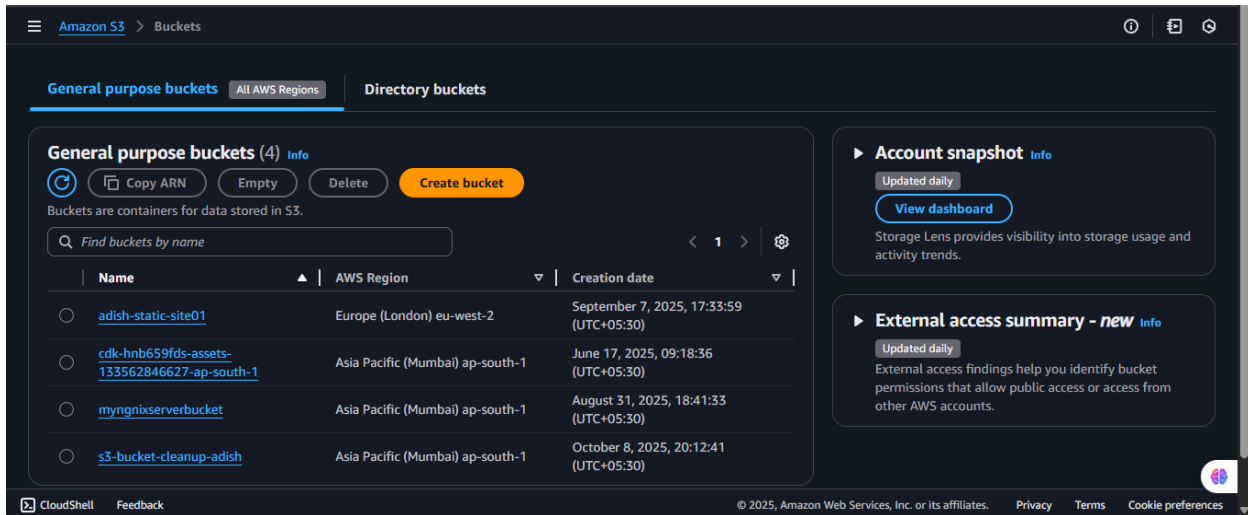


## Step 1:- Create the S3 Bucket and list of bucket

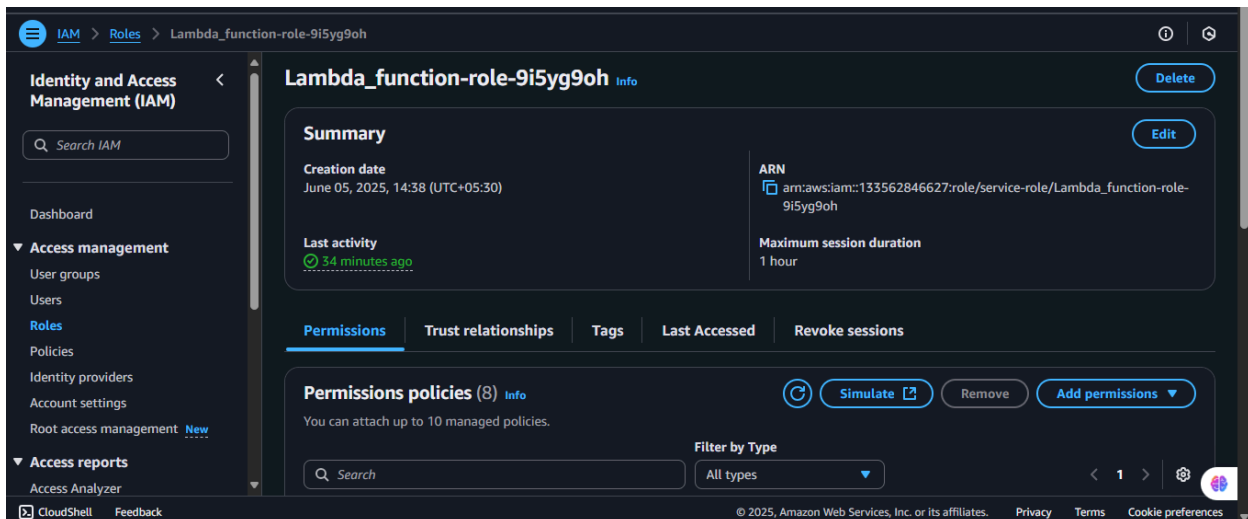


The screenshot shows the Amazon S3 console interface. At the top, there are tabs for "General purpose buckets" (selected) and "Directory buckets". Below the tabs, there's a section for "General purpose buckets (4)" with buttons for "Copy ARN", "Empty", "Delete", and "Create bucket". A search bar labeled "Find buckets by name" is present. Below the search bar is a table listing the buckets:

| Name   | AWS Region                       | Creation date                           |
|--|----------------------------------|---|
| adish-static-site01                          | Europe (London) eu-west-2        | September 7, 2025, 17:33:59 (UTC+05:30) |
| cdk-hnb659fds-assets-133562846627-ap-south-1 | Asia Pacific (Mumbai) ap-south-1 | June 17, 2025, 09:18:36 (UTC+05:30)     |
| myngnixserverbucket                          | Asia Pacific (Mumbai) ap-south-1 | August 31, 2025, 18:41:33 (UTC+05:30)   |
| s3-bucket-cleanup-adish                      | Asia Pacific (Mumbai) ap-south-1 | October 8, 2025, 20:12:41 (UTC+05:30)   |

On the right side, there are two panels: "Account snapshot" (Updated daily, View dashboard) and "External access summary - new" (Updated daily, Info). The footer shows "CloudShell", "Feedback", and copyright information for Amazon Web Services, Inc. or its affiliates.

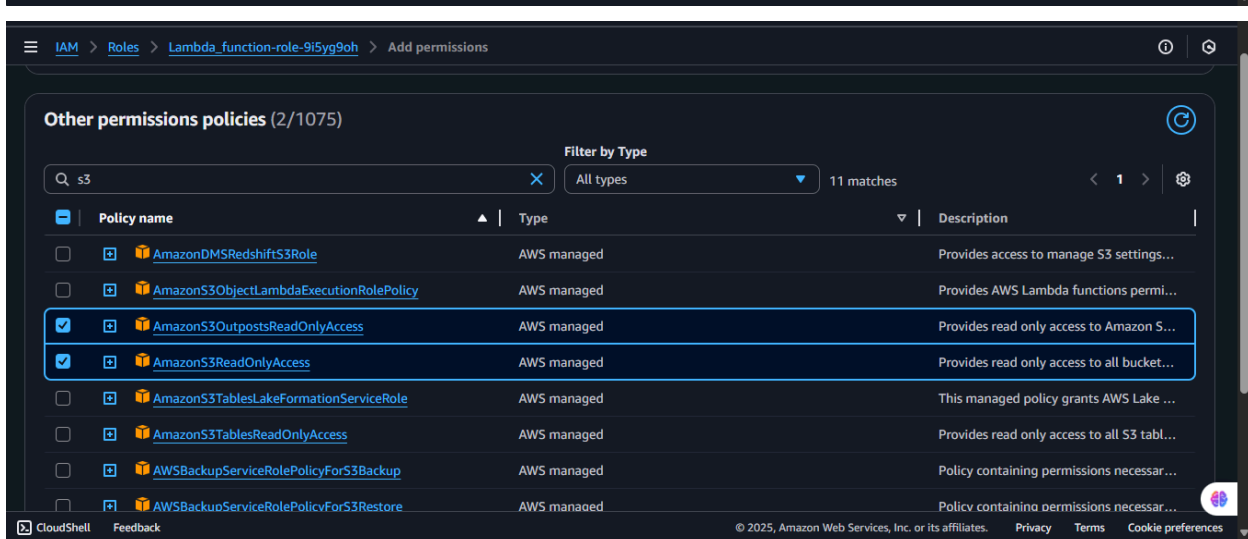
## Step 2 : - Create IAM Role



The screenshot shows the IAM console interface for the role "Lambda\_function-role-9i5yg9oh". The left sidebar shows the "Identity and Access Management (IAM)" menu with options like "Dashboard", "Access management", "User groups", "Users", "Roles" (selected), "Policies", "Identity providers", "Account settings", and "Root access management". The main content area shows the role's "Summary" with the following details:

- Creation date:** June 05, 2025, 14:38 (UTC+05:30)
- Last activity:** 34 minutes ago
- ARN:** arn:aws:iam::133562846627:role/service-role/Lambda\_function-role-9i5yg9oh
- Maximum session duration:** 1 hour

Below the summary, there are tabs for "Permissions", "Trust relationships", "Tags", "Last Accessed", and "Revoke sessions". The "Permissions" tab is selected, showing "Permissions policies (8)" with a "Simulate" button and a "Filter by Type" dropdown set to "All types".



The screenshot shows the "Add permissions" screen in the IAM console for the role "Lambda\_function-role-9i5yg9oh". The left sidebar shows the "IAM" menu with options like "Roles" (selected) and "Add permissions". The main content area shows "Other permissions policies (2/1075)" with a search bar containing "s3" and a "Filter by Type" dropdown set to "All types". There are 11 matches listed in a table:

| Policy name  | Type        | Description                                 |
|--|-------------|---|
| AmazonDMSRedshiftS3Role  | AWS managed | Provides access to manage S3 settings...    |
| AmazonS3ObjectLambdaExecutionRolePolicy                            | AWS managed | Provides AWS Lambda functions permi...      |
| <input checked="" type="checkbox"/> AmazonS3OutpostsReadOnlyAccess | AWS managed | Provides read only access to Amazon S...    |
| <input checked="" type="checkbox"/> AmazonS3ReadOnlyAccess         | AWS managed | Provides read only access to all bucket...  |
| AmazonS3TablesLakeFormationServiceRole                             | AWS managed | This managed policy grants AWS Lake ...     |
| AmazonS3TablesReadOnlyAccess                                       | AWS managed | Provides read only access to all S3 tabl... |
| AWSBackupServiceRolePolicyForS3Backup                              | AWS managed | Policy containing permissions necessar...   |
| AWSBackupServiceRolePolicyForS3Restore                             | AWS managed | Policy containing permissions necessar...   |

The footer shows "CloudShell", "Feedback", and copyright information for Amazon Web Services, Inc. or its affiliates.

### Step 3 :- Create Lambda Function

Lambda > Functions > Create function

Create function

info

Choose one of the following options to create your function.

☒ Author from scratch  
Start with a simple Hello World example.

☐ Use a blueprint  
Build a Lambda application from sample code and configuration presets for common use cases.

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

Basic information

Function name  
Enter a name that describes the purpose of your function.  
Monitor-Unencrypted-S3  
Function name must be 1 to 64 characters, must be unique to the Region, and can't include spaces. Valid characters are a-z, A-Z, 0-9, hyphens (-), and underscores (\_).

Runtime  
Info  
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.  
Python 3.13

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

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Lambda > Functions > Create function

Permissions

info

By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

▼ Change default execution role

Execution role  
Choose a role that defines the permissions of your function. To create a custom role, go to the [IAM console](#).  
☐ Create a new role with basic Lambda permissions  
☒ Use an existing role  
☐ Create a new role from AWS policy templates

Existing role  
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.  
service-role/Lambda\_function-role-9i5yg9oh  
View the Lambda\_function-role-9i5yg9oh role on the IAM console.

► Additional configurations

Use additional configurations to set up networking, security, and governance for your function. These settings help secure and customize your Lambda function deployment.

