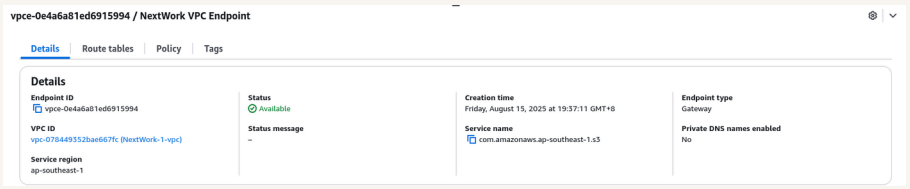
nextwork.org

VPC Endpoints

Sean Calderon



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a GOAT! It is super useful if you want to build secure and scalable network infrastructure.

How I used Amazon VPC in this project

For today's project, I used Amazon VPC to create S3 Gateway to direct route my traffic coming from my VPC.

This project took me...

I took this project almost 45 minutes and it was rewarding to see policies taking in effect almost immediately and effectively and also fulfilling to setup fully working gateway as an endpoint to my VPC.

In the first part of my project...

Step 1 - Architecture set up

In this step, I am going to setup my infrastructure which is the foundations of today's project - a VPC, EC2 instance and S3 bucket.

Step 2 - Connect to EC2 instance

In this step, I am going to connect directly to my EC2 instance.

Step 3 - Set up access keys

In this step, I am going to give my EC2 instance access to my AWS environment.

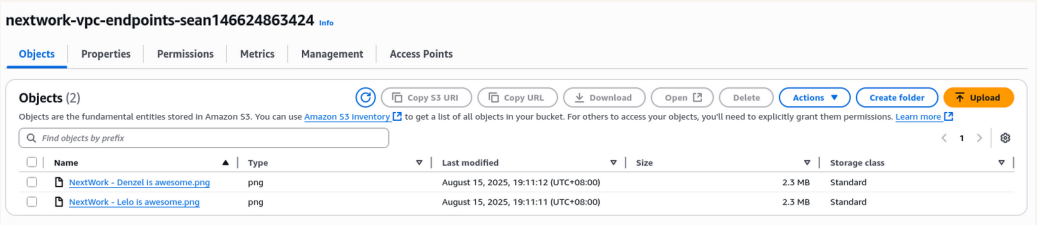
Step 4 - Interact with S3 bucket

In this step, I am going to my EC2 Instance again and access my S3 bucket through it.

Architecture set up

I started my project by launching the core service of this project which is the VPC, and then spinned up an EC2 instance.

In this step, I set up a new bucket with name nextwork-vpc-endpoints-sean146624863424 and then I uploaded two files into my shiny new bucket.



Access keys

Credentials

To set up my EC2 instance to interact with my AWS environment, I configured access keys with a command "aws configure"

Access keys are simply credentials that are needed to log in to AWS infrastructure.

The secret access key is like the password that pairs with your access key ID (your username). You need both to access AWS services. Secret is a key word here - anyone who has it can access your AWS account, so I need to keep this away from anyone.

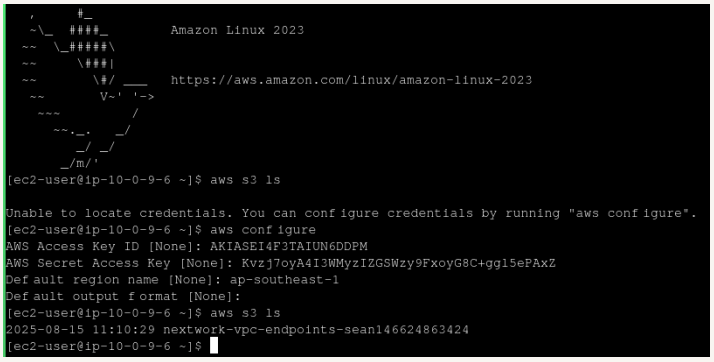
Best practice

Although I'm using access keys in this project, a best practice alternative is to use AWS CloudShell - a browser based CLI or use AWS CLI v2 and then enable authentication through IAM Identity Center.

Connecting to my S3 bucket

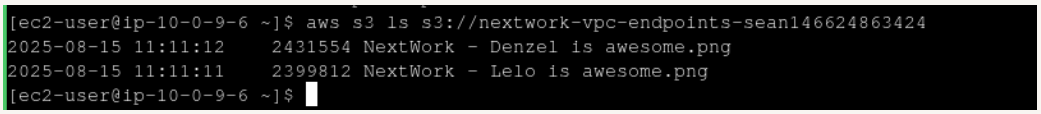
The command I ran was "aws s3 ls" and the command is used to list S3 buckets available.

The terminal responded with returned my S3 bucket's name. This indicated that the access keys I set up is correctly implemented.



Connecting to my S3 bucket

I also tested the command "aws s3 ls s3://nextwork-vpc-endpoints-sean146624863424" which returned lists of objects that reside on my S3 bucket.



Uploading objects to S3

To upload a new file to my bucket, I first ran the command "sudo touch /tmp/test.txt" which creates text file with a filename test that lives in the /tmp directory and created with administrative privileges.

The second command I ran was "aws s3 cp /tmp/test.txt s3://nextwork-vpc-project-sean146624863424" which is a command that will upload my txt file directly to my s3 bucket.

The third command I ran was "aws s3 ls nextwork-vpc-project-sean146624863424" which validated the file was successfully uploaded into S3 bucket.

```
[ec2-user@ip-10-0-9-6 ~]$ sudo touch /tmp/nextwork.txt
[ec2-user@ip-10-0-9-6 ~]$ aws s3 cp /tmp/nextwork.txt s3://nextwork-vpc-endpoints-sean146624863424
upload: ../../tmp/nextwork.txt to s3://nextwork-vpc-endpoints-sean146624863424/nextwork.txt
[ec2-user@ip-10-0-9-6 ~]$ aws s3 ls s3://nextwork-vpc-endpoints-sean146624863424
2025-08-15 11:11:12    2431554 NextWork - Denzel is awesome.png
2025-08-15 11:11:11    2399812 NextWork - Lelo is awesome.png
2025-08-15 11:30:37          0 nextwork.txt
[ec2-user@ip-10-0-9-6 ~]$
```

In the second part of my project...

Step 5 - Set up a Gateway

In this step, I am going set up a way for my VPC and S3 to communicate directly.

Step 6 - Bucket policies

In this step, I am going to setup a super secure bucket policy to limit my S3 bucket access's to only traffic from my endpoint.

Step 7 - Update route tables

In this step, I am going to test my VPC endpoint set up to access S3 bucket through my EC2 instance.

Step 8 - Validate endpoint conection

In this step, I am going to validate my work, and get to my EC2 instance to interact with my S3 bucket one again.

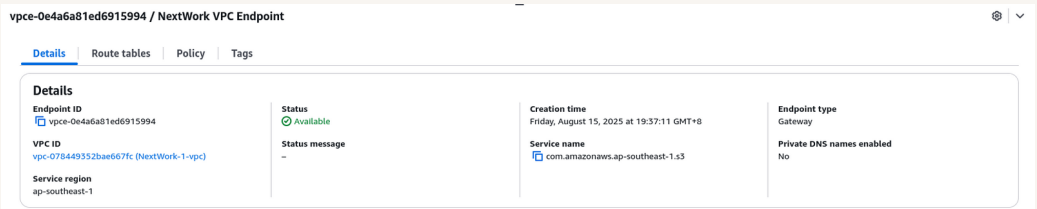

Sean Calderon
NextWork Student

Setting up a Gateway

I set up an S3 Gateway, which is a type of endpoint gateway that is specifically for S3 and DynamoDB

What are endpoints?

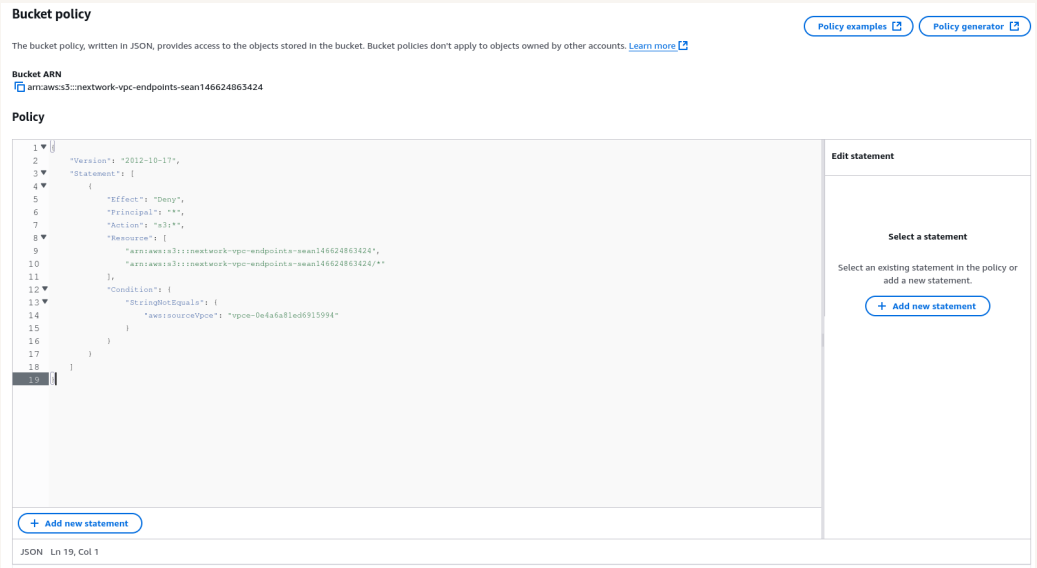
An endpoint is an entrypoint for services to directly access another services without the need of going out the internet.



Bucket policies

A bucket policy is a type of IAM policy designed for setting access permissions to an S3 bucket. Using bucket policies, you get to decide who can access the bucket and what actions they can perform with it.

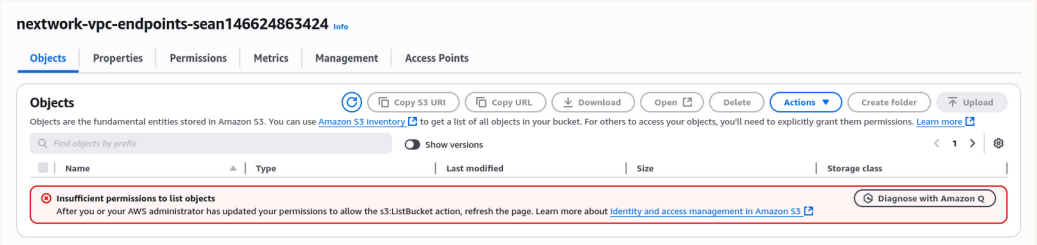
This policy denies all actions (s3:*) on my S3 bucket and its objects to everyone (Principal: "*") unless the access is from the VPC endpoint with the ID defined in aws:sourceVpce. In other words, only traffic coming from my VPC endpoint can access



Bucket policies

Right after saving my bucket policy, my S3 bucket page showed 'denied access' warnings. This was because I am accessing my S3 bucket details and properties outside my VPC which is not allowed in the policy.

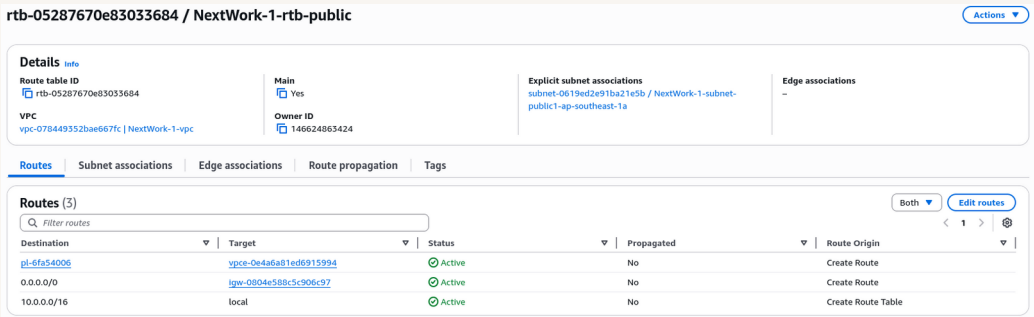
I also had to update my route table because the VPC endpoint is not associated yet with my routing table which means traffic will not be directed to the endpoint.



Route table updates

To update my route table, I added a new rule specifying the destination to S3 and the target which the traffic will be directed to is the VPC endpoint which is my gateway to the S3 bucket.

After updating my public subnet's route table, my terminal could return the list of objects that are present on my S3 bucket.



Endpoint policies

An endpoint policy is a permission based access control just like bucket policies and IAM policies.

I updated my endpoint's policy by editing the policy in the properties tab of the VPC endpoint. I could see the effect of "DENY" right away.

The place to learn & showcase your skills

Check out nextwork.org for more projects