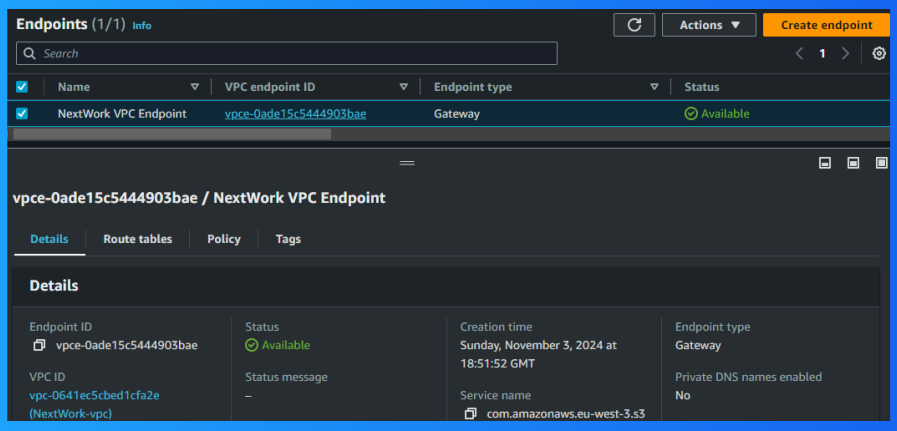
NextWork.org

VPC Endpoints

NI nikhil7_94@hotmail.com



NI
nikhil7_94@hotmail.com
NextWork Student
NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a private isolated network in the cloud where you can securely run resources like servers and databases. It's useful because it gives full control over network settings, security and connectivity to the internet.

How I used Amazon VPC in this project

Today I learned how to set up direct, private access to S3 from my VPC.

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

One thing I didnt expect was there are different ways to allow or deny access to S3.

This project took me...

I took around 1 and half hour with this project.

NI
nikhil7_94@hotmail.com
NextWork Student
NextWork.org

In the first part of my project...

Step 1 - Architecture set up

In this step Im going to create a VPC from scratch, launch an EC2 instance which I will connect to using EC2 Instance Connect later and set up an S3 bucket.

Step 2 - Connect to EC2 instance

Now Im going to connect directly to my EC2 instance.

Step 3 - Set up access keys

In this step I will give my EC2 instance access to your AWS environment so I can access to the S3 bucket list.

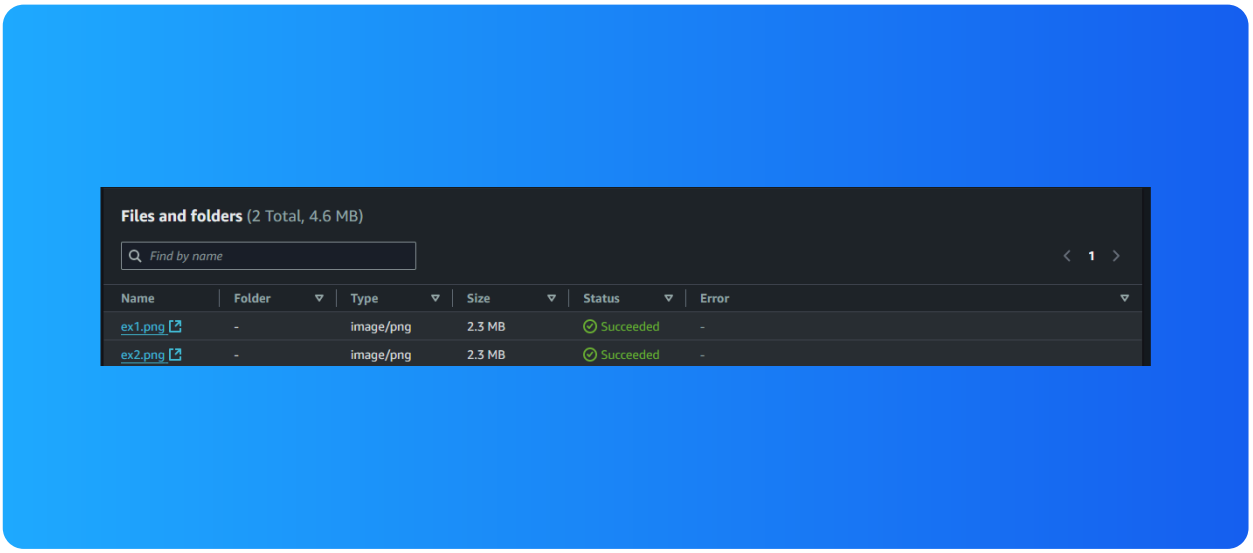
Step 4 - Interact with S3 bucket

Now Im going to get my EC2 instance to access my S3 bucket.

Architecture set up

I started my project by launching a VPC and an EC2 instance.

I also set up an S3 bucket.



Access keys

Credentials

To set up my EC2 instance to interact with my AWS environment, I configured the access key, the secret key, region code name and the output format.

Access keys are credentials for my applications and other servers to log into AWS and talk to my AWS services and resources.

Secret access keys are like a password of the access key. It is needed to log in with the credentials.

Best practice

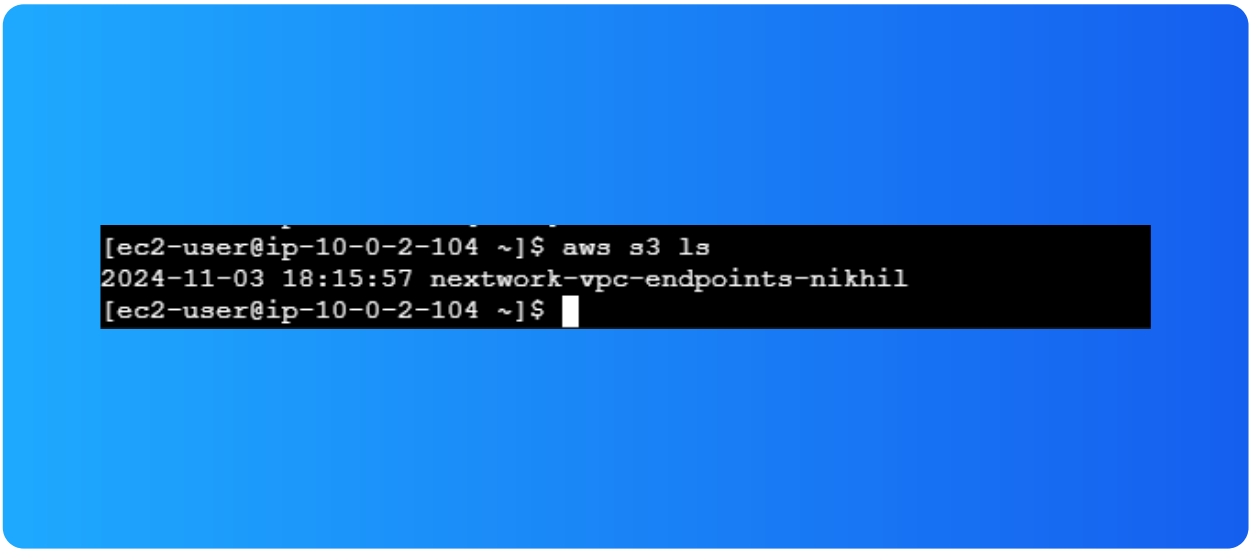
Although I'm using access keys in this project, a best practice alternative is to use an IAM role with the necessary permissions and then attaching that role to my EC2 instance.

NI
nikhil7_94@hotmail.com
NextWork Student
NextWork.org

Connecting to my S3 bucket

The command I ran was "aws s3 ls". This command is used to list all the S3 buckets in my account.

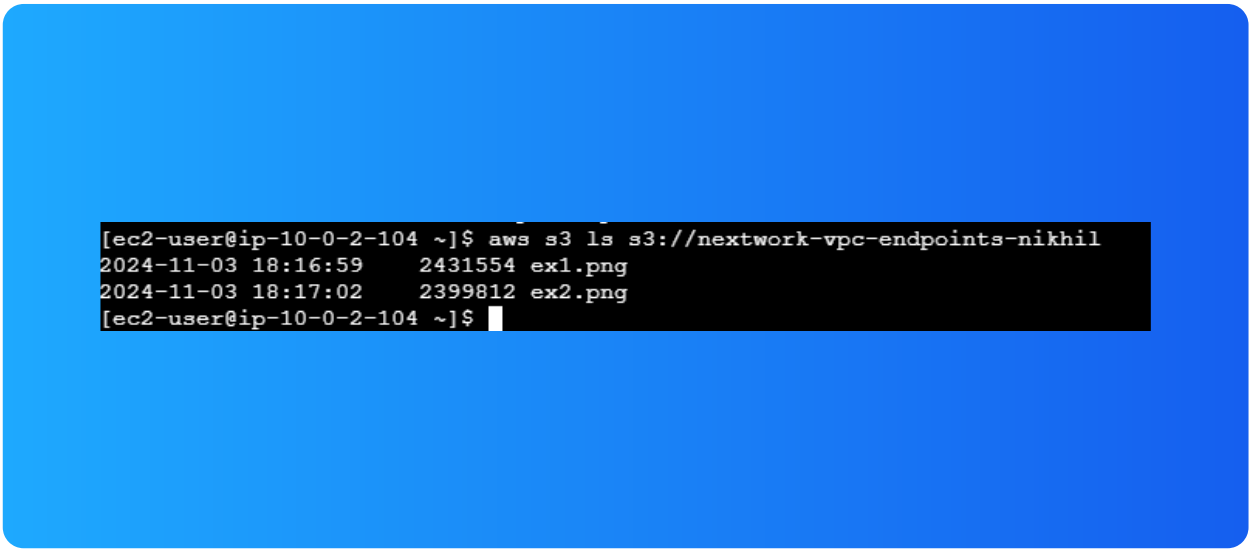
The terminal responded with the list of S3 buckets in my account. This indicated that the access keys I set up correctly.



NI
nikhil7_94@hotmail.com
NextWork Student

Connecting to my S3 bucket

I also tested the command "aws s3 ls s3://nextwork-vpc-endpoints-nikhil" which returned the list of objects inside that S3 bucket indicated.



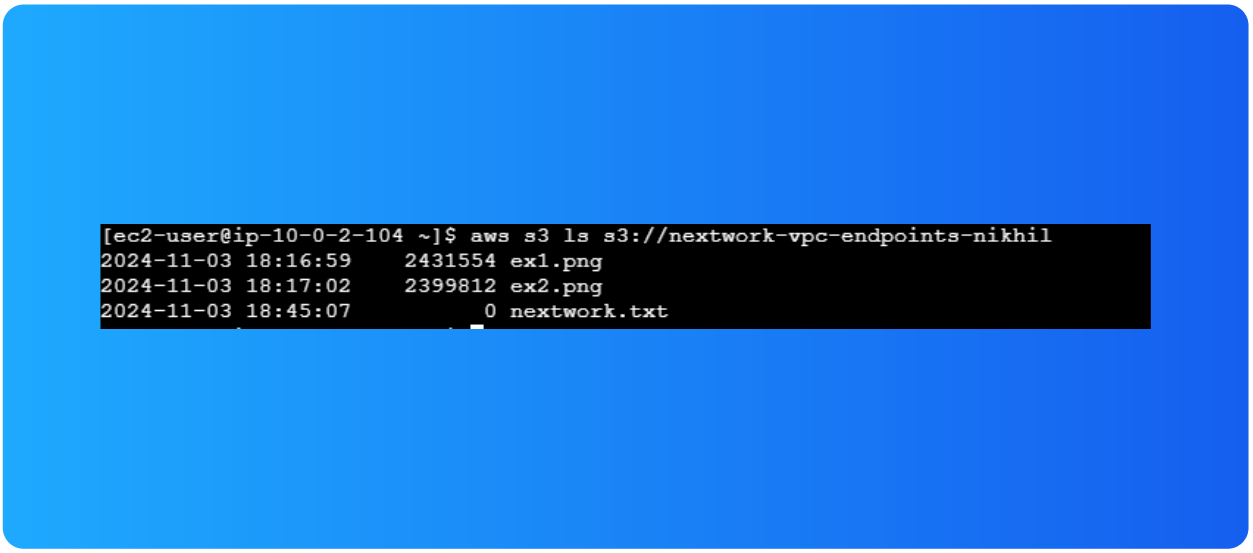
NI
nikhil7_94@hotmail.com
NextWork Student

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 .txt file.

The second command I ran was "aws s3 cp /tmp/nextwork.txt s3://nextwork-vpc-endpoints-nikhil". This command will add the empty .txt file to my S3 bucket.

The third command I ran was "aws s3 ls s3://nextwork-vpc-endpoints-nikhil" which validated that the .txt file was added to the S3 bucket correctly.



NI
nikhil7_94@hotmail.com
NextWork Student
NextWork.org

In the second part of my project...

Step 5 - Set up a Gateway

In this step I will set up a way for your VPC and S3 to communicate direclty.

Step 6 - Bucket policies

Now I will limit my S3 bucket access's to only traffic from your endpoint.

Step 7 - Update route tables

In this step I will test my VPC endpoint set up.

Step 8 - Validate endpoint conection

Now I will test my VPC endpoint set up again and restrict my VPC's acccess to my AWS environment.

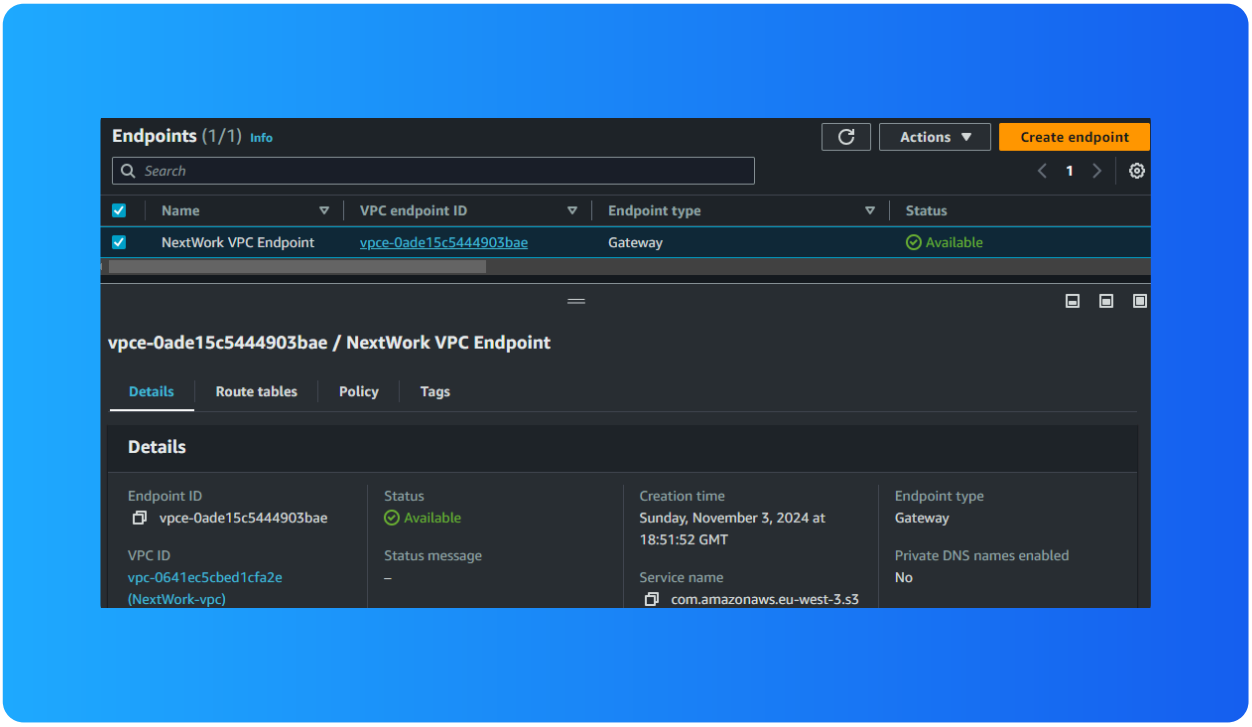
NI
nikhil7_94@hotmail.com
NextWork Student

Setting up a Gateway

I set up an S3 Gateway, which is a type of endpoint used specifically for Amazon S3 and DynamoDB. It work by simply adding a route to your VPC route table that directs traffic bound for S3 to head straight for the Gateway instead of the internet.

What are endpoints?

An endpoint is a service that allows private connections between my VPC and other AWS services without needing the traffic to go over the internet.

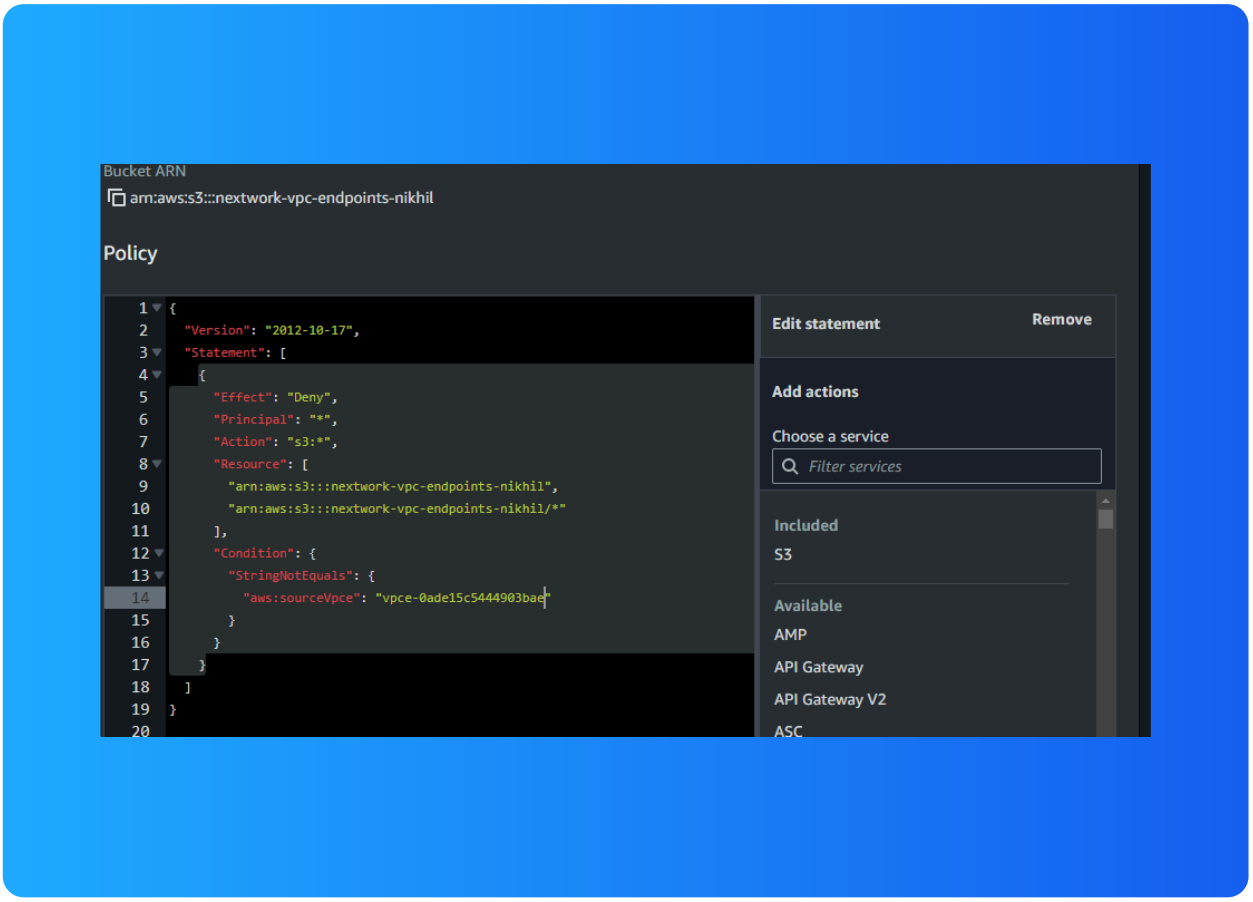


NI
nikhil7_94@hotmail.com
NextWork Student

Bucket policies

A bucket policy is a type of IAM policy designed for setting access permissions to an S3 bucket.

My bucket policy will deny all actions (s3:*) on your S3 bucket and its objects to everyone (Principal: "*")... unless the access is from the VPC endpoint with the ID defined in aws:sourceVpce.

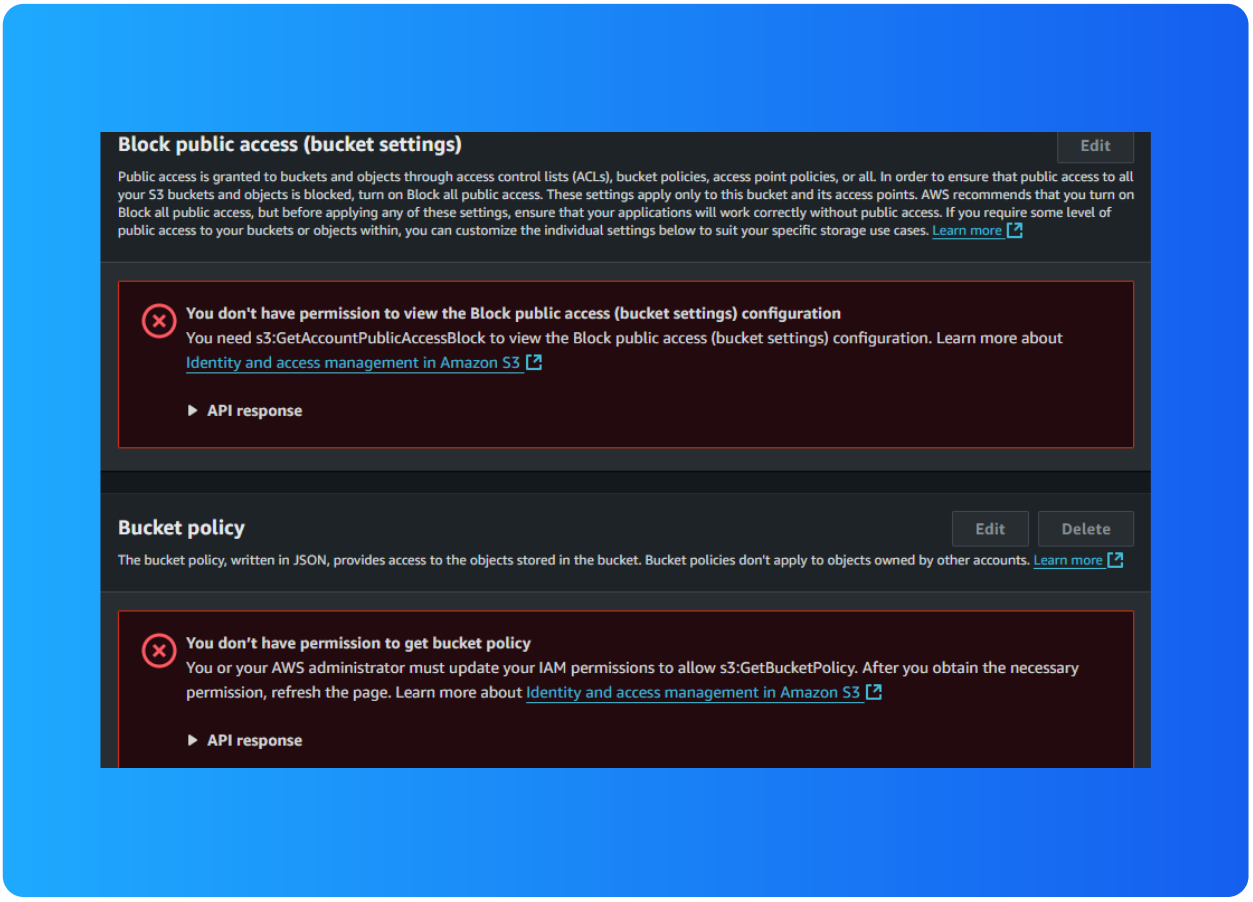


NI
nikhil7_94@hotmail.com
NextWork Student

Bucket policies

Right after saving my bucket policy, my S3 bucket page showed 'denied access' warnings. This was because my policy denies all actions unless they come from your VPC endpoint. This means any attempt to access your bucket from other sources is blocked.

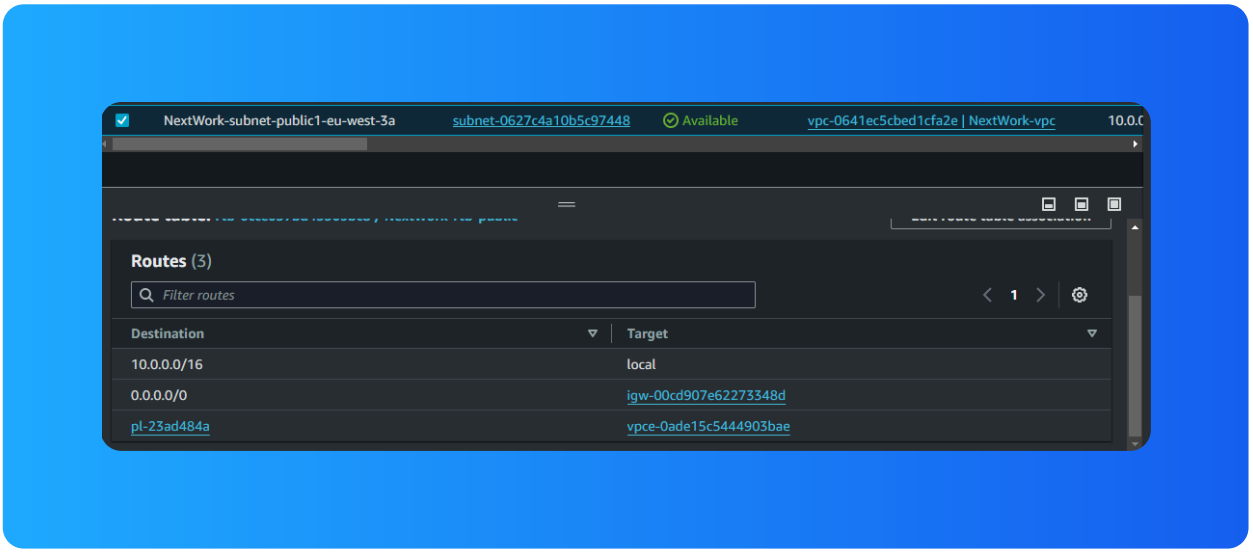
I also had to update my route table because didnt have a route that directs traffic bound for S3 to my VPC endpoint, traffic from my EC2 instance is actually trying to get to your S3 bucket through the public internet instead.



Route table updates

To update my route table, I modified the route table of the endpoint so it can access without the route of the public internet.

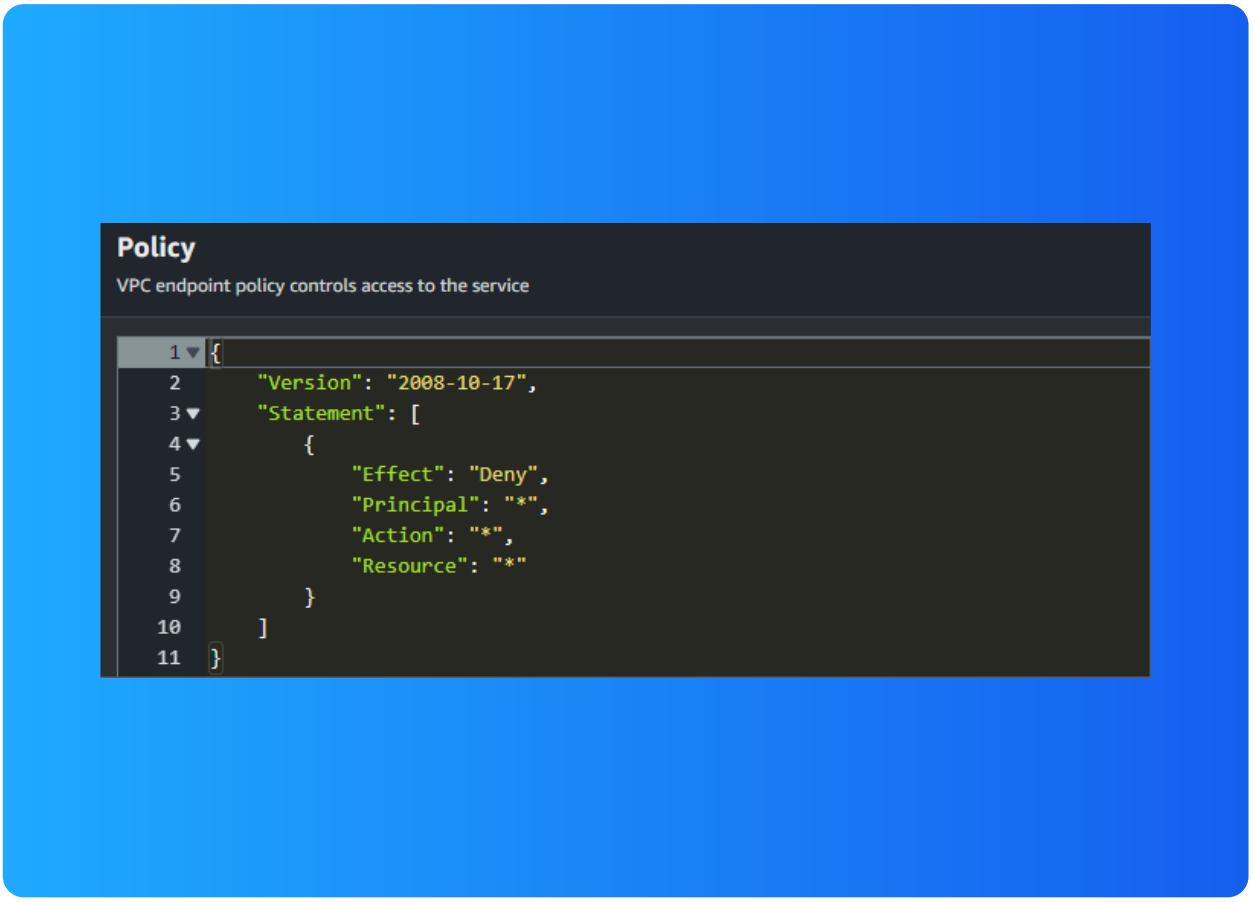
After updating my public subnet's route table, my terminal could return a response showing the list of objects in the S3 bucket.



Endpoint policies

An endpoint policy is used to allow or deny access to the resources by permissions.

I updated my endpoint's policy by denying all access instead of allowing. I could see the effect of this right away, because I got access denied when I try to see my list of S3 bucket.



Everyone should be in a job they love.

Check out nextwork.org for more projects