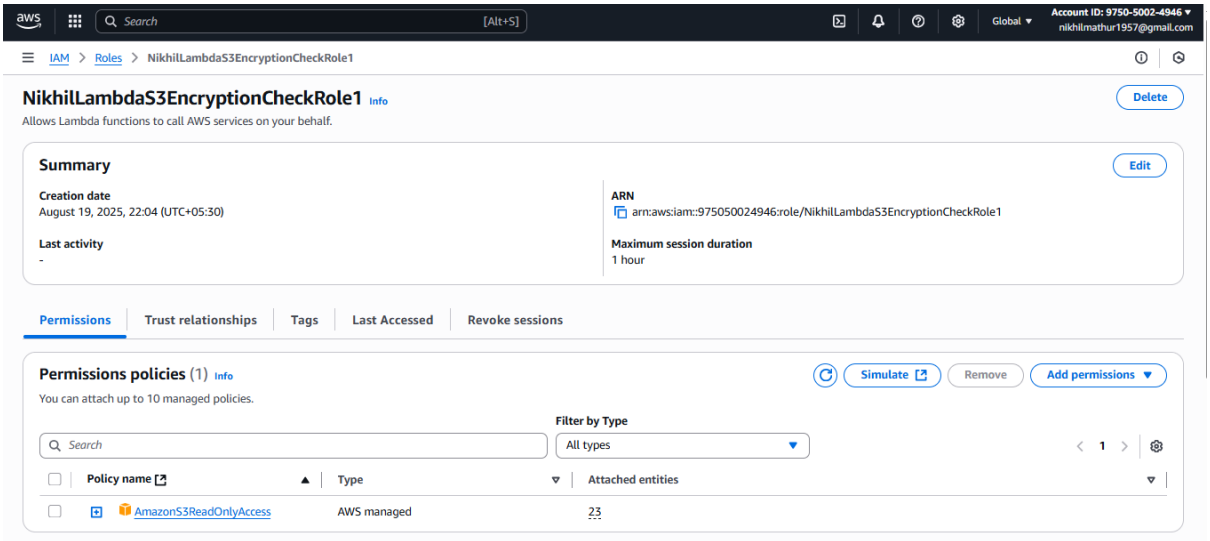
Assignment 3: Monitor Unencrypted S3 Buckets Using AWS Lambda and Boto3

Objective: To enhance your AWS security posture by setting up a Lambda function that detects any S3 bucket without server-side encryption.

Task: Automate the detection of S3 buckets that don't have server-side encryption enabled.

Lambda Function Creation:

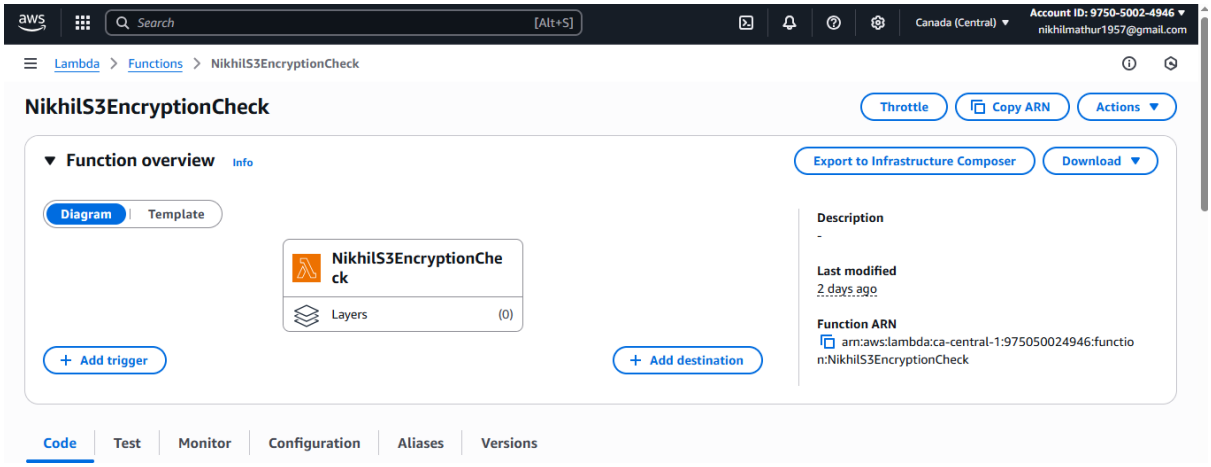
1. **Create an IAM Role for Lambda**
   - AWS Console => IAM =>Roles => Create role.
   - Trusted Entity type: AWS Services
   - Use Case: Lambda
   - Click Next



Permissions policies: AmazonEC2FullAccess
Role name: NikhilLambdaEC2ControlRole1
Click Create role.

2. **Create the Lambda Function**
   Go to AWS Console => Lambda.
   Click Create function.
   Select Author from scratch
   Function name: **NikhilS3EncryptionCheck**
   Runtime: Python 3.13
   Permissions:

Expand Change default execution role.
Select Use an existing role.
Choose **NikhilLambdaEC2ControlRole1** from the dropdown.
Note => I choose the role **prashantb12-role-9p53470y** for permission access to run the code.
Click Create function.



3. Add Python Code to Control EC2

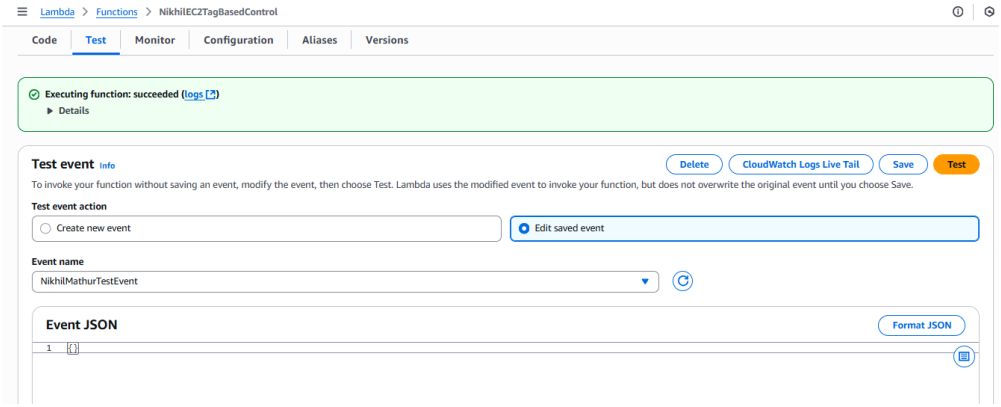
Assignment3.py

Assignment-3 > Assignment3.py

```python
import boto3
from botocore.exceptions import ClientError

def lambda_handler(event, context):
    s3 = boto3.client("s3")

    # Get all S3 buckets
    response = s3.list_buckets()
    buckets = response["Buckets"]

    non_encrypted_buckets = []

    for bucket in buckets:
        bucket_name = bucket["Name"]
        try:
            # Check encryption settings
            enc = s3.get_bucket_encryption(Bucket=bucket_name)
            rules = enc["ServerSideEncryptionConfiguration"]["Rules"]

            # If rules exist, SSE is enabled
            print(f" {bucket_name} has encryption: {rules}")

        except ClientError as e:
            error_code = e.response["Error"]["Code"]
            if error_code == "ServerSideEncryptionConfigurationNotFoundError":
                print(f" {bucket_name} does NOT have encryption enabled")
                non_encrypted_buckets.append(bucket_name)
            else:
                print(f" Could not check bucket {bucket_name}: {e}")
```

```
30
31      if non_encrypted_buckets:
32          print("Buckets without encryption:", non_encrypted_buckets)
33      else:
34          print("All buckets have encryption enabled ✅")
35
36      return {"NonEncryptedBuckets": non_encrypted_buckets}
37
```

Create the test case



Click for deploy the code

Test the code