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Lambda > Functions > Monitor-Unencrypted-S3

Code

Test

Monitor

Configuration

Aliases

Versions

General configuration

Triggers

Permissions

Destinations

Function URL

Environment variables

Tags

VPC

RDS databases

General configuration

info

Edit

Description  
-

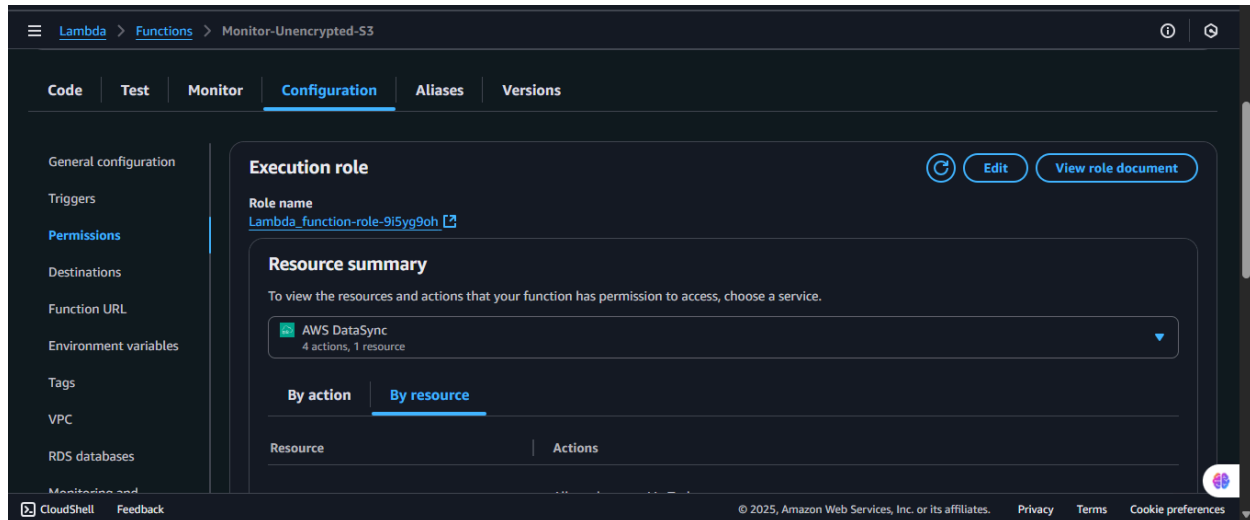
Memory  
128 MB

Ephemeral storage  
512 MB

Timeout  
1 min 0 sec

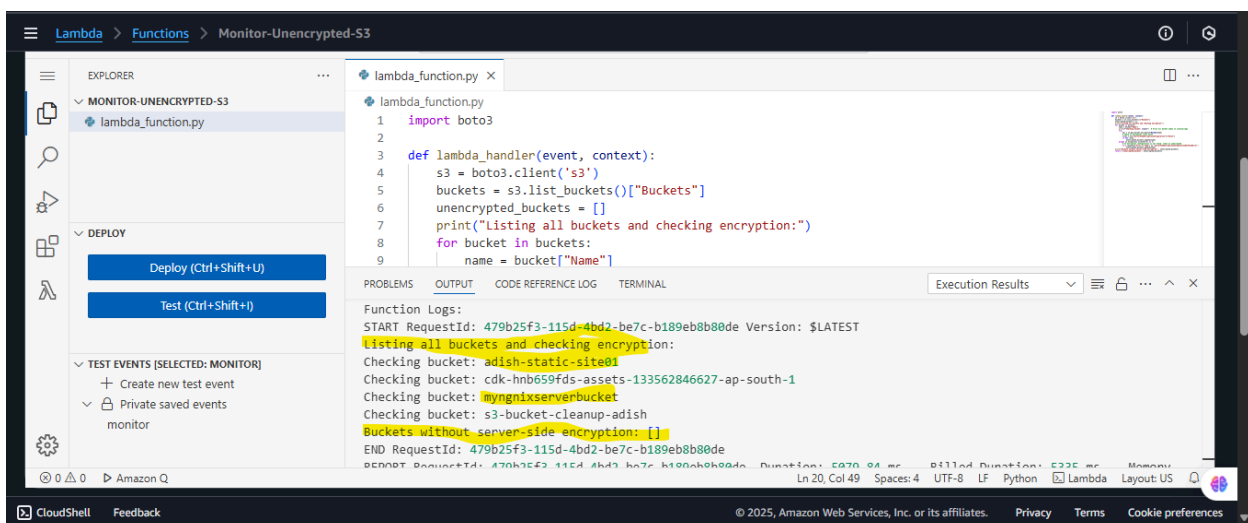
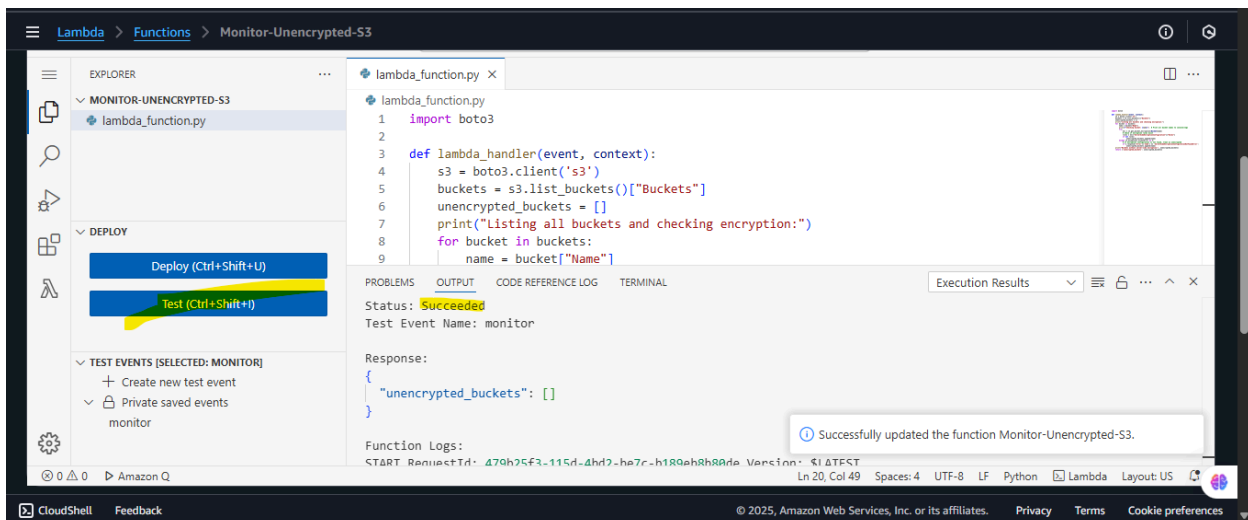
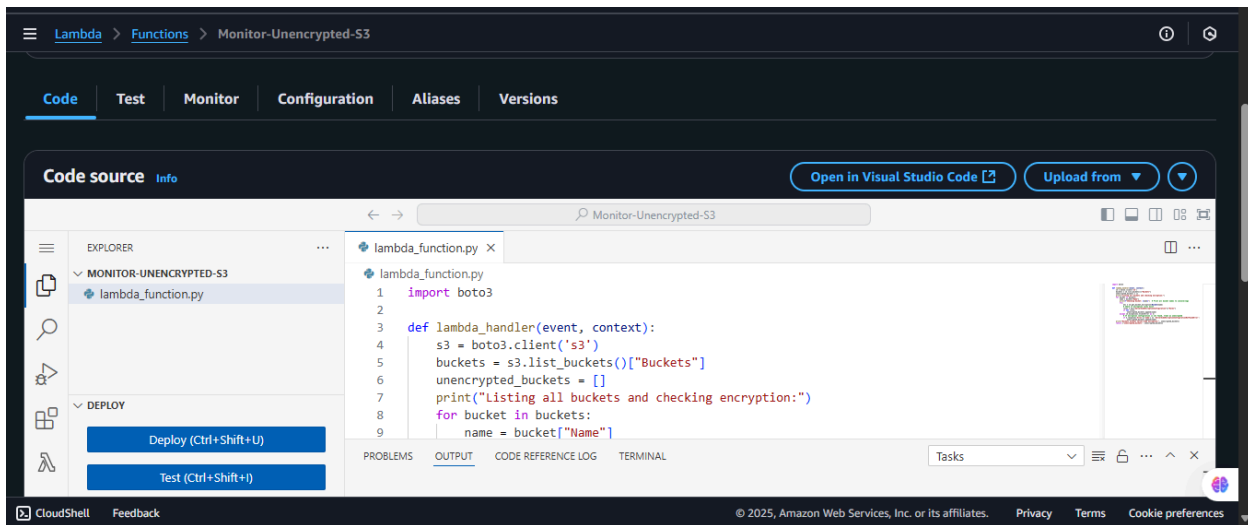
SnapStart  
None

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



```
import boto3

def lambda_handler(event, context):
    s3 = boto3.client('s3')
    buckets = s3.list_buckets()["Buckets"]
    unencrypted_buckets = []
    print("Listing all buckets and checking encryption:")
    for bucket in buckets:
        name = bucket["Name"]
        print(f"Checking bucket: {name}") # Print all bucket names to
console/logs
        try:
            enc = s3.get_bucket_encryption(Bucket=name)
            # Check if encryption rules exist
            rules = enc["ServerSideEncryptionConfiguration"]["Rules"]
            if not rules:
                unencrypted_buckets.append(name)
        except s3.exceptions.ClientError as e:
            # If encryption configuration is not found, treat as
unencrypted
            if e.response['Error']['Code'] ==
'ServerSideEncryptionConfigurationNotFoundError':
                unencrypted_buckets.append(name)
    print("Buckets without server-side encryption:", unencrypted_buckets)
    return {'unencrypted_buckets': unencrypted_buckets}
```



Lambda > Functions > Monitor-Unencrypted-S3

EXPLORER

MONITOR-UNENCRYPTED-S3

lambda\_function.py

DEPLOY

Deploy (Ctrl+Shift+U)

Test (Ctrl+Shift+I)

TEST EVENTS [SELECTED: MONITOR]

Create new test event

Private saved events

monitor

lambda\_function.py

```
1 import boto3
2
3 def lambda_handler(event, context):
4     s3 = boto3.client('s3')
5     buckets = s3.list_buckets()["Buckets"]
6     unencrypted_buckets = []
7     print("Listing all buckets and checking encryption:")
8     for bucket in buckets:
9         name = bucket["Name"]
```

PROBLEMS OUTPUT CODE REFERENCE LOG TERMINAL

Execution Results

Checking bucket: cdK-hnb659fds-assets-133562846627-ap-south-1

Checking bucket: mygnnixserverbucket

Checking bucket: s3-bucket-cleanup-adish

Buckets without server-side encryption: []

END RequestId: 479b25f3-115d-4bd2-be7c-b189eb8b88de

REPORT RequestId: 479b25f3-115d-4bd2-be7c-b189eb8b88de Duration: 5079.84 ms Billed Duration: 5335 ms Memory Size: 128 MB Max Memory Used: 92 MB Init Duration: 254.81 ms

Request ID: 479b25f3-115d-4bd2-be7c-b189eb8b88de

0 0 0 Amazon Q

Ln 20, Col 49 Spaces: 4 UTF-8 LF Python Lambda Layout: US

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences