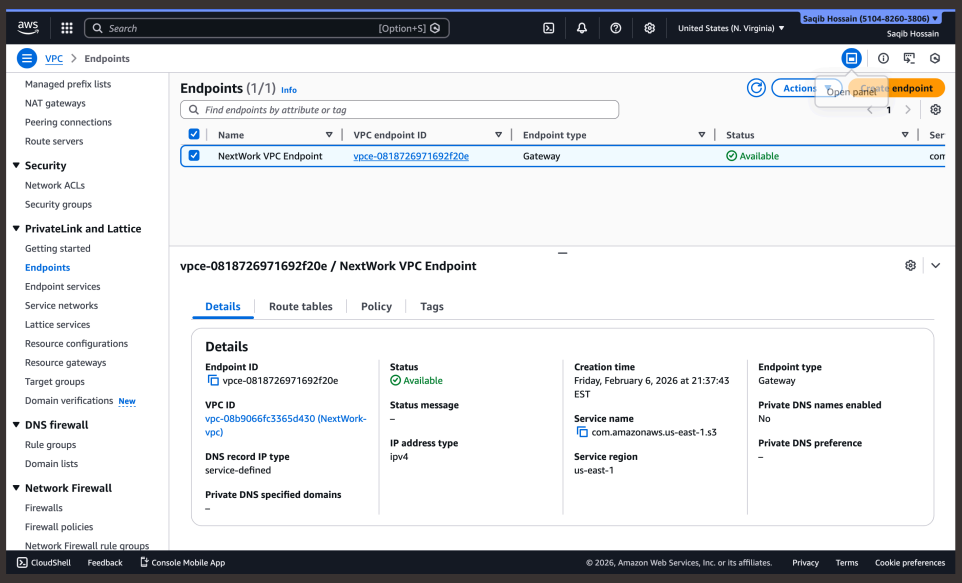
nextwork.org

VPC Endpoints

saqibh49@gmail.com



saqibh49@gmail.com
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

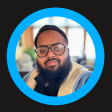
Amazon VPC is your own private section of the AWS cloud where you can set up networks, subnets, and security rules however you want, and it is useful because it keeps your data secure and isolated from the public internet while still letting you connect the resources that need to talk to each other.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create an EC2 instance, an S3 bucket and a VPC endpoint. Then I connect to it via instance connect. Finally, I changed the bucket policy and endpoint policy to allow and deny certain types of traffic to test the endpoint.

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

One thing I didn't expect in this project was how granular the controls for keeping traffic out and in an AWS environment could be.



saqibh49@gmail.com
NextWork Student

This project took me...

This project took me 45 minutes.

saqibh49@gmail.com
NextWork Student

In the first part of my project...

Step 1 - Architecture set up

In this step, I will set up my VPC, EC2 instance and S3 bucket so I can test out how to connect from my VPC to my S3 bucket in a more secure way.

Step 2 - Connect to EC2 instance

In this step, I will connect with my EC2 instance because that's the first step to accessing my S3 bucket from y VPC.

Step 3 - Set up access keys

In this step, I will create an access key because without that, my EC2 instance won't be able to see my S3 bucket and any other AWS resources outside my VPC.

Step 4 - Interact with S3 bucket

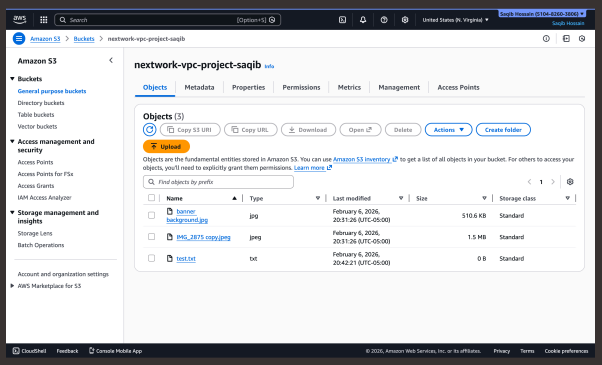
In this step, I will connect to my S3 bucket from my EC2 instance because now I have my access keys.

saqibh49@gmail.com
NextWork Student

Architecture set up

I started my project by launching a VPC, a public subnet and an EC2 instance

I also set up an S3 bucket with 2 files in it.




saqibh49@gmail.com
NextWork Student

Access keys

Credentials

To set up my EC2 instance to interact with my AWS environment, I configured my access keys and my S3 bucket.

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

Secret access keys are basically the password to a username. Both are needed to access AWS.

