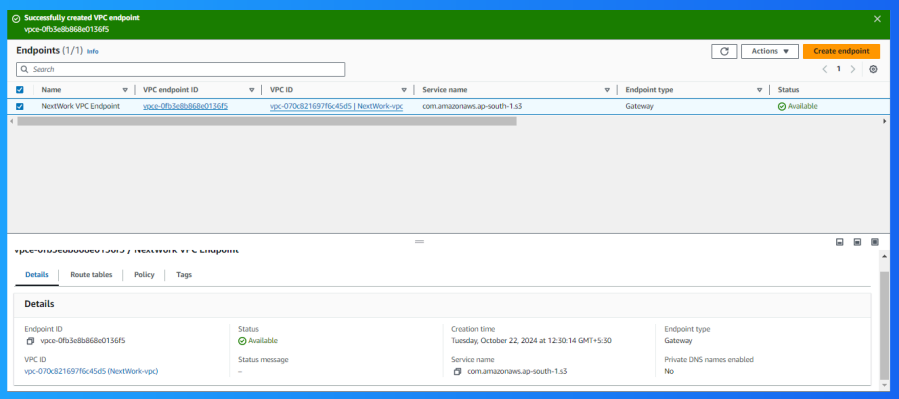
NextWork.org

# VPC Endpoints

Roshan Thomas



**Roshan Thomas**
NextWork Student



# Introducing Today's Project!

## What is Amazon VPC?

Amazon VPC (Virtual Private Cloud) allows you to create an isolated network within AWS, providing control over network settings, security, and access. It's useful for securely hosting applications, managing traffic, and integrating on-premise networ

## How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a secure network. I set up a public subnet and security groups to control access. This allowed my instance to communicate with the internet and access Amazon S3.

## One thing I didn't expect in this project was...

I didn’t expect the complexity of configuring VPC endpoints and security groups for S3 access. While I knew the concepts, the steps for a secure connection were more intricate than I anticipated.

## This project took me...

2 Hours and 40 Minutes

**Roshan Thomas**
NextWork Student

NextWork.org

# In the first part of my project...

## Step 1 - Architecture set up

I'm going to create a VPC, launch an EC2 instance within it, and set up an S3 bucket. This will provide a secure environment for my resources and allow me to directly connect my EC2 instance to S3, improving performance and security.

## Step 2 - Connect to EC2 instance

I'm going to connect to my EC2 instance using EC2 Instance Connect to gain direct access and interact with the instance's terminal. This will allow me to attempt to access Amazon S3 through the public internet and observe the results.

## Step 3 - Set up access keys

I'm going to create access keys for my EC2 instance so it can securely access and manage AWS services, including Amazon S3. This will allow me to interact with these services from within the instance and perform various tasks.

## Step 4 - Interact with S3 bucket

I'm going to use my EC2 instance to access the S3 bucket I created. This will demonstrate how I can interact with S3 resources from within my VPC and perform tasks like listing objects and uploading files.

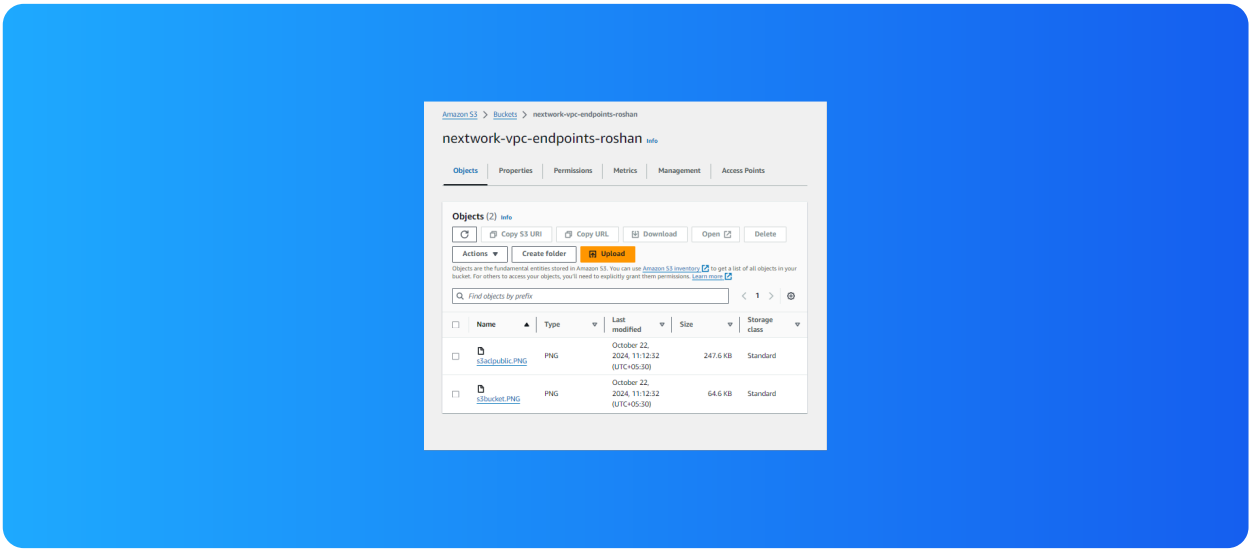
**Roshan Thomas**
NextWork Student



# Architecture set up

I started my project by launching a VPC named NextWork-vpc with a single public subnet and an EC2 instance named Instance - NextWork VPC Endpoints. I also created a security group named SG - NextWork VPC Endpoints for the EC2 instance.

I also set up an S3 bucket named nextwork-vpc-endpoints-roshan and uploaded two files to it. This will allow me to access and manage these files from my EC2 instance.



**Roshan Thomas**
NextWork Student



# Access keys

## Credentials

To set up my EC2 instance to interact with my AWS environment, I configured its access key ID, secret access key, default region name, and output format. This allowed me to securely authenticate the instance and access AWS services.

Access keys are credentials that provide authentication for your AWS account. They consist of an access key ID and a secret access key, which are used to securely access and manage AWS services.

Secret access keys are a crucial part of AWS credentials, providing a secure method of authentication. They are used in conjunction with access key IDs to grant access to AWS services and resources.

## Best practice

Although I'm using access keys, a best practice alternative is to use IAM roles for enhanced security and reduced risk.

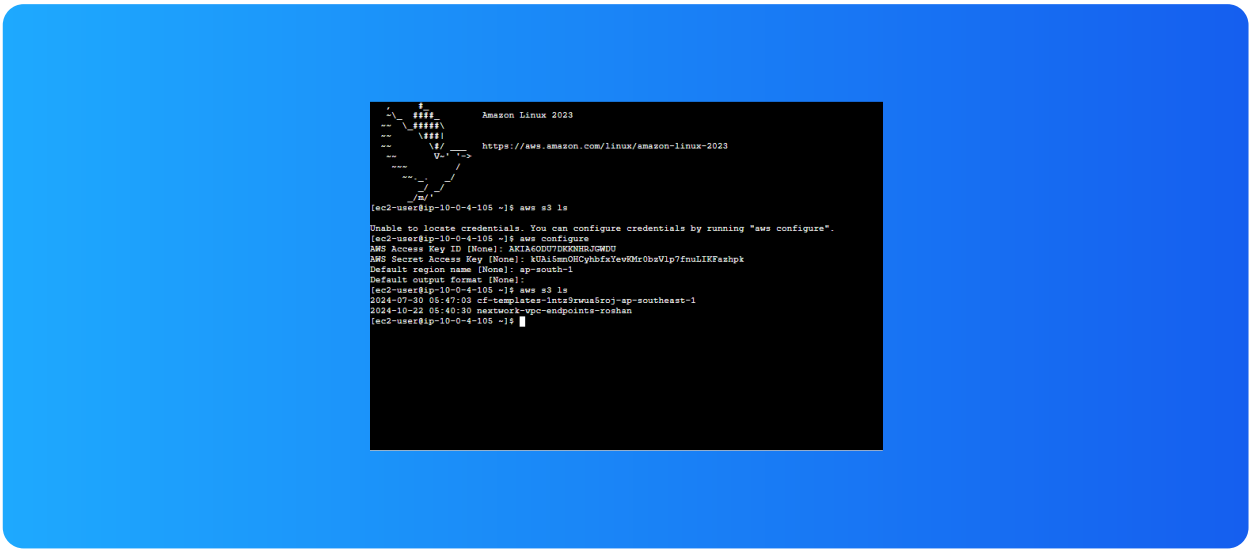
**Roshan Thomas**
NextWork Student



# Connecting to my S3 bucket

The command I ran was aws s3 ls. This command is used to list the S3 buckets that I have access to within my AWS account.

The terminal responded with "Unable to locate credentials." This indicated a misconfiguration with the access keys. I needed to double-check and ensure they were entered correctly.

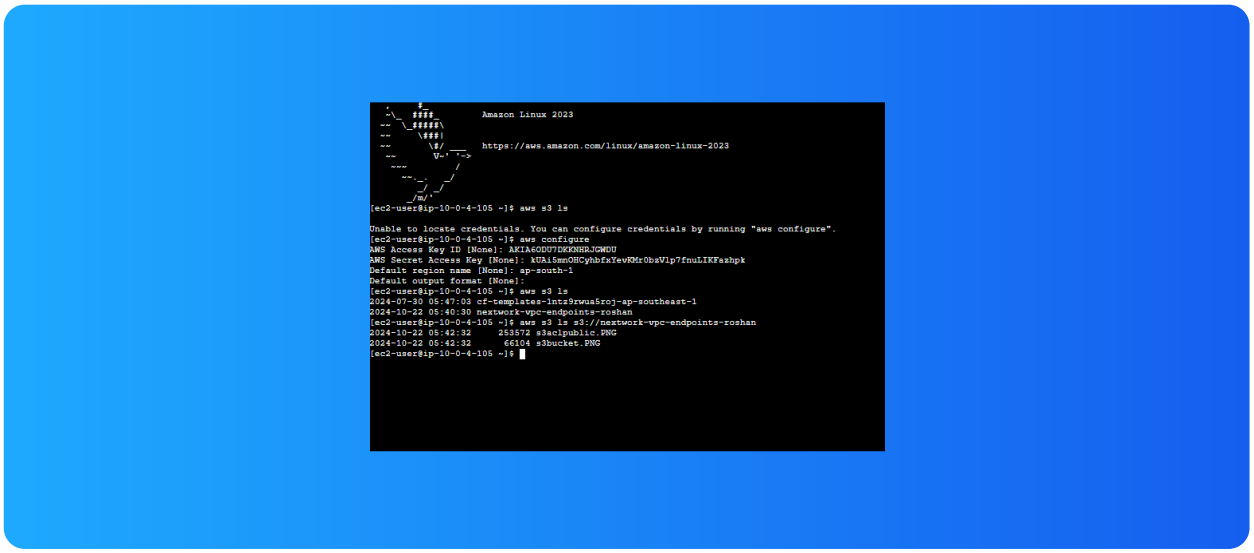


**Roshan Thomas**
NextWork Student

NextWork.org

# Connecting to my S3 bucket

I also tested the command aws s3 ls s3://nextwork-vpc-endpoints-yourname, which returned a list of objects within my S3 bucket. This command allowed me to view the contents of the bucket and verify that the files I uploaded were successfully stored.



**Roshan Thomas**
NextWork Student

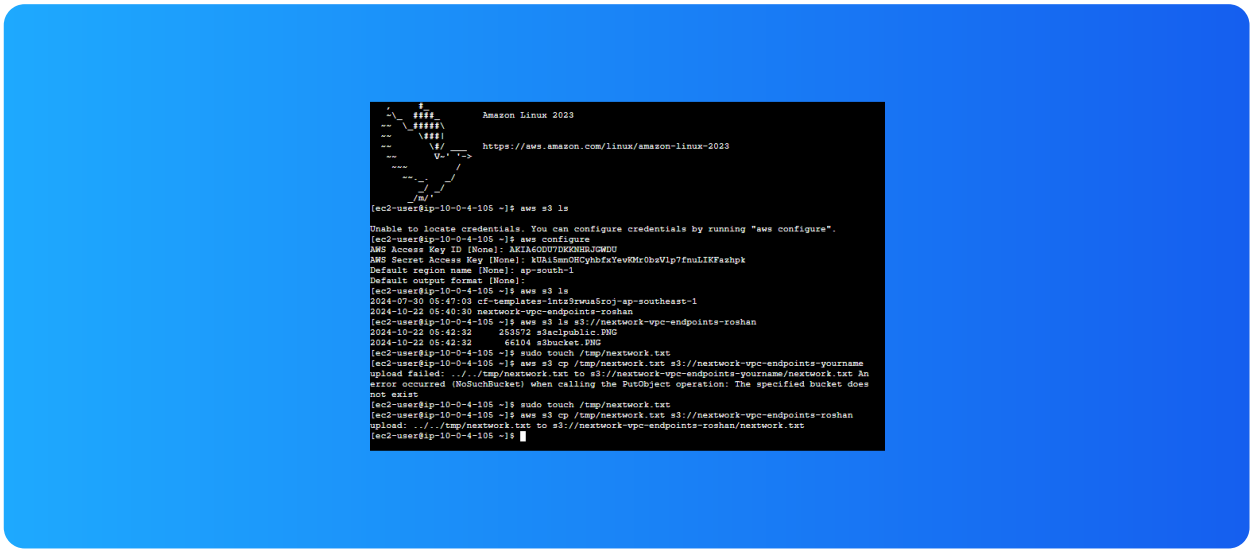
NextWork.org

# Uploading objects to S3

To upload a new file to my bucket, I first ran the command sudo touch /tmp/nextwork.txt. This command creates an empty text file named nextwork.txt in the /tmp directory on my EC2 instance.

The second command I ran was aws s3 cp /tmp/nextwork.txt s3://nextwork-vpc-endpoints-roshan. This command will upload the nextwork.txt file to my S3 bucket named nextwork-vpc-endpoints-roshan.

The third command I ran was aws s3 ls s3://nextwork-vpc-endpoints-roshan, which validated that the nextwork.txt file was successfully uploaded to my S3 bucket.



**Roshan Thomas**
NextWork Student



# In the second part of my project...

## Step 5 - Set up a Gateway

I'm going to create a VPC endpoint to connect my EC2 instance directly to S3. This will improve security and performance by eliminating the need for traffic to go through the public internet.

## Step 6 - Bucket policies

I'm going to create a bucketpolicy that restricts access to my S3 bucket to only traffic coming from my VPC endpoint.It help me validate if the endpoint is functioning correctly and providing direct access to S3 without relying on the public internet

## Step 7 - Update route tables

I'm going to test my VPC endpoint setup by attempting to access my S3 bucket from my EC2 instance. This will help me validate if the endpoint is functioning correctly and providing direct access to S3 without relying on the public internet.

## Step 8 - Validate endpoint conection

I'm going to test my VPC endpoint setup by accessing my S3 bucket from my EC2 instance. I will also restrict my VPC's access to my AWS environment to ensure security.

**Roshan Thomas**
NextWork Student

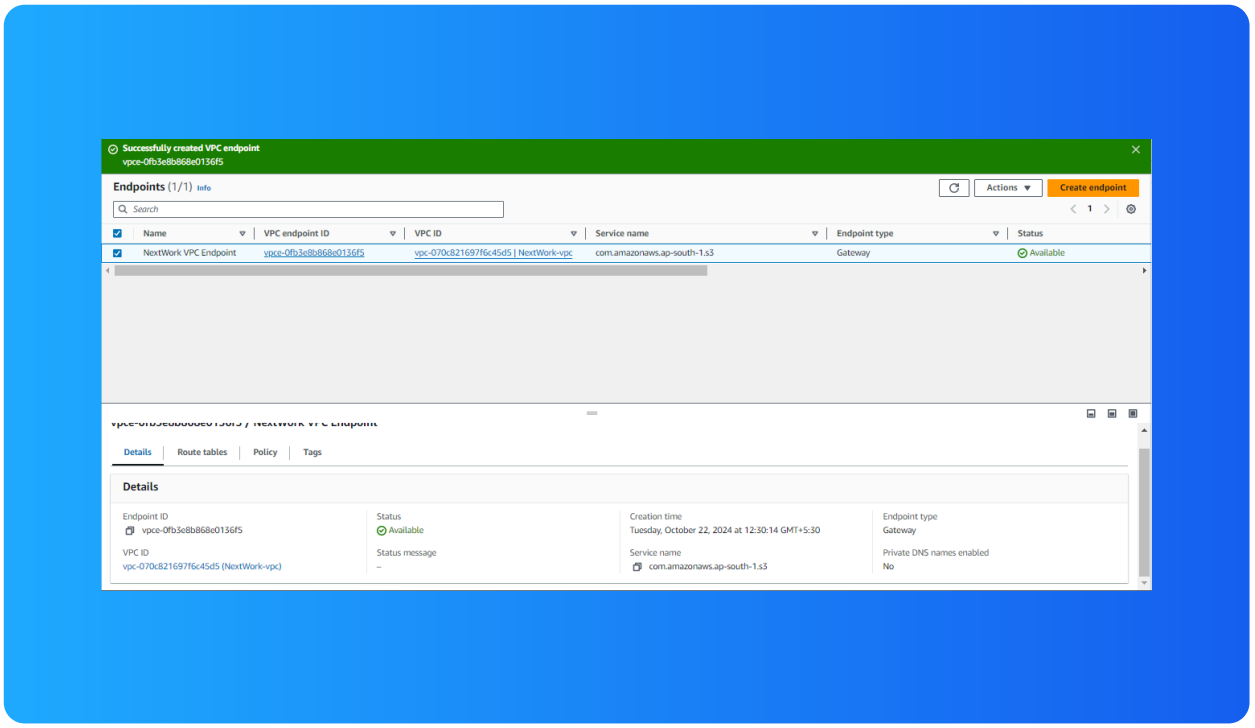
NextWork.org

# Setting up a Gateway

I set up an S3 Gateway, which is a type of VPC endpoint for Amazon S3 and DynamoDB. It creates a route to direct traffic to the gateway instead of the internet.

## What are endpoints?

An endpoint is a service that allows you to connect your VPC to other AWS services without going through the public internet. This provides a more secure and efficient way for your resources to communicate with these services.



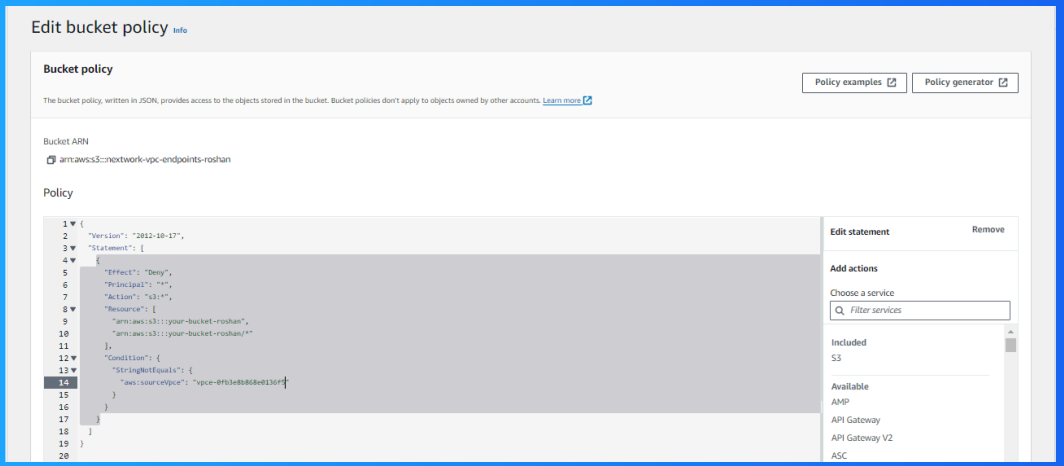
**Roshan Thomas**
NextWork Student

NextWork.org

# Bucket policies

A bucket policy is a type of IAM policy that controls access to an S3 bucket. It defines who can access the bucket and what actions they are allowed to perform.

My bucket policy will deny all access to my S3 bucket and its objects, except for traffic coming from the VPC endpoint with the specified ID. It will ensure that only my EC2 instance, which is connected through the VPC endpoint, can access the bucket



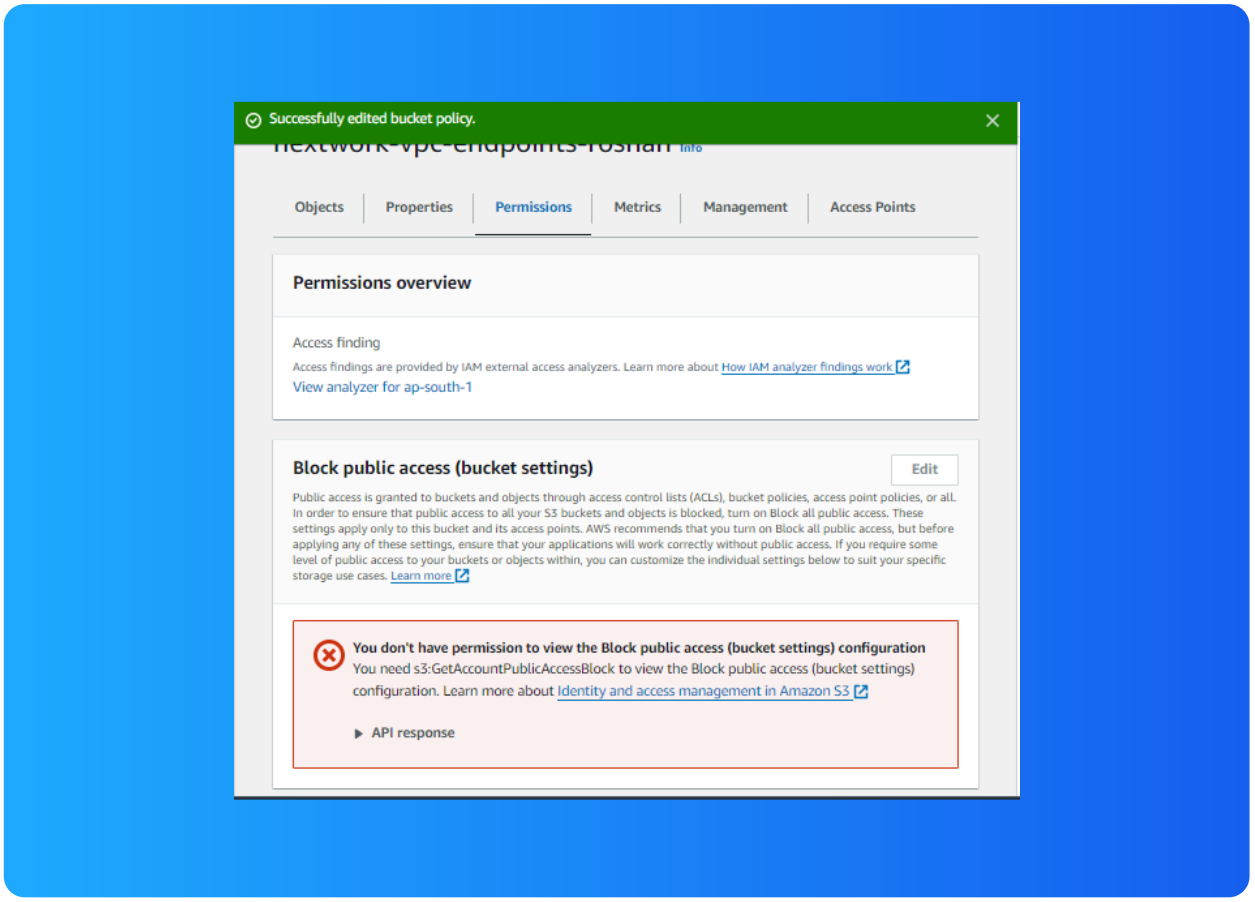
**Roshan Thomas**
NextWork Student



# Bucket policies

Right after saving my bucket policy, I saw "denied access" warnings. This was because I needed to configure the VPC endpoint's route table to allow traffic to the S3 bucket.

I also had to update my route table to direct traffic from my EC2 instance to the VPC endpoint. This allowed my instance to access the S3 bucket.



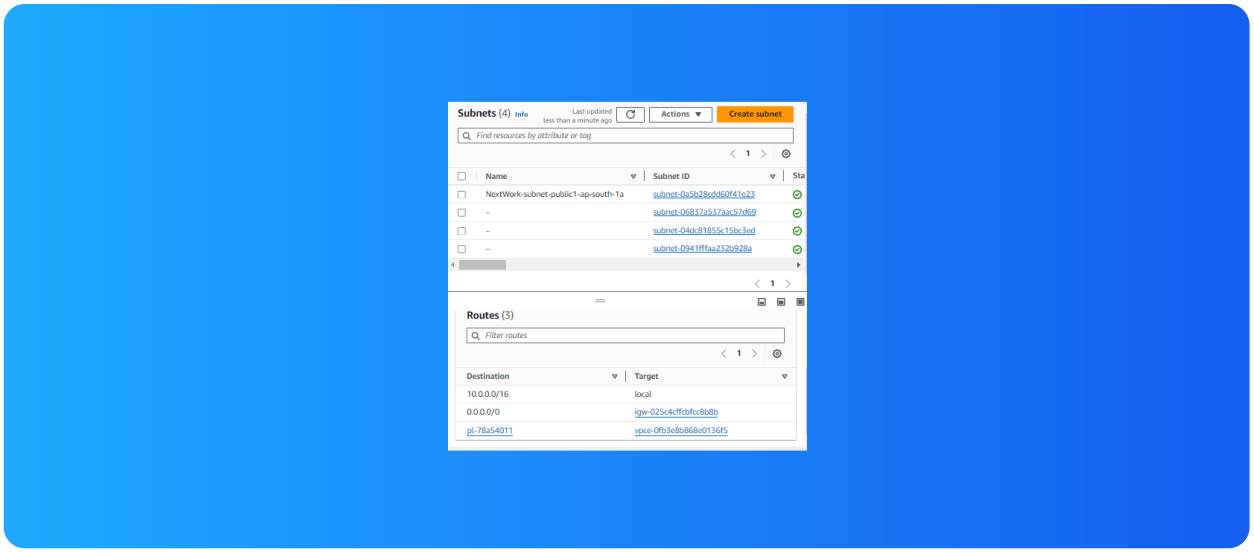
**Roshan Thomas**
NextWork Student

NextWork.org

# Route table updates

To update my route table, I added a new route with the destination CIDR block set to 0.0.0.0/0 and the target set to my VPC endpoint. This allowed my EC2 instance to access the S3 bucket.

After updating my public subnet's route table, my terminal could return a list of objects within my S3 bucket, indicating that my EC2 instance can now successfully access the bucket through the VPC endpoint.



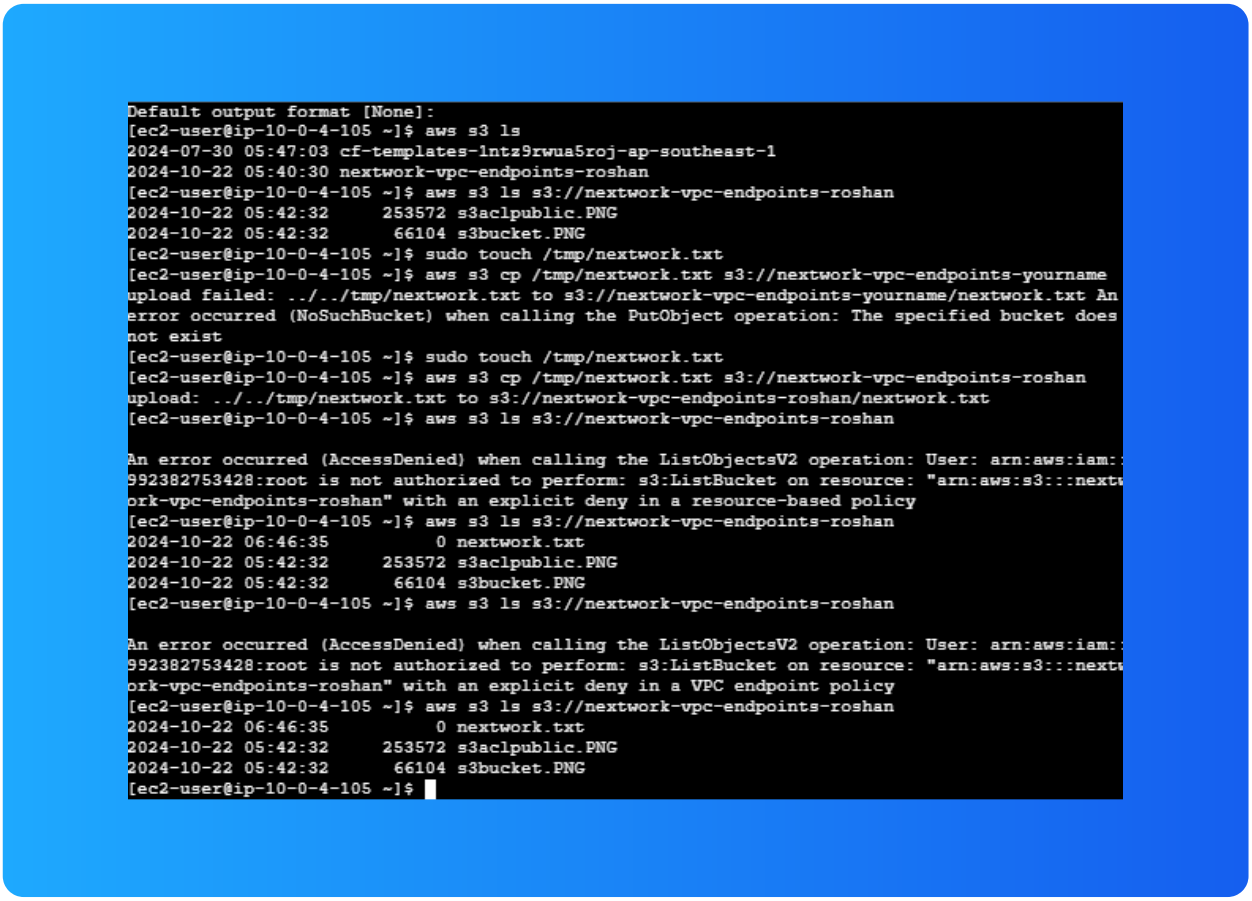
**Roshan Thomas**
NextWork Student

NextWork.org

# Endpoint policies

An endpoint policy is a type of IAM policy that controls access to a VPC endpoint. It allows you to define which AWS services can be accessed through the endpoint and what actions are permitted.

I updated my endpoint's policy by allowing access. I could see the effect of this right away, because I was able to successfully access my S3 bucket from my EC2 instance, confirming that the policy and VPC endpoint were correctly configured.



# Everyone should be in a job they love.

Check out nextwork.org for more projects