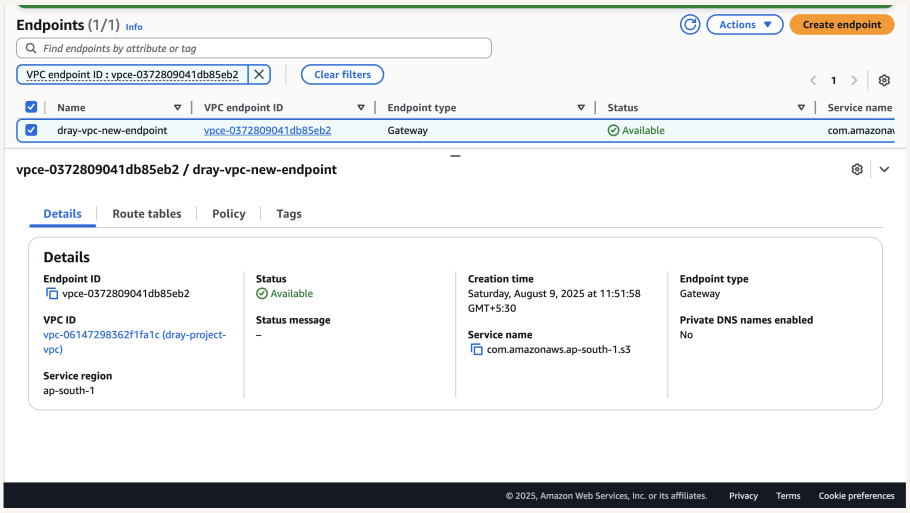
VPC Endpoints

Gaurav Balpande



G
Gaurav Balpande
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is the fundamental networking tool which is used for creation of private space within the AWS region. It is needed for security and to easily manage the resources.

How I used Amazon VPC in this project

In today's project i had learn how to interactwith Amazon S3 which is not in VPC and also to do that with the help of endpoint. For this I used tools like EC2 instance,S3,VPC endpoint and IAM roles.

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

One thing I never expected is that we can even add files with the use of EC2 instance and that too with AWS CLI.

This project took me...

it took near to 1.30 hr and it slightly hard.

In the first part of my project...

Step 1 - Architecture set up

In this step,we are going to build the infrastructure by building one VPC with instance in it. and also S3 bucket to store.

Step 2 - Connect to EC2 instance

In this step we are going to launch Ec2 instance and connect to the instance with Amazon instance connect.

Step 3 - Set up access keys

In this step we are going to build access key and password for authentication so that we can configure aws resources with the help of aws cli.

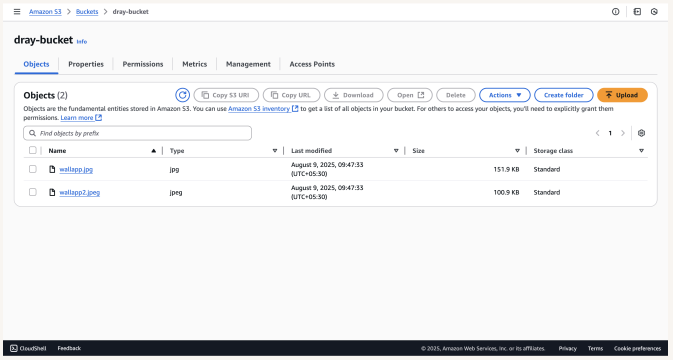
Step 4 - Interact with S3 bucket

In this step,we are heading back to EC2 instance and then will try to run command so that we can the information about Amazon S3.

Architecture set up

I started my project by launching an EC2 instance in our public subnet. This is done to create connection with S3 bucket.

I also set up the Amazon S3 bucket with two files inside it.



Access keys

Credentials

To set up my EC2 instance to interact with my AWS environment, I configured the access key and password this is because Aws cli dont have access on its own to access the AWS resources.

Access keys are like password which link access key id.

Secret access keys are like a password that pair with our access key id.

Best practice

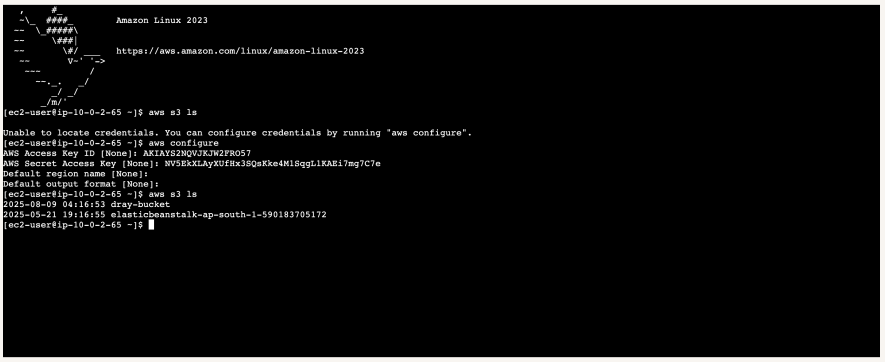
Although I'm using access keys in this project, a best practice alternative is to use IAM role.

Gaurav Balpande
NextWork Student

Connecting to my S3 bucket

The command I ran was aws s3 ls This command is used to list all the buckets in Amazon s3.

The terminal responded with name of two buckets This indicated that the access keys I set up is successfully set



Connecting to my S3 bucket

I also tested the command aws s3 ls s3://dray-bucket which returned two files name wallapp.jpg and wallapp2.jpg

Uploading objects to S3

To upload a new file to my bucket, I first ran the command sudo touch /tmp/test.txt This command creates an empty file

The second command I ran was aws s3 cp /tmp/test.txt s3://dray-bucket This command will copy the empty file to the bucket.

The third command I ran was aws s3 ls s3://dray-bucket which validated that its been copied successfully.

In the second part of my project...

Step 5 - Set up a Gateway

In this step, we are going to set the VPC endpoint to prevent acces over the internet and set to private connection.

Step 6 - Bucket policies

In this step for checking purpose we are going to block all traffic to S3 but only allow the endpoint traffic. It will help in whether endpoint is working fine or not.

Step 7 - Update route tables

In this step, we are first going to test the connection of the endpoint and if it had any error we will resolve it.

Step 8 - Validate endpoint conection

In this step,again we are going to test the connection and also will solve any issue if arrived.

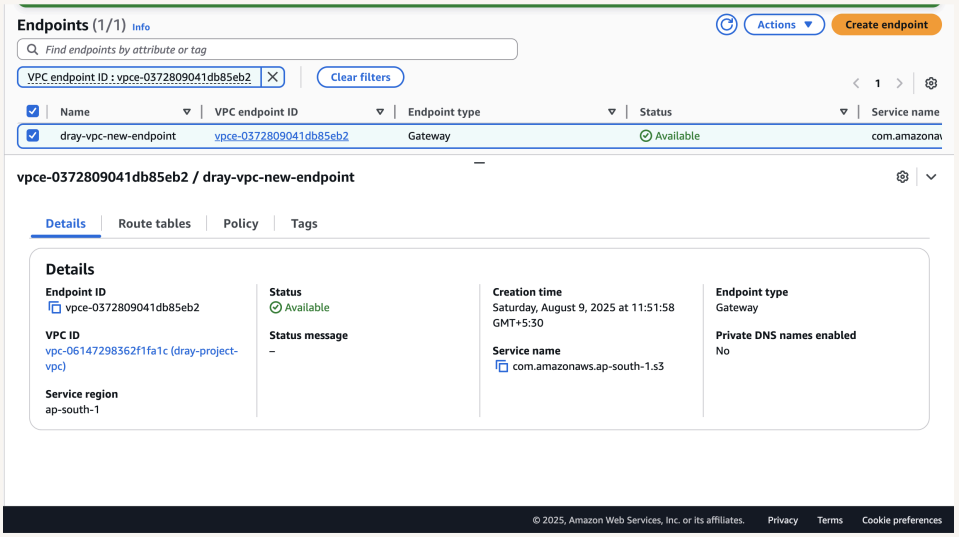
Gaurav Balpande
NextWork Student

Setting up a Gateway

I set up an S3 Gateway, which is the endpoint for Amazon S3 bucket which provide private connection between the instance and S3 bucket.

What are endpoints?

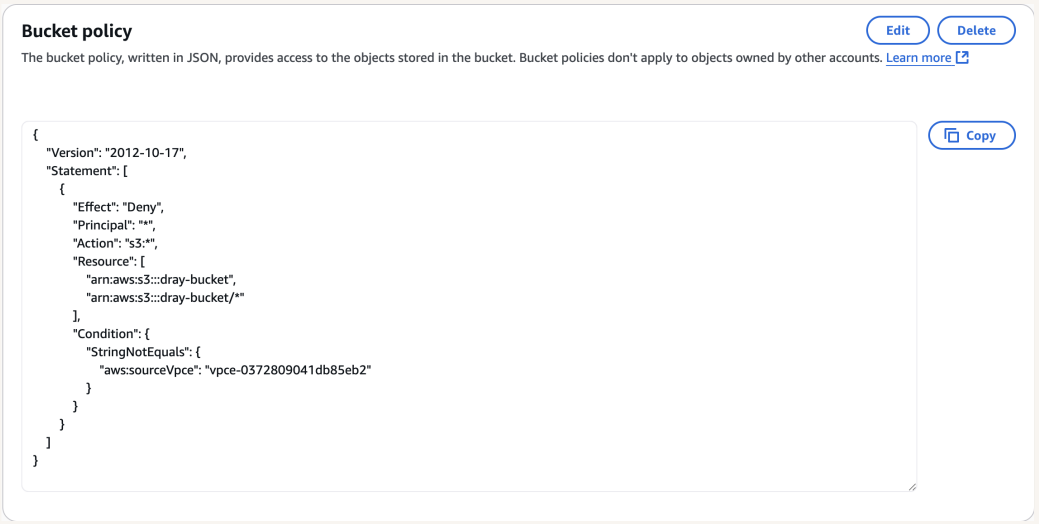
An endpoint is an service which provide direct private connection between VPC and other AWS resources.



Bucket policies

A bucket policy is like a IAM role which will allow or deny traffic based on the policy.

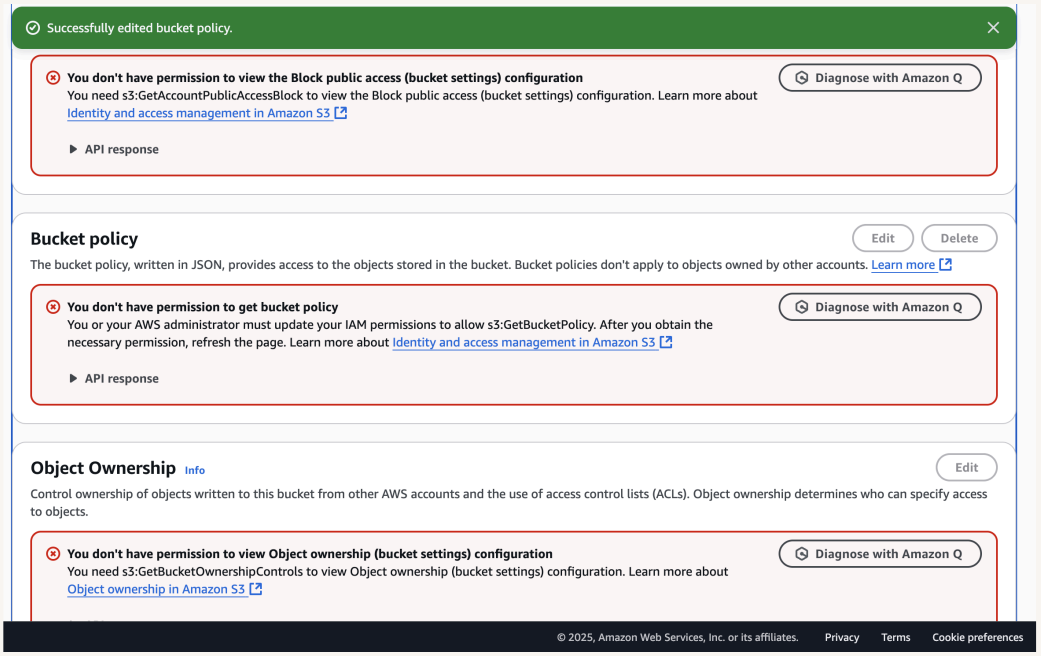
My bucket policy will block all traffic except the traffic from the endpoint.



Bucket policies

Right after saving my bucket policy, my S3 bucket page showed 'denied access' warnings. This was because we had only blocked all access except from the endpoint.

I also had to update my route table because it will give path to the endpoint.

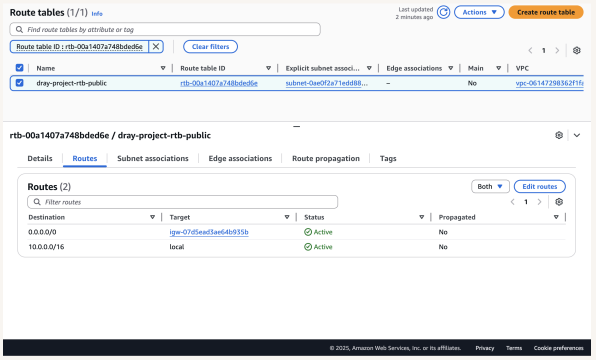


Gaurav Balpande
NextWork Student

Route table updates

To update my route table, I went to endpoint and there I assign route table to it.

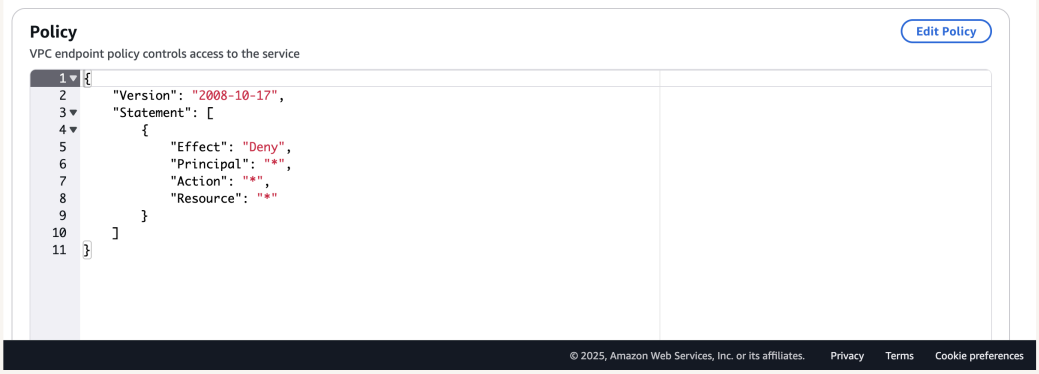
After updating my public subnet's route table, my terminal could return 2025-08-09 06:17:18 155578 wallapp.jpg 2025-08-09 06:17:19 103333 wallapp2.jpeg



Endpoint policies

An endpoint policy is a policy with the help of which we can allow or deny access easily and within less time.

I updated my endpoint's policy by changing allow to deny in action I could see the effect of this right away, because i cant access the buckey in AWS CLI



The place to learn & showcase your skills

Check out nextwork.org for more projects