Best practice

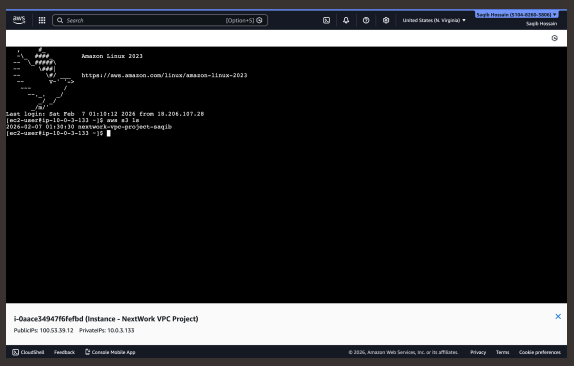
Although I'm using access keys in this project, a best practice alternative is to use an IAM role with the correct permissions.

saqibh49@gmail.com
NextWork Student

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 AWS account.

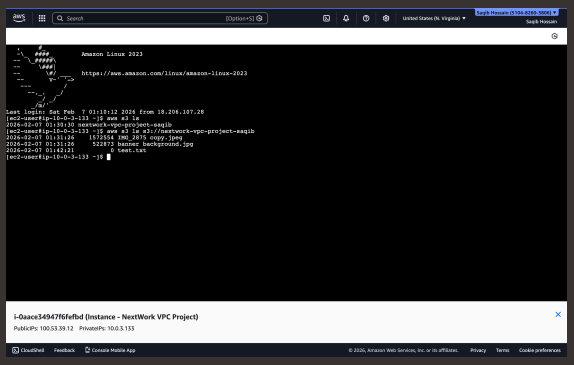
The terminal responded with a list of all the S3 buckets in my AWS account. This indicated that the access keys I set up have successfully allowed my EC2 instance to connect with my S3 bucket and more broadly is allowing it to see all AWS sservices outside the VPC.



saqibh49@gmail.com
NextWork Student

Connecting to my S3 bucket

I also tested the command aws s3 ls a3://nextwork-vpc-project-saqib which returned a list of all the files within my S3 bucket.



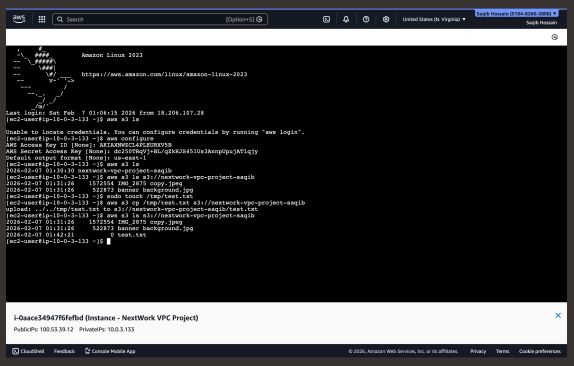
saqibh49@gmail.com
NextWork Student

Uploading objects to S3

To create a new file, I first ran the command sudo touch /tmp/test.txt. This command creates a new blank text file.

The second command I ran was aws s3 cp /tmp/test.txt s3://nextwork-vpc-project-saqib. This command will move the blank text file I just created into my s3 bucket.

The third command I ran was aws s3 ls s3://nextwork-vpc-project-saqib, which validated that the file was moved into my s3 bucket by listing out the bucket's contents.



saqibh49@gmail.com
NextWork Student

In the second part of my project...

Step 5 - Set up a Gateway

In this step, I will creating a VPC endpoint because that is a much more secure way of accessing AWS resources from within a VPC than using the open internet

Step 6 - Bucket policies

In this step, I will be setting my S3 bucket's policy to only allow traffic from my gateway. This will verify whether the data being sent from my VPC to my S3 bucket is actually using this new secure route.

Step 7 - Update route tables

In this step, I will test whether or not my VPC endpoint is working because that's how I'll be able to tell if my instance is actually using the endpoint to acces my S3 or if its just using the public internet still.

Step 8 - Validate endpoint conection

In this step, I will be accessing my S3 from my VPC via the endpoint to verify that everything is indeed working as it should be.

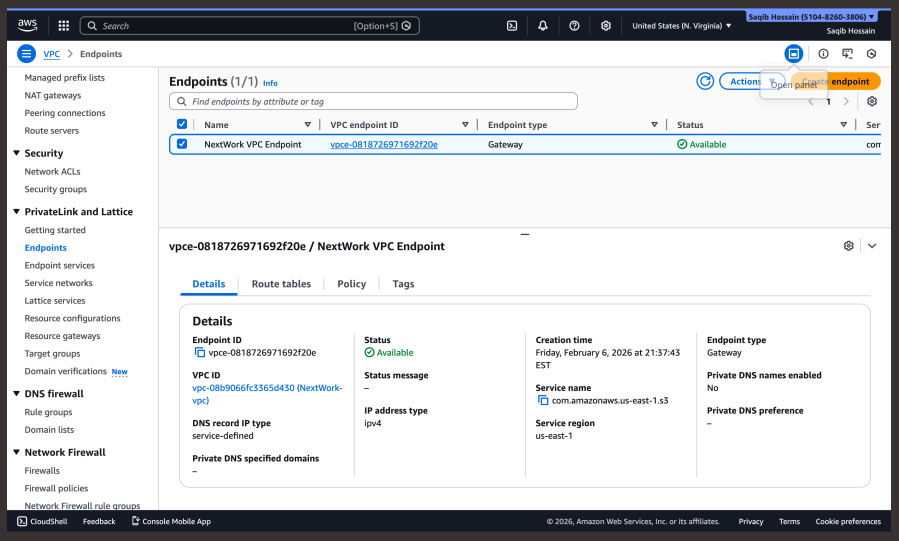
saqibh49@gmail.com
NextWork Student

Setting up a Gateway

I set up an S3 Gateway, which is a type of endpoint that supports only S3 and DynamoDB.

What are endpoints?

An endpoint is a path on a VPC's route table that connects directly to outside AWS services without using the open internet.



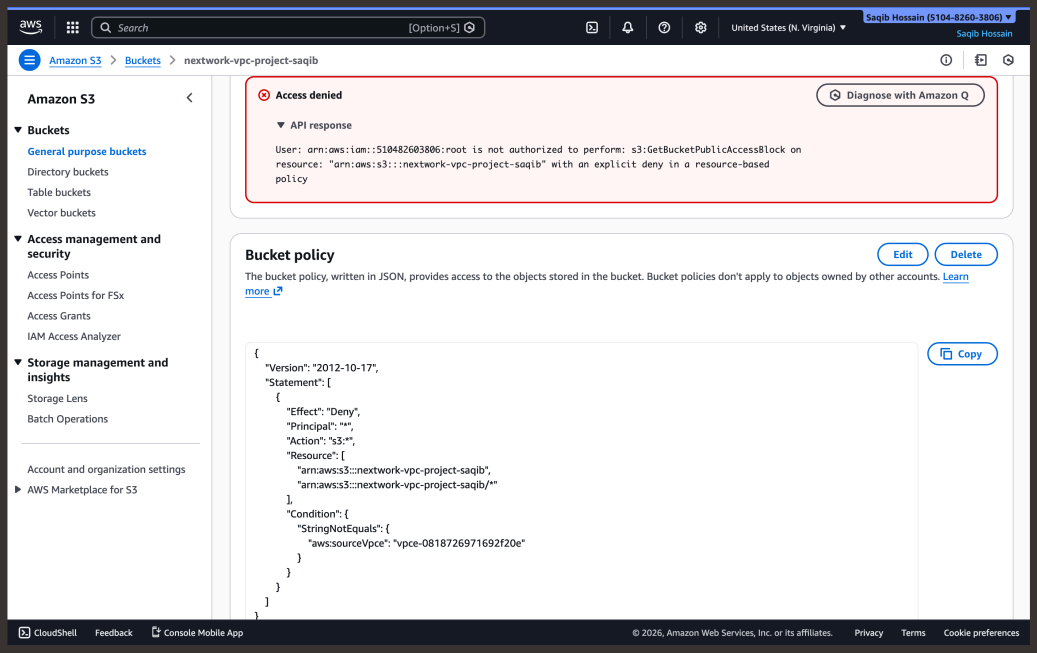
saqibh49@gmail.com
NextWork Student

nextwork.org

Bucket policies

A bucket policy is an IAM policy specifically for an S3 bucket rather than for a user or role.

My bucket policy will block all traffic that isnt coming from my VPC gateway.

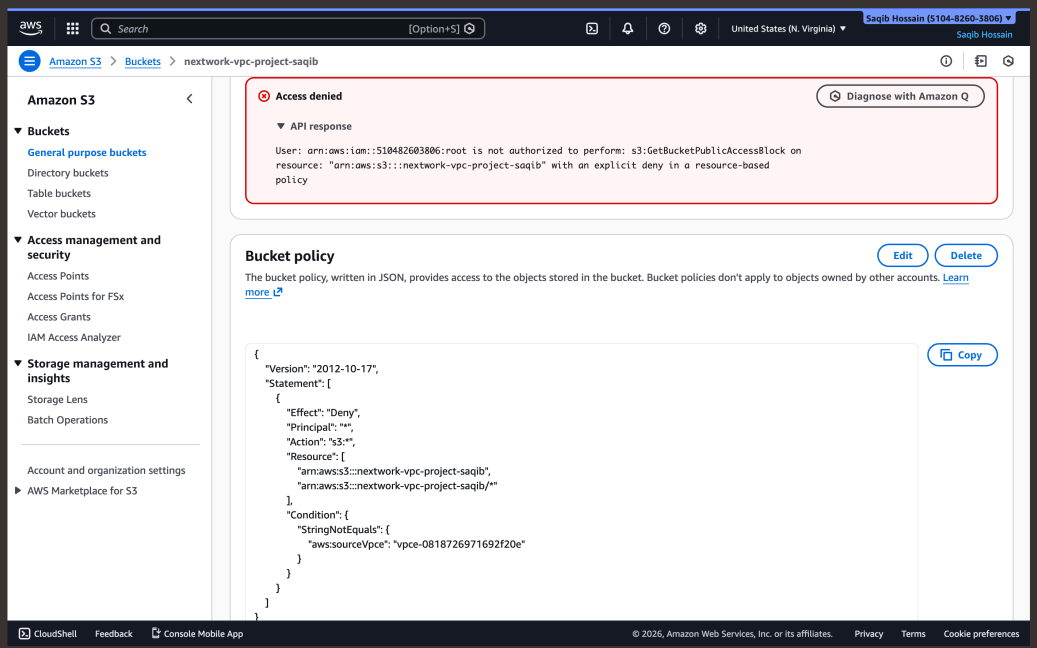


saqibh49@gmail.com
NextWork Student

Bucket policies

Right after saving my bucket policy, my S3 bucket page showed 'denied access' warnings. This was because my policy is blocking all access unless it is through my vpc endpoint, including access through the aws management console.

I also had to update my route table because without a connection between my route table and my endpoint, there's no way for my VPC to send traffic through the endpoint.

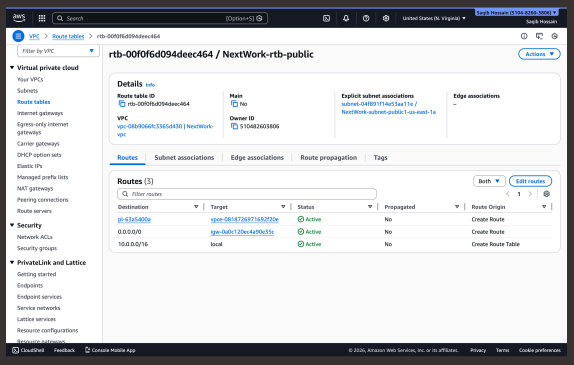


saqibh49@gmail.com
NextWork Student

Route table updates

To update my route table, I added the route by associating my bucket policy with my public route table.

After updating my public subnet's route table, my terminal could return the contents of my S3 bucket.

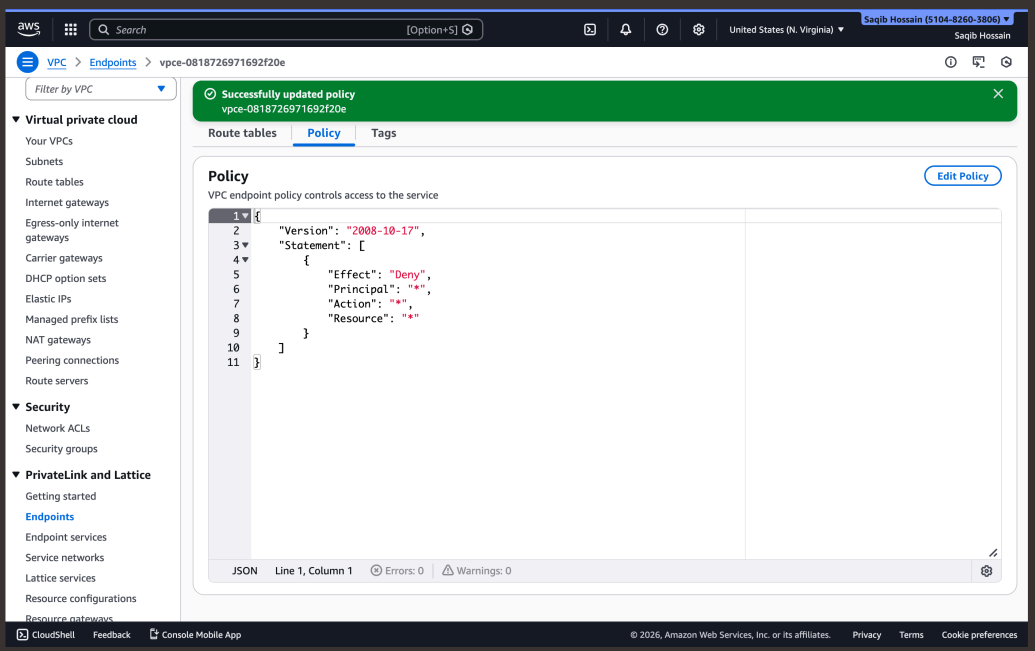


saqibh49@gmail.com
NextWork Student

Endpoint policies

An endpoint policy is a set of rules for what kind of traffic is allowed to pass through an endpoint.

I updated my endpoint's policy by setting the allow traffic policy to ddeny traffic. I could see the effect of this right away, because in my EC2 instance connect, I could no longer see the contents of my S3 bucket.



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects