

Q1: serve s3 from cloudfront with blocked access to s3

### Create bucket info

Buckets are containers for data stored in S3.

#### General configuration

**AWS Region**  
Europe (Frankfurt) eu-central-1

**Bucket name** info  
static-hosting-trial-bucket-123421

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

#### 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.

### Upload info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose [Add files](#) or [Add folder](#).

#### Files and folders (0)

All files and folders in this table will be uploaded.

Home / Downloads / hello-world-html

css

index.html

1 folder selected (containing 1 item), 1 other item selected (245 bytes)

Remove

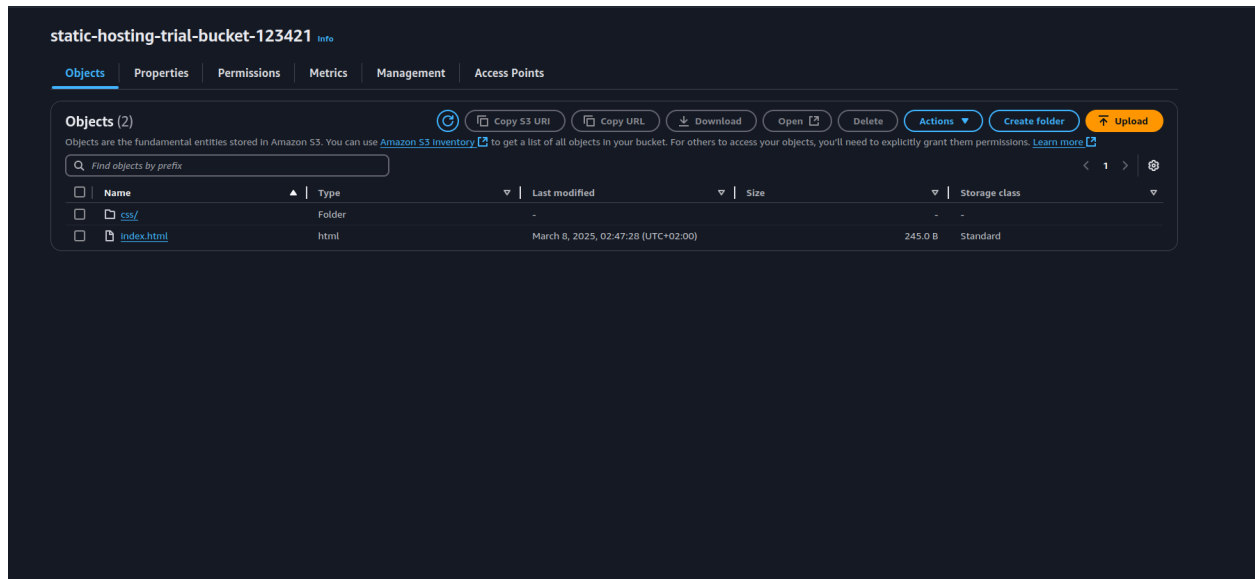
Add files

Add folder

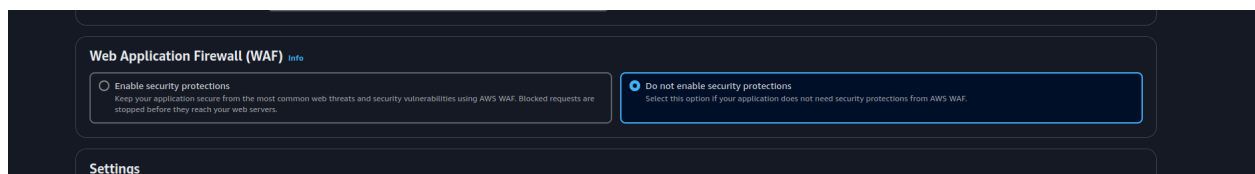
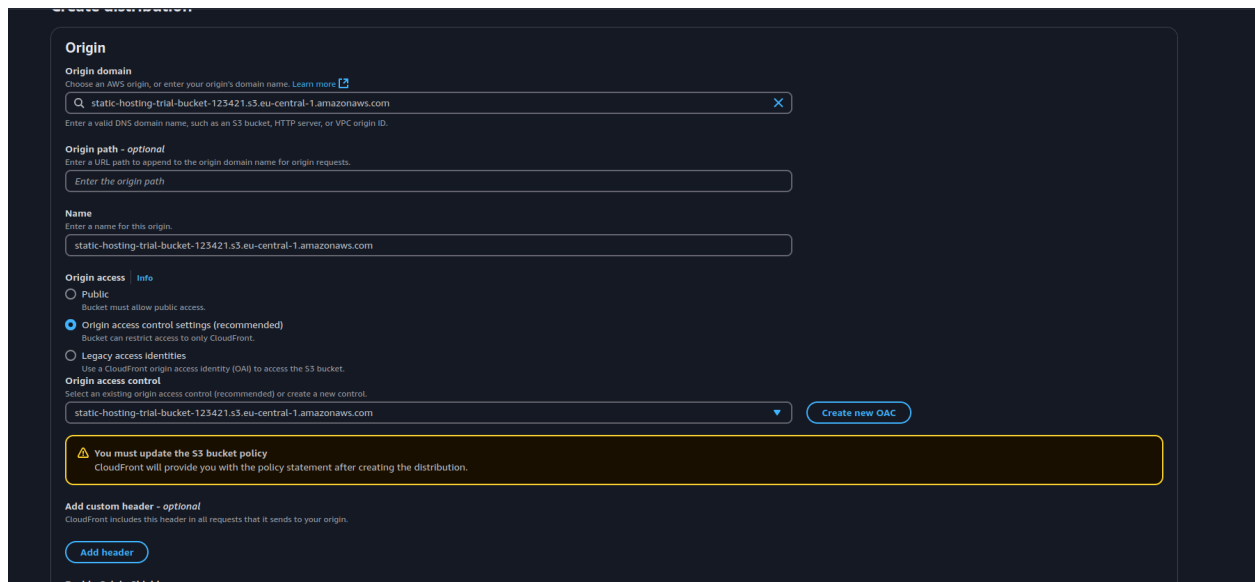
No files or folders  
chosen any files or folders to upload.

