key
Runtime settings
Edit
Edit runtime management configuration
Runtime
Python 3.13
Handler
lambda_function.lambda_handler
Architecture
x86_64
Runtime management configuration
Layers
Edit
Add a layer
Merge order
Name
Layer version
Compatible runtimes
Compatible architectures
Version ARN
There is no data to display.
CloudShell
Feedback
Privacy
Terms
Cookie preferences



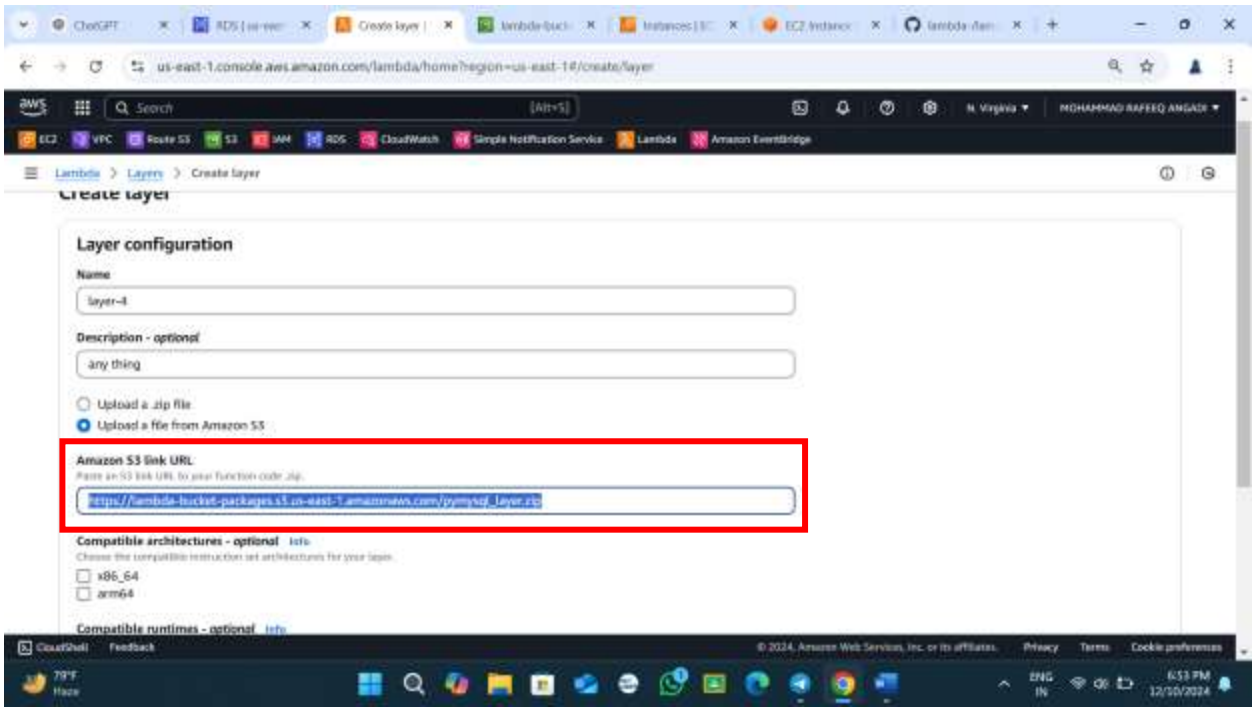


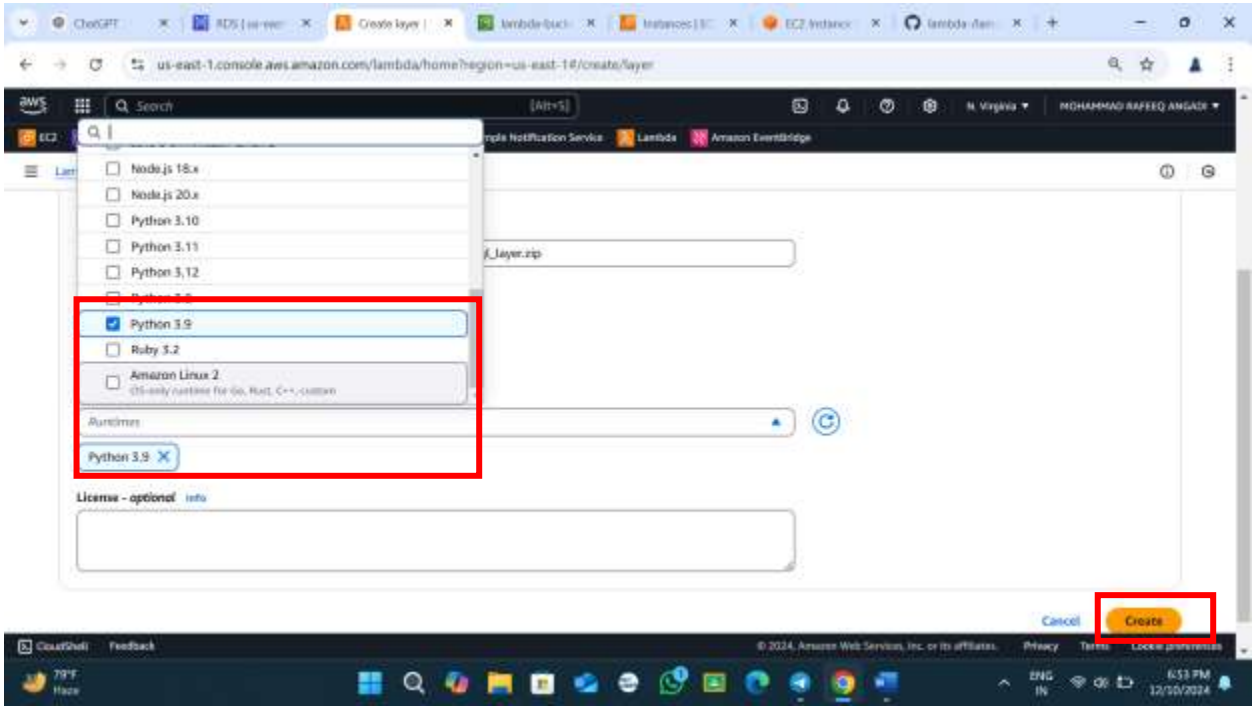
And go to s3 copy the s3 package url

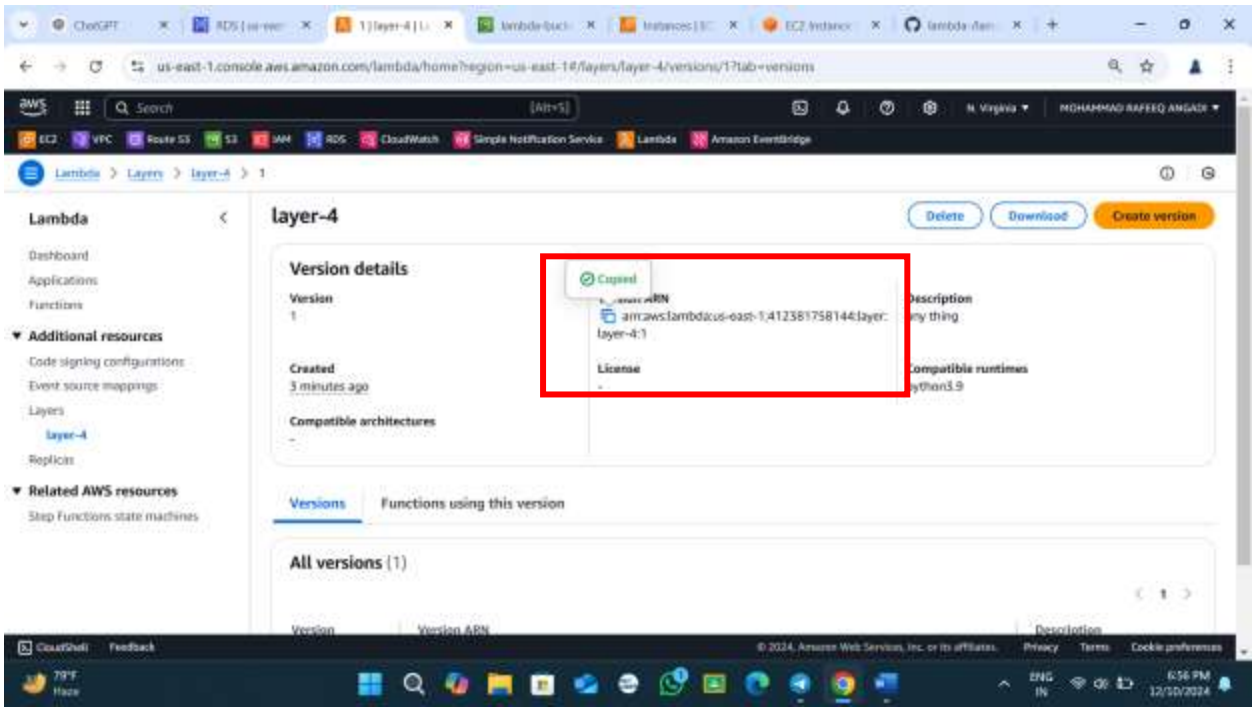




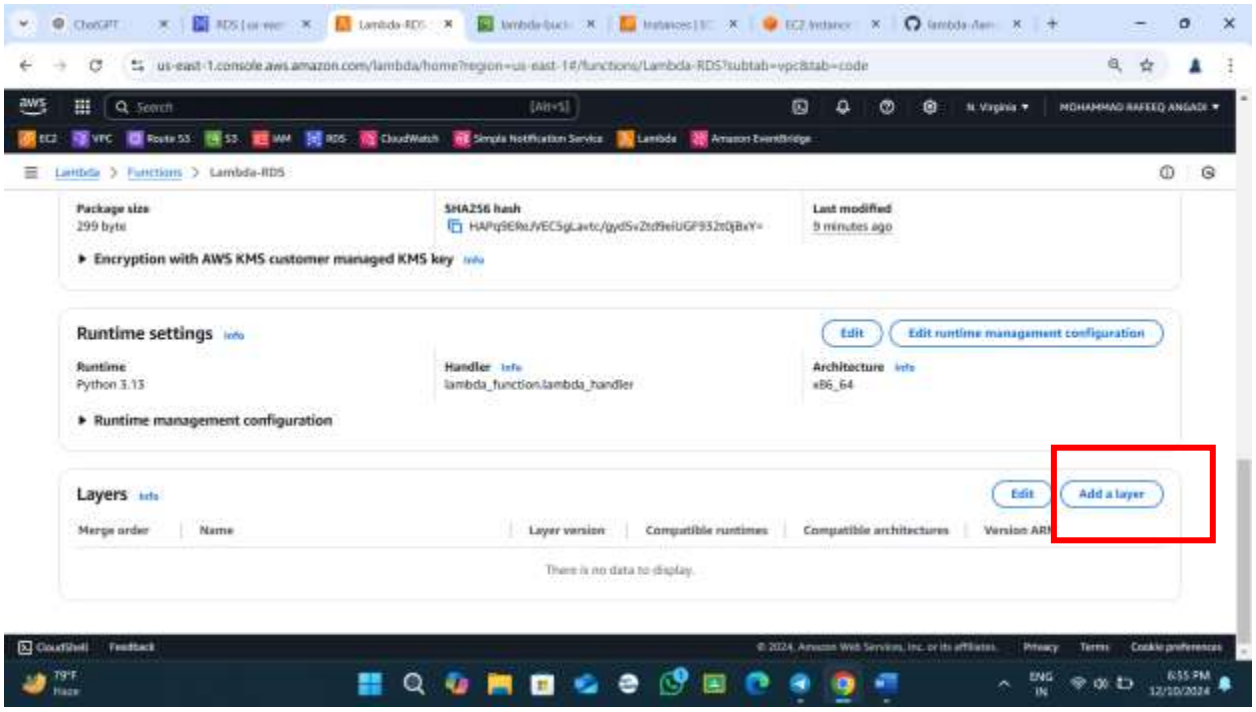
And past into the lambda like shown below

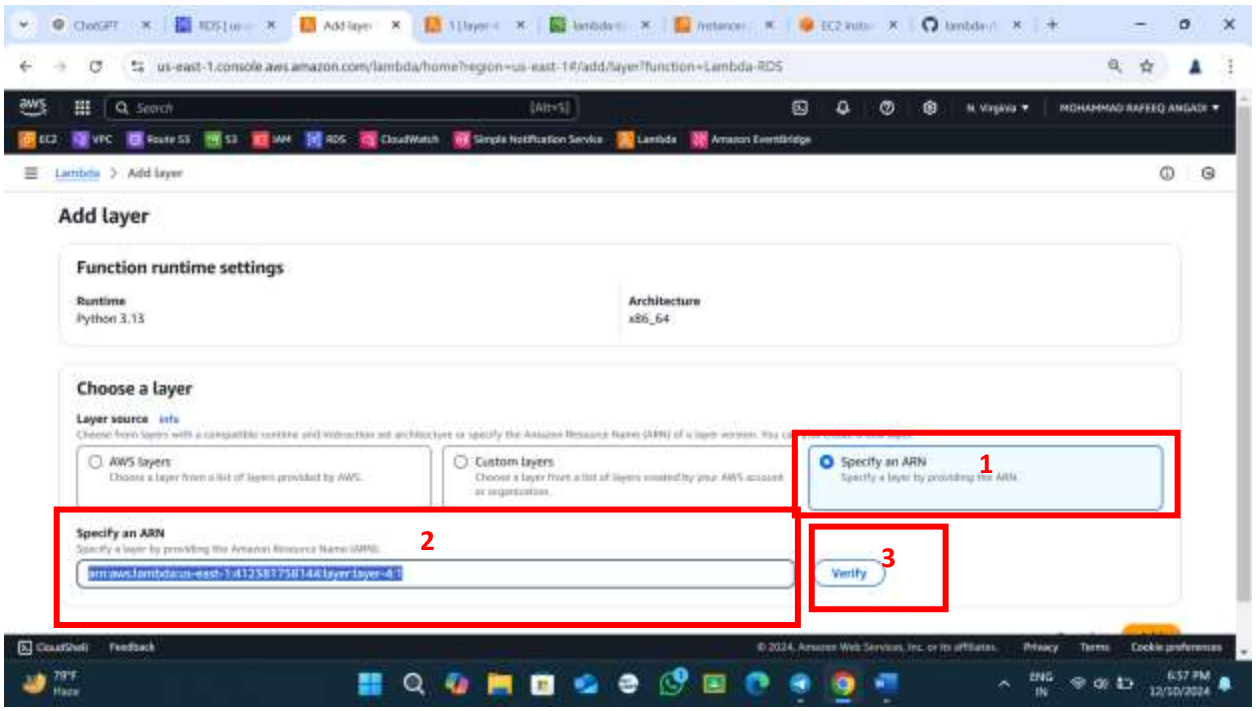

Layer configuration
Name
layer-4
Description - optional
any thing
Upload a .zip file
Upload a file from Amazon S3
Amazon S3 link URL
Compatible architectures - optional
x86_64
arm64
Compatible runtimes - optional

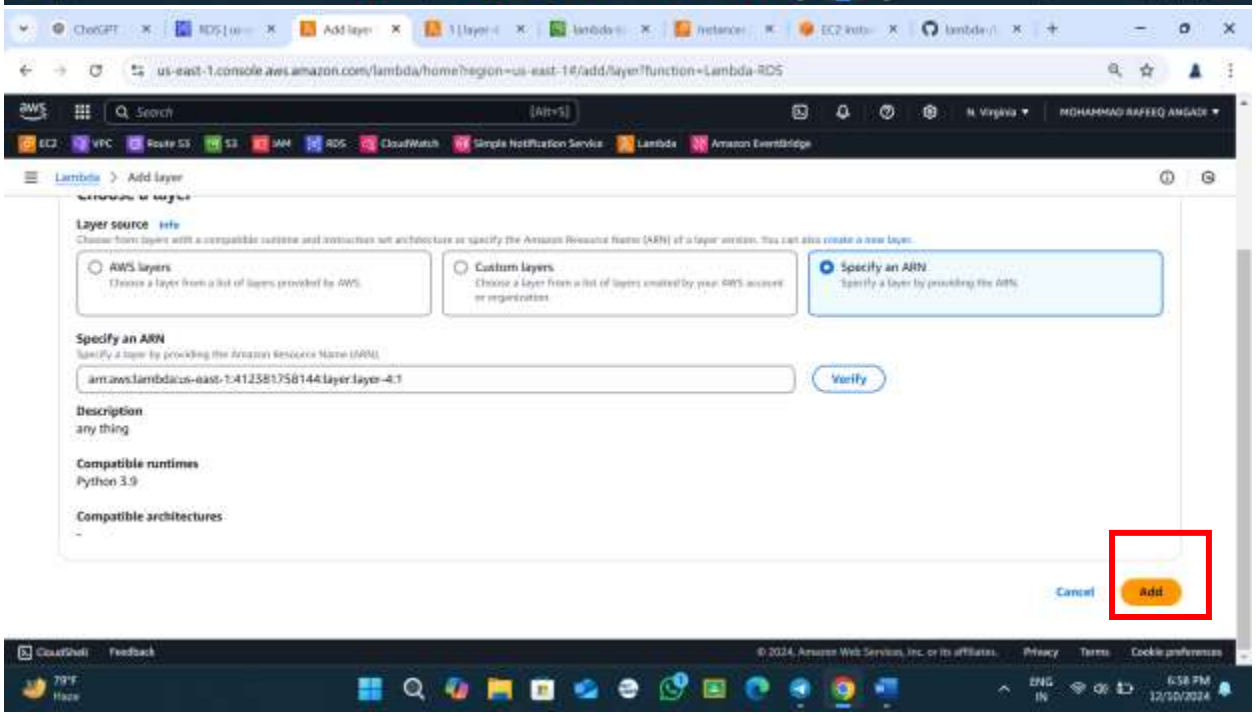

Node.js 18.x
Node.js 20.x
Python 3.10
Python 3.11
Python 3.12
Python 3.9
Ruby 3.2
Amazon Linux 2
Runtimes
Python 3.9
License - optional
Cancel
Create



Add the layer to function







7. Lambda Code

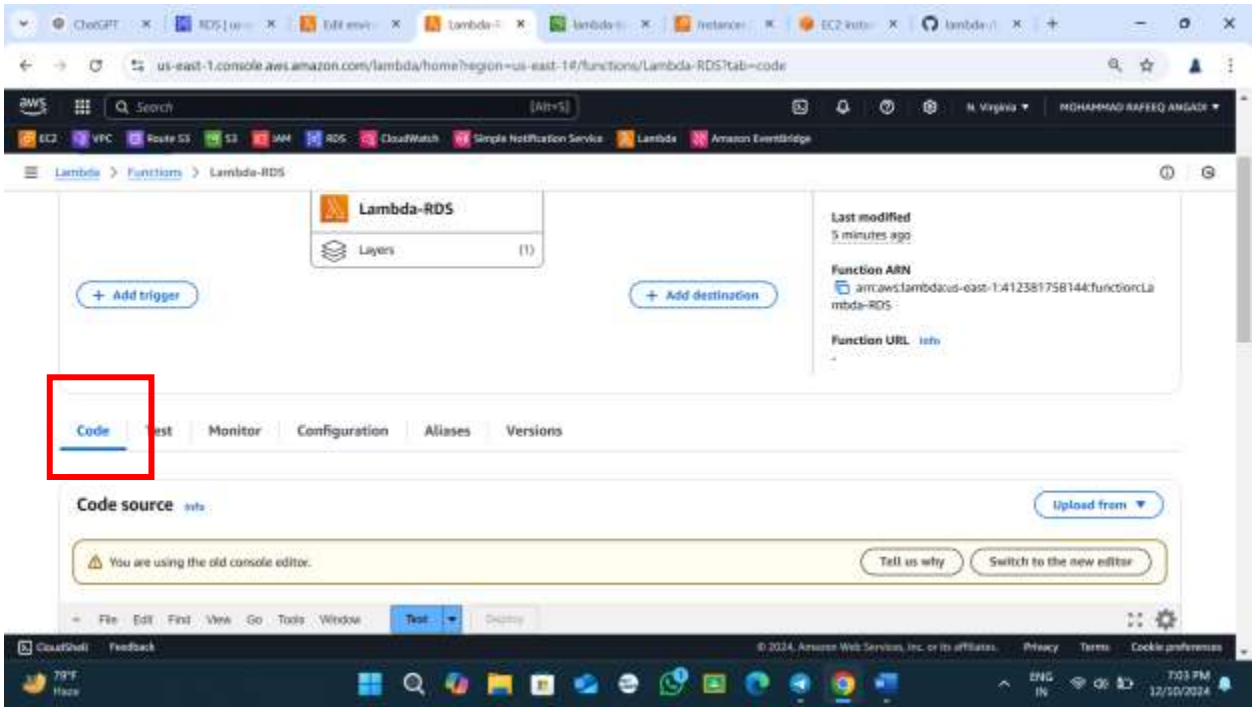
copy the below code:

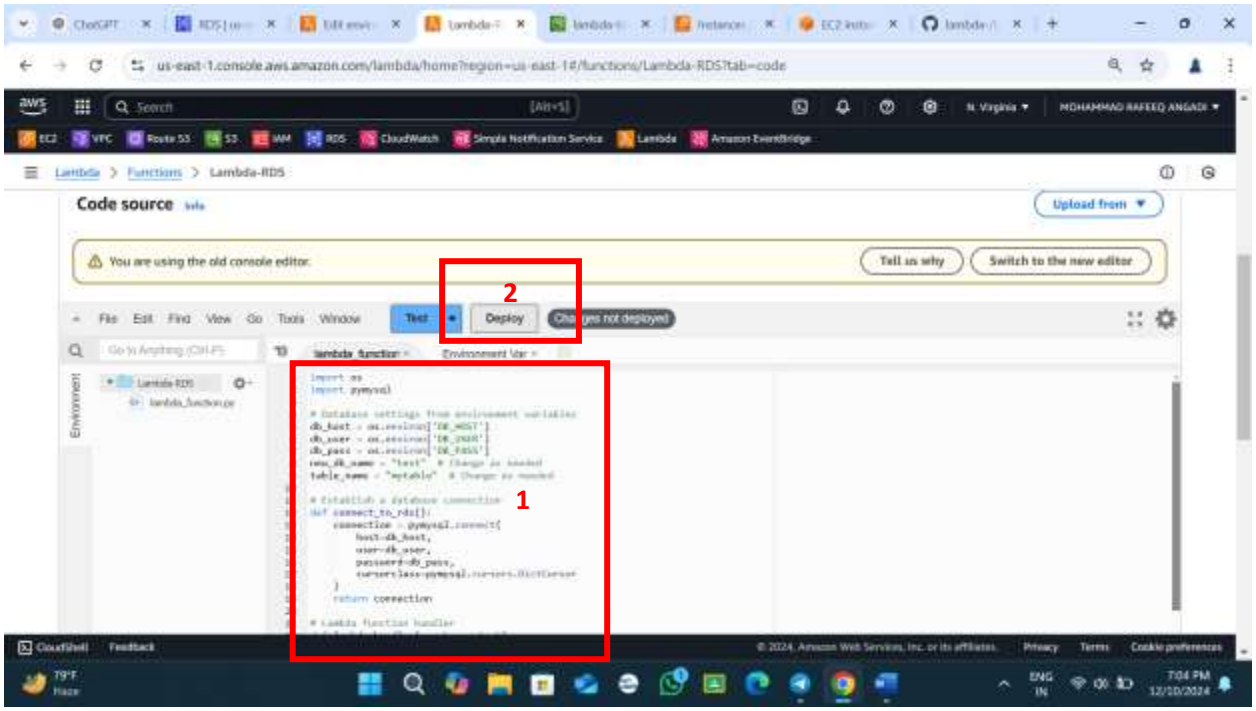
```
import os

import pymysql
```

```
# Database settings from environment variables
db_host = os.environ['DB_HOST']
db_user = os.environ['DB_USER']
db_pass = os.environ['DB_PASS']
new_db_name = "test"  # Change as needed
table_name = "mytable"  # Change as needed

# Establish a database connection
def connect_to_rds():
    connection = pymysql.connect(
        host=db_host,
        user=db_user,
        password=db_pass,
        cursorclass=pymysql.cursors.DictCursor
    )
    return connection

# Lambda function handler
def lambda_handler(event, context):
    try:
        connection = connect_to_rds()
        with connection.cursor() as cursor:
            # Create a new database
            create_db_sql = f"CREATE DATABASE IF NOT EXISTS {new_db_name};"
            cursor.execute(create_db_sql)
```

```
        # Select the new database
        cursor.execute(f"USE {new_db_name};")

        # Create a new table
        create_table_sql = f"""
        CREATE TABLE IF NOT EXISTS {table_name} (
            id INT AUTO_INCREMENT PRIMARY KEY,
            name VARCHAR(255) NOT NULL,
            created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
        );
        """
        cursor.execute(create_table_sql)

        print(f"Database '{new_db_name}' and table '{table_name}' created successfully.")
        return {
            'statusCode': 200,
            'body': f"Database '{new_db_name}' and table '{table_name}' created
successfully."
        }
    except Exception as e:
        print("Error:", str(e))
        return {
            'statusCode': 500,
            'body': str(e)
        }
    finally:
        connection.close()
```

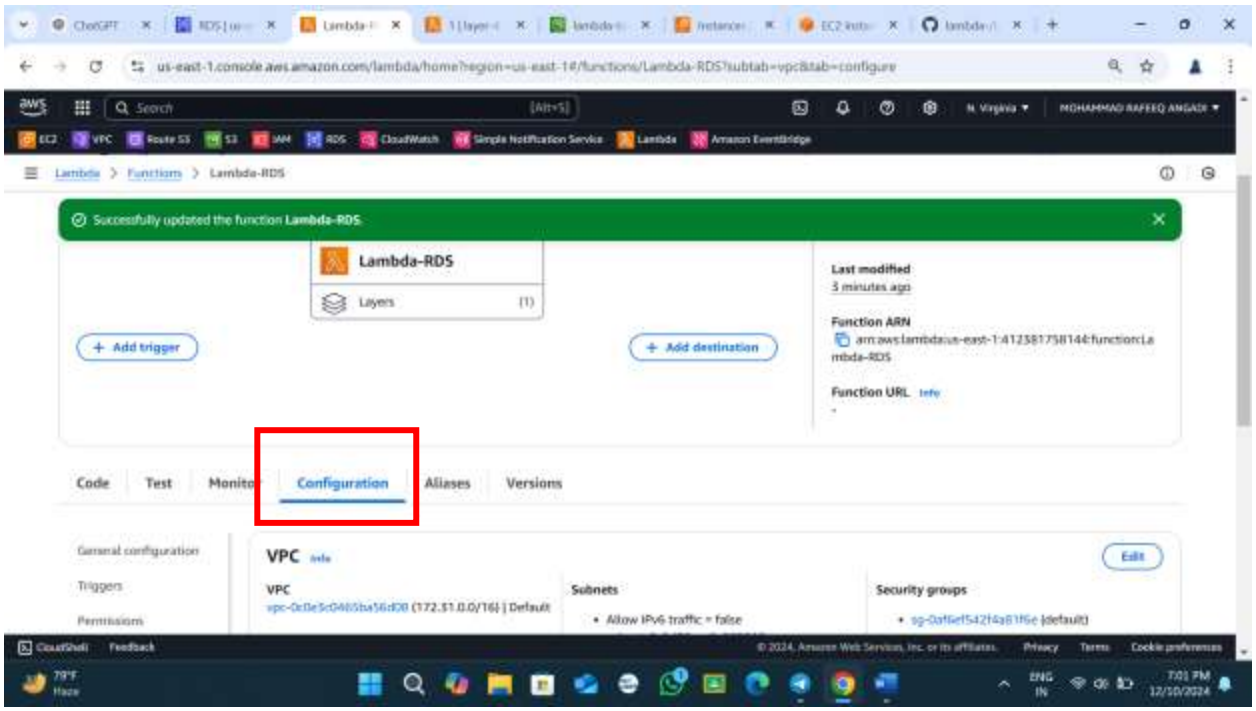
and paste the code into code tab

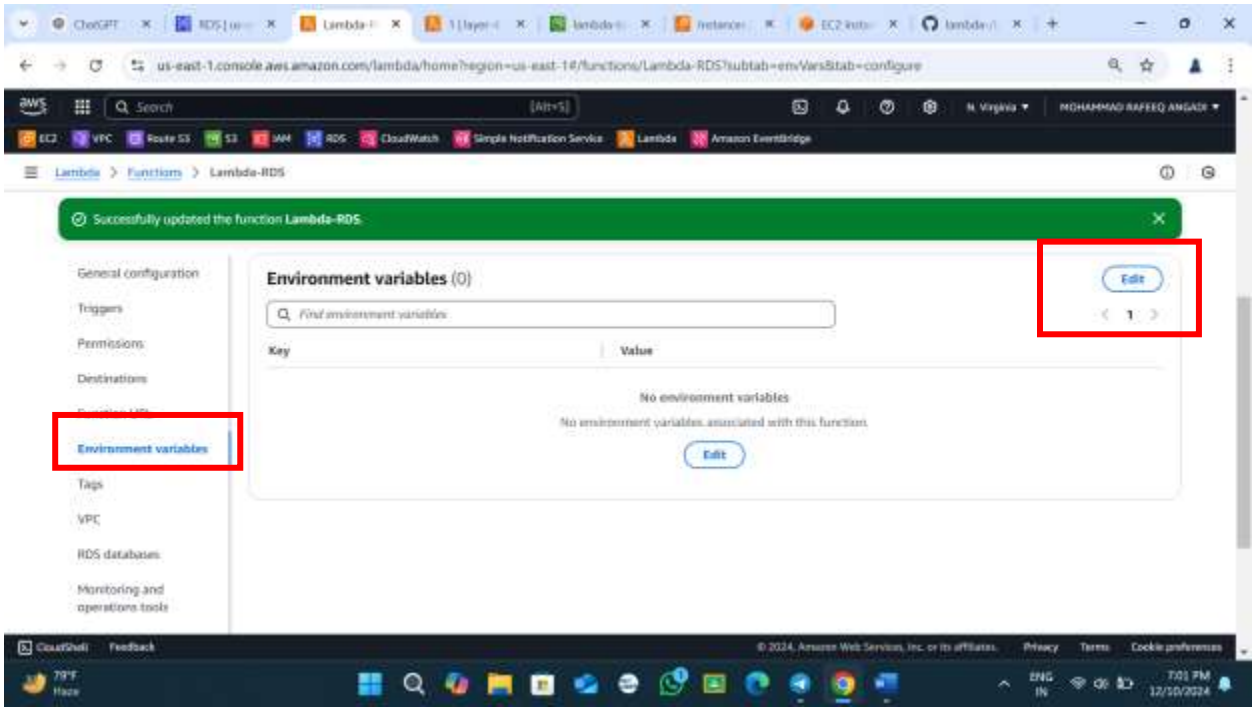


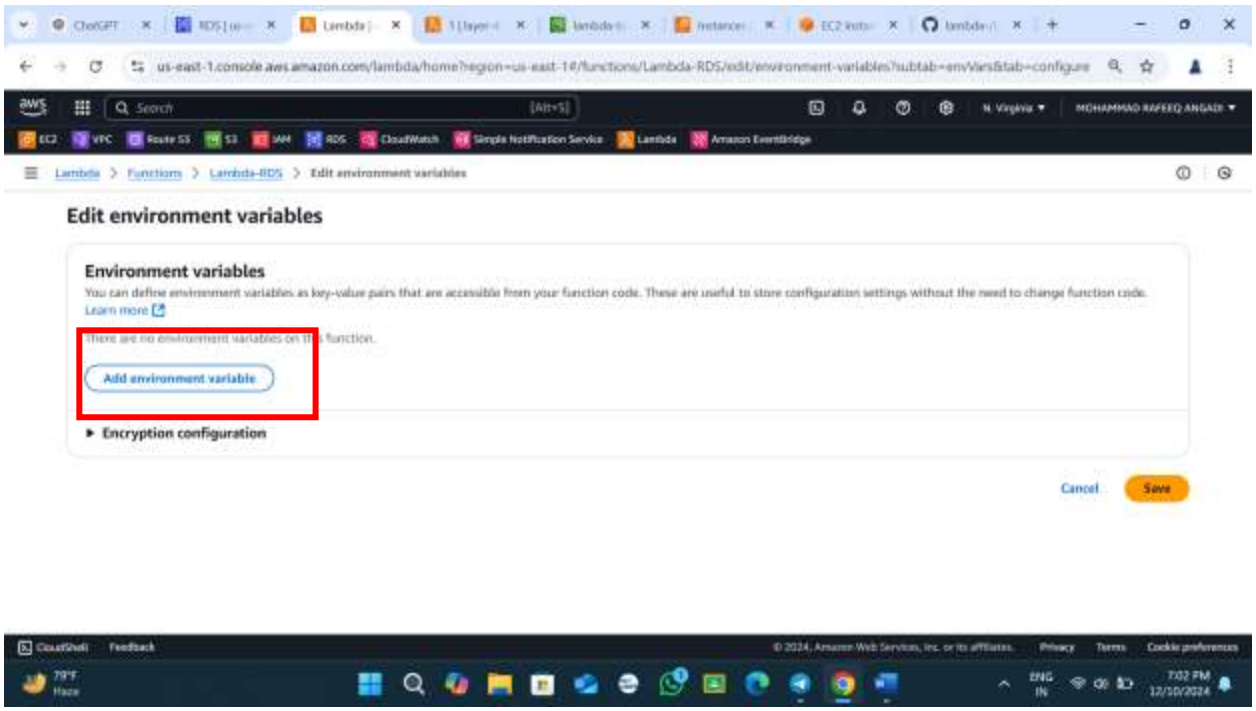


Click Deploy button

go to lambda configurations

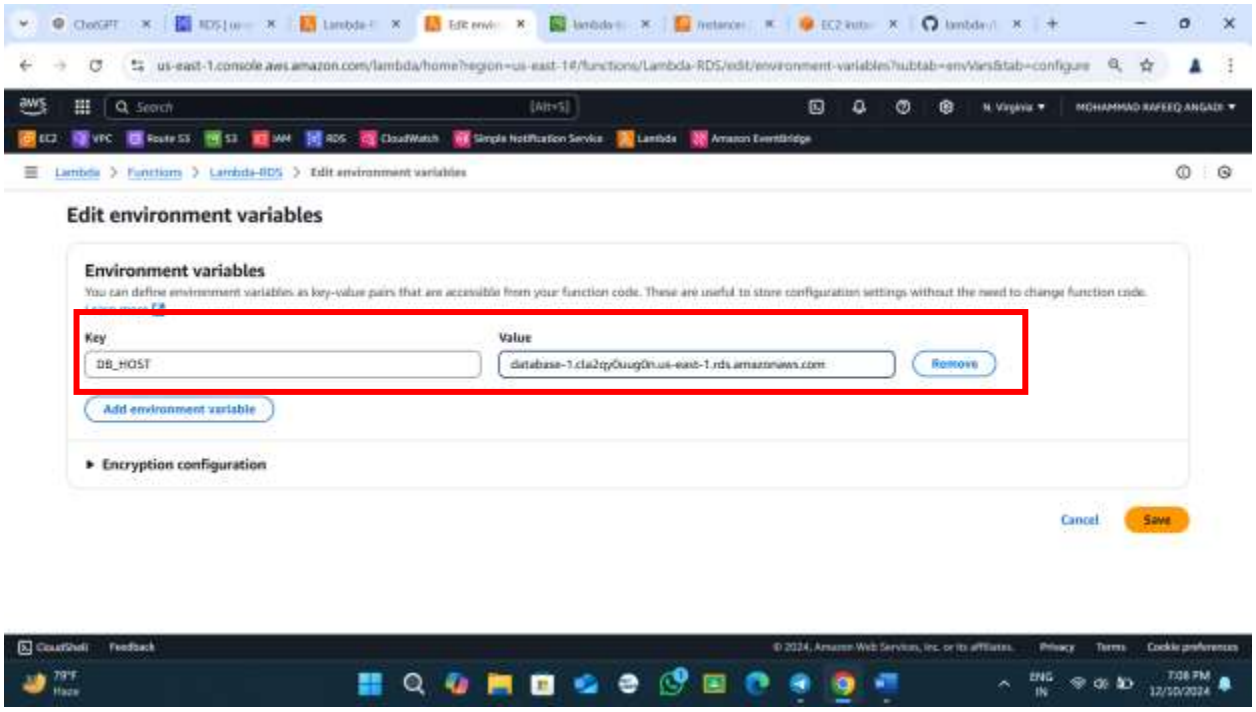

Successfully updated the function Lambda-RDS.
Lambda-RDS
Layers (1)
+ Add trigger
+ Add destination
Last modified
3 minutes ago
Function ARN
Function URL
Code
Test
Monitor
Configuration
Aliases
Versions
General configuration
Triggers
Permissions
VPC
Edit
Subnets
Security groups


Successfully updated the function Lambda-RDS.
General configuration
Triggers
Permissions
Destinations
Environment variables
Tags
VPC
RDS databases
Monitoring and operations tools
Environment variables (0)
Edit
Key
Value
No environment variables
Edit

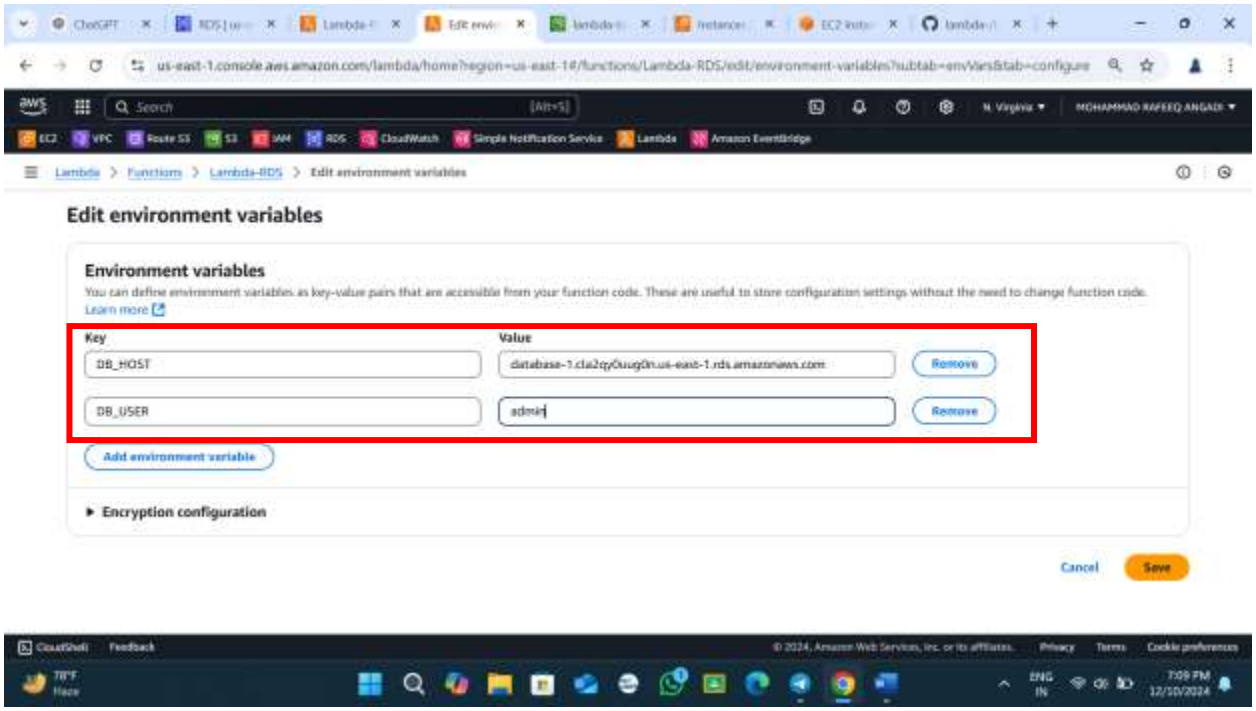


Give the below environment variables shown as below image

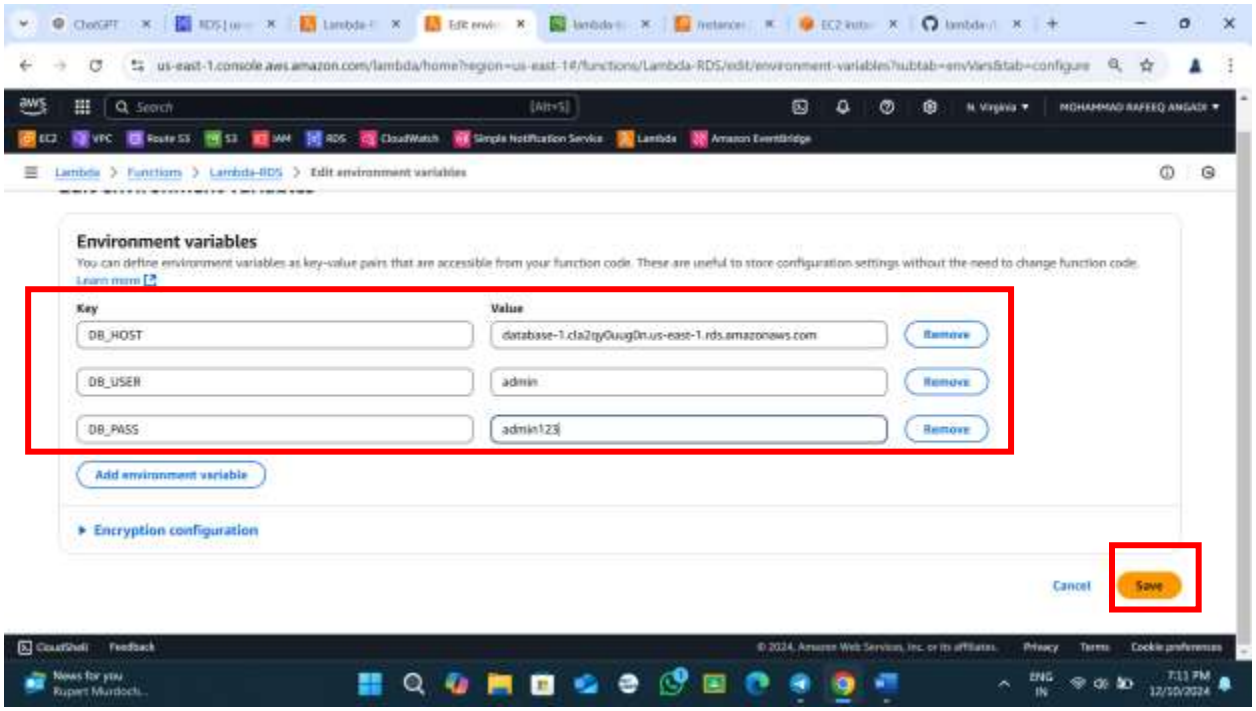
DB_HOST **your data base endpoint**



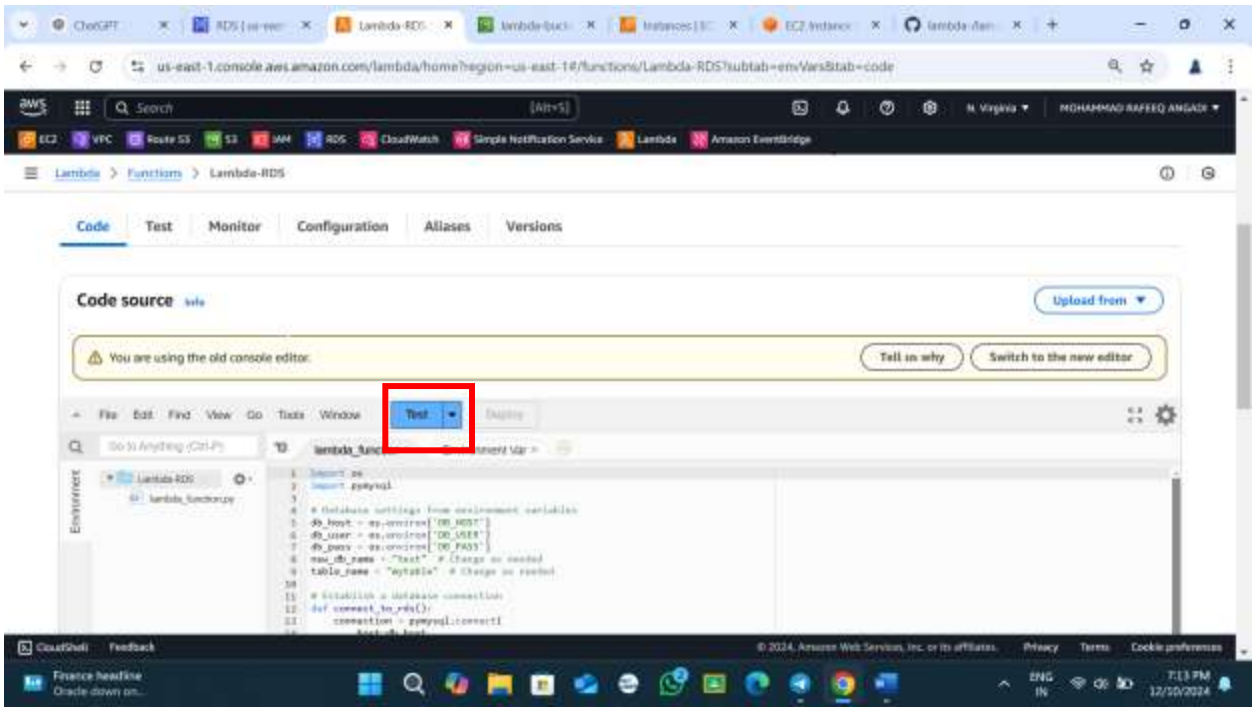
DB_USER your data base user name

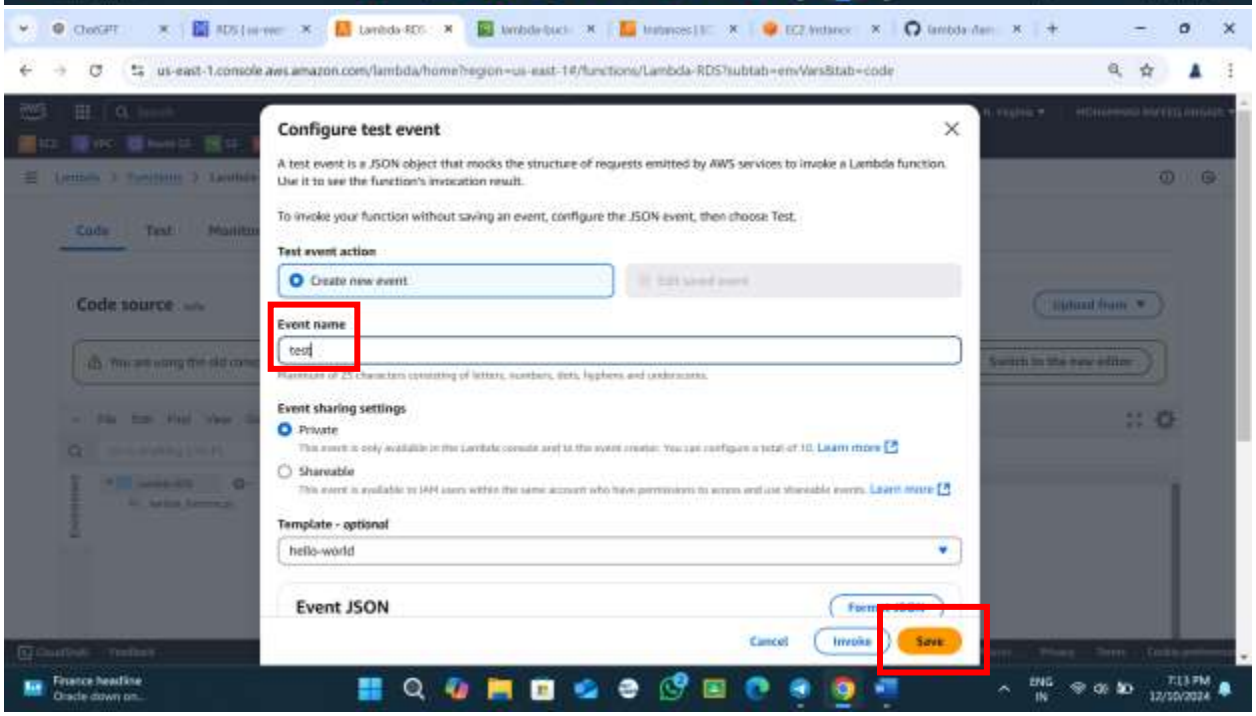


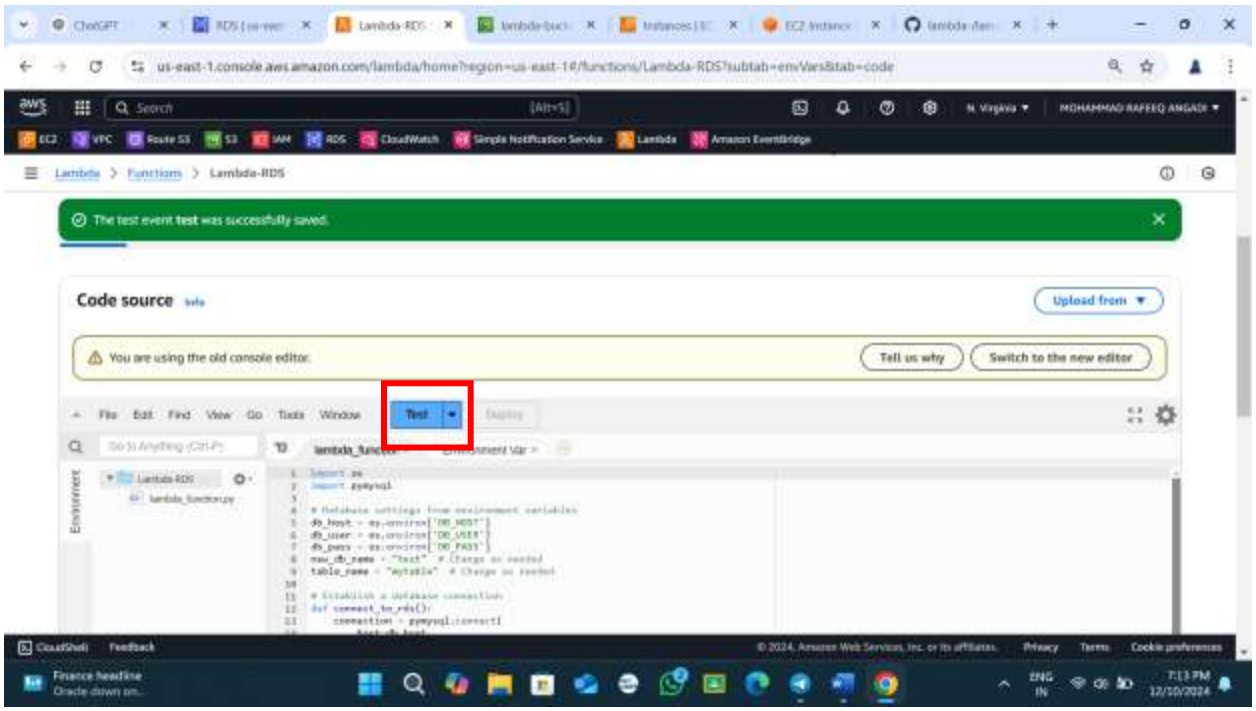
DB_PASS your database password



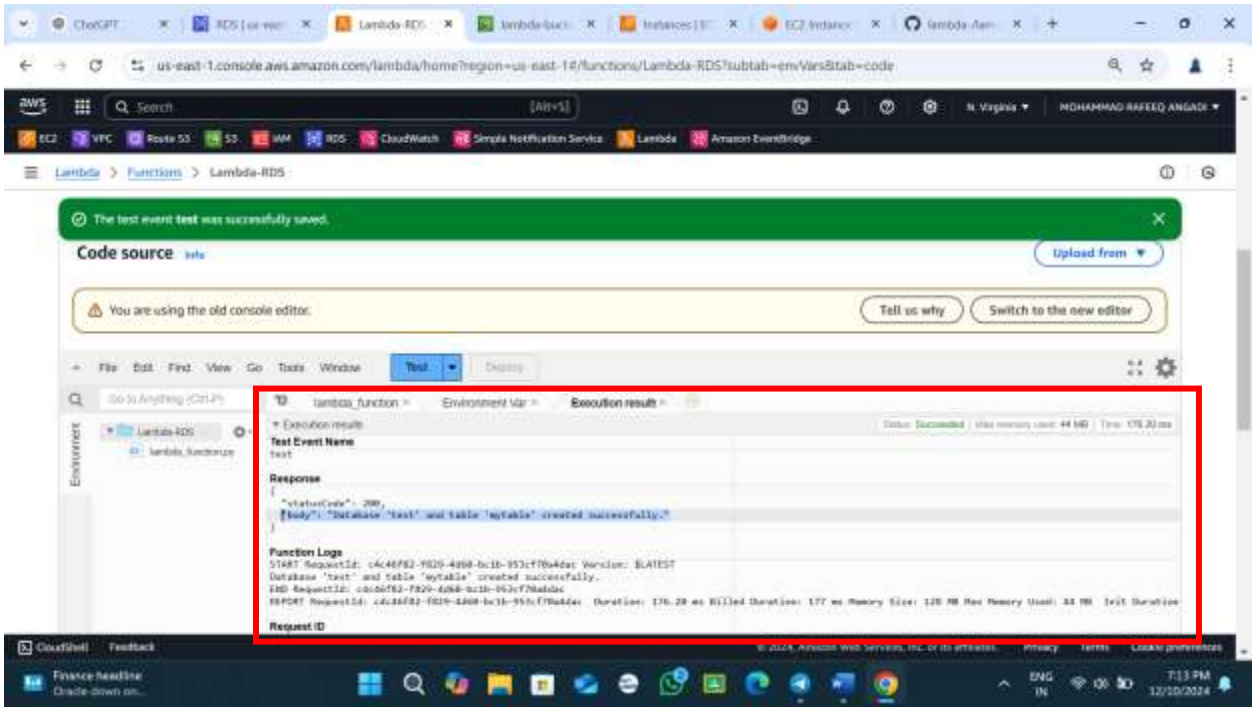
And click on test like shown in the below image


us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/Lambda-RDS?subtab=envVarsStab=code
Lambda > Functions > Lambda-RDS
Code
Test
Monitor
Configuration
Aliases
Versions
Code source
Upload from
You are using the old console editor.
Tell us why
Switch to the new editor
File Edit Find View Go Tools Window
Test
Deploy
Environment
Lambda-RDS
lambda_function.py
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/Lambda-RDS?subtab=envVarsStab=code
Configure test event
A test event is a JSON object that mocks the structure of requests emitted by AWS services to invoke a Lambda function. Use it to see the function's invocation result.
To invoke your function without saving an event, configure the JSON event, then choose Test.
Test event action
Create new event
Edit saved event
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
Format JSON
Cancel
Invoke
Save
Code source
Upload from
Switch to the new editor



200 means success



200 means success see created Database with test and inside created table name is mytable

---
