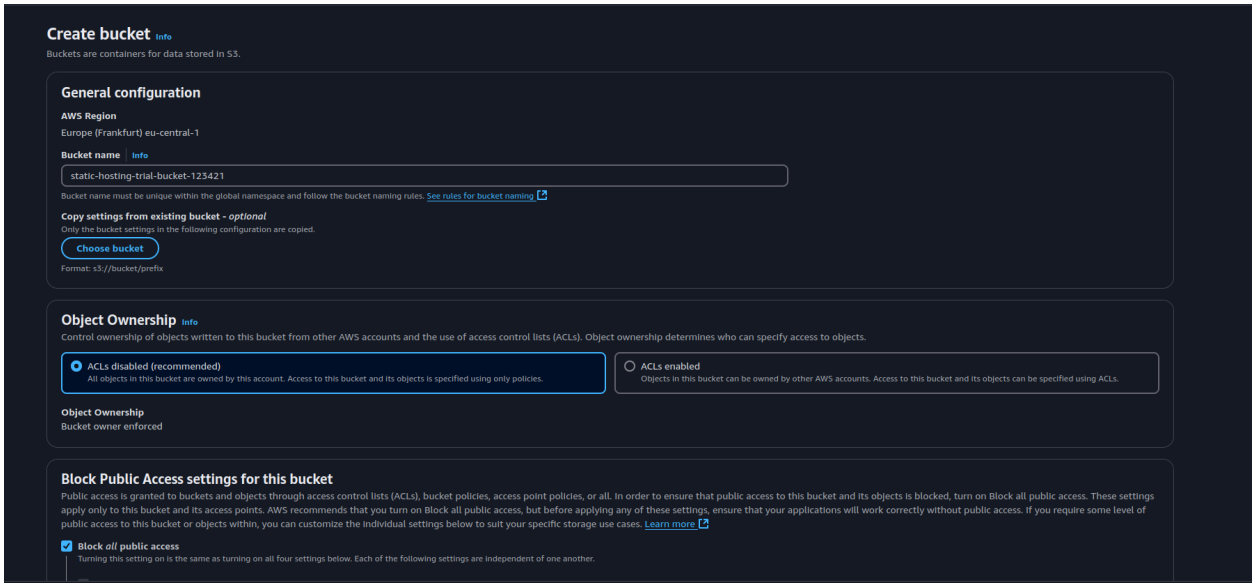
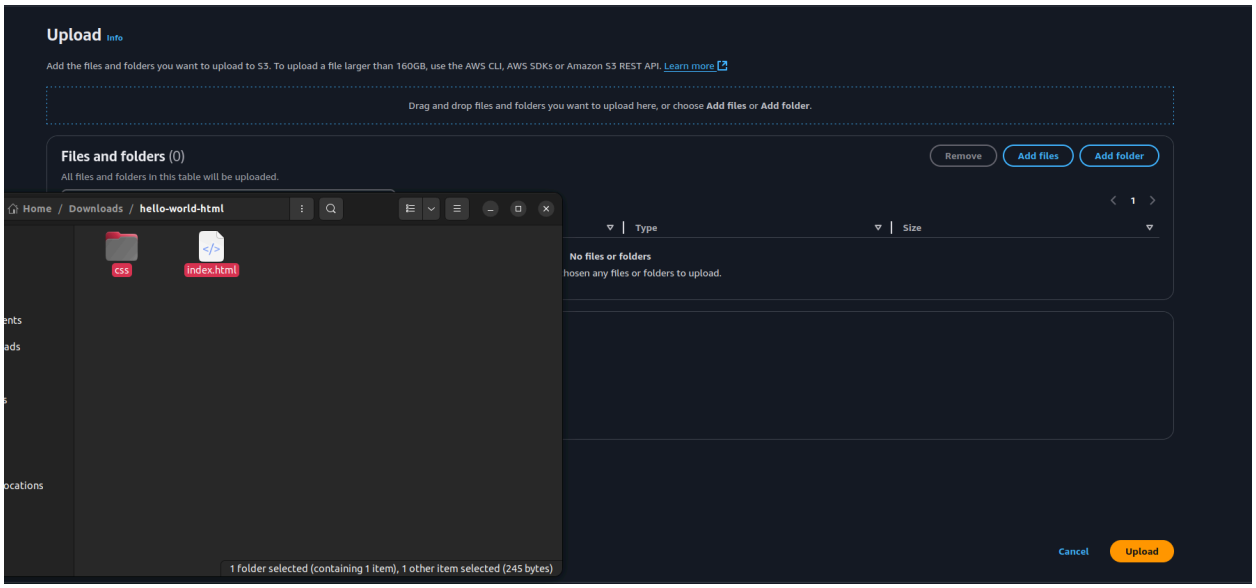
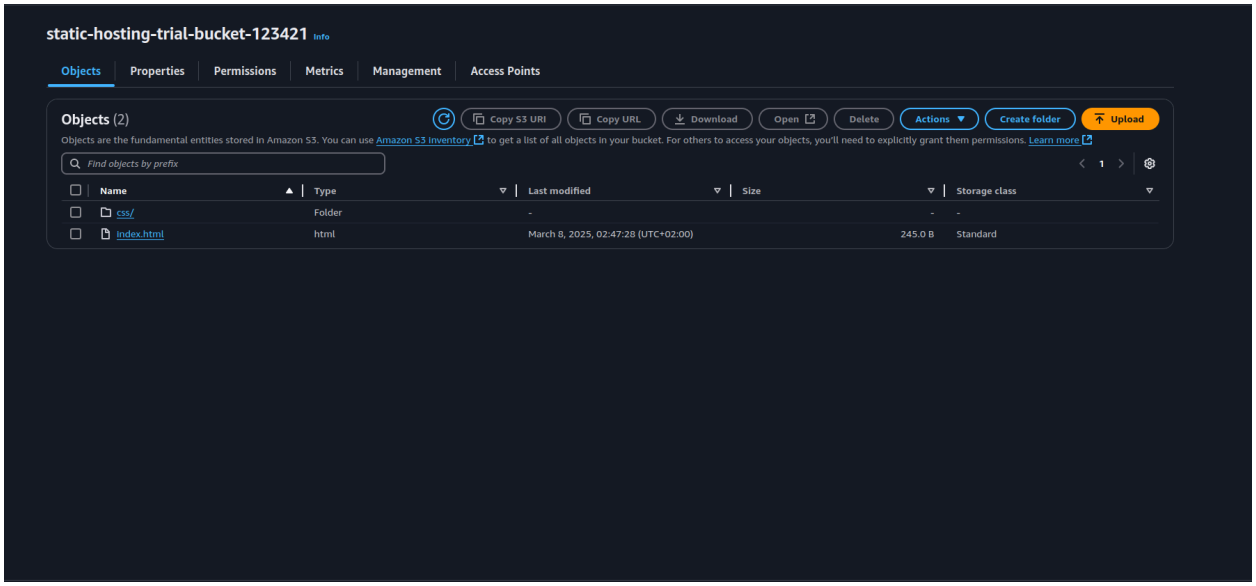
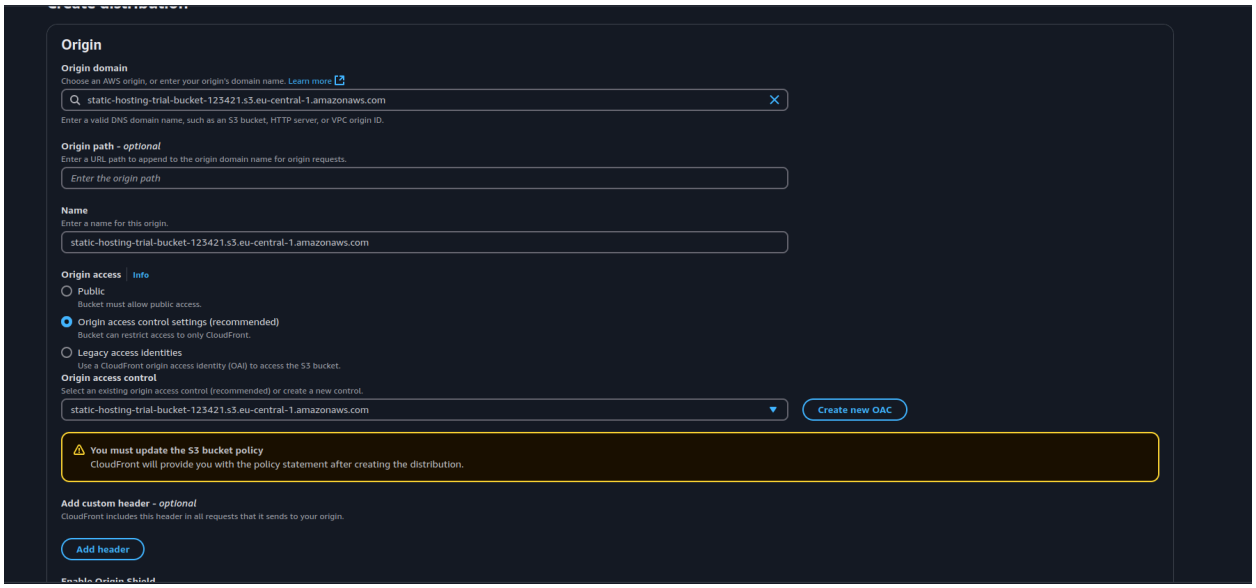
Q1: serve s3 from cloudfront with blocked access to s3

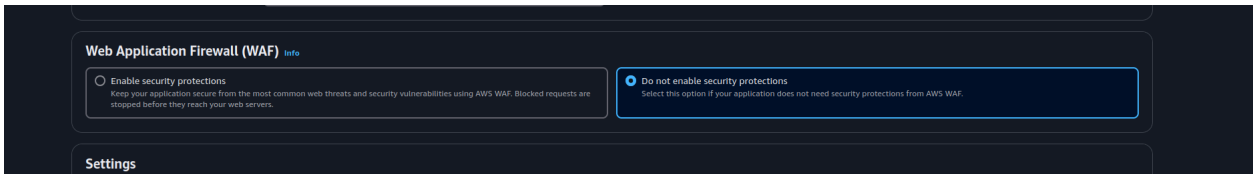




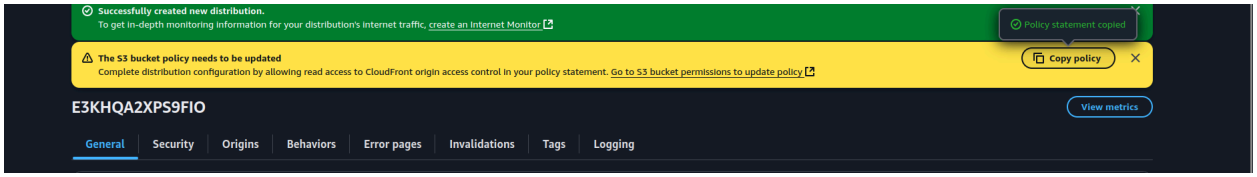


In the cloudfront page

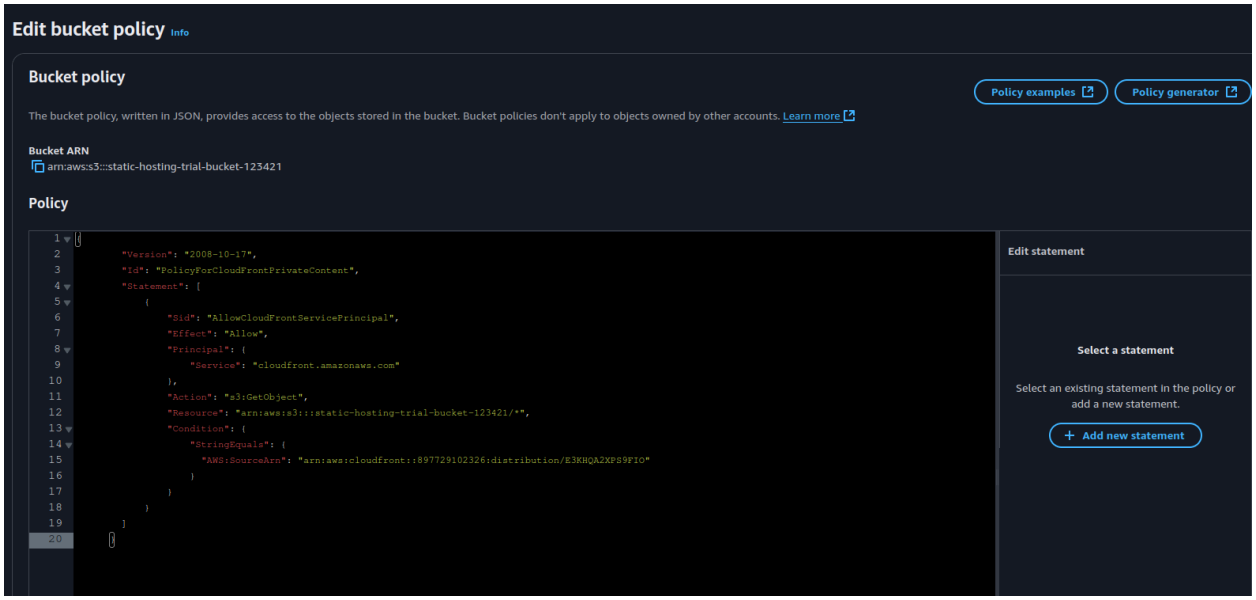


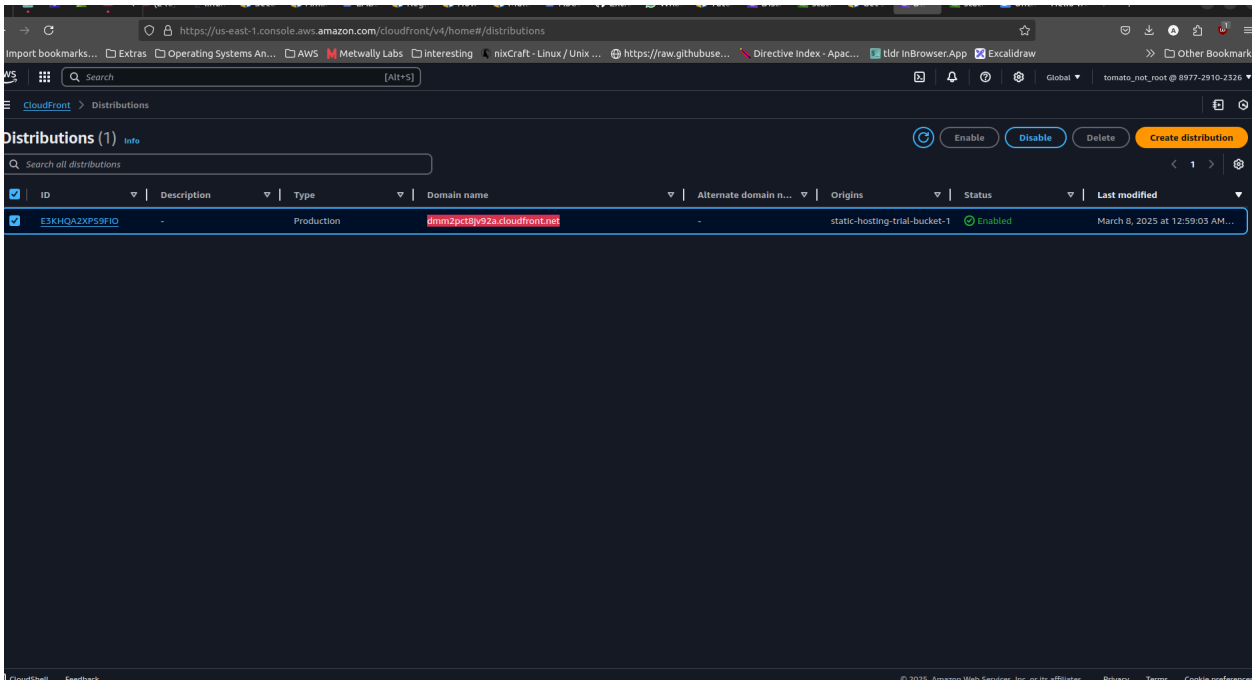


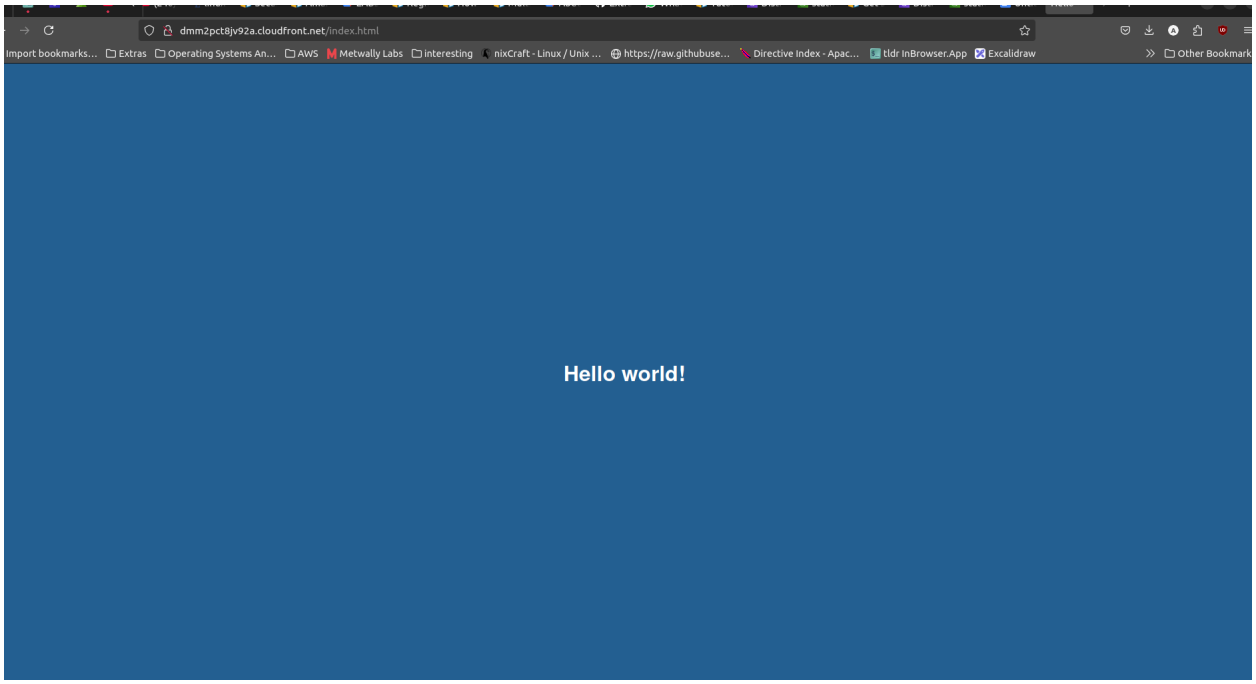
And the rest the default config was used



Copying the policy


Edit bucket policy Info
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
{
"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/E3KHQA2XPS9FIO"
}
}
}
]
}
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
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]
Global
tomato_not_root @ 8977-2910-2326
CloudFront > Distributions
Distributions (1) Info
Enable
Disable
Delete
Create distribution
Search all distributions
ID
Description
Type
Domain name
Alternate domain n...
Origins
Status
Last modified
E3KHQA2XPS9FIO
-
Production
dmm2pct8jv92a.cloudfront.net
-
static-hosting-trial-bucket-1
Enabled
March 8, 2025 at 12:59:03 AM...

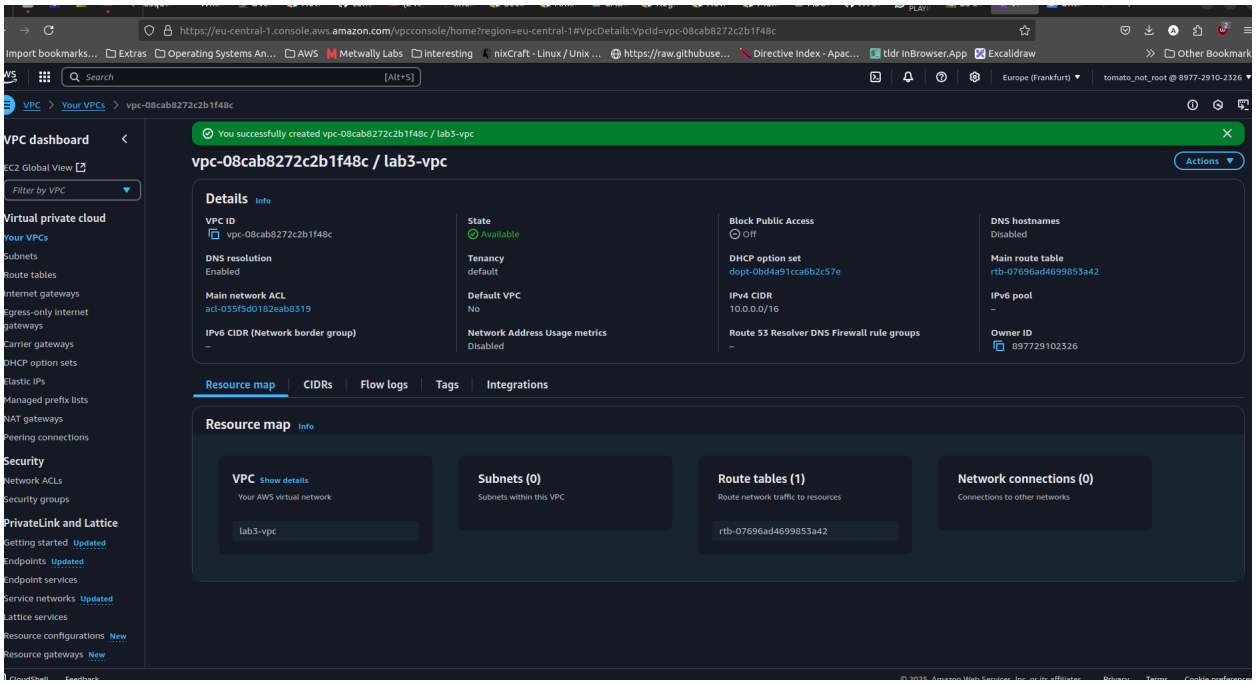


And we can finally access it using the domain name/index.html

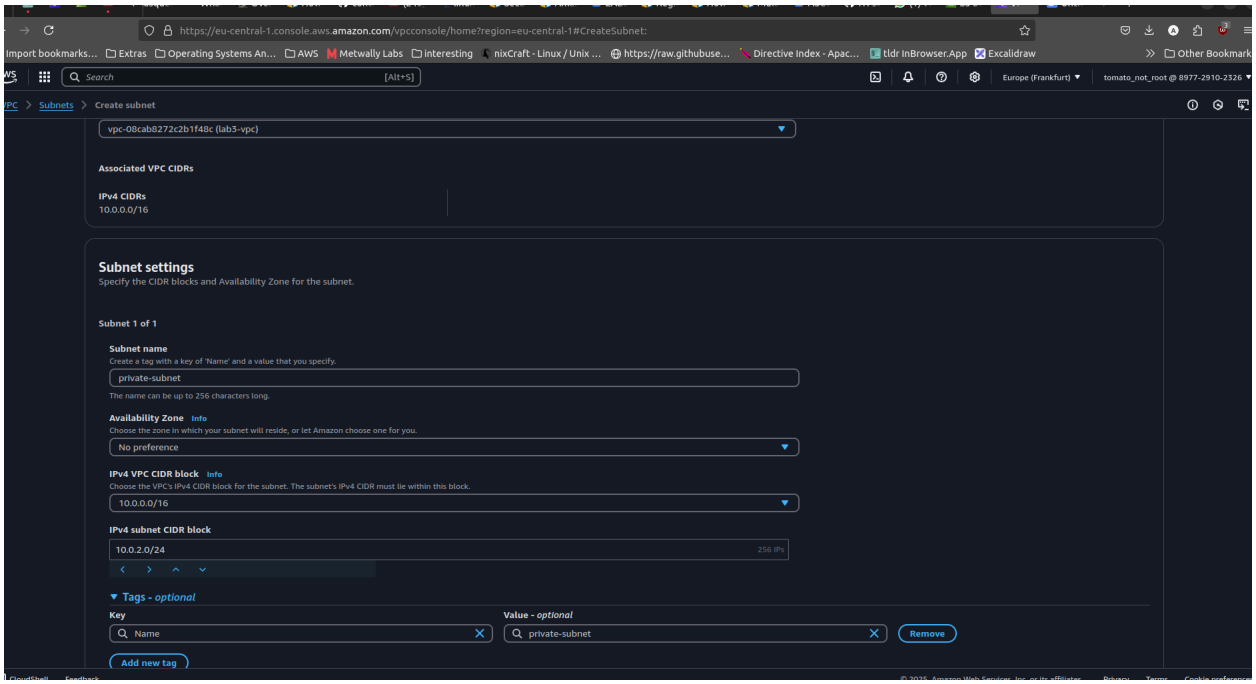
Q2:

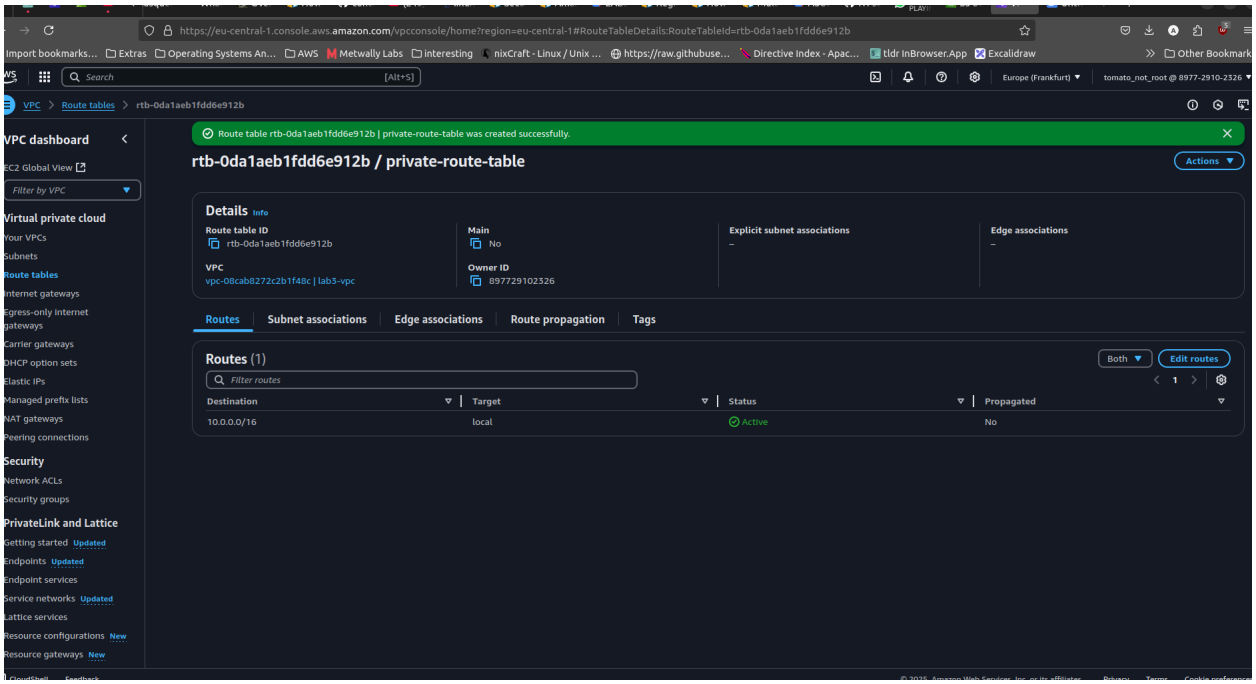
The solution of question 2 is the same terraform code as Lab2 Q2 but with modifynig the autoscaling number to 4 instead of 2 and the code could be found at: https://github.com/abdulrahmanalaa123/ITI-sessions/tree/master/AWS/Lab2

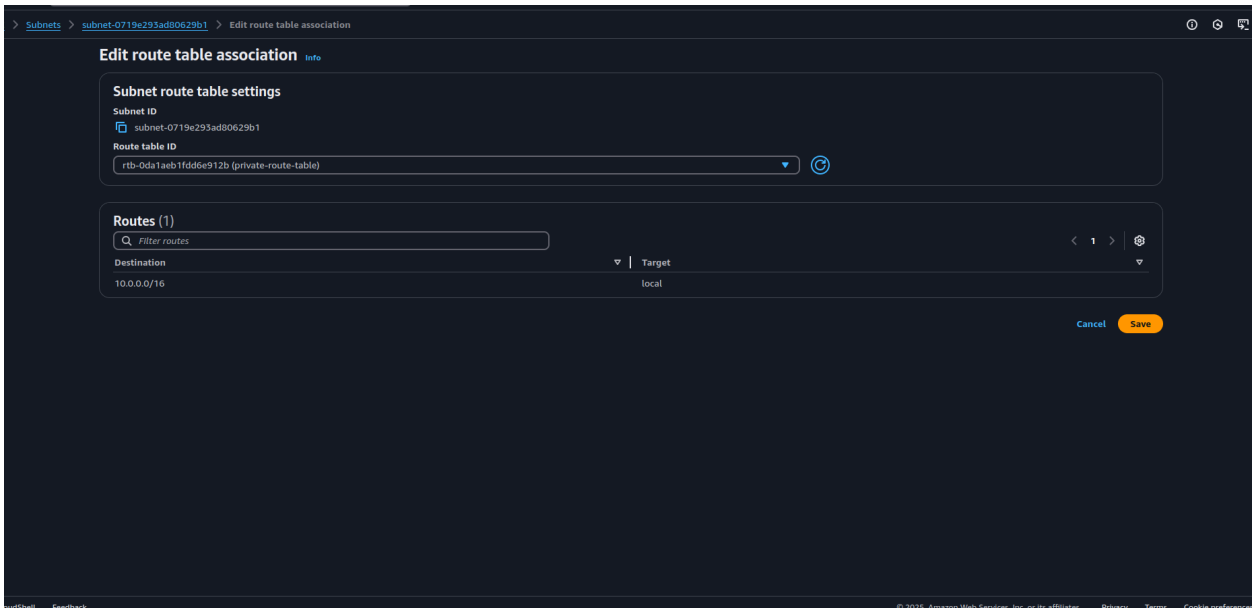
Q3: create a vpc



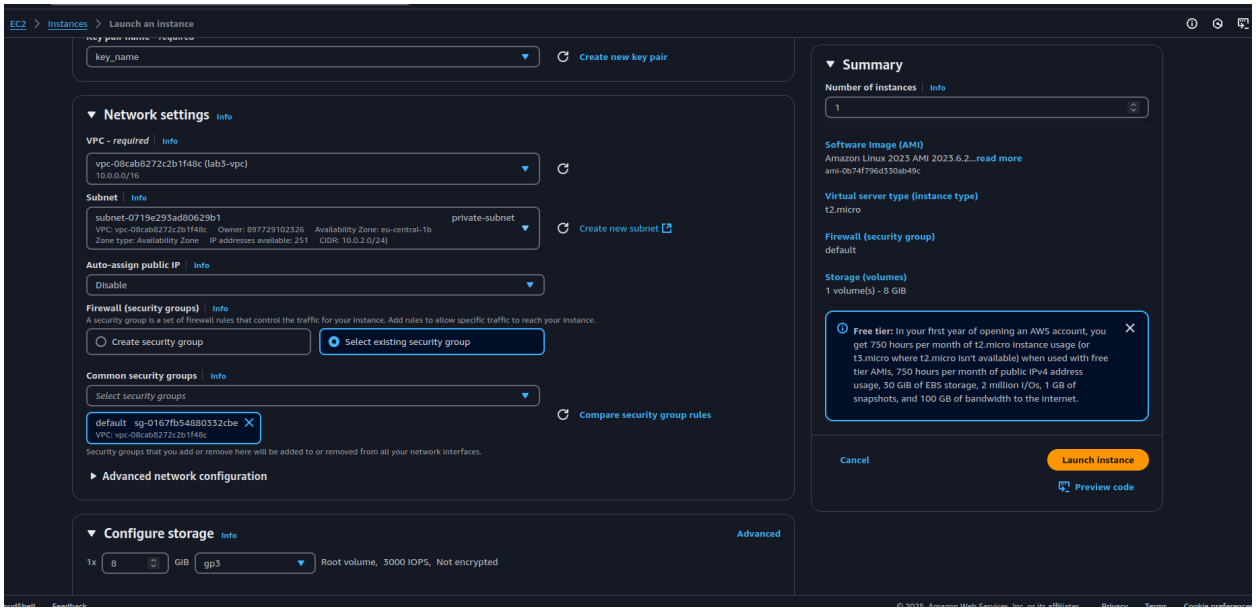
Create a private subnet


https://eu-central-1.console.aws.amazon.com/vpcconsole/home?region=eu-central-1#CreateSubnet:
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
Name
private-subnet
Remove
Add new tag

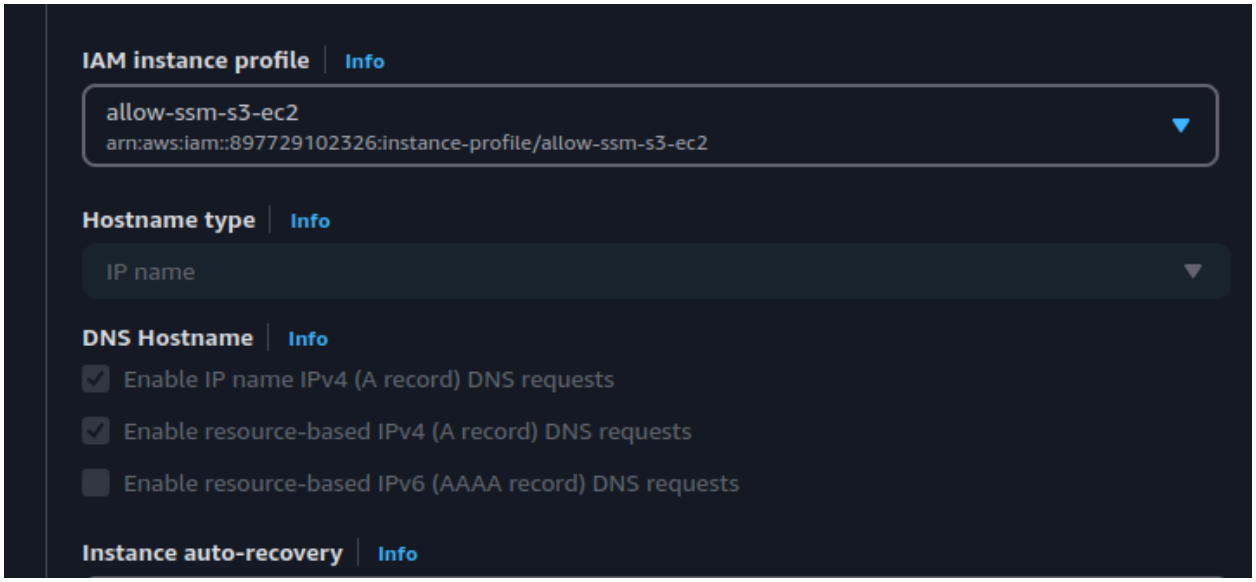

https://eu-central-1.console.aws.amazon.com/vpcconsole/home?region=eu-central-1#RouteTableDetails:RouteTableId=rtb-0da1aeb1fdd6e912b
VPC > Route tables > rtb-0da1aeb1fdd6e912b
Route table rtb-0da1aeb1fdd6e912b | private-route-table was created successfully.
rtb-0da1aeb1fdd6e912b / private-route-table
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
Both
Edit routes
Destination
Target
Status
Propagated
10.0.0.0/16
local
Active
No
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



Associate the route table with the subnet

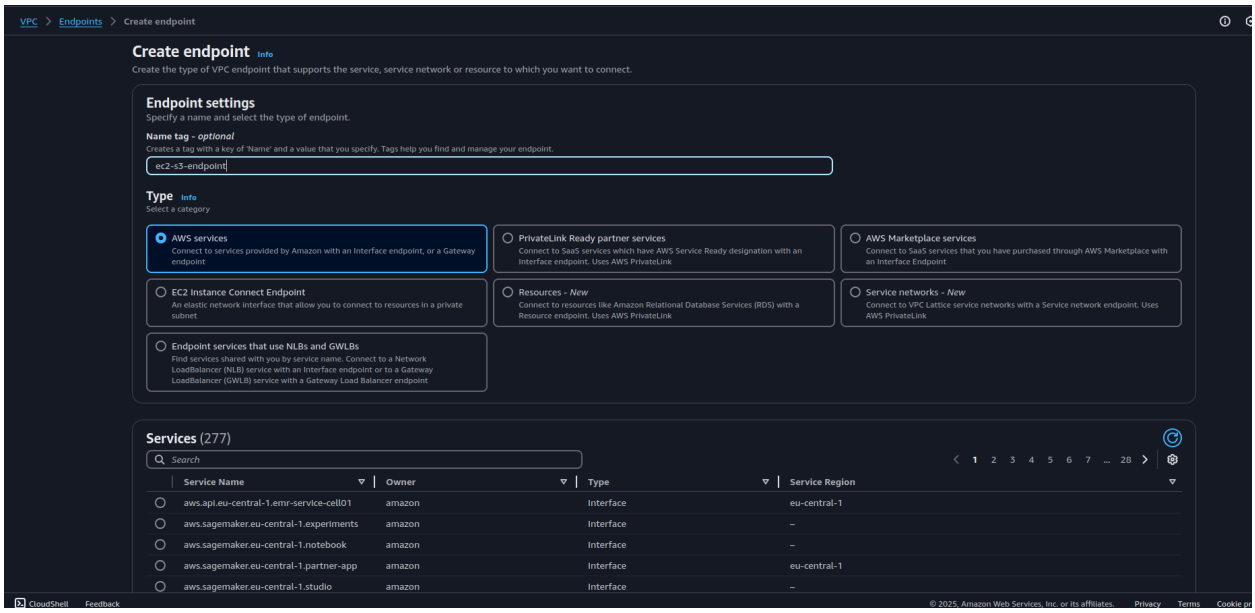


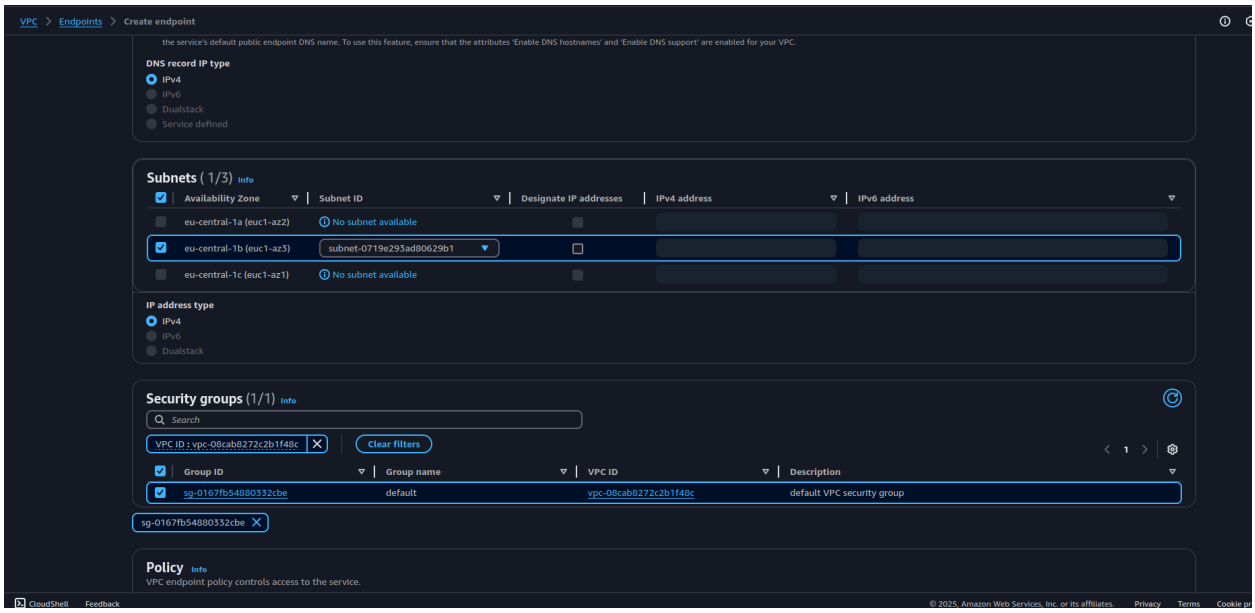
Need to give the ec2 instance a role to be able to access the s3 and systems session manager to be able to ssh into it

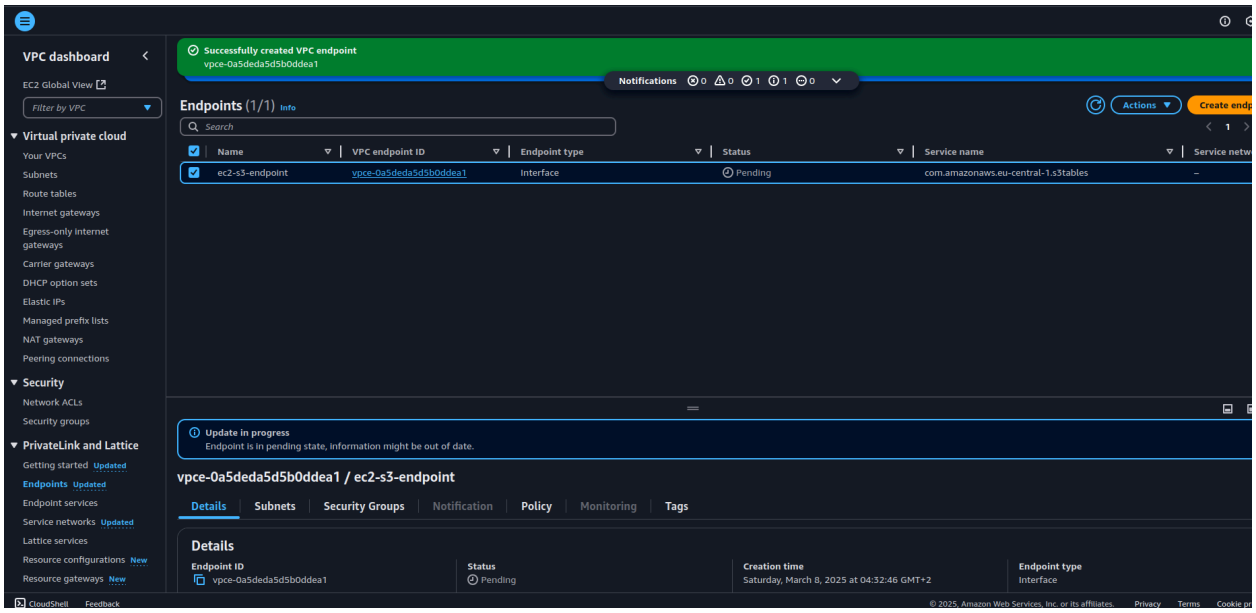


And the user-data for installing apache

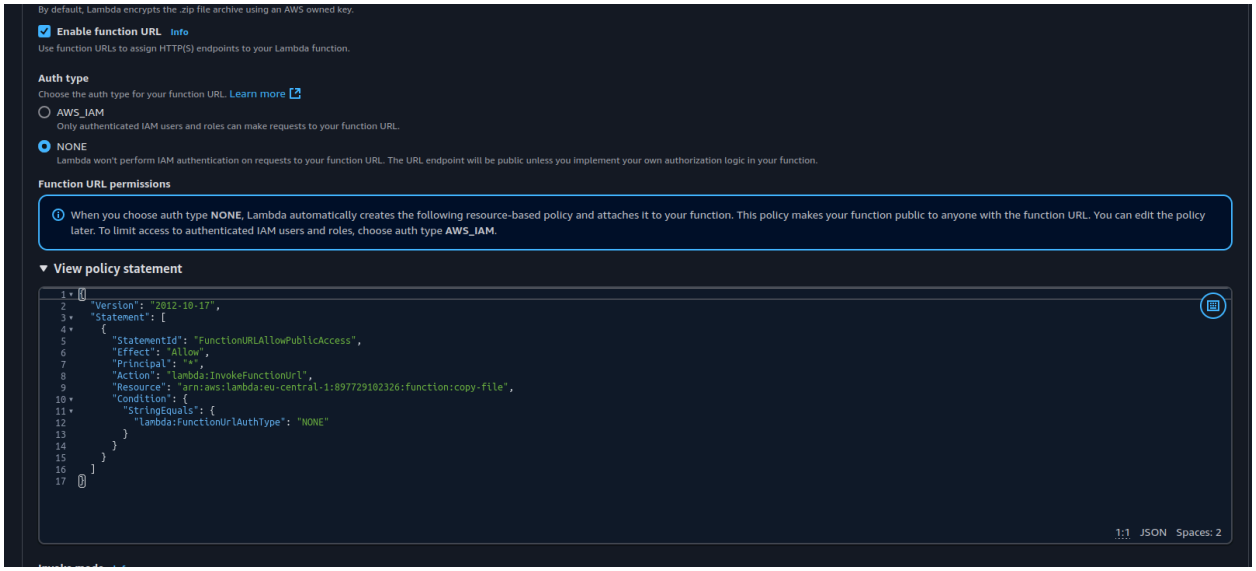
Create a vpc endpoint and attach it to the private subnet that the ec2 is located inside and its directly added to the route table


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-s3-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)
Search
1 2 3 4 5 6 7 ... 28
Service Name
Owner
Type
Service Region
aws.api.eu-central-1.emr-service-cell01 amazon Interface eu-central-1
aws.sagemaker.eu-central-1.experiments amazon Interface –
aws.sagemaker.eu-central-1.notebook amazon Interface –
aws.sagemaker.eu-central-1.partner-app amazon Interface eu-central-1
aws.sagemaker.eu-central-1.studio amazon Interface –
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie pr

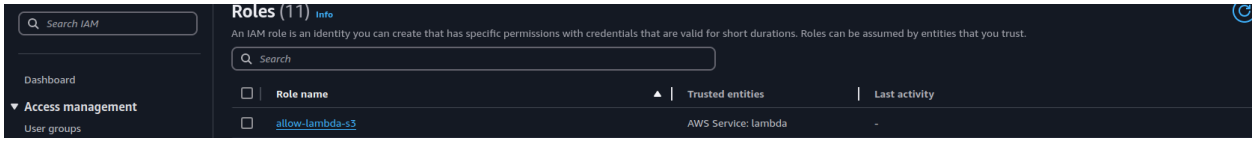

VPC > Endpoints > Create endpoint
the service's default public endpoint DNS name. To use this feature, ensure that the attributes 'Enable DNS hostnames' and 'Enable DNS support' are enabled for your VPC.
DNS record IP type
IPv4
IPv6
Dualstack
Service defined
Subnets (1/3) Info
Availability Zone
Subnet ID
Designate IP addresses
IPv4 address
IPv6 address
eu-central-1a (euc1-az2) No subnet available
eu-central-1b (euc1-az3) subnet-0719e293ad80629b1
eu-central-1c (euc1-az1) No subnet available
IP address type
IPv4
IPv6
Dualstack
Security groups (1/1) Info
Search
VPC ID : vpc-08cab8272c2b1f48c
Clear filters
1
Group ID
Group name
VPC ID
Description
sg-0167fb54880332cbe default vpc-08cab8272c2b1f48c default VPC security group
sg-0167fb54880332cbe
Policy Info
VPC endpoint policy controls access to the service.
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie pr



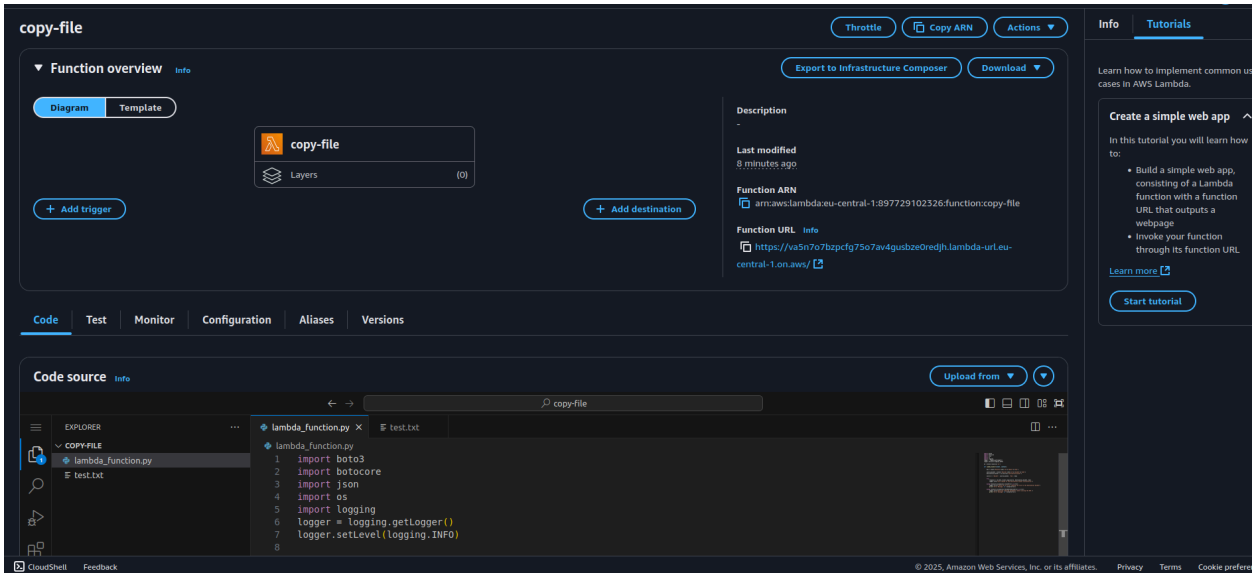
Q4: create a lambda function which uploads a file to an s3 bucket
Create a role for the lambda function



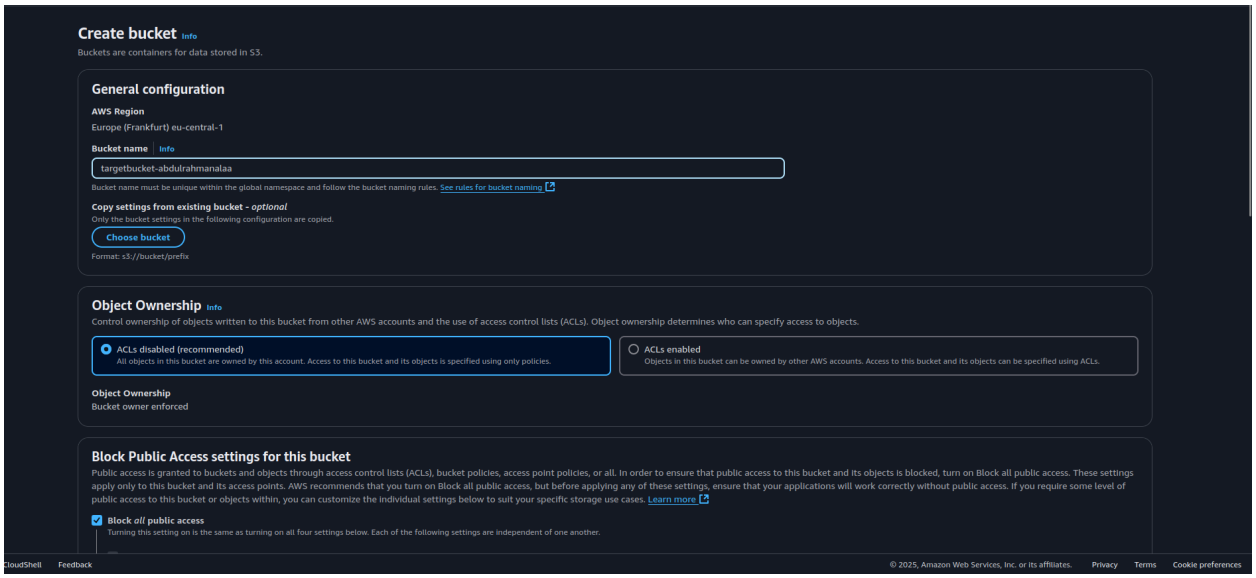
Assigning a function url for my lambda to enable programmatic invoking
And create a role for the lambda to enable s3 access

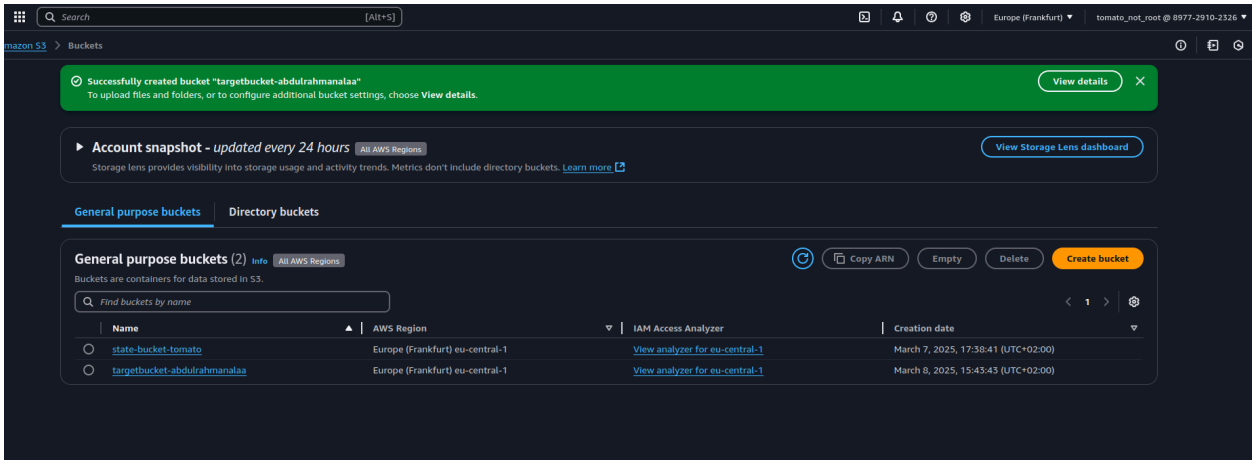


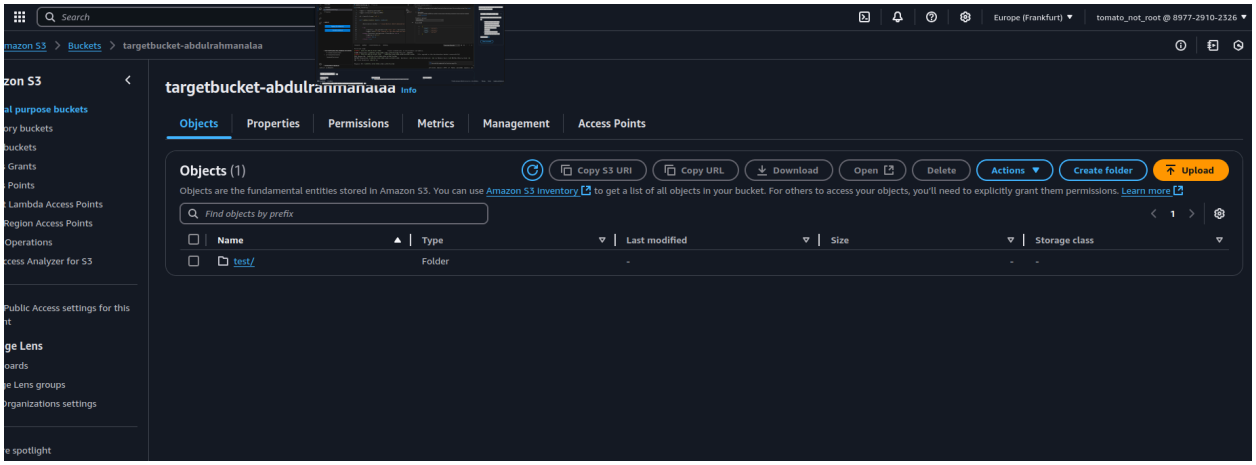
Create the function attached the role configured for public access

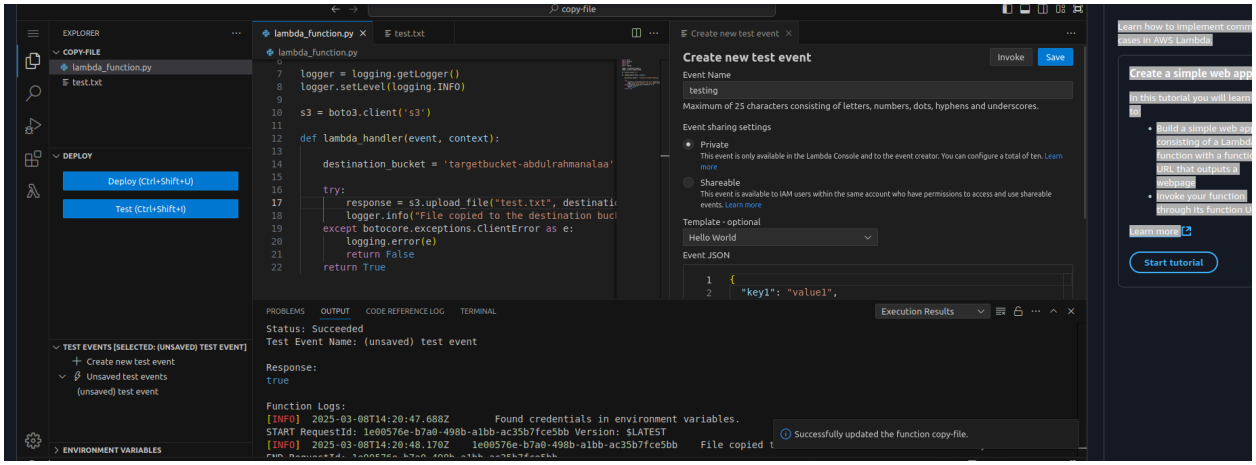


Now create the s3 bucket fo storing my test file

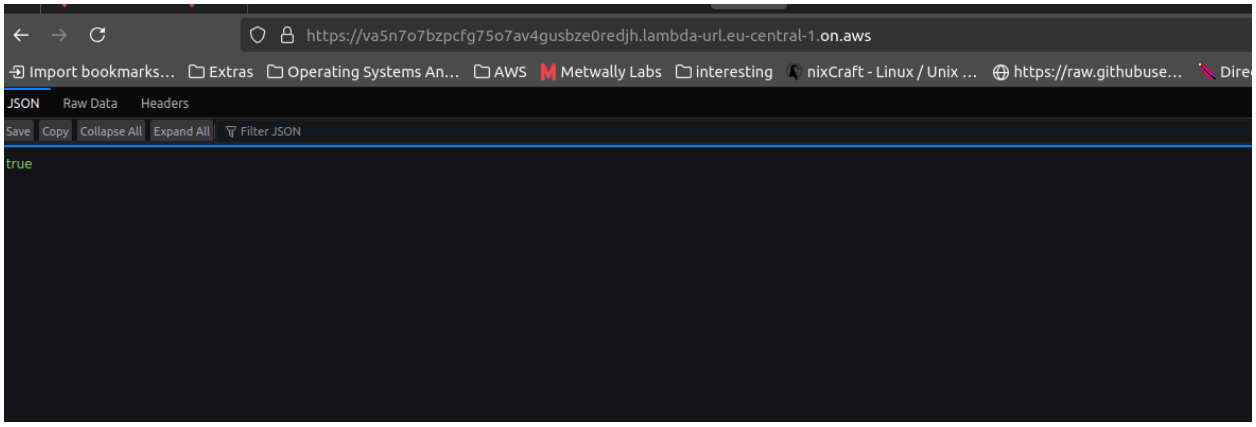




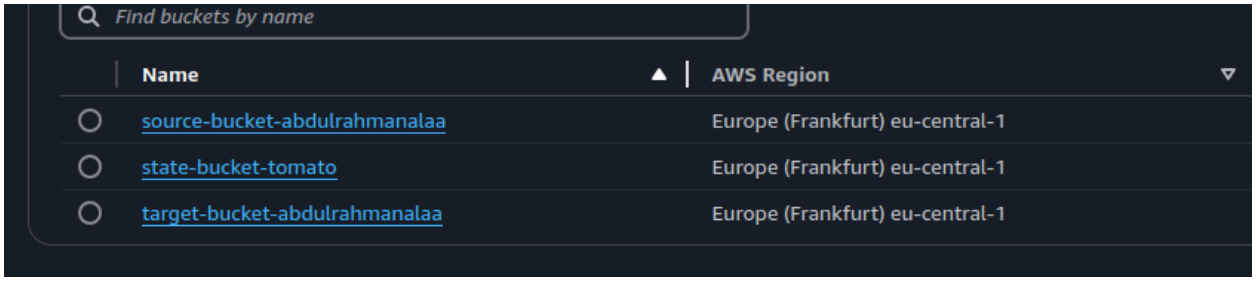


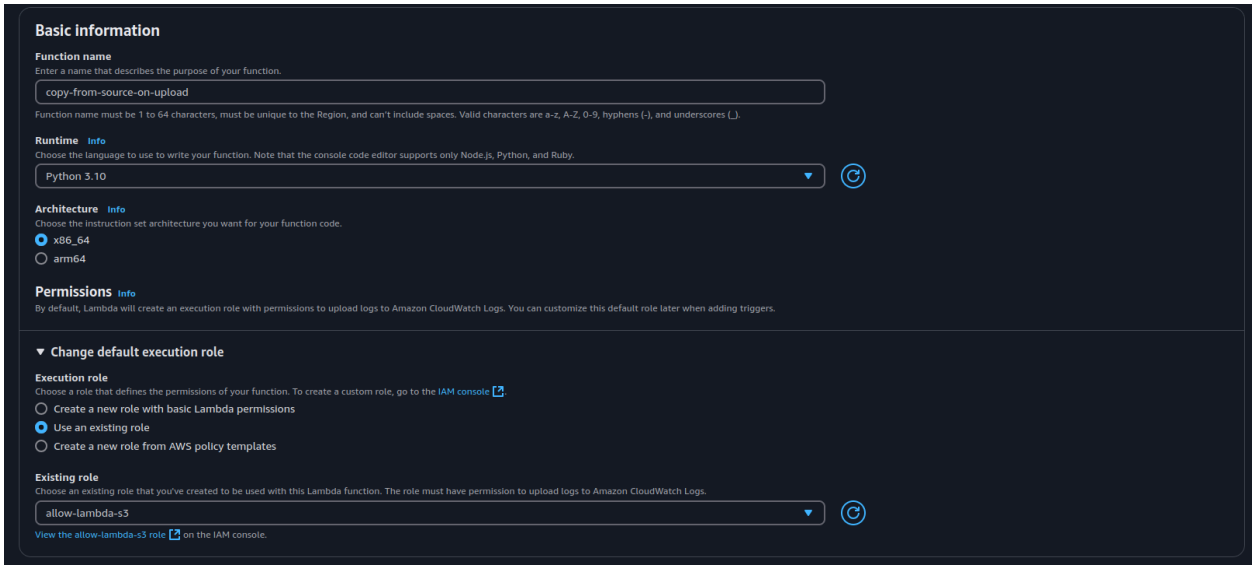


Running the test event we can see that the text file is copied inside the bucket with the proper credentials available on the lambda and can be publicly invoked using the function's link

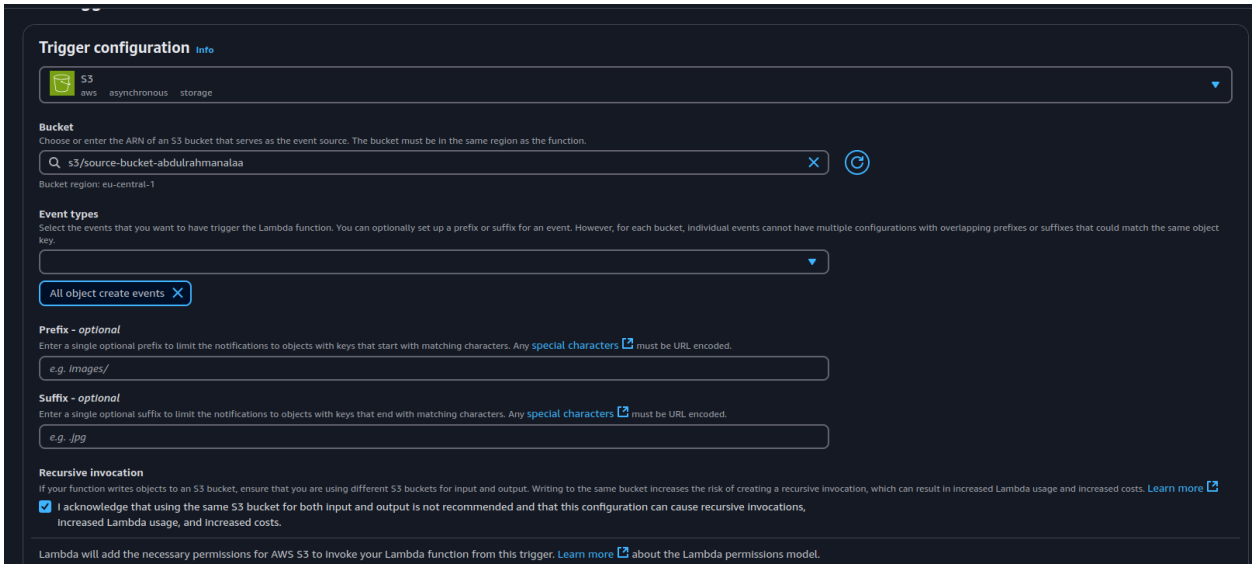


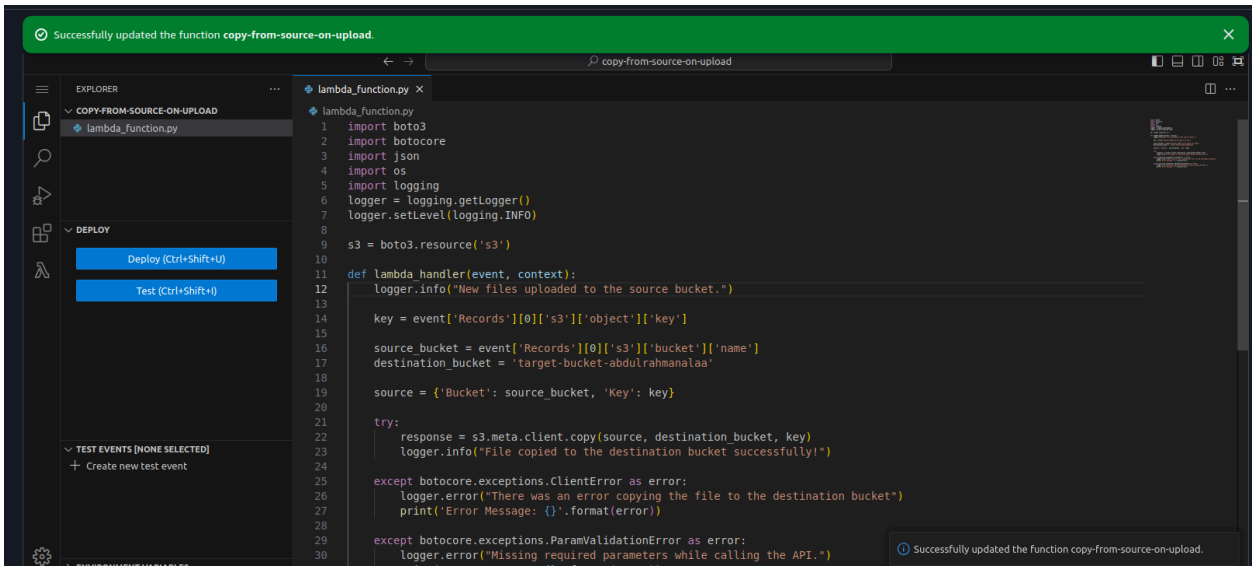
Q5: create a lambda function triggered on s3 to copy file from bucket to another
Create the source-bucket-abdulrahmanalaa
Create the target-bucket-abdulrahmanalaa



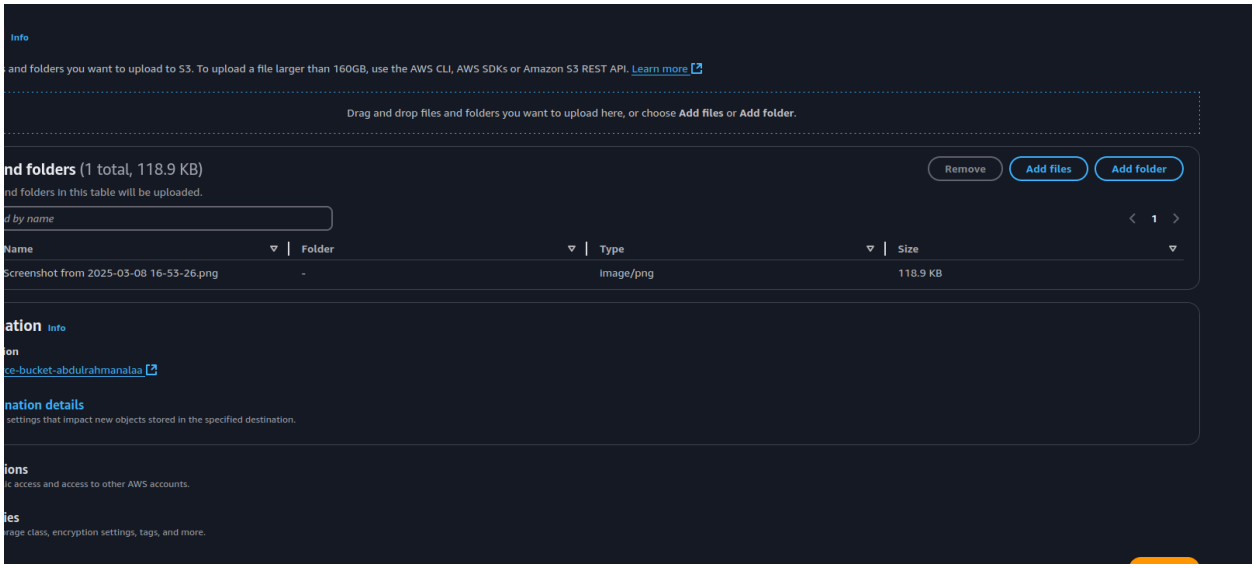


Attaching a trigger on the source s3 bucket



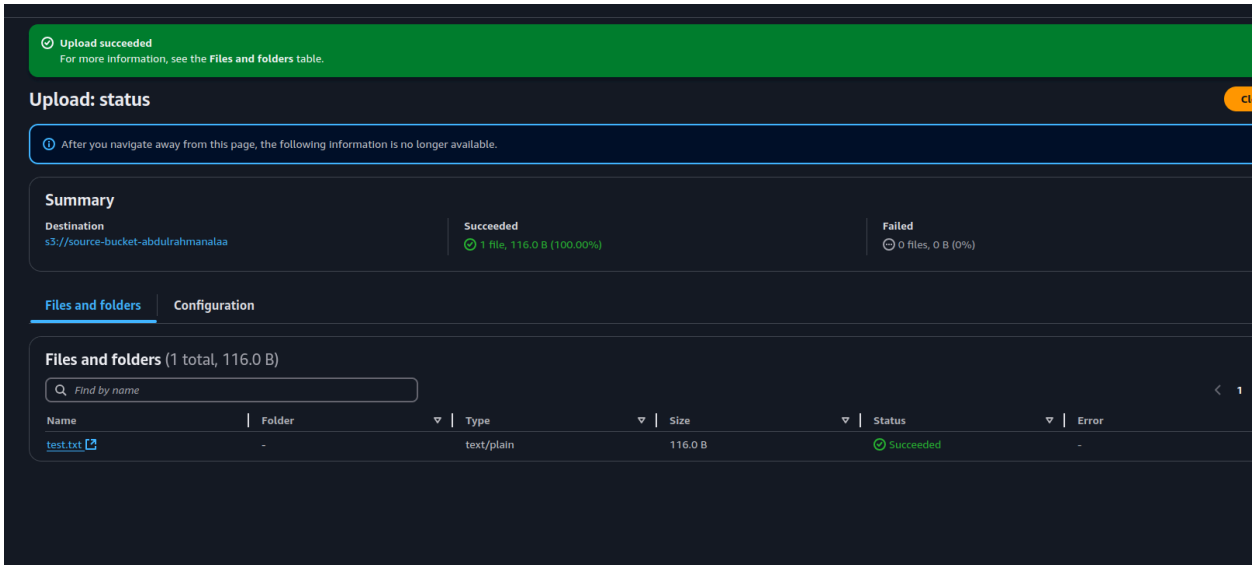


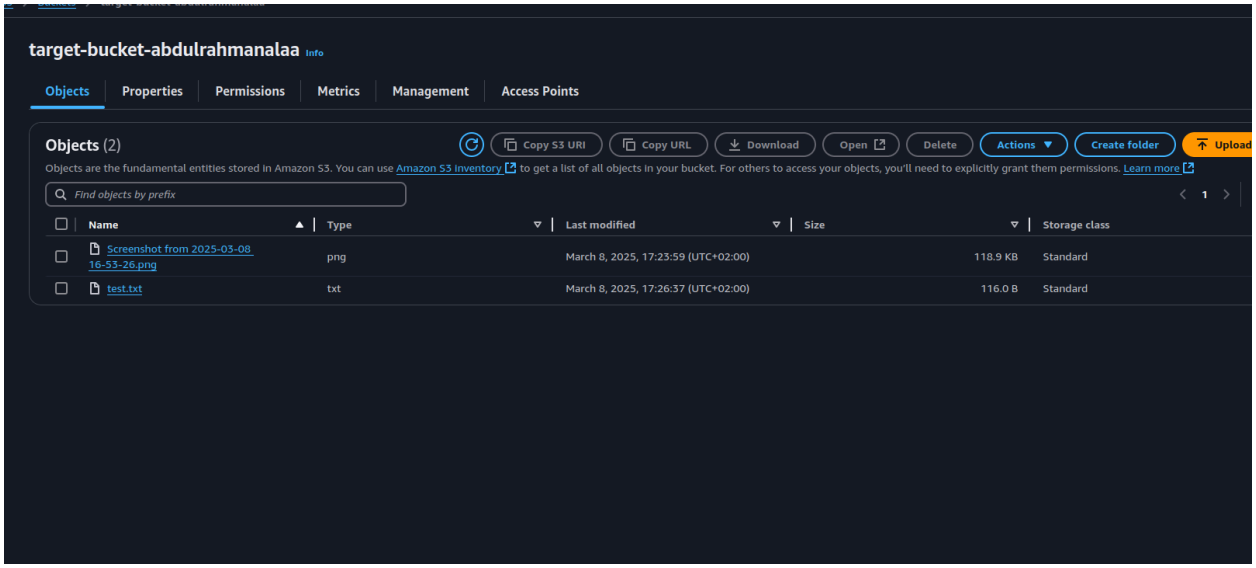
The code for copying form the source bucket to the target bucket
Now adding a file to the source-bucket



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 ccan be found in https://github.com/abdulrahmanalaa123/ITI-sessions/tree/master/AWS/Lab3