Cancel

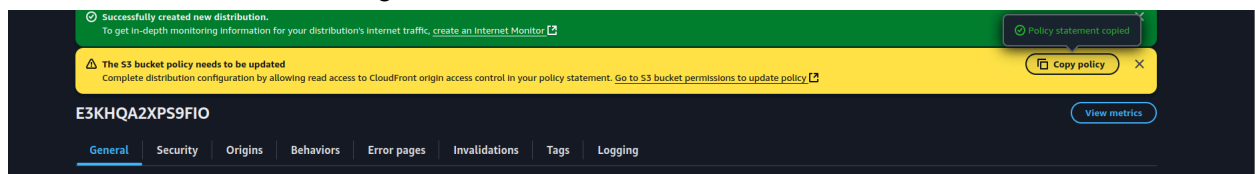
Upload



In the cloudfront page



And the rest the default config was used



Copying the policy

Edit bucket policy

Bucket policy

Policy examples

Policy generator

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Bucket ARN

arn:aws:s3:::static-hosting-trial-bucket-123421

Policy

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

```
{
  "Version": "2008-10-17",
  "Id": "PolicyforCloudFrontPrivateContent",
  "Statement": [
    {
      "Sid": "AllowCloudFrontServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudfront.amazonaws.com"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::static-hosting-trial-bucket-123421/*",
      "Condition": {
        "StringEquals": {
          "AWS:SourceArn": "arn:aws:cloudfront::897729102326:distribution/E3KHQA2XP89F10"
        }
      }
    }
  ]
}
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

https://us-east-1.console.aws.amazon.com/cloudfront/v4/home#/distributions

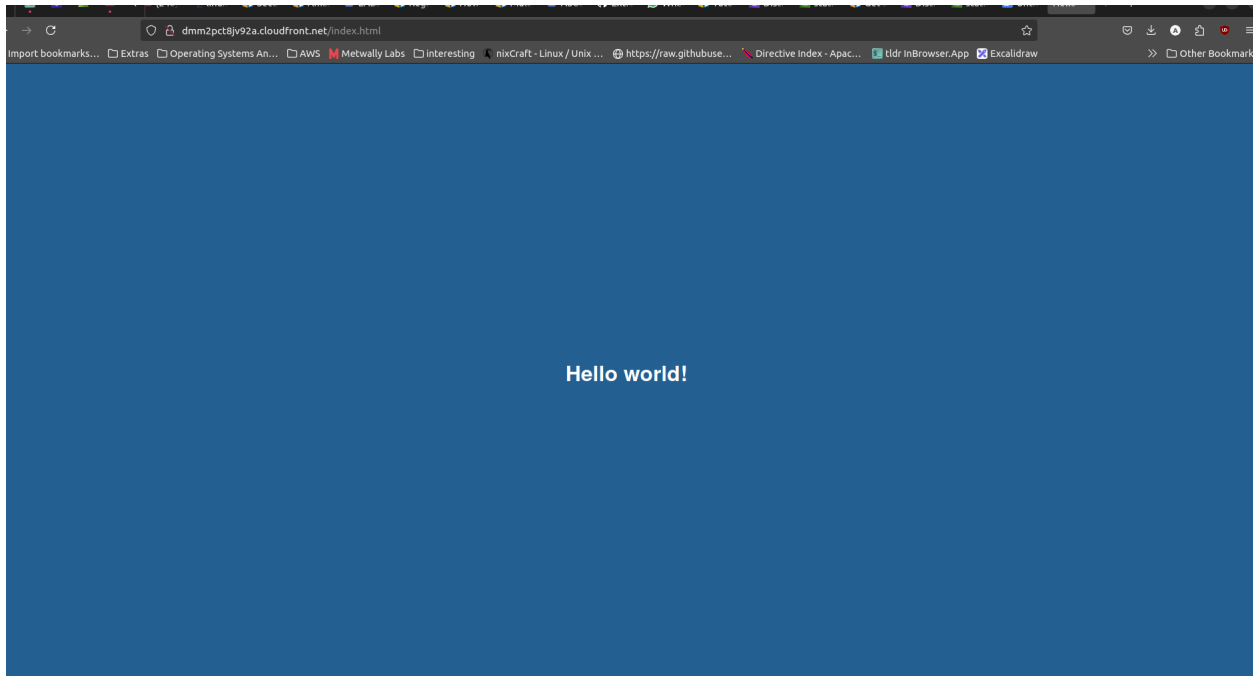
CloudFront > Distributions

Distributions (1)

Search all distributions

Enable Disable Delete Create distribution

ID	Description	Type	Domain name	Alternate domain n...	Origins	Status	Last modified
E3KHQA2XP89F10	-	Production	dmm2pct8ly92a.cloudfront.net	-	static-hosting-trial-bucket-1	Enabled	March 8, 2025 at 12:59:03 AM...



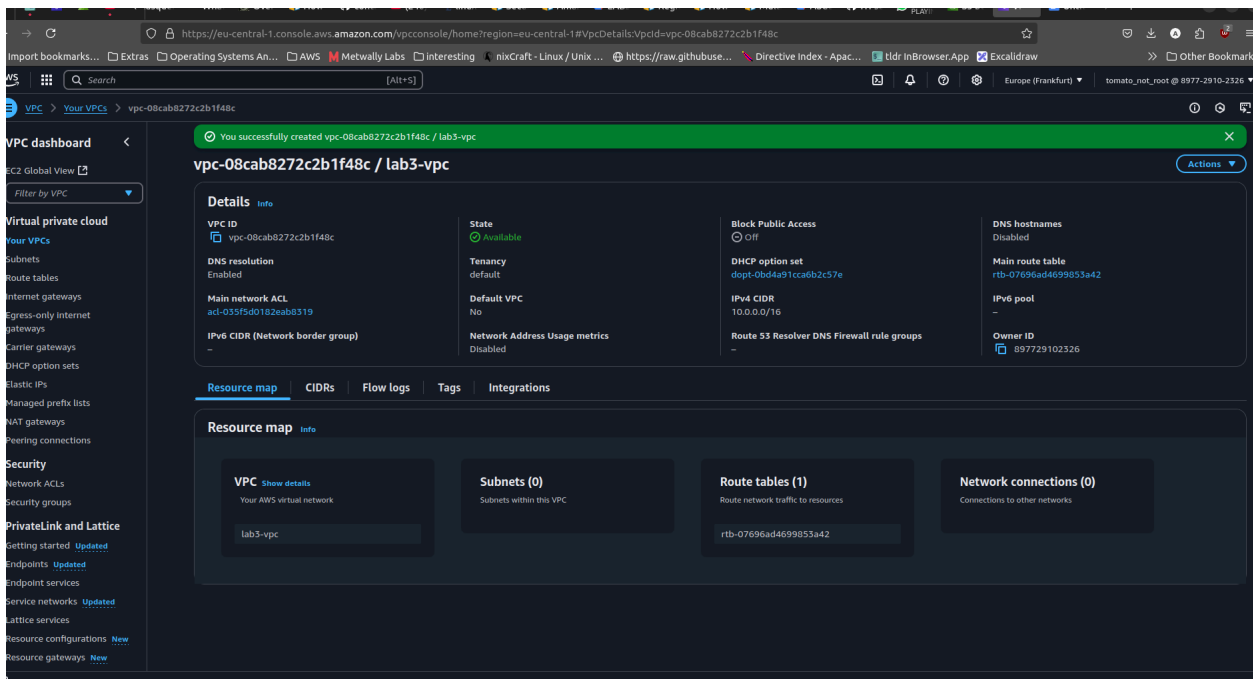
And we can finally access it using the domain name/index.html

Q2:

The solution of question 2 is the same terraform code as Lab2 Q2 but with modifyng the autoscaling number to 4 instead of 2 and the code could be found at:

<https://github.com/abdurahmanalaa123/ITI-sessions/tree/master/AWS/Lab2>

Q3: create a vpc



Create a private subnet

→ <https://eu-central-1.console.aws.amazon.com/vpcconsole/home?region=eu-central-1#CreateSubnet>

Import bookmarks... Extras Operating Systems An... AWS Metwally Labs Interesting nixCraft - Linux / Unix ... https://raw.githubuse... Directive index - Apac... tldr inBrowser.App Excalidraw Other Bookmark

Search [Alt+S]

VPC > Subnets > Create subnet

vpc-08cab8272c2b1f48c (lab3-vpc)

Associated VPC CIDRs

IPv4 CIDRs  
10.0.0.0/16

Subnet settings  
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name  
Create a tag with a key of 'Name' and a value that you specify.  
private-subnet  
The name can be up to 256 characters long.

Availability Zone info  
Choose the zone in which your subnet will reside, or let Amazon choose one for you.  
No preference

IPv4 VPC CIDR block info  
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.  
10.0.0.0/16

IPv4 subnet CIDR block  
10.0.2.0/24 256 IPs

Tags - optional

Key Value - optional

Q Name X private-subnet X Remove

Add new tag

→ <https://eu-central-1.console.aws.amazon.com/vpcconsole/home?region=eu-central-1#RouteTableDetails:RouteTableId=rtb-0da1aeb1fdd6e912b>

Import bookmarks... Extras Operating Systems An... AWS Metwally Labs Interesting nixCraft - Linux / Unix ... https://raw.githubuse... Directive index - Apac... tldr inBrowser.App Excalidraw Other Bookmark

Search [Alt+S]

VPC > Route tables > rtb-0da1aeb1fdd6e912b

VPC dashboard <

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only Internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Security

Network ACLs

Security groups

PrivateLink and Lattice

Getting started Updated

Endpoints Updated

Endpoint services

Service networks Updated

Lattice services

Resource configurations New

Resource gateways New

Route table rtb-0da1aeb1fdd6e912b | private-route-table was created successfully.

rtb-0da1aeb1fdd6e912b / private-route-table Actions

Details info

Route table ID  
rtb-0da1aeb1fdd6e912b

Main  
No

Explicit subnet associations  
-

Edge associations  
-

VPC  
vpc-08cab8272c2b1f48c | lab3-vpc

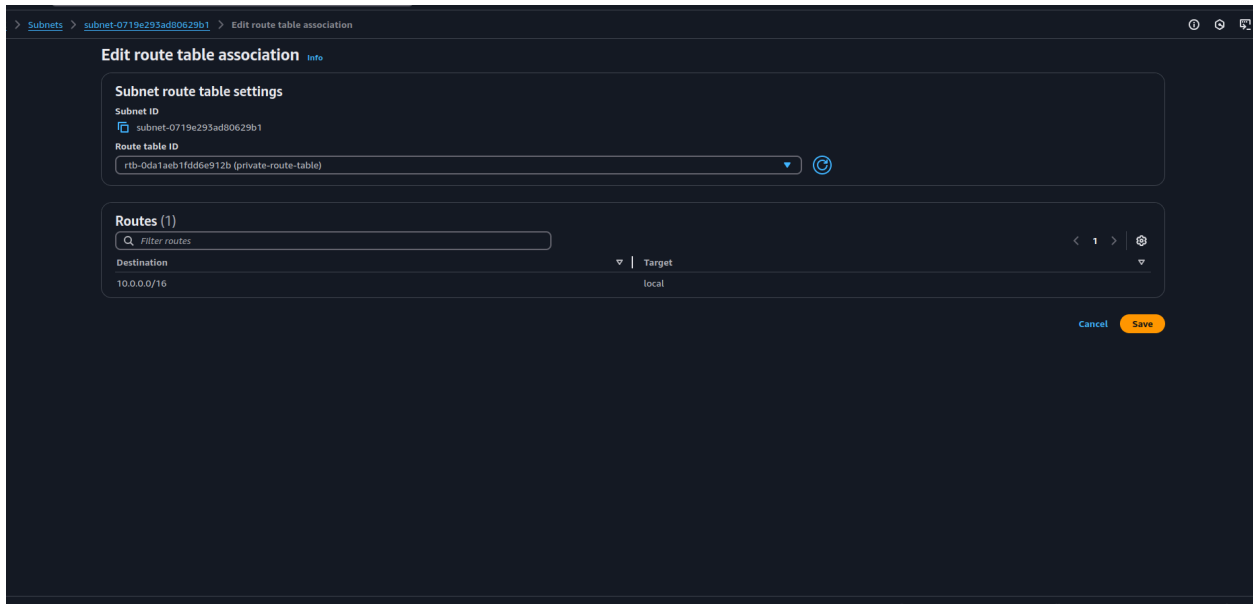
Owner ID  
897729102326

Routes Subnet associations Edge associations Route propagation Tags

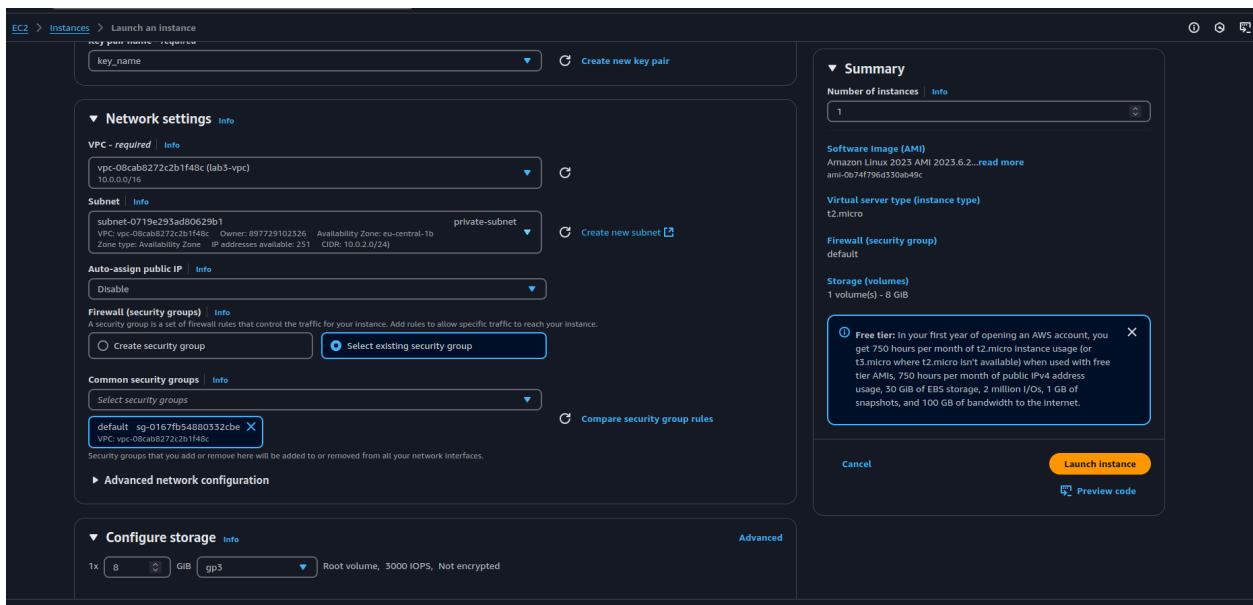
Routes (1)

Filter routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No



Associate the route table with the subnet



Need to give the ec2 instance a role to be able to access the s3 and systems session manager to be able to ssh into it

**IAM instance profile** | [Info](#)

allow-ssm-s3-ec2  
arn:aws:iam::897729102326:instance-profile/allow-ssm-s3-ec2 ▼

**Hostname type** | [Info](#)

IP name ▼

**DNS Hostname** | [Info](#)

- ☒ Enable IP name IPv4 (A record) DNS requests
- ☒ Enable resource-based IPv4 (A record) DNS requests
- ☐ Enable resource-based IPv6 (AAAA record) DNS requests

**Instance auto-recovery** | [Info](#)

And the user-data for installing apache

```
#!/bin/bash
sudo yum update -y
sudo yum install -y httpd
systemctl start httpd
systemctl enable httpd
chmod 644 /var/www/html/index.html
systemctl restart httpd
```

Create a vpc endpoint and attach it to the private subnet that the ec2 is located inside and its directly added to the route table

VPC > Endpoints > Create endpoint

Create endpoint

Info

Create the type of VPC endpoint that supports the service, service network or resource to which you want to connect.

Endpoint settings

Specify a name and select the type of endpoint.

Name tag - optional

Creates a tag with a key of 'Name' and a value that you specify. Tags help you find and manage your endpoint.

ec2-43-endpoint

Type

Info

Select a category

☒ AWS services

Connect to services provided by Amazon with an interface endpoint, or a Gateway endpoint

☐ PrivateLink Ready partner services

Connect to SaaS services which have AWS Service Ready designation with an interface endpoint. Uses AWS PrivateLink

☐ AWS Marketplace services

Connect to SaaS services that you have purchased through AWS Marketplace with an interface Endpoint

☐ EC2 Instance Connect Endpoint

An elastic network interface that allow you to connect to resources in a private subnet

☐ Resources - New

Connect to resources like Amazon Relational Database Services (RDS) with a Resource endpoint. Uses AWS PrivateLink

☐ Service networks - New

Connect to VPC Lattice service networks with a Service network endpoint. Uses AWS PrivateLink

☐ Endpoint services that use NLBs and GWLBs

Find services shared with you by service name. Connect to a Network LoadBalancer (NLB) service with an interface endpoint or to a Gateway LoadBalancer (GWLB) service with a Gateway Load Balancer endpoint

Services (277)

Q Search

Service Name	Owner	Type	Service Region
<input type="radio"/> aws.apl.eu-central-1.emr-service-cell01	amazon	Interface	eu-central-1
<input type="radio"/> aws.sagemaker.eu-central-1.experiments	amazon	Interface	-
<input type="radio"/> aws.sagemaker.eu-central-1.notebook	amazon	Interface	-
<input type="radio"/> aws.sagemaker.eu-central-1.partner-app	amazon	Interface	eu-central-1
<input type="radio"/> aws.sagemaker.eu-central-1.studio	amazon	Interface	-

CloudShell

Feedback

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

VPC > Endpoints > Create endpoint

the service's default public endpoint DNS name. To use this feature, ensure that the attributes 'Enable DNS hostnames' and 'Enable DNS support' are enabled for your VPC.

DNS record IP type

☒ IPv4

☐ IPv6

☐ Dualstack

☐ Service defined

Subnets (1/3)

Info

☒ Availability Zone

Subnet ID

Designate IP addresses

IPv4 address

IPv6 address

☐ eu-central-1a (eu1-a22)

No subnet available

☒ eu-central-1b (eu1-a23)

subnet-0719e293ad80629b1

☐

☐ eu-central-1c (eu1-a21)

No subnet available

IP address type

☒ IPv4

☐ IPv6

☐ Dualstack

Security groups (1/1)

Info

Q Search

VPC ID : vpc-08cab8272c2b1f48c

Clear filters

☒ Group ID

Group name

VPC ID

Description

☒ sg-0167fb54080532cbe

default

vpc-08cab8272c2b1f48c

default VPC security group

sg-0167fb54080532cbe

Policy

Info

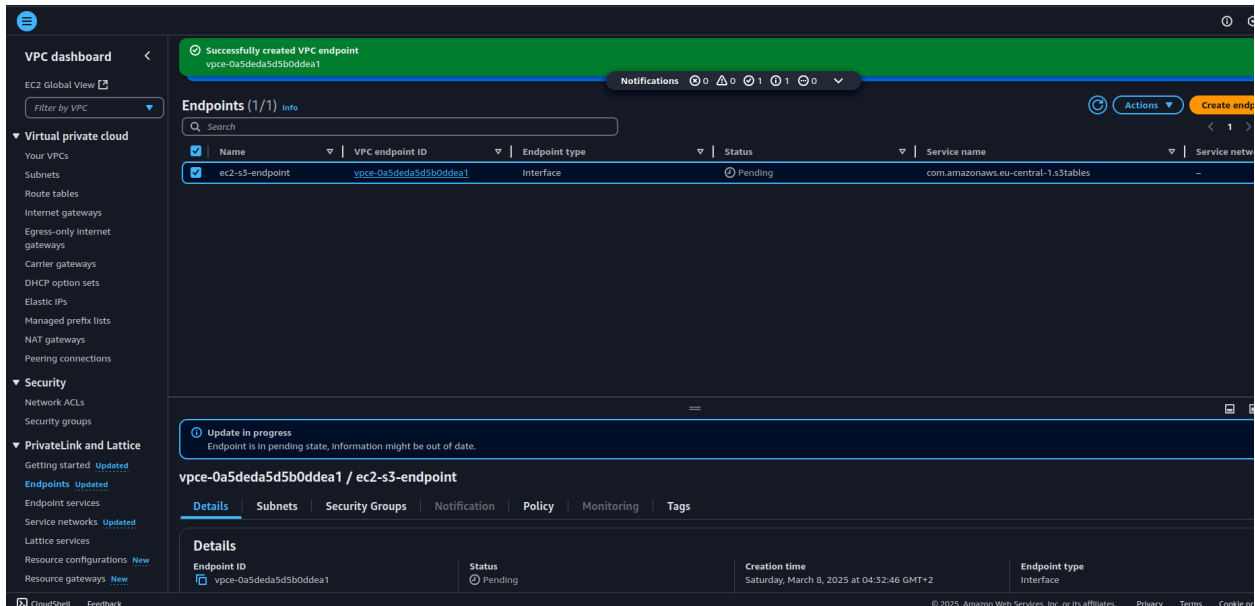
VPC endpoint policy controls access to the service.

CloudShell

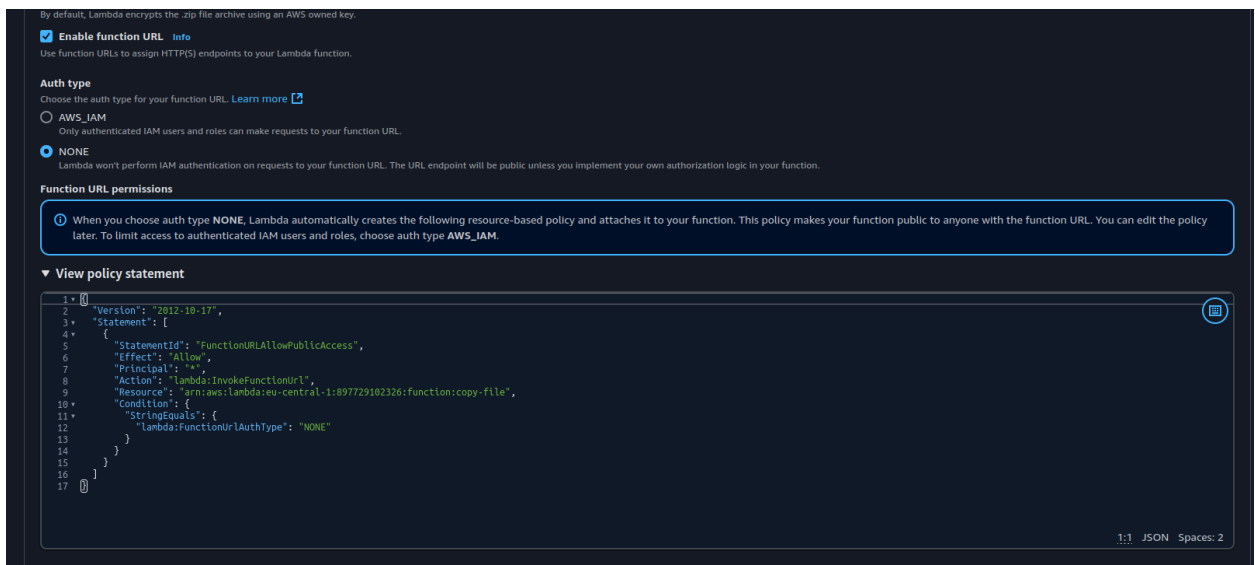
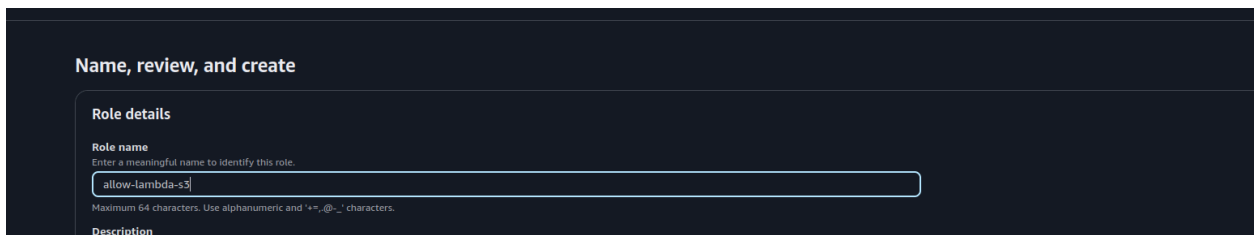
Feedback

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

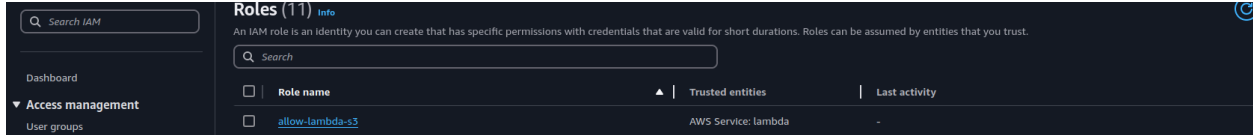




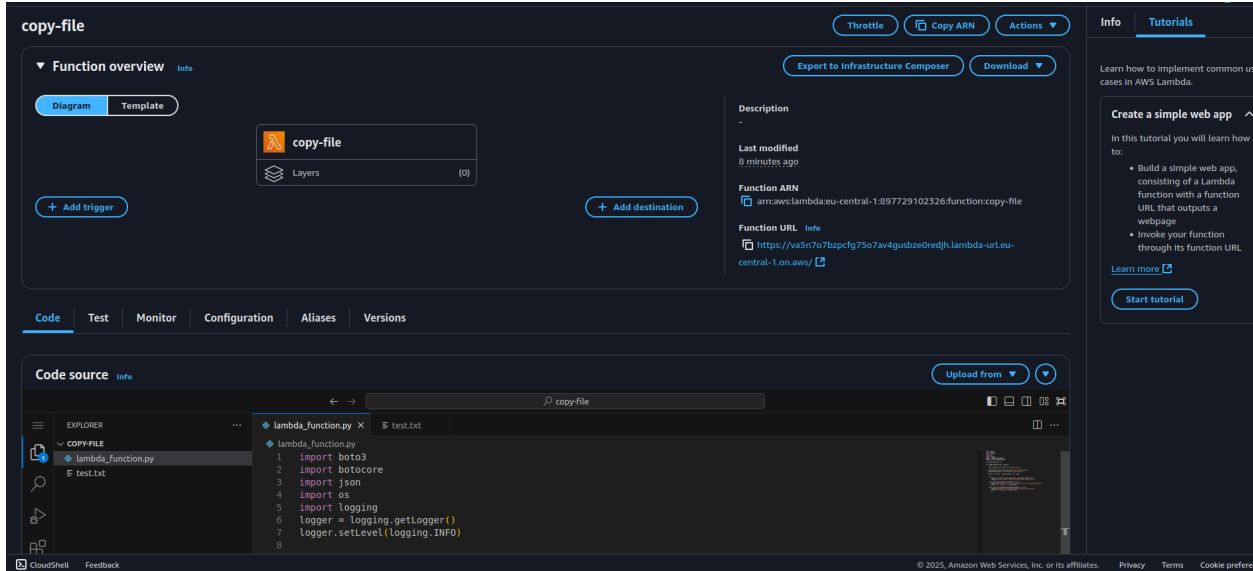
Q4: create a lambda function which uploads a file to an s3 bucket  
Create a role for the lambda function



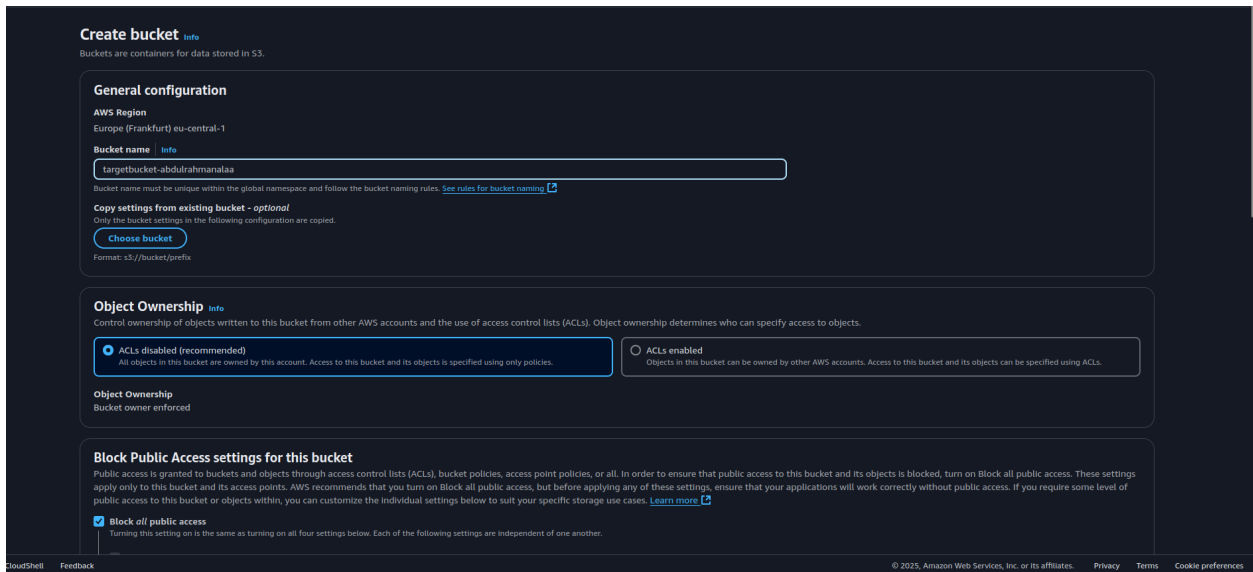
Assigning a function url for my lambda to enable programmatic invoking  
And create a role for the lambda to enable s3 access

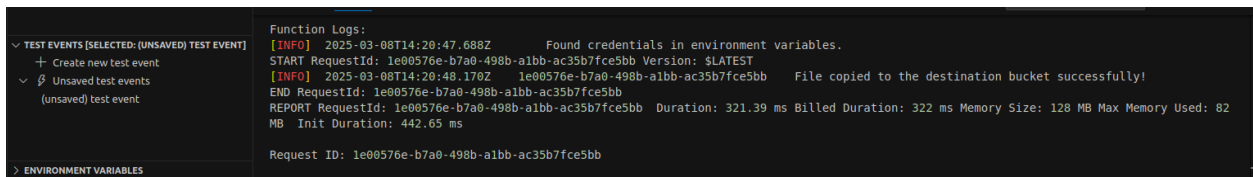
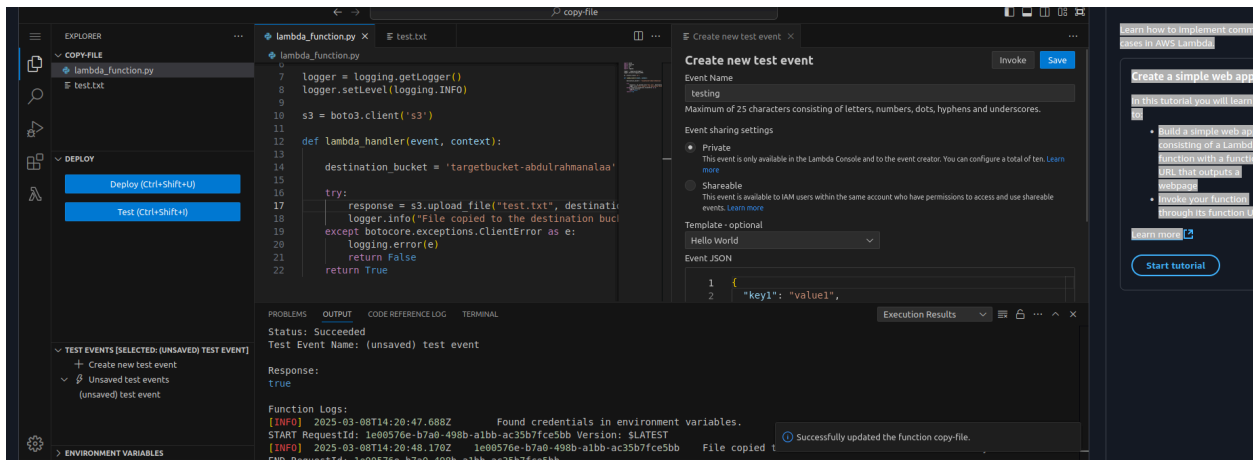
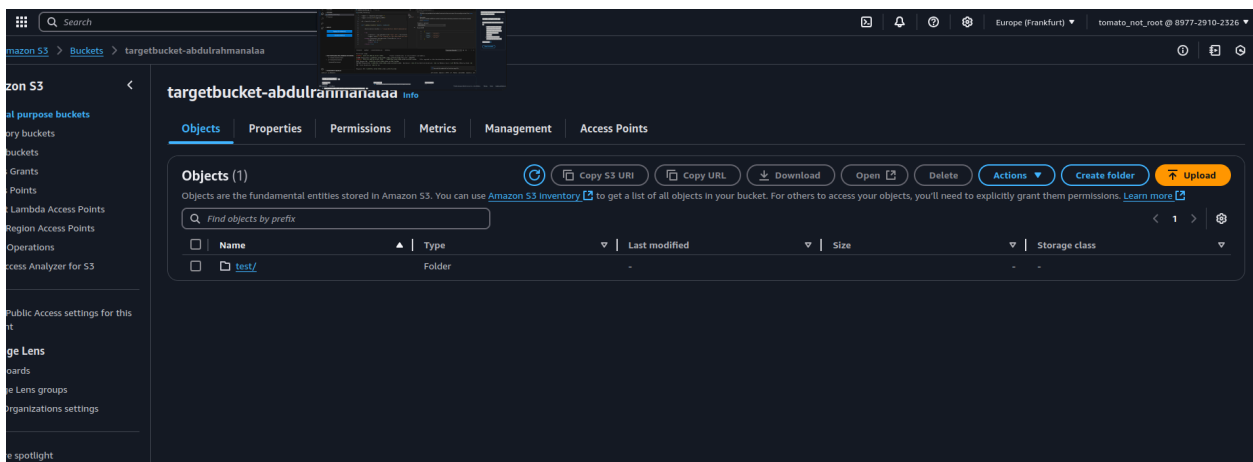
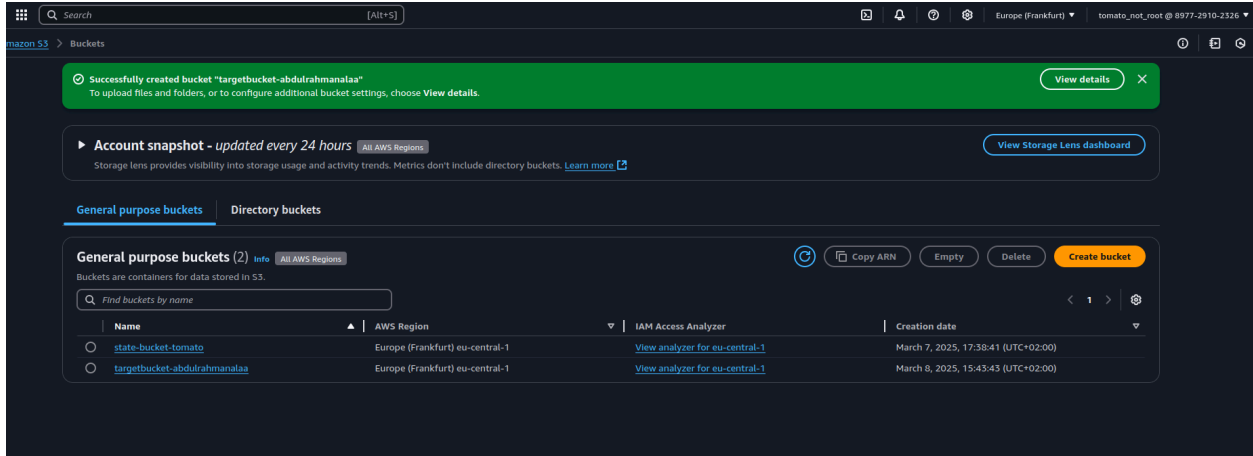


Create the function attached the role configured for public access

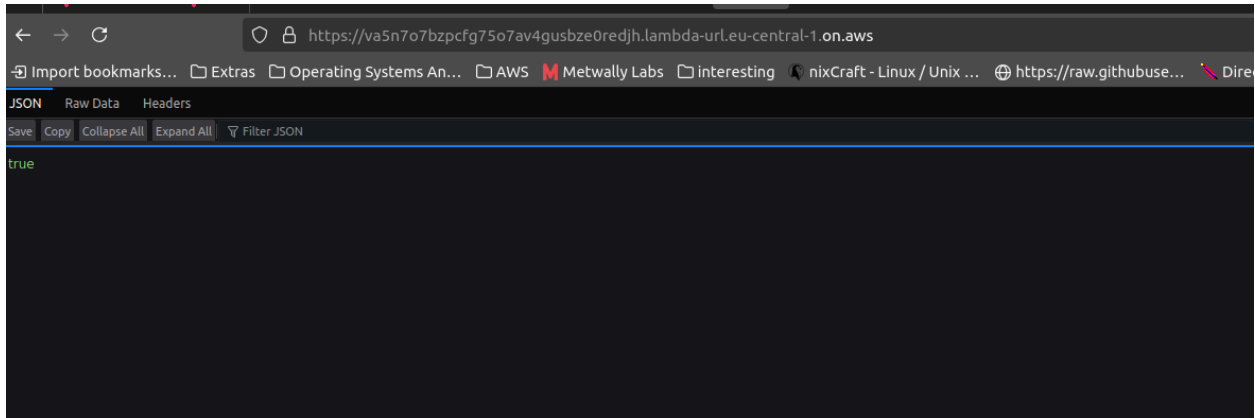


Now create the s3 bucket fo storing my test file

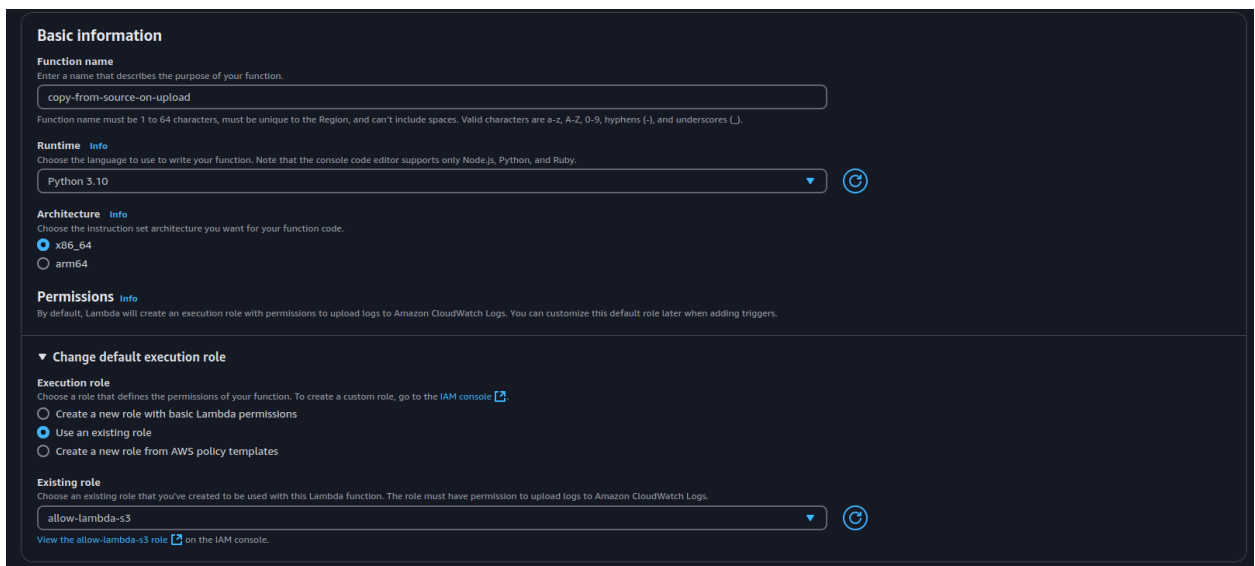
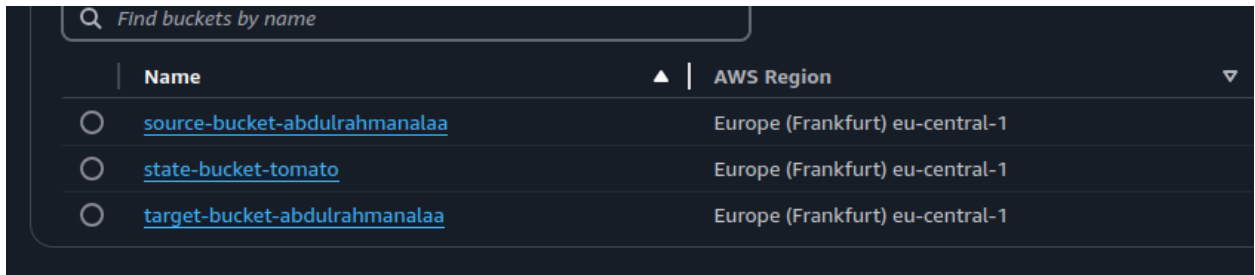




Running the test event we can see that the text file is copied inside the bucket with the proper credentials available on the lambda and can be publicly invoked using the function's link



Q5: create a lambda function triggered on s3 to copy file from bucket to another  
Create the source-bucket-abdulrahmanalaa  
Create the target-bucket-abdulrahmanalaa



Attaching a trigger on the source s3 bucket

### Trigger configuration Info

s3

aws asynchronous storage

#### Bucket

Choose or enter the ARN of an S3 bucket that serves as the event source. The bucket must be in the same region as the function.

✕ 🔄

Bucket region: eu-central-1

#### Event types

Select the events that you want to have trigger the Lambda function. You can optionally set up a prefix or suffix for an event. However, for each bucket, individual events cannot have multiple configurations with overlapping prefixes or suffixes that could match the same object key.

All object create events ✕

#### Prefix - optional

Enter a single optional prefix to limit the notifications to objects with keys that start with matching characters. Any [special characters](#) must be URL encoded.

#### Suffix - optional

Enter a single optional suffix to limit the notifications to objects with keys that end with matching characters. Any [special characters](#) must be URL encoded.

#### Recursive invocation

If your function writes objects to an S3 bucket, ensure that you are using different S3 buckets for input and output. Writing to the same bucket increases the risk of creating a recursive invocation, which can result in increased Lambda usage and increased costs. [Learn more](#)

☒ I acknowledge that using the same S3 bucket for both input and output is not recommended and that this configuration can cause recursive invocations, increased Lambda usage, and increased costs.

Lambda will add the necessary permissions for AWS S3 to invoke your Lambda function from this trigger. [Learn more](#) about the Lambda permissions model.

🔍 Successfully updated the function **copy-from-source-on-upload**.

← →

copy-from-source-on-upload

🔍 📄 📁 ⚙️

EXPLORER

📁 COPY-FROM-SOURCE-ON-UPLOAD

📄 lambda\_function.py

DEPLOY

Deploy (Ctrl+Shift+U)

Test (Ctrl+Shift+I)

TEST EVENTS (NONE SELECTED)

+ Create new test event

lambda\_function.py

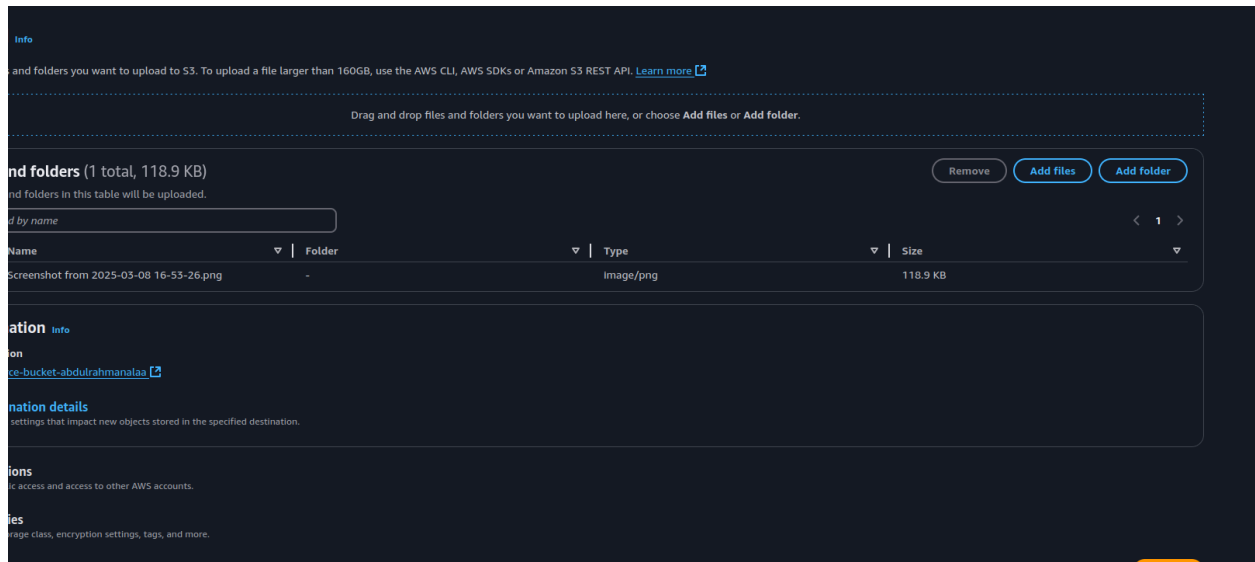
```

1  import boto3
2  import boto3
3  import json
4  import os
5  import logging
6  logger = logging.getLogger()
7  logger.setLevel(logging.INFO)
8
9  s3 = boto3.resource('s3')
10
11
12 def lambda_handler(event, context):
13     logger.info("New files uploaded to the source bucket.")
14
15     key = event['Records'][0]['s3']['object']['key']
16
17     source_bucket = event['Records'][0]['s3']['bucket']['name']
18     destination_bucket = 'target-bucket-abdulrahmanalaa'
19
20     source = {'Bucket': source_bucket, 'Key': key}
21
22     try:
23         response = s3.meta.client.copy(source, destination_bucket, key)
24         logger.info("File copied to the destination bucket successfully!")
25
26     except botocore.exceptions.ClientError as error:
27         logger.error("There was an error copying the file to the destination bucket")
28         print('Error Message: {}'.format(error))
29
30     except botocore.exceptions.ParamValidationError as error:
31         logger.error("Missing required parameters while calling the API.")

```

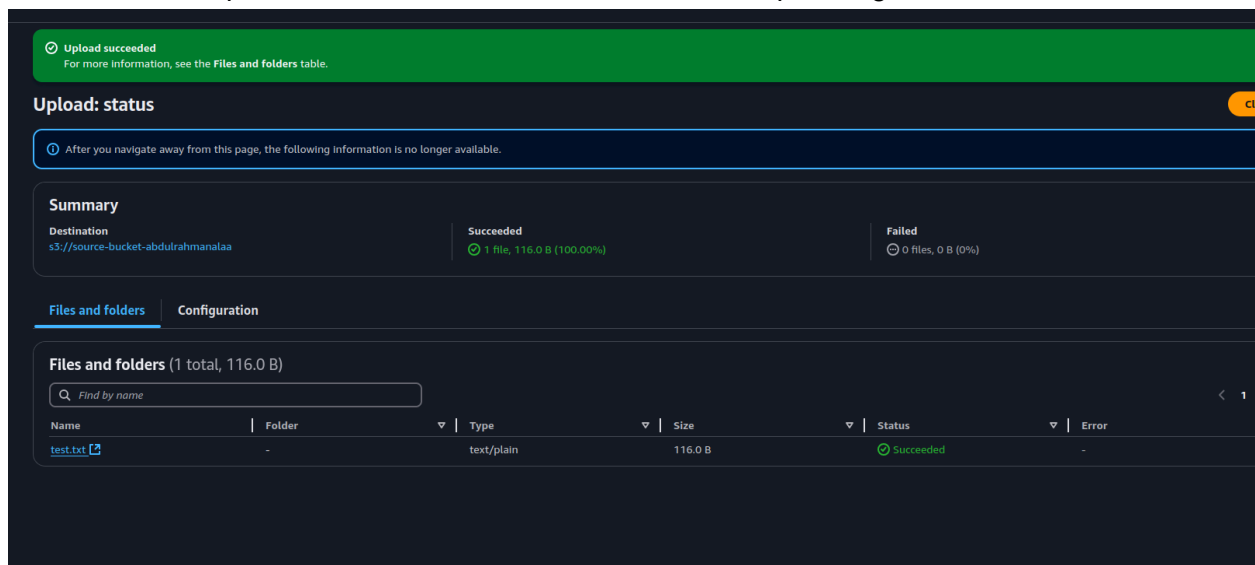
The code for copying form the source bucket to the target bucket

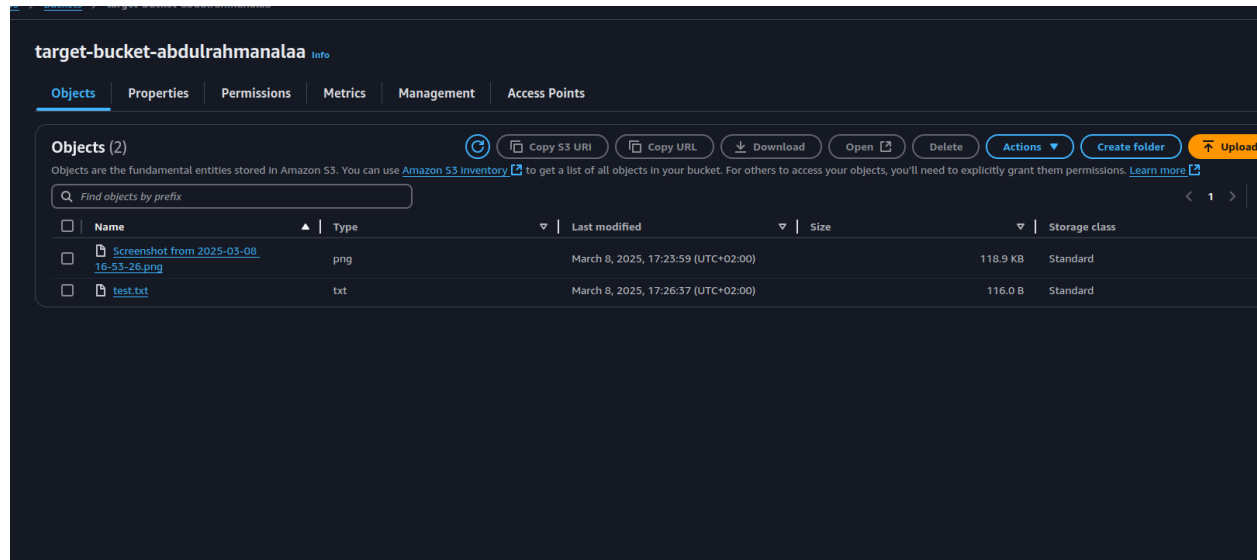
Now adding a file to the source-bucket



Uploading an image to the source bucket

You can see its uploaded due to the test function ran after uploading the test file





The code can be found in  
<https://github.com/abdulrahmanalaa123/ITI-sessions/tree/master/AWS/Lab3>