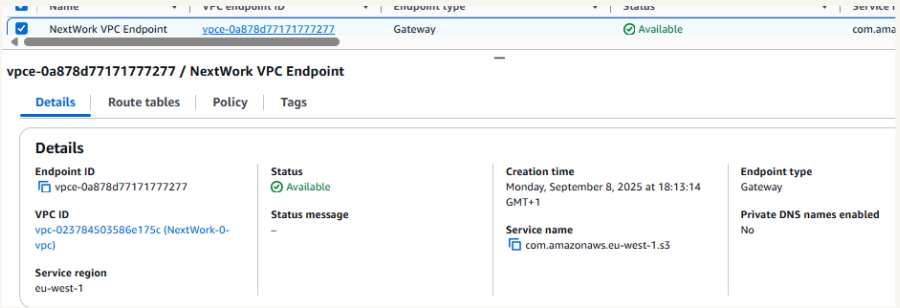
nextwork.org

VPC Endpoints

OR ucbethuel



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is Virtual Private Cloud and it is useful because it helps us create private network and connect our resources together.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC Endpoint to connect to amazon s3 resource internally without going through the public route.

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

null

This project took me...

This project took me 1 hour 32 mins.

In the first part of my project...

Step 1 - Architecture set up

In this step, I will create my PC from scratch, launch my S3 and EC2 instnace.

Step 2 - Connect to EC2 instance

In this step, I will be connecting to directly my ec2 instance.

Step 3 - Set up access keys

In this step, I will give my ec2 instance accessto aws environment using access key.

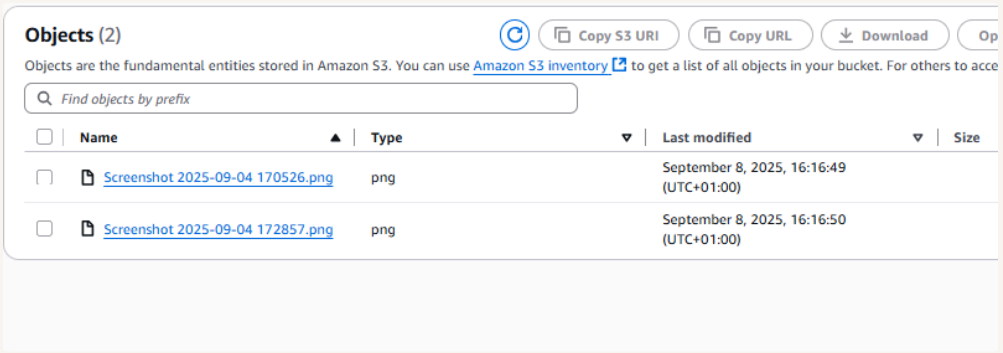
Step 4 - Interact with S3 bucket

In this step, I will ec2 instance access t my s3 aws resource.

Architecture set up

I started my project by launching an ec2 instance.

I also set up aws s3 resource



Access keys

Credentials

To set up my EC2 instance to interact with my AWS environment, I configured my aws environment by providing the details regarding 1. Access Id 2. Secret key 3. region code 4. output format.

Access keys are credentials which is needed for us to get access to aws services via CLI.

Secret access keys are like password for logging in to our aws via CLI.

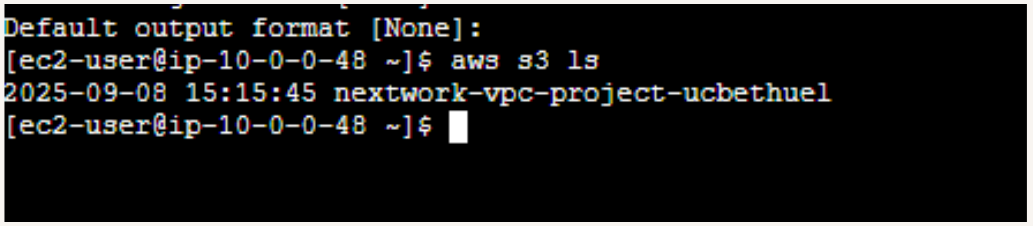
Best practice

Although I'm using access keys in this project, a best practice alternative is to use AWS CloudShell, AWS CLI V2.

Connecting to my S3 bucket

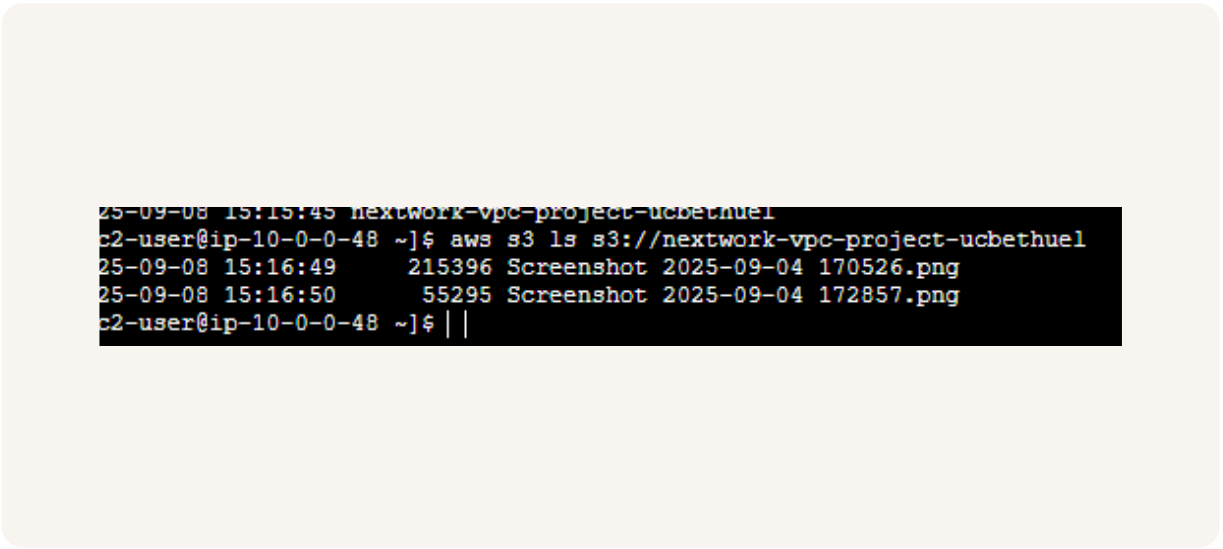
The command I ran was "aws s3 ls" This command is used to list available s3 resources linked to my account.

The terminal responded with list of available buckets. This indicated that the access keys I set up was succesfuly.



Connecting to my S3 bucket

I also tested the command aws s3 ls s3://nextwork-vpc-project-ucbethuel which returned list of object in my bucket.

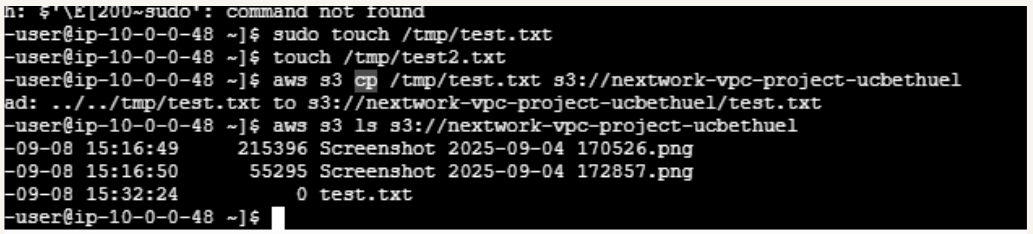


Uploading objects to S3

The first command I ran was aws s3 ls. This command is used to list s3 services connected to my account.

The second command I ran was "aws s3 cp /tmp/test.txt s3://nextwork-vpc-project-ucbethuel" This command will copy file form a source (i.e /tmp/test.txt) to a destination (i.e s3://nextwork-vpc-project-ucbethuel)

The third command I ran was s3://nextwork-vpc-project-ucbethuel which validated that the test.txt file was copied.



In the second part of my project...

Step 5 - Set up a Gateway

In this step, I will set up VPC endpoint so that my VPC can connect directly without using public routes.

Step 6 - Bucket policies

I will be validating first if our VPC endpoint actually work and in order to validate, i have to block all traffic except the ones coming within aws.

Step 7 - Update route tables

In this step, I will be testing my Bucket to see if i can still use public route or just my VPC endpoint alone.

Step 8 - Validate endpoint conection

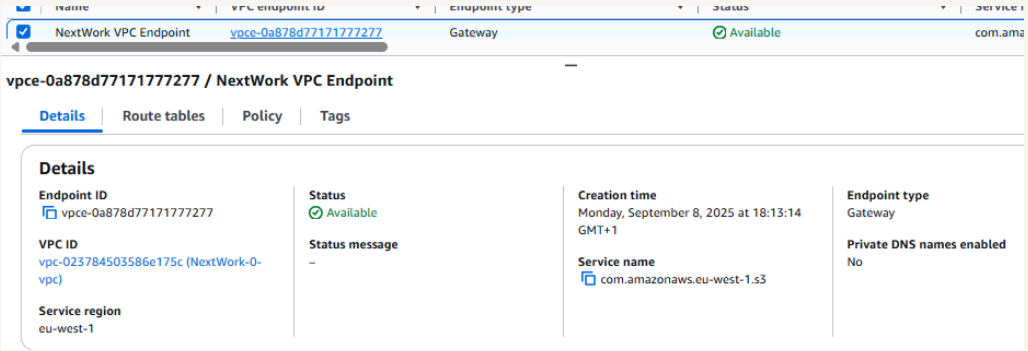
In this step, I will test my bucket one more time.

Setting up a Gateway

I set up an S3 Gateway, which allows us to connect to s3 without going through the public route.

What are endpoints?

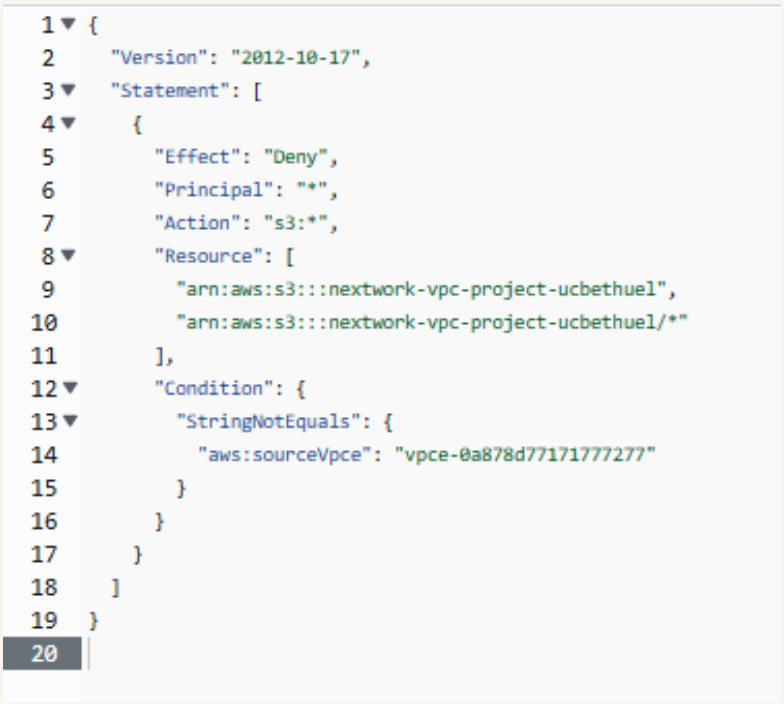
An endpoint is an internal route which connect amazon global services to our VPC.



Bucket policies

A bucket policy are rules that guide the a mangement of a buckets.

My bucket policy will deny all a endpoint access except the one coming from my VPC endpoint.

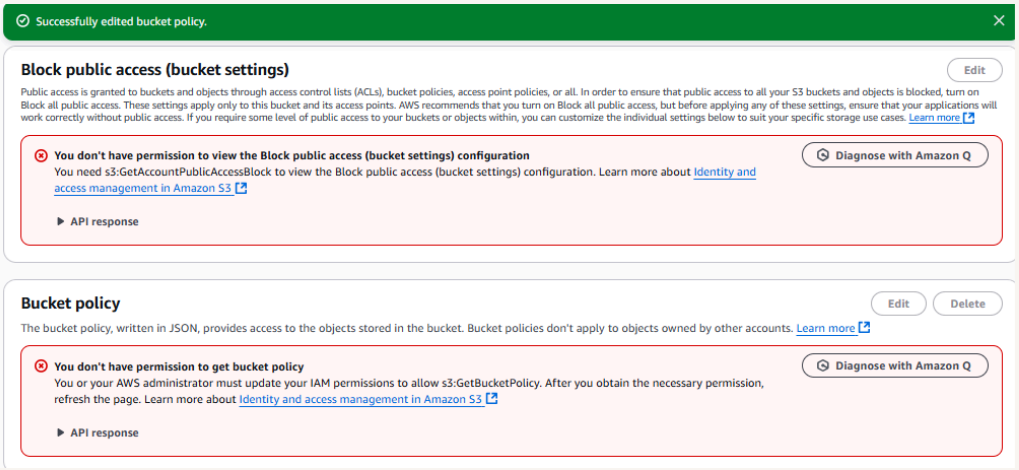


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::nextwork-vpc-project-ucbethuel",
        "arn:aws:s3:::nextwork-vpc-project-ucbethuel/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-0a878d77171777277"
        }
      }
    }
  ]
}
```

Bucket policies

Right after saving my bucket policy, my S3 bucket page showed 'denied access' warnings. This was because I blocked all kind of endpoint access, except only my VPC endpoint.

I also had to update my route table because traffic coming from my ec2 need to know the nearest place to follow in order to get to aws s3 resource.



Route table updates

To update my route table, I added it from my vpc endpoint and choose the subnet associated to ec2 instance.

After updating my public subnet's route table, my terminal could return the list of objects in my s3 buckets.

Endpoint policies

An endpoint policy is a rule that guide if an endpoint can access a resource like s3 or not.

I updated my endpoint's policy by chenging Effect key value to "Dany", and I could see the effect of this right away, even when i revise back to "Allow".

The place to learn & showcase your skills

Check out nextwork.org for